UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Exact name of registrant as specified in its charter)

IronNet, Inc.

7900 Tysons One Place, Suite 400
McLean, VA

Registrant’s telephone number, including area code: (443) 300-6761

Delaware

83-4599446

(State or other jurisdiction of incorporation)

Common Stock, par value $0.0001 per share

Trading Symbol(s)

IRNT

Name of each exchange on which registered

The New York Stock Exchange

Warrants to purchase common stock

IRNT.WS

The New York Stock Exchange

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Exchange Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the past 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirement for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” “smaller reporting company,” and “emerging growth company” in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☐ Accelerated filer ☐

Non-accelerated filer ☒ Smaller reporting company ☐

Emerging growth company ☒

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant has filed a report on and attestation to its management’s assessment of the effectiveness of its internal control over financial reporting under Section 404(b) of the Sarbanes-Oxley Act (15 U.S.C. 7262(b)) by the registered public accounting firm that prepared or issued its audit report ☐

If securities are registered pursuant to Section 12(b) of the Act, indicate by check mark whether the financial statements of the registrant included in the filing reflect the correction of an error to previously issued financial statements. ☐

Indicate by check mark whether any of those error corrections are restatements that required a recovery analysis of incentive-based compensation received by any of the registrant’s executive officers during the relevant recovery period pursuant to § 240.10D-1(b). ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

As of July 31, 2022, the last day of the registrant's most recently completed second fiscal quarter, the aggregate market value of the voting and non-voting common stock held by non-affiliates, based on the closing price of $2.22 per share on July 29, 2022, was approximately $134.3 million.

There were 111,775,430 shares of Common Stock, par value $0.0001 per share, outstanding as of May 11, 2023.
DOCUMENTS INCORPORATED BY REFERENCE

Items 10, 11, 12, 13 and 14 of Part III of this Annual Report on Form 10-K are incorporated by reference from the registrant’s amendment to this Form 10-K to be filed on Form 10-K/A with the Securities and Exchange Commission no later than 120 days after the end of the registrant’s fiscal year covered by this report.

INTRODUCTORY NOTE

On August 26, 2021 (the “Business Combination Closing Date”), IronNet Cybersecurity, Inc., a Delaware Corporation (“Legacy IronNet”), LGL Systems Acquisition Corp., a Delaware corporation (“LGL”) and LGL Systems Merger Sub Inc., a Delaware corporation and wholly-owned subsidiary of LGL (“Merger Sub”), consummated the closing of the transactions contemplated by the Agreement and Plan of Reorganization and Merger, dated as of March 15, 2021, by and among LGL, Merger Sub and IronNet, as amended by Amendment No. 1 to Agreement and Plan of Reorganization and Merger, dated as of August 6, 2021 (the “Business Combination Agreement”). Pursuant to the terms of the Business Combination Agreement, a business combination of Legacy IronNet and LGL was effected by the merger of Merger Sub with and into Legacy IronNet, with Legacy IronNet surviving as a wholly-owned subsidiary of LGL (the “Business Combination”). Following the consummation of the Business Combination on the Business Combination Closing Date, LGL changed its name from LGL Systems Acquisition Corp. to IronNet, Inc.

Unless the context indicates otherwise, references in this Annual Report on Form 10-K to “IronNet,” “we,” “us,” “our,” the “Company” and similar terms refer to IronNet, Inc. (f/k/a LGL Systems Acquisition Corp.) and its consolidated subsidiaries (including Legacy IronNet). References to “LGL” refer to the predecessor company prior to the consummation of the Business Combination.
This Annual Report on Form 10-K, including, without limitation, statements under the heading “Management's Discussion and Analysis of Financial Condition and Results of Operations,” includes forward-looking statements within the meaning of Section 27A of the Securities Act and Section 21E of the Exchange Act. These forward-looking statements can be identified by the use of forward-looking terminology, including the words “believes,” “estimates,” “anticipates,” “expects,” “intends,” “plans,” “may,” “will,” “potential,” “projects,” “predicts,” “continue,” or “should,” or, in each case, their negative or other variations or comparable terminology. There can be no assurance that actual results will not materially differ from expectations. Such statements include, but are not limited to, any statements relating to our ability to consummate any acquisition or other business combination and any other statements that are not statements of current or historical facts. These statements are based on management’s current expectations, but actual results may differ materially due to various factors, including, but not limited to:

- our ability to consummate the Proposed Transaction (as defined below) with C5;
- our future operating or financial results;
- changes in our strategy, future operations, financial position, estimated revenues and losses, projected costs, prospects and plans;
- the implementation, market acceptance and success of our business model and growth strategy;
- our expectations and forecasts with respect to the size and growth of the cybersecurity industry and our products and services in particular;
- the ability of our products and services to meet customers’ compliance and regulatory needs;
- our ability to compete with others in the cybersecurity industry;
- our ability to retain pricing power with our products;
- our ability to grow our market share;
- our ability to attract and retain qualified employees and management;
- our ability to adapt to changes in consumer preferences, perception and spending habits and develop and expand our product offerings and gain market acceptance of our products, including in new geographies;
- developments and projections relating to our competitors and industry;
- our ability to develop and maintain our brand and reputation;
- developments and projections relating to our competitors and industry;
- the impact of health epidemics, including the COVID-19 pandemic, on our business and on the economy in general;
- our expectations regarding our ability to obtain and maintain intellectual property protection and not infringe on the rights of others;
- expectations regarding our status as an emerging growth company under the JOBS Act;
- our future capital requirements and sources and uses of cash;
- our ability to obtain funding for our operations and future growth; and
- our business, expansion plans and opportunities.

The forward-looking statements contained in this Annual Report on Form 10-K are based on our current expectations and beliefs concerning future developments and their potential effects on us. Future developments affecting us may not be those that we have anticipated. These forward-looking statements involve a number of risks, uncertainties (some of which are beyond our control) and other assumptions that may cause actual results or performance to be materially different from those expressed or implied by these forward-looking statements. These risks and uncertainties include, but are not limited to, those factors described under the heading “Risk Factors” in Part I, Item 1A. in this Annual Report on Form 10-K. Should one or more of these risks or uncertainties materialize, or should any of our assumptions prove incorrect, actual results may vary in material respects from those projected in these forward-looking statements. We undertake no obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise, except as may be required under applicable securities laws. These risks and others described under “Risk Factors” may not be exhaustive.

By their nature, forward-looking statements involve risks and uncertainties because they relate to events and depend on circumstances that may or may not occur in the future. We caution you that forward-looking statements are not guarantees of future performance and that our actual results of operations, financial condition and liquidity, and developments in the industry in which we operate may differ materially from those made in or suggested by the forward-looking statements contained in this Annual Report on Form 10-K. In addition, even if our results of operations, financial condition and liquidity, and developments in the industry in which we operate are consistent with the forward-looking statements contained in this Annual Report on Form 10-K, those results or developments may not be indicative of results or developments in subsequent periods.
<table>
<thead>
<tr>
<th>PART I</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Item 1. Business</td>
<td>5</td>
</tr>
<tr>
<td>Item 1A. Risk Factors</td>
<td>18</td>
</tr>
<tr>
<td>Item 1B. Unresolved Staff Comments</td>
<td>36</td>
</tr>
<tr>
<td>Item 2. Properties</td>
<td>36</td>
</tr>
<tr>
<td>Item 3. Legal Proceedings</td>
<td>36</td>
</tr>
<tr>
<td>Item 4. Mine Safety Disclosures</td>
<td>37</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART II</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Item 5. Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities</td>
<td>37</td>
</tr>
<tr>
<td>Item 6. [Reserved]</td>
<td>37</td>
</tr>
<tr>
<td>Item 7. Management’s Discussion and Analysis of Financial Condition and Results of Operations</td>
<td>38</td>
</tr>
<tr>
<td>Item 7A. Quantitative and Qualitative Disclosures About Market Risk</td>
<td>47</td>
</tr>
<tr>
<td>Item 8. Financial Statements and Supplementary Data</td>
<td>49</td>
</tr>
<tr>
<td>Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosures</td>
<td>67</td>
</tr>
<tr>
<td>Item 9A. Controls and Procedures</td>
<td>67</td>
</tr>
<tr>
<td>Item 9B. Other Information</td>
<td>68</td>
</tr>
<tr>
<td>Item 9C. Disclosure Regarding Foreign Jurisdictions that Prevent Inspections</td>
<td>68</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART III</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Item 10. Directors, Executive Officers and Corporate Governance</td>
<td>69</td>
</tr>
<tr>
<td>Item 11. Executive Compensation</td>
<td>69</td>
</tr>
<tr>
<td>Item 13. Certain Relationships and Related Transactions, and Director Independence</td>
<td>69</td>
</tr>
<tr>
<td>Item 14. Principal Accounting Fees and Services</td>
<td>69</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PART IV</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Item 15. Exhibits, Financial Statement Schedules</td>
<td>70</td>
</tr>
<tr>
<td>Item 16. Form 10-K Summary</td>
<td>73</td>
</tr>
</tbody>
</table>
SUMMARY OF RISK FACTORS

Below is a summary of material factors that make an investment in our securities speculative or risky. Importantly, this summary does not address all of the risks and uncertainties that we face. Additional discussion of the risks and uncertainties summarized in this risk factor summary, as well as other risks and uncertainties that we face, can be found under the section titled “Risk Factors” in this Annual Report on Form 10-K. The below summary is qualified in its entirety by that more complete discussion of such risks and uncertainties. You should consider carefully the risks and uncertainties described under the section titled “Risk Factors” in this Annual Report on Form 10-K as part of your evaluation of an investment in our securities:

- We have a history of losses and we may not be able to achieve or sustain profitability in the future, which raises substantial doubt about our ability to continue as a going concern.
- There can be no assurance that we will consummate the Proposed Transaction with C5 or that the Proposed Transaction (as defined herein), if consummated, will enhance stockholder value, and speculation and uncertainty regarding the outcome of the Proposed Transaction may adversely impact our business and results of operations.
- We must regain compliance with New York Stock Exchange requirements for the continued listing of our common stock.
- The event we pursue bankruptcy protection, we will be subject to the risks and uncertainties associated with such proceedings.
- If organizations do not adopt cloud-enabled, and/or software as a service (“Saas”)—delivered cybersecurity solutions that may be based on new and untested security concepts, our ability to grow our business and results of operations may be adversely affected.
- Competition from existing or new companies could cause us to experience downward pressure on prices, fewer customer orders, reduced margins, the inability to take advantage of new business opportunities and loss of market share.
- If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.
- We rely on third-party data centers and our own colocation data centers to host and operate our platform, and any disruption of or interference with its use of these facilities may negatively affect our ability to maintain the performance and reliability of our platform, which could cause our business to suffer.
- Our future success will be substantially dependent on our ability to attract, retain, and motivate the members of our management team and other key employees throughout our organization, and the loss of one or more key employees or an inability to attract and retain highly skilled employees could harm our business.
- If we are unable to maintain successful relationships with our distribution partners, or if our distribution partners fail to perform, our ability to market, sell and distribute our platform and solutions efficiently will be limited, and our business, financial position and results of operations will be harmed.
- Our business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could have an adverse effect on our business and results of operations.
- The success of our business will depend in part on our ability to protect and enforce our intellectual property rights.
- We are subject to laws and regulations, including governmental export and import controls, sanctions, and anti-corruption laws, that could impair our ability to compete in our markets and subject us to liability if we are not in full compliance with applicable laws.
- Our management has identified material weaknesses in our internal control over financial reporting and may identify additional material weaknesses in the future or otherwise fail to maintain an effective system of internal controls, which may result in material misstatements of our financial statements or cause us to fail to meet our periodic reporting obligations.
- Our international operations and plans for future international expansion expose us to significant risks, and failure to manage those risks could adversely impact our business.

ITEM 1. BUSINESS

PART I

Overview

We are Transforming Cybersecurity Through Collective Defense® using our behavioral analytics technology. We compete in the Network Detection and Response (“NDR”) category, which is a growing aspect of modern enterprise security, but which does include major competitors. Our value proposition and competitive differentiator is our IronNet Collective Defense platform (“Collective Defense”). Our founder and CEO, GEN Keith B. Alexander (Ret.), the longest serving Director of the National Security Agency (“NSA”) and Commander of Cyber Command in U.S. history, serves as a valuable business development resource for establishing relationships with larger enterprise and government buyers. The majority of our current revenue comes from our IronDefense™ and IronDome™ products which combined create the IronNet Collective Defense platform. IronDefense is a network detection and response (“NDR”) cybersecurity product intended for organizations with a more sophisticated cyber stack. The platform uses IronDefense’s artificial intelligence (“AI”), machine learning (“ML”), behavioral analytics, and operational tradecraft expertise to quickly identify specific network behaviors or events indicative of malicious threats. Enriched by our cyber tradecraft knowledge, alerts produced by our company help analysts quickly contextualize and prioritize threats that pose the greatest risks. By doing this we are able to provide clients, across a variety of industries, nation-state-level defensive capabilities to reduce cyber risk. In mid-2022, we introduced IronRadar™, an easy-to-install threat intelligence feed that enables cybersecurity teams to proactively detect and block command and control (“C2”) infrastructure before an attack, expanding our offering with a solution intended for, and obtainable by, organizations of all sizes.

We take a differentiated and potentially transformational approach to the cybersecurity problem facing every organization today. With an ever-increasing cybersecurity threat posed by advanced persistent threat (“APT”) actors, our team of experts has developed a solution that automates and scales knowledge about how APTs operate and their tactics, techniques and procedures, in order to defeat them; few individuals and even fewer companies have that knowledge or capability. Our differentiated market offering called IronDome offers users a collective defense model to help mitigate threats posed by an APT enhanced by its IronDefense platform, offering our clients new protections against an APT with its technology.

Cybersecurity has advanced from a niche technical concern to a mainstream consideration for organizations of all sizes and in all sectors. Security protection concerns are most intense where safety or life-critical consequences might arise in response to a cyber threat. Power companies, financial services firms,
healthcare companies, space development, military organizations, and government agencies thus have the greatest need for security protection, and now make considerable investments in cybersecurity. The primary security challenge in modern organizations is the complexity that has evolved in the typical business or government entity. Applications, networks, systems, endpoints, and data have experienced considerable sprawl as the costs associated with computing have decreased significantly. This is especially true for cloud-based infrastructure and SaaS-based applications, where cheap ubiquitous services are now available on-demand and for nearly every purpose imaginable.

Modern organizations must therefore develop security protections that address such growth, often delivered in the context of digital transformation initiatives. An additional complication is that hackers have been augmented by determined, capable adversaries, often funded or otherwise backed by criminal groups or nation-states. Serious consideration must thus be given to the types of protections that are necessary to defend against the threat from such capable threat actors.

An additional dimension is that the velocity associated with computing infrastructure and their associated threats has accelerated. Agile DevOps processes generate new features at increasing rates, sometimes hourly for popular services, and hackers use automated platforms to bombard targeted infrastructure with alarming intensity. Security engineers thus require controls that are automated and that address this challenge of increased speed. Manually controlled point solutions no longer stop threats.

A further complication is the massive and increasing scale associated with the types of systems operated by larger enterprise teams. Large-scale IT and network systems remove the ability for organizations to rely on manual maintenance, fixed configurations, and simple asset management. Furthermore, the visibility of assets that might be well-known by smaller organizations can only be approximated in large-scale settings. This greatly complicates the challenge of delivering security in a large-scale setting.

In response to these challenges, modern Chief Information Security Officers (“CISOs”) put considerable time and effort into designing and implementing a workable security architecture. Individual CISO-led teams—even if they focus their efforts—have come to recognize that they cannot address the cybersecurity challenge on their own. It is well-understood in the cybersecurity community that enterprise security teams need considerable external assistance, coordination and cooperative guidance.

Some of this assistance is obvious: Businesses rarely develop their own security tools, but rather buy from vendors or adjust open-source tools. Similarly, information sharing groups have emerged to support cooperative discussions between experts. It is therefore not controversial to suggest that businesses and agencies need to work together to address cybersecurity threats. The big question, instead, is how this objective can be best achieved. This is one of the challenges addressed by IronNet.

Background of IronNet

We are a global cybersecurity company revolutionizing how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing former NSA cybersecurity operators with offensive and defensive cyber experience, we integrate deep tradecraft knowledge into our industry-leading products to solve the most challenging cyber problems facing the world today. GEN Alexander founded our company in 2014 to solve the major cybersecurity problem he witnessed and defined during his tenure as former head of the NSA and founding Commander of U.S. Cyber Command: You can’t defend against threats you can’t see. Our innovative approach provides the ability for groups of organizations—within an industry sector, supply chain, state or country, for example—to see, detect and defend against sophisticated cyber attacks earlier and faster than ever before.

We have defined a new market category called Collective Defense. As the first mover in this category, we have developed our Collective Defense platform, the first, and to our knowledge, the only solution that can identify anomalous (potentially suspicious or malicious) behaviors on computer networks and share this intelligence anonymously and in real time among Collective Defense community members. Collective Defense communities comprise groups of organizations that have common risks, such as a supply chain, a business ecosystem, or across an industry sector, a state, or a country. This cybersecurity model delivers timely, actionable, and contextual alerts and threat intelligence on attacks targeting enterprise networks, and functions as an early-warning detection system for all community members.

This new platform addresses a large and unwavering compound problem: limited threat visibility for increasingly borderless enterprises across sectors and at the national level, paired with ineffective threat knowledge sharing across companies and sectors and a “go it alone” approach to cybersecurity. These operational gaps, combined with market dynamics like the increased velocity of sophisticated cyber attacks and the deepening scarcity of qualified human capital, have set our mission to transform how cybersecurity is waged.

Understanding Collective Cyber Defense

Ideally the U.S. Government could defend the nation against cyberattacks similar to what was developed for the Intercontinental Ballistic Missile (“ICBM”) missile threat. Unfortunately, the ability to enact such a defense would likely require limiting personal freedoms on the internet that Americans currently enjoy. Legislation limiting personal freedoms would likely be challenging to pass and thus the probability of that happening in the near future is low. A 2020 Cyberspace Solarium Commission report contains over 80 recommendations to address the issue of cybersecurity, with one of them being “Reshaping the Cyber Ecosystem.” That report states:

“Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit adversaries’ activities. Over time this will reduce the frequency, scope, and scale of their cyber operations. Because the vast majority of this ecosystem is owned and operated by the private sector, scaling up security means partnering with the private sector and adjusting incentives to produce positive outcomes.”

The IronNet Collective Defense platform is a means for the private sector to “raise the baseline” level of security by partnering amongst themselves to “produce positive outcomes.” This overview function is a differentiator for our portfolio of offerings, making us one of the few companies that has the ways, ends and means to enact this transformational concept due to the technical capabilities required to ensure its success.

To understand our platform and solution approach, it is best to begin with an outline of how collective defense can reduce cybersecurity risk for larger organizations. This approach benefits from many years of organizations beginning to share data through various groups such as Information Sharing and Analysis Organizations (“ISAO”). We are the first major commercial vendor to offer an end-to-end means to take full advantage of the collective concept.

Toward a Collective Cyber Defense

Businesses and agencies will only cooperate on collective cybersecurity initiatives if they see meaningful benefits with low associated risk. Admittedly, this is how almost all business decisions are made, but large-scale cybersecurity introduces an added benefit for collective defense—namely, that cyber protection schemes work much better when they involve a wider range of intelligence, visibility, and security coverage. Working together on cybersecurity thus introduces clear benefits for participants.

Nevertheless, cooperation between businesses, agencies, and other groups must address two ends of the spectrum: upside benefits and downside risks for each of the entities and groups involved. In both instances, the case can be made that, for large-scale infrastructure, both benefits and risks can cascade, perhaps even accelerating as lateral traversal of an attack occurs. That is, threats to someone else’s system, however remote, might cascade across networks and systems.

Within a large organization, collective protection across business units can have comparable benefit, particularly in companies that evolved through mergers and acquisitions, where a collective defense can help to bring together disparate data sources, defensive perspectives, and protection platforms into a common defense. Such intra-enablement within a large organization is a major focus area for IronNet.
The primary benefits of a collective defense for large-scale cyber defense, whether stretched across a sector, combined between multiple organizations, or combined across the business units of one company, include the following:

Early Warning System—An organization can develop a more effective early warning system if other groups share their indicators in real-time. Not engaging in such sharing limits the ability of a local team to capitalize on early warning that a cascading attack might be underway.

Broader Visibility—By working together with other groups, the local security team benefits from broader visibility, including an improved understanding of how local enterprise changes (e.g., Domain Name System ("DNS")-related) might cascade to other targets.

Strength in Numbers—The fact that cooperation increases visibility into a cyber threat means that organizations who cooperate with external groups are able to leverage strength-in-numbers and thereby provide better security support.

The corresponding risks that must be managed in the development of any large-scale cooperative arrangement for cybersecurity include the following:

Privacy of Shared Data—The possibility emerges that sharing information with a cooperative might result in leaked data or a serious privacy incident. For highly regulated industries, sharing with governments may also expose businesses to some regulatory risk (although this is partially mitigated by certain provisions of the Cybersecurity Information Sharing Act of 2015). If the data is not properly anonymized or otherwise does not comply with legal requirements. Controls must be in place to ensure that cooperating teams are not exposed to this risk.

Attribution of Incidents—Public attribution of an embarrassing or problematic cybersecurity incident to a sharing entity may reduce (or even remove) the willingness of that organization (and others) to share further information about vulnerabilities that might reflect poorly on their own actions. This is less an issue for collective defenses implemented across the business units of a single organization.

Competitive Relationship—The risk of one company directly assisting its competitor through participation in a collective defense scheme (e.g., AT&T assisting Verizon, or General Motors assisting Toyota) cannot be ignored. The legal and marketing teams from participating organizations would be wise to adopt the airline and energy industry’s observations that a mutual focus on safety helps every participant.

The benefits and risks of cooperation for large-scale cybersecurity across heterogeneous groups must be carefully balanced in setting up a collective defense. Too often, collectives are developed that leave participants wondering what’s in it for them, and how potential problems might be avoided. One of our main value propositions is that cooperative cybersecurity will work best when such concerns are carefully curated by a trusted provider with a world-class platform.

Role of Government in Collective Defense

One challenge federal governments have in supporting collective cyber defense is that most large businesses are multinational. This suggests that while national allegiance might be easily identified (e.g., Verizon is American, Huawei is Chinese), such allegiance must address the interests of the company’s shareholders. This emphasis is often misunderstood by government agencies who are focused exclusively on national interests.

Federal governments also have the additional role of regulating and sometimes punishing organizations not meeting their security requirements. This obligation complicates government cooperation with business on cybersecurity, at least to the extent that governments are permitted to regulate based on voluntarily shared information. Organizations would thus be hesitant to share information with a cooperative involving government if the reported incident might lead to regulatory investigation.

The biggest challenge, however, is that the majority of critical infrastructure is owned and operated by the private sector. This implies that security telemetry, indicators, and early warnings will come from the private sector, even for many military applications and defense government activities. This fact is often not understood by citizens and politicians who may demand that government step in and fix large-scale cybersecurity threats. This is usually just not practically feasible.

Government must work hard to share the information it uniquely controls, such as classified indicators that might be downgraded for sharing externally or be shared in a more limited context to defend critical infrastructure. Businesses must also recognize that their obligations extend beyond just the shareholder. This recognition that cooperative sharing is in the best interests of the organization and society in general is an important driver behind our platform offering.

Overview of our Product Offerings

The Collective Defense platform comprises two flagship products:

**IronDefense** is an advanced NDR solution that uses AI-driven behavioral analytics to detect and prioritize anomalous activity inside individual enterprises. We leverage advanced Artificial Intelligence/Machine-Learning ("AI/ML") algorithms to detect previously unknown threats that have not been identified and “fingerprinted” by industry researchers, in addition to screening any known threats, and apply our Expert System to prioritize the severity of the behaviors—all at machine speed and cloud scale.

**IronDome** is a threat-sharing solution that facilitates a crowdsourcing-like environment in which the IronDefense threat detections from an individual company are shared among members of a Collective Defense community, consisting of our customers who have elected to permit their information to be anonymously shared and cross-correlated by our IronDome systems. IronDome analyzes threat detections across the community to identify broad attack patterns and provides anonymized intelligence back to all community members in real time, giving all members early insight into potential incoming attacks. Automated sharing across the Collective Defense community enables faster detection of attacks at earlier stages.

Our Collective Defense platform is designed to deliver strong network effects. Every customer contributing its threat data (anonymously) into the community is able to reap benefits from the shared intelligence of the other organizations. The collaborative aspect of Collective Defense, and the resulting prioritization of alerts based on their potential severity, helps address the known problem of “alert fatigue” that plagues overwhelmed security analysts.

Our Collective Defense platform is largely cloud-deployed and is scalable to include small-to-medium businesses and public-sector agencies as well as multinational corporations. The Collective Defense platform was available to customers on-premise and in hybrid environments until December 2022. We provide professional cybersecurity services such as incident response and threat hunting, as well as programs to help customers assess cybersecurity governance, maturity, and readiness. Our Customer Success ("CS") services are designed to create shared long-term success measures with our customers, delivering services from other cybersecurity vendors by working alongside customers as partners and offering consultative and service capabilities beyond implementation.

Our Collective Defense platform is a subscription-based pricing and flexible delivery model, with 83.6% of our revenue for the fiscal year ended January 31, 2023 related to deployments involving our key partner, Amazon Web Services. Until December 2022, we also supported private cloud, or Hyper Converged Infrastructure ("HCI") such as Nutanix as well as on-premise environments through hardware and virtual options. To make it as easy as possible for customers to add Collective Defense into their existing security stack, we built a rich set of Application Programming Interfaces ("APIs") that enable integrations with standard security products, including security information and event management ("SIEM"), security orchestration, automation, and response ("SOAR"); endpoint detection and response ("EDR"); next-generation firewall ("NGFW") tools; and cloud-native logs from the major public cloud providers.

**IronRadar™**, a product offering introduced in mid-2022, is an easy-to-install threat intelligence feed that enables cybersecurity teams to proactively detect and block C2 infrastructure before an attack. IronRadar expands our offering with a solution intended for, and available by, organizations of all sizes. In the future, we believe this product can be primarily sold through an ecosystem of partners.

We describe our go-to-market strategy for the IronNet Collective Defense platform as driving a critical public-private partnership for cybersecurity that is needed to better secure companies, sectors and nations at a time when a siloed approach to cyber defense is no longer practical and detection and response must be nearly real-time. Our approach is to secure as partners and customers both large public sector entities, including both government, military and their supply chains, as well as
large, private sector organizations with a sophisticated cyber stack and frequently businesses that support critical infrastructure. Our goal over time is to reach a level of scale and sector diversity from organizations of similar industry sector, state, country, supply chain, or tailored business ecosystem such that as each Collective Defense community grows, so does the volume of shared data, and the value of our platform for each of those members thereby expands both technically and commercially.

Some of the world's largest enterprises, government organizations, high-profile brands, and governments trust us to protect their networks. Our customers are diversified across multiple industries including energy, communications, government, space development, financial services and healthcare. Our value proposition particularly resonates at the current time with organizations protecting critical infrastructure.

Over time we have been recognized in the cybersecurity industry by independent third-party analysts, including Gartner, Forrester, ITC, 451 Research Group, including in February 2022 by SE Labs Ltd, having received a AAA rating for Enterprise Advanced Security NDR Detection. In December 2022, we announced we had been prioritized by the United States Federal Risk and Authorization Management Program (“FedRAMP”) to pursue a Provisional Authority to Operate (“P-ATO”) from the Joint Authorization Board (“JAB”). The goal of the FedRAMP program is to grow the use of secure cloud technologies in use by government agencies and enhance the framework by which the government secures and authorizes cloud technologies. Inotio is pursuing FedRAMP High certification to help protect the government's most sensitive, unclassified data in cloud computing environments.

Industry Background

Cybersecurity trends

There are a number of key trends driving the need for a new approach to cybersecurity.

Increased velocity of sophisticated attacks

Continuously, adversaries are well-trained, possess significant technological and human resources, and are highly deliberate and targeted in their attacks. Adversaries today range from militaries and intelligence services of well-funded nation-states, to sophisticated criminal organizations motivated by financial gains, to hackers leveraging readily available advanced techniques. The breadth availability and rapid evolution of cyber attack toolkits and use of regional cloud infrastructure or compromised servers to launch attacks make it nearly impossible for security teams to keep up with cyber threats. Given sufficient amount of time and resources, a determined adversary will have the ability to breach current cyber defenses of almost any enterprise, organization, or government.

Rear-facing and insufficient tools

Gartner, an industry research firm, estimates that worldwide spending on global information security will be $186.2 billion by 2024. Even with increased cybersecurity spending, however, security outcomes have not substantially improved. With multiple headline-making breaches occurring in 2022, it is not surprising that security decision-makers are more concerned about external attacks than any other attack vector. Breaches come in various ways, however, and are much more evenly spread in frequency among external attacks, lost/stolen assets, internal incidents, and third-party providers. The lack of equally sophisticated threat intelligence sharing allowed this hack to penetrate networks more deeply, and for much longer. The evolving threat landscape has rendered traditional defense approaches incapable of protecting organizations against next-generation threats.

The current generation of security products focuses on signature-based approaches that often have limited ability to collect, process, and analyze vast amounts of data—attributes that are required to be effective in today’s increasingly dynamic threat landscape. This includes traditional and next-generation firewalls, Intrusion Detection and Prevention Systems (“IDPS”), SIEMs, and other similar tools that are designed to manage policies for network traffic and rely on rear-facing threat intelligence indicators of compromise (“IoCs”) based on IP, domains, file hashes and other signature-based intelligence from known threats. They are not fundamentally designed to detect advanced, never-before-seen, “unknown unknown” cyber threats in a timely and scalable fashion.

The borderless enterprise where the network is no longer the perimeter

Cloud, IoT and SaaS applications have expanded the attack surface and cyber vulnerabilities. According to Gartner, in 2022, 31% of all workers worldwide were remote (a mix of hybrid and fully remote), including 53% of the U.S. workforce. The reality of the borderless enterprise will fundamentally change network cyber defenses from a centralized command and control defensive strategy using traditional on-premise blocking infrastructure to a distributed detect and respond strategy that fuses different sources of telemetry data across network, endpoints, and logs into actionable intelligence using large-scale behavioral analysis for security teams to take action.

Security of qualified human capital

Even with the most sophisticated AI-based cyber technology in place, the human element of cybersecurity investigation, triage, and research plays an important role in risk reduction. As our Collective Defense platform is detecting and prioritizing anomalies, the analysts and threat hunters are ultimately deciding which alerts to triage, investigate, and manage through to response and mitigation. Organizations are consistently under-resourced in this area, however, as the ratio of the volume of network traffic versus the number of cybersecurity specialists to analyze that traffic is severely lopsided, resulting in Security Operations Center (“SOC”) staff overwhelmed and burnout. According to Gartner’s most recent predictions report on cybersecurity, by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents. The 2022 (ISC)² Cybersecurity Workforce Study, which provides two critical measures of the cybersecurity profession – the Cybersecurity Workforce Estimate and the Cybersecurity Workforce Gap suggests a global cybersecurity workforce gap of 5.4 million people, and the need for organizations to have fresh perspectives about hiring, corporate culture, job satisfaction, career pathways, professional development and the future of cybersecurity work.

Cloud impact on enterprise cyber defenses

As digital transformation has accelerated in all industries, traditional security controls implemented on companies' on-premise networks are often no longer available and often must operate differently for the outsourcing of IT infrastructure and operations to the public cloud provider. While the cloud is designed to make business easier, Management and Security Operations are different from traditional on-premise security, as the teams do not have access to the underlying networks or logs, and therefore have limited visibility of cloud infrastructure. The major cloud providers have introduced logging and basic detection using signature-based detection strategies, but these require additional third-party or custom capabilities to provide sufficient defenses. Security vendors have attempted to fill the security gaps by introducing new products for the cloud based on existing on-premise technologies, but these are often cloud bolt-ons that provide limited detection and visibility for cloud environments and are complex to deploy, difficult to scale, brittle to maintain, and costly to own.

Limitations of existing products

Existing detection and threat sharing methods have a number of limitations, including:

Legacy signature-based products

Signature-based products are designed to detect known attacks using a repository of previously identified indicators of compromise, but are not capable of detecting or responding to unknown threats. Used by network security, endpoint security, SIEMs and other standard defense-in-depth cybersecurity solutions as a core detection method, these signature-based detections have resulted in many significant breaches due to the failure of legacy defenses to detect a previously unknown or modified version of a previously known attack. While current technologies remain essential, there were several noteworthy breaches in 2022, including ransomware attacks against schools and colleges, as well as healthcare and technology companies like Twitter (Jun 2022) and Uber (Sept 2022), and it is not surprising that security professionals are most concerned with attacks that can evade traditional defenses.
The following diagram depicts several differences between legacy approaches and our new approach:

First generation network-based behavioral analysis products
First generation network-based behavioral analysis products provide a basic level of outlier detection using Bayesian analysis or other statistical methods to identify obvious patterns in small networks. Often marketed as AI solutions, these solutions lack the scale, correlation, or analysis capabilities needed to detect threats hiding in plain sight within networks commonly seen at mid-sized or larger enterprises with thousands of devices, hundreds of applications, multiple physical sites, and multi-cloud architectures.

Traditional network infrastructure providers offer infrastructure monitoring products designed to identify network bottlenecks and other network reliability or performance issues. Increasingly, these vendors have added bolt-on cybersecurity capabilities that can provide security teams’ networks with asset discovery and some network visibility, but they struggle with the algorithmic analysis needed to detect new and unknown threats with high fidelity or the forensic capabilities required by security operations teams to investigate, triage, and respond to an identified network anomaly.

Threat intelligence sharing products
Threat intelligence products are designed to share massive amounts of non-specific signature-based IoCs that commonly focus on IP addresses and domains of known threats and often only after a substantial period of time by the contributing organization. The lack of timeliness or specificity to an enterprise severely limits the effectiveness of the shared information from a cyber defense perspective. By the time this information is shared, usually weeks or months after an attack, a sophisticated attacker only needs to slightly modify their methods by changing their attack infrastructure to enable them to bypass cyber defenses of their targeted enterprises, industries, or nations.

Information Sharing and Analysis Centers (“ISACs”) and other threat sharing groups
Threat sharing groups emerged more than 20 years ago as a way for security teams to work together to collect, analyze, and share actionable threat information within their member communities. We believe this is a substantial step in the right direction; however, threat sharing in these groups relies largely on signature-centric threat intelligence platforms that struggle with timeliness and specificity of their intelligence or ad hoc manual forms of communication, such as email and only with a subset of security defenders with whom an analyst has a personal relationship. ISACs and similar groups are the right organizations, but they need technological solutions that enable them to share contextual, relevant, and timely information in real time across the full community.

Creating a new market segment: Collective Defense
We are creating a new market category with Collective Defense. With our Collective Defense platform, we developed the first and, to our knowledge, the only solution that can identify and rate anomalous behaviors on the network and share this anonymized threat intelligence among Collective Defense community members (who may comprise a supply chain, state, or country) as an early-warning system for all.

The power of Collective Defense is that multiple companies can essentially work as a team to detect and defend against attackers early in the network threat intrusion cycle. This differentiated approach allows customers to:

Gain real-time visibility across the threat landscape
Our Collective Defense platform leverages proven behavioral analytics, ML, and AI techniques across anonymized participant data to identify stealthy, sophisticated threats that otherwise may be missed by an individual enterprise and signature-based tools. The platform has been designed to deliver real-time visibility of cyber threats targeting supply chains, industries, regions, or any custom IronDome Collective Defense grouping.

Reduce impact of cyber attacks with help from fellow cyber defenders
Our Collective Defense ecosystem acts as a collaboration hub to enable participants to automatically share real-time detections, triage outcomes, threat indicators, and other insights with members of their Collective Defense group. When suspicious behaviors are identified by any member, IronDome automatically shares a proactive warning to all members at machine speed so each member can prioritize their defense against the identified cyber threat.

Improve effectiveness of existing cybersecurity investments
Threat intelligence is valuable, actionable, and relevant only when received in time, before a threat enters a network. Our innovative collective threat intelligence provides immediate alerts at machine speed and context into urgent threats, enabling organizations to prioritize threats and build a proactive defense. This information can be used by a customer’s existing network, endpoint, or other security tools to identify and stop adversaries from retargeting their attack.

The following diagram depicts several differences between legacy approaches and our new approach:
Our Solution: The IronNet Collective Defense Platform

Our anonymized IronNet Collective Defense platform comprises two tightly integrated proprietary technologies: Our NDR solution, IronDefense, and our innovative collective threat-sharing solution, IronDome. Our platform offers a unified set of technologies that powers a wide range of network behavioral detection, security operations, real-time threat landscape visibility, threat sharing, and peer SOC-analyst collaboration capabilities. By focusing on cloud deployments, we are able to more rapidly and cost-effectively deploy in our customers’ environments, with 83.6% of which by revenue were in the public cloud as of January 31, 2023. Our expanding set of open APIs and ecosystem integrations enable us to add new sources of data for behavioral analysis and Collective Defense sharing and collaboration to detect and stop targeted cyber attacks.

Armed with elite detection capabilities and combined offensive operator experience at the highest level of the U.S. government, our founders set out to build a behavioral analytics solution to detect threats heading toward, or already in, the network. A growing portfolio of proprietary analytics forms the backbone of IronDefense. However, while effective in detecting unknown anomalies, behavioral analytics by itself is insufficient in modern, noisy networks where anomalies are common and can lead to a high number of false positives. For many NDR vendors in the industry, the solution is to tune their analytics to be less sensitive in order to deliver reduced false-positive rates at the expense of letting true positives into the network. We undertook a different strategy to meet this challenge. We introduced our expert system scoring algorithms, supported by our elite cyber hunters, to increase IronDefense’s detection specificity while preserving the sensitivity of its analytics.

Powered by IronDefense’s threat detections, IronDome, which we introduced in 2018, is the foundation of our Collective Defense platform, a purpose-built, cloud-native, and holistic platform that is capable of defending, analyzing, and correlating threats from various sources. It delivers timely, actionable, and contextual insights to attacks targeting an enterprise and, from there, is able to provide early warning to all members of the Collective Defense ecosystem.

The differentiated value of our Collective Defense platform is its ability to build a dynamic, comprehensive picture of the threat environment, much like radar for cyberspace, based on real-time, anonymized alert correlation across any participating member environments. It also provides situational context and peer insights for greater visibility and context of the threat landscape at any given time.

In August 2022, we announced our membership in the Joint Cyber Defense Collaborative (“JCDC”) and an agreement with the Cybersecurity and Infrastructure Security Agency (“CISA”) to share information from our Collective Defense platform to help the agency defend against increased global cyber threats. In February 2023, we formalized a new public sector partnership establishing a communications channel between our threat analysts and the DoD. The channel is intended to facilitate active collaboration of known and emerging threats, enabling us to inform the DoD of threat activity in near real time and vice versa. Through this public-private partnership, our anonymized IronDome data, in addition to our IronRadar visibility into key threat related C2 Server findings, is an important advancement of our collective defense mission.

Correlated alerts for threat detection earlier in the intrusion cycle

We are not aware of any other vendor in the market with a similar approach to cybersecurity. Even though community members bring disparate network environments, such as cloud, on-premise or hybrid, to the Collective Defense ecosystem, correlated threats stand out given that the adversarial behaviors are typically consistent, no matter who the target is.

Our Collective Defense platform comprises two flagship products:

**IronDefense**

IronDefense is an advanced NDR solution that provides behavior-based and AI-driven analytics at the network level to detect anomalous activity at individual enterprises and prioritize the highest threats in a company’s network. We leverage novel AUM algorithms to deliver high-fidelity analytics required to detect previously unknown threats. In addition, we provide advanced enrichment techniques via IronDefense’s Expert System, which has been designed to achieve high efficacy levels, low false positive rates, and improved visibility compared to legacy approaches. This is all done at network speed and cloud scale.

Most current cybersecurity tools focus on detecting the final “action-on-target” step of an intrusion. At this stage, identification is easier but the insights come far too late to stop attackers from getting into positions in the network to exfiltrate data, steal IP, or accomplish other malicious objectives. IronDefense uses advanced analytics based on metadata from the traffic in the customer’s network to identify anomalous activity earlier in the intrusion kill chain.

Key components of IronDefense include:
IronDefense behavioral analysis engine
IronDefense leverages behavior-based and correlation-based detections to identify threats targeting industries and companies earlier in the intrusion cycle, and to identify the underlying behavior and methods to counter unknown threats, or customizations that attackers will implement to target companies in the future. Our behavioral analytics are built upon algorithms that form the foundation of our patented IronDefense platform. They are computationally designed to understand normal network behavior by applying tests to create a benchmark of standard, acceptable traffic patterns in the network. Detected anomalies are grouped with similar instances of traffic behavior to minimize alerting and to aggregate events within the customers' networks. IronDefense enhancements in March 2022 include the ability to detect malicious payloads, allowing for better protection of managed and unmanaged devices from malware, ransomware, and APTs.

IronDefense Expert System
IronDefense includes an Expert System that automates security operations playbooks of how top cyber operations hunters leverage contextual data and other sources of telemetry data later on in the detection and response process and applies it to the risk scoring of anomalies detected by its behavioral analysis. This enables us to preserve IronDefense's detection accuracy without sacrificing the sensitivity of its algorithms by leveraging the wisdom of our elite cyber hunters triaging thousands of alerts from real-world environments. Our Expert System also alleviates the “alert fatigue” that plagues every SOC, by minimizing the tedious steps in an investigation, reducing alert fatigue and allowing security teams to focus on responding to high risk detection in their environments. The Expert System is continually optimized through machine learning from anonymized triaged outcomes by our cyber hunters using IronDefense.

IronDefense correlation threat engine
Threat analysts and hunters spend a significant portion of their time triaging individual alerts by identifying corroborating evidence and related information. In March 2022, we launched a new threat correlation engine for the automated correlation of detections and alerts. The threat engine models adversary attack techniques and pre-correlates anomalous activity by threat categories to improve risk scoring and alert prioritization, as well as to dramatically reduce alert load. This system leverages a multi-pass system that first optimizes for detecting as many potential instances of a particular type of threat activity and enriching detections with threat intelligence and other external and internal data sources to optimize for detection precision. Events are further aggregated by entity information, attack stage identification, and time sequence data to deliver a timeline of an attack and scored by risk to the enterprise.

IronDefense threat hunting interface
IronDefense includes a threat hunting interface built by our elite cyber hunters to empower security operations teams to conduct detailed investigative workflows and forensic analysis of threats detected by IronDefense. The hunting interface empowers security analysts to investigate across all raw traffic, network metadata, logs, telemetry data, and collective threat intelligence captured by IronDefense, all the way down to full-packet capture of individual network flows. In March 2022, we enhanced the platform’s hunt panel for extended hunt capabilities, expanding the investigation window to 30, 60, and 90 days (per individual customer service level agreement) over metadata and the associated packet capture (“PCAP”) data. This capability offers IronNet customers a fully integrated hunt platform designed for easy pivoting from an isolated alert down to the metadata and full PCAP associated with that alert, providing more time to respond and triage based on longer-term historical analysis and historical context.

IronDefense sensors
IronDefense sensors are cloud, virtual, and physical sensors that are deployed at the network perimeter to ingest “north-south” traffic within internal networks to provide “east-west” traffic visibility across an enterprise. Cloud sensors are available for public cloud environments to ingest raw traffic data directly from Infrastructure-as-a-Service virtual networks from Amazon Web Services (“AWS”), a major cloud provider. The sensor extracts rich network session metadata from the raw traffic and sends it to our behavior analysis engine for processing and expert system validation. The IronDefense sensors also continuously collect full raw traffic packet capture for inspection during hunting operations.

IronDefense direct data ingest
IronDefense has the ability to utilize a wide-range of data types and telemetry data directly from existing sources. These data sources include standard protocols such as DNS, HTTP/S, or Active Directory; common network log formats such as BRO/ZEEK or NetFlow; Cloud Provider logs such as AWS VPC, AWS CloudTrail or Microsoft Azure NSG logs; and application logs such as Office 365.

IronDome
IronDome is a threat-exchange solution that facilitates a crowdsourced-like environment in which the IronDefense findings from an individual company are automatically and anonymously exchanged within groups of related entities, such as portfolio companies, supply chains, industries, or nations, for correlation and further analysis. IronDome analyzes threat detections across companies to identify broad attack patterns and provides anonymized intelligence back to all customers in real time, serving as an early warning system for all.

IronDome enables Collective Defense member enterprises to actively exchange individual anonymized cyber anomalies at machine speed across a community of public-private peers. This capability allows companies to identify stealthy attackers earlier in the attack cycle when many of their methods fall below the threshold of detection at a single company by allowing companies to aggregate data and run higher-order analysis across industry data.

Key components of IronDome include:
IronDome Collective Defense communities
IronDome threat exchange is organized by communities of enterprises based on their business ecosystem, industry, region, or nation. Enterprises can be members of multiple communities based on their sharing preference and threat sharing needs. As customer adoption grows, the network effect of each additional enterprise participating in IronNet’s Collective Defense platform will amplify the breadth and depth of its dataset and intelligence.

IronDome collective threat intelligence exchange
IronDome links together communities of enterprises to provide contextual insights into the threat landscape. Machine and human intelligence is shared in real time across the community by threat correlations, as well as outcomes and insights related to how various analysis at different enterprises rated and triaged similar threats in their environment. Real-time feedback of these insights delivers enhanced threat landscape visibility and detection insights that allow members to immediately react to active threats targeting their industry and to adjust their defenses to combat the threat.

IronDome Cyber Radar View
IronDome creates a radar-like view of cybersecurity that links private and public sector stakeholders in their Collective Defense community. The dashboard provides an anonymized real-time view of threats targeting an enterprise’s business ecosystem, supply chain, industry, or region.

Called Collective Defense communities, spearheaded by a “cornerstone” company or organization, an IronDome could be established for a company’s business ecosystem, such as a wealth management firm with many portfolio companies; a sector-based collaborative, such as in within energy or finance), or a cross-sector formation; states and countries; and private-public sector configurations.

In each Collective Defense community, members agree to share anonymized data about threats detected on their individual networks with the collective, on an ongoing basis. This collaborative approach is designed to “flip the script” on attackers by raising the defensive capabilities of any one player. If correlated alerts and attribution based on behaviors suggest that a nation-state is involved, Collective Defense participants can voluntarily share threat information with
the government for cyber defense on a national scale as needed to defend the nation.
The Collective Defense platform is primarily deployed in cloud environments. It was historically available for private cloud, on-premise, and hybrid environments. We stopped offering these deployment options to new customers in December 2022. The Collective Defense Platform is scalable to include small- medium businesses as well as multinational corporations.

Threat Intelligence
Using information derived from the Collective Defense Platform, we also provide our customers with threat intelligence.

IronNet Threat Intelligence Rules
We augment third-party signature based detection rules with threat intelligence rules (“TIRs”) based on significant community findings. These detection rules for network, endpoint, or other security tools allow customers to proactively protect themselves against known threats through more secure controls.

IronNet Threat Intelligence Brief
The monthly IronNet Threat Intelligence Brief provides top observed threats across our Collective Defense communities. It includes significant community findings, such as network behavioral anomalies that were rated as suspicious or malicious by us and/or participant analysts, TIR, a snapshot of monthly correlated alerts, and threat research highlights.

IronRadar
IronRadar is a threat intelligence feed for organizations seeking to improve their cybersecurity posture by becoming more proactive and filling a key gap in their detection tools. It can identify threats as new C2 servers appear and before they are used in sophisticated cyber attacks. C2 infrastructures are the “brain” behind successful, malicious cyber attacks, including malware, ransomware, ransomware-as-a-service, and living-off-the-land attacks, as examples. As dangerous cyber weapons, C2 infrastructures are used by cyber criminals to communicate nefarious commands to systems inside a compromised network. IronRadar uses an innovative process that fingerprints a server and determines whether it is adversary infrastructure while those servers are being stood up, even before a cyber attack is initiated. It then enriches the data with context into purpose-built intelligence updates for proactively blocking adversarial infrastructure.

Delivered via a robust API, IronRadar can be consumed by a firewall, a SIEM, a threat intel platform, or any other threat hunting tools. In this way, it empowers SOC teams not only to ingest the data but also to automatically block the attack before it has an impact on the organization.

Using the data from the feed, SOC analysts can query their SIEM data to find communication to adversary infrastructure, reducing the mean time to threat detection and allow cyber defenders to proactively detect and block new adversary infrastructure during the critical, incipient stage. IronRadar complements the ongoing work of the IronNet Threat Research team, which regularly monitors the internet for adversary infrastructure including Cobalt Strike.

Key Benefits of Our Solutions
Our solution offers our customers several benefits, including:

- differentiated business value that includes behavioral analytics, which find threats that other tools cannot;
- real-time threat-sharing across communities; and
- value to the Collective Defense ecosystem through integrations.

Behavioral analytics that find threats that other tools cannot detect

Superior threat behavior detection to see unknown threats
IronDefense examines the network traffic itself, which is much harder for an attacker to evade or manipulate. IronDefense threat detections are based on advanced, high-fidelity analytics and AI/ML detection capabilities built by top cyber subject matter experts (“SMEs”), continuous PCAP, an expert system that applies the judgment and tradecraft playbooks of the nation’s top cyber defenders, and integrated cyber hunting (packet level visibility that improves speed and depth of investigations).

Visibility across the full enterprise to close threat detection gaps
IronDefense network detections fill the known void in threat visibility, which is being able to see unknown, novel threats on the network that other tools cannot see. The Collective Defense platform complements EDR and logs to provide comprehensive visibility across the threat landscape.

Cognitive detection, correlation, and prioritization analytics for reduced false positives
Our Collective Defense platform collects, processes, correlates, and analyzes high-fidelity data from customer networks (anonymized), threat intelligence on real-world attacks, significant community findings, and correlated alerts in the Collective Defense communities. We use this data to continually train and enhance our IronDefense behavioral analytics to increase the signal-to-noise ratio to detect new, unknown attacks with high-fidelity analytics. We automatically chain and score related events into signals to increase analyst visibility.

Data ingest at scale for a broader view of the threat landscape
IronDefense gathers data streams from a variety of sources to build a more comprehensive picture of threats. Network sensors provide streaming capture of all network packets for detection and visibility into all protocols activity. Network logs provide asset discovery and device metadata for event enrichment and contextualization. Cloud data on user activity and usage patterns only the cloud provider can collect. Security ecosystem data provide entity and user operational state which supplements network and cloud data collected.

The only real-time threat sharing capability across companies for stronger defense

The ability to defend better as a collective force
Our Collective Defense platform orchestrates threat-sharing and collaboration in real time to deliver immediate visibility and instant sharing of malicious cyber threats targeting supply chains, industries, regions, or any custom Collective Defense community to reduce impact of cyber attacks with help from fellow cyber defenders. IronDome acts as a collaboration hub to enable members to automatically share real-time detections, triage outcomes, threat indicators, and other insights with members of their Collective Defense community.

Faster warning and response capabilities
When suspicious behaviors are identified by any member, IronDome automatically shares a proactive warning to all members at machine speed so each member can prioritize their defense against the identified cyber threat. This capability allows companies to identify stealthy attackers earlier in the attack cycle when many of their methods fall below the threshold of detection at a single company by allowing companies to aggregate data and run higher-order analyses across industry data. The platform supports opt-in anonymized sharing with governments for national response when necessary.

Real-time sharing of peer insights for stronger defense
Our Collective Defense platform allows community members to share threat context, prevalence, and expert commentary about how to triage and respond, much like the Waze app for traffic, except for cybersecurity. By banding together and working together with peers, Collective Defense community members are better able to pool and optimize resources so they can achieve “defensive economies of scale” that allow them to keep up with and counteract cyber attackers.

Deep subject matter expertise to improve customer defense
We have an elite cyber operations team working directly with customers' security teams to detect, triage, and respond. Our teams are led by cyber offensive and defensive SMEs. The team composition is made up of employees that have direct intelligence community and offensive cyber experience balanced with industry professionals with experience in both enterprise security and research.

A force multiplier effect to help strained SOC teams
Our deep SME knowledge enables a multiplier effect for severely strained SOC analysts, who can leverage insights from our security analysts and threat hunters, as well as peer insights and triage outcomes from the Collective Defense community. This approach addresses the cyber talent shortage, improving the effectiveness of SOC teams and optimizing tools and human resources. Our high-fidelity analytics and threat intelligence provide autonomous identification, prioritization, and recommendation to accelerate incident investigation and the response process.

Added value to the cybersecurity ecosystem
Easy-to-use deployment for faster time to value
Our Collective Defense platform has been designed to be easy to provision, configure, and manage, working seamlessly with a suite of SIEM, SOAR, EDR, and NGFW APIs to streamline siloed security products. These integrations provide a natural complement to IronDefense and reinforce the users’ existing security infrastructures. Analysts do not need to re-learn anything and can see detections from a single view.

Security for any environment
We have historically provided security protection across cloud, on-premise, and virtual environments to support customers with different needs; however, 83.6% of deployments by revenue as of January 31, 2023 were in the public cloud. Our public cloud partner is AWS. The on-premise deployment option is no longer offered as of December 2022 and we are working to transition legacy customers to our cloud-based solution.

Improved effectiveness of existing security investments
IronDefense automates many of the time-consuming threat discovery and investigation steps and indicates the severity of anomalous activity. Our customers’ analysts can make decisions in a shorter amount of time.

Industry Recognition, Designations, and Certifications
In February 2022, we were tested by SE Labs Ltd., a private, independently-owned and run testing company that assesses security products and services, and received their highest rating (AAA) for Enterprise Advanced Security - NDR Detection.

In March 2022, we were named by the U.S. Department of Homeland Security as a member of the CISA recently formed JCDC. We have collaborated with CISA for a number of years with key innovations in the new generation of cybersecurity public-private partnerships, including when as an initiating member in 2018 in the Cyber Information Sharing and Collaboration Program.

In December 2022, we announced we had been prioritized by the United States Federal Risk and Authorization Management Program (“FedRAMP”) to pursue a P-ATO from the JAB. The goal of the FedRAMP program is to grow the use of secure cloud technologies in use by government agencies and enhance the framework by which the government secures and authorizes cloud technologies. We are pursuing FedRAMP High certification to help protect the government’s most sensitive, unclassified data in cloud computing environments.

Department of Homeland Security Continuous Diagnostics & Monitoring
We are registered with The Department of Homeland Security (“DHS”) Continuous Diagnostics & Monitoring (“CDM”) program recognizing cybersecurity tools and sensors that are reviewed by the DHS program for conformance with Section 508, federal license users and CDM technical requirements. We also received two separate acceptances/approvals for the DHS CDM Approved Products List for IronDefense (IRO-0002-20180103) and IronDome (IRO-0004-20180405).

GDPR-compliant
We are committed to data privacy and are compliant under the European Union (“EU”) General Data Protection Regulation (“GDPR”).

ISO/IEC 27001
ISO 27001 is an international standard for information security management systems. An ISO 27001 certification demonstrates that we have addressed the following areas: security policy, organization and information security, asset management, human resources security, physical and environmental security, communication and operations management, access control, information systems acquisition, security incident management, business continuity management, and compliance.

SOC2 Type II
We are also SOC2 Type II certified, demonstrating the operational effectiveness of our controls to meet the criteria for the security, availability, confidentiality, and processing integrity principles of the SOC2 standard.

Our Technology
Cloud-native architecture
Our platform is designed to be secure, highly scalable, redundant, resilient, and high-performing. Delivering from the cloud is intended to enable agility, ease of use, and flexible detection of threats within individual enterprises and the correlation and sharing of those insights with their broader Collective Defense communities.

Flexible architecture for all enterprise networks
Our Collective Defense platform enables enterprises to add behavioral detection and Collective Defense to their on-premise, cloud, or multi-cloud infrastructure. Our platform can monitor workloads in major public cloud providers and on-premise physical and virtual networks from a single platform. Our Collective Defense platform can monitor network traffic and raw traffic in AWS or leverage existing logs to detect threats targeting their cloud infrastructure. With us, enterprises can apply the power of IronNet Collective Defense to their IT infrastructure and share collective threat intelligence with their Collective Defense community to detect threats targeting their community.

APIs/integrations
The Collective Defense platform and architecture is built around a rich set of APIs intended to efficiently and effectively complement and expand a
customer’s existing security infrastructure, such as SIEMs, EDRs, NGFWs, IT service management (“ITSM”) workflow tools, and other common cybersecurity tools. The platform includes the ability to query and interact with these tools, allowing customers and partners to integrate its detection into their security operations and to execute native response against detected threats. By connecting existing security systems to the IronNet Collective Defense platform, we allow our customers to drive higher efficiencies and value from their security investments. For example, we integrate with CrowdStrike to provide 1-click containment and can leverage CrowdStrike information to provide host details in the IronDefense Threat Hunting interface to deliver a seamless security operations experience across network and devices.

Data center operations
The Collective Defense platform utilizes a combination of global and customer infrastructure to deliver the solution. Customers can choose a variety of deployment options for their own enterprise however global and Collective Defense community level information is hosted in AWS data centers located in the United States and regional AWS data centers to support our international business. Our technology infrastructure, combined with the use of AWS resources, provides us with a distributed and scalable architecture on a global scale.

Our Services

Cyber Operations Center (“CyOC”)
IronDefense customers can extend their SOC with our dedicated CyOC team, which comprises expert offensive and defensive cybersecurity operators with experience defending both private and public sectors against sophisticated threats. From monitoring to threat hunting, we enhance IronDefense capabilities by providing customers 24/7/365 NDR services backed by Collective Defense, enabling customer SOC analysts to spend more time focusing on strategic tasks. Our cybersecurity operators add to the power of IronDefense by leveraging best practices to deliver advanced NDR capabilities that meet compliance standards. Our services are scalable, measurable, and cost-effective, and they provide complete real-time visibility into the network.

CyOC services include the following:

Hunt collaboration
Our Hunt Team comprises highly technical security analysts with real-world operational experience in defending highly secure networks across industries and sectors. Our analysts leverage our IronDefense platform to work side-by-side with customers’ security operations personnel to detect and mitigate threats identified in the customer network.

Threat notifications
The CyOC team continually monitors and researches events and anomalies found in customer networks. The IronNet Customer Portal is used to notify customers of IronDefense findings of interest related to a customer’s network. Notification is distributed to members determined by the customer and includes full event analysis and mitigation recommendation.

Rule deployment
The CyOC’s Threat Intelligence analysts support customer operations by providing context to manual hunt operations and alert triage. The team produces tailored threat information to customer instances of IronDefense through Threat Intelligence Rule updates based on current suspicious and malicious IoCs, IronDome insights, emerging threat research, and results of research by our malware reverse engineers.

Reachback support
The CyOC team offers remote event collaboration, incident response, cybersecurity expertise, and platform support for IronDefense related security operations.

Reporting
Periodic Insight reports are provided to customers on threat trends correlated to the customer’s network and sector. These reports provide summarized and actionable IoCs associated with high-risk network behaviors mapped to the MITRE ATT&CK Detection framework to identify the stage and progression of the threat. These reports also include a detailed list of resulting TIR deployed to customer instances of IronDefense.

Custom hunt tracking
Introductory and advanced training for end-users on analytics, alerts, entity enrichment, hunting, and network defense techniques are available. Periodic on-site side-by-side hunt operations, threat identification techniques, and review of newly implemented product features are also available.

Detection Engineering
A repeatable process to enable detection of adversary tactics, techniques, and procedures (“TTPs”) over netflow data, allowing us to convert the intelligence from our Threat Research team and work with our Hunt Operations team to create rules using a Sigma-like query syntax from TTPs and evaluate their outputs for efficacy. Using those outputs, we can engineer new detections that will generate alerts if those behaviors are observed, going forward, across our entire customer base.

Customer Success Team
Through our core products and services, we seek to increase our customers’ visibility into the threat landscape, reduce the impact of a potential attack and improve the overall effectiveness of cybersecurity investments. One of the ways we do this is with our dedicated CS team. While some vendors charge a premium for expert Customer Success care, we include access to our CS team as part of a customer’s subscription, including a dedicated Customer Success Manager for the life of the subscription.

At the onset of a new deployment, our CS team works with customer stakeholders to map out what success looks like, determine the key deliverables required to achieve those goals and create a success plan for the life of the partnership.

Governance and Maturity Services
These services measure adherence to specific regulatory or contractual requirements and provide measurable data as to the maturity of the organization’s cybersecurity capabilities.

Cybersecurity Readiness Services
Given that threat actors continuously change their tactics, techniques, and procedures, these services are designed to ensure organizations are prepared for the latest and most immediate threats.

Incident Response Services
We provide incident response and digital forensic investigative services powered by an accomplished team with deep expertise. We specialize in providing incident response and digital forensic investigative services to companies of all sizes, ranging from large U.S. Fortune 50 companies to smaller organizations.

Training
Leveraging decades of cybersecurity experience, our results-focused training programs enable customers to unlock a higher level of cyber resilience. We adopt a hands-on approach to build technical proficiency and operational confidence using industry best practices. Cyber skillset training techniques include hunt methodology, offensive methodology, data analytics for security intelligence, SOC leadership, cyber threat intelligence operations, executive education, and custom cyber threat seminars.

Sales and Marketing
During the second half of 2022, fiscal year ended January 31, 2023, we significantly reduced our company headcount, notably in sales and marketing. We refocused a smaller and now more senior direct sales force on a strategy targeting larger public and private sector organizations with a more sophisticated cyber stack. We believe we have a differentiated ability to convene CEOs, CISOs, and other leaders within an entire industry, such as energy company CEOs. We have a sales team presence in the United States as well as sales leadership in EMEA.

Our marketing organization employs high-tech multichannel digital and content marketing for lead generation, public relations, social media and thought leadership programs to drive awareness. Our public relations and media program has resulted in coverage in business press, cybersecurity trade media and industry trade media.

Our event program is focused on exposure to audiences that are aligned to our refocused sales strategy. We incorporate a combination of both large industry events with regional and sector-focused field marketing events that allow us to capture leads on new customers. We also have an integrated thought leadership program wherein we host monthly webinars with our executives, customers, and other thought leaders, in addition to participating in partner hosted-webinars and invited opportunities (e.g., America’s Future Series).

We focus on providing compelling content for both demand generation and awareness-building. Our monthly Threat Intelligence Briefs summarize the IOCs and detections our SOC has discovered in order to inform the efforts of other operations analysts in the cybersecurity space. Our threat researchers produce in-depth analysis on topics such as ransomware detection and unique technical observations about the SUNBURST attack, Log4j, cyber implications of the Ukraine-Russia war, and other topics, which have been featured in media outlets. We believe this helps build credibility with the security analyst audience, a key influencer in the buying process.

Our Partnership Ecosystem
Our partner ecosystem consists of leading organizations that have been carefully selected to help us deliver the power of Collective Defense across a variety of dimensions.

Technology partners
When used together, our partner integrations leverage our collective threat intelligence to react in real time, as well as proactively combat threats across the entire network, and create workflows that mitigate compromised devices. Our integrations are designed to increase the efficiency of security teams with smarter, more effective workflows built through collective threat intelligence. To streamline the alert triage and incident response processes, IronDefense can integrate with a number of security products, including:

- SIEM tools to retrieve logs, share detections, and retrieve analyst feedback;
- SOAR tools to share detections, retrieve analyst feedback, and augment existing playbooks;
- EDR platforms to ingest endpoint event and entity context and initiate response to malicious activity; and
- NGFW products to dynamically block malicious activity and ingest logs for analysis.

Current and planned future integrations and APIs include:

Cloud
- AWS

SIEM
- Splunk
- IBM QRadar
- Microsoft Azure Sentinel
- LogRhythm

SOAR
- Cortex XSOAR (formerly Demisto)
- Splunk Phantom
- Swimlane

ITSM
- ServiceNow

EDR
- CrowdStrike
- Carbon Black
- SentinelOne

NGFW
- Palo Alto Networks
- Checkpoint Software Technologies

SACE/CASB
- Zscaler

Research and Development
15
Our product and engineering teams are responsible for the architecture and implementation of our Collective Defense platform. Our team of data scientists, data engineers, and emerging threat researchers work together to continually improve the analytics which drive IronDefense. Our Cloud Infrastructure and Sensor teams are dedicated to making IronDome reliable and scalable in the cloud. In addition, our CyOC provides overwatch capabilities of IronDome which provides further novel detection as well as proactive response and threat intelligence updates to all community participants.

We are built upon innovations in cybersecurity technology, delivering continuous improvement in detection and mitigation of threats. Our expertise and history in defense and cybersecurity brings a holistic point of view to the design of our solutions, allowing us to find novel threats and threat them in real time. We focus investment on research into emerging threats and advanced data science to keep our Collective Defense platform at the forefront of the global security landscape. We use feedback from our customers and channel partners, as well as studies of market needs, to guide product development, ensuring prioritization of new integrations, product features and functionality.

We have a regular weekly cadence to report internally on our own infrastructure and security operations, as well as the health of all our customer instances. On an annual basis, we use a third-party penetration testing team to test our environment. Additionally, we use our internal Red Team to perform periodic testing and vulnerability scans for all our environments.

**Competition**

The market for our products and services is intensely competitive and characterized by rapid changes in technology, customer requirements, and by frequent new product and service offerings and improvements. We compete with a range of established and emerging security solution vendors. Conditions in our market could change rapidly and significantly as a result of technological advancements, partnerships, or acquisitions by competitors or continuing market consolidation and we expect the competitive environment to remain intense.

Our competitors include the following by general category:

- first-generation NDR vendors such as DarkTrace or Vectra Networks, who offer point products based on Bayesian analysis, outlier analysis, and heuristic detection-based detection;
- legacy network infrastructure and performance monitoring companies such as ExtraHop and Arista Networks, who are adding security use cases to their infrastructure products; and
- legacy infrastructure detection and protection products ("IDPS") and Sandbox from companies such as Cisco and FireEye.

We compete on the basis of a number of factors, including but not limited to our ability to:

- detect advanced network threats and to prevent security breaches;
- anonymously correlate and share threats in real-time across a community of peer enterprises;
- share human-intelligence across a Collective Defense community on how peer enterprises have rated and triaged similar detections; and
- integrate with other participants in the security ecosystem.

We also compete on our:

- time to value, price, and total cost of ownership;
- brand awareness, reputation, and trust in our services;
- strength of sales, marketing, and channel partner relationships; and
- customer success, cyber hunt, and cyber advisory services.

Although some of our competitors enjoy greater resources, higher brand recognition, broader range of IT and security products, larger existing customer bases, or more mature intellectual property portfolios, we believe that we compete favorably with respect to these factors.

**Intellectual Property**

We believe that our intellectual property rights are valuable and important to our business. We rely on trademarks, patents, copyrights, trade secrets, license agreements, intellectual property assignment agreements, confidentiality procedures, non-disclosure agreements, and employee non-disclosure and invention assignment agreements to establish and protect our proprietary rights. Though we rely in part upon these legal and contractual protections, we believe that factors such as the skills and ingenuity of our employees and the functionality and frequent enhancements to our solutions are larger contributors to our success in the marketplace.

As of April 14, 2023, we had five issued U.S. patents and eight pending applications in the United States covering our technology (two of which are allowed), as well as 38 issued international patents, four pending international patent applications, and nine filed PCT applications, of which five are expired. Our issued patents expire between 2035 and 2041.

As of April 14, 2023, we had five registered brands in the United States, comprising four single-class trademark registrations and five single- and multiple-class service mark registrations. Four of those five brands are also registered internationally. In addition, we own pending multi-class, combined trademark/service mark applications in both the United States and abroad. We believe these registrations and pending applications offer robust protection for all of our brands. We intend to pursue additional intellectual property protection to the extent we believe it would be beneficial and cost-effective.

Despite our efforts to protect our intellectual property rights, they may not be respected in the future or may be invalidated, circumvented, or challenged. Our industry is characterized by the existence of a large number of patents and frequent claims and related litigation based on allegations of patent infringement or other violations of intellectual property rights. We believe that competitors will try to develop products that are similar to our products and that may infringe our intellectual property rights. Our competitors or other third parties may also claim that our security platform and other solutions infringe their intellectual property rights. In particular, some companies in our industry may have extensive patent portfolios. From time to time, third parties may in the future assert claims of infringement, misappropriation and other violations of intellectual property rights against us and our customers, with whom our agreements may obligate us to indemnify against these claims. Successful claims of infringement by a third party could prevent us from offering certain products or features, require us to develop alternate, non-infringing technology, which could require significant time and during which we could be unable to continue to offer our affected products or solutions, require us to obtain a license, which may not be available on reasonable terms or at all, or force us to pay substantial damages, royalties, or other fees.

**Government Regulation**

Our business activities are subject to various federal, state, local, and foreign laws, rules, and regulations. Compliance with these laws, rules, and regulations has not had, and is not expected to have, a material effect on our capital expenditures, results of operations and competitive position as compared to prior periods. Nevertheless, compliance with existing or future governmental regulations, including, but not limited to, those pertaining to global trade, consumer and data
protection, and taxes, could have a material impact on our business in subsequent periods. For more information on the potential impacts of government regulations affecting our business, see the section titled “Risk Factors” contained in Part I, Item 1A of this Annual Report on Form 10-K.

Employees and Human Capital Resources
Our employees worldwide power our innovation, contributing unique perspectives and a growth mindset to create breakthrough technologies and transformative solutions. We are committed to fostering a diverse and inclusive workplace that attracts and retains exceptional talent. Through ongoing employee development, comprehensive compensation and benefits, and a focus on health, safety and employee wellbeing, we strive to help our employees in all aspects of their lives so they can do their best work, every single day. In response to the COVID-19 pandemic, we implemented significant changes in the best interest of employees at the time, including having evolved to a remote culture, a practice we have retained.

As of January 31, 2023, we had 104 full-time employees. Of these employees, 96 are in the United States and eight are in international locations. We have not experienced work stoppages and believe our employee relations are good.

Diversity and Inclusion
Innovation at our company comes from the diverse perspectives, knowledge, and experiences of our employees. We strive to create an inclusive workplace where people can bring their authentic selves to work. We employ inclusive recruitment practices to source diverse candidates and mitigate potential bias.

Compensation, Benefits and Well-being
We offer competitive compensation and benefits that support our employees’ overall well-being. To ensure alignment with our short- and long-term objectives, our compensation programs for all employees include base pay, short-term incentives, and opportunities for long-term incentives. We offer benefits including comprehensive health and wellness insurance, company match for health and wellness accounts, paid time-off and leaves, pet insurance, an Employee Assistance Program (to include counseling opportunities), legal advice, parental leave, discount programs to various travel vendors, and a retirement matching program.

Environmental Controls
The laws of several jurisdictions, including U.S. federal law, imposes criminal and/or civil liability on any person or company that contaminates the environment with any hazardous substance that could cause injury to the community or environment. Violation of environmental laws can involve monetary fines and imprisonment. We expect our employees, officers and directors to comply with all applicable environmental laws when conducting the business of the Company.

Anti-discrimination Controls
In order to provide equal employment and advancement opportunities to all individuals, employment decisions are based on merit, qualifications, and abilities. We do not discriminate in employment opportunities or practices on the basis of race, color, religion, sex, sexual orientation, gender identity, national origin, age, or disability. We strive to make reasonable accommodations for qualified individuals with known disabilities. This policy governs all aspects of employment, including selection, job assignment, compensation, discipline, termination, and access to benefits and training. Employees with questions or concerns about discrimination in the workplace are encouraged to bring these issues to the attention of their immediate supervisor or a People and Culture Manager. Employees can raise concerns and make reports without fear of reprisal. Anyone found to be engaging in unlawful discrimination will be subject to disciplinary action, up to and including termination of employment.

Available Information
Our Internet address is www.ironnet.com. Our investor relations website is located at https://ir.ironnet.com. Our Annual Reports on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and our Proxy Statements, and any amendments to these reports, are available through our investor relations website, free of charge, after we file them with the U.S. Securities and Exchange Commission (the “SEC”). These filings with the SEC are also available on the SEC’s website located at www.sec.gov.

We announce material information to the public through a variety of means, including filings with the SEC, blogs (including https://www.ironnet.com/blog), press releases, public conference calls, our website (www.ironnet.com) and the investor relations section of our website (https://ir.ironnet.com). In addition to these channels, we will continue to use social media to communicate with our customers and the public. We use these channels to communicate with investors and the public about our company, our products and services and other matters. Therefore, we encourage investors, the media and others interested in our company to review the information we make public in these locations, as such information could be deemed to be material information. Further, corporate governance information, including our corporate governance guidelines, code of business conduct and ethics, and committee charters, is also available on investor relations section of our website.

The content on or accessible through our websites are not incorporated by reference into this Annual Report on Form 10-K or in any other report or document we file with the SEC, and any references to our websites are intended to be inactive textual references only.

17
Risks Related to Our Business and Industry

We have a history of losses and may not be able to achieve or sustain profitability in the future. We have incurred net losses in all periods since our inception. We experienced net losses of $111.0 million and $242.6 million for fiscal year 2023 and fiscal year 2022, respectively. As of January 31, 2023, we had an accumulated deficit of $528.7 million. We cannot predict when or whether we will ever reach or maintain profitability. We will also continue to incur significant operating expenses, which will negatively affect our results of operations if our total revenue does not increase. We cannot assure you that we will achieve increases in our total revenue or improvements in our results of operations. We also expect to incur significant additional legal, accounting, and other expenses as a public operating company. Any failure to increase our revenue as we invest in our business or to manage our costs could prevent us from achieving or maintaining profitability or positive cash flow.

There is substantial doubt about our ability to continue as a going concern, and holders of our common stock could suffer a total loss of their investment. We will need to raise additional capital to continue our operations, which capital may not be available on terms acceptable to us, or at all, and which could reduce our ability to compete and could harm our business. Our history of losses and negative cash flows raise substantial doubt regarding our ability to continue as a going concern, which may negatively impact the price of our common stock. If we are unable to continue as a going concern, we may have to liquidate our assets and may receive less than the value at which those assets are carried on our financial statements, and it is likely that investors will lose all or a part of their investment. Further, the perception that we may be unable to continue as a going concern may impede our ability to pursue strategic opportunities or operate our business due to concerns regarding our ability to discharge our contractual obligations. In addition, if there remains substantial doubt about our ability to continue as a going concern, investors or other financing sources may be unwilling to provide additional funding to us on commercially reasonable terms, or at all. In addition, we may not be able to access a portion of our existing cash, cash equivalents and investments due to market conditions. For example, on March 10, 2023, the Federal Deposit Insurance Corporation ("FDIC"), took control and was appointed receiver of Silicon Valley Bank ("SVB"). If other banks and financial institutions enter receivership or become insolvent in the future in response to financial conditions affecting the banking system and financial markets, our ability to access our existing cash, cash equivalents and investments may be threatened and could have a material adverse effect on our business and financial condition. Any failure or delay to secure additional financing, or our ability to access our existing cash, cash equivalents and investments, could force us to delay, limit or terminate our operations, make further reductions in our workforce, liquidate all or a portion of our assets and/or seek protection, or Bankruptcy protection, under Chapters 7 or 11 of the United States Bankruptcy Code.

In the absence of additional sources of liquidity, management anticipates that our existing cash and cash equivalents and anticipated cash flows from operations, will not be sufficient to meet our operating and liquidity needs for any meaningful period of time following the filing of this report. We will likely need to engage in equity or debt financings to secure additional funds. If we raise additional equity financing, stockholders would experience significant dilution of their ownership interests to the extent we issue a significant number of shares of common stock, and the market price of the common stock could decline. Our current convertible debt contains restrictions on our future debt financing, but if we engage in future debt financing, the holders of debt would have priority over the holders of common stock, and we may be required to accept terms that restrict our operations or our ability to incur additional indebtedness or to take other actions that would otherwise be in the interests of the debt holders. In addition, adverse macroeconomic developments, including without limitation inflation, slowing economic growth, rising interest rates or a potential economic recession, may reduce our ability to access such capital. Any of the above could harm our business, results of operations and financial condition. In the event that sufficient additional funds are not obtained through sales of securities, funding facilities, borrowing arrangements and/or asset sales on a timely basis, we may be required to reduce expenses through the delay, reduction or curtailment of our projects, or further reduction of costs for facilities and administration, or winding down of our company. Moreover, if we do not obtain such additional funds, there is substantial doubt about our ability to continue as a going concern and there is increased risk of insolvency and up to total loss of investment to our stockholders and other security holders. As of the date hereof, we have not obtained a solvency opinion or otherwise conducted a valuation of our properties to determine whether our debts exceed the fair value of our property within the meaning of applicable solvency laws. If we are or become insolvent, holders of our common stock or other securities may lose the entire value of their investment.

There can be no assurances that we will be able to raise additional capital in sufficient amounts or on favorable terms, or at all. If we are unable to raise adequate additional capital when required or in sufficient amounts or on terms acceptable to us, we may reduce operations, liquidate assets (potentially at a loss), cease operations altogether, pursue an acquisition of our company at a price that may result in up to a total loss on investment for our stockholders, file for bankruptcy or seek other protection from creditors, or liquidate all of our assets. There can be no assurance that we will consummate the proposed acquisition transaction with C5 or that the proposed transaction, if completed, would enhance stockholder value, and speculation and uncertainty regarding the outcome of the proposed transaction may adversely impact our business and results of operations.

In December 2022, we announced that we had begun negotiating with C5 a potential transaction by which C5 would acquire all of our common stock that it does not currently own (the "Proposed Transaction"). We continue to negotiate definitive agreements with respect to the Proposed Transaction. However, there can be no assurance of the terms, timing or structure of any transaction, or whether any such transaction will take place at all, and any such transaction is subject to risks and uncertainties. The process of reviewing the Proposed Transaction may involve significant resources and costs. In addition, the review of the Proposed Transaction may cause or result in:

- disruption of our business;
- difficulty in maintaining or negotiating and consummating new business or strategic relationships or transactions;
- diversion of the attention of management;
- increased stock price volatility;
- increased costs and advisory fees; and
- challenges in hiring and retaining key employees.
If we are unable to mitigate these or other potential risks related to the uncertainty caused by our exploration of the Proposed Transaction, it may disrupt our business or could have a material adverse effect on our financial condition and results of operations in future periods.

Our ability to complete the Proposed Transaction, if our board of directors decides to pursue it, will depend on numerous factors, some of which are outside of our control, including market conditions, industry trends and the availability of financing to C5 and other potential buyers on commercially acceptable terms. Even if the Proposed Transaction is completed, there can be no assurance that it will be successful or have a positive effect on stockholder value. Our board of directors may also determine that no transaction is in the best interests of stockholders. Further, it is not certain what impact the Proposed Transaction, or any other potential transaction, or a decision not to pursue any potential transaction, may have on our stock price, business, financial condition, and results of operations.

We must regain compliance with New York Stock Exchange requirements for the continued listing of our common stock.

On October 25, 2022, we received the Initial Notice from the NYSE, indicating that we are no longer in compliance with the NYSE continued listing standards, set forth in Section 802.01C of the NYSE Listed Company Manual because the average closing price of our common stock was less than $1.00 per share over a period of 30 consecutive trading days. On December 21, 2022, we received the Second Notice from the NYSE, indicating that we are no longer in compliance with the NYSE continued listing standards, set forth in Section 802.01E of the NYSE Listed Company Manual because of our failure to timely file the Quarterly Report for the quarter ended October 31, 2022. On January 24, 2023, we received the Third Notice from the NYSE, indicating that we are no longer in compliance with the NYSE continued listing standards, set forth in Section 802.01E of the NYSE Listed Company Manual because our average global market capitalization over a consecutive 30 trading-day period was less than $50 million and, at the same time, our last reported shareholders’ equity was less than $50 million.

The Notices have no immediate impact on the listing of our common stock and our common stock will continue to be listed and traded on the NYSE under the common stock trading symbol "ERNT" during applicable cure periods, subject to our continued compliance with the plan and other listing requirements of the NYSE. However, until the NYSE determines that we have regained compliance, our common stock trading symbol will have an added designation of "*.BC" to indicate that the status of our common stock is "below compliance" with the NYSE continued listing standards.

The Notices and compliance with the plan do not affect our business operations or our reporting obligations with the Securities and Exchange Commission, and it does not conflict with or cause an event of default under any of our material debt or other agreements. Failure to maintain our NYSE listing could negatively impact us and our shareholders by reducing the willingness of investors to hold our common stock because of the resulting decreased price, liquidity and trading of our common stock, limited availability of price quotations, and reduced news and analyst coverage. These developments may also require brokers trading in our common stock to adhere to more stringent rules and may limit our ability to raise capital by issuing additional shares in the future. Delisting may adversely impact the perception of our financial condition, and cause reputational harm with investors and parties conducting business with us. In addition, the perceived decreased value of employee equity incentive awards may reduce their effectiveness in encouraging performance and retention.

In the event we pursue bankruptcy protection, we will be subject to the risks and uncertainties associated with such proceedings.

In the event we file for relief under the United States Bankruptcy Code, our operations, our ability to develop and execute our business plan and our continuation as a going concern will be subject to the risks and uncertainties associated with bankruptcy proceedings, including, among others: our ability to execute, confirm and consummate a plan of reorganization; the high costs of bankruptcy proceedings and related fees; our ability to obtain sufficient financing to allow us to emerge from bankruptcy and execute our business plan post-emergence, and our ability to comply with terms and conditions of that financing; our ability to continue our operations in the ordinary course; our ability to maintain our relationships with our customers, business partners, counterparty, employees and other third parties; our ability to obtain, maintain or renew contracts that are critical to our operations on reasonably acceptable terms and conditions; our ability to attract, motivate and retain key employees; the ability of third parties to use certain limited safe harbor provisions of the United States Bankruptcy Code to terminate contracts without first seeking Bankruptcy Court approval; the ability of third parties to force us to into Chapter 7 proceedings rather than Chapter 11 proceedings and the actions and decisions of our stakeholders and other third parties who have interests in our bankruptcy proceedings that may be inconsistent with our operational and strategic plans. Any delays in our bankruptcy proceedings would increase the risks of our being unable to reorganize our business and emerge from bankruptcy proceedings and may increase our costs associated with the bankruptcy process or result in prolonged operational disruption for us. Also, we would need the prior approval of the bankruptcy court for transactions outside the ordinary course of business during the course of any bankruptcy proceedings, which may limit our ability to respond timely to certain events or take advantage of certain opportunities. Because of the risks and uncertainties associated with any bankruptcy proceedings, we cannot accurately predict or quantify the ultimate impact of events that could occur during any such proceedings. There can be no guarantees that if we seek Bankruptcy protection we will emerge from Bankruptcy protection as a going concern or that holders of our common stock will receive any recovery from any bankruptcy proceedings.

In the event we are unable to pursue Bankruptcy protection under Chapter 11 of the United States Bankruptcy Code, or, if pursued, successfully emerge from such proceedings, it may be necessary to pursue Bankruptcy protection under Chapter 7 of the United States Bankruptcy Code for all or a part of our businesses.

In the event we are unable to pursue Bankruptcy protection under Chapter 11 of the United States Bankruptcy Code, or, if pursued, successfully emerge from such proceedings, it may be necessary for us to pursue Bankruptcy protection under Chapter 7 of the United States Bankruptcy Code for all or a part of our businesses. In such event, a Chapter 7 trustee would be appointed or elected to liquidate our assets for distribution in accordance with the priorities established by the United States Bankruptcy Code. We believe that liquidation under Chapter 7 would result in significantly smaller distributions being made to our stakeholders than those we might obtain under Chapter 11 primarily because of the likelihood that the assets would have to be sold or otherwise disposed of in a distressed fashion over a short period of time rather than in a controlled manner and as a going concern. We have a considerable amount of debt, which may limit our ability to fulfill our obligations and/or to obtain additional financing.

As of the date of this report, we have $27.8 million of indebtedness outstanding. Our capital structure and reliance on indebtedness can have several important consequences, including, but not limited to, the following:

- The terms of our indebtedness restrict our ability to incur additional indebtedness in certain instances.
- If future cash flows are insufficient, we may not be able to make principal or interest payments on our debt obligations when such obligation become due, which could result in the occurrence of an event of default under one or more of those debt instruments.
- Our leverage level could make it more difficult for us to satisfy our obligations to our lenders, resulting in possible defaults on and acceleration of such indebtedness.
- Our leverage level could place us at a competitive disadvantage compared to any competitors that have less debt or comparable debt at more favorable interest rates and that, as a result, may be better positioned to withstand economic downturns.
- Our indebtedness has the general effect of reducing our flexibility to react to changing business and economic conditions insofar as they affect our financial condition. The interest rates at which we might secure additional financings may be higher than our currently outstanding debt instruments or higher than forecasted at any point in time, which could adversely affect our business, financial condition, results of operations and cash flows.
- Market conditions could affect our access to capital markets, restrict our ability to secure financing to make planned capital expenditures and investments and pay other expenses, which could adversely affect our business, financial condition, cash flows and results of operations.
rate of cybersecurity spending and could adversely affect our
for our platform and services generally, and business spend management specifically. In addition, our revenues are dependent on the number of users of our services. Historically, during economic downturns there have been
The factors discussed above have and may continue to influence our customers' behavior, spending patterns and general demand for our platform and services and could result in anticipated savings, could result in total costs and expenses that are greater than expected and could disrupt our business.
Between September 2022 and November 2022, we reduced our headcount by a total of 111 employees, representing approximately 44% of our workforce, as part of our initiatives to re-balance our cost structure. These reductions in force are expected to result in approximately $20.0 million in annualized cost savings in total. However, we may incur additional expenses not currently contemplated due to events associated with the reductions in force, for example, the reductions in force may have a future impact on other areas of our liabilities and obligations, which could result in losses in future periods. The annualized cost savings are estimates and subject to a number of assumptions, and actual results may differ materially. We may not realize, in full or in part, the anticipated benefits and savings from these reductions in force due to unforeseen difficulties, delays or unexpected costs. If we are unable to realize the expected operational efficiencies and cost savings from the announced reductions in force, our operating results and financial condition would be adversely affected. In addition, we may need to undertake additional workforce reductions or restructuring activities in the future. Furthermore, our initiatives to re-balance our cost structure, including the reductions in force, may be disruptive to our operations. For example, our workforce reductions could yield unanticipated consequences, such as attrition beyond planned staff reductions, increased difficulties in our day-to-day operations and reduced employee morale. If employees who were not affected by the reductions in force seek alternative employment, this could result in us seeking contractor support at unplanned additional expense or harm our productivity. Our workforce reductions could also harm our ability to attract and retain qualified personnel who are critical to our business. Any failure to attract or retain qualified personnel could prevent us from successfully developing or selling our products, which would adversely affect our business.

We limited our operating history makes it difficult to evaluate our current business and our future prospects and may increase the risk of your investment.
We were founded in 2014 and we launched our first cybersecurity network detection and response product, IronDefense, in 2016 and our first collective defense product, IronDome, in 2018. Our limited operating history makes it difficult to evaluate our current business, our future prospects, and other trends, including our ability to plan for and model future growth. We have encountered, and we will continue to encounter, risks, uncertainties, and difficulties frequently experienced by rapidly growing companies in evolving industries, including our ability to achieve broad market acceptance of cloud-enabled, and/or SaaS delivered cybersecurity solutions and our platform, attract additional customers, grow partnerships, compete effectively, build and maintain effective compliance programs, and manage increasing expenses as we continue to invest in our business. If we do not address these risks, uncertainties and difficulties successfully, our business, and results of operations will be harmed. Further, we have limited historical financial data and operate in a rapidly evolving market. As a result, any predictions about our future revenue and expenses may not be as accurate as they would be if we had a longer operating history or operating in a more predictable market.

Weakened global economic conditions may harm our industry, business and results of operations.
Our overall performance depends in part on worldwide economic conditions. Global financial developments, downturns and global health crises or pandemics seemingly unrelated to us or the cybersecurity industry, may harm us, including due to disruptions or restrictions on our employees’ ability to work and travel. The United States and other key international economies have been affected from time to time by falling demand for a variety of goods and services, restricted credit, poor economic growth, volatility in credit, equity and foreign exchange markets, disruptions in access to bank deposits or lending commitments due to bank failures, bankruptcies, outbreaks of COVID-19 and the resulting impact on business continuity and travel, supply chain disruptions, inflation and overall uncertainty with respect to the economy, including with respect to tariff and trade issues. For example, inflation rates, particularly in the United States, have increased recently to levels not seen in years, and increased inflation may result in decreased demand for our products and services, increases in our operating costs (including our labor costs), reduced liquidity and limits on our ability to access credit or otherwise raise capital. In addition, the Federal Reserve has raised, and may again raise, interest rates in response to concerns about inflation, which coupled with reduced government spending and volatility in financial markets may have the effect of further increasing economic uncertainty and heightening these risks. Additionally, financial markets around the world experienced volatility following the invasion of Ukraine by Russia in February 2022. In response to the invasion, the US, UK and EU, along with others, imposed significant new sanctions and export controls against Russia, Russian banks and certain Russian individuals and may implement additional sanctions or take further punitive actions in the future. The full economic and social impact of the sanctions imposed on Russia (as well as possible future punitive measures that may be implemented), as well as the counter measures imposed by Russia, in addition to the ongoing military conflict between Ukraine and Russia, which could conceivably expand into the surrounding region, remains uncertain; however, both the conflict and related sanctions have resulted and could continue to result in disruptions to trade, commerce, pricing stability, credit availability, and/or supply chain continuity, in both Europe and globally, and has introduced significant uncertainty into global markets. As the adverse effects of this conflict continue to develop and potentially spread, both in Europe and throughout the rest of the world, our customers may be negatively impacted, which in turn may cause them to delay purchasing decisions, affect subscription renewal rates and otherwise depress our customers’ spending levels. As a result, our business and results of operations may be adversely affected by the ongoing conflict between Ukraine and Russia, particularly to the extent it escalates to involve additional countries, further economic sanctions or wider military conflict. We have current and potential new customers throughout Europe. If economic conditions in Europe and other key markets for our platform continue to remain uncertain or deteriorate further, many customers may delay or reduce their cybersecurity spending.

In addition, prior to March 10, 2023, we had a banking relationship with SVB. As of the closure of SVB on March 10, 2023, we held approximately $8.1 million in cash, cash equivalents and investments at or through SVB, which represented approximately 96% of our total cash, cash equivalents and investments as of that date. SVB was closed on March 10, 2023 by the California Department of Financial Protection and Innovation, which appointed the FDIC as receiver. On March 12, 2023, the U.S. Treasury, Federal Reserve, and FDIC announced that SVB depositors would have access to all of their money starting March 13, 2023. On March 13, 2023, we were able to access all $8.1 million in cash, cash equivalents and investments held at or through SVB. While we have not experienced any losses in such accounts, the recent failure of SVB exposed us to significant credit risk prior to the completion by the FDIC of the resolution of SVB in a manner that fully protected all depositors. We are in the process of transferring some of our deposits to multiple banks to limit our credit risk. However, our access to funding sources and other credit arrangements in amounts adequate to finance or capitalize our current and projected future business operations could be significantly impaired by factors that affect us, the financial institutions with which we have arrangements directly, or the financial services industry or economy in general. These factors could include, among others, events such as liquidity constraints or defaults, the ability to perform obligations under various types of financial, credit or liquidity agreements or arrangements, disruptions or instability in the financial services industry or financial markets, or concerns or negative expectations about the prospects for companies in the financial services industry. These factors could involve financial institutions or financial services industry companies with which we have financial or business relationships, but could also include factors involving financial markets or the financial services industry generally.

The factors discussed above have and may continue to influence our customers' behavior, spending patterns and general demand for our platform and services and prompt our customers to take additional precautionary measures to limit or delay expenditures and preserve capital and liquidity as they monitor global economic conditions and the risk of a global recession. The growth of our revenues and potential profitability of our business depends on demand for our platform and services generally, and business spend management specifically. In addition, our revenues are dependent on the number of users of our services. Historically, during economic downturns there have been reductions in spending on cybersecurity as well as pressure for extended billing terms or pricing discounts, which would limit our ability to grow our business and negatively affect our operating results. These conditions affect the rate of cybersecurity spending and could adversely affect our
customers’ ability or willingness to subscribe to our services, delay prospective customers’ purchasing decisions, reduce the value or duration of their subscriptions or affect renewal rates, all of which could harm our operating results.

If organizations do not adopt cloud-enabled, and/or SaaS-delivered cybersecurity solutions that may be based on new and untested security concepts, our ability to grow our business and results of operations may be adversely affected.

Our future success depends on the growth in the market for cloud-enabled and/or SaaS-delivered cybersecurity solutions. The use of SaaS solutions to manage and automate security and IT operations is rapidly evolving. As such, it is difficult to predict our potential growth, customer adoption and retention rates, customer demand for our solutions, or the success of existing or future competitive products. Any expansion in our market depends on a number of factors, including the cost, performance and perceived value associated with our solutions and those of our competitors. If our solutions do not achieve widespread adoption or there is a reduction in demand for our solutions due to a lack of customer acceptance, technological challenges, competing products, privacy or other liability concerns, decreases in corporate spending, weakening economic conditions, or otherwise, it could adversely affect our business, results of operations and financial results, resulting from such things as early terminations, reduced customer adoption rates, increased customer churn, reduced sales and decreased sales. Negative or worsening conditions in the general economy both in the United States and abroad, including conditions resulting from financial and credit market fluctuations and inflation, could cause a decrease in corporate spending on enterprise software in general, and in the cybersecurity industry specifically, and negatively affect the rate of growth of our business. We do not know whether the trend in adoption of cloud-enabled and/or SaaS-delivered cybersecurity solutions that we have experienced in the past will continue in the future. Furthermore, if we or other SaaS security providers experience security incidents, loss, or disclosure of customer data, disruptions in delivery, or other problems, the market for SaaS solutions as a whole, including our security solutions, could be negatively affected.

In addition to reliance on a cloud-enabled and/or SaaS-delivered model, our cybersecurity offerings utilize a novel and relatively new approach to collective defense that relies on customers sharing sensitive customer information with us. Some of that raw customer information may contain personal or confidential information, or data perceived to be personal or confidential information. From that customer information, we generate analytics that allow us to deliver threat knowledge and network intelligence at machine speed across a wide variety of industries. Because this new approach requires the sharing of sensitive customer information, concerns may exist that sharing of the customer information may violate, or be perceived as potentially violating, privacy laws or providing a competitive advantage to another entity. As a result, some current or prospective customers may decide not to procure our products or share any customer information. Such lack of acceptance could have negative effects on us, including reduced or lost revenues or inadequate information being available for our analysis, thus making our products less effective. In addition, uncertainties about the regulatory environment concerning personal information and the potential liability raised by sharing such information could further inhibit the broad-scale adoption of our solutions.

Historically, information sharing related to cybersecurity has been a very well accepted concept from a theoretical perspective but very difficult to implement in practice. Companies are generally reluctant to share their sensitive cyber information with other entities, despite knowing the advantages of doing so. Although raw customer information will not be shared with other parties, it does undergo filtering, concatenation, and other transformations within our solutions with the goal of removing any sensitive or personal information. Misperceptions may exist, however, about what information gets shared, with whom that information is shared, and the jurisdictions (including foreign countries) of the companies with which the information gets shared. Further, concerns of existing or potential customers may exist related to the ability to completely remove any indicia of the source company, general market rejection of information sharing, or specific market skepticism of our approach to collective defense, which may further add to a lack of customer acceptance.

In addition to the potential concerns related to sharing sensitive information in a system consisting of commercial or potentially competitive entities, additional concerns can arise when governments become involved as participants in the collective defense ecosystem. From a commercial perspective, companies frequently view information sharing with governments as risky, based on perceptions that the governments might use such shared information to take action against the companies or to otherwise utilize it in a way that will expose such companies to liability. Such perceptions could lead commercial entities to stop sharing, not procure our services in the first place, or terminate their relationship with us altogether. Similarly, governments (as customers) may be unable to properly process such data or utilize it in a meaningful way, or share useful information back into our solutions. Any of these concerns could lead to reduced sales or contribute to a lack of customer acceptance. In addition, the mere involvement of one or more government entities may harm our reputation with certain companies.

If we are unable to attract new customers, our future results of operations could be harmed.

To expand our customer base, we will need to convince potential customers to allocate a portion of their discretionary budgets to purchase our platform and solutions. Our sales efforts have often involved educating our prospective customers about the uses and benefits of our platform and solutions. Enterprises and governments that use legacy security products, such as signature-based or malware-focused products, firewalls, intrusion prevention systems and endpoint technologies, may be hesitant to purchase our platform and solutions if they believe that legacy security products are more cost effective, provide substantially the same functionality as our platform and solutions or provide a level of cybersecurity that is sufficient to meet their needs.

We may have difficulty convincing prospective customers of the value of adopting our solutions. Even if we are successful in convincing prospective customers that a cloud-enabled platform like ours is critical to protect against cyberattacks, they may not decide to purchase our platform and solutions for a variety of reasons, some of which are out of our control. For example, any future deterioration in general economic conditions may cause our current and prospective customers to cut their overall security and IT operations spending, and such cuts may fall disproportionately on cloud-based security solutions. Economic weakness, customer financial difficulties, and constrained spending on security and IT operations may result in decreased revenue and adversely affect our results of operations and financial condition. Additionally, if the incidence of cyberattacks were to decline, or enterprises or governments perceive that the general level or relative risk of cyberattacks has declined, our ability to attract new customers and expand sales of our solutions to existing customers could be adversely affected. If organizations do not continue to adopt our platform and solutions, our sales will not grow as quickly as anticipated, or at all, and our business, results of operations, and financial condition would be harmed.

If our customers do not renew their subscriptions for our products, our future results of operations could be harmed.

In order for us to maintain or improve our results of operations, it is important that our customers renew their subscriptions for our platform and solutions when existing contract terms expire, and that we expand our commercial relationships with our existing customers by selling additional subscriptions. Our customers have no obligation to renew their subscriptions after the expiration of their contractual subscription period, which is generally one year, and in the normal course of business, some customers have elected not to renew. In addition, our customers may renew for shorter contract subscription lengths or cease using certain solutions. Our customer retention and expansion may decline or fluctuate as a result of a number of factors, including our customers’ satisfaction with our services, concerns related to our current financial position and disclosed bankruptcy risk, our pricing, customer security and networking issues and requirements, our customers’ spending levels, mergers and acquisitions involving our customers, industry developments, competition and general economic conditions. Our public sector customers are also subject to budgetary cycles and funding authorizations, and funding reductions or delays can result in delays in such customers renewing their contracts with us. We have experienced several of these delays in the current fiscal year, which has delayed our ability to grow our annual recurring revenue and therefore reduced revenues below our previous expectations, in addition to delaying expected cash flows. If our efforts to maintain and expand our relationships with our existing customers are not successful, our business, results of operations, and financial condition may materially suffer.

As a first mover in collective defense for the commercial sector, we may face significant liability if we are unable to effectively anonymize and safeguard our customers’ data.

We are the first major commercial vendor to offer an end-to-end means to take full advantage of the collective defense concept that relies on customers sharing sensitive customer information with us. While raw customer information is not shared with other parties and shared data undergoes filtering and other transformations within our solution, with the goal of removing any sensitive or personal information, it is possible that customer information could be accessed by third parties (including competitors of our clients), through a failure of our procedures to effectively anonymize the shared data or as a result of hackers gaining access to the raw data collected by us. To the extent we are not able to effectively anonymize and protect our customers’ data, we may be subject to liability, which

21
could adversely affect our business, results of operations and financial condition. In addition, given the novelty of our approach, it is possible that other risks related to our clients’ data could surface of which we are currently unaware.

Competition from existing or new companies could cause us to experience downward pressure on prices, fewer customer orders, reduced margins, the inability to take advantage of new business opportunities and loss of

market share.

The market for cybersecurity solutions is intensely competitive, fragmented, and characterized by rapid changes in technology, customer requirements, industry standards, increasingly sophisticated attackers, and by frequent introductions of new or improved products to combat security threats. We expect to continue to face intense competition from our current competitors, as well as from new entrants into the market. If we are unable to anticipate or react to these challenges, our competitive position could weaken, and we could experience a decline in revenue or reduced revenue growth, and loss of market share that would adversely affect our business, financial condition and results of operations. The ability to compete effectively will depend upon numerous factors, many of which are beyond our control, including, but not limited to:

• product capabilities, including performance and reliability, of our platform, including our services and features particularly in the areas of analytics and collective defense, compared to those of our competitors;
• our ability, and the ability of our competitors, to improve existing products, services and features, or to develop new ones to address evolving customer needs;
• our ability to attract, retain and motivate talented employees;
• our ability to establish, capitalize on, maintain, and grow relationships with distribution and technology partners;
• the strength of our sales and marketing efforts; and
• acquisitions or consolidation within our industry, which may result in more formidable competitors.

Our competitors include the following companies by general category:

• first-generation NDR vendors such as DarkTrace or Vectra Networks, who offer point products based on Bayesian analysis, outlier analysis, and heuristic detection-based detection;
• network security vendors, such as Cisco and Palo Alto Networks, Inc., who are supplementing their core network security additional behavioral-based detection with behavioral-based detection, threat intelligence and security operations solutions;
• legacy network infrastructure and performance monitoring companies such as ExtraHop and Arista Networks, who are adding security use cases to their infrastructure products; and
• legacy infrastructure detection and protection products (IDPS) and SandBox from companies such as Cisco and FireEye.

Many of these competitors have greater financial, technical, marketing, sales, and other resources, greater name recognition, longer operating histories, and a significantly larger base of customers than we do. They may be able to devote greater resources to the development, promotion, and sale of services than we can, and they may offer lower pricing than we do. Further, they may have greater resources for research and development of new technologies, the provision of customer support, and the pursuit of acquisitions, or they may have other financial, technical or other resource advantages. Our larger competitors have substantially broader and more diverse product and services offerings as well as routes to market, which may allow them to leverage their relationships based on other products, or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing our products.

Conditions in our market could change rapidly and significantly as a result of technological advancements, partnering or acquisitions by competitors or continuing market consolidation. Some of our current or potential competitors have made or could make acquisitions of businesses or establish cooperative relationships that may allow them to offer more directly competitive and comprehensive solutions than were previously offered and adapt more quickly to new technologies and customer needs. These competitive pressures in the market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margins, increased net losses and loss of market share. Further, many competitors that specialize in providing protection from particular types of security threats may be able to deliver these more targeted security products to the market quicker than we can or may be able to convince organizations that these more limited products meet their needs.

Even if there is significant demand for cloud-based security solutions like ours or if our competitors include functionality that is, or is perceived to be, equivalent to or better than ours in legacy products that are already generally accepted as necessary components of an organization’s cybersecurity architecture, we may have difficulty increasing the market penetration of our platform. Furthermore, even if the functionality offered by other security and IT operations providers is different and more limited than the functionality of our platform, organizations may elect to accept such limited functionality in lieu of adding products from additional vendors like us. If we are unable to compete successfully, our business, financial condition, and results of operations would be adversely affected.

Competitive pricing pressure may reduce gross profits and adversely affect our financial results.

If we are unable to maintain our pricing due to competitive pressures or other factors, our margins may be reduced and our gross profits, business, results of operations and financial condition may be adversely affected. The subscription prices for our platform, solutions, and professional services may decline for a variety of reasons, including competitive pricing pressures, discounts, anticipation of the introduction of new solutions by competitors, or promotional programs offered by us or our competitors. Competition continues to increase in the market segments in which we operate, and we expect competition to further increase in the future. Larger competitors with more diverse product and service offerings may reduce the price of products or subscriptions that compete with ours or may bundle them with other products and subscriptions in an effort to leverage their existing market share to make it harder for newer companies, like us, to effectively compete.

If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.

Real or perceived defects, errors, or vulnerabilities in our platform and solutions, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of our solutions, actions or inactions by employees or contractors that create vulnerabilities in our platform or solutions, or the failure of customers to take action on attacks identified by our platform could harm our reputation and adversely affect our business, financial position, and results of operations. Because our cloud-enabled security platform is complex, it may contain defects or errors that are not detected until after deployment. We cannot assure you that our products will detect all cyberattacks, especially in light of the rapidly changing security threat landscape that our solution seeks to address. Due to a variety of both internal and external factors, including, without limitation, defects or misconfigurations of our solutions, our solutions could become vulnerable to security incidents (both from intentional attacks and accidental causes) that cause them to fail to secure networks and detect and block attacks. In addition, because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that our cloud-enabled security platform is unable to detect or prevent until after some of our customers are affected. For example, certain computer hackers may be supported or directly employed by so-called nation-states, which are generally defined as sovereign territories with individuals who share a common history and set of ideals. In the context of cybersecurity, certain aggressive nation-states with a history of disregarding generally acceptable computer network norms may employ particularly sophisticated and experienced actors who focus on being persistent, unpredictable, and innovative, with the ability to tap into significant nation-state budgets. This allows such nation-state attackers to develop expansive attack playbooks and access to cutting-edge technology to facilitate their attacks, including new, or so-called zero-day, attacks. Such nation-state attackers could
successfully attack us or our customers, which could significantly harm our reputation. Additionally, our platform may falsely indicate a cyberattack or threat that does not actually exist, which may lessen customers’ trust in our solutions.

Moreover, as our cloud-enabled security platform is adopted by an increasing number of enterprises and governments, it is possible that the individuals and organizations behind advanced cyberattacks will begin to focus on finding ways to defeat our security platform. If this happens, our systems and subscription customers could be specifically targeted by attackers and could result in vulnerabilities in our platform or undermine the market acceptance of our platform and could adversely affect our reputation as a provider of security solutions. Because we host customer data on our cloud and other platforms, which in some cases may contain personally identifiable information (“PII”) or potentially confidential information, a security compromise, or an accidental or intentional misconfiguration or malfunction of our platform could result in PII and other customer data being accessible to attackers or to other customers. Further, if a high-profile security breach occurs with respect to another next-generation or cloud-enabled security system, our customers and potential customers may lose trust in such solutions generally, and cloud-enabled security solutions in particular.

Organizations are increasingly subject to a wide variety of attacks on their networks, systems, and endpoints. No security solution, including our platform, can address all possible security threats or block all methods of penetrating a network or otherwise perpetrating a security incident. There could be situations where our solutions detect attacks against a customer but the customer does not address the vulnerability, which could cause customers and the public to erroneously believe that our solutions were not effective. Real or perceived security breaches of our customers’ networks could cause disruption or damage to their networks or other negative consequences and could result in negative publicity to us, damage to our reputation, and other customer relations issues, and may adversely affect our revenue and results of operations.

As a cybersecurity provider, we may be a target of cyberattacks. If our internal networks, systems data or are are perceived to have been compromised, our reputation may be damaged and our financial results may be negatively affected.

As a provider of security solutions, our platform may be specifically targeted by bad actors for attacks intended to circumvent our security capabilities or to exploit our platform as an entry point into customers’ endpoints, networks, or systems. In particular, because we have been involved in the identification of organized cybercriminals and nation-state actors, we may be the subject of intense efforts by sophisticated cyber adversaries who seek to compromise our systems or leverage our access. We are also susceptible to inadvertent compromises of our systems and data, including those arising from process, coding, or human errors. A successful attack or other incident that compromises us or our customers’ data or results in an interruption of service could have a significant negative effect on our operations, reputation, financial resources, and the value of our intellectual property. We cannot assure you that any of our efforts to manage this risk will be effective in protecting us from such attacks.

It is virtually impossible to eliminate the risk of such compromises, interruptions in service, or other security incidents affecting our internal systems or data. Organizations are subject to a wide variety of attacks on their networks, systems and endpoints, and techniques used to sabotage or to obtain unauthorized access to networks in which data is stored or through which data is transmitted change frequently. Furthermore, employee error or malicious activity could compromise its systems. As a result, we may be unable to anticipate these techniques or implement adequate measures to prevent an intrusion into our networks, which could result in unauthorized access to customer data, intellectual property including access to our source code, and information about vulnerabilities in our product, which in turn could reduce the effectiveness of our solutions, or lead to cyberattacks or other intrusions of our customers’ networks. If any of these events were to occur, they could damage our relationships with our customers and could have a negative effect on our ability to attract and retain new customers. We have expended, and we anticipate we will continue to expend significant amounts and resources in an effort to prevent security breaches and other security incidents impacting our systems and data. Since our business is focused on providing reliable security services to our customers, an actual or perceived security incident affecting our internal systems or data or data of its customers would be especially detrimental to our reputation and customer confidence in our solutions.

In addition, while we maintain, and we will continue to maintain, insurance policies that may cover certain liabilities in connection with a cybersecurity incident, we cannot be certain that the insurance coverage will be adequate for liabilities actually incurred, that insurance will continue to be available to us on commercially reasonable terms, or at all, or that any insurer will not deny coverage as to any future claim. The successful assertion of one or more large claims that exceed available insurance coverage, or the occurrence of changes in insurance policies, including premium increases or the imposition of large deductible or coinsurance requirements, could have a material adverse effect on our business, including our financial condition, results of operations and reputation.

We rely on third-party data centers and our own colocation data centers to host and operate our platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our platform, which could cause our business to suffer.

Our customers depend on the continuous availability of our platform. We currently host our platform and serve our customers using a mix of third-party data centers, primarily AWS, and, primarily for our own use, in our own data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints. Also, customers may be subject to the same risk if they necessarily host our solutions in their own data centers.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our platform:

- the development and maintenance of the infrastructure of the internet;
- the performance and availability of third-party providers of cloud infrastructure services with the necessary speed, data capacity, and security for providing reliable internet access and services;
- decisions by the owners and operators of the data centers where our cloud infrastructure is deployed to terminate our contracts, discontinue services, shut down operations or facilities, increase prices, change service levels, limit bandwidth, declare bankruptcy or prioritize the traffic of other parties;
- physical or electronic break-ins, acts of war or terrorism, human error or interference (including by disgruntled employees, former employees or contractors) and other catastrophic events;
- cyberattacks, including denial of service attacks, targeted at us, our data centers, or the infrastructure of the internet;
- failure by us to maintain and update our cloud infrastructure to meet our data capacity requirements;
- errors, defects, or performance problems in our software, including third-party or open-source software incorporated in our software;
- improper deployment or configuration of our solutions;
- the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network;
- the failure of our disaster recovery and business continuity arrangements; and
- effects of third-party software updates with hidden malware, similar to the supply chain attack that occurred via SolarWinds.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions, adversely affect renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-enabled and/or SaaS-delivered cybersecurity solution is unreliable. We may experience service interruptions and
other performance problems due to a variety of factors. The occurrence of any of these factors, or if it is unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

If we do not effectively train our direct sales force, we may be unable to add new customers or increase sales to existing customers, and our business will be adversely affected.

We depend on our direct sales force to obtain new customers and increase sales with existing customers. Our ability to achieve significant revenue growth will depend, in large part, on our success in training and retaining sufficient numbers of qualified individuals. In the markets where we do business or plans to do business. In addition, a large percentage of our salesforce is new to our business and selling our solutions, and therefore this team may be less effective than our more seasoned sales personnel. Furthermore, hiring sales personnel in new countries, or expanding our existing presence, requires upfront and ongoing expenditures that we may not recover if the sales personnel fail to achieve full productivity. If we are unable to train a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business and results of operations will be adversely affected.

Because we recognize revenue from subscriptions to our platform and other forms of providing customers with access to our software over the term of the subscription or contract, downturns or upturns in new business will not be immediately reflected in our results of operations.

We generally recognize revenue from customers ratably over the terms of their subscription or contract term, which average over three years in length, though may be as short as one year or less. As a result, a substantial portion of the revenue that we report in each period is attributable to the recognition of deferred revenue relating to agreements that we entered into during previous periods. Consequently, any increase or decline in new sales or renewals in any one period will not be immediately reflected in our revenue for that period. Any such change, however, would affect our revenue in future periods. Accordingly, the effect of downturns in new sales and potential changes in our rate of renewals may not be fully reflected in our results of operations until future periods.

A limited number of customers represent a substantial portion of our revenue. If we fail to retain these customers, our revenue could decline significantly.

We derive a substantial portion of our revenue from a limited number of customers. For the fiscal year 2022, six customers accounted for 51% of our revenue, with two of those customers accounting for 21% of our annual revenue.

As a result of our customer concentration, which can vary from period to period, our revenue could fluctuate materially and could be materially and disproportionately impacted by purchasing decisions of these customers or any other significant future customer. Any of our significant customers may decide to purchase less than they have in the past, may alter their purchasing patterns at any time with limited notice, or may decide not to continue to license our products at all, any of which could cause our revenue to decline and adversely affect our financial condition and results of operations. If we do not further diversify our customer base, we will continue to be susceptible to risks associated with customer concentration.

Our results of operations may fluctuate significantly, which could make our future results difficult to predict and could cause our results of operations to fall below expectations.

Our results of operations have varied significantly from period to period, and we expect that our results of operations will continue to vary as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including:

- our ability to attract new and retain existing customers;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of customers;
- the timing and length of our sales cycles;
- changes in customer or distribution partner requirements or market needs;
- changes in the growth rate of our market;
- the timing and success of new product and service introductions by us or our competitors or any other competitive developments, including consolidation among our customers or competitors;
- the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of our platform;
- decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in our pricing policies or those of our competitors;
- any disruption in our relationship with distribution partners;
- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solutions;
- significant security breaches of, technical difficulties with or interruptions to, the use of our platform;
- extraordinary expenses such as litigation or other dispute-related settlement payments or outcomes;
- rising inflation and our ability to control costs, including our operating expenses;
- general economic conditions, both in domestic and foreign markets;
- future accounting pronouncements or changes in our accounting policies or practices;
- negative media coverage or publicity;
- political events, including the ongoing conflict between Russia and Ukraine;
- the amount and timing of operating costs and capital expenditures related to the expansion of our business; and
- increases or decreases in expenses caused by fluctuations in foreign currency exchange rates.

In addition, we experience seasonal fluctuations in our financial results as we can receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in the fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of our customers. Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other results from period to period.

24
As a result of this variability, our historical results of operations should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for these or other reasons, our stock price could fall substantially, and we could face costly lawsuits, including securities class action suits.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense. Our revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for our platform, particularly with respect to large organizations and government entities. Customers often view the subscription to our platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test, and qualify our platform and solutions prior to entering into or expanding a relationship with us. Large enterprises and government entities in particular often undertake a significant evaluation process that further lengthens our sales cycle.

Our direct sales team develops relationships with our customers, and works with our distribution partners on account penetration, account coordination, sales and overall market development. We spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals, and unanticipated administrative, processing, and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of our efforts to secure sales after investing resources in a lengthy sales process could adversely affect our business and results of operations.

If we are unable to attract and retain qualified personnel, our business could be harmed. There is significant competition for personnel with the technical and technical knowledge that we will require across our technology, cyber, sales, professional services and administrative support functions. Competition for these personnel in the Washington, D.C. metro area, where our corporate headquarters is located, and in other locations where we maintain offices or otherwise operate, is competitive, especially for experienced sales professionals, engineers and data scientists experienced in designing and developing cybersecurity software. Although our current remote work environment facilitates our ability to attract talent across a wider geographic base, we have from time to time experienced, and we expect to continue to experience, difficulty in hiring and retaining employees with appropriate qualifications. Many of the companies with which we compete for experienced personnel have greater resources than us. Our competitors also may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. We may also be subject to allegations that employees we hire have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees’ inventions or other work product, or that they have been hired in violation of non-compete provisions or non-solicitation provisions.

In addition, job candidates and existing employees often consider the value of the equity awards they receive in connection with their employment. Volatility or lack of performance in our stock price may also affect our ability to attract and retain key employees. Some of our employees will become vested in a substantial amount of equity awards, which may give them a material amount of personal wealth. This may make it more difficult for us to retain and motivate these employees, and this wealth could affect their decision about whether or not they continue to work for us. Any failure to successfully attract, integrate or retain qualified personnel to fulfill our current or future needs could adversely affect our business, results of operations and financial condition.

If we are not able to maintain and enhance our brand and our reputation as a provider of high-efficacy cybersecurity solutions, our business and results of operations may be adversely affected. We believe that maintaining and enhancing our brand and our reputation as a provider of high-efficacy cybersecurity solutions is critical to our relationship with our existing customers and distribution partners and our ability to attract new customers and partners. The successful promotion of our brand will depend on a number of factors, including our investment in marketing efforts, our ability to continue to develop additional features for our platform, our ability to successfully differentiate our platform from competitive cloud-enabled or legacy security solutions and, ultimately, our ability to detect and remediate cyberattacks. Although we believe it is important for our growth, these brand promotion activities may not be successful or yield increased revenue.

In addition, independent industry or financial analysts and research firms often test our solutions and provide reviews of our platform, along with the products of our competitors, and perception of our platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive as compared to those of our competitors’ products, our brand may be adversely affected. Our solutions may fail to detect or prevent threats in any particular test for a number of reasons that may or may not be related to the efficacy of our solutions in real world environments. To the extent potential customers, industry analysts, or testing firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our solutions or services do not provide significant value, we may lose customers, and our reputation, financial condition, and business would be harmed. Additionally, the performance of our distribution partners may affect our brand and reputation if customers do not have a positive experience with these partners. In addition, we have in the past worked, and we will continue to work, with high profile customers and to assist in analyzing and remediating high profile cyberattacks. This work with such customers and cyberattacks may expose us to negative publicity and media coverage. Negative publicity, including about the efficacy and reliability of our platform, our products offerings, our professional services and the customers we work with, even if inaccurate, could adversely affect our reputation and brand.

If we are unable to maintain successful relationships with our distribution partners, or if our distribution partners fail to perform, our ability to market, sell and distribute our platform and solutions efficiently will be limited, and our business, financial position and results of operations will be harmed. In addition to our direct sales force, we rely on certain key distribution partners to sell and support our platform. An increasing amount of our sales flow through our distribution partners, and we expect our reliance on such partners to continue to grow for the foreseeable future. Additionally, we have entered into, and we intend to continue to enter into, partnerships with third parties to support our future growth plans. The loss of a substantial number of distribution partners, or the failure to recruit additional partners, could adversely affect our results of operations. Our ability to achieve revenue growth in the future will depend in part on our success in maintaining successful relationships with our distribution partners and in training them to independently sell and deploy our platform. If we fail to effectively manage our existing sales channels, or if our distribution partners are unsuccessful in fulfilling the orders for our solutions, or if we are unable to recruit and retain a sufficient number of high quality distribution partners who are motivated to sell our products, our ability to sell our products and results of operations will be harmed.

Our business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could have an adverse effect on our business and results of operations.

Our future growth depends, in part, on increasing sales to government organizations. Demand from government organizations is often unpredictable, subject to budgetary uncertainty and typically involves long sales cycles. We have made significant investments to address the government sector, but we cannot assure you that these investments will be successful, or that we will be able to maintain or grow our revenue from the government sector. In fiscal year 2022 and 2023, several contracts that we previously expected would be signed with government organizations have not yet materialized due to funding delays. Sales to U.S. federal, state and local governmental agencies have not accounted for, and may never account for, a significant portion of our revenue. U.S. federal, state and local government sales are subject to a number of challenges and risks that may adversely impact our business. Sales to such government entities include the following risks:

- selling to governmental agencies can be highly competitive, expensive and time-consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;
- government certification requirements applicable to our products may change and, in doing so, restrict our ability to sell into the U.S. federal government sector until it has attained the required certifications;
- government demand and payment for our platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our platform;

25
• governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our platform, which would adversely impact our revenue and results of operations, or institute fines or civil or criminal liability if the audit were to uncover improper or illegal activities;

• interactions with the U.S. federal government may be limited by post-employment ethics restrictions on members of our management;

• foreign governments may have concerns with purchasing security products from a company that employs former NSA employees and officials, which may negatively impact sales; and

• governments may require certain products to be manufactured, hosted, or accessed solely in their country or in other relatively high-cost manufacturing locations, and we may not manufacture all products in our customers’ countries, which may result in our customers being subject to additional requirements, after the fact, for a company that previously had no such requirements, affecting our ability to sell our products in those countries.

We have been prioritized by the United States Federal Risk and Authorization Management Program ("FedRAMP") to pursue a P-ATO from the JAB with the goal to achieve FedRAMP High status. Even if we were to achieve FedRAMP High status, such certification is costly to maintain, and if we were to lose such a certification in the future it would restrict our ability to sell to government customers. It is also possible that additional guidelines and/or certifications, such as the Cybersecurity Maturity Model Certification, will be required to expand participation in the government sectors.

The occurrence of any of the foregoing could cause governments and governmental agencies to delay or refrain from purchasing our solutions in the future or otherwise have an adverse effect on our business and results of operations.

We may not scale and adapt our existing technology in a timely and cost-effective manner to meet our customers' performance and other requirements.

Our future growth will be dependent upon our ability to continue to meet the needs of new customers and the expanding needs of our existing customers as their use of our solutions grows. As our customers gain more experience with our solutions, the number of events, the amount of data transferred, processed, and stored by our solutions and the number of locations where our platform and services are being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of our customers, we intend to continue to make significant investments to increase capacity and to develop and implement new technologies in our service and cloud infrastructure operations. These technologies, which include databases, applications, and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new, and untested. We may not be successful in developing or implementing these technologies. In addition, it takes a significant amount of time to plan, develop, and test improvements to our technologies and infrastructure, and we may not be able to accurately forecast demand or predict the results we will realize from such improvements. To the extent that we do not effectively scale our operations to meet the needs of our growing customer base and to maintain performance as our customers expand their use of our solutions, we may not be able to grow as quickly as anticipated, customers may reduce or cancel use of our solutions and we may be unable to compete as effectively and our business and results of operations may be harmed.

Additionally, we have made, and we will continue to make, substantial investments to support growth at our data centers partners and improve the profitability of our cloud platform. If our cloud-based server costs were to increase or pricing pressure causes price movements out of proportion with changes in unit operating and maintenance costs, our business, results of operations and financial condition may be adversely affected. Although we expect that we will receive similar services from other third parties, if any of our arrangements with third-party providers are terminated, we could experience interruptions on our platform and in our ability to make our solutions available to customers, as well as delays and additional expenses in arranging alternative cloud infrastructure services. Ongoing improvements to cloud infrastructure may be more expensive than anticipated and may not yield the expected savings in operating costs or the expected performance benefits. In addition, we may be required to re-invest any cost savings achieved from our prior cloud infrastructure improvements in future infrastructure projects to maintain the levels of service required by our customers. We may not be able to maintain or achieve cost savings from our investments, which could harm our financial results.

The success of our business will depend in part on our ability to protect and enforce our intellectual property rights.

We believe that our intellectual property is an essential asset of our business, and our success and ability to compete will depend in part upon protection of intellectual property rights. We have relied, and we will continue to rely, on a combination of patent, copyright, trademark, and trade secret laws, as well as confidentiality procedures and contractual provisions, to establish and protect our intellectual property rights in the United States and abroad, all of which provide only limited protection. The efforts we have taken to protect our intellectual property may not be sufficient or effective, and our trademarks, copyrights and patents may be held invalid or unenforceable. Moreover, we cannot assure you that any patents will be issued with respect to our currently pending patent applications, including in a manner that will give us adequate defensive protection or competitive advantages, or that any patents issued to us will not be challenged, invalidated or circumvented. We have filed for patents in the United States and in certain non-U.S. jurisdictions, but such protections may not be available in all countries in which we will operate or in which we will seek to enforce intellectual property rights, or the intellectual property rights may be difficult to enforce in practice. For example, many foreign countries have compulsory licensing laws under which a patent owner must grant licenses to third parties under certain circumstances. In addition, many countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. Moreover, we may need to expend additional resources to defend our intellectual property rights in these countries, and our inability to do so could impair our business or adversely affect our plans for international expansion. Our currently issued patents and any patents that may be issued in the future with respect to pending or future patent applications may not provide sufficiently broad protection or they may not prove to be enforceable in actions against alleged infringers.

We may not be effective in policing unauthorized use of our intellectual property, and even if we do detect violations, litigation may be necessary to enforce our intellectual property rights. Protecting against the unauthorized use of intellectual property rights, technology and other proprietary rights is expensive and difficult, particularly outside of the United States. Any enforcement efforts undertaken, including litigation, could be time-consuming and expensive and could divert management’s attention, which could harm our business and results of operations. Further, attempts to enforce rights against third parties could also provoke these third parties to assert their own intellectual property or other rights against us, or challenge our intellectual property rights which could result in a holding that invalidates or narrows the scope of our intellectual property rights, in whole or in part. The inability to adequately protect and enforce our intellectual property and other proprietary rights could seriously harm our business, results of operations and financial condition. Even if we are able to secure our intellectual property rights, we cannot assure you that such rights will provide us with competitive advantages or distinguish our services from those of our competitors or that our competitors will not independently develop similar technology, duplicate any of our technology, or design around our patents.

Claims by others that we infringe their proprietary technology or other intellectual property rights could result in significant costs and substantially harm our business, financial condition, results of operations and prospects.

Claims by others that we infringe or misappropriate their proprietary technology or other intellectual property rights could harm our business. Companies in the cybersecurity industry could hold patents and also protect their copyright, trade secret and other intellectual property rights, entering into litigation based on allegations of patent infringement or other violations of intellectual property rights. We will face increasing competition as we grow and the possibility of intellectual property rights claims against us could also grow. In addition, to the extent we hire personnel from competitors, we may be subject to allegations that such personnel have divulged proprietary or other confidential information of competitors to us. From time to time, third parties may assert claims of infringement or misappropriation of intellectual property rights against us. Although there have been no such claims made against us to date, there can be no assurance that such claims may not be made in the future.

Third parties may in the future also assert claims against our customers or distribution partners, whom our standard license and other agreements may obligate us to indemnify against claims that our solutions infringe the intellectual property rights of third parties. As the number of products and competitors in the cybersecurity market increases and overlaps occur, claims of infringement, misappropriation, and other violations of intellectual property rights may increase. While we intend to increase the size of our patent portfolio, many of our competitors and others may now and in the future have significantly larger and more mature patent portfolios.
than we have. In addition, future litigation may involve non-practicing entities, companies, or other patent owners who have no relevant product offerings or revenue and against whom our own patents may therefore provide little or no deterrence or protection. Any claim of intellectual property infringement by a third party, even a claim without merit, could cause us to incur substantial costs defending against such claim, could distract our management from our business and could require us to cease use of such intellectual property.

Additionally, our insurance may not cover intellectual property rights infringement claims that may be made. In the event that we fail to successfully defend ourselves against an infringement claim, a successful claimant could secure a judgment or otherwise require payment of legal fees, settlement payments, ongoing royalties, or other costs or damages; or we may agree to a settlement that prevents us from offering certain services or features; or we may be required to obtain a license, which may not be available on reasonable terms, or at all, to use the infringing technology. If we are prevented from using a certain technology or intellectual property, we may be required to develop alternative, non-infringing technology, which could require significant time, during which we could be unable to continue to offer our affected services or features, effort and expense, and may ultimately not be successful.

Although third parties may offer a license to their technology or other intellectual property, the terms of any offered license may not be acceptable, and the failure to obtain a license or the costs associated with any license could cause our business, financial condition and results of operations to be adversely affected. In addition, some licenses may be nonexclusive, and therefore our competitors may have access to the same technology licensed to us. If a third party does not offer us a license to its technology or other intellectual property on reasonable terms, or at all, we could be enjoined from continued use of such intellectual property. As a result, we may be required to develop alternative, non-infringing technology, which could require significant time, during which we could be unable to continue to offer our affected products, subscriptions or services, effort, and expense and may ultimately not be successful. Any of these events could harm our business, financial condition and results of operations.

We license technology from third parties, and our inability to maintain those licenses could harm our business. We currently incorporate, and will in the future incorporate, technology that we license from third parties, including software, into our solutions. We cannot be certain that our licensors do not or will not infringe on the intellectual property rights of third parties or that our licensors have or will have sufficient rights to the licensed intellectual property in all jurisdictions in which we may sell our platform. Some of our agreements with our licensors may be terminated by them for convenience, or otherwise provide for a limited term. If we are unable to continue to license technology because of intellectual property infringement claims brought by third parties against our licensors or us, or if we are unable to continue the license agreements or enter into new licenses on commercially reasonable terms, our ability to develop and sell solutions and services containing that technology would be limited, and our business could be harmed. Additionally, if we are unable to license technology from third parties, we may be forced to acquire or develop alternative technology, which we may be unable to do in a commercially feasible manner or at all, and may require us to use alternative technology of lower quality or performance standards. This could limit or delay our ability to offer new or competitive solutions and increase our costs. As a result, our margins, market share, and results of operations could be significantly harmed.

If we are not able to satisfy data protection, security, privacy, and other government- and industry-specific requirements or regulations, our business, results of operations, and financial condition could be harmed. Personal privacy, data protection, information security, telecommunications regulations, and other laws, regulations, and industry standards (including proposed new or proposed versions) applicable to specific categories of information are significant issues in the United States, Europe, and in other key jurisdictions where we offer our solutions, including in South and East Asia and the Middle East. The data that we collect, analyze and store is subject to a variety of laws and regulations, including regulation by various government agencies. The U.S. federal government, and various state and foreign governments, have adopted or proposed limitations on the collection, distribution, use, and storage of certain categories of information, such as PII of individuals, health information, and other sector-specific types of data, including but not limited to regulations promulgated by Federal Trade Commission and under the provisions of the Electronic Communication Privacy Act, Computer Fraud and Abuse Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act. Laws and regulations outside the United States, and particularly in Europe, often are more restrictive than those in the United States. Such laws and regulations may require companies to implement privacy and security policies, permit customers to access, correct, and delete personal information stored or maintained by such companies, inform individuals of security breaches that affect their personal information, and, in some cases, obtain individuals’ consent to use PII for certain purposes. In addition, some foreign governments require that any information of certain categories, such as financial or PII collected in a country not be transferred outside of that country without consent. We also may find it necessary or desirable to join industry or other self-regulatory bodies or other information security or data protection-related organizations that require compliance with their rules pertaining to information security and data protection. We also may be bound by additional, more stringent contractual obligations relating to our collection, use and disclosure of personal, financial and other data. We cannot yet determine the impact of future laws, regulations, standards, or perception of their requirements may have on our business. For example, the European Commission adopted the European General Data Protection Regulation ("GDPR"), that applies to the processing of certain personal data of data subjects in the European Economic Area ("EEA"). As compared to previously data protection law in the European Union, the GDPR imposes additional obligations and risk upon our business and increases substantially the penalties to which we could be subject in the event of any non-compliance. Administrative fines for certain violations under the GDPR can amount up to 20 million Euros or four percent of worldwide annual revenue for the prior fiscal year, whichever is higher. We have incurred substantial expense in complying with the obligations imposed by the GDPR, and we may be required to do so in the future, potentially making significant changes in our business operations, which may adversely affect our revenue and our business overall. Additionally, we are unable to predict how obligations under the GDPR will be applied to us or our customers.

Among other requirements, the GDPR regulates transfers of personal data subject to the GDPR to third countries that have not been found to provide adequate protection to such personal data, including the United States. We have undertaken certain efforts to conform transfers of personal data from the EEA to the United States and other jurisdictions based on our understanding of current regulatory obligations and the guidance of data protection authorities. Despite this, we may be unsuccessful in establishing or maintaining conforming means of transferring such data from the EEA, in particular as a result of continued legal and legislative activity within the European Union. For example, in July 2020 the European Court of Justice (“ECJ”) invalidated the EU-U.S. Privacy Shield in a decision known as Schrems II. The ECJ’s decision also raised questions about the continued validity of one of the primary alternatives to the EU-U.S. Privacy Shield, namely the European Commission’s Standard Contractual Clauses, and EU regulators have issued additional guidance regarding considerations and requirements that we and other companies must consider and undertake when using the Standard Contractual Clauses. Although the EU has presented a new set of contractual clauses, at present, there are few, if any, viable alternatives to the EU-U.S. Privacy Shield and the Standard Contractual Clauses. The ECJ’s decision and other regulatory guidance or developments otherwise may impose additional obligations with respect to the transfer of personal data from the EU and Switzerland to the United States, each of which could restrict our activities in those jurisdictions, limit our ability to provide products and services in those jurisdictions, or increase our costs and obligations and impose limitations upon our ability to efficiently transfer personal data from the EU and Switzerland to the United States.

Further, the exit of the United Kingdom (UK) from the EU, often referred to as Brexit, has created uncertainty with regard to data protection regulation in the UK. Specifically, the UK exited the EU on January 1, 2020, subject to a transition period that ended December 31, 2020. While the Data Protection Act of 2018, that “implements” and complements the GDPR achieved Royal Assent on May 23, 2018 and is now effective in the United Kingdom, it is still unclear whether transfer of data from the EEA to the United Kingdom will remain lawful in the long term under GDPR. With the expiration of the transition period, companies will have to comply with the GDPR and the GDPR as incorporated into United Kingdom national law, which has the ability to separately fine up to the greater of £17.5 million or 4% of global turnover. On June 28, 2021, the European Commission announced a decision of “adequacy” concluding that the UK ensures an equivalent level of data protection to the GDPR, which provides some relief regarding the legality of continued personal data flows from the EEA to the UK. Some uncertainty remains, however, as this adequacy determination must be renewed after four years and may be modified or revoked in the interim. We cannot fully predict how the Data Protection Act, the UK GDPR, and other UK data protection laws or regulations may develop in the medium to longer term nor the effects of divergent laws and guidance regarding how data transfers to and from the UK will be regulated.
The implementation of the GDPR has led other jurisdictions to either amend, or propose legislation to amend their existing data privacy and cybersecurity laws to resemble all or a portion of the requirements of the GDPR. For example, on June 28, 2018, California adopted the California Consumer Privacy Act of 2018, or CCPA, which went into effect on January 1, 2020. The CCPA has been characterized as the first “GDPR-like” privacy statute to be enacted in the United States because it contains a number of provisions similar to certain provisions of the GDPR. In addition, the California Privacy Rights Act of 2020, or the CPRA was passed by California voters in November 2020. The CPRA amends the CCPA by creating additional privacy rights for California consumers and additional obligations on businesses, which could subject us to additional compliance costs as well as potential fines, individual claims and commercial liabilities. The majority of the CPRA provisions took effect on January 1, 2023. The CCPA and CPRA could mark the beginning of a trend toward more stringent privacy legislation in the United States, as other states or the federal government may follow California’s lead and increase protections for U.S. residents. For example, on March 2, 2021, the Virginia Consumer Data Protection Act, which took effect on January 1, 2023, was signed into law and on June 8, 2021, Colorado enacted the Colorado Privacy Act (the “CPA”), which also takes effect on July 1, 2023.

Evolving and changing definitions of personal data and personal information within the European Union, the United States, and elsewhere, especially relating to classification of IP addresses, machine identification, location data and other information, may limit or inhibit our ability to operate or expand our business, including limiting partnerships that may involve the sharing of data. Further, we may be affected by evolving notions of data sovereignty, or the concept that data collected in a particular jurisdiction must be either physically maintained in that jurisdiction or maintained in compliance with all local law, including under all conditions or controls mandated by the jurisdiction in which it was collected. In light of current regulatory trends, such data sovereignty requirements may increase causing us to expend additional resources and increase our applicable budgets to remain compliant or cease doing business in such jurisdiction.

Even the perception of privacy or security concerns, whether or not valid, may harm our reputation, inhibit adoption of our products by current and future customers, or adversely impact our ability to attract and retain workforce talent. In addition, changes in laws or regulations that adversely affect the use of the internet, including laws impacting net neutrality, could impact our business. We expect that existing laws, regulations and standards may be interpreted in new manners in the future. Future laws, regulations, standards, and other obligations, and changes in the interpretation of existing laws, regulations, standards and other obligations could require us to modify our solutions, restrict our business operations, increase our costs and impair our ability to maintain and grow our customer base and increase our revenue.

Beyond broader data processing regulations affecting our business, the cybersecurity industry may face direct regulation. In 2018, Singapore introduced what is believed to be the world’s first cybersecurity licensing requirement, mandating that providers of specific types of incident response services receive a government license before providing such services. License requirements such as these may impose upon us significant organizational costs and high barriers of entry into new markets.

Although we have worked and will continue to work to comply with applicable laws and regulations, certain applicable industry standards and our contractual obligations and other legal obligations, along with laws, regulations, standards and obligations are evolving and may be modified, interpreted and applied in an inconsistent manner from one jurisdiction to another, and may conflict with one another. In addition, they may conflict with other requirements or legal obligations that apply to us or our business or the security features and services that our customers expect from our solutions. As such, we cannot assure ongoing compliance with all such laws, regulations, standards and obligations. Any failure or perceived failure by us or our employees, representatives, contractors, distribution partners, agents, intermediaries, or other third parties to comply with applicable laws and regulations, or applicable industry standards that we represent compliance with or that may be asserted to apply to us, or to comply with employee, customer, partner, and other data privacy and data security requirements pursuant to contract and our stated notices or policies, could result in enforcement actions, including fines, imprisonment of company officials and public censure, claims for damages by customers and other affected individuals, damage to our reputation and loss of goodwill (both in relation to existing customers and prospective customers), or any of which could have a material adverse effect on our operations, financial performance and business. Any inability of us or our employees, representatives, contractors, distribution partners, agents, intermediaries, or other third parties to adequately address privacy and security concerns, even if unfounded, or comply with applicable laws, regulations, standards and obligations, could result in additional cost and liability to us, damage our reputation, inhibit sales, and adversely affect our business and results of operations.

Failure to comply with laws and regulations applicable to our business could subject us to fines and penalties and could also cause us to lose customers in the public sector or negatively impact our ability to contract with the public sector.

Our business is subject to regulation by various federal, state, local and foreign governmental agencies, including agencies responsible for monitoring and enforcing privacy and data protection laws and regulations, employment and labor laws, workplace safety, product safety, environmental laws, consumer protection laws, anti-bribery laws, import and export controls, federal securities laws and tax laws and regulations. In certain jurisdictions, these regulatory requirements may be more stringent than in the United States. Noncompliance by us, our employees, representatives, contractors, distribution partners, agents, intermediaries, or other third parties with applicable regulations or requirements could subject us to:

- investigations, enforcement actions and sanctions;
- mandatory changes to our platform;
- disgorgement of profits, fines and damages;
- civil and criminal penalties or injunctions;
- claims for damages by our customers or distribution partners;
- termination of contracts;
- loss of intellectual property rights; and
- temporary or permanent debarment from sales to government organizations.

If any governmental sanctions are imposed, or if we do not prevail in any possible civil or criminal litigation, our business, results of operations and financial condition could be adversely affected. In addition, responding to any action will likely result in a significant diversion of management’s attention and resources and an increase in professional fees. Enforcement actions and sanctions could harm our business, results of operations and financial condition.

We endeavor to properly classify employees as exempt versus non-exempt under applicable law. Although there are no pending or threatened material claims or investigations against us asserting that some employees are improperly classified as exempt, the possibility exists that some of our current or former employees could be classified as exempt employees.

These laws and regulations will impose added costs on our business, and failure by us, our employees, representatives, contractors, distribution partners, agents, intermediaries, or other third parties to comply with these or other applicable regulations and requirements could lead to claims for damages, penalties, termination of contracts, loss of exclusive rights in our intellectual property and temporary suspension or permanent debarment from government contracting. Any such damages, penalties, disruptions or limitations in our ability to do business with the public sector could result in reduced sales of our products, substantial product inventory write-offs, reputational damage, penalties, and other sanctions, any of which could harm our business, reputation, and results of operations.

We are subject to laws and regulations, including governmental export and import controls, sanctions, and anti-corruption laws, that could impair our ability to compete in our markets and subject us to liability if we are not in full compliance with applicable laws.

We are subject to laws and regulations, including governmental export controls, that could subject us to liability or impair our ability to compete in our markets. Our products are subject to U.S. export controls, including the U.S. Department of Commerce’s Export Administration Regulations, and we and our employees,
representatives, contractors, agents, intermediaries, and other third parties are also subject to various economic and trade sanctions regulations administered by the U.S. Treasury Department’s Office of Foreign Assets Control and other governmental authorities. We incorporate standard encryption algorithms into our products, which, along with the underlying technology, may be exported outside of the U.S. only with the required export authorizations, including by license, license exception or other appropriate government authorizations, which may require the filing of further encryption registration and classification requests. Furthermore, U.S. export control laws and economic sanctions prohibit the shipment of certain cloud-based solutions to countries, governments, and persons targeted by U.S. sanctions. Governmental regulation of the import or export of our products, or our failure to obtain any required import or export authorization for our products under the laws of the United States or other countries, could harm our ability to engage in international trade and adversely affect our revenue. Moreover, any new export or import restrictions, new legislation or shifting approaches in the enforcement or scope of existing regulations, or in the countries, persons or technologies targeted by such regulations, could result in decreased use of our products by, or in our decreased ability to export our products to existing or potential customers or to conduct business with foreign parties. An actual or alleged violation of these laws or regulations would negatively affect our business, financial condition and results of operations.

Various countries regulate the import of certain encryption technology, including through import permit and license requirements, and have enacted laws that could limit our ability to distribute our products or could limit our customers’ ability to implement our products in those countries. Changes in our products or changes in export and import regulations may create delays in the introduction of our products into international markets, prevent our customers with international operations from deploying our products globally or, in some cases, prevent the export or import of our products to certain countries, governments or persons altogether. Any change in export or import regulations, economic sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons or technologies targeted by such regulations, could result in decreased use of our products by, or in our decreased ability to export or sell our products to, existing or potential customers with international operations. Under these global trade and sanctions laws and regulations, as well as other laws governing our operations, various government agencies may seek to impose modifications to business practices, including cessation of business activities in sanctioned countries or with sanctioned persons or entities and modifications to compliance programs, which may increase compliance costs, and may subject us to fines, penalties and other sanctions. Any decreased use of our products or limitation on our ability to export or sell our products would likely adversely affect our business, results of operations and financial condition.

We are also subject to the U.S. Foreign Corrupt Practices Act of 1977 ("FCPA"), the U.K. Bribery Act 2010 (the "Bribery Act"), and other anti-corruption, sanctions, anti-bribery, anti-money laundering and similar laws in the United States and other countries in which it conducts activities. Anti-corruption and anti-bribery laws, which have been enforced aggressively and are interpreted broadly, prohibit companies and their employees, agents, intermediaries, and other third parties from promising, authorizing, making or offering improper payments or other benefits to government officials and others in the private sector. We leverage third parties, including intermediaries, agents, and distribution partners, to conduct our business in the United States and abroad, to sell subscriptions to our platform and to collect information about cyber threats. We and these third-parties may have direct or indirect interactions with officials and employees of government agencies or state-owned or affiliated entities and may be held liable for the corrupt or other illegal activities of these third-party business partners and intermediaries, our employees, representatives, contractors, distribution partners, agents, intermediaries, and other third parties, even if we do not explicitly authorize such activities.

While we have, and we will continue to have, policies and procedures to address compliance with FCPA, Bribery Act and other applicable anti-corruption, sanctions, anti-bribery, anti-money laundering and similar laws, we cannot assure you that they will be effective, or that all of our employees, representatives, contractors, distribution partners, agents, intermediaries, or other third parties have taken, or will not take actions, in violation of our policies and applicable law, for which we may be ultimately held responsible. As we increase our international sales and business, our risks under these laws may increase. Noncompliance with these laws could subject us to investigations, severe criminal or civil sanctions, settlements, prosecution, loss of export privileges, suspension or debarment from U.S. government contracts, other enforcement actions, disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, whistleblower complaints, adverse media coverage and other consequences. Any investigations, actions, or sanctions could harm our reputation, business, results of operations, and financial condition.

We also collect information about cyber threats from open sources, intermediaries, and third parties that we make available to our customers. While we have implemented certain procedures to facilitate compliance with applicable laws and regulations in connection with the collection of this information, we cannot assure you that these procedures have been effective or that we, or third parties, many of whom we do not control, have complied with all laws or regulations in this regard. Failure by us or our employees, representatives, contractors, distribution partners, agents, intermediaries, or other third parties to comply with applicable laws and regulations in the collection of this information also could have negative consequences, including reputational harm, government investigations and penalties.

Although we have taken precautions to prevent our information collection practices and services from being provided in violation of such laws, our information collection practices and services may have been in the past, and could in the future be, provided in violation of such laws. If we or our employees, representatives, contractors, distribution partners, agents, intermediaries, or other third parties fail to comply with these laws and regulations, we could be subject to civil or criminal penalties, including the possible loss of export privileges and fines. We may also be adversely affected through reputational harm, loss of access to certain markets, or otherwise. Obtaining the necessary authorizations, including any required license, for a particular transaction may be time-consuming, is not guaranteed and may result in the delay or loss of sales opportunities.

Some of our technology incorporates “open source” software, which could negatively affect our ability to sell our platform and subject us to possible litigation.

Our products and subscriptions contain third-party open source software components, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products and subscriptions. The use and distribution of open source software may entail greater risks than the use of third-party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code. Many of the risks associated with use of open source software cannot be eliminated and could negatively affect our business. In addition, the wide availability of source code used in our solutions may increase the risk of security vulnerabilities, which may result in delays in the introduction of our products, decreased use of our products or decreased ability to export our products to existing or potential customers with international operations. Under these global trade and sanctions laws and regulations, as well as other laws governing our operations, various government agencies may seek to impose modifications to business practices, including cessation of business activities in sanctioned countries or with sanctioned persons or entities and modifications to compliance programs, which may increase compliance costs, and may subject us to fines, penalties and other sanctions. Any decreased use of our products or limitation on our ability to sell our products would likely adversely affect our business, results of operations and financial condition.

Some open source licenses contain requirements that we must make available source code for modifications or derivative works we create based upon the type of open source software we use. If we use our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release the source code of our proprietary software to the public, including authorizing further modification and redistribution, or otherwise be limited in the licensing of our services, each of which could provide an advantage to our competitors or other entrants to the market, create security vulnerabilities in our solutions, require us to re-engineer all or a portion of our platform, and could reduce or eliminate the value of our services. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales.

The terms of many open source licenses have not been interpreted by U.S. courts, and there is a risk that these licenses could be construed in ways that could impose unanticipated conditions or restrictions on our ability to commercialize products and subscriptions incorporating such software. Moreover, we cannot assure you that our processes for controlling our use of open source software in our products and subscriptions has been or will be effective. From time to time, we may face claims from third parties asserting ownership of, or demanding release of, the open source software or derivative works that we developed using such software (which could include our proprietary source code), or otherwise seeking to enforce the terms of the applicable open source license. These claims could result in litigation. Litigation could be costly to defend, have a negative effect on our results of operations and financial condition or require us to devote additional research and development resources to change our solutions. Responding to any infringement or noncompliance claim by an open source vendor, regardless of its validity, discovering certain open source software code in our platform, or a finding that we have breached the terms of an open source software license, could harm our business, results of operations and financial condition, by, among other things:

• resulting in time-consuming and costly litigation;
• diverting management’s time and attention from developing our business;
• requiring us to pay monetary damages or enter into royalty and licensing agreements that we would not normally find acceptable;
• causing delays in the deployment of our platform or service offerings to our customers;
• requiring us to stop offering certain services or features of our platform;
• requiring us to redesign certain components of our platform using alternative non-infringing or non-open source technology, which could require significant effort and expense;
• requiring us to disclose our software source code and the detailed program commands for our software;
• prohibiting us from charging license fees for the proprietary software that uses certain open source; and
• requiring us to satisfy indemnification obligations to our customers.

We provide service level commitments under some of our customer contracts. If we fail to meet these contractual commitments, we could be obligated to provide credits for future service and our business could suffer. Certain of our customer agreements contain service level commitments, which contain specifications regarding the availability and performance of our platform. Any failure of or disruption to our infrastructure could impact the performance of our platform and the availability of services to customers. If we are unable to meet our stated service level commitments or if we suffer extended periods of poor performance or unavailability of our platform, we may be contractually obligated to provide affected customers with service credits for future subscriptions, and, in certain cases, refunds. To date, there has not been a material failure to meet our service level commitments, and we do not currently have any material liabilities accrued on our balance sheet for such commitments. However, our revenue, other results of operations and financial condition could be harmed if we suffer performance issues or downtime that exceeds the service level commitments under our agreements with our customers.

We may become involved in litigation that may adversely affect us.

We may be subject to claims, suits and government investigations and other proceedings including patent, product liability, class action, whistleblower, personal injury, property damage, labor and employment, commercial disputes, compliance with laws and regulatory requirements and other matters, and we may become subject to additional types of claims, suits, investigations and proceedings as our business develops. While we believe that we have acted in compliance in all material respects with applicable antitrust laws, such investigation, as well as any other claims, suits, and government investigations and proceedings that may be asserted against us in the future, are inherently uncertain and their results cannot be predicted with certainty. Regardless of outcome, any of these types of legal proceedings could have an adverse impact on us because of legal costs and diversion of management attention and resources, and could cause us to incur significant expenses or liability, adversely affect our brand recognition, and/or require us to change our business practices. The expense of litigation and the timing of this expense from period to period are difficult to estimate, subject to change and could adversely affect our results of operations. It is possible that a resolution of one or more such proceedings could result in substantial damages, settlement costs, fines and penalties that could adversely affect our business, consolidated financial position, results of operations, or cash flows in a particular period. These proceedings could also result in reputational harm, sanctions, consent decrees, or orders requiring a change in our business practices. Because of the potential risks, expenses and uncertainties of litigation, we may, from time to time, settle disputes, even where we have meritorious claims or defenses, by agreeing to settlement agreements. Because litigation is inherently unpredictable, we cannot assure you that the results of any of these actions will not have a material adverse effect on our business, financial condition, results of operations, and prospects.

Our ability to maintain customer satisfaction will depend in part on the quality of our customer support.

Once our platform is deployed within our customers’ networks, our customers depend on our customer support services to resolve any issues relating to implementation and maintenance of the platform. If we do not provide effective ongoing support, our ability to sell additional subscriptions to existing customers would be adversely affected and our reputation with potential customers could be damaged. Many larger organizations have more complex networks and require higher levels of support than smaller customers. Failure to maintain high-quality customer support could also have a material adverse effect on our business, results of operations and financial condition.

We may need to raise additional capital to maintain and expand our operations and invest in new solutions, which capital may not be available on terms acceptable to us, or at all, and which could reduce our ability to compete and could harm our business.

Retaining or expanding our current levels of personnel and products offerings may require additional funds to respond to business challenges, including the need to develop new products and enhancements to our platform, improve our operating infrastructure, or acquire complementary businesses and technologies. The failure to raise additional capital or generate the significant capital necessary to expand our operations and invest in new products could reduce our ability to compete and could harm our business. Accordingly, we may need to engage in additional equity or debt financings to secure additional funds. If we raise additional equity financing, stockholders may experience significant dilution of their ownership interests and the market price of the common stock could decline. If we engage in debt financing, the holders of debt would have priority over the holders of common stock, and we may be required to accept terms that restrict our operations or our ability to incur additional indebtedness or to take other actions that would otherwise be in the interests of the debt holders. Any of the above could harm our business, results of operations and financial condition.

Our business is subject to the risks of warranty claims, product returns, product liability, and product defects from real or perceived defects in our solutions or their misuse by customers or third parties, and indemnity provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses.

We may be subject to liability claims for damages related to errors or defects in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our products may harm our business and results of operations. Although we generally have limitations of liability provisions in our terms and conditions of sale, these provisions may not fully or effectively protect us from claims as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the United States or other countries. These provisions may also be negotiated to varying levels with different customers. The sale and support of products also entails the risk of product liability claims. Additionally, our agreements with customers and other third parties typically include indemnification or other provisions under which we agree to indemnify or otherwise be liable to them for losses suffered or incurred as a result of claims regarding intellectual property infringement, breach of agreement, including confidentiality, privacy and security obligations, violation of applicable laws, damages caused by failures of our solutions or to property or persons, or other liabilities relating to or arising from our products and services, or other acts or omissions. These contractual provisions often survive termination or expiration of the applicable agreement. As we continue to grow, the possibility of these claims against us will increase. Large indemnity obligations, whether for intellectual property or other claims, could harm our business, results of operations and financial condition.

Additionally, our platform and solutions may be used by our customers and other third parties who obtain access to our solutions for purposes other than for which the platform was intended. For example, the platform might be misused by a customer to monitor an employee’s activities in a manner that violates the employee’s privacy rights under applicable law. During the course of performing certain solution-related services and professional services, our teams may have significant access to our customers’ networks. We cannot be sure that a disgruntled employee or customer may not take advantage of such access, which may make our customers vulnerable to malicious activity by such employee. Any such misuse of our platform could result in negative press coverage and negatively affect our reputation, which could result in harm to our business, reputation and results of operations.
We derive 15% and 10% of our total revenue from our international customers for fiscal year 2023 and fiscal year 2022, respectively. Our growth strategy includes expansion into target geographies, but there is no guarantee that our international operations expose us to significant risks, and failure to manage those risks could adversely impact our business.

We maintain insurance to protect against certain claims associated with the use of our products, but our insurance coverage may not adequately cover any claim asserted against us. In addition, even claims that ultimately are unsuccessful could result in the expenditure of funds in litigation, divert management’s time and other resources, and harm our business and reputation.

Future acquisitions, strategic investments, partnerships, or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our results of operations and financial condition.

As part of our business strategy, we have in the past completed investments in and/or acquisitions of complementary companies, services, or technologies. However, our ability to acquire and integrate other companies, services, or technologies in a successful manner in the future is not guaranteed. We may not be able to find suitable investment and/or acquisition candidates, and we may not be able to complete such investments and/or acquisitions on favorable terms, if at all. If we do complete investments and/or acquisitions, we may not ultimately strengthen our competitive position or ability to achieve our business objectives, and any investments and/or acquisitions we complete could be viewed negatively by our customers or investors. In addition, if we are unsuccessful at integrating any acquisitions, or the technologies associated with such acquisitions, our revenue and results of operations could be adversely affected. Any integration process may require significant time and resources, and we may not be able to manage the process successfully. We may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an investment or acquisition transaction, including accounting charges. We may have to pay cash, incur debt or issue equity securities to pay for any such acquisition, each of which could adversely affect our financial condition and the market price of our common stock. The sale of equity or issuance of debt to finance any such investment or acquisitions could result in dilution to stockholders. The occurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations.

Additional risks we may face in connection with investments and/or acquisitions include:

- diversion of management time and focus from operating our business to addressing acquisition integration challenges;
- coordination of engineering, analytics, research and development, operations, and sales and marketing functions;
- integration of product and service offerings;
- retention of key employees from the acquired company;
- changes in relationships with strategic partners as a result of product acquisitions or strategic positioning resulting from the acquisition;
- cultural challenges associated with integrating employees from the acquired company into the organization;
- integration of the acquired company’s accounting, management information, human resources and other administrative systems;
- the need to implement or improve controls, procedures, and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies;
- financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that are not adequately addressed and that cause our reported results to be incorrect;
- liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and other known and unknown liabilities;
- unanticipated write-offs or charges; and
- litigation or other claims in connection with the acquired company, including claims from terminated employees, customers, former stockholders or other third parties.

The failure to address these risks or other problems encountered in connection with acquisitions and investments could cause us to fail to realize the anticipated benefits of these investments and/or acquisitions, cause us to incur unanticipated liabilities, and harm our business generally.

Our international operations expose us to significant risks, and failure to manage these risks could adversely impact our business.

We derive 15% and 10% of our total revenue from our international customers for fiscal year 2023 and fiscal year 2022, respectively. Our growth strategy includes expansion into target geographies, but there is no guarantee that such efforts will be successful. These international operations will require significant management attention and financial resources and are subject to substantial risks, including:

- greater difficulty in negotiating contracts with standard terms, enforcing contracts, and managing collections, including longer collection periods;
- higher costs of doing business internationally, including costs incurred in establishing and maintaining office space and equipment for international operations and creating international operating entities, where applicable;
- management communication and integration problems resulting from cultural and geographic dispersion;
- risks associated with trade restrictions and foreign legal requirements, including any importation, certification, and localization of our platform that may be required in foreign countries;
- greater risk of unexpected changes in applicable foreign laws, regulatory practices, tariffs, and tax laws and treaties;
- compliance with anti-bribery laws, including the FCPA, the U.S. Travel Act and the Bribery Act, violations of which could lead to significant fines, penalties, and collateral consequences;
- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;
- the uncertainty of protection for intellectual property rights in some countries;
- general economic and political conditions in these foreign markets;
- foreign exchange controls or tax regulations that might prevent us from repatriating cash earned outside the United States;
- political and economic instability in some countries;
- the potential for foreign government demands for access to information or corporate property;
- double taxation of international earnings and potentially adverse tax consequences due to changes in the tax laws of the United States or the foreign jurisdictions in which we operate;
- unexpected costs for the localization of services, including translation into foreign languages and adaptation for local practices and regulatory requirements;
requirements to comply with foreign privacy, data protection, and information security laws and regulations and the risks and costs of noncompliance;

greater difficulty in identifying, attracting and retaining local qualified personnel, and the costs and expenses associated with such activities;

greater difficulty identifying qualified distribution partners and maintaining successful relationships with such partners;

differing employment practices and labor relations issues; and

difficulties in managing and staffing international offices and increased travel, infrastructure, and legal compliance costs associated with multiple international locations.

Adverse changes in global, regional or local economic conditions, including recession or slowing growth, the COVID-19 pandemic or other global or local health issues, changes or uncertainty in fiscal, monetary, or trade policy, higher interest rates, tighter credit, inflation, lower capital expenditures by businesses including on IT infrastructure, increases in unemployment, and lower consumer confidence and spending, periodically occur. Increased costs for supply chain expenses, driven in part by inflation, have negatively impacted our results of operations and may continue to impact our results of operations. Inflation may also continue to cause increased supply, employee, facilities and infrastructure costs, decreased demand for our services and volatility in the financial markets. To the extent such inflation continues, increases or both, it may reduce our margins and have a material adverse effect on our results of operations.

Additionally, all of our sales contracts are currently denominated in U.S. dollars. However, a strengthening of the U.S. dollar could increase the cost of our solutions to our international customers, which could adversely affect our business and results of operations. In addition, an increasing portion of operating expenses is expected to be incurred outside the United States and denominated in foreign currencies, and will be subject to fluctuations due to changes in foreign currency exchange rates. If we become more exposed to currency fluctuations and are not able to successfully hedge against the risks associated with currency fluctuations, our results of operations could be adversely affected.

In addition, international nation states continue to increase their threats of action against other countries and high profile companies in them, as has most recently been evidenced by statements made by certain leaders relating to the recent military activity in Ukraine. The fact that we provide products and services to high profile customers in many of the countries that have been and remain under such threats and the high profile of leaders associated with us make those customers and us potential targets for attacks by those nation states and their proxies creating additional risks to our ability to continue to expand and operate effectively.

Our success will depend in large part on our ability to anticipate and effectively manage these risks. The expansion of our international operations and entry into additional international markets will require significant management attention and financial resources. Our failure to successfully manage international operations and the associated risks could limit the future growth of our business.

Our ability to use our net operating loss carryforwards and certain other tax attributes may be limited.

As of January 31, 2023 and January 31, 2022, we had aggregate U.S. federal and state net operating loss carryforwards of $111.0 million and $324.8 million, respectively, which may be available to offset future taxable income for income tax purposes.

U.S. federal net operating loss carryforwards generated in taxable years beginning before January 1, 2018 may be carried forward for 20 years to offset future taxable income. Under tax legislation commonly referred to as the Tax Cuts and Jobs Act (the “Tax Act”), as modified by the Coronavirus Aid, Relief, and Economic Security Act (the “CARES Act”), U.S. federal net operating losses generated in taxable years beginning after December 31, 2017, can be carried forward indefinitely, but the deductibility of such net operating loss carryforwards in taxable years beginning after December 31, 2020 is limited to 80% of taxable income. It is uncertain if and to what extent various states will conform their tax laws and regulations to the Tax Act or the CARES Act.

If not utilized, $25.3 million of our U.S. federal net operating loss carryforwards expire on various dates through 2037 and $299.5 million are able to be carried forward indefinitely under current law. Realization of these net operating loss carryforwards depends on future taxable income, and there is a risk that, even if we achieve profitability, our existing carryforwards could expire unused or be subject to limitations and be unavailable to offset future income tax liabilities, which could adversely affect our results of operations.

In addition, under Sections 382 and 383 of the Internal Revenue Code of 1986, as amended (the “Code”), if a corporation undergoes an “ownership change,” generally defined as a greater than 50% change in (by value) in ownership by “5 percent shareholders” over a rolling three-year period, the corporation’s ability to use our pre-change net operating loss carryovers and other pre-change tax attributes to offset our post-change income or taxes may be limited. We may experience ownership changes in the future as a result of shifts in our stock ownership (which may be outside of our control). In addition, at the state level, there may be periods during which the use of net operating loss carryforwards is suspended or otherwise limited, which could accelerate or permanently increase state taxes owed. As a result, if we earn net taxable income, our ability to use pre-change net operating loss carryforwards to offset U.S. federal taxable income may be subject to limitations, which could potentially result in increased future tax liability to us.

Taxing authorities may successfully assert that we should have collected or in the future should collect sales and use, value added or similar taxes, and we could be subject to liability with respect to past or future sales, which could adversely affect our results of operations.

We do not collect sales and use, value added or similar taxes in all jurisdictions in which we have sales because we have been advised that such taxes are not applicable to our services in certain jurisdictions. Sales and use, value added, and similar tax laws and rates vary greatly by jurisdiction. Certain jurisdictions in which we do not collect such taxes may assert that such taxes are applicable, which could result in tax assessments, penalties and interest, to us or our customers for the past amounts, and we may be required to collect such taxes in the future. If we are unsuccessful in collecting such taxes from our customers, we could be held liable for such costs, which may adversely affect our results of operations.

Our operations and intercompany arrangements will be subject to the tax laws of various jurisdictions, and we could be obligated to pay additional taxes, which would harm our results of operations.

We plan to expand our international operations and staff to support our business in international markets. We expect that we will generally conduct international operations through wholly owned subsidiaries and may be required to register with and obtain licenses from, as applicable, relevant taxing authorities in various jurisdictions. The amount of taxes paid in different jurisdictions may depend on the application of the tax laws of the various jurisdictions, including the United States, to our international business activities, changes in tax rates, new or revised tax laws or interpretations of existing tax laws and policies, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements. The relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. If such a disagreement were to occur, and our position was not sustained, we could be required to pay additional taxes, interest and penalties, which could result in one-time tax charges, higher effective tax rates, reduced cash flows and lower overall profitability of our operations.

We will be subject to U.S. federal, state, and local income, sales, and other taxes in the United States and income, withholding, transaction, and other taxes in numerous foreign jurisdictions. Significant judgment will be required in evaluating our tax positions and our worldwide provision for taxes. During the ordinary course of our business, there are many activities and transactions for which the ultimate tax determination may be uncertain. In addition, our tax obligations and effective tax rates could be adversely affected by changes in the relevant tax, accounting and other laws, regulations, principles and interpretations, including those relating to income tax nexus, by recognizing tax losses or lower than anticipated earnings in jurisdictions where we have lower statutory rates and higher than anticipated earnings in jurisdictions where we have higher statutory rates, by changes in foreign currency exchange rates, or by changes in the valuation of our deferred tax assets and liabilities. We may be audited in various jurisdictions, and such jurisdictions may assess additional taxes, sales taxes and value added taxes.
against it. Even if we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have an adverse effect on our results of operations or cash flows in the period or periods for which a determination is made.

If our estimates or judgments on our critical accounting policies prove to be incorrect or financial reporting standards or interpretations change, our results of operations could be adversely affected.

The preparation of financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the amounts reported in our consolidated financial statements and accompanying notes. We have historically based our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as discussed in the section titled “Management’s Discussion and Analysis of Financial Condition and Results of Operations.” The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant assumptions and estimates used in preparing our consolidated financial statements will include, and may include in the future, those related to revenue recognition; allowance for doubtful accounts; costs to obtain or fulfill a contract; valuation of common stock; valuation of stock-based compensation; carrying value and useful lives of long-lived assets; loss contingencies; and the provision for income and related deferred taxes. Our results of operations may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our results of operations to fall below the expectations of industry or financial analysts and investors, resulting in a decline in the market price of the common stock.

Additionally, we will regularly monitor our compliance with applicable financial reporting standards and review new pronouncements and drafts thereof that are relevant to us. As a result of new standards, changes to existing standards and changes in their interpretation, we might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems so that they reflect new or amended financial reporting standards, or we may be required to restate our published financial statements. Such changes to existing standards or changes in their interpretation may have an adverse effect on our reputation, business, financial position and profit, or cause an adverse deviation from our revenue and operating profit targets, which may negatively impact our financial results.

Our business will be subject to the risks of natural catastrophic events and to interruption by man-made problems such as power disruptions, computer viruses, data security breaches or terrorism.

A significant natural disaster, such as an earthquake, a fire, a flood, or significant power outage could have a material adverse impact on our business, results of operations and financial condition. Natural disasters could affect our personnel, data centers, supply chain, manufacturing vendors, or logistics providers’ ability to provide materials and perform services such as manufacturing products or assisting with shipments on a timely basis. In addition, climate change could result in an increase in the frequency or severity of natural disasters. In the event that we or our service providers’ information technology systems or manufacturing or logistics abilities are hindered by any of the events discussed above, we could result in missed financial targets, such as revenue, for a particular quarter. In addition, computer malware, viruses and computer hacking, fraud, theft and phishing attacks have become more prevalent in the cybersecurity industry, and our internal systems may be victimized by such attacks. Likewise, we could be subject to other man-made problems, including but not limited to power disruptions, terrorist acts and the ongoing conflict between Russia and Ukraine.

Although we maintain incident management and disaster response plans, in the event of a major disruption caused by a natural disaster or man-made problem, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in our development activities, lengthy interruptions in service, breaches of data security and loss of critical data, and our insurance may not cover such events or may be insufficient to compensate it for the potentially significant losses we may incur. Acts of terrorism and other geo-political unrest could also cause disruptions in our business or the business of our supply chain, manufacturers, logistics providers, partners, or customers or the economy as a whole. Any disruption to our supply chain, manufacturers, logistics providers, partners or customers that impacts sales at the end of a fiscal quarter could have a significant adverse impact on our financial results. All of the aforementioned risks may be further increased if disaster recovery plans prove to be inadequate. To the extent that any of the above should result in delays or cancellations of customer orders, or the delay in the manufacture, deployment, or shipment of our products, our business, financial condition, and results of operations would be adversely affected.

Our management previously identified material weaknesses in our internal control over financial reporting, which resulted in a restatement of our unaudited condensed consolidated financial statements in a prior fiscal year. In the future, we may identify additional material weaknesses or otherwise fail to maintain effective internal control over financial reporting, which may result in material misstatements of our financial statements or cause us to fail to meet our periodic reporting obligations.

In connection with the preparation and audit of our consolidated financial statements for the fiscal year ended January 31, 2022, we and our independent registered public accounting firm identified material weaknesses in our internal control over financial reporting. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of our annual or interim financial statements will not be prevented or detected on a timely basis. We did not have a sufficient number of personnel with an appropriate degree of accounting and internal controls knowledge, experience, and training to appropriately analyze, record and disclose accounting matters commensurate with our accounting and reporting requirements, which resulted in an inability to consistently establish appropriate authorities and responsibilities in pursuit of our financial reporting objectives. This material weakness contributed to the following additional separation of duties material weaknesses in that certain personnel had the ability to both (i) create and post journal entries within our general ledger system, and (ii) prepare and review account reconciliations. We did not design and maintain effective controls over information technology (“IT”) general controls for information systems that are relevant to the preparation of our financial statements. Specifically, we did not design and maintain: (i) program change management controls for the financial systems to ensure that information technology program and data changes affecting financial IT applications and underlying accounting records are identified, tested, authorized and implemented appropriately; (ii) appropriate user access controls to ensure appropriate segregation of duties and that adequately restrict user and privileged access to financial applications, programs and data to appropriate personnel; (iii) computer operations controls to ensure data backups are authorized and restorations monitored; and (iv) testing and approval controls for program development to ensure that new software development is aligned with business and IT requirements. We did not design and maintain effective controls over the accounting for stock-based compensation modifications.

As discussed in the Form 8-K as filed with the SEC on April 25, 2022, on April 22, 2022, the Audit Committee of the Board of Directors (the “Audit Committee”) of the Company determined, based on the analysis and recommendation of management, that our unaudited consolidated financial statements and related disclosures included in the Quarterly Report on Form 10-Q for the quarterly period ended October 31, 2021, as filed with the Securities and Exchange Commission (the “SEC”) on December 15, 2021, should no longer be relied upon due to an error. The error was the result of the Company not appropriately applying modification accounting to stock-based compensation awards that were issued and outstanding as of August 26, 2021, the closing date of the merger between the Company and Legacy IronNet. This overstatement relates to stock-based compensation expense for certain of our options and warrants. This restatement relates to stock-based compensation expense for certain of the Company’s outstanding restricted stock units (“RSA’s”) granted pursuant to Legacy IronNet’s 2014 Stock Incentive Plan. We filed an amendment to the Form 10-Q with the SEC on May 2, 2022.

With the oversight of senior management, we have instituted and continue to execute on plans to remediate these material weaknesses and will continue to take remediation steps, including hiring additional key supporting accounting personnel with public company reporting and accounting operations experience, implementing the required segregation of roles and duties both in manual and systems related processes including for journal entries and account reconciliations, and formalizing the documentation and performance of information technology general controls for information systems utilized for financial reporting. While we implement and execute on our plan to remediate the material weaknesses described above, we cannot predict the success of such plans or the outcome of our assessment of these plans at this time. If the steps are insufficient to remediate the material weaknesses successfully and otherwise establish and maintain effective internal control over financial reporting, the reliability of our financial reporting, investor confidence, and the value of our common stock could be materially and adversely affected. We can give no assurance that the implementation of this plan will remediate these deficiencies in our internal control over financial reporting or that additional material weaknesses or significant deficiencies in our internal control over financial reporting will not be identified in the future.
future. The failure to implement and maintain effective internal control over financial reporting could result in errors in our financial statements that could result in a restatement of our financial statements, causing us to fail to meet our reporting obligations.

We may expend substantial funds in connection with the tax liabilities that arose upon the settlement of restricted stock units.

We may expend substantial funds to satisfy minimum statutory tax withholding and remittance obligations that arose upon settlement of a portion of our restricted stock units. Our RSUs typically vest over a period of four years. On the settlement dates for our RSUs, we have undertaken sell-to-cover transactions where a portion of the stock subject to the RSUs is sold in public sales upon settlement of the RSUs, the proceeds of which are paid to the Company and subsequently remitted to the relevant tax authorities to cover certain tax liabilities on behalf of the holders of our RSUs at the applicable minimum statutory rates based on the then current value of the underlying shares of our common stock, which we refer to as a net settlement. In connection with these net settlements, we withhold and remit the tax liabilities on behalf of the RSU holders to the relevant tax authorities in cash.

It has come to our attention that certain tax liabilities pertaining to RSUs that were net settled in calendar year 2022 were not included in our previously filed quarterly employment tax returns and were not timely remitted to the relevant tax authorities, including the Internal Revenue Service. We are in the process of correcting these errors; however, we may be subject to interest and penalties, which if levied could have a material adverse effect on our business, financial condition and results of operations.

Risks Related to Ownership of Our Securities

The market price of our securities has been and is likely to be highly volatile, and you may not be able to resell your securities at or above the purchase price. The trading price of our securities has been and is likely to be volatile, and you could lose all or part of your investment.

The following factors, in addition to other factors described in this “Risk Factors” section and included elsewhere in this Annual Report on Form 10-K, may have a significant impact on the market price of our securities:

• threatened or actual litigation or government investigations;
• the occurrence of severe weather conditions and other catastrophes;
• publication of research reports or news stories about us, our competitors or our industry, or positive or negative recommendations or withdrawal of research coverage by securities analysts;
• the public’s reaction to our press releases, our other public announcements and our filings with the SEC;
• announcements by us or our competitors of acquisitions, business plans or commercial relationships;
• any major change in our Board or senior management;
• additional sales of our securities by us, our directors, executive officers or principal stockholders;
• adverse market reaction to any indebtedness we may incur or securities we may issue in the future;
• short sales, hedging and other derivative transactions in our securities;
• exposure to capital market risks related to changes in interest rates, realized investment losses, credit spreads, equity prices, foreign exchange rates and performance of insurance linked investments;
• our creditworthiness, financial condition, performance, and prospects;
• our dividend policy and whether dividends on our common stock have been, and are likely to be declared and paid from time to time;
• perceptions of the investment opportunity associated with our securities relative to other investment alternatives;
• regulatory or legal developments;
• changes in general market, economic, and political conditions;
• conditions or trends in our industry, geographies or customers; and
• changes in accounting standards, policies, guidance, interpretations or principles.

In addition, broad market and industry factors may negatively affect the market price of our securities, regardless of our actual operating performance, and factors beyond our control may cause our stock price to decline rapidly and unexpectedly. In addition, in the past, companies that have experienced volatility in the market price of their stock have been subject to securities class action litigation. As described in the "Legal Proceedings" section of this report, in April 2022 a purported class action complaint was filed alleging violations of the federal securities laws against a group of defendants including us and certain of our current and former executive officers. We intend to defend the matter vigorously, but litigation of this type is expensive and could result in substantial costs and diversion of management's attention and resources, which could have an adverse effect on our business, financial condition, results of operations or prospects. Any adverse determination in litigation could also subject us to significant liabilities.

A small number of stockholders will continue to have substantial control over us, which may limit other stockholders' ability to influence corporate matters and delay or prevent a third party from acquiring control over us.

Our directors, executive officers, and beneficial owners of 5% or more of our voting securities and their respective affiliates, beneficially owned, in the aggregate, approximately 30% of our outstanding common stock as of January 31, 2023. This significant concentration of ownership may have a negative impact on the trading price for our common stock because investors often perceive disadvantages in owning stock in companies with controlling stockholders. In addition, these stockholders will be able to exercise influence over all matters requiring stockholder approval, including the election of directors and approval of corporate transactions, such as a merger or other sale of our company or our assets. This concentration of ownership could limit stockholders' ability to influence corporate matters and may have the effect of delaying or preventing a change in control, including a merger, consolidation or other business combination, or discouraging a potential acquirer from making a tender offer or otherwise attempting to obtain control, even if that change in control would benefit the other stockholders.

There can be no assurance that we will be able to comply with the continued listing standards of the NYSE.

If NYSE delists our securities from trading for failure to meet the listing standards, we and our stockholders could face significant negative consequences including:

• limited availability of market quotations for our securities;
• a determination that our common stock is a “penny stock” which will require brokers trading in our common stock to adhere to more stringent rules,
• possibly resulting in a reduced level of trading activity in the secondary trading market for shares of our common stock;
• a limited amount of analyst coverage; and
• a decreased ability to issue additional securities or obtain additional financing in the future.
If our operating and financial performance in any given period does not meet the guidance provided to the public or the expectations of investment analysts, the market price of our common stock may decline.

We may, but are not obligated to, provide public guidance on our expected operating and financial results for future periods. Any such guidance will consist of forward-looking statements, subject to the risks and uncertainties described in this Annual Report on Form 10-K and in our other public filings and public statements. Our actual results may not always be in line with or exceed any guidance it has provided, especially in times of economic uncertainty. If, in the future, our operating or financial results for a particular period do not meet any guidance provided or the expectations of investment analysts, or if we reduce our guidance for future periods, the market price of our common stock may decline as well. Even if we do issue public guidance, there can be no assurance that we will continue to do so in the future.

We qualify as an “emerging growth company” as well as a “smaller reporting company.” The reduced public company reporting requirements applicable to emerging growth companies and smaller reporting companies may make our common stock less attractive to investors.

We qualify as an “emerging growth company” under SEC rules. As an emerging growth company, we are permitted and plan to rely on exemptions from certain disclosure requirements that are applicable to other public companies that are not emerging growth companies. These provisions include, but are not limited to: (1) an exemption from compliance with the auditor retention requirement in the assessment of internal control over financial reporting pursuant to Section 404 of Sarbanes-Oxley, (2) not being required to comply with any requirement that may be adopted by the PCAOB regarding mandatory audit firm rotation or a supplement to the auditor’s report providing additional information about the audit and the financial statements, (3) reduced disclosure obligations regarding executive compensation arrangements in periodic reports, registration statements, and proxy statements, and (4) exemptions from the requirements of holding a nonbinding advisory vote on executive compensation and stockholder approval of any golden parachute payments not previously approved. Further, Section 102(b)(1) of the JOBS Act exempts emerging growth companies from being required to comply with new or revised financial accounting standards until private companies (that is, those that have not had a Securities Act registration statement declared effective or do not have a class of securities registered under the Exchange Act) are required to comply with the new or revised financial accounting standards. The JOBS Act provides that a company can elect to opt out of the extended transition period and comply with the requirements that apply to non-emerging growth companies but any such election to opt out is irrevocable. As a result, the information we provide will be different than the information that is available with respect to other public companies that are not emerging growth companies.

We are also a “smaller reporting company” as defined by Rule 12b-2 of the Exchange Act. We may continue to be a smaller reporting company even after we are no longer an emerging growth company. We may take advantage of certain of the scaled disclosures available to smaller reporting companies and will be able to take advantage of these scaled disclosures for so long as the market value of our common stock held by non-affiliates is less than $250.0 million measured on the last business day of our second fiscal quarter, or our annual revenue is less than $100.0 million measured during the most recently completed fiscal year and the market value of our common stock held by non-affiliates is less than $700.0 million measured on the last business day of our second fiscal quarter.

We cannot predict whether investors will find our securities less attractive because we will rely on these exemptions. If some investors find our securities less attractive as a result of our reliance on these exemptions, the trading prices of our securities may be lower than they otherwise would be, there may be less active trading market for our securities and the trading prices of our securities may be more volatile.

We have no current plans to pay cash dividends on our common stock. As a result, stockholders may not receive any return on investment unless they sell their common stock for a price greater than the purchase price.

We have no current plans to pay dividends on our common stock. Any future determination to pay dividends will be made at the discretion of the Board, subject to applicable laws. It will depend on a number of factors, including our financial condition, results of operations, capital requirements, contractual, legal, tax and regulatory restrictions, general business conditions, and other factors that the Board may deem relevant. In addition, the ability to pay cash dividends may be restricted by the terms of debt financing arrangements, as any future debt financing arrangement likely will contain terms restricting or limiting the amount of dividends that may be declared or paid on the common stock. As a result, stockholders may not receive any return on an investment in our common stock unless they sell their shares for a price greater than that which they paid for them.

We may issue additional shares of common stock or other equity securities without your approval, which would dilute your ownership interests and may depress the market price of our common stock.

We may issue additional shares of common stock or other equity securities without your approval, which would dilute your ownership interests and may depress the market price of our common stock. In addition, the number of shares available for issuance under our equity incentive plans automatically increases each year under the terms of those plans. We may also issue additional shares of common stock or other equity securities of equal or senior rank in the future in connection with, among other things, future acquisitions or repayment of outstanding indebtedness, without stockholder approval, in a number of circumstances.

The issuance of additional shares or other equity securities of equal or senior rank would have the following effects:

• existing stockholders’ proportionate ownership interest in our company will decrease;
• the amount of cash available per share, including for payment of dividends in the future, may decrease;
• the relative voting strength of each share of previously outstanding common stock may be diminished; and
• the market price of our common stock may decline.

Provisions in our organizational documents and provisions of the DGCL may delay or prevent an acquisition by a third party that could otherwise be in the interests of stockholders.

Our amended and restated certificate of incorporation (the “Charter”) and our amended and restated bylaws contain several provisions that may make it more difficult or expensive for a third party to acquire control of our company without the approval of the Board. These provisions, which may delay, prevent or deter a merger, acquisition, tender offer, proxy contest, or other transaction that stockholders may consider favorable, include the following:

• the division of the Board into three classes and the election of each class for three-year terms;
• advance notice requirements for stockholder proposals and director nominations;
• provisions limiting stockholders’ ability to call special meetings of stockholders, to require special meetings of stockholders to be called, and to take action by written consent;
• restrictions on business combinations with interested stockholders;
• in certain cases, the approval of holders representing at least 66 2/3% of the total voting power of the shares entitled to vote generally in the election of directors will be required for stockholders to adopt, amend or repeal the bylaws, or amend or repeal certain provisions of the Charter;
• no cumulative voting; and
the ability of the Board to designate the terms of and issue new series of preferred stock without stockholder approval, which could be used, among other things, to institute a rights plan that would have the effect of significantly diluting the stock ownership of a potential hostile acquirer, likely preventing acquisitions by such acquirer.

These provisions of the Charter and amended and restated bylaws could discourage potential takeover attempts and reduce the price that investors might be willing to pay for the shares of our common stock in the future, which could reduce the market price of the common stock.

The provision of our Charter requiring exclusive venue in the Court of Chancery in the State of Delaware and the federal district courts of the United States for certain types of lawsuits may have the effect of discouraging lawsuits against directors and officers.

Our Charter provides that, unless we consent in writing to the selection of an alternative forum, the Court of Chancery of the State of Delaware shall be the sole and exclusive forum for: (1) any derivative action, suit or proceeding brought on our behalf, (2) any action, suit or proceeding asserting a claim of breach of fiduciary duty owed by any director, officer or stockholder to the company or our stockholders, (3) any action, suit or proceeding arising pursuant to any provision of the DGCL, the Charter or our amended and restated bylaws, (4) any action asserting a claim against us governed by the internal affairs doctrine. The Charter further provides that, unless we consent in writing to the selection of an alternative forum, the federal district courts of the United States of America shall, to the fullest extent permitted by law, be the exclusive forum for the resolutions of any complaint asserting a cause of action arising under the Securities Act. The exclusive forum clauses described above shall not apply to suits brought to enforce a duty or liability created by the Exchange Act, or any other claim for which the federal courts have exclusive jurisdiction. Although these provisions are expected to benefit us by providing increased consistency in the application of applicable law in the types of lawsuits to which they apply, the provisions may have the effect of discouraging lawsuits against directors and officers. The enforceability of similar choice of forum provisions in other companies’ certificates of incorporation has been challenged in legal proceedings and there is uncertainty as to whether a court would enforce such provisions. In addition, investors cannot waive compliance with the federal securities laws and the rules and regulations thereunder. It is possible that, in connection with any applicable action brought against us, a court could find the choice of forum provisions contained in the Charter to be inapplicable or unenforceable in such action. If so, we may incur additional costs associated with resolving such action in other jurisdictions, which could harm our business, financial condition or results of operations.

General Risk Factors

We will continue to incur significant costs as a result of operating as a public company, and our management will continue to devote substantial time to compliance initiatives.

As a public company, we have incurred and will continue to incur significant legal, accounting and other expenses. As a public company, we are subject to the reporting requirements of the Exchange Act, the Sarbanes-Oxley Act of 2002 (the “Sarbanes-Oxley Act”), the Dodd-Frank Wall Street Reform and Consumer Protection Act, as well as rules adopted, and to be adopted, by the SEC and Nasdaq. Our management and other personnel need to continue to devote a substantial amount of time to comply with these requirements. Moreover, these rules and regulations have increased, and will continue to increase, our legal and financial compliance costs and make some activities more time-consuming and costly. The increased costs may increase our net loss. For example, these rules and regulations make it more difficult and more expensive for us to obtain director and officer liability insurance and we may be forced to accept reduced policy limits or incur substantially higher costs to maintain the same or similar coverage as we did prior to becoming a public company. These rules and regulations are often subject to varying interpretations, in many cases due to their lack of specificity, and, as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This could result in future uncertainty regarding compliance matters and higher costs necessitated by ongoing revisions to disclosure and governance practices. The impact of these requirements could also make it more difficult for us to attract and retain qualified persons to serve on our Board, our board committees or as our executive officers. As a public company, we are obligated to develop and maintain proper and effective internal controls over financial reporting and any failure to maintain the adequacy of these internal controls may adversely affect investor confidence in our company and, as a result, the value of shares of our common stock.

Pursuant to Section 404 of the Sarbanes Oxley Act (“Section 404”), we are required to furnish a report by our management on our internal control over financial reporting, including an attestation report on internal control over financial reporting issued by our independent registered public accounting firm. To maintain compliance with Section 404, we engage in a process to document and evaluate our internal control over financial reporting, which is both costly and challenging. In this regard, we will need to continue to dedicate internal resources, engage outside consultants and refine and revise a detailed work plan to assess and document the adequacy of internal control over financial reporting, continue steps to improve control processes as appropriate, validate through testing that controls are functioning as documented and implement a continuous reporting and improvement process for internal control over financial reporting. Despite our efforts, there is a risk that neither we nor our independent registered public accounting firm will be able to conclude that our internal control over financial reporting is effective as required by Section 404.

If we are unable to conclude that our internal controls over financial reporting are effective, or if our independent registered public accounting firm determines we have a material weakness or significant deficiency in our internal controls over financial reporting we could lose investor confidence in the accuracy and completeness of our financial reports, the market price of shares of our common stock could decline, and we could be subject to sanctions or investigations by the SEC, the SEC or other regulatory authorities. Failure to remedy any material weakness in our internal control over financial reporting, or to implement or maintain other effective control systems required of public companies, could also negatively impact our ability to access the capital markets.

In addition, effective disclosure controls and procedures enable us to make timely and accurate disclosure of financial and non-financial information that we are required to disclose. As a public company, if our disclosure controls and procedures are ineffective, we may be unable to report our financial results or make other disclosures accurately on a timely basis, which could cause our reported financial results or other disclosures to be materially misstated and result in the loss of investor confidence and cause the market price of shares of our common stock to decline.

If securities or industry analysts do not publish research or reports about our business or publish negative reports, the market price of our common stock could decline.

The trading market for our common stock will be influenced by the research and reports that industry or securities analysts publish about us or our business. If regular publication of research reports ceases, we could lose visibility in the financial markets, which in turn could cause the market price or trading volume of our common stock to decline. Moreover, if one or more of the analysts who cover us downgrade our common stock or if reporting results do not meet their expectations, the market price of our common stock could decline.

ITEM 1B. UNRESOLVED STAFF COMMENTS

Not applicable.

ITEM 2. PROPERTIES

Our corporate headquarters occupy approximately 12,000 square feet in Tysons, Virginia, part of the Washington, D.C. metropolitan region, under a lease that expires in June 2026. We have a data center co-location facility in Reston, Virginia, and we also utilize AWS regional cloud services located around the world for our storage needs and to help deliver our solution.

As a now primarily remotely-operated company, we believe that our existing facilities are sufficient for our current needs and that suitable additional or substitute space will be available on commercially reasonable terms to meet our future needs.

ITEM 3. LEGAL PROCEEDINGS
From time to time, we may become involved in legal proceedings arising in the ordinary course of our business. Except as set forth below, we are not currently a party to any material legal proceedings, and we are not aware of any pending or threatened legal proceeding against us that we believe could have an adverse effect on our business, operating results or financial condition.

Securities Litigation
On April 22, 2022, a federal securities class action lawsuit was filed by a purported stockholder in the United States District Court for the Eastern District of Virginia (the "Court"). On July 15, 2022, the Court appointed a lead plaintiff for the action, and ordered that the action bear the caption In re IronNet, Inc. Securities Litigation, No. 1:22-cv-004499-RDA-JFA. On August 29, 2022, the lead plaintiff filed an amended complaint on behalf of a proposed class consisting of those who acquired our securities between September 14, 2021 and December 15, 2021. The amended complaint names us, our current Chief Executive Officer, our former co-Chief Executive Officer, and our former Chief Financial Officer as defendants and asserts claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 ("1934 Act") as amended, for alleged misrepresentations and/or omissions in September 2021 regarding our financial guidance for fiscal year 2022 and a claim under Section 20A of the 1934 Act, as amended, for alleged trading on material nonpublic information by our current Chief Executive Officer. The amended complaint seeks an unspecified amount of damages on behalf of the putative class and an award of costs and expenses, including reasonable attorneys’ fees.

On October 26, 2022, the defendants filed a motion to dismiss the amended complaint. On November 30, 2022, the lead plaintiff filed an opposition. On December 21, 2022, the defendants filed a reply in support of the motion to dismiss.

We believe the claims are without merit, intend to defend the case vigorously, and have not recorded a liability related to this lawsuit because, at this time, we are unable to determine whether an unfavorable outcome is probable or to estimate reasonably possible losses.

ITEM 4. MINE SAFETY DISCLOSURES
Not applicable.

PART II

ITEM 5. MARKET FOR COMMON EQUITY AND RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Market Information
Our common stock and public warrants to purchase common stock ("Public Warrants") are currently listed on NYSE under the symbols “IRNT” and “IRNT.WS,” respectively.

Holders
As of April 15, 2023, there were 318 holders of record of the common stock and five holders of record of our Warrants.

Dividend Policy
We have never declared or paid any dividends on shares of our common stock. We anticipate that we will retain all of our future earnings, if any, for use in the operation and expansion of our business and do not anticipate paying cash dividends in the foreseeable future. Any decision to declare and pay dividends in the future will be made at the sole discretion of our Board and will depend on, among other things, our results of operations, cash requirements, financial condition, contractual restrictions and other factors that our Board may deem relevant.

Recent Sales of Unregistered Securities
Between November 2022 and December 2022, we issued 2,511,365 shares to Tumim (as defined below) as payment under the Purchase Agreement (as defined below). See “Tumim Stone Capital Committed Equity Financing” for more detail regarding the Purchase Agreement. The issuance of these shares to Tumim was exempt from registration pursuant to Section 4(a)(2) of the Securities Act.

In addition, in December 2022, we issued 1,363,636 shares to 3i (as defined below) as partial payment under the Convertible Notes (as defined below). See "Liquidity and Capital Resources-3i Convertible Debt Facility" for more detail regarding the Convertible Notes. The issuance of these shares to 3i was exempt from registration pursuant to Section 3(a)(9) of the Securities Act.

ITEM 6. [RESERVED]
The following discussion and analysis of our financial condition and results of operations should be read in conjunction with the annual consolidated financial statements and related notes included in Part II, Item 8 of this Annual Report on Form 10-K. The consolidated financial statements in this report are presented in U.S. dollars (USD) rounded to the nearest thousand, with the amounts in this Management’s Discussion and Analysis of Financial Condition and Results of Operations (“MD&A”) rounded to the nearest tenth of a million. Therefore, differences in the tables between totals and sums of the amounts listed may occur due to such rounding.

The following discussion contains forward-looking statements that involve risks and uncertainties. Our actual results could differ materially from those discussed in the forward-looking statements. Factors that could cause or contribute to these differences include those discussed below, in the annual consolidated financial statements and related notes included in Part II, Item 8 of this Form 10-K, and in the sections of this report titled “Cautionary Note Regarding Forward-Looking Statements” and “Risk Factors.” Our fiscal year end is January 31, and our fiscal quarters end on April 30, July 31, October 31, and January 31. Our fiscal years ended January 31, 2023 and January 31, 2022 are referred to herein as “fiscal year 2023” and “fiscal year 2022,” respectively.

Business Combination and Basis of Presentation
We were originally known as LGL Systems Acquisition Corp. (“LGL”). On August 26, 2021, LGL consummated the Business Combination with IronNet Cybersecurity, Inc. (“Legacy IronNet”) pursuant to the Business Combination Agreement (the “Merger”). Legacy IronNet survived the Merger as a wholly-owned subsidiary of LGL. In connection with the closing of the Merger, LGL changed its name from LGL Systems Acquisition Corp. to IronNet, Inc. The Merger was accounted for as a reverse recapitalization (the “Reverse Recapitalization”). Under this method of accounting, LGL is treated as the “acquired” company and Legacy IronNet is treated as the acquirer for financial reporting purposes. The Reverse Recapitalization was treated as the equivalent of Legacy IronNet issuing and selling stock for the net assets of LGL, accompanied by a recapitalization. The net assets of LGL are stated at historical cost, with no goodwill or other intangible assets recorded.

As a result of Legacy IronNet being the accounting acquirer in the Merger, the financial reports filed with the SEC by the Company subsequent to the Merger are prepared as if Legacy IronNet is the accounting predecessor of the Company. The historical operations of Legacy IronNet are deemed to be those of the Company. See Note 3 in the accompanying annual consolidated financial statements for more information.

As a public company, we have been and will continue to be required to implement procedures and processes to address public company regulatory requirements and customary practices. We expect to continue to incur additional annual expenses as a public company for, among other things, directors’ and officers’ liability insurance, director fees and additional internal and external accounting, legal and administrative resources, including increased audit and legal fees.

Overview
GEN Keith B. Alexander (Ret) founded our company in 2014 to solve the major cybersecurity problem he witnessed and defined during his tenure as former head of the NSA and founding Commander of U.S. Cyber Command: You can’t defend against threats you can’t see. Our innovative approach provides the ability for groups of organizations—within an industry sector, supply chain, state or country, for example—to see, detect and defend against sophisticated cyber attacks earlier and faster than ever before.

IronNet has defined a new market category called Collective Defense. IronNet has developed the Collective Defense platform, a solution that can identify anomalous (potentially suspicious or malicious) behaviors on computer networks and share this intelligence anonymously and in real time among members of a Collective Defense community. Collective Defense communities comprise groups of organizations that have common risks, such as a supply chain, a business ecosystem, or across an industry sector, a state, or a country. This cybersecurity model delivers timely, actionable, and contextual alerts and threat intelligence on attacks targeting enterprise networks, and functions as an early-warning detection system for all community members.

This new platform addresses a large and unwavering compound problem: limited threat visibility for increasingly borderless enterprises across sectors and at the national level, paired with ineffective threat knowledge sharing across companies and sectors and a “go it alone” approach to cybersecurity. These operational gaps, combined with market dynamics like the increased velocity of sophisticated cyber attacks and the deepening scarcity of qualified human capital, have set our mission to transform how cybersecurity is waged.

Our Business
We have focused on the development and delivery of a suite of advanced cybersecurity capabilities for detection, alerting, situational awareness and hunt/remediation combined into a comprehensive Collective Defense platform. In addition to our Collective Defense platform, our product offering also includes a threat intelligence feed sold primarily through our partner ecosystem that enables the cybersecurity stack to block adversary infrastructure immediately. We complement these capabilities, delivered to both commercial and public sector enterprises, with professional services.

Product, Subscription and Support Revenue
Our primary line of business is the delivery of integrated software capabilities through our Collective Defense platform. The platform, targeting larger organizations with a more mature cybersecurity infrastructure, is comprised of two flagship products:

IronDefense is an advanced Network Detection Response (“NDR”) solution that uses AI-driven behavioral analytics to detect and prioritize anomalous activity inside individual enterprises. IronNet leverages advanced AI/ML algorithms to detect previously-unknown threats, which are those that have not been identified and “fingerprinted” by industry researchers, in addition to screening known threats, and applies its Expert System to prioritize the severity of the behaviors—all at machine speed and cloud scale.

IronDome is a threat-sharing solution that facilitates a crowdsource-like environment in which the IronDefense threat detections from an individual company are shared among members of a Collective Defense community, consisting of our customers who have elected to permit their information to be anonymously shared and cross-correlated by our IronDome systems. IronDome analyzes threat detections across the community to identify broad attack patterns and provides anonymized intelligence back to all community members in real time, giving all members early insight into potential incoming attacks. Automated sharing across the Collective Defense community enables faster detection of attacks at earlier stages.

Our Collective Defense platform is designed to deliver strong network effects. Every customer contributing its threat data (anonymously) into the community is able to reap benefits from the shared intelligence of the other organizations. The collaborative aspect of Collective Defense, and the resulting prioritization of alerts based on their potential severity, helps address the known problem of “alert fatigue” that plagues overwhelmed security analysts.

Our Collective Defense platform is cloud-deployed and is scalable to include small-to-medium businesses and public-sector agencies as well as multinational corporations. The Collective Defense platform was available to customers on premise and in hybrid environments until December 2022. We provide professional cybersecurity services such as incident response and threat hunting, as well as programs to help customers assess cybersecurity governance, maturity, and readiness. Our cybersecurity services are designed to create shared long-term success measures with our customers, differentiating us from other cybersecurity vendors by working alongside customers as partners and offering consultative and service capabilities beyond implementation.

Our Collective Defense platform is a subscription-based pricing and flexible-delivery model, with 83.6% of our revenue for the fiscal year ended January 31, 2023 related to deployments involving our key partner, AWS. To make it as easy as possible for customers to add Collective Defense into their existing security stack, we have built a rich set of APIs that enable integrations with standard security products, including SIEM, SOAR, EDR, NGFW tools, and cloud-native logs from the major public cloud providers.

IronRadar is a threat-sharing solution that proactively and automatically updates customer cybersecurity tools to be able to detect and block malicious indicators of adversary infrastructure. IronRadar, which we launched during the fiscal year ended January 31, 2023, is intended to broaden our market reach to companies of all
sizes, including those with less sophisticated cybersecurity infrastructure, and leverage our key partner relationships as the primary route to market. Developed by our team of elite threat hunters, IronRadar scours the internet fingerprinting servers to determine whether they are C2 infrastructure while being stood up, even before a cyber attack, such as ransomware, is initiated. This threat detection and response solution identifies known and unknown C2 infrastructure and is built from the ground up to be easy to deploy, making it easy for security teams to integrate IronRadar into existing tools, including SIEM/SOAR, TIP, EDRs, and firewalls, to increase effectiveness and defense. Once set up, IronRadar is regularly updated and automatically fed into a customer’s security landscape to proactively block threats, enabling faster response and creating efficiencies for security teams. IronRadar is currently available for purchase via subscription and also sold directly from the AWS Marketplace.

Professional Services
We sell professional services, including development of national cybersecurity strategies, cyber operations monitoring, security, training, red team, incident response and tailored maturity assessments. Revenue derived from these services is recognized as the services are delivered.

Financing to Date
Historically, we have financed our operations primarily through private placements of common stock, issuance of debt, warrants and redeemable convertible preferred stock.

In connection with the execution of the Merger Agreement, a number of purchasers (each, a “Subscriber”) purchased an aggregate of 12,500,000 shares of our common stock (the “PIPE Shares”), for a purchase price of $10.00 per share and an aggregate purchase price of $125.0 million. As a result of the Merger, we also received $13.3 million held in Legacy LGL’s trust account from proceeds related to public trust shares, net of stockholder redemptions. Transaction costs related to the issuance of the trust shares were $9.0 million.

On September 15, 2022, we issued a senior unsecured convertible promissory note to 3i, LP (“3i”) for an aggregate principal amount of $10.3 million, net of debt discount for cash proceeds of $10.0 million. For more information, see “Liquidity and Capital Resources—3i Convertible Debt Facility.”

In December 2022, we issued and sold senior secured promissory notes in an aggregate principal amount of $6.9 million to a total of eight lenders, including certain members of our Board of Directors or their affiliates. In April 2023, we issued and sold an additional Director Note in the amount of $0.3 million to the lender not affiliated with our directors.

Between December 2022 and May 2023, we issued and sold senior secured convertible promissory notes in an aggregate amount of $13.1 million to C5 Capital Limited (“C5”), one of our major stockholders. For more information see “Liquidity and Capital Resources—Director and C5 Loans.” We continue to negotiate with C5 as to a potential acquisition of our company by C5, as described below under “Recent Developments—C5 Strategic Transaction.”

During fiscal year 2023, we incurred a net loss of $111.0 million, of which $36.9 million related to non-cash expense related to stock-based compensation, and used $64.9 million in cash to fund our operations. As of January 31, 2023, we had $7.6 million of cash on hand to continue to fund operations.

Recent Developments
Going concern
Management expects that operating losses and negative cash flows from operating activities will continue in the foreseeable future as we continue to work to fund our operations. As of January 31, 2023, there is substantial doubt about our ability to continue to operate as a going concern within one year from the issuance of our consolidated financial statements.

Based on our current planned operations, in the absence of additional sources of liquidity, management anticipates that our existing cash and cash equivalents and anticipated cash flows from operations will not be sufficient to meet our operating and liquidity needs for any meaningful period of time following the filing of this report. There is no assurance that management will be able to obtain additional liquidity or be successful in raising additional funds or that such funds, if available, will be available on attractive terms or that they will not have a significant dilutive effect on our existing stockholders. In the event we determine that additional sources of liquidity will not be available to us or will not allow us to meet our obligations as they become due, we may need to file a voluntary petition for relief under the United States Bankruptcy Code in order to implement a plan of reorganization, court-supervised sale, and/or liquidation.

Reductions in force
Between September 2022 and November 2022, our headcount was reduced by approximately 111 employees, or approximately 44% of our workforce as part of our initiatives to re-balance our cost structure.

We do not expect to incur future material charges in connection with these reductions in force. These reductions in force are expected to result in approximately $20.0 million of annualized cost savings in total. We may incur additional expenses not currently contemplated due to events associated with the reductions in force. The annualized cost savings are estimates and subject to a number of assumptions, and actual results may differ materially.

Notice of failure to satisfy continued listing rules
On October 25, 2022, we received a written notice (the “Initial Notice”) from the New York Stock Exchange (the “NYSE”) that we are no longer in compliance with the NYSE continued listing standards, set forth in Section 802.01C of the NYSE Listed Company Manual because the average closing price of our common stock was less than $1.00 per share over a period of 30 consecutive trading days. On December 21, 2022, we received a second written notice (the “Second Notice”) from the NYSE that we are no longer in compliance with the NYSE continued listing standards, set forth in Section 802.01E of the NYSE Listed Company Manual as a result of our failure to timely file our Report on Form 10-Q for the period ended October 31, 2022. On January 24, 2023, we received a third written notice (the “Third Notice”, together with the Initial Notice and Second Notice, the “Notices”) from the NYSE that we are no longer in compliance with the NYSE’s continued listing standards, set forth in Section 802.01B of the NYSE Listed Company Manual because our average global market capitalization over a consecutive 30 trading-day period was less than $50.0 million and, at the same time, our last reported shareholders’ equity was less than $50.0 million.

The Notices have no immediate impact on the listing of our common stock, which will continue to be listed and traded on the NYSE during applicable cure periods, and do not result in a default under our material debt or other agreements. To address this issue, we intend to monitor the trading price of our listed securities and take steps to increase the value of our shares through implementation of our business strategy, and are considering all available options to regain compliance with the NYSE’s continued listing standards. We are also in communication with the NYSE regarding our plans for regaining compliance with the continued listing standards. See “Risk Factors—The Company must regain compliance with New York Stock Exchange requirements for the continued listing of its common stock” for additional information.

Tamin Purchase Notices
Between November 25, 2022 and December 14, 2022, we issued a series of purchase notices (the “Purchase Notice”) to Tamin Stone Capital, LLC (“Tamin”) pursuant to the terms of a Common Stock Purchase Agreement (the “Purchase Agreement”) we entered into with Tamin on February 11, 2022. Pursuant to the Purchase Notices, we issued 2,511,365 shares of our common stock to Tamin and received aggregate proceeds of approximately $0.6 million. For more information on the Purchase Agreement, see “Liquidity and Capital Resources—Tamin Capital Committed Equity Financing.”

Director and C5 Loans
Between December 14, 2022 and April 20, 2023, we issued senior secured promissory notes in an aggregate principal amount of $7.2 million to a total of eight lenders, including certain members of our Board of Directors or their affiliates. On January 11, 2023, January 12, 2023, February 8, 2023, February 27, 2023, April 13, 2023,
C5 Strategic Transaction

On December 28, 2022, we entered into an agreement with C5 pursuant to which we agreed to a mutual exclusivity period through January 31, 2023 to seek to negotiate definitive agreements with respect to a potential offer by C5 to acquire all of the outstanding common stock of the Company not presently owned by C5 and certain of its affiliates (the “Proposed Transaction”). Commencement of the exclusivity period was subject to C5 providing $2.0 million of financing described above under “Director and C5 Loans.” The exclusivity period was subsequently extended on multiple occasions following additional financing from C5. While we no longer remain under contractual exclusivity with C5, we are continuing to negotiate definitive agreements with C5 with respect to the Proposed Transaction.

Key Business Metrics

We monitor the following key metrics to measure our performance, identify trends, formulate business plans and make strategic decisions.

Recurring Software Customers

We believe that our ability to increase the number of subscription and other recurring contract type customers on our platform is an indicator of our market penetration, the growth of our business, and our potential future business opportunities. Our recurring software customers include customers who have a recurring contract for either or both of our IronDefense and IronDome platforms. These platforms are generally sold together, but they also can be purchased on a standalone basis. The following table sets forth the number of recurring software customers as of the dates presented:

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurring Software Customers</td>
<td>66</td>
<td>88</td>
</tr>
<tr>
<td>Year-over-year growth</td>
<td>(23.7)%</td>
<td>226%</td>
</tr>
</tbody>
</table>

Our recurring software customer count was negatively impacted in the second half of fiscal year 2023 by our current liquidity situation. We believe that our ability to strengthen our financial position and liquidity would also improve our customer retention and net new customer acquisition. In addition, the fiscal year 2022 customer count above includes 17 entities protected under one contract. Beginning in fiscal year 2023, we no longer count a contract to protect multiple entities as multiple customers. The customer count for fiscal year 2022 would be 72 using the same methodology.

Annual Recurring Revenue (“ARR”)

ARR is calculated at a particular measurement date as the annualized value of our then existing customer subscription contracts and the portions of other software and product contracts that are to be recognized over the course of the contracts and that are designed to renew, assuming any contract that expires during the 12 months following the measurement date is renewed on its existing terms. The following table sets forth our ARR as of the dates presented:

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual recurring revenue</td>
<td>$26.2</td>
<td>$31.8</td>
</tr>
<tr>
<td>Year-over-year growth</td>
<td>(18.3)%</td>
<td>23%</td>
</tr>
</tbody>
</table>

ARR decreased in fiscal year 2023 as a result of the decrease in recurring software customer count in the second half of fiscal year 2023 and the decrease in the number of existing contracts.

Dollar-based Average Contract Length

Our dollar-based average contract length is calculated from a set of customers against the same metric as of a prior period end. Because many of our customers have similar buying patterns and the average term of our contracts is more than 12 months, this metric provides a means of assessing the degree of built-in revenue repetition that exists across our customer base.

We calculate our dollar-based average contract length as follows:

a. Numerator: We multiply the average total length of the contracts, measured in years or fractions thereof, by the respective revenue recognized for fiscal year 2023 and 2022 as applicable.

b. Denominator: We use the revenue attributable to software and product customers for fiscal year 2023 and 2022 in the numerator. This effectively represents the revenue base that is being generated by those customers.

Dollar-based average contract length is obtained by dividing the Numerator by the Denominator. Our dollar-based average contract length increased from 2.7 to 3.2 years, or 19% for fiscal year 2023 as compared to fiscal year 2022. The re-emergence of longer term contracts in our average has led to the increase in our average contract length as of the end of the most recent reporting period.

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dollar-based average contract length</td>
<td>3.2</td>
<td>2.7</td>
</tr>
</tbody>
</table>
measure. In addition, other companies, including companies in our industry, may calculate similarly-titled non-GAAP measures differently or may use other measures to evaluate their performance, all of which could reduce the usefulness of our metric of calculated billings as a tool for comparison. Because of these and other limitations, you should consider calculated billings along with revenue and our other GAAP financial results.

The following table presents a reconciliation of revenue, the most directly comparable financial measure calculated in accordance with GAAP, to calculated billings:

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023 (in millions)</th>
<th>2022</th>
<th>2023 vs 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue</td>
<td>$27.3</td>
<td>$27.5</td>
<td>(0.2)%</td>
</tr>
<tr>
<td>Add: Total Deferred revenue, end of period</td>
<td>27.1</td>
<td>33.6</td>
<td>(19.3)%</td>
</tr>
<tr>
<td>Less: Total Deferred revenue, beginning of period</td>
<td>33.6</td>
<td>34.0</td>
<td>(0.4)%</td>
</tr>
<tr>
<td>Calculated billings</td>
<td>$20.8</td>
<td>$27.1</td>
<td>(6.3)%</td>
</tr>
</tbody>
</table>

Adjusted Net Loss

The following table shows our Adjusted Net Loss, a non-GAAP measure, for fiscal years 2023 and 2022 respectively, which excludes the impacts of stock-based compensation expense, the revaluation of the Private Warrants prior to their cashless exercise, and transaction costs incurred related to the Merger from our net loss.

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023 ($ in thousands)</th>
<th>2022</th>
<th>2023 vs 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net loss</td>
<td>$</td>
<td>(11.018)</td>
<td>$ (242,647)</td>
</tr>
<tr>
<td>Stock based compensation expense (1)</td>
<td>36,858</td>
<td>156,596</td>
<td></td>
</tr>
<tr>
<td>Change in fair value of warrant liabilities</td>
<td>(6)</td>
<td>11,265</td>
<td></td>
</tr>
<tr>
<td>Transaction costs expense (2)</td>
<td></td>
<td>3,166</td>
<td></td>
</tr>
<tr>
<td>Adjusted Net Loss</td>
<td>$ (74,158)</td>
<td>$ (71,620)</td>
<td></td>
</tr>
</tbody>
</table>

Components of Our Results of Operations

Revenue

Our revenues are derived from sales of product, subscriptions, subscription-like software products and software support contracts as well as from professional services. Products, subscriptions and support revenues accounted for 94% of our revenue in fiscal year 2023 and for 92% of our revenue in fiscal year 2022. Professional services revenues accounted for 6% of our revenue in fiscal year 2023 as compared to 8% in fiscal year 2022.

Our typical customer contracts and subscriptions range from one to five years. We typically invoice customers annually, in advance. We combine intelligence dependent hardware and software licenses as well as subscription-type deliverables with the related threat intelligence and support and maintenance as a single performance obligation, as it delivers the essential functionality of our cybersecurity solution. Most companies also participate in the Frontbase collective defense software solution that provides them access to our collective defense infrastructure linking participating stakeholders. We recognize revenue for this single performance obligation ratably over the expected term with the customer. Amounts that have been invoiced are recorded in deferred revenue or they are recorded in revenue if the revenue recognition criteria have been met. Judgment is required for the assessment of material rights relating to renewal options associated with our contracts.

Professional services revenues are generally sold separately from our products and include services such as development of national cyber security strategies, cyber operations monitoring, security, training, red team, incident response and tailored maturity assessments. Revenue derived from these services is recognized as the services are delivered.

Cost of Revenue

Cost of product, subscription and support revenue includes expenses related to our hosted security software and AWS Marketplace, employee-related costs of our customer facing support, such as salaries, bonuses and benefits, an allocated portion of administrative costs, the amortization of deferred costs, and expense related to establishing an inventory reserve.

Cost of professional services revenue consists primarily of employee-related costs, such as salaries, bonuses and benefits, cost of contractors and an allocated portion of administrative costs.

Gross Profit

Gross profit, calculated as total revenue less total costs of revenue, is affected by various factors, including the timing of our acquisition of new customers, renewals from existing customers, the data center and bandwidth costs associated with operating our cloud platform, the extent to which we expand our customer support organization, and the extent to which we can increase the efficiency of our technology and infrastructure through technological improvements. Also, we view our professional services in the context of our larger business and as a lead generator for potential future product sales. Because of these factors, our services revenue and gross profit may fluctuate over time.

Operating Expenses

Research and development

Our research and development efforts are aimed at continuing to develop and refine our products, including adding new features and modules, increasing their functionality, and enhancing the usability of our platform. Research and development costs primarily include personnel-related costs and acquired software costs. Research and development costs are expensed as incurred.

Sales and marketing

Sales and marketing expenses consist primarily of employee compensation and related expenses, including salaries, bonuses and benefits for our sales and marketing employees, sales commissions that are recognized as expenses over the period of benefit, marketing programs, travel and entertainment expenses, and allocated overhead costs. We capitalize our sales commissions and recognize them as expenses over the estimated period of benefit.

General and administrative
General and administrative costs include salaries, stock-based compensation expenses, and benefits for personnel involved in our executive, finance, legal, people and culture, and administrative functions, as well as third-party professional services and fees, and overhead expenses.

Interest expense
Interest expense consists of interest expense incurred.

Other income
Other income consists primarily of interest income and foreign currency gains.

Change in fair value of warrant liabilities
The change in fair value of warrant liabilities includes the adjustments to the warrant liability to reflect its fair value as of the end of the reporting period.

Provision for income taxes
Provision for income taxes consists of federal and state income taxes in the United States and income taxes and withholding taxes in certain foreign jurisdictions in which we conduct business. We maintain a full valuation allowance on our U.S. federal and state deferred tax assets.

Results of Operations

Comparison of Fiscal Year 2023 and Fiscal Year 2022
The following tables set forth our consolidated statements of operations in dollar amounts and as a percentage of total revenue for each period presented and the year over year change for each line item in dollar amounts and as a percentage:

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023</th>
<th>2022</th>
<th>Change $</th>
<th>Change %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>($) in thousands</td>
<td>%</td>
<td>($) in thousands</td>
<td>%</td>
</tr>
<tr>
<td>Product, subscription and support revenue</td>
<td>25,703</td>
<td>94</td>
<td>$ 25,347</td>
<td>92</td>
</tr>
<tr>
<td>Professional services revenue</td>
<td>1,554</td>
<td>6</td>
<td>$ 2,197</td>
<td>8</td>
</tr>
<tr>
<td>Total revenue</td>
<td>27,257</td>
<td>100</td>
<td>27,544</td>
<td>100</td>
</tr>
<tr>
<td>Cost of product, subscription and support revenue</td>
<td>13,467</td>
<td>49</td>
<td>8,225</td>
<td>30</td>
</tr>
<tr>
<td>Cost of professional services revenue</td>
<td>527</td>
<td>2</td>
<td>1,158</td>
<td>4</td>
</tr>
<tr>
<td>Total cost of revenue</td>
<td>13,994</td>
<td>51</td>
<td>9,383</td>
<td>34</td>
</tr>
<tr>
<td>Gross profit</td>
<td>13,263</td>
<td>49</td>
<td>18,161</td>
<td>66</td>
</tr>
<tr>
<td>Operating expenses</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research and development</td>
<td>32,426</td>
<td>119</td>
<td>52,899</td>
<td>192</td>
</tr>
<tr>
<td>Sales and marketing</td>
<td>31,530</td>
<td>116</td>
<td>82,922</td>
<td>301</td>
</tr>
<tr>
<td>General and administrative</td>
<td>57,000</td>
<td>209</td>
<td>112,099</td>
<td>407</td>
</tr>
<tr>
<td>Total operating expenses</td>
<td>120,976</td>
<td>444</td>
<td>247,920</td>
<td>900</td>
</tr>
<tr>
<td>Operating loss</td>
<td>(107,713)</td>
<td>(395)</td>
<td>(229,759)</td>
<td>(834)</td>
</tr>
<tr>
<td>Interest expense</td>
<td>(1,273)</td>
<td>(5)</td>
<td>(1,155)</td>
<td>(4)</td>
</tr>
<tr>
<td>Other income</td>
<td>108</td>
<td>0</td>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>Other expense</td>
<td>(2,080)</td>
<td>(8)</td>
<td>(28)</td>
<td>0</td>
</tr>
<tr>
<td>Change in fair value of warrant liabilities</td>
<td>6</td>
<td>0</td>
<td>(1,125)</td>
<td>(41)</td>
</tr>
<tr>
<td>Loss before income taxes</td>
<td>(110,952)</td>
<td>(407)</td>
<td>(242,182)</td>
<td>(879)</td>
</tr>
<tr>
<td>Provision for income taxes</td>
<td>(58)</td>
<td>(0)</td>
<td>(465)</td>
<td>2</td>
</tr>
<tr>
<td>Net loss</td>
<td>(111,010)</td>
<td>(407)</td>
<td>(242,647)</td>
<td>(881)</td>
</tr>
</tbody>
</table>

Revenue
Total revenue decreased by $0.3 million or 1% in fiscal year 2023, compared to fiscal year 2022.

Product, subscription and support revenue increased by $0.4 million or 1% primarily due to the net effect of our transition from contracts that had non-recurring elements which did not renew in full, replaced by revenues from contract forms that were designed to fully renew with legacy customers and signing new customers.

Professional services revenue decreased by $0.6 million or 29% in fiscal year 2023, compared to fiscal year 2022, primarily due to a decrease in the volume of professional services provided to customers during fiscal year 2023.

Cost of revenue
Total cost of revenue increased by $4.6 million or 49% in fiscal year 2023, compared to fiscal year 2022. Cost of product, subscription and support revenue increased by $5.2 million or 64%, in fiscal year 2023, compared to fiscal year 2022. The increase was primarily due to an increase in cloud subscription customers, costs incurred to fully ramp cloud hosting environments related to a significant revenue customer that was onboarded in the second half of fiscal year 2023, an increase in allocated labor costs related to software support services, duplicative charges that occurred while certain customers transitioned from their on-premises to cloud hosted deployment formats, and the establishment of an inventory reserve during fiscal year 2023.

Cost of professional services revenue decreased by $0.6 million or 55% in fiscal year 2023, compared to fiscal year 2022. This decrease was primarily due to a decrease in headcount and a decrease in the volume of professional services provided to customers.

Gross Profit and Gross Margin
Certain business decisions related to cost of revenue resulted in a decrease in product subscription, and support gross margin to 48% in fiscal year 2023, which would have been approximately 58% during the period when excluding the expense incurred related to establishing an inventory reserve, as compared to 68% in fiscal year 2022, and an increase in professional services gross margin to 66% in fiscal year 2023 as compared to 47% in fiscal year 2022. The period over period decrease in margin for software was primarily the result of cloud costs for a significant revenue customer that ramped up in the second half of fiscal year 2023, as well as duplicative charges that occurred while certain customers transitioned from their on-premises to cloud hosted deployment formats, the establishment of an inventory

42
reserve during fiscal year 2023, and an increase in allocated labor costs related to software support services. Professional services margin will continue to be volatile contract to contract.

The following tables show gross profit and gross margin, respectively, for product, subscription and support revenue and professional services revenue for fiscal years 2023 and 2022.

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023</th>
<th>2022</th>
<th>Change $</th>
<th>Change %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product, subscription and support gross profit</td>
<td>$12,236</td>
<td>$17,122</td>
<td>$(4,886)</td>
<td>(29)%</td>
</tr>
<tr>
<td>Professional services gross profit</td>
<td>1,027</td>
<td>1,039</td>
<td>(12)</td>
<td>1%</td>
</tr>
<tr>
<td>Total gross profit</td>
<td>$13,263</td>
<td>$18,161</td>
<td>$(4,898)</td>
<td>(27)%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023</th>
<th>2022</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product, subscription and support margin</td>
<td>47.6%</td>
<td>67.6%</td>
<td>(20.0)%</td>
</tr>
<tr>
<td>Professional services margin</td>
<td>66.1%</td>
<td>47.2%</td>
<td>18.8%</td>
</tr>
<tr>
<td>Total gross margin</td>
<td>48.7%</td>
<td>65.9%</td>
<td>(17.2)%</td>
</tr>
</tbody>
</table>

### Operating expenses

#### Research and development

Research and development expenses decreased by $20.5 million or 39%, in fiscal year 2023, as compared to fiscal year 2022, primarily as the result of non-cash stock compensation expenses of $22.9 million incurred in fiscal year 2022 triggered by the modification of restricted stock units ("RSUs"), as compared to $5.8 million in fiscal year 2023. The remaining decrease of $3.4 million was driven by a decrease in headcount, a reduction in allocated labor costs related to software support services, and cost saving actions.

#### Sales and marketing

Sales and marketing expenses decreased by $51.4 million or 62% in fiscal year 2023, as compared to fiscal year 2022, primarily due to non-cash stock compensation expense of $51.8 million incurred in fiscal year 2022 triggered by the modification of RSUs, as compared to $4.1 million in fiscal year 2023. The remaining decrease of $3.7 million was driven by the decrease in headcount and cost saving actions.

#### General and administrative

General and administrative expenses decreased by $55.1 million or 49% in fiscal year 2023, as compared to fiscal year 2022, primarily due to non-cash stock compensation expense of $81.9 million incurred in fiscal year 2022 triggered by the modification of RSUs, as compared to $27.0 million in fiscal year 2023. The remaining decrease of $0.2 million was primarily driven by the decrease in headcount and cost saving actions.

#### Interest expense

The increase in interest expense of $0.1 million is due to interest expense incurred on the Convertible Note, C5 Notes, and Director Notes of $1.3 million during fiscal year 2023, as compared to $1.2 million in interest expense incurred in fiscal year 2022 related to loans paid off at the date of the Merger.

#### Other income

Other income increased by $0.1 million or 331% in fiscal year 2023, as compared to fiscal year 2022, primarily due to historical foreign currency adjustments.

#### Other expense

Other expense increased by $2.1 million or 7,329% in fiscal year 2023, as compared to fiscal year 2022, primarily as the result of the decrease in fair value of the commitment fee derivative asset established related to the Purchase Agreement entered into with Tumim.

### Change in fair value of warrants liabilities

Change in fair value of warrants liabilities is the result of the exercise of 5.2 million Private Warrants during fiscal year 2022 and the change in fair value.

### Provision for income taxes

The provision for income taxes decreased by $0.4 million primarily due to our continued net loss position, the accumulation of net loss carryforwards and offsetting valuation allowance.

### Liquidity and Capital Resources

Based on our current planned operations, in the absence of additional sources of liquidity, management anticipates that our existing cash and cash equivalents and anticipated cash flows from operations will not be sufficient to meet our operating and liquidity needs for any meaningful period of time following the date of this report. There is no assurance that management will be able to obtain additional liquidity or be successful in raising additional funds or that such required funds, if available, will be available on attractive terms or that they will not have a significant dilutive effect on our existing stockholders. In the event we determine that additional sources of liquidity will not be available to us or will not allow us to meet our obligations as they become due, we may need to file a voluntary petition for relief under the United States Bankruptcy Code in order to implement a plan of reorganization, court-supervised sale, and/or liquidation.

Prior to March 10, 2023, we had a banking relationship with SVB. As of the closure of SVB on March 10, 2023, we held approximately $8.1 million in cash, cash equivalents and investments at or through SVB, which represented approximately 96% of our total cash, cash equivalents and investments as of that date. SVB was closed on March 10, 2023 by the California Department of Financial Protection and Innovation, which appointed the FDIC as receiver.

On March 12, 2023, the U.S. Treasury, Federal Reserve, and FDIC announced that SVB depositors would have access to all of their money starting March 13, 2023. On March 13, 2023, we were able to access all $8.1 million in cash, approximately 96% of our total cash, cash equivalents and investments as of that date. SVB was closed on March 10, 2023 by the California Department of Financial Protection and Innovation, which appointed the FDIC as receiver. We are in the process of transferring some of our deposits to multiple banks to limit any future credit risk.

### Sources of Liquidity

We have incurred losses and negative cash flows from operations since inception. Through January 31, 2023, we have funded our operations with proceeds from sales of common stock and redeemable convertible preferred stock, proceeds related to the public trust shares held by LGL that were received as part of the recapitalization, the sale of Convertible Notes (as described below) to 3i, loans issued to the Board of Directors and C5, and receipts from sales of our products and services to customers in the ordinary course of business. As of January 31, 2023, we had cash and cash equivalents of $7.6 million, $8.9 million in convertible debt outstanding under the Convertible Note, $5.0 million in convertible debt outstanding under the C5 Notes, and $6.9 million in debt outstanding under the Director Notes, all described below. To date, our primary source of liquidity has been the financing transactions described below and we are seeking additional debt funding in order to
continue our operations. Our current indebtedness matures on June 30, 2023, and we will need to either extend the maturity date of this date or raise additional funds to repay the debt in order to avoid an event of default on our current indebtedness.

Tumim Stone Capital Committed Equity Financing

On February 11, 2022, we entered into the Purchase Agreement with Tumim, pursuant to which Tumim has committed to purchase up to $175 million of common stock (the “Total Commitment”), at our direction from time to time, subject to the satisfaction of the conditions in the Purchase Agreement. Also on February 11, 2022, we entered into a registration rights agreement with Tumim (the “Registration Rights Agreement”), pursuant to which we filed with the SEC a registration statement to register for resale under the Securities Act the shares of common stock that may be issued to Tumim under the Purchase Agreement. Pursuant to the terms of the Purchase Agreement, at the time we signed the Purchase Agreement and the Registration Rights Agreement, we paid a cash fee of $1.8 million, or 1% of the Total Commitment, to Tumim as consideration for its commitment to purchase shares of our common stock under the Purchase Agreement.

The sales of common stock by us to Tumim under the Purchase Agreement, if any, will be subject to certain limitations and may occur, from time to time at our sole discretion, over the approximately 36-month period commencing upon the date of initial satisfaction of all conditions to Tumim’s purchase obligations set forth in the Purchase Agreement. We have the right, but not the obligation, from time to time at our sole discretion, to direct Tumim to purchase certain amounts of our common stock, subject to certain restrictions and limitations in the Purchase Agreement, that we specify in purchase notices that we deliver to Tumim under the Purchase Agreement (each such purchase, a “Purchase”). Shares of common stock will be issued to Tumim at either (i) a 3% discount to the average daily volume weighted average price (the “VWAP”) of the common stock during the three consecutive trading days from the date that a purchase notice with respect to a particular purchase (a “VWAP Purchase Notice”) is delivered to Tumim (a “Forward VWAP Purchase”), or (ii) 5% discount to the lowest daily VWAP during the three consecutive trading days from the date that a VWAP Purchase Notice with respect to a particular purchase is delivered to Tumim (an “Alternative VWAP Purchase”). Each VWAP Purchase Notice to Tumim will specify whether the applicable purchase is a Forward VWAP Purchase or an Alternative VWAP Purchase, and will direct that Tumim purchase the applicable number of shares of common stock at the applicable purchase price. There is no upper limit on the price per share that Tumim could be obligated to pay for the common stock under the Purchase Agreement. The purchase price per share of common stock to be sold in a Purchase will be appropriately adjusted for any reorganization, recapitalization, non-cash dividend, stock split, reverse stock split or other similar transaction.

Through January 31, 2023, we sold 2,511,365 shares to Tumim for gross proceeds of $0.6 million under the Purchase Agreement. However, we are not currently able to sell additional shares of common stock to Tumim under the Purchase Agreement.

3i Convertible Debt Facility

On September 14, 2022, we entered into a Securities Purchase Agreement (the “SPA”) with 3i, under which we agreed to sell and issue senior unsecured convertible promissory notes (the “Convertible Notes”) to 3i in an aggregate principal amount of up to approximately $25.8 million, which are convertible into shares of our common stock, subject to certain conditions and limitations. On September 15, 2022, we issued a Convertible Note under the SPA with a maturity date of March 15, 2024 in the aggregate principal amount of $10.3 million for net cash proceeds after debt discount of $10.0 million. Upon the satisfaction of additional conditions set forth in the SPA that have not yet been met, we may issue an additional Convertible Note in the principal amount of $15.5 million at a second closing.

The Convertible Notes bear interest at an annual rate of 5.00% per annum, payable monthly on the first of each month (the “Installment Date”), beginning the first month that is 90 days following the issuance date, payable in cash and/or shares of common stock, at our option. The interest rate will increase to an annual rate of 10.00% per annum upon the occurrence and during the continuance of an event of default under the Convertible Notes. Each Convertible Note issued pursuant to the SPA will have a maturity date of 18 months from issuance, which may be extended at the option of 3i in certain instances.

The Convertible Notes provide a conversion right in which 3i may convert any portion of the principal, together with any unpaid interest and other unpaid amounts, into shares of common stock at a conversion price of $7.50 per share, subject to adjustments in accordance with the terms of the Convertible Notes. However, we will not issue any shares of common stock upon conversion of any Convertible Notes, or otherwise, if the issuance of such common stock, together with any common stock issued in connection with the SPA and the transaction contemplated thereby, would exceed 20,373,592 shares, except that such limitation shall not apply in the event that we obtain the approval of our stockholders as required by the applicable rules of the NYSE for issuances of shares of common stock in excess of such amount. The Convertible Notes also contains provisions that provide 3i with the right, subject to certain exceptions, to require the Company to redeem all or a portion of the Convertible Notes in cash. This convertible feature has been bifurcated from the host contract and accounted for separately as a derivative.

On each monthly Installment Date, we shall repay the lesser of $0.7 million and the principal amount then outstanding, plus accrued and unpaid interest, in cash and/or shares of common stock, at our option (the “Installment Amount”). In certain instances, 3i will also have the right to accelerate some of the monthly repayment obligations. For any Installment Amount paid in the form of shares of common stock, the applicable conversion price will be equal to the lesser of (a) $7.50, and (b) the greater of (x)95% of the lowest VWAP in the five trading days immediately prior to such conversion, and (y) a “floor price” of approximately $0.44, subject to adjustment in accordance with the terms of the Convertible Notes. For any Installment Amount paid in cash, the price paid will be equal to 105% of the Installment Amount.

On September 14, 2022, in connection with our entry into the SPA, we also entered into a Registration Rights Agreement with 3i (the “Registration Rights Agreement”). Pursuant to the Registration Rights Agreement, we agreed to file with the Securities and Exchange Commission (the “SEC”), within 60 calendar days following the date of the Registration Rights Agreement, a registration statement covering the resale of the shares of common stock issuable upon conversion of the outstanding Convertible Notes. This registration statement was filed on November 14, 2022 and declared effective by the SEC on November 30, 2022.

During the year ended January 31, 2023, we elected to pay one of the Installment Amounts due in cash and one Installment Amount through a combination of cash and the issuance of common stock, which resulted in the issuance of 1,363,636 shares of common stock for an aggregate conversion amount of $6.4 million. As of January 31, 2023, we had $8.9 million in principal and accrued and unpaid interest outstanding related to the Convertible Notes.

Director and C5 Loans

Between December 14, 2022 and December 16, 2022, we issued and sold senior secured promissory notes in an aggregate principal amount of $6.9 million (the “Initial Director Notes”) to a total of eight lenders, which included seven lenders who are either our directors or entities affiliated with our directors. Subsequently we and the holders of the Initial Director Notes agreed to amend and restate the Initial Director Notes to be substantially in the form to be issued to C5 (the “Director Notes”). This amendment and restatement occurred on January 11, 2023. In April 2023, we issued and sold an additional Director Note in the amount of $0.3 million to the lender not affiliated with our directors. The Director Notes bear interest at a rate of 13.8% per annum from the respective dates of the Initial Director Notes, and the Director Notes are payable at scheduled maturity on June 30, 2023. As of January 31, 2023, we had $7.0 million in principal and accrued interest outstanding related to the Director Notes.

On December 30, 2022, we issued and sold a senior secured convertible promissory note in the principal amount of $2.0 million (the “Initial C5 Note”) to an affiliate of C5, which was amended and restated, the “Restated C5 Note”). On January 12, 2023, February 8, 2023, February 27, 2023, April 13, 2023, May 2, 2023, and May 8, 2023, we issued additional senior secured convertible promissory notes to affiliates of C5 (together with the Restated C5 Note, the “C5 Notes”) in principal amount of $3.5 million, $4.0 million, $2.25 million, $0.6 million, $0.9 million, and $0.4 million, respectively. Each of the C5 Notes bear interest at a rate of 13.8% per annum from the date of issuance (or in the case of the Restated C5 Note, from the date of the Initial C5 Note), and all such notes are payable at scheduled maturity on June 30, 2023, subject to acceleration in certain circumstances.

Our obligations under the Director Notes and the C5 Notes are secured by substantially all of our assets, excluding our intellectual property. The C5 Notes provide C5 with the right, at any time on or after the date that is five calendar days prior to maturity, to convert all or any portion of the aggregate principal amount of the C5 Notes, together with any accrued and unpaid interest and any other unpaid amounts, into shares of our common stock at a conversion price

44
Revenue is recognized when all of the following criteria are met:

- **Identification of the contract, or contracts, with a customer**—A contract with a customer to account for exists when (i) we enter into an enforceable contract with a customer that defines each party’s rights regarding the goods or services to be transferred and identifies the payment terms related to these goods or services, (ii) the contract has commercial substance and the parties are committed to perform, and (iii) we determine that collection of
Identification of the performance obligations in the contract—Performance obligations promised in a contract are identified based on the goods or services that will be transferred to the customer that are both capable of being distinct, whereby the customer can benefit from the goods or service either on its own or together with other resources that are readily available from third parties or from us, and are distinct in the context of the contract, whereby the transfer of the goods or services is separately identifiable from other promises in the contract. To the extent a contract includes multiple promised goods or services, we apply judgment to determine whether promised goods or services are capable of being distinct and distinct in the context of the contract. If these criteria are not met the promised goods or services are accounted for as a combined performance obligation.

Determination of the transaction price—The transaction price is determined based on the consideration to which we will be entitled in exchange for transferring goods or services to the customer.

Allocation of the transaction price to the performance obligations in the contract—We allocate the transaction price to each performance obligation based on the amount of consideration expected to be received in exchange for transferring goods and services to the customer. If the contract contains a single performance obligation, the entire transaction price is allocated to the single performance obligation.

Recognition of revenue when, or as, we satisfy performance obligations—We satisfy performance obligations either over time or at a point in time. Revenue is recognized at or over the time the related performance obligation is satisfied by transferring a promised good or service to a customer.

Costs to Obtain or Fulfill a Contract
We capitalize incremental costs of obtaining a non-cancelable subscription and support revenue contract and on professional services revenue as contract acquisition costs. The capitalized amounts consist primarily of sales commissions paid to our direct sales force. The capitalized amounts are recoverable through future revenue streams under all non-cancelable customer contracts. Amortization of capitalized costs, which occurs on a straight line basis, is included in sales and marketing expense in the accompanying consolidated statements of operations. Contract fulfillment costs include appliance hardware and installation costs that are essential in providing the future benefit of the solution, which are also capitalized. We amortize our contract fulfillment costs ratably over the contract term in a manner consistent with the related revenue recognition on that contract and are included in cost of revenue.

Stock-based Compensation
Stock compensation expense for stock options is recognized on a straight line basis and with a provision for forfeitures matched to historical experience for matured grant cohorts. Stock compensation expense for RSUs granted under the 2014 Plan, which contain both service and performance conditions, is recognized on a graded-scale basis matched to the length and vesting tranches for each grant. Stock compensation expense for RSUs granted under the 2021 Plan have only service vesting conditions. Expense will be recognized on a straight-line basis for all RSU awards with only service conditions. In the event that a RSU grant holder is terminated before the award is fully vested for RSUs granted under either Plan, the full amount of the unvested portion of the award will be recognized as a forfeiture in the period of termination. The fair value of RSUs is based on the fair value of our common stock on the date of the grant.

We use the Black-Scholes pricing model to estimate the fair value of options on the date of grant. The use of a valuation model requires management to make certain assumptions with respect to selected model inputs. We grant stock options at exercise prices determined equal to the fair value of common stock on the date of the grant. The fair value of our common stock at each measurement date is based on a number of factors, including the results of third-party valuations, our historical financial performance, and observable arms-length sales of our capital stock including convertible preferred stock, and the prospects of a liquidity event, among other inputs. We estimate an expected forfeiture rate for stock options, which is factored into the determination of stock-based compensation expense. The volatility assumption is based on the historical and implied volatility of our peer group with similar business models. The risk-free interest rate is based on U.S. Treasury zero-coupon issues with a remaining term equal to the expected life assumed at the date of grant. The dividend yield percentage is zero because we do not currently pay dividends nor do we intend to do so in the future. These estimates involve inherent uncertainties and the use of different assumptions may have resulted in stock-based compensation expense that was different from the amounts recorded.

Leases
In February 2016, the Financial Accounting Standards Board (“FASB”) issued Accounting Standards Update (“ASU”) No. 2016-02, Leases (Topic 842) Section A—Leases: Amendments to the FASB Accounting Standards Codification. The standard requires lessees to recognize the assets and liabilities arising from leases on the balance sheet and retains a distinction between finance leases and operating leases. The classification criteria for distinguishing between finance leases and operating leases are substantially similar to the classification criteria for distinguishing between capital leases and operating leases in the previous lease guidance. We adopted this standard and related amendments in the first quarter of fiscal 2023, using the modified retrospective approach.

The modified retroactive approach provides a method for recording existing leases at adoption with a cumulative adjustment to retained earnings. We elected the package of practical expedients which permits us to not reassess (1) whether any expired or existing contracts are or contain leases, (2) the lease classification for any expired or existing leases, and (3) any initial direct costs for any expired or existing leases as of the effective date. We also elected the practical expedient lease considerations to not allocate lease considerations between lease and non-lease components for real estate leases. As such, real estate lease considerations are treated as a single lease-component and accounted for accordingly.

We applied a portfolio approach to effectively account for the lease liabilities and right-of-use lease assets. We exclude leases with an initial term of 12 months or less from the application of Topic 842.

Adoption of the new standard resulted in the recording of $1.1 million and $2.7 million of current lease liabilities and long-term lease liabilities, respectively, and $2.9 million in corresponding right-of-use lease assets. The difference between the approximate value of the right-of-use lease assets and lease liabilities is attributable to deferred rent, which is comprised of tenant improvement allowance and rent abatement. The cumulative change in the beginning accumulated deficit was $0.02 million due to the adoption of Topic 842. There was no material impact on the Company’s consolidated statement of operations or consolidated statements cash flows. Comparative periods continue to be presented in accordance with legacy guidance in Topic 840.

Recently Issued Accounting Standards
Refer to Note 1 of the notes to our consolidated financial statements included in this Form 10-K for our assessment of recently issued and adopted accounting standards.

Emerging Growth Company (“EGC”) Status
We are an emerging growth company, as defined in the JOBS Act. Under the JOBS Act, emerging growth companies can delay adopting new or revised accounting standards issued subsequent to the enactment of the JOBS Act until those standards apply to private companies. We have elected to use this extended transition period for complying with certain new or revised accounting standards that have different effective dates for public and private companies until the earlier of the date we (i) are no longer an EGC or (ii) affirmatively and irrevocably opt out of the extended transition period provided in the JOBS Act. As a result, our consolidated financial statements may or may not be comparable to companies that comply with new or revised accounting pronouncements as of public companies’ effective dates.
ITEM 7A. Quantitative and Qualitative Disclosures about Market Risk

We have operations in the United States and internationally, and we are exposed to market risk in the ordinary course of our business, including the effects of foreign currency fluctuation. Information relating to quantitative and qualitative disclosures about these market risks is set forth below.

Foreign Currency Risk

The significant majority of our sales contracts are denominated in U.S. dollars, with a small number of contracts denominated in foreign currencies. A portion of our operating expenses are incurred outside the United States, denominated in foreign currencies and subject to fluctuations due to changes in foreign currency exchange rates, particularly changes in the Singapore Dollar, British Pound, Japanese Yen and Australian Dollar. Additionally, fluctuations in foreign currency exchange rates may cause us to recognize transaction gains and losses in our consolidated statements of operations. The effect of a hypothetical 10% change in foreign currency exchange rates applicable to our business would not have a material impact on our historical consolidated financial statements for fiscal year 2023 or fiscal year 2022. As the impact of foreign currency exchange rates has not been material to our historical operating results, we have not entered into derivative or hedging transactions, but we may do so in the future if our exposure to foreign currency becomes more significant.
ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA

ITEM 8 — Financial Statements and Supplementary Data

INDEX TO FINANCIAL STATEMENTS

<table>
<thead>
<tr>
<th>Report of Independent Registered Public Accounting Firm (PCAOB ID: 238)</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consolidated Financial Statements:</td>
<td>51</td>
</tr>
<tr>
<td>Consolidated Balance Sheets as of January 31, 2023 and 2022</td>
<td>52</td>
</tr>
<tr>
<td>Consolidated Statements of Operations for the years ended January 31, 2023 and 2022</td>
<td>53</td>
</tr>
<tr>
<td>Consolidated Statements of Comprehensive Loss for the years ended January 31, 2023 and 2022</td>
<td>54</td>
</tr>
<tr>
<td>Consolidated Statements of Changes in Stockholders' (Deficit) Equity for the years ended January 31, 2023 and 2022</td>
<td>55</td>
</tr>
<tr>
<td>Consolidated Statements of Cash Flows for the years ended January 31, 2023 and 2022</td>
<td>56</td>
</tr>
<tr>
<td>Notes to Consolidated Financial Statements</td>
<td>49</td>
</tr>
</tbody>
</table>
To the Board of Directors and Stockholders of IronNet, Inc.

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of IronNet, Inc. and its subsidiaries (the “Company”) as of January 31, 2023 and 2022, and the related consolidated statements of operations, of comprehensive loss, of changes in stockholders’ (deficit) equity and of cash flows for the years then ended, including the related notes (collectively referred to as the “consolidated financial statements”). In our opinion, the consolidated financial statements present fairly, in all material respects, the financial position of the Company as of January 31, 2023 and 2022, and the results of its operations and its cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America.

Substantial Doubt about the Company’s Ability to Continue as a Going Concern

The accompanying consolidated financial statements have been prepared assuming that the Company will continue as a going concern. As discussed in Note 1 to the consolidated financial statements, the Company has incurred a net loss, cash outflows from operating activities, and an accumulated deficit that raise substantial doubt about its ability to continue as a going concern. Management’s plans in regard to these matters are also described in Note 1. The consolidated financial statements do not include any adjustments that might result from the outcome of this uncertainty.

Basis for Opinion

These consolidated financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on the Company’s consolidated financial statements based on our audits. We are a public accounting firm registered with the Public Company Accounting Oversight Board (United States) (PCAOB) and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits of these consolidated financial statements in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement, whether due to error or fraud. The Company is not required to have, nor were we engaged to perform, an audit of its internal control over financial reporting. As part of our audits we are required to obtain an understanding of internal control over financial reporting but not for the purpose of expressing an opinion on the effectiveness of the Company's internal control over financial reporting. Accordingly, we express no such opinion.

Our audits included performing procedures to assess the risks of material misstatement of the consolidated financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the consolidated financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements. We believe that our audits provide a reasonable basis for our opinion.

Significant Transactions with Related Parties

As discussed in Note 14 to the consolidated financial statements, the Company has entered into significant lending transactions with certain members of the Board of Directors and C5 Capital Limited, all related parties.

/s/ PricewaterhouseCoopers LLP

Washington, District of Columbia

May 16, 2023

We have served as the Company's auditor since 2019.
IronNet, Inc.
Consolidated Balance Sheets
(in thousands, except per share data)

<table>
<thead>
<tr>
<th></th>
<th>January 31, 2023</th>
<th>January 31, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Current assets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash and cash equivalents</td>
<td>$7,568</td>
<td>$47,673</td>
</tr>
<tr>
<td>Accounts receivable</td>
<td>3,373</td>
<td>1,991</td>
</tr>
<tr>
<td>Unbilled receivables</td>
<td>717</td>
<td>4,637</td>
</tr>
<tr>
<td>Related party receivables</td>
<td>—</td>
<td>2,333</td>
</tr>
<tr>
<td>Accounts and related party receivables</td>
<td>$4,090</td>
<td>9,861</td>
</tr>
<tr>
<td>Inventory</td>
<td>2,669</td>
<td>4,581</td>
</tr>
<tr>
<td>Deferred costs</td>
<td>3,138</td>
<td>2,999</td>
</tr>
<tr>
<td>Prepaid warranty</td>
<td>1,218</td>
<td>829</td>
</tr>
<tr>
<td>Prepaid expenses</td>
<td>1,743</td>
<td>3,660</td>
</tr>
<tr>
<td>Other current assets</td>
<td>818</td>
<td>1,458</td>
</tr>
<tr>
<td><strong>Total current assets</strong></td>
<td>$21,244</td>
<td>$70,661</td>
</tr>
<tr>
<td>Deferred costs</td>
<td>2,975</td>
<td>3,243</td>
</tr>
<tr>
<td>Property and equipment, net</td>
<td>5,972</td>
<td>5,606</td>
</tr>
<tr>
<td>Prepaid warranty</td>
<td>1,141</td>
<td>1,229</td>
</tr>
<tr>
<td>Deposits and other assets</td>
<td>2,327</td>
<td>493</td>
</tr>
<tr>
<td><strong>Total assets</strong></td>
<td>$33,659</td>
<td>$81,232</td>
</tr>
<tr>
<td><strong>Liabilities and stockholders' (deficit) equity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Current liabilities</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts payable</td>
<td>$7,287</td>
<td>$2,348</td>
</tr>
<tr>
<td>Accrued expenses</td>
<td>9,973</td>
<td>4,709</td>
</tr>
<tr>
<td>Deferred revenue</td>
<td>17,180</td>
<td>16,049</td>
</tr>
<tr>
<td>Deferred rent</td>
<td>—</td>
<td>159</td>
</tr>
<tr>
<td>Related party notes payable</td>
<td>11,845</td>
<td>—</td>
</tr>
<tr>
<td>Convertible notes payable</td>
<td>8,128</td>
<td>—</td>
</tr>
<tr>
<td>Conversion features on convertible notes payable</td>
<td>734</td>
<td>—</td>
</tr>
<tr>
<td>Income tax payable</td>
<td>412</td>
<td>542</td>
</tr>
<tr>
<td>Other current liabilities</td>
<td>735</td>
<td>689</td>
</tr>
<tr>
<td><strong>Total current liabilities</strong></td>
<td>$56,294</td>
<td>24,496</td>
</tr>
<tr>
<td>Deferred revenue</td>
<td>9,961</td>
<td>17,517</td>
</tr>
<tr>
<td>Deferred rent</td>
<td>—</td>
<td>769</td>
</tr>
<tr>
<td>Warrants</td>
<td>—</td>
<td>7</td>
</tr>
<tr>
<td>Other long-term liabilities</td>
<td>2,128</td>
<td>—</td>
</tr>
<tr>
<td><strong>Total liabilities</strong></td>
<td>$68,383</td>
<td>$42,789</td>
</tr>
<tr>
<td><strong>Stockholders' (deficit) equity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preferred stock, $0.0001 par value; none issued or outstanding</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Common stock, $0.0001 par value; 111,466 and 88,876 shares issued and outstanding at January 31, 2023 and January 31, 2022, respectively</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>Additional paid-in capital</td>
<td>493,902</td>
<td>455,849</td>
</tr>
<tr>
<td>Accumulated other comprehensive income</td>
<td>59</td>
<td>271</td>
</tr>
<tr>
<td>Accumulated deficit</td>
<td>(528,696)</td>
<td>(417,686)</td>
</tr>
<tr>
<td><strong>Total stockholders' (deficit) equity</strong></td>
<td>$34,724</td>
<td>38,445</td>
</tr>
<tr>
<td><strong>Total liabilities and stockholders' (deficit) equity</strong></td>
<td>$33,659</td>
<td>$81,232</td>
</tr>
</tbody>
</table>

The accompanying notes are an integral part of these financial statements.
<table>
<thead>
<tr>
<th></th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product, subscription and support revenue</td>
<td>$25,703</td>
<td>$25,347</td>
</tr>
<tr>
<td>Professional services revenue</td>
<td>1,554</td>
<td>2,197</td>
</tr>
<tr>
<td><strong>Total revenue</strong></td>
<td>27,257</td>
<td>27,544</td>
</tr>
<tr>
<td>Cost of product, subscription and support revenue</td>
<td>13,467</td>
<td>8,225</td>
</tr>
<tr>
<td>Cost of professional services revenue</td>
<td>527</td>
<td>1,158</td>
</tr>
<tr>
<td><strong>Total cost of revenue</strong></td>
<td>13,994</td>
<td>9,383</td>
</tr>
<tr>
<td><strong>Gross profit</strong></td>
<td>13,263</td>
<td>18,161</td>
</tr>
<tr>
<td><strong>Operating expenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research and development</td>
<td>32,426</td>
<td>52,899</td>
</tr>
<tr>
<td>Sales and marketing</td>
<td>31,550</td>
<td>82,922</td>
</tr>
<tr>
<td>General and administrative</td>
<td>57,000</td>
<td>112,099</td>
</tr>
<tr>
<td><strong>Total operating expenses</strong></td>
<td>120,976</td>
<td>247,928</td>
</tr>
<tr>
<td><strong>Operating loss</strong></td>
<td>(107,713)</td>
<td>(229,759)</td>
</tr>
<tr>
<td>Interest expense</td>
<td>(1,273)</td>
<td>(1,155)</td>
</tr>
<tr>
<td>Other income</td>
<td>108</td>
<td>25</td>
</tr>
<tr>
<td>Other expense</td>
<td>(2,080)</td>
<td>(28)</td>
</tr>
<tr>
<td>Change in fair value of warrant liabilities</td>
<td>6</td>
<td>(31,265)</td>
</tr>
<tr>
<td><strong>Loss before income taxes</strong></td>
<td>(110,952)</td>
<td>(242,182)</td>
</tr>
<tr>
<td>Provision for income taxes</td>
<td>(58)</td>
<td>(465)</td>
</tr>
<tr>
<td><strong>Net loss</strong></td>
<td>(111,010)</td>
<td>(242,647)</td>
</tr>
<tr>
<td>Basic and diluted net loss per common share</td>
<td>(1.07)</td>
<td>(3.03)</td>
</tr>
<tr>
<td>Weighted average shares outstanding, basic and diluted</td>
<td>104,049</td>
<td>79,953</td>
</tr>
</tbody>
</table>

The accompanying notes are an integral part of these financial statements.
IronNet, Inc.
Consolidated Statements of Comprehensive Loss
($ in thousands)

<table>
<thead>
<tr>
<th></th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net loss</td>
<td>$(111,010)</td>
<td>$(242,647)</td>
</tr>
<tr>
<td>Foreign currency translations adjustment, net of tax</td>
<td>$(212)</td>
<td>$231</td>
</tr>
<tr>
<td>Total Comprehensive loss</td>
<td>$(111,222)</td>
<td>$(242,416)</td>
</tr>
</tbody>
</table>

The accompanying notes are an integral part of these financial statements.
<table>
<thead>
<tr>
<th>Common Stock</th>
<th>Additional Paid-In Capital</th>
<th>Accumulated Deficit</th>
<th>Accumulated Other Comprehensive Income</th>
<th>Subscription Notes Receivable</th>
<th>Total Stockholders' (Deficit) Equity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shares</td>
<td>Amount</td>
<td>Shares</td>
<td>Amount</td>
<td>Shares</td>
<td>Amount</td>
</tr>
<tr>
<td>Balance at January 31, 2022</td>
<td>88,876</td>
<td>$9</td>
<td>$455,849</td>
<td>$(417,686)</td>
<td>$271</td>
</tr>
<tr>
<td>Exercise of stock options and settlement of restricted stock units</td>
<td>18,730</td>
<td>2</td>
<td>294</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Statutory tax withholding related to net-share settlement of restricted stock units</td>
<td>(15)</td>
<td>-</td>
<td>-</td>
<td>(91)</td>
<td>-</td>
</tr>
<tr>
<td>Common stock issued under common stock purchase agreement</td>
<td>2,511</td>
<td>-</td>
<td>586</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Common stock issued for repayment of convertible debt</td>
<td>1,364</td>
<td>-</td>
<td>406</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Stock-based compensation</td>
<td>-</td>
<td>-</td>
<td>36,858</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Net loss</td>
<td>-</td>
<td>-</td>
<td>(111,010)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Foreign currency translation adjustment</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(212)</td>
<td>-</td>
</tr>
<tr>
<td>Balance at January 31, 2023</td>
<td>111,466</td>
<td>$11</td>
<td>$493,902</td>
<td>$(528,696)</td>
<td>$59</td>
</tr>
<tr>
<td>Balance at January 31, 2021</td>
<td>66,934</td>
<td>$7</td>
<td>$180,853</td>
<td>$(175,039)</td>
<td>$40</td>
</tr>
<tr>
<td>Issuance of common stock</td>
<td>755</td>
<td>-</td>
<td>365</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Merger recapitalization</td>
<td>4,555</td>
<td>1</td>
<td>(12,027)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Issuance of PIPE Shares</td>
<td>12,500</td>
<td>1</td>
<td>109,857</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Issuance of common stock upon exercise of Public Warrants</td>
<td>29</td>
<td>-</td>
<td>330</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Issuance of common stock upon exercise of Private Warrants</td>
<td>3,188</td>
<td>-</td>
<td>21,492</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Issuance of merger earnout shares</td>
<td>1,078</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Interest earned on subscription notes receivable</td>
<td>-</td>
<td>-</td>
<td>8</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Settlement of related party loan receivable for common shares</td>
<td>(108)</td>
<td>-</td>
<td>(1,075)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Payment of note receivable and settlement of notes receivable for common shares</td>
<td>(55)</td>
<td>-</td>
<td>(550)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Stock-based compensation</td>
<td>-</td>
<td>-</td>
<td>156,596</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Net loss</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(242,647)</td>
<td>-</td>
</tr>
<tr>
<td>Foreign currency translation adjustment</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Balance at January 31, 2022</td>
<td>88,876</td>
<td>$9</td>
<td>$455,849</td>
<td>$(417,686)</td>
<td>$271</td>
</tr>
</tbody>
</table>

The accompanying notes are an integral part of these financial statements.
### IronNet, Inc.
#### Consolidated Statements of Cash Flows

($ in thousands)

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31,</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cash flows from operating activities</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net loss</td>
<td>$ (111,010)</td>
<td>$ (242,647)</td>
</tr>
<tr>
<td>Adjustments to reconcile net loss to net cash used in operating activities:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Depreciation and amortization</td>
<td>2,336</td>
<td>1,092</td>
</tr>
<tr>
<td>Gain on sale of fixed assets</td>
<td>(27)</td>
<td>(6)</td>
</tr>
<tr>
<td>Loss of disposal of fixed assets</td>
<td>117</td>
<td>—</td>
</tr>
<tr>
<td>Bad debt expense</td>
<td>1,283</td>
<td>—</td>
</tr>
<tr>
<td>Employee stock-based compensation</td>
<td>36,858</td>
<td>156,596</td>
</tr>
<tr>
<td>Change in fair value of warrant liabilities</td>
<td>(6)</td>
<td>11,265</td>
</tr>
<tr>
<td>Change in fair value of conversion options</td>
<td>(103)</td>
<td>—</td>
</tr>
<tr>
<td>Change in fair value of commitment fee</td>
<td>1,555</td>
<td>—</td>
</tr>
<tr>
<td>Conversion option accretion</td>
<td>326</td>
<td>—</td>
</tr>
<tr>
<td>Non-cash interest expense</td>
<td>897</td>
<td>1,155</td>
</tr>
<tr>
<td>Non-cash interest income on amounts due from stockholders</td>
<td>—</td>
<td>(8)</td>
</tr>
<tr>
<td>Excess inventory adjustment</td>
<td>2,744</td>
<td>—</td>
</tr>
<tr>
<td><strong>Changes in operating assets and liabilities:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts and related party receivable</td>
<td>4,489</td>
<td>(3,194)</td>
</tr>
<tr>
<td>Deferred costs</td>
<td>(272)</td>
<td>(1,718)</td>
</tr>
<tr>
<td>Inventories</td>
<td>(832)</td>
<td>(2,401)</td>
</tr>
<tr>
<td>Prepaid expenses</td>
<td>1,918</td>
<td>(1,614)</td>
</tr>
<tr>
<td>Other current assets</td>
<td>(124)</td>
<td>(2,407)</td>
</tr>
<tr>
<td>Prepaid warranty</td>
<td>(301)</td>
<td>(144)</td>
</tr>
<tr>
<td>Deposits and other assets</td>
<td>865</td>
<td>(196)</td>
</tr>
<tr>
<td>Accounts payable</td>
<td>4,939</td>
<td>398</td>
</tr>
<tr>
<td>Accrued expenses</td>
<td>(2,306)</td>
<td>971</td>
</tr>
<tr>
<td>Income tax payable</td>
<td>(130)</td>
<td>454</td>
</tr>
<tr>
<td>Other liabilities</td>
<td>(692)</td>
<td>(689)</td>
</tr>
<tr>
<td>Deferred rent</td>
<td>(134)</td>
<td>—</td>
</tr>
<tr>
<td>Deferred revenue</td>
<td>(6,425)</td>
<td>(477)</td>
</tr>
<tr>
<td>Warrants</td>
<td>—</td>
<td>20</td>
</tr>
<tr>
<td>Operating lease liability</td>
<td>(972)</td>
<td>—</td>
</tr>
<tr>
<td><strong>Net cash used in operating activities</strong></td>
<td>(64,872)</td>
<td>(83,684)</td>
</tr>
<tr>
<td><strong>Cash flows from investing activities</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchases of property and equipment</td>
<td>(142)</td>
<td>(1,714)</td>
</tr>
<tr>
<td>Capitalized software development costs</td>
<td>(2,375)</td>
<td>(2,166)</td>
</tr>
<tr>
<td>Proceeds from the sale of fixed assets</td>
<td>32</td>
<td>—</td>
</tr>
<tr>
<td><strong>Net cash used in investing activities</strong></td>
<td>(2,498)</td>
<td>(3,872)</td>
</tr>
<tr>
<td><strong>Cash flows from financing activities</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exercise of stock options</td>
<td>296</td>
<td>—</td>
</tr>
<tr>
<td>Statutory tax withholding related to net-share settlement of restricted stock units</td>
<td>(91)</td>
<td>—</td>
</tr>
<tr>
<td>Cash received to fund employee tax obligation for vested RSUs</td>
<td>20,401</td>
<td>—</td>
</tr>
<tr>
<td>Cash remitted to fund employee tax obligation for vested RSUs</td>
<td>(12,467)</td>
<td>—</td>
</tr>
<tr>
<td>Payment of equity line commitment fee</td>
<td>(1,750)</td>
<td>—</td>
</tr>
<tr>
<td>Proceeds from issuance of convertible notes</td>
<td>10,000</td>
<td>—</td>
</tr>
<tr>
<td>Proceeds from issuance of related party debt</td>
<td>11,900</td>
<td>—</td>
</tr>
<tr>
<td>Payment of debt issuance costs</td>
<td>(284)</td>
<td>—</td>
</tr>
<tr>
<td>Repayment of debt</td>
<td>(1,023)</td>
<td>—</td>
</tr>
<tr>
<td>Payment of finance lease obligations</td>
<td>(98)</td>
<td>—</td>
</tr>
<tr>
<td>Proceeds from issuance of common stock</td>
<td>586</td>
<td>694</td>
</tr>
<tr>
<td>Proceeds from borrowing under SVB bridge loan</td>
<td>—</td>
<td>15,000</td>
</tr>
<tr>
<td>Payment of SVB bridge loan</td>
<td>—</td>
<td>(15,000)</td>
</tr>
<tr>
<td>Payment of PPP loan</td>
<td>—</td>
<td>(5,580)</td>
</tr>
<tr>
<td>Merger recapitalization</td>
<td>—</td>
<td>4,213</td>
</tr>
<tr>
<td>Proceeds from issuance of PIPE shares</td>
<td>—</td>
<td>125,000</td>
</tr>
<tr>
<td>Payment of merger transaction costs</td>
<td>—</td>
<td>(21,179)</td>
</tr>
<tr>
<td>Proceeds from stock subscriptions</td>
<td>—</td>
<td>293</td>
</tr>
<tr>
<td><strong>Net cash provided by financing activities</strong></td>
<td>27,470</td>
<td>103,441</td>
</tr>
<tr>
<td>Effect of exchange rate changes on cash and cash equivalents</td>
<td>(212)</td>
<td>245</td>
</tr>
<tr>
<td><strong>Net change in cash and cash equivalents</strong></td>
<td>(40,050)</td>
<td>14,130</td>
</tr>
<tr>
<td><strong>Cash and cash equivalents</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beginning of the period</td>
<td>$ 47,673</td>
<td>$ 31,543</td>
</tr>
<tr>
<td>End of the period</td>
<td>$ 7,568</td>
<td>$ 47,673</td>
</tr>
</tbody>
</table>

**Supplemental disclosure of cash flow information**

| Cash paid for interest | $ 126 | — |

**Supplemental disclosures of non-cash investing and financing activities**

| Interest earned on subscription notes receivable | — | 8 |
| Liquid purchases of property and equipment | — | 28 |
| Non-cash settlement of related party loan receivable for common shares | — | 1,075 |
| Initial classification of warrant liabilities | — | 10,234 |
| Cashless exercise of warrants classified as liabilities | — | 10,214 |

The accompanying notes are an integral part of these financial statements.

Organization
IronNet, Inc., formerly known as LGL Systems Acquisition Corporation (“Legacy LGL”), was incorporated in the state of Delaware on April 30, 2019 for the purpose of entering into a merger, share exchange, asset acquisition, stock purchase, recapitalization, reorganization or other similar business combination with one or more businesses or entities.

On March 15, 2021, Legacy LGL entered into an Agreement and Plan of Reorganization and Merger (“Merger Agreement”), as amended on August 6, 2021, by and among Legacy LGL, LGL Systems Merger Sub Inc. (the “Merger Sub”) and IronNet Cybersecurity, Inc. ("Legacy IronNet"). On August 26, 2021, the Merger Agreement was consummated and the Merger was completed (the “Merger”). In connection with the Merger, Legacy LGL changed its name to IronNet, Inc., and the New York Stock Exchange (“NYSE”) ticker symbols for its Class A common stock and warrants were changed to “IRNT” and “IRNT WS” respectively.

Throughout the notes to the consolidated financial statements, unless otherwise noted, “we,” “us,” “our,” “IronNet,” the "Company," and similar terms refer to Legacy IronNet and its subsidiaries prior to the consummation of the transactions associated with the Merger, and IronNet, Inc. and the Company's subsidiaries after the Merger.

Pursuant to the Merger Agreement, at the effective time of the Merger, (i) each outstanding share of Legacy IronNet common stock and preferred stock (with each share of Legacy IronNet preferred stock being treated as if it were converted into ten (10) shares of Legacy IronNet common stock on the effective date of the Merger) was converted into the right to receive (a) a number of shares of Company common stock equal to the Exchange Ratio (as defined below) and (b) a cash amount payable in respect of fractional shares of Legacy IronNet common stock that would otherwise be issued in connection with the foregoing conversion, if applicable, and (ii) each Legacy IronNet option, restricted stock unit, restricted stock award that was outstanding immediately prior to the closing of the Merger (and by its terms did not terminate upon the closing of the Merger) remains outstanding and (x) in the case of options, represents the right to purchase a number of shares of Company common stock equal to the number of shares of Legacy IronNet common stock subject to such option multiplied by the Exchange Ratio used for Legacy IronNet common stock (rounded down to the nearest whole share) at an exercise price per share equal to the current exercise price per share for such option divided by the Exchange Ratio (rounded up to the nearest whole cent) and (y) in the case of restricted stock units and restricted stock awards, represent a number of shares of Company common stock equal to the number of shares of Legacy IronNet common stock subject to such restricted stock unit or restricted stock award multiplied by the Exchange Ratio (rounded down to the nearest whole share). In addition, Legacy IronNet stockholders and eligible holders of options, restricted stock unit awards and restricted stock awards (as applicable, only to the extent time vested as of the closing of the Merger) were also eligible to receive additional merger consideration in the form of a pro rata portion of 1,078 shares of Company common stock if the volume weighted average closing share price for the Company’s common stock equaled or exceeded $13.00 for ten (10) consecutive days during the two-year period following the closing of the Merger. This condition was satisfied and the additional shares of Company common stock were issued in September 2021.

The Merger was accounted for as a reverse recapitalization. Under this method of accounting, Legacy LGL has been treated as the acquired company for financial reporting purposes. This determination was primarily based on Legacy IronNet stockholders being the majority stockholders and holding majority voting power in the combined company, Legacy IronNet senior management comprising the majority of the senior management of the combined company, and Legacy IronNet ongoing operations comprising the ongoing operations of the combined company. Accordingly, for accounting purposes, the Merger was treated as the equivalent of Legacy IronNet issuing shares for the net assets of Legacy LGL, accompanied by a recapitalization. The net assets of Legacy LGL were recognized at fair value (which was consistent with carrying value), with no goodwill or other intangible assets recorded. Operations prior to the Merger in these financial statements are those of Legacy IronNet and the retained earnings of Legacy IronNet has been carried forward after the Merger. Share numbers and the related earnings (loss) per share calculations for all periods prior to the Merger have been retrospectively adjusted for the equivalent number of shares reflecting the exchange ratio established in the Merger. Refer to Note 3. Reverse Recapitalization and Restructuring for additional information.

Nature of Operations
IronNet provides a suite of technologies that provide real-time threat assessment and updates, behavioral modeling, big data analytics, and proactive threat detection and response capabilities as well as consulting services and training programs to protect against current and emerging cyber-threats.

Basis of Presentation and Principles of Consolidation
The accompanying consolidated financial statements have been prepared on the accrual basis of accounting in accordance with accounting principles generally accepted in the United States of America (“U.S. GAAP”). The consolidated financial statements include the accounts of all subsidiaries, all of which are wholly owned for the fiscal years ended January 31, 2023 and 2022. Intercompany accounts and transactions have been eliminated in consolidation.

Use of Estimates
The preparation of financial statements in conformity with U.S. GAAP requires the use of estimates and assumptions by management in determining the reported amounts of assets and liabilities and disclosures of contingent assets and liabilities at the date of the consolidated financial statements and the reported amounts of revenues and expenses during the reporting period. Such management estimates and assumptions include, but are not limited to, the period of benefit for deferred commissions, the useful life of property and equipment, stock-based compensation expense, fair value of warrants, embedded derivatives within convertible debt agreements, and income taxes. If the underlying estimates and assumptions upon which the financial statements are based change in future periods, actual amounts may differ from those included in the accompanying consolidated financial statements.

Liquidity
In accordance with Accounting Standards Update (“ASU”) 2014-15, Disclosure of Uncertainties about an Entity’s Ability to Continue as a Going Concern (Subtopic 205-40), the Company has evaluated whether there are conditions and events, considered in the aggregate, that raise substantial doubt about the Company’s ability to continue as a going concern within one year after the date that the consolidated financial statements are issued. For the year ended January 31, 2023, the Company incurred a net loss of $(511,010), and as of January 31, 2023, the Company had an accumulated deficit of $528,696. In addition, during the year ended January 31, 2023, the Company used $64,873 of cash in operating activities. Because of the numerous risks and uncertainties associated with the Company’s commercialization and development efforts, the Company is unable to predict when it will become profitable, and it may never become profitable. The Company’s inability to achieve and then maintain profitability would negatively affect its business, financial condition, results of operations and cash flows.

As of January 31, 2023, the Company had cash and cash equivalents of $57,568, which is not legally restricted to use, and collectable receivables

56
of $4,090, accounts payable and accrued expenses of $17,269, including $6,987 due to taxing authorities, $8,927 in principal amounts owed on convertible debt, and $11,900 in principal amounts owed on related party debt, as discussed in Note 12. In February 2022, the Company entered into an equity line with Tumim Stone Capital, LLC ("Tumim") under which the Company may, in its discretion, sell shares of its common stock to Tumim subject to various conditions and limitations set forth in the purchase agreement with Tumim. In November and December 2022, the Company issued shares of common stock to Tumim for net proceeds of $586. The Company is not currently able to raise additional funds under the equity line with Tumim.

On September 14, 2022, the Company entered into a Securities Purchase Agreement ("SPA") with 3i LP ("3i"), which is an affiliate of Tumim, pursuant to which the Company agreed to sell and issue senior unsecured convertible promissory notes in the aggregate principal amount of up to $25,750. On September 15, 2022, the Company issued a Convertible Note to 3i in the principal amount of $10,300, net of discount for cash proceeds of $10,000. The Company may, subject to a number of conditions set forth in the SPA with 3i, including specified minimum trading prices and trading volumes, and the repayment or conversion of a specified portion of the initial Convertible Note, borrow an additional $15,450 from 3i on the same terms and conditions as set forth in the initial Convertible Note. As of the date of this report, the conditions to the additional borrowing have not been met.

Between December 14, 2022 and April 20, 2023, the Company issued senior secured promissory notes in an aggregate principal amount of $7,200 to a total of eight lenders including directors of the Company. Between January 11, 2023 and May 8, 2023, the Company issued senior secured convertible promissory notes in the aggregate principal amount of $13,095 to entities affiliated with C5 Capital Limited ("C5"), a beneficial owner of more than 5% of the Company’s outstanding common stock. As of January 31, 2023, the Company had issued $6,900 in senior secured promissory notes to eight lenders and $5,000 in senior secured convertible promissory notes to C5. See Note 12 for more information.

The Company’s future capital requirements will depend on many factors, including, but not limited to, its ability to attract and retain customers and their willingness and ability to pay for the Company's products and services, and the timing and extent of spending to support its efforts to market and develop its products. Further, the Company may enter into future arrangements to acquire or invest in businesses, products, services, strategic partnerships, and technologies. The Company needs additional equity or debt financing in order to continue its operations, which it may not be able to raise on terms acceptable to it or at all. If additional funds are not available to the Company on acceptable terms, or at all, the Company’s business, financial condition, and results of operations would be adversely affected.

During the year ended January 31, 2023, the Company undertook a restructuring that reduced its headcount by approximately 44%. Refer to Note 3 for additional information. Subsequent to January 31, 2023, the Company undertook additional actions to reduce its operating expenses and preserve its cash. Despite the Company’s current operating plans to focus its business, reduce its expenses, improve its margins and mitigate uncertainties related to the foregoing, management believes that the Company does not have sufficient cash and cash equivalents on hand to support current operations for at least one year from the date of issuance of these consolidated financial statements without additional financing. Management has concluded that there is substantial doubt about the Company’s ability to continue as a going concern. The financial statements do not include any adjustments that might become necessary should the Company be unable to continue as a going concern.

Based on its current planned operations, in the absence of additional sources of liquidity, management anticipates that the Company’s existing cash and cash equivalents and anticipated cash flows from operations will not be sufficient to meet the Company’s operating and liquidity needs for any meaningful period of time following the date of this report. In the event the Company determines that additional sources of liquidity will not be available to it or will not allow it to meet its obligations as they become due, the Company may need to file a voluntary petition for relief under the United States Bankruptcy Code in order to implement a plan of reorganization, court-supervised sale, and/or liquidation.

Summary of Significant Accounting Policies

Cash Equivalents
The Company considers all highly-liquid instruments readily convertible into known amounts of cash with original maturities of three months or less to be cash equivalents.

Accounts and Loan Receivable
Accounts receivable, including unbilled, are generated from contracts with customers. Management determines the need for an allowance for doubtful accounts by evaluating individual customer receivables and considering a customer’s financial condition, credit history and current economic conditions. Individual uncollectible accounts are written off against the allowance when collection of the individual accounts appears doubtful. Management has evaluated the need for an allowance for doubtful accounts and at January 31, 2023 and 2022, the Company recorded an allowance for doubtful accounts of $1,283 and $0, respectively.

Concentrations of Credit Risk
The Company’s assets that are exposed to credit risk consist primarily of cash and cash equivalents and accounts receivable. Cash and cash equivalents are maintained at financial institutions and, at times, balances may exceed federally insured limits. The Company has never experienced any losses related to these balances. Amounts on deposit in excess of federally insured limits of $250 or accounts not included in federally insured limits at January 31, 2023 approximate $6,769. Accounts receivable consist primarily of amounts due from commercial entities.

As of January 31, 2023, the Company held cash deposits at Silicon Valley Bank ("SVB") in excess of government insured limits. On March 10, 2023, SVB was closed by the California Department of Financial Protection and Innovation, and the Federal Deposit Insurance Corporation ("FDIC") was appointed as receiver and SVB was subsequently transferred into a new entity, Silicon Valley Bridge Bank, N.A. ("SVB Bridge Bank"). On March 12, 2023, the U.S. Treasury Department, the Federal Reserve and the FDIC jointly announced enabling actions that fully protect all SVB depositors’ insured and uninsured deposits, and that such depositors would have access to all of their funds starting March 13, 2023. On March 13, 2023, the Company was able to access its full deposits with SVB.

Inventory
Inventory is stated at the lower of cost or net realizable value. The Company recorded an inventory provision of $2,744 and $0 for January 31, 2023 and 2022, respectively, to reduce slow-moving, obsolete or unusable inventories to their net realizable values for January 31, 2023 and 2022. Substantially all inventory is finished goods.

Deferred Costs
The Company amortizes contract fulfillment costs ratably over the contract term in a manner consistent with the related revenue recognition on that contract and are included in cost of revenue. These costs include appliance hardware and installation costs that are essential in providing the future benefit of the solution.

Deferred Commissions

57
Sales commissions paid to initially obtain a contract are considered incremental and recoverable costs and are deferred and then amortized on a straight-line basis over the period of benefit determined to be between one and five years, which includes the contractual and expected renewal periods. Incremental sales commissions that may be paid upon the renewal of a contract are also considered incremental and recoverable costs, which are deferred and amortized on a straight-line basis over the renewal period. The Company recognizes the incremental costs to initially obtain a contract with a customer on the consolidated balance sheet if the Company expects the benefit of those costs to be longer than one year. Amortization expense is included in sales and marketing expenses in the accompanying consolidated statement of operations.

Sales commissions paid upon renewal are substantially lower than the commissions paid to initially obtain the contract and are expensed in the period the contract is renewed. The majority of customer contracts are annual and as a result these renewals commissions are paid on an annual basis.

**Property and Equipment**

Property and equipment is stated at cost and depreciated over the asset's estimated useful life using the straight-line method. Expenditures for major additions and improvements are capitalized and minor replacements for maintenance, and repairs are charged to expense as incurred. The Company has incurred repair and maintenance charges of $28 and $12 for the years ended January 31, 2023 and 2022, respectively. When property and equipment is retired or otherwise disposed of, the cost and accumulated depreciation and amortization is removed and any resulting gain or loss is included in the results of operations.

Property and equipment are stated at cost, less accumulated depreciation and amortization. Depreciation is computed using the straight-line method over the estimated useful lives of the respective assets, as follows:

<table>
<thead>
<tr>
<th>Property</th>
<th>Useful Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer and other equipment</td>
<td>3-5 years</td>
</tr>
<tr>
<td>Leasehold improvements</td>
<td>Shorter of life of lease or life of asset</td>
</tr>
<tr>
<td>Furniture and fixtures</td>
<td>7 years</td>
</tr>
<tr>
<td>Software</td>
<td>3 years</td>
</tr>
</tbody>
</table>

**Deferred Revenue (Contract Liabilities)**

Deferred revenue, which is a contract liability, consists of amounts for which the Company has the unconditional right to bill or advance from customers for which have not yet recognized revenue. The Company generally bills customers in advance. To the extent the Company bills customers in advance of the contract commencement date, the amounts recoverable and corresponding deferred revenue amounts are netted to zero on the consolidated balance sheets, unless the Company has the unconditional right to receive the consideration at the time the customer has been invoiced. To the extent the Company has the unconditional right to bill or advance from customers, if the customer has not yet been invoiced, unbilled receivables are established for the amount for which the Company has the unconditional right to bill, with corresponding deferred revenue established for the portion for which the Company has not yet recognized revenue. Included within deferred revenue are certain amounts collected from customers that can be refundable, all or in part, under termination for convenience provisions. There is no history of refunds to customers in connection with such provisions.

**Leases**

The Company leases certain office space and equipment and determines if a contract is a lease or contains a lease at the inception of the contract and reassesses that conclusion if the contract is modified. All leases are assessed for classification as an operating lease or a finance lease. Right-of-use (“ROU”) assets for operating leases are included in the deposits and other assets caption and ROU assets associated with finance leases are included within the property and equipment, net caption of the Company's consolidated balance sheet. The current portions of operating and finance lease liabilities are included in the other current liabilities caption and the long-term portion of operating lease liabilities is presented in the other long-term liabilities payable caption of the consolidated balance sheet.

ROU assets represent the Company's right to use an underlying asset for the lease term and lease liabilities represent its obligation to make lease payments arising from the lease. ROU assets and liabilities are recognized at the lease commencement date based on the estimated present value of lease payments over the lease term. The ROU asset is adjusted for any lease payments made and excludes lease incentives and initial direct costs incurred. If the leases do not provide an implicit rate, the Company uses an incremental borrowing rate based on the information available at the lease commencement date in determining the present value of lease payments. The incremental borrowing rate is determined using a portfolio approach based on the rate of interest that the Company would pay to borrow an amount equal to the lease payments on a collateralized basis over a similar term. The Company uses quoted interest rates obtained from financial institutions as an input to derive its incremental borrowing rate as the discount rate for the lease. Leases with an initial term of 12 months or less are not recorded on the balance sheet, and the Company recognizes lease expense for these leases on a straight-line basis over the lease term. For lease agreements entered into or reassessed after the adoption of Topic 842, the Company combines lease and non-lease components.

The Company has elected the practical expedient offered by the standard to not separate the lease from non-lease components and accounts for them as a single lease component. The Company elected to not separate the lease from non-lease components and accounts for them as a single lease component. The Company elected the practical expedient permitted under the transition guidance, which allows the Company to carry forward its historical lease classification, in its assessment on whether a contract is or contains a lease, and its initial direct costs for any leases that existed prior to adoption of the new standard. The Company has elected, for all classes of underlying assets, not to recognize ROU assets and lease liabilities for leases with a term of twelve months or less. Lease cost for short-term leases is recognized on a straight-line basis over the lease term.

**Foreign Currency Translation**

The United States Dollar (USD) is the functional currency of the Company and its subsidiaries in the United States. The subsidiaries' financial statements are maintained in their functional currencies, which is the local currency in their country of origin. The foreign subsidiaries' financial statements are translated into USD. Assets and liabilities are translated into USD using the period-end foreign exchange rates. Income and expenses are translated into USD using the weighted-average exchange rates in effect during the period. Equity accounts are translated at historical exchange rates. The effects of these translation adjustments are reported as a component of accumulated other comprehensive income (loss) included in consolidated statements of changes in stockholders' equity.

**Revenue Recognition**

The Company's revenues are derived from sales of products, subscriptions, support and maintenance and other services. Revenue is recognized when all of the following criteria are met:

- Identification of the contract, or contracts, with a customer—A contract with a customer to account for exists when (i) the Company enters into an enforceable contract with a customer that defines each party’s rights regarding the goods or services to be transferred and identifies the payment terms related to these goods or services, (ii) the contract has commercial substance and the parties are committed to perform, and (iii) the Company determines that collection of substantially all consideration to which it will be entitled in exchange for goods or services that will be transferred is probable based on the customer’s intent and ability to
pay the promised consideration.

- **Identification of the performance obligations in the contract**—Performance obligations promised in a contract are identified based on the goods or services that will be transferred to the customer and that are both capable of being distinct, whereby the customer can benefit from the goods or services either on its own or in conjunction with other resources that are readily available from third parties or from us, and are distinct in the context of the contract, whereby the transfer of the goods or services is separately identifiable from other promises in the contract. To the extent a contract includes multiple promised goods or services, the Company applies judgment to determine whether promised goods or services are capable of being distinct and distinct in the context of the contract. If these criteria are not met the promised goods or services are accounted for as a combined performance obligation.

- **Determination of the transaction price**—The transaction price is determined based on the consideration to which the Company will be entitled in exchange for transferring goods or services to the customer.

- **Allocation of the transaction price to the performance obligations in the contract**—The Company allocates the transaction price to each performance obligation based on the amount of consideration expected to be received in exchange for transferring goods and services to the customer. If the contract contains a single performance obligation, the entire transaction price is allocated to the single performance obligation. Contracts that contain multiple performance obligations require an allocation of the transaction price to each performance obligation based on a relative SSP ("Standalone Selling Price") basis. However, these types of arrangements are infrequent as most of the Company's arrangements comprise a single performance obligation. The Company determines standalone selling price taking into account available information such as historical selling prices of the performance obligation, geographic location, overall strategic pricing objective, market conditions and approved pricing guidelines related to the performance obligations.

- **Recognition of revenue when, or as, the Company satisfies performance obligations**—The Company satisfies performance obligations either over time or at a point in time as discussed in further detail below. Revenue is recognized at or over the time the related performance obligation is satisfied by transferring a promised good or service to a customer. The Company generates revenue from the sales of product, cloud-based subscriptions, support and maintenance, and other services, primarily through the indirect relationships with partners or direct relationships with end customers through the direct sales force. The Company accounts for the contracts with customers in accordance with Accounting Standards Update (ASU) 2014-09, Revenue from Contracts with Customers, regarding Accounting Standards Codification Topic 606 ("ASC 606"), and all related interpretations.

Revenue from subscriptions to the cloud-based solutions, which allow customers to use the hosted security software over a contracted period without taking possession of the software and managed services where the Company provides managed detection and response services for customers, are recognized over the contractual term. The Company’s software offering is marketed, sold, and monitored as a single integrated cybersecurity solution, including software, compute hosting for analytics and sensors which may include hardware, intelligence feeds, and support services. This suite of products and services is a single overall cybersecurity solution that represents one performance obligation.

Professional services, which include incident response, security assessments, and other strategic security consulting services are offered on a time-and-materials basis or through fixed fee arrangements, and the Company recognizes the associated revenue as the services are delivered.

**Software Development Costs**
The Company’s software platform, which has been developed internally, can be provided to customers by utilizing either a software or cloud platform, in which the customer can access the product via the cloud, or software can be downloaded into the customer’s environment and may be supported by hardware. In this case, although customers have the ability to download the software into their own environment for purposes of detecting and defending against threats, the customer can benefit from the possession of the software and run it independently without significant penalty. For that reason, the costs related to the development of the Company’s software products and any specifically identifiable upgrades or enhancements qualify for accounting under ASC 350-40 Intangibles - Goodwill and Other - Internal-Use Software. There is no other software developed internally for the purpose of selling or marketing externally that does not require the Company's ongoing involvement.

The Company capitalizes qualifying internal-use software development costs incurred during the application development stage for internal tools and cloud-based applications used to deliver its services, provided that management with the relevant authority authorizes and commits to the funding of the project, it is probable the project will be completed, and the software will be used to perform the function intended. Costs related to preliminary project activities and post implementation activities are expensed as incurred. Capitalized internal-use software development costs are included in property and equipment and are amortized on a straight-line basis over their estimated useful life once it is ready for its intended use, which has been identified as 3 years for the Company's software products. Amortization of capitalized internal-use software development costs is included within general and administrative expense. As of January 31, 2023 and January 31, 2022, capitalized costs were $5,171, before $1,855 of amortized cost and $2,795, before $86 of amortized cost, respectively.

**Research and Development**
Research and development costs are expensed in the year incurred and relate to new product developments and new features and are primarily personnel related costs and acquired software costs. These costs totaled $32,426 and $22,899 for the fiscal years ended January 31, 2023 and 2022, respectively.

**Advertising**
The Company expenses advertising costs as incurred. Advertising costs were $138 and $1,789 for the fiscal years ended January 31, 2023 and 2022, respectively and are included in the sales and marketing expenses.

**Income Taxes**
Income taxes are accounted for under the asset and liability method. Deferred tax assets and liabilities are recognized for the future tax consequences attributable to differences between the financial statement carrying amount of existing assets and liabilities and their respective tax bases. Deferred tax assets and liabilities are measured using enacted tax rates expected to apply to taxable income in the years in which those temporary differences are expected to be recovered or settled. The effect on deferred tax assets and liabilities of a change in tax rates is recognized in income in the period that includes the enactment date.

The Company is subject to income taxes in U.S. federal jurisdictions and various state jurisdictions. Tax regulations within each jurisdiction are subject to interpretation of the related tax laws and regulations and require significant judgment to apply. The Company recognizes tax liabilities for uncertain tax positions when it is more likely than not that a tax position will not be sustained upon examination and settlement with various taxing authorities. Liabilities for uncertain tax positions are measured based upon the largest amount of benefit that is greater than 50% likely of being realized upon settlement. The guidance on accounting for uncertainty in income taxes also addresses de-recognition, classification, interest and penalties on income taxes, and accounting in interim periods. Management has evaluated the Company’s tax positions and has concluded that the Company has taken no uncertain tax positions that require adjustment to the financial statements.
Fair Value of Financial Instruments

A financial instrument’s categorization within the fair value hierarchy is based upon the lowest level of input that is significant to the fair value measurement. The inputs are prioritized into three levels that may be used to measure fair value:

Level 1: Inputs that reflect quoted prices for identical assets or liabilities in active markets that are observable.

Level 2: Inputs that reflect quoted prices for similar assets or liabilities in active markets; quoted prices for identical or similar assets or liabilities in markets that are not active; or model-derived valuations in which significant inputs are observable or can be derived principally from, or corroborated by, observable market data.

Level 3: Inputs that are unobservable to the extent that observable inputs are not available for the asset or liability at the measurement date.

Warrant Liabilities

Simultaneously with the closing of Legacy LGL’s Initial Public Offering, LGL Systems Acquisition Holding Company, LLC, a Delaware limited liability company purchased an aggregate of 5,200 Private Warrants at a price of $1.00 per Private Warrant, for an aggregate purchase price of $5.2 million from Legacy LGL in a private placement that occurred simultaneously with the completion of the Public Offering. Each Private Warrant entitles the holder to purchase one share of common stock at $11.50 per share. The purchase price of the Private Warrants was added to the proceeds from the Public Offering and was held in the Trust Account until the closing of the Merger. The Private Warrants (including the shares of common stock issuable upon exercise of the Private Warrants) were not transferable, assignable or salable until 30 days after the closing date of the Merger, and they may be exercised on a cashless basis and are non-redeemable so long as they are held by the initial purchasers of the Private Warrants or their permitted transferees.

The Company evaluated the warrants issued by Legacy LGL, the legal predecessor, to purchase its common stock in a private placement concurrently with its initial public offering (the “Private Warrants”) under ASC 815-40, Derivatives and Hedging—Contracts in Entity’s Own Equity, and concluded that they do not meet the criteria to be classified in stockholders’ equity. Specifically, the provisions in the Private Warrant agreement provide for potential changes to the settlement amounts dependent upon the characteristics of the warrant holder and the holder of a warrant is not an input into the pricing of a fixed-for-fixed option on equity shares, such a provision would preclude the warrant from being classified in equity. Since the Private Warrants meet the definition of a derivative under ASC 815, the Company recorded these Private Warrants as liabilities on their balance sheet at fair value, with subsequent changes in their respective fair values recognized in the consolidated statement of operations at each reporting date. The fair value adjustments were determined by using the listed price of Public Warrants, which are similar instruments with a quoted price in an active market. The Private Warrants are deemed equity instruments for income tax purposes, and accordingly, there is no tax accounting related to changes in the fair value of the Private Warrants recognized.

Between September 2021 and October 2021, when the majority of these warrants were exercised on a cashless basis, the formula for such exercises made each Private Warrant effectively exercisable to purchase approximately 0.66 shares of Company common stock on a non-cash basis, each subject to its own exercise calculation applicable to the day on which the exercise was made. The Private Warrants were also redeemable in cash for $11.50 for a share of common stock. No Private Warrants were redeemed on the $11.50 cash basis. A total of 5,390 Private Warrants were exercised on a cashless basis into 3,188 shares of Class A common stock. No Private Warrants were exercised on a cashless basis during the fiscal year ended January 31, 2023. As of January 31, 2023 and January 31, 2022, the Company had 10 Private Warrants outstanding and not exercised. During the fiscal year ended January 31, 2023, the Company recognized non-cash income of $6 related to change in fair value of warrants in the consolidated statements of operations. During the fiscal year ended January 31, 2022, the Company recognized $11,265 of non-cash expense related to change in fair value of warrants in the consolidated statements of operations.

Embedded Conversion Features

The Company evaluates embedded conversion features within convertible debt under ASC 815 - Derivatives and Hedging to determine whether the embedded conversion feature(s) should be bifurcated from the host instrument and accounted for as a derivative at fair value with changes in fair value recorded in earnings. If the conversion feature does not require derivative treatment under ASC 815, the instrument is evaluated under ASC 470-20 - Debt with Conversion and Other Options for consideration of any beneficial conversion features.

Stock-based Compensation

The Company recognizes expense for stock-based compensation awards based on the estimated fair value of the award on the date of grant. For stock options, this will be amortized on a straight-line basis over the employee’s or director’s requisite service period, which is generally the vesting period of the award. For RSU awards with both service and performance conditions, stock-based compensation expense is recognized on a graded basis matched to the length of time and vesting tranches of each grant. For RSU awards with only service conditions, stock-based compensation expense will be recognized on a straight-line basis over the employee’s or director’s requisite service period, which is generally the vesting period of the award.

The fair value of stock options is estimated at the date of grant using the Black-Scholes option pricing model. The use of a valuation model requires management to make certain assumptions with respect to the expected life and stock price volatility. The expected life represents the average period the options are expected to be outstanding and is based on historical data and adjusted for the effects of any unexercised and expected to become unexercised options. The expected volatility is based on historical volatility of a company with similar business models. The risk-free interest rate is based on U.S. Treasury zero-coupon yields with a remaining term equal to the expected life assumed at the date of grant. The dividend yield percentage is zero, as the Company does not currently pay dividends nor does the Company intend to do so in the future.

Prior to the Merger, the fair value of each stock RSU was estimated on the grant date using the Black-Scholes pricing model based on the same assumptions utilized for calculating fair market value of the stock options and utilizing the as-converted equivalent price of securities issued during the period. In addition to any time or performance-based vesting conditions, the RSU awards granted by the Company prior to the Merger contained an additional vesting requirement that required the occurrence of a liquidity event. As of the closing of the Merger, which represented the satisfaction of the liquidity event vesting requirement for outstanding RSUs, all RSUs issued prior to the completion of the Merger were revalued using the closing share price on that date. In the event that a RSU grant holder is terminated before the award is fully vested, the full amount of the unvested portion of the award will be recognized as a forfeiture in the period of termination.

Common Stock

The Company has 500,000 shares of voting common stock authorized for issuance. As of January 31, 2023, a total of 110,716 shares of common stock were issued and outstanding, with 4,361 shares reserved for issuance upon the settlement of outstanding RSUs, 530 shares reserved for issuance upon exercise of outstanding stock options, 9,436 shares available for grant under the 2021 Equity Incentive Plan, 8,596 shares reserved for issuance upon the exercise of Public Warrants and 10 shares reserved for issuance upon the exercise of Private Warrants.

Recently Issued Accounting Standards

60
The Company is an emerging growth company ("EGC"), as defined in the JOBS Act. Under the JOBS Act, EGCs can delay adopting new or revised accounting standards issued subsequent to the enactment of the JOBS Act until those standards apply to private companies. The Company has elected to use this extended transition period for complying with certain new or revised accounting standards that have different effective dates for public and private companies until the earlier of the date the Company (i) is no longer an EGC or (ii) affirmatively and irrevocably opt out of the extended transition period provided in the JOBS Act. As a result, the consolidated financial statements may or may not be comparable to companies that comply with new or revised accounting pronouncements as of public companies’ effective dates.

New Accounting Pronouncements Adopted in Fiscal Year 2023

In February 2016, the Financial Accounting Standards Board ("FASB") issued Accounting Standards Update ("ASU") 2016-02, Leases (Topic 842) ("Topic 842"), which outlines a comprehensive lease accounting model that supersedes the previous lease guidance. The guidance requires lessors to recognize lease liabilities and corresponding right-of-use assets for all leases with lease terms greater than 12 months. It also changes the definition of a lease and expands the disclosure requirements of lease arrangements. In July 2018, the FASB issued ASU 2018-11, Leases (Topic 842) - Targeted Improvements, which provides the option of an additional transition method that allows entities to initially apply the new lease guidance at the adoption date and recognize a cumulative-effect adjustment to the opening balance of retained earnings in the period of adoption. The Company adopted the standard on February 1, 2022 using the modified retrospective basis. Using the modified retrospective approach, the Company determined an incremental borrowing rate at the date of adoption based on the total lease term and total minimum rental payments.

The modified retrospective approach provides a method for recording existing leases at adoption with a cumulative adjustment to retained earnings. The Company elected the package of practical expedients which permits the Company to not reassess (1) whether any expired or existing contracts are or contain leases, (2) the lease classification for any expired or existing leases, and (3) any initial direct costs for any expired or existing leases as of the effective date. The Company also elected the practical expedient to use hindsight when determining the lease term, and the practical expedient lease considerations to not allocate lease considerations between lease and non-lease components for real estate leases. As such, real estate lease considerations are treated as a single lease-component and accounted for accordingly. The Company excludes leases with an initial term of 12 months or less from the application of Topic 842.

Adoption of the new standard resulted in the recording of $974 and $2,654 of current operating lease liabilities and long-term operating lease liabilities, respectively, and $2,685 in corresponding right-of-use ("ROU") lease assets on that date. The difference between the approximate value of the ROU lease assets and lease liabilities is attributable to deferred rent, which is comprised of tenant improvement allowance and rent abatement. There was no material impact on the Company’s consolidated statement of operations or consolidated statement of cash flows as a result of the adoption of Topic 842. The Company’s comparative periods continue to be presented and disclosed in accordance with legacy guidance in Topic 840. Refer to Note 11 for additional information.

In August 2020, the FASB issued ASU No. 2020-06, Debt—Debt with Conversion and Other Options (Subtopic 470-20) and Derivatives and Hedging—Contracts in Entity’s Own Equity (Subtopic 815-40): Accounting for Convertible Instruments and Contracts in an Entity’s Own Equity ("ASU 2020-06"), which simplifies accounting for convertible instruments by removing major separation models required under current U.S. GAAP. The ASU also removes certain settlement conditions that are required for equity-linked contracts to qualify for the derivative scope exception, and it simplifies the diluted earnings per share calculation in certain areas. ASU 2020-06 is applicable for fiscal years beginning after December 15, 2023 or the time at which the Company no longer qualifies as an EGC, with early adoption permitted. The Company elected to early adopt this ASU as of February 1, 2022 using the modified retrospective method. The adoption of ASU 2020-06 had an immaterial impact on the Company’s consolidated financial statements and related disclosures for the fiscal year ended January 31, 2023.

Recent Accounting Pronouncements Not Yet Adopted

In June 2016, the FASB issued ASU 2016-13, Measurement of Credit Losses on Financial Instruments (Topic 326). This standard requires a new method for recognizing credit losses that is referred to as the current expected credit loss ("CECL") method. The CECL method requires the recognition of all losses expected over the life of a financial instrument upon origination or purchase of the instrument, unless the Company elects to recognize such instruments at fair value with changes in profit and loss (the fair value option). This standard is effective for the Company for the earlier of the fiscal year beginning after December 15, 2022 or the time at which the Company no longer qualifies as an EGC. As a result, this ASU became effective for the Company as of February 1, 2023. Management does not expect the impact of adopting this standard to be material.

2. Revenue

Product, subscription and support revenue

The Company sells a collective defense software solution that is comprised of two product offerings, IronDefense and IronDome. Through December 2022, the software platform was delivered through both on-premises licenses bundled with on-premises hardware and through subscription software. The Company stopped offering on-premises deployment options in December 2022. During fiscal year 2023, the Company launched IronRadar, a new product intended to broaden the Company’s market reach to companies of all sizes that is delivered via subscription software.

The security appliance deliverables include proprietary operating system software and hardware together with regular threat intelligence updates and support, maintenance, and warranty. The Company combines intelligence dependent hardware and software licenses with the related threat intelligence and support and maintenance as a single performance obligation, as it delivers the essential functionality of the cybersecurity solution. The Company recognizes revenue for this single performance obligation ratably over the expected term. Judgement is required for the assessment of material rights relating to renewal options associated with the Company’s contracts. Revenue from subscriptions, which allow customers to use the Company’s security software over a contracted period without taking possession of the software, and managed services, where the Company provides managed detection and response services for customers, is recognized over the contractual term. The cloud-based subscription revenue, where the Company also provides hosting, recognized for the fiscal year ended January 31, 2023 and 2022 were $21,457 and $13,968, respectively. Overall product, subscription, and support revenue recognized for the years ended January 31, 2023 and 2022 were $25,783 and $25,347, respectively.

Professional services revenue

The Company sells professional services, including cyber operations monitoring, security, training and tailored maturity assessments. Revenue derived from these services is recognized as the services are delivered. Revenue recognized from professional services for the fiscal years ended January 31, 2023 and 2022 was $1,554 and $2,197, respectively.

Customer concentration

For the fiscal year ended January 31, 2023, eight customers accounted for 65%, or $16,536, with two of those customers accounting for 22% of the Company’s revenue, and for the fiscal year ended January 31, 2022, six customers accounted for 51%, or $15,975, with two of those customers accounting for 21%, of the Company’s revenue. As of January 31, 2023, and January 31, 2022, two customers represented 56% and 49% of the total accounts receivable balance, respectively.
Significant customers are those which represent at least 10% of the Company’s total revenue for a fiscal year. The following table presents customers that represent 10% or more of the Company’s total revenue:

<table>
<thead>
<tr>
<th>Customer</th>
<th>Fiscal Year Ended January 31, 2023</th>
<th>Fiscal Year Ended January 31, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10%</td>
<td>11%</td>
</tr>
<tr>
<td>Customer A</td>
<td>12%</td>
<td>10%</td>
</tr>
<tr>
<td>Customer B</td>
<td></td>
<td>21%</td>
</tr>
</tbody>
</table>

Deferred costs
The Company defers contract fulfillment costs that includes appliance hardware. The balances in deferred costs are as follows:

- **Balance at February 1, 2021**: $2,805
- **Amounts recognized in cost of revenue**: (2,095)
- **Costs deferred**: 3,899
- **Foreign exchange**: (3)

**Total: $4,606**

- **Balance at January 31, 2022**: $4,604
- **Amounts recognized in cost of revenue**: (2,608)
- **Costs deferred**: 2,366

**Total: $4,362**

Deferred revenue
Deferred revenue represents amounts received from and/or billed to customers in excess of revenue recognized. Amounts that have been invoiced are recorded in accounts receivable and in deferred revenue or revenue depending on whether the revenue recognition criteria have been met. During the fiscal years ended January 31, 2023 and January 31, 2022, the Company recognized revenue of $14,405 and $12,509, respectively, which was included in the deferred revenue balance at the beginning of each of the respective periods.

Remaining performance obligations
As of January 31, 2023, the remaining performance obligations totaled $42,982. The Company’s recognition of revenue in the future thereon will be in:

<table>
<thead>
<tr>
<th>Years Ending January 31</th>
<th>2024</th>
<th>2025</th>
<th>2026</th>
<th>2027</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$25,050</td>
<td>13,576</td>
<td>3,817</td>
<td>539</td>
</tr>
<tr>
<td></td>
<td>$42,982</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reverse Recapitalization and Restructuring

**Reverse Recapitalization**
As discussed in Note 1, the Company completed the Merger on August 26, 2021. Pursuant to the terms of the Merger Agreement, Merger Sub was merged with and into Legacy IronNet, with Legacy IronNet surviving the Merger as a wholly-owned subsidiary of Legacy LGL.

The following table reconciles the elements of the Merger to the consolidated statement of cash flows for the fiscal year ended January 31, 2022:

<table>
<thead>
<tr>
<th>Recapitalization and Associated Transactions</th>
<th>$173,015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash (Trust)</td>
<td>173,015</td>
</tr>
<tr>
<td>Redemption</td>
<td>(159,763)</td>
</tr>
<tr>
<td>Less: fees to underwriters and advisors</td>
<td>(9,038)</td>
</tr>
<tr>
<td>Net cash received from Merger recapitalization</td>
<td>4,214</td>
</tr>
<tr>
<td>Issuance of PIPE Shares</td>
<td>125,000</td>
</tr>
<tr>
<td>Less: PIPE fees to underwriters and advisors</td>
<td>(21,179)</td>
</tr>
<tr>
<td>Net cash received from PIPE Shares and Merger recapitalization</td>
<td>103,821</td>
</tr>
<tr>
<td>Less: debt settlement</td>
<td>(21,266)</td>
</tr>
<tr>
<td>Net proceeds from Merger recapitalization, PIPE Shares and debt settlement</td>
<td>82,555</td>
</tr>
</tbody>
</table>
The number of outstanding shares of common stock of the Company as of January 31, 2022 is summarized as follows:

<table>
<thead>
<tr>
<th>Shares by Type</th>
<th>Number of Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>IronNet Class A Common Stock outstanding previous to the Merger</td>
<td>67,502</td>
</tr>
<tr>
<td>Issuance of common stock (exercise of ISOs and warrant)</td>
<td>29</td>
</tr>
<tr>
<td>Number of Shares issued at the date of the business combination (Recapitalization)</td>
<td></td>
</tr>
<tr>
<td>LGL Class A Common Stock outstanding previous to the Merger</td>
<td>17,259</td>
</tr>
<tr>
<td>Less: Redemption of LGL Class A previous to the Merger</td>
<td>(15,929)</td>
</tr>
<tr>
<td>Total Class A Shares issued to former LGL shareholders</td>
<td>1,321</td>
</tr>
<tr>
<td>LGL Founders Shares</td>
<td>3,234</td>
</tr>
<tr>
<td>PIPE Shares</td>
<td>12,500</td>
</tr>
<tr>
<td>Number of Shares issued at the Merger</td>
<td>17,075</td>
</tr>
<tr>
<td>Number of Shares issued (redeemed) following the consummation of the Merger</td>
<td></td>
</tr>
<tr>
<td>Earnout Shares</td>
<td>1,078</td>
</tr>
<tr>
<td>Private Warrants (Exercised)</td>
<td>3,188</td>
</tr>
<tr>
<td>Public Warrants (Exercised)</td>
<td>29</td>
</tr>
<tr>
<td>Exercise of ISOs</td>
<td>158</td>
</tr>
<tr>
<td>Payments on subscription notes receivable</td>
<td>(55)</td>
</tr>
<tr>
<td>Shares repurchased related to loan pay-off</td>
<td>(108)</td>
</tr>
<tr>
<td>Total Shares of Common Stock as of January 31, 2022</td>
<td>88,876</td>
</tr>
</tbody>
</table>

In connection with the closing of and as a result of the consummation of the Merger, certain members of the Company’s management and employees received bonus payments in the aggregate amount of $515. The bonuses have been reflected in general and administrative expenses in the consolidated statements of operations.

The Company incurred transaction costs in connection with the Merger. The transaction costs considered incremental have been expensed as incurred and these amounts, $2,328 for the fiscal year ended January 31, 2022, are included in general and administrative expenses in the accompanying consolidated statements of operations. On August 26, 2021, the Company received $15,251 held in Legacy LGL’s trust account, net of redemptions. Transaction costs related to the issuance of the trust shares were $9,038, which were recorded in additional paid in capital on the consolidated balance sheet.

The following activity occurred in connection with the consummation of the Merger:

**IronNet Class A Common Stock (Legacy IronNet Founders Shares) and Preferred Shares**

Pursuant to the Merger Agreement, at the effective time of the Merger, each outstanding share of Legacy IronNet preferred shares and common stock was converted into Class A common stock in the Combined company based on the Exchange Ratio established as part of the Merger, with each preferred share treated as if it were converted into ten shares of Legacy IronNet common stock on the effective date of the Merger. The Exchange Ratio was 0.8141070 of a share of Company common stock per fully-diluted share of Legacy IronNet common stock.

**PIPE Shares**

On August 26, 2021, a number of purchasers (each, a “Subscriber”) purchased from the Company an aggregate of 12,500 shares of Company common stock (the “PIPE Shares”), for a purchase price of $10.00 per share and an aggregate purchase price of $125,000, pursuant to separate subscription agreements entered into effective as of March 15, 2021 (each, a “Subscription Agreement”). Pursuant to the Subscription Agreements, the Company granted certain registration rights to the Subscribers with respect to the PIPE Shares. The sale of the PIPE Shares was consummated concurrently with the closing of the Merger in an amount of $125,000. Transaction costs related with the issuance were $21,179, which were recorded in the consolidated statement of cash flows as a financing activity.

**Founders Shares**

Reflects 3,234 shares of Class A common stock (the “Founder Shares”) for an aggregate purchase price of $24, or approximately $0.007 per share.

**Debt Settlements**

**Loan and Security Agreement**

On June 21, 2021, Legacy IronNet entered into a Loan and Security Agreement (“Term Loan” or “SVB Bridge”) with SVB Innovation Credit Fund VIII, L.P. for term loan advances of up to $15,000 to provide for working capital needs over the period leading up to completion of the combination with Legacy LGL. The Term Loan was able to be prepaid at any time and had a term for up to six months, or until the date on which Legacy IronNet completed its combination with Legacy LGL, whichever came sooner, and bore monthly interest at a per annum rate equal to eight percent, as well as customary fees for de-SPAC bridge loans of this nature. As of August 26, 2021, in conjunction with the Merger, the Company repaid the term loan principal and accrued interest in an aggregate amount of $15,609.

**PPP loan**

On April 21, 2020, Legacy IronNet entered into a Paycheck Protection Program (“PPP”) loan from the US Small Business Administration pursuant to the provisions of the Coronavirus Aid, Relief and Economic Security (“CARES”) Act, receiving loan funds of $5,550. The loan bore interest at 1% and was payable in monthly installments beginning on September 15, 2021. The unsecured loan was evidenced by a promissory note of the Company with PNC Bank (the “Lender”). On August 26, 2021, in conjunction with the Merger, the Company repaid in full all amounts due and terminated all commitments and obligations under the unsecured PPP loan.

**Loans to Employees**

On December 29, 2018, Legacy IronNet entered into a loan with a former executive of the Company with a principal balance of $1,000 bearing an interest rate of 2.76% for a term of three years, which was secured by a pledge of certain shares of Legacy IronNet Class A common stock. As of August 26, 2021, in conjunction with the merger, the Company resolved the loan by having the executive surrender to the Company 108 shares that would have otherwise been issuable to the executive in the Merger.

**Earnout Agreement**

Pursuant to the terms of the Merger Agreement, Eligible Legacy IronNet Equity holders (as defined in the Merger Agreement) had the right to receive up to 1,078 shares (the “Earnout Shares”), to be issued at any time during the two years after of the Closing Date following the occurrence of the triggering event, which is “…the date, occurring after the Closing Date and on or prior to the second anniversary of the Closing Date, on which the volume-weighted average closing sale price of one share of IronNet Stock quoted on the New York Stock Exchange”.

63
(or such other principal securities exchange or securities market on which the shares of Acquiror Stock are then listed) is equal to or greater than $13.00 for any ten (10) consecutive Trading Days occurring after the Closing Date.”

As of the close of trading on September 10, 2021, the requisite conditions of the earnout triggering event were satisfied and the Company issued 1,078 Earnout Shares to the Eligible Legacy IronNet Equity holders.

Legacy IronNet Restricted Stock Units and Stock Options

Pursuant to the terms of the Merger Agreement, each Legacy IronNet RSU and stock option outstanding immediately prior to the closing of the Merger, and which based on their terms did not terminate upon the closing of the Merger, remained outstanding. In the case of Legacy IronNet stock options, they were converted based on the number of shares of Legacy IronNet common stock subject to that option, multiplied by the Exchange Ratio, at an exercise price per share equal to the current exercise price per share for that option, divided by the Exchange Ratio. In the case of Legacy IronNet RSUs, they were converted based on the number of shares of Company common stock equal to the number of shares of Legacy IronNet common stock subject to that award, multiplied by the Exchange Ratio.

Under the terms of Legacy IronNet’s 2014 Stock Incentive Plan, the vesting of each RSU award was subject to, among other conditions, including a service requirement, the occurrence of a liquidity event, as defined by the Plan. On August 26, 2021, in connection with the close of the Merger with Legacy LGL, the Company’s Board of Directors resolved to deem the Merger as satisfying the Liquidity Event condition. The resolution resulted in a modification of the RSUs under ASC 718 “Compensation—Stock Compensation.” As a consequence of modification of the awards outstanding, the Company recognized a non-cash expense in an amount of $169,360 during fiscal year 2022 related to 15,780 RSUs that remained outstanding as of January 31, 2022 under the 2014 Plan.

Restructuring

Between September 2022 and November 2022, the Company undertook a restructuring to reduce headcount by approximately 44%, which resulted in a reduction of approximately 111 positions. In connection with this action, the Company recorded total pre-tax charges of $513,439 for the fiscal year ended January 31, 2023, which includes $659 related to one-time severance payments, which were paid in cash during the third quarter as well as non-cash stock-based compensation expense of $12,780. This amount is comprised of $13,266 of non-cash accelerated vesting of restricted stock units, offset by forfeitures of $486.

4. Property and Equipment

Property and equipment consist of the following at January 31:

<table>
<thead>
<tr>
<th></th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer and other equipment</td>
<td>$4,900</td>
<td>$5,369</td>
</tr>
<tr>
<td>Leasehold improvements</td>
<td>1,416</td>
<td>1,416</td>
</tr>
<tr>
<td>Furniture and fixtures</td>
<td>388</td>
<td>388</td>
</tr>
<tr>
<td>Software</td>
<td>5,171</td>
<td>2,795</td>
</tr>
<tr>
<td>ROU asset</td>
<td>297</td>
<td></td>
</tr>
<tr>
<td><strong>Less: Accumulated depreciation and amortization</strong></td>
<td>(6,200)</td>
<td>(4,362)</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>5,972</td>
<td>5,806</td>
</tr>
</tbody>
</table>

Depreciation and amortization expense on property and equipment was $2,336 and $1,092 for the years ended January 31, 2023 and January 31, 2022, respectively.

5. Stock Incentive Plans

Legacy IronNet’s Board of Directors adopted, and its stockholders approved Legacy IronNet’s 2014 Stock Incentive Plan (the “2014 Plan”) on September 29, 2014, and on October 17, 2014, respectively. The 2014 Plan was periodically amended, most recently on June 7, 2019. The 2014 Plan permitted the grant of incentive stock options (“ISOs”), non-qualified stock options (“NSOs”), stock appreciation rights, restricted stock, RSUs, and other stock-based awards. ISOs were only able to be granted to Legacy IronNet’s employees and to Legacy IronNet’s subsidiary corporations’ employees. All other awards could be granted to employees, directors and consultants of Legacy IronNet and to any of Legacy IronNet’s parent or subsidiary corporation’s employees or consultants. As of August 26, 2021, the closing date of the Merger, no additional awards will be granted under the 2014 Plan. The terms of the 2014 Plan will continue to govern the terms of outstanding equity awards that were granted prior to the closing date.

On August 26, 2021, per the Merger Agreement, the outstanding Legacy IronNet ISO and RSU grants issued under the 2014 Plan were converted to their post-transaction equivalents based on the conversion ratio, totaling 18,972 shares in the Company when exercised or converted.

The 2021 Equity Incentive Plan (the “2021 Plan”) was approved by Legacy LGL’s board of directors and by its stockholders on August 26, 2021. Under the 2021 Plan, upon its effectiveness, the Company was able to grant ISOs, RSUs and other equity securities to acquire, to convert into, or to receive up to 13,500 shares of common stock. The terms of the 2021 Plan include an evergreen provision that provides for an automatic share increase on February 1 of each year, in an amount equal to 5.0% of the sum of (a) the total number of shares of the Company’s common stock outstanding on January 31 of the immediately preceding fiscal year, plus (b) the number of shares of common stock reserved for issuance under the 2021 Plan as of January 31 of the immediately preceding fiscal year, but which have not yet been issued. In accordance with the evergreen provision, on February 1, 2022, the number of shares that can be issued under the 2021 Plan increased by 4,934 shares, with a new limit following the increase of 18,434 shares.

As of January 31, 2023, 9,436 share equivalents remained available to issue under the 2021 Plan.

Awards under the 2014 Plan and the 2021 Plan (together, the “Stock Incentive Plans”) normally vest over a forty-eight month period, some of which have a first year cliff vest for the first 25% of their vesting, during which time no vesting occurs. In limited cases, vesting as short as twelve months with no cliff, vesting based on performance criteria and acceleration under certain events have also been permitted; however, such exceptions apply to less than 20% of the shares underlying awards currently outstanding under the Stock Incentive Plans.
Stock Options

The exercise price of each stock option granted under the Stock Incentive Plans may not be less than the fair market value per share of the underlying Class A common stock on the date of grant. The Board of Directors establishes the term and the vesting of all options issued under the Stock Incentive Plans; however, in no event will the term exceed ten years.

Presented below is a summary of the status of the stock options under the 2014 Stock Incentive Plan, as no stock options have been granted under the 2021 Plan:

<table>
<thead>
<tr>
<th>Option Type</th>
<th>Outstanding at January 31, 2022</th>
<th>Number of Shares</th>
<th>Weighted Average Exercise Price</th>
<th>Weighted Average Remaining Contractual Term (Years)</th>
<th>Intrinsic Value of Outstanding Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vested</td>
<td></td>
<td>530</td>
<td>0.56</td>
<td>3.8</td>
<td>$ 772</td>
</tr>
<tr>
<td>Exercisable at January 31, 2023</td>
<td></td>
<td>530</td>
<td>0.56</td>
<td>3.8</td>
<td>$ 772</td>
</tr>
<tr>
<td>Non-vested at January 31, 2022</td>
<td></td>
<td>10,310</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For the fiscal years ended January 31, 2023 and 2022, the Company recorded insignificant amounts of compensation cost related to stock options. The fair value of shares under stock options granted that vested were $2 and $2,062 for the fiscal years ended January 31, 2023 and 2022, respectively.

Stock compensation expense for stock options is recognized on a straight-line basis and with a provision for forfeitures matched to historical experience for matured grant cohorts. At January 31, 2023, there was no unrecognized compensation cost related to unvested stock options. All stock options were vested as of January 31, 2023.

The Company uses the Black-Scholes option pricing model to estimate the fair value of options granted. The Black-Scholes model takes into account the fair value of an ordinary share and the contractual term and expected volatility of the option, expected volatility, dividend yield, and risk-free interest rate. Prior to becoming a public company, the fair value of the Company’s common stock was determined utilizing an external third-party pricing specialist.

The contractual term of the option ranges from the one to ten years. Expected volatility is the average volatility over the expected terms of comparable public entities from the same or similar industry as a substitute for the historical volatility of the Company’s common shares, which is not determinable without an active external or internal market. The risk-free interest rate for periods within the expected life of the option is based on the U.S. Treasury yield curve in effect at the time of grant. The Company has not historically distributed dividends and does not expect to distribute any dividends.

Restricted Stock Units

In addition to the applicable time or performance-based vesting criteria, the RSUs granted under the 2014 Plan contained an additional vesting requirement that required the occurrence of a liquidity event. On August 26, 2021, the date of the Merger, the Board of Directors resolved that the Merger constituted a liquidity event, which triggered the liquidity event criteria for vesting under then outstanding RSU awards.

As the closing of the Merger represented the satisfaction of the liquidity event vesting requirement for outstanding RSUs, and vesting was not probable until that time, all RSUs issued prior to the completion of the Merger were re-valued at the date of the Merger using the closing share price on that date. All RSUs were assigned a fair value of $12.85 per share. Subsequent to the closing of the Merger, the fair value of RSUs is based on the fair value of the Company’s common stock on the date of the grant or any further modification.

Presented below is a summary of the status of outstanding RSUs:

<table>
<thead>
<tr>
<th>RSU Status</th>
<th>Number of Shares</th>
<th>Weighted Average Grant Date Fair Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-vested at February 1, 2021</td>
<td>9,712</td>
<td>$ 11.75</td>
</tr>
<tr>
<td>Granted</td>
<td>5,900</td>
<td>$ 8.20</td>
</tr>
<tr>
<td>Vested</td>
<td>(3,818)</td>
<td>$ 12.01</td>
</tr>
<tr>
<td>Non-vested at January 31, 2022</td>
<td>10,310</td>
<td>$ 9.57</td>
</tr>
<tr>
<td>Non-vested at February 1, 2022</td>
<td>10,310</td>
<td>$ 9.57</td>
</tr>
<tr>
<td>Granted</td>
<td>(8,982)</td>
<td>$ 3.36</td>
</tr>
<tr>
<td>Non-vested at January 31, 2023</td>
<td>4,361</td>
<td>$ 6.76</td>
</tr>
</tbody>
</table>

As of January 31, 2023, there are 23,151 RSUs outstanding, which is comprised of 8,998 RSUs with only service conditions, 1,302 RSUs with only performance conditions, and 12,851 RSUs with both service conditions and performance conditions. Of the outstanding RSUs, 652 shares with only performance conditions have vested, 5,492 RSUs with only service conditions have vested, and 12,646 RSUs with both service conditions and performance conditions have vested as of January 31, 2023.

Stock compensation expense for RSUs granted under the 2014 Plan, which contain both service and performance conditions, is recognized on a graded-scale basis, recognizing expense over the respective vesting period for each tranche of shares under each award granted. Stock compensation expense for RSUs granted under the 2021 Plan have only service vesting conditions and expense will be recognized on a straight-line basis for all RSU awards with only service conditions. In the event that an RSU holder is terminated before the award is fully vested for RSUs granted under either Plan, the full amount of the unvested portion of the award will be recognized as a forfeiture in the period of
term. For the fiscal year ended January 31, 2023, the Company recorded $36,858 of stock-based compensation expense, net of actual forfeitures, related to RSUs, of which $15,011 is associated with RSUs on a graded vesting schedule and $21,847 is associated with RSUs on a straight-line vesting schedule. For the fiscal year ended January 31, 2022, the Company recorded $156,560 of stock-based compensation expense, net of actual forfeitures, related to RSUs, of which $155,518 is associated with RSUs on a graded vesting schedule and $1,042 is associated with RSUs on a straight-line vesting schedule.

The Company's default tax withholding method for RSUs is the sell-to-cover method, under which shares with a market value equivalent to the tax withholding obligation are sold on behalf of the holder of the RSUs upon vesting and settlement to cover the tax withholding liability and the cash proceeds from such sales are then remitted by the Company to taxing authorities. Refer to Note 9 for additional information.

As of January 31, 2023, there was approximately $12,688 of unrecognized compensation cost related to unvested RSUs without performance obligations. The weighted-average remaining vesting period was 2.63 years.

Employee Stock Purchase Plan ("ESPP")

In August 2021, Legacy LGL's Board of Directors adopted, and its stockholders approved, the ESPP. The ESPP became effective immediately upon the Closing of the Merger.

The purpose of the ESPP is to provide a means by which eligible employees and certain designated companies may be given an opportunity to purchase shares of the Company's common stock, to assist in retaining the services of eligible employees, to secure and retain the services of new employees and to provide incentives for such persons to exert maximum efforts for the Company's success.

The Plan includes two components: a 423 Component and a Non-423 Component. The Company intends that the 423 Component will qualify as options issued under an "employee stock purchase plan" as that term is defined in Section 423(b) of the Code. Except as otherwise provided in the ESPP or determined by the Board of Directors, the Non-423 Component will operate and be administered in the same manner as the 423 Component.

The ESPP contains an evergreen provision that provides for an automatic annual share increase on February 1 of each year, in an amount equal to the lesser of (i) 1% of the total number of shares of common stock outstanding on January 31st of the preceding fiscal year, and (ii) 2,709 shares of Common Stock. In accordance with the evergreen provision, the number of shares of common stock reserved for issuance under the ESPP increased by 889 shares on February 1, 2022. Inclusive of the prior limit of 2,700 shares, the new limit following the increase was 3,589 shares.

As of January 31, 2023, there were no purchases of shares for an eligible employee.

6. Stockholders' Equity

Common Stock

As of January 31, 2023, the Company had 500,000 shares of Class A common stock authorized and 110,716 shares of common stock issued and outstanding at $0.0001 par value per share.

As of January 31, 2022, the Company had 500,000 shares of Class A common stock authorized and 88,876 shares of common stock issued and outstanding at $0.0001 par value per share.

Each share of Common Stock has 1 vote.

Tumim Common Stock Purchase Agreement

On February 11, 2022, the Company entered into a Common Stock Purchase Agreement (the “Purchase Agreement”) with Tumim, pursuant to which Tumim has committed to purchase up to $175,000 of common stock (the “Total Commitment”), at the Company's direction from time to time, subject to the satisfaction of the conditions in the Purchase Agreement. Also on February 11, 2022, the Company entered into a registration rights agreement with Tumim (the “Registration Rights Agreement”), pursuant to which the Company filed with the SEC a registration statement to register for resale under the Securities Act (the “ELOC Registration Statement”), the shares of common stock that may be issued to Tumim under the Purchase Agreement. The SEC declared the ELOC Registration Statement effective on March 17, 2022.

The sales of common stock to Tumim under the Purchase Agreement, if any, are subject to certain limitations and may occur, from time to time at the Company's sole discretion, over the approximately 36-month period commencing upon the initial satisfaction of all conditions to Tumim’s purchase obligations set forth in the Purchase Agreement (the “Commencement Date”).

From and after the Commencement Date, the Company has the right, but not the obligation from time to time to direct Tumim to purchase amounts of common stock, subject to certain limitations in the Purchase Agreement, specified in purchase notices that will be delivered to Tumim under the Purchase Agreement (each such purchase, a “Purchase”). Shares of common stock will be issued from the Company to Tumim at either (i) 3% discount to the average daily volume weighted average price (the “VWAP”) of the common stock during the three consecutive trading days from the date that a purchase notice with respect to a particular purchase (“VWAP Purchase Notice”) is delivered from the Company to Tumim (a “Forward VWAP Purchase”), or (ii) 5% discount to the lowest daily VWAP during the three consecutive trading days from the date that a VWAP Purchase Notice with respect to a particular purchase is delivered from the Company to Tumim (an “Alternative VWAP Purchase”). There is no upper limit on the price per share that Tumim could be obligated to pay for the common stock under the Purchase Agreement. The purchase price per share of common stock to be sold in a Purchase will be appropriately adjusted for any reorganization, recapitalization, non-cash dividend, stock split, reverse stock split or other similar transaction.

Pursuant to the terms of the Purchase Agreement, at the time the Purchase Agreement and the Registration Rights Agreement were signed, the Company paid a cash fee of $1,750, or 1% of the Total Commitment, to Tumim as consideration for its commitment to purchase shares of the Company's common stock under the Purchase Agreement. The cash paid related to the Commitment Fee was recorded in the consolidated statement of cash flows as a financing activity. The Commitment Fee qualifies as a derivative asset under ASC 815-40 Derivatives and Hedging --- Contracts in Entity's Own Equity and was established as an asset on the consolidated balance sheet, which will be adjusted-over the period of the agreement to reflect fair value, with changes in fair value being recognized as a component of other expense. The Commitment Fee is measured at fair value categorized within Level 3 of the fair value hierarchy and the value derived was not determined to be material. Changes in fair value of the Commitment Fee during the fiscal year ended January 31, 2023 of $1,555 was recognized in other expense in the consolidated statement of operations. As of January 31, 2023, the fair value of the Commitment Fee on the consolidated balance sheet was $195. The Company also incurred $96 in transaction costs related to the issuance of the Purchase Agreement, which was recognized in other expense on the consolidated statement of operations.

During the fiscal year ended January 31, 2023, the Company sold 2,511 shares to Tumim under the Purchase Agreement for gross proceeds of $586. The Company is not currently able to raise additional funds under the equity line with Tumim.
Preferred Stock

The Company is authorized to issue 100,000 shares of preferred stock with a par value of $0.0001 per share with such designation, rights and preferences as may be determined from time to time by the Company’s board of directors. At January 31, 2023, there were no shares of preferred stock issued or outstanding.

Public Warrants

On November 12, 2019, Legacy LGL sold 17,250 units at a price of $10.00 per unit (the “Units”) in its Initial Public Offering, which included the full exercise by the underwriters of the over-allotment option to purchase an additional 2,250 units. Each Unit consisted of one share of Legacy LGL Class A common stock, par value $0.0001 per share, and one-half of one warrant to purchase one share of Legacy LGL Class A common stock (the “Public Warrants”).

Public Warrants may only be exercised for a whole number of shares at a price of $11.50 per share. No fractional shares will be issued upon exercise of the Public Warrants. The Public Warrants became exercisable in September 2021 and will expire five years after the completion of the Merger or earlier upon redemption or liquidation.

Once the Public Warrants became exercisable upon the effective date of the Company’s S-1 registration statement filed in September 2021, the Company obtained the ability to redeem the Public Warrants:

- in whole and not in part;
- at a price of $0.01 per warrant;
- upon not less than 30 days’ prior written notice of redemption; and
- if, and only if, the reported last sale price of the Company’s common stock equals or exceeds $18.00 per share (as adjusted for stock splits, stock dividends, reorganizations, recapitalizations and the like and subject to adjustment as described below) for any 20 trading days within a 30-trading day period ending on the third business day prior to the notice of redemption to the warrant holders.

If the Company calls the Public Warrants for redemption, management will have the option to require all holders that wish to exercise the Public Warrants to do so on a “cashless basis,” as described in the Warrant Agreement.

As of January 31, 2023, there were 8,596 Public Warrants outstanding and not exercised.

7. Fair Value Measurements

Fair value is defined as the price that would be received to sell an asset in an orderly transaction or paid to settle a liability in an orderly transaction between market participants at the measurement date. Accounting standards utilize a fair value hierarchy that prioritizes the inputs to valuation techniques used to measure fair value into three levels, which are described below:

- Level 1 – Quoted prices (unadjusted) for identical assets or liabilities in active markets.
- Level 2 – Observable inputs other than quoted prices that are either directly or indirectly observable for the asset or liability.
- Level 3 – Unobservable inputs that are supported by little or no market activity.

These levels are not necessarily an indication of the risk of liquidity associated with the financial assets or liabilities disclosed. Assets and liabilities are classified in their entirety based on the lowest level of input that is significant to the fair value measurement, as required under ASC 820-10 “Fair Value Measurement.”

On September 15, 2022, the Company issued the Convertible Note. Pursuant to the terms of the Convertible Note, under certain circumstances the Company may be required to redeem all or a portion of the Convertible Note in cash, as disclosed in Note 12. The convertible feature is measured at fair value categorized within Level 3 of the fair value hierarchy, with the fair value determined to be $103. As of January 31, 2023, the fair value of the convertible feature was $671.

During the fiscal year ended January 31, 2023, the Company issued two secured convertible promissory notes to C5 in the amount of $5,000. These secured convertible promissory notes may require the Company to convert all or a portion of the principal and accrued and unpaid interest into shares of redeemable stock at the option of the holder up to five calendar days prior to maturity, as disclosed in Note 12. The convertible feature is measured at fair value categorized within Level 3 of the fair value hierarchy, with the fair value determined to be $63. The Company determined the fair value of the convertible feature using a Black-Scholes option-pricing model, and the value derived was determined to not be material. There was not determined to be a material change in the fair value of the convertible feature of the secured convertible promissory notes from the date of issuance through January 31, 2023.

As discussed in Note 6, the Company established a derivative asset related to the Commitment Fee incurred when entering into the Securities Purchase Agreement with 3i, which is measured at fair value categorized within Level 3 of the fair value hierarchy, with the value determined to not be material.

The Company’s Private Warrants have terms similar to, and are subject to substantially the same redemption features as, the Public Warrants, as the transfer of a Private Warrant to anyone who is not a permitted transferee would result in the Private Warrant being converted to a Public Warrant. The Company determined that the fair value of each Private Warrant is equivalent to that of a Public Warrant. There have been observable transactions in the Company’s Public Warrants and the Public Warrants had adequate trading volume between independent investors on the public market to provide a reliable indication of value. As of January 31, 2023, the fair value of the Private Warrants was equal to that of the Public Warrants as they had substantially the same terms. However, as they are not actively traded, they are listed as a Level 2 investment in the fair value hierarchy table below.

Investments with an original maturity of three months or less at the date of purchase are considered cash equivalents, while all other investments are classified as short-term or long-term based on their maturities and their availability for use in current operations.

The following table presents assets and liabilities measured at fair value on a recurring basis:

<table>
<thead>
<tr>
<th>Description</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred Stock</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Warrants</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Convertible Note</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Convertible Promissory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commitment Fee</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private Warrants</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
January 31, 2023

<table>
<thead>
<tr>
<th>Assets</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash equivalents</td>
<td>$ 6</td>
<td>—</td>
<td>—</td>
<td>$ 6</td>
</tr>
<tr>
<td>Commitment Fee</td>
<td>$ —</td>
<td>—</td>
<td>195</td>
<td>$ 195</td>
</tr>
<tr>
<td>Total financial assets</td>
<td>$ 6</td>
<td>—</td>
<td>195</td>
<td>$ 201</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Liabilities</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warrants</td>
<td>$ —</td>
<td>—</td>
<td>—</td>
<td>$ 0</td>
</tr>
<tr>
<td>Conversion options</td>
<td>$ —</td>
<td>—</td>
<td>734</td>
<td>$ 734</td>
</tr>
<tr>
<td>Total</td>
<td>$ —</td>
<td>—</td>
<td>734</td>
<td>$ 734</td>
</tr>
</tbody>
</table>

The Company recognized a non-cash income of $6 related to the change in fair value of warrants during the period ended January 31, 2023.

The following table presents a summary of the changes in the fair value of the Company's Level 3 financial instruments:

<table>
<thead>
<tr>
<th>Convertible Notes Derivative Liability</th>
<th>C5 Notes Derivative Liability</th>
<th>Commitment Fee Derivative Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fair Value as of January 31, 2022</td>
<td>$ -</td>
<td>$ -</td>
</tr>
<tr>
<td>Commitment fee derivative asset established at time of Purchase Agreement</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Conversion feature liability established at issuance of Convertible Notes</td>
<td>774</td>
<td>-</td>
</tr>
<tr>
<td>Conversion feature liability established at issuance of C5 Notes</td>
<td>-</td>
<td>63</td>
</tr>
<tr>
<td>Change in fair value</td>
<td>(103)</td>
<td>-</td>
</tr>
<tr>
<td>Fair value as of January 31, 2023</td>
<td>$ 671</td>
<td>$ 63</td>
</tr>
</tbody>
</table>

8. Income Taxes

The components of the provision for income taxes are comprised of the following for the fiscal years ended January 31:

<table>
<thead>
<tr>
<th>Current income taxes</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>$ -</td>
<td>$ -</td>
</tr>
<tr>
<td>State</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>Foreign</td>
<td>48</td>
<td>464</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deferred income taxes</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total income tax expense</td>
<td>$ 58</td>
<td>$ 465</td>
</tr>
</tbody>
</table>

For the years ended January 31, 2023 and 2022, the foreign income (loss) before provision for income tax was $51 and $1,774, respectively. For the years ended January 31, 2023 and 2022, the domestic loss before provision for income tax was ($110,609) and ($243,956), respectively.

Indefinite reinvestment is determined by management's judgment about and intentions concerning the future operations of the Company. As part of its business strategies, the Company has determined that all earnings from foreign continuing operations will be deemed indefinitely reinvested outside of the United States. The Company’s plans to indefinitely reinvest certain earnings are supported by projected working capital and long-term capital requirements in each foreign subsidiary location in which the earnings are generated.

A reconciliation of income tax expense at the U.S. federal statutory income tax rate to annual income tax expense at the Company’s effective tax rate is as follows:

<table>
<thead>
<tr>
<th>Income tax expense computed at U.S. federal statutory income tax rate</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ (23,217)</td>
<td>21.0%</td>
<td>$ (50,575)</td>
</tr>
<tr>
<td>State income taxes</td>
<td>(8,434)</td>
<td>7.63%</td>
</tr>
<tr>
<td>Permanent items</td>
<td>7,623</td>
<td>(6.90)%</td>
</tr>
<tr>
<td>Valuation allowance</td>
<td>36,661</td>
<td>(33.16)%</td>
</tr>
<tr>
<td>Change in State Tax Rate</td>
<td>(12,761)</td>
<td>11.54%</td>
</tr>
<tr>
<td>Other</td>
<td>186</td>
<td>(0.17)%</td>
</tr>
<tr>
<td>Income tax expense computed at U.S. federal statutory income tax rate</td>
<td>$ 58</td>
<td>(0.06)%</td>
</tr>
</tbody>
</table>

Income tax expense was $58 and $465 for the fiscal years ended January 31, 2023 and 2022, respectively. The effective tax rate for the fiscal years ended January 31, 2023 and 2022 was (0.06)% and (0.1)% respectively.

Deferred Income Taxes

Deferred income taxes reflect the net tax effects of temporary differences between the carrying amounts of assets and liabilities and their tax bases, as well as from net operating loss and carryforwards.
Significant components of the Company’s deferred tax assets and (liabilities) are as follows:

<table>
<thead>
<tr>
<th>Deferred tax assets</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net operating loss carryforward</td>
<td>$118,465</td>
<td>$81,955</td>
</tr>
<tr>
<td>Intangible assets</td>
<td>601</td>
<td>610</td>
</tr>
<tr>
<td>Depreciation and amortization</td>
<td>281</td>
<td>118</td>
</tr>
<tr>
<td>RSU Assets</td>
<td>9,766</td>
<td>8,499</td>
</tr>
<tr>
<td>Others</td>
<td>657</td>
<td>285</td>
</tr>
<tr>
<td>Deferred revenue</td>
<td>4,241</td>
<td>5,786</td>
</tr>
<tr>
<td>Lease Liabilities</td>
<td>760</td>
<td>—</td>
</tr>
<tr>
<td>Gross deferred tax assets</td>
<td>132,520</td>
<td>95,533</td>
</tr>
<tr>
<td>Valuation allowance</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

**Deferred tax liabilities**

<table>
<thead>
<tr>
<th>Deferred tax liabilities</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deferred costs</td>
<td>(1,835)</td>
<td>(1,843)</td>
</tr>
<tr>
<td>ROU Assets</td>
<td>(540)</td>
<td>—</td>
</tr>
<tr>
<td>Net deferred tax assets (liabilities)</td>
<td>$—</td>
<td>$—</td>
</tr>
</tbody>
</table>

**Income Tax Valuation Allowance**

The following summarizes changes to valuation and qualifying accounts for fiscal year 2023 and fiscal year 2022:

<table>
<thead>
<tr>
<th>Fiscal Year Ended</th>
<th>Balance at Beginning of Period</th>
<th>Charged to Costs &amp; Expenses</th>
<th>Federal/State NOL</th>
<th>Balance at End of Period</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>January 31, 2023</td>
<td>95,533</td>
<td>476</td>
<td>36,510</td>
</tr>
<tr>
<td></td>
<td>January 31, 2022</td>
<td>41,849</td>
<td>10,662</td>
<td>43,022</td>
</tr>
</tbody>
</table>

As of January 31, 2023 and January 31, 2022, the Company had net operating loss carryforwards (NOLs) available to offset federal taxable income of approximately $413,570 and $324,787, respectively. $25,270 of the federal NOLs expire on various dates through 2037 and $388,500 are able to be carried forward indefinitely to offset 80% of future taxable income. The Company has tax effected state NOL carryforwards of approximately $31,616 as of January 31, 2023 and $31,749 as of January 31, 2022 that expire on various dates through 2037.

In accordance with IRC Section 382, the extent to which net operating loss carryforwards can be used to offset future taxable income may be limited, depending on the extent of any ownership changes as defined by federal and various state and local jurisdictions. These limitations may result in the expiration of net operating loss carry forwards before utilization.

In assessing the realizability of the Company's net deferred tax assets, management considers whether it is more likely than not that some portion or all of the net deferred tax assets will be recognized. The ultimate realization of the net deferred tax assets is dependent upon the generation of taxable income during the periods in which temporary differences become deductible. Management considers taxes paid, if any, scheduled reversal of deferred tax liabilities, projected future taxable income, and tax planning strategies that can be implemented by the Company in making this assessment. Based upon the level of historical taxable income, scheduled reversal of deferred tax liabilities, and projections for taxable income over the periods in which the temporary differences become deductible based on available tax planning strategies, management presently believes it is more likely than not that the Company will not realize all of the benefits of these deductible differences and, accordingly, has established a valuation allowance against the net deferred tax assets at January 31, 2023 and 2022.

The Company recognizes a tax position taken or expected to be taken (and any associated interest and penalties) if it is more likely than not that it will be sustained upon examination, including resolution of any related appeals or litigation processes, based on the technical merits of the position. The Company measures the tax position at the largest amount of benefit that is greater than 50% likely of being realized upon ultimate settlement.

Management evaluated all income tax positions and determined that there were no uncertain tax positions that required reserves as of January 31, 2023 and 2022. The Company files tax returns in the United States federal jurisdiction and in many state jurisdictions. The tax years 2018 through 2023 remain open to examination by the major taxing jurisdictions to which the company is subject. No examinations are currently open.

On March 27, 2020, the Coronavirus Aid, Relief and Economic Security ("CARES") Act was enacted and signed into U.S. law to provide economic relief to individuals and businesses facing economic hardship as a result of the COVID-19 pandemic. Changes in tax laws or rates are accounted for in the period of enactment. The income tax provisions of the CARES Act did not have a significant impact on the Company's current taxes, deferred taxes, or uncertain tax positions.

**Accrued Expenses**

Accrued expenses consisted of the following:

<table>
<thead>
<tr>
<th></th>
<th>January 31, 2023</th>
<th>January 31, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accrued expenses</td>
<td>$976</td>
<td>$2,438</td>
</tr>
<tr>
<td>Taxes payable on behalf of employees related to vested RSUs</td>
<td>6,987</td>
<td>2,271</td>
</tr>
<tr>
<td>Unvouched payables</td>
<td>2,010</td>
<td>2,271</td>
</tr>
<tr>
<td>Total accrued expenses</td>
<td>$10,972</td>
<td>$4,709</td>
</tr>
</tbody>
</table>

The balance in accrued expenses as of January 31, 2023 is primarily comprised of the cash proceeds from the sale of shares on behalf of the holders of vested RSUs to cover the associated tax withholding liability under the self-cover method.

The balance in accrued expenses at January 31, 2022 includes $1,129 in cash received from a customer in January 2022, which was due to be remitted to a third party as a part of a factoring arrangement. This payment was due from the customer directly to the third party, and was remitted to the third party during the first quarter of fiscal year 2023. The balance also includes $722 in sales tax payable, primarily consisting of an accrual for remaining obligations combined with potential interest and penalties related to the results of a sales tax nexus review. The
Company resolved these liabilities with the respective state jurisdictions during the fiscal year ended January 31, 2023.

Prepaid Expenses

The prepaid expenses balances as of January 31, 2023 and 2022 include $909 and $1,803, respectively, related to directors and officers insurance purchased by the Company in August 2021.

Deferred Payroll Taxes

In fiscal year 2021, Legacy IronNet elected to defer the Company’s portion of payroll taxes, as permitted under the CARES Act. 50% of the deferred payroll tax was paid in December 2021, with the remaining 50% paid in December 2022. As of January 31, 2022, the balance was $689 and is included in other current liabilities on the consolidated balance sheet.

10. Commitments and Contingencies

In the ordinary course of business, the Company and its subsidiaries may become defendants in certain shareholder claims and other litigation. The Company records a liability when it is probable that a loss has been incurred and the amount is reasonably estimable. To date, no such liability has been recorded.

11. Leases

The Company leases office space under the terms of noncancelable operating leases that expire at various dates through November 2026. Certain operating lease agreements provide for an annual 2.75% escalation of the base rent. The Company is also responsible for operating expenses, which are classified as variable lease costs. Lease terms may include options to extend or terminate the lease, typically at the Company’s own discretion. Renewal options are regularly evaluated and the renewal period will be included in the lease term when exercise of the renewal option is considered reasonably certain. There are no active leases that have a renewal option that is reasonably certain of being exercised.

The Company holds leases that include both lease (e.g., payments including rent, taxes, and insurance costs) and non-lease components (e.g., common-area or other maintenance costs). As the Company has elected the practical expedient to group lease and non-lease components for all leases, these are accounted for as a single lease component. The Company’s leases do not include any residual value guarantees or material restrictive covenants.

Lease expense for both operating and finance leases is recognized on a straight-line basis over the lease term and is recorded in operating expenses on the consolidated statements of operations. Interest expense incurred on finance lease liabilities is calculated using the effective interest method and is recorded in interest expense on the consolidated statements of operations.

The lease balances are located in the following positions on the consolidated balance sheet.

<table>
<thead>
<tr>
<th>Balance Sheet Location</th>
<th>January 31, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets</td>
<td></td>
</tr>
<tr>
<td>Operating</td>
<td></td>
</tr>
<tr>
<td>Deposits and other assets</td>
<td>$1,885</td>
</tr>
<tr>
<td>Financing</td>
<td></td>
</tr>
<tr>
<td>Property and equipment, net</td>
<td>$205</td>
</tr>
<tr>
<td>Liabilities</td>
<td></td>
</tr>
<tr>
<td>Current</td>
<td></td>
</tr>
<tr>
<td>Operating</td>
<td></td>
</tr>
<tr>
<td>Other current liabilities</td>
<td>$607</td>
</tr>
<tr>
<td>Financing</td>
<td></td>
</tr>
<tr>
<td>Other current liabilities</td>
<td>$130</td>
</tr>
<tr>
<td>Non-current</td>
<td></td>
</tr>
<tr>
<td>Operating</td>
<td></td>
</tr>
<tr>
<td>Other long-term liabilities</td>
<td>$2,047</td>
</tr>
<tr>
<td>Financing</td>
<td></td>
</tr>
<tr>
<td>Other long-term liabilities</td>
<td>$81</td>
</tr>
</tbody>
</table>

Total lease costs for the fiscal year ended January 31, 2023 were:

<table>
<thead>
<tr>
<th>Fiscal Year Ended January 31, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating lease cost</td>
</tr>
<tr>
<td>Short-term lease cost</td>
</tr>
<tr>
<td>Variable lease cost</td>
</tr>
<tr>
<td>Finance lease cost:</td>
</tr>
<tr>
<td>Amortization of right-of-use assets</td>
</tr>
<tr>
<td>Interest on lease liabilities</td>
</tr>
<tr>
<td>Total finance lease cost</td>
</tr>
</tbody>
</table>

The following table summarizes future scheduled lease payments as of January 31, 2023:

<table>
<thead>
<tr>
<th>Fiscal year ending January 31,</th>
<th>Operating Leases</th>
<th>Finance Leases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2024</td>
<td>$775</td>
<td>$144</td>
</tr>
<tr>
<td>2025</td>
<td>775</td>
<td>48</td>
</tr>
<tr>
<td>2026</td>
<td>797</td>
<td>45</td>
</tr>
<tr>
<td>2027</td>
<td>658</td>
<td>-</td>
</tr>
<tr>
<td>2028</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total</td>
<td>2,985</td>
<td>237</td>
</tr>
<tr>
<td>Less: Imputed Interest</td>
<td>331</td>
<td>26</td>
</tr>
<tr>
<td>Present value of net lease payments</td>
<td>$2,654</td>
<td>$211</td>
</tr>
<tr>
<td>Lease liability, current portion</td>
<td>$607</td>
<td>$130</td>
</tr>
<tr>
<td>Lease liability, net of current portion</td>
<td>$2,047</td>
<td>$81</td>
</tr>
<tr>
<td>Total lease liability</td>
<td>$2,654</td>
<td>$211</td>
</tr>
</tbody>
</table>

Supplemental information related to operating and finance leases are as follows:

70
Cash paid for amounts included in the measurement of lease liabilities $1,178
Operating cash flows from operating leases $4
Financing cash flows from finance leases 98

Weighted average remaining lease term (in years)
Operating leases 3.83
Finance leases 2.09

Weighted average discount rate
Operating leases 6.36%
Finance leases 10.10%

Disclosures Related to Periods Prior to Adoption of the New Lease Standard

The Company recorded rent expense of $1,462 for the fiscal year ended January 31, 2022.

The minimum aggregate future obligations under noncancelable operating leases as of January 31, 2022 were as follows:

<table>
<thead>
<tr>
<th>Fiscal Year ending January 31</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2023</td>
<td>$1,025</td>
</tr>
<tr>
<td>2024</td>
<td>755</td>
</tr>
<tr>
<td>2025</td>
<td>775</td>
</tr>
<tr>
<td>2026</td>
<td>797</td>
</tr>
<tr>
<td>2027</td>
<td>658</td>
</tr>
<tr>
<td>Total</td>
<td>$3,010</td>
</tr>
</tbody>
</table>

As the Company did not hold finance leases as of January 31, 2022, there were no future minimum lease payments under finance leases at that time.

12. Debt

5% Convertible Promissory Notes due 2024

On September 14, 2022, the Company entered into the SPA with 3i, under which the Company agreed to sell and issue Convertible Notes to 3i in an aggregate principal amount of up to $25,750, which are convertible into shares of the Company's common stock, subject to certain conditions. On September 15, 2022, the Company issued a Convertible Note under the SPA in the principal amount of $10,300, including a 3% Original Issue Discount ("OID"), with an 18-month term. Upon the satisfaction of additional conditions set forth in the SPA that have not been met, the Company may issue an additional Convertible Note in the principal amount of $15,450 at a second closing.

The Convertible Notes bear interest at an annual rate of 5.00% per annum, payable monthly on the first of each month (the "Installment Date"), beginning the first month that is 90 days following the issuance date, payable in cash and/or shares of the Company's common stock, at the Company's option. The interest rate will increase to an annual rate of 10.00% per annum upon the occurrence and during the continuance of an event of default as defined in the Convertible Notes. Each Convertible Note issued pursuant to the SPA will have a maturity date of 18 months from the date of issuance, which may be extended at the option of 3i in certain instances.

The Convertible Notes provide a conversion right pursuant to which 3i may convert any portion of the principal, together with any unpaid interest and other unpaid amounts, into shares of common stock at a conversion price of $7.50 per share, subject to adjustments in accordance with the terms of the Convertible Notes. The Convertible Note also contains provisions that provide 3i with the right, subject to certain exceptions, to require the Company to redeem all or a portion of the Convertible Note in cash. This convertible feature has been bifurcated from the host contract and accounted for separately as a derivative. The bifurcation of the embedded derivative created a debt discount of $774 which reduced the book value of the $10,300 Convertible Note and increases prospectively the amount of interest expense to be recognized over the life of the Convertible Note. Due to the provisions that may provide 3i with the right to require the Company to redeem all or a portion of the Convertible Note in cash, the balance of the Convertible Note is included in current liabilities on the consolidated balance sheet. As of January 31, 2023, the carrying value of the Convertible Note approximated fair value based on Level 2 inputs.

On each monthly Installment Date, the Company shall repay the lesser of $687 and the principal amount then outstanding, plus accrued and unpaid interest, in cash and/or shares of common stock, at the Company's option (the "Installment Amount"). In certain instances, but no more than once per calendar month, 3i will also have the right to accelerate the repayment of one monthly repayment obligation based on the conversion price on the acceleration date. For any Installment Amount paid in the form of shares of common stock, the applicable conversion price will be equal to the lesser of (a) $7.50, and (b) the greater of (x) 95% of the lowest VWAP in the five trading days immediately prior to such conversion, and (y) a "floor price" of approximately $0.44, subject to adjustment in accordance with the terms of the Convertible Notes. For any Installment Amount paid in cash, the price paid will be equal to 100% of the Installment Amount. The proceeds received from the Convertible Notes were used to fund general corporate and working capital needs. During the year ended January 31, 2023, the Company elected to pay one of the Installment Amounts due in cash and one Installment Amount through a combination of cash and the issuance of common stock, which resulted in the issuance of 1,364 shares of common stock for an aggregate conversion amount of $406. As of January 31, 2023, the effective interest rate on the Convertible Notes was 11.9%. Interest expense for the fiscal year ended January 31, 2023 related to the Convertible Notes was $431, which was a result of effective interest of $190 incurred under the $10,300 Convertible Note, as well as $241 in interest expense related to the amortization of related debt issuance costs of $284 and OID of $300. The Company also recognized interest expense of $138 related to the accretion of the debt discount created by the embedded conversion feature. Interest expense is included in interest expense in the consolidated statement of operations.

The following table presents the components of the Convertible Notes:

<table>
<thead>
<tr>
<th>January 31, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>3i Convertible Promissory Notes $8,471</td>
</tr>
<tr>
<td>Less: unamortized original issue discount and issuance costs (343)</td>
</tr>
<tr>
<td>Total $8,128</td>
</tr>
</tbody>
</table>
Company. At the time of issuance of the Initial Directors Notes, each of the holders of the Director Notes executed a Security Agreement, under which the Company’s obligations under the Initial Director Notes were secured by substantially all of the assets of the Company, excluding the Company’s intellectual property. The Director Notes, together with the C5 Notes described below, rank senior in right of payment to any of the Company’s existing and future indebtedness for borrowed money.

On January 11, 2023, the Company and the holders agreed to amend and restate the Initial Director Notes to be substantially in the form of the secured promissory notes issued to C5 and discussed below (the “Director Notes”). As amended and restated, the Director Notes bear interest at a rate of 13.8% per annum from the respective dates of the Initial Director Notes. All principal and accrued interest is due and payable at scheduled maturity on June 30, 2023. Upon issuance of the Director Notes, each of the holders executed an Amended and Restated Security Agreement which secure the Company’s obligations under the Director Notes by substantially all of the assets of the Company, excluding the Company’s intellectual property. The proceeds received from the Director Notes will be used to fund general corporate and working capital needs, including for purposes of remitting amounts due to taxing authorities for tax withholdings received for RSUs settled under the sell-to-cover method, as discussed in Note 5. On April 20, 2023, the Company issued and sold an additional Director Note in the amount of $300 to one of the initial lenders from December 2022 who is not affiliated with the board of directors. As of January 31, 2023, the carrying value of the Director Notes approximated fair value based on Level 2 inputs. Interest expense for the fiscal year ended January 31, 2023 was $127 and is included in interest expense in the consolidated statement of operations.

Convertible Promissory Notes with C5

On December 30, 2022, the Company issued a secured convertible promissory note in the principal amount of $2,000 (the “Initial C5 Note”) to an affiliate of C5, which was amended and restated on January 11, 2023 (as amended and restated, the “Restated C5 Note”). On January 12, 2023, February 8, 2023, February 27, 2023, April 13, 2023, May 2, 2023, and May 8, 2023, the Company issued additional senior secured convertible promissory notes to affiliates of C5 (together with the Restated C5 Note, the “C5 Notes”) in principal amounts of $3,000, $4,000, $2,250, $595, $830, and $400, respectively. As of January 31, 2023, the Company had issued secured convertible promissory notes to C5 in the amount of $5,000. Each of the C5 Notes bears interest at an annual rate of 13.8% per annum from the date of issuance (or in the case of the Restated C5 Note, from the date of the Initial C5 Note), and are payable at scheduled maturity on June 30, 2023, subject to acceleration in certain circumstances. The C5 Notes, together with the Director Notes, rank senior in right of payment to any of the Company’s existing and future indebtedness for borrowed money. The Company’s obligations under the C5 Notes are secured by substantially all of the assets of the Company, excluding the Company’s intellectual property, as governed by an Amended and Restated Security Agreement executed by C5 on January 4, 2023.

The C5 Notes provide C5 with the right, at any time on or after the date that is five calendar days prior to maturity, to convert all or any portion of the aggregate principal amount of the C5 Notes, together with any accrued and unpaid interest and any other unpaid amounts, into shares of the Company’s common stock, par value $0.0001 per share, at a conversion price of $2.00 per share. In the event that any shares of common stock are issued upon conversion of the C5 Notes, the Company has agreed to grant specified registration rights to C5.

This convertible feature has been bifurcated from the host contract and accounted for separately as a derivative. The bifurcation of the embedded derivative created a debt discount of $63 which reduced the book value of the $5,000 C5 Notes outstanding at January 31, 2023 and increases prospectively the amount of interest expense to be recognized over the life of the C5 Notes. The proceeds received from the C5 Notes were used to fund general corporate and working capital needs.

As of January 31, 2023, the carrying value of the C5 Notes approximated fair value based on Level 2 inputs. Interest expense related to the C5 Notes for the fiscal year ended January 31, 2023 was $46.

The Company also recognized interest expense of $8 related to the accretion of the debt discount created by the embedded conversion feature, which is included in interest expense in the consolidated statement of operations.

Debt Repayments

The following are scheduled principal repayments on debt, including convertible notes which can be settled in shares as of January 31, 2023, however the balances presented are classified as current in the consolidated balance sheet:

<table>
<thead>
<tr>
<th>Fiscal year ending January 31,</th>
<th>Principal</th>
</tr>
</thead>
<tbody>
<tr>
<td>2024</td>
<td>$20,140</td>
</tr>
<tr>
<td>2025</td>
<td>687</td>
</tr>
<tr>
<td>Total</td>
<td>$20,827</td>
</tr>
</tbody>
</table>

The Company had an accrued interest liability of $181 as of January 31, 2023 and no accrued interest liability as of January 31, 2022.

13. Net Income (Loss) Per Share Attributable to Common Stockholders

The Company computes basic earnings (loss) per share (“EPS”) by dividing net income or loss available to common stockholders by the weighted average number of common shares outstanding for the reporting period. Diluted EPS is computed similarly to basic net earnings per share, except that it reflects the effect of potential shares that would be issued if stock option awards, restricted stock units, convertible notes, warrants and preferred shares, to the extent issued, were converted into or exercised for common stock, to the extent dilutive.

The following table summarizes the computation of basic and diluted net loss per share attributable to common stockholders:

<table>
<thead>
<tr>
<th>Numerator: Net loss</th>
<th>Fiscal Year Ended January 31, 2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ (111,010)</td>
<td>$ (242,647)</td>
<td></td>
</tr>
</tbody>
</table>

| Denominator: Basic and Diluted Weighted-average shares in computing net loss per share attributable to common stockholders | 104,049 | 79,853 |

<table>
<thead>
<tr>
<th>Net loss attributable to common stockholders—basic and diluted</th>
<th>Fiscal Year Ended January 31, 2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ (1.07)</td>
<td>$ (1.33)</td>
<td></td>
</tr>
</tbody>
</table>

Since the Company was in a net loss position for all periods presented, diluted net loss per share attributable to common stockholders will be the same as the basic net loss per share, as, in a net loss position, the inclusion of all potential common shares outstanding would be antidilutive. The potential shares of common stock excluded from the computation of diluted net loss per share for the periods presented due to their antidilutive impacts are as follows:

72
As of January 31, 2023  As of January 31, 2022

Shares of common stock issuable from stock options  530  1,317
Unvested RSUs  4,361  10,638
Convertible notes  3,873  —
Warrants  8,606  8,606
Potential common shares excluded from diluted net loss per share  17,370  20,561

14. Related Party Transactions

Product, subscription and support revenue from Related Parties

Certain investors and companies who the Company is affiliated with purchased software, subscription and support revenue during the periods presented. The Company recognized $948 and $1,744 of revenue from contracts with related parties for the fiscal years ending January 31, 2023, and 2022, respectively. The corresponding receivable was $0 and $3,233 after the Company recorded an allowance for bad debt of $1,283 and $0 as of January 31, 2023, and 2022, respectively. During the year ended January 31, 2023, the Company recorded a corresponding bad debt expense of $1,283 within general and administrative expenses on the consolidated statement of operations.

Secured Promissory Note Financings with Directors and C5

During the year ended January 31, 2023, the Company issued and sold $6,900 of Director Notes to related parties, and issued and sold $5,000 in C5 Notes. Refer to Note 12 for additional information.

15. Retirement Plans

The Company provides a retirement savings plan for the benefit of its employees, including its executive officers. The plan is intended to qualify as a tax-qualified 401(k) plan so that contributions, and income earned on such contributions, are not taxable to participants until withdrawn or distributed from the plan (except in the case of contributions under the 401(k) plan designated as Roth contributions). The 401(k) plan provides that each participant may contribute up to an annual statutory limit. Participants who are at least 50 years old can contribute additional amounts based on statutory limits for “catch-up” contributions. Under the plan, each employee is fully vested in his or her deferred salary contributions. Employee contributions are held and invested by the plan’s trustee as directed by participants. The Company also fully matches employee contributions up to the first 4% of salary, which amounts are fully vested.

16. Segment and Geographic Information

Segments are defined as components of an enterprise for which separate financial information is evaluated regularly by the chief operating decision maker (“CODM”), in deciding how to allocate resources and assess performance. The CODM reviews financial information presented on a consolidated basis for the purposes of allocating resources and evaluating financial performance. Accordingly, management has determined that the Company operates as one operating segment.

The following table presents revenue by geographic location:

<table>
<thead>
<tr>
<th></th>
<th>Fiscal Year Ended January 31,</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2023</td>
</tr>
<tr>
<td>United States</td>
<td>$23,099</td>
</tr>
<tr>
<td>International</td>
<td>4,158</td>
</tr>
<tr>
<td>Total</td>
<td>$27,257</td>
</tr>
</tbody>
</table>

Substantially all of the Company’s long-lived assets are located in the United States.

17. Subsequent Events

Audit Committee Investigation

In March 2023, the Audit Committee of the Company’s Board of Directors concluded an internal investigation, which was originally disclosed in the Company’s notification of late filing on Form 12b-25 filed with the SEC on December 16, 2022. The Audit Committee, assisted by independent legal counsel, conducted an investigation of allegations raised in a letter to the Company by a former employee. The investigation determined that the claims were unsubstantiated.

73
We did not design and maintain effective controls over the accounting for stock-based compensation modifications. This material weakness resulted in the restatement of our unaudited condensed consolidated financial statements as of and for the three months ended October 31, 2021. The error was corrected within our Annual Report on Form 10-K, filed on May 2, 2022.

We did not design and maintain effective controls over the accounting for stock-based compensation modifications. This material weakness resulted in the restatement of our unaudited condensed consolidated financial statements as of and for the three months ended October 31, 2021. The error was corrected within our Annual Report on Form 10-K, filed on May 2, 2022.

We did not design and maintain effective controls over information technology ("IT") general controls for information systems that are relevant to the preparation of our financial statements. Specifically, we did not design and maintain: (i) program change management controls for the financial systems to ensure that information technology program and data changes affecting financial IT applications and underlying accounting records are identified, tested, authorized and implemented appropriately; (ii) appropriate access controls to ensure appropriate segregation of duties and that adequately restrict user and privileged access to financial applications, programs and data to appropriate personnel; (iii) computer operations controls to ensure data backups are authorized and restorations monitored; and (iv) testing and approval controls for program development to ensure that new software development is aligned with business and IT requirements. This material weakness did not result in a material misstatement to the consolidated financial statements.

Management determined that these material weaknesses continued to exist as of January 31, 2023. These material weaknesses could result in a misstatement of substantially all accounts or disclosures that would result in a material misstatement to the annual or interim consolidated financial statements that would not be prevented or detected.

Changes in Internal Control Over Financial Reporting

There were no changes in our internal control over financial reporting during the quarter ended January 31, 2023, that have materially affected, or are reasonably likely to materially affect, our internal control over financial reporting.

Remediation Plan

We have continued implementation of a plan to remediate these material weaknesses. These remediation measures are ongoing and have included the following:

- We hired additional accounting and finance resources with public company experience, including expertise in technical accounting and complex transactions, including stock-based compensation arrangements, in addition to utilizing third-party consultants and specialists, to supplement our internal resources;
- We are revising account reconciliation controls within all business processes to require proper segregation of duties of preparer and reviewer utilizing the additional personnel mentioned above;
we are implementing comprehensive access control protocols to implement restrictions on user and privileged access to certain applications and establishing additional controls over the preparation and review of journal entries; and

we have redesigned and strengthened financial system and application change management controls, testing and approval controls for program development, as well as data backup and restoration controls.

The elements of our remediation will continue to be accomplished over time and are subject to continued review, implementation and testing by management, as well as oversight by the audit committee of our board of directors, to determine that it is achieving our objectives. We are in the process of designing and implementing the steps to remediate these weaknesses. The material weaknesses will not be considered remediated until our remediation plan has been fully designed and implemented, the applicable controls operate for a sufficient period of time, and we have concluded, through testing, that the newly implemented and enhanced controls are operating effectively.

ITEM 9B. OTHER INFORMATION

None

ITEM 9C. DISCLOSURE REGARDING FOREIGN JURISDICTIONS THAT PREVENT INSPECTIONS

Not applicable.
ITEM 10. DIRECTORS AND EXECUTIVE OFFICERS OF THE REGISTRANT
The information required by Item 10 will be set forth in an amendment to this Form 10-K to be filed on Form 10-K/A with the SEC no later than 120 days after the end of the fiscal year covered by this Annual Report on Form 10-K and is incorporated herein by reference.

We have adopted the IronNet, Inc. Code of Business Conduct and Ethics that applies to all officers, directors and employees. The Code of Business Conduct and Ethics is available on our website at www.ir.ironnet.com. If we make any substantive amendments to the Code of Business Conduct and Ethics or grant any waiver from a provision of the Code to any executive officer or director, we will promptly disclose the nature of the amendment or waiver on our website.

ITEM 11. EXECUTIVE COMPENSATION
The information required by Item 11 will be set forth in an amendment to this Form 10-K to be filed on Form 10-K/A with the SEC no later than 120 days after the end of the fiscal year covered by this Annual Report on Form 10-K and is incorporated herein by reference.

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT AND RELATED SHAREHOLDER MATTERS
The information required by Item 12 will be set forth in an amendment to this Form 10-K to be filed on Form 10-K/A with the SEC no later than 120 days after the end of the fiscal year covered by this Annual Report on Form 10-K and is incorporated herein by reference.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS, AND DIRECTOR INDEPENDENCE
The information required by Item 13 will be set forth in an amendment to this Form 10-K to be filed on Form 10-K/A with the SEC no later than 120 days after the end of the fiscal year covered by this Annual Report on Form 10-K and is incorporated herein by reference.

ITEM 14. PRINCIPAL ACCOUNTING FEES AND SERVICES.
The information required by Item 14 will be set forth in an amendment to this Form 10-K to be filed on Form 10-K/A with the SEC no later than 120 days after the end of the fiscal year covered by this Annual Report on Form 10-K and is incorporated herein by reference.
ITEM 15. EXHIBITS, FINANCIAL STATEMENTS, AND SCHEDULES

(a) Financial Statements, Financial Statement Schedules and Exhibits.

(1) Financial Statements.

The financial statements required by Item 15(a) are filed as part of this Annual Report on Form 10-K under Item 8 “Financial Statements and Supplementary Data.”

(2) Financial Statement Schedules.

All schedules are omitted as the required information is not applicable or the information is presented in the financial statements or related notes.

(3) Exhibits.
<table>
<thead>
<tr>
<th>Exhibit Number</th>
<th>Description</th>
<th>Form</th>
<th>File No.</th>
<th>Exhibit</th>
<th>Filing Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Agreement and Plan of Reorganization and Merger, dated March 15, 2021, by and among the registrant, LGL Systems Merger Sub Inc. and IronNet Cybersecurity, Inc.</td>
<td>S-4/A</td>
<td>333-256129</td>
<td>2.1</td>
<td>August 6, 2021</td>
</tr>
<tr>
<td>2.2</td>
<td>Amendment No. 1 to Agreement and Plan of Reorganization and Merger, dated August 6, 2021, by and among the registrant, LGL Systems Merger Sub Inc. and IronNet Cybersecurity, Inc.</td>
<td>S-4/A</td>
<td>333-256129</td>
<td>2.2</td>
<td>August 6, 2021</td>
</tr>
<tr>
<td>3.1</td>
<td>Amended and Restated Certificate of Incorporation of the registrant.</td>
<td>8-K</td>
<td>001-39125</td>
<td>3.1</td>
<td>September 1, 2021</td>
</tr>
<tr>
<td>3.2</td>
<td>Amended and Restated Bylaws of the registrant.</td>
<td>8-K</td>
<td>001-39125</td>
<td>3.2</td>
<td>September 1, 2021</td>
</tr>
<tr>
<td>4.1</td>
<td>Specimen Warrant Certificate</td>
<td>S-1/A</td>
<td>333-234124</td>
<td>4.3</td>
<td>October 21, 2019</td>
</tr>
<tr>
<td>4.2</td>
<td>Warrant Agreement Between Continental Stock Transfer &amp; Trust Company and the registrant</td>
<td>8-K</td>
<td>001-39125</td>
<td>4.1</td>
<td>November 12, 2019</td>
</tr>
<tr>
<td>4.3</td>
<td>Senior Unsecured Convertible Note, dated September 15, 2022</td>
<td>8-K</td>
<td>001-39125</td>
<td>4.1</td>
<td>September 15, 2022</td>
</tr>
<tr>
<td>4.4</td>
<td>Form of Amended and Restated Secured Promissory Note</td>
<td>8-K</td>
<td>001-39125</td>
<td>99.1</td>
<td>January 4, 2023</td>
</tr>
<tr>
<td>4.5</td>
<td>Form of Amended and Restated Security Agreement</td>
<td>8-K</td>
<td>001-39125</td>
<td>99.2</td>
<td>January 4, 2023</td>
</tr>
<tr>
<td>4.6*</td>
<td>Description of Securities</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.3</td>
<td>March 15, 2021</td>
</tr>
<tr>
<td>10.1</td>
<td>Form ofPIPE Subscription Agreement</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.2</td>
<td>September 1, 2021</td>
</tr>
<tr>
<td>10.2</td>
<td>Amended and Restated Registration Rights Agreement</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.2</td>
<td>September 1, 2021</td>
</tr>
<tr>
<td>10.3*</td>
<td>Form of Indemnification Agreement</td>
<td>S-4/A</td>
<td>333-256129</td>
<td>10.12</td>
<td>August 6, 2021</td>
</tr>
<tr>
<td>10.4*</td>
<td>IronNet Cybersecurity, Inc. 2014 Equity Incentive Plan, as amended to date</td>
<td>S-4/A</td>
<td>333-256129</td>
<td>10.9</td>
<td>August 6, 2021</td>
</tr>
<tr>
<td>10.5*</td>
<td>IronNet. Inc. 2021 Equity Incentive Plan</td>
<td>S-1/B</td>
<td>333-261158</td>
<td>99.2</td>
<td>November 18, 2021</td>
</tr>
<tr>
<td>10.7*</td>
<td>Form of Stock Option Grant Package under IronNet, Inc. 2021 Equity Incentive Plan</td>
<td>S-8</td>
<td>333-261158</td>
<td>99.3</td>
<td>November 18, 2021</td>
</tr>
<tr>
<td>10.8*</td>
<td>Form of RSU Grant Package under IronNet, Inc. 2021 Equity Incentive Plan</td>
<td>S-8</td>
<td>333-261158</td>
<td>99.4</td>
<td>November 18, 2021</td>
</tr>
<tr>
<td>10.9*</td>
<td>Employment Agreement, dated May 8, 2019, by and between the registrant and GEN Keith Alexander</td>
<td>S-4/A</td>
<td>333-256129</td>
<td>10.13</td>
<td>August 6, 2021</td>
</tr>
<tr>
<td>10.10*</td>
<td>Employment Agreement, dated September 13, 2022, by and between the registrant and Cameron D. Pforr</td>
<td>10-Q</td>
<td>001-39125</td>
<td>10.6</td>
<td>May 2, 2023</td>
</tr>
<tr>
<td>10.11</td>
<td>Completion Stock Purchase Agreement, dated February 11, 2022, by and between the registrant and Tumim Stone Capital LLC</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>February 14, 2022</td>
</tr>
<tr>
<td>10.12</td>
<td>Registration Rights Agreement dated February 11, 2022, by and between the registrant and Tumim Stone Capital LLC</td>
<td>8-K</td>
<td>001-39125</td>
<td>4.1</td>
<td>February 14, 2022</td>
</tr>
<tr>
<td>10.13</td>
<td>Securities Purchase Agreement, dated September 14, 2022, by and between the registrant and 3i, LP</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>September 15, 2022</td>
</tr>
<tr>
<td>10.14</td>
<td>Registration Rights Agreement dated September 14, 2022, by and between the registrant and 3i, LP</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.2</td>
<td>September 15, 2022</td>
</tr>
<tr>
<td>10.15*</td>
<td>Separation Agreement, dated as of September 15, 2022, by and between the registrant and James C. Gerber</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.3</td>
<td>September 15, 2022</td>
</tr>
<tr>
<td>10.16*</td>
<td>Separation Agreement, dated as of September 15, 2022, by and between the registrant and William Welch</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.4</td>
<td>October 4, 2022</td>
</tr>
<tr>
<td>10.17*</td>
<td>Separation Agreement, dated as of November 18, 2022, by and between the registrant and Donald Closer</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>10.18*</td>
<td>Non-Employee Director Compensation Policy</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>21.1*</td>
<td>List of Subsidiaries</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>23.1*</td>
<td>Consent of PricewaterhouseCoopers LLP</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>31.1*</td>
<td>Certification of Principal Executive Officer Pursuant to Rules 17a-14(a) and 15d-14(a) under the Securities Exchange Act of 1934, as Adopted Pursuant to Section 302 of the Sarbanes-Oxley Act of 2002</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>31.2*</td>
<td>Certification of Principal Executive Officer Pursuant to Rules 17a-14(a) and 15d-14(a) under the Securities Exchange Act of 1934, as Adopted Pursuant to Section 302 of the Sarbanes-Oxley Act of 2002</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>31.3*</td>
<td>Certifications of Principal Executive Officer and Principal Financial Officer Pursuant to 18 U.S.C. Section 1350, as Adopted Pursuant to Section 906 of the Sarbanes-Oxley Act of 2002</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>101.INS*</td>
<td>Inline XBRL Instance Document – instance document does not appear in the Interactive Data File because its XBRL tags are embedded within the Inline XBRL document.</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>101.CAL*</td>
<td>Inline XBRL Taxonomy Extension Calculation Linkbase Document</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>101.DEF*</td>
<td>Inline XBRL Taxonomy Extension Definition Linkbase Document</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>101.LAB*</td>
<td>Inline XBRL Taxonomy Extension Label Linkbase Document</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
<tr>
<td>101.PRE*</td>
<td>Inline XBRL Taxonomy Extension Presentation Linkbase Document</td>
<td>8-K</td>
<td>001-39125</td>
<td>10.1</td>
<td>November 18, 2022</td>
</tr>
</tbody>
</table>

* Filed herewith.

\(^\) These certifications are being furnished solely to accompany this Annual Report pursuant to 18 U.S.C. Section 1350, and are not being filed for purposes of Section 18 of the Securities Exchange Act of 1934, as amended, and are not to be incorporated by reference into any filing of the registrant, whether made before or after the date hereof, regardless of any general incorporation language in such filing.

+ Indicates a management contract or compensatory plan, contract or arrangement.
None.

Pursuant to the requirements of the Securities Exchange Act of 1934, the Company has duly caused this report to be signed on its behalf by the undersigned thereunto duly authorized.

IRONNET, INC.

Date: May 16, 2023

By: /s/ Cameron D. Pforr

Cameron D. Pforr
Chief Financial Officer
(On behalf of the Registrant)
POWER OF ATTORNEY

KNOW ALL BY THESE PRESENTS, that each of the undersigned hereby constitutes and appoints each of Keith B. Alexander, Cameron D. Pforr and S. Scott Alridge, and each or any one of them, as his or her true and lawful attorney-in-fact and agent, with full power of substitution and resubstitution, for him or her and in his or her name, place and stead, in any and all capacities, to sign any and all amendments to this Annual Report on Form 10-K, and to file the same, with all exhibits thereto, and other documents in connection therewith, with the Securities and Exchange Commission, granting unto said attorneys-in-fact and agents, and each of them, full power and authority to do and perform each and every act and thing requisite and necessary to be done in connection therewith, as fully to all intents and purposes as he or she might or could do in person, hereby ratifying and confirming all that said attorneys-in-fact and agents, or any of them, or their or his substitutes or substitute, may lawfully do or cause to be done by virtue hereof.

Pursuant to the requirements of the Securities Act of 1933, this report has been signed by the following persons in the capacities and on the dates indicated.

<table>
<thead>
<tr>
<th>Signature</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s/ GEN Keith B. Alexander (Ret.)</td>
<td>GEN Keith B. Alexander (Ret.)</td>
<td>Chief Executive Officer, President and Chairman (Principal Executive Officer)</td>
</tr>
<tr>
<td>/s/ Cameron D. Pforr</td>
<td>Cameron D. Pforr</td>
<td>Chief Financial Officer (Principal Financial and Accounting Officer)</td>
</tr>
<tr>
<td>/s/ Donald R. Dixon</td>
<td>Donald R. Dixon</td>
<td>Director</td>
</tr>
<tr>
<td>/s/ Mary E. Gallagher</td>
<td>Mary E. Gallagher</td>
<td>Director</td>
</tr>
<tr>
<td>/s/ GEN John M. Keane (Ret.)</td>
<td>GEN John M. Keane (Ret.)</td>
<td>Director</td>
</tr>
<tr>
<td>/s/ Robert V. LaPenta Jr.</td>
<td>Robert V. LaPenta Jr.</td>
<td>Director</td>
</tr>
<tr>
<td>/s/ VADM John M. McConnell (Ret.)</td>
<td>VADM John M. McConnell (Ret.)</td>
<td>Director</td>
</tr>
<tr>
<td>/s/ Michael J. Rogers</td>
<td>Michael J. Rogers</td>
<td>Director</td>
</tr>
<tr>
<td>/s/ Theodore E. Schlein</td>
<td>Theodore E. Schlein</td>
<td>Director</td>
</tr>
<tr>
<td>/s/ VADM Jan E. Tighe (Ret.)</td>
<td>VADM Jan E. Tighe (Ret.)</td>
<td>Director</td>
</tr>
</tbody>
</table>
Description of Securities

IronNet, Inc. ("we," "our," "us," or the "Company") has two classes of securities registered under Section 12 of the Securities Exchange Act of 1934, as amended (the “Exchange Act”): common stock, par value $0.0001 par value per share (the “Common Stock”), and public warrants, each whole public warrant exercisable for one share of Common Stock at an exercise price of $11.50 per share (the “Public Warrants”).

The following description of the material terms of our share capital includes a summary of specified provisions of our charter documents. This description is qualified by reference to our Second Amended and Restated Certificate of Incorporation (the “A&R Certificate”) and our bylaws and Public-Warrant-related documents, each of which is filed as an exhibit to our Annual Report on 10-K.

General

Our A&R Certificate authorizes us to issue up to 500,000,000 shares of Common Stock, $0.0001 par value per share, and 100,000,000 shares of preferred stock, $0.0001 par value per share.

Common Stock

Voting Rights

Each holder of Common Stock is entitled to one vote for each share on all matters submitted to a vote of the stockholders, including the election of directors. Under our A&R Certificate, our stockholders will not have cumulative voting rights. Because of this, the holders of a majority of the shares of Common Stock entitled to vote in any election of directors can elect all of the directors standing for election.

Dividend Rights

Subject to preferences that may apply to any then-outstanding preferred stock, the holders of Common Stock are entitled to receive ratably those dividends, if any, as may be declared from time to time by the board of directors out of legally available funds. We do not anticipate paying any cash dividends in the foreseeable future.

Liquidation Rights

In the event of our liquidation, dissolution or winding up, holders of Common Stock will be entitled to share ratably in the net assets legally available for distribution to stockholders after the payment of all of our debts and other liabilities and the satisfaction of any liquidation preference granted to the holders of any then-outstanding shares of preferred stock.

Preemptive or Similar Rights

Holders of Common Stock have no preemptive, conversion or subscription rights and there are no redemption or sinking fund provisions applicable to the Common Stock. The rights, preferences and privileges of the holders of Common Stock are subject to, and may be adversely affected by, the rights of the holders of shares of any series of preferred stock that we may designate in the future.

Preferred Stock

Under our A&R Certificate our board of directors may, without further action by our stockholders, fix the rights, preferences, privileges and restrictions of up to an aggregate of 100,000,000 shares of preferred stock in one or more series and authorize their issuance. These rights, preferences and privileges could include dividend rights, conversion rights, voting rights, terms of redemption, liquidation preferences and the number of shares constituting any series or the designation of such series, any or all of which may be greater than the rights of Common Stock. Any issuance of preferred stock could adversely affect the voting power of holders of Common Stock and the likelihood that such holders would receive dividend payments and payments on liquidation. In addition, the issuance of preferred stock could have the effect of delaying, deterring or preventing a change of control or other corporate action. No shares of preferred stock are outstanding. We have no present plans to issue any shares of preferred stock.

Warrants

As of January 31, 2023, there were 8,606,473 warrants to purchase Common Stock outstanding, consisting of 8,596,273 public warrants exercisable for our common stock at an exercise price of $11.50 per share (subject to adjustment) included in the units issued in the initial public offering of LGL Systems Acquisition Corporation (the “Public Warrants”) and 10,200 private warrants issued to LGL Systems Acquisition Holding Company, LLC in a
private placement simultaneously with the initial public offering of LGL Systems Acquisition Corporation (the “Private Warrants” and, together with the Public Warrants, the “Warrants”). Each Warrant entitles the registered holder to purchase one share of Common Stock at a price of $11.50 per share. The Warrants will expire at 5:00 p.m., New York City time, on August 26, 2026, or earlier upon redemption or liquidation.

Holders of Public Warrants cannot pay cash to exercise their Public Warrants unless we have an effective and current registration statement covering the issuance of the shares underlying such Warrants and a current prospectus relating thereto. Notwithstanding the foregoing, if a registration statement covering the shares of Common Stock issuable upon exercise of the Public Warrants is not effective within a specified period following the closing of the Business Combination, warrant holders may, until such time as there is an effective registration statement and during any period when we shall have failed to maintain an effective registration statement, exercise Warrants on a cashless basis pursuant to the exemption provided by Section 3(a)(9) of the Securities Act, provided that such exemption is available. If that exemption, or another exemption, is not available, holders will not be able to exercise their Warrants on a cashless basis. In the event of such cashless exercise, each holder would pay the exercise price by surrendering the Warrants for that number of shares of Common Stock equal to the quotient obtained by dividing (x) the product of the number of shares of Common Stock underlying the Warrants, multiplied by the difference between the exercise price of the Warrants and the “fair market value” (defined below) by (y) the fair market value. The “fair market value” for this purpose will mean the average reported closing price of the shares of Common Stock for the 10 trading days ending on the third trading day prior to the date of exercise.

The Private Warrants are identical to the Public Warrants except that such warrants are not redeemable by us so long as they are held by the Sponsor or its permitted transferees. The Sponsor or its permitted transferees have the option to exercise the Private Warrants on a cashless basis. If the Private Warrants are held by holders other than the Sponsor and LGL’s current independent directors or their permitted transferees, the Private Warrants will be redeemable by us and exercisable by the holders on the same basis as the Public Warrants.

We may call the Public Warrants for redemption, in whole and not in part, at a price of $0.01 per warrant,

• at any time after the warrants become exercisable;
• upon not less than 30 days’ prior written notice of redemption to each warrant holder;
• if, and only if, the reported last sale price of the shares of Common Stock equals or exceeds $18.00 per share (as adjusted for stock splits, stock dividends, reorganizations and recapitalizations), for any 20 trading days within a 30 trading day period commencing at any time after the warrants become exercisable and ending on the third trading day prior to the notice of redemption to warrant holders; and
• if, and only if, there is a current registration statement in effect with respect to the shares of Common Stock underlying such warrants.

The right to exercise will be forfeited unless the Warrants are exercised prior to the date specified in the notice of redemption. On and after the redemption date, a record holder of a warrant will have no further rights except to receive the redemption price for such holder’s warrant upon surrender of such warrant.

The redemption criteria for our Warrants was established at a price which is intended to provide warrant holders a reasonable premium to the initial exercise price and provide a sufficient differential between the then prevailing share price and the warrant exercise price so that if the share price declines as a result of our redemption call, the redemption will not cause the share price to drop below the exercise price of the Warrants.

If we call the Warrants for redemption as described above, our management will have the option to require all holders that wish to exercise Warrants to do so on a “cashless basis.” In such event, each holder would pay the exercise price by surrendering the Warrants for that number of shares of Common Stock equal to the quotient obtained by dividing (x) the product of the number of shares of Common Stock underlying the Warrants, multiplied by the difference between the exercise price of the Warrants and the “fair market value” (defined below) by (y) the fair market value. The “fair market value” for this purpose shall mean the average reported closing price of the shares of Common Stock for the 10 trading days ending on the third trading day prior to the date on which the notice of redemption is sent to the holders of Warrants.

The Warrants were issued in registered form under the Warrant Agreement between Continental Stock Transfer & Trust Company, as warrant agent, and us. The Warrant Agreement provides that the terms of the Warrants may be amended without the consent of any holder to cure any ambiguity or correct any defective provision, but requires the
approval, by written consent or vote, of the holders of at least a majority of the then outstanding Warrants, if such modification or amendment is being undertaken prior to, or in connection with, the closing, or Warrants, if such modification or amendment is being undertaken after the closing.

The exercise price and number of shares of Common Stock issuable on exercise of the Warrants may be adjusted in certain circumstances including in the event of a stock dividend, or our recapitalization, reorganization, merger or consolidation. The Warrants will not be adjusted for issuances of shares of Common Stock at a price below their respective exercise prices.

The Public Warrants may be exercised upon surrender of the warrant certificate on or prior to the expiration date at the office of the warrant agent, with the subscription form, as set forth in the warrant, duly executed, accompanied by full payment of the exercise price (unless the exercise is on a cashless basis, if applicable), by certified or official bank check payable to the order of the warrant agent, for the number of Public Warrants being exercised. The warrant holders do not have the rights or privileges of holders of shares of Common Stock and any voting rights until they exercise their Public Warrants and receive shares of Common Stock. After the issuance of shares of Common Stock upon exercise of the Public Warrants, each holder will be entitled to one vote for each share held of record on all matters to be voted on by stockholders.

Public Warrant holders may elect to be subject to a restriction on the exercise of their Public Warrants such that an electing warrant holder would not be able to exercise their Public Warrants to the extent that, after giving effect to such exercise, such holder would beneficially own in excess of 4.9% or 9.8% (as specified by the holder) of the shares of Common Stock outstanding immediately after giving effect to such exercise.

**Anti-Takeover Provisions**

**Section 203 of the Delaware General Corporation Law**

We are subject to Section 203 of the DGCL, which generally prohibits a publicly held Delaware corporation from engaging in any business combination with any interested stockholder for a period of three years after the date that such stockholder became an interested stockholder, with the following exceptions:

- before such date, the board of directors of the corporation approved either the business combination or the transaction that resulted in the stockholder becoming an interested stockholder;
- upon completion of the transaction that resulted in the stockholder becoming an interested stockholder, the interested stockholder owned at least 85% of the voting stock of the corporation outstanding at the time the transaction began, excluding for purposes of determining the voting stock outstanding, but not the outstanding voting stock owned by the interested stockholder, those shares owned (1) by persons who are directors and also officers and (2) employee stock plans in which employee participants do not have the right to determine confidentially whether shares held subject to the plan will be tendered in a tender or exchange offer; or
- on or after such date, the business combination is approved by the board of directors and authorized at an annual or special meeting of the stockholders, and not by written consent, by the affirmative vote of at least 662/3% of the outstanding voting stock that is not owned by the interested stockholder.

In general, Section 203 defines a “business combination” to include the following:

- any merger or consolidation involving the corporation and the interested stockholder;
- any sale, transfer, pledge or other disposition of 10% or more of the assets of the corporation involving the interested stockholder;
- subject to certain exceptions, any transaction that results in the issuance or transfer by the corporation of any stock of the corporation to the interested stockholder;
- any transaction involving the corporation that has the effect of increasing the proportionate share of the stock or any class or series of the corporation beneficially owned by the interested stockholder; or
- the receipt by the interested stockholder of the benefit of any loans, advances, guarantees, pledges or other financial benefits by or through the corporation.
In general, Section 203 defines an “interested stockholder” as an entity or person who, together with the person’s affiliates and associates, beneficially owns or within three years prior to the time of determination of interested stockholder status did own, 15% or more of the outstanding voting stock of the corporation.

A Delaware corporation may “opt out” of these provisions with an express provision in its original certificate of incorporation or an express provision in its amended and restated certificate of incorporation or amended and restated bylaws resulting from a stockholders’ amendment approved by at least a majority of the outstanding voting shares. We have not opted out of these provisions. As a result, mergers or other takeover or change in control attempts of us may be discouraged or prevented.

**Certificate of Incorporation and Bylaws**

Among other things, our A&R Certificate and amended and restated bylaws:

- permit our board of directors to issue up to 100,000,000 shares of preferred stock, with any rights, preferences and privileges as they may designate, including the right to approve an acquisition or other change of control;
- provide that the authorized number of directors may be changed only by resolution of our board of directors;
- provide that, subject to the rights of any series of preferred stock to elect directors, directors may only be removed in the manner specified in Section 141(k) of the DGCL;
- provide that all vacancies, including newly created directorships, may, except as otherwise required by law, be filled by the affirmative vote of a majority of directors then in office, even if less than a quorum, or by the sole remaining director;
- require that any action to be taken by our stockholders must be effected at a duly called annual or special meeting of stockholders and not be taken by written consent or electronic transmission;
- provide that stockholders seeking to present proposals before a meeting of stockholders or to nominate candidates for election as directors at a meeting of stockholders must provide advance notice in writing, and also specify requirements as to the form and content of a stockholder’s notice;
- provide that special meetings of our stockholders may be called by (i) the chairperson of the board of directors, (ii) the chief executive officer or (iii) a majority vote of the board of directors; and
- not provide for cumulative voting rights, therefore allowing the holders of a majority of the shares of Common Stock entitled to vote in any election of directors to elect all of the directors standing for election, if they should so choose.

The amendment of any of these provisions would require approval by the holders of at least 66 2/3% of the voting power of all of our then-outstanding capital stock entitled to vote generally in the election of directors, voting together as a single class.

The combination of these provisions will make it more difficult for our existing stockholders to replace our board of directors as well as for another party to obtain control of us by replacing our board of directors. Since our board of directors has the power to retain and discharge our officers, these provisions could also make it more difficult for existing stockholders or another party to effect a change in management. In addition, the authorization of undesignated preferred stock makes it possible for our board of directors to issue preferred stock with voting or other rights or preferences that could impede the success of any attempt to change our control.

These provisions are intended to enhance the likelihood of continued stability in the composition of our board of directors and its policies and to discourage coercive takeover practices and inadequate takeover bids. These provisions are also designed to reduce our vulnerability to hostile takeovers and to discourage certain tactics that may be used in proxy fights. However, such provisions could have the effect of discouraging others from making tender offers for our shares and may have the effect of delaying changes in our control or management. As a consequence, these provisions may also inhibit fluctuations in the market price of our stock.

The A&R Certificate provides to the fullest extent permitted by law, that derivative actions brought in the company’s name, actions against directors, officers and employees for breach of fiduciary duty and other similar actions may be brought only in the Court of Chancery in the State of Delaware and, if brought outside of Delaware, the stockholder bringing the suit will be deemed to have consented to service of process on such stockholder’s
counsel except any action (A) as to which the Court of Chancery in the State of Delaware determines that there is an indispensable party not subject to the jurisdiction of the Court of Chancery (and the indispensable party does not consent to the personal jurisdiction of the Court of Chancery within ten days following such determination), (B) which is vested in the exclusive jurisdiction of a court or forum other than the Court of Chancery or (C) for which the Court of Chancery does not have subject matter jurisdiction. Any person or entity purchasing or otherwise acquiring any interest in shares of the company’s Common Stock shall be deemed to have notice of and consented to the forum provisions in the A&R Certificate. The A&R Certificate further provides that the federal district courts of the United States of America will be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act.

Section 27 of the Exchange Act creates exclusive federal jurisdiction over all suits brought to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder. As a result, the exclusive forum provision of our A&R Certificate will not apply to suits brought to enforce any duty or liability created by the Exchange Act or any other claim for which the federal courts have exclusive jurisdiction.

Although we believe this provision benefits us by providing increased consistency in the application of Delaware law in the types of lawsuits to which it applies, a court may determine that this provision is unenforceable, and to the extent it is enforceable, the provision may have the effect of discouraging lawsuits against our directors and officers, although our stockholders will not be deemed to have waived our compliance with federal securities laws and the rules and regulations thereunder and therefore bring a claim in another appropriate forum. Additionally, we cannot be certain that a court will decide that this provision is either applicable or enforceable, and if a court were to find the choice of forum provision contained in the A&R Certificate to be inapplicable or unenforceable in an action, we may incur additional costs associated with resolving such action in other jurisdictions, which could harm our business, operating results and financial condition.

Transfer Agent

The transfer agent for our securities is Continental Stock Transfer & Trust Company. The transfer agent’s address is One State Street Plaza, 30th Floor New York, New York 10004.

Listing

Our Common Stock and Public Warrants are traded on the New York Stock Exchange under the symbols “IRNT” and “IRNT.WS”, respectively.
IronNet, Inc.
Non-Employee Director Compensation Policy
(effective November 23, 2021)

The purpose of this Non-Employee Director Compensation Policy (the “Policy”) of IronNet, Inc., a Delaware corporation (the “Company”), is to provide a total compensation package that enables the Company to attract and retain, on a long-term basis, high-caliber directors who are not employees or officers or consultants of the Company or its subsidiaries (“Outside Directors”). In furtherance of the purpose stated above, all Outside Directors shall be paid compensation for services provided to the Company as set forth below:

I. Cash Retainers

(a) Annual Retainer for Board Membership, Chairperson and Lead Independent Director. Each Outside Director shall receive $30,000 on an annual basis for general availability and participation in meetings and conference calls of the Company’s Board of Directors (the “Board”). If the Chairperson of the Board is also an Outside Director, he or she shall receive an additional $20,000 on annual basis for service in such capacity. If the Chairperson of the Board is not an Outside Director, and the Board has appointed a Lead Independent Director, the Lead Independent Director shall receive an additional $20,000 on annual basis for service in such capacity.

(b) Annual Retainers for Committee Service. The following additional annual cash retainers for service on committees of the Board (each, a “Committee”) will apply:

| Committee Chairperson               | $ 20,000 |
| Audit Committee member (other than Chairperson): | $ 8,000 |
| Compensation Committee Chairperson:  | $ 12,000 |
| Compensation Committee member (other than Chairperson): | $ 5,000 |
| Nominating and Corporate Governance Committee Chairperson: | $ 7,500 |
| Nominating and Corporate Governance Committee member (other than Chairperson): | $ 3,500 |

(c) Timing of Payments. The cash retainers described above will be paid in equal quarterly installments (in arrears as soon as practicable, but in no event more than 30 days, following each fiscal quarter end). If an Outside Director joins the Board or a Committee at a time other than effective as of the first day of a fiscal quarter, each cash retainer amount that is scheduled to be paid for the fiscal quarter will be prorated based on days served in the applicable fiscal quarter, with the prorated amount paid for the first fiscal quarter in which the Outside Director provides the service, and regular full quarterly payments thereafter. If an Outside Director terminates service on the Board or a Committee during the course of a fiscal quarter, the cash retainer amount for the fiscal quarter in which such termination occurs will be prorated based on days served in such fiscal quarter. All annual cash fees are vested upon payment.

II. Equity Grants

All grants of equity awards to Outside Directors pursuant to this Policy will be automatic and nondiscretionary (without the need for any additional corporate action by the Board or the Compensation Committee) and will be made in accordance with the following provisions:

(a) Initial Grants. Upon the initial election or appointment of an Outside Director to the Board, such Outside Director will receive a grant of restricted stock units (“RSUs”) under the Company’s 2021 Equity Incentive Plan (the “2021 Plan”), covering a number of shares of the Company’s common stock (the “Common Stock”) equal to (i) $240,000 divided by (ii) the average closing price of the Common Stock for the 10 trading days preceding the effective...
date of the Outside Director’s election or appointment to the Board (the “Initial Grant”). The RSUs subject to the Initial Grants will vest in equal installments annually over three years, with one-third of the RSUs vesting on the each of the first, second and third anniversaries of the date of grant, subject to such Outside Director’s Continuous Service (as defined in the 2021 Plan) through each such vesting date.

(b) **Annual Grants.** On the date of each annual meeting of the Company’s stockholders (an “Annual Meeting”), each Outside Director who continues as a director of the Company following the Annual Meeting shall receive a grant of RSUs under the 2021 Plan, covering a number of shares of Common Stock equal to (i) $180,000 divided by (ii) the average closing price of the Common Stock for the 10 trading days preceding the date of the Annual Meeting. The RSUs subject to the Annual Grants will vest in full on the earlier of (i) the first anniversary of the date of grant, or (ii) the date of the next Annual Meeting, in either case subject to such director’s Continuous Service with the Company until such vesting date. No Outside Director shall be granted an Annual Grant in the same fiscal year that such person received his or her Initial Grant.

(c) **Acceleration of Initial Grants and Annual Grants.** Notwithstanding the foregoing vesting schedules, all Initial Grants and Annual Grants granted pursuant to this Policy shall vest in full immediately prior to, but conditioned upon, the closing of a Change in Control as defined under the 2021 Plan, subject to such Outside Director remaining in Continuous Service with the Company until immediately prior to the closing of such Change in Control.

(d) **Settlement and Deferral.** Unless an Outside Director elects to defer the delivery of Common Stock to be issued upon settlement of vested RSUs under Initial Grants and Annual Grants as described below, the Common Stock shall be delivered on the applicable vesting date, or as soon as practicable thereafter, subject to the terms and conditions of the applicable form of RSU grant notice and agreement approved by the Board; provided, that such Common Stock shall be delivered no later than the date that is the 15th day of the third calendar month of the year following the calendar year in which such shares are no longer subject to a “substantial risk of forfeiture” within the meaning of Treasury Regulations Section 1.409A-1(d). Outside Directors may defer the receipt of Common Stock underlying Initial Grants and Annual Grants pursuant to this Policy by completing a deferral election form provided by the Company. An election to defer the receipt of Common Stock subject to an Initial Grant or an Annual Grant must be made by delivering the election form to the Company, in the case of an Annual Grant, before the Annual Meeting to which such Annual Grant relates, and, in the case of the Initial Grant, on the date of or by no later than thirty (30) days after the Outside Director’s initial appointment or election to the Board; provided, however, that a deferral election only applies to compensation paid for services performed after the election. No deferral election will be given effect unless it complies with the deferral election rules of Section 409A of the Code. If an Outside Director elects to defer delivery of Common Stock to be issued upon settlement of vested RSUs, any vested RSUs granted pursuant to this Policy will be settled in Common Stock on the earlier of (i) an Outside Director’s “separation from service” (as such term is defined in Treasury Regulations Section 1.409A-1(h) without regard to any alternative definition thereunder) from the Company (a “Separation from Service”) for any reason (provided that the RSUs will be settled six months and one day after such separation from service, or, if earlier, upon the Outside Director’s death, if the Outside Director is a specified employee under Treasury Regulation Section 1.409A-1(i) at the time of separation), or (ii) a Change in Control that also constitutes a “change in control event” (as determined under Treasury Regulations Section 1.409A-3(i)(5)) (a “Change in Control”).

(e) **Additional Provisions.** All provisions of the 2021 Plan not inconsistent with this Policy will apply to awards granted to Outside Directors. Outside Directors will be required to execute an RSU award agreement in a form satisfactory to the Company prior to receipt of an Initial Grant or Annual Grant. An Outside Director may decline all or any portion of his or her compensation by giving notice to the Company prior to the date cash is to be paid or equity awards are to be granted, as the case may be.

### III. Expenses

The Company will reimburse all reasonable out-of-pocket expenses incurred by Outside Directors in attending meetings of the Board or any Committee thereof. The Company will reimburse Outside Directors for ordinary, necessary and reasonable out-of-pocket travel expenses to cover in-person attendance at and participation in Board and committee meetings; provided, that the Outside Director timely submit to the Company appropriate documentation substantiating such expenses in accordance with the Company’s travel and expense policy, as in effect from time to time.
IV. Section 409A

It is the intent of this Policy that this Policy and all payments hereunder be exempt from or otherwise comply with the requirements of Section 409A of the Internal Revenue Code, as amended, and the rules and regulations thereunder (“Section 409A”) so that none of the compensation to be provided hereunder will be subject to the additional tax imposed under Section 409A, and any ambiguities or ambiguous terms herein will be interpreted to be so exempt or comply. In no event will the Company reimburse an Outside Director for any taxes imposed or other costs incurred as a result of Section 409A.

V. Revisions

The Board or the Compensation Committee may amend, alter, suspend or terminate this Policy at any time and for any reason. The Board or the Compensation Committee in its discretion may change and otherwise revise the terms of awards to be granted under this Policy, including, without limitation, the number of shares subject thereto, for awards of the same or different type granted on or after the date the Board or the Compensation Committee determines to make any such change or revision. No amendment, alteration, suspension or termination of this Policy will materially impair the rights of an Outside Director with respect to compensation that already has been paid or awarded, unless otherwise mutually agreed between the Outside Director and the Company. Termination of this Policy will not affect the Board’s or the Compensation Committee’s ability to exercise the powers granted to it under the Plan with respect to Awards granted under the Plan pursuant to this Policy prior to the date of such termination.

VI. Non-Employee Director Compensation Limit

Notwithstanding the foregoing, the aggregate value of all compensation granted or paid, as applicable, to any individual for service as a Nonemployee Director (as defined in the Plan) shall in no event exceed the limits set forth in Section 3(d) of the Plan.
<table>
<thead>
<tr>
<th>Name of Subsidiary</th>
<th>Jurisdiction of Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>IronNet Cybersecurity, Inc.</td>
<td>United States (Delaware)</td>
</tr>
<tr>
<td>High Degree, LLC</td>
<td>United States (Delaware)</td>
</tr>
<tr>
<td>IronNet International, LLC</td>
<td>United States (Delaware)</td>
</tr>
<tr>
<td>IronNet Cybersecurity Singapore Pte Ltd</td>
<td>Singapore</td>
</tr>
<tr>
<td>IronNet Cybersecurity Japan, GK</td>
<td>Japan</td>
</tr>
<tr>
<td>IronNet Cybersecurity UK Ltd.</td>
<td>England and Wales</td>
</tr>
<tr>
<td>IronNet Australia Pty Ltd.</td>
<td>Australia</td>
</tr>
<tr>
<td>IronNet Cybersecurity FZ-LLC</td>
<td>United Arab Emirates</td>
</tr>
</tbody>
</table>
CONSENT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

We hereby consent to the incorporation by reference in the Registration Statements on Form S-8 (Nos. 333-263663 and 333-261158) of IronNet, Inc. of our report dated May 16, 2023 relating to the financial statements, which appears in this Form 10-K.

/s/ PricewaterhouseCoopers LLP
Washington, District of Columbia
May 16, 2023
I, Keith B. Alexander, certify that:

1. I have reviewed this Annual Report on Form 10-K of IronNet, Inc.;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

   (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

   (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   (c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   (d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

   (a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

   (b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: May 16, 2023

By: /s/ GEN Keith B. Alexander (Ret.)

GEN Keith B. Alexander (Ret.)
Chief Executive Officer, President and Chairman
(Principal Executive Officer)
I, Cameron D. Pforr, certify that:

1. I have reviewed this Annual Report on Form 10-K of IronNet, Inc.;
2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;
3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;
4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:
   (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;
   (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;
   (c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and
   (d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and
5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):
   (a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and
   (b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: May 16, 2023

By: /s/ Cameron D. Pforr
Cameron D. Pforr
Chief Financial Officer
(Principal Financial Officer)
Pursuant to the requirement set forth in Rule 13a-14(b) of the Securities Exchange Act of 1934, as amended, (the “Exchange Act”) and Section 1350 of Chapter 63 of Title 18 of the United States Code (18 U.S.C. §1350), GEN Keith B. Alexander (Ret.), Chief Executive Officer of IronNet, Inc. (the “Company”), and Cameron D. Pforr, Chief Financial Officer of the Company, each hereby certifies that, to the best of his knowledge:

1. The Company’s Annual Report on Form 10-K for the fiscal year ended January 31, 2023, to which this Certification is attached as Exhibit 32.1 (the “Annual Report”), fully complies with the requirements of Section 13(a) or Section 15(d) of the Exchange Act; and

2. The information contained in the Annual Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

Dated: May 16, 2023

By: /s/ GEN Keith B. Alexander (Ret.)

GEN Keith B. Alexander (Ret.)
Chief Executive Officer, President and Chairman
(Principal Executive Officer)

By: /s/ Cameron D. Pforr

Cameron D. Pforr
Chief Financial Officer
(Principal Financial Officer)

This certification accompanies the Form 10-K to which it relates, is not deemed filed with the Securities and Exchange Commission and is not to be incorporated by reference into any filing of the Company under the Securities Act of 1933, as amended, or the Securities Exchange Act of 1934, as amended (whether made before or after the date of the Form 10-K), irrespective of any general incorporation language contained in such filing.