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

FORM 10-K

(Mark One)
☒ ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the fiscal year ended January 31, 2022
or
☐ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
Commission file number 001-39125

IronNet, Inc.
(Exact name of registrant as specified in its charter)

Delaware		**83-4599446**
(State or other jurisdiction of incorporation)		**(IRS Employer Identification No.)**
7900 Tysons One Place, Suite 400 McLean, VA		**22102**
(Address of principal executive offices)		**(Zip Code)**

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

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	**Trading Symbol(s)**	**Name of each exchange on which registered**
Common Stock, par value $0.0001 per share	**IRNT**	**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 of 1934 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 ☐

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 June 30, 2021, 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 $9.99 per share on the date, was approximately $172.3 million. On August 27, 2021, the registrant completed a business combination with IronNet Cybersecurity, Inc., changed its name from LGL Systems Acquisition Corp. to IronNet, Inc. and changed its fiscal year end from December 31 to January 31.

There were 100,426,374 shares of Common Stock, par value $0.0001 per share, outstanding as of May 2, 2022.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive proxy statement relating to its 2022 Annual Meeting of Stockholders (the "Proxy Statement") to be filed with the Securities and Exchange Commission pursuant to Regulation 14A, not later than 120 days after the close of the registrant's fiscal year, are incorporated by reference in Part III of this Annual Report on Form 10-K. Except with respect to information specifically incorporated by reference in this Annual Report on Form 10-K, the Proxy Statement is not deemed to be filed as part of this Annual Report on Form 10-K.

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.

CAUTIONARY NOTE REGARDING FORWARD-LOOKING STATEMENTS

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 recognize the anticipated benefits of the Business Combination, which may be affected by, among other things, competition and the ability of the combined business to grow and manage growth profitably;
- our future operating or financial results;
- future acquisitions, business strategy and expected capital spending;
- 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;
- the impact of the COVID-19 pandemic on customer demands for our products;
- 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 or 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.

IronNet, Inc.
Table of Contents
FORM 10-K

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 experienced rapid growth in recent periods, and if we do not manage our future growth, our business and results of operations will be adversely affected.
- We have a history of losses and we may not be able to achieve or sustain profitability in the future.
- 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.

PART I

ITEM 1. BUSINESS

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 Co-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 significant majority of our current revenue comes from our IronDome™ and IronDefense™ products. IronDefense is an NDR cybersecurity product that uses 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.

We are a metric-driven organization with 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.

Cyber-security 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, telecommunications companies, 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 a number of 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."

Our collective defense model, IronDome, is a means for the private sector to "raise the baseline" level of security by partnering amongst themselves to "produce positive outcomes." This overwatch 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 Security Act of 2014) 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 something that might reflect poorly on their own actions. This is less an issue for collective defenses implemented across the business units of one 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 heterogenous 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 multi-national. 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 defensive 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 Platform Offering

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 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 largely cloud-deployed (public or private), though it is also available in on-premise and hybrid environments, and is scalable to include small-to-medium businesses and public-sector agencies as well as multinational corporations. 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, 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 63% of our revenue for the year ended January 31, 2022 related to deployments involving our key public cloud providers Amazon Web Services and Microsoft Azure. We also support 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.

We describe our go-to-market strategy as "land and expand with network effects." Our approach is to initially secure influential "cornerstone" customers and then expand into their respective Collective Defense communities with additional "community members" from organizations of similar industry sector, state, country, supply chain, or tailored business ecosystem. 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.

We sell into both public and private organizations and the business ecosystems that support them. We have identified tens of thousands of prospective cornerstone customers and more than 100,000 potential community customers.

Some of the world's largest enterprises, government organizations, high-profile brands, and governments trust us to protect their networks. Our customers include a top global hedge fund, eight of the top 10 U.S. energy companies (based on revenue), a leading Asian mobile phone carrier, two U.S. Department of Defense ("DoD") branches, a mid-sized bank in the Europe, Middle East and Africa ("EMEA") region, four U.S. state agencies, U.K. and Singapore government entities, and a large global holding company. Most recently, we have grown a Collective Defense community for the space industrial base. This community includes five commercial space companies, including Intuitive Machines, Axiom Space, Satelles, and X-Energy.

We began targeting large enterprises and Fortune 500 companies, but the flexibility and scalability of our cloud-native platform and enhance go-to-market approach enabled us to expand our customer base to smaller companies as well. We have been recognized in the cybersecurity industry by independent third-party analysts, including Gartner, Forrester, IDC, 451 Research Group, and Omdia, who called our analytics a "potential game changer" in a June 2020 report. In August 2020, we announced that we had achieved "FedRAMP-ready" for Agency Authorization status, as approved by the Federal Risk and Authorization Management Program

("FedRAMP"). In January 2021, the global insurance brokerage Marsh named the Collective Defense platform as one of its industry- recognized Cyber Catalyst solutions. In February 2022, we earned from SE Labs Ltd. a AAA rating for Enterprise Advanced Security NDR Detection.

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

Increasingly, 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 broad 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, up from $124.2 billion in 2018. Even with increased cybersecurity spending, however, security outcomes have not substantially improved. The recent widespread SolarWinds/SUNBURST cyberattack is just one example of how a sophisticated adversary can thoroughly permeate an industry, geography or supply chain. 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 are 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.

Scarcity 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 overwhelm and burnout. The 2021 (ISC)² Cybersecurity Workforce Study, which provides two critical measures of the cybersecurity profession—the Cybersecurity Workforce Estimate and the Cybersecurity Workforce Gap, suggests that the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets. Despite estimates that there are 4.19 million cybersecurity professionals worldwide, the Cybersecurity Workforce Gap persists due to the accelerated evolution of the threat landscape and its impact on organizations' security practices.

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, they miss a large swath of dangerous threats that evade detection, as evidenced by the major SolarWinds/SUNBURST supply chain and Microsoft Exchange server attacks widely reported in the news media in 2020 and 2021.

Log and event management products

SIEMs and similar log management products are designed for compliance, reporting, and security incident management purposes, but they struggle with the scale and processing required to deliver the behavioral-analysis capabilities across current and historical data to detect new or modified versions of known threats. While these systems provide useful correlation capabilities, security operation teams are increasingly leveraging these systems for central aggregation points for workflow, ticketing, and case management, rather than for detection.

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.

Infrastructure monitoring/network performance monitoring and diagnostic-based products

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 team 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.

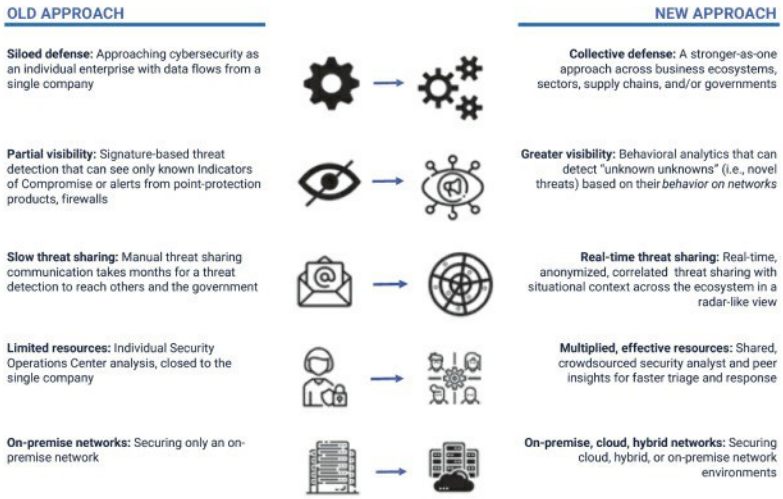
Reduce impact of cyber attacks with help from fellow cyber defenders

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:



A new cybersecurity model: from reactive, individual defense to proactive, Collective Defense

Our Solution: The Collective Defense Platform

Our Collective Defense platform comprises two tightly integrated proprietary technologies: Our NDR solution, IronDefense, and our innovative collective threat-sharing solution, IronDome.

Our Collective Defense 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. We can rapidly and cost effectively deploy in our customer's environments, 63% of which by revenue were in the public cloud as of January 31, 2022, but we also support private cloud and on-premise infrastructure. 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.

related 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, as was the case with the SolarWinds/SUNBURST attack.

Our Collective Defense platform comprises two flagship products:

ıDefense

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 AI/ML 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:

ıDefense 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.

ıDefense 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 preservice 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.

ıDefense 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.

ıDefense 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.

ıDefense 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 major cloud providers such as Amazon Web Services ("AWS") and Microsoft Azure deployments. 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.

ıDefense 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.

nDome

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:

nDome 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.

nDome 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 analysts 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.

nDome Cyber Radar View

IronDome creates a radar-like view of cyberspace 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, but is also available for private cloud, on-premise, and hybrid environments, and it is scalable to include small- medium businesses as well as multinational corporations.

eat Intelligence

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

nNet 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, threat intelligence rules, a snapshot of monthly correlated alerts, and threat research highlights.

Key Benefits of Our Solution

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.

avioral analytics that find threats that other tools cannot detect

uperior 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).

isibility 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.

ognitive 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.

ata 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.

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

he 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 response, 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. Approximately one-half of our cyber operations experts have NSA or U.S. Department of Defense experience, and 40% have cyber offensive, intel, or research experience.

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 can provide security protection across cloud, multi-cloud, on-premise, and virtual environments to support customers with different needs, however 63% of deployments by revenue as of January 31, 2022 were in the public cloud. Our public cloud partners include AWS and Microsoft Azure. We have private cloud options based on Nutanix for customers that want to leverage their own on-premise HCI environments. The on-premise deployment option is our hardware appliance or virtual application.

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 March 2022, IronNet was named by the U.S. Department of Homeland Security as a member of the Cybersecurity & Infrastructure Security Agency's ("CISA") recently formed Joint Cyber Defense Collaborative (JCDC). IronNet has 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 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 January 2021, the global insurance brokerage Marsh named the Collective Defense platform as one of its industry-recognized Cyber Catalyst solutions. This evaluation program is designed to help organizations make more informed choices about cybersecurity products and services to manage their cyber risk, by providing independent reviews conducted by insurers who fully understand the impact of risk exposure.

We have achieved “FedRAMP ready” status for Agency Authorization status, as approved by the FedRAMP. Our achievement of this status means the FedRAMP PMO has determined that we can meet the FedRAMP security requirements and could be granted an Authority to Operate from federal agencies.

GDPR- compliant

We are committed to data privacy and are compliant under the European Union (“EU”) General Data Protection Regulation (“GDPR”). We are also an active member of the EU/ Swiss-US Privacy Shield Framework through the U.S. Department of Commerce. The EU/Swiss-U.S. Privacy Shield Framework provides a method for companies to transfer personal data to the United States from the EU in a way that is consistent with EU law and acceptable under EU 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 I and SOC2 Type II

We are also SOC2/Type I and Type II certified, verifying that we have a suitable design of controls to meet the criteria for the security, availability, confidentiality, and processing integrity principles of the SOC2 standard. Having Type II attestation demonstrates the operational effectiveness of our design controls.

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).

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. Individual enterprises can choose to deploy our products and solutions using a variety of public and private cloud deployment options including AWS and Microsoft Azure. Enterprises that prefer to leverage their own private cloud infrastructure using hyper converged infrastructure can deploy our products and solutions through our partnership with Nutanix.

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 and Azure 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 Threat Intelligence Rules 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.

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.

Our Sales and Marketing

Sales

We use a "to and through" sales strategy. By maintaining a direct sales force consisting of senior-level account executives with deep security and high-tech experience, we have been able to leverage extensive professional networks and build inroads to strategic accounts. Because of this and the caliber of our senior leadership team, we believe we have a differentiated ability to convene CEOs, CISOs, and other leaders within an entire industry, such as energy company CEOs. This is what enables our cornerstone/community selling approach.

We have two sales teams in the United States: Public Sector, covering federal, state and local segments and Commercial covering both critical infrastructure (energy, oil & gas, and related segments) and enterprise (financial services, insurance, tech, and a variety of other sectors). We have direct sales staff in six countries, as well as a growing portfolio of channel, managed services and technology partners across the United States, EMEA, and Asia-Pacific regions to scale our ability to discover, qualify, and close business.

In addition, we have inside sales development teams to expand our selling capabilities. These teams focus on early qualification and development of opportunities that the inside sales development team will either close directly or transition to the field sales teams (for named accounts). These inside teams' primary objective is filling Collective Defense communities with smaller companies.

Marketing

Our marketing organization employs high-tech multichannel digital and content marketing for lead generation, aggressive public relations, social media and thought leadership programs to drive awareness, and specialization in strategies such as employee advocacy and search engine optimization. We were recently the top organic search engine result for "Network Detection and Response" in a competitive market.

Our public relations and media program has resulted in regular 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 sales strategy. We incorporate a combination of both large industry events like Black Hat with regional and sector-focused field marketing events that allow us to capture leads on new customers to build out Collective Defense communities. 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 Russia-Ukraine war, and other topics, which have been featured in media outlets. 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

- Azure
- GCP

SIEM

- Splunk
- IBM QRadar
- Microsoft Azure Sentinel LogRhythm

SOAR

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

ITSM

- ServiceNow

EDR

- CrowdStrike
- Carbon Black
- Forescout
- Tanium

NGFW

- Palo Alto Networks
- Checkpoint Software Technologies
- Zscaler

Go To Market ("GTM") Partners

With our GTM partners, we seek to accelerate service growth and value for their customers through a mutually beneficial program.

Raytheon Technologies

This partnership delivers cybersecurity solutions that defend against advanced threats that leverage behavior-based network traffic analysis and collective defense. The Raytheon-IronNet partnership combines our Collective Defense Platform with Raytheon's Managed Security Operations Center, Managed Detection and Response ("MDR") and Cyber Security Operations Center capabilities. This partnership delivers new analytical solutions that strengthen enterprise protection, along with a customized onboarding to integrate and operate the platform.

Accenture

We work with Accenture to help companies protect critical infrastructure by quickly deploying and updating a system of machine-speed, advanced threat analytics across IT and Operational Technology, which automatically filters out the noise of false positives with the insight provided by community sourced context. Accenture provides the expertise in scalable implementation when it orchestrates our collective defense platform, delivering actionable attack information in real-time for their customers to prevent impact to critical infrastructure.

MDR/MSSP Partners

Chosen channel partners work with us to develop and deliver an end-to-end solution designed to detect and prevent damaging and difficult-to-detect cyberattacks that continue to plague organizations across public and private sectors. For example, our partnership with Booz Allen Hamilton ("BAH") brings together unique capabilities, helping customers to navigate the complexities of the current threat landscape more easily. BAH provides a full spectrum of professional services including consulting, technical, scientific and project delivery for the government and private sector. The joint offering of BAH and our collective defense platform brings advancements in machine learning and AI, which provides innovative cyber defense detection to discover both known and unknown cyber threats, allowing a more thorough and effective approach to network security for their clients.

Our other integration and sales partners include Atlantic Data Forensics, Blacklake Security, Jacobs Engineering Group, Unlimited Technology, ArmorText, Carahsoft, Domain Tools, Ensign Infosecurity, Forescout and Global Cyber Alliance.

Our Research and Development

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 share 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.

Our 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;
- 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; and
- legacy network infrastructure and performance monitoring companies such as ExtraHop and Arista Networks, who are adding security use cases to their infrastructure products.

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.

Our 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 12, 2022, we had three issued patents and seven pending applications in the United States covering our technology, as well as 37 issued international patents, six pending international patent applications, and five filed PCT applications. Our issued patents expire between 2035 and 2037.

As of April 12, 2022, 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 or 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.

Our Facilities

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 also lease office space in Raleigh, North Carolina. 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. We believe that our existing facilities are sufficient for our current needs. In the future, we may need to add new facilities and expand our existing facilities as we add employees, grow our infrastructure and evolve our business, and we believe that suitable additional or substitute space will be available on commercially reasonable terms to meet our future needs.

Our Employees / 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.

As of January 31, 2022, we had 316 full-time employees. Of these employees, 93% are in the United States and 7% 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.

Our Diversity Ambassadors team's mission is to build a more diverse and inclusive company through clear and measurable goals across all levels and geographies, and encouraging and enabling all our employees to drive change and create an inclusive environment for everyone every day through educational, professional, and social programs. The mission of the Diversity Ambassadors is to establish a world-class program that continually delivers an accurate assessment of diversity, equity, and inclusion to decision makers across the company, and empowers us to operate in accordance with our values.

The Diversity Ambassador team seeks to achieve this vision by focusing on efforts that have been studied to show results, such as voluntary training, using disaggregated data to provide transparency into the fabric of our company, disassembling the employee lifecycle and re-engineering it so that all team members have equal access to a level playing field, targeting early talent recruiting, sponsorship, and creating employee-driven diversity teams.

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 welfare 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. Our gym reimbursement program in the United States further helps to support employees' physical well-being.

In response to the COVID-19 pandemic, we implemented significant changes in the best interest of employees as well as the communities in which we operate. This includes having the vast majority of our employees work from home, while implementing additional safety measures for employees continuing critical on-site work. We have also provided a work-from-home reimbursement program, as well as online classes and weekly newsletters to assist employees in that transition. To create a specific focus on the mental health and wellbeing of our employees, we created the "Unplug" program that provides several company- wide paid days off to help employees balance their work and life responsibilities. Additionally, to show a connection between IronNet and the employee, we also match their charitable contributions made to philanthropic organizations of their choice.

Employees have the opportunity to join two other Ambassador groups whose intent, among other things, is to promote a culture of community and increase comradery. The groups include 'Remote Worker' whose focus is to join employees together through activities and support a family oriented philosophy; and 'Philanthropy' whose purpose is to connect employees through charitable programs and initiative.

Growth and Development

We actively foster a learning culture where employees are empowered to drive their career progression, supporting professional development and providing on-demand learning platforms. Employees enjoy three company paid learning platforms, and our education reimbursement program offers each eligible employee an allowance for long-term undergraduate and graduate studies, as well as short-term professional development where each department is awarded a budget for career training. Additionally, IronNet sponsors various leadership training opportunities through outside vendors as well as group technical training sessions. We host all-employee monthly brown-bag learning sessions which include topics from time management to tricks in Excel. Our monthly newsletter is full of other suggested training opportunities within our hosted portals. Career Development Plans have been curated for each member of our technical and security groups to allow them a clear line of sight between where they are now within their career at IronNet, where they could be, and what steps they should take to excel to the next level. Our internship program is available on an annual basis where college students are invited to participate in learning and mentorship opportunities with the hopes of full-time employment after graduation. Our development programs play a critical role in engaging and retaining our employees as these programs offer opportunities to continually enhance their skills for a variety of career opportunities across the company.

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. IronNet strives 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 of 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.

ITEM 1A. RISK FACTORS

RISK FACTORS

Investing in our common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below together with all of the

other information contained in this Annual Report on Form 10-K, including our financial statements and related notes appearing elsewhere in this Annual Report on Form 10-K and in the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations," before deciding to invest in our common stock. If any of the events or developments described below were to occur, our business, prospects, operating results and financial condition could suffer materially, the trading price of our common stock could decline, and you could lose all or part of your investment. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties not presently known to us or that we currently believe to be immaterial may also adversely affect our business.

Risks Related to Our Business and Industry

We have experienced rapid growth in recent periods, and if we do not manage our future growth, our business and results of operations will be adversely affected.

We have experienced rapid revenue growth in recent periods we expect to continue to invest broadly across our organization to support our growth. For example, our headcount grew from 246 full-time employees as of January 31, 2021 to 316 full-time employees as of January 31, 2022. Although we have experienced rapid growth historically, we may not be able sustain our current growth rates, nor can we assure you that our investments to support our growth will be successful. The growth and expansion of our business will require us to invest significant financial and operational resources and the continuous dedication of our management team. We have encountered and will continue to encounter, risks and difficulties frequently experienced by rapidly growing companies in evolving industries, including market acceptance of our products, adding new customers, intense competition, and our ability to manage our costs and operating expenses. Our future success will depend in part on our ability to manage our growth effectively, which will require us to, among other things:

- effectively attract, integrate and retain a large number of new employees, particularly members of our sales and marketing, data science, and research and development teams;
- further improve our platform and products, including our cloud modules and security capabilities, analytics, collective defense capabilities, and visualizations, and IT infrastructure, including expanding and optimizing our data centers, collection, and analytic capabilities, to support our business needs;
- enhance our information and communication systems to ensure that our employees and offices around the world are well coordinated and can effectively communicate with each other and our growing base of customers and partners; and
- improve our financial, management, and compliance systems and controls.

If we fail to achieve these objectives effectively, our ability to manage our expected growth, ensure uninterrupted operation of our platform and key business systems, and comply with the rules and regulations applicable to our business could be impaired. Additionally, the quality of our platform and services could suffer and we may not be able to adequately address competitive challenges. Any of the foregoing could adversely affect our business, results of operations, and financial condition.

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 $242.6 million and $55.4 million for fiscal 2022 and fiscal 2021, respectively. As of January 31, 2022, we had an accumulated deficit of $417.7 million. While we have experienced significant growth in revenue in recent periods, we cannot predict when or whether we will reach or maintain profitability. We also expect our operating expenses to increase over our historical expenses in the future as we continue to invest for future growth, which will negatively affect our results of operations if our total revenue does not increase. We cannot assure you that these investments will result in substantial increases in our total revenue or improvements in our results of operations. In addition to the anticipated costs to grow our business, we also expect to incur significant additional legal, accounting, and other expenses as a newly 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.

Our limited 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 in 2016, IronDefense, and our first collective defense product in 2018, IronDome. 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 operated in a more predictable market.

The COVID-19 pandemic could adversely affect our business, operating results and future revenue.

The ongoing COVID-19 pandemic has and may continue to impact worldwide economic activity and financial markets. Some of the precautionary measures taken at the outset of the pandemic, many of which we have now made largely permanent and sustainable, and associated economic issues, both in the United States and across the globe, could negatively affect our cybersecurity efforts, significantly delay and lengthen our sales cycles, impact our sales and marketing efforts, reduce employee efficiency and productivity, slow our international expansion efforts, increase cybersecurity risks, and create operational or other challenges, any of which could harm our business and results of operations. Moreover, due to our subscription-based business model, the effect of the COVID-19 pandemic may not be fully reflected in our results of operations until future periods, if at all.

In addition, the COVID-19 pandemic, and variants thereof, may disrupt the operations of our prospective clients, customers, and partners for an indefinite period of time. Some of our customers have been negatively impacted by the COVID-19 pandemic, which could result in delays in accounts receivable collection, or result in decreased technology spending, including spending on cybersecurity, which could negatively affect our revenues. Some of our prospective clients have also been negatively impacted by the COVID-19 pandemic, which could result in delays in sales or lengthen purchasing decisions.

More generally, the COVID-19 pandemic, including the emergence of variant strains of COVID-19, has adversely affected economies and financial markets globally, and continued uncertainty could lead to a prolonged economic downturn, which could result in a larger customer turnover than is currently anticipated, reduced demand for our products and services, and increased length of sales cycles, in which case our revenues could be significantly impacted. The impact of the COVID-19 pandemic may also exacerbate other risks discussed in this "Risk Factors" section and elsewhere in this Annual Report on Form 10-K. It is not possible at this time to estimate the impact that the COVID-19 pandemic could have on our business, as the impact will depend on future developments, which are highly uncertain and cannot be predicted.

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 retention rates, or decreased sales. 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, including a downturn due to the outbreak of diseases such as COVID-19, 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 expands 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, 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. 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 clients' 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 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; and

•legacy network infrastructure and performance monitoring companies such as ExtraHop and Arista Networks, who are adding security use cases to their infrastructure products.

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 or data are or 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 entirely 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 serves our customers using a mix of third-party data centers, primarily AWS and Microsoft Azure, 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 factors as some of them 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 expand and 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 recruiting, training and retaining sufficient numbers of sales personnel, particularly in international markets. We have expanded our sales organization significantly in recent periods and expect to continue to add additional sales capabilities in the near term. There is significant competition for sales personnel with the skills and technical knowledge that we require. New hires require significant training and may take significant time before they achieve full productivity, and this delay is accentuated by our long sales cycles. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain 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. We cannot predict whether, or to what extent, our sales will increase as we expand our sales force or

how long it will take for sales personnel to become productive. If we are unable to hire and 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 or upturns 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%, or $13,975, with two of those customers accounting for 21% of our revenue, and for fiscal year 2021, six customers accounted for 46%, or $13,381, with one of those customers accounting for 10%, of our revenue. Significant customers are those which represent at least 10% of our total revenue at each respective period ending date. The following table presents customers that represented 10% or more of our total annual revenue:

	Year Ended January 31,	
	2022	2021
Customer A	*	10%
Customer B	11%	*
Customer C	10%	*
	21%	10%

* Less than 10%

As a result of this customer concentration, 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:

- the impact of the COVID-19 pandemic, including the emergence of variant strains of COVID-19, on our operations, financial results, and liquidity and capital resources, including on customers, sales, expenses, and employees;
- 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;
- our ability to successfully expand our business domestically and internationally;
- 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;
- 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.

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.

We rely heavily on the services of our senior management team, and if we are not successful in attracting or retaining senior management personnel, we may not be able to successfully implement our business strategy.

Our future success will be substantially dependent on our ability to attract, retain, and motivate the members of our management team. In particular, we will be highly dependent on the services of our co-chief executive officers, who will be critical to our future vision and strategic direction. We will also rely on our leadership team in the areas of operations, security, analytics, engineering, product management, research and development, marketing, sales, partnerships, mergers and acquisitions, support, and general and administrative functions. Gen Alexander, our founder, is important to our future growth as he provides access to key decisionmakers within government agencies and the private sector, and his leadership role would be difficult to replace. Although we expect that we will enter into new employment agreements with some of our key personnel, our employees, including our executive officers, will be employed on an "at-will" basis, which means they may terminate their employment with us at any time. If one or more of our key employees resigns or otherwise ceases to provide us with their service, our business could be harmed.

If we are unable to attract and retain qualified personnel, our business could be harmed.

There is significant competition for personnel with the skills 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. Although we anticipate that they may increase in the future, 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;
- 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 locations that meet these requirements, affecting our ability to sell these products to governmental agencies.

We have achieved "FedRAMP- ready" status, but such status is only available for a certain period of time before which it must be utilized. If not utilized, we would likely have to go through certain parts of the FedRAMP process again in order to sell our products to government agencies. Moreover, even if we were to achieve FedRAMP-certified 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 costs, our business, results of operations and financial condition may be adversely affected. Although we expect that we could 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 relevant technology. If we are prevented from using 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 against 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 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. Despite our efforts to attempt to comply with the GDPR, a regulator may determine that a customer has not done so and subject it to fines and public censure, which could harm our business.

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 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 will take 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 will take 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 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), 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 have been incorrectly 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 UK 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 could expose us to security vulnerabilities.

Some open source licenses contain requirements that we make available source code for modifications or derivative works we create based upon the type of open source software we use. If we combine 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 we 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. We have not to date received any indemnification claims from third parties. However, 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 our 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 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 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, and we are likely to continue to complete, investments in and/or acquisitions of complementary companies, services, or technologies. The 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 incurrence 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.

If we cannot maintain our company culture as we grow, we could lose the innovation, teamwork, passion and focus on execution that have contributed to our success, and our business may be harmed.

We believe that our corporate culture has been a contributor to our success, which we believe fosters innovation, teamwork, passion and focus on building and marketing our platform. As we grow and develop the infrastructure of a public operating company, it may be difficult to maintain our corporate culture. Any failure to preserve that culture could harm our future success, including our ability to retain and recruit personnel, innovate and operate effectively and execute on our business strategy. Additionally, our productivity and the quality of our solutions may be adversely affected if we do not integrate and train new employees quickly and effectively. If we experience any of these effects in connection with future growth, it could impair our ability to attract new customers, retain existing customers and expand their use of our platform, all of which would adversely affect our business, financial condition and results of operations.

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.

We derived 10% and 7% of our total revenue from our international customers for fiscal 2022 and fiscal 2021, respectively. Our growth strategy includes expansion into target geographies, but there is no guarantee that such efforts will be successful. We expect that our international activities will continue to grow in the future, as we continue to pursue opportunities in international markets. 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.

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.

As we continue to develop and grow our business globally, our success will depend in large part on our ability to anticipate and effectively manage these risks. The expansion of our existing 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, 2022 and January 31, 2021, we had aggregate U.S. federal and state net operating loss carryforwards of $324.8 million and $154.6 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 (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 report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. Our intercompany relationships will be subject to complex transfer pricing regulations administered by 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 relating to 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, fraudulent use attempts 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 and terrorist acts.

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 identified material weaknesses in our internal control over financial reporting, which resulted in a restatement of our unaudited condensed consolidated financial statements as of and for the period ended October 31, 2021. 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 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 the Company's outstanding restricted stock units ("RSUs") 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. 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.

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 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 43% of our outstanding common stock as of January 31, 2022. 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 attestation 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 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.

Our management has limited experience in operating a public company.

Our executive officers have limited experience in the management of a publicly traded company. Our management team may not successfully or effectively manage our transition to a public company that will be subject to significant regulatory oversight and reporting obligations under federal securities laws. Our limited experience in dealing with the increasingly complex laws pertaining to public companies could be a significant disadvantage in that we are likely that an increasing amount of their time may be devoted to these activities, which will result in less time being devoted to the management and our growth. We may not have adequate personnel with the appropriate level of knowledge, experience, and training in the accounting policies, practices or internal control over financial reporting required of public companies in the United States. The development and implementation of the standards and controls necessary for us to achieve the level of accounting standards required of a public company in the United States may require costs greater than expected. It is possible that we will be required to expand its employee base and hire additional employees to support our operations as a public company, which will increase our operating costs in future periods.

Future sales, or the perception of future sales, could cause the market price of our common stock to drop significantly, even if our business is doing well.

Sales of a substantial number of shares of our common stock in the public market could occur at any time. These sales, or the perception in the market that members of our management or holders of a large number of shares intend to sell shares, could reduce the market price of our common stock.

Our warrants, if exercised, would increase the number of shares eligible for future resale in the public market and result in dilution to stockholders, which may have an adverse effect on the market price of our common stock.

We have warrants outstanding to purchase an aggregate of approximately 8.6 million shares of our common stock at $11.50 per share, subject to adjustment. To the extent the warrants are exercised, it will increase the number of issued and outstanding shares of common stock, which will result in dilution to our stockholders and increase the number of shares eligible for resale in the public market. Sales of substantial numbers of such shares in the public market could adversely affect the market price of our common stock.

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 securities in the future without your approval. For example, under our equity incentive plans, we may issue a significant number of shares of common stock, both upon the exercise of currently outstanding stock options and settlement of currently outstanding restricted stock units, as well as the exercise of stock options or settlement of restricted stock units that we may grant from time to time under these plans. 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 sell shares of common stock to Tumim Stone Capital LLC ("Tumim") under a common stock purchase agreement that we entered into with Tumim in February 2022 (the "Purchase Agreement") at prices which will fluctuate based on the price of our common stock. Depending on market liquidity at the time, sales of such shares may cause the trading price of our common stock to fall. If and when we do sell shares to Tumim, after Tumim has acquired the shares, Tumim may resell all, some, or none of those shares at any time or from time to time in its discretion. Therefore, sales to Tumim by us could result in substantial dilution to the interests of other holders of our common stock. Additionally, the sale of a substantial number of shares of our common stock to Tumim, or the anticipation of such sales, could make it more difficult for us to sell equity or equity-related securities in the future at a time and at a price that we might otherwise wish to effect sales.

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 behalf of our company, (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 NYSE, 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 to 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 the 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 also lease office space in Raleigh, North Carolina. 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.

We believe that our existing facilities are sufficient for our current needs. In the future, we may need to add new facilities and expand our existing facilities as we add employees, grow our infrastructure and evolve our business, and we believe 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. 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, captioned Grad v. IronNet, Inc., et al., No. 1:22-cv-004499 (E.D. Va.), was filed by our purported stockholder in the United States District Court for the Eastern District of Virginia on behalf of a proposed class consisting of those who acquired our securities between September 15, 2021 and December 20, 2021. The complaint names us, our co-CEOs, and our CFO as defendants and asserts claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934, as amended, for alleged misrepresentations and/or omissions in a September 14, 2021 press release regarding our business and financial prospects, our ability to predict the timing of significant customer opportunities, and our disclosure controls and procedures. The complaint seeks an unspecified amount of damages on behalf of the putative class and an award of costs and expenses, including reasonable attorneys' fees. 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 estimate reasonably possible losses or determine whether an unfavorable outcome is probable.

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. Prior to the consummation of the Business Combination, our common stock and our Public Warrants were listed on NYSE under the symbols "DFNS" and "DFNS.WS," respectively.

Holders

As of April 15, 2022, there were 383 holders of record of the common stock and three 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

In connection with Legacy LGL's initial public offering (the "Initial Public Offering"), Legacy LGL issued an aggregate of 5,200,000 warrants (the "Private Warrants") at a price of $1.00 per Private Warrant. Following the Business Combination, each Private Warrant entitled the holder to purchase one share of our common stock at $11.50 per share. In September and October 2021, 5,189,800 of the Private Warrants were exercised on a cashless basis in exchange for 3,188,229 shares of our common stock. The issuance of these shares was exempt from registration pursuant to Section 3(a)(9) of the Securities Act.

ITEM 6. [RESERVED]

ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

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, 2022 and January 31, 2021 are referred to herein as fiscal year 2022 and fiscal year 2021, 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 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 hire additional personnel and 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 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.

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. We compliment these capabilities, delivered to both commercial and public sector enterprises, with professional services.

Software, Subscription and Support

Our primary line of business is the delivery of our integrated software capabilities through our Collective Defense platform. The platform is comprised of 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 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 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 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 largely cloud-deployed (public or private), though it is also available in on-premise and hybrid environments, and is scalable to include small-to-medium businesses and public-sector agencies as well as multinational corporations. 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 CS 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 68% of our revenue for the year ended January 31, 2022 related to deployments involving our key public cloud providers Amazon Web Services and Microsoft Azure. We also support private cloud, or 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 APIs that enable integrations with standard security products, including SIEM, SOAR, EDR, NGFW tools, and cloud-native logs from the major public cloud providers.

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, 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. Transaction costs associated with the issuance of the PIPE shares were $21.2 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.

During fiscal year 2022, we incurred a net loss of $242.6 million, of which $156.6 million related to a non-cash expense related to the modification of Restricted Stock Units, as well as a further non-cash expense to reflect the increase in fair market value in Private Warrants through the dates they were exercised, and used $83.7 million in cash to fund our operations. As of January 31, 2022, we had $47.7 million of cash on hand to continue to fund operations.

We expect our capital and operating expenditures to increase in connection with our ongoing activities, as we:

1. continue to invest in research and development related to new technologies;
2. increase our investment in marketing and advertising, as well as the sales and distribution infrastructure for its products and services;
3. maintain and improve operational, financial, and management information systems;
4. hire additional personnel;
5. obtain, maintain, expand, and protect our intellectual property portfolio; and
6. enhance internal functions to support our operations as a publicly-traded company.

Key Factors Affecting Our Performance

New customer acquisition

Our future growth depends in large part on our ability to acquire new customers. If our efforts to attract new customers are not successful, our revenue may decline in the future. Our IronDefense and IronDome platforms are designed to be used in conjunction with point solutions to capture and share critical data and findings to enable our behavioral analytics to identify threats and for defenders to respond more accurately and quickly. We believe that we have significant room to capture additional market share and intend to continue to invest in sales and marketing to engage our prospective customers, increase brand awareness, and drive adoption of our solution.

Customer retention

Our ability to increase revenue depends in large part on our ability to retain existing customers.

Investing in business growth

Since inception, we have invested significantly in the growth of our business. While remaining judicious and targeted in our investments, we intend to continue to invest in our research and development team to lead product improvements, our sales team to broaden our brand awareness and our general and administrative expenses to increase for the foreseeable future given the additional expenses for finance, compliance and investor relations as we grow as a public company. In addition to our internal growth, we may also consider acquisitions of businesses, technologies, and assets that complement and bolster additional capabilities to our product offerings.

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. We have a history of growing the number of customers who have contracted for our platforms on a recurring basis, which does not include our professional services customers. 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. We have consistently increased the number of such customers period-over-period, and we expect this trend to continue as we increase subscription offerings to small and medium-sized businesses, in addition to increased subscription offerings for our larger enterprise customers. The following table sets forth the number of recurring software customers as of the dates presented:

	January 31,	
	2022	**2021**
Recurring Software Customers	88	27
Year-over-year growth	226 %	35 %

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:

	January 31,	
	2022	**2021**
	($ in millions)	
Annual recurring revenues	$ 31.8	$ 25.8
Year-over-year growth	23 %	72 %

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 2022 and 2021, as applicable.

b. Denominator: We use the revenue attributable to software and product customers for fiscal year 2022 and fiscal year 2021 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 decreased from 2.9 to 2.7 years, or (7)%, for the year ended January 31, 2022 as compared to fiscal year 2021. As our revenues and our customer base increases, we expect our average contract length to trend downward over time. Declines in average contract length are not reflective of the average lifetime of a customer.

	January 31,	
	2022	**2021**
	(in years)	
Dollar-based average contract length	2.7	2.9

Calculated Billings

Calculated billings is a non-GAAP financial measure that we believe is a key metric to measure our periodic performance. Calculated billings represent our total revenue plus the change in deferred revenue in a period. Calculated billings in any particular period aims to reflect amounts invoiced or invoiceable to customers to access our software-based, cybersecurity analytics products, cloud platform and professional services, together with related support services, for our new and existing customers. We typically invoice our customers on multi-year or annual contracts in advance, either annually or monthly.

Calculated billings decreased $15.8 million, or (37)%, for fiscal year 2022 as compared to fiscal year 2021, primarily due to the timing of unusually high multi-year contract billings during the latter half of fiscal year 2021 as we typically invoice customers multi-year or annually in advance and, to a lesser extent, monthly in advance.

While we believe that calculated billings may be helpful to investors because it provides insight into the cash that will be generated from sales of our subscriptions, this metric may vary from period-to-period for a number of reasons, and therefore has a number of limitations as a quarter-to-quarter or year-over-year comparative 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:

	Year Ended January 31,			
	2022	**2021**	**2022 vs 2021**	
	($ in millions)			
Revenue	$ 27.5	$ 29.2	$ (1.7)	(6)%
Add: Total Deferred revenue, end of period	33.6	34.0	(0.4)	-1
Less: Total Deferred revenue, beginning of period	34.0	20.3	13.7	67
Calculated billings	$ 27.1	$ 42.9	$ (15.8)	(37)%

Adjusted Net Loss

The following table shows our Adjusted Net Loss, a non-GAAP measure, for fiscal year 2022, 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. These expenses were nonexistent as of January 31,2021:

	For the Year Ended January 31, 2022
	($ in thousands)
Net loss	$ (242,647)
Stock compensation expense (1)	156,596
Change in fair value of warrants liabilities	11,265
Transaction costs expense (2)	3,166
Adjusted Net Loss	$ (71,620)

1. Total stock based compensation of $156.6 million has been recorded within research and development of $22.9 million, sales and marketing of $51.8 million, and general and administrative expense of $81.9 million on the statement of operations

2. Transaction expenses have been recorded within general and administrative expense on the statement of operations

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 92% of our revenue in fiscal year 2022 and for 85% of our revenue in fiscal year 2021. Professional services revenues accounted for 8% of our revenue in fiscal year 2022 as compared to 15% in fiscal year 2021.

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 IronDome collective defense software solution that provides them access to IronNet's collective defense infrastructure linking participating stakeholders. As a result, 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. Significant 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, employee-related costs of our customer facing support, such as salaries, bonuses and benefits, an allocated portion of administrative costs and the amortization of deferred costs.

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 significant lead generator for 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.

We intend to continue to make significant investments in our sales and marketing organization to drive additional revenue, further penetrate the market and expand our global customer base. In particular, we will continue to invest in growing and training our sales force, broadening our brand awareness and expanding and deepening our channel partner relationships. We expect our sales and marketing expenses to decrease as a percentage of our revenue over the long term, although our sales and marketing expenses may fluctuate as a percentage of our revenue from period to period due to the timing and extent of these expenses.

G*eneral 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.

We expect that general and administrative expenses will increase in absolute dollars as we hire additional personnel and enhance our systems, processes, and controls to support the growth in our business as well as our increased compliance and reporting requirements as a public company.

Other income

Other income consists primarily of interest income

Other expense

Other expense consists primarily of interest expense and foreign currency exchange losses.

Change in fair value of warrants liabilities

Change in fair value of warrants liabilities consists of the change in the fair value of warrants between the time on which they were valued as of the prior quarterly reporting period and the date on which they were exercised.

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 2022 and Fiscal Year 2021

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:

	Fiscal Year Ended January 31,				2022 vs 2021	
	2022		2021		Change $	Change %
	($ in thousands)					
Product, subscription and support revenue	$ 25,347	92 %	$ 24,701	85 %	$ 646	3 %
Professional services revenue	2,197	8 %	4,526	15 %	(2,329)	(51)%
Total revenue	27,544	100 %	29,227	100 %	(1,683)	(6)%
Cost of product, subscription and support revenue	8,225	30 %	5,393	18 %	2,832	53 %
Cost of professional services revenue	1,158	4 %	1,629	5 %	(471)	(29)%
Total cost of revenue	9,383	34 %	7,022	24 %	2,361	34 %
Gross profit	18,161	66 %	22,205	76 %	(4,044)	(18)%
Operating expenses						
Research and development	52,899	192 %	25,754	88 %	27,145	105 %
Sales and marketing	82,922	301 %	30,381	104 %	52,541	173 %
General and administrative	112,099	407 %	21,347	73 %	90,752	425 %
Total operating expenses	247,920	900 %	77,482	265 %	170,438	220 %
Operating loss	(229,759)	-834 %	(55,277)	-189 %	(174,482)	316 %
Other income	25	0 %	71	0 %	(46)	(65)%
Other expense	(1,183)	-4 %	(90)	0 %	(1,093)	1,214 %
Change in fair value of warrants liabilities	(11,265)	-41 %	-	0 %	(11,265)	100 %
Loss before income taxes	(242,182)	-879 %	(55,296)	-189 %	(186,886)	338 %
Provision for income taxes	(465)	-2 %	(77)	0 %	(388)	504 %
Net loss	$ (242,647)	-881 %	$ (55,373)	-190 %	$ (187,274)	338 %

Revenue

Total revenue decreased by $1.7 million or (6)% in fiscal year 2022 compared to fiscal year 2021.

Product, subscription and support revenue increased by $0.6 million primarily due to the net effect of the Company's transition from contracts that had material non-recurring elements which would 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 $2.3 million or (51)% in fiscal year 2022 compared to fiscal year 2021, primarily due to the completion of a national cybersecurity strategy engagement in EMEA and a key enterprise engagement, in fiscal year 2021. Professional services accounted for 8% of our total revenue in fiscal year 2022 and 15% of our total revenue in fiscal year 2021.

Cost of revenue

Total cost of revenue increased by $2.4 million or 34%, in fiscal year 2022, compared to fiscal year 2021. Cost of product, subscription and support revenue increased by $2.8 million or 53%, in fiscal year 2022, compared to fiscal year 2021. The increase was due primarily to an increase in customer count during fiscal year 2022 as compared to fiscal year 2021, as well as costs incurred to fully ramp cloud hosting environments related to a significant revenue customer that was onboarded in fiscal year 2021, and a $0.7 million charge due to one-time product, subscription and support cost adjustments.

Cost of professional service revenue decreased by $0.5 million or (29)% in fiscal year 2022, compared to fiscal year 2021. The decrease in cost of service revenue was primarily due to a decrease in overall professional services revenue in 2022 compared to fiscal year 2021.

Gross Profit and Gross Margin

Customer mix changes resulted in a decrease in software gross margin to 68% in fiscal year 2022 compared to 78% in fiscal year 2021, and a decrease in professional services gross margin to 47% in fiscal year 2022 as compared to 64% in fiscal year 2021. The decrease in margin in fiscal year 2022 as compared to 2021 for software was primarily the result of onboarding a significant revenue customer in fiscal year 2021 which did not fully ramp their cloud costs until fiscal year 2022, and the delivery of a key significant service contract in EMEA in fiscal year 2021. Professional services margin will continue to be volatile contract to contract as we scale our business.

We expect that gross margins will improve in the near term. The in-period effect of the one-time adjustments to product, subscription and support gross margin related to an amortization catch-up for deployed sensors of $0.7 million was 2.0% impact to gross margin in fiscal year 2022. Margins may remain volatile compared to fiscal year 2021 due to the continuing presence of large contracts in our revenue mix.
The following tables show gross profit and gross margin, respectively, for software products and support revenue and professional services revenue for fiscal year 2022 as compared to fiscal year 2021.

	Fiscal Year Ended January 31,		2022 vs 2021	
	2022	2021	Change $	Change %
	($ in thousands)			
Product, subscription and support gross profit	$ 17,122	$ 19,308	$ (2,186)	(11)%
Professional services profit	1,039	2,897	(1,858)	(64)%
Total gross profit	$ 18,161	$ 22,205	$ (4,044)	(18)%

	2022	2021	Change
Product, subscription and support margin	67.6 %	78.2 %	(10.6)%
Professional services margin	47.3 %	64.0 %	(16.7)%
Total gross margin	65.9 %	76.0 %	(10.1)%

Operating expenses

Research and development

Research and development expenses increased by $27.1 million or 105%, in fiscal year 2022, compared to fiscal year 2021, primarily as the result of non-cash stock compensation expenses of $22.9 million, which was triggered by the modification of the restricted stock units. The remaining increase of $4.2 million was driven by the ramping of external costs to support product development and the increase in internal headcount, with some increase driven by cloud computing costs.

Overall research and development expenditure was 192% of total revenues in fiscal year 2022 as compared to 88% in fiscal year 2021, with the increase primarily being driven by an increase in non-cash stock compensation expense. We expect that our overall research and development expenditure rate as a percentage of revenues will decline in the future as compared to fiscal year 2022.

Sales and marketing

Sales and marketing expenses increased by $52.5 million or 173% in fiscal year 2022 as compared to fiscal year 2021, primarily as the result of non-cash stock compensation expenses of $51.8 million, which was triggered by the modification of the restricted stock units. The remaining increase of $0.7 million is due to the expansion of sales and marketing efforts as the Company is focused on growth.

Overall sales and marketing expenditure was 301% of total revenues in fiscal year 2022 as compared to 104% in fiscal year 2021, with the increase primarily being driven by the increase in non-cash stock compensation expense. We expect that our overall sales and marketing expenditure rate as a percentage of revenues will decline in the future as compared to fiscal year 2022.

General and administrative

General and administrative expenses increased by $90.8 million or 425% in fiscal year 2022, as compared to fiscal year 2021, primarily due to non-cash stock compensation expenses of $81.9 million, which was triggered by the modification of the restricted stock units. The remaining increase of $8.9 million was the result of an increase in costs related to becoming a publicly traded company and the overall efforts to grow and support business operations, including increased headcount, directors and officers insurance costs, and the implementation of systems to support operations as a public company.

Overall general and administrative expense was 407% of total revenues in fiscal year 2022 as compared to 73% in fiscal year 2021, with the increase primarily being driven by the increase in non-cash stock compensation expense. We expect that our overall G&A expenditure rate as a percentage of revenues will decline in the future.

Other income

Other income decreased by $46 thousand or (65)% in fiscal year 2022, compared to fiscal year 2021, primarily as the result of interest income.

Other expense

Other expense decreased by $1.1 million or 1,214% in fiscal year 2022, compared to fiscal year 2021, primarily as the result of interest expense related to loans outstanding during the year. These debts and the interest were paid off at the date of the Merger.

Change in fair value of warrants liabilities

Simultaneously with the closing of the Initial Public Offering, LGL Systems Acquisition Holding Company, LLC, a Delaware limited liability company, purchased an aggregate of 5,200,000 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 Initial 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 Initial 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 warrants issued by Legacy LGL, our legal predecessor, to purchase its common stock in a private placement concurrently with its Initial Public Offering (the "Private Warrants"), were evaluated under ASC 815-40, Derivatives and Hedging—Contracts in Entity's Own Equity, and it was determined that they do not meet the criteria to be classified as stockholders' equity, and as such will be accounted for as liabilities, as further discussed in Note 1 of the notes to our consolidated financial statements included in this Form 10-K.

For the private warrants that have been exercised since the date of the Merger, the change in fair value of warrants liabilities consists of the change in fair value between the date on which they were valued, which is the date of the Merger, through the date on which they were exercised. The change in fair value of warrant liabilities for those private warrants that remain outstanding at the end of fiscal year 2022 consists of the change in fair value between the date of the Merger and January 31, 2022.

Provision for income taxes

The change in provision for income taxes was immaterial to the results of operations primarily due to our continued net loss position, the accumulation of net loss carryforwards, and offsetting valuation allowance.

Liquidity and Capital Resources

Sources of Liquidity

We have incurred losses and negative cash flows from operations since inception. Through January 31, 2022, 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, loans, and receipts from sales of our products and services to customers in the ordinary course of business. As of January 31, 2022, we had cash and cash equivalents of $47.7 million, with no debt outstanding as of the end of the fiscal year. As of January 31, 2021, we had $31.5 million cash and cash equivalents and $5.6 million loans payable.

As of January 31, 2022, we had approximately 8.6 million Warrants outstanding. Each Warrant is exercisable to purchase one share of common stock at $11.50 per share. Assuming the exercise in full of all of the Warrants for cash, we would receive up to an aggregate of approximately $99 million from the exercise of the Warrants. However, there can be no assurances that the Warrants will ever be exercised or that we will receive any proceeds from the exercise thereof.

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 have filed with the SEC the registration statement to register for resale under the Securities Act, the shares of common stock that have been and 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 $1.75 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 initial satisfaction of all conditions to Tumim's purchase obligations set forth in the Purchase Agreement (the "Commencement," and the date on which the Commencement occurs, the "Commencement Date"), including that the registration statement covering the resale by Tumim of shares of common stock that have been and may be issued under the Purchase Agreement is declared effective by the SEC. From and after the Commencement Date, we will 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 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 a (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 (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.

Long- Term Liquidity Requirements

Based on our growth plan, we believe that our cash on hand and collectable receivables, the cash generated from sales of our products and services and proceeds from the Tumim Stone Capital committed financing will satisfy our working capital and capital requirements for at least the next twelve months. See Note 1 and Note 17 in the accompanying Notes to the Consolidated Financial Statements, respectively, for our going concern assessment and discussion of the terms of the equity line.

Following the closing of the Merger, we no longer have any indebtedness, as all amounts then outstanding were repaid.

Our future capital requirements will depend on many factors, including, but not limited to the rate of our growth, our ability to attract and retain customers and their willingness and ability to pay for our products and services, and the timing and extent of spending to support our efforts to market and develop our products. Further, we may enter into future arrangements to acquire or invest in businesses, products, services, strategic partnerships, and technologies. As such, we may be required to seek additional equity or debt financing. In the event that additional financing is required from outside sources, we may not be able to raise it on terms acceptable to us or at all. If additional funds are not available to us on acceptable terms, or at all, our business, financial condition, and results of operations could be adversely affected.

Cash Flows

For Fiscal Year 2022 and Fiscal Year 2021

The following table summarizes our cash flows for the periods presented:

	Year Ended January 31,	
	2022	**2021**
	(in millions)	
Net cash used in operating activities	$ (83.7)	$ (42.7)
Net cash (used in) provided by investing activities	$ (3.9)	$ 0.1
Net cash provided by financing activities	$ 103.4	$ 63.3

Operating Activities

Net cash used in operating activities during fiscal year 2022 was $(83.7) million, which resulted from a net loss of $(242.6) million, primarily driven by the modification of the restricted stock units awards of $156.6 million and related non-cash expenses. There was also an increase in the fair value of warrants liabilities of $11.3 million and an increase in accrued expenses. This was offset by an increase in accounts receivable of $3.2 million, attributable to higher than usual, multi-year cash prepayments received in 2021 as compared to the current year, and an increase in inventory of $0.5 million. We also saw a decrease in services revenue and increases in cost of sales totaling approximately $2.8 million as more customers' analytics came more fully online during 2022.

Net cash used in operating activities during fiscal year 2021 was $(42.7) million, which resulted from a net loss of $(55.4) million, primarily driven by growth-related operating expenses exceeding gross profits from sales, adjusted for non-cash charges of $1.4 million and net cash inflows of $11.3 million from changes in operating assets and liabilities. Non-cash charges primarily consisted of $1.2 million of depreciation and amortization expense, $0.2 million in losses on the sale of fixed assets as the result of the closure of facilities, offset by a net credit in stock-based compensation expense due to increased forfeiture rates in fiscal 2021. Cash used in operating activities during fiscal year 2021 benefited from the change in deferred revenue of $13.7 million, offset by a decrease in accounts receivable of $3.4 million, which were the result of timing of new customer contracts.

Investing Activities

Net cash used in investing activities during fiscal year 2022 of $(3.9) million was primarily due to $(3.9) million in purchases of property and equipment.

Net cash provided by investing activities during fiscal year 2021 of $0.1 million was primarily due to $1.0 million in proceeds from the maturity of

investments and $0.1 million in proceeds from the sale of property and equipment offset by $1.0 million in purchases of property and equipment.

Financing Activities

Net cash provided by financing activities of $103.4 million during fiscal year 2022 was primarily due to gross proceeds from the Merger recapitalization of $13.3 million and issuance of PIPE Shares of $125.0 million and bank borrowings of $15.0 million, offset by loan repayments of $5.6 million.

Net cash provided by financing activities of $63.3 million during fiscal year 2021 was primarily due to net proceeds from our sale of preferred stock of $57.4 million, the net proceeds from loans of $5.6 million and the issuance of common stock, including upon exercise of stock options by employees of $0.3 million.

Contractual obligations

Our principal commitments consist of lease obligations for office space. As of January 31, 2022, we had lease payment obligations of $4.0 million, of which $1.0 million is payable within twelve months. For more information regarding our lease obligations, see Note 12, Commitments and Contingencies to the consolidated financial statements.

During fiscal year 2022 and in future years, we have made and expect to continue to make additional investments in our product, scale our operations, and continue to enhance our security measures. We will continue to expand the use of software systems to scale with our overall growth.

Critical Accounting Policies and Estimates

Our financial statements are prepared in accordance with GAAP. The preparation of these financial statements require us to make estimates and assumptions that affect the reported amounts of assets, liabilities, revenue and expenses, as well as related disclosures. We evaluate our estimates and assumptions on an ongoing basis. Our estimates are based on historical experience and various other assumptions that we believe to be reasonable under the circumstances. Our actual results could differ from these estimates.

The critical accounting policies, assumptions and judgements that we believe have the most significant impact on our consolidated financial statements are described below.

Revenue Recognition

Our revenues are derived from sales of software, subscriptions, support and maintenance, and other services. We satisfy our performance obligations to recognize revenue for a single performance obligation ratably over the expected term with the customer.

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

1.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 substantially all consideration to which we 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.

2.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.

3.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.

4.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 on a relative standalone selling price based on the observable selling price of our products and services.

5.Recognition of revenue when, or as, we satisfy performance obligations—We satisfy 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.

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.

We use the Black-Scholes pricing model to estimate the fair value of options on the date of grant. On August 26, 2021, the Board determined that the Liquidity Event Satisfaction for the restricted stock units will be deemed to have been met as a result of the Merger and authorized that the shares of common stock subject to the awards will be delivered, in accordance with the terms of the Restricted Stock Unit Agreement. The Board's determination of the Liquidity Event Satisfaction being met as a result of the Merger qualified as a modification of the original terms of the RSU Agreements as of the date of the Merger. All RSUs issued prior to the completion of the Merger were re-valued using a fair value of $12.85, which was the closing share price of our common stock on that date. Subsequent to the closing of the Merger, the fair value of RSUs will be based on the fair value of our common stock on the date of the grant.

As a consequence, we recognized non-cash expense subsequent to the Merger in an amount of $156.6 million related to 20,127,730 outstanding RSUs. This consists of $155.5 million associated with RSUs on a graded vesting schedule, which were issued under the 2014 Plan and $1.1 million associated with RSUs on a straight-line vesting schedule, issued under the 2021 Plan. 10,638,068 RSUs remain unvested as of January 31, 2022.

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.

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 year to date 2022 or fiscal year 2021. 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

Report of Independent Registered Public Accounting Firm

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, 2022 and 2021, and the related consolidated statements of operations, of comprehensive loss, of changes in stockholders' 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, 2022 and 2021, 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.

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.

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.

Emphasis of Matter

As discussed in Note 1 to the consolidated financial statements, the Company and its subsidiaries are subject to risks and uncertainties that could affect amounts reported in the Company's financial statements in future periods. Management's evaluation of the events and conditions and management's plans to mitigate these matters are described in Note 1.

/s/ PricewaterhouseCoopers LLP

Baltimore, Maryland

May 2, 2022

We have served as the Company's auditor since 2019.

IronNet, Inc.
Consolidated Balance Sheets
(in thousands, except per share data)

	As of January 31,	
	2022	**2021**
Assets		
Current assets		
Cash and cash equivalents	$ 47,673	$ 31,543
Accounts receivable	1,991	1,643
Unbilled receivables	4,637	1,425
Related party receivables and loan receivables	3,233	3,599
Account and loan receivables	9,861	6,667
Inventory	4,581	2,180
Deferred costs	2,599	2,068
Prepaid warranty	829	1,037
Prepaid expenses	3,660	2,046
Other current assets	1,458	126
Total current assets	70,661	45,667
Deferred costs	3,243	2,056
Property and equipment, net	5,606	2,792
Prepaid warranty	1,229	878
Deposits and other assets	493	298
Total assets	$ 81,232	$ 51,691
Liabilities and stockholders' equity		
Current liabilities		
Accounts payable	$ 2,348	$ 1,922
Accrued expenses	4,709	2,591
Deferred revenue	16,049	12,481
Deferred rent	159	134
Short-term PPP loan	—	3,487
Income tax payable	542	88
Other current liabilities	689	689
Total current liabilities	24,496	21,392
Deferred rent	769	928
Deferred revenue	17,517	21,563
Warrants	7	—
Long-term PPP loan	—	2,093
Other long-term liabilities	—	689
Total liabilities	42,789	46,665
Stockholders' equity		
Preferred stock, $0.0001 par value; 100,000 shares authorized; none issued or outstanding	—	—
Class A common stock; $0.0001 par value; 500,000 shares authorized; 88,876 and 66,934 shares issued and outstanding at January 31, 2022 and January 31, 2021, respectively	9	7
Additional paid-in capital	455,849	180,853
Accumulated other comprehensive (loss) income	271	40
Accumulated deficit	(417,686)	(175,039)
Subscription notes receivable	—	(835)
Total stockholders' equity	38,443	5,026
Total liabilities and stockholders' equity	$ 81,232	$ 51,691

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

IronNet, Inc.
Consolidated Statements of Operations
(in thousands, except per share data)

	Year Ended January 31,	
	2022	**2021**
Product, subscription and support revenue	$ 25,347	$ 24,701
Professional services revenue	2,197	4,526
Total revenue	27,544	29,227
Cost of product, subscription and support revenue	8,225	5,393
Cost of professional services revenue	1,158	1,629
Total cost of revenue	9,383	7,022
Gross profit	18,161	22,205
Operating expenses		
Research and development	52,899	25,754
Sales and marketing	82,922	30,381
General and administrative	112,099	21,347
Total operating expenses	247,920	77,482
Operating loss	(229,759)	(55,277)
Other income	25	71
Other expense	(1,183)	(90)
Change in fair value of warrants liabilities	(11,265)	—
Loss before income taxes	(242,182)	(55,296)
Provision for income taxes	(465)	(77)
Net loss	$ (242,647)	$ (55,373)
Basic and diluted net loss per common share	$ (3.03)	$ (0.86)
Weighted average shares outstanding, basic and diluted	79,953	64,562

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

IronNet, Inc.
Consolidated Statements of Comprehensive Loss
($ in thousands)

	Year Ended January 31,	
	2022	**2021**
Net loss	$ (242,647)	$ (55,373)
Change in net unrealized (losses) gains on available for sale investments, net of tax	—	(397)
Foreign currency translations adjustment, net of tax	231	42
Total comprehensive loss	$ (242,416)	$ (55,728)

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

IronNet, Inc.
Consolidated Statements of Changes in Stockholders' Equity
For the Years Ended January 31, 2022 and 2021
($ in thousands, number of preferred stock and common stock in thousands)

	Series A Preferred Stock		Series B Preferred Stock		Class A Common Stock		Class B Common Stock		Additional Paid- In Capital	Accumulated Deficit	Accumulated Other Comprehensive Income (Loss)	Subscription Notes Receivable	Total Stockholders' Equity
	Shares	Amount	Shares	Amount	Shares	Amount	Shares	Amount					
Balance at January 31, 2020, as previously reported	794	$ 32,500	1,217	$ 88,711	36,138	$ 4	17,607	$ 2	$ 2,041	$ (119,666)	$ 394	$ (900)	$ (118,125)
Retroactive application of recapitalization (1)	(794)	(32,500)	(1,217)	(88,711)	23,984	2	(17,607)	(2)	121,194	—	—	—	121,194
Adjusted Balance at January 31, 2020	—	$ —	—	$ —	60,122	$ 6	—	$ —	$ 123,235	$ (119,666)	$ 394	$ (900)	$ 3,069
Issuance of common stock	—	—	—	—	6,812	1	—	—	57,608	—	—	—	57,609
Interest earned on subscription notes receivable	—	—	—	—	—	—	—	—	16	—	—	(16)	—
Payments on subscription notes receivable	—	—	—	—	—	—	—	—	—	—	—	81	81
Stock-based compensation	—	—	—	—	—	—	—	—	(6)	—	—	—	(6)
Unrealized gain on investments	—	—	—	—	—	—	—	—	—	—	(396)	—	(396)
Net loss	—	—	—	—	—	—	—	—	—	(55,373)	—	—	(55,373)
Foreign currency translation adjustment, net of tax of $0	—	—	—	—	—	—	—	—	—	—	42	—	42
Balance at January 31, 2021	—	$ —	—	$ —	66,934	$ 7	—	$ —	$ 180,853	$ (175,039)	$ 40	$ (835)	$ 5,026
Issuance of common stock	—	—	—	—	755	—	—	—	365	—	—	—	365
Merger recapitalization (Note 3)	—	—	—	—	4,555	1	—	—	(12,027)	—	—	—	(12,026)
PIPE Shares	—	—	—	—	12,500	1	—	—	109,857	—	—	—	109,858
Issuance of common stock related to Public Warrants	—	—	—	—	29	—	—	—	330	—	—	—	330
Issuance of common stock related to Private Warrants	—	—	—	—	3,188	—	—	—	21,492	—	—	—	21,492
Issuance of earnout	—	—	—	—	1,078	—	—	—	—	—	—	—	—
Interest earned on subscription notes receivable	—	—	—	—	—	—	—	—	8	—	—	(8)	—
Settlement of related party loan receivable for common shares	—	—	—	—	(108)	—	—	—	(1,075)	—	—	—	(1,075)
Payment of note receivable and settlement of note receivables for common shares	—	—	—	—	(55)	—	—	—	(550)	—	—	843	293
Stock-based compensation	—	—	—	—	—	—	—	—	156,596	—	—	—	156,596
Net loss	—	—	—	—	—	—	—	—	—	(242,647)	—	—	(242,647)
Foreign currency translation adjustment, net of tax of $0	—	—	—	—	—	—	—	—	—	—	231	—	231
Balance at January 31, 2022	—	$ —	—	$ —	88,876	$ 9	—	$ —	$ 455,849	$ (417,686)	$ 271	$ —	$ 38,443

(1) Prior to the Merger, as discussed in Note 3, Legacy IronNet Series A and Series B preferred stock were converted 1:10 to Legacy IronNet Class A common stock and Legacy IronNet Class B common stock was converted 1:1 to Legacy IronNet Class A common stock. All Legacy IronNet Class A common stock was then converted to Legacy LGL Class A common stock at the Exchange Ratio of approximately 0.8141070. The conversion has been retroactively restated as of January 31, 2020.

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

IronNet, Inc.
Consolidated Statements of Cash Flows
($ in thousands)

	Year Ended January 31,	
	2022	**2021**
Cash flows from operating activities		
Net loss	$ (242,647)	$ (55,373)
Adjustments to reconcile net loss to net cash provided by (used in) operating activities:	-	
Depreciation and amortization	1,092	1,162
Loss (Gain) on sale of fixed assets	(6)	219
Bad debt expense	—	33
Employee stock based compensation	156,596	(6)
Non-cash interest expense	1,155	—
Change in fair value of warrants liabilities	11,265	—
Non-cash interest on amounts due from stockholder	(8)	—
Changes in operating assets and liabilities:		—
Accounts receivable	(3,194)	(3,356)
Deferred costs	(1,718)	(1,038)
Inventories	(2,401)	(217)
Prepaid expenses	(1,614)	(538)
Other current assets	(2,407)	(72)
Deposits and other assets	(196)	104
Prepaid warranty	(144)	424
Accounts payable	398	1,628
Accrued expenses	971	751
Income tax payable	454	76
Other short-term liabilities	(689)	-
Deferred rent	(134)	(158)
Deferred revenue	(477)	13,711
Warrants	20	—
Net cash used in operating activities	(83,684)	(42,650)
Cash flows from investing activities	-	
Purchases of property and equipment	(3,880)	(952)
Proceeds from the sale of fixed assets	8	61
Proceeds from the maturity of investments	—	1,003
Net cash (used in) provided by investing activities	(3,872)	112
Cash flows from financing activities		
Proceeds from issuance of common stock	694	57,593
Proceeds from borrowing SVB Bridge loan	15,000	—
Proceed from borrowing PPP loan	—	5,580
Payment of loan - SVB Bridge	(15,000)	—
Payment of PPP loan	(5,580)	—
Merger recapitalization	4,213	—
Proceeds from PIPE shares	125,000	—
Payment of transaction costs	(21,179)	—
Proceeds from stock subscriptions	293	81
Net cash provided by financing activities	103,441	63,254
Effect of exchange rate changes on cash and cash equivalents	245	21
Net change in cash and cash equivalents	16,130	20,737
Cash and cash equivalents	-	
Beginning of the period	$ 31,543	$ 10,806
End of the period	47,673	31,543
Supplemental disclosures of non-cash investing and financing activities		
Interest earned on subscription notes receivable	$ 8	$ 16
Unpaid 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.

1.Organization and Nature of Operations, Basis of Presentation, and Summary of Significant Accounting Policies

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 our 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 our existing stockholders being the majority stockholders and holding majority voting power in the combined company, our senior management comprising the majority of the senior management of the combined company, and our 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 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 years ended January 31, 2022 and 2021. 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, 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

As of January 31, 2022, the Company had cash and cash equivalents of $47.7 million and collectable receivables of $13.8 million. The Company continues to benefit from being debt free, having paid off previous balances on our PPP Loan and SVB Bridge facility, as well as continuing to fund our operations from the proceeds from the merger that closed on August 26, 2021 and secured gross funding of $138.25 million. As discussed under Subsequent Events, the Company has also secured a $175 million equity line with Tumim Capital, which remains available to fund future operations in the absence of any material adverse conditions. The Company, based on our forecast and the proceeds from the recent merger, as well as plans which could be executed to moderate internal and external expenditures as needed, has concluded that we will have sufficient liquidity to fund operations for the period ended 12 months from the issuance of these financial statements.

The Company's future capital requirements will depend on many factors, including, but not limited to the rate of our growth, our ability to attract and retain customers and their willingness and ability to pay for our products and services, and the timing and extent of spending to support our

efforts to market and develop our products. Further, we may enter into future arrangements to acquire or invest in businesses, products, services, strategic partnerships, and technologies. As such, we may be required to seek additional equity or debt financing. In the event that additional financing is required from outside sources, we may not be able to raise it on terms acceptable to us or at all. If additional funds are not available to us on acceptable terms, or at all, our business, financial condition, and results of operations could be adversely affected. The financial statements do not include any adjustments that might become necessary should the Company be unable to continue as a going concern.

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.

Account 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. Management has evaluated the need for an allowance for doubtful accounts and no amounts were recorded as of January 31, 2022 and 2021.

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, 2022 approximates $46,695. Accounts receivable consist primarily of amounts due from commercial entities. Historically, the Company has not experienced significant losses related to accounts receivable and, therefore, believes that the credit risk related to accounts receivable is minimal.

Inventory

Inventory is stated at the lower of cost or net realizable value. No provisions have been made to reduce slow-moving, obsolete or unusable inventories to their net realizable values for January 31, 2022 and 2021. Substantially all of our inventory is finished goods.

Deferred Costs

The Company amortizes 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. These costs include appliance hardware and installation costs that are essential in providing the future benefit of the solution.

Deferred Commissions

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, maintenance, and repairs are charged to expense as incurred. The Company has incurred repair and maintenance charges of $12 and $10 for the years ended January 31, 2022 and 2021, 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:

Computer and other equipment	3-5 years
Leasehold improvements	Shorter of life of lease or life of asset
Furniture and fixtures	7 years
Software	3 years

Deferred Revenue (Contract Liabilities)

Deferred revenue, which is a contract liability, consists of amounts for which we have the unconditional right to bill or advance from customers for which have not yet recognized revenue. We generally bill our customers in advance. To the extent the Company bills customers in advance of the contract commencement date, the accounts receivable and corresponding deferred revenue amounts are netted to zero on the consolidated balance sheets, unless we have 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 we have the unconditional right to bill, with corresponding deferred revenue established for the portion for which we have not yet recognized revenue.

Foreign Currency Translation

The United States Dollar (USD) is the functional currency of IronNet and our subsidiaries in the United States. Our subsidiaries' financial statements are maintained in their functional currencies, which is the local currency in their country of origin. Our foreign subsidiaries' financial statements are translated into USD. Assets and liabilities are translated into USD using the period-end spot 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 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, 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. Determination of SSP requires judgment. We determine 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 internally approved pricing guidelines related to the performance obligations.

- **Recognition of revenue when, or as, we satisfy 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.

We generate revenue from the sales of cloud based subscriptions, managed services and professional services, primarily through our indirect relationships with our partners or direct relationships with end customers through our direct sales force. We account for our 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 our cloud-based solutions, which allow customers to use our hosted security software over a contracted period without taking possession of the software and managed services where we provide 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, inclusive of 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 we recognize 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 is unable to take 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, 2022, capitalized costs were $2.7 million, net of $86 of amortized cost.

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 $52,899 and $25,754 for the years ended January 31, 2022 and 2021, respectively.

Advertising

The Company expenses advertising costs as incurred. Advertising costs were $1,789 and $2,631 for the years ended January 31, 2022 and 2021, 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.

We evaluated the warrants issued by Legacy LGL, our 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 because 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, we recorded these Private Warrants as liabilities on the 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, as described in Note 8. 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.

Over the period of September 2021 through 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 0.6 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. In September and October 2021, 5,190 Private Warrants were exercised on a cashless basis into 3,188 shares of Class A common stock. As of January 31, 2022, the Company had 10 Private Warrants outstanding and not exercised. During the period 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.

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 restricted stock unit ("RSU") awards, stock-based compensation expense is recognized on a graded basis matched to the length of time and vesting tranches of each grant.

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 selected model inputs. The Company grants stock options at exercise prices determined equal to the fair value of common stock on the date of the grant. The computation of expected option life is based on an average of the vesting term and the maximum contractual life of the Company's stock options, as the Company does not have sufficient history to use an alternative method to the simplified method to calculate an expected life for employees. The Company estimates 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 the Company's 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, 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

We have 500,000 shares of voting common stock authorized for issuance. As of January 31, 2022, a total of 88,876 shares of common stock issued and outstanding, with 20,128 held for future exercise of outstanding RSUs, 1,317 held for future exercise of stock options, 9,803 shares available for grant under the 2021 Equity Incentive Plan, 8,596 shares reserved for public warrant conversion, and approximately 10 shares reserved for private warrant conversion.

Recently Issued Accounting Standards

We are an emerging growth company, 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. 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.

New Accounting Pronouncements Adopted in Fiscal 2022

In December 2019, the FASB issued Accounting Standards Update No. 2019-12, Income Taxes (Topic740): Simplifying the Accounting for Income Taxes, which modifies and eliminates certain exceptions to the general principles of ASC 740, Income Taxes. ASU 2019-12 was adopted in the first quarter of fiscal 2022. The prospective adoption of ASU 2019-12 was not material.

In August 2018, the FASB issued ASU 2018-15, Intangibles—Goodwill and of Other—Internal-Use Software (Subtopic 350-40): Customer's Accounting for Implementation Costs Incurred in a Cloud Computing Arrangement That Is a Service Contract. ASU 2018-15 was adopted in the third quarter of fiscal 2022. The prospective adoption of ASU 2018-15 was not material.

Recent Accounting Pronouncements Not Yet Adopted

The FASB issued ASU No.2016-02, Leases (Topic 842) ("ASU 2016-02"), which supersedes the current lease requirements in ASC 840, Leases. ASU 2016-02 requires lessees to recognize a right-of-use asset and related lease liability for all leases, with a limited exception for short-term leases. Leases will be classified as either finance or operating, with the classification affecting the pattern of expense recognition in the statement of operations. Currently, leases are classified as either capital or operating, with any capital leases recognized on the consolidated balance sheets. The reporting of lease-related expenses in the consolidated statements of operations and cash flows will be generally consistent with the current guidance. The new lease guidance will be effective the earlier of the year ending January 31, 2023 or the time at which we no longer qualify as an EGC and will be applied using a modified retrospective transition method to either the beginning of the earliest period presented or the beginning of the year of adoption. The Company is currently evaluating the impact of adopting the new standard. The adoption of this standard will require the recognition of a right of use asset and liability on the Company's consolidated balance sheets.

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 years beginning after December 15, 2022 or the time at which we no longer qualify as an EGC. Management does not expect the impact of adopting this standard to be material.

2.Revenue

Software, subscription and support revenue

The Company sells a collective defense software solution that provides a near real time collective defense infrastructure that is comprised of two product offerings, IronDefense and IronDome. The software platform is delivered through both on-premises licenses bundled with on-premises hardware and through subscription software.

Our security appliance deliverables include proprietary operating system software and hardware together with regular threat intelligence updates and support, maintenance, and warranty. We combine 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 our cybersecurity solution. As a result, we recognize revenue for this single performance obligation ratably over the expected term with the customer. Significant judgement is required for the assessment of material rights relating to renewal options associated with our contracts.

Revenue from subscriptions, which allow customers to use our security software over a contracted period without taking possession of the software, and managed services, where we provide managed detection and response services for customers, is recognized over the contractual term. The cloud-based subscription revenue, where we also provide hosting, recognized for the years ended January 31, 2022 and 2021 was $15,960 and $10,062, respectively. Overall software, subscription, and support revenue recognized for the years ended January 31, 2022 and 2021, was $25,347 and $24,701, 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 years ended January 31, 2022 and 2021 was $2,197 and $4,526, respectively.

Customer concentration

For the year ended January 31, 2022, six customers accounted for 51%, or $13,975, with two of those customers accounting for 21%, of the Company's revenue, and for the year ended January 31, 2021, six customers accounted for 46%, or $13,381, with one of those customers accounting for 10%, of the Company's revenue. As of January 31, 2022, and January 31, 2021, two and three customers represent 49% and 85% of the total accounts receivable balance, respectively.

Significant customers are those which represent at least 10% of the Company's total revenue at each respective period ending date. The following table presents customers that represent 10% or more of the Company's total revenue:

	Year Ended January 31,	
	2022	**2021**
Customer A	*	10%
Customer B	11%	*
Customer C	10%	*
	21%	10%

* - less than 10%

Deferred costs

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

Balance at February 1, 2020	$	3,080
Cost of revenue recognized		(1,151)
Costs deferred		876
Balance at January 31, 2021		2,805
Balance at February 1, 2021		2,805
Cost of revenue recognized		(2,095)
Costs deferred		3,899
Foreign exchange		(5)
Balance at January 31, 2022	$	4,604

The balance of deferred commissions at January 31, 2022 and 2021 were $1,238 and $1,319, respectively. Deferred commissions are included in the Deferred costs on the Consolidated Balance Sheets of which $844 is current and $393 is long-term as of January 31, 2022.

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, 2022 and January 31, 2021, the Company recognized revenue of $12,509 and $7,809, respectively, which was included in the deferred revenue balance at the beginning of each of the respective periods.

The balance in deferred revenue is as follows:

Balance at February 1, 2020	$	20,312
Revenue recognized		(25,271)
Revenue deferred		38,940
Foreign exchange		63
Balance at January 31, 2021		34,044
Balance at February 1, 2021		34,044
Revenue recognized		(29,133)
Revenue deferred		28,663
Foreign exchange		(8)
Balance at January 31, 2022	$	33,566

Remaining performance obligations

As of January 31, 2022, the remaining performance obligations totaled $33,566. The Company's recognition of revenue in the future thereon will be in:

Years Ending January 31,		
2023	$	16,049
2024		9,771
2025		5,852
2026		1,894
	$	33,566

3.Reverse Recapitalization

As discussed in Note 1., on August 26, 2021, the Company completed the Merger**.** 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 year ended January 31, 2022:

		Recapitalization and Associated Transactions
Cash (Trust)	$	173,015
Redemptions		(159,763)
Less: fees to underwriters and advisors		(9,038)
Net cash received from Merger recapitalization		4,214
Issuance of PIPE Shares		125,000
Less: PIPE fees to underwriters and advisors		(21,179)
Net cash received from PIPE Shares and Merger recapitalization		108,035
Less: debt settlement		(21,266)
Net proceeds from Merger recapitalization, PIPE Shares and debt settlement	$	86,769

The number of outstanding shares of common stock of the Company as of January 31, 2022 is summarized as follows:

Shares by Type	Number of Shares
IronNet Class A Common Stock outstanding previous to the Merger	67,502
Issuance of common stock (exercise of ISOs and warrant)	29
Number of Shares issued at the date of the business combination (Recapitalization)	
LGL Class A Common Stock outstanding previous to the Merger	17,250
Less: Redemption of LGL Class A previous to the Merger	(15,929)
Total Class A Shares issued to former LGL shareholders	1,321
LGL Founders Shares	3,234
PIPE Shares	12,500
Number of Share issued at the Merger	17,055
Number of Shares issued (redeemed) following the consummation of the Merger	
Earnout Shares	1,078
Private Warrants (Exercised)	3,188
Public Warrants (Exercised)	29
Exercise of ISOs	158
Payments on subscription notes receivable	(55)
Shares repurchase related to loan pay-off	(108)
Total Shares of Common Stock as of January 31, 2022	88,876

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 has 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 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 $13,251 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 provision of the Coronavirus Aid, Relief and Economic Security ("CARES") Act, receiving loan funds of $5,580. 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. As of January 31, 2021, Legacy IronNet had an interest accrual of $44 related to the PPP loan.

Loans to Employees

On December 29, 2018, Legacy IronNet entered into a loan with a current 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 Equityholders (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 (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 Equityholders.

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.

4.Prepaid Expenses

The increase in prepaid expenses in the current year primarily relates to $3.2 million in directors and officers insurance purchased in August 2021, of which $1.8 million makes up the balance of prepaid expenses at January 31, 2022.

5.Property and Equipment

Property and equipment consists of the following at January 31:

	2022	2021
Computer and other equipment	$ 5,369	$ 3,701
Leasehold improvements	1,416	1,582
Furniture and fixtures	388	386
Software	2,795	629
	9,968	6,298
Less: Accumulated depreciation and amortization	(4,362)	(3,506)
	$ 5,606	$ 2,792

Depreciation and amortization expense on property and equipment was $1,092 and $1,162 for the years ended January 31, 2022 and January 31, 2021, respectively.

6.Stock Incentive Plans

Legacy IronNet's Board of Directors adopted and the 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, restricted stock units "RSUs," and other stock-based awards. ISOs were only able to be granted to Legacy IronNet's employees and to any of the employees of Legacy IronNet's subsidiary corporations' employees. All other awards could be granted to employees, directors and consultants of Legacy IronNet's 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 Combined Company when exercised or converted.

The 2021 Equity Incentive Plan (the "2021 Plan") was approved by Legacy LGL's stockholders on August 26, 2021. Under the 2021 Plan, the Company may grant ISOs, RSUs and other equity securities to acquire, to convert into, or to receive up to 13,500 shares of Class A common stock. As of January 31, 2022, 9,803 share equivalents remained available to issue under the 2021 Plan.

All share equivalents issued or issuable 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 share equivalents authorized under the Stock Incentive Plans.

Stock Options

The exercise price of each ISO 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:

	Number of Shares (in thousands)	Weighted Average Exercise Price	Weighted Average Remaining Contractual Term (Years)	Intrinsic Value of outstanding options
Outstanding at February 1, 2020	3,602	$ 0.54	5.9	$ 4,088
Granted	-	-	-	-
Exercised	(403)	$ 0.52	5.2	$ 468
Forfeited or expired	(1,017)	$ 0.57	6.1	-
Outstanding at January 31, 2021	2,182	$ 0.53	5.9	$ 5,573
Exercisable at January 31, 2021	1,995	$ 0.53	5.9	$ 5,570
Outstanding at February 1, 2021	2,182	$ 0.53	4.9	$ 5,573
Granted	-	-	-	-
Exercised	(749)	$ 0.49	4.8	$ 1,940
Forfeited or expired	(116)	$ 0.57	5.3	-
Outstanding at January 31, 2022	1,317	$ 0.55	4.9	$ 3,773
Exercisable at January 31, 2022	1,293	$ 0.54	4.9	$ 3,706

For the years ended January 31, 2022 and 2021, the Company recorded $43 and ($6) of compensation cost related to stock options, respectively. There were no options granted during the years ended January 31, 2022 and 2021. The total fair value of shares vested, net of forfeitures, was $2,062 and $1,672 for the years ended January 31, 2022 and 2021, respectively.

Stock compensation expense for ISOs is recognized on a straight-line basis and with a provision for forfeitures matched to historical experience for matured grant cohorts. At January 31, 2022, total unrecognized compensation cost, adjusted for estimated forfeitures, related to unvested stock options was not significant. The weighted-average remaining vesting period of unvested stock options at January 31, 2022 was 4.9 years.

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 and expected term of the stock 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 noted above, the RSUs granted under the 2014 Plan contained an additional vesting requirement that also required the occurrence of a liquidity event. On 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. As detailed in Note 3, in connection with the close of the Merger with Legacy LGL, the Company recognized a non-cash expense for awards issued under the 2014 Plan in an amount of $155,518 during fiscal year 2022.

Presented below is a summary of the status of outstanding RSUs, including showing the vesting status based on time and performance-based criteria, other than the liquidity event condition:

	Number of Shares (in thousands)	Weighted Average Grant Date Fair Value
Non-vested at February 1, 2020	14,397	$ 1.62
Granted	2,029	3.08
Vested	(5,090)	1.70
Forfeited or expired	(1,624)	2.06
Non-vested at January 31, 2021	9,712	$ 1.82
Non-vested at February 1, 2021	9,712	$ 11.75
Granted	5,900	8.20
Vested	(3,818)	12.01
Forfeited or expired	(1,484)	12.85
Non-vested at January 31, 2022	10,310	$ 9.57

As of January 31, 2022, there are 20,128 RSUs outstanding, which is comprised of 3,697 RSUs with only service conditions, 1,303 RSUs with only performance conditions, and 15,128 RSUs with both service conditions and performance conditions. Of the outstanding RSUs, 651 shares with only performance conditions have vested and 9,167 RSUs with both service conditions and performance conditions have vested as of January 31, 2022.

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. 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.

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. 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.

We recognized a total stock-based compensation expense, net of actual forfeitures, of $156,560 during the year ended January 31, 2022. $155,518 of this balance is associated with RSUs on a graded vesting schedule and $1,042 is associated with RSUs on a straight-line vesting schedule. As no RSUs vested until the occurrence of the liquidity event, which occurred on August 26, 2021, no stock-based compensation was recognized associated with RSUs in the year ended January 31, 2021.

As of January 31, 2022, there was approximately $46,568 of unrecognized compensation cost related to unvested RSUs without performance obligations. The weighted-average remaining vesting period was 2.68 years.

Employee Stock Purchase Plan

In August 2021, Legacy LGL's Board of Directors adopted, and its stockholders approved, the 2021 Employee Stock Purchase Plan (the "ESPP"). The ESPP became effective immediately upon the closing of the Merger, and authorizes the issuance of shares of common stock pursuant to purchase rights granted to our employees.

The purpose of the ESPP is to provide a means by which our eligible employees and certain designated companies may be given an opportunity to purchase shares of our common stock, to assist us 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 our success. The Plan includes two components: a 423 Component and a Non-423 Component. We intend 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 our board of directors, the Non-423 Component will operate and be administered in the same manner as the 423 Component.

The price at which the common stock is purchased under the ESPP is equal to 85% of the fair market value of our common stock on the offering date or the purchase date, whichever is lower. Offerings, which are granted by the board of directors, will consist of one or more purchase periods and will not exceed a period of more than 27 months beginning on the offering date. The number of shares of common stock reserved for issuance automatically increase on February 1 of each year, by an amount that is the lesser of 1% of the total number of shares of common stock outstanding on January 31 of the preceding year, and 2 million shares, as determined by our board of directors. As of January 31, 2022, 2.7 million shares may be issued under the plan, and there have been no purchases of shares for any eligible employee.

7.Stockholders' Equity

Common Stock

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

Each share of Common Stock has 1 vote.

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, 2022, 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 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.

In connection with the Merger, the Public Warrants were recorded within equity at a fair value of $15,740. The fair value of the Public Warrants issued by the Company was determined using the quoted price. In October 2021, 29 Public Warrants were exercised in an amount of $330 and 29 shares were issued at a price of $11.50. As of January 31, 2022, the Company had 8,596 Public Warrants outstanding and not exercised.

8.Fair Value Measurements

The fair value of the financial assets and liabilities are included at the amount at which the instrument could be exchanged in a current transaction between willing parties, other than in a forced or liquidation sale. The Company has assessed that the fair value of cash and cash equivalents, accounts receivable, prepaid expenses and other current assets, accounts payable and accrued expenses approximates their carrying amounts largely due to the short-term maturities. The Company has also assessed the fair value of the Private Warrants due to the conclusion that they should be recorded as liabilities measured at fair value.

The Company's Private Warrants have similar terms 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 were observable transactions in the Company's Public Warrants during the year ended January 31, 2022 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, 2022, 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 in the fair value hierarchy table below. Changes in the fair value of the Private Warrants at each reporting period end date were recognized within the accompanying consolidated statement of operations in the change in fair value of warrant liabilities.

The carrying amounts and fair values of financial assets and liabilities, which are either Level 1 or Level 2 instruments, are as follows:

	January 31, 2022				January 31, 2021			
	Level 1	Level 2	Level 3	Total	Level 1	Level 2	Level 3	Total
Cash equivalents	$ 102	$ —	$ —	$ 102	$ 102	$ —	$ —	$ 102
Private Warrants	—	7	—	7	—	—	—	—
Total assets	$ 102	$ $ 7	$ $ —	$ $ 109	$ 102	$ —	$ —	$ 102

The Company recognized a non-cash expense of $11,265 related to the change in fair value of warrants during the period ended January 31, 2022.

9.Income Taxes

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

	2022	2021
Current income taxes		
Federal	$ -	$ -
State	1	8
Foreign	464	69
Deferred income taxes	—	—
Total income tax expense	$ 465	$ 77

For the years ended January 31, 2022 and 2021, the foreign income (loss) before provision for income tax was $1,774 and $660, respectively. For the years ended January 31, 2022 and 2021, the domestic loss before provision for income tax was ($243,956) and ($55,956), respectively.

Indefinite reinvestment is determined by management's judgment about and intentions concerning the future operations of the Company. As part of our business strategies, we have determined that all earnings from our foreign continuing operations will be deemed indefinitely reinvested outside of the United States. Our 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:

	2022		2021	
Income tax expense computed at U.S. federal statutory income tax rate	$ (50,575)	21.0 %	$ (11,628)	21.0 %
State income taxes	(10,190)	4.2 %	(2,257)	4.1 %
Permanent items	8,197	-3.4 %	321	-0.6 %
Valuation allowance	53,577	-22.2 %	13,632	-24.6 %
Other	(544)	0.3 %	9	—
Income tax expense computed at U.S. federal statutory income tax rate	**$ 465**	**-0.1 %**	**$ 77**	**-0.1 %**

Income tax expense was ($0.5) million and ($0.1) million for the years ended January 31, 2022 and 2021, respectively. The effective tax rate for the years ended January 31, 2022 and 2021 was 0.1% 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:

	2022	2021
Deferred tax assets		
Net operating loss carryforward	$ 81,955	$ 38,933
Accruals and other	610	757
Intangibles	123	136
Depreciation and amortization	118	70
RSU	8,499	-
Others	285	-
Deferred revenue	5,786	2,754
Gross deferred tax assets	97,376	42,650
Valuation allowance	(95,533)	(41,849)
Net deferred tax asset	1,843	801
Deferred tax liabilities		
Deferred costs	(1,843)	(801)
Net deferred tax assets (liabilities)	$ -	$ -

Income Tax Valuation Allowance

The following summarizes changes to valuation and qualifying accounts for fiscal year 2022 and fiscal year 2021 (in thousands):

Income Tax Valuation Allowance		Balance at Beginning of Period	Charged to Costs & Expenses	Federal/State NOL	Balance at End of Period
Year Ended					
	January 31, 2022	41,849	10,662	43,022	95,533
	January 31, 2021	28,219	(128)	13,758	41,849

As of January 31, 2022 and January 31, 2021, the Company had net operating loss carryforwards (NOLs) available to offset federal taxable income of approximately $324,787 and $154,566 respectively. $25,270 of the federal NOLs expire on various dates through 2037 and $299,517 are able to be carried forward indefinitely to offset 80% of future taxable income. The company has tax effected state NOL carryforwards of approximately $13,749 as of January 31, 2022 and $6,223 as of January 31, 2021 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 our 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 may 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, 2022 and 2021.

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, 2022 and 2021. The Company files tax returns in the United States federal jurisdiction and in many state jurisdictions. The tax years 2017 through 2021 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 do not have a significant impact on our current taxes, deferred taxes, or uncertain tax positions.

10.Accrued Expenses

The balance in accrued expenses at January 31, 2022 includes $1.1 million 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 that is in place. This payment was due from the customer directly to the third party, and will be remitted to the third party. 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 is in process of resolving these liabilities with the respective state jurisdictions.

11.COVID-19 – CARES Act Provision

During fiscal 2021, in response to the increased economic uncertainties that the impact of the COVID-19 pandemic was expected to have on our business, results of operations, liquidity and capital resources, Legacy IronNet took measures to ensure that we could continue the continuity of our business operations through the use of funding measures which included the PPP loan from the US Small Business Administration pursuant to the CARES Act. The purpose of the loan was for small businesses to keep their workforces employed through the pandemic. Legacy IronNet received loan funds of $5,580 on April 21, 2020. 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 Legacy IronNet with PNC Bank (the “Lender”). As detailed in Note 3, 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. As of January 31, 2021, the Company had an interest accrual of $44 related to the PPP loan.

In addition to seeking and receiving the PPP loan under the CARES Act, Legacy IronNet also elected to defer the Company portion of payroll taxes under the CARES Act. Half of the deferred payroll tax from March 1, 2020 through December 31, 2020 was paid on December 31, 2021, with the remaining 50% due on December 31, 2022. The balance of the payroll tax deferral is $689 as of January 31, 2022 and is included in other current liabilities on the consolidated balance sheet.

12.Commitments and Contingencies

Contingencies

In the ordinary course of business, the Company and our subsidiary 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.

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. The following is a schedule by year of the future minimum lease payments required under the Company’s operating leases:

Years Ending January 31,	
2023	$ 1,025
2024	755
2025	775
2026	797
2027	658
	$ 4,010

The Company is recognizing the total cost of our office leases ratably over the respective lease periods. The difference between rent paid and rent expense is reflected as deferred rent in the accompanying balance sheets.

Rent expense totaled $1,462 and $1,984 for the years ended January 31, 2022, and January 31, 2021, respectively, which is recognized in the general and administrative line item in the consolidated statement of operations.

In the second fiscal quarter of 2021, we completed lease buyouts of two office spaces in Maryland, for leases that were expiring in fiscal 2021 and fiscal 2022, and made payments of $394 to facilitate early terminations for those leases. We also decreased our lease portfolio in Japan and New York as a result of the Company moving to a more fully remote posture.

13.Earnings (Loss) per Share

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 shares, except that it reflects the effect of potential shares that would be issued if stock option awards, Restricted Stock Units, Public and Private Warrants and preferred shares, to the extent issued, were converted into common stock, to the extent dilutive.

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

	Year ended	
	2022	2021
Numerator: Net loss	$ (242,647)	$ (55,373)
Denominator: Basic and Diluted Weighted-average shares in computing net loss per share attributable to common stockholders	79,953	64,562
Net loss attributable to common stockholders—basic and diluted	$ (3.03)	$ (0.86)

Earnings per share calculations for the period prior to the Merger has been retrospectively restated to the equivalent number of shares reflecting the exchange ratio established in the reverse recapitalization. Subsequent to the Transactions, earnings per share will be calculated based on the weighted average number of shares of common stock then outstanding.

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:

	Year Ended January 31,	
	2022	2021
Shares of common stock issuable from stock options	1,317	2,182
Total RSUs unvested pending settlement	10,638	15,712
Private Warrants	10	—
Public Warrants	8,596	—
Potential common shares excluded from diluted net loss per share	20,561	17,894

As of January 31, 2021 there were no Private or Public Warrants outstanding due to the fact that the Legacy LGL consolidated balance sheet was consolidated and combined with Legacy IronNet as of the effective date of the Merger. Legacy LGL Public and Private Warrants as of August 26, 2021 were 8,625 and 5,200, respectively.

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 $1,744 and $1,860 of revenue from contracts with related parties for the years ending January 31, 2022, and January 31, 2021, respectively. The corresponding receivable was $3,233 and $2,541 as of January 31, 2022, and January 31, 2021, respectively. The Company also had an outstanding receivable from employees of $1,058 as of January 31, 2021, which was paid in full during the current year.

Subscription Notes Receivables

As of January 31, 2021, the Company held $835 of subscription notes receivable related to shares of common stock in Legacy IronNet that were issued to certain employees in exchange for promissory notes, which were determined to be recourse loans. During the years ended January 31, 2022 and January 31, 2021, the Company received repayments of balances due of $843 and $81, respectively. As of January 31, 2022, there are no remaining balances for subscription notes receivables. The subscription notes receivables' accrued interest ranged from 1.40% to 2.70%, compounded annually. Interest earned on the subscription notes receivable for the years ended January 31, 2022 and January 31, 2021 was $8 and $16, respectively.

15.Retirement Plans

We provide a retirement savings plan for the benefit of our employees, including our named 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 also 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. We also fully match employee contributions up to the first 4% of salary, which amounts are fully vested.

16. Segment and Geographic Information

The Company determines our operating segments based on ASC 280, Segment Reporting. 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:

	Year Ended January 31,	
	2022	2021
	($ in thousands)	
United States	$ 24,726	$ 27,147
International	2,818	2,080
Total	$ 27,544	$ 29,227

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

17. Subsequent Events

The Company has evaluated our January 31, 2022 financial statements for subsequent events through the date the financial statements were issued.

Restricted Stock Units

Following the end of fiscal year 2022, the Compensation Committee approved the issuance of grants of 6,910 Restricted Stock Units under the terms of the 2021 Equity Incentive Plan, which consists of 766 RSUs granted on February 2, 2022 with a fair value of $3.15 per share, 1,690 RSUs granted on March 9, 2022 with a fair value of $4.64 per share, 4,000 RSUs granted on March 15, 2022 with a fair value of $3.71 per share, and 453 RSUs granted on April 21, 2022 with a fair value of $2.89 per share. All of the awards granted have terms consistent with the terms of the awards granted under the 2021 plan during fiscal year 2022.

Evergreen Increases

Under the terms of the 2021 Plan, the number of shares and share equivalents that can be issued under the plan increased on February 1, 2022 by 4,934 shares, an amount equal to 5.0% of the sum of (a) the total number of shares of the Registrant's common stock outstanding on January 31st 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 31st of the immediately preceding fiscal year, but which have not yet been issued. Inclusive of the prior limit of 13.5 million shares, the new limit following the increase was 18.4 million shares, of which 7.6 million remain ungranted.

Under the terms of the 2021 Employee Stock Purchase Plan (the "ESPP"), the number of shares and share equivalents that can be issued under the plan increased on February 1, 2022 by 889 shares, 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) 2,000 shares of Common Stock. There were 88,876 shares of the Company that were outstanding as of January 31,2022. Inclusive of the prior limit of 2.7 million shares, the new limit following the increase was 3,589 shares, of which all remain available.

Tumim Stone Capital Committed Equity Financing

As reported in the Form S-1 filed on March 10, 2022 (the "Prospectus"), on February 11, 2022, the Company entered into the Common Stock Purchase Agreement (the "Purchase Agreement") with Tumim Stone Capital, LLC ("Tumim"), pursuant to which Tumim has committed to purchase up to $175 million 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 the registration statement that included the Prospectus 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. 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 $1,750,000, 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.

As further described in the ELOC Registration Statement, the sales of common stock by IronNet to Tumim under the Purchase Agreement, if any, will be 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," and the date on which the Commencement occurs, the "Commencement Date"), including that the registration statement that includes the Prospectus covering the resale by Tumim of shares of common stock that have been and may be issued under the Purchase Agreement is declared effective by the SEC. The SEC declared the ELOC Registration Statement effective on March 17, 2022.

From and after the Commencement Date, the Company has the right, but not the obligation, from time to time at its sole discretion, to direct Tumim to purchase certain amounts of our common stock, subject to certain limitations in the Purchase Agreement, that it specifies 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 a (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 (a "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.

Tumim has no right to require the Company to sell any shares of common stock to Tumim, but Tumim is obligated to make purchases as directed by the Company, subject to the satisfaction of conditions set forth in the Purchase Agreement at Commencement and thereafter at each time that the Company may direct Tumim to purchase shares of its common stock under the Purchase Agreement.

Although the Purchase Agreement provides that the Company may sell up to $175 million of its common stock to Tumim, only 48,503 shares of common stock have been registered for resale, which represents shares of common stock that may be issued to Tumim from and after the Commencement Date, if and when the Company elects to sell shares to Tumim under the Purchase Agreement. Depending on the market prices of common stock at the time the Company elects to issue and sell shares to Tumim under the Purchase Agreement, additional shares of common stock may need to be registered for resale under the Securities Act in order to receive aggregate gross proceeds equal to the $175,000,000 Total Commitment available under the Purchase Agreement. If all of the 48,503 shares offered by Tumim for resale under the ELOC Registration Statement were issued and outstanding (without taking into account the 19.99% Exchange Cap limitation), such shares would represent approximately 34% of the total number of shares of common stock outstanding and approximately 47% of the total number of outstanding shares held by non-affiliates. If the Company elects to issue and sell more than 48,503 shares to Tumim, which the Company has the right, but not the obligation, to do, any such additional shares must first be registered for resale under the Securities Act, which could cause additional substantial

dilution to Company stockholders. The number of shares ultimately offered for resale by Tumim is dependent upon the number of shares the Company may elect to sell to Tumim under the Purchase Agreement from and after the Commencement Date.

The net proceeds under the Purchase Agreement will depend on the frequency and prices at which the Company sell shares of its stock to Tumim. It is expected that any proceeds received from such sales to Tumim will be used for working capital and general corporate purposes.

Securities Litigation

On April 22, 2022, a federal securities class action lawsuit, captioned Grad v. IronNet, Inc., et al., No. 1:22-cv-004499 (E.D. Va.), was filed by our purported stockholder in the United States District Court for the Eastern District of Virginia on behalf of a proposed class consisting of those who acquired our securities between September 15, 2021 and December 20, 2021. The complaint names us, our co-CEOs, and our CFO as defendants and asserts claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934, as amended, for alleged misrepresentations and/or omissions in a September 14, 2021 press release regarding our business and financial prospects, our ability to predict the timing of significant customer opportunities, and our disclosure controls and procedures. The complaint seeks an unspecified amount of damages on behalf of the putative class and an award of costs and expenses, including reasonable attorneys' fees. 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 estimate reasonably possible losses or determine whether an unfavorable outcome is probable.

ITEM 9. CHANGES IN AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURE

None

ITEM 9A. CONTROLS AND PROCEDURES

Evaluation of Disclosure Controls and Procedures

Disclosure controls and procedures (as such terms are defined in Rules 13a-15(e) and 15d-15(e) under the Exchange Act) are designed to ensure that information required to be disclosed in our reports filed or submitted under the Exchange Act is recorded, processed, summarized and reported within the time periods specified in the SEC's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed in reports filed or submitted under the Exchange Act is accumulated and communicated to management, including our Chief Executive Officer and Chief Financial Officer, to allow timely decisions regarding required disclosure. In designing and evaluating disclosure controls and procedures, management recognizes that any controls and procedures, no matter how well designed and operated, can provide only reasonable assurance of achieving the desired control objectives. In addition, the design of disclosure controls and procedures must reflect the fact that there are resource constraints and that management is required to apply judgment in evaluating the benefits of possible controls and procedures relative to their costs.

Under the supervision and with the participation of our management, including our Chief Executive Officer and Chief Financial Officer, we conducted an evaluation of the effectiveness of our disclosure controls and procedures as of the end of the year ended January 31, 2022. Based upon that evaluation, our Chief Executive Officer and Chief Financial Officer concluded that the Company's disclosure controls and procedures were not effective as of January 31, 2022 due to the material weaknesses in our internal control over financial reporting described below.

Management's Report on Internal Control over Financial Reporting

Due to the timing of the closing of the Merger, and pursuant to Section 215.02 of the SEC Division of Corporation Finance's Regulation S-K Compliance & Disclosure Interpretations, this Annual Report on Form 10-K does not include a report of management's assessment regarding our internal control over financial reporting.

Because we qualify as an emerging growth company under the JOBS Act, this Annual Report on Form 10-K does not include an attestation report of our registered public accounting firm regarding internal control over financial reporting.

Changes in Internal Control Over Financial Reporting

There were no changes in our internal control over financial reporting during the quarter ended January 31, 2022, that have materially affected, or are reasonably likely to materially affect, our internal control over financial reporting.

Material weaknesses in internal control over financial reporting

Our internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with U.S. GAAP and includes those policies and procedures that: (1) pertain to the maintenance of records that in reasonable detail accurately and fairly reflect our transactions and the dispositions of our assets; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with U.S. GAAP and that receipts and expenditures are being made only in accordance with appropriate authorizations of our management and board of directors; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of assets that could have a material effect on our financial statements.

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.

Management determined that, as of January 31, 2022, 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, which constitutes a material weakness. This material weakness contributed to the following additional material weaknesses:

- 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. However, this error was corrected as of the date of this report on Form 10-K and the consolidated financial statements are correctly stated for the year ended January 31, 2022.

- We did not design and maintain effective controls over the review of journal entries and account reconciliations. Specifically, certain personnel have had the ability to both (i) create and post journal entries within our general ledger system, and (ii) prepare and review account reconciliations. This material weakness did not result in a material misstatement to the consolidated financial statements.

- 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. This material weakness did not result in a material misstatement to the consolidated financial statements.

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.

Remediation Plan

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

- we hired and continued to hire additional accounting and finance resources with public company experience, including expertise in technical accounting and complex transactions, 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 are redesigning and strengthening 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 plan can only 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 a variety of 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.

PART III

ITEM 10. DIRECTORS AND EXECUTIVE OFFICERS OF THE REGISTRANT

The information required by this item is hereby incorporated by reference to the Proxy Statement for the 2022 Annual Meeting of Stockholders to be filed with the SEC within 120 days of January 31, 2022.

ITEM 11. EXECUTIVE COMPENSATION

The information required by this item is hereby incorporated by reference to the Proxy Statement for the 2022 Annual Meeting of Stockholders to be filed with the SEC within 120 days of January 31, 2022.

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT AND RELATED SHAREHOLDER MATTERS

The information required by this item is hereby incorporated by reference to the Proxy Statement for the 2022 Annual Meeting of Stockholders to be filed with the SEC within 120 days of January 31, 2022.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS, AND DIRECTOR INDEPENDENCE

The information required by this item is hereby incorporated by reference to the Proxy Statement for the 2022 Annual Meeting of Stockholders to be filed with the SEC within 120 days of January 31, 2022.

ITEM 14. PRINCIPAL ACCOUNTING FEES AND SERVICES.

The information required by this item is hereby incorporated by reference to the Proxy Statement for the 2022 Annual Meeting of Stockholders to be filed with the SEC within 120 days of January 31, 2022.

PART IV

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.

Exhibit Number	Description	Incorporated by Reference			
		Form	File No.	Exhibit	Filing Date
2.1	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.	S-4/A	333-256129	2.1	August 6, 2021
2.2	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.	S-4/A	333-256129	2.2	August 6, 2021
3.1	Amended and Restated Certificate of Incorporation of the registrant.	8-K	001-39125	3.1	September 1, 2021
3.2	Amended and Restated Bylaws of the registrant.	8-K	001-39125	3.2	September 1, 2021
4.1	Specimen Warrant Certificate	S-1/A	333-234124	4.3	October 21, 2019
4.2	Warrant Agreement Between Continental Stock Transfer & Trust Company and the registrant	8-K	001-39125	4.1	November 12, 2019
10.1	Form of PIPE Subscription Agreement	8-K	001-39125	10.3	March 15, 2021
10.2	Amended and Restated Registration Rights Agreement	8-K	001-39125	10.2	September 1, 2021
10.3+	Form of Indemnification Agreement	S-4/A	333-256129	10.12	August 6, 2021
10.4+	IronNet Cybersecurity, Inc. 2014 Equity Incentive Plan, as amended to date	S-4/A	333-256129	10.9	August 6, 2021
10.5+	IronNet, Inc. 2021 Equity Incentive Plan	S-8	333-261158	99.2	November 18, 2021
10.6+	IronNet, Inc. 2021 Employee Stock Purchase Plan	S-4/A	333-256129	10.11	August 6, 2021
10.7+	Form of Stock Option Grant Package under IronNet,Inc. 2021 Equity Incentive Plan	S-8	333-261158	99.3	November 18, 2021
10.8+	Form of RSU Grant Package under IronNet, Inc. 2021 Equity Incentive Plan	S-8	333-261158	99.4	November 18, 2021
10.9+	Employment Agreement, dated May 8, 2019, by and between the registrant and GEN Keith Alexander	S-4/A	333-256129	10.13	August 6, 2021
10.10+	Employment Agreement, dated February 7, 2019,by and between the registrant and William E. Welch	S-4/A	333-256129	10.14	August 6, 2021
10.11+	Employment Agreement, dated February 7, 2019, by and between the registrant and Sean Foster	S-4/A	333-256129	10.15	August 6, 2021
10.12+	Employment Agreement, dated September 6, 2019, by and between the registrant and James C. Gerber	S-1	333-263456	10.15	March 10, 2022
10.13+	Employment Agreement, dated September 19, 2019, by and between the registrant and Donald Closser	S-1	333-263256	10.16	March 10, 2022
10.14	Common Stock Purchase Agreement, dated February 11, 2022, by and between IronNet, Inc. and Tumim Stone Capital LLC	8-K	001-39125	10.1	February 14, 2022
10.15	Registration Rights Agreement dated February 11, 2022, by and between Ironnet, Inc. and Tumim Stone Capital LLC	8-K	001-39125	4.1	February 14, 2022
21.1*	List of Subsidiaries				
23.1*	Consent of PricewaterhouseCoopers LLP				
31.1*	Certification of Principal Executive Officer Pursuant to Rules 13a-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.				
31.2*	Certification of Principal Financial Officer Pursuant to Rules 13a-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.				
32.1^	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.				
101.INS*	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.				
101.SCH*	Inline XBRL Taxonomy Extension Schema Document				
101.CAL*	Inline XBRL Taxonomy Extension Calculation Linkbase Document				
101.DEF*	Inline XBRL Taxonomy Extension Definition Linkbase Document				
101.LAB*	Inline XBRL Taxonomy Extension Label Linkbase Document				
101.PRE*	Inline XBRL Taxonomy Extension Presentation Linkbase Document				
104*	Cover Page Interactive Data File (formatted as inline XBRL with applicable taxonomy extension information contained in Exhibits 101.SCH, 101.CAL, 101.DEF, 101.LAB and 101.PRE).				

* 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.

ITEM 16. FORM 10-K SUMMARY

None.

SIGNATURES

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 2, 2022

By: /s/ James C. Gerber
James C. Gerber
Chief Financial Officer
(On behalf of the Registrant and as Principal Financial Officer)

POWER OF ATTORNEY

KNOW ALL BY THESE PRESENTS, that each of the undersigned hereby constitutes and appoints each of Keith B. Alexander, James C. Gerber 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.

Signature	Title	Date
/s/ GEN Keith B. Alexander (Ret.) GEN Keith B. Alexander (Ret.)	Co-Chief Executive Officer, President and Chairman (Principal Executive Officer)	May 2, 2022
/s/ William E. Welch William E. Welch	Co-Chief Executive Officer and Director	May 2, 2022
/s/ James C. Gerber James C. Gerber	Chief Financial Officer (Principal Financial and Accounting Officer)	May 2, 2022
/s/ Donald R. Dixon Donald R. Dixon	Director	May 2, 2022
/s/ Mary E. Gallagher Mary E. Gallagher	Director	May 2, 2022
/s/ GEN John M. Keane (Ret.) GEN John M. Keane (Ret.)	Director	May 2, 2022
/s/ Robert V. LaPenta Jr. Robert V. LaPenta Jr.	Director	May 2, 2022
/s/ Vadm. John M. McConnell (Ret.) Vadm. John M. McConnell (Ret.)	Director	May 2, 2022
/s/ André Pienaar André Pienaar	Director	May 2, 2022
/s/ Michael J. Rogers Michael J. Rogers	Director	May 2, 2022
/s/ Theodore E. Schlein Theodore E. Schlein	Director	May 2, 2022
/s/ Vadm. Jan E. Tighe (Ret.) Vadm. Jan E. Tighe (Ret.)	Director	May 2, 2022

Exhibit 21.1

Subsidiaries of IronNet, Inc.

Name of Subsidiary	Jurisdiction of Organization
IronNet Cybersecurity, Inc.	United States (Delaware)
High Degree, LLC	United States (Delaware)
IronNet International, LLC	United States (Delaware)
IronNet Cybersecurity Singapore Pte Ltd	Singapore
IronNet Cybersecurity Japan, GK	Japan
IronNet Cybersecurity UK Ltd.	England and Wales
IronNet Australia Pty Ltd.	Australia
IronNet Cybersecurity FZ-LLC	United Arab Emirates

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 2, 2022 relating to the financial statements, which appears in this Form 10-K.

/s/ PricewaterhouseCoopers LLP
Baltimore, Maryland
May 2, 2022

Exhibit 31.1

CERTIFICATION OF PRINCIPAL EXECUTIVE OFFICER PURSUANT TO RULES 13a-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

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):

6.

(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 2, 2022

By: /s/ GEN Keith B. Alexander (Ret.)
GEN Keith B. Alexander (Ret.)
Co-Chief Executive Officer, President and Chairman
(*Principal Executive Officer*)

Exhibit 31.2

CERTIFICATION OF PRINCIPAL FINANCIAL OFFICER PURSUANT TO RULES 13a-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

I, James C. Gerber, 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 2, 2022

By: /s/ James C. Gerber
James C. Gerber
Chief Financial Officer
(*Principal Financial Officer*)

Exhibit 32.1

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

In connection with the Annual Report of IronNet, Inc. (the "Company") on Form 10-K for the year ended January 31, 2022 as filed with the Securities and Exchange Commission on the date hereof, to which this Certification is attached as Exhibit 32.1 (the "Report"), I hereby certify, pursuant to 18 U.S.C. § 1350, as adopted pursuant to § 906 of the Sarbanes-Oxley Act of 2002, that:

(1) The Report fully complies with the requirements of Section 13(a) or Section 15(d) of the Securities Exchange Act of 1934, as amended; and

(2) The information contained in the Report fairly presents, in all material respects, the financial condition of the Company at the end of the period covered by the Report and the results of operations of the Company for the periods covered in the financial statements in the Report.

Dated: May 2, 2022

By: /s/ GEN Keith B. Alexander (Ret.)
GEN Keith B. Alexander (Ret.)
Co-Chief Executive Officer, President and Chairman
(*Principal Executive Officer*)

By: /s/ James C. Gerber
James C. Gerber
Chief Financial Officer
(*Principal Financial Officer*)