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

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): June 16, 2021

LGL SYSTEMS ACQUISITION CORP.
(Exact Name of Registrant as Specified in Charter)

Delaware	**001-39125**	**83-4599446**
(State or Other Jurisdiction of Incorporation)	**(Commission File Number)**	**(IRS Employer Identification No.)**

165 W. Liberty Street, Suite 220 **Reno, NV** **(Address of Principal Executive Offices)**	**89501** **(Zip Code)**

(705) 393-9113
(Registrant's telephone number, including area code)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

☒ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

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

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Units, each consisting of one share of Class A common stock and one-half of one redeemable warrant	**DFNS.U**	**The New York Stock Exchange**
Class A Common Stock, $0.0001 par value per share	**DFNS**	**The New York Stock Exchange**
Redeemable warrants, exercisable for shares of Class A common stock	**DFNS WS**	**The New York Stock Exchange**

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

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. ☐

Item 8.01. Other Events.

The report attached hereto as Exhibit 99.1 (the "Report") was commissioned and utilized by management of LGL Systems Acquisition Corp. ("LGL") in connection with its evaluation of its proposed merger with IronNet Cybersecurity, Inc. ("IronNet"). The Report is incorporated into this Item 8.01 by reference.

Important Information and Where to Find It

This report and the Report relate to a proposed transaction between LGL and IronNet. LGL has filed with the Securities and Exchange Commission ("SEC") a registration statement on Form S-4 (as the same may be amended, the "Registration Statement") that includes a proxy statement to be distributed to LGL's stockholders in connection with LGL's solicitation of proxies for the vote by LGL's stockholders in connection with the proposed business combination and other transactions described in the Registration Statement, as well as a preliminary prospectus relating to the offer of LGL's securities to be issued to IronNet's stockholders in connection with the completion of the proposed business combination described in the Registration Statement. After the Registration Statement is declared effective, LGL will mail the definitive proxy statement/prospectus to stockholders of LGL as of a record date to be established for voting on the proposed business combination. LGL also will file other relevant documents from time to time regarding the proposed transaction with the SEC. INVESTORS AND SECURITY HOLDERS OF LGL ARE URGED TO READ THE PRELIMINARY PROXY STATEMENT/PROSPECTUS AND, ONCE AVAILABLE, THE DEFINITIVE PROXY STATEMENT/PROSPECTUS AND OTHER RELEVANT DOCUMENTS THAT HAVE BEEN OR WILL BE FILED BY LGL FROM TIME TO TIME WITH THE SEC CAREFULLY AND IN THEIR ENTIRETY BECAUSE THEY CONTAIN OR WILL CONTAIN IMPORTANT INFORMATION ABOUT THE PROPOSED TRANSACTION. Investors and security holders will be able to obtain free copies of the proxy statement/prospectus and other documents containing important information about LGL and IronNet once such documents are filed with the SEC, through the website maintained by the SEC at http://www.sec.gov. Copies of the documents filed with the SEC by LGL when and if available, can be obtained free of charge on LGL's website at https://www.dfns.ai or by directing a written request to LGL Systems Acquisition Corp., 165 Liberty St., Suite 220, Reno, NV 89501 or to info@dfnsi.ai.

Participants in the Solicitation

LGL and IronNet and their respective directors and executive officers, under SEC rules, may be deemed to be participants in the solicitation of proxies of LGL's stockholders in connection with the proposed transactions. Information regarding the persons who may, under SEC rules, be deemed to be participants in the solicitation of proxies from LGL's stockholders in connection with the proposed transactions described in the Registration Statement and the interests that such persons have in such transactions are set forth in the proxy statement/prospectus included in the Registration Statement.

No Offer or Solicitation

This communication shall neither constitute an offer to sell or the solicitation of an offer to buy any securities, nor shall there be any sale of securities in any jurisdiction in which the offer, solicitation or sale would be unlawful prior to the registration or qualification under the securities laws of any such jurisdiction.

Item 9.01. Financial Statements and Exhibits.

Exhibit No.	Descripton
99.1	Report, dated February 23, 2021, titled, *Independent Assessment of IronNet Cybersecurity, Inc*., prepared by 5by5 Consulting LLC

SIGNATURE

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

Date: June 16, 2021

By: /s/ Robert LaPenta Jr.
Name: Robert LaPenta Jr.
Title: Co-Chief Executive Officer and Chief Financial Officer

Important Information and Where to Find It

This following report relates to a proposed transaction between LGL Systems Acquisition Corp. ("LGL") and IronNet Cybersecurity, Inc. ("IronNet"). LGL has filed with the Securities and Exchange Commission ("SEC") a registration statemsent on Form S-4 (as the same may be amended, the "Registration Statement") that includes a proxy statement to be distributed to LGL's stockholders in connection with LGL's solicitation of proxies for the vote by LGL's stockholders in connection with the proposed business combination and other transactions described in the Registration Statement, as well as a preliminary prospectus relating to the offer of LGL's securities to be issued to IronNet's stockholders in connection with the completion of the proposed business combination described in the Registration Statement. After the Registration Statement is declared effective, LGL will mail the definitive proxy statement/prospectus to stockholders of LGL as of a record date to be established for voting on the proposed business combination. LGL also will file other relevant documents from time to time regarding the proposed transaction with the SEC. INVESTORS AND SECURITY HOLDERS OF LGL ARE URGED TO READ THE PRELIMINARY PROXY STATEMENT/PROSPECTUS AND, ONCE AVAILABLE, THE DEFINITIVE PROXY STATEMENT/PROSPECTUS AND OTHER RELEVANT DOCUMENTS THAT HAVE BEEN OR WILL BE FILED BY LGL FROM TIME TO TIME WITH THE SEC CAREFULLY AND IN THEIR ENTIRETY BECAUSE THEY CONTAIN OR WILL CONTAIN IMPORTANT INFORMATION ABOUT THE PROPOSED TRANSACTION. Investors and security holders will be able to obtain free copies of the proxy statement/prospectus and other documents containing important information about LGL and IronNet once such documents are filed with the SEC, through the website maintained by the SEC at http://www.sec.gov. Copies of the documents filed with the SEC by LGL when and if available, can be obtained free of charge on LGL's website at https://www.dfns.ai or by directing a written request to LGL Systems Acquisition Corp., 165 Liberty St., Suite 220, Reno, NV 89501 or to info@dfnsi.ai.

Participants in the Solicitation

LGL and IronNet and their respective directors and executive officers, under SEC rules, may be deemed to be participants in the solicitation of proxies of LGL's stockholders in connection with the proposed transactions. Information regarding the persons who may, under SEC rules, be deemed to be participants in the solicitation of proxies from LGL's stockholders in connection with the proposed transactions described in the Registration Statement and the interests that such persons have in such transactions are set forth in the proxy statement/prospectus included in the Registration Statement.

No Offer or Solicitation

This communication shall neither constitute an offer to sell or the solicitation of an offer to buy any securities, nor shall there be any sale of securities in any jurisdiction in which the offer, solicitation or sale would be unlawful prior to the registration or qualification under the securities laws of any such

Independent Assessment of IronNet Cybersecurity Inc.

23 Feb 2021

Prepared by

Jeff Buss, Captain (Ret.) USN (MS, MBA, MS, CISSP, SEC+, C|EH, ITIL v3)

William Ogle (MS, CISSP, CISM, CISA, CDPSE, CIPM)

5by5 Consulting LLC

9801 Washingtonian BLVD, Suite 200

Gaithersburg, MD 20878

240-600-0953

Limitation of Liability:

5by5 Consulting has used its best efforts in producing this report for the client in accordance with the client's request and time provided. 5by5 Consulting cannot be held responsible for any specific issues, risks, opportunities, recommendations, processes, strategies or tools identified in this report. 5by5's obligation to the client terminates upon the delivery of the final version of this report. 5by5 will not be liable for any incidental, special, punitive, indirect or consequential damages of any kind including, without limitation, lost profits, lost data, lost revenues and loss of business opportunity whether or not 5by5 Consulting was aware or should have been aware of the possibility of these damages. The maximum liability that 5by5 consulting could be deemed to have to the client is the amount equal to the fee paid for the services provided.

Table of Contents

Overview

This is an independent assessment of IronNet Cybersecurity Inc. (IronNet) conducted by 5by5 Consulting LLC in February of 2021. The purpose of this assessment is twofold, first is to examine the platform and services IronNet offers to gauge the market viability of those offerings. Second is to examine the internal defensive measures in place at IronNet as of February 2021 to assess if reasonable controls have been put in place to secure clients as well as corporate data. This assessment was conducted both virtually as well as on-site and included a document review, interviews with IronNet's leadership team, a site visit and customer interviews.

Executive Summary

> *"While in government we saw attacks that could have been prevented if companies had the ability to work together collectively, in real-time to share insights and to collaborate on defenses. IronNet was created to fill that void."*
> -General (Ret.) Keith Alexander, Founder and Executive Chairman, Former Director of the NSA & US Cyber Command

IronNet is a highly capable, metric-driven organization with a differentiated and potentially transformational approach to the cybersecurity problem facing every organization today. With an ever-increasing cyber security threat posed by advanced persistent threat (APT) actors, who better to help solve this problem then the longest standing Director of the National Security Agency (NSA) and Commander of Cyber Command in our Nation's history, General Keith Alexander and the team of experts he has assembled? It takes knowledge of how advanced persistent threats (APT) operate and their tactics, techniques and procedures in order to defeat them, few individuals and even fewer companies have that knowledge or capability. IronNet's unique market offering called IronDome offers users a collective defense model to help mitigate threats posed by an APT enhanced by their IronDefense platform. Said another way, clients might actually have a chance against an APT with this technology, because let's face it, right now, they don't.

A look at whether IronNet has reasonable defensive measures in place across people, processes and technology found that they have invested a lot of time and effort into their security architecture and have obtained an impressive array of certifications as well as have undergone extensive audits and testing to ensure they are meeting industry standards. They have highly skilled people in critical security roles and have mature processes in place for crucial areas like change management, data protection and software development. They have a robust technology stack to defend their network and skilled analysts to operate them. IronNet takes training seriously and requires annual training for all members of the organization on information security and has a defined training track for their security analysts. While this is not a guarantee a company will not have a security breach, we have found that IronNet has taken reasonable precautions to protect against it.

Approach

In order to assess IronNet's product, services, market position as well as internal defensive measures the following approach was used.

1. A document request list was submitted, and a review of documentation posted in the data site repository was conducted.
2. Interviews were conducted with the majority of the senior leadership team to include the Chief Information Officer (CIO)/Chief Information Security Officer (CISO), Head of Product Development, Co-Chief Executive Officer's (CEO)and Chief Financial Officer (CFO).
3. Video teleconferences were held with key clients (3).
4. A site visit was conducted at the Mclean, Virginia IronNet offices.

IronNet – Overview

Based in the greater Washington DC area, IronNet was founded in 2014 and offers three products (IronDome, IronDefense and Digital Detect) in addition to a variety of cyber security services. The vast majority of their current revenue comes from their IronDome and IronDefense products which will be the focus of this assessment. IronDefense is a network detect and response 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 unique cyber tradecraft knowledge, alerts produced by IronNet help analysts quickly contextualize and prioritize threats that pose the greatest risks. By doing this IronNet is able to provide clients, across a variety of industries, nation-state-level defensive capabilities to reduce cyber risk. Do clients need this type of service? The Cyberspace Solarium Commission report suggests they do.

> *"The reality is that we are dangerously insecure in cyber. Your entire life-your paycheck, your health care, your electricity, increasingly relies on networks of digital devices that store, process and analyze data. These networks are vulnerable, if not already compromised. Our country has lost hundreds of billions of dollars to nation-state-sponsored intellectual property theft using cyber espionage."*[1]

1 (Solarium, 2020)

Network Detection and Response (NDR) Market

Overview

IronNet is categorized by Gartner to be in the NDR segment of the cybersecurity market. Gartner characterizes vendors in the NDR markets as those companies that specialize in using advanced analytical techniques like machine learning and automated intelligence, to continuously analyze network traffic, flow records and log data.[2] NDR vendors are able to go beyond the traditional signature-based techniques, like virus scanning and basic intrusion detection systems which can tell if you are infected, to a more proactive behavior-based analysis identifying symptoms that you might be infected. Using a medical analogy, going to the doctor for a COVID test will tell you if you are infected with the virus vs behavior analytics which observes your symptoms (loss of taste, loss of smell etc.) and behaviors (going to a large super-bowl party) to let you know you have a high probability of having an infection. In order for signature-based methods to be effective, the virus must first be understood and thus it is reactive in nature and only identifies known threats. Hacker's techniques have advanced dramatically in the past 5 years and signature-based detection is often not effective at recognizing unknown or advanced attacks. An example of this is the recent SolarWinds incident where hackers were able to install a backdoor via a software update allowing them to install malware, which in turn allowed them to spy on their victims. This type of advanced attack is not able to be detected using the traditional signature-based approach.

In their 11 June 2020 article entitled "Market Guide for Network Detection and Response" Gartner analyzed 17 companies in what they referred to as a "crowded market with low barrier to entry".[3] In order to be included in this category vendors had to meet the following requirements:

- Analyze raw network packet traffic or traffic flows (for example, NetFlow records) in real time or near real time.
- Monitor and analyze north/south traffic (as it crosses the perimeter), as well as east/west traffic (as it moves laterally throughout the network).
- Be able to model normal network traffic and highlight suspicious traffic that falls outside the normal range.
- Offer behavioral techniques (non-signature-based detection), such as machine learning or advanced analytics that detect network anomalies.
- Provide automatic or manual response capabilities to react to the detection of suspicious network traffic.

2 (Bricata, 2021)
3 (Orans, 2020)

Two areas of differentiation noted in the article were the ability to terminate, decrypt and analyze Transport Layer Security (TLS) traffic natively as well as the ability to provide automated response capabilities. IronNet, it was noted, does not decrypt TLS traffic. It was discovered during interviews and document review that IronNet has numerous abilities and algorithms using AI, ML and behavioral analytics to detect suspicious TLS traffic. An example of this is their Certificate Spike Analytic that detects illegitimate TLS beaconing. For automation, IronNet integrates with SIEM and SOAR tools allowing for users to automate responses but does not currently offer automated response as a service offering. Adding TLS break and inspect as well as automated response may be something for IronNet to consider in the future as they scale their business.

IronNet's key differentiator in the market is the concept of collective defense which no other vendors we found in the NDR market offer. This transformational approach infused with rich data, tradecraft knowledge, advanced analytics and a scalable, easy to use platform offers a potential means for IronNet to disrupt the cybersecurity market.

Collective Defense – Why it matters

Ideally the US Government could defend the nation against cyber-attacks similar to what was developed for the Intercontinental Ballistic Missile (ICBM) missile threat. Unfortunately, the ability of the US Government to enact such a defense would likely require limiting personal freedoms on the internet that the American people 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. The Cyberspace Solarium Commission report submitted in July of 2020 contains over 80 recommendations to address the issue of cybersecurity with one of them being "Reshaping the Cyber Ecosystem".

> "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." [4]

4 (Solarium, 2020)

IronNet's 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 IronNet's portfolio of offerings and one of the few companies that have the ways, ends and means to enact this transformational concept due to the technical capabilities required to ensure its success.

How it works

IronNet offers two primary platforms, IronDefense and IronDome that work together to provide clients a unique cybersecurity solution that transcends most of the cyber security offerings available today. IronDefense receives network traffic via a virtual or physical device to capture network traffic e.g., Switch Port Analyzer (SPAN) port on a switch. Deep packet inspection is then performed, and metadata is forwarded to the IronDefense servers located in the Amazon Web Services (AWS) cloud. Analysts then apply behavior models, AI and ML to identify anomalous behavior and a score is determined (1-1000) based on the severity of the behavior determined by the analytic. Informed by IronDefense's Expert System the risk scored alert is delivered to the client via a secure portal or ingested into the clients Security Information and Event Management (SIEM) tool e.g. Splunk, QRadar. This provides the analyst a way to prioritize and triage alerts based on criticality, greatly reducing the number of alerts they need to take action.

Data from IronDefense is anonymized and sent to the IronDome system which then allows for sharing across industry sectors. The concept of IronDome is unique, grouping data from companies related by industry or infrastructure profile, focusing AI, ML, and behavior analytics on those data sets to detect advanced threats and then communicating the results to subscribers. Chart 1 below illustrates how IronNet delivers value via the collective defense model and illustrates how in 2020 they took 4.6 million alerts and turned them into 2,089 prioritized and scored indicators of compromise for their clients.

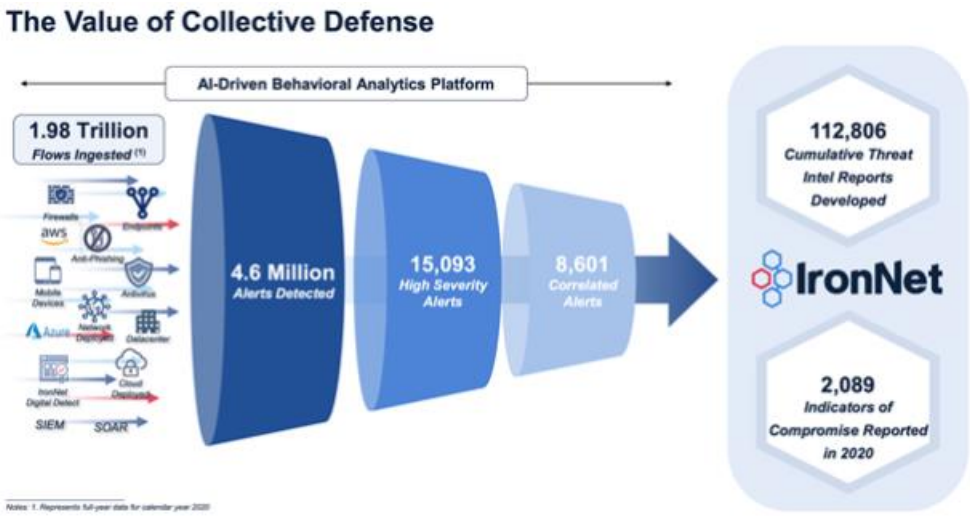


Figure 1. The Value of Collective Defense[5]

Key features of IronNet[6]

- Tradecraft Expertise: Knowledge of APT's tactics, techniques and procedures is applied throughout the IronNet process.
- Advanced Analytics: AI, ML, behavioral analytics along with operational tradecraft expertise is used to identify advanced/unknown threats.
- Expert System: Orchestrates contextual data and tradecraft cyber expertise to determine risk of identified anomalies to the organization.
- Integrated Hunt: Enables seamless pivoting from detection to investigation by providing packet-level visibility and integrated data enrichments to help investigate threats.
- Collective Defense: IronDome delivers threat insights and visibility across industry participants enabling proactive detection and collective response to threats targeting the industry.

5 (IronNet, 2021)
6 (IronNet, 2021)

Business Value

IronNet in the Security Operation Center (SOC)

In the Second Annual Study on the Economics of Security Operations Center released in January 2021 by the Ponemon Institute LLC[7], they reported that the perceived return on investment of the SOC is dropping, mainly due to the complexity of the SOC responsibilities. This problem is exacerbated by the continuously evolving threat landscape as well as the plethora of tools on the market to help solve parts of the problem. Figure 1 below illustrates that the minimization of false positives, threat intelligence reporting, the use of technologies such as automation and machine learning, intrusion detection and threat hunting are all rated as being very important for a SOC. IronNet's products cover all of those highly important SOC activities and delivers prioritized indicators of compromise data to the end user in an easy to digest and easy to investigate fashion.

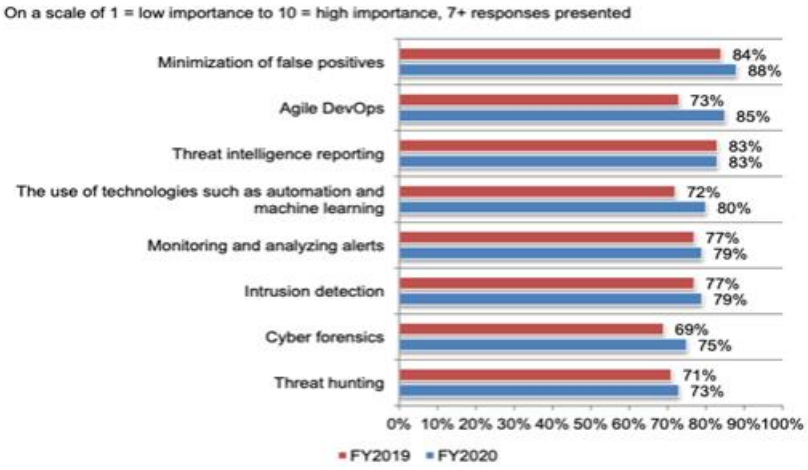


Figure 2. The Importance of SOC Activities[8]

7 (Ponemon, 2021)
8 (Ponemon, 2021)

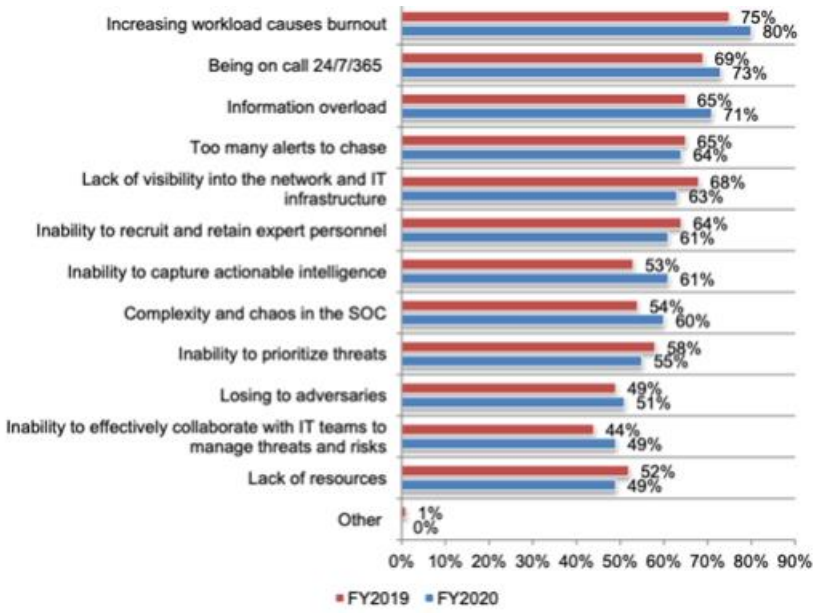


Figure 3. What makes working in the SOC painful?[9]

When asked "what makes working in the SOC so painful?", Ponemon Institute survey participants responded with the following responses as indicated in Figure 3. IronDefense and IronDome are designed to help reduce SOC workload, reduce information overload, reduce the number of alerts to chase, allow greater visibility into a network and IT infrastructure, capture and share actionable intelligence, reduce chaos and complexity in the SOC, prioritize threats and allow for collaboration across industries. IronNet can help make working in the SOC less painful by addressing eight of the twelve pain points identified in the Ponemon institute survey for SOC operators. Clients verified that the IronNet approach works, and does indeed help reduce alert fatigue, which could make working in a SOC a little less painful.

9 (Ponemon, 2021)

IronNet Capability vs the SIEM Market

IronNet integrates currently with SIEM technologies vs competes with them. IronNet delivers high fidelity alerts in a prioritized/triaged fashion using their scoring mechanism and feeds those alerts into a SIEM system or user portal. As seen in Chart 1 turning 4.6 million alerts into 2,086 indicators of compromise is what most SIEM tools attempt to do but require the user to cull through the 4.6 million alerts to do it. One of the challenges most SIEM users face is getting all of needed data forwarded into the SIEM tools correctly. Without the correct data, a SIEM is of little value. Many SIEM providers charge "by the drink" based on the volume of data going into the SIEM and requires users to understand this data and what value can be derived from it to most effectively utilize their SIEM tool. IronNet is able to harvest a rich pool of data using their netflow and packet capture technology which alleviates the need to ensure users get the data ingestion set up perfectly into their SIEM environments. Where and how to place these sensors as well as tuning them is done by the IronNet team in collaboration with the client. This is of substantial value for a security team with the potential added benefit of being able to conduct real time asset and data lineage mapping.

IronNet Capability vs the NDR Market

Gartner refers to the NDR market as a "*crowded market with low barrier to entry*" and thus differentiating the IronNet product and services to show clear value are critical to establish and gain market share in the NDR market. [10] IronNet's key differentiator in the NDR market includes tradecraft knowledge of APTs tactics, techniques and procedures as well as a unique means to help their clients defend against these high-end pervasive actors via the collective defense model they refer to as IronDome. Another differentiator in the NDR market for IronNet is the way they perform behavioral detection, leveraging both AI and ML techniques. IronNet's behavioral detection analytics includes supervised and unsupervised ML used by some technologies in the NDR market. The AI/ML and behavioral analytics methodology that IronNet uses, complimented by their tradecraft knowledge, provides an advantage in the NDR market to deliver detection of advanced threats that other competitors are unable to see. With an impressive list of key differentiators, happy clients, key partnerships across leading cybersecurity companies and the added benefit of collective defense via IronDome, IronNet is well positioned from a technology standpoint to lead the NDR market going forward.[11]

Who will benefit from IronNet products?

It would be hard to find a company that would not benefit from the advanced detection and collective defense capabilities offered by IronNet, making the total addressable market for the IronNet product very large and growing. IronDome is a new, transformational approach that

10 (Orans, 2020)
11 (451 Research LLC , Sept 2019)

could potentially disrupt what analysts project to be a $238B market in cybersecurity by 2023.[12] IronNet will likely benefit from the recent SolarWinds breach as their technology is one of the few that was able to pick up the adversary's activity using advanced analytics. Customers confirmed that IronNet is faster and more accurate at identifying threats than their in-house tools and because of IronNet's technology they are able to reduce the number of tools in their inventory. Large public and private organizations as well as managed service providers will likely benefit the most from IronNet's technology. Managed service providers can then pass off the value of IronNet's products down to smaller customers.

Challenges

Gartner puts NDR in the Trough of Disillusionment in their hype cycle for security operations report for 2020 and cites that it will be two to five years before there is mainstream adoption for NDR products. Gartner defines the "*Trough of Disillusionment*" as "*the technology does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.*" Gartner goes on to further state that "NDR has begun to pull out of the Trough of Disillusionment as adoption of the tools continues to grow" and cites the following recommendations for those looking at NDR vendors [13]

- NDR users need to ensure their security teams have the training needed to effectively operate the NDR platforms and gain the maximum value from their purchase.
- More and more traffic is being encrypted via SSL/TLS.
- Careful planning and coordination is needed for NDR sensor placement as is the line rate capture of the sensors used for NDR.
- A keen understanding of traffic patterns and protocol patterns is needed in order to maximize value of the investment in an NDR platform.
- There is significant competition in the space with vendors like Darktrace, ExtraHop and FireEye.

Trust is vital for IronNet to succeed. Allowing access to sensitive packet capture data requires a significant amount of client trust. Thus, a breach would be potentially devastating for IronNet. Ensuring effective internal defensive measures are in place for security and privacy are of paramount importance for IronNet's business model to be successful. As IronNet's profile increases so does their probability of being targeted by an APT.

12 (Statista, 2021)
13 (Shoard, 2020)

Security and Privacy - Internal Defensive Measures (IDM)

IronNet demonstrates a comprehensive and effective security program. Reasonable measures have been put in place across technology, processes and people to ensure controls meet or exceed industry best practices and are evidenced by a lack of critical vulnerabilities, no security breaches noted as well as extensive audits (SOC 2, GDPR, FedRAMP and ISO 27001) attested by independent 3rd parties.

Technology

IronNet uses the National Institutes of Standards and Technology (NIST) Cyber Security Framework (CSF) five key functions of cybersecurity (Identify, Protect, Detect, Respond, Recover) as a framework to ensure controls are in place across their enterprise.[14] This is an industry best practice and allows for a standardized way to articulate their IDM efforts and technology in place to support the defense of their network. IronNet's security architecture is built with defense in depth and uses a variety of tools and technology to support the NIST CSF 5 key functions of cybersecurity (see below). AWS resources are used and aid in providing a scalable and DEVOPS friendly environment. The use of AWS also aids in their resilience in terms of business continuity and disaster recovery.

IronNet has over 50 different software/technologies deployed across their enterprise.[15] [16]
They have a well-defined technology roadmap both for internal security tools and for their IronDefense and IronDome products, enhanced by their mature software development life cycle and change management processes (see section on processes). IronNet uses many of these technologies to help secure their network to ensure confidentiality, integrity and availability of both their internal and external platforms.

The effective orchestration of their extensive technology investment was illustrated during a conversation with the IronNet CIO/CISO, where it was stated that there are no outstanding critical vulnerabilities over 60 days old. A deeper look found KirkpatrickPrice performed a Red Team assessment on IronNet's web application and API assets, the report was issued 5 Feb 2021 with only one medium finding that was reported as remediated.[17] A more comprehensive Red Team test was completed by KirkpatrickPrice from 15 June 2020 – 3 July 2020 with follow ups performed 8 Sept 2020 and 27 Jan 2021. The Red Team report dated 27 Jan 2021 found five Critical, eight High and ten Medium vulnerabilities that were verified remediated by

14 (NIST, 2021)
15 (Kratos Defense, 2020)
16 (IronNet, 2021)
17 (KirkpatrickPrice, 5 Feb 2021)

KirkpatrickPrice prior to the 27 Jan 2021 report.[18] While a Red Team is not able to go through every attack scenario, it is a good validation of the sufficiency of the entire security program and the organizations' ability to withstand most attacks from unauthorized parties to gain access to IronNet systems and data. It was noted in the data review that "Data security incidents of data breaches suffered by the Company is not applicable to IronNet", which is also a good indicator that the IronNet security team knows how to effectively defend their network.

Kratos, serving as a third-party assessment organization (3PAO), conducted a comprehensive readiness assessment as part of the FedRAMP program on the IronCloud Software as a Service (SaaS) offering 14 April 2020 – 15 May 2020. This in-depth assessment was culminated in a 62 page report dated 22 July 2020 and looked at IronNet's System Security Plan, policies, procedures, Contingency Plan, Incident Response Plan, Configuration Management Plan, as well as vulnerability and configuration scans for the infrastructure, web applications, and databases. Findings of the assessment:[19]

> "IronNet is fully prepared to support Federal Government customers in the IronCloud environment. IronCloud is compliant with the required Federal mandates, including the requirement for use of only FIPS 140-2 validated cryptographic modules, integration of Common Access Card/Personal Identity Verification (CAC/PIV) credentials, Digital Identity level 2 requirements, active vulnerability remediation, and records management."

Kratos also noted the following strengths.

- Strong leadership and commitment to the FedRAMP program
- Mature, well defined, and comprehensive configuration management using defined AWS components to deploy the SaaS services. Inheriting services from the AWS GovCloud provides a comprehensive baseline configuration.

Protection of client data

Ensuring the protection of client data is critical for the collective defense model to be successful. A review of controls in place was highlighted in the FedRAMP assessment conducted by Kratos: [20]

- IronNet customers access their data over the internet via traffic traversing through the IronDefense external boundary, which is protected with gateways, routers, firewall, encrypted tunnels, web content filters, data loss prevention, and additional boundary protections.
- Data from IronNet sensors that are deployed on a customer's network is separated physically via the AWSback-end.

18 (KirkpatrickPrice, 27 Jan 2021)
19 (Kratos Defense, 2020)
20 (Kratos Defense, 2020)

- All programmatic communication is done via Application Programming Interfaces' (API) and a customer's browser using HTTPS over TLS 1.2.
- IronCloud is a multi-tenant environment and provides separation of customer data in several ways.
    - Each customer has a dedicated virtual private cloud (VPC) containing that customers data and each customer has a dedicated S3 bucket encrypted with a unique advanced encryption standard (AES) key.

In summary, IronNet has a well thought out security architecture to handle their customers data with the appropriate technologies and mechanisms in place to provide reasonable assurance to customers that their data is protected.

Process

The IronNet platform as well as their security architecture is built following modern architecture practices including a Software Development Life Cycle (SDLC) inclusive of Continuous Delivery and Continuous Integration (CI/CD). The CI/CD and agile software pipeline is a strength of IronNet helping with their ability to rapidly respond to the market for feature requests, feature enhancements and product updates. IronNet's SDLC process is well documented and is maturing into the full adoption of the CI/CD process which will likely benefit them in the future. It was also noted that IronNet performs static application security testing (SAST) via SonarQube which enhances release code quality, application security and helps ensure that a company's codebase is clean. This is an industry best practice and illustrates a commitment to producing quality code for external and internal use.

IronNet has a formalized and well-defined change management process that is in line with industry best practices. The have a weekly, bi-monthly and monthly recurring meetings focused on ensuring impacts of changes are properly vetted with key stakeholders from across the organization and that changes are approved and tracked. IronNet includes a Threat Working Group as well as integration of open-source intelligence and commercial threat intelligence feeds into their change management process which is a leading practice not seen at most companies. This is highlighted by the inclusion of their Red Team into the change management process.

IronNet security and privacy processes are well documented and evidenced by third-party auditor attestations listed below. The investment in third-party attestations provide reasonable assurance that the product, process, and service conform to industry best practices. These certifications and audits were not well advertised on their website or in some of the client facing material reviewed and may be an area for IronNet to consider in the future.

- **ISO/IEC 27001:2013 Certified since 2017**[21]

  The ISO/IEC 27001 standard is an internationally recognized "Information Security Management System" to help organizations manage policies and processes to achieve cyber security objectives. The ISO/IEC 27001 certification is administered through a third party who conducts an independent audit to validate adherence to the security controls.

  The ISO/IEC 27001 Certification demonstrates the organizations compliance with the mandated requirements and illustrates the certified organizations commitment to use industry best practices.

- **System and Organization Controls Report (SOC) Type I and Type II audits**

IronNet underwent a Type II System and Organization Controls Report (SOC) audit that covered the period 01 Sept 2019 – 31 Aug 2020. A SOC Type 1 report provides managements description of a service organizations system and an auditor report on that description. A SOC Type II goes a step further and provides an auditor report and opinion of the operating effectiveness and controls and requires evidence to be provided regarding how those control have operated over a period of time. IronNet's SOC Type II report is 103 pages long and contained the following findings:[22]

- "The controls stated in the description were suitably designed throughout the period 1 September, 2019, to August 31, 2020, to provide reasonable assurance that IronNet CyberSecurity, Inc.'s service commitments and system requirement would be achieved based on applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary control assumed in the design of IronNet Cybersecurity Inc.'s control throughout that period."
- "The controls stated in the description operated effectively throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that IronNet CyberSecurity, Inc.'s service commitments and system requirements were achieved based on applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of IronNet Cybersecurity, Inc.'s controls operated effectively throughout that period."

21 (see Appendix B)
22 (KirkpatrickPrice, 1 Sept 2019 – 31 Aug 2020)

- **EU General Data Protection Regulation (GDPR)**

  KirkpatrickPrice performed a compliance audit for IronNet Cybersecurity which concluded on 31 August 2020[23] A review of the approach used by KirkpatrickPrice found that an in-depth analysis of the 49 GDPR articles was conducted via interviews, policy reviews and evidence collection for each of the questions contained in the articles. Each question was assessed in detail with findings and recommendations noted for each highlighted in a 100-page audit report. No major findings were noted.

  - "Based on our objective analysis, we determined that IronNet Cybersecurity, Inc. has implemented safeguards that meet the protections required by GDPR, and the data protection program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of nonpublic personal information is protected as of August 31, 2020."

- **Member of the Swiss-U.S. Privacy Shield Framework**

  IronNet holds a certification until 31 Dec 2021 and has a Compliance Certificate from the European Data Protection Office which is valid until 8 Nov 2021.

- **Department of Homeland Security Continuous Diagnostics and Monitoring Program** IronNet is registered with the Department of Homeland Security (DHS) Continuous Diagnostics and Monitoring (CDM) program, recognizing cybersecurity tools and sensors are reviewed by the DHS program for conformance with Section 508 Federal license users and CDM technical requirements

  - **Finding:** In 2018 IronNet received two acceptances/approvals for the DHS Continuous Diagnostics & Monitoring Approved Products List (CDM APL) for IronDefense (IRO-0002-20180103) and IronDome (IRO-0004-20180405)

- **FedRamp Accreditation**

  FedRAMP "Ready" designation on 29 July 2020 (Package ID FR2020681957) indicating an accredited 3rd Party Assessor attested to the readiness of IronNet's cloud offering. [24]

  - **Finding:** Listed on the FedRAMP Marketplace as a FedRAMP ready vendor (see Attachments)

23 (KirkpatrickPrice, 31 August 2020)
24 (Kratos Defense, 2020)

People

IronNet has an impressive portfolio of cybersecurity leaders in their organization to include their security department, which is separate from their external facing security organization they referred to as the CyOC. Having two separate, but complimentary security organizations is a strength of IronNet as they are able to leverage talent across the two when necessary. IronNet's SOC team is all US based and offshore resources are used, mainly in India, to help with API development.

IronNet's organizational roles and responsibilities follows a traditional hierarchical structure as evidenced from the SOC 2 Report.[25] The CIO/CISO reports directly to the Co-CEO's. The size of the SOC team, span of control and structure are aligned with industry best practices. A strength noted in multiple reports was IronNet's training program which includes standard and advanced training, such as training in threat hunting. IronNet provides product, cyber skill set training, cyber exercises, and workforce development to both clients and IronNet personnel. One of the key differentiators for IronNet is having tradecraft knowledge of how APT's operate which they use not only externally for clients but internally as well. Normal turnover was noted for key personnel in the security operation center. There has been some turnover of senior technical staff which is something IronNet needs to consider as they evolve their business as ensuring retention of critical technical staff will likely be vital for IronNet and their brand going forward.

25 (KirkpatrickPrice, 1 Sept 2019 – 31 Aug 2020)

References

51 Research LLC . (Sept 2019). *Network Visibility, Detection and Response.* 451 Research LLC .
Bricata. (2021). Retrieved from https://bricata.com/blog/signature-detection-vs-network-behavior/.
IronNet. (2021, Febuary). IronNet Sales & Product Presentation. (Will Ogle, Jeff Buss, Interviewer)
Keith Alexander, D. C. (2021, Febuary). Interviews with CISO/CIO and Head of Product Development . (Will Ogle, Jeff Buss, Interviewer)
KirkpatrickPrice. (31 August 2020). *GDPR Compliance Audit.* KirkpatrickPrice.
KirkpatrickPrice. (1 Sept 2019 – 31 Aug 2020). *IronNet Cybersecurity, Inc. Type II System and Organization Controls Report (SOC 2)* .KirkpatrickPrice.
KirkpatrickPrice. (27 Jan 2021). *Internal|External|Database|Social Engineering Penetration Test Remediation Report.* KirkpatrickPrice.
KirkpatrickPrice. (5 Feb 2021). *Web Application and API Penetration Test Remediation Report.* KirkpatrickPrice.
Kratos Defense. (2020). *FEDRAMP Moderate Readiness Assessment Report (RAR) Version 1.3.* Kratos Defense.
NIST. (2021, Feb). *Cyberframework Five-Functions.* Retrieved from NIST Cyber Framework: https://www.nist.gov/cyberframework/online-learning/five-functions
Orans, L. H. (2020, June). *Market Guide for Network Detection and Response*. Retrieved from Gartner: www.gartner.com
Ponemon. (2021, January). *Second Annual Study on the Economic of Security Operation Centers: What is the true Cost for Effective Results? Jan 2021, Ponemon Institute, Sponsored by FireEye.* Retrieved from respond-software.com: https://respond-software.com/resources/reports-ebooks/second-economics-of-the-soc/
Shoard, P. (2020, June 23). *Hype Cycle for Security Operations.* Retrieved from Gartner: https://www.gartner.com
Solarium. (2020, July). *United States of America Cyberspace Solarium Commission Report, July 2020.* Retrieved from www.Solarium.gov/report.
Statista. (2021, Feb). *Worldwide-security-as-a-service-market-size.* Retrieved from Statista.com: https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

Glossary of Terms, Abbreviations and Acronyms

3PAO	Third Party Assessment Organization
AES	Advanced Encryption Standard
API	Application Programming Interface
APT	Advanced Persistent Threat
AWS	Amazon Web Services
CAC/PIC	Common Access Card/Personal Identity Verification
CDM	Continuous Diagnostics and Monitoring
CI/CD	Continuous Integration and Continuous Delivery
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSF	Cyber Security Framework
CyOC	Cyber Operations Center at IronNet
DHS	Department of Homeland Security
EDR	Endpoint Detection and Response
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
HTTPS	Hypertext Transfer Protocol Secure
IDM	Internal Defensive Measures
NDR	Network Detection and Response
NIST	National Institutes of Standards and Technology
SAST	Static Application Security Testing
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SOAR	Security Orchestration and Automated Response
SOC	Security Operations Center
SOC 2	System and Organization Controls Report – Type II
SPAN	Switched Port Analyzer
SWOT	Strengths, Weaknesses, Opportunities and Threats
TAM	Total Addressable Market
TLS	Transport Layer Security
VPC	Virtual Private Cloud

Appendix A: Strengths Weaknesses Opportunity Threats (SWOT) Analysis

Strengths Weaknesses Opportunity Threats (SWOT) Analysis

Strengths:

- Leadership Team
- Strong vision and purpose
- Scalable products that solve a significant need
- In-depth tradecraft knowledge
- Great customer service

Weaknesses

- Crowded NDR market
- Low barrier to entry into the NDR market
- A high level of trust is required for clients
- IronDefense does not break TLS traffic
- No auto-mitigation/automated response
- Turnover of technical personnel

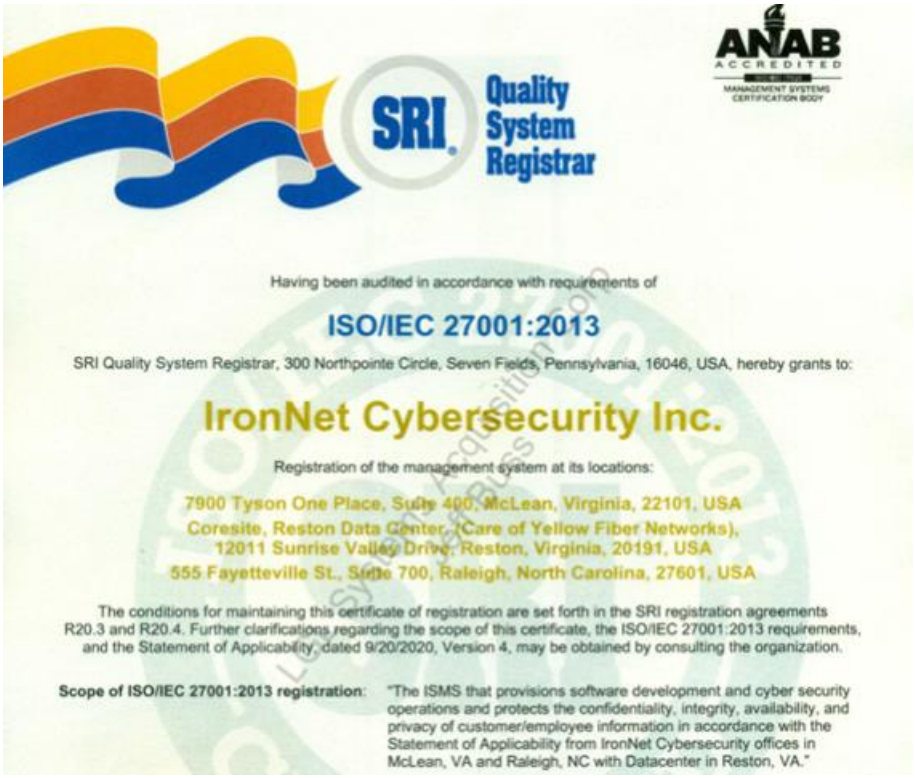
Opportunities

- IronDome is potentially Transformational
- Federal market
- Large and increasing Total Addressable Market (TAM)
- Possibility to expand market share after SolarWinds breach

Threats

- Data Breach
- Loss of key personnel
- Loss of key leadership
- Reputational damage
- International perception of former NSA personnel

Appendix B: Supporting Due Diligence:
ISO/IEC 27001:2013 Certification



SRI Quality System Registrar

ANAB ACCREDITED MANAGEMENT SYSTEMS CERTIFICATION BODY

Having been audited in accordance with requirements of

ISO/IEC 27001:2013

SRI Quality System Registrar, 300 Northpointe Circle, Seven Fields, Pennsylvania, 16046, USA, hereby grants to:

IronNet Cybersecurity Inc.

Registration of the management system at its locations:

7900 Tyson One Place, Suite 400, McLean, Virginia, 22101, USA
Coresite, Reston Data Center, (Care of Yellow Fiber Networks),
12011 Sunrise Valley Drive, Reston, Virginia, 20191, USA
555 Fayetteville St., Suite 700, Raleigh, North Carolina, 27601, USA

The conditions for maintaining this certificate of registration are set forth in the SRI registration agreements R20.3 and R20.4. Further clarifications regarding the scope of this certificate, the ISO/IEC 27001:2013 requirements, and the Statement of Applicability, dated 9/20/2020, Version 4, may be obtained by consulting the organization.

Scope of ISO/IEC 27001:2013 registration: "The ISMS that provisions software development and cyber security operations and protects the confidentiality, integrity, availability, and privacy of customer/employee information in accordance with the Statement of Applicability from IronNet Cybersecurity offices in McLean, VA and Raleigh, NC with Datacenter in Reston, VA."

FEDRAMP Ready attestation