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 4, 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 12, 2021, titled, *Assessment of the IronNet Cybersecurity Platform: Delivering an Advanced Collective Cyber Defense,* prepared by TagCyber

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 4, 2021

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

Exhibit 99.1

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 jurisdiction.

Assessment of the IronNet Cybersecurity Platform:
Delivering an Advanced Collective Cyber Defense

Prepared by
Dr. Edward Amoroso
Chief Executive Officer, TAG Cyber LLC
Distinguished Research Professor, NYU
eamoroso@tag-cyber.com

Version 1.0
February 12, 202[1]

Summary

An independent assessment is provided by TAG Cyber[1] of the IronNet Cybersecurity platform and associated solutions for delivering advanced collective defense protection to enterprise. The assessment includes description of the cyber threats addressed by IronNet, overview of the IronNet commercial offering, comparison to similar security solutions, and analysis of how the IronNet approach – particularly its collective dome concept – can be used most effectively.

Key Takeaways

- **IronNet competes in the Network Detection and Response (NDR) category, which is a growing aspect of modern enterprise security, but which does include major competitors.**
- **IronNet's unique value proposition strength and clear competitive differentiator is its collective defense concept based on the IronDome concept.**
- **IronNet's Co-CEO, General Keith Alexander, serves as an excellent business development resource for establishing relationships with larger enterprise and government buyers.**

Contents

Introduction

Section 1: Understanding Collective Cyber Defense

1.1 Toward a Collective Cyber Defense

1.2 Role of Government in Collective Defense

1.3 Cyber Threats to Infrastructure

1.4 Malicious Threat Actors

Section 2: Overview of IronNet Cybersecurity

1 Founded in 2016 by Dr. Edward Amoroso, TAG Cyber provides world class research and advisory services with advanced market reporting for cyber security teams. TAG Cyber's goal is to bridge the communication gap between commercial security vendors and enterprise practitioners. TAG Cyber's insights are delivered through an innovative on-line portal with support for expert on-demand research.

Copyright © TAG Cyber LLC

2.1 Cyber Security Analytics for Large-Scale Protection

2.2 IronNet Cybersecurity Approach to Infrastructure Protection

2.3 IronNet Cybersecurity Competitive Assessment

2.4 Developing an Infrastructure Protection Solution

Section 3: Assessment Conclusions

References

Introduction

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 cyber.

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 come down so much. This is especially true for cloud-based infrastructure and SaaS-based applications, where cheap ubiquitous services are now available on-demand and for every purpose imaginable.

Modern organizations must therefore develop security protections that address such growth, often delivered in the context of digital transformation initiatives. An addition 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 addition 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 platform 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 cyber challenge on their own. It is well-understood in the cyber security 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 business and agencies need to work together to address cyber threats. The big question, instead, is how this objective can be best achieved. This is one of the challenges addressed by IronNet.

Copyright © TAG Cyber LLC

This report is intended to provide an independent assessment of the IronNet commercial offering. To do so properly, context is required for how an advanced collective cyber defense can be established, because this is a major differentiator for the IronNet solution. Its platform offers buyers the opportunity to take advantage of the visibility and insights provided by other businesses and government agencies.

The report is organized into two parts: Section 1 provides an overview of collective cyber defense, including the role of the Federal Government, cyber threats to infrastructure, and threat actor types. Section 2 is the bulk of the report, introducing the IronNet solution offering. This is done by first introducing security analytics for large-scale cyber, and then outlining the IronNet platform approach. Competitive differentiation and practical implementation guidance are included.

Section 1: Understanding Collective Cyber Defense

To properly understand the IronNet platform and solution approach, it is best to begin with an outline of how collective defense can reduce cyber 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) [3]. IronNet is the first major commercial vendor to offer an end-to-end means to take full advantage of the collective concept.

1.1 Toward a Collective Cyber Defense

Businesses and agencies will only cooperate on collective cyber security initiatives if they see meaningful benefits with low associated risk. Admittedly, this is how almost all business decisions are made, but large-scale cyber security 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 in cyber security 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 to you.

It is also important to mention that within a large organization, collective protection across business units can have comparable benefit. Particularly in companies that evolved through mergers and acquisitions, 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 also 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 much 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.

Copyright © TAG Cyber LLC

- *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., 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 will 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 cyber security 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 government may also expose businesses to some regulatory risk (although this is partially mitigated by certain provisions of the Cybersecurity Information Security Act of 2014 (CISA) [2]) 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 cyber security 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 cyber security 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 main value proposition from IronNet is that cooperative cyber security will work best when such concerns are carefully curated by a trusted provider with a world-class platform.

1.2 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 to regulate and sometimes punish organizations not meeting their security requirements. This obligation complicates government cooperation with business on cyber security, 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.

Copyright © TAG Cyber LLC

The biggest challenge, however, is that the majority of critical 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 cyber security 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 IronNet's platform offering.

1.3 Cyber Threats to Infrastructure

Any collective to support large-scale infrastructure protection must begin with an accurate identification of cyber threats. Experts know that risk is measured by combining the probability of bad outcomes with the consequences of an attack. In the context of infrastructure protection, risks are driven by malicious threats and consequences of compromise to valued assets. To understand cyber risk, one must understand these components.

The familiar CIA model of confidentiality, integrity, and availability offers a textbook view of cyber threats to any asset. The model can be used to create a hierarchical representation of threats to large-scale systems. These levels of the hierarchy can be driven by general or domain-specific issues to highlight scenarios that target infrastructure assets. The depth and details of the hierarchy should always be selected to help security experts understand the relevant threats.

Every large-scale entity involved in the provision of essential critical services or assets must engage in a detailed threat breakdown, usually with many levels of decomposition. In some cases, the resulting threat hierarchy might include thousands of leaf nodes in the decomposition structure, each corresponding to a path in the tree, and each representing one specific threat scenario that must be addressed by the security scheme.

It is desirable to map scenarios from the threat tree for one organization to that of another. For example, the distributed denial of service (DDOS) threat to companies will be easy to connect between different organizations. Banks, government agencies, and even the military will likely experience comparable DDOS issues and can therefore easily coordinate on an integrated response using naming, routing, and other shared attributes of potential attacks.

The consequences of any attack on the assets of a particular infrastructure will vary with the specific circumstances. Each sector of a national or critical infrastructure ecosystem may experience different consequences as the result of a hostile cyber activity. Customers of telecommunications providers, for example, may experience severe consequences as a result of even temporary service outages. Other industries, such as fashion or entertainment, might not view temporary unavailability as serious.

Similarly, other contextual factors will influence the severity of consequence for threats to different large-scale infrastructure owners. For example, a large retail organization might view targeted denial of service threats before the holiday season as having significant implications. In contrast, the same retailer might view an availability attack at a less bust time of year as having a significantly smaller impact. This difference matters because it influences the measurement of risk.

Copyright © TAG Cyber LLC

An additional complicating factor is that many organizations evaluate risk based on measurement of hard consequences, which involve concrete financial, business, and tangible asset loss, as well as soft consequences, which involve reputation and image. Regardless of the nature of the consequence, however, all organizations will establish a view of their top risks, and many of these will be driven primarily by consequences – regardless of the likelihood of attack.

This discussion of threat is important in the context of providing an assessment of IronNet since it helps to identify the challenges that exist for enterprise teams – even with such a massive number of existing commercial security vendors. A major differentiating factor for IronNet is that its solution offering centers on a collective defense concept that directly addresses the lowering of cyber risks for large-scale organizations.

1.4 Malicious Threat Actors

Many taxonomies exist regarding the specific types of bad actors that an organization must contend with. These descriptions of malicious entities include at least the following five threat actor groups:

- *Hackers and Vandals* – This group is driven by curiosity as well as reputational standing within their social group. Hackers and vandals do not try to damage society or physically harm people, so they tend to be more easily reasoned with when caught.
- *Purpose-Driven Groups* – This group is driven by philosophical, political, or religious beliefs. Such motivation results in determined cyber threat campaigns. The famous hacking group Anonymous falls into this category of purpose-driven malicious acting groups.
- *Business Competitors* – Competing organizations with low integrity might aggressively seek to gain a business advantage through hacking. This may result in seeking to obtain competition-sensitive information through illegal purchase on the Dark Web.
- *Criminal Organizations* – This group is driven by financial motivation. Electronic fraud often involving social engineering with robust workflow processes to target credit cards, identities, medical information, insurance data, and other common means of cyber theft.
- *Nation-State Military* – This group is the most difficult to defend against, and in many commercial scenarios, represents an intractable problem. If a nation-state such as China or Russia decides to target a business entity, then that entity is almost certain to fall victim.

Organizations use their own risk analysis to determine the malicious actors most threatening to their operation. For example, an organization that scouts sports talent is highly unlikely to be targeted by a nation-state military; however, that agency would be wise to consider potential attacks from hackers and competitors as more significant threats. Such organizations may also have a broader base of threat actors—like illicit news and paparazzi groups—that might not threaten other sectors.

Security collectives, even across the business units of a single large organizations, are especially useful in determining which threat actors should be watched. The techniques and tactics of a threat actor might be well-known by one group in the collective, but perhaps less well-known by others. This uneven recognition of threat can be evened out through use of a collective defense such as provided commercially by IronNet.

Copyright © TAG Cyber LLC

Part 2: Overview of IronNet Cybersecurity

Co-founded in 2016 by General Keith Alexander, former Director of the US National Security Agency (NSA) and Commander of the United States Cyber Command, IronNet focuses on advanced behavioral threat detection for enterprise networks. IronNet uses advanced analytics and sensors that pull data from defined locations in an enterprise and provides alerts that are culled in an automated manner.

2.1. Cyber Security Analytics for Large-Scale Protection

Security analytics are uniquely suited to larger infrastructure. That is, it is unlikely that one would propose a real-time, telemetry-based monitoring system with 24/7 coverage for an individual personal computer system – unless that personal computer was connected to a larger system or contained highly sensitive information. In contrast, however, it would be quite important to apply some sort of telemetry-based analysis capability for large-scale national or critical infrastructure protection.

Security telemetry consists of data collected by remote sensors for the purpose of improved visibility, insight, and monitoring of that target environment. Engineering issues in the integration of telemetry into a security environment such as from IronNet include where to put sensors, how to securely pull the telemetry to a collection point, and how to tune the sensors to collect the right type and amount of data.

The type of security telemetry required to protect large-scale systems will certainly vary from one implementation to another. For instance, pure information technology (IT) ecosystems will generate different log information and event data than ecosystems that combine IT systems with operational technology (OT), perhaps in the context of industrial control or factory automation. Many OT systems, for example, use unique protocols on top of the traditional TCP/IP protocol suite.

Nevertheless, requirements can be developed for the specific attributes required in any telemetry system being connected and used to protect infrastructure from attacks. The security telemetry attributes listed below, all of which represent key considerations in the design of the IronNet solution, are best suited to large-scale systems, but can also be adapted and used for smaller systems:

- *Relevancy* – Telemetry for cyber security must be relevant to the protection goal. Event logs or records for networks that don't support mission-critical applications will not be relevant to the central protection task.
- *Accuracy* – Measurements inherent in collected data must accurately portray the system attribute being analyzed. If such measurements are crudely estimated, for example, then bad decisions could result.
- *Coverage* – Telemetry for large-scale infrastructure requires coverage analysis to determine the best assessment. By way of analogy, determining the weather in the entire US would be poorly represented by data from only one state.
- *Detail* – Data to support infrastructure protection must include sufficient detail to expose relevant threats. Event logs, for instance, that only show the beginning and end of sessions are unlikely to be useful to security teams.
- *Attribution* – Knowing the source of large-scale infrastructure data can be helpful in establishing context. Where attribution has privacy implications, caution must be exercised to ensure that such efforts are conducted consistent with legal and policy frameworks.

Copyright © TAG Cyber LLC

In the early days of data collection for security analytics, the general view was that more data was always better. Modern security operations center (SOC) teams would disagree with this assessment, because getting the right data from the key sources for review and analysis is the most important element of any analytic process. This approach minimizes unnecessary workloads and improves overall security analytic process flow.

Aggregation of collected data for IronNet customers involves sensors that pull data from relevant systems. These deployed sensors create and share telemetry to identify local posture. The tasking is preprogrammed but can be adjusted locally and remotely from a management center. Aggregated data can be shared securely with an analysis function in an analytic backend for query, analysis, and alerting. This summarized data is then provided in a user-friendly form to analysts to conduct further assessment and triage, and to take action, where appropriate. This is supported by an analytic back-end system.

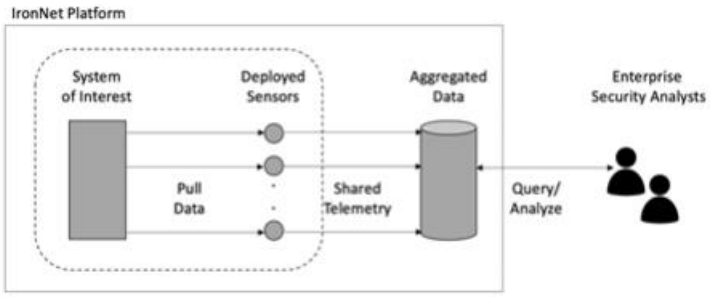

Figure 2.1.1. IronNet Telemetry Collection and Aggregation Method

The customer system of interest and the deployed sensors can be logically or physically adjacent, whereas the aggregation and analysis function is usually done remotely. This is not a rule, certainly – and some situations emerge where the relevant data or systems are not co-located with sensors—but typically these situations are resolved by routing the relevant data to the IronNet sensor through other network infrastructure products.

The pulling, sharing, and analyzing data through sensors into the analytic backend, and then out to an analyst in a SOC is characteristic of any telemetry-based security protection for infrastructure. Such detailed monitoring would likely be unnecessary for a small system, such as an individual PC, because PCs generally do not cause large-scale issues if hacked. Infrastructure is harder to understand, which is why pulling data allows for better understanding of operation.

The algorithms required to identify relevant issues in collected data are focused on predicting or detecting conditions that warrant security attention. Prediction occurs when the detected condition corresponds to an *indication and warning (I&W)*, observed *before* some undesired consequence can occur. Obviously, I&W detection is preferred to observing an attack that has started or even completed, because in these cases, the damage might already have begun and is, therefore, harder to stop.

The overall analytic goal for IronNet customers is*correlation* – which involves comparison of data looking for connections, patterns, or other relationships that connect one set of events to another. Such correlations are most usable when automated, because such an approach supports rapid recognition.

Copyright © TAG Cyber LLC

The typical approach involves security analysts curating the process, with threat hunters guiding technology to draw fundamental security conclusions.

Three general strategies exist in the development of IronNet's algorithms to support correlation between collected data and potential attack indications in a target infrastructure:

- *Signature-Matching* – This involves comparison of known patterns against observed activity. Signature patterns include lists of suspicious Internet Protocol (IP) addresses or domains to be searched for in activity logs. These signature-based approaches can also include the type, size, location, hash values, and names of files used by an attacker, or even, in some cases, structured representations of a series of specifically denominated attack steps. The strength is that if patterns are known, as with anti-virus software, then doing a check is a good idea. The weakness is that patterns are often unknown. IronNet can perform signature-based solutions but differentiates itself from competitors through its greater emphasis on behavioral analytics.
- *Behavioral Analytics* – This approach involves more dynamic comparison of behavior with observed activity. The activity being reviewed includes live operation of a customer system, such as whether an application is trying to establish a network connection or invoke an unusual operation. Behavioral analytic analysis is more complex than signature-based review but is also better at detecting indicators of attack, unknown threat vectors, and attack techniques. The strength of this approach, which is central to IronNet's solution, is that signatures don't have to be known in advance, so detecting zero-day attacks becomes possible. The weakness is that higher false positive rates can occur if profiles of expected behavior are immature.
- *Machine Learning* – This approach involves advanced means for detection of cyber security threats. Machine learning tools typically scan input to make determinations based on previously processed training examples or abstractions from live data; and they establish a categorization of what is being reviewed. This approach to security threat detection is similar to how machine learning supports visualization and categorization of objects. The strength is the potential to recognize previously unknown types of attacks. The weakness is that the method requires an enormous amount of data. This data can be used off-line for machine learning or ingested live for deep learning-based analysis.

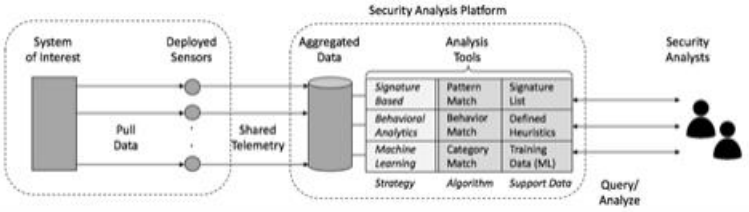

Figure 2.1.2. IronNet Correlation Algorithm Strategies

As depicted in Figure 2.1.2, the IronNet solution combine all three strategies into an effective security analysis platform for infrastructure protection. Nothing precludes the pre-processing of telemetry for known signatures, especially in cases where a rich source of intelligence is available. Similarly, if an obvious behavioral pattern exposes a malicious intent, then it is reasonable for a customer to deploy this method in advance of more powerful machine learning analysis.

Copyright © TAG Cyber LLC

Organizations within the same sector or across critical sectors will have comparable threat issues. This suggests a mutual interest in cooperating to share data to improve identification of both known and emerging threats. A reasonable heuristic for such processing is that having more relevant data improves establishment of data relationships. It should be a goal for any team protecting critical infrastructure to try to work with peer groups in the same industry. IronNet enables such cooperation.

Challenges do emerge for organizations to cooperate and share data to reduce their mutual cyber security risk. These challenges are addressed directly by the IronNet team in the following areas:

- *Competition* – Competitive forces might cause different companies to question whether cooperation is in their interest. Some industries will gravitate toward a coordinated approach (e.g., airlines agreeing to cooperate on safety issues). But other industries might include participants who benefit when their competitor is breached (e.g., retail, telecommunications, and sometimes even banking). By deploying a common platform infrastructure with strong separation controls, IronNet helps to enable such cooperation.
- *Attribution* – If shared information can be easily attributed to a reporting source, then cases emerge where this can be used to embarrass the sharing entity, or even influence customer behavior. Anonymity options are essential in any information sharing initiative designed to support cooperative cyber protection. IronNet includes strong controls to ensure that attribution is not compromised.
- *Liability* – This emerges in cases where the legal implications of an incident might be unknown or under consideration. Regulated organizations must report incidents, but in the earliest stages of a case, reporting obligations might not be known, and the tendency will be to delay sharing until the liability posture of an incident are understood. This liability protection model is also consistent with the IronNet solution.

None of these challenges are insurmountable but require careful attention if the goal is to create a cooperative protection solution for multiple infrastructure organizations. In the next section of this report, we will examine how IronNet constructed its platform to serve the technical needs of their SOC team customers for correlating telemetry, while also addresses operational challenges for reporting organizations.

2.2 IronNet Cybersecurity Approach to Infrastructure Protection

The IronNet system integrates the knowledge and capabilities of its highly skilled cyber threat analysts, many of whom previously conducted offensive and defensive operations in support of national security missions. The system also shares data from multiple industries in real-time to create a collective defense fabric at scale. The company is truly in a unique position to provide effective large-scale infrastructure protection.

The commercial platform for supporting data collection and analytics to serve the threat hunter is called*IronDefense*. Telemetry is collected from IronDefense sensors deployed across an enterprise at key locations to collect full packet capture (PCAP), which is then analyzed for potential threat attributes and then combined with collected metadata to create highly enriched metadata, known as IronFlows, which is presented for analysis to the commercial platform backend.

The IronDefense backend serves the threat hunter who might choose to integrate IronNet metadata with other telemetry and data analytics on a complementary platform such as Splunk in the SOC. The backend also provides event information to be rendered into the IronVue analyst front-end. In addition, the backend analysis presented in IronVue can be used to coordinate detection, prevention, and response activities with industry peers through the IronDome collective defense platform.

Copyright © TAG Cyber LLC

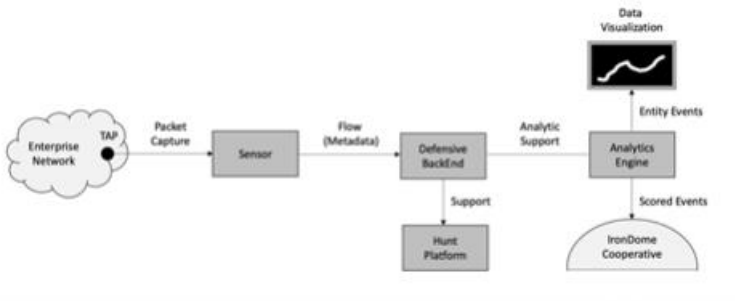

Figure 2.2.1 IronDefense Processing Flow

The IronDefense processing includes the functional components required to translate raw network data into actionable intelligence. This is the overarching goal of any live defensive protection system for large-scale infrastructure. A key design objective is to minimize the time between collection and interpretation, and to simplify each of the interfaces, thus ensuring an open design so that third-party systems, such as hunt platforms, can be easily integrated into the overall process flow.

The analytics component included in the IronDefense platform supports the following real-time functional and process objectives for the customer's SOC team:

- *Advanced Behavioral Analytics* – The behavioral analytics used by the IronNet system are driven by predictive behavioral models developed by IronNet data scientists supported by US government and academic research centers.
- *Driving Key Decisions* – An expert system conducts contextual data analysis based on tradecraft insights and risk determinations made by human analysts in a SOC and leveraging the core insights of the IronNet team's prior offensive and defensive national security experience.
- *Focusing Detection Priorities* – The IronNet expert system provides useful context to any mathematics-only solution, because while a true-positive might be detected, it might not be of local interest. Adware attacks, for example, might produce a positive detection, but might not be a high priority to the local team.
- *Support for Hunt* – The SOC hunter's investigative case work utilizes the collected data in a tool that provides rapid, easy access to packet-level data and other contextual information.

Some of the major functional advantages of an analytics-rich processing environment include detection of threats at scale, which is important for infrastructure, where visibility and identification of otherwise unknown threats can be a challenge. Collection of data from key north-south and east-west collection points expands this visibility aperture and enables better response. The tradecraft insights embedded in the behavioral algorithms also help ensure that good mitigation and response decisions are made.

The purpose of IronNet's IronDome collective defense platform is to create and support a cooperative cyber defensive system based on the live sharing of anomaly and event information for members. The collective group is built from willing peers, presumably enterprise and government organizations, who understand the need to belong to a trusted group that can expand the attack visibility surface beyond their own perimeters and enterprise networks.

Copyright © TAG Cyber LLC

One advantage of this arrangement is faster time-to-detection rate for a member and the identification of threats that might have gone unnoticed in a single environment. In addition, members avoid the challenge of working in isolation against a nation-state adversary that focuses on leveraging similar offensive playbooks against a sector. The collective defense addresses this asymmetry. Here is the normal detection time for an enterprise, usually about 100 days from breach to awareness:

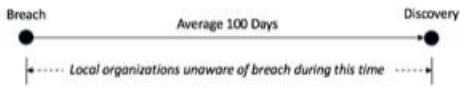

Figure 2.2.2 Breach Detection Time for an Organization in Isolation

When a SOC team has access to detection flow information from multiple enterprise teams in a collective such as IronDome, the potential emerges that threat warnings arrive much more quickly. If two organizations are vulnerable to some breach X, then the possibility arises that one might detect it more quickly and can notify the other. The result is a reduction in time-to-detection for the organization being notified, as shown below:

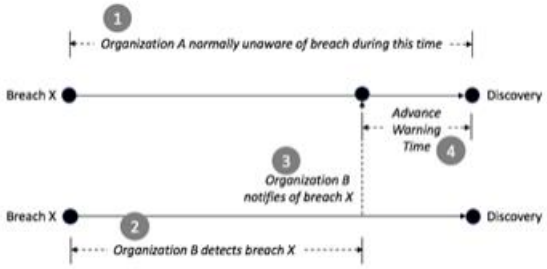

Figure 2.2.3 Reducing Breach Detection Time Through Cooperative Notification

The advantages of such cooperation should be obvious, and the IronDome infrastructure is set up to support this type of mutual sharing. It includes mechanisms to support the following important goals for cooperative cyber defense:

- *Industry-Wide Threat Visibility* – This aspect of IronDome solution provides participants to obtain shared event summaries with analytics for security awareness and threat insights across communities that have comparable risk profiles.
- *Community Triage* – IronDome leverages shared insights to detect broad or targeted campaigns that would not be easily detected by a participant in isolation. This aggregation capability can also work across different sectors or risk profiles.

- *Automated Machine-Speed Sharing* – IronDome automatically shares sector-based threat insights from participants and supports the maintenance of near-real-time threat analysis about cyber security issues being observed.
- *Cross Sector Defense* – Ultimately, IronDome supports a cross sector defense for participants through exchanges across different industries, regions, and even national organizations. The result is a powerfully woven, integrated cyber defense.

These capabilities obviously rely on shareable events being passed securely and anonymously to the IronNet Cloud, where the engine and analytics store and process the information. Feedback is then shared with an IronDome of different companies, which is essentially a trusted collective that benefits from the scored events, correlations, notifications, and suspicious behavioral reports provided by the IronNet engine.

The greatest hurdle to large-scale collective protection via IronDome is that many organizations have a long-held,built-in hesitation to share threat and vulnerability information externally. This is a reasonable concern, because capable adversaries covet knowledge of IT infrastructure, network design, deployed applications, and security architectures in designing a targeted offensive. Information sharing can expose this data to external entities and might cascade to an adversary.

The design goals that can minimize information sharing concerns amongst participants include the following requirements:

- *Participant Anonymity* – When a participant shares vulnerability information with a group, the attribution should provide context around the shared item but nothing more. This implies that casual marking of a shared vulnerability with its originator is not a desired practice and could easily undermine the establishment of effective sharing. Anonymity must be embedded in the sharing infrastructure, presumably using encryption or blinding as part of the protocol.
- *Secure Storage* – The means for storing shared vulnerabilities must be trusted to be highly secure. If external, untrusted actors find their way into shared databases, then this can represent an undesirable leak, and can also undermine the trusted group. Secure storage techniques must therefore be in place, and this would presumably include best-in-class cyber security functions, procedures, and policies.
- *Trusted Groups* – The community for sharing should involve a group of participants who are mutually trusted to handle information, maintain discretion, share sufficient information to balance what is ingested, and to be a helpful partner should unexpected challenges emerge in the context of sharing (such as during an incident). Trusted groups are easier to develop when small, but context increases with the size of the group. A proper balance should be desired.

The IronDome solution includes support for these important requirements and embeds the associated functional support directly into the platform. It should be obvious, however, that despite any functional measure put in place, the most important aspect of any cooperative, collective cyber defense is the mutual trust that exists between participants. For this reason, great care must be taken when selecting teams to include in a sharing group – whether within a sector, or across multiple ones.

2.3 IronNet Cybersecurity Competitive Assessment

Before explaining how an organization would work with IronNet to develop an infrastructure protection solution, it is helpful to pause and describe the competitive commercial landscape, especially in the context of so-called *network detection and response (NDR)*. In so doing, the unique aspects of the IronNet approach can be highlighted – but more importantly, integration of IronNet's platform with other existing security tools can be shown.

The NDR category is an industry-analyst created category in which the latter stages of security protection – that is, the shift-right tasks of detection and response – are focused on more aggressively that the earlier stages of security protection – namely, the shift-left tasks of identification and prevention. This designation matches much of what IronNet does for customers, but it undersells IronNet's usefulness in identifying early indications and warning.

Nevertheless, the clearest comparison to IronNet does come from the NDR community, and the narratives below include descriptions of each competitor and their respective strengths and weaknesses with respect to IronNet. It is the belief here that feature-by-feature comparison (e.g., what connectors are included, what development processes are used, and which compliance certifications have been obtained) are less important than the key comparative areas highlighted below.

Darktrace

The Darktrace NDR platform uses AI-based self-learning to detect attacks and insider threats. Darktrace emphasizes early detection, using its technology to find evidence of breaches without the need to use signatures or rules. The focus is on protecting users, devices, cloud containers, and workflows to build a model of what is normal in a customer organization. Darktrace's massive advertising campaign (including print magazines) emphasizes AI for security.

FireEye

The FireEye NDR platform also focuses on detecting indicators of imminent oron-going cyber threats. Their Network Security and Forensics solution uses signature-free detections with the ability to detect zero-day vulnerabilities. This is done through a combination of code analysis, statistical analysis, attack emulation, and machine learning using sandbox technology. FireEye was recently involved in the SolarWinds attack, where they are generally accepted to have been first to identify the campaign.

Trinity Cyber

Trinity Cyber is not an NDR vendor but has created a network security team that closely resembles IronNet in background, mission, and interest. With Tom Bossert and Steve Ryan (both well-known former senior government officials) at the helm, Trinity Cyber obtains early-adopter clients who are excited to work with these famous technologists. Trinity Cyber is growing and is likely to compete with IronNet for general network security business.

Vectra

The Vectra NDR platform, like Dark Trace, also emphasizes advanced intelligent,AI-driven security support for SaaS, cloud, and traditional enterprise. Their Cognito solution detects network threats with machine learning methods and includes remediation support. Vectra uses the machine learning to enrich collected metadata and includes a SaaS application that supports investigation and threat hunting for their enterprise customers.

IronNet

Like Vectra and Darktrace, the IronNet solution combines signature, behavioral, and machine learning methods into an NDR solution that also detects early indications and warning. Like Trinity Cyber, IronNet uses General Keith Alexander as a market and sales influencer with enterprise buyers. Like FireEye, IronNet identifies public campaign evidence such as SolarWinds. Unlike the others, however, IronNet includes a collective defense concept that is unique and powerful.

Copyright © TAG Cyber LLC

	Collective Support	NDR Focus	Campaign Identification	Advanced Algorithms	Iconic Founder
IronNet	Dome	Yes	Yes	Yes	Alexander
Darktrace	No	Yes	Yes	AI Focus	No
FireEye	No	Yes	Yes	Sandbox	No
Trinity	No	Yes	Yes	Yes	Bossert
Vectra	No	Yes	Yes	AI Focus	No

Figure 2.3.1 Competitive Assessment of IronNet

2.4 Developing an Infrastructure Protection Solution

The era of government protecting business and citizenry from serious attacks including from foreign adversaries might be viewed as having passed – at least in the context of cyber security. That is, while it remains reasonable to expect government to ensure that physical attacks such as from bombs and missiles are prevented, it is sadly neither correct nor reasonable to expect any nation's military, regardless of its ability, to stop major cyber threats from hitting its citizenry and business community.

As a result, every organization must develop its own plan and associated solution for infrastructure protection. The good news is that this plan and solution can be constructed using existing enterprise security programs as a base. That is, the types of functional, procedural, and policy decisions made to stop enterprise-grade threats represent the correct underlying security base on which to build a foundational model for dealing with larger threats.

Three attributes must be met by an organization before cyber risks to critical infrastructure can be properly addressed via a cooperative sharing group. These attributes line up directly with the belief structure of the stakeholders and decision-makers in the information technology, infrastructure, and cyber security groups. These attributes cannot be just imposed on an organization. Rather, they must be closely held by the relevant principals:

- *Risk Acknowledgement* – An organization acknowledge security risk to their infrastructure. If the belief exists that vulnerabilities are minor and that infrastructure cannot be seriously degraded via cyber threats, then participation in a cooperative group would likely not be successful. Organizations must be willing to acknowledge the presence of risk before joining any collective sharing group.
- *Willingness to Share* – An organization must also recognize the bidirectional nature of information sharing. That is, joining a cooperative cannot be done to collect data from others. Rather, just like in any trusting relationship, it must include an open willingness to share information with other members of the group. Anonymous, non-attribution can be helpful, but willingness to share is essential.

Copyright © TAG Cyber LLC

- *Desire to Mitigate* – The purpose of any cooperative sharing group is to provide a rich source of information, from which actionable intelligence can be derived. Involvement in the group should therefore be predicated on the desire to actually mitigate cyber security risk, rather than to meet some compliance obligation, or to collect interesting information for the entertainment of the board.

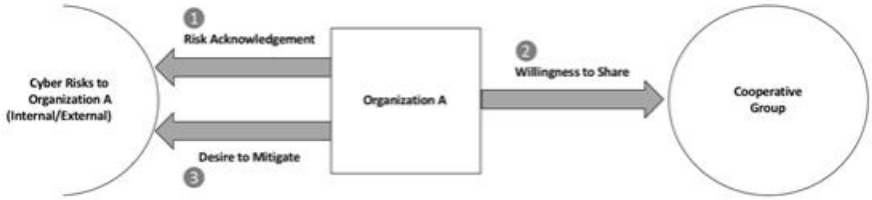

Figure 2.4.1 Three Attributes Required to Succeed in a Cooperative

These three conditions must be met honestly by the organization and are listed here to help make the collective involvement successful. Any organization that doesn't fully accept the presence of cyber risk, doesn't plan on sharing relevant information with others, and has no intention to use the shared data as the basis for real security mitigation and response, would be advised to invest their time and efforts into other types of management activity.

It is worth mentioning that some organizations like to be part of information sharing groups to collect information relevant to executive and board presentations. Board members, in particular, like to be provided context around cyber threats, including malicious actor attribution, so sharing often helps to obtain this information. So long as the ultimate purpose in educating board members is to improve the overall security posture of the organization, this motivation for joining a collective seems acceptable.

The concept of trust between participants in any cyber cooperative is influenced by a couple of factors. First, there is the business or government sector between participants. It is not a stretch to assume that participants in a common sector will tend to be more trusting of information being ingested, simply because the vantage point will be similar. Two banks, for example, will tend to trust their relative interpretations of some vulnerability and its consequence.

Second, the relative size of sharing participants will influence mutual trust. A general rule is that most organizations will tend to trust information from larger or peer groups but will be more tentative about information coming from a smaller participant. This is not a perfect correlation, because a large bank might trust information coming from a tiny, but expert advisory group. In general, though, peer or larger organizations tend to be assigned more confidence in the information being shared.

These two factors – sector and size – can be merged into aso-called measure of *peer correlation* that can be useful in analyzing the potential effectiveness of a given cooperative. By creating a simple grid on these two factors, we can depict the degree to which participants will tend to view the level of correlation for information being shared generally. Two large banks, for example, might find some shared data highly correlative, whereas a small retail shop might find the same data less applicable.

Copyright © TAG Cyber LLC

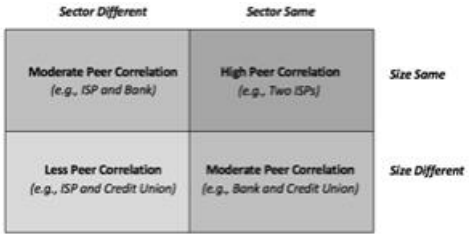

Figure 2.4.2 IronNet's Approach to Cooperative Peer Correlation

It is worth noting that competitive forces will clearly influence the willingness of a given organization to share information with a cooperative group. While it is true that many industries such as transportation and energy tend to not differentiate based on relative security capability, there are some industries such as telecommunications where this is not true. Cooperatives that include entities competing on cyber-related capability will have to work harder to maintain mutual trust.

Joining an information sharing group will introduce a myriad of management questions from the legal and privacy teams in any organization, especially larger ones with more attack consequence. These questions are best addressed before the decision has been made to join a sharing group, so as to avoid the costs of unraveling entry. The biggest issues that tend to require consideration when joining any cyber security cooperative are the following:

- *Protecting Information* – By sharing information with a cooperative, the organization introduces the possibility, however potentially small, that sensitive data will be mishandled and leaked. To deal with this issue, cooperatives must include world-class mechanisms for protecting and handling data both in storage and at rest. Participants should have influence on how these privacy and security mechanisms are selected and managed to maximize comfort levels.
- *Working with Competitors* – If a cooperative includes competitors, then legal teams will want a clear understanding of all policies and procedures used for interaction and sharing, especially in industries that are government regulated. The primary concern is that the sharing should never create cooperative marketing or pricing advantages for sharing participants, or any other business practice considered illegal or unethical. Legal teams will want documented evidence of how this all works.
- *Avoiding Unexpected Risk* – In general, enterprise legal, privacy, and security teams will be averse to any unexpected risk that might emerge as a result of joining a sharing cooperative. This requires that cooperative cyber sharing groups must include clear documentation of the experiences and expectations for all participants. New risks can always emerge, but surprise should be minimized.

The best way to handle these legal and privacy issues is to directly involve staff from these organizations into the decision-making process around joining or establishing a group. Companies such as IronNet Cybersecurity can provide excellent advice to companies considering use of cooperative such as their IronDome, and can help legal, policy, and privacy staff become more knowledgeable and comfortable around what to expect.

Copyright © TAG Cyber LLC

Section 3: Assessment Conclusions

Based on the review and analysis described in this report, three major conclusions can be drawn with respect to IronNet's cyber security solution for enterprise.

Collective Dome Advantage – IronNet has a clear advantage over its competitors with its cyber collective concept based on IronDome. This should be the primary marketing message to support growth and should be the basis for most advertising, marketing collateral, and involvement with industry analysts. The barrier to entry for competitors in this aspect of cyber security protection is considerable, so IronNet will have sufficient time in 2021 to build up a lead in this area of cyber risk management.

NDR Market Involvement – The NDR market is a growing and vibrant segment of the cyber security industry, so IronNet is wise to list involvement in this area. Requests for Proposal (RFPs) often include NDR as a requirement, so IronNet will want to be included. That said, NDR is a crowded area, with many firms, including ones not considered competitors to IronNet, such as Palo Alto Networks, AT&T, and Verizon, listing it as a capability. NDR is thus a *necessary* designation, but a non-differentiator.

Role of Iconic Founder – The role of General Keith Alexander at IronNet should continue as a sales influencer, business developer, and relationship developer. Many prospective customers view him with great reverence, so this should be leveraged fully. The IronNet sales process, however, must expand to include sales lead management, product marketing, and contract pipeline development processes that are independent of the General's direct influence. This will accelerate IronNet's growth.

References

[1] https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos.
[2] https://www.congress.gov/bill/114th-congress/senate-bill/754

Copyright © TAG Cyber LLC