On the Radar: IronNet Cybersecurity applies analytics, threat intelligence for collective defense

IronDome service delivers machine-speed visibility of industry-specific threats

Publication Date: 05 Jun 2020 | Product code: INT005-000126

Eric Parizo

Omdia view

Catalyst

Enterprises are not proficient at working collaboratively to share intelligence to prevent cyberattacks. IronNet Cybersecurity was created to change that.

The brainchild of General Keith Alexander, US Army, Retired, IronNet offers technology to help enterprises discover threats they otherwise might overlook. The vendor does this by enabling organizations to work together collectively in real time to share threat intelligence, collaborate on evolving threats, and develop better, more effective defenses.

The solution set offers a multifaceted approach that includes IronDefense, a network behavioral analytics platform, and IronDome, a real-time sector-specific platform that collects, analyzes, and shares threat intelligence on a regional and/or national level.

Key messages

- IronNet provides the technical underpinnings for enterprises to collaboratively improve intelligence sharing and attack detection.
- IronNet takes aim at Fortune 500 companies and other high-value targets that understand rapid detection is as important as prevention.
- IronNet offers in-depth network traffic analytics, including on encrypted traffic, as a key differentiator to find anomalies and behaviors indicative of attacks.
- IronNet's premium solutions have traditionally targeted large organizations with mature cybersecurity capabilities, but it has recently introduced entry-level offerings designed for midsize firms.

Omdia view

IronNet seeks to stand out from its primary network traffic analytics and network detection and response (NTA/NDR) competitors, including Darktrace, ExtraHop, and Vectra, by providing both behavioral-based and signature-based threat detection. Its ability to discern needle-moving insights from encrypted network traffic flows, and do it without the heavy proprietary hardware required by Cisco's competing Stealthwatch product, is a potential game changer.

Where it ambitiously aims to change the entire cybersecurity industry, however, is with its collective defense platform, IronDome, which enables threat intelligence sharing and defensive collaboration. There is no other solution like it on the market, and it goes beyond what information sharing and analysis centers (ISACs) and other industry groups that share threat intelligence can do by bridging the technology and process gaps that inhibit real-time information sharing.

Well-resourced enterprises in key vertical segments that are willing to share cybersecurity intelligence and best practices with other organizations in their industries can significantly benefit from the IronNet Cybersecurity solution set.

Recommendations for enterprises

Why put IronNet Cybersecurity on your radar?

When he served as commander of United States Cyber Command (USCYBERCOM), the Department of Defense organization charged with leading the nation's cybersecurity defense, Keith Alexander realized that there were two key problems that prevented both the public and private sector from stopping cyberattacks. First was a lack of real-time visibility into anomalous activity happening across a wide variety of networks. Second was an inability to share threat intelligence that could be used to stop attacks before they were successful.

IronNet Cybersecurity was founded to solve both of those problems for the public sector and key private sector industries. It does this with behavior-based network traffic analysis, identifying, enriching, and scoring anomalous events and suspicious network traffic activity. It also enables customers in common verticals to share threat intelligence in real time, allowing them to share information about and ultimately prevent intrusions targeting similar organizations.

The vendor's solution has traditionally been targeted at large enterprises, often costing more than $1 million per year, and consists of a package of products, managed NDR services, and advisory services. A sizable, high-performance on-premises sensor deployment is necessary for its IronDefense solution, along with a mature security operation commitment.

More recently, IronNet introduced a sub-$75,000 product-only entry-level offering that is competitive with other NTA vendors' offerings in the space. This offering is accompanied by a virtual network sensor for smaller environments.

IronNet's IronDome industry-specific, anonymous collective defense collaboration software-as-a-service (SaaS) system for real-time threat sharing is unique in the industry, offering the first viable solution for realizing General Alexander's vision of enabling improved cybersecurity across numerous organizations through collective defense.

Highlights

The IronDefense architecture relies on several distinct components. A series of on-premises hardware and virtual network sensor devices (1Gbps or 10Gbps), deployed off a tap or span port at the network perimeter, analyze inbound network traffic by parsing protocols to generate unique metadata. Larger deployments commonly deploy additional sensors inside an enterprise's network to monitor east–west traffic. That metadata is then scrutinized by IronNet's analytics system, deployed either in Amazon Web Services (AWS), in Microsoft Azure, or at the customer's location, using more than two dozen proprietary analytics engines as well as IDS/IPS signature-detection capability on the IronDefense sensors. Events are automatically enriched with customer-specific contextual data and IronNet proprietary and third-party threat intelligence data and are then compared with baseline network behavior or probabilistic detection models to identify anomalous activity. This contextualization results in a behavior score that is prioritized by risk level; events with scores above a certain threshold are flagged as anomalous.

Its ability to peer inside encrypted traffic flows and discern malicious activity without decryption relies largely on an analysis of the SSL/TLS handshake or exchange of encryption key data used to facilitate the encrypted flow transaction and on other related indicators such as encryption protocols and server-name indication.

Customers using the IronDome collective defense service agree to anonymously share details on scored events with other customers in a given sector such as energy or healthcare. Participating customers' IronDefense instances automatically triage behavioral event metadata, which has been stripped of any customer-identifiable information, and pass it to IronDome for additional analysis and correlation. IronDome's correlation engine compares each new event with past shared events from all of that sector's other IronDome customers; known attacks are correlated and matched with related past events, while new suspicious behavior results in a proactive warning to all participants. IronDome also supports collaboration among participants, allowing discussion of and knowledge sharing about specific incidents, anonymously by default. IronDome collective defense communities can be organized by industry sector, by business ecosystem, or by larger geographic or national groups. A customer can be a participant in multiple applicable IronDome communities.

Finally, IronNet also offers a variety of professional services and optional consulting services, including "red team" threat hunting.

Customers interact with the vendor's IronVue user interface (UI), an interface which allows cybersecurity analysts access to their IronDefense hunt platform. It enables them to view and investigate incidents, including in-depth event-defined queries such as using raw PCAP network traffic metadata to identify the source of malicious behavior. Additionally, customers can interact with IronDefense programmatically through an API that integrates with existing security information and event management (SIEM) or security orchestration, automation, and response (SOAR) tools already in place.

Background

IronNet was founded in 2014 by a group of military, government, and commercial experts led by retired US Army general Keith Alexander. Alexander served a distinguished 40-year military career, capped by his tenure as commander of USCYBERCOM and director of the National Security Agency (NSA). IronNet's management team includes a mix of former US military cybersecurity leaders and longtime cybersecurity industry executives.

The company began day-to-day operations following a $32 million Series A investment in 2015 led by Kleiner Perkins and ForgePoint Capital. It raised a $78 million Series B investment in 2018, led by its initial investors with the addition of C5 Capital, to accelerate its sales and R&D efforts.

After an initial focus on North America, in late 2019 IronNet announced its expansions into the Europe, Middle East, and Africa and Asia Pacific regions.

Current position

IronNet Cybersecurity has declined to detail its exact number of customers, but it is believed to have at least several dozen paying customers. It has more than 250 employees, hiring more than 100 new workers in 2019.

Its primary competitors are NTA vendors, including Darktrace, ExtraHop, and Vectra, and cybersecurity platform vendors such as Cisco Systems with its Stealthwatch solution. The vendor's IronDome solution functions like a next-generation threat intelligence platform (TIP), but the vendor does not see itself directly competing in the TIP segment because of its focus on sharing firsthand behavior-based threat insights as opposed to static third-party signatures.

IronNet is currently operating IronDome instances for energy and utilities (its largest customer group), financial services, healthcare and life sciences, US public sector, and US defense. It is also working with international customers on establishing regional IronDome instances.

The vendor's average purchase package costs in the six-figure to low-seven-figure range in US dollars, and the company recently diversified its offering to include an entry-level sub-$75,000 1Gbps offering, part of a push to broaden its target customer base.

Recent product updates include a new collective defense visualization dashboard, new cloud deployment option in Microsoft Azure, new 1Gbps VMware sensor, and expanding behavior-detection focus. This includes a knowledge-based signature-detection capability that uses a customized version of the open source Suricata inspection engine with Proofpoint's rule set via a technology partnership. A variety of integrations have been completed this year with a number of third-party SIEM, security orchestration, and IT service management vendors.

The vendor's key short-term challenges include expanding its NTA/NDR capabilities to a variety of public and private cloud environments in which network telemetry data is often limited and must be collected differently, demonstrating the ROI of its IronDome real-time threat-intelligence-sharing solution with proof of how customers can successfully help defend each other, and moving down-market with lower-cost options for smaller customers.

Data sheet

Key facts

Table 1: Data sheet: IronNet Cybersecurity

Product name	IronDefense, IronDome	**Product classification**	Network traffic analysis; threat intelligence platforms
Version number	3.4.x	**Release date (latest version)**	April 2020
Industries covered	Energy, healthcare, financial services, defense, government	**Geographies covered**	North America; Europe, Middle East, and Africa; Asia Pacific
Relevant company sizes	5,000+ employees	**Licensing options**	Monthly subscription-based pricing
URL	www.ironnet.com	**Routes to market**	Direct sales supplemented by a growing system integrator, value-added reseller, and managed security service provider channel strategy
Company headquarters	Tyson, Virginia, US	**Number of employees**	250+

Source: Omdia

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets because their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Omdia Market Radar: Threat Intelligence Platforms, INT003-000291 (December 2018)

Author

Eric Parizo, Senior Analyst, Cybersecurity Accelerator

askananalyst@omdia.com

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com