EMA Vendor to Watch: IronNet Cybersecurity

Corporate Information

It's not necessary for a cyber security startup to have star power to be successful, but it doesn't hurt. The fact that new threat intelligence sharing and security analytics vendor IronNet Cybersecurity was founded by former long-running NSA chief Keith Alexander surely helped the company generate significant venture funding—to the tune of $110 million in two rounds. Although the company was actually founded in 2014, it operated in stealth mode with the first element of its solution until late 2017, when it delivered the other half of its combined security analytics and threat intelligence sharing solution. The startup holds two patents on its IronDefense security analytics and IronDome threat intelligence sharing products. Among the early customers using IronDome are five of the ten largest electric utility providers in the U.S. In addition to CEO Keith Alexander, the company is led by other former high-ranking NSA and U.S. Cyber Command veterans including Chief Operating Officer Brett Williams, Chief Scientist James Heath, CIO George Lamont, and CTO Michael Ehrlich. The latest infusion of venture backing came in May 2018, with a $78 million B round from UK-based C5 Capital, as well as ForgePoint Capital and venture titan Kleiner Perkins Caufield & Byers. The company has 180 employees.

EMA
IRONNET
VENDOR TO WATCH
APRIL 2019

IronNet
Cybersecurity

Value Proposition

Although it will have to prove its bona fides among a crowded and competitive field of threat intelligence sharing vendors, IronNet Cybersecurity is unique in the speed with which its IronDome system can deliver new threat intelligence targeted at participants in specific industries—energy production is the best example. IronNet offers a unique combination of advantages, including the sharing of suspect behaviors discovered by participants the moment the IronDefense system observes them and anonymously shares data with IronDefense instances deployed at other industry peers through the IronDome system. This is in contrast to how sharing commonly occurs today, where security operators get an alert, investigate whether that potential indicator represents a real threat, and then work through a long forensic and legal process before sharing a signature-based indicator months after the initial incident. Given the too-high number of days it still takes to find and confirm real attacks within an enterprise, this immediacy is essential. Anonymized chat also allows participants to discuss what they're seeing and share observations about events without revealing who their employers are. At the same time, once a customer/participant in an exchange confirms an indicator of compromise based on collected events, it is instantly pushed out to all others in the exchange. Also fairly unique is the scalability of the infrastructure IronNet uses to gather threat intelligence among participants. IronDefense sensors are capable of sustained throughput of 10 Gbps, and the IronDefense analytics backend can support a large number of sensors—the largest product deployment today supports over twenty 10-Gbps sensors.

IronDefense operates on raw network traffic gathered by the company's sensors, which are deployed in the customer's network. That data is analyzed for anomalous behavior and then fed into the company's own expert system to contextualize and prioritize events. The system can take tens of thousands of suspect behaviors and boil them down to a reasonable number of alerts per day for participant analysts to investigate. To continually improve the accuracy of the expert system used in IronDefense to detect malicious behaviors, IronNet constantly runs simulations to test the analytics and system rules to see how they respond to simulated malicious behaviors it should be able to identify. Then, data scientists and developers are tasked with improving the analytics where the system fails to recognize malicious behaviors. Such tests are also run periodically against the production infrastructure of participants in the energy threat intelligence exchange to determine how it stacks up with existing defense-in-depth solutions and where the analytics might need additional improvements.

EMA Perspective

The downside to sharing all suspect events rather than confirmed IOCs is that a lot of the information is based on benign events that a customer's analysts must sift through. In addition, IronDome requires the skills of a Level 3 security analyst to operate among participants in a given exchange. This can limit the number of potential customers that would find the TI exchange useful.

IronNet has taken good steps to lower the barrier to adoption by anonymizing data specific to each participant and only sharing metadata and communications with IP addresses outside the enterprise's control. The anonymized chat capability also helps reduce friction and add value to the industry-specific threat exchanges.

But as other TI vendors and Information Sharing and Analysis Centers (ISACs) have found, getting buy-in from a broad enough range of participants to provide useful visibility into industry-specific attacks is not easy to accomplish. There are industries more open to sharing threat intelligence than others. In addition to regional power utilities and regional healthcare providers, another vertical is the defense industrial complex, with its proclivity to subcontract large projects to each other. In highly competitive verticals, such as financial services, there is extremely limited interest in sharing any industry-specific threat intelligence that may benefit a rival company.

Still, recognition in the industry continues to grow around the fact that there are ongoing, strategic cyberattack campaigns carried out against certain sectors of the economy by nation-state actors: Iranian state sponsors attacking the energy sector, Russian state hackers targeting financial services, and Chinese state hackers attempting to steal intellectual property. Because these actors use similar techniques in their campaigns, sharing threat behaviors among members in vertical markets can give participants a speed boost in time to detect threats against such well-organized campaigns.

IronNet Cybersecurity upped the ante in the fast-growing and well-financed digital threat intelligence management market. It brings a formidable list of advantages to the game.

About Vendor to Watch: EMA Vendors to Watch are companies that deliver unique customer value by solving problems that had previously gone unaddressed or provide value in innovative ways. The designation rewards vendors that dare to go off the beaten path and have defined their own market niches.

About EMA: Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.