Cool Vendors in Security Operations and Threat Intelligence

Published 5 May 2020 - ID G00720794 - 14 min read

By Analysts Brad LaPorte, Peter Firstbrook, Neil MacDonald, Toby Bussa

Security and risk management leaders should consider Cool Vendors of security technology to meet evolving requirements to detect and respond to threats. Cool Vendors aren't the right choice for every organization, but they demonstrate new approaches to address difficult issues.

Overview

Key Findings

- Security and risk management (SRM) leaders with mature capabilities are increasingly willing to consider newer solutions to improve threat detection and response, as well as their use of existing solutions.
- SRM leaders have an overwhelming number of vulnerabilities to address and often overlook foundational gaps in firmware security and control misconfiguration.
- SRM leaders are seeking solutions to programmatically test their security posture and prioritize control gap activities based on business risk.
- Many organizations seek to improve their threat detection and response capabilities by purchasing tools like endpoint detection and response (EDR) and security information and event management (SIEM), but lack the resources and expertise to use them effectively.

Recommendations

Security and risk management leaders should:

- Evaluate providers through trials, rather than only through RFP processes. Many solutions boast simple, fast deployments and cloud-based management, resulting in trials that are low or no cost to the organization.
- Ignore vendor terminology (such as machine learning [ML], artificial intelligence [AI] and analytics), and test providers on their ability to apply their technology solution to the organization's specific use cases, risks and needs.

Analysis

Alert fatigue and resource constraints are a continuing problem for many Gartner clients (see "How to Use Threat Intelligence for Security Monitoring and Incident Response" and "Adopt a Lean Digital Security Organization to Mitigate the Skills Shortage"). Today's threat landscape requires more investment than ever in expertise and processes; but, more often than not, organizations still purchase multiple security tools without these other necessary investments. Having too many security tools and threat intelligence that isn't fine-tuned or applicable to your environment can easily overwhelm your resources with unnecessary notifications and false positives. By ultimately greatly reducing alert fatigue, SRM leaders can free up resources and effectively reduce bottom-line costs. The easier and faster solutions can be implemented, the faster these benefits can be realized. More is not always better.

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

What You Need to Know

Security and risk management leaders responsible for security operations should evaluate creative approaches to improve their ability to detect and respond to threats in their IT environment, and to improve the efficiency of their security controls. The products and services presented in this research help address those areas by helping security teams detect attacks, prioritize vulnerabilities and optimize their security technology tools.

Eclypsium

Beaverton, Oregon, U.S. (eclypsium.com)

Analysis by Neil MacDonald

Why Cool: Eclypsium offers enterprises a life cycle approach to continuously manage the risk of firmware across most of their IT portfolio. This life cycle approach to device risk management is cool because the only alternative for most enterprises was to track their disparate device configurations and firmware versions manually using spreadsheets and by visiting dozens of individual vendor sites to gather the information. Eclypsium has built a cloud-based (optionally it can be kept on-premises) database of all major firmware offerings typically found in most enterprises for network, network storage and endpoint devices. Agents and stand-alone scanners for endpoints and remote calls to network gear gather firmware and device details. From this, enterprises can build hardware inventory and automatically validate if firmware versions are known, vulnerable and up to date, and can identify tampering and potential supply chain malware implantation.

Attacks such as Spectre, Meltdown and subsequent variants, as well as recent APT41 attacks on the firmware of Cisco and Citrix hardware have shown the importance (and the difficulty) of maintaining updated firmware versions. Further, typical endpoint protection platform (EPP)

offerings (see "Magic Quadrant for Endpoint Protection Platforms") don't assess the basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI) or firmware of the system they are running on. Yet, the impact of a firmware attack is quite high as an exploit at the firmware layer could impact the integrity of everything running above it, including the hypervisor in virtualized environments.

Eclypsium's database is comprehensive and growing with more than 5 million unique firmware components and device profiles, covering more than 30 different equipment and device manufacturers. Some larger vendors' versions number in the thousands. The database itself is becoming a cool differentiator for Eclypsium as it can now analyze new firmware versions for vulnerabilities, potential backdoors and malware that may have been placed into the vendor's supply chain by an adversary. It also provides a reputation service on the firmware versions, allowing enterprises to make decisions on what version they should install.

Challenges: The most significant challenge is that enterprises are unaware of the problem with firmware risks across their IT hardware fleet (see "How to Mitigate Firmware Security Risks in Data Centers, and Public and Private Clouds"). Because most EPP or network security offerings don't identify firmware and hardware risks and don't patch their devices, the risk is latent and without a centralized and automated way to manage, and thus it tends to be addressed sporadically. Worse, the budget and responsibility for device security are often spread across multiple teams.

To get detailed visibility across the entire fleet of devices, Eclypsium uses a combination of agentless and agent-based technology. On desktop and laptop devices, Eclypsium deploys an agent (or a stand-alone executable) that adds to operational complexity. Agentless technology is used to assess security of network appliances and other connected devices, but it has limited visibility into device internals. Support for most Internet of Things (IoT) and operational technology (OT) devices is a roadmap item, and mobile device firmware is not a part of the offering.

Firmware updating varies widely among device manufacturers. Eclypsium can identify risky and outdated devices and offer remediation through firmware patching. However, automatic remediation of hardware and firmware is a complex process most organizations simply don't have.

Finally, as enterprises shift more workloads to the public cloud, the responsibility to secure and patch cloud hardware/firmware belongs to the IaaS provider. Here, the Eclypsium agent can only provide visibility. A report by Eclypsium researchers demonstrated an attack on a cloud-provisioned bare metal systems raising awareness of this potential issue.

Who Should Care: Any information security or IT operations professional responsible for infrastructure security including endpoint and network devices should be aware of the significant latent risk that is lurking in unmanaged firmware versions. Eclypsium's life cycle approach to firmware and hardware risk management will appeal to security leaders in risk-aware, risk-averse organizations looking to gain visibility and address threats to device integrity from firmware,

including the assessment of new devices before deployment. In many cases Eclypsium's offering will replace cumbersome manual approaches, and it offers a way to automate and continuously manage firmware risk.

GreyNoise

Washington, D.C., U.S. (greynoise.io)

Analysis by Brad LaPorte

Why Cool: The internet is overrun with "mass scanning" activity that is continuously looking at billions of routable IP addresses. This very noisy traffic can be benign, such as Shodan, Censys, Sonar, and ShadowServer data, or it can be malicious, such as SSH worms (Mirai), IoT worms, Conficker, etc. GreyNoise analyzes and collects this omnidirectional internetwide traffic and identifies the activity that is not targeting you. This is very effective in identifying pointless security events and false positives that would have been generated in your environment. This allows users to focus their attention on more important, targeted threats to their networks. GreyNoise presents this extraneous data to users in an easy-to-use UI and API, where they can then filter this out from their existing workflow.

GreyNoise has free, standard and enterprise versions that are currently utilized by thousands of users around the globe every day. In addition, GreyNoise has partnered with several market-leading security operations and threat intelligence providers over the past year, which is commendable given the small size of their company and the length of time since it launched its platform. Clients that use GreyNoise have reported that this solution generally reduces unnecessary alerts by more than 25%.

Challenges: The threat intelligence market is very fragmented, comprising more than a hundred vendors. In this very busy space, GreyNoise is the only threat intelligence solution that exclusively focuses on "anti-threat intelligence," or more importantly on what not to look at. GreyNoise's biggest challenge is competing against this vast number of vendors while continuing to show value as a complementary solution. GreyNoise will need to ensure its approach proves out or it will be challenged by buyers on why it works and whether it is worth their investment. Since its solution is considered complementary, extra effort will be required to highlight its differentiation and so it is not viewed as a commoditized optional product.

Who Should Care: Security and risk management leaders of mature security monitoring programs at large or midsize enterprises looking for a way to rapidly increase the effectiveness of their security technologies and threat intelligence capabilities should consider GreyNoise. Especially if they have budget and resource constraints. GreyNoise reduces false positives so resources can focus on what is really important and take action on it.

Red Canary

Denver, Colorado, U.S. (redcanary.com)

Analysis by Toby Bussa

Why Cool: There are many providers that offer managed endpoint and detection and response (MEDR) services. As MEDR races toward becoming a commodity offering, differentiating in this market is challenging. One of Red Canary's key differentiators in this market is its security orchestration and automation (SOA) for response capability with its Act offering. The product automates customer-defined processes or plays in response to threats and other conditions that can be identified via the collected endpoint telemetry. The external exposure of SOA capabilities to customers is still nascent in the managed detection and response market.

Red Canary has also made strong contributions to the security community through the release of its Atomic Red Team tests. These tests allow organizations to simulate a variety of the tactics in the MITRE ATT&CK framework. This can aid organizations in understanding how they would log, detect and respond to various attack tactics, either individually or chained together (aka "chain reactions") to more closely mimic an attack against their organization.

Red Canary's MDR service is delivered via several EDR technologies like Carbon Black, CrowdStrike, and Elastic (formerly Endgame) and Microsoft Defender ATP. The MDR service provides 24/7 monitoring and investigation that use automated and human-powered event investigation, as well as on-demand threat hunting. Red Canary MDR leverages the MITRE ATT&CK framework that maps detections to attacker tactics, techniques and procedures. It also uses behavioral profiles to baseline expected behavior on endpoints, so deviations can be detected and investigated.

Challenges: Security services like Red Canary's that focus on using EDR technologies are limited to monitoring only endpoints, namely Windows, Mac and Linux. While a majority of attacks start at the endpoint level, or may touch an endpoint while moving laterally through an organization, relying solely on EDR may not detect attacks against other assets and environments that are not visible to the endpoint. The use of EDR agents may also have challenges covering "the cloud." Attacks against SaaS, such as business email compromise attacks against Office 365, cannot be detected via EDR technologies. Deploying EDR into IaaS may also prove challenging depending on how those environments are used, e.g., the licensing implications for an EDR agent when virtual instances use may be heavily elastic. Red Canary has a proprietary Linux agent that can be deployed to aid monitoring of those instance types in IaaS environments.

Who Should Care: Security and risk management leaders who have, or are planning to deploy, EDR or modern EPP with EDR, and lack the expertise to effectively use these technologies, especially where 24/7 threat monitoring, detection and response are required should consider Red Canary. Midsize enterprise leaders who lack security staff and are interested in using built-in and customizable automation and response capabilities should also consider Red Canary.

XM Cyber

Tel Aviv, Israel (xmcyber.com)

Analysis by Peter Firstbrook

Why Cool: XM Cyber is one of a new breed of breach and attack simulation (BAS) tools that enables organizations to perform continuous attack and threat simulation testing to better understand the effectiveness of their security controls. XM Cyber can perform automated penetration testing using common attack tools to illustrate an attacker's view of the environment. Capture-the-flag-like tests can run simulated attacks targeted at key corporate computing assets, revealing the full attack kill chain that might lead to breaches or disruptions.

XM Cyber reporting provides specific actionable remediation guidance to reduce the attack surface. Its guidance is tailored to the customer's environment, giving remediation options based on business resource constraints. Attack techniques are aligned to the MITRE ATT&CK framework. XM Cyber can be operated as a cloud application (SaaS) or an on-premises management server. Agent sensors are deployed on some machines (i.e., 10%) in different LAN segments. XM Cyber has also launched a BAS tool for testing Amazon Web Service applications.

Challenges: XM Cyber is one of a number of new vendors in this market. It has to successfully differentiate its product from the pack, while leveraging partnerships and the channel to accelerate its growth. BAS tools are not yet well-known, thus, while the need for these types of tools is apparent, the demand is still low. Buyers of these tools must already be at a sufficient maturity level with basic asset inventory, network topology and environmental awareness. Organizations with less-mature security postures might not benefit fully from implementing BAS, but may still benefit from specific tests against critical assets. Not all attacks can be simulated and not all simulations can test every attack type. BAS doesn't replace vulnerability management, but certainly it can help set priorities by providing insight into where the risks are and test security controls.

Who Should Care: Middle to high maturity security organizations looking to improve the security posture and continuously test critical defenses would benefit from BAS tools. Those that wish to test using real exploit techniques and get an attacker view of their environment would benefit from XM Cyber.

Where Are They Now?

Verodin (acquired by FireEye)

Maclean, Virginia, U.S. (www.fireeye.com/solutions/verodin-security-instrumentation.html)

Analysis by Toby Bussa

Profiled in "Cool Vendors in Security Operations and Threat Intelligence," 2019

Why Cool Then: Verodin called itself a security instrumentation platform (SIP). This instrumentation of the security infrastructure allows an organization to continuously verify configuration state and efficacy. Verodin takes a similar approach to other vendors in the BAS market, but with a strong focus on continuously managing, measuring and improving security controls' effectiveness. Verodin provides a platform that emulates attacks, but it goes beyond assessing if attacks are successful or not. It integrates with the multiple tools of the

organization's security infrastructure to assess how it performed against the attacks, going beyond assessing prevention to also test detection and response capabilities.

Where They Are Now: On 28 May 2019, Verodin was acquired by FireEye for $250 million. FireEye indicated at the time of the acquisition that, in addition to continuing to be sold as a stand-alone solution, Verodin will be integrated with FireEye Helix and be leveraged by FireEye's Mandiant Managed Defense Service and as an Expertise On Demand automated solution. On 16 April 2020, FireEye rebranded Verodin as Mandiant Security Validation.

Who Should Care: Mandiant Threat Intelligence now provides potential and existing Mandiant Security Validation customers with the enhanced depth and breadth of visibility into attacks through the platform's content library. Mandiant Services also leverages Mandiant Security Validation in its services, e.g., offering Mandiant Purple Team Assessment. Existing customers should ensure that any features previously promised before the acquisition remain a roadmap commitment. They should monitor any indications of strategy shift following the acquisition.

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.