REPORT REPRINT

ExtraHop jumps into security analytics and incident response with Reveal(x)

ERIC OGREN, PATRICK DALY, JASMINE RISHI

06 MAR 2018

Active threats inevitably disclose themselves as they use the network to locate other devices to penetrate, stockpile stolen data, and transmit confidential data to external web domains. ExtraHop has launched Reveal(x) to provide real-time network traffic analytics to detect threats and accelerate incident responses.

ExtraHop has begun 2018 by releasing Reveal(x), a product that builds on the vendor's performance-monitoring heritage with network traffic analytics in delivering advanced threat detection for enterprise security operations. Active threats inevitably disclose themselves as they use the network to locate other devices to penetrate, stockpile stolen data, and transmit confidential data to external web domains. Reveal(x) reassembles copies of raw network traffic into sessions of L2-7 traffic across more than 50 different protocols to discover and immediately classify connected devices by application type, catch attacks by the way they utilize the network and interact with critical assets, and give incident responders prioritized alerts with the implications and packet-level evidence necessary for expedited remediation.

THE 451 TAKE

Security operations centers (SOCs) are turning to network traffic analytic offerings such as Reveal(x) as a first-alert data source to detect and rapidly mobilize against threats that are active within the business. An advantage to interpreting observed network traffic is that SOC analysts can respond to alerts as soon as threats give themselves away instead of struggling to piece together insights from reported log data. Reveal(x) goes a step further in characterizing affected assets by application type and value to the business to help prioritize remediation efforts. It detects threats and delivers correlated, concise investigation guidance built on cloud-based machine learning. REST APIs facilitate an approach that partners with security information and event management (SIEM) and security automation and orchestration (SAO) products, as well as countermeasure providers, for managing workflows and remediation playbooks. We believe enterprise security personnel should have network traffic analytics as part of their internal architecture to espy nefarious activity. The ability to categorize assets and integrate with remediation automation and orchestration processes is an additional bonus.

CONTEXT

Seattle-based ExtraHop Networks was founded in 2007 by Jesse Rothstein and Raja Mukerji. Rothstein currently serves as CTO, and Mukerji holds the position of CCO. The company appointed Arif Kareem, who was previously president of Fluke Networks, as president and CEO in 2016. It has raised a total of $61.6m in five funding rounds, most recently $41m in a series C led by Technology Crossover Ventures. ExtraHop has an extensive roster of technology partners such as Cisco, AWS and Splunk. It also boasts a variety of customers across several verticals, including Bentley University, DigiCert, McKesson and Lockheed Martin.

The company has spent the past 10 years as a network operations vendor providing real-time analysis of wire data to help control network and application performance. Last year, ExtraHop announced its IT operations and monitoring service, Addy, an addition to its platform that uses machine learning for real-time threat detection and IT operations insight. Addy foreshadowed Reveal(x)'s reliance on analyzing transactions, application and user sessions, and network flows, and describing connected assets in its entry into the network security space.

STRATEGY

ExtraHop's decision to venture into security operations is an effort to stay up to date with its customers' needs. After introducing its ransomware-detection service in 2016, the company saw significant uptake in security use cases among its customer base looking to extend knowledge of performance and lateral traffic into security insights. Its strategy is to leverage its networking strengths to assist security teams. ExtraHop plugs contextualized and correlated data into the security ecosystem of SIEM alert processing, as well as SAO specialists such as Phantom and ServiceNow, to handle remediation workflow and playbooks.

The vendor has also hired new sales assessment and marketing teams to expand its channel partners and better place its security products as it enters a new, crowded market. Establishing partnerships with MSSPs, VARs and SIs

could open up a new avenue for sales in multitenant SOCs. This could improve Reveal(x)'s economies of scale and attract SMB customers that may otherwise be unable to afford a sophisticated security analytics platform.

PRODUCTS

Although Reveal(x) leverages much of the foundational technology within ExtraHop's network performance optimization platform, the offering differs in that it is specifically designed to aid security operations teams in detecting, investigating and responding to incidents. The company is marketing Reveal(x) as a three-in-one offering capable of improving east-west visibility, identifying abnormal behaviors and triggering automated threat responses. Reveal(x) is either deployed on-premises as an out-of-band physical or virtual server, or in the cloud employing AWS or Azure. It decrypts encrypted traffic and captures a complete record of the data, including the application and protocol data as well as user interactions and the content of the traffic.

The product conducts real-time analysis of traffic behavior to identify all connected devices and classify critical network assets. Anomaly detection deploying cloud-based machine learning then provides insights for potential threats. By creating wire data from unstructured packets, ExtraHop claims that it can offer more in-depth analysis than can be achieved by analyzing the network flow data and packet headers alone. When an anomaly is detected, the system provides a dedicated UI to help SOC analysts understand the anomaly and its role in the attack chain. In addition, dashboards display unusual activity that a security analyst might want to monitor, such as use of deprecated cryptography.

Alerts contain a detailed summary of the suspicious behavior that prompted them. In the example of data exfiltration, Reveal(x) can tell a customer exactly how much data was stolen and when it occurred. A live activity map visualizes relationships and interactions. The vendor claims that the process from which Reveal(x) detects foreign activity to sending a notification happens within seconds.

An existing partnership with Phantom helps make Reveal(x) even more useful for incident response and remediation use cases as alerts generated by ExtraHop can automatically feed into Phantom's SAO platform to trigger a Phantom playbook. Customers should find value in this as it further automates the response process and reduces the manual burden on enterprise security operations teams.

Reveal(x)'s analyst dashboard gives customers a full view of active devices in the environment and any alerts those devices have generated. Alert information can be visualized in a variety of ways, including by specific endpoint or distinct user groups. The dashboard also enables users to create a timeline of an attacker's lateral movements between network assets and identify what type of reconnaissance they conducted while in the network, all of which is valuable intelligence for incident response teams. In addition, analysts can view this information in a summarization underneath the graphic, which details the event's interval, peak value, expected range and deviation, as well as the anomaly's security implications. Analysts can click directly into the related packets.

COMPETITION

ExtraHop's value starts with its ability to interpret network activity, particularly east-west traffic within the network. This brings other network security devices into direct competition, including those from Awake Security, Darktrace, Vectra Networks, FireEye (with SmartVision), Cisco (Stealthwatch), SecBI and Palo Alto (features from Magnifier). Many of these operate on header information and do not move up the stack to interpret traffic contents. Reveal(x) applies its network visibility to discover and classify assets (number of connections, transaction rates, protocols used, etc.) in ways that are unique, and decrypts traffic out of band. Most of ExtraHop's rivals are further along in offering SAO integration features. Reveal(x) uncovers living threats that security teams must then figure out how to fix – we would not be surprised if ExtraHop was more assertive with SAO features in future product releases.

With its entry into security analytics, ExtraHop will encounter a host of SIEM-oriented competitors that approach the problem of detecting living threats via analysis of log and event data. Although Reveal(x) is clearly differentiated by its use of the network as its primary data source, ExtraHop can expect to vie with SIEM providers such as IBM (with QRadar), Splunk, AlienVault, McAfee, MicroFocus ArcSight, Exabeam, Securonix, RSA (NetWitness) and LogRhythm. The product's foray into automated incident response and its ability to track an attacker's movement throughout the network will also bring ExtraHop up against threat-hunting players like Sqrrl, which was recently acquired by AWS, IBM (with its i2 product), Forcepoint and Endgame.

SWOT ANALYSIS

STRENGTHS
ExtraHop's expertise in network performance analytics gives the company a solid foundation on which to build its security analytics portfolio from wire data (not logs).

WEAKNESSES
As with most network traffic analytic products, finding threats means that someone has to remediate them. Reveal(x) relies on partners to close the loop by managing remediation actions.

OPPORTUNITIES
ExtraHop can expand its asset classification capabilities to move up the stack in reporting traffic anomalies in terms of users (as opposed to IP addresses) and applications, and the communications between them.

THREATS
Many enterprise security operations centers have standardized analytics detection, SAO logic and custom script development on SIEM interfaces.