REPORT REPRINT

Tripwire has Axon to grind: endpoint visibility for expanding enterprise environments

ERIC OGREN, KATHRYN BALL

1 DEC 2016

The war against IT as playthings for malicious actors has been waged, and plenty of security vendors are hopping on the train toward new coordinated infrastructure protection. Besides an updated vulnerability management tool, Tripwire Axon agents for Enterprise extend its reach to account for the growing number of endpoint and IoT devices on an organization's complex network.

451 Research®

 |

Tripwire released a round of product updates in August, on the heels of Black Hat 2016. The security controls vendor is focusing its efforts on bringing lightweight tools to expanding enterprise IT environments in order to reduce security blind spots. The constant conversations surrounding the new frontier of IT and IoT security means it's no surprise that Tripwire is looking to get some skin in the game. These new updates are just the beginning. Tripwire's newest Axon release promises to shine light into the dark corners of the network to better protect corporate endpoints.

THE 451 TAKE

Tripwire's leap at the opportunity to provide visibility into hard-to-touch enterprise IT horizons comes during an opportune moment for the longtime security, compliance management and IT Ops vendor. As we've witnessed, it's clear that the initial concern of the unsupervised IT landscape is legitimate. Companies are scrambling to protect themselves and their customers from the next onslaught of attacks. In doing so, enterprises may benefit from Tripwire's latest Axon release to provide a clearer idea of the endpoints sitting on their networks, as well as a quicker and easier way to manage the streams of data being produced from these various new devices. Deep visibility into an organization's network and security configuration management will continue to be necessary tools in any security team's toolbox. We view it as a security imperative to know what devices are on the network, what comprises compliant configurations for devices, and when unauthorized changes are made that put the enterprise at risk.

CONTEXT

Portland, Oregon-based Tripwire was established in 1997, and pulled into the Belden belt at the beginning of 2015 as a leading product line in the company's Industrial Cyber Security division. Since then, Tripwire has spent much of its energy and resources on managing security around the total network infrastructure and emerging industrial Internet of Things (IoT).

As the IoT landscape has expanded, and malicious actors manipulate the low-hanging fruit that are unprotected devices, organizations are beginning to focus on identifying and hardening endpoints and assets in their own environments. Tripwire's efforts in this area focus on compliance and security across an enterprise's own attack service as it expands to include these emerging technology implementations. The company's current employee headcount is roughly 500.

TECHNOLOGY

Tripwire announced a few key releases within its enterprise offering in August, including the newest version of its vulnerability assessment product Tripwire IP360, and a new enterprise agent for its security data collection platform Tripwire Axon, announced in March. The Tripwire Axon agents for Enterprise 8.5 were announced within the same time frame as the updated Tripwire IP360. Tripwire Axon is the company's cyber-security data collection platform built for the enterprise, with scalability and industrial IoT in mind.

The platform aims to optimize the collection, aggregation and application of data from expansive enterprise environments, which now often include a great deal of nontraditional endpoints. Tripwire hopes Axon will provide the capability to extract data from every endpoint found on the network, from enterprise IT to industrial IoT devices. The Tripwire Axon agents are built to reuse data across security controls, rather than pulling from different streams separately.

Tripwire Enterprise is the company's security configuration management tool that focuses on threat detection, compliance enforcement and security automation. The Tripwire Axon agents are lightweight and modular, essentially reducing the total ownership costs by operating on fewer resources, and providing individually selectable data collection based on the customer's own environment and threat profile. A specific feature that often troubles other vendors is resiliency, or the ability to operate through system updates or other interruptions. Tripwire Axon agents for Tripwire Enterprise continue to collect data after the operating system or network changes, or after an outage occurs, even on remote networks.

Tripwire IP360 8.0 is a vulnerability and security risk management tool that works to discover and profile network assets, and allows for the delivery of dynamic vulnerability prioritization metrics. Prioritizations are made off of the combination of business assets and vulnerability scoring. Tripwire states that the tool is able to discover more than 118,000 security-relevant conditions, anywhere from vulnerabilities and configurations to applications and operating systems. These conditions are determined by the Tripwire Vulnerability and Exposure Research Team (VERT), which provides up-to-date intelligence on vulnerabilities that directly relate to enterprise applications such as Java, ImageTragick and others.

Tripwire IP360 also centralizes data aggregation, and allows for role-based management and reporting in one location with the intention to minimize its own impact on a customer's network and systems. Tripwire IP360 is now said to be faster and more resilient due to its ability to distribute scanning across multiple appliances, allowing for further visibility across large and complex networks. Updates to this product focus on usability, with a new user interface to complement Tripwire IP360's command line interface to automate vulnerability management workflows.

The user interface contains new search, filter and export capabilities, while the vulnerability assessment tool itself still provides continuous network scanning. One last addition to Tripwire's list of product updates and launches is the Tripwire Configuration Compliance Manager (CCM) Express, the newest version of the compliance tool that runs complementary to Tripwire Enterprise. Tripwire CCM Express aims to simplify the process for midsized organizations with 'audit ready' reporting of compliance status across monitored systems.

Tripwire CCM Express does not require additional agent software, and offers policies for specific regulations such as HIPAA, PCI DSS and FISMA. A significant innovation is Tripwire's messaging bus to streamline communications between enterprise security components. The messaging bus keeps the Tripwire Axon endpoint community up to date with policies, and ensures accurate reports for endpoint visibility.

COMPETITION

Coordinated enterprise security is one of the most highly competitive of recognized security segments. Tripwire has the advantage of avoiding the malware research treadmill by starting with IT-defined compliant configurations, recognizing unauthorized changes to the operating environment, and scanning for the root causes of those changes.

However, many vendors provide coordinated endpoint and network security products. Tripwire's competition traditionally comes from other vendors in the policy compliance, file integrity monitoring and vulnerability management market spaces including AlienVault, LogRythym, Symantec, McAfee, Cimcor, New Net Technologies, Splunk and IBM.

SIEMs as a class are oriented toward event retention in support of compliance audits and forensic investigations. SIEM must normalize data formats and resolve semantic differences across partner data sources to detect intrusions. Network security vendors branching out to endpoint security represent an important class of future competitors. We see Check Point, Cisco, Fortinet, Palo Alto and Sophos all offering network, endpoint and messaging bus features focused on the vulnerability/exploit/patch security processes. We also see traditional endpoint security vendors McAfee, Microsoft, Symantec and Trend Micro adding network detection and enforcement to their security portfolios.

The main idea is that a coordinated reaction involving network detection and endpoint protection is likely required when a penetrated endpoint is detected. Tripwire's vulnerability management product, IP360, competes directly with similar product lines at Tenable (SecurityCenter), Rapid7 (Nexpose), Tanium and Qualys. Qualys and Tanium also come up as competitors with executable file integrity monitoring features, along with Accelerite and OSSEC. Tripwire's endpoint security products compete with Tanium, Fidelis (AccessData), Endgame and FireEye (HX Series).

SWOT ANALYSIS

STRENGTHS

Tripwire has a strongly differentiated product set with a loyal base anxious for Tripwire Axon and Tripwire IP360 products. The technology tilts toward enforcing IT policies, which rids Tripwire of the need to chase specifics of the 'attacks du jour.'

WEAKNESSES

A stronger network capability would allow Tripwire to deliver Tripwire Axon features for mobile devices, tablets and cloud applications where endpoint software is impractical.

OPPORTUNITIES

IoT, with its landscape of devices that defy network upgrade and patch processes, presents a significant opportunity for Tripwire. We expect to see Tripwire offer slimmed-down industrial IoT Tripwire Axon features, perhaps delivered through its Belden parent.

THREATS

The shift of applications from on-premises datacenters to the cloud reduces enterprise dependencies on its infrastructure. Tripwire needs to carefully monitor competitors offering AWS or Azure solutions, while developing Axon extensions for cloud workloads.