FireEye Powers the Next Generation Security Operation Center With Orchestration and Platform Enhancements


MILPITAS, CA -- (Marketwired) -- 05/05/16 -- FireEye, Inc. (NASDAQ: FEYE), the leader in stopping today's advanced cyber attacks, today announced FireEye® Security Orchestrator™ (FSO™) -- the orchestration and automation solution leading FireEye's efforts to help customers build their next generation Security Operations Center (SOC) and reduce the impact of a breach.

Enhancements to the intelligence-led FireEye Global Threat Management Platform were also announced, focusing on detecting non-malware based email attacks, providing greater visibility into attackers' lateral spread, guiding investigation activities, and offering high availability features for deploying FireEye inline.

"As cyber threats have become more sophisticated, the security industry has responded with complex defensive layers that force organizations to manage an overwhelming number of technologies and alerts," said David DeWalt, CEO and chairman of the board, FireEye. "FireEye Security Orchestrator uses innovative technology to deliver automated playbooks informed by a decade of experience responding to sophisticated threats -- addressing the growing resource constraints that are slowing down today's security operations. As part of our mission to enable the faster, next generation SOC, FireEye is also the only company to now offer continuous inline protection powered by industry-leading MVX technology."

FireEye Security Orchestrator

Based on FireEye's recently-acquired Involas, FireEye Security Orchestrator provides a solution for cross-vendor orchestration, automation, and a central hub for security operations processes. By unifying workflows across numerous security technologies and the FireEye Threat Management Platform, organizations can simplify repetitive, manual processes that are prone to human error.

Features of FireEye Security Orchestrator include:

- **Playbooks** informed by Mandiant® expertise that act as codified procedures to shrink incident response times;
- **Case Management** for security analysts to manage incidents centrally;
- **Automation and documentation of manual processes** designed to eliminate the majority of operational errors and ensure that policies are enforced consistently;
- **Investigative Workbench** that facilitates the ability to aggregate, search, correlate, and take action for events of interest;
- **User-friendly reporting and analysis** to monitor efficiency and effectiveness of security investments;
- **Orchestration Deployment Services** providing expertise to design and deploy orchestration and automation to maximize return on investment; and
- **Cyber Security Coalition (CSC) partnerships and deep integrations** with technology providers such as Blue Coat, BMC Software, MobileIron, PhishMe, Splunk and many more to enable our customers to unlock the value of orchestration and automation through an open ecosystem.

"CyberArk supports FireEye's commitment to continuing to improve threat response capabilities for customers with Security Orchestrator," said Adam Bosnian, executive vice president, global business development at CyberArk and head of the C3 Alliance. "As a CSC partner and through integrations of our respective solutions, which incorporate privileged account security best practices and privileged activity data, we enable customers to better detect and respond to threats."

"Simplifying security in organizations that are increasingly mobile first demands integrated solutions that unify security architectures," said John Spencer, vice president strategic partnerships, MobileIron. "MobileIron and FireEye now provide a powerful framework that our joint customers can take advantage of to make securing their data faster and less resource-intensive."

"Blue Coat and FireEye are committed to protecting our shared customers by working together to address their needs," said Bradon Rogers, SVP of product strategy and operations, Blue Coat. "As a CSC partner, we will ensure simplicity for
To learn more about FireEye Security Orchestrator, which will be available this quarter, please visit: https://www.fireeye.com/products/security-orchestrator.html.

**Network Security (NX)**

A foundational component of the next generation SOC is always-available, real-time protection that ensures resilient defense. FireEye research has shown that inline deployments reduce alert volume up to 76 percent. However, organizations have historically struggled to deploy inline security and balance it with business continuity. As a result, environments that rely on traditional security and out-of-band sandboxes are more exposed to fast-spreading cyber threats like ransomware.

FireEye has been a leader in enabling inline protection to secure against known and unknown threats with low false-positives. Updates to NX take a step further with stateful high availability (HA) and automatic failover, creating a transparent end-user experience to prevent business disruption. This allows organizations to more confidently balance inline security with business continuity. FireEye is also the only vendor to offer this security at scale -- to 4Gbps inline protection -- using the MVX technology.

To learn more about updates to Network Security, which are available now for selected models, please visit: https://www.fireeye.com/products/nx-network-security-products.html.

**Email Security (EX & ETP)**

High efficacy detection is also a cornerstone for the next generation SOC. FireEye is continuing to innovate both the on-premise and cloud versions of its Email Security products. FireEye Threat Intelligence shows that threats are increasingly delivered via emails that do not contain malware but instead use spear-phishing techniques -- sender impersonation and credential harvesting. FireEye Email Security is designed to protect against these new categories of email threats, preventing costly breaches. Organizations can now consume FireEye Email Security alerts in FSO and use them to initiate response workflows based on the severity of the threat, assets targeted, or the context behind the threat.

To learn more about updates to FireEye Email Security, which will be available this quarter, please visit: https://www.fireeye.com/products/ex-email-security-products.html.

**Threat Analytics Platform™ (TAP™)**

Further addressing the resource strains of security teams and the need for faster response workflows, TAP introduces the Guided Investigations™ feature to increase efficiency and augment investigation capabilities to decrease response time. The feature leads users through FireEye's industry-leading investigative methods by prepopulating a series of "next step" searches that provide useful context to the investigation. Guided Investigations streamlines the pivot from search to action by utilizing predictive analytics based on specific attack scenarios to suggest five or more queries for the responder to pursue.

To learn more about Guided Investigations in TAP, which is available now, please visit: https://www.fireeye.com/products/threat-analytics-platform.html.

**Enterprise Forensics (PX/IA)**

Threat investigations are also enabled by the FireEye Network Forensics Platform and Investigation Analysis system, the industry's fastest lossless network data capture and retrieval solution. FireEye has expanded this solution to now provide centralized analysis and visualization, including insights into attacker attempts at lateral spread within a victim organization. Responders can gain additional context through deeper integration with FireEye Network, Email, and Endpoint Security as well as FireEye Malware Analysis. This enables them to drive more effective and efficient investigations.

To learn more about updates to Enterprise Forensics, which are available now, please visit: https://www.fireeye.com/products/enterprise-forensics.html.

To learn more about recent updates to FireEye as a Service™, please visit: https://www.fireeye.com/products/fireeye-as-a-service.html.

For more information about the latest Mandiant Consulting services, please visit: https://www.fireeye.com/services.html.
About FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 4,700 customers across 67 countries, including more than 730 of the Forbes Global 2000.

Forward-Looking Statements

This press release contains forward-looking statements, including statements related to the expectations, beliefs, features, benefits and availability of FireEye Security Orchestrator and enhancements to the FireEye Global Threat Management Platform. These forward-looking statements involve risks and uncertainties, as well as assumptions which, if they do not fully materialize or prove incorrect, could cause the results of FireEye to differ materially from those expressed or implied by such forward-looking statements. The risks and uncertainties that could cause such results to differ materially from those expressed or implied by such forward-looking statements include customer demand and adoption of FireEye's solutions; real or perceived defects, errors or vulnerabilities in FireEye’s products or services; the ability of FireEye to retain and recruit highly experienced and qualified personnel; FireEye’s ability to react to trends and challenges in its business and the markets in which it operates; FireEye’s ability to anticipate market needs or develop new or enhanced products and services to meet those needs; competitive pressures faced by FireEye; and general market, political, economic, and business conditions; as well as those risks and uncertainties included under the captions “Risk Factors” and “Management’s Discussion and Analysis of Financial Condition and Results of Operations,” in FireEye’s annual report on Form 10-K filed with the Securities and Exchange Commission on February 26, 2016, which is available on the Investor Relations section of the company’s website at investors.FireEye.com and on the SEC website at www.sec.gov. All forward-looking statements in this press release are based on information available to the company as of the date hereof, and FireEye does not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made. Any future service, feature, objective or benefit that may be referenced in this release is for information purposes only and is not a commitment to deliver any service, feature, objective or benefit. FireEye reserves the right to modify future plans at any time.

© 2016 FireEye, Inc. All rights reserved. FireEye, Mandiant, Invotas, Security Orchestrator, FSO, MVX, Threat Analytics Platform, TAP, Guided Investigations and FireEye as a Service are registered trademarks or trademarks of FireEye, Inc. in the United States and other countries. All other brands, products or service names are or may be trademarks or service marks of their respective owners.

Source: FireEye

News Provided by Acquire Media