

Intel Security Unveils New Strategy to Provide Better Protection, Faster Detection and Streamlined Correction

Tuesday, October 27, 2015 07:00:00 PM (GMT)

Focus on integrated, open security systems with cloud-first technology empowers organizations to resolve more threats, faster, with fewer resources

News Highlights:

- Corporate strategy concentrates on control points at the cloud and the endpoint to address the expanding attack surface, imperative of time, and acute resource constraints that plague organizations today
- *New:* McAfee Endpoint Security 10.X establishes an agile endpoint services platform designed to reduce the complexity of endpoint security environments, improve performance and visibility into advanced threats, and speed detection and remediation
- *New:* McAfee Active Response, endpoint threat detection and response solution, helps improve threat detection and enables incident response agility with ease and efficiency
- Growing industry adoption of McAfee Data Exchange Layer and Intel Security support for Structured Threat Integration Expression (STIX) simplify integration of real-time protection, detection, and correction processes across threat intelligence sources, tools and data

FOCUS 15 -- Today, Intel Security unveiled its new [corporate strategy](#) aimed at enabling businesses around the globe to more aggressively and effectively defend against data breaches and targeted attacks. Through a more integrated and more open security system that unifies the key phases of the threat defense lifecycle, the new strategy focuses on the endpoint and the cloud as the most effective areas for advanced visibility and practical operational control. These control points are enabled by world-class threat detection and analytics. The strategy also emphasizes a simplified user experience powered by centralized management and a connected architecture across Intel and third-party products. Through this open and integrated system, Intel Security aims to empower organizations to resolve more threats, faster, with fewer resources.

Intel Security will continue to focus on its core strength of protecting organizations against known threats, and is expanding its investment in tools that help detect new threats faster and enable automated workflows to rapidly correct them. By unifying protection, detection and correction with real-time centralized management into an adaptive feedback loop, known as the threat defense lifecycle, security then evolves and learns in an iterative cycle that improves over time. This model helps organizations become more effective at blocking threats, identifying compromises, and implementing remediation as well as countermeasure improvements more quickly.

"The rising volume and complexity of attacks present a vicious cycle of challenges for organizations and makes speed and efficiency critical," said Chris Young, Senior Vice President and General Manager of Intel Security Group. "With a rapidly expanding attack surface, and a shortage of relevant talent and expertise, defenders need to win on visibility into events, simplified management, and capabilities that empower teams to close the loop on attacks in progress – faster, more effectively, and with fewer resources."

In support of the new strategy, Intel Security is also announcing new solutions that will each serve as a foundation for future technologies and products. McAfee Endpoint Security 10.X delivers a new streamlined and agile endpoint services platform, enabling protection for devices with faster scanning and deployment. McAfee Active Response, a new endpoint threat detection and response solution, supplies on-demand and continuous visibility into an array of endpoint activities with powerful, automated tools to respond to and monitor threat events. The solutions can be used and managed together using Intel Security's broadly adopted centralized management platform for a high-speed, high-accuracy, closed-loop approach to the threat defense lifecycle. Intel Security also now supports the Structured Threat Integration Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) standards designed to enhance detection of threats through sharing of threat intelligence.

McAfee® Endpoint Security

Serving as the foundation for Intel Security's dynamic endpoint strategy, McAfee Endpoint Security 10.X enables customers to uniquely tackle the threat defense lifecycle with reduced complexity and better performance. McAfee Endpoint Security 10.X introduces a new platform built to enable real-time communication between threat defenses for more effective protection against emerging threats. By sharing and leveraging security events, it can act against potentially dangerous applications, downloads, websites and files at the moment suspicious behaviors are observed, and before a system becomes patient zero. Its extensible architecture provides a framework for IT teams who are burdened with multiple solutions to enhance protection, detection and correction against today's advanced threats.

Key features in McAfee Endpoint Security 10.X include:

- **Intelligent Endpoint Protection:** access to real-time intelligence and actionable threat forensics from defenses that communicate and learn from each other to combat advanced threats
- **Strong and Effective Performance:** faster scanning, threat updates, maximized CPU and protection performance that is proven to be effective in third-party tests
- **Collaborative Protection Framework:** simplifies and removes complexity of duplicate technologies, connects other solutions, including third parties, and enables more defenses to communicate with each other using Intel Security's endpoint security framework

More information on McAfee Endpoint Security [here](#).

McAfee Active Response

McAfee Active Response is a new endpoint threat detection and response solution that gives security practitioners the tools they need to hunt, identify and correct issues rapidly, continuously, and in the manner that makes the most sense for their businesses. Managed by the central management platform, McAfee ePolicy Orchestrator® (ePO™), it is easy to use with other Intel Security and partner products as part of an efficient threat defense lifecycle.

With McAfee Active Response, analysts and administrators can access rich security event and state details from endpoints on demand and set up persistent collectors to monitor for risky changes in security posture. This continuous visibility improves threat detection and expands incident response capabilities with detailed live, interactive, and ongoing investigation and analysis. Insights become part of comprehensive reporting and prioritized alerts and actions via ePO. By adding on to an existing central management environment, users gain unified deployment, monitoring, scalability and extensibility, with no extra management agent and no need for incremental staff to administer.

More information on McAfee Active Response [here](#).

Open Platform and Expanding Threat Intelligence Ecosystem

The Security Connected platform from Intel Security was designed to orchestrate management, analytics and intelligence operations. Taking the concept of Security Connected a step further down the path of true integration, Intel Security's new strategy relies heavily on the ongoing development and evolution of an open platform built on standards and published interfaces for multi-vendor security information sharing.

To improve detection of threats through sharing of threat intelligence, Intel Security now supports the STIX and TAXII standards. Explaining details of zero-day and targeted malware, McAfee Advanced Threat Defense now generates a thorough malware report in STIX format that can be consumed by other compliant analysis or reporting products, including the McAfee Enterprise Security Manager. Additionally, the McAfee Threat Intelligence Exchange and McAfee Enterprise Security Manager can both ingest third-party threat intelligence in STIX format to enrich analysis and permit correlation between internal and external threat data.

Changing the dynamics of threat detection and response, the McAfee Data Exchange Layer (DXL) is an ultra-fast, bidirectional communication fabric that enables information and context sharing between connected technologies. Through the [Intel Security Innovation Alliance](#), security solutions from 16 vendors are now running on or working with DXL, creating an advanced security ecosystem for enterprises.

More about McAfee DXL [here](#).

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. The mission of Intel Security is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com

No computer system can be absolutely secure.

Note: Intel, the Intel logo, McAfee and the McAfee logo are registered trademarks of Intel Corporation in the United States and other countries. Other names and brands may be claimed as the property of others.

© 2015 Intel Corporation

View source version on businesswire.com: <http://www.businesswire.com/news/home/20151027005554/en/>

--30-- XA/SF

Contact:

Intel Security

Heather Haas, 408-346-5735

heather.haas@intel.com

or

Zeno Group

Sarah Lewis, 650-801-0937

sarah.lewis@zenogrup.com

Copyright Business Wire 2015

1.2

Industries: Technology, Data Management, Internet, Networks, Software, Security

Languages: English

Primary Identifiers: INTC-US

Related Identifiers: INTC-US, US458140100

Source: Intel Security

Subjects: Product/Service, Trade Show