McAfee
2821 Mission College Blvd.
Santa Clara, CA 95054-1549

McAfee Takes Human-Machine Teaming to New Levels

Empowers Security Operations Team with Comprehensive Security Solutions that include a New Data Architecture, Behavior Analytics Offering and Enhanced Integrations

Santa Clara, Calif., March 27, 2018 – McAfee, the device-to-cloud cybersecurity company, today announced an expanded product portfolio that evolves security operations teams capabilities and allows for rapid response to today's most advanced cybersecurity threats. McAfee's new Enterprise Security Manager (ESM 11) leverages a new data architecture optimized for scalability, performance, faster search, and collaboration. The new architecture along with new enhancements to McAfee Behavioral Analytics, McAfee Investigator, and McAfee Advanced Threat Defense, including integrations with McAfee Active Response, helps security operation teams optimize their security infrastructure so they can better leverage automation, improve detection, streamline workflows, and ultimately harnessing the power of human-machine teaming to improve response time and overall security outcomes.

According to Gartner, Inc., "Enterprises are striving to keep up with the current threat landscape with too many manual processes, while struggling with a lack of resources, skills and budgets. Security and risk management leaders should determine which security orchestration, automation and response (SOAR) tools improve security operations efficiency, quality and efficacy."[1]

With advanced analytics and McAfee's new and enhanced security operations solutions combined, organizations can now more efficiently collect, enrich and share data, turn security events to actionable insights and act to confidently detect and correct sophisticated threats faster.

"Existing tools and approaches are too reliant on human expertise," says Jason Rolleston, vice president of security analytics, McAfee. "The answer is human-machine teaming, where analytics- and machine learning-powered solutions augment the security team to detect more threats, faster and with fewer people."

Today's announcements also build upon McAfee's leadership position within security information and event management (SIEM) solutions. Gartner named the company a Leader, for the seventh consecutive year, in the December 2017 "Gartner Magic Quadrant for Security Information and Event Management."[2]

Benefits from the updates and enhancements to McAfee ESM 11, McAfee Behavioral Analytics, McAfee Investigator and McAfee Active Response include:

New McAfee ESM 11:

- **Flexible Data Architecture:** The open and scalable data bus architecture at the heart of McAfee ESM 11 shares huge volumes of raw, parsed and correlated security events to allow threat hunters to easily search recent events, reliably retaining and storing data for compliance and forensics, and enables data-hungry analytics applications.
- **Scalable Ingestion and Query Performance** The new McAfee ESM 11 architecture allows for flexible horizontal expansion with active-active high availability, allowing organizations to rapidly query billions of events. Additional ESM appliances or virtual machines can be added at any point to add ingestion, query performance and redundancy.

New McAfee Behavioral Analytics:

- **Identify Threats with Machine Learning:** Big data security analytics and machine learning technology discover new and unusual high-risk security threats without requiring extensive configuration or knowledge.
- **Prioritization of Threats:** McAfee Behavioral Analytics distills billions of security events down to hundreds of anomalies to produce a handful of prioritized threat leads.
- **Collaboration and Integration:** McAfee Behavioral Analytics integrates with the McAfee portfolio, including McAfee ESM, McAfee ePolicy Orchestrator, and McAfee Data Exchange Layer, along with other third-party security information and event management (SIEM) solutions.

New McAfee Investigator:

- **Activity Feed:** Feed shares data with open source and third-party tools to streamline workflows and improve collaboration.
- **Shorter Time to Insights:** Expanded investigation guides include logon anomalies and new navigation features to multi-select findings for faster case closure.

New McAfee Active Response:

- **New Integrations:** Integration between McAfee Investigator and McAfee Active Response enables analysts to scope the impact of a threat across their endpoints in real-time. Enhanced integration between McAfee Active Response and McAfee Advanced Threat Defense enables investigators to view detailed sandbox reports and indicators of compromise (IOC) including a new threat timeline report that visualizes attack execution steps from a single workspace.
- **Detection and Remediation:** Powerful new capabilities to detect Powershell exploits and remediate by isolating a host.

McAfee ESM 11 and McAfee Behavioral Analytics are available to customers today. McAfee Investigator will be available in April, and enhancements to McAfee Advanced Threat Defense and McAfee Active Response will be available in May.

Resources

- Landing page: https://www.mcafee.com/us/solutions/intelligent-security-operations.aspx
- Blog: Separating signal from noise
- Blog: A Model for Human and Machine Interaction: Human-Machine Teaming Grows up

- Report: Disrupting the Disruptors, Art or Science?
- ESG Report: Automation and Analytics versus the Chaos of Cybersecurity Operations
- 2017 Gartner Magic Quadrant for SIEM, Dec. 2017

About McAfee
McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all. www.mcafee.com

[1]Innovation Insight for Security Orchestration, Automation and Response, Claudio Neiva, Craig Lawson, Toby Bussa, Gorka Sadowski, 30 November 2017
[2]Gartner Magic Quadrant for Security Information and Event Management, Kelly M. Kavanagh, Toby Bussa, 4 December 2017.

– 30 –

MEDIA CONTACTS:

Tracy Holden
McAfee
Tracy_Holden@McAfee.com
408-346-5965

Sarah Erman
Zeno Group
Sarah.Erman@ZenoGroup.com
650-801-0937