Build a Coordinated and Unified Defense
Automate and orchestrate security actions across the threat defense lifecycle

McAfee and Splunk have teamed up to combine industry-leading McAfee® enterprise security offerings with the infrastructure control capabilities of Splunk® Phantom, a security automation and orchestration platform. The joint solution allows you to reduce complexity and improve operational efficiency through integrated, adaptive, and orchestrated intelligence and response capabilities. It helps you work smarter by automating repetitive tasks and allowing your team to focus their attention on other mission-critical decisions. It also helps you respond faster and reduce dwell times by automating detection, investigation, and response workflows. Finally, it helps you strengthen your defenses by integrating your entire security infrastructure together, so that each part is actively participating in your defense strategy.
Complex Environments Can Lead to Increased Risk and Higher Operating Costs

With the proliferation of devices across local, mobile, and cloud environments, it’s not surprising that the average large enterprise can have 50 or more security vendors, creating an extremely tough landscape to manage. In today’s heterogeneous IT environments, enterprises that rely on stand-alone products and unintegrated management consoles that do not communicate to share threat intelligence face greater risk and higher operational costs.

McAfee and Phantom Joint Solution

In response to an increasingly complex IT ecosystem and expanding attack surface, McAfee and Splunk offer customers an integrated, unified, and cohesive threat defense lifecycle. Splunk, through its membership in the McAfee Security Innovation Alliance, allows customers to maximize their security investments while also optimizing their security operations and improving their overall threat defenses.

McAfee and Splunk> Phantom App Integration

McAfee ePolicy Orchestrator (McAfee ePO) and Phantom

The McAfee ePO App for Splunk> Phantom allows customers to execute endpoint-based investigative and containment actions using the McAfee ePO platform from Phantom. Actions supported include: tagging devices, querying for device information, and device quarantine actions.

McAfee Enterprise Security Manager and Phantom

The McAfee Enterprise Security Manager App for Splunk> Phantom ingests data from the SIEM and makes it available to the Phantom Platform. Inbound events are parsed on the Phantom Platform, making event characteristics like the rule, signature, and actionName available for further automation and orchestration activities.

McAfee Advanced Threat Defense and Splunk> Phantom

The McAfee Advanced Threat Defense App for Splunk> Phantom allows customers to programatically submit executables to McAfee Advanced Threat Defense for analysis. Phantom receives and parses the analysis results, making the data available for additional automation and orchestration activities.

OpenDXL and Phantom

The OpenDXL App for Phantom enables customers to post and lookup event data using the Data Exchange Layer (DXL) fabric.

McAfee Active Response and Splunk> Phantom

Splunk> Phantom integrates with McAfee Active Response via OpenDXL to provide customers with the ability to search for hash values using McAfee Active Response. Lookups can be performed as part of an automation playbook or as an on-demand action during investigations on Phantom.
McAfee Threat Intelligence Exchange and Splunk> Phantom

Phantom integrates with McAfee Threat Intelligence Exchange via OpenDXL to allow customers to consume McAfee Threat Intelligence Exchange data by different apps within Phantom. This makes the most accurate and up-to-date threat intelligence available to all participating systems in the environment.

About Splunk

Splunk Inc. helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data. Join millions of passionate users and try Splunk for free today.

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

Learn More

For more information, visit the McAfee Security Innovation Alliance www.mcafee.com.