Build a Coordinated and Unified Defense

Automate and orchestrate security actions across the threat defense lifecycle

McAfee and Phantom have teamed up to combine industry-leading McAfee® enterprise security offerings with the infrastructure control capabilities of the Phantom 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.
**SOLUTION BRIEF**

**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 Phantom offer customers an integrated, unified, and cohesive threat defense lifecycle. Phantom, 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 Phantom App Integration**

**McAfee ePolicy Orchestrator (McAfee ePO) and Phantom**
The McAfee ePO App for Phantom allows customers to execute endpoint-based investigative and containment actions using the McAfee ePO platform from the Phantom Platform. 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 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 Phantom**
The McAfee Advanced Threat Defense App for Phantom allows customers to programmatically submit executables to McAfee Advanced Threat Defense for analysis. The Phantom Platform 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 Phantom**
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 the Phantom Platform.
McAfee Threat Intelligence Exchange and Phantom

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

About Phantom

The Phantom Platform automates and orchestrates key stages of security operations, from prevention to triage and resolution, delivering dramatic increases in productivity and effectiveness. Ranging from simple automation to fully autonomous response, Phantom lets you choose the best balance that fits your organization’s needs while increasing security and accelerating security operations. Focused on closing the security skills gap by enabling enterprise security operations to work smarter, respond faster, and strengthen their defenses, Phantom provides the flexibility to connect in-house and third-party systems into one open, integrated, and extensible platform.

About McAfee

McAfee is one of the world’s leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the 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