FORTINET AND PHANTOM INTEGRATED SECURITY SOLUTION

Advanced Security Automation and Orchestration

Cybersecurity threats are increasing in diversity, complexity and sophistication from hacktivists, cyber criminals and nation states. For many organizations, the mobility and cloud revolutions have greatly increased the complexity of security their infrastructure, applications, users and services. Facing an expanding attack surface, enterprises are looking for ways to significantly reduce risk, as well as detect and respond to cybersecurity threats quickly and effectively.

Most Security Operations Center (SOC) teams would agree that one of the largest security risks comes from their limited capacity to investigate and respond to the security alerts they receive. An unknown amount of risk lies in uninvestigated alerts. The impact of a successful attack can be significant; customers may be lost, revenue may be impacted, and the organization could experience immeasurable brand damage.

Security Automation and Orchestration (SA&O) platforms act as a force multiplier for resource-constrained security teams. They allow teams to automate time-consuming investigations and even automatically remediate well-known threats where the team has an established Standard Operating Procedure (SOP). This allows the team to dramatically scale their capacity and reduce the amount of uninvestigated and unresolved alerts, thereby reducing the organization's security risk exposure in the process.

SA&O platforms can also reduce the time to containment and remediation. Whether the platform is operating without an analyst approving security actions (e.g. out-of-the-loop or on-the-loop supervision) or with analysts reviewing security actions before they are performed (e.g. in-the-loop supervision), speed is gained in all cases—resulting in reduced risk.

As the leader in SA&O, Phantom has partnered with Fortinet to deliver a joint, robust and integrated solution that allows for seamless automation and orchestration of security operations activities, from prevention to triage and resolution, while delivering dramatic increases in productivity and effectiveness.

SOLUTION DESCRIPTION

Phantom automates and streamlines enterprise security operations. It addresses problematic security trends: dramatic increases in attack volume, severe shortages in qualified personnel, growing complexity of IT security environments, and investors and regulators holding management to task for breaches. The platform arms teams with the automation, orchestration, event and case management, collaboration, and reporting capabilities that ready them to defend their company's business.

Phantom ingests and operates on high-fidelity security data in real time from a wide variety of sources, providing unprecedented security operational efficiency. It helps teams triage, investigate, decide, and act on events and cases across the threat lifecycle. The platform automates execution of security actions while orchestrating response plans across infrastructure and people.

SOLUTION BENEFITS

- Integrate systems and technologies easily, providing a layer of connective tissue between them.
- Reduce Mean-time-to-Resolution (MTTR) with automated response to threats.
- Lower overhead costs while reallocating SOC personnel to more productive and rewarding tasks.
- Leverage the most-validated security protection offered by Fortinet's award-winning FortiGate network security platform.
- Leverage Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

FORTINET
Fabric-Ready

Phantom-Fortinet integration is accomplished through the Fortinet FortiGate App for Phantom. The award-winning Fortinet FortiGate network security platform provides high performance, layered security services and granular visibility for an end to end protection across the entire enterprise network. Innovative security processor (SPU) technology delivers high-performance application layer security services (NGFW, SSL inspection, and threat protection), coupled with the industry's fastest SSL inspection engine to help protect against malware hiding in SSL/TLS encrypted traffic. The FortiGate enterprise firewall platform also leverages global threat intelligence to protect individual customers, by using Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

The Phantom and Fortinet integrated security solution combines advanced security automation and orchestration capabilities from Phantom with the industry-leading security protection from Fortinet to deliver security without compromise.

ABOUT PHANTOM

Phantom is the leading Security Operations Platform. It integrates your team, processes, and tools together. Work smarter, respond faster, and strengthen your defenses with Phantom. Learn more at www.phantom.us

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

February 22, 2018 10:59 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:SB-Fortinet-Phantom:sb-fortinet-phantom