Joint Solution Brief

Accelerate Threat Detection and Response

The Challenge

Defending the modern corporate network is a complicated task. Security practitioners usually use a variety of tools and information sources to spot potential malicious threats, evaluate the intent of each suspicious event and then act to mitigate their impact. This is a complex and time-consuming process requiring skilled staff that are increasingly in short demand.

Integrated Solution

The Phantom security automation and orchestration platform is designed to maximize the efficiency of your security staff by automating the tasks they repeat on a frequent basis. The Gigamon Application for Phantom uses the GigaSECURE® Security Delivery Platform to automate workflows orchestrated by Phantom, both for gathering relevant data from the network and for enforcing traffic management and blocking decisions.

Joint Solution Benefits

- Increase the efficiency of your security analysts by automating predictable tasks through customizable playbooks.
- Accelerate and automate threat identification and mitigation.
- Extend the capability and value of existing security architectures using these joint solutions, including third-party products that also have Phantom applications.
- Reduce training requirements by automating required actions on the GigaSECURE® Security Delivery Platform and other connected security technologies.

Introduction

Today's security operations teams face growing challenges in combating potential threats and data breaches. They face ever-increasing speed of network data, combined with the vast number of attackers and resources available to breach traditional network defenses and have insufficient time for threat inspection. Network protection is also hampered by the sheer number and variety of security tools that a security analyst needs to identify and resolve an incident.

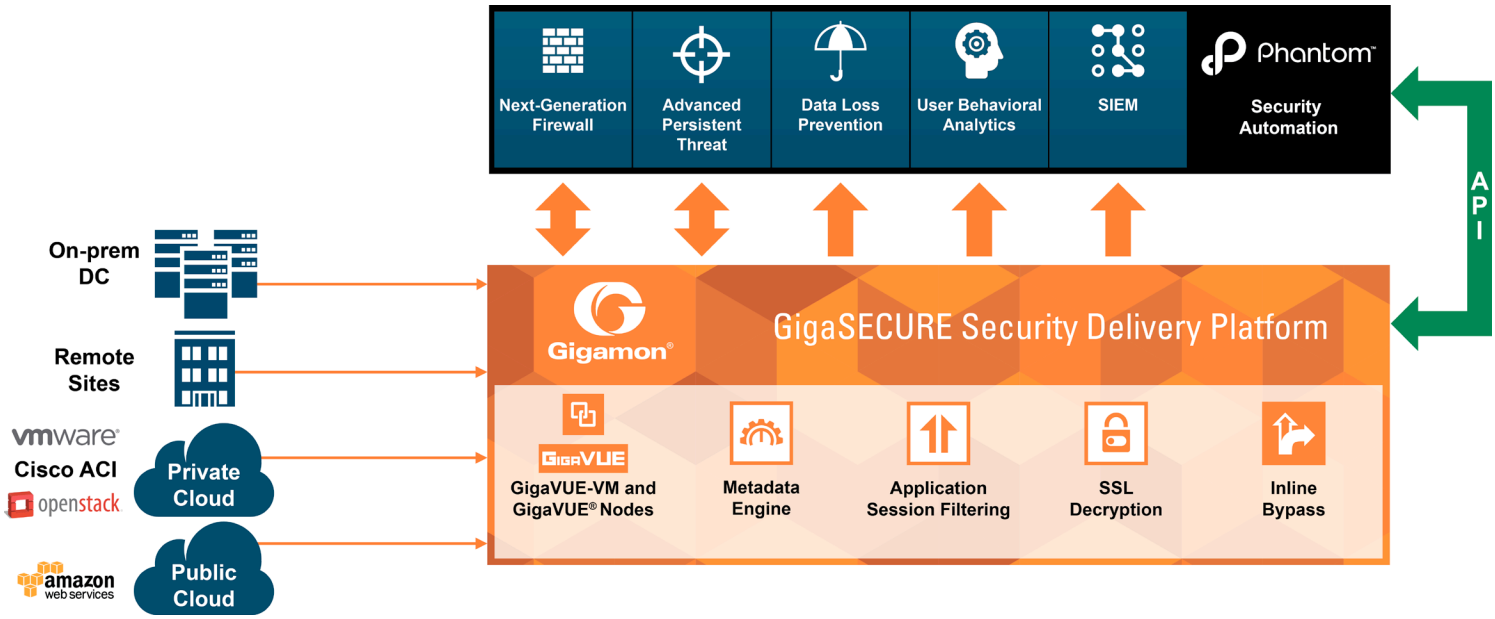
Finding a way to automate predictable tasks is paramount to accelerate and maximize the impact each security analyst can have. Gathering explicit data specifically selected to identify known risks can help give the advantage to the defending security operations team. Collecting contextual data and making it available to a chosen tool at the appropriate time of investigation automatically also helps, as does isolating devices on the network from sending or receiving suspect traffic.

The Gigamon and Phantom Joint Solution

Phantom automates and orchestrates key stages of security operations from prevention to triage and resolution, delivering a dramatic increase in productivity and effectiveness by automating predictable workflows, from simple automation to fully autonomous responses.

The Gigamon App for Phantom allows enterprises to automate and orchestrate security operations and management tasks in support of the Gigamon Defender Lifecycle Model. Automating steps in and between the Detection, Prediction and Containment phases of the model accelerate threat detection and remediation as well as increasing the efficiency of the security analysts involved. Utilizing the Gigamon REST API to integrate with the Phantom solution, the GigaSECURE® Security Delivery Platform can be configured to collect critical network data and send it to an analytics solution. Alerts from that analysis can trigger actions such as collecting additional contextual information to send to another security or monitoring tool, copying a flow of traffic to a recorder for later analysis, or blocking traffic on the network to or from a suspect device.

Playbooks, which record the desired workflow for consistent, accurate, automated execution, can be developed by the security operator or customized from those provided by vendors such as Gigamon and Phantom or from the Phantom community. Many Gigamon ecosystem partners already provide Phantom applications, integrating their technology with the playbooks, with new applications being frequently released.



The current version of the Gigamon App for Phantom supports the following key actions:

- Post Rule
- Delete Rule
- Get Map
- Get Maps
- Test Connectivity

With these actions, users can build a wide variety of automated workflows. Gigamon will be adding to these rules in later versions of the application.

Learn More

For more information on the Phantom and Gigamon solution, contact:

Phantom®
www.phantom.us

Gigamon®
www.gigamon.com

3248-01 10/17