Solution brief

Vectra Active Enforcement for the Splunk Phantom security automation and orchestration platform

KEY BENEFITS

- Reduce the time spent on cybersecurity threat investigations
- Quickly identify and block advanced cyber attacks and quarantine compromised host devices
- Improve security analyst productivity using simple event tags to automate response actions
- Selectively trigger response actions based on threat type, risk and certainty
- Combine automated behavior-based threat analysis with real-time enforcement

The solution

There is a need to close the cybersecurity skills gap facing enterprise security operations teams. The Vectra Active Enforcement application for Splunk Phantom enables security teams to quickly expose a variety of hidden cyber attack behaviors, pinpoint host devices at the center of an attack, and block threats before data is damaged or lost.

Vectra technology and product

The Cognito™ threat detection and response platform from Vectra® provides the fastest, most efficient way to find and stop hidden cyber attackers inside your network. Vectra automates the manual, time-consuming tasks associated with a Tier-1 analyst’s role by delivering real-time attack visibility and putting attack details at your fingertips to empower immediate action.

Uniquely combining data science, modern machine learning techniques and behavioral analysis based on artificial intelligence, Cognito performs non-stop, automated threat hunting to quickly and efficiently find hidden and unknown attackers before they do damage.

Cognito also delivers blind-spot-free threat detection by directly analyzing all network traffic to gain high-fidelity visibility into the actions of all host devices – including IoT and BYOD – from campus to data center to cloud, leaving attackers with nowhere to hide.

Splunk Phantom technology and product

The Splunk Phantom security automation and orchestration platform is the force multiplier you need to marshal the full power of your security investment. The Splunk Phantom platform allows you to automatically respond to known threats using your documented processes and workflows.

For more complex incidents that require human analysis, Splunk Phantom allows you to automatically unify incident details with the key threat intelligence you need to speed-up decision making.

Once a course of action is determined, the Splunk Phantom platform can resume orchestration, executing prescribed actions across your infrastructure at machine speed.

The Splunk Phantom automation and orchestration platform seamlessly integrates your existing security technologies. The platform executes digital playbooks to achieve results in seconds that may normally take minutes or hours to accomplish. It also ensures that your process is repeated the same way, every time.

Vectra Active Enforcement for Splunk Phantom

With Cognito, automation plays a pivotal role. Cognito automatically pinpoints physical host devices at the center of an attack, and tracks and scores threats in context over the full duration of the attack.

The Vectra Threat Certainty Index™ displays alerts with threat and certainty scores so security teams instantly know which host devices with attack indicators pose the biggest risk with the highest degree of confidence.

The Vectra Active Enforcement application for Splunk Phantom automates the response phase by enabling quick and effective enforcement action by perimeter and endpoint security or network access control (NAC) solutions.

The success or failure of security teams often depends on the speed of incident response. Sophisticated attackers thrive by staying under the radar, and detecting them often requires hours to days of manual threat hunting by highly trained security analysts.

On average, it takes 99 days between the time a network is compromised and the time the attack is detected, according to the M-Trends 2017 report from Mandiant Consulting. In addition, 67% of data breaches are discovered by a third-party, such as a law enforcement agency.

Vectra Active Enforcement directly addresses this challenge. First, it automates the tedious, manual threat hunting performed by Tier-1 security analysts and consolidates vast amounts of Cognito threat data into simple, actionable answers that save time, effort and money.

This automation offers two benefits – security analysts can stop active attacks before damage is done and general IT staff can address more threat investigations. Vectra customers have reported 75-90% reductions in time spent on threat investigations.

Vectra Active Enforcement for Splunk Phantom turns Cognito threat detections into action by integrating with other leading security solutions to stop attacker traffic and quarantine compromised host devices. Flexible enforcement actions allow security teams to extend response capabilities to firewall, endpoint and NAC solutions in a layered environment.

Workflow responses

Responses can be triggered in a variety of ways to initiate and streamline operational workflows. Splunk Phantom can receive an alert based on risk of a host or type of detection from Cognito and respond appropriately as defined by a Splunk Phantom playbook. Analysts can also trigger a response from the Cognito UI by using predefined event tags.

In addition, a response can be fully automated based on the type of threat, as well as threat and certainty scores of specific host devices, including PCI in-scope hosts and hosts with personally identifiable information (PII) or protected health information (PHI). By automating threat hunting, analysis and response, security teams can condense weeks of work into seconds and take action before damage is done.

Use case: Streamlined and efficient enforcement workflow

Challenge: When it comes to hunting-down and responding to network cyber attacks, even a highly qualified team of security analysts can be overburdened by manual, inefficient processes.

Solution: Vectra Active Enforcement for Splunk Phantom makes the best use of time and talent, while empowering IT and security generalists to have a positive impact on the security of the network. It allows host devices to be selected for enforcement action using the following methods:

- Host devices manually tagged in the Cognito UI after review by a security analyst
- Based on host device threat and certainty scores (automated)
- Based on detection type observed on a host device (automated)
- This level of automation empowers staff to find and resolve issues quickly, while conserving time, money and talent.

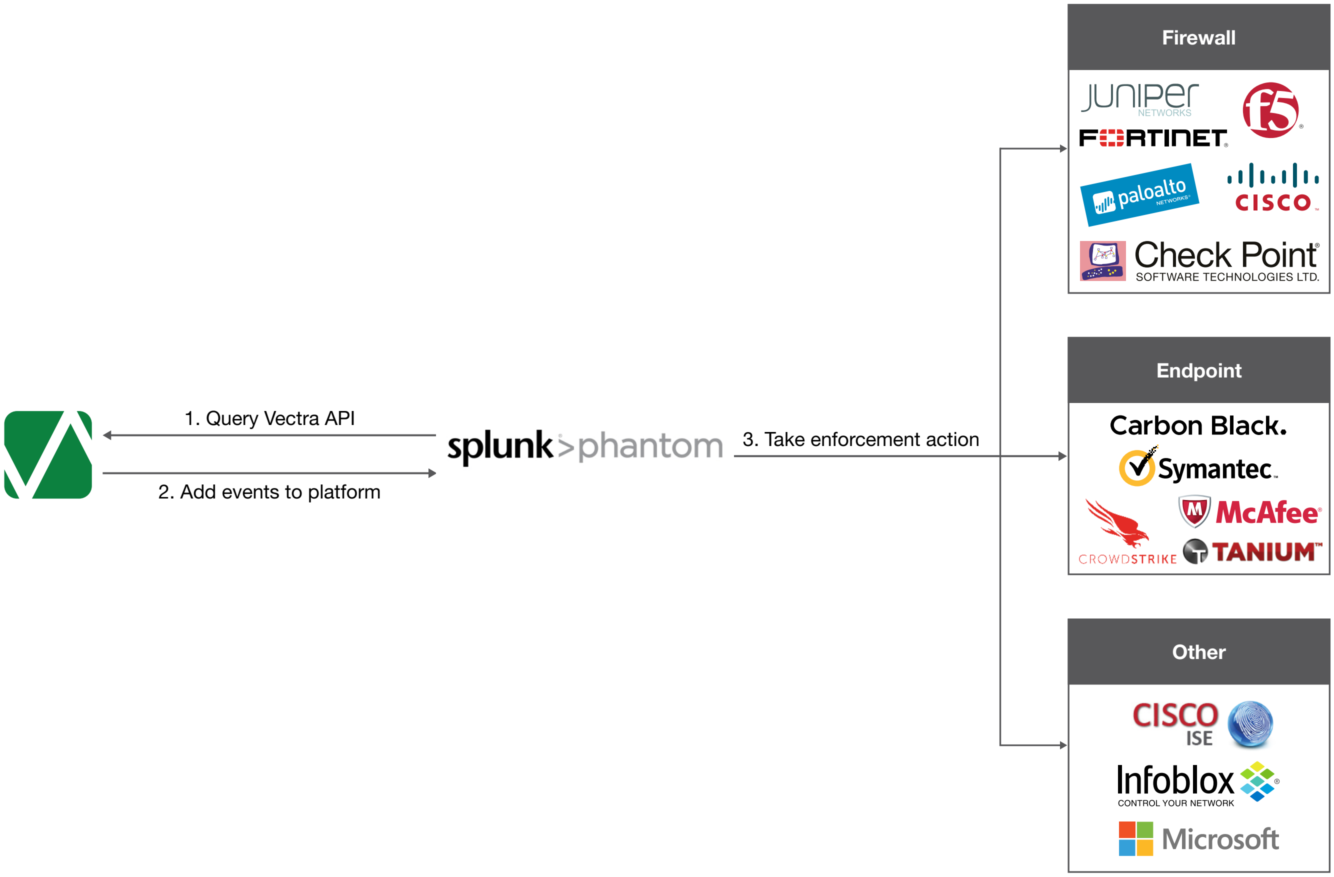
Use case: Make existing security tools smarter

Challenge: Organizations have large sets of tools that lack understanding of the risk level of a threat or context to the organization, and thus cannot be used in isolation to respond to a cyber attack.

Solution: Cognito automatically scores the detections for each affected host device in terms of threat to the organization and the certainty of the attack. Analysts can use these threat and certainty scores to drive dynamic response rules that align to the risk profile of any organization.

Vectra Active Enforcement provides flexible enforcement actions for a wide range of leading security controls, including:

- Block outward communication from a host to the internet via a firewall
- Kill a suspect process or quarantine a suspect host with endpoint technology
- Trigger granular policy with NACs to limit communications that the IP address can engage with across the network



Vectra Active Enforcement integrates with other leading security controls to stop malicious traffic or quarantine a compromised host device

Enable additional use cases

In addition to Vectra Active Enforcement for Splunk Phantom, the Vectra and Splunk Phantom solution can be leveraged for additional uses.

Threat context and host correlation data from Cognito can enrich the context of your entire security infrastructure and enable rapid investigation. This contextual enrichment of threats between an array of security tools can be automated to the degree of choice with Splunk Phantom playbooks, eliminating the need for manual data search between platforms.

The joint solution also enables users of ticketing systems to receive context automatically, investigate incidents faster and take decisive action in less time.

About Vectra

Vectra® is an artificial intelligence company that is transforming cybersecurity. Its Cognito™ platform is the fastest, most efficient way to detect and respond to cyberattacks, reducing security operations workload by 168X. Cognito performs real-time attack hunting by analyzing rich metadata from network traffic, relevant logs and cloud events to detect attacker behaviors within all cloud and data center workloads, and user and IoT devices. Cognito correlates threats, prioritizes hosts based on risk and provides rich context to empower response. Cognito integrates with endpoint, NAC, firewall security to automate containment, and provides a clear starting point for searches within SIEM and forensic tools.

About Splunk Phantom

Splunk Phantom 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, Splunk Phantom lets you choose the best balance that fits your organization's needs while increasing security and accelerating security operations. Splunk Phantom provides the flexibility to connect in-house and third-party systems into one open, integrated and extensible platform. For more information, visit Splunk Phantom.

VECTRA®
Security that thinks.®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai