Solution brief

VECTRA®

DEMISTO

A PALO ALTO NETWORKS® COMPANY

Vectra Active Enforcement for the Demisto security automation and orchestration platform

KEY BENEFITS

- Collaborative cybersecurity ensures faster, more efficient threat investigations
- Improves investigative efficiency by automating data enrichment and analysis
- Selectively triggers response actions based on threat type, risk and certainty
- Combines 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 Demisto 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 compromised or stolen.

Vectra technology and product

The Cognito™ automated threat detection and response platform from Vectra® provides the fastest, most efficient way to detect and stop attackers in your network.

Cognito automates the manual, time-consuming tasks associated with a Tier 1 analyst's role by providing real-time attack visibility, prioritizing the highest-risk threats and putting contextual 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 – from the cloud and data center workloads to user and IoT devices – leaving attackers with nowhere to hide.

Demisto technology and product

Demisto Enterprise helps security operations centers scale their resources, improve incident response times, and capture evidentiary support while working and solving problems the way humans are wired.

Demisto Enterprise is the first comprehensive security operations platform to combine intelligent automation with collaborative, human social learning and experience.

Demisto's intelligent automation is provided by DBot, which works with your team via a new concept, Security ChatOps, for fully automated, playbook-based workflows, cross-correlation, information sharing and curation from investigation through response and beyond.

Use case: Vectra Active Enforcement for Demisto

With Cognito, automation plays a pivotal role. It 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.

Vectra Active Enforcement for Demisto automates the response phase by enabling quick and effective enforcement action by perimeter and endpoint security solutions.

Challenge: The success or failure of security teams often boils down to 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.

Solution: Vectra Active Enforcement directly addresses this challenge. First, Cognito automates the tedious, manual threat hunting performed by Tier 1 security analysts and consolidates vast amounts of threat data down to 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 seamless and quick investigation workflows are enabled through integration with ticketing systems and war-room capabilities. Vectra customers have reported 75-90% reductions in time spent on threat investigations.

Vectra Active Enforcement for Demisto turns Cognito threat detections into action by integrating with other leading security solutions to stop attacker traffic or quarantine compromised host devices. Collaboration and forensics investigative capabilities provide efficiency and advanced investigation features by automating data enrichment and analysis with Demisto automation scripts.

Workflow responses

Responses can be triggered in a variety of ways to initiate and streamline operational workflows. Demisto can receive an alert from Vectra and respond appropriately as defined by a default or custom Demisto playbook. Analysts can also trigger a response by kicking-off a Demisto playbook from the Cognito UI 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.

Investigate and collaborate with Demisto Security ChatOps:

- Collaborate and take notes in context of investigations to expand insights and simplify handoffs
- DBot automatically detects duplicate incidents to reduce redundant work based on data in the virtual war room
- Issue data enrichment ChatOps commands and response tasks to DBot from within the virtual war room
- Delegate to and mentor junior analysts via collaborative chat rooms

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

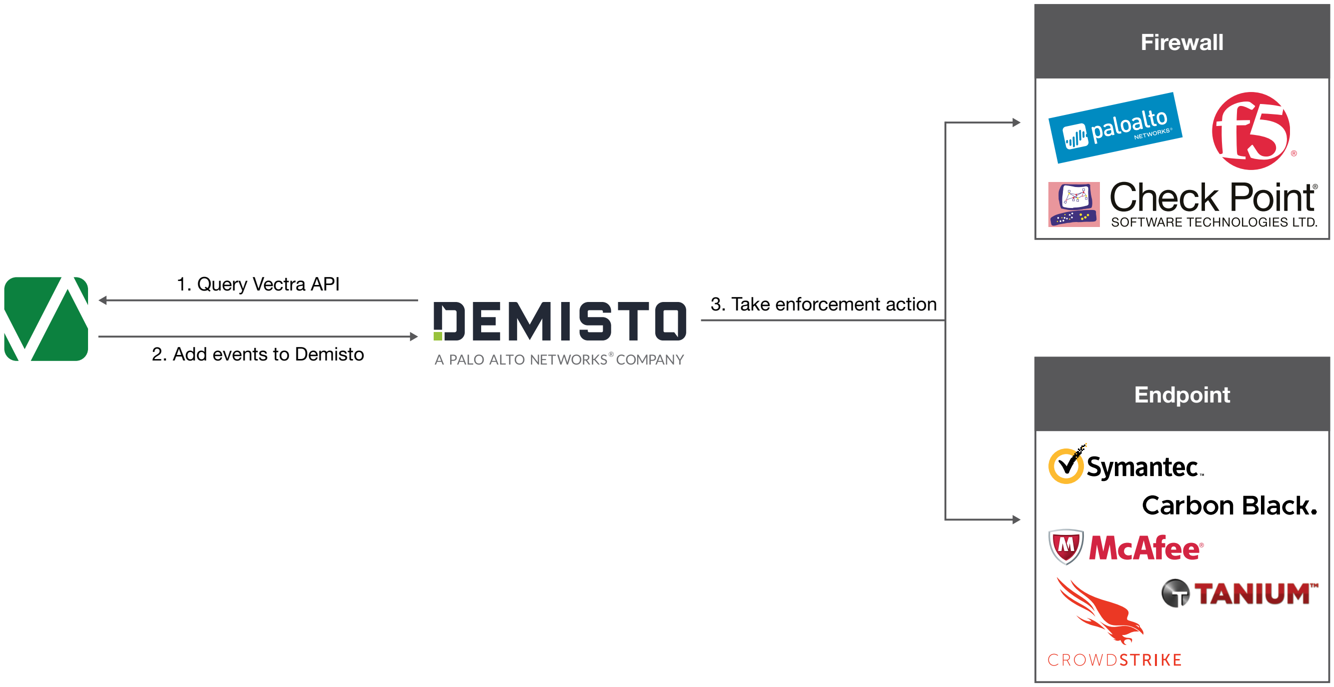
- Block a host device at a firewall
  - Palo Alto Networks
  - Checkpoint
  - F5
- Isolate or quarantine a host device using advanced endpoint solutions
  - Carbon Black
  - Crowdstrike
  - McAfee
  - Symantec
- Kill a malicious process using advanced endpoint solutions
  - Carbon Black
  - Tanium
  - Crowdstrike

Use case: Investigation efficiency using contextually enriched security infrastructure data

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. In a real world environment, these analysts need to be in constant communication.

Solution: Vectra Active Enforcement for Demisto makes the best use of time and talent, while empowering IT and security generalists with advanced analytics for complex investigations and collaboration.

Cognito provides prioritized host scoring to drive investigations in which analysts using Demisto can run interactive queries on Vectra S-series sensors, bringing rich data to the virtual war room. This level of automation empowers staff to find and resolve issues quickly while conserving time, money and talent.



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

Use case: Rapid enforcement workflow across layered security products

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

Solution: Cognito automatically scores threat detections for each affected host device in terms of risk 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.

Additional use cases

- Investigation efficiency through contextual enrichment of data from the security infrastructure.
- Seamless and quick investigation workflows enabled through integration with ticketing systems.

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 Demisto

Demisto helps Security Operations Centers scale their human resources, improve incident response times, and capture evidence while working to solve problems collaboratively. Demisto Enterprise is the first comprehensive, bot-powered Security ChatOps platform to combine intelligent automation with collaboration. Demisto's intelligent automation is powered by DBot which works with teams to automate playbooks, correlate artifacts, enable information sharing and auto document the entire incident lifecycle. Demisto is backed by Accel and has offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.

VECTRA®
Security that thinks®

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