SOLUTION BRIEF

Vectra and Palo Alto Networks: Stopping threats with network-based behavioral analytics

As the rate and sophistication of cyberattacks increase, security teams are increasingly pressed to turn cutting-edge security analytics into action. The integration between Vectra® and Palo Alto Networks enables security staff to quickly expose a variety of hidden attacker behaviors, pinpoint the specific hosts at the center of a cyberattack, and block the threat before data is lost.

Vectra technology and product

The Cognito® network threat detection and response platform provides the fastest, most efficient way to find and stop attackers once they are inside a network. Cognito delivers real-time attack visibility and puts attack details at your fingertips to empower immediate action.

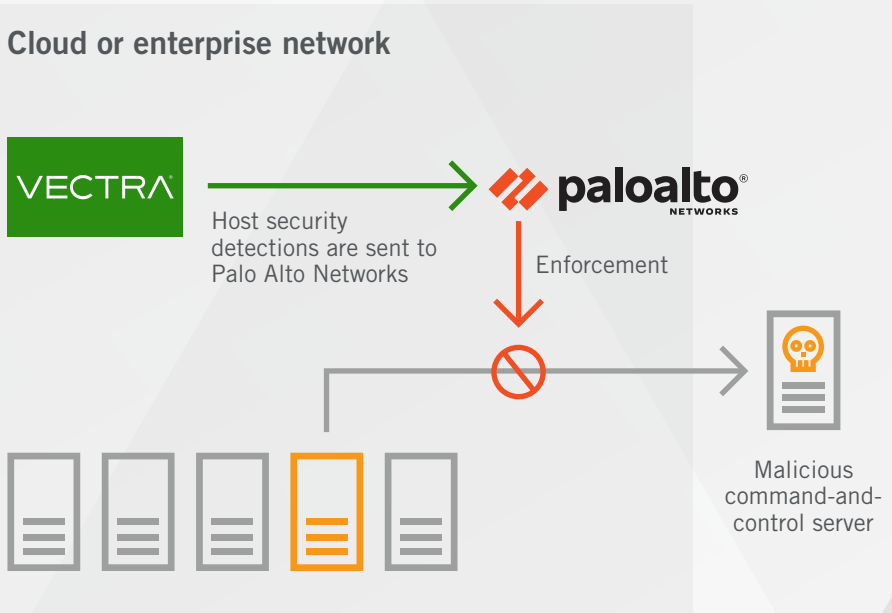
Leveraging artificial intelligence, Cognito performs non-stop, automated threat hunting with always-learning behavioral models to quickly and efficiently find hidden and unknown attackers before they do damage.

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

The integration between Vectra and Palo Alto Networks enables security staff to quickly expose a variety of hidden attacker behaviors.

KEY BENEFITS

- Automate network defenses by combining behavior-based threat detection with real-time enforcement.
- Identify and block advanced attacker behaviors and quarantine compromised hosts.
- Empower security analysts to respond to threats by triggering blocking actions using simple event tags.
- Trigger blocking actions based on type of threat, risk, and certainty. Stopping threats with network-based behavioral analytics



Vectra and Palo Alto Networks

The Palo Alto Networks and Vectra partnership aligns behavioral threat detection and realtime enforcement between the two companies in real time, providing our joint customers with increased visibility and synchronized protection to effectively combat today's advanced threats.

> Joint customers can rapidly integrate Palo Alto Networks with Cognito in a matter of minutes with Vectra Active Enforcement.

Success or failure of a security team can often boil down to time-to-response. Sophisticated attackers thrive by staying under the radar, and detecting them can often require hours to days of investigation from highly trained security analysts. According to the M-Trends 2017 report from Mandiant Consulting, it takes 99 days between when a network is compromised and when the attack is detected.

The integration between Cognito and Palo Alto Networks directly addresses this challenge. First, Cognito automates the work of Tier-1 security analysts to find hidden signs of an attack. Vectra Active Enforcement turns this detected threat into action by integrating with Palo Alto Networks dynamic block lists to stop the malicious traffic or quarantine a compromised host. Support for Panorama allows staff to extend blocking to any Palo Alto Networks firewall in a distributed environment.

Vectra turns detected threat into action by integrating with Palo Alto Networks dynamic block lists to stop the malicious traffic.

Blocking can be triggered in a variety of ways to support any operational workflow. Analysts can trigger blocks from the Cognito user interface through the use of predefined event tags. Alternatively, blocks can be fully automated based on the type of threat, as well as threat and certainty scores of specific hosts (e.g., PCI in-scope hosts, host with PHI). By automating analysis and response, security teams can condense weeks of work into seconds and take action before damage is done.

USE CASE: Empowering analysts to stop attacks

CHALLENGE

Finding and retaining qualified security staff is a challenge for most organizations, and even in the best of cases, most networks generate more security alerts than staff have the time to analyze.

SOLUTION

The combination of Cognito threat detection and response with Palo Alto Networks enforcement 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.

Cognito users can quickly pinpoint the hosts at the center of an active attack, rapidly verify the detection with on-demand forensics, and trigger a dynamic block of the affected device – all from within the Cognito user interface. This level of automation empowers staff to find and resolve issues quickly, while preserving time, money and talent.

USE CASE: Automated blocking based on threat and certainty

CHALLENGE

Many behavioral analysis solutions simply flag anomalies, which require more extensive analysis to determine an appropriate response. This leads to a very familiar bottleneck of human analysis, which leads to delayed responses and ultimately the loss of data.

SOLUTION

In addition to automating the hunt for threats, Cognito automatically scores each detection and each affected host in terms of threat to the network and the certainty of the attack.

These scores retain context over time, and correlate the progression of an attack across multiple phases of attack. Staff can use these threat and certainty scores of detections and hosts to drive dynamic blocking rules that align to the risk profile of any organization.

By automating analysis and response, security teams can condense weeks of work into seconds and take action before damage is done.

For more information please contact a service representative at sales-inquiries@vectra.ai.

About Vectra

Vectra® is transforming cybersecurity by applying advanced AI to detect in-progress attacks and hunt for hidden threats. Vectra and its flagship Cognito® platform enable the world's most consequential organizations to detect cyberattacks in real time and empower threat hunters to perform highly conclusive incident investigations. Vectra reduces business risk by eliminating security gaps in cloud, data center and enterprise environments. Behind the Cognito platform, Vectra threat researchers identify and investigate cyberattacks, vulnerabilities and malicious behaviors that are unknown to the world. With data sets from this research, data scientists develop the machine learning algorithms and behavioral analysis that drive Cognito.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Email info@vectra.ai vectra.ai