VECTRA®

Vectra and Palo Alto Networks

Stopping threats with network-based behavioral analytics

paloalto NETWORKS®

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.

The challenge

As the rate and sophistication of cyber attacks 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 cyber attack, and block the threat before data is lost.

Vectra technology and product

The Cognito™ automated 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.

Vectra and Palo Alto Networks

The Palo Alto Networks and Vectra partnership aligns behavioral threat detection and real-time 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.

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.

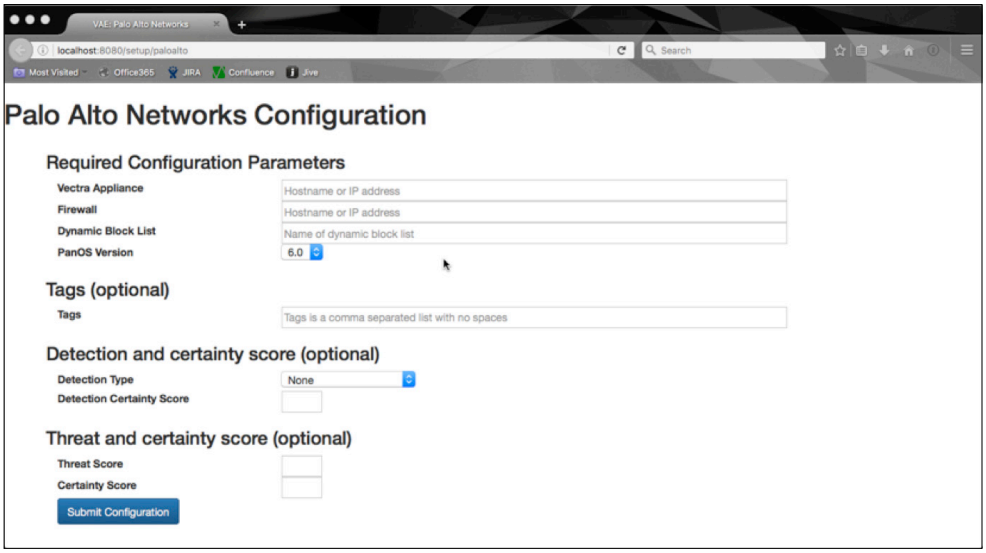
Staff can use these threat and certainty scores of detections and hosts to drive dynamic blocking rules that align to the risk profile of any organization.

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 Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com



VECTRA®
Security that thinks®

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