

# PALO ALTO NETWORKS VECTRA NETWORKS

## Stopping Threats With Network-Based Behavioral Analytics

### 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

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 Networks® 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 Networks Advanced Threat Defense

Vectra Networks delivers a new class of advanced threat defense that delivers real-time detection and analysis of active network intrusions. Vectra technology provides deep, continuous analysis of both internal and Internet-facing network traffic to automatically detect all phases of a breach as attackers attempt to spy, spread, and steal within your network.

Vectra directly analyzes network traffic in real time using a patent-pending combination of data science, machine learning, and behavioral analysis to detect attacker behaviors and user anomalies in the network. All detections are correlated and prioritized to show an attack in context, and Vectra Networks' machine learning adapts as attacks evolve.

### Palo Alto Networks & Vectra Networks

The partnership between Palo Alto Networks and Vectra Networks aligns behavioral threat detection with real-time enforcement, 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 Vectra Networks in a matter of minutes with Vectra Active Enforcement (VAE).

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 days to months of investigation from highly trained security analysts.

The integration between Vectra Networks and Palo Alto Networks directly addresses this challenge. First, Vectra automates the work of data scientists and security analysts to find hidden signs of an attack. Vectra Active Enforcement (VAE) 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™ network security management 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 Vectra 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. By automating analysis and response, security teams can condense weeks of work into seconds and take action before damage is done.

## USE CASE #1

### *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 alerts than staff have time to analyze.

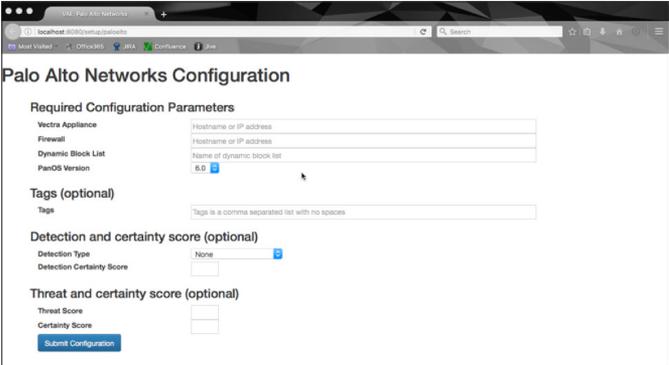
**Solution:** The combination of Vectra Networks automated analysis with Palo Alto Networks enforcement makes the best use of time and talent, while empowering IT and security generalists to have a positive impact on the security of the network. Vectra users can quickly pinpoint the hosts at the center of an active attack, quickly verify the detection with on-demand forensics, and trigger a dynamic block of the affected device – all from within the Vectra Networks user interface. This level of automation empowers staff to find and resolve issues quickly, while preserving time, money and talent.

## USE CASE #2

### *Automated Blocking Based on Threat and Certainty*

**Challenge:** Many behavioral analysis solutions simply flag anomalies, which require 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 automatically detecting threats, Vectra automatically scores each detection, and each affected host, in terms of threat to the network and the certainty of the attack. These scores retain content over time and correlate the progression of an attack across multiple phases of the 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.



The screenshot shows a web browser window displaying the 'Palo Alto Networks Configuration' page. The page is divided into several sections: 'Required Configuration Parameters' with fields for 'Vectra Appliance', 'Firewall', 'Dynamic Block List', and 'PanOS Version'; 'Tags (optional)' with a 'Tags' field; 'Detection and certainty score (optional)' with 'Detection Type' and 'Detection Certainty Score' fields; and 'Threat and certainty score (optional)' with 'Threat Score' and 'Certainty Score' fields. A 'Submit Configuration' button is located at the bottom left of the form.

## About Vectra Networks

Vectra Networks is the leader in real-time detection of active cyber attacks. Our Automated Threat Management solution continuously monitors internal traffic to pinpoint cyber attacks inside networks as they happen. Vectra prioritizes attacks that pose the greatest business risk so organizations can quickly prevent or prevent data loss.

## 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](http://www.paloaltonetworks.com)



4401 Great America Parkway  
Santa Clara, CA 95054

Main: +1.408.753.4000

Sales: +1.866.320.4788

Support: +1.866.898.9087

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2016 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <http://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. vectra-networks-tpsb-100616