PALO ALTO NETWORKS AND SAVVIUS

Technology Segment: Network Monitoring and Analytics

Network packets are critical to security investigations, however most organizations lack the network packets needed to investigate security incidents since they only keep packets for days or weeks, and it can take months for breaches to be detected. Savvius Vigil automates the collection of network traffic needed for security investigations, captures the critical packets that led up to the alert, and can save that data for months.

Highlights

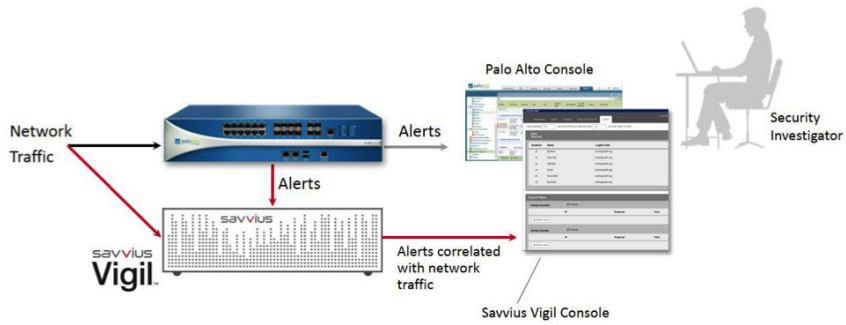
- Investigate security alerts as they happen, or even months later
- Capture security alerts from Palo Alto Networks Next-Generation Firewall and review only network traffic associated with these security alerts
- Reduce TCO with this integration

Palo Alto Networks Security Platform

By classifying and judging all traffic based on application, user and content, Palo Alto Networks® Next-Generation Security Platform provides the ability to isolate unique and targeted attacks with context and analysis to help security staff prioritize efforts and operate more efficiently. The integrated platform also reprograms itself automatically upon the detection of an unknown attack, creating and disseminating protection mechanisms, a process that does not rely on manual intervention. Our platform can reduce complexity by consolidating investments in multiple products, which can lead to higher usability while lowering capital and operational expenses.

Palo Alto Networks and Savvius Vigil

Savvius Vigil integrates with Palo Alto Networks Next-Generation Firewall via syslog. When an alert is triggered by the firewall, the Savvius Vigil appliance captures the specific network traffic that caused the alert. Savvius Vigil continuously collects all network packets, receives security alerts generated by Palo Alto Networks PAN-OS® and only stores traffic associated with Palo Alto Networks security alerts, discarding unassociated packets. Savvius Vigil stores network traffic data from five minutes before through five minutes after the alert triggered.



Investigating the alert simply requires downloading the network packet file for analysis with Savvius Omnipeek network visibility and performance diagnostics software or any other network forensics solution.

Use Case

How timely and efficiently you can respond to a breach or security alert can determine the length of time a breach is in your networks. Investigating those security alerts identified by Palo Alto Networks Firewall requires access to the network packets. These packets can be difficult to access due to the limited storage time that network traffic is stored. The Savvius Vigil appliance can store months of network traffic feeds, enabling you to investigate these breaches and review only network traffic aligned to security alerts identified by Palo Alto Networks PAN-OS.

This integration was showcased at ShowNet Interop Tokyo in 2016, where Savvius Vigil received an average of more than 300,000 events per day. Savvius Vigil was able to beat out almost 300 other vendors to receive a Best of Show award in the Network Management and Monitoring category. The full case study is available at http://events.savvius.com/shownet-case-study.

About Savvius

Savvius offers a range of powerful software and appliance products that automate the collection of critical network data for network forensics in security investigations and for network and application visibility and performance diagnostics. Savvius products are trusted by network and security professionals at over 6,000 companies in 60 countries around the world. Visit www.savvius.com for information about Savvius Omnipliance®, Savvius Omnipeek®, Savvius Vigil™, and Savvius Insight™, and to learn about Savvius technology and channel partners.

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.

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