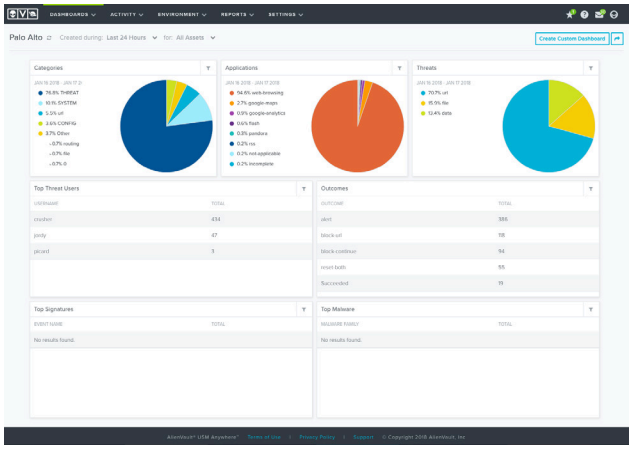
DATA SHEET

AlienVault® USM Anywhere™ and Palo Alto Networks Next-Generation Firewall

Closed-Loop Threat Detection and Response

The disconnected nature of today's security environment demands innovation. As threats continue to evolve, organizations acquire more and more point solutions to maintain their security and mitigate their risk. Unfortunately, these point solutions are typically disconnected from each other, delivering sub-optimal protection that requires additional management effort along with often complex inter-product orchestrations to be developed. This requires time, money, and resources that most organizations simply don't have.



Break through this "threat cycle" with AlienVault USM Anywhere and Palo Alto Networks Next-Generation Firewalls. Together, these solutions deliver closed-loop threat detection and response capabilities to effectively address the threat cycle and deliver the security outcomes your organization needs.

A Unified Approach to Enhanced Threat Detection & Response

The AlienVault USM Anywhere platform is built with an architecture that delivers modularity and extensibility through AlienApps. AlienApps are modular software components tightly integrated into the USM Anywhere platform that deliver technology quickly through the platform to extend, orchestrate, and automate functionality between the built-in security controls in USM Anywhere and the other tools that IT security teams need, including Palo Alto Networks Next-Generation Firewalls.

With the AlienApp for Palo Alto Networks, threats detected by USM Anywhere can be manually or automatically forwarded to the Palo Alto Network Next-Generation Firewall to block the threat, and protect the organization from further risk or harm.

Closed-Loop Detection of Threats

Through the AlienApp for Palo Alto Networks, USM Anywhere collects log data from the Palo Alto Networks Next-Generation Firewall. USM Anywhere performs threat analysis on this data, along with log and event data aggregated from other network, system, application, and devices.

Including log data from Palo Alto Network Next-Generation Firewall in its threat analysis allows USM Anywhere to deliver more comprehensive threat detection, enhancing threat visibility and reducing the mean time to detect threats.

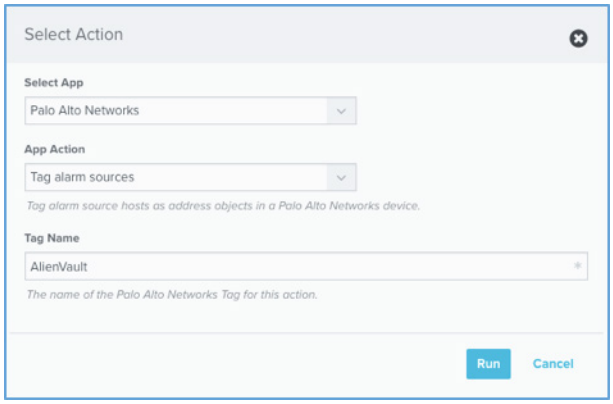
Orchestrated Threat Response

When AlienVault USM Anywhere detects a threat, customers can rapidly respond by tagging IP addresses of those detected threats and sending them to the Palo Alto Next-Generation Firewall through a manually or automatically-defined action. The Next-Generation Firewall will apply the policy that matches the tag to block or isolate traffic (depending on the policy) to those IP addresses determined as a threat.

By performing these actions directly within USM Anywhere, users avoid having to leverage multiple consoles and multiple security personnel to implement the response. This eliminates friction from the incident response process and accelerates the time to respond to threats.

How it Works

- USM Anywhere detects a network communication from or to a malicious IP address
- USM Anywhere, either through a user-executed action or automatically, tags the IP address of the malicious host or infected asset, and sends the tagged IP address to the Palo Alto Networks Next-Generation Firewall
- The Palo Alto Networks Next-Generation Firewall identifies the policy that matches the tag and applies that policy to the indicated IP address, resulting in traffic to or from that IP being blocked



Benefits of the Combined Solution

SAVE TIME & MONEY	REDUCE TIME TO DETECTION & RESPONSE
• Enable focus on threat response and not writing complex security analytics rules	• Automate policy enforcement between USM Anywhere and Palo Alto Networks Next-Generation Firewall for rapid response
• Reduce the time and expense of integrating and managing multiple point security solutions	• Enhance threat visibility and analysis, reducing the mean time to detection of incidents
• Increase the performance of your existing security solutions to minimize the need to procure new point products for new threats	• Eliminate friction in the incident response process, accelerating the time to respond to threats

About AlienVault

AlienVault's award-winning products are designed and priced to ensure that all organizations have access to world-class security. By integrating essential security capabilities into a Unified Security Management™ (USM™) platform, and then powering that platform with up-to-the-minute threat intelligence from AlienVault Labs and our Open Threat Exchange™ – the world's largest crowd-sourced collaborative threat exchange – AlienVault provides its more than 5,000 commercial customers with a unified, simple, and affordable solution that simplifies and centralizes threat detection, incident response, and compliance management for cloud, hybrid cloud, and on-premises environments

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.