Partner Data Sheet

paloalto NETWORKS

Industry

Firewall and Endpoint Threat Detection

Website

www.paloaltonetworks.com

Company Overview

As the next-generation security company, Palo Alto Networks is leading a new era in cybersecurity by safely enabling all applications and preventing advanced threats from achieving their objectives for tens of thousands of organizations around the world.

Product Overview

The Palo Alto Networks platform natively brings together all key security functions including firewall, URL filtering, IDS/IPS, and endpoint and **advanced threat protection.**

Solution Highlights

The Palo Alto Networks next-generation firewall is the only one that attempts to fully classify traffic (including user association), and then make all of that classification knowledge available to all control and enforcement options. It's an approach that allows for precise, flexible control of traffic based on: applications, users, and the information content of the traffic.

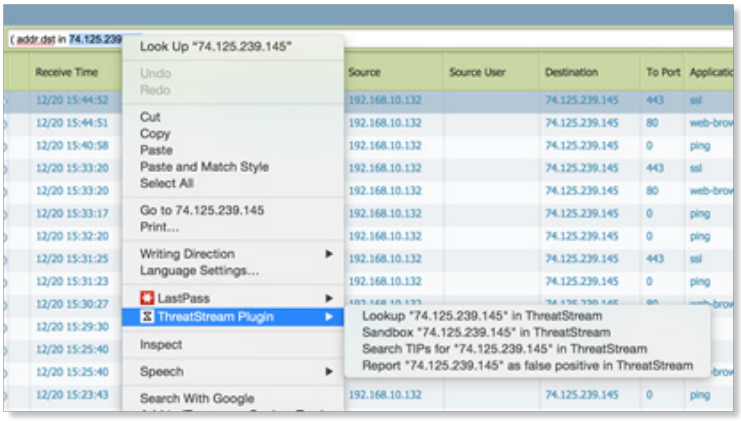
ANOMALI

Product Overview

The threat landscape is continually expanding and organizations are under continuous attack and overwhelmed with alerts. Thousands of incidents occur each day and security professionals only have time to deal with dozens. This creates operational chaos. Security teams need next-generation security solutions to help them respond faster, defend proactively and invest smarter.

Just-in-Time Intelligence

Threat intelligence is continuously gathered, categorized, risk ranked (for severity and confidence) in Anomali's ThreatStream platform and then delivered in real-time to your Palo Alto Networks instance for detection of security threats in your enterprise infrastructure for the security and threat intelligence teams to quickly see high priority threats to your business. Each of the selected IOCs for integration into your Palo Alto Networks instance enriched with factors such as risk score to add context and relevance to the delivered information



Benefits of the Joint Offering

The Anomali Palo Alto Networks integration is quick and easy. The Anomali API delivers threat intelligence from the ThreatStream platform via a web server that the Palo Alto Networks Dynamic Block List sources from. This list is comprised of the most malicious Indicators of Compromise (IOC's) based on the ThreatStream platform Retina process risk ranking analysis and an indicator type recognition.

Benefits of Anomali

- Easy-to-use interface to view threat information received through STIX/TAXII feeds.
- Analyze and correlate data into actionable information: SIEM rules, reports, and dashboards.
- Pinpoint IOCs - quickly search for a specific indicator, search for an indicator type over a time range, and drill-down into details.
- Eliminate unnecessary, duplicative and irrelevant indicators - before they enter your infrastructure.
- Identify and prioritize the events that matter now - without DIY scripting.
- Machine-to-Machine learning algorithms scale to accommodate thousands of IOCs per minute across your environment.

Benefits of Palo Alto Networks

- Purposely built into the platform from the ground up with cyberthreat prevention in mind
- Better security than legacy firewalls, UTMs, or point threat detection products
- Next Generation Firewall
- Prevent successful cyberattacks by eliminating gaping holes
- Safely enable applications and business operations
- Eliminate the age-old compromise between security posture and business performance

Seamless and Automated

The Anomali API provides seamless, automated integration of indicator data to deliver near, real-time threat intelligence to your Palo Alto Networks Firewall and reduce your operational workload by blocking the obvious problem at the edge of the network.

Extend the Functionality of the Firewall

After the configured rule fires using the Anomali Dynamic Block List successfully block an IOC, Anomali enables the analyst to take the process one step further using the browser-integrated Anomali Plugin to drill down into the IOC to understand the context and details of why this was a malicious indicator to a level unmatched by our competitors making the security and threat intelligence team that much more knowledge, efficient, and effective.

About Anomali

Anomali™ is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, the ThreatStream platform enables organizations to proactively identify and combat cyber threats targeting their operations.
www.anomali.com

About Palo Alto Networks

As the next-generation security company, Palo Alto Networks is leading a new era in cybersecurity by safely enabling all applications and preventing advanced threats from achieving their objectives for tens of thousands of organizations around the world. Palo Alto Networks is one of the fastest growing security companies in the market because of their deep expertise, commitment to innovation, and game-changing security platform focused on bringing an end to the era of breaches by uniquely integrating our Next-Generation Firewall, Advanced Endpoint Protection, and Threat Intelligence Cloud. With the Palo Alto Networks platform, organizations can confidently pursue a digital-first strategy as they implement key technology initiatives within the cloud and increasingly mobile networks, while maintaining complete visibility and control, to protect their most valued data assets and critical control systems.

For more information contact Anomali sales at info@anomali.com

ANOMALI

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com