Palo Alto Networks Panorama and NETSCOUT

Bringing Threat Detection and Mitigation Closer Together

Benefits

The integration between Palo Alto Networks NGFWs and NETSCOUT allows you to:

- Combine network visibility, threat detection, and investigation with centralized enforcement.
- Immediately send discovered threat information from Omnis Cyber Intelligence to Panorama for rapid and precise mitigation.

The Challenge

You can't protect what you can't see. For threat detection to be effective, network visibility must extend from the network core to the edge and out to the cloud. Combining intelligent threat detection with comprehensive visibility is required to understand and mitigate attacks in the network.

But detection is only the first step to solving the problem. Once threats are detected, mitigation must be performed to prevent data loss and other undesirable outcomes. Unfortunately, mitigation and detection are functions best handled by tools tailored for each task and rarely do they work together. As a result, security teams are faced with the challenge of taking actionable decisions on one tool from threats reported by another.

Until now, joint customers who use NETSCOUT Omnis Cyber Intelligence to detect indicators of compromise (IoCs) and optimize their security posture and Palo Alto Networks Panorama for their perimeter protection had to manually copy IoC information—a process that could be hindered by user error or time.

NETSCOUT Omnis Cyber Intelligence

Omnis® Cyber Intelligence (OCI) is an enterprise-wide network threat and risk investigation solution designed to reduce the impact of cyberthreats on your business. Leveraging multiform factor, scalable, and intelligent NETSCOUT InfiniStreamNG®, vSTREAM® with Cyber Adapter, and CyberStream instrumentation, Omnis Cyber Intelligence provides comprehensive end-to-end visibility—the foundational requirement for effective cybersecurity. Combining comprehensive security visibility with contextual, real-time analytics and NETSCOUT's ATLAS global threat intelligence, Omnis Cyber Intelligence provides the ability to promptly and efficiently detect, validate, investigate, and respond to cyberthreats, whether on-premises or in the cloud. Organizations will benefit from having a cost-effective and highly scalable cyberthreat analytics system at their fingertips that can easily integrate with other security enforcement and reporting platforms.

Palo Alto Networks Panorama

Panorama™ is a security management solution that provides consistent rules in an ever-changing network and threat landscape. Manage your network security with a single security rule base for firewalls, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, access control, and data filtering. This crucial simplification, along with App-ID™ technology-based rules, dynamic security updates, and rule usage analysis, reduces administrative workload and improves your overall security posture.

Palo Alto Networks and NETSCOUT

The NETSCOUT Omnis Cyber Intelligence integration with Palo Alto Networks Panorama takes threat detection and mitigation to a new level by combining threat intelligence, detection, investigation, and response, with the most comprehensive Next-Generation Firewall management platform, to connect technology, process, and people.

Use Case: Take Threats Found During Investigations and Send Data to an Enforcement Tool for Mitigation

Challenge

Security operations teams need to be able to take IoCs and incorporate them into enforcement tools for mitigation. This manual process has always been cumbersome, slow, and potentially inaccurate, as threat data must be copied from the detection tool to a different security tool before any enforcement or mitigation can happen.

Solution

NETSCOUT Omnis Cyber Intelligence can utilize Panorama's RESTful API, allowing it to communicate directly with the security policy. This enables security operations to send detected or investigated threats from Omnis Cyber Intelligence directly to Panorama with the click of a button, informing Panorama of known bad actors or URLs and populating related objects used for enforcement. Enforcement policies can then be sent out to appropriate Palo Alto Networks Next-Generation Firewalls for mitigation of discovered threats.

Palo Alto Networks and NETSCOUT Integrations

Product integrations between Palo Alto Networks and NETSCOUT include:

- NETSCOUT integrates smart DDoS protection with Cortex® XSOAR

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Visit www.netscout.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

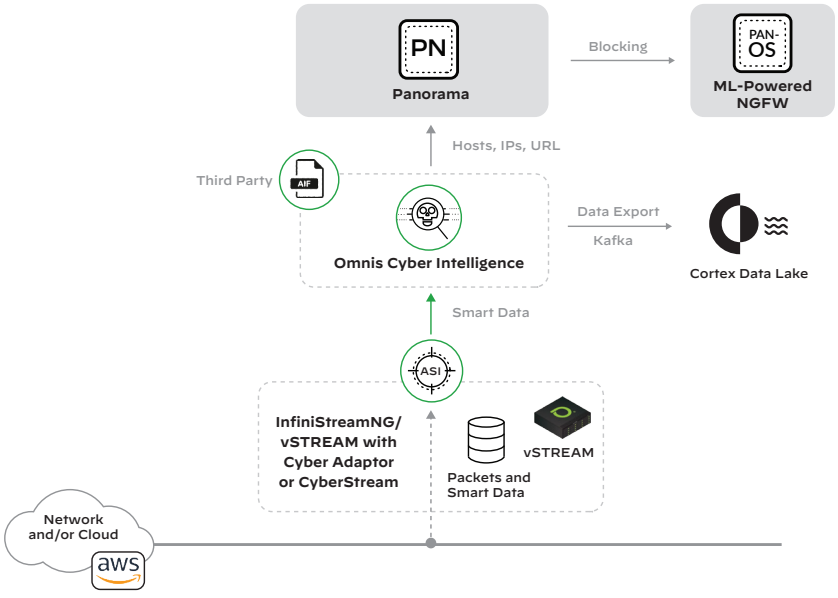

Figure 1: Threat detection with OCI informing Panorama for enforcement

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com