PALO ALTO NETWORKS

Product Name: Next-Generation Firewall

Main Website: https://www.paloaltonetworks.com/

Product Website: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall

Product Integration Type

Firewall

Integration Objective

- Integrates with Palo Alto Networks Next-Generation Firewall to mitigate malicious IP addresses and web URLs
- Both standalone PAN devices and PANAROMA are supported
- Cyphort compiles the list of malicious IP addresses from CNC IP addresses seen in infections and web URLs from network downloads. To avoid false-positives, the reputation of CNC IP addresses and web urls are checked
- As of version 3.5, SmartCore pushes the CNC IP addresses and web URLs automatically to PAN without any need for manual intervention

Customer Value Proposition

Integrates with existing third party infrastructure in the customer's environment to block calls to malicious CNC server IP addresses and bad websites. Integration with Panaroma makes it easier to push IP addresses and web URLs to multiple PAN devices.

Tested Vendor Versions

- PAN: 6.1
- Panaroma: 7.1

Integration Classification

Blocking: Firewall and Web Proxy

Integration Details

Enterprise. Can work in large environments with a variety of integration points.

Integration Method

Push: SmartCore pushes CNC IP addresses and Web URLs to PAN.

Integration Detail Summary (API, CLI)

- CNC IP addresses are pushed to DAG (dynamic address groups) on the PAN
- Mitigated URLs are pushed into a custom URL category which is attached to security policies to implement desired behavior
- CNC IP addresses and Web URLs can be added or removed from PAN using Cyphort UI
- User can also specify “expiry days” on the Cyphort Manager UI to automatically remove the CNC IP addresses from PAN after the specified number of days expire

Cyphort Manager GUI Component

- Yes
- Cyphort Manager configuration: Settings can be configured under Settings -> Environmental Settings

GUI Operational Use Case

Under the Mitigation tab in the Cyphort Manager, the CNC IP addresses show up under Firewalls. The web URLs show up under Secure Web Gateway. The administrator can push or remove IP addresses/web URLs from the PAN manually. From release 3.5 onwards, CNC IP/ web URL addresses can be pushed automatically to PAN without the need for manual intervention.

Threat Score Impact

No

Integration Documentation

N/A

Integration Demo

No

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com

Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com