ENHANCE YOUR PALO ALTO NETWORKS ENVIRONMENT WITH ALGOSEC

Enterprises running Palo Alto Networks-only environments need comprehensive business-driven network security policy management for their entire hybrid network – extending policy management and visibility across routers, SDNs, and the public cloud.

Palo Alto Network's Panorama provides basic network-focused security management of your Palo Alto devices. But what about the rest of your network? You want full visibility and control over your entire hybrid network.

Adding the AlgoSec Security Management solution to your Palo Alto Networks environment enhances your network security so you can benefit from a holistic approach and gain a business-driven focus on your network.

Central Policy Management

While Panorama's central policy management lets you easily create and edit security rules, AlgoSec extends these capabilities by providing comprehensive change management throughout the entire change process – capturing requests, from planning to implementation.

You get full risk analysis, so you can implement these rules directly to your network devices and business applications with zero-touch automation with a streamlined approval process, as well as validate that your security policies were correctly implemented.

These changes are all recorded so that there is a full audit-trail -- supporting internal regulatory requirements as well as industry-specific compliance standards such as PCI DSS, SOX, GLBA, and NERC. Out-of-the-box audit-ready compliance reports are automatically generated.

Centralized Visibility

While Panorama provides network-level visibility and insights into Palo Alto Networks devices in your data center, you can extend this visibility to your entire hybrid network and also gain application-level visibility by integrating with AlgoSec.

AlgoSec provides centralized visibility for both network devices and business applications over your entire network, including hybrid networks, SDNs, and routers. With AlgoSec you can easily visualize complex networks with a dynamic network topology map.

paloalto NETWORKS

By enriching your Palo Alto Network environment with the AlgoSec Security Management Suite, your organization gains:

- Comprehensive end-to-end change management through the entire change lifecycle
- Zero-touch automation including policy push
- A full audit trail of every rule change to easily document compliance
- Out-of-the-box regulatory compliance reports
- Application connectivity tied to your security policy for rule recertification and auditing
- An interactive and dynamic topology map of your entire hybrid environment
- Ability to prioritize and remediate vulnerabilities according to risk and business needs
- Comprehensive risk analysis across firewalls, routers, security groups, and SDN platforms
- Network ChatOps to allow self-service traffic queries and opening of change tickets across the business with no training requirements

AlgoSec automatically understands the firewalls in the path of a traffic request, identifying business application connectivity and services based on actual traffic flows, and generates an interactive, up-to-date connectivity map. You can understand the impact of network security policies on traffic, quickly troubleshoot connectivity issues, plan changes, and perform "what-if" traffic analysis directly, via APIs or using natural language processing with AlgoBot, AlgoSec's ChatOps solution.

Network Security Insights

While Panorama can help identify compromised hosts and surface malicious behavior, AlgoSec enriches this information from vulnerability scanners and identifies compliance violations on the business application-level and firewall rules. AlgoSec then ties the information gained from these vulnerability reports into its risky rule assessment.

AlgoSec instantly assesses, prioritizes, and mitigates risk across your entire hybrid network based on what your business values most — the applications that power it. AlgoSec discovers and prioritizes all risks, mapping them to their associated rules and business applications, in your security policy. This way, you know exactly which applications and firewall rules introduce risk and your security teams can prioritize its response based on the actual threats to the business.

Automated Threat Response

AlgoSec automation utilizes Panorama's rich set of APIs coupled with dedicated add-ons for popular SIEM solutions to enhance insights from your SIEM solutions. AlgoSec enriches security incident data with its business context to assess the severity, risk, and business impact of an attack.

AlgoSec ties security incidents directly to the actual impacted business processes, including the applications, servers, networks and traffic flows, and security devices. Once identified, AlgoSec neutralizes the attack by automatically isolating any compromised or vulnerable servers from the network. AlgoSec then automatically generates a full audit trail to assist with cyber threat forensics and compliance reporting.

Network Security Management

The AlgoSec Network Security solution provides business-driven central network security management for your entire hybrid network – your local data centers, and public and private clouds.

AlgoSec makes the rule recertification process painless, automatically associating the relevant business applications supported by each firewall rule, enabling you to quickly and easily review the firewall rules. AlgoSec recommendations changes to help clean and optimize the policy so you can clean up rules that connect to unused or decommissioned applications, uncover unused, duplicate, overlapping or expired rules, consolidate and reorder rules, and even tighten overly permissive "ANY" rules without impacting business requirements.

Break down organizational silos with network ChatOps. AlgoBot is an intelligent chatbot that handles network security policy management tasks for you. AlgoBot answers your questions, submitted in plain English, and personally assists with security policy change management processes – without requiring manual inputs or additional research. Get the answers fast. Can you reach your cloud server from your desktop or is there a firewall rule or security group blocking it? Get the answers instantly, and even open up change requests via chat.