PALO ALTO NETWORKS AND ESENTIRE

Cybersecurity Protection for the SSL Blindspot and Beyond

Highlights

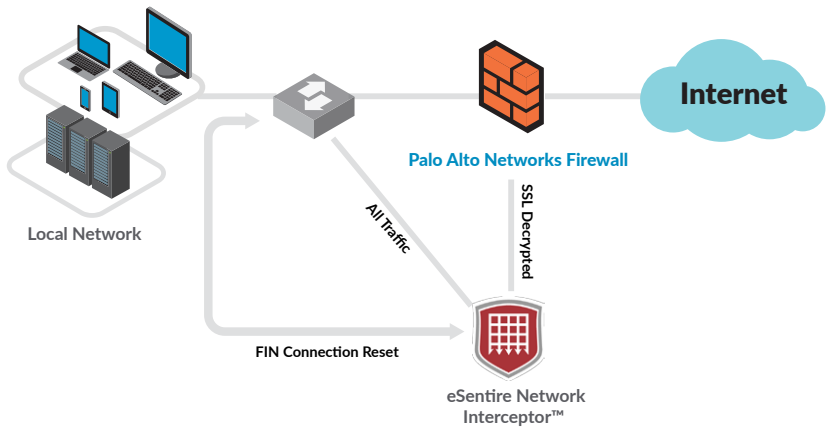
eSentire and Palo Alto Networks provide small to mid-sized organizations with an end-to-end, fully managed cybersecurity service:

- Provides real-time threat protection from both known and unknown attacks through advanced capabilities, including full packet capture, robust threat intelligence, and behavior-based analytics
- Protects an organization's security blindspot – malware hidden inside SSL
- Reduces security risk and provides reassurance through eSentire's 24X7 Global Security Operations Centers that actively monitor, hunt, investigate and contain threats instantly

eSentire® and Palo Alto Networks® customers can now capitalize on unprecedented protection against today's sophisticated attacks, including one of an organization's biggest blindspots – encrypted SSL Traffic. While encryption is critical for network privacy and authentication, the usage of SSL can create blindspots for traditional security controls.

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 uniquely integrates their Next-Generation Firewall, Advanced Endpoint Protection, and Threat Intelligence Cloud into a tightly integrated platform that delivers automated prevention against cyberattacks – known and unknown.

The Managed Detection and Response™ service from eSentire keeps mid-sized organizations safe from constantly evolving cyber attacks . The Managed Detection and Response service goes far beyond just intrusion prevention (IDS/IPS) and security information and event management (SIEM). It leverages behavioral, reputational and signature-based capabilities to vastly improve detection of potential cyberattacks. It's more effective because eSentire 24x7 Security Operations Center (SOC) analysts utilize powerful forensic tools to fully investigate and respond to never-before-seen attacks before they can do harm to your network.



Addressing an Organization's Biggest Security Blindspot

eSentire and Palo Alto Networks have partnered to deliver advanced threat protection, including active monitoring, detection, alerting and blocking of both known and unknown attacks. By combining the power of Palo Alto Network's Next Generation Security Platform with eSentire's Managed Detection and Response security service, organizations get advanced protection across one of their biggest threat blindspots – encrypted SSL traffic.

Beyond the SSL Blindspot

eSentire's Network Inteceptor™ Next Gen IDS/IPS integration with Palo Alto Networks Next-Generation Firewall provides organizations with advanced threat protection:

- Real-time SSL traffic decryption by Palo Alto Networks NGFW, full packet capture and SSL threat inspection by eSentire.
- Real-time detection and alerting of advanced threats, including those contained within SSL traffic.
- Complete network security monitoring and remediation by eSentire's 24X7 Global Security Operations Centers.
- End-to-end cybersecurity protection delivered as a service.

Solution:

The integration between Palo Alto Networks Next-Generation Firewall and eSentire's Network Interceptor IDS/IPS provides organizations with real-time threat monitoring, detection, alerting and containment for all network traffic, including SSL traffic.

Organizations require a supported Palo Alto Networks appliance with SSL decryption offloading capabilities (Decryption Port Mirroring), plus eSentire Network Interceptor IDS/IPS version 9.9.0:

- PA-7000 Series, PA-5000 Series, PA-3000 Series
- Dedicated interface on a private network with a collection system (eSentire)
- Decryption Port Mirroring license

Decrypted SSL traffic is SPAN'd into eSentire's Network Interceptor IDS/IPS appliance for visibility, detection, alerting and blocking of malware.

About eSentire

We've re-engineered the traditional SIEM and IDS/IPS to detect more than just yesterday's threats. M Managed Detection and Response's industry leading threat intel provides real-time protection against known threats, while always-on full traffic capture, log correlation, and behavior-based analytics come together to also detect the unknown. It gets even smarter with our 24X7 elite team of cyber-security analysts that work as an extension of your team to hunt, investigate, identify and escalate threats in real-time. The result is far more effective protection against the sophisticated threats that traditional security technology simply can't detect.

eSentire is a proven industry leader, keeping mid-size organizations safe from constantly evolving cyber attacks that traditional security defenses simply can't detect. eSentire combines people, process and technology to deliver an unmatched, premium level service that detects, remediates and communicates sophisticated cyber threats in real-time, 24/7.

Find out more at **www.esentire.com**

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, Palo Alto Networks 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**

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com