LOGRHYTHM AND PALO ALTO NETWORKS FOR INTEGRATED ENTERPRISE SECURITY

Benefits

LogRhythm and Palo Alto Networks for integrated enterprise security:

- Dynamic defense for detecting and responding to network-based attacks.
- Real-time event contextualization and prioritization for enterprise security intelligence.
- Deep visibility into firewall traffic originating from users, networks and endpoints.
- Tight integration for comprehensive, end-to-end threat lifecycle management.

LogRhythm and Palo Alto Networks have partnered to deliver enterprise-wide threat detection and response through deep forensic visibility, advanced behavioral analytics, and automated incident response orchestration and remediation.

Next-generation firewalls from Palo Alto Networks capture rich user and application context to enable granular control of applications and prevention of advanced threats. LogRhythm integrates with Palo Alto Networks by collecting and contextualizing this data in real time and applying automated stream-based analytics against both it and other security data tied to user, network and endpoint behavior. LogRhythm alarms warn of advanced threats by leveraging granular Palo Alto Networks next-generation telemetry, while LogRhythm's SmartResponse™ plug-ins can initiate automated responses such as instructing Palo Alto Networks to actively block advanced threats or malicious activities at the perimeter.

The Palo Alto Networks and LogRhythm integration provides:

- Highly accurate and corroborated threat detection by continuously analyzing Palo Alto Networks next-generation firewall activity with other log, security and machine data to expose attacks and anomalous endpoint, network and user behavior.
- Unprecedented network visibility across distributed environments to quickly identify malicious activity, such as data exfiltration attempts, compromised user accounts, and rogue processes.
- Automated and streamlined incident response to stop threats and reduce organizational risk via out-of-the-box LogRhythm SmartResponse™ plug-ins that add malicious IPs to a Palo Alto Networks NGFW policy.

LogRhythm extends the industry-leading capabilities of Palo Alto Networks next-generation firewalls by delivering the market's most advanced, automated analytics for advanced threat detection and response to events originating from inside and outside the network. Fully interactive visualization tools and context-aware event management deliver end-to-end threat lifecycle management capabilities for protecting the network and reducing mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).

About LogRhythm

LogRhythm empowers organizations to detect, respond to and neutralize cyber threats early in the threat lifecycle to prevent damaging data breaches and cyber incidents. LogRhythm solutions also deliver rapid compliance automation and assurance, and enhanced IT intelligence.

LogRhythm's award-winning Security Intelligence Platform integrates next-gen SIEM and log management with network forensics, endpoint monitoring and multidimensional security analytics. Its collaborative incident response orchestration and patented SmartResponse™ automation framework help security teams perform end-to-end threat lifecycle management. LogRhythm's unified solution powers the next-gen SOC, accelerating the detection and response to emergent threats across the holistic attack surface.

About Palo Alto Networks

Palo Alto Networks® (NYSE: PANW) is leading a new era in cybersecurity by protecting tens of thousands of enterprise, government, and service provider networks from cyberthreats. Because of our deep expertise, commitment to innovation and game-changing security platform, 28k+ customers have chosen us and we are the fastest-growing security company in the market. Our Next-Generation Security Platform consists of three major elements: Next-Generation Firewall, Threat Intelligence Cloud, and Advanced Endpoint Protection. The Next-Generation Firewall delivers application, user and content visibility and control as well as protection against network based cyberthreats integrated within the firewall through our proprietary hardware and software architecture. A global Threat Intelligence Cloud provides central intelligence capabilities as well as automation of delivery of preventative measures against cyberattacks. Advanced Endpoint Protection delivers protection against cyberattacks that aim to exploit software vulnerabilities on a broad variety of fixed and virtual endpoints. Learn more at www.paloaltonetworks.com.

By combining Palo Alto Networks Next-Generation Security Platform with the threat detection capabilities of LogRhythm's award-winning Security Intelligence Platform, customers benefit from new levels of cyberthreat protection. The integrated solution provides broader understanding of network activity that can be analyzed across the universe of machine data to deliver greater visibility for enterprise-wide security intelligence.

Use Case #1

Detect and Respond to Advanced Threats

Challenge: Advanced persistent threats often leverage customized, zero-day malware to evade detection by traditional perimeter solutions; and once an intrusion gets through, organizations are unable to detect malicious behavior.

Solution: LogRhythm's advanced machine analytics can perform behavioral profiling using application and user data collected by Palo Alto Networks next-generation firewalls to detect abnormal host or network activity, such as excessive outbound connections with non-whitelisted locations.

Response: Integration between LogRhythm and Palo Alto Networks accelerates threat remediation through an out-of-the-box LogRhythm SmartResponse™ plug-in that can automatically shut down the unauthorized processes or services and immediately add the suspicious IPs to Palo Alto Networks NGFW policy to prevent network access.

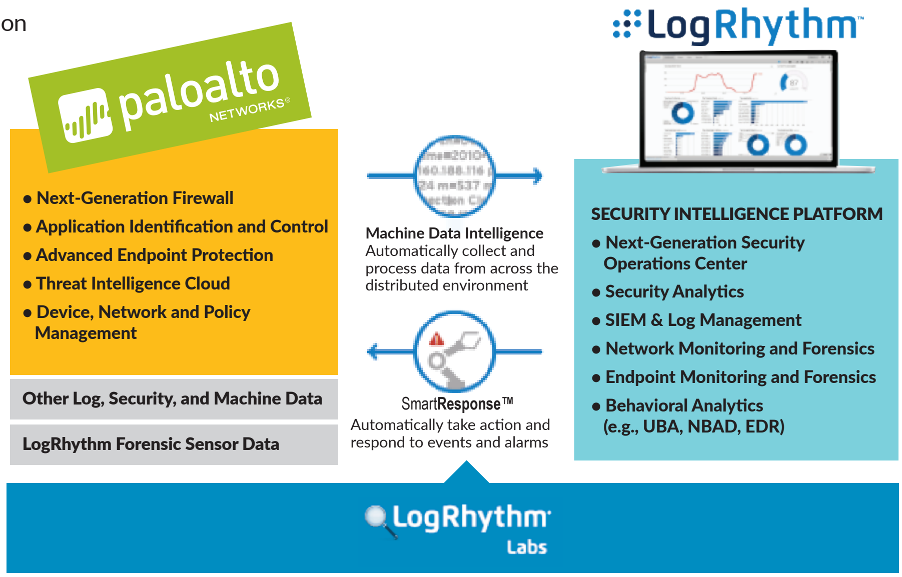
Use Case #2

Prevent Data Exfiltration

Challenge: An increasingly mobile workforce results in malware being introduced into the network by users who unknowingly access unsecured public networks and/or travel in high risk areas. Once an infected host accesses the corporate network, the organization is susceptible to numerous threats, such as data exfiltration and sabotage.

Solution: LogRhythm's behavioral analytics can automatically detect abnormal user, endpoint or network activity, such as malware communicating with an external site. Additional application and user context collected by Palo Alto Networks next-generation firewalls expedites the process of identifying the source of an outbound attack.

Additional Benefit: LogRhythm administrators can take immediate protective action by approving an out-of-the-box SmartResponse™ plug-in that adds the external IP to a Palo Alto Networks NGFW policy until further forensic analysis can verify the legitimacy of the IP.



- Next-Generation Firewall
- Application Identification and Control
- Advanced Endpoint Protection
- Threat Intelligence Cloud
- Device, Network and Policy Management

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data

Machine Data Intelligence
Automatically collect and process data from across the distributed environment

SmartResponse™
Automatically take action and respond to events and alarms

SECURITY INTELLIGENCE PLATFORM

- Next-Generation Security Operations Center
- Security Analytics
- SIEM & Log Management
- Network Monitoring and Forensics
- Endpoint Monitoring and Forensics
- Behavioral Analytics (e.g., UBA, NBAD, EDR)

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