PRODUCT OVERVIEW

LogRhythm and Fortinet: Enterprise Security Intelligence

Fortinet and LogRhythm have developed an integrated offering for comprehensive enterprise security intelligence and incident response management. LogRhythm gathers intelligence from Fortinet's FortiGate high performance network security platform and correlates it against other security device and machine data throughout the IT environment. This integration delivers multi-dimensional behavioral analytics, extended visibility and continuous monitoring for real-time threat detection & response.

LogRhythm for Enterprise Security Intelligence

- ☑ Multi-Dimensional Behavioral Analytics
- ☑ Real-time event contextualization
- ☑ Adaptive defense for protecting vulnerable assets
- ☑ Tight integration for consolidated threat management

The integration provides:

- Identification and tighter control over mobile devices and associated user activity through the combination of comprehensive device identification with behavioral and statistical profiling
- Deeper visibility and contextual awareness into network events with advanced correlation across the entire IT environment to deliver enterprise-wide security analytics
- Access to the most up-to-date threat research and response via the embedded security expertise of LogRhythm Labs™ and FortiGuard™ Labs to help organizations detect advanced attacks and protect against the latest threats
- Automated and immediate action against a broad range of network threats and intrusion attempts
- Continuous compliance assurance to ensure that appropriate personnel are alerted to network events tied to specific regulatory requirements

LogRhythm leverages Fortinet's Unified Threat Management and Next-generation Firewall capabilities to deliver greater visibility and control over enterprise networks. Fortinet monitors and detects a broad range of activity on the network, including mobile device connections, application activity by users, internal resources accessing suspicious external IP addresses, and intrusion attempts. LogRhythm incorporates this information into an automated Risk Based Prioritization (RBP) rating to ensure that the most important events are identified and acted upon first.

LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's award-winning Security Intelligence Platform unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence. LogRhythm delivers:

- Next Generation SIEM and Log Management
- Independent Host Forensics and File Integrity Monitoring
- Network Forensics with Application ID and Full Packet Capture
- State-of-the art Machine Analytics
  - Advanced Correlation and Pattern Recognition
  - Multi-dimensional User / Host / Network Behavior Anomaly Detection
- Rapid, Intelligent Search
- Large data set analysis via visual analytics, pivot, and drill down
- Workflow enabled automatic response via LogRhythm's Smart**Response**™
- Integrated Case Management

Fortinet

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2012 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise - from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

By combining Fortinet's Unified Threat Management and Next-generation Firewall technologies with LogRhythm's behavioral analysis, advanced correlation, pattern recognition, and forensic capabilities, customers benefit from new levels of cyber threat protection. The combined 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.

Detect and Respond to APTs

Challenge Zero day exploits are designed to evade detection by traditional IDS/IPS solutions, and once an intrusion gets through, organizations are unable to detect malicious behavior. Detecting these attacks requires extensive visibility and analysis of multiple attack vectors with a focus on identifying behavior patterns tied to malicious activity.

Solution LogRhythm's advanced machine analytics can perform behavioral profiling using geolocation and other data provided by Fortinet to detect excessive outbound connections being established with non-whitelisted locations or detect when the number of destination IPs exceeds a normal threshold.

Additional Benefit When LogRhythm detects non-whitelisted processes starting or suspicious network connections being established, an out-of-the-box Smart**Response**™ plug-in can automatically shut down the unauthorized processes or services and an administrator can immediately add the suspicious IPs to Fortinet's Next-generation Firewall to prevent future network access.

Monitor User Activity on Mobile Devices

Challenge With the increasingly common acceptance of bring-your-own-device (BYOD) policies, enterprises are finding it difficult to monitor user activity on mobile devices. Organizations need to be able to quickly identify suspicious user behavior and/or potentially compromised or stolen devices in order to secure their networks.

Solution Fortinet detects and identifies mobile devices connecting to the network and sends information to LogRhythm, which then automatically creates a baseline of expected behavior for each mobile device. Administrators are then notified when new or abnormal behavior from a mobile device is observed which could be indicative of compromised credentials or a stolen device.

Additional Benefit LogRhythm's Smart**Response**™ plug-in can immediately send details about suspicious mobile device activity to a List that can add relevant context to any alarm or investigation to surface higher priority threats. This delivers critical information to administrators who can configure their Fortinet Next-generation Firewall to deny further access to the corporate network.