LogRhythm

Joint Solution Brief

Fortinet FortiGate

LogRhythm and Fortinet integrate to provide comprehensive enterprise security intelligence and incident response management

Benefits

- Automated and immediate action against a broad range of network threats and intrusion attempts
- Deeper visibility and contextual awareness into network events with advanced correlation across the entire IT environment to deliver enterprise-wide security analytics
- Continuous compliance assurance to ensure that appropriate personnel are alerted to network events tied to specific regulatory requirements
- Unparalleled security protection leveraging the Fortinet FortiGate Next-Generation Firewall and the Fortinet Security Fabric

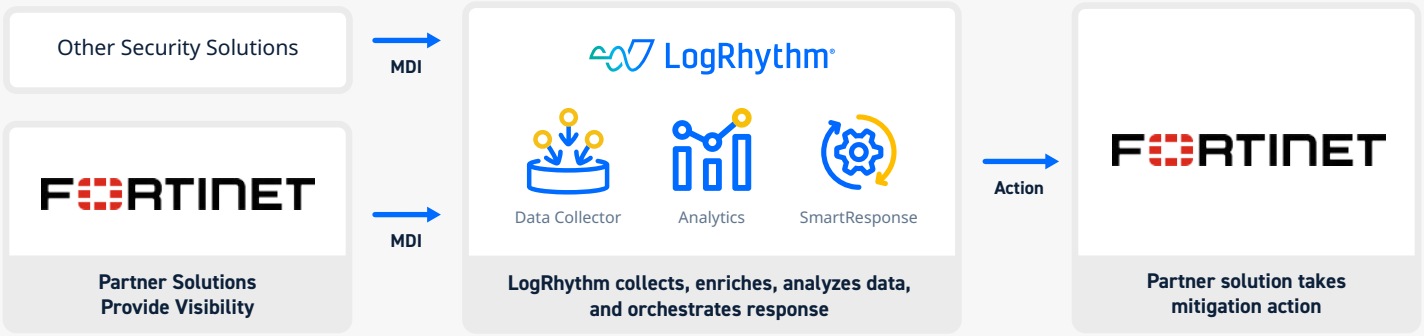
Solution Overview

LogRhythm and Fortinet have collaborated to create an integrated solution for enterprise security intelligence and incident response. LogRhythm collects data from the Fortinet FortiGate Next-Generation Firewall (NGFW) and correlates it with other security device and machine data, offering multi-dimensional behavioral analytics and continuous monitoring. This integration with LogRhythm SIEM enables analysts to detect, respond to, and monitor network events with contextual awareness, providing enhanced control over mobile devices, access to up-to-date threat research, and immediate action against various network threats.

FORTINET

About LogRhythm and Fortinet

LogRhythm and Fortinet work together to help organizations around the globe increase visibility and protect against modern cyberattacks. LogRhythm offers extensive support for and integration across Fortinet's product portfolio. The integrated solution empowers security teams to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence. LogRhythm and Fortinet empower security teams to navigate a changing threat landscape with confidence.



Fortinet FortiGate NGFWs provide industry-leading threat protection and decryption at scale with a custom ASIC architecture. They also deliver Secure Networking with integrated features like SD-WAN, switching and wireless, and 5G.

The integration between the FortiGate Next-Generation Firewall and LogRhythm ensures greater visibility and control over enterprise networks. The solution enables automated risk-based prioritization, empowering organizations to detect, respond to, and neutralize cyberthreats early in the threat lifecycle. LogRhythm combines security information and event management (SIEM), log management, network forensics, and security analytics, accelerating threat detection and response across the entire attack surface. Fortinet FortiGate NGFW is the world's most deployed network firewall, delivering unparalleled AI-powered security performance and threat intelligence, along with full visibility and security and networking convergence. The combined technologies provide customers with advanced cyberthreat protection and a comprehensive understanding of network activity for enterprise-wide security intelligence.

Use Cases

Detect and Respond to Advanced Persistent Threats

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-allow listed locations or detect when the number of destination IPs exceeds a normal threshold.

Additional Benefit:

When LogRhythm detects non-allow listed processes starting or suspicious network connections being established, an out-of-the-box SmartResponse™ can automatically shut down the unauthorized processes or services and immediately add the suspicious IPs to Fortinet FortiGate Next-Generation Firewall to prevent 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 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 SmartResponse™ can immediately send details about suspicious mobile device to Fortinet FortiGate Next-Generation Firewall, which can then deny the device further access to the corporate network. This process can be completely automated or require up to three levels of authorization.

How Automated Workflows Work

To enhance security response efficiency, organizations can leverage LogRhythm's SmartResponse™ for Fortinet FortiGate, an integral part of LogRhythm's security orchestration, automation, and response (SOAR) solution. This tool expedites the reaction to malware threats, minimizing potential damage and eliminating the need for manual intervention by security analysts.

The SmartResponse™ is designed to seamlessly work with Fortinet, offering advanced capabilities to end users. Although LogRhythm has a dedicated engineering team for building plugins, the framework is inherently open, allowing Fortinet's customers to modify existing plugins or create custom integrations as needed.

The LogRhythm SmartResponse™ for Fortinet FortiGate includes various pre-configured actions that can execute automatically in response to an alarm or be manually triggered through analyst workflows. Each action can be set to require approval before execution. The following table provides examples of actions and their corresponding use cases.

LogRhythm SmartResponse™ for Fortinet FortiGate V3.1

Action	Description	Use Case
Add Domain to Group	Adds a domain to a specified group	Runs this action to add a domain to a specified group. For example, an analyst can run this action to block traffic to a malicious domain
Add IP to Group	Adds an IP address or IP range to a specified group	Run this action to add an IP address or IP range to specified group. For example, an analyst can run this action to reconfigure the firewall to block traffic from an attacking IP range
Display Group Info	Displays names of members of a specified group	Run this action to view all the members of the specified group