LogRhythm

Joint Solution Brief

Combining LogRhythm Threat Management and Check Point Network Protection

Benefits

- ✓ Correlate firewall activity against user, network, and endpoint behavior
- ✓ Leverage real-time, actionable threat intelligence
- ✓ Reduce the number of false positives and false negatives
- ✓ Gain deep visibility across the enterprise

Solution Overview

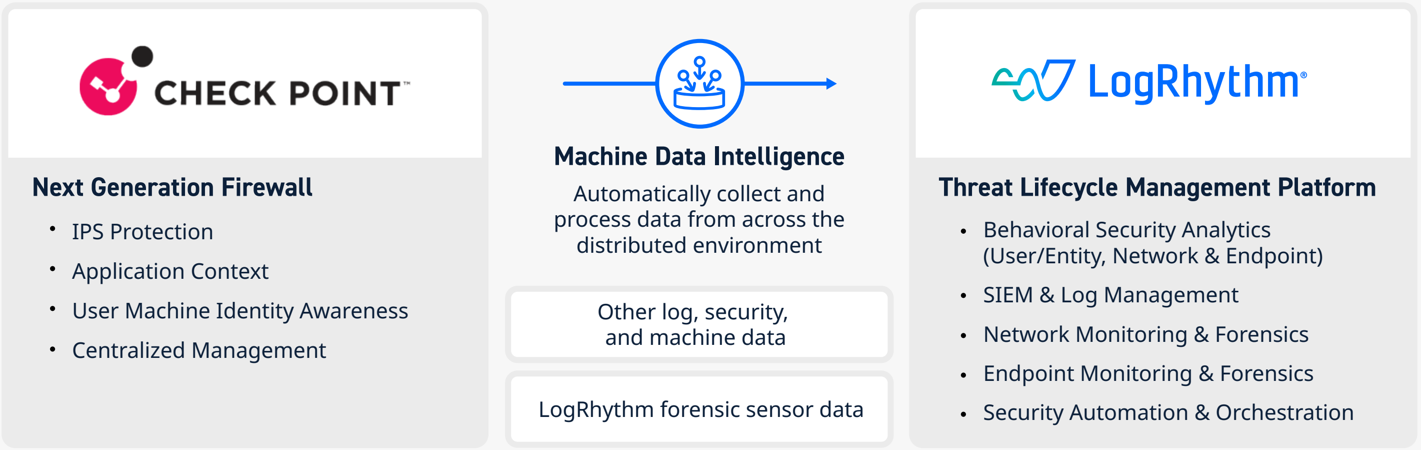
In today's ever-growing threat landscape, visibility is important in securing an organization. Check Point collects enriched data from across network, cloud, mobile, and endpoint devices. LogRhythm SIEM incorporates this rich context and actionable intelligence and centralizes detection of threats. The joint solution provides insight necessary to accelerate the detection and response to advanced emerging threats. Attack containment and remediation is accelerated by LogRhythm's automated workflows that trigger action by Check Point.

When a Check Point device detects a security threat, event logs are sent to LogRhythm via Check Point Log Exporter. The LogRhythm SmartResponse™ for Check Point can automatically disconnect a session to prevent escalation of a potential threat. The security administrator can display host, network, and session information when investigating suspicious activity via the web console.

CHECK POINT™

About LogRhythm and Check Point

LogRhythm and Check Point work together to help organizations increase network visibility and protect against modern cyberattacks. The combined 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 Check Point empower security teams to navigate a changing threat landscape with confidence.



CHECK POINT

Next Generation Firewall

- IPS Protection
- Application Context
- User Machine Identity Awareness
- Centralized Management

Machine Data Intelligence

Automatically collect and process data from across the distributed environment

Other log, security, and machine data

LogRhythm forensic sensor data

LogRhythm

Threat Lifecycle Management Platform

- Behavioral Security Analytics (User/Entity, Network & Endpoint)
- SIEM & Log Management
- Network Monitoring & Forensics
- Endpoint Monitoring & Forensics
- Security Automation & Orchestration

Log Collection

Securing an organization's network and operations begins with high-fidelity and trustworthy log and network traffic data. LogRhythm uses a single schema, Machine Data Intelligence (MDI) Fabric, to normalize structure and unstructured data. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts that allow for precision rule creation and comprehensive remediation efforts in the event of an attack. LogRhythm ingests Check Point data, including network, endpoint, cloud, and mobile device events via Check Point Log Exporter.

How It Works

LogRhythm SIEM collects from every device, application, and sensor in an environment while our MDI Fabric classifies and adds contextual information to every log message. Logs are ingested by the LogRhythm SIEM platform where they are parsed and normalized to the LogRhythm schema. Normalized data is then sent to LogRhythm's analytics engine and storage tier for analysis, storage, and reporting via consolidated dashboards containing all security events.

When used with Check Point, LogRhythm leverages the Check Point Log Exporter to collect network, endpoint, cloud, and mobile device logs and event data from Check Point devices.

How Automated Workflows Work

To streamline security response workflows, organizations can use LogRhythm SmartResponse, which is part of LogRhythm's security orchestration, automation, and response (SOAR) capabilities. LogRhythm SmartResponse accelerates response to suspicious or unauthorized authentication requests to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the LogRhythm SmartResponse for Check Point integration.

The LogRhythm SmartResponse for Check Point contains multiple actions that can be configured to execute automatically in response to an alarm or manually through analyst workflow. Each action can also be configured to require approval before execution.

Action	Description	Use Case
Create Check Point V4 Configuration file	Execute this response and rerun it before using other available actions whenever you change the fixed-value parameter	Functionality that must run first, before other SmartResponse functions can execute
Add Existing Host to Group	Add an existing host to a group	Add an existing host to a group to apply a set ofdefined permissions
Add IP/IP Range to Group	Adds an IP address or IP range to a group	Add an IP address or IP range to a group to apply a set
Create SAM Rule	Creates a SAM rule in Check Point	Creates a security monitoring rule to block traffic to and from a specified host without the need to refresh policies
Delete Host	Deletes a host in Check Point	Delete a particular host by using host name as parameter
Delete Network	Deletes a host in Check Point	Delete a particular network by using network name as parameter
Disconnect Session	Disconnects the session in Check Point	Disconnect a particular active session by using session UID as parameter
Install Policy	Installs the policy on Targeted object in Check Point	Install a policy package on target(s) by using target name(s) as a parameter
Show Host Information	Provides host information	Display details of any host
Show Network Information	Provides network information	Display details of any network
Show Session Information	Provides session information	Display details of any session

For more information, request a LogRhythm demo.