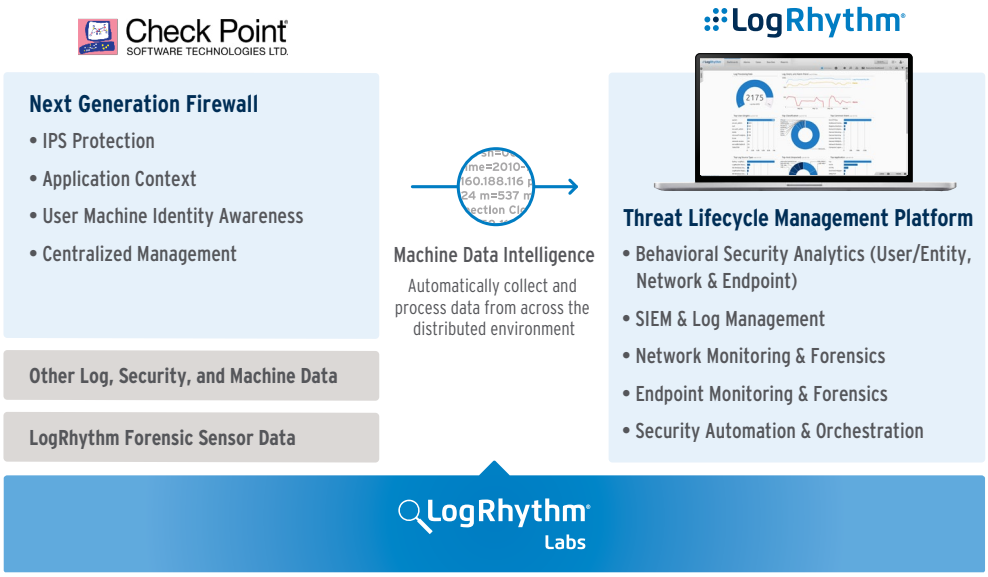
LogRhythm and Check Point: Integrated Enterprise Security

LogRhythm and Check Point offer an integrated solution for enterprise threat lifecycle management and next generation network protection. LogRhythm collects extensive insight into the entire security gateway from Check Point via OPSEC LEA for detailed visibility into the users, groups, applications, machines and connection types. LogRhythm's SmartResponse™ automation framework enables customers to build a plug-in to leverage Check Point for immediate protective action.

The integration provides:

- Real-time correlation of next generation firewall activity against user, network and endpoint behavior for enterprise-wide threat detection and response
- Increased visibility and enhanced breach detection capabilities through the integration of network security data with multi-dimensional behavior analytics
- Accurate threat detection by linking meaningful events with conditional logic and modern threat analytics to reduce the number of false positives and false negatives

Combining Check Point's next generation firewall capabilities with the multi-dimensional behavioral analytics of LogRhythm delivers enterprise-wide continuous monitoring and real-time threat detection and response.



About LogRhythm

- Empowers organizations to rapidly detect, respond to and neutralize cyber-threats
- Provides a holistic platform for end-to-end Threat Lifecycle Management, uniquely unifying next-gen SIEM, log management, network & endpoint forensics, advanced behavior analytics & machine learning, and security automation and orchestration
- Delivers rapid compliance automation and assurance, and enhanced IT intelligence
- Consistent market leadership including recognition as a Leader in Gartner's Magic Quadrant since 2012

Check Point
SOFTWARE TECHNOLOGIES LTD.

About Check Point

- The worldwide leader in securing the Internet, providing customers with uncompromised protection against all types of threats
- Pioneered the industry with FireWall-1 and its patented stateful inspection technology
- Continues to develop new innovations based on the Software Blade Architecture
- Provide flexible, simple, and easy to deploy security modules that enable customers to select the security they need to build a custom security solution

LogRhythm and Check Point are tightly integrated, combining the functionality of Check Point's next generation firewalls with the threat management capabilities of LogRhythm's Threat Lifecycle Management Platform. The combined offering empowers customers to identify true behavioral anomalies, internal and external threats, and prevent breaches based on accurate enterprise security intelligence.

LogRhythm for Unified Threat Lifecycle Management

- Dynamic defense for detecting and stopping unauthorized network threats
- Multi-dimensional behavioral analytics to deliver real-time security intelligence
- Deep visibility into all aspects of user, network and endpoint behavior activity throughout the IT environment
- Tight integration for consolidated threat management

Protection from Endpoint Breaches

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

Solution:
LogRhythm's ability to baseline "normal" behavior reduces the incident response process by automatically detecting abnormal host or network activity, such as malware communicating with an external site. Additional application and user context collected by Check Point Next Generation Firewalls expedites the process of identifying the source of an outbound attack.

Additional Benefit:
Organizations can build a SmartResponse plug-in between LogRhythm and Check Point that accelerates threat remediation by blocking all communication with an external IP address and/or port associated with an exfiltration attempt. With such a plug-in, LogRhythm can automatically send the attacking IP address and port to the Check Point firewall to immediately block communication and prevent data from being stolen.

Securing the Mobile Infrastructure

Challenge:
External attackers will frequently scan a network to identify open ports to launch an attack. Once an open port is detected, attackers will establish a connection, but since the activity appears to be normal, it frequently goes undetected.

Solution:
LogRhythm collects, processes and analyzes Check Point logs in real time via API integration using OPSEC LEA, automatically detecting when suspicious port scan activity is taking place. LogRhythm's AI Engine can then automatically identify when port scan activity is followed by a sustained connection from the same IP indicating that a potential attack is taking place.

Additional Benefit:
Organizations can use scripting to further tighten the link between LogRhythm and Check Point. For example, after an attack has been detected, a script can be used to add the attacking IP to a Check Point ACL. Another script can be written to add the attacking IP to a list of known attackers, which can be used to flag future activity originating from the same source.