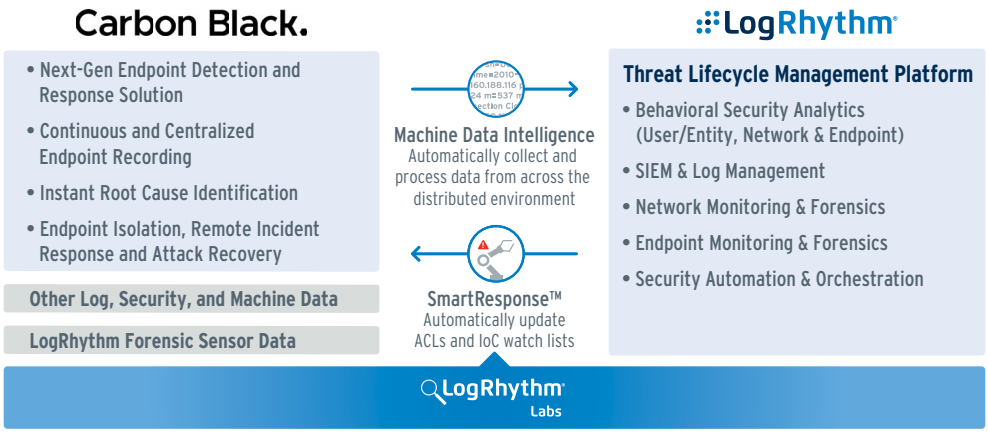
LogRhythm and Carbon Black for Integrated Threat Discovery and Remediation

LogRhythm and Carbon Black have partnered to deliver enterprise-wide threat detection and response. LogRhythm's Threat Lifecycle Management platform continuously collects, normalizes, and analyzes rich, dynamic endpoint telemetry captured by Carbon Black's entire security portfolio, including Cb Defense, Response, and Protection. Carbon Black data is then combined with the petabytes of other machine data LogRhythm collects and analyzes from across the distributed environment. This analysis provides a holistic view of attack activity and enables proactive detection of threats originating from or targeting an endpoint before they can result in a high-impact incident or data breach.

When a threat or indication of compromise is detected within your environment, a LogRhythm SmartResponse™ plugin can automatically instruct Carbon Black to take immediate action on the impacted endpoint including but not limited to isolating the host from the network, killing a process on the "host," or deleting a file from the host. Additionally, if warranted, an analyst can launch a SmartResponse plugin to automatically start a memory dump from an impacted endpoint to return a record of all activity that occurred on the host for forensic analysis. LogRhythm's SmartResponse Automation Framework supports several execution options including fully automated response, one-click execution, and multi-level approval.

The integration between LogRhythm and Carbon Black allows your organization to:

- Detect and prioritize intrusions faster by correlating detailed endpoint activity with other environmental context to recognize early indicators of potential compromise
- Visualize high priority events in a Carbon Black-specific dashboard within LogRhythm's centralized console
- Automate investigatory and response processes including deployment of real-time countermeasures on an endpoint to prevent further impact and expedite incident response
- Streamline processes that were once significantly manual, including attack analysis and adaptive threat defense



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

Carbon Black.

About Carbon Black.

Carbon Black is the leading provider of next-generation endpoint security. Carbon Black's Predictive Security Cloud provides advanced protection for more than 14 million endpoints across 3,300 customers, including 31 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks. For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.

LogRhythm and Carbon Black are tightly integrated, combining the value of best-of-breed endpoint detection and response and next-generation antivirus platform with the threat management capabilities of LogRhythm's Threat Lifecycle Management Platform. The combined offering empowers your security team to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence.

LogRhythm for Integrated Enterprise Security Intelligence

- 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

Use Case: Prevent the Spread of Advanced Malware (Endpoint Lockdown)

Challenge:
Once an attacker controls an endpoint, it can be used to compromise additional systems. Left undetected, malware can quickly propagate across your network, so it is imperative your security professionals quickly detect compromised endpoints and take immediate protective action to reduce the risk of experiencing a high-impact incident or data breach.

Solution:
Cb Response continuously records all endpoint activity and provides this telemetry to LogRhythm's Security Intelligence Platform. LogRhythm combines this information with other flow, event, and machine data, and performs real-time analytics to detect behavioral anomalies and indicators of compromise on endpoints. This visibility ensures your security team is quickly alerted to the first signs of malware within the corporate network.

Additional Benefit:
LogRhythm SmartResponse plugins are designed to actively defend against attacks by initiating actions that offset the threat. When a compromised endpoint is detected, a LogRhythm SmartResponse plugin can instruct Carbon Black to isolate the endpoint from the network until the malware has been eradicated.

Use Case: Detect Insider Threats

Challenge:
Insider threats leverage endpoints to transfer stolen data to external sites or locally writable media. Your security analysts need to be able to distinguish between legitimate day-to-day business operations and data exfiltration attempts.

Solution:
To help organizations detect data theft, Carbon Black captures all critical endpoint activity including new processes, registry modifications, network connections, file executions, etc. LogRhythm correlates this endpoint telemetry with other machine data to create baselines for what should be considered normal behavior. This enables highly focused alerts in response to behavioral indicators associated with data exfiltration on an endpoint. Your analysts can automatically kill suspicious transfers using a SmartResponse plugin.

Additional Benefit:
In response to suspected data theft, security analysts can leverage a LogRhythm SmartResponse plugin that instructs Carbon Black to perform a memory dump on the impacted endpoint. Results are automatically pulled into LogRhythm's console, allowing analysts to quickly assess the scope of the incident and take remedial action.