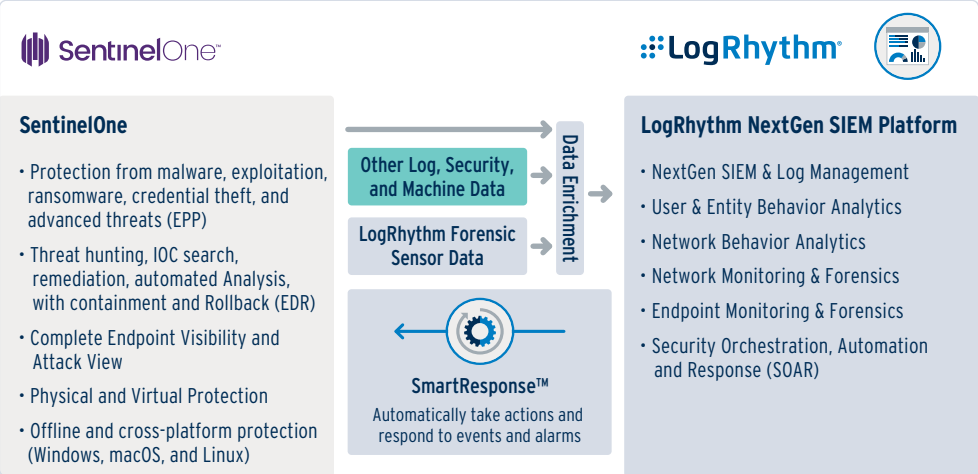
LogRhythm and SentinelOne: Integrated Enterprise Security

LogRhythm and SentinelOne provide an integrated enterprise security solution to prevent, detect, and respond to threats in your environment. LogRhythm's security analytics automatically incorporate rich endpoint telemetry from SentinelOne, enabling real-time cyberthreat protection and providing analytics in depth for comprehensive security monitoring.

The integration allows customers to:

- Deliver SentinelOne's comprehensive endpoint data to the LogRhythm NextGen Security Information and Event Management (SIEM) Platform to protect diverse modes of attack:
  - Executables and fileless malware
  - Document- and browser-based exploits
  - Access-based vectors leveraging scripts or user credentials
- Rapidly detect and respond to threats by centrally analyzing rich endpoint activity with machine data, environmental context, and threat intelligence to capture early indicators of potential compromise
- Streamline processes and accelerates response by remotely invoking custom LogRhythm SmartResponseTM actions from the SentinelOne agent:
  - Perform/abort a vulnerability or virus scan
  - Isolate the host from the network
  - Get process list
  - Check hash values for reputation
  - Broadcast a message
  - Blacklist executables

By ingesting SentinelOne's detailed endpoint data into the LogRhythm NextGen SIEM Platform, your organization enjoys industry-leading enterprise security intelligence and threat management capabilities. The combination enables centralized monitoring of systems and applications throughout your environment. Moreover, the integration ensures accurate, up-to-date, and relevant information, enabling rapid response to security threats.



About LogRhythm

- Empowers organizations to rapidly detect, respond to, and neutralize damaging cyberthreats with NextGen SIEM
- Unifies user and entity behavior analytics (UEBA), network behavior analytics (NTBA), and security orchestration, automation and response (SOAR)
- Serves as the foundation for the AI-enabled SOC via LogRhythm's Threat Lifecycle Management (TLM) workflow
- Measurably secures cloud, physical, and virtual infrastructures for both IT and OT environments
- Recognized as a Leader on the Gartner SIEM Magic Quadrant

About SentinelOne

SentinelOne delivers autonomous endpoint protection through a single agent that successfully prevents, detects, and responds to attacks across all major vectors. Designed for extreme ease of use, the S1 platform saves customers time by applying AI to automatically eliminate threats in real time for both on premise and cloud environments and is the only solution to provide full visibility across networks directly from the endpoint. To learn more visit sentinelone.com or follow us at @SentinelOne, on LinkedIn, YouTube, or on Twitter.

LogRhythm and SentinelOne combine the value of an industry-leading endpoint protection platform with the threat management capabilities of LogRhythm's NextGen SIEM. The combined offering empowers customers to identify and prioritize internal and external threats and accelerate their response with comprehensive security intelligence.

LogRhythm for Integrated Enterprise Security Intelligence

- Dynamic defense for detecting and stopping unauthorized network threats
- Full-spectrum analytics to deliver real-time security intelligence
- Deep visibility into all aspects of user, network, and endpoint behavior activity throughout the IT environment
- Embedded security orchestration and automation streamlines response processes

Data Sharing for End-To-End Threat Management

Challenge:
Security teams face numerous alarms and alerts every day. Filtering and prioritizing events consumes their already-constrained resources. Organizations need the ability to correlate data from disparate security products and effectively distinguish the real threats from false alarms.

Solution:
LogRhythm collects and processes rich endpoint data from SentinelOne and analyzes it centrally alongside other machine data sources. Correlating log data from multiple sources generates prioritized alerts identifying suspicious activity within the environment.

Additional Benefit:
LogRhythm SmartResponse™ plug-ins are designed to actively defend against attacks by initiating actions that neutralize cyberthreats. If unusual network traffic were detected, SmartResponse actions instruct SentinelOne to send a message to the host and automatically isolate it from the network. By reducing the time to perform common mitigation steps, security teams can prevent escalation of high-risk incidents.

Protect Against Advanced Malware

Challenge:
Once attackers controls an endpoint, they are likely to attempt to compromise additional systems. Left undetected, malware can quickly propagate across the network. It is imperative that security professionals quickly detect compromised endpoints and take immediate action to reduce the risk of a high-impact incident or data breach.

Solution:
SentinelOne dynamically detects advanced malware, exploits, and insider/script-based attacks and provides this telemetry to the LogRhythm NextGen SIEM Platform. LogRhythm combines this information with other flow, event, and machine data, and performs real-time analytics to recognize anomalies and indicators of compromised endpoints. Prioritized alarms and integrated playbooks ensure security teams quickly act on the first signs of malware, preventing costly damages.

Additional Benefit:
LogRhythm SmartResponse actions enable analyst to perform/abort a scan, disconnect/reconnect to the network, retrieve a list of processes, check hash values for reputation, broadcast a message, and blacklist executables.