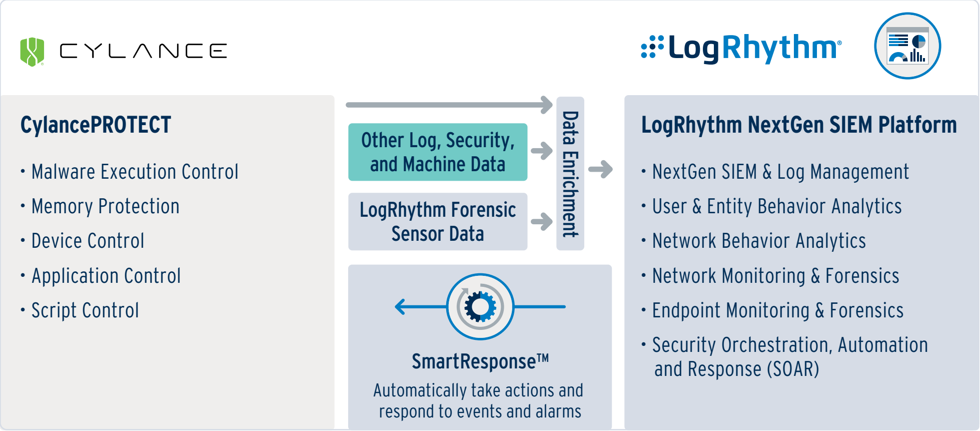
LogRhythm and Cylance for Integrated Threat Discovery and Remediation

LogRhythm and Cylance have partnered to deliver enterprise-wide threat prevention, analysis, and response. The LogRhythm NextGen SIEM platform continuously collects, normalizes, and analyzes rich, dynamic endpoint telemetry captured by CylancePROTECT. Cylance 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 malicious 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.

The integration between LogRhythm and Cylance allows mutual customers to:

- Detect and prioritize intrusions faster by correlating detailed endpoint activity with other environmental data to recognize early indicators of potential compromise
- Adopt a prevention-first methodology, using machine learning that harnesses algorithmic science and artificial intelligence to determine whether objects are good or bad in real time
- Visualize high-priority events in a Cylance-focused 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 largely manual, such as attack analysis and adaptive threat defense


CYLANCE
LogRhythm
CylancePROTECT
• Malware Execution Control
• Memory Protection
• Device Control
• Application Control
• Script Control
Other Log, Security, and Machine Data
LogRhythm Forensic Sensor Data
Data Enrichment
SmartResponse™
Automatically take actions and respond to events and alarms
LogRhythm NextGen SIEM Platform
• NextGen SIEM & Log Management
• User & Entity Behavior Analytics
• Network Behavior Analytics
• Network Monitoring & Forensics
• Endpoint Monitoring & Forensics
• Security Orchestration, Automation and Response (SOAR)

About LogRhythm

- Empowers organizations to rapidly detect, respond to, and neutralize damaging cyberthreats with NextGen SIEM
- Unifies user and entity behavior analytics (UEBA), network traffic and 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 Cylance

- Cylance® is revolutionizing cybersecurity with products and services that proactively prevent, rather than reactively detect, the execution of advanced persistent threats and malware
- Cylance is the first company to apply artificial intelligence, algorithmic science, and machine learning to cybersecurity to prevent the most advanced security threats in the world
- Using a breakthrough predictive analysis process, CylancePROTECT® quickly and accurately identifies what is benign and what is a threat, and prevents malicious code from ever executing on a targeted system
- This technology is deployed on over ten million endpoints and protects hundreds of enterprise clients worldwide including Fortune 100 organizations and government institutions. For more information visit: www.cylance.com

LogRhythm and Cylance are tightly integrated, combining the value of best-of-breed prevention, endpoint detection and response, and forensics tools with the threat management capabilities of LogRhythm's NextGen SIEM. The combined offering empowers customers to prevent attacks, identify behavioral anomalies and internal and external threats, and prioritize 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: End-to-End Threat Management

Challenge:
Your security team is faced with numerous alarms and alerts. Filtering and prioritizing events consumes a security team's already-constrained resources. Your organization needs the ability to correlate data from disparate security products and effectively distinguish the real threats from false alarms.

Solution:
LogRhythm collects and processes endpoint data from Cylance and analyzes it centrally alongside diverse machine data. Correlating log data from multiple sources generates prioritized alerts to identify suspicious activity within the environment.

Additional Benefit:
SmartResponse™ plug-ins enable active defense by initiating actions to neutralize specific cyberthreats. By reducing the time to perform common mitigation steps, SmartResponse helps prevent high-risk incidents from escalating.

Use Case: Prevent the Spread of Advanced Malware

Challenge:
Once an attacker 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 protective action to reduce the risk of a high-impact incident or data breach.

Solution:
CylancePROTECT's architecture consists of a small agent that integrates with the LogRhythm Platform. The endpoint detects and prevents malware through tested mathematical models on the host, independent of a cloud or signatures. Cylance provides this telemetry to the LogRhythm Platform, which centrally analyzes it with other event, log, and flow data to detect anomalies and indicators of compromised endpoints. This real-time visibility ensures that security teams are quickly alerted to the first signs of malware within the corporate network.

Additional Benefit:
When suspicious activity is detected, LogRhythm SmartResponse plugins can be executed to rapidly neutralize a potential threat. Actions include "Display Host Status," which takes host info such as host name or IP and returns scan data and other data about that host, and "Quarantine Global File," which takes file name/hash as an input and quarantines the file globally.