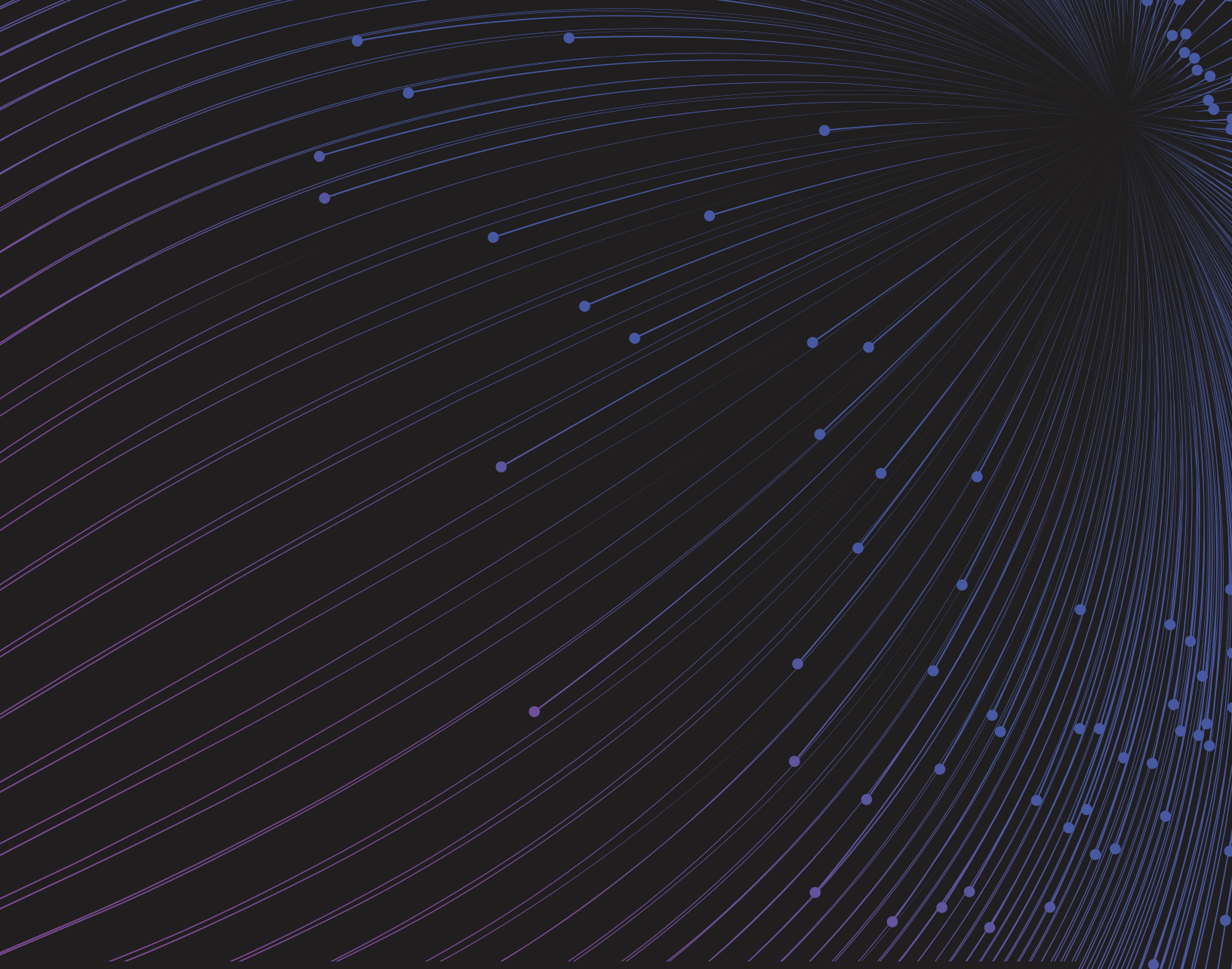

Cylance® and LogRhythm Partner To Deliver Prevention and Visibility

Enabling a Single Source Across All Data and Assets

CYLANCE

LogRhythm®

Introduction

Cylance and LogRhythm have partnered to deliver enterprise-wide AI based threat prevention, analysis, and response. Cylance AI driven prevention and protection stops advanced threats and changes the security engineer's tactics from defensive to offensive. The LogRhythm NextGen SIEM Platform continuously collects, normalizes, and analyzes rich, dynamic endpoint telemetry captured by Cylance technology. Cylance data is then combined with the petabytes of other machine data that 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.

Value Statement

The integration between Cylance technology and LogRhythm allows mutual customers to:

- 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
- 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 Cylance-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 labor-intensive, including attack analysis and adaptive threat defense

Use Cases

Lower Mean Time To Respond (MTTR) To Alerts

- Challenge: SOC analysts must sort through and prioritize a myriad of alerts.
- Solution: With Cylance's prevention-first methodology, which lowers noise, along with the machine learning, advanced analytics, and actionable intelligence of LogRhythm's NextGen SIEM platform, customers can respond faster with greater efficiency and accuracy to modern threats such as automated blacklisting of malware throughout the organization when detected.
- Additional Benefit: SOC analysts will get more time back to perform more important tasks for the security organization.

End To End Threat Management

- Challenge: Allocating the appropriate filters to expose the root issue and prioritize events consumes already constrained resources.
- Solution: LogRhythm incorporates endpoint data from Cylance technology into automated advanced correlation rules. This delivers highly-focused alerts that identify when suspicious activity is occurring within environments.
- Additional Benefit: SmartResponse™ plugins are designed to actively defend against attacks by initiating actions that neutralize specific cyberthreats. SmartResponse also collects telemetry data and status information from endpoints protected by Cylance technology.

Prevent the Spread of Advanced Malware

- Challenge: Once an attacker controls an endpoint, it can be used to compromise additional systems. Left undetected, malware can quickly propagate across the network.
- Solution: CylancePROTECT's architecture consists of a lightweight agent that integrates with existing security software like the LogRhythm NextGen SIEM Platform. The endpoint will detect and prevent malware and deliver threat information to LogRhythm, allowing LogRhythm to update the rest of the security ecosystem through SmartResponse actions. In addition, SmartResponse actions allow for automated blacklisting of malware on endpoints protected by Cylance technology.

SmartResponse Technology

- SmartResponse uniquely enables automated incident response. It also allows semi-automated, approval-based operation so users can review the situation before countermeasures are executed. The integration of CylancePROTECT® into LogRhythm SmartResponse Automation Framework is an example of how users can integrate with current and future security technologies easily. The CylancePROTECT integration can be informational like obtaining host data, or action oriented like quarantining a file with a given file name or hash. This reduces the time needed to perform common investigation and mitigation steps, preventing high-risk compromises from snowballing.
- Additionally, many other automated actions are planned to support the above and other advanced use cases.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first security solutions and specialized services that change the way organizations approach endpoint security. Cylance security solutions combine AI driven predictive prevention with dynamic threat detection and response to deliver full spectrum threat prevention and threat visibility across the enterprise.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organizations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm platform combines user and entity behavior analytics (UEBA), network traffic and behavior analytics (NTBA) and security automation & orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations center (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.
www.logrhythm.com

API Driven Features	Description
LogRhythm Playbooks and SmartResponse	▪ Through API integration and SmartResponse, many Playbooks feature CylancePROTECT. SmartResponse gives contextual data on an alarm, either automatically, or upon request.
Data Enrichment	▪ LogRhythm calls the Cylance API frequently to get threat information and update its dashboard. LogRhythm then performs data enrichment to the rest of the environment, including CylancePROTECT, for more information.
Environment Check/Update	▪ Users can check devices via the Cylance API for up to date status on device date, threat details, alerts, etc.
Blacklisting	▪ Given a hash, update the Cylance blacklist. The hash can come from a Cylance detection or somewhere else (FW, CERT list, etc.).
Malware Hunting	▪ Given a hash, search Cylance endpoints to see if the hash has been seen. The hash can come from Cylance or another device, CERT list, etc.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE

20180914-0423