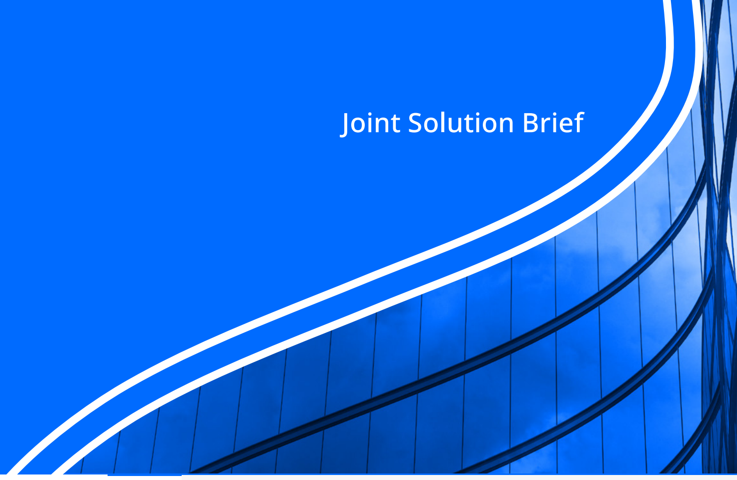
LogRhythm

Joint Solution Brief



LogRhythm and Cisco:
Integrated Enterprise Security

LogRhythm is an enterprise-class platform that seamlessly combines security information and event management (SIEM), log management, file integrity monitoring, and machine analytics using host, user, application, and network log data. LogRhythm addresses an ever-changing landscape of threats and challenges with a full suite of high-performance tools for security, compliance, and operations.

In regard to the Cisco Security product line, LogRhythm provides the following support:

Cisco Secure Product	Log Source Normalization	Smart Response™
Cisco SecureX		X
Cisco Secure Network Analytics	X	X
Cisco Secure Malware Analytics		X
Cisco Secure Email	X	
Cisco Secure Endpoint	X	X
Cisco AnyConnect Secure Mobility Client	X	
Cisco Secure Firewall	X	X
ASA Adaptive Security Appliance	X	X
Threat Defense	X	
Firepower Series Appliances	X	X
Threat Defense Virtual Firepower	X	
Threat Defense Manager Firepower Management Center	X	
ASA Virtual Adaptive Security Virtual Appliance (ASAv)	X	
Cisco Identity Services Engine (ISE)	X	X
Duo / Cisco Secure Access by Duo	X	
Cisco Secure Web Appliance	X	
Cisco Meraki	X	X
Cisco pxGrid		X
Cisco Umbrella/Cloudlock	X	X

cisco

About LogRhythm and Cisco

LogRhythm and Cisco work together to help organizations around the globe increase network visibility and secure their IT environments. LogRhythm offers extensive support for and integration across Cisco's product portfolio, automatically incorporating, normalizing, and contextualizing log flow and event data captured from over two dozen Cisco products. LogRhythm SIEM performs advanced analytics across these data sets, as well as all other machine data collected across an organization to deliver real-time detection of advanced threats.

Cisco SecureX

The Cisco SecureX platform unifies visibility by connecting cisco secure portfolio and other solutions such as LogRhythm. This integration strengthens a user's security across network, endpoint, cloud, and applications, and provides increased environmental context and advanced correlation. LogRhythm continually collects the data from Cisco Secure products. Analysts can investigate observables across the solutions. Using generated alarm details, an analyst can use a SmartResponse™ to create an incident in Cisco SecureX so they can track the real-time investigation or manage security actions in response to the potential threat. This ultimately enables real-time protection and significantly reduces detection and response times.

Use Case: Centralized Monitoring and Response

Challenge

Organizations face a complex and evolving security landscape due to continuous and emerging threats. Managing multiple security products across their IT infrastructure may make it difficult to give proper attention to these threats.

Solution

Cisco SecureX unifies the Cisco Secure portfolio with an organization's entire security infrastructure, including the LogRhythm SIEM platform. Organizations can streamline their security operations and their security teams can focus on quickly responding to and neutralizing threats. LogRhythm offers SmartResponses for Cisco SecureX including one that allows security teams to create a case in Cisco SecureX to help track an investigation or manage security actions in response to emerging threats.

Cisco Secure Malware Analytics

LogRhythm continually ingests and analyzes malware and threat intelligence data provided by Cisco Secure Malware Analytics. This data is correlated with data collected across the IT environment to proactively identify and defend against emerging threats within the network. Analysts are empowered to prioritize high-risk events and take action.

Use Case: Optimizing Threat Intelligence

Challenge

The volume of malicious activity and the speed at which it can propagate make it difficult for information security professionals to know which events pose the greatest risk to their organizations.

Solution

Cisco Secure Malware Analytics dynamically analyzes key behavioral indicators and malware artifacts to provide a view of malware. LogRhythm consumes this intelligence in real time, performing advanced behavioral analysis to recognize when network activity with known bad actors is observed within the customer environment. This visibility enables administrators to quickly discover and qualify threats that represent real risk in their environment.

Cisco Identity Services Engine (ISE)

The integration between LogRhythm and Cisco ISE offers deep visibility into the activities of those connected to the network and the devices, by monitoring their device type, profile, and posture and utilizing LogRhythm's correlation and forensic analysis capabilities with Cisco ISE contextualized data. Leveraging LogRhythm's automated behavioral analysis and correlation with Cisco ISE endpoint profiling, posture assessment, and contextual awareness, offers real-time alerting and reporting on suspicious, unauthorized activity. LogRhythm's compliance packages combined with the enforcement of Cisco ISE's active endpoint profile policy, automates detection and response for user and device violation for continuous compliance.

Use Case: Enhanced Network Access Control

Challenge

With the growing number of outside devices and potential access points in today's enterprise, access control is more difficult than ever before. Without the means to collect, correlate, and analyze relevant data, bridging the gap between acceptable device behavior profiles and potential suspicious activity can be almost impossible.

Solution

Multidimensional behavioral analysis modules in LogRhythm's AI Engine automatically profile device behavior, creating safelists of acceptable activity such as processes or services, network connections, etc. These behavioral safelists can be correlated against device profiles within ISE to significantly enhance network visibility and rapidly identify suspicious and/or malicious activity.

Additional Benefit

SmartResponse enforces continuous compliance and protects the network by dynamically adapting alarms, investigations, and reports to stay up-to-date by automatically adding non-compliant or suspiciously behaving devices to a list and/or quarantining such devices.

Cisco Umbrella

LogRhythm continually consumes and analyzes internet activity data provided by Cisco Umbrella and combines this with other machine data collected from across the environment to help organizations identify and defend against attacks targeting their network. By leveraging domain and IP data from Cisco Umbrella with LogRhythm's threat intelligence and analytics capabilities, customers can reduce the time to detect and contain threats, increase visibility into internet activity across all locations and users, identify cloud apps used across the business, and reduce remediation costs and breach damage. Additionally, LogRhythm has SmartResponses that allow analysts to automatically retrieve information about threats to a domain, IP, and URL for further analysis and block them.

Use Case: Defend Against Malicious DNS Requests

Challenge

In the last couple years, remote work has risen and with it, organizations' attack surfaces have increased, and the risk of a breach has escalated.

Solution

Cisco Umbrella provides DNS-based security by blocking access to known malicious domains and IP addresses, while also noting ones that seem risky. This prevents remote workers from accessing malicious websites or unintentionally downloading malware. As LogRhythm ingests this network activity data, security teams can receive real-time alerts when remote workers attempt to access such malicious domains or when they were blocked by Cisco Umbrella. This data that is also correlated with LogRhythm data to enable increased investigative abilities. If domains that presented as risky, were found to not be a risk, analysts can use a SmartResponse to unblock them.

Additional Benefit

SmartResponse can initiate an automated response to any malicious domain or URL by blocking them until they can be further investigated. The blocklist action can be completely automated or subject to authorization.

Cisco Secure Endpoint

The integration between LogRhythm and Cisco Secure Endpoint offers organizations increased visibility into threats to their endpoints and enriched context regarding suspicious activities. Cisco Secure Endpoint receives malware intelligence from Cisco Talos, which it correlates against files, telemetry data, and file behavior. LogRhythm then applies scenario and behavioral-based analytics on this data, as well as other log and machine data throughout the environment. Security teams can visualize high-priority events in a dashboard within LogRhythm's centralized console and are empowered to proactively defend against new and emerging threats. Intelligence is further used to help analysts map incidents to MITRE ATT&CK™ techniques, which can assist in the development of mitigation, detection, and response actions.

Use Case: Advanced Malware Detection

Challenge

Malware attacks are growing more frequent and advanced. Some are delivered via email attachments and can evade traditional detection. Once executed, the malware can spread throughout the network, stealing sensitive information as it spreads. Without the proper solutions, it may be hard for security teams to identify and respond to these threats in a timely manner.

Solution

Cisco Secure Endpoint can detect the malicious activity and immediately block the malware from executing. By integrating Cisco Secure Endpoint with LogRhythm, analysts gain greater visibility into endpoint activity and receive alerts and notifications in real time. LogRhythm offers a SmartResponse that allows security teams to isolate the infected computer containing the malware and preventing it from spreading to other systems in the network.

For more information, request a LogRhythm demo.
logrhythm.com/demo