Joint Solution Brief

LogRhythm

Varonis Data Security Platform

Integrating Varonis' data-level visibility across on-prem and cloud apps into LogRhythm SIEM

Benefits

- ✓ Detect and stop suspicious activity, such as abnormal data usage or unauthorized network access
- ✓ Improve threat detection with a prioritized list of risk indicators
- ✓ Reduce false positives with multi-dimensional behavioral analytics
- ✓ Integrate data, user, network, and endpoint activity into a single pane of glass

Solution overview

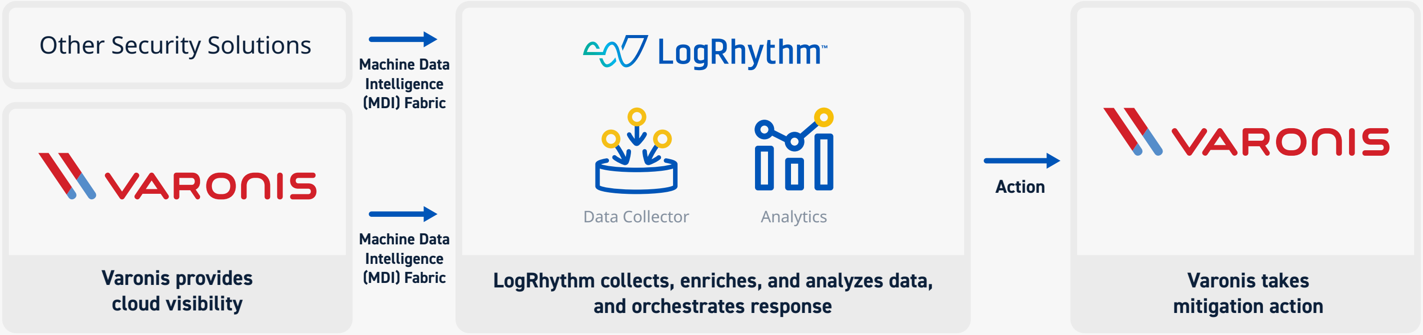
Together, LogRhythm and Varonis offer an integrated solution for comprehensive enterprise security and threat management. LogRhythm's advanced correlation and pattern recognition integrates Varonis' data-level visibility, providing a single pane of glass for comprehensive alerting and investigation.

LogRhythm and Varonis are tightly integrated, combining the value of Varonis' data classification, access intelligence, and data activity monitoring with the threat management capabilities of LogRhythm SIEM. The combined offering empowers customers to identify behavioral anomalies that could indicate internal or external threats and prioritize their response. With both platforms integrated together, security teams have deep visibility into exactly what happened during an incident, down to the level of what data was touched. LogRhythm and Varonis deliver unprecedented intelligence, up-to-date situational awareness, and comprehensive security analytics.

VARONIS

About LogRhythm and Varonis

LogRhythm and Varonis are working together to help protect offline, on-premises, hybrid, or cloud environments against modern cyberattacks. LogRhythm offers extensive support for and integration across Varonis' product portfolio. The combined solution empowers security teams to identify behavioral anomalies, internal threats, and to prioritize their responses based on accurate enterprise security intelligence.


Other Security Solutions
VARONIS
Varonis provides cloud visibility
Machine Data Intelligence (MDI) Fabric
Machine Data Intelligence (MDI) Fabric
LogRhythm
Data Collector
Analytics
LogRhythm collects, enriches, and analyzes data, and orchestrates response
Action
VARONIS
Varonis takes mitigation action

Intelligence collection

LogRhythm continuously collects and analyzes dynamic data captured by Varonis — with rich context from behavior analytics, threat detection, and risk monitoring — and leverages this with petabytes of other machine data to rapidly detect and prioritize high-risk threats and events and enable security teams to neutralize them before they become high-impact incidents or data breaches.

The integration helps analysts analyze and track data, account activity, and user behavior for suspicious activity. This delivers rich context and actionable insight to protect data against insider threats, ransomware, and potential breaches. Correlation between LogRhythm and Varonis alerts enhance the analysis and response process.

How it works

Varonis is a data security platform that protects unstructured data both on-prem and in the cloud from ransomware, insider threats, and cyberattacks. Varonis empowers enterprises to discover overexposed sensitive data and stale data, protect against data breaches, and remediate risk without interrupting business continuity. Varonis proactively identifies security threats with user behavior analytics and data activity monitoring and can reduce the blast radius of a potential attack with automated remediation capabilities.

Both Varonis built-in alerts and custom alerts can be ingested by the LogRhythm SIEM platform. Based on the customer's configuration, risk lists are generated that include malicious indicators, such as IP addresses, domains, URLs, and hashes, which are used for correlation via AI Engine rules. These risk lists of malicious indicators can drastically improve detection in LogRhythm SIEM. With Varonis, LogRhythm users can enrich indicators anywhere in the platform and obtain valuable context around them.

How LogRhythm and Varonis integrate

Syslog data is continually brought in from Varonis into LogRhythm for immediate recognition of user/entity, network, and endpoint behavior involving malicious sources, emerging threats, and indicators of compromise. This provides deep forensic visibility into activity to and from threatening IPs, URLs, and domains that have been identified by Varonis, allowing for the delivery of operational threat intelligence to customers' security controls for real-time monitoring and alerting. Moreover, the integration allows analysts to conduct investigations and generate a variety of reports, such as Alarm and Response Reports and Log Detail Reports.

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