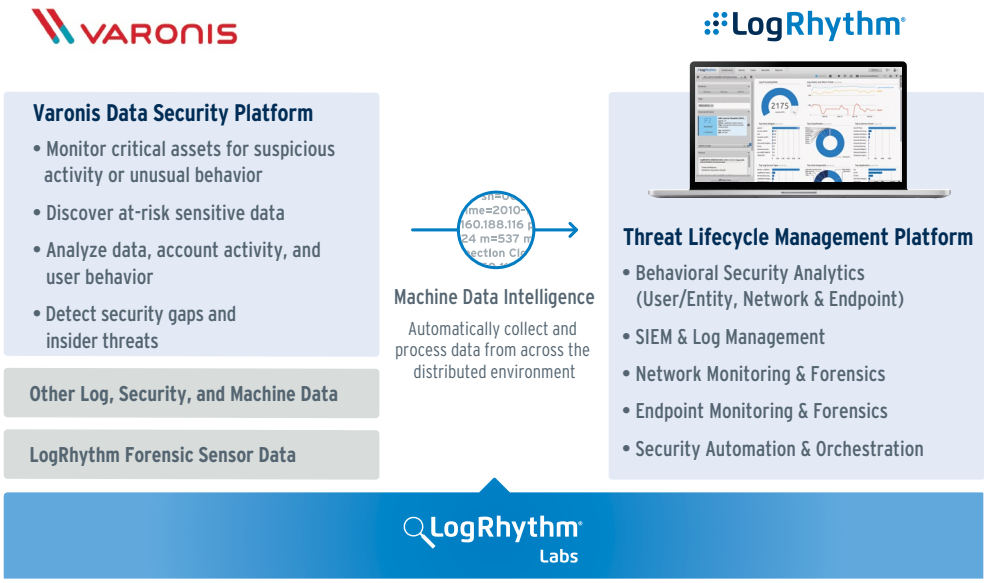
LogRhythm and Varonis: Integrated Enterprise Security

LogRhythm and Varonis have developed an integrated solution for comprehensive enterprise security and threat management. LogRhythm's advanced correlation and pattern recognition incorporates the rich context and threat intelligence that Varonis provides, building a single pane of glass for alerting and investigation. Together, Varonis and LogRhythm deliver unprecedented intelligence, up-to-date situational awareness and comprehensive security analytics.

The Integration Provides:

- Rich context and actionable insight to protect data against insider threats, ransomware, and potential breaches
- Ability to analyze and track data, account activity, and user behavior for suspicious activity
- Correlation between Varonis and LogRhythm alerts, for enhanced analysis and response

LogRhythm continuously collects and analyzes dynamic data captured by Varonis — with rich context from behavior analytics, threat detection, and risk monitoring — and leverages this in combination 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.



About LogRhythm

- Empowers organizations to rapidly detect, respond to, and neutralize damaging cyberthreats with Threat Lifecycle Management
- Unifies data lake technology, machine learning, security analytics, and security automation and orchestration in a single end-to-end solution
- Serves as the foundation for the artificial intelligence-enabled security operations center to secure customers' cloud, physical, and virtual infrastructures for both IT and OT environments
- Consistent market leadership including recognition as a Leader in Gartner's Magic Quadrant since 2012

About Varonis

- Varonis is a Data Security Platform that protects file and email systems from ransomware, insider threats, and cyberattacks
- Empowers enterprises to discover overexposed sensitive data, prioritize vulnerable and stale data, protect against data breaches, and remediate risk without interrupting business
- Identifies security threats by building context around the content of data, performing user behavior analytics, and monitoring file and email activity to protect enterprise data

LogRhythm and Varonis are tightly integrated, combining the value of Varonis' discovery, threat detection, and analytics capabilities with the threat management capabilities of LogRhythm's Threat Lifecycle Management Platform. The combined offering empowers customers to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence.

LogRhythm for Unified Threat Lifecycle Management

- 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

Defend Against Insider Threats

Challenge:
Insider threats pose a significant risk to organizations. They can be challenging to detect, and often takes months to uncover.

Solution:
LogRhythm can incorporate the threat detection capabilities provided by the unstructured data analysis from Varonis to alert security teams to the warning signs of suspicious behavior before it becomes a high-profile incident.

Additional Benefit:
SmartResponse™ plug-ins can be designed to actively defend against insider attacks by initiating actions that disable accounts, revoke access, interrupt sessions, and terminate processes.

Respond, Remediate, and Investigate Cyberattacks

Challenge:
Cyberattacks are continuing to affect enterprises across the globe with devastating effects.

Solution:
Varonis and LogRhythm combine discovery, threat detection, investigation, and response capabilities, enabling security teams to prevent cyberattacks before they can fully realize their objective.

Additional Benefit:
Increased visibility into user data access patterns alongside authentication, endpoint binary, and network activity.