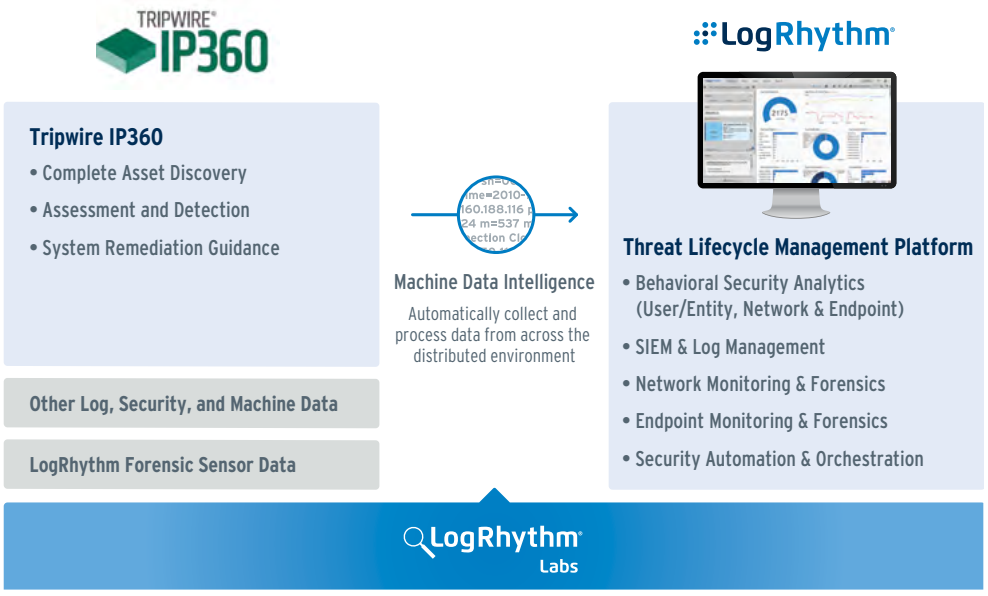
LogRhythm and Tripwire: Integrated Enterprise Security

LogRhythm and Tripwire have developed an integrated solution for comprehensive enterprise security and threat management. LogRhythm automatically incorporates vulnerability data imported directly from Tripwire IP360 via API, delivering real-time cyber threat protection through up-to-date situational awareness and comprehensive security analytics.

The integration allows users to:

- Understand the security risk of your IT environment by automatically identifying assets within defined risk ranges and the applications running on those assets.
- Expose security threats including vulnerabilities, misconfigurations, and exposures; and establish timelines and thresholds for remediation and exceptions.
- Analyze data pertaining to the removal of vulnerable libraries, registry keys, and whether a remediation has taken place.
- Initiate automated responses using Tripwire IP360 risk scoring based on impact, ease of exploit, and age.

By correlating Tripwire IP360's comprehensive vulnerability data with powerful LogRhythm security analytics, customers enjoy comprehensive enterprise security and threat management capabilities. The combination delivers the ability to monitor and secure the entire range of systems and applications across your organization and to respond to security threats based on accurate, relevant, and up-to-date information.



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 Tripwire

- Tripwire is a leading provider of integrity assurance solutions that drive security, compliance, and operational excellence. As the inventor of file integrity monitoring (FIM), Tripwire has a 20-year history of innovation.
- Today, Tripwire helps organizations, including half of the Fortune 500, achieve visibility across their networks, reduce their attack surfaces, and stay on top of suspicious changes – steps considered foundational to system and data integrity.
- Tripwire's award-winning portfolio includes configuration management, file integrity management, asset discovery, vulnerability management, and log collection.

LogRhythm and Tripwire seamlessly integrate to combine the value of a best-of-breed vulnerability management platform with the threat management capabilities of LogRhythm's Threat Lifecycle Management (TLM) 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 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

Protecting Vulnerable Assets

Challenge:
Many organizations don't have the ability to tie current vulnerability data to potential threats and ongoing attacks. This results in a lack of visibility into which threats are immediately relevant, hindering the organization's ability to respond quickly and appropriately.

Solution:
LogRhythm can incorporate the results of Tripwire IP360 vulnerability scans into automated advanced correlation rules. This delivers highly focused alerts that warn when attacks designed to exploit known vulnerabilities are impacting a vulnerable device.

Additional Benefit:
SmartResponse™ plug-ins are designed to actively defend against attacks by initiating actions that mitigate neutralize specific cyber threats. These include adding attacking IPs to firewall ACLs, disabling accounts that may have been compromised and killing suspicious processes and services.

Adaptive Defense

Challenge:
When a security incident takes place, organizations need assurances that the steps they have taken to secure their network have been successful. Performing a vulnerability scan on the entire network in response to any potential incident is inefficient and knowing which devices to scan is difficult.

Solution:
When a security incident or attack has taken place, LogRhythm identifies which devices have been targeted and/or successfully impacted and includes all relevant context in the alarm. Using this context, a SmartResponse plug-in can automatically initiate an ad-hoc vulnerability scan on only the impacted devices.

Additional Benefit:
By automatically adding vulnerable devices to a list, SmartResponse can dynamically adapt LogRhythm alarms to stay up-to-date without manual intervention.