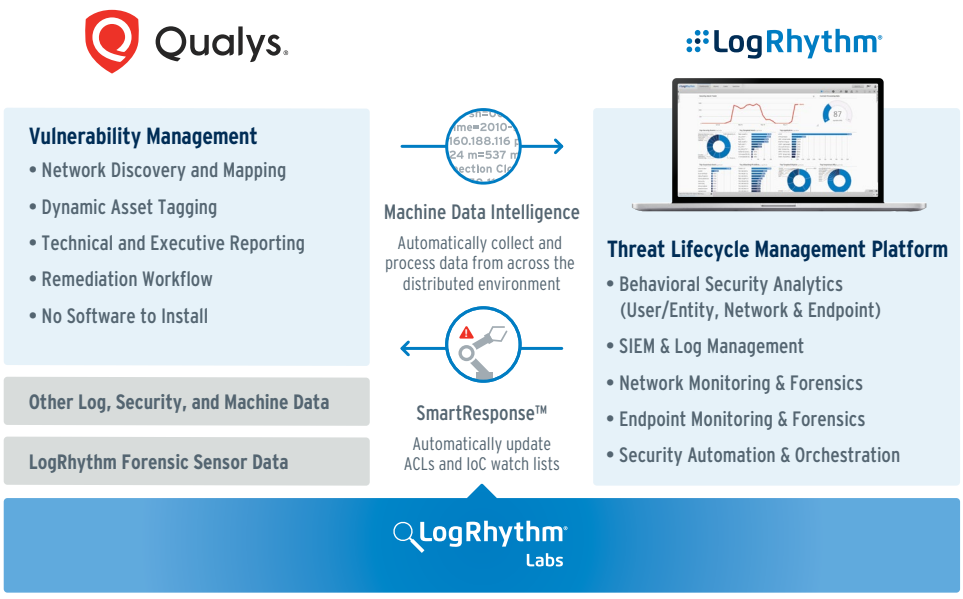
LogRhythm and Qualys: Integrated Enterprise Security

LogRhythm and Qualys have developed an integrated solution for comprehensive enterprise security intelligence and threat management. LogRhythm's advanced correlation and pattern recognition automatically incorporates vulnerability data imported directly from Qualys, delivering real-time cyber threat protection based on up-to-date situational awareness and comprehensive security analytics.

The integration provides:

- Real-time situational awareness via a Qualys Cloud Platform VM feed that identifies and catalogs assets and discovers vulnerabilities at the scale of customers' organizations
- Alarm capabilities that notify users when imported vulnerabilities match preset thresholds
- Normalized Qualys Cloud Platform vulnerability data that can be used in LogRhythm's Threat Lifecycle Management Platform to help users prioritize events

By leveraging Qualys Cloud Platform's open platform and APIs to feed accurate and timely vulnerability data into LogRhythm's Threat Lifecycle Management Platform, customers enjoy industry leading enterprise security intelligence and threat management capabilities. The combination delivers the ability to monitor and secure the entire range of systems and applications throughout the IT environment 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 cyber-threats
- Provides a holistic platform for end-to-end Threat Lifecycle Management, uniquely unifying next-gen SIEM, log management, network & endpoint forensics, advanced behavior analytics & machine learning and security automation and orchestration
- Delivers rapid compliance automation and assurance, and enhanced IT intelligence
- Consistent market leadership, including recognition as a Leader in Gartner's Magic Quadrant since 2012

About Qualys

- Qualys, Inc. is a pioneer and leading provider of cloud-based security and compliance solutions.
- The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds.
- The Qualys Cloud Platform and integrated suite of solutions are used by over 9,300 customers in more than 120 countries, including a majority of each of the Forbes Global 100 and Fortune 100.

LogRhythm and Qualys are tightly integrated, combining the value of best-of-breed vulnerability management 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

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 and which can be ignored, hindering the organization's ability to respond quickly and appropriately.

Solution:
LogRhythm can incorporate the results of Qualys vulnerability scans into automated advanced correlation rules. This delivers highly focused alerts that identify when an attack designed to exploit known vulnerabilities is impacting a vulnerable device.

Additional Benefit:
SmartResponse™ Plug-ins are designed to actively defend against attacks by initiating actions that neutralize specific cyber threats. These include adding attacking IPs to firewall ACLs, disabling accounts that may have been compromised and terminating 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:
SmartResponse can dynamically adapt LogRhythm alarms to stay up-to-date without manual intervention by automatically adding vulnerable devices to a list. Alarms designed to detect vulnerability exploits use those lists to identify legitimate targets for increased accuracy.