PRODUCT OVERVIEW

LogRhythm and BeyondTrust: Integrated Enterprise Security

LogRhythm
The Security Intelligence Company

LogRhythm and BeyondTrust have developed an integrated solution for enterprise security analytics and threat management. LogRhythm automatically incorporates vulnerability data from BeyondTrust's Retina CS to deliver real-time cyber threat protection based on up-to-date situational awareness and comprehensive security intelligence.

The integration delivers:

- Real-time correlation of exposed vulnerabilities including missing patches and configuration weaknesses across the entire IT environment for enterprise threat intelligence
- Increased visibility and enhanced breach detection capabilities through the integration of network security data with multi-dimensional behavioral analysis
- Accurate threat detection by linking meaningful events with conditional logic and current threat analytics to reduce the number of false positives and false negatives

Combining BeyondTrust's vulnerability and threat management capabilities with the multi-dimensional behavioral analytics of LogRhythm's Security Intelligence Platform delivers enterprise-wide continuous monitoring and real-time threat detection and response.

LogRhythm for Integrated Enterprise Security

- ✓ Dynamic defense for protecting vulnerable and exploited assets
- ✓ Multi-dimensional behavioral analytics to deliver real-time security intelligence
- ✓ Focused and automated vulnerability scanning for targeted devices
- ✓ Tight integration for consolidated threat management

LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's award-winning Security Intelligence Platform unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence. LogRhythm delivers:

- Next Generation SIEM and Log Management
- Independent Host Forensics and File Integrity Monitoring
- Network Forensics with Application ID and Full Packet Capture
- State-of-the art Machine Analytics
  - Advanced Correlation and Pattern Recognition
  - Multi-dimensional User / Host / Network Behavior Anomaly Detection
- Rapid, Intelligent Search
- Large data set analysis via visual analytics, pivot, and drill down
- Workflow enabled automatic response via LogRhythm's Smart**Response**™
- Integrated Case Management

BeyondTrust

BeyondTrust is the only security solution vendor providing Context-Aware Security Intelligence, giving customers the visibility and controls necessary to reduce their IT security risks, while at the same time simplifying their compliance reporting.

We empower our customers to protect their infrastructure and data across the entire IT landscape: making every device - whether on a desk or in a data center, in a pocket or a virtual machine, or in the cloud - as secure as possible. Our solutions identify and remediate the vulnerabilities that form the basis for cyber-attacks, and mitigate internal threats that arise from the accidental or intentional misuse of system or device privileges. In short, we protect from both the external and internal threat.

BeyondTrust offers consistent policy-driven vulnerability and privilege management, role-based access control, monitoring, logging, auditing and reporting to protect internal assets from the inside out. The company's products empower IT governance to strengthen security, improve productivity, drive compliance, and reduce expense across physical, virtual, mobile and cloud environments.

LogRhythm and BeyondTrust are tightly integrated, combining the functionality of BeyondTrust's Retina vulnerability management solutions with the threat management capabilities of LogRhythm. The combined offering empowers customers to identify highly corroborated behavioral anomalies, internal and external threats, and prevent breaches based on accurate enterprise security intelligence.

Securing Vulnerable Assets

Challenge With the increasingly sophisticated and rapidly evolving threat landscape, organizations must be able to bridge the gap between current vulnerability data and ongoing attacks in order to gain true enterprise security intelligence.

Solution LogRhythm combines data from BeyondTrust's Retina CS vulnerability scans with other machine data for advanced correlation and pattern recognition. High-priority alarms are generated when an attack designed to exploit a known vulnerability is targeting a vulnerable system.

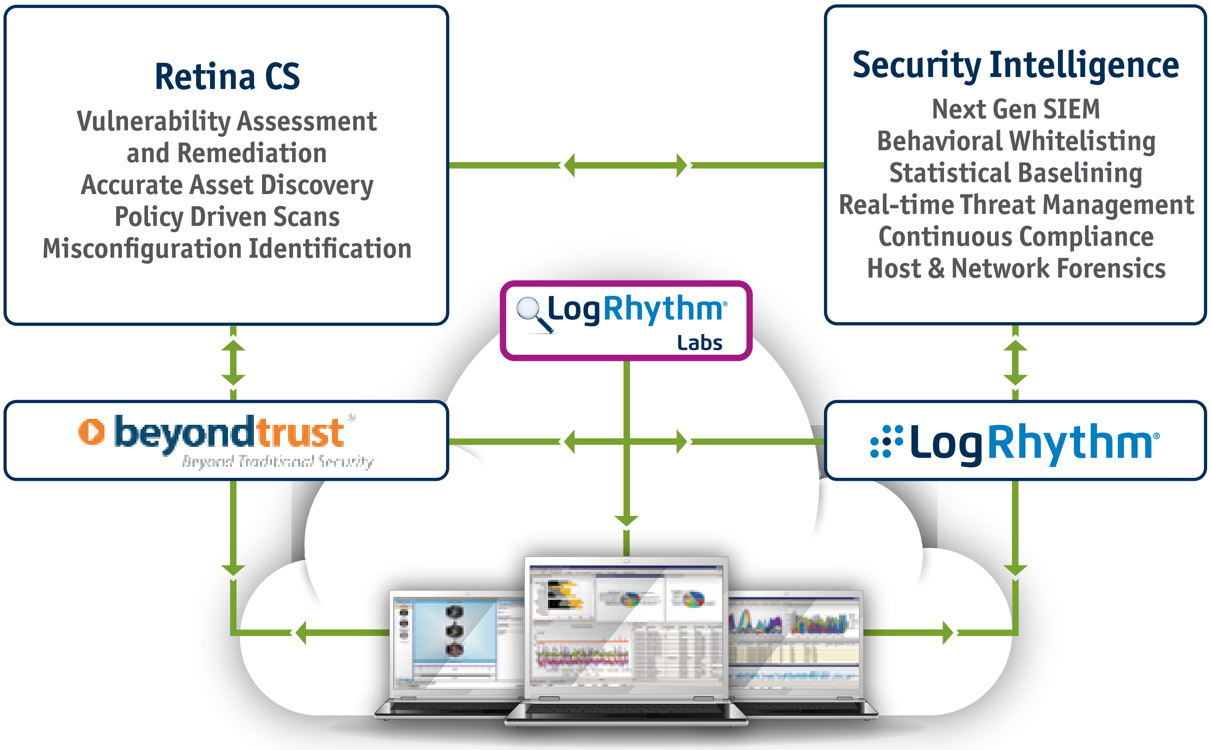
Additional Benefit Smart**Response**™ plug-ins can initiate immediate protective action by isolating the vulnerable system to prevent the attack from spreading within the environment.

Risk Management

Challenge The rapid adoption of mobile devices, cloud applications and virtualized environments adds additional complexity to security and risk management. Among the challenges is identifying weaknesses within a network that attackers would exploit to get to the desired target or data.

Solution Retina CS is a unified platform that captures and reports on privilege and vulnerability data across the entire IT environment. LogRhythm correlates this data with other machine data and applies behavioral analytics to identify abnormal behavior and suspicious activity within the network.

Additional Benefit LogRhythm's AI Engine can automatically profile behavior to build whitelists of acceptable activity for applications, hosts and networks, helping reduce the time it takes to identify suspicious activity and prioritize vulnerable systems.



Retina CS

Vulnerability Assessment and Remediation
Accurate Asset Discovery
Policy Driven Scans
Misconfiguration Identification

Security Intelligence

Next Gen SIEM
Behavioral Whitelisting
Statistical Baselining
Real-time Threat Management
Continuous Compliance
Host & Network Forensics

Realtime Monitoring

Advanced Alerts

SmartResponse™

Visualization

Forensics/Analytics

Reporting