



Editorial Contact:
Marc Gendron
(781) 237-0341
marc@mgpr.net

NEWS RELEASE

FOR IMMEDIATE DISTRIBUTION

LogRhythm Extends Standard for SIEM 2.0 with LRX Product Line

Log Deduplication, Active Directory Integration, and New Appliances Establish New Benchmark for Total Performance and Usefulness

BOULDER, Colo., Sep. 30, 2009 – [LogRhythm](#), the company that makes log data useful, today announced its new LRX line of integrated [log and event management](#) appliances. The LRX line enables organizations to process billions of logs per day while extracting fine-grained security, compliance, and operational intelligence. By combining new Log Deduplication™ technology, a 64 bit architecture, and deep Active Directory integration with powerful new LRX appliances, LogRhythm raises the bar for [SIEM 2.0](#) capabilities that it established in 2004 with the release of the first integrated log and event management solution.

Log Deduplication: Stemming the Log Deluge

The collection, normalization, and analysis of [log data](#) is now a requirement for compliance with most regulatory mandates and is a critical component of in-depth security strategies. With organizations generating hundreds of millions of logs per day, a manual or homegrown approach is no longer feasible. The acuteness of the challenge is captured by the SANS institute estimate that up to 25% of all enterprise data can be log data. To help organizations crunch mountains of log data and detect key events in real-time, LogRhythm's new LRX line of appliances feature new [Log Deduplication](#) technology and 64 bit performance. Using Log Deduplication, LogRhythm LRX appliances efficiently handle redundant data to significantly reduce storage requirements and costs while delivering lightning fast searches. Organizations can keep all of their log data, while reducing storage overhead by up to 90 percent. Furthermore, the LRX line

delivers new levels of performance, analysis, and correlation of network flow data and host data.

“The implementation of LogRhythm throughout our global organization has paid off in real and measureable ways. It has saved us from the flaw-ridden approach of manually wading through millions of log entries daily, and reduced operational costs in terms of man-hours spent investigating problems,” said Michael Chapman, Director, Digital Security and Network Operations at Ascent Media. “We use LogRhythm for security investigations, regulatory compliance assurance, and identifying trends in our infrastructure which would have been very difficult, if not impossible, to glean via any other means. LogRhythm has set the standard for SIEM 2.0. We are looking forward to deploying the new features in the 5.0 release, especially de-duplication and Active Directory integration, which will be valuable innovations for us.”

Active Directory Integration Delivers New Insights into User Activity

To help provide early detection of [insider threats](#) and other suspicious user activity, LogRhythm has supplemented its User Activity Monitoring capabilities to include deep integration with Active Directory (AD). By automatically synchronizing with AD domains and sub-domains, LogRhythm provides visibility into actions by AD Users, Groups and Group Members. In addition, AD group filters can be applied for searches, alerts, and other analysis functions to help organizations detect and protect against suspicious activity by employees, contractors, and other trusted users with access to network resources.

Delivering SIEM 2.0

LogRhythm led the move to the new generation of [SIEM](#) in 2004 when it introduced the first fully integrated enterprise-class Log and Event Management solution for security, compliance, operations and business intelligence applications. The company has continued to lead the way in defining and delivering second generation SIEM solutions that customers are looking for, characterized by:

- Fully integrated Log Management, [Log Analysis](#) and Event Management
- Enhanced network, host and data awareness through [File Integrity Monitoring](#), Network Flow Analysis, and [Endpoint Monitoring](#) & Control
- User Activity Monitoring across all network, host and application layers
- Ease of Use, Implementation, and Support

- Next generation analytics, search, and forensics
- A highly scalable building blocks architecture
- A focus on total performance that addresses collection, processing, search, alerting, reporting, restoration, and forensics
- A design architected to be extensible for multiple applications and uses

“Logs represent the digital fingerprints of activity that occurs within an organization’s IT infrastructure. They are the single richest source of data for understanding what is happening at the network, system, and application layer as it affects security, compliance and operations,” said Chris Petersen, co-founder and CTO of LogRhythm. “However, first generation log management and SIEM products lack the integration, performance, and “full stack” monitoring capabilities required to deliver the full potential of this technology platform. With the LogRhythm LRX line, we are delivering what customers want in a SIEM 2.0 product – a single integrated solution that provides unprecedented visibility across the entire IT stack. Our log and event management platform, combined with file integrity monitoring, user activity monitoring, data leak protection and network flow analysis provides the end-to-end analysis capabilities required to monitor and protect today’s ever changing and often targeted networks.”

SIEM 2.0 Trade Up Offer

To help organizations transition from legacy first generation SIEM products to the next generation capabilities of the LRX family, LogRhythm is offering a trade-up program. The LogRhythm SIEM 2.0 Trade Up offer enables enterprises to purchase LogRhythm appliances by reallocating budget dollars currently slotted for maintenance, support and upgrades of their legacy SIEM 1.0 solution.

Pricing and Availability

LogRhythm LRX appliances are available immediately with prices starting at \$25,000.

About LogRhythm

LogRhythm provides enterprise-class log and event management, file integrity monitoring, and endpoint monitoring & control in a single integrated solution that empowers organizations to comply with regulations, secure their networks, and optimize IT operations. The company received the 2009 SC Magazine Readers Trust Award for [best SIEM](#) solution, is a Colorado Company to Watch for 2009, a finalist for the 2009 Red Herring 100 Award, and received the SC Magazine 2009 Best Buy for [digital](#)

[forensics](#) products. LogRhythm is privately held and based in Boulder, Colorado with European Headquarters in Maidenhead, England, and Asia Pacific operations in Hong Kong. For more information visit: www.logrhythm.com.

#