

# Log Management and SIEM 2.0. File Integrity Monitoring. Network and User Monitoring. **ONE INTEGRATED SOLUTION**

LogRhythm is an enterprise-class platform that seamlessly combines Log Management & SIEM 2.0, File Integrity Monitoring, and Network & User Monitoring into a single integrated solution. It is highly reliable and cost-effective, and can scale to fit the needs of any enterprise. With LogRhythm, you can invest in a single solution to address requirements and challenges throughout your organization, whether they are related to compliance, security or IT operations.

A wealth of valuable information can be derived from log data – whether it originates in applications, databases, servers, network devices or endpoint systems. By automating the collection, organization, analysis, archiving and reporting of all log data, LogRhythm enables organizations to easily meet specific requirements, whether driven by internal best practices or one of many compliance regulations. LogRhythm delivers valuable, timely and actionable insights into security, availability, performance and audit-related issues.

LogRhythm’s unique and comprehensive solution empowers our customers to centralize, simplify, and strengthen their capabilities with compliance, security and IT operations.

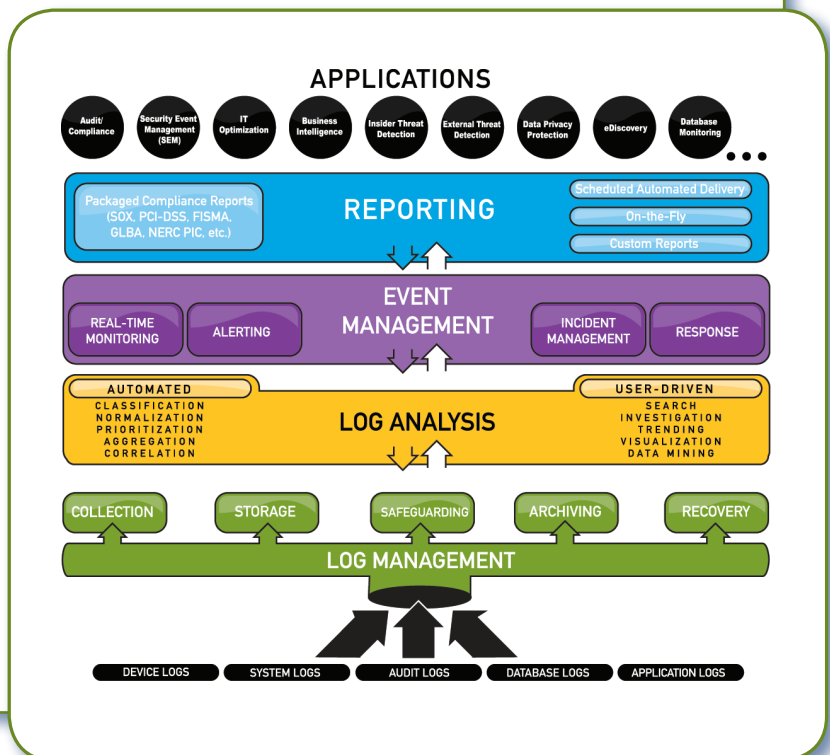
## Increased Protection and Greater Compliance Assurance in One Solution

LogRhythm delivers unprecedented awareness and insight into what’s happening on your network, from routers to host systems to endpoint devices, both inside and outside the network. Comprehensive log and event information is combined with specific user activity data – from end-users to administrators, and privileged insiders to external bad guys. LogRhythm delivers a complete view into what events are happening when, and provides rapid access to detailed information about who or what is responsible for the event, and the extent of its impact.

Most organizations face regulatory requirements for log management, event management, file integrity and privileged user monitoring. Whatever the driver – PCI-DSS, SOX, HIPAA, FISMA, NERC CIP, GLBA, GCSx, GPG13, etc – organizations face huge challenges in meeting these requirements easily, efficiently, and affordably. The cost of acquisition, deployment and ongoing management of disparate solutions, even if they are offered by one vendor, is substantial. That’s where LogRhythm comes in.

By fully integrating Log Management & SIEM 2.0, with File Integrity Monitoring and Network & User Monitoring in one solution LogRhythm enables customers to:

- Reduce acquisition costs
- Simplify ongoing management
- Decrease the “Time-to-Comply”
- Increase the collective value derived from their solution



## One Integrated Solution

### Log Management & SIEM 2.0

- Automatically centralize & archive ALL logs
- Real-time event monitoring & alerting
- Powerful analytics & trending
- Automated reporting
- Real-time correlation & forensic investigations
- High-performance, scalable & easy-to-use
- Performs log deduplication for enterprise-wide data reduction

### File Integrity Monitoring

- Monitors ALL types of files and directories in near real-time
- Provides "user-aware" context to file changes
- Automated alerting on changes to critical files
- Fine-grained controls & filters
- Out-of-the-box support for common operating systems & applications
- Tracks user access/modifications of confidential files

### Network & User Monitoring

- Monitors network and host connections
- Monitors what processes/services are running on key systems
- Provides interactive correlation of data related to the user, host, application, port, etc.
- Alerts & reports on the misuse of privileged user access
- Provides an independent audit of user behavior across the entire IT stack

Intelligent IT Search. Pre-packaged Compliance Reports, Alerts & Investigations.  
Fully Integrated. Centralized Management Console.

## Turnkey Appliance Solutions

While LogRhythm is available as software-only, LogRhythm appliances provide turnkey, scalable solutions for enterprises of all sizes. All software is pre-installed, configured and ready to go.

LogRhythm appliances come in a variety of models including High Availability solutions that support business continuity and information assurance for LogRhythm deployments. Because of LogRhythm's distributed, incrementally scalable architecture, deployments can start with a single appliance and scale from there by simply adding appliances. Regardless of the performance, storage or geographic requirements, LogRhythm is architected for flexible and efficient expansion.

To find out which LogRhythm solution best fits your needs, contact us at [info@logrhythm.com](mailto:info@logrhythm.com).



LRX2 model shown

"LogRhythm provides a single view into all log and event data. Having meaningful data in one place empowers me to act quickly and precisely with appropriate security measures."

*Bernie Rominski*  
IT Security Officer  
Regis Corporation

"LogRhythm has set the standard for SIEM 2.0 and as such, has proven to be an invaluable tool for Ascent Media's global security operations."

*Michael Chapman*  
Director Digital Security and Network Operations  
Ascent Media

### LogRhythm Headquarters

3195 Sterling Circle  
Boulder, CO  
80301  
303-413-8745

### LogRhythm EMEA

Siena Court, The Broadway  
Maidenhead Berkshire SL6 1NJ  
United Kingdom  
+44 (0) 1628 509 070

### LogRhythm Asia Pacific Ltd.

8/F Exchange Square II  
8 Connaught Place, Central  
Hong Kong  
+852 2297 2812