PRODUCT OVERVIEW

Log Management | See what you're missing. Federal Security Intelligence

LogRhythm
The Security Intelligence Company

LogRhythm's comprehensive log management solution helps federal organizations comply with a myriad of regulations (FISMA, NERC CIP, HIPAA, DoDI, NIST CSF, etc.) and combat cyber threats. It is an enterprise-class platform that seamlessly combines Log Management, File Integrity Monitoring, Host Activity Monitoring, and Network Forensics into a single integrated solution. LogRhythm addresses an ever-changing landscape of threats and challenges with a full suite of high-performance tools for security, compliance, and operations. It delivers comprehensive, useful and actionable insight into what is really going on in and around an enterprise IT environment. LogRhythm's platform delivers:

- Fully Integrated Log & Event Management
- Multi-dimensional Big Data Security Analytics
  - Advanced Correlation & Pattern Recognition
  - Automated Behavioral Whitelisting
  - Statistical Baselining
- Extended Visibility and Context
  - Independent Host and Network Monitoring
  - File Integrity Monitoring
  - Enterprise-wide Network Visibility
- Powerful, Rapid Forensics
- Intelligent, Process-Driven Smart**Response**™
- Ease-of-use and Simplified Management
- Common Controls for Rapid Adoption

Federal Certifications

LogRhythm has obtained its
Certificate of Networthiness (CoN# 201416842),
FIPS 140-2 (FIPS# 1817)
Common Criteria certification (VID# 10389)
DADMS (#91947)
CHESS

One Integrated Solution

Adaptable Continuous Monitoring for Risk Management

- Real-time event monitoring & alerting
- Advanced correlation & pattern recognition
- Real-time Big Data Security Analytics
- Centralization & secure archiving of ALL logs
- Automated, comprehensive reporting for third party auditors
- High-performance, scalability & ease-of-use
- Comprehensive support for network and security devices, servers, operating systems and applications.
- Smart**Response**™ remediation for Continuous Management
- Multi-dimensional Behavioral Analytics

Compliance Automation and Assurance

- Direct alignment to NIST guidelines for log management
- Automated third-party security authorization with out of the box support for multiple regulations (FISMA, DoDI, HIPAA, NERC CIP, etc.)
- Automated alerting on compliance violations
- Fully integrated log and event management to address multiple components of the CAESARS Framework
- Embedded Expertise by LogRhythm Labs for continuous updates to built-in compliance packages
- Comprehensive packages for operating best practices and continuous compliance

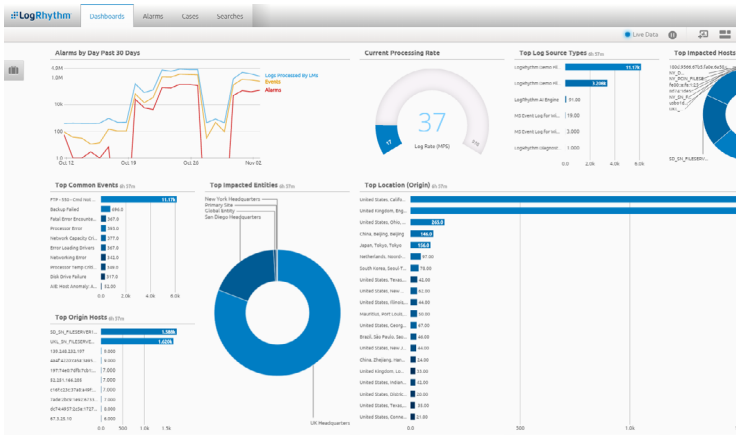
Protection from Advanced Persistent Threats

- Identification, monitoring and protection of targeted assets and data
- Establish behavioral profiling and monitor for suspicious activity
- Alerting & reporting on the misuse of privileged user access to protect against insider threats and stolen credentials
- Monitoring of removable media with active response to prevent data loss
- Independent monitoring of file integrity and host activity for extended visibility and endpoint protection
- Out-of-the-box Smart**Response**™ Plug-ins for active defense from APTs
- Automated behavioral whitelisting of acceptable activities by users, hosts, applications, etc.

Designed for Practical, Everyday Use

A wealth of valuable information can be derived from log data – originating from applications, databases, servers, network devices or host systems. LogRhythm enables organizations to detect and respond to advanced threats, automate compliance assurance and intelligently optimize IT operations by automating the collection, organization, analysis, archiving and reporting of all log data. By fully integrating Log Management with File Integrity Monitoring, Host Activity Monitoring, and Network Forensics into one solution LogRhythm helps government organizations:

- Expand and accelerate threat detection & response capabilities
- Reduce acquisition costs and management overhead
- Automate compliance
- Establish an effective continuous monitoring program



It is cost-effective, easily deployed, scales to fit the needs of any organization, and is operated and managed through an easy-to-use, wizard-driven console. With LogRhythm, customers can invest in a single solution to address security, compliance, and operations issues related to requirements and challenges throughout their IT organizations.

Flexible Deployment Options

LogRhythm can be implemented in any combination of hardware, software and virtual instances. It is designed to meet the deployment requirements of any enterprise and scaling is as simple as plugging in additional appliances as requirements expand. True High Availability (HA) exists at all layers of the product including collection, processing and event management.

LogRhythm offers support for VMware ESX, Microsoft Hyper-V, Amazon EC2, and Citrix XenServer. High Availability with automatic failover is also available.

Strategic Technology Integration

LogRhythm integrates with an extensive array of third party security technologies to deliver comprehensive and dynamic cyber threat defense and compliance automation. This includes collecting and correlating data from focused security products (vulnerability management, IDS/IPS, AV/AM, DPI, etc.) and two-way communication with strategic security and compliance technology solutions (SIEM, GRC, DLP, HBSS, etc.).

Classified Environments

LogRhythm is architected to support unidirectional communication for operating within classified environments

- Integration with one-way Data Diodes
- Fully-encrypted communication for secure collection
- Multi-tenant architecture for logical data segregation
- Granular role-based access controls
- Standard STIG documentation for any deployment

"Our organization uses LogRhythm to comply with FISMA and NIST security controls. LogRhythm collects and centralizes log data and provides e-mail alerting and reporting on security events."

System Administrator, State & Local Government
Source: TechValidate. TVID: B7A-E82-DCE

"LogRhythm makes quick work of digging through system logs...a quite extensive log management, analysis and event management solution for pretty much any size of network."

GCNLAB TEST

©2014 LogRhythm Inc. | LogRhythm_Log_Management_Federal_Security_Intelligence_Datasheet_12.14