PRODUCT OVERVIEW

LogRhythm Verticals

The number of industries hosting high-profile, confidential data on frequently accessed and increasingly vulnerable networks means that the demand for true security intelligence has never been greater. LogRhythm's unified Security Intelligence Platform combines enterprise-class SIEM, Log Management, File Integrity Monitoring and Machine Analytics, with Host and Network Forensics. Organizations spanning a multitude of verticals are turning to LogRhythm to secure their networks, meet compliance requirements, and obtain actionable insight into their IT environments. High-level benefits include:

- Integrated File Integrity Monitoring to ensure protected and confidential information is not changed or inappropriately modified
- Enterprise-wide user activity monitoring to identify insider threats, compromised credentials and misuse of privileged accounts
- Embedded expertise via purpose-built Security Analytics Suites designed to address specific security challenges
- Compliance automation assurance with real-time alerts, out-of-the-box reports and advanced correlation rules

Banking and Finance:

LogRhythm helps financial institutions increase fraud detection and prevention while meeting compliance requirements through industry leading advanced analytics, automated behavioral analysis, and pattern recognition.

- Integrated File Integrity Monitoring to detect suspicious access, deletion and modification to confidential data
- Privileged User Monitoring to identify improper usage of authorized and compromised credentials.
- Industry leading archiving capabilities with digital chain of custody
- Out-of-the-box Compliance Automation Suites for PCI DSS, SOX and GLBA with comprehensive reports, forensic investigations and real-time alerts that map directly to specific mandates

> "We are using LogRhythm for real-time event monitoring, forensic research, alerting on security events, monitoring of user activity, and compliance reporting."
>
> **Security Manager**
> **Large Enterprise Banking Company**
>
> *Source: TechValidate. TVID: B0B-962-F1A*

Retail and Hospitality:

LogRhythm delivers comprehensive solutions for retailers and other enterprises to protect customer credit card information and meet compliance requirements.

- Retail Cyber Crime Security Analytics Suite with embedded correlation rules, reports, alarms and investigations designed to monitor the credit card processing environment
- Superior collection capabilities for remote retail locations with custom support for point-of-sale (POS) systems
- Fully integrated File Integrity Monitoring to detect suspicious access, deletion and modification to confidential data
- Out-of-the-box Compliance Automation Suite for PCI DSS

> "LogRhythm provides in-depth enterprise wide visibility so we can focus on exception based management rather than trying to watch it all ourselves. This allows our staff to focus on other important security matters.
>
> It also enforces several key controls aspects of our SOX and PCI audit requirements with alarm response reports to track our follow up to any alarm event and is used for reporting for an audit period as evidence of our tracking. It really simplifies things."
>
> **Security Manager**
> **S&P 500 Consumer Services Company**
>
> *Source: TechValidate. TVID: 7C2-0B0-599*

Energy and Utilities:

Using LogRhythm, Energy and Utilities organizations are able to better protect high-profile, critical infrastructures from advanced threats while meeting industry regulations.

- Comprehensive collection to meet industry specific requirements including secure remote collection for substations and collection from SCADA devices
- One-way communication capabilities for classified network segments.
- Integration with Data Historians
- Out-of-the-box Compliance Automation Suite for NERC CIP, NEI, and NRC

> "The LogRhythm deployment will be at the heart of our isolated networks, providing a centralized location to detect changes in our most secure networks."
>
> **IT Professional**
> **Large Enterprise Energy & Utilities Company**
>
> *Source: TechValidate. TVID: F95-691-44D*

Higher Education:

LogRhythm enables higher education institutions to secure confidential student data, optimize IT operations and meet compliance requirements through powerful machine analytics and embedded expertise.

- Proactive protection and real-time monitoring of extended networks with multiple segments
- Out-of-the-box Compliance Automation Suite for HIPAA and PCI DSS
- Flexible architecture options and specific higher education discounts available

> "LogRhythm gives us the ability to actually digest the huge volume of logs across the server infrastructure, and to identify and react to suspicious activity in real time."
>
> **Security Manager**
> **Educational Institute**
>
> *Source: TechValidate. TVID: 69D-9D4-CFA*

Healthcare:

LogRhythm helps healthcare organizations secure patient data, improve visibility into different log sources from EHR/EMR platforms, and comply with industry regulations.

- Comprehensive, secure collection and archiving from integrated ePHI platforms
- 2014 Edition Ambulatory (#IG-3201-14-0027) and Inpatient (#IG-3201-14-0028) Modular EHR ONC HIT Certification to support Meaningful Use
- Out-of-the-box Compliance Automation Suite for HIPAA and HITECH

> "We use LogRhythm with HIPAA compliance, user password issues, log collection from audit focused systems, database logs, and malware outbreak detection."
>
> **Senior IT Architect**
> **Large Enterprise Health Care Company**
>
> *Source: TechValidate. TVID: 572-586-256*

ONC Certified HIT℠

Government:

LogRhythm delivers continuous monitoring, robust collection capabilities, and continuous compliance assurance to federal organizations.

- Fully integrated log management and SIEM
- Secure, remote collection for geographically dispersed networks
- Out-of-the-box Compliance Automation Suite for FISMA, DoDI, NERC CIP, NIST etc.
- Certificate of Networthiness from the US Army (CoN# 201210344), FIPS 140-2 (FIPS# 1817) and Common Criteria certification (VID# 10389).

> "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: 572-586-256*

Common Criteria · U.S. ARMY · FIPS 140-2 CRYPTOGRAPHY