LogRhythm SIEM Platform

Gain unmatched visibility, protection, and threat detection across all surface areas, systems, and assets

For organizations that require an on-prem solution due to regulatory requirements or IT preference, the LogRhythm SIEM Platform is the industry's most complete platform, providing the latest security functionality and analytics. With LogRhythm SIEM, your team has embedded modules, dashboards, and rules that help you quickly deliver on the mission of your security operations center (SOC): threat monitoring, threat hunting, threat investigation, and incident response at a low total cost of ownership.

Benefits

- **Prevent:** Reduce your cybersecurity exposure
- **Detect:** Eliminate blind spots across your environment
- **Respond:** Shut down attacks and limit damage and disruption
- **Find your fit:** Flexible deployment options

Problems we solve

Log management

Swiftly search across your organization's vast data to easily find answers, identify IT and security incidents, and quickly troubleshoot issues.

Security analytics

Don't get bogged down in meaningless alarms. With advanced machine analytics, your team will accurately detect malicious activity through security and compliance use case content and risk-based prioritized alarms that immediately surface critical threats.

UEBA

Detect anomalous user behavior before data is corrupted or exfiltrated with user and entity behavior analytics (UEBA).

SIEM

Detect and respond to threats measurably faster. With the LogRhythm SIEM Platform operating as your team's command center, your security operation will become more effective and efficient through automated workflows and accelerated threat detection and response capabilities.

SOAR

Work smarter, not harder. Collaborate, streamline, and evolve your team's security maturity with security orchestration, automation, and response (SOAR) that is embedded in the LogRhythm SIEM and integrates with more than 80 partner solutions.

Build a resilient defense

LogRhythm has assembled the world's most capable and respected ecosystem of people and partners to help your team build a resilient defense at the cutting edge of cyber technology.

LogRhythm Labs

Nobody understands adversaries better than we do. Our LogRhythm Labs team proactively analyzes emerging threats from all corners of the web and builds rules, dashboards, reports, and compliance modules to give your organization the upper hand.

Security maturity

With two decades of experience in cybersecurity, LogRhythm brings together the most complete technology to help you improve your security posture. With our Security Operations Maturity Model (SOMM), we help you set a baseline and then we create a plan to achieve your security goals together.

Preferred by security pros

Most cybersecurity tools are complicated, clunky, and frustrating to use. The LogRhythm SIEM Platform is easy to set up and use, letting your analysts see the entire threat landscape and a timeline of events. We help busy and lean security teams save the day without the frustration.

Services to support your team

When you work with LogRhythm, you have a team of experts available to help you with your security goals. We offer targeted services to help you achieve expert-level status and improve your organization's security maturity.

The LogRhythm-powered SOC includes our SIEM solution and security use case content from LogRhythm Labs, all supported by the real-world expertise of our Customer Success team.

Out-of-the-box value

The LogRhythm SIEM Platform simplifies work and decreases mean time to detect (MTTD) and mean time to respond (MTTR) by enabling security operations across the threat lifecycle:

- **Collect**: Gather, normalize, and interpret data from more than 950 third-party products and cloud sources
- **Discover**: Choose from over 1,100 preconfigured, out-of-the-box correlation rule sets and use a wizard-based drag-and-drop GUI to create and customize rules for your environment
- **Qualify**: Use prebuilt threat analytics, Threat Intelligence Service feeds, and risk-based prioritization to focus your efforts
- **Investigate**: Optimize and standardize your analysts' workflow with case management, playbooks, and metrics
- **Neutralize**: Choose from fully automated playbook actions or semi-automated, approval-based response actions that allow users to review before countermeasures are executed
- **Recover**: Streamline the compliance process with our Consolidated Compliance Framework that provides reporting for dozens of regulations

Robust support for log sources and data collection

The LogRhythm SIEM offers out-of-the-box support for 1,000 log sources, with the ability to ingest custom log sources, ensuring that all network log data can be collected and analyzed for threat behaviors.

Analytics modules

Prebuilt analytics modules contain models and alarms that recognize known patterns and characteristics of bad behavior, whether from malicious outsiders or insider threats.

Alarm prioritization

Threat prioritization scores and prioritizes alarms based on risk.

Case management

Case management improves compliance with federal regulations by centralizing collaborative incident management and evidence collection.

Prebuilt playbooks

The LogRhythm SIEM Platform features pre-built playbook atuomation actions that provide critical threat context, case grouping, and fast triage to keep you focused on incident response.

Automated response

LogRhythm SmartResponse™ integrates LogRhythm's platform with our network of Technology Alliance Partners, enabling faster incident response.

Simplified compliance

LogRhythm's comprehensive library prebuilt compliance and threat detection modules are unmatched. By automatically detecting violations as they occur the burden of manual reviews is removed. Compliance content, including rules, investigations, and reports are mapped to the individual controls for each regulation.

Deployment options

Our flexible deployment options ensure that you get the best fit for your organization — no matter if you deploy to the data center or cloud.

Software offerings can be pre-deployed in the data center on a LogRhythm server or on your preferred server or virtual machine with appropriate specs. In addition, our SIEM experience is also provided with the ease and flexibility of our SaaS offering. Data collectors can be deployed on-premises and in the cloud.

Which deployment option is right for you?

Capability	LogRhythm SIEM Platform	LogRhythm Cloud SIEM
Managed infrastructure	✗	✓
Managed software updates	✗	✓
Managed knowledge base updates	✗	✓
Knowledge base	✓	✓
User and entity behavior analytics (UEBA)	✓	✓
Network detection and response (NDR)	✓	Partial[1]
Entity, network, and host management	✓	✓
AI Engine rule creation	✓	✓
REST API access (internal)	✓	✓
Active directory integration	✓	No[2]
Single sign-on (SSO)	✓	✓
Full log collection	✓	✓
Data archiving	✓	✓
Reporting	✓	✓
Case management	✓	✓
High availability	✓	N/A
Disaster recovery	✓	N/A
Web console	✓	✓
Custom dashboards	✓	✓
Message Processing Engine (MPE) rule creation	✓	✓
SmartResponse	✓	Yes, from agent
Playbooks	✓	✓
Log Distribution Services (LDS)	✓	✗

[1] LogRhythm Cloud integration with on-premise network monitors to retrieve PCAPs in the web console is not supported.

[2] Windows Host Wizard and Lists based on AD Groups in LogRhythm Cloud require available workarounds. User management via AD sync has moved to single sign-on in LogRhythm Cloud.

Ready to defend.

LogRhythm helps busy and lean security operations teams save the day—day after day. There's a lot riding on the shoulders of security professionals. LogRhythm helps lighten this load. As allies in the fight, LogRhythm combines a comprehensive and flexible SIEM platform, technology partnerships, and advisory services to help SOC teams close the gaps.

Learn more at logrhythm.com and schedule a demo today!

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 2 8019 7185

www.logrhythm.com