

LogRhythm SIEM

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



For organizations that require a self-hosted solution due to regulatory requirements or IT preference, [LogRhythm SIEM](#) is the industry's most complete platform, providing the latest security functionality and analytics. LogRhythm SIEM offers 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.

LogRhythm SIEM streamlines incident investigation and response through a visual analyst experience. Analysts see an entire security story about a user or host helping your team quickly investigate and respond to threats. LogRhythm SIEM provides the details you need to investigations and shut down attacks before serious damage occurs.

LogRhythm supports different collection mechanisms. LogRhythm features a JSON parsing engine embedded within LogRhythm's [System Monitor \(SysMon\)](#), the SIEM's collection mechanism. The new engine, which is compatible starting with LogRhythm version 7.13, ingests cloud-native log sources significantly faster and can collect thousands of messages per second. And now LogRhythm offers unlimited System Monitors, making scaling easy and at no additional cost.

Out-of-the-box Value

LogRhythm SIEM 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.

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

Protect against insider threats with LogRhythm's embedded deterministic [user and entity behavior analytics \(UEBA\)](#) monitoring. To detect anomalies using machine learning, leverage LogRhythm UEBA, our advanced analytics UEBA solution.



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 LogRhythm SIEM and integrates with more than 80 partner solutions.



Endpoint Monitoring

Fulfill security and compliance use cases by supplementing traditional log collection with rich host activity data from data collection and endpoint monitoring.

How We Help

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. LogRhythm SIEM 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 meet security operational goals and save time.

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.

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 as a self-hosted option or in the cloud.

Which Deployment Option is Right For You?

Capability	 Self-Hosted SIEM	 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	⊙	⊗ 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	⊙	⊙ – from agent
Playbooks	⊙	⊙
Log Distribution Services (LDS)	⊙	⊗

¹ LogRhythm Cloud integration with self-hosted 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.

* LogRhythm UEBA and LogRhythm NDR are add-on components to the SIEM.

 Request a demo today: logrhythm.com/demo