

LogRhythm SIEM

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, [LogRhythm SIEM](#) is the industry's most complete platform, providing the latest security functionality and analytics. LogRhythm SIEM offers embedded modules, dashboards, and 1 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 investigate and shut down attacks before serious damage occurs.

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.



SIEM

Detect and respond to threats measurably faster. With LogRhythm SIEM 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 LogRhythm SIEM and integrates with more than 80 partner solutions.