Ready to Defend

LogRhythm™

Your ally in cybersecurity.

LogRhythm helps busy and lean security operations teams protect critical information and infrastructure from emerging cyberthreats. As allies in the fight, we combine a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help 4,000+ security operations center teams close gaps.

We understand there's a lot riding on the shoulders of security professionals—the reputation and success of your company, the security of customer data, the availability of critical systems—the weight of protecting the world. LogRhythm helps lighten this load.

Our people are on the frontlines defending against many of the world's most significant cyberattacks. Based on these experiences, we've built the industry's most comprehensive platform, emboldening security teams to navigate the threat landscape with confidence. Together, LogRhythm and our customers are **ready to defend**.

Your most resilient defense.

LogRhythm is built to provide unmatched visibility, protection, and threat detection across all surface areas, systems, and assets.

Prevent

Reduce your cybersecurity exposure

- Introduce and support a security operations maturity model (SOMM) across your organization's internal and external systems
- Be more vigilant against threats across remote and hybrid work environments
- Ensure security compliance across vulnerable touchpoints

Detect

Eliminate blind spots

- Identify emerging threats that other vendor solutions and legacy systems miss
- Improve threat detection with advanced models and machine learning (ML) that reduces false positives
- Observe anomalies across your entire data footprint, gaining real-time visibility into threat

Respond

Shut down the attack

- Get more meaningful alerts with context for enabling faster, more effective decision-making
- Automate mundane tasks allowing your team to focus on complex problems that require skills and creativity
- Quarantine endpoints, shut down network access, suspend users, and kill processes with the click of a button

Contain

Limit damage and disruption

- Gain the insight and support you need to identify the type of attack so you can take fast action
- Quickly determine which (if any) critical business systems have been compromised, what data has been affected, and whether any unauthorized entry points remain
- Gather forensic evidence for future prosecution

Navigate a changing threat landscape with confidence.

LogRhythm's flexible deployment options ensure you get the best fit for your organization.

Axon Security Operations Platform

Cloud-Native SecOps

Axon is built from real-world security experience. Our engineers and analysts have been on the frontlines of helping secure more than 4,000 companies around the world, and our development team and LogRhythm Labs continuously monitor and identify emerging cyber tactics. We've built a security operations platform to detect and disarm bad actors, while also providing an easy-to-use analyst experience delivered from the cloud.

With a potent combination of detection and collection technology, hybrid security analytics, and automation, we help security teams navigate an ever-changing threat landscape with confidence.

Hybrid security analytics

- Reduction of false positives by over 90% eliminates alert fatigue
- Improved security posture with real-time and accurate detection of lateral movement, exfiltration, malware compromise, ransomware, and other threats
- Immediate time to value with rules-based detection of known threats

Detection and collection

- Easy onboarding and management of network and cloud log sources ensure total visibility
- Agentless, real-time detection of network threat indicators helps monitor an easy entry point for attackers
- Out-of-the-box content helps automate and expand detections

Analyst experience

- Unified analyst experience delivers prioritized incidents for faster outcomes
- Easy-to-understand stand narrative reduces investigation and resolution time, freeing time for SOC planning, threat hunting, and trend tracking
- A simplified and productive user experience improves analyst morale and retention

LogRhythm SIEM

On-Premise SecOps

For organizations that require an on-premise solution due to regulatory requirements or IT preference, LogRhythm SIEM is the industry's most complete platform providing the latest security functionality, including security analytics. With LogRhythm SIEM, your team has an integrated set of modules that deliver on the fundamental mission of your SOC: threat monitoring, threat hunting, threat investigation, and incident response at the lowest total cost of ownership.

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.

SIEM

Detect and respond to threats provably 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 with security orchestration, automation, and response (SOAR) that is integrates into the LogRhythm SIEM and works with more than 80 partner solutions.

UEBA

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

Build a resilient defense.

LogRhythm has assembled the world's most capable and respected ecosystem of people and partners. Build a resilient defense with our analysts, experimentalists, engineers, and data scientists working at the cutting edge of cyber technology.

Preferred by security pros

Most cybersecurity systems are complicated, clunky, and frustrating to use. We believe SecOps teams deserve better. Our platforms are easy to set up and use. With an intuitive interface and dashboard, security analysts can oversee the entire threat landscape—while lessening the distraction of false alerts.

LogRhythm Labs

Nobody understands adversaries better than we do. LogRhythm Labs is our mission control center for proactively analyzing emerging threats from all corners of the web and building content to defend against them. We give your organization the upper hand by bringing you continuously improving intelligence and tools—based on the threats your organization and thousands of others are facing.

Security maturity

With two decades of experience in cybersecurity, LogRhythm brings together the most complete technology to improve your security posture. A deep arsenal of traces, metrics, and logs for all applications and environments enable organizations secure their systems and stay out of the news.

"LogRhythm is an excellent SIEM for learning content because the building blocks are simple and easy to implement; all content development concepts are literally represented as drag-and-drop building blocks that can be easily manipulated, furthermore, the statistical building blocks include powerful anomaly detection capabilities that are extremely difficult or impossible to implement in other SIEMs."

– Project Director, Services Organization

Gartner Peer Insights

Recommended by cyber authorities, analysts and customers.

Gartner®

9 Years

Gartner Magic Quadrant*

Named a leader in SIEM nine years in a row.

FORRESTER®

258% ROI

LogRhythm customers saw a 258% average ROI over three years according to the Total Economic Impact Report.

2021

G2 Grid® Leader

G2 Grid® Leader in SIEM, System Security & Incident Response Summer, Fall, & Winter 2021

*Gartner, Magic Quadrant for Security Information and Event Management, 29 June 2021, Kelly Kavanagh, Toby Bussa, John Collins. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Build a future free of cyber risk.

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—the reputation and success of their company, the safety of citizens and organizations across the globe, the security of critical resources—the weight of protecting the world.

LogRhythm helps lighten this load. The company is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an ever-changing threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps.

Together, LogRhythm and our customers are ready to defend. Learn more at logrhythm.com.

LogRhythm™

1.866.384.0713 // info@logrhythm.com