Be Security First

LogRhythm®

Your job is to keep your organization safe from cyberattacks.

But parsing through increasing amounts of log data across disparate systems and cloud applications can leave major gaps in visibility throughout the environment. Prioritizing threats may become an overwhelming task when strapped with little resources.

So how do you elevate securing your organization to the next level? You need to inspire and encourage a security-first mindset across the enterprise.

To do so, your team must implement a resilient and adaptable security strategy that builds confidence and board-level support to scale your threat detection and response.

No pressure, right? Luckily, there is a holistic solution that can provide your security operations center (SOC) quick time to value and measurable return on investment.

Here’s how LogRhythm can help.

Mature Your Security Operations

The LogRhythm NextGen SIEM Platform empowers your team to advance your organization’s overall security posture and operations maturity. LogRhythm strengthens your SOC and ensures you are ready to face whatever threats may come your way.

Detect threats earlier and faster than ever before.

When it comes to stopping threats, seconds matter. We built the LogRhythm UI for speed and efficiency. LogRhythm enables you to surface threats, search through log data, make decisions, collaborate, and respond to security incidents faster than ever before. Through machine learning and scenario-based analytics, LogRhythm surfaces emerging threats as they occur so your team can act fast.

Do more with the resources you have in place today.

Focus on detecting and responding to threats instead of spending your valuable time maintaining, caring for, and feeding your SIEM. LogRhythm includes a library of continuously updated data processing content and threat scenarios, so your team won’t have to spend time writing scripts, building rules, and creating reports. With greater flexibility, your team can customize and tailor it to meet the unique needs of your organization.

Gain deep visibility across your network.

Through its security operations and analytics capabilities, the LogRhythm NextGen SIEM Platform eliminates blind spots across the enterprise, giving you complete visibility into your IT and OT environments.

LogRhythm collects data from physical, virtual, and cloud sources to ensure that you always know what’s happening on your network. You’ll spot and catch every anomaly and threat — enabling you to successfully keep your business safe from cyberattacks.

Prove reduced risk to your board.

Your board needs to feel confident in your team’s ability to identify and stop threats and keep the company’s reputation and critical assets secure. And you need the board to continue to invest in your security programs. With reports that illustrate the types of threats you face and your team’s detection and response trendlines, you’ll be able to readily demonstrate your team’s value.

Build for today. Scale for tomorrow.

The amount of data your team is responsible for protecting is large and is growing rapidly. It’s important to know that your investment will easily flex to meet your future needs. The LogRhythm platform scales to massive data volumes while delivering high performance and streamlined administration — reducing your overall operating costs.

Build Your SOC on a Solid Foundation

To protect your organization from risk, your team must be able to detect and respond to a threat — before your network is compromised. How do you do this successfully? Shorten your mean time to detect (MTTD) and mean time to respond (MTTR) to a cyberthreat.

The LogRhythm NextGen SIEM Platform

Our NextGen SIEM solution operates as your team's central nervous system to alert on threats and enact countermeasures — all in real time. With LogRhythm, your team will detect and respond to threats measurably faster. Your security operation will become more effective and efficient through automated workflows and accelerated threat detection and response capabilities.

The LogRhythm NextGen SIEM Platform is comprised of the LogRhythm XDR Stack and LogRhythm UserXDR.

Deploy On-Prem or in the Cloud

Our flexible deployment options ensure that you get the best fit for your organization — no matter what your goals and environmental needs may be. LogRhythm Cloud provides our complete NextGen SIEM experience with the ease and flexibility of a SaaS solution.

LogRhythm XDR Stack

With the LogRhythm XDR Stack, your team has an integrated set of capabilities 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.

AnalytiX

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

DetectX

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.

RespondX

Work smarter, not harder. Collaborate, streamline, and evolve your team with security orchestration, automation, and response (SOAR) that is seamlessly integrated into the LogRhythm NextGen SIEM and works with more than 80 partner solutions.

UserXDR

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

MistNet NDR by LogRhythm

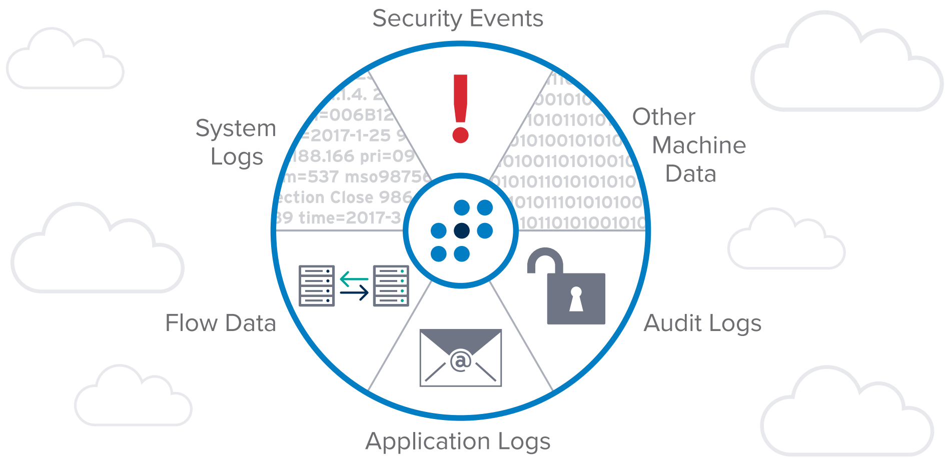
Secure your network against pervasive threats with our network detection and response solution that works alone or in combination with the LogRhythm NextGen SIEM Platform. MistNet NDR by LogRhythm combines machine learning, rules-based detection and threat intelligence to discover and identify threats across desktops, data centers, and the cloud.

Powered by patent-pending TensorMist-AI™ technology, MistNet NDR uses distributed computing that easily scales data collection and analytics and lowers operating costs.

Behind the UI of our NextGen SIEM

Input

Real-Time Data Collection (on-prem and cloud-sourced)



Real-Time Data Generation

Network Monitoring

- DPI & Application ID
- Full Packet Capture

Endpoint Monitoring

- File & Registry Monitoring
- Process Activity

Real-Time Context

Internal

- Users
- Hosts

External

- Threat Intelligence

Analytics

Processing

- Time Normalization
- Metadata Extraction
- Uniform Data Classification
- Threat & Risk Contextualization

MACHINE DATA INTELLIGENCE (MDI) FABRIC

Machine Analytics

- Behavioral Profiling
- AI & Machine Learning
- Black/Whitelisting
- Advanced Correlation
- Statistical Analysis
- Deep Packet Analytics

Search Analytics

- Unstructured Search
- Log Analysis
- Contextual Search
- Pivot & Drill-Down
- Visualizations
- Contextual Lookups

Output

Actionable Intelligence

- Incident Tracking & Metrics
- Risk Prioritized Alarms
- Reports
- Real-Time Dashboards

Workflow

Security Orchestration, Automation and Response

- Case Collaboration
- Evidence Locker
- Automated Response
- Playbooks

Persistence

Data Storage and TTL

- Hot/Warm Tiered Storage
- Configurable TTL
- Cold Data Archiving and Retrieval

An Award-Winning Platform

We're proud of our accolades. We've earned every one of them. From being a Leader in the Gartner Magic Quadrant for the better part of a decade to receiving the Gartner PeerInsights™ Customers' Choice designation four years in a row, the recognition we've received points to our innovation and dedication to delivering security solutions that help you protect your business, your brand, and your reputation.

At LogRhythm, we understand the complexity of your job. Our laser focus on security translates into targeted innovation to give your team the solutions it needs to overcome the challenges it faces every day. The LogRhythm NextGen SIEM Platform is designed to improve your organization's overall security posture and defeat any threat that attempts to breach your environment.

From R&D to our customer success team, we see ourselves as your partner in the fight against cyberthreats. Customer success is one of our core company values. Let our customers tell you about their experiences firsthand.

Visit www.logrhythm.com to read and watch in-depth reviews from real customers.

Market Leader for UBA

Best SIEM Product

Our Commitment to Your Success

LogRhythm Labs

It's crucial to have resources that keep your organization well informed of the latest incidents and breaches that could pose a threat. LogRhythm Labs can help with a dedicated team that delivers use case content encompassing the latest information on emerging threats, changing compliance mandates, and security best practices.

We Can Help

Dealing with the change that comes with running a SOC takes guts, grit, and the ability to establish confidence when faced with uncertainty and doubt. To be resilient, you need to ensure that security is a top priority in your organization and that you can show the value of your program. For this to happen, you must be a change agent and establish a security-first mindset in your organization.

Our Professional Services can help you keep pace with a changing security landscape, boosting the performance and effectiveness of your security team and platform. Customers use our service offerings to accelerate time to value, ensure seamless deployment, and tune their platform. Customers also rely on our subscription services to augment their security team with our experts.

LogRhythm lives and breathes the security-first mindset that creates resilience — from being one of the frontrunners to implement the Zero Trust framework for our own organization to our dedication to innovation and education. Together, we can be security first.

About LogRhythm

LogRhythm’s award-winning NextGen SIEM Platform makes the world safer by protecting organizations, employees, and customers from the latest cyberthreats. It does this by providing a comprehensive platform with the latest security functionality, including security analytics; network detection and response (NDR); user and entity behavior analytics (UEBA); and security orchestration, automation, and response (SOAR).

Learn how LogRhythm empowers companies to **be security first** at logrhythm.com.

Schedule a demo today.

www.logrhythm.com/demo

LogRhythm®

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301