LogRhythm

Unleash the Power of Your SOC

Your job is to keep your organization safe from cyberattacks.

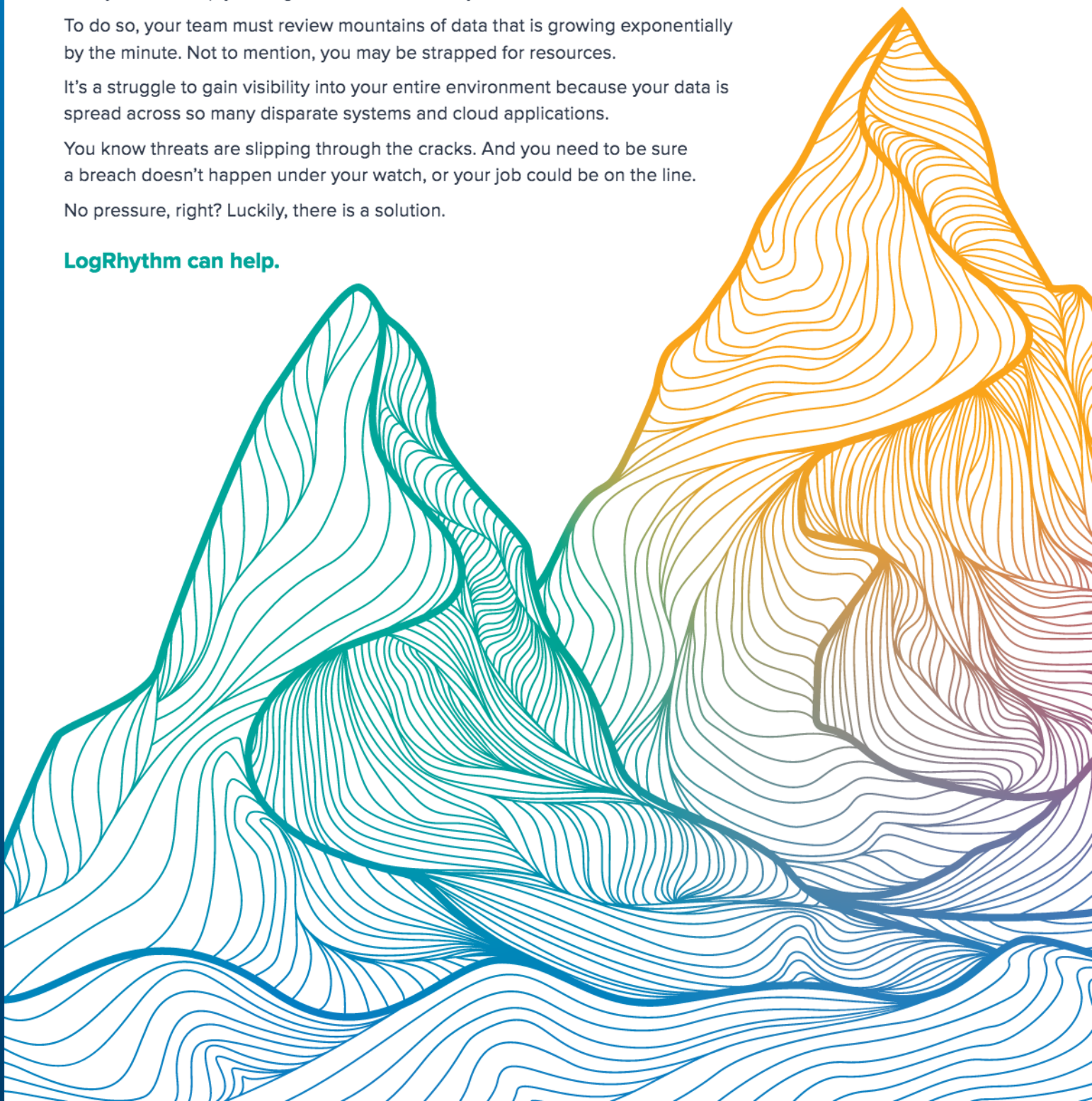
To do so, your team must review mountains of data that is growing exponentially by the minute. Not to mention, you may be strapped for resources.

It's a struggle to gain visibility into your entire environment because your data is spread across so many disparate systems and cloud applications.

You know threats are slipping through the cracks. And you need to be sure a breach doesn't happen under your watch, or your job could be on the line.

No pressure, right? Luckily, there is a solution.

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 security operations center (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. And because of the platform's flexibility, your team can tailor it to meet the unique requirements 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, LogRhythm UserXDR, and LogRhythm NetworkXDR.

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 products 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.

UserXDR

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

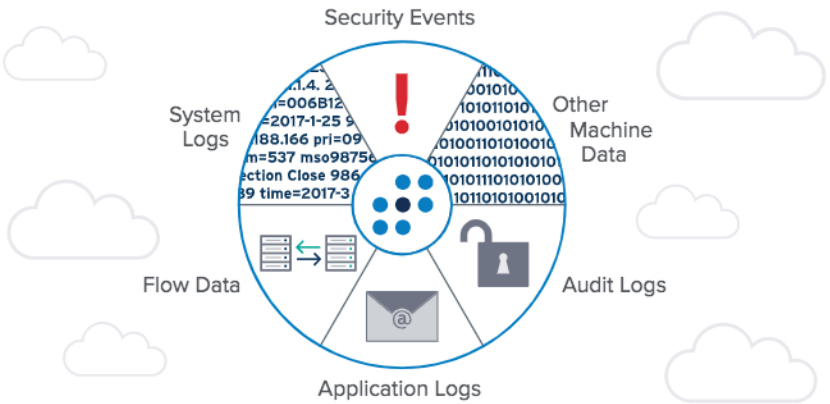
NetworkXDR

Go beyond limited traffic analysis to detect rapidly spreading network-borne threats and reduce risk to your organization.

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

MACHINE DATA INTE

Machine Analytics

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

Uniform Data Classification

Threat & Risk Contextualization

LLIGENCE (MDI) FABRIC

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

Our Commitment to Your Success

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 leading the Forrester Wave™ for Security Analytics Platforms, 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 first hand.

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

We Can Help

No IT environment is the same, and no organization has the exact same security challenges. Our team of security experts is here to help you solve these challenges and reduce your organization's risk.

Schedule a customized demo today.

www.logrhythm.com/demo

About LogRhythm

LogRhythm empowers more than 4,000 customers across the globe to measurably mature their security operations program. LogRhythm's award-winning NextGen SIEM Platform delivers comprehensive security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralization of threats.

Built by security professionals for security professionals, LogRhythm enables security professionals at leading organizations like NASA, and XcelEnergy to promote visibility for their cybersecurity program and reduce risk to their organization each and every day. LogRhythm is the only provider to earn the Gartner Peer Insights' Customer Choice for SIEM designation three years in a row.

To learn more, please visit logrhythm.com

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

LogRhythm®