LogRhythm®

Security. Made Smarter.

Your job is to keep your organization safe from cyberattacks. To do so, your team has to review a monumental amount of data that is growing exponentially by the minute. Your team is strapped for resources, and it's nearly impossible to have visibility of your entire environment because the 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?

There has to be a better solution. LogRhythm can help.

Intelligent Threat Detection and Response

We built LogRhythm with you in mind. Everything our team of security experts architects into our NextGen SIEM Platform is designed to help you do your job better and more efficiently.

Uncover threats faster. Work smarter.

When it comes to stopping threats, seconds matter. The LogRhythm UI is built for speed and efficiency. You'll search, make decisions, collaborate, and respond faster with LogRhythm than with any other solution. Through machine learning and scenario-based analytics, LogRhythm will surface threats in real time so your team can act fast.

Spend your precious time on important work.

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 turnkey embedded content that is continuously updated, so your team won't have to spend time writing scripts, building rules, and creating reports. And because the platform is flexible, your team can still tailor it to the unique requirements of your organization.

See shifts in behavior as they happen.

When a bad actor is moving across your environment, a behavioral shift is often a primary indicator. LogRhythm's intelligent analytics put advanced threat detection at your fingertips. The platform detects behavioral shifts that originate from both inside and outside your organization. If a threat is happening, you'll see it.

Prove reduced risk to your board.

Your board needs to feel confident in your team's ability to identify and stop threats to keep the company's reputation and critical assets secure. And you need the board to continue to invest in your security programs. With built-in reports that illustrate your team's time to detect and respond to threats and incidents, you'll be able to easily demonstrate your organization's security maturity.

Build for today. Scale for tomorrow.

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

Build Your SOC on a Strong Foundation

To protect your organization from risk, your team must be able to detect and respond to a threat early in the Cyber Attack Lifecycle. To do this successfully, you have to shorten your mean time to detect (MTTD) and mean time to respond (MTTR) to a cyberthreat.

Threat Lifecycle Management is the fundamental workflow of an effective security operations center (SOC). This series of aligned SecOps capabilities and processes gives your team holistic visibility of your IT and OT environments so you can quickly detect, mitigate, and recover from a security incident.

LogRhythm delivers Threat Lifecycle Management by bringing together traditionally disparate capabilities into one unified platform. With LogRhythm, your team has a single UI where they can evaluate alarms, investigate threats, and respond to incidents.

NextGen SIEM

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.

User and Entity Behavioral Analytics (UEBA)

User and entity behavioral analytics play a critical role in giving your team visibility into user behavior. LogRhythm UEBA uses advanced machine learning to perform profiling and anomaly detection so your team can easily identify insider threats, privilege abuse, compromised accounts, and more.

Network Traffic & Behavioral Analytics (NTBA)

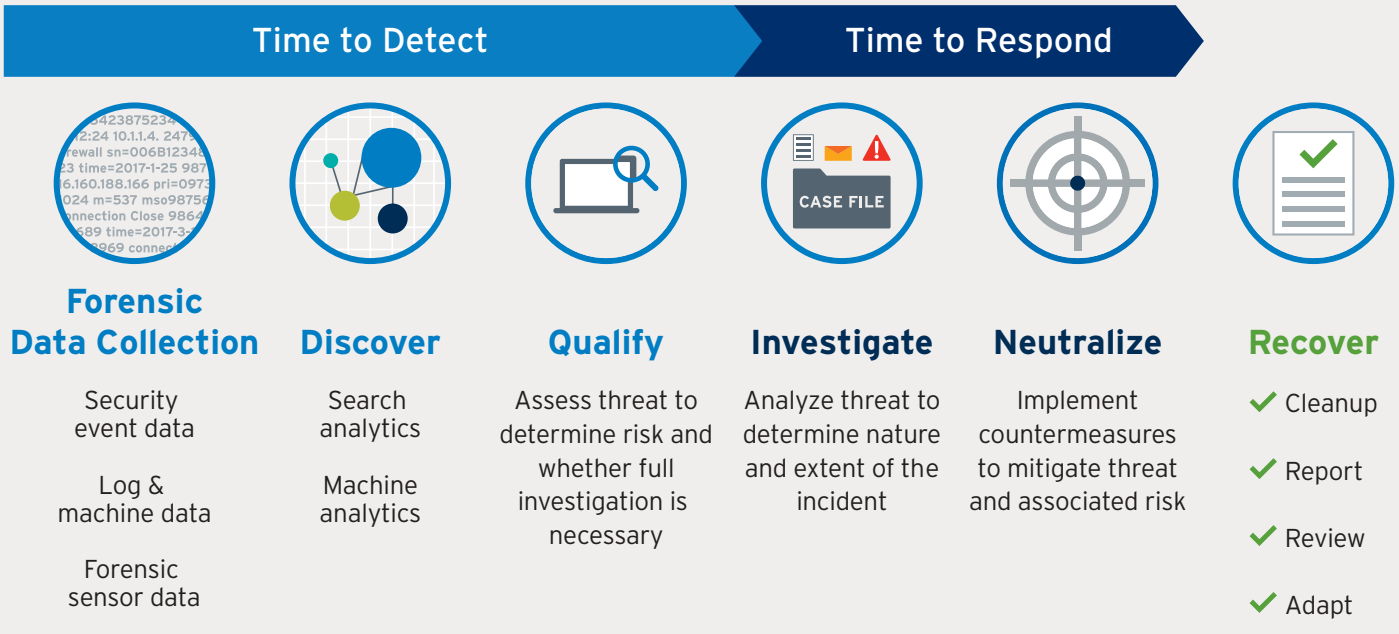
With NTBA, your team can detect, analyze, and prioritize network-based threats and automate actions to stop an attack on your network.

Security Automation & Orchestration (SAO)

Whether you have a team of one or a team of 20, LogRhythm accelerates threat qualification, investigation, and response to make your team more efficient and effective so you can do more with the resources you already have.

Compliance

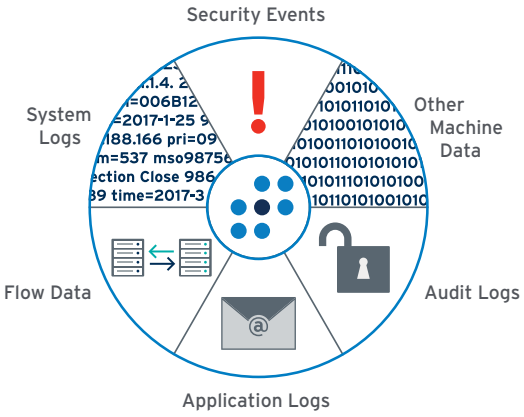
LogRhythm helps you address unique compliance challenges with preconfigured compliance automation modules that address regulatory frameworks such as GDPR, SOX, PCI-DSS, HIPAA, and many more.



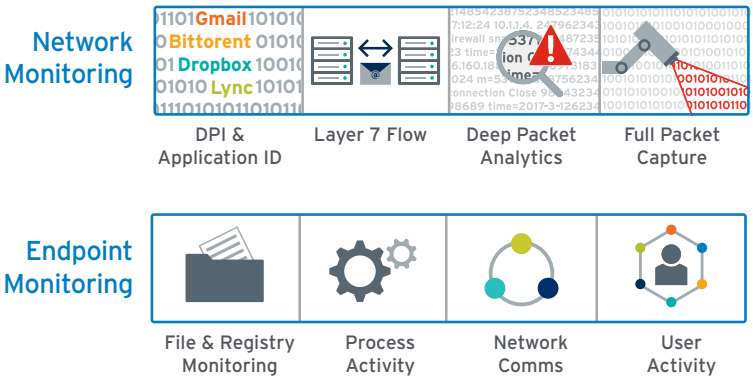
Behind the UI of our NextGen SIEM Platform

Input

Real-Time Data Collection

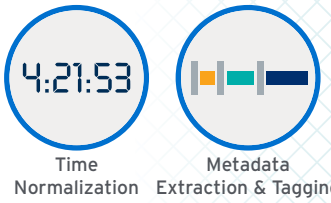


Real-Time Data Generation

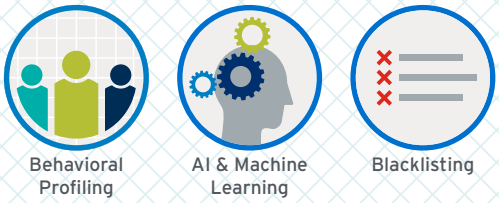


Analytics

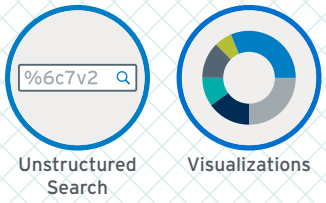
Processing



Machine Analytics



Search Analytics

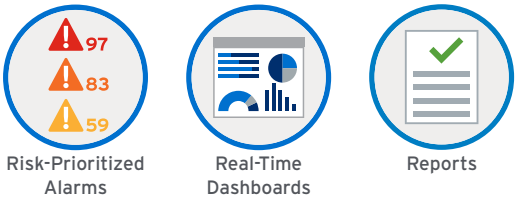


MACHINE DATA INTELLIGENCE (MDI) FABRIC

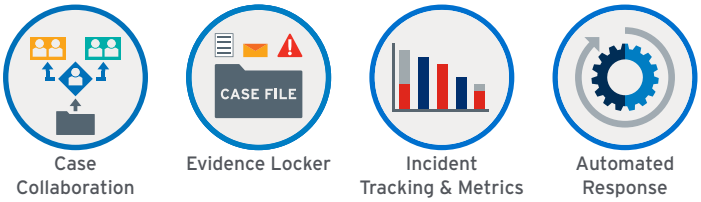
LogRhythm Labs Research & Intelligence

Output

Actionable Intelligence



Security Automation and Orchestration



Our Commitment to Your Success

At LogRhythm, we believe in empowering a culture of success—for you and for your business. Our platform is designed by security professionals who understand how complicated your job is. This laser focus on security translates into targeted innovation that gives your team solutions that help reduce the challenges and complexities your team faces every day.

In our world, threats don't stop, and they're constantly changing. Our LogRhythm Labs team continually provides research and relevant content updates that help to protect your organization from the latest-breaking threat.

From R&D to customer success, we see ourselves as a partner in your fight against cyberthreats. It's one of our core values as a company.

About LogRhythm

LogRhythm is the world leader in NextGen SIEM, empowering organizations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm platform combines user and entity behavior analytics (UEBA), network traffic and behavior analytics (NTBA) and security automation & orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations center (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

www.logrhythm.com

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

Frost & Sullivan 2017 Best Practices Award — Global SIEM Enabling Technology Leadership Award

SANS Best of 2016 Winner in SIEM

SC Media Recommended

Gartner — A 2017 Leader SIEM Magic Quadrant

Gartner peerinsights customer choice 2017

Forrester Wave Leader 2017 — Security Analytics Platforms

LogRhythm®

Learn more: info@logrhythm.com

Call today: 1-866-384-0713