

NextGen SIEM with the Benefits of SaaS

Visibility, detection, and response is critical for enterprise security. LogRhythm Cloud delivers our NextGen SIEM experience and capabilities along with the deployment ease and flexible operations of a SaaS solution. LogRhythm Cloud is securely hosted and fully administered by LogRhythm to reduce the burden of performing routine management and maintenance tasks from initial deployment through ongoing upgrades. Out-of-the-box and custom analytics, dashboards, and many other customizable features allow you to maximize the effectiveness of your team.

LogRhythm takes care of:

- Deployment
- SIEM health
 - Services and components monitoring
- Data management
- Regular LogRhythm Knowledge Base (KB) updates
 - New and updated device support
 - New and updated analytics content
- Security of platform
- Infrastructure
 - 24x7 infrastructure monitoring and management
 - Capacity changes
 - Software patching and updates

With LogRhythm Cloud, all core LogRhythm NextGen SIEM Platform infrastructure is maintained in the cloud. Data collectors can be deployed on-premises and in the cloud. You can also integrate on-premises or cloud-deployed instances of LogRhythm SysMon and NetMon with the core LogRhythm Cloud infrastructure, to get deeper visibility into host and network data.

Your security is our top business driver. Your data is both secured and optimized for transfer over the internet through encryption both in transit and at rest with additional options for compression and scheduling.

LogRhythm Cloud's rapid deployment and simplified maintenance enable stronger security in your organization by giving your team back time spent on administrative tasks, so they can effectively hunt and respond to cyberthreats. In turn, this reduction increases your organization's security maturity.

Don't Sacrifice Capabilities or Usability

Don't settle on a cloud solution with a reduced SIEM feature set compared to on-premises offering. LogRhythm customers will recognize the same intuitive interface, award-winning comprehensive threat management, compliance, and security orchestration, automation, and response (SOAR) capabilities in LogRhythm Cloud as available in any on-premise LogRhythm NextGen SIEM Platform deployment, along with the added benefit of reduced administrative costs.

The LogRhythm Cloud Advantage

Realize the full analyst experience of next-gen SIEM in a cloud offering

- Increase analyst effectiveness with embedded security orchestration, automation, and response (SOAR) capabilities
- Reduce mean time to detect (MTTD) and mean time to respond (MTTR) through LogRhythm's full set of analytics

Maximize your security team's time and expertise

- Detect known and unknown attacks and threats with risk-based, prioritized scoring
- Reduce upkeep time with 24x7 monitoring of infrastructure and the latest software and patches
- Maintain your focus on security operations while LogRhythm provides consistent infrastructure and software administration

Achieve swift time-to-value through rapid deployment

- No required hardware implementation or software installation, database setup, initial configuration, or other parameters to delay time-to-value
- Cut your deployment time down to minutes
- See immediate value upon onboarding your data sources



“ Solution maintenance is never on my mind when using LogRhythm Cloud. It just runs. Instead of spending my first week setting up new hardware and software, I identified a new production use case. It was so valuable that we’re implementing the same technique across multiple other networks. ”

- Kevin Merolla, Global IT security manager, Chart Inc

Increased ROI with LogRhythm SOAR

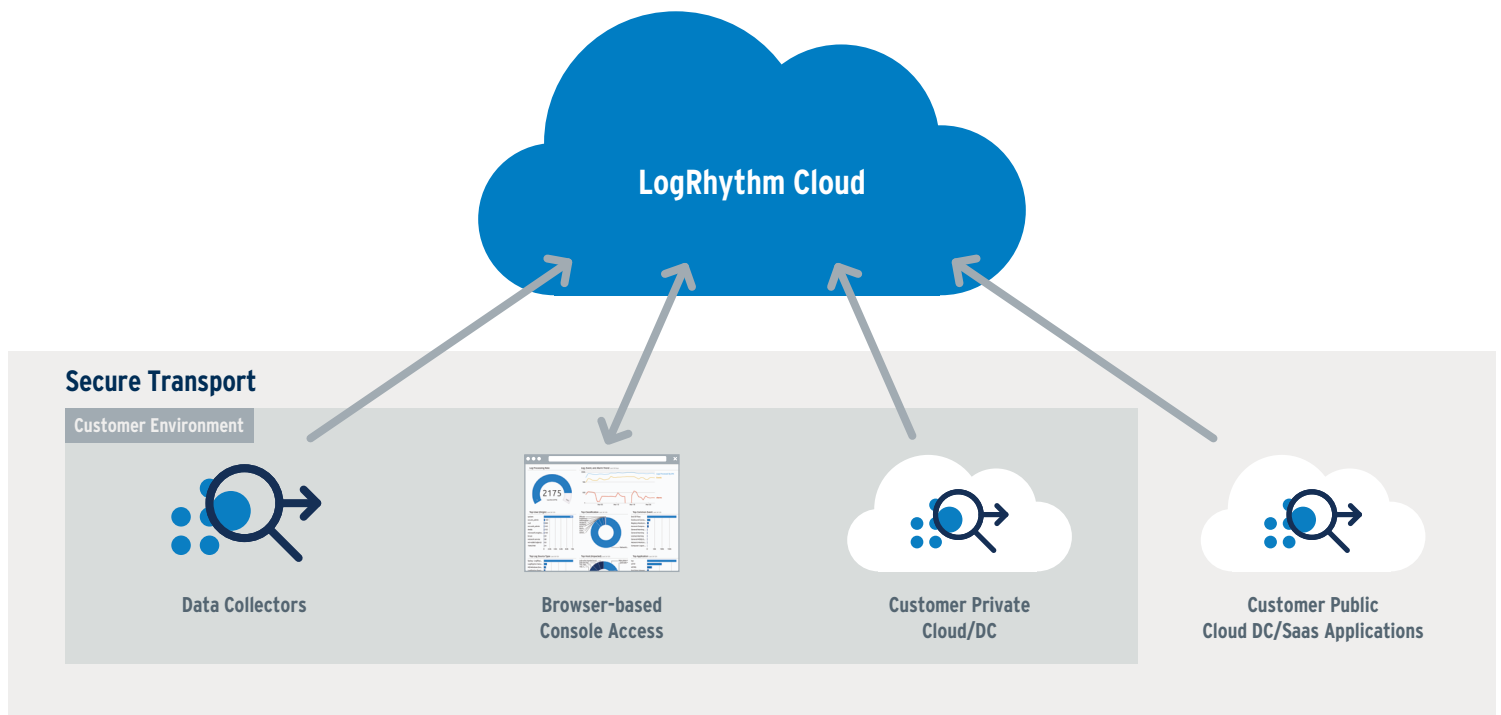
It's critical to quickly prioritize and neutralize threats in your environment. LogRhythm Cloud includes our embedded SOAR solution to provide increased efficiency and higher-quality incident response with low mean time to response (MTTR). LogRhythm SOAR offers a full range of comprehensive features for incident investigation and response:

- Case Management streamlines workflows and enables teams to track incidents, collaborate, and collect evidence.
- Case Playbook offer guided procedures for standardized incident response.
- Case Metrics provide a workflow timeline with key milestones.
- Contextualization features enable quick threat intelligence and business context enrichment during investigations.
- Dashboard views and reporting offer flexible views and summaries for demonstrating improvements and compliance.
- SmartResponse™ Automation executes actions across third-party integrations for efficient collaboration, effortless contextualization, and rapid remediation.

LogRhythm's SOAR solution offers immediate value and ease of use without requiring integration of yet another costly security product. For LogRhythm Cloud customers, SOAR is an integrated component of our SaaS offering.

Licensing

LogRhythm Cloud is licensed by volume and offered via subscription.



Get started today. [Contact us](#) to schedule a demo.