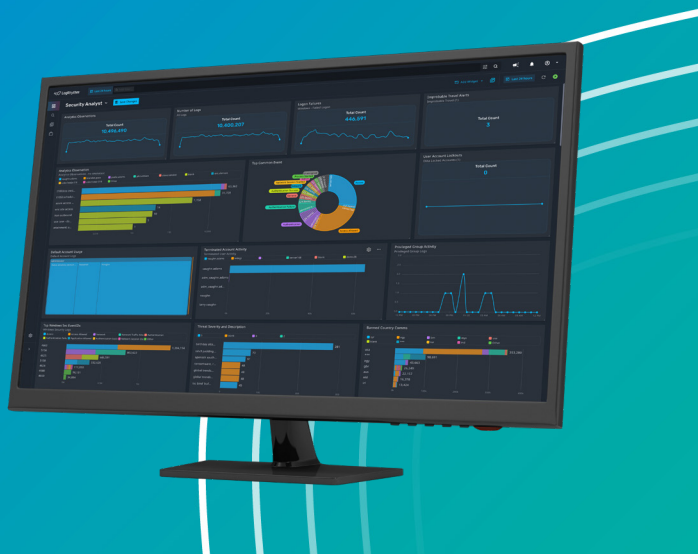
LogRhythm | LRQA NETTITUDE

Data Sheet

LogRhythm Axon

A Cloud-Native SIEM Platform



There is a lot riding on the shoulders of your security operations team—protecting the organization's reputation, safeguarding sensitive client information, and ensuring the organization's ability to deliver products and services. When security teams are stretched to the limit, LogRhythm Axon helps lighten the load to make your life easier.

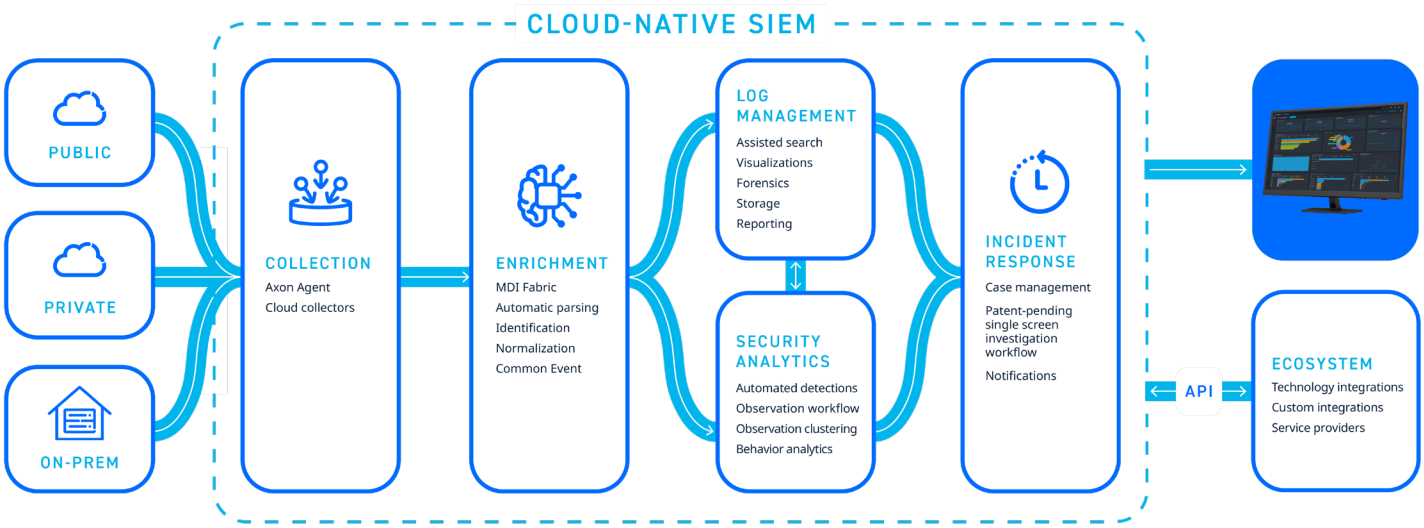
LogRhythm Axon is a cloud-native security information and event management (SIEM) platform built for security teams that are overwhelmed by immense amounts of data and an ever-evolving threat landscape. Optimized for the analyst experience, LogRhythm Axon's powerful security analytics, intuitive workflow, and simplified incident response give analysts contextual insight into cybersecurity threats so they can reduce noise and quickly secure the environment. LogRhythm Axon reduces the burden of managing threats and the operating infrastructure, helping security teams prioritize and focus on the work that matters.

Benefits

- **Save Time:** An open cloud-native SIEM platform that alleviates time spent managing and maintaining infrastructure while easily integrating with other applications.
- **Gain Comprehensive Visibility:** Automatically collect data from SaaS, self-hosted cloud, and on-prem sources from LogRhythm's hosted collectors and on-prem agents. Metadata extraction combined with easy-to-use tools to build custom parsers ensures visibility across your environment in a centralized console.
- **Find Threats Faster:** Search driven widgets and an intuitive dashboard make it easier to monitor, detect, investigate, and respond to threats. Ensure threat detection engineering with the ability to test your analytics rules.
- **Execute Seamlessly:** Surface critical threats and secure your environment with powerful security analytics and simplified incident response. Leverage out-of-the-box content or author your own custom content.

Cloud-Native SIEM Made Easy

- Scalable and Open Cloud-Native SaaS Platform
- Powerful Security Analytics
- Simplified Incident Response
- Automatic Log Collection and Enrichment
- Optimized for the Analyst Experience



Key Features

Open Cloud-Native SaaS Architecture

Ease the burden of managing and maintaining infrastructure to focus on the work that matters and scale smoothly as your security operations center (SOC) grows. Designed to easily integrate with other cloud services and on-prem applications, LogRhythm Axon automatically onboards new data sources. With a cloud-native architecture, automated updates enable continuous and quick delivery of enhancements.

Automatic and Flexible Collection of Logs

Flexible collection of logs from SaaS, self-hosted cloud, and on-prem at the point of ingestion in near real-time gives you visibility as soon as possible. Integrations from LogRhythm Axon cloud collector, LogRhythm Axon agent, and customizable API and Webhook connections ensure you have visibility into your environment.

Enrichment and Normalization of Logs

Log data is normalized and enriched into LogRhythm Axon with our patented Machine Data Intelligence (MDI) Fabric to improve searchability and analytics across disparate log sources. With deep intelligence into common and unique data source types and pre-built processing rules, MDI Fabric ensures that metadata is automatically and accurately extracted at the point of ingestion.

Analytics Rule Builder

Leverage quality out-of-the box content mapped to the MITRE ATT&CK® framework and build your own custom threat detections based on criteria that matter to your organization. Quickly investigate suspicious activity by automatically surfacing critical threats for investigation in the LogRhythm Axon dashboard.

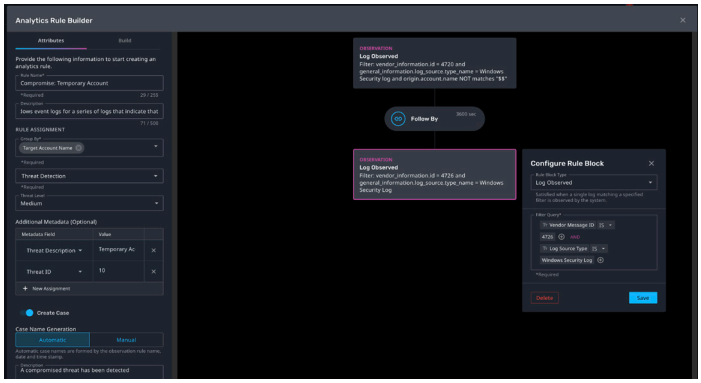


Figure 1: Surface the most critical threats for investigation using the analytics rule builder.

Analytics Rules Testing

Enable threat detection engineering with the ability to test analytics rules to confirm rules are fine-tuned and optimized for your environment. Easily conduct red team exercises and penetration tests to check for exploitable vulnerabilities within the LogRhythm Axon user interface (UI).

Case Management and Notifications

Increase SOC efficiency by automating incident response and investigation workflows through automatically creating cases from analytics rules for faster response times. Prioritize workflows by assigning threat severity levels to surface which events require immediate attention and always stay on top of case activity via the case management dashboard and email notifications.

Single Screen Investigation Workflow

Attain faster and more accurate threat investigation by being able to view contextual insight and evidence of a case side by side without the need to pivot to different tabs within the UI. With a case detail panel, an evidence list panel, and a single log inspector panel, analysts can make well-informed decisions by drilling down into logs, individual observations, security analytics, and raw metadata all within a single pane of glass.

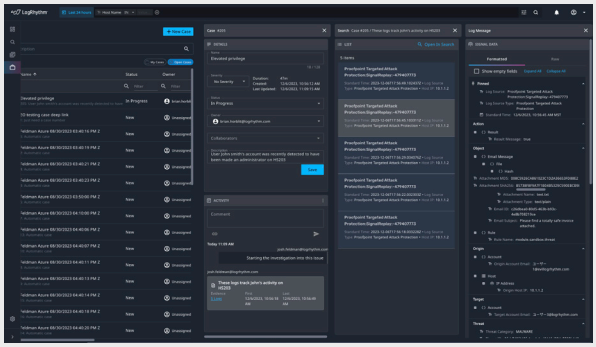


Figure 2: Gain quicker response times with contextual insight of a case in one centralized workflow.

Simplified Licensing

Simplify budgeting and make it more predictable with licensing based on the daily ingest rate of data and the length of time it is retained in the platform.

Easy Parsing

LogRhythm's Policy Builder feature only requires a few clicks to create log parsing policies for logs. Easy guided workflows help build new policies to ensure future data can be easily searched and automatically fed into visualizations and detections.

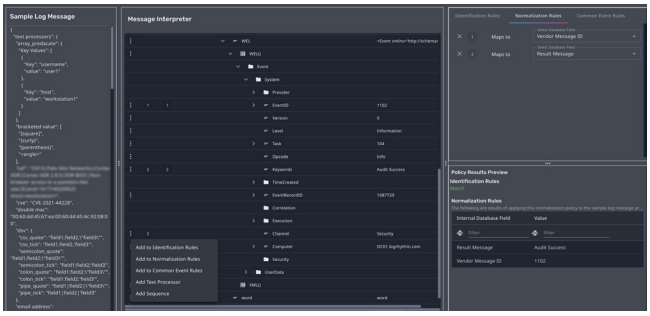


Figure 3: Easily parse unidentified logs with LogRhythm Policy Builder feature.

Intuitive Dashboard, Assisted Search, and Reporting Capabilities

Search the entire log store at any time and continuously monitor via dashboards to enhance visibility into investigations and security analytics. Facilitate fast decision making with assisted search that prompts context as an analyst types in search keys and values. Search common events to find relevant security events across different vendors' log sources without having prior knowledge of the underlying log structure. Save dashboards and searches and schedule specific reports daily, monthly, and/or quarterly.

Guided and Instinctive Workflows

Detect, investigate, and respond to threats more easily with workflows that are consistent across the platform which additionally reduces ramp time on the platform.

Professional and Consulting Services

Gain a faster time to value with flexible options to choose what is right for your business. Learn more about services for LogRhythm.

About LogRhythm

LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights so they can respond with speed and efficiency. With deployment flexibility, out-of-the-box integrations, and advisory services, customers can confidently monitor, detect, investigate, and respond to cyberattacks.

Interested in seeing LogRhythm Axon in action? Request a demo today!

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 2 8019 7185

www.logrhythm.com