Data Sheet

AnalytiX

Data Visibility, Normalization, and Analysis – at Scale

Digital transformation is rapidly increasing data sources, changing your environment. Data stored in different locations makes visibility across log data difficult. Complicating matters, devices and applications generate log and machine data with varying logging standards, creating inconsistencies in the content, taxonomy, and syntax of logs across vendors. Without standardization, searching across data is complex.

LogRhythm AnalytiX eases your log management issues. As part of the LogRhythm NextGen SIEM Platform, AnalytiX centralizes log data, enriching it with contextual details and applying a consistent schema across all data types. With AnalytiX, you can search through data to find anomalies and identify IT and security events.

Enrich Data with Machine Data Intelligence

Like most businesses, your organization generates a tremendous amount of data. But making sense of it all is challenging.

As part of our AnalytiX product, Machine Data Intelligence (MDI) Fabric helps you create consistent and predictable datasets by classifying, contextualizing, and normalizing every log message. Our data normalization and enrichment framework extracts metadata from log messages or collected data, assigns metadata to it, enriches synthetic data, and maps it to classification and common event taxonomy, enabling your team to deepen its understanding of log and machine data.

Automate Correlation and Analysis

AnalytiX gives your team insight into threats and behavioral anomalies—as they occur—through continuous analysis and correlation via AI Engine, LogRhythm's rule engine. AI Engine delivers automated, continuous analysis and correlation across all activity to identify risks, threats, and critical operational issues in real time.

AI Engine is easy to use. Analysts can create sophisticated event processing rules using a drag-and-drop editor, which includes triggering on filter match, thresholds, whitelists/blacklists, and absence of events. AI Engine automatically identifies and alerts on actionable events with precision, supporting security, compliance, and operations use cases. Unlike others in the market, AI Engine's advanced correlation rule sets run out-of-the-box and can be customized to fit your needs.

Expand Visibility Across Your Environment

When it comes to data, you don't want any surprises. AnalytiX provides a holistic view of your environment, helping you diagnose security and operational issues using centralized visibility. Interpret, sort, and organize search results and data faster with our advanced visualization tools. Use customizable dashboards and search layouts, trends, and relationship data for more accurate results.

Benefits

- **Faster assessment** of security events and trends using consistent and predictable datasets
- **Assured detection** of threats and behavioral anomalies with continuous analysis and correlation
- **Greater productivity** with automation and advanced search capabilities
- **Immediate value** with out-of-the-box rules and simple-to-use search

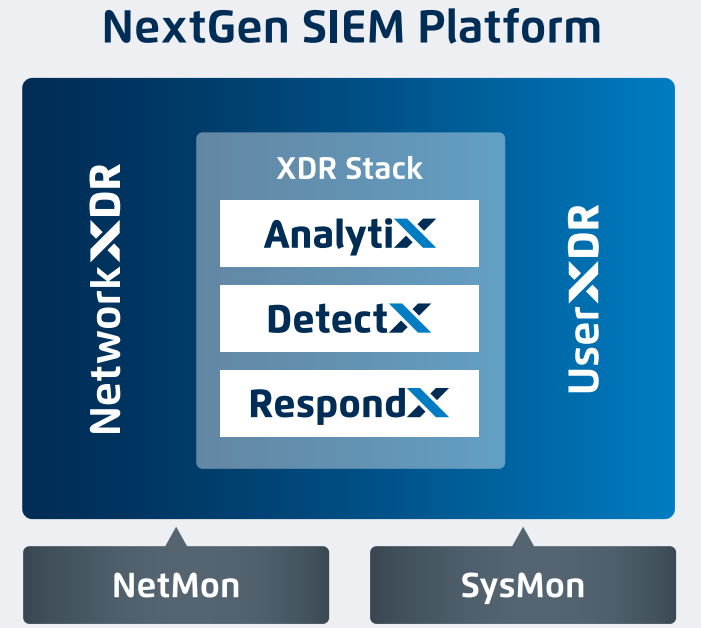
Features

- **Structured and unstructured search** makes finding answers easy, even without knowing the underlying data structure or learning a new query language
- **Standardized data syntax and contextual details** normalize and enrich log and machine data
- **Machine Data Intelligence (MDI) Fabric** enables collection of an extensive array of log and security data across physical, virtual, and cloud environments, including collection of custom application logs
- **AI Engine** facilitates automated, continuous analysis and correlation across all activity with minimal processing for real-time identification of risks, threats, and critical operational issues
- **Centralized dashboards** speed interpretation of search results and analysis
- **Node Link Graph** filters data and helps visualize activity and relationships of interest for faster analysis and results

Advance Your Security Operations Maturity with the XDR Stack

The NextGen SIEM Platform is a comprehensive set of capabilities that include the XDR Stack and other supporting elements:

- AnalytiX is a log management solution that centralizes your log data, enriches is with contextual details and applies a consistent schema across all data types.
- DetectX allows you to focus your efforts with targeted and prioritized threat detection.
- RespondX is a seamlessly integrated security orchestration, automation, and response (SOAR) that enables your team to effectively collaborate, qualify, and manage incidents with improved quality and speed.
- NetworkXDR helps you detect and respond to network-borne threats like lateral movement and internal access abuse.
- UserXDR helps you identify user-based threats such as compromised accounts and malicious insiders that can be difficult to detect.
- NetMon provides real-time visibility and security analytics to monitor your agency's entire network.
- SysMon helps you gain access to rich endpoint data to detect and respond to threats faster.



Deployment Options

The LogRhythm NextGen SIEM Platform can be deployed via multiple configurations including on-premise, SaaS, and hybrid.

Appliances

- Pre-staged
- Horizontal and vertical scalability
- Building-block architecture

Software

- Reference designs for dedicated hardware or virtual
- Mix and match with appliances
- Aligns to appliance building blocks

Cloud

- Support for private and public
- Reference designs and pre-created images
- Full SaaS

See AnalytiX and the XDR Stack in action. Request a demo today.
logrhythm.com/demo

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

www.logrhythm.com