Data Collection

Unlock Valuable Context During Collection and Normalization

You can't fight what you can't see. Visibility is essential to all security teams. To gain greater visibility and successfully monitor and address security challenges, you need the capacity to collect data from various sources. Just as critical, you need context from the data you collect to accelerate your detection and response.

LogRhythm's Data Collection, Parsing, and Enrichment Process

LogRhythm's NextGen SIEM Platform enhances your visibility into data sources—including common, custom, and cloud data sources—so you can spot threats and remediate them quickly. LogRhythm classifies and normalizes the data long before you hit search, unlocking valuable metadata to aid your investigation. LogRhythm's NextGen SIEM Platform ingests more than 900 distinctive data sources to help your team easily alarm across the most important data sources for your enterprise. Additionally, LogRhythm SysMon helps your team access rich endpoint data by consolidating and collecting log and machine data from local and remote environments and cloud infrastructure to give you a big picture view of your entire data ecosystem.

LogRhythm Open Collector

LogRhythm Open Collector is the next evolution in data collection technology, giving your team stronger support and ease of use for cloud and custom data sources. Open Collector simplifies the process of delivering data from cloud services/applications and reduces the complexity of supporting custom data sources with Elastic Beats. The Beats framework provides greater versatility to support varying data sources and increased flexibility for creating custom shippers. Due to the open-source nature of the technology, users and contributors regularly update data types and capabilities that are available. Open Collector is backwards compatible to LogRhythm version 7.2.

Achieve Normalization and Contextualization with MDI Fabric

The breadth of data sources in your organization and the consistency at which the data is parsed and normalized have a direct impact on the effectiveness of data analysis. Ineffective data classification and field mapping can create issues when querying data. Incorrect classification can lead you astray by creating false positives when detecting threats.

LogRhythm's patented Machine Data Intelligence (MDI) Fabric—a framework for data enrichment and normalization—provides unique, rich metadata that helps your team quickly troubleshoot issues and ensure accurate analysis. Other SIEM solutions require you to have extensive knowledge of the underlying data structure, but MDI Fabric removes those constraints. Using classification, contextualization, and critical field normalization, our MDI Fabric empowers operations teams to execute use cases quickly and effectively.

Benefits

- **Reduce the time and resources** needed to onboard new data sources
- **Achieve precise data analysis** and search through effective normalization
- **Gain comprehensive visibility** through support for a wide range of data sources
- **Bolster cloud log source collection** with LogRhythm-supported Beats for top cloud sources

Features

- **Uses lightweight agents** for minimal performance impact
- **Simplifies data delivery** using Elastic Beats
- **Includes MDI common schema** for data consistency
- **Enables authentication and encryption** for secure data transmission

LogRhythm Data Collection Process

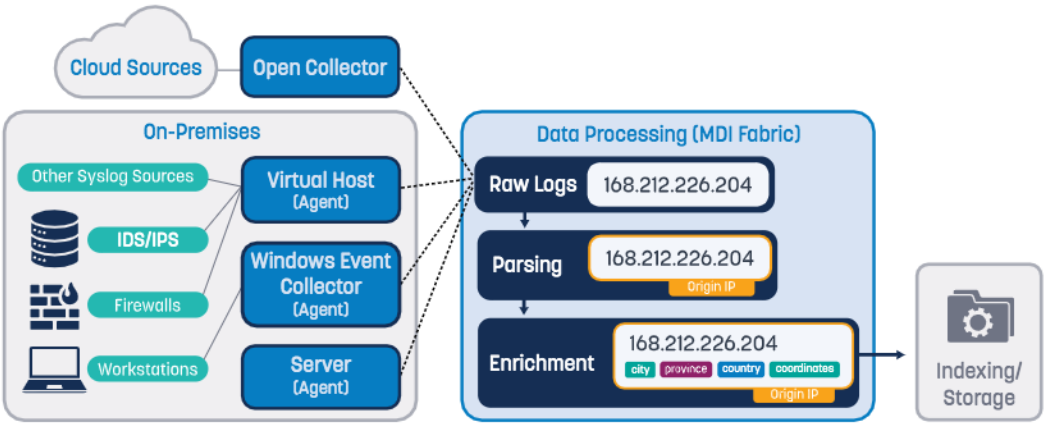

Figure 1: LogRhythm's data collection parsing integration process

LogRhythm centralizes log data from on-prem and cloud environments. MDI Fabric helps process and parse the data into easy-to-understand metadata to help you understand your environment. Specifically, LogRhythm uses the following tools:

- **Endpoint Agent:** This refers to lightweight software installed on a corporate device that collects data. Data transmits from the agent on the endpoint to the SIEM for parsing, enrichment, and normalization. While agents are the most common method of collection, it's also possible to connect directly to the device using a network protocol or API call.
- **Data Transmission:** Data transmits via authenticated and encrypted TLS communications that can be compressed to minimize the use of bandwidth.
- **Data Parsing:** This involves the process of matching logs to rules to determine which text strings need to be mapped to which fields in the database. Mapping to the appropriate fields is a common challenge, yet it's a critical phase in data collection and aggregation to unlock contextualization.
- **Data Normalization:** This involves normalizing various fields, such as time, location, identity, and other critical categories during classification. For example, normalizing for time allows time zone differences so analysts can understand the true timeline of an event. In this process, data enrichment occurs when additional fields are added.

Enhanced Data Collection with Open Collector

- Simplified framework for shipping data
- Built on open-source software with community support
- Greater focus on security (working on adding additional detail)

Available Cloud Sources

This list reflects LogRhythm provided sources that are available today and that offer additional built-in functionality. Other sources are available through the open-source community.

- **AWS S3** (a service that provides object storage through a web service interface)
- **G Suite** (a suite of cloud-computing, productivity and collaboration tools)
- **EventHub** (an Azure collection point for Azure services and sources)
- **Gmail Message Tracking** (a service that allows you to track emails or search for a specific email address or message ID)
- **PubSub** (supports cloud-based, message-oriented middleware technologies including message queuing and publish/subscribe messaging for GCP collection)
- **Sophos Central** (a service that provides logs from their Intercept-x, Endpoint, XG Firewall, Web Protection, Mobile Protection, Email Protection, Sever Protection, Secured Wi-Fi, and Device Encryption)

Learn more about LogRhythm's data collection services. Contact our sales team today.

sales@logrhythm.com

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

www.logrhythm.com