Gartner®

Market Guide for Log Monitoring and Analysis Solutions

8 April 2025 - ID G00817552 - 13 min read

By: Gregg Siegfried, Pankaj Prasad

Initiatives: I&O Operations Management; Evolve Service Management and Cloud Operations

Everything generates log telemetry, making log monitoring and analysis solutions crucial for understanding system and service health and accelerating problem diagnosis. Use this Market Guide to understand the diversity of solutions available and select the products that best support your use cases.

More on This Topic
This is part of an in-depth collection of research. See the collection:

- What I&O Leaders Need to Know About Observability

Overview

Key Findings

- Insights from log data have become vital to enterprises seeking to understand system behavior, analyze performance and carry out faster troubleshooting and root cause analysis.

- The growing volume of logs is increasing the financial pressure on IT operations while difficulty measuring the value of log monitoring and analysis complicates the investment justification.

- Log data is often distributed across a wide geographic footprint and without a centralization strategy — such as telemetry pipelines — in place, analysis is inefficient and diminishes data value.

- Although log monitoring and analysis serves many constituencies such as DevOps, I&O, cybersecurity and product management, organizations struggle to ensure that the right data is available to the right actors at the right time.

Recommendations

- Maximize the value of log data by implementing a telemetry pipeline architecture to enrich, transform and normalize logs and regulate the flow of telemetry to analysis systems. This also reduces operational and governance overhead.

- Expand stakeholder utility by consolidating data from multiple sources into a centralized log monitoring and analysis solution. The central store facilitates comprehensive insights about system behavior and performance, as well as expedited troubleshooting and root cause analysis.

- Increase cost and data efficiency by managing the content, location and retention of log telemetry. Modern log monitoring and analysis solutions include policy-driven capabilities that support this.

- Maximize flexibility by embracing support for open standards such as OpenTelemetry. This goes beyond simply using OpenTelemetry Protocol (OTLP) as a transport. The standardized schema and semantic conventions can simplify analysis as well.

Market Definition

Gartner defines log monitoring and analysis solutions as products that ingest structured and unstructured log telemetry from a variety of sources. They are used to observe and understand the behavior of applications, services and infrastructure. Log monitoring and analysis solutions enable analysis of log telemetry, either via human operator or machine intelligence, to identify or explain changes in system behavior, outages, or performance degradation. Log monitoring and analysis solutions are used by IT operations, security operations, site reliability engineers, cloud and platform teams, application developers, and product owners.

Nearly every element involved with today’s technology delivery platforms generates some form of log telemetry (logs), which can take many forms, as do the tools used to analyze them. Some organizations use logs as diagnostic and investigative tools, only relying on them to explain anomalies and idiosyncrasies, while others use the content of logs to find anomalies, and can generate events and alerts accordingly.

Although most cybersecurity use cases are covered by the adjacent market of security information and event management, there is overlap, with some vendors participating in both markets.

Log monitoring solutions help improve anomaly detection and resolution, customer experience, security stance and compliance with regulatory requirements.

Example use-case scenarios addressed by log monitoring and analysis solutions include:

- **Aggregation:** Short-term storage for operations-related activities like diagnosis, troubleshooting, debugging, root cause analysis, post-mortems, reporting, generic analysis and forensics. Long-term storage can include all of the above use cases, in addition to compliance with regulatory requirements.
- **Analytics:** This includes real-time and offline analytics for tracking and analysis of user and system behavior, with the objective of improving user experience and improving business outcomes. Analytics are also used for assessing the quality of the functional use cases delivered by the applications, and to perform trend analysis.
- **Observability:** Log analysis, sometimes in conjunction with other telemetry signals, provides valuable insights into system and business operations. This includes the solution’s ability to act as a source of events and alerts to upstream IT operations management (ITOM) and IT service management (ITSM) systems.

- **Monitoring:** Log monitoring is primarily used for pattern detection, performance bottlenecks and health assessment, to improve overall uptime and ensure optimal user experience.
- **Security:** This use case for log monitoring solutions is primarily focused on risk and threat detection and analysis, vulnerability assessment, and compliance. A combination of other use cases are used to achieve this, including monitoring, analytics and aggregation.

Many observability platforms and telemetry pipeline tools include log monitoring and analysis capabilities as well.

Mandatory Features

Log monitoring and analysis solutions must have the following capabilities:

- **Ingestion and storage** of structured and unstructured logs from multiple sources, including standard and nonstandard log formats, from applications, operating systems and networks.
- **Parsing and indexing** ingested logs that are collected.
- **Search, analysis and visualization** of logs through different methods, including statistical analysis, pattern recognition, correlations and machine learning (ML), and through manual querying.

Common Features

Log monitoring and analysis solutions commonly include additional capabilities, such as:

- Ability to generate events or alerts based on a variety of criteria, including log content, as well as metadata, such as volume or rate.
- Support for multiple tiers of storage, with a way to migrate data between tiers, based on age or other criteria.
- Custom agents or support for common interfaces, such as syslog or Fluent Bit.
- Federation with other instances or other vendor repositories, allowing users to search across multiple log datasets at once.
- Custom query and analytics language that supports advanced data analysis.

- Native interfaces with other ITOM tools and products, such as automated incident response and ITSM.
- Telemetry pipeline capabilities to collect, enrich, transform and route logs.
- AI-based features, including ML or generative AI.

Market Description

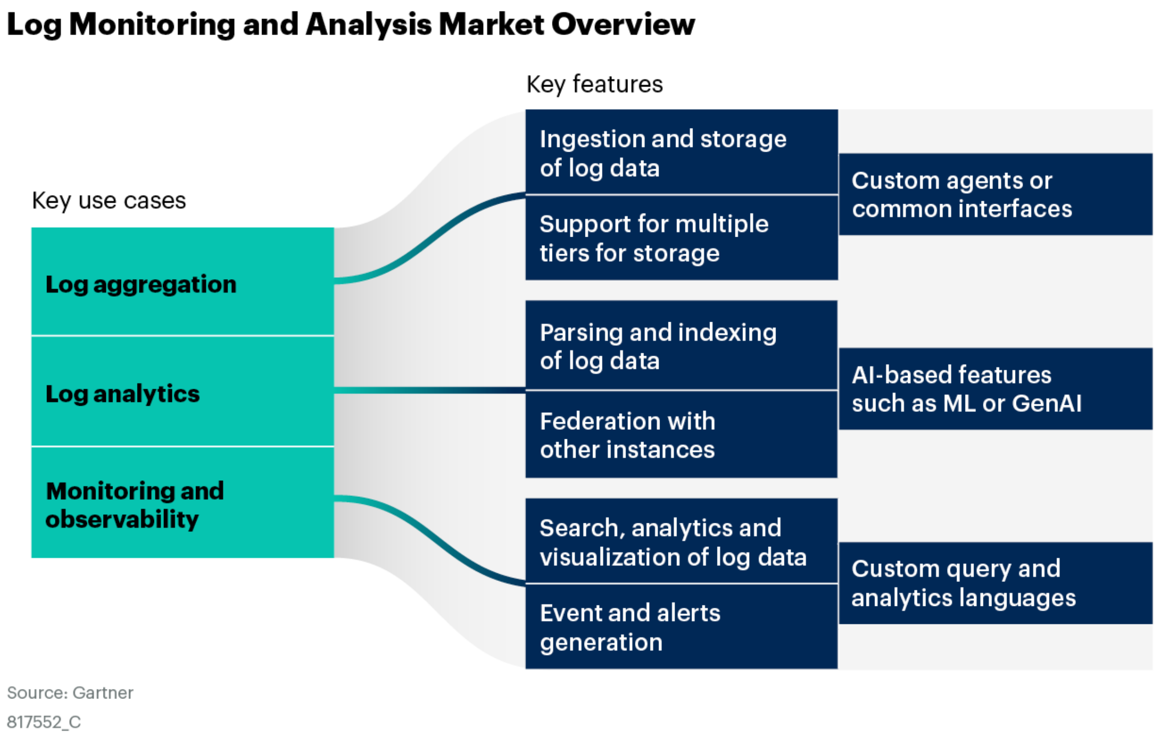
Log monitoring and analysis solutions enable organizations to collect, analyze and act on log telemetry. Logs are created by virtually every component involved in the delivery of IT services — physical and cloud infrastructure, networks, operating systems, middleware platforms and applications. Not all of this data is useful, and the useful data may only be of interest for a limited time.

> **Organizations that use logs only for diagnostics and to identify the cause of a service-affecting issue have different tooling requirements than those that use logs as a source of alerts and events.**

A variety of terminology is used to refer to log monitoring and analysis. Log management, log monitoring and log analytics are three common monikers. Log monitoring and analysis is intended to encompass the full life cycle of collection, analysis, event generation and expiration. In recent years, telemetry pipeline products have arisen to support centralized transformation, enrichment, reduction and routing of log data to potentially multiple analysis solutions. Telemetry pipelines are currently covered as a separate market and, while there are vendors that offer both pipelines and analysis, this Market Guide is centered on the latter.

An overview of the use cases and capabilities associated with log monitoring and analysis solutions can be seen in Figure 1.

Figure 1: Log Monitoring and Analysis Market Overview


Log Monitoring and Analysis Market Overview
Key use cases
Log aggregation
Log analytics
Monitoring and observability
Key features
Ingestion and storage of log data
Support for multiple tiers for storage
Custom agents or common interfaces
Parsing and indexing of log data
Federation with other instances
AI-based features such as ML or GenAI
Search, analytics and visualization of log data
Event and alerts generation
Custom query and analytics languages

Source: Gartner
817552_C

Market Direction

Log monitoring and analysis is not new — many such solutions have been available on the market for years. The ability to collect, analyze and alert upon the contents of logs, especially those in syslog format, has long been included in infrastructure monitoring tools. Splunk, in many ways, spearheaded the idea of centralized log monitoring.

Log data remains the most voluminous flavor of telemetry (although distributed traces may be catching up), and is costly to move around and store. Time series lends itself to aggregation, and individual datapoints are small. Logs can be generated in many different formats, which also poses a problem when trying to analyze them centrally. Free text is giving away to JSON as a standard, but even with JSON, different sources of log data use different nomenclature for the same data — hostname versus nodename for example. What's more, whenever you need to add the word 'and' or 'or' to analysis queries, the margin for error and inefficiency increases.

Stand-alone log monitoring and analysis solutions will continue to exist, but the trend toward embedding these capabilities in other products is clear. Many observability platforms that originally focused on managing metrics and traces, and were intended to integrate with discrete log monitoring and analysis solutions, have implemented advanced log handling of their own. This enables a 'better together' story by allowing more collective, in-place telemetry analysis rather than relying on integration to gain insights from log data.

Telemetry pipeline products also benefit from synergy with log monitoring and analysis. Some log monitoring vendors have begun to offer telemetry pipeline capabilities, and some telemetry pipeline vendors are adding log monitoring and analysis.

Security information and event management (SIEM) tools most resemble log monitoring and analysis in both implementation and use case. It is principally the target audience or buying center that differs the most. There are vendors such as CrowdStrike, Elastic and Cisco that offer products to both I&O and SecOps users for management, analysis and eventing on the contents of log data. Some organizations may choose to take advantage of this synergy rather than using the log management capabilities of their observability platforms or deploying stand-alone log monitoring and analysis products.

Finally, as these are fundamentally data management products, there is no shortage of AI capabilities being added to them, some of which are quite impressive in their ability to deliver enhanced insight and correlation or better cost control.

Market Analysis

The vendor landscape for log monitoring and analysis solutions is relatively stable but competitive. Product capabilities are evolving rapidly on a trajectory similar to that of other cloud-based data management markets. There is a rich open-source ecosystem, with tools such as ClickHouse, Fluent Bit and Grafana Loki in common use.

The easy availability of cloud-based object storage has changed the economics and driven the feature set of log monitoring and analysis tools. This has allowed vendors to build storage tiering into their products directly, enabling customer choice based on cost and data access requirements.

Software as a service (SaaS) remains the dominant delivery model for today's log monitoring and analysis solutions. Some vendors support self-managed instances as well, which may be a requirement for organizations concerned about data sovereignty. Unlike time series data, the chance of logs containing PII or other sensitive data is quite high, so controlling where the data is stored is important. Related to this are features that support the automatic scanning and masking of sensitive data — often aided by AI — that can minimize the risk of unauthorized disclosure. Stand-alone vendors often support federated analysis across multiple instances of their product, so splitting data between cloud-hosted and self-hosted repositories and building cross-instance analytics is viable. However, it is also potentially costly and with uncertain performance.

For most organizations, the benefits of being able to correlate log data with other types of telemetry by storing it in their observability platform's data lake will be hard to ignore. Gartner expects to see the use of stand-alone log monitoring and analysis solutions slow — unless there are special requirements at hand that make this unpalatable. Others, particularly those already colocating SIEM and operations logs, may decide to retain this separation for complexity management or supportability purposes.

> **There are a few vendors that offer all-in-one observability, log analysis and SIEM solutions today, but Gartner has not seen widespread adoption of those to date. Some vendors claim to offer such solutions but they are actually multiple products glued together.**

At present, your deployment choices boil down to:

- Combined observability + log monitoring and analysis
- Combined SIEM + log monitoring and analysis
- Stand-alone log monitoring and analysis

Representative Vendors

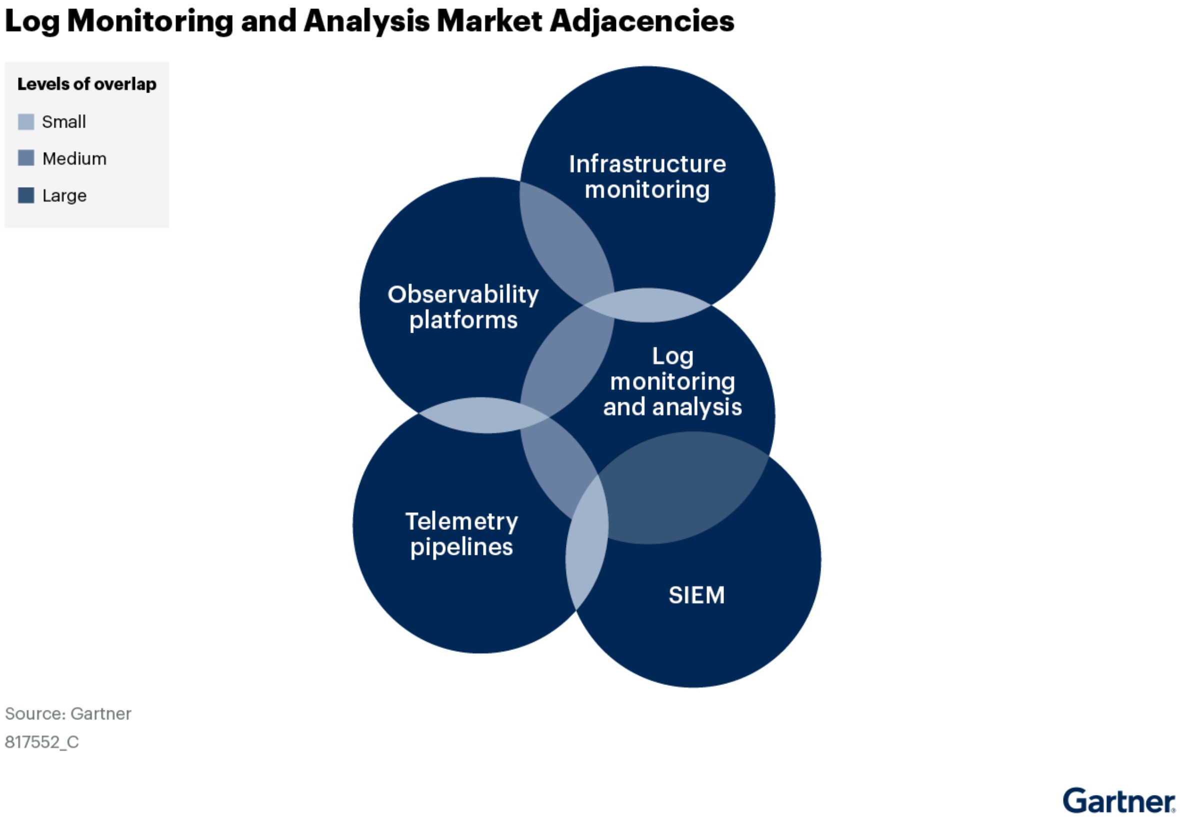
The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Vendor Selection

Log monitoring and analysis covers a lot of ground, and the vendor landscape is quite diverse. This research is centered on I&O, so dedicated cybersecurity log monitoring vendors, or SIEMs (see Magic Quadrant for Security Information and Event Management) are not mentioned unless they also have solutions that address I&O use cases (see Note 1).

Observability platform vendors are increasingly adding log monitoring and analysis features and capabilities to their products as will be evident in the list below. Some traditional log monitoring and analysis vendors are now offering observability platform features and capabilities as well — the trend moves both ways. What is becoming abundantly clear is that it is not necessary to maintain disparate observability and log monitoring solutions if you don't want to. As Figure 2 indicates below, log monitoring and analysis is both adjacent to and overlaps with the observability platforms, SIEM, infrastructure monitoring and telemetry pipeline markets. The degree of overlap varies with SIEM having the most.

Figure 2: Log Monitoring and Analysis Market Adjacencies

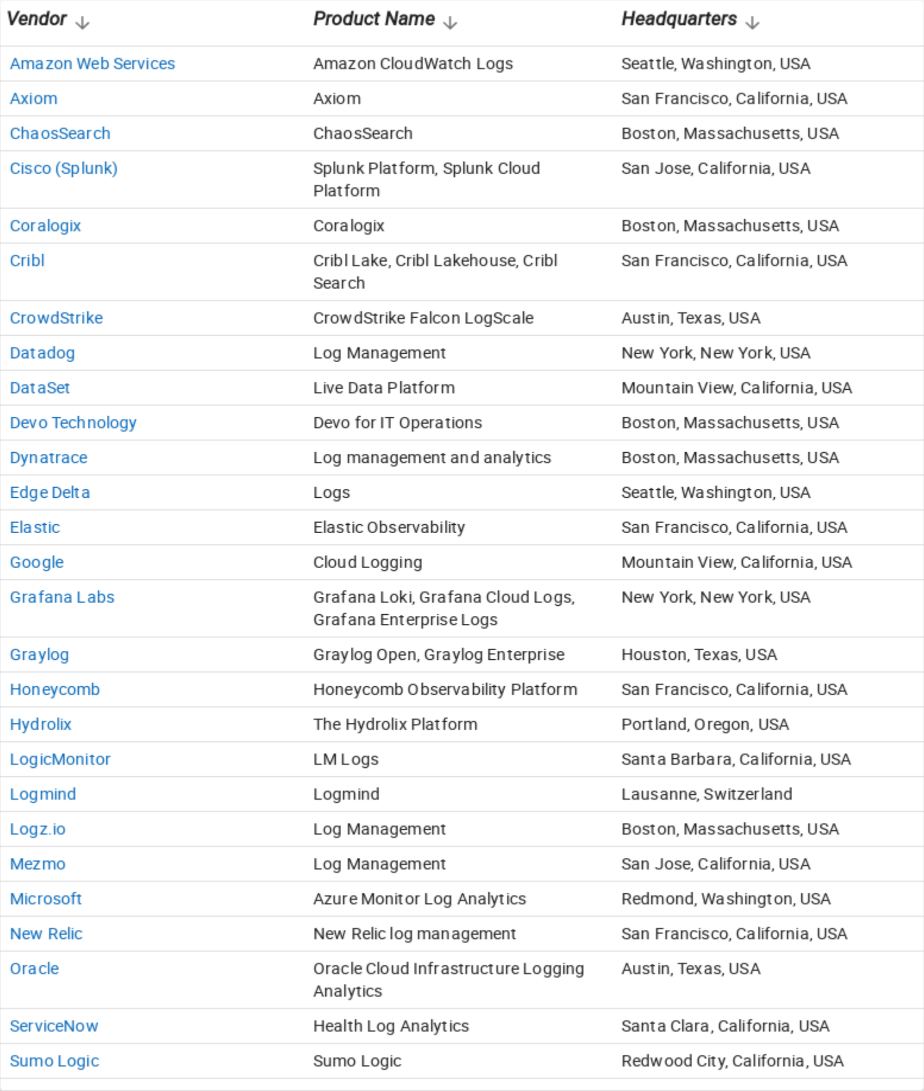

Log Monitoring and Analysis Market Adjacencies
Levels of overlap
Small
Medium
Large
Infrastructure monitoring
Observability platforms
Log monitoring and analysis
Telemetry pipelines
SIEM
Gartner

Source: Gartner
817552_C

See Table 1 for a list of representative vendors for the log monitoring and analysis market.

Table 1: Representative Vendors in Log Monitoring and Analysis

(Enlarged table in Appendix)



Vendor	Product Name	Headquarters
Amazon Web Services	Amazon CloudWatch Logs	Seattle, Washington, USA
Axiom	Axiom	San Francisco, California, USA
ChaosSearch	ChaosSearch	Boston, Massachusetts, USA
Cisco (Splunk)	Splunk Platform, Splunk Cloud Platform	San Jose, California, USA
Coralogix	Coralogix	Boston, Massachusetts, USA
Cribl	Cribl Lake, Cribl Lakehouse, Cribl Search	San Francisco, California, USA
CrowdStrike	CrowdStrike Falcon LogScale	Austin, Texas, USA
Datadog	Log Management	New York, New York, USA
DataSet	Live Data Platform	Mountain View, California, USA
Devo Technology	Devo for IT Operations	Boston, Massachusetts, USA
Dynatrace	Log management and analytics	Boston, Massachusetts, USA
Edge Delta	Logs	Seattle, Washington, USA
Elastic	Elastic Observability	San Francisco, California, USA
Google	Cloud Logging	Mountain View, California, USA
Grafana Labs	Grafana Loki, Grafana Cloud Logs, Grafana Enterprise Logs	New York, New York, USA
Graylog	Graylog Open, Graylog Enterprise	Houston, Texas, USA
Honeycomb	Honeycomb Observability Platform	San Francisco, California, USA
Hydrolix	The Hydrolix Platform	Portland, Oregon, USA
LogicMonitor	LM Logs	Santa Barbara, California, USA
Logmind	Logmind	Lausanne, Switzerland
Logz.io	Log Management	Boston, Massachusetts, USA
Mezmo	Log Management	San Jose, California, USA
Microsoft	Azure Monitor Log Analytics	Redmond, Washington, USA
New Relic	New Relic log management	San Francisco, California, USA
Oracle	Oracle Cloud Infrastructure Logging Analytics	Austin, Texas, USA
ServiceNow	Health Log Analytics	Santa Clara, California, USA
Sumo Logic	Sumo Logic	Redwood City, California, USA

Source: Gartner (March 2025)

Market Recommendations

I&O leaders looking to derive insights from and gain control of log telemetry should:

- **Identify data sources:** Before selecting a log monitoring platform, IT leaders should identify potential log data sources. They should develop a comprehensive strategy for infrastructure, network, application, cloud, SaaS and automation domain logs.

- **Define architecture:** Establish and maintain architecture patterns for the flow of telemetry from managed workloads to the analysis tools used to process it. Use of a telemetry pipeline to process and shape the data may be beneficial, but is not a requirement for responsible log data management.

- **Prioritize centralized management:** Choose log solutions that support multiple use cases and can be managed centrally to ease administrative and management overhead. Select tools that ease data exchange with different groups and enable correlation between logs, traces and metrics.

- **Establish governance:** Increase efficiency by governing the content, location and retention of log telemetry. This falls under the heading of telemetry life cycle management and is very similar to the governance processes that data teams use to manage business data. Many log monitoring and analysis solutions include policy controls that can simplify this.

- **Use AI enablement:** Automate analysis and insight generation using the AI features of log monitoring and analysis solutions. These can range from source identification to anomaly detection to root cause analysis. Not only can capabilities like these accelerate problem resolution, they may improve time to value as well.

- **Implement log data life cycle:** For solutions that support tiering, implement a log data life cycle strategy that prioritizes high-performance storage for recent logs (less than seven days old) while transitioning older data to cost-effective, lower-performance storage. This ensures optimal query performance and reduced infrastructure costs.

Note 1: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Innovation Insight: Log Monitoring and Analysis Solutions

Log Management for Security Operations Use Cases

Hype Cycle for Monitoring and Observability, 2024

Solution Path for Optimizing Monitoring and Observability

Integrate Observability and Security to Mitigate Risk

Magic Quadrant for Observability Platforms

Critical Capabilities for Observability Platforms

Guidance Framework for Deploying Centralized Log Management and Monitoring

Table 1: Representative Vendors in Log Monitoring and Analysis

Vendor ↓	*Product Name* ↓	*Headquarters* ↓
Amazon Web Services	Amazon CloudWatch Logs	Seattle, Washington, USA
Axiom	Axiom	San Francisco, California, USA
ChaosSearch	ChaosSearch	Boston, Massachusetts, USA
Cisco (Splunk)	Splunk Platform, Splunk Cloud Platform	San Jose, California, USA
Coralogix	Coralogix	Boston, Massachusetts, USA
Cribl	Cribl Lake, Cribl Lakehouse, Cribl Search	San Francisco, California, USA
CrowdStrike	CrowdStrike Falcon LogScale	Austin, Texas, USA
Datadog	Log Management	New York, New York, USA
DataSet	Live Data Platform	Mountain View, California, USA
Devo Technology	Devo for IT Operations	Boston, Massachusetts, USA
Dynatrace	Log management and analytics	Boston, Massachusetts, USA
Edge Delta	Logs	Seattle, Washington, USA
Elastic	Elastic Observability	San Francisco, California, USA
Google	Cloud Logging	Mountain View, California, USA

Vendor ↓	*Product Name* ↓	*Headquarters* ↓
Grafana Labs	Grafana Loki, Grafana Cloud Logs, Grafana Enterprise Logs	New York, New York, USA
Graylog	Graylog Open, Graylog Enterprise	Houston, Texas, USA
Honeycomb	Honeycomb Observability Platform	San Francisco, California, USA
Hydrolix	The Hydrolix Platform	Portland, Oregon, USA
LogicMonitor	LM Logs	Santa Barbara, California, USA
Logmind	Logmind	Lausanne, Switzerland
Logz.io	Log Management	Boston, Massachusetts, USA
Mezmo	Log Management	San Jose, California, USA
Microsoft	Azure Monitor Log Analytics	Redmond, Washington, USA
New Relic	New Relic log management	San Francisco, California, USA
Oracle	Oracle Cloud Infrastructure Logging Analytics	Austin, Texas, USA
ServiceNow	Health Log Analytics	Santa Clara, California, USA
Sumo Logic	Sumo Logic	Redwood City, California, USA

Source: Gartner (March 2025)