chronosphere

# Chronosphere Telemetry Pipeline

Transform logs at the edge to boost your InfoSec posture and reduce SIEM costs

## The Impact of Growing Log Volumes on Security

Over the past year, organizations experienced 250% log data growth on average. This level of telemetry growth creates several challenges for InfoSec teams:

### Rising Costs Create Data Silos:

It's increasingly cost-prohibitive to centralize and retain large volumes of data in a SIEM tool. As a result, teams silo logs across data sources, SIEM endpoints, and storage targets, impacting both threat detection and investigations. Additionally, short retention policies may cause teams to lose access to data needed to investigate a breach.

### Poor Data Quality Slows Investigations:

Security data comes in various formats from different sources. This inconsistency can make it harder to locate the information you need during an investigation. Moreover, teams often lack contextual information that can speed up analysis.

### Increasing Compliance and Data Protection Requirements:

Organizations need to comply with a growing number of regulatory standards. This puts increasing pressure on InfoSec teams to protect sensitive information in their logs and retain events to meet compliance requirements.

## The Solution: Take Control Over Your Security Data

From the creators of Fluent Bit and Calyptia, Chronosphere Telemetry Pipeline enables you to seamlessly manage logs from any source to any destination. It integrates with your existing sources in minutes, enabling turnkey processing and giving you the freedom to find the right security tool for your needs.

### Reduce SIEM Costs:

Eliminate log data waste by centrally filtering out noise. By optimizing your data, you can reduce the TCO of your SIEM tooling and free capacity for new datasets.

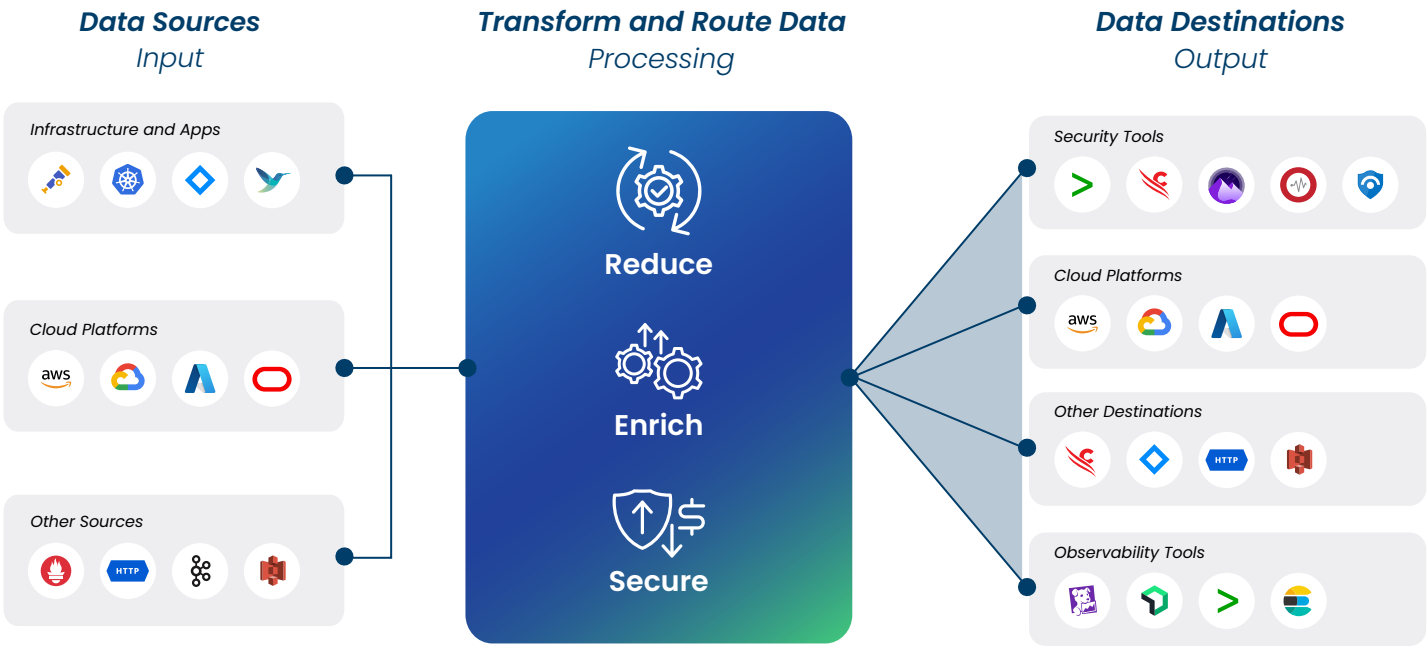
### Enrich and Normalize Data in Real Time:

Enrich logs with information from third-party sources, such as GeoIP or threat feed data. Normalize data from many different sources, simplifying investigations downstream.

### Meet Compliance Requirements:

Run Telemetry Pipelines locally to redact PII and other sensitive information from your logs before the data leaves your environment. Route a copy of every log to low-cost archive storage to ensure long-term retention.

# How it works




### Collect and Route Logs From Any Source to Any Destination

- **Seamless Integration:** Integrate with dozens of data sources and destinations OOTB, such as Splunk, CrowdStrike, Kafka, Graylog, Amazon S3 and more.
- **Quick Onboarding:** Adding new sources and destinations is streamlined with a low-code/no-code interface, without extensive coding.
- **Open-Source Compatibility:** Built on Fluent Bit, with support for all open standards and signals, including OpenTelemetry and Prometheus.
- **Comprehensive Data Routing:** Send logs to destinations that best fit your needs, with support for all formats and protocols.

### Process Logs In-Flight With Turnkey Transformations

- **Enrichment:** Enhance logs with additional context.
- **Redaction:** Automatically redact sensitive data such as PII.
- **Deduplication:** Eliminate duplicate log entries.
- **Enrichment:** Enhance logs with additional context.
- **Compression:** Reduce the size of log data.
- **Parsing:** Convert logs into structured formats.
- **Aggregations:** Combine related log entries.

### Automated Pipeline Operations

- **Automatic Load Balancing:** Distributes log data evenly across the infrastructure.
- **Automatic Retry:** Handles temporary issues by retrying failed data transfers.
- **Automatic Healing:** Detects and resolves issues without manual intervention.
- **Automatic Monitoring:** Continuously monitors the performance and data amount of the pipeline.
- **One-Command Scaling:** Adjust capacity with a single command and set thresholds to automatically increase capacity.

# Built for Performance and Efficiency

Developed by the creators of Fluent Bit, it leverages the proven reliability of the leading open-source log processor.

### Low Infrastructure Cost

- Written in C, it requires **significantly fewer resources** compared to other solutions.
- Over **20x more efficient** than other leading pipeline solutions.

### Kubernetes Native

- Natively integrated with Kubernetes and **deployed as a Kubernetes operator.**
- Full support for Kubernetes **annotations, tolerations, taints, and high availability** with out-of-the-box Kubernetes Fleet Management.

### Fleet Management

- Scalable, **centralized control over Fluent Bit agents** across thousands of machines.
- Simplifies management of **configurations, performance monitoring, and deployment updates.**