CloudFabrix

Optimization of IT Log Data with Log Intelligence

Cyber attacks are getting sophisticated by the minute, necessitating early detection of malicious activity. Stringent government policies and compliances necessitate building robust log management systems.

And, increased reliance on technology to support hybrid work models necessitates efficient management of large log data generated by devices in disparate locations.

Log intelligence is in demand by organizations that need robust systems to address the aforementioned issues and create a secure and efficient Log Management.

Log Management Trends in 2022 and Beyond

CISOs face stringent government regulations, such as the current administration mandating 12-18 months of log retention

- Chief Enterprise Architects worry that the average cost of a single enterprise service outage is $400K and the average MTTR is over 7 hrs.
- Companies such as Facebook lose $65 million and 4.8% of their stock valuation over a 5-hour outage.
- Security breaches mar organizational reputation and prove a threat to business.
- 91% of leaders agree that monitoring tools are siloed and domain-specific, complicating the log management landscape.
- VP Cloud/IT Services acknowledge the accelerated pace of digital transformation post-COVID-19 and recognize the need for more sophisticated security monitoring and SIEM adoption.
- Log management market size reaches $2.3 billion in 2021 and is expected to grow to $4.1 billion by 2026 at a CAGR of 11.9%.

Why are Current Log Management Solutions Falling Short?

Observability tools and security tools have their data collection agent to send data to their data source, which could be any third-party AIOps platform or SIEM tool. These data sources soon turn into data swamps, meaning any kind of data is collected without verifying if it's actionable.

> *In our experience, it's not uncommon to see ten terabytes of data ingested into these data sources. When the data is not processed or qualified, it contributes to a high TCO (Total Cost of Ownership), which includes the people cost, hardware and storage cost and licensing cost. Since most tools are licensed on ingested data, voluminous data unrefined for use increases TCO. Since not all ingested data is actionable, the MTTR (Mean Time to Repair) is exceptionally high as your people try to find a needle in the haystack when incidents and failures happen.*

Current log management systems fall short of delivering on the high expectations of your customers and even your employees, who want to focus on the most critical insights and data and leave the rest to technology.

How Does Sophisticated Log Intelligence Help?

With a future-proof log intelligence solution, you could have any observability or SIEM tool you want as long as it has any endpoints required to bridge the data to the log intelligence solution.

Log Intelligence by CloudFabrix, for instance, brings all of the data into cfxEdge- a high-throughput data collector which can ingest all data into the cloud. Moreover, it can also run preliminary correlation and AI/ML capabilities at the edge to start with.

Once you bring the data into cfxCloud, we have AI/ML pipelines comprising 800+ bots that can route data to multiple locations- any-to-any switch.

Our customers typically keep one copy into an S3/Minio bucket or use Infoblox to enrich the log stream to get more data from the sources. Once the log stream is enriched, we run AI/ML on top of it for correlation.

This may look like:

- Full-fidelity copy in low cost S3 bucket with timestamps
- S3 object log replay from a timestamp to a desired time interval to your choice of stream for security breach or compliance needs
- Looking at it in a schema-agnostic way
- Normalizing/de-normalizing the payload
- Dealing with streaming analytics
- Routing
- Defining the output schema pertaining to any output tools
- Processing notifications

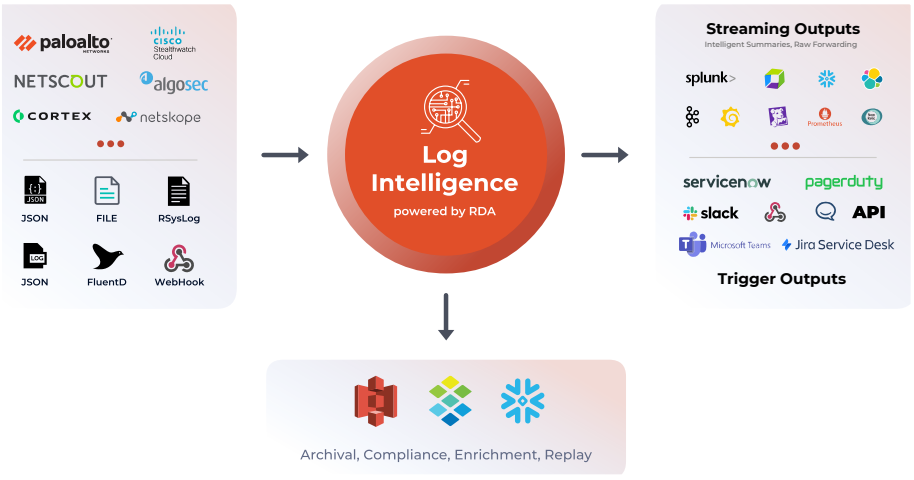
Now, the data is a lot more actionable.

MTTR typically improves by 60% or more, and TCO and licensing costs decrease.

CloudFabrix's Log Intelligence comes with observability pipelines but is a self-service platform, so you can build your own pipelines using bots.

You can also perform in-place analytics for data at the edge for IoT devices and perform basic correlation at the edge itself before you send data to the cloud. Or, you could add in Snowflake for further processing. Everything is possible, courtesy of Robotic Data Automation Fabric by CloudFabrix.

Data integration allows you to connect to data sources on the fly, eliminating the need to write inward agents. Data automation processes data streams, extracts metadata, runs observability pipelines, creates service blueprints and stores artifacts into the cloud platform. Finally, the data intelligence layer uses expendable AI and AIOps Studio alongside AI/ML apps to yield a highly efficient log management solution in a pure cloud environment.



The Key Use Cases of CloudFabrix Log Intelligence

01. Log Reduction, Routing, Replay

Several domain-specific observability tools create a data deluge, which leads to exorbitant storage and archival costs with SIEM and analytics platforms. Correlation and noise reduction across the entire stack can optimize cost and create actionable intelligence.

Customers also need full-fidelity log archival for long-term decision making and compliance purposes. In the wake of audits and security breaches, you may need to replay logs from a particular timestamp. Storing full logs in SIEM and analytical systems can get cost prohibitive. So, customers look to route streaming logs to multiple destinations, such as a low-cost S3 bucket for archival, compliance and replay and selectively to SIEM.

- We record logs with timestamps so that you can go to RDAF in the event of a breach or compliance need to replay the logs from a particular timestamp.
- Leverage observability pipelines with pre-built data bots for aggregation and correlation to lead to noise reduction. Reduce TCO by up to 50% and SIEM costs by 40%, all the while improving predictive analytics for actionable intelligence. You also improve MTTR by 60% with log intelligence.
- Integrate CloudFabrix's Log Intelligence with popular enterprise log/event collectors, firewalls, IPS/IDS devices, security devices, SIEM, XDR platforms and data lakes.
- Route data to multiple destinations- an S3 bucket, a SIEM or an analytics solution.
- Replay logs from the S3 bucket on-demand for auditing and analysis purposes.

02. Log Enrichment

Organizations are now looking to add context by enriching logs and transforming them for unwanted fields or content to enhance searchability with the underlying analytics platform.

- CloudFabrix Log Intelligence enables you to enrich the data while streaming the data.
- Add CMDB, CVE, MITRE ATT&CK, and TIP for better context.
- Perform Geo IP or DNS Lookups or add more verbosity to logs to make them searchable and actionable.
- Trim unwanted fields to improve MTTR and MTTI by 60%.
- Store full fidelity logs to AWS, Azure, and GCP S3 bucket.

3. Log EdgeAI / IIoT and Predictive Analytics

Organizations utilizing the Internet of Things technology want to optimize their log ingestion at the edge and apply intelligence to the decision making of what should be sent to the cloud for correlation. They also need to add verbosity with NLP to the data at the edge.

Enterprises are looking to find patterns, anomalies and alerts using logs at the edge or in the cloud. They also want to leverage AI/ML and analytics solutions such as Snowflake for predictive analytics for real-time log data streams.

- CloudFabrix's Log Intelligence can run a worker node- a small footprint agent- directly on edge to perform correlation before sending the data to the cloud.
- Log Intelligence service reduces edge to cloud costs by 80% using observability pipelines at cfxEdge. The pipelines conduct analysis and send selective logs to cfxCloud over a secure, low-latency network.
- Log Intelligence deploys AI/ML data pipelines for clustering and regression using OpenAI, IBM Watson Databots and NLP pipelines using GPT-3 and Hugging Face Databots.
- Data pipelines boost productivity by over 40%.
- CloudFabrix's Log Intelligence can store data in Snowflake and query selective logs based on query keys from SIEM.

Consumption-Based Model in the Cloud

Finally, everyone from IT, SRE, CloudOps, DevSecOps, Splunk, Elastic, SumoLogic, DataOps and DevOps is wary of additional infrastructural setup for log intelligence.

Log Intelligence service cfxCloud can be deployed on-premises and as an AWS SaaS-based offering for seamless onboarding. cfxCloud reduces the onboarding and POC time by 50% and enables customers to pay only for what they use.

What Sets CloudFabrix's Log Intelligence Apart?

While most providers offer log noise reduction, log data routing and data transformation capabilities, what truly sets our Log Intelligence service apart are:

- Capabilities around Log enrichment
- Log predictive analytics, AI/ML
- Edge to core capabilities with RDAF
- Holistic deployment models- On-premise, SaaS, Hybrid
- Usability- RDA Studio, Bot Marketplace
- Extensibility- Extensions, roboticdata.ai.

Without log enrichment, data lacks context and correlation is poor. Therefore, enterprises can't reduce the volume and subsequent cost of the log data deluge.

What's more, each customer environment is different in its topology and infrastructure. We discover all of that and enrich the logs before correlation. We can do a lot with AI/ML capabilities in terms of clustering, classification and regression.

Ultimately, log intelligence leads to better MTTR, MTTI, low TCO, easy management & higher productivity.

Read more about CloudFabrix Log Intelligence