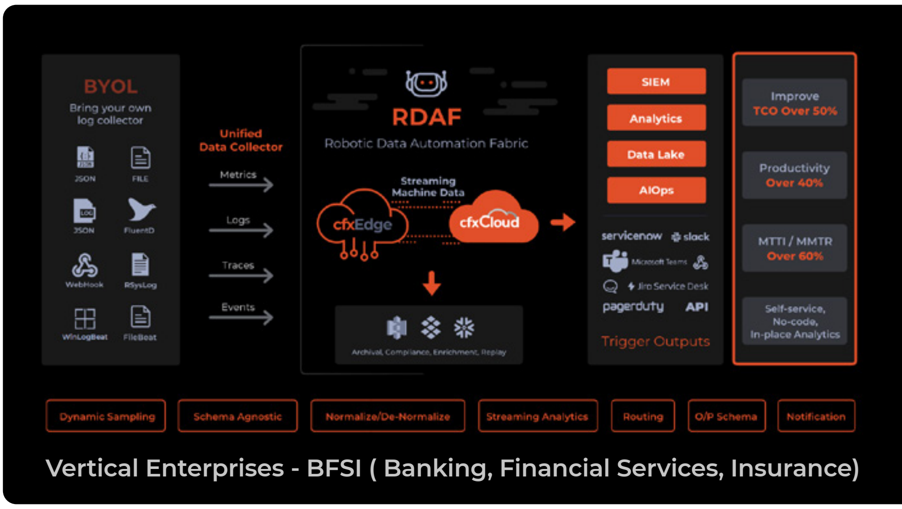
CloudFabrix

Data Intelligence and Automation cfxCloud

Log Intelligence

Right data, at the right time and right place!

Digital First businesses are striving for service assurance, which has become the lifeblood for their business processes. These processes are increasingly getting complex across legacy and cloud native applications, multi-cloud distributed services, the rise of edge and leverage containers, Kubernetes and microservices architectures. Common practice is to collect and analyze logs to make a system observable, as log files contain most of the data from full stack alerts and events. Log Intelligence is very effectively used for implementing cyber secuirty mandates for log retention for 12-18 months, preventing security breaches by optimizing Security Incident and Event Management(SIEM), predictive and business analytics, incident response, cloud automation and orchestration.



Vertical Enterprises - BFSI (Banking, Financial Services, Insurance)

Log Intelligence Use cases, Challenges and Solutions

Log Reduction with aggregation and correlation across diverse data sources

Challenges

- Customers are struggling with plethora of domain specific observability tools which result into data tsunami. This is leading to exorbitant storage and archival costs with SIEM and analytics platforms. Customers are looking for correlation and noise reduction across the full stack for actionable intelligence and cost optimization

Log intelligence Service

- Log Intelligence solution leverages observability pipelines with prebuilt DataBots to aggregate the logs and correlate for noise reduction thus reducing the TCO by up to 50% and reduce SIEM costs by 40% and improving predictive analytics for actionable intelligence.
- The solution integrates with popular enterprise log/event collectors, firewalls, IPS/IDS devices, security devices, Data lakes, SIEM and XDR platforms.

Log Enrichment and DataOps for context

Challenges

- Customers are looking to add context by enriching the logs and transform the logs for unwanted fields/content, to enhance searchability with analytics platform.

Log intelligence Service

- Log Intelligence solution enriches or transform the logs with more context, for example doing geo IP or DNS lookups or adding more verbosity, or trimming for unwanted fields, to make the logs more actionable and searchable improving Mean Time to Insights (MTTI) and Mean Time to Resolution (MTTR) by 60%

Log Routing to multiple destinations for archival, compliance and replay

Challenges

- Customers want full fidelity log archival for long term decision making and compliance as mandated by government bodies and replay purposes when there are audits and security breaches.
- Storing these full logs in SIEM or analytical systems gets cost prohibitive, also ability to replay them on demand becomes important.
- To mitigate this, customers are looking to route the streaming logs to multiple destinations, a low cost S3 bucket for archival, compliance and replay while sending selective logs to SIEM or analytic systems.

Log intelligence Service

- Log Intelligence solution leverages observability pipelines to route data to multiple sources – an S3 bucket, a SIEM and / or analytics system
- The solution also can replay the logs from S3 bucket on demand for audit and analysis on security breaches.

EdgeAI / Industrial IOT (IIOT)

Challenges

- Customers are also looking at optimizing their log ingestion at the edge and apply intelligence on what data needs to be sent to the cloud for correlation.

Log intelligence Service

- The service reduces edge to cloud costs by 80% using observability pipeline at cfxEdge. The pipeline analyzes and sends selective logs over secure and low latency network to cfxCloud.

Log Operational Intelligence with Predictive Analytics and AI/ML

Challenges

- Customers are looking to find patterns, anomalies and alert using logs either at the edge or cloud. They want to leverage AI/ML and analytics solutions like SnowFlake for predictive analytics, for real time log data streams.

Log intelligence Service

- Log Intelligence solution deploys AI/ML data pipelines for clustering, regression leveraging OpenAI, IBM Watson Databots and NLP pipelines using GPT-3 and Hugging Face Databots. The data pipelines improve productivity by more than 40%
- The solution connects with disparate data sinks or visual dashboards with template engines.
- The solution can also store data in SnowFlake and can query selective logs based on query keys from SIEM.

Seamless onboarding as a cloud and edge service

Challenges

- IT, SRE, CloudOps, DevSecOps teams, Splunk, Elastic, Sumo Logic admins, as well as DevOps, DataOps teams are vary of additional infrastructure setup to onboard log intelligence. They are looking for a cloud based service which is each to onboard with pay as you go consumption.

Log intelligence Service

- Log Intelligence service cfxCloud can be deployed on premises, as well as an AWS SaaS based offering for seamless onboarding. Customer has the choice to deploy on premises, in cfxCloud or datapath on premises or customer's VPC with control path in cfxCloud. cfxCloud securely integrates with cfxEdge over a low latency, messaging interface.
- cfxEdge service is deployed at the edge and enables high throughput and intelligent ingest and integrates with cfxCloud on secure, low latency messaging. cfxCloud reduces the onboarding & POC time by 50% and customer only pays for use.

Robotic Data Automation Fabric™

Log Intelligence solution is based on RDAF. RDAF is world's first data fabric architected to unify data observability, AIOps and automation domains and take on the challenges of data intelligence and automation. RDAF consolidates your disparate data sources, converges on the root cause by applying dynamic AI/ML pipelines and concludes by remediating with intelligent automation.

Why Log Intelligence solution?

Consolidate	Converge	Conclude
Improved TCO → Upto 50% reduction in log volumes → log correlation and noise reduction for Data in Motion → Reduce Edge to Cloud costs by up to 80% → Reduce SIEM costs by upto 40% → Pay per use	**Improve Productivity by 40%** → Self service, In-place, No Code IDE to build on the fly data observability pipelines	**Deepen customer insights and business outcomes** → Upto 60% improvement in MTTI / MMTR → Explainable AI for → Unsupervised, Federated, Reinforcement learning
On the fly integration → disparate historical and real time data sources → Broad endpoints supported → Json, File, Syslog (TCP/UDP), Rsyslog, Fluentd, Filebeat, Webhook → BYOT - Bring your own tool → Support broad open telemetry and cloud tools → Broad SIEM, Operational Intelligence and Visual dashboards support	**Democratize Data access** → Converge by correlating and contextualizing siloed tools → DataOps - Contextualize, Correlate, Transform, Enrich	**Prescriptive Analytics and Data Automation** → Transformed, contextualized and enriched data for SIEM → Anomaly detection → Data Routing, Data Optimization, Data Replay → Event Correlation, Alerting, RCA, Service Management
Optimized Ingest → Parallel high throughput streaming and batch ingest → Secure log ingest at the cfxEdge or cfxCloud → Seamless onboarding	**Reduce risk** → inflight detection and alerting → leverage AI to find patterns, anomalies	**Compliance** → PII Masking, Lineage and Governance for GDPR, CCPA requirements **Lifecycle management and Cloud enablement** → Move your important data to the cloud