Coralogix

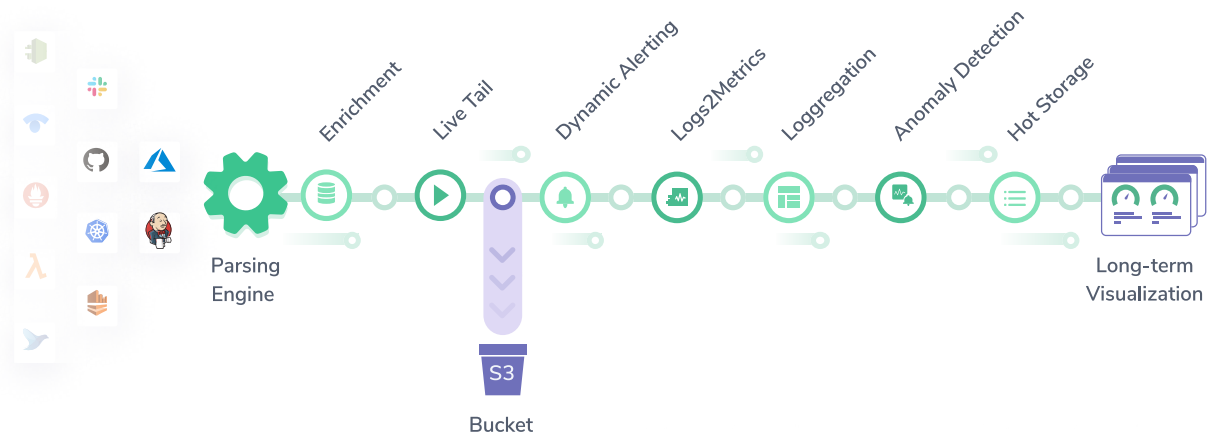
Ensure Compliance with Updated CERT-In Cyber Security Directions

Updated Cyber Security Directions released by the Indian Computer Emergency Response Team (CERT-In) on 28 April, 2022 will require organizations to ***securely maintain log data from all ICT systems for a rolling period of 180 days within Indian jurisdiction***.

Infinite Retention Powered by Streama©

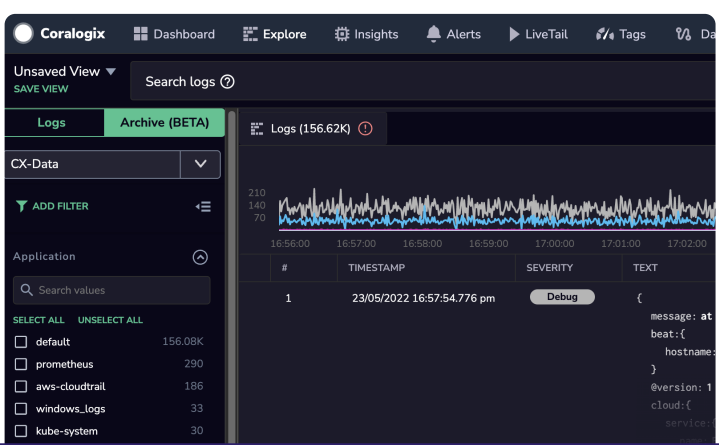
With growing log volumes and increasingly strict retention regulations, the cost of storing and analyzing them with traditional approaches can become a significant challenge and financial burden.

As data enters Coralogix, it is parsed and enriched and then stored in your Amazon S3 bucket. This means no matter what level of analysis and monitoring you need, you always maintain full access to your data for as long as you need it.



Query Your Archive Directly from the Coralogix Platform

Data in your Amazon S3 bucket can be queried directly from the Coralogix UI and CLI using the familiar Elasticsearch syntax, without counting against your daily quota. Data can then be easily exported or reindexed to the Coralogix platform.



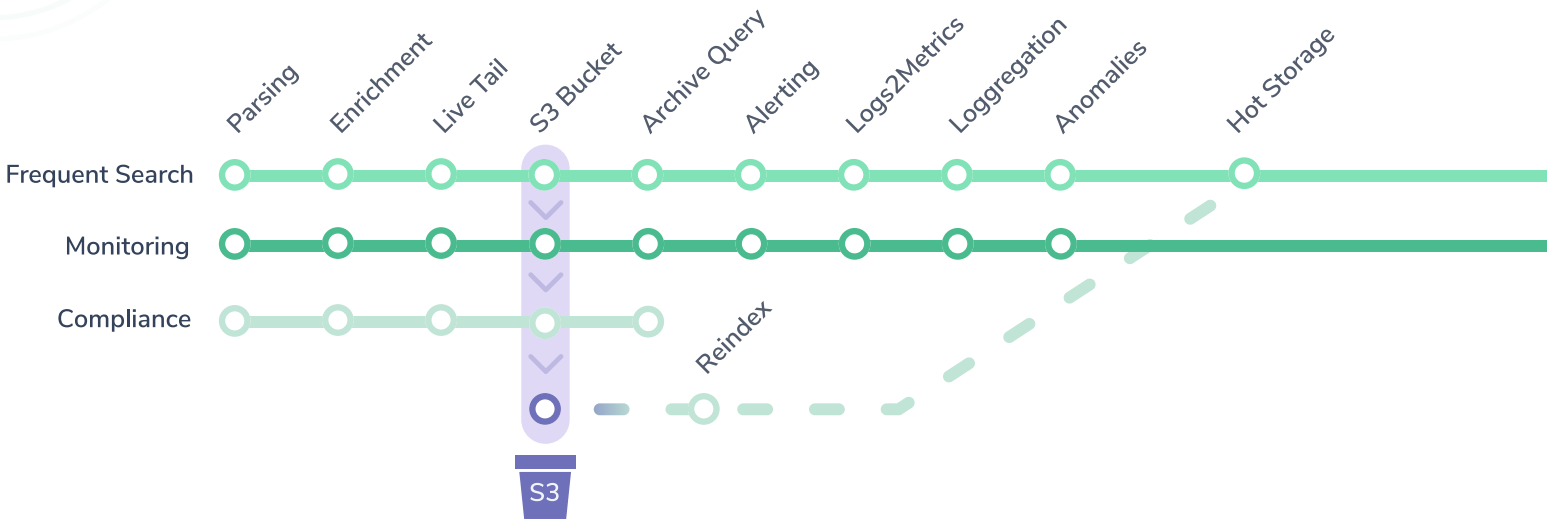
Keep Your Data Secure Within Indian Jurisdiction

- Configure your Amazon S3 bucket to reside in AWS's Mumbai Region
- Maintain complete control over your data, and how long you store it, with much lower costs
- Export archive query results for full compliance with CERT-In's directions

Advanced TCO Optimization & Direct Archive Query

Using the Total Cost of Ownership (TCO) Optimizer, you can assign data to one of three pipelines according to application, subsystem, and log severity level. This means you pay for the value of your data, rather than volume.

With infinite retention afforded by direct archive query feature, data that is selectively indexed can be kept in hot storage with a more limited retention. All data is accessible from the archive regardless of indexing and retention.



Monitoring

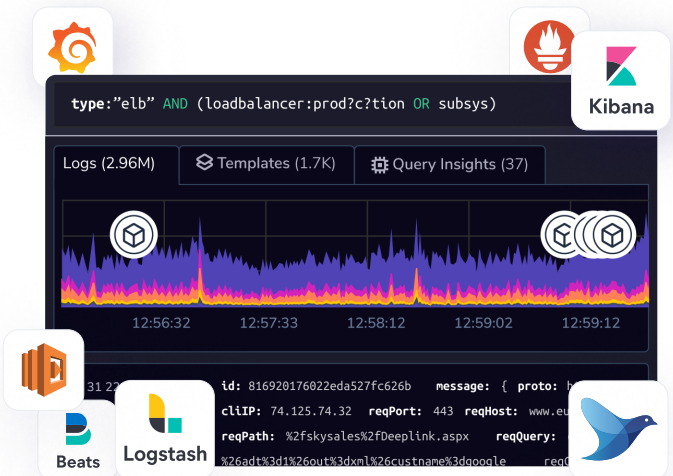
Unlock limitless insights into system health and behavior using advanced analytics and alerting features without needing to index the data.

Frequent Search

Selectively index frequently searched data for lightning-fast query results in addition to insights available in the Monitoring use case.

Compliance

Parse, enrich, and then archive low value data for compliance with the ability to query and export at any time without counting against quota.



Leverage Logs2Metrics to Extract Insights Without Indexing

Generate metrics on the fly from your logs, without ever indexing the raw log data. These metrics are stored for a full year for visualization and alerting at no additional cost.

All metrics can then be viewed in the Coralogix UI, Grafana, SQL clients, Tableau, and Kibana together with logs, tracing, and security data.

> *"We archive logs for compliance and can query them extensively from the Coralogix platform. For logs that we want to convert to metrics, get anomaly detection, and all that stuff we send to Monitoring."*

Vikramaditya M - Lead Engineer

cult.fit