Coralogix

Stateful Streaming Analytics Platform for Logs, Metrics, and Security Data
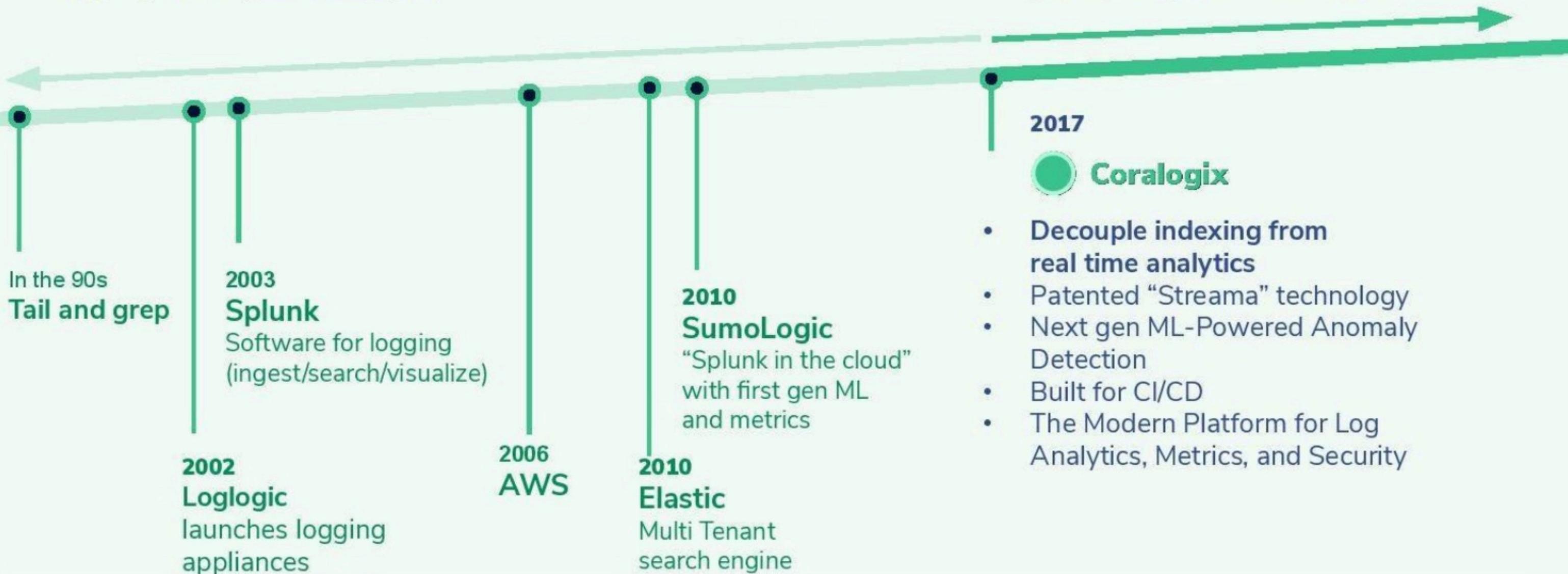
Modern observability with no reliance on storage or indexing

Platforms/Tools to Identify and Resolve Issues

Legacy Solutions are reactive–
Ingest, **Index**, **then Analyze**

Modern Observability is proactive –
Ingest, **Analyze**, then Index

2017

Coralogix

- **Decouple indexing from real time analytics**
- Patented "Streama" technology
- Next gen ML-Powered Anomaly Detection
- Built for CI/CD
- The Modern Platform for Log Analytics, Metrics, and Security

In the 90s
Tail and grep

2003
Splunk
Software for logging
(ingest/search/visualize)

2002
Loglogic
launches logging
appliances

2006
AWS

2010
SumoLogic
"Splunk in the cloud"
with first gen ML
and metrics

2010
Elastic
Multi Tenant
search engine

Coralogix

2

Legacy Solutions

Modern Observability

- **Store logs as unstructured system data**
  High storage costs and overages

- **Triages and prioritizes data before indexing**
  Full data coverage & up to 70% storage savings

- **Analyze data once it's been indexed**
  Reactive, manual alerting; Slow MTTI/MTTR

- **Analyzes data in real time using ML**
  Proactive monitoring; Reduced MTTI/MTTR

- **Data streams are unpredictable**
  Data loss/throttling when quotas are exceeded

- **Auto-scales to meet your needs**
  No overages, throttling or data loss EVER

- **Built for legacy architecture and workflows**
  Incompatibility with modern CI/CD pipelines

- **Born in the cloud, built for CI/CD**
  Proactive monitoring and feedback loops

- **Use proprietary search languages**
  Vendor lock-in, requires full-time SME

- **Uses OS syntax known by most engineers**
  No vendor lock-in, no SME required

Coralogix

Coralogix At-a-Glance

2015 Founded	**2K+** Customers	**10** Fortune 100 Customers	**3M+** Events Processed Per Second
3 Patents for "Streama" Tech	**$40M+** Raised	**9.8/10** G2 Crowd	**500K+** Apps Monitored

Ariel Assaraf, CEO
Veteran of the elite Israeli
intelligence unit 8200. GL at Verint

Matt Handler, COO & Pres.
Former leader at Sumo Logic,
NTT, Whitehat, LogLogic, HP.

Yoni Farin, CTO
Led engineering groups at
Verint and Motorola

Secure by Design

Coralogix is fully compliant with the highest standards of privacy and security and provides multiple geographic data centers for compatibility with various local privacy laws.

Endless Data Integrations

Over 100 integrations - Pluggable API for any integration creation in under 24H

| Code Libraries	Log Shipper	CI/CD	Cloud Providers	Containerization
Python	logstash	Jenkins	AWS	Docker
Java	Fluentd	Circle CI	Azure	Kubernetes
.Net	Filebeat	GitHub	GCP	And Many More...

Any data, Any dashboard, Any syntax

Not a data warehouse, a data platform

Connect any data, in any format, and view anywhere including our purpose-built UI, Kibana, Grafana, SQL clients, Tableau, or using our CLI and full API support.

Avoid vendor lock-in, and streamline setup and adoption in your organization.
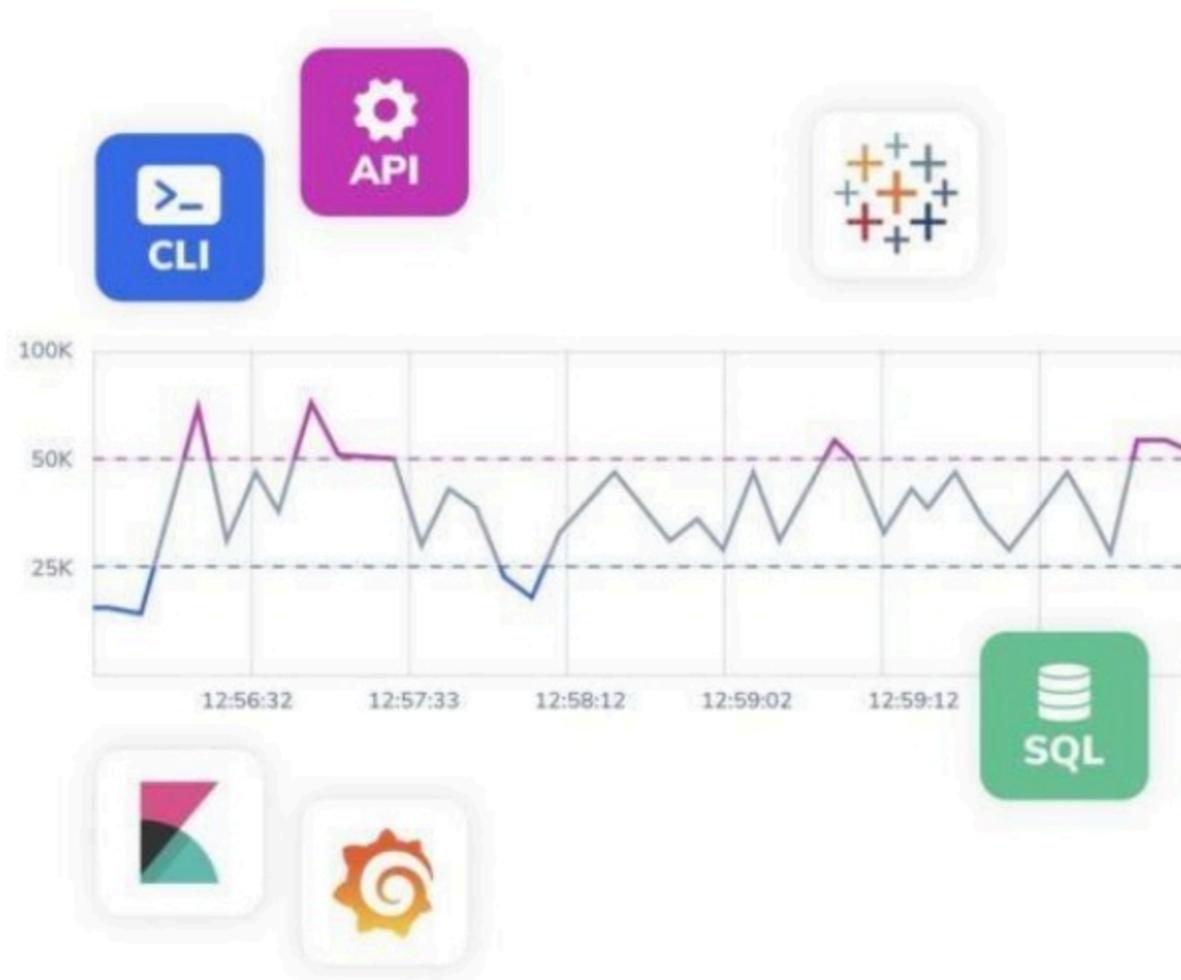
The Coralogix Platform

Full Observability to Build, Run, and Secure Modern Applications & Infrastructures

Log Analysis

Analyze, monitor, and visualize your log data before indexing for proactive insights with no coverage or cost limitations.
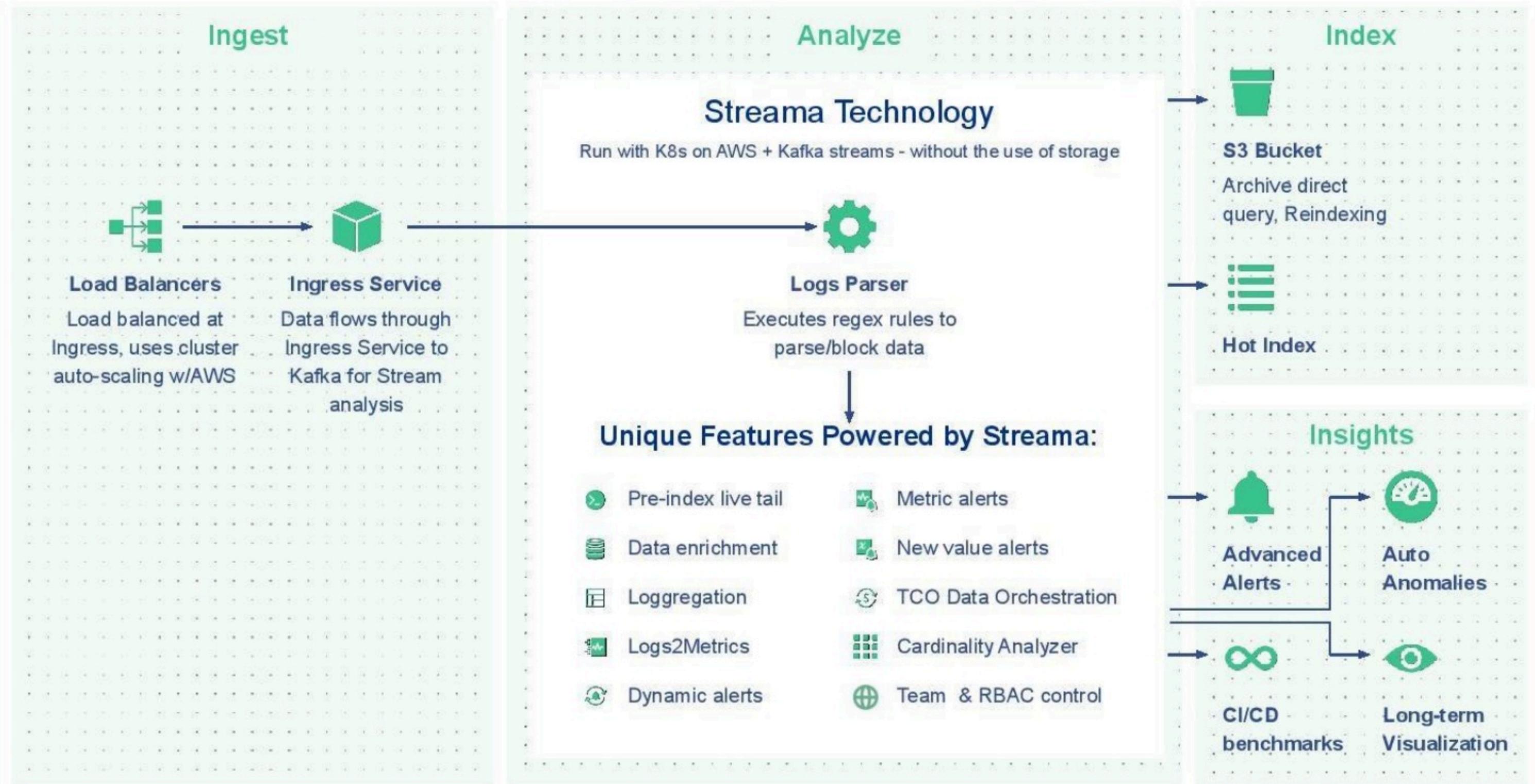
Metrics

Track, visualize, and alert on all system metrics, with unlimited cardinality and labeling for no extra cost.

Security

Fully secure your cloud environments within minutes. Easy to set up, no need for data standardization, no coverage uncertainty.

Coralogix

Ingest

Analyze

Index

Streama Technology

Run with K8s on AWS + Kafka streams - without the use of storage

Load Balancers

Load balanced at Ingress, uses cluster auto-scaling w/AWS

Ingress Service

Data flows through Ingress Service to Kafka for Stream analysis

Logs Parser

Executes regex rules to parse/block data

S3 Bucket

Archive direct query, Reindexing

Hot Index

Unique Features Powered by Streama:

Pre-index live tail

Data enrichment

Loggregation

Logs2Metrics

Dynamic alerts

Metric alerts

New value alerts

TCO Data Orchestration

Cardinality Analyzer

Team & RBAC control

Insights

Advanced Alerts

Auto Anomalies

CI/CD benchmarks

Long-term Visualization

Solutions Powered by Streama

Log Analysis & Metrics

CI/CD Acceleration & Benchmarks

Cost (TCO) Optimization

Network & Cloud Security

Contextual Data Analysis

Homegrown Alternative

Streama powered Log Analytics

ABOVE NORMAL
1.5x

EXPECTED
26%

ACTUAL ERROR RATIO
66%

Feb 24   11:10am   6:40pm   11:40pm   4:40am   9:40am GMT

Between 1:19 AM - 2:19 AM, a sequence of 3 logs was broken by 1 log for V10VE / BECL-Application   WARNING

Log Clustering & Anomaly Detection

Automatically cluster millions of logs at ingestion for faster investigations, higher-level analytics, and more accurate anomalies. Convert data to trackable metrics before indexing to extract previously unattainable system and business insights.

Machine learning algorithms learn your logs, and detect unusual system behavior like error ratio spikes and log flow anomalies without relying on static thresholds.
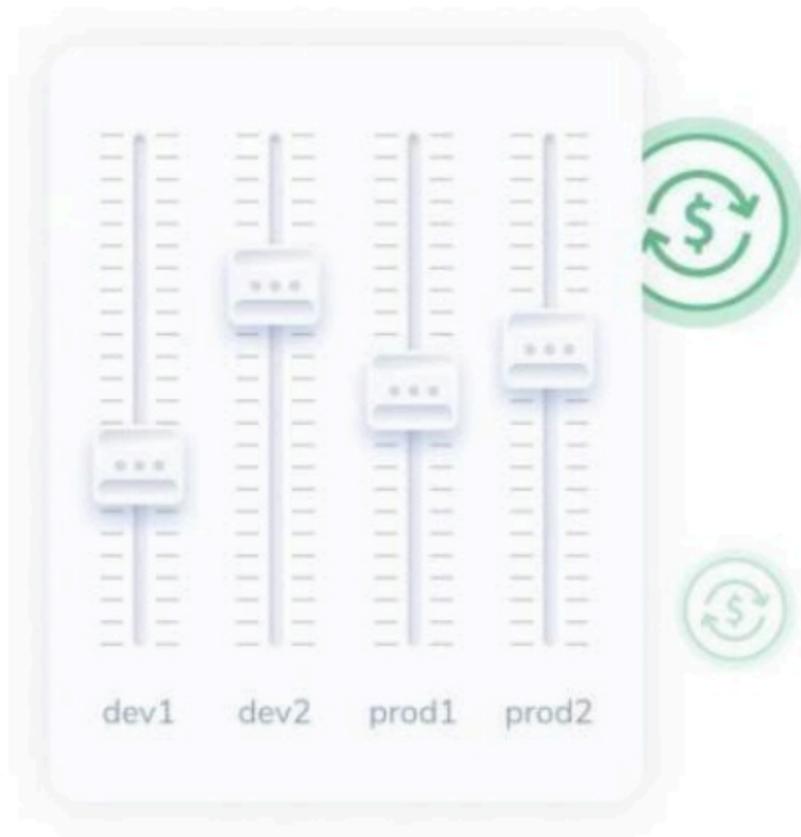
Streama powered Log Analytics

ML-Powered Alerting

The most extensive alerting mechanism in the market, Coralogix pinpoints critical issues and dramatically reduces false positives to avoid alert fatigue. Track the critical parts of your system and SLOs using advanced alerts including:

- Dynamic thresholds
- 'Ratio between' queries
- New value detection
- Cardinality alerts
- Metric Alerts
- Query Flow Alert

🔔 **ALERT**

Too many failed login attempts by a user

12 minutes ago

Login Failed / Login Success in the last 10 minutes has exceeded the ratio of 0.2

Streama powered Metrics

Unlimited Granularity, Cardinality, and Labeling

Pay per GB ingested and access unlimited granularity, cardinality, and labeling with no additional costs. With Coralogix, you get maximum coverage for your systems and minimum complexity when it comes to pricing.

Streama powered Metrics

Seamless Visualization

Gain visibility into unique system and business metrics for better observability. Metricbeat or Prometheus forwarders send metric data for seamless visualization in Kibana and Grafana.

Convert Logs to Metrics

Our Logs2Metrics feature converts log data to trackable metrics, before indexing. The value of your data shouldn't be lost in the noise. This feature extracts a wealth of system and business insights.
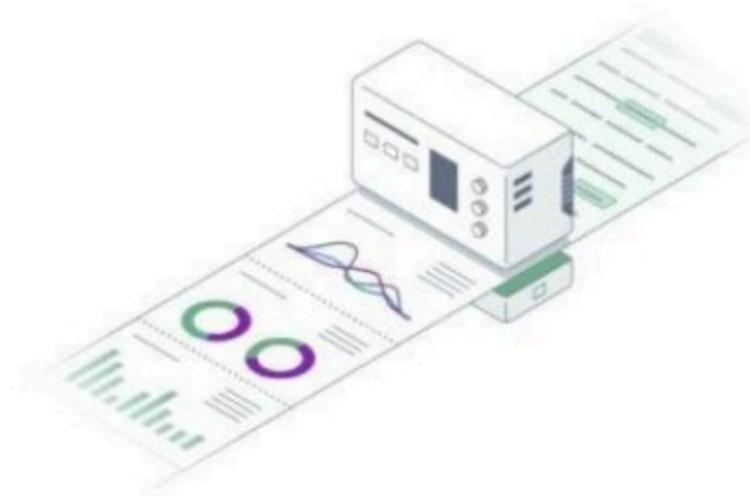
Cloud Security

Mirror Traffic From Any Source

Connect any source of information to complete your security observability, including Audit logs, Cloudtrail, GuardDuty or any other source. Monitor your security data in one of 100+ pre-built dashboards or easily build your own using our variety of visualization tools and APIs.

CloudTrail

VPC Flow Logs

AuditBeat

Syslog

Packet Data