Coralogix

The SaaS Observability Survival Guide

BY JOANNA WALLACE

ENGINEERING MANAGER

3 INTRODUCTION

<PART 1>

4 BREAKDOWN OF CATEGORIES

5 LOG ANALYTICS
5 ARCHIVING CAPABILITIES
6 TRACING AND APPLICATION PERFORMANCE MONITORING
6 ALERTING
6 INTEGRATIONS
7 COMPLIANCE
7 SUPPORT
8 COST AND SCALABILITY OF PRICING

<PART 2>

9 COMPARING SAAS OBSERVABILITY SOLUTIONS

12 LOG ANALYTICS
12 ARCHIVING CAPABILITIES
13 TRACING AND APM
13 ALERTING
14 INTEGRATIONS
15 COMPLIANCE
15 SUPPORT
16 COST AND SCALABILITY OF PRICING

<PART 3>

17 CORALOGIX AND WHY IT’S UNIQUE

18 THE STREAMA ARCHITECTURE
18 COST OPTIMIZATION FOR EVERYONE
18 ACCESS YOUR ARCHIVE WITH REMOTE QUERY
19 THE MOST SOPHISTICATED ALERTING ON THE MARKET
20 THE BEST SUPPORT ON THE MARKET

21 SUMMARY

INTRODUCTION

The microservice architecture allows companies to adopt an agile method of building and deploying software. This architecture makes building, deploying, and scaling applications easier. The downside is microservice architectures are more difficult to detect and troubleshoot problems in specific components.

SaaS observability providers can give companies insight into how their microservice software functions. They can reduce resolution times and improve user experience without needing in-house teams to analyze high-volume data. In this eBook, you will see four observability providers on the market and how their solutions differ. The aim is to show what to assess when choosing an observability provider and to give insight into which fits your needs.

<PART 1>

BREAKDOWN OF CATEGORIES

To properly assess SaaS observability vendors, we need to categorize essential features. The chosen features are critical to implementing an insightful, productive, cost-effective observability platform. The categories used to differentiate between vendors include the following list:

LOG ANALYTICS

Log Analytics attempts to make sense of an extensive set of log data. A human cannot read hundreds or thousands of logs and make sense of what is happening in the system. Log analytics process the data, making it human-readable so systems engineers and DevOps teams can understand system behaviors. These can help with troubleshooting, compliance audits, and detecting suspicious activity.

Log analysis processes include log centralization, queries, aggregations, and machine-learning analysis. Each has a different purpose and helps achieve observability. Virtually all observability solutions have some form of log centralization and queries. However, aggregation and effective machine-learning algorithms are more vital for successful observability. Machine learning algorithms should grow as your system evolves so newly formed issues can be quickly found and fixed. While machine learning and log analytics may be built in-house, it takes a lot of time and specialized expertise to generate such a system and is usually not cost-effective. SaaS solutions are functional out of the box.

ARCHIVING CAPABILITIES

Archiving Capabilities are needed by any observability SaaS platform to retain historical data for troubleshooting and KPI analysis or to keep adequately long historical information to meet compliance regulations. Compliance requirements need to balance with the added cost and time to run data analysis on large data sets, meaning users need to choose which data is archived carefully. SaaS observability providers ideally give some method to query archived data so it can be used when necessary.

SaaS observability providers can forward observability data to a self-managed storage solution. Long-term storage is generally optimized for size instead of query speed to reduce cost since the data will be used infrequently. Some providers allow for querying directly on these data stores.

TRACING AND APPLICATION PERFORMANCE MONITORING

Tracing is the ability to track a request as it travels through a system. An input can trigger a trace, such as a user clicking a button. Once initialized, a root span will track all events resulting from the input. The entire path of the event can be followed and used to find bottlenecks or errors in a microservice architecture.

Traces are essential in microservice architectures to achieve observability and application performance monitoring (APM). APM tools will use trace data to show where application and infrastructure resource consumption is occurring in your system. These metrics are critical for keeping MTTR low and customer satisfaction high.

ALERTING

Alerting allows DevOps teams to receive notifications when there is a problem in the system requiring acknowledgment. Alerts are sent when a metric exceeds preset thresholds.

SaaS observability offerings can provide static and dynamic thresholds for alerts. Static thresholds require your team to define when the system should send an alert. Static thresholds are very difficult to define for most metrics and often cause false positives where the team would receive an alert when there is no problem with the system. Dynamic alerts rely on machine-learning algorithms to set thresholds for alerts. The better the algorithm can adapt to your software system, the fewer false positive alerts are expected.

INTEGRATIONS

Integrations in SaaS observability refers to an assemblage of third-party systems that can communicate and form a cohesive system. Integrations are built by each SaaS provider or the tool they are linking to. The more integrations the SaaS provider offers, the more opportunity a company has to integrate since they are more likely to meet requirements.

Integrations may be with third-party providers that generate observability data. These include cloud providers that run software like AWS and Azure and each cloud provider's various services. Integrations may also be with cluster management systems like Kubernetes. At a lower level, integrations with observability standard solutions like Open Telemetry can also be useful. If the SaaS observability provider does not include built-in visualizations, an integration with a tool like Grafana may be required. Providers may include such connections simply to meet user preferences as well.

COMPLIANCE

Compliance requirements are different for companies depending on their location and industry. Health technology companies in the USA must comply with HIPAA; parts of this compliance are ensuring all data is encrypted and implementing two-factor authentication. The GDPR applies to all technology companies with applications in Europe; one aspect of this compliance regulation is to ensure personal data is encrypted to reduce the probability of a data breach.

Observability providers will receive a large amount of data from your software system. As a result, the provider should act according to the regulations your company is bound by. Some companies store compliance data in long-term storage and observability data to ensure analysis is possible when a breach occurs. This is possible when the vendors hold the accreditation needed to meet the regulation.

SUPPORT

SaaS observability providers all provide some sort of customer support. This support is needed when users are stuck on integrations, need help analyzing or visualizing data, or need help with cost optimization or scaling.

Support can be provided in different ways. Documentation, FAQs, and sample projects are all forms of support that should be easy for users to find as a first step to solving their problems. These documents can also inform users of features they may need to be aware of.

Support should also include the ability to talk to someone when documentation is insufficient. This type of support can sometimes be locked behind a paywall, so request an account with a support package to meet your needs.

COST AND SCALABILITY OF PRICING

Many SaaS observability providers offer an inexpensive or free tier. However, observability consumes a considerable amount of data, and the cost may not scale expectedly for every observability provider. When choosing a SaaS provider, compare data storage, analysis, and transmission rates to ensure basic functionality falls within budget. Users sometimes need to choose between the cost and efficacy of their solution by reducing data sent to the SaaS provider to keep costs manageable.

SaaS observability providers sometimes use tiered accounts or hide some features behind a paywall. When determining which provider to use, look for the features you would want to use now and in the future to ensure they will be accessible.

<PART 2>

COMPARING SAAS OBSERVABILITY SOLUTIONS

FEATURE	CORALOGIX	DATADOG	SUMO LOGIC	ELASTIC
LOG ANALYTICS	Centralization Log queries Machine Learning Automatic aggregation	Centralization Log queries	Centralization Log queries Machine Learning Automatic aggregation	Centralization Log queries Machine Learning Custom aggregation
ARCHIVING CAPABILITIES	Data forwarding Automatic data forwarding for compliance Queryable archive with results in under 1 minute	Data forwarding	Data forwarding Automatic log forwarding to AWS S3 Ingest archived data using time range (maximum 12 hours)	Data lifecycle management Queryable cold tier
TRACING AND APPLICATION PERFORMANCE MONITORING	Application resource consumption Infrastructure resource consumption Kubernetes and AWS EC2 support	Infrastructure resource consumption End-to-end APM Kubernetes and AWS EC2 support	Infrastructure resource consumption Load consumption	Infrastructure resource consumption Load consumption
ALERTING	Static threshold alerting Dynamic threshold alerting Anomaly detection	Static threshold alerting Anomaly detection	Static threshold alerting Dynamic threshold alerting Anomaly detection	Static threshold alerting Anomaly detection
INTEGRATIONS	AWS Microsoft Azure Google Cloud Platform Container Orchestration (e.g. Kubernetes) Prometheus Open Telemetry And more	AWS Microsoft Azure Google Cloud Platform Container Orchestration (e.g. Kubernetes) Prometheus Open Telemetry And more	AWS Microsoft Azure Google Cloud Platform Container Orchestration (e.g. Kubernetes Monitoring) Prometheus Open Telemetry And more	AWS Microsoft Azure Google Cloud Platform Container Orchestration (e.g. Kubernetes) Prometheus Open Telemetry And more

FEATURE		CORALOGIX	DATADOG	SUMO LOGIC	ELASTIC
COMPLIANCE	GDPR	✓	✓	✗	✗
	CCPA	✓	✓	✗	✗
	HIPAA	✓	✓	✓	✓
	ISO/IEC 27001	✓	✓	✓	✓
	ISO/IEC 27701	✓	✗	✗	✗
	PCI	✓	✗	✓	✓
	SOC 2 TYPE II	✓	✓	✓	✓
SUPPORT		↘ Tutorials ↘ Code samples ↘ Support via chat available 18h/day and 7days/week ↘ Issues discussed within 2 minutes	↘ Tutorials ↘ Code samples ↘ Support via chat (account dependent) ↘ General issues are discussed within 12 business hours with premium support	↘ Tutorials ↘ Code samples ↘ Service support via tickets ↘ General issues are discussed within 1 business day with premium support	↘ Tutorials ↘ Code samples ↘ Support via chat (account dependent) ↘ Development support within 2 business days with a development account
COST AND SCALABILITY OF PRICING		↘ Consistent price per GB of analysis ↘ No feature lockout	↘ Variable price per GB of analysis (based on used feature) ↘ Features separated into account packages	↘ Variable price per GB of analysis (based on used feature) ↘ Features separated into account packages	↘ Variable price per GB of analysis based on cluster configuration ↘ Features separated into tiered account packages

LOG ANALYTICS FEATURES IN SAAS OBSERVABILITY SOLUTIONS

Each of the compared SaaS observability solutions provides customizable capabilities for log analytics. These include event counts, statistical operations like averages and percentiles, and interpolations.

Coralogix, Sumo Logic, and Elastic provide machine-learning models for log analytics. This analysis will learn the typical behaviors of your software system and can notify you when abnormal behavior is detected. Elastic also allows users to manually configure machine learning models when the preconfigured models are insufficient, but this requires specialized expertise.

Coralogix and DataDog also provide pattern aggregation features for logs. These convert logs into metrics when similar values are detected in the log data. This conversion enhances pattern recognition and allows for a straightforward graphical representation of log events.

ARCHIVING CAPABILITIES IN SAAS OBSERVABILITY SOLUTIONS

All SaaS observability solutions limit how much data is in frequently-queried (hot) storage. This is the most expensive storage and should be reserved only for relevant, recent data. Typically this is at most seven days but can be adjusted. Once the data is older than required, it should be moved to an archive.

Coralogix, DataDog, and Sumo Logic each allow data to be forwarded to an external archive after some time. Data is automatically moved once it expires. Sumo Logic and DataDog have an extra feature where data can be sent directly to the archive when it matches some pre-configured setting. This allows data needed for compliance but not analysis to be stored efficiently.

Elastic is a data storage solution, so instead of sending data to an external archive (like AWS S3), data is sent to a different Elastic cluster. Depending on the query frequency needed, clusters are set up with different storage tiers for hot, warm, or cold data.

Sumo Logic can query archived data but is limited to time-based queries requiring DevOps teams to know when an event occurred to search efficiently. Coralogix allows direct queries to run on archived data using typical query languages like SQL and Lucene. Coralogix has also developed a piped query language named DataPrime that is simple, but allows for powerful and fast event transformations and aggregations. DataPrime enables users to analyze and discover archived data in a sophisticated manner not available through the other providers.

TRACING AND APM FEATURES IN SAAS OBSERVABILITY SOLUTIONS

While traces can provide insight into application performance, complex systems should use a combination of observability data to provide deeper insights into where the system is experiencing bottlenecks and failures.

Coralogix, DataDog, and SumoLogic each provide application performance monitoring using trace data. They all link to OpenTelemetry, allowing them to collect trace data using this standard, open-source model. They can monitor user actions to determine whether performance issues affect user experience.

Elastic contains an APM system built with the Elastic Stack to monitor applications in real time. It collects performance and response time information for different software actions, such as database queries, and uses this information to find performance issues. The APM metrics collection software can augment an existing Elastic observability setup.

ALERTING IN SAAS OBSERVABILITY SOLUTIONS

Coralogix, DataDog, Sumo Logic, and Elastic all provide static alerting capabilities for tracked observability data. Static thresholds can be applied to multiple metrics with some statistical logic applied to the data, such as averages, sums, or maximum values. Each of the providers has machine-learning capabilities that can be used to set further alarms. These include anomaly detection, forecasting anomalies, and outlier events.

Coralogix provides dynamic thresholds for alerts. A machine-learning algorithm is applied to observability data to track typical behavior for your software. The threshold is automatically adjusted to alert users according to how their system typically behaves. This allows for fewer false alarms than other providers, where DevOps teams respond when an issue is not present in the system.

One unique alert type available through Coralogix is flow alerts. These alerts are triggered when multiple events occur in sequence. For example, a flow alert could be triggered if high CPU usage is followed by HTTP error rates spiking. Coralogix allows users to chain events with OR, AND, and NOT boolean operators allowing for multiple logical combinations of custom alerts. When data is centralized in Coralogix, flow alerts allow users to break typical data silos and create alerts using multiple data sources.

INTEGRATIONS AVAILABLE IN SAAS OBSERVABILITY SOLUTIONS

Integrations allow users to send observability data (metrics, traces, and logs) to the SaaS observability tool for analysis. The SaaS providers may require data to be sent from your software system to the tool, or they may pull the data from your software system. In either case, a secure integration is required.

Coralogix, DataDog, Sumo Logic, and Elastic provide integrations with many common tools. Each provides integrations with major cloud providers Amazon AWS, Google Cloud, and Microsoft Azure. Each SaaS observability provider also connects with container orchestration platforms like Kubernetes. However, Sumo Logic connects to their monitoring service, while others like Coralogix provide deeper integrations with tools like Filebeat and Fluentd.

Open-source metric and trace tools are also commonly required integrations. Prometheus and OpenTelemetry serve each of these observability data needs. Each tool here provides a method to integrate with these open-source tools. Sumo Logic, for example, uses Telegraf to collect and send metrics from Prometheus to its collector. Coralogix provides a remote-write connection using the Prometheus operator when using it within a Kubernetes native deployment.

COMPLIANCE CREDENTIALS

Each SaaS observability vendor has a breadth of security and compliance credentials. Before choosing a vendor, knowing which credentials you will need to meet before vendor lock-in is best. If your company may need to adhere to new compliance regulations, choose a vendor with a breadth of accreditations to increase the likelihood of support.

DataDog, Sumo Logic, and Coralogix offer a SaaS-only deployment. This means there is no option for on-premise deployment. Some companies may not be able to use these services if they have data sovereignty regulations. Without this type of requirement, Cloud-based SaaS providers can comply with regulations.

SUPPORT FROM SAAS OBSERVABILITY SOLUTIONS

Support comes in different forms to help users plug into a SaaS platform. This includes tutorials, code samples, and support staff to help with specific problems via chat, phone, or email.

Each of the compared SaaS providers provides tutorials and code samples. Some of these may be written by community members to help others integrate with the SaaS platform. When the setup is more complex, more documentation is required. Some documentation can be quite complex, and users may have difficulty following it correctly. Having support staff is helpful when this is the case.

Coralogix provides personalized support over chat to its users. Response times are swift (15s median response time), and 24/7, so you can fix your issue faster. Sumo Logic allows users to create support tickets when a bug is suspected in their service. DataDog and Elastic provide support over chat and email, but the level of support is account-tier dependent.

COST AND SCALABILITY OF PRICING OF SAAS OBSERVABILITY SOLUTIONS

DataDog and Sumo Logic use a pricing model based on available features. Regardless of which features are chosen, there is a cost per GB or the processing unit for data stored on the platforms. Feature sets may include application performance monitoring, cloud security monitoring, and log analytics.

Elastic uses a tiered account model and scales cost per GB of stored data. Each account does include some observability functionality, with the standard and gold accounts having the same observability features and more being added in each of the platinum and enterprise accounts.

Coralogix does not hide any features behind a paywall. The model is to pay only for data usage regardless of what analysis is being done on that data. The technology behind the Coralogix solution analyzes data in-stream without indexing or centralizing data storage, so the platform can provide a unique, scalable pricing solution.

<PART 3>

CORALOGIX AND WHY IT’S UNIQUE

Coralogix differentiates itself from the rest of the market in five clear ways.

THE STREAMA ARCHITECTURE

Coralogix is built on a fundamentally different architecture, called Streama©. The power of Streama is in its scalability. The entire architecture is CPU bound, meaning Coralogix can scale effortlessly to match any demand, instantly. Secondly, Streama is a stream processing architecture. This means data can be routed, transformed, aggregated, and analyzed in stream, before it ever touches a database. This makes Coralogix far more scalable than any other vendor on the market, and means that Coralogix runs at a fraction of the cost.

COST OPTIMIZATION FOR EVERYONE

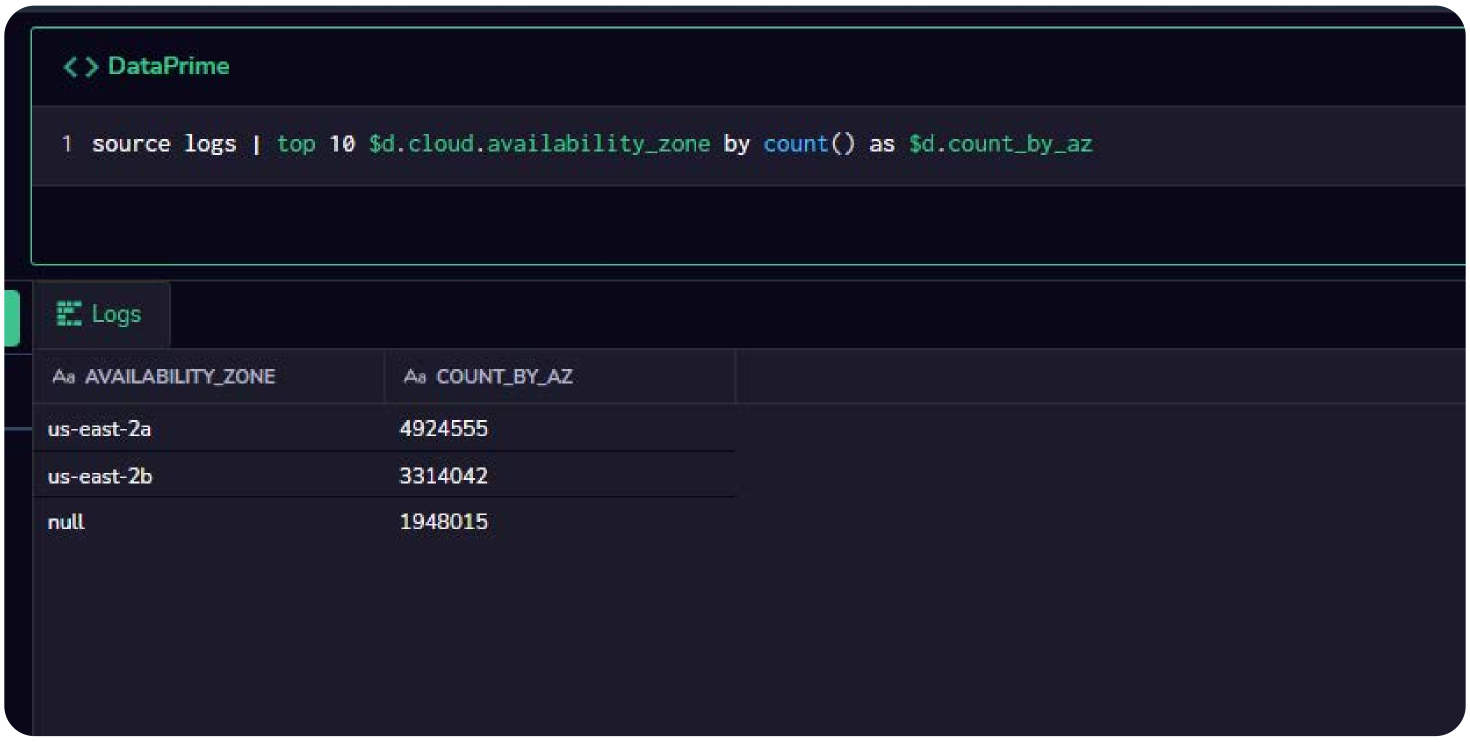
Every other vendor will only allow customers to optimize their storage and processing costs, once they're spending enough money. This is because cost-optimization is something our competitors have included later in the game, and it directly impacts their bottom line. Coralogix is built with customer efficiency in mind. The more efficient the customer is, the more efficiently the platform runs. All of our customers get access to the TCO Optimizer instantly, which enables them to route data into low cost storage where it can be ingested at an **85% discount** and queried using Coralogix Remote Query.

ACCESS YOUR ARCHIVE WITH REMOTE QUERY

Most archives require that logs are compressed. If they are ever needed, the user must first reindex the data from the archive into their high cost storage, and then they can access it. This causes two problems:

- There is a cost associated with reindexing, meaning the initial cost savings of archiving are impacted.
- How does the user know how much data to reindex? This is a dangerous, and potentially expensive guessing game.

Coralogix breaks this paradigm by offering Remote Query. With an archive hosted in their own account, Coralogix customers can utilize Remote Query to directly query their archive from the customer interface, with blazing fast data processing that handles 10TB queries in under 10 seconds.



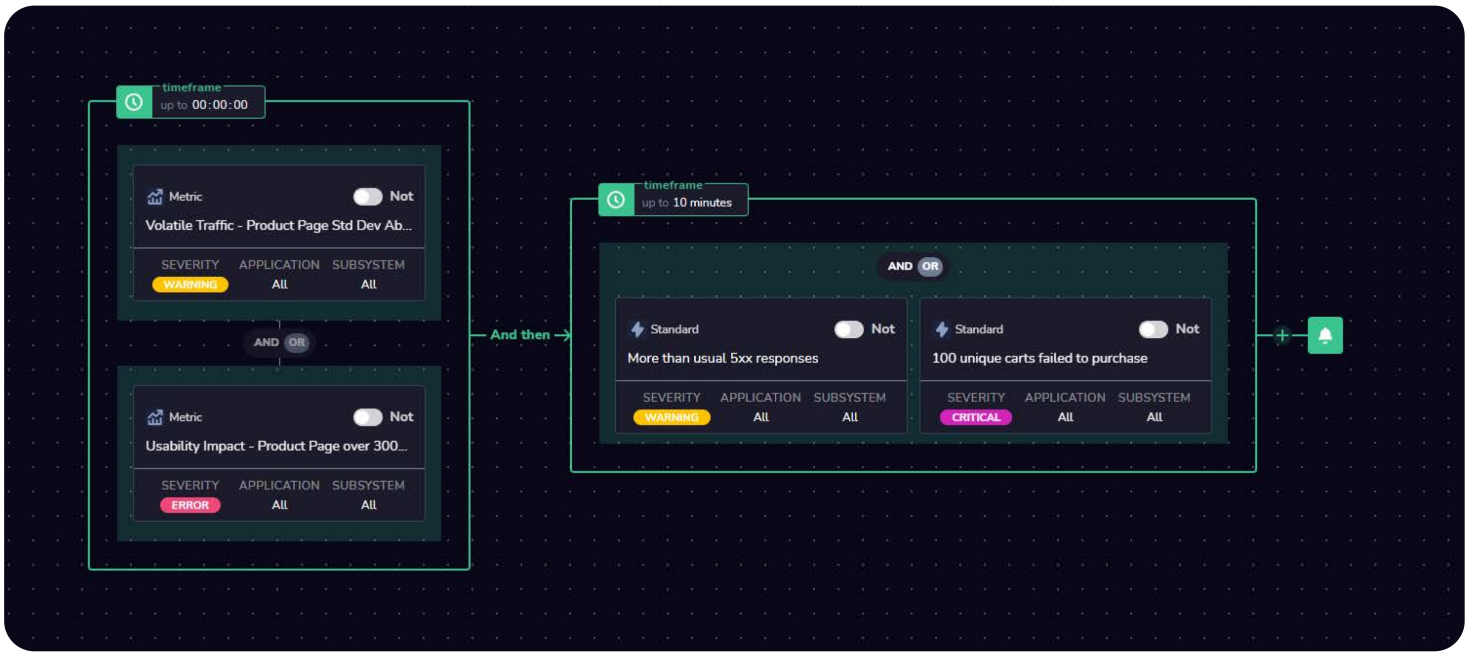
```
source logs | top 10 $d.cloud.availability_zone by count() as $d.count_by_az
```

AVAILABILITY_ZONE	COUNT_BY_AZ
us-east-2a	4924555
us-east-2b	3314042
null	1948015

And with the power of DataPrime, Coralogix's very own data discovery and query language, Coralogix customers can deep dive into their data in a way that is simply impossible in other vendors.

THE MOST SOPHISTICATED ALERTING ON THE MARKET

Coralogix supports alerting that is not available in any other platform. For example, Flow Alerts. Coralogix Flow Alerts allow customers to chain together multiple alert types, to orchestrate complex scenarios over time. Flow Alerts are *the only alerts on the market* that allow users to orchestrate logs, metrics, traces & security data in the same flow.



Volatile Traffic - Product Page Std Dev Ab...

SEVERITY	APPLICATION	SUBSYSTEM
WARNING	All	All

Usability Impact - Product Page over 300...

SEVERITY	APPLICATION	SUBSYSTEM
ERROR	All	All

More than usual 5xx responses

SEVERITY	APPLICATION	SUBSYSTEM
WARNING	All	All

100 unique carts failed to purchase

SEVERITY	APPLICATION	SUBSYSTEM
CRITICAL	All	All

THE BEST SUPPORT ON THE MARKET

Coralogix regularly signs 2 minute response time SLAs with customers, and it does this for all of its customers. If you ingest 10GB/day or 1TB/a day, it doesn't matter. In fact, 2 minutes is a comfortable number, with the true response time median regularly sitting at between 15 and 30 seconds. This, coupled with a median resolution time of 1 hour, means Coralogix customers are speaking to a person and having their issues solved in a fraction of the time that the other SaaS vendors can provide.

SUMMARY

When working with microservices, observability is key to maintaining your software system and ensuring users have a good experience. We have discussed different categories when choosing a SaaS observability tool to meet your company's observability needs.

Each SaaS provider will have different strengths to use when analyzing your system. Make sure you look to the future when choosing your observability provider so your company can grow with that provider to continue offering a quality product even at scale. Before choosing your provider based on features alone, ensure a cost analysis not only for today's cost but for cost at scale so your provider can help you grow without consuming your profits.

ABOUT CORALOGIX

We're rebuilding the path to observability using a real-time streaming analytics pipeline that provides monitoring, visualization, and alerting capabilities without the burden of indexing.

By enabling users to define different data pipelines per use case, we provide deep insights for less than half the cost.

In short, we are streaming the future of data.

Built for tomorrow's data scale

2K+	10K+	500K+	3M+
Global Customers	DevOps and Engineering Users	Applications Monitored	Events Processed Per Second

Your data is telling yesterday's story —
Find out what it can tell you today.

Create an Account

Get a Demo

Monitoring
US-west-2 is using more CPU than usual
Security
Logs
error volume anomaly detected
Tracing
We found 500 traces with duration >120ms
Metrics
The supplied query is over 10
WARNING