Real-Time Visibility and Monitoring in Your **Cloud Environment**

aws marketplace

splunk> | aws

The cloud journey

The cloud has become essential to modernizing IT and enabling digital initiatives for organizations large and small. Organizations are in the midst of their cloud journey and seek to accelerate innovation, increase efficiency, and optimize IT spend.

Cloud migration typically starts by **"lifting and shifting"** existing workloads to the cloud. However, merely shifting applications and data from on-premises infrastructure to cloud platforms in a bulk cloud migration does not unlock the full potential of the cloud. Companies also need to **refactor** their applications, for example, by leveraging managed cloud services such as Amazon DynamoDB instead of maintaining their own NoSQL database.

Furthermore, as companies mature in their cloud journey and **re-architect** their applications to microservices as well as embrace modern infrastructure such as containers, Kubernetes and serverless functions, they stand to gain more benefits.

While the cloud provides agility, efficient scalability, and resilience, it also adds new operational considerations. In this e-book, we will show an effective framework for monitoring modern infrastructure and services in AWS environments with Splunk Infrastructure Monitoring.
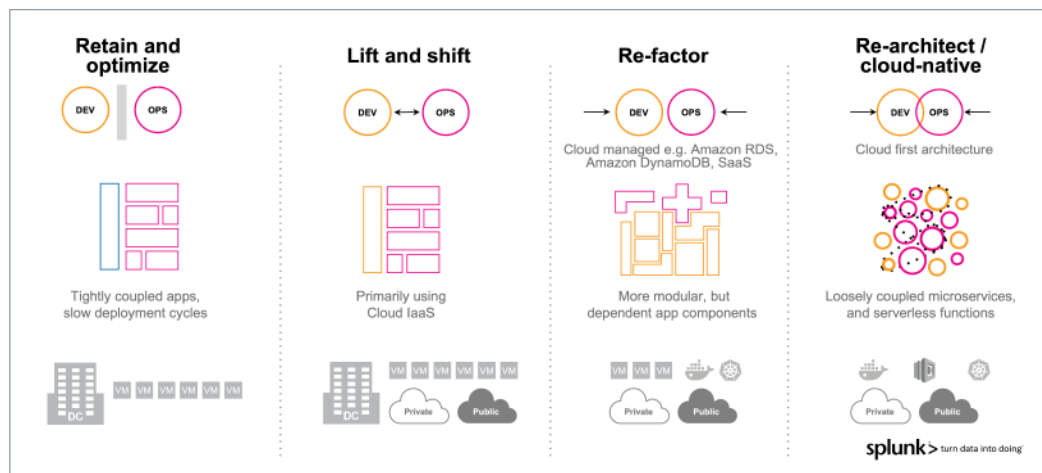
What's changed in the cloud and why traditional approaches to monitoring no longer work

As organizations continue their journey towards cloud-native, the volume of operational data they must deal with is significantly greater and more difficult to process. Cloud enables practically unlimited scalability with elastic and automatic provisioning of resources. However, the elastic nature of modern infrastructure also means that the individual components are often ephemeral and dynamic.

Ephemeral infrastructure and the distributed nature of cloud applications exponentially increase the cardinality of performance metrics as well. Frequent application releases add to the complexity of troubleshooting. Traditional monitoring tools cannot make sense of data coming from disparate sources in real-time, leading to higher mean-time-to-detect and mean-time-to-resolution.

End-users' expectations have never been higher. Applications need to provide a flawless end-user experience irrespective of the pressures placed on the system by varying load, sudden changes in traffic patterns, or other variables associated with scaling across devices and geographies. According to a recent study by Akamai,[1] a 100-millisecond increase in latency can reduce conversion rates by 7 percent. Companies often fall short if they retrofit traditional monitoring tools and strategies in modern cloud environments. What they need is real-time observability to gain insights on how their entire system is performing before the end-user is affected.

1. Akamai Online Retail Performance Report: Milliseconds Are Critical, April 19, 2017

Cloud-native boosts velocity, but also increases complexity

Complex interdependencies

- 10s or even 100s of loosely coupled, polyglot microservices
- System behavior is unpredictable and changes over time

Elastic, short-lived infrastructure

- AWS Cloud, abstracted infrastructure is extremely dynamic
- Volume of objects and metrics to monitor skyrockets

Frequent application changes

- Developers are key users - monitoring is not limited to Ops
- No single user has an accurate mental model - troubleshooting is a team sport

Modern approaches to monitoring

Monitoring is an integral part of the DevOps toolchain that enables developers and operations teams to quickly detect, triage, troubleshoot, and resolve performance issues—before such issues can impact end-users.

The core features of a modern monitoring platform are outlined below:

Real-time problem detection:

Because modern software-defined infrastructure spins up and down within minutes, every second counts in delivering a flawless end-user experience. The ability to instantly discover and accurately alert on anomalies is now imperative.

Auto-discovery and integrations:

The monitoring platform should be able to automatically discover applications or AWS services and provide pre-built curated visualizations. Out-of-the-box monitoring of every layer of infrastructure allows DevOps teams to correlate metrics across systems to understand the interdependencies between services.

Accurate alerting:

Even traditional and simplistic monitoring tools can fire off an alert when a metric crosses a static threshold. But such static alerting approaches are not adequate in constantly changing, ephemeral cloud environments. An advanced monitoring approach provides sophisticated alerting capabilities including dynamic baselines, automatic outlier detection, and sudden changes leveraging AI and ML.

High cardinality analytics:

Ephemeral cloud infrastructure and the distributed nature of cloud-native applications exponentially increase the cardinality of performance metrics. Tagging and labels are the basic tenets in cloud architectures to aggregate, segment, slice-and-dice data and get meaningful insights. Traditional tools struggle to provide high cardinality analytics at scale in real-time.

Monitoring-as-a-Service:

The DevOps paradigm of "you build it, you own it" boosts agility in part by decentralizing operational responsibility to individual teams. More people across the organization now need access to monitoring, and this decentralization can easily lead to fragmented tools and data. Fragmentation can lead to higher costs and, even worse, highly inefficient operations. Most monitoring tools were designed for a world in which operations were the responsibility of a small group of experts and lack the necessary capabilities to enable monitoring-as-a-service.

Modern monitoring platforms provide centralized management so teams and users have access controls and can gain transparency and control over consumption—allowing for better collaboration.

Splunk Infrastructure Monitoring:
How it works

Real-time streaming architecture

Splunk Infrastructure Monitoring is the real-time metrics solution purpose-built to monitor ephemeral clouds, containers, and serverless environments with high cardinality at massive scale. Driven by our patented streaming architecture, our approach to ingest, store, and retrieve data is fundamentally different from traditional batch and query-based solutions.
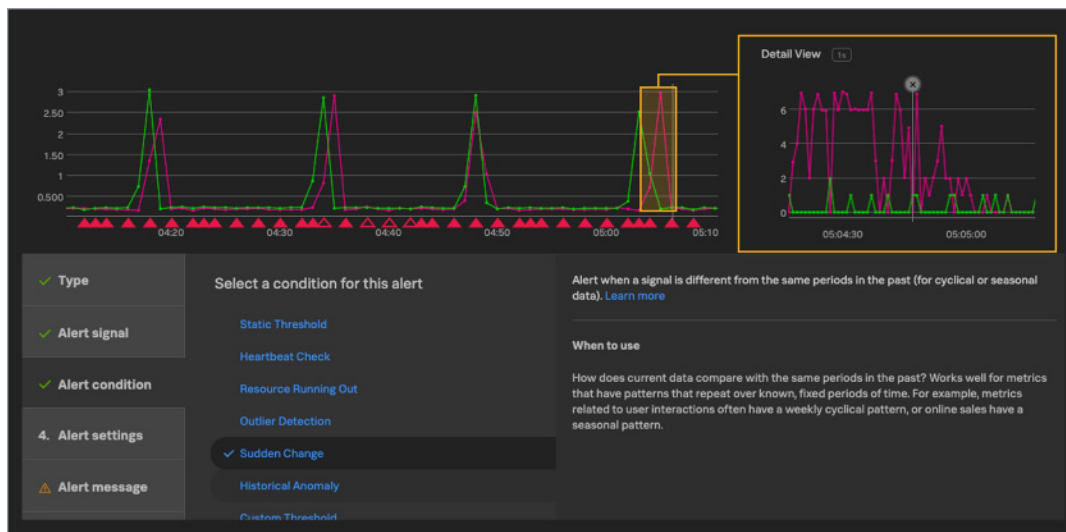
As metric data streams into Splunk, metadata is separated from metric value data as they serve separate use cases. Human-readable metadata is a central tenant in cloud-native environments to search, filter, sort, and group, while metric values are analyzed and directly streamed to components such as dashboards, alerts, and automation. Our streaming architecture allows customers to get insights and take action in real-time—dashboards refresh, alerts fire, and automation tasks trigger all within seconds—whereas other solutions take much longer.
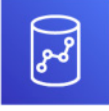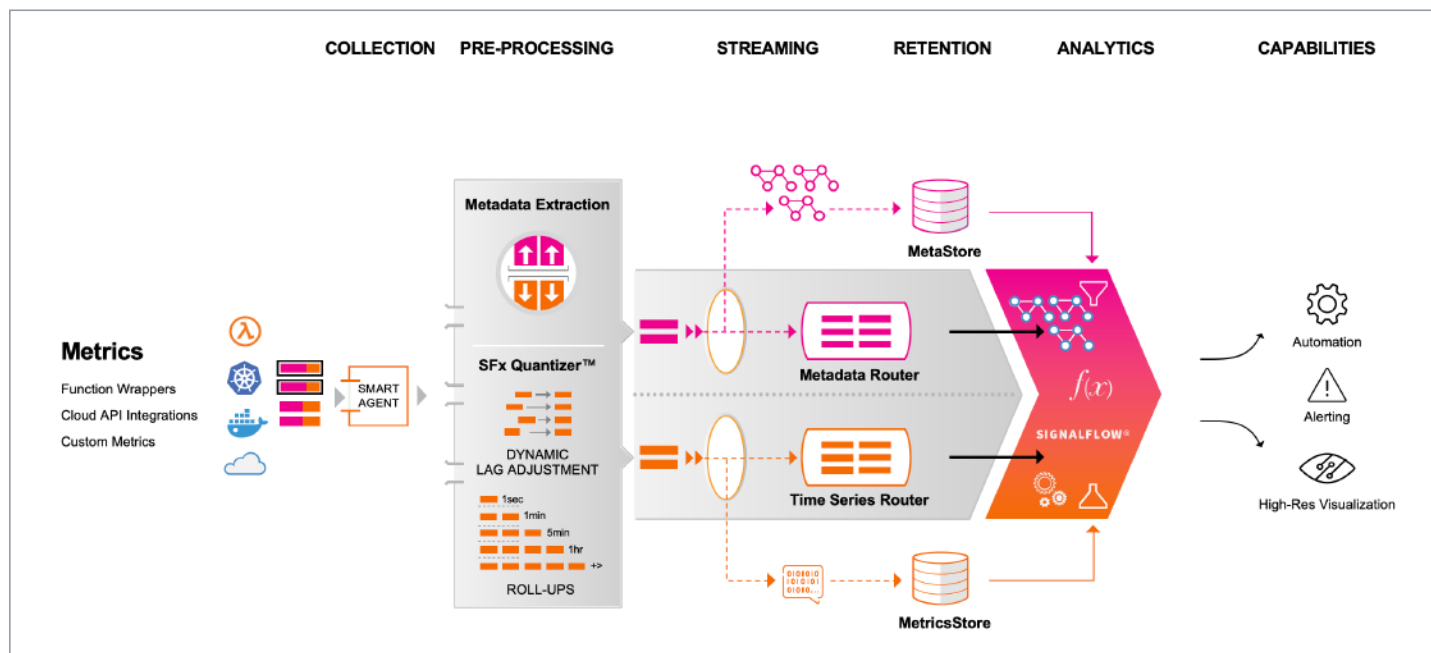
Accurate and sophisticated alerting

Splunk Infrastructure Monitoring provides point-and-click machine learning capabilities to create accurate alerts, helping to avoid alert storms.

Sophisticated algorithms such as Historical Anomaly, Sudden Change, and Resource Running Out go beyond alerting on static thresholds and evaluate conditions, alerting you only when there is a true anomaly. In addition, there are more than 20 built-in statistical functions to ensure alert accuracy by not only looking at the raw metric data but also evaluating trends and patterns.

Deep visibility into AWS services

Monitor your entire AWS environment in one place. Splunk Infrastructure Monitoring works seamlessly with AWS and provides out-of-the-box visibility into AWS and your services.

Open and flexible data collection

Splunk provides complete flexibility and choice to ingest data from AWS environments:

Cloud APIs: Seamless interconnection with Amazon CloudWatch to ingest data from AWS-managed services such as Amazon DynamoDB, Amazon Redshift, Elastic Load Balancers, and many others.

Splunk Infrastructure Monitoring Smart Agent: Open-source host-based agent to automatically discover AWS compute services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS), as well as deployed application services such as MongoDB, Cassandra, Nginx and many others.

AWS App Mesh: Out-of-the-box visibility into application performance using a seamless integration with AWS App Mesh.

AWS Lambda Extensions: Using the Splunk extension, DevOps teams can automatically ingest AWS Lambda platform performance metrics in real time and easily understand the performance, usage, and bottlenecks across the entire AWS Lambda environment.

AWS Distro for OpenTelemetry: The AWS Distro for OpenTelemetry comes bundled with Splunk's exporter to seamlessly send observability data to Splunk.

AWS Lambda Function Wrappers: Get real-time visibility with up to 1 second resolution. Wrappers also provide an easy mechanism to instrument your code for custom metrics that matter, e.g. business KPIs.

SMART AGENT

SMART AGENT

Instantly discover deployed application and services as well as host, container metrics with open source Smart Agent

AMAZON CLOUDWATCH

AMAZON CLOUDWATCH

Leverage Amazon CloudWatch integration to monitor every AWS service with Amazon CloudWatch metrics

AWS APP MESH

AWS APP MESH

Get out-of-box visibility into performance of microservices using Splunk integration for AWS App Mesh

AWS LAMBDA FUNCTION WRAPPERS

AWS LAMBDA FUNCTION WRAPPERS

Use AWS Lambda wrapper functions to see invocations, error durations, and cold starts for functions in real time

AWS LAMBDA EXTENSIONS

AWS LAMBDA EXTENSIONS

Ingest AWS Lambda platform metrics in real time

Kubernetes Navigator: Real-time monitoring and AI-driven analytics for Amazon EKS

Kubernetes Navigator is the easiest way for DevOps and site reliability engineering (SRE) teams to understand and manage the performance of containerized applications using an intuitive, out-of-the-box UI that provides visibility throughout the entire Kubernetes environment.

With Kubernetes Navigator, teams can detect, triage, and resolve performance issues faster than ever before. DevOps and SRE teams can successfully navigate the complexity associated with Kubernetes at scale by taking advantage of these features:

- **Dynamic Cluster Map:** An intuitive way to instantly understand the health of Kubernetes clusters.
- **Drill-downs:** Faster and effective troubleshooting with quick drill-downs.
- **Logs in context:** Deep linking to contextual logs to gain granular insights, eliminate context switching, and accelerate root cause analysis.
- **Kubernetes Analyzer:** AI-driven analytics to automatically surface recommendations and expedite troubleshooting.
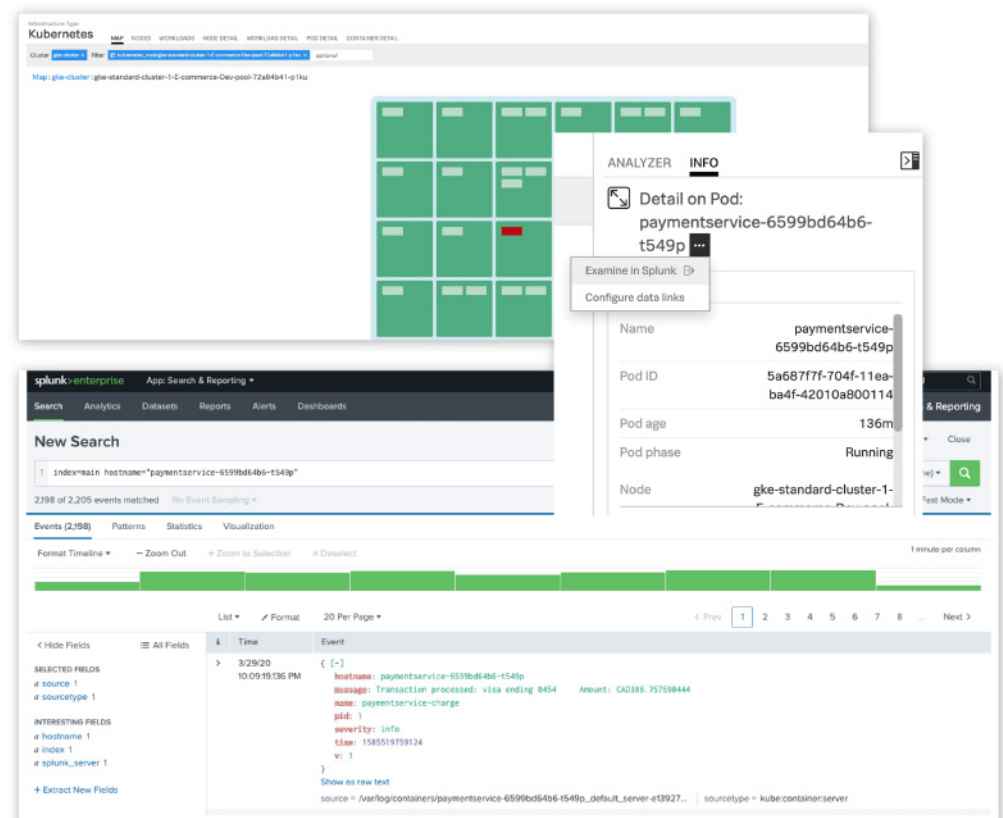
Real-time visibility into AWS Lambda

Whether your applications are 100% serverless or a mix of serverless and traditional apps, you can monitor your entire cloud stack with Splunk in real-time. Use the Splunk extension for AWS Lambda, functions wrappers and Amazon CloudWatch interconnections to get comprehensive, end-to-end visibility.

Any language, any runtime:

The Splunk Extension for AWS Lambda provides automatic and real-time visibility into AWS Lambda functions written in any language or runtime.

Monitor key business performance metrics:

Splunk function wrappers provide an easy mechanism to instrument your code for custom metrics that matter, e.g. business KPIs. Simply add a few additional lines within your function to capture and send those metrics to Splunk without incurring any performance overhead.
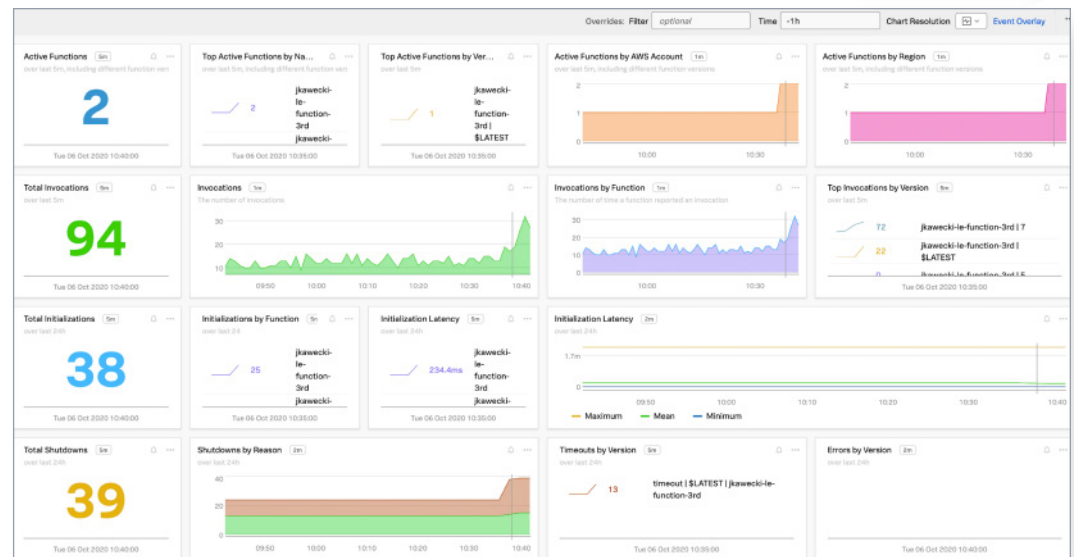
Future growth and success begin with modernizing infrastructure:
Start your cloud journey with Splunk and AWS

Modern apps run on modern infrastructure. Our customers partner with Splunk and AWS to accelerate their journey to cloud and infrastructure modernization.

Customer outcomes:

- **90 percent faster** mean-time-to-detect

- **8 times** DevOps productivity

- **95 percent** performance improvement

Whether you've just begun embracing the cloud or have already accelerated cloud adoption, future-proof your observability investment with an enterprise-grade solution trusted by leading companies for real-time cloud monitoring. Get started with a free trial of Splunk Infrastructure Monitoring today.

Acquia's average time spent resolving an incident dropped from **.23 hours to .17 hours — a 26% reduction** —saving it **140 hours** per month.

Read the Aquia customer story

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. Splunk Infrastructure Monitoring is available in AWS Marketplace.