



Monitoring and Reporting on AWS

Business Goals

WHY DO YOU NEED OBSERVABILITY?



Create new
revenue streams



Improve Operational
and Financial
efficiency



Lower
Business Risk

Monitoring more than failures



Is it behaving
as expected?



What is the usage?

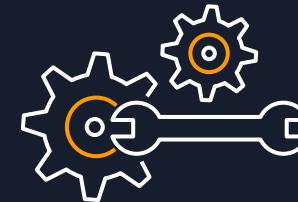


What is the
business impact?

Monitoring impacts operational and business outcomes



Get visibility



Troubleshoot
in real time



Improve customer
experience



Build highly-
resilient apps

Operational

Business

What is Observability?



Foundation for observability: data drives decisions



Logs



Metrics



Traces



AWS monitoring and observability services help you maintain SLAs by **detecting, investigating, and remediating** problems to achieve

Availability

Reliability

Performance

AWS observability tools

► Infrastructure monitoring

Perform real-user monitoring on websites and end-points

Easily correlate logs, metrics and traces to quickly identify service bottle-necks

Dynamic dashboards based on resource tags

► Application monitoring

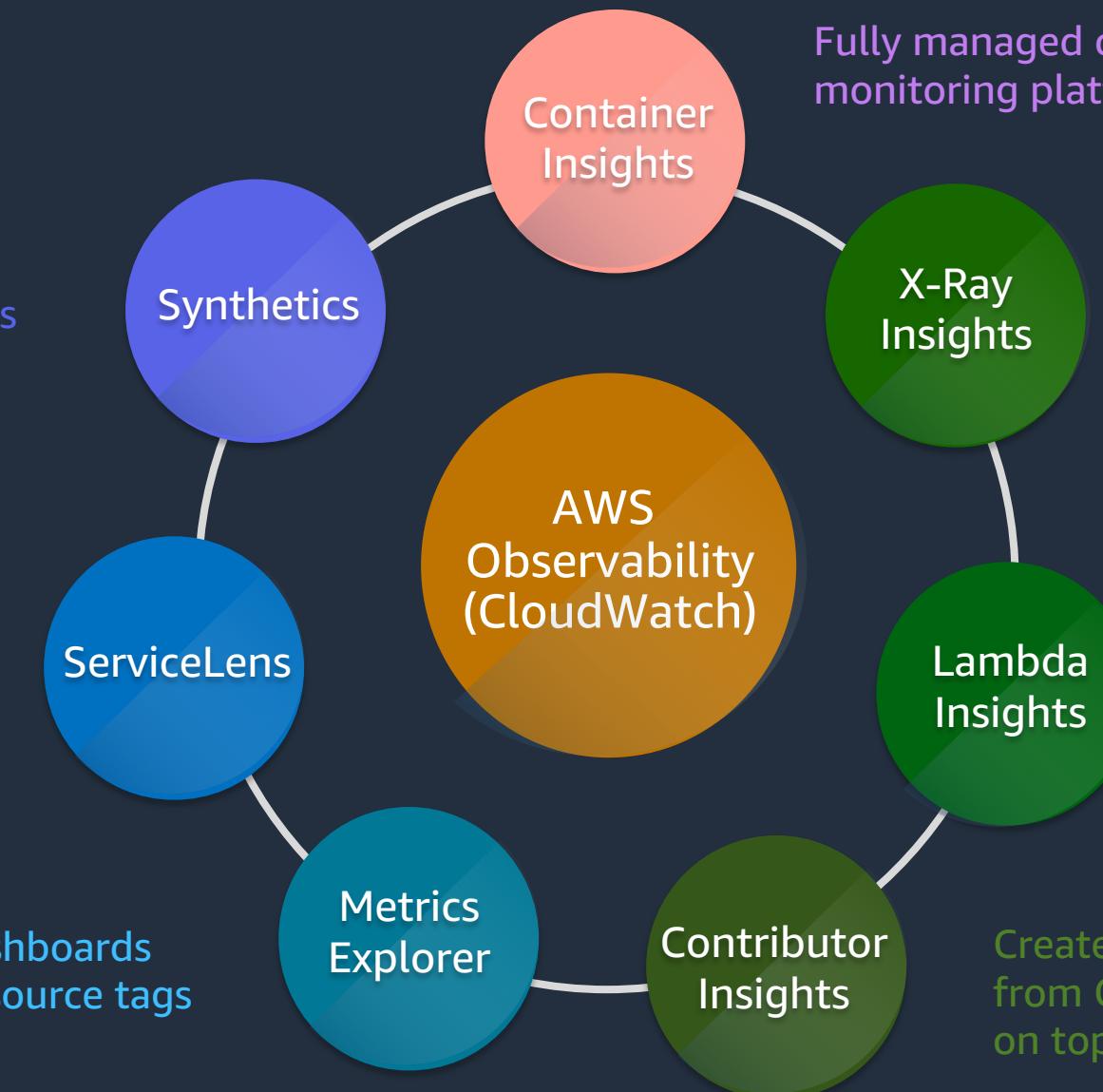
Fully managed container monitoring platform

Automatically identifies issues using Anomaly Detection and notifies you

Deeper insights into lambda performance and health metric data

Create time-series data from CloudWatch logs on top contributors

► Synthetic monitoring



AWS Services for Observability

CUSTOMER CHOICES



INFRASTRUCTURE

VMs, Containers, OS

AWS NATIVE



Amazon
CloudWatch

OPEN SOURCE



Amazon Managed
Service for Prometheus



Amazon Managed
Service for Grafana

PARTNER

APN



AWS SERVICES

Vended Monitoring



Amazon
CloudWatch



AWS
X-Ray



Amazon Distro for
Open Telemetry

X



APPLICATION PERFORMANCE

Tracing and Profiling



Amazon
CloudWatch



AWS
X-Ray



Amazon
CodeGuru



Amazon Distro for
Open Telemetry

APN



END-USER

Synthetic Monitoring



Amazon
CloudWatch



APN

Amazon CloudWatch

OBSERVABILITY OF YOUR AWS RESOURCES AND APPLICATIONS



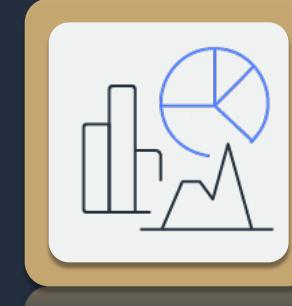
Observability
on a single
platform
across
applications
and
infrastructure



Easiest way to
collect metrics
in AWS and on-
premises



Improve
operational
performance
and resource
optimization



Get
operational
visibility and
insight



Derive
actionable
insights
from logs

Amazon CloudWatch Concepts

- Metrics
- Namespaces
- Dimensions
- Time Stamps
- Units
- Statistics
- Periods
- Aggregation
- Alarms
- Regions

CloudWatch Logs

STORE LOGS IN NEAR REAL-TIME

Collect logs from:

- Amazon EC2 instances
- On-premises servers
- VPC Flow Logs
- AWS CloudTrail
- AWS Lambda
- Other AWS Services

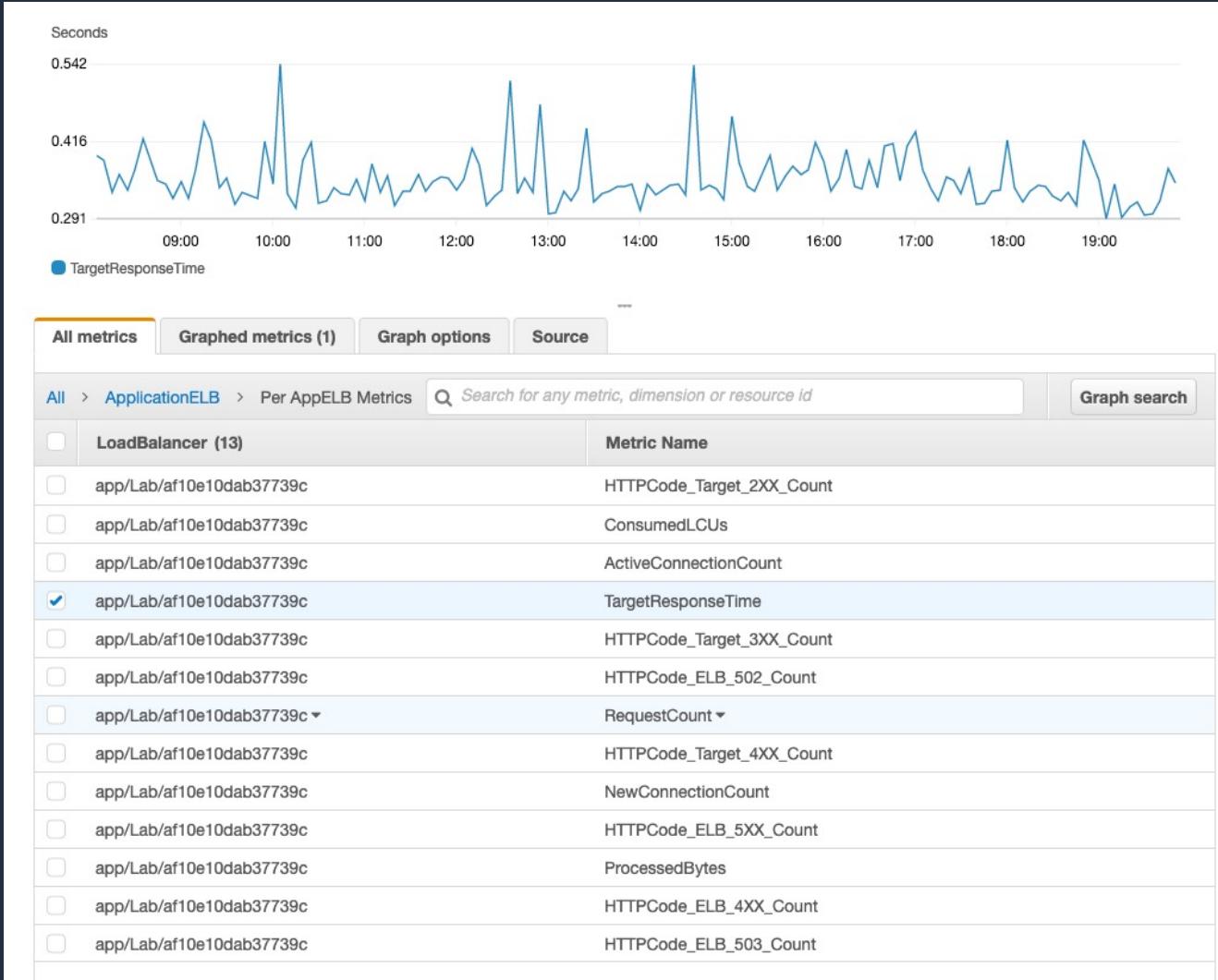
Log data can be stored and accessed indefinitely in highly durable, low-cost storage so you don't have to worry about filling up hard drives.

The screenshot shows the AWS CloudWatch Logs interface. At the top, the navigation path is CloudWatch > CloudWatch Logs > Log groups > application.log. To the right, there are buttons for Delete, Actions, Query log group, and View all log events. The main title is "application.log". Below it, the "Log group details" section provides information: Retention (Never expire), Creation time (5 months ago), Stored bytes (14.67 MB), KMS key ID (-), Metric filters (1), Subscriptions (LambdaStream_centralized-logging-LogStreamer-1A2RQLP14N1TW), and ARN (arn:aws:logs:eu-west-1:012345678910:log-group:application.log:*). Below this, tabs for Log streams, Metric filters, and Contributor Insights are visible. The "Log streams (5)" section lists five entries, each with a checkbox, a log stream name, and a last event time. The entries are: i-077f7e49ee1c0112c (1/10/2020, 8:00:49 PM), i-03343584efd07d2a6 (11/29/2019, 8:03:35 PM), i-09bd407810ebfa83f (11/29/2019, 8:00:52 PM), and i-0bf3c984cda70e7c0 (9/19/2019, 9:00:35 PM).

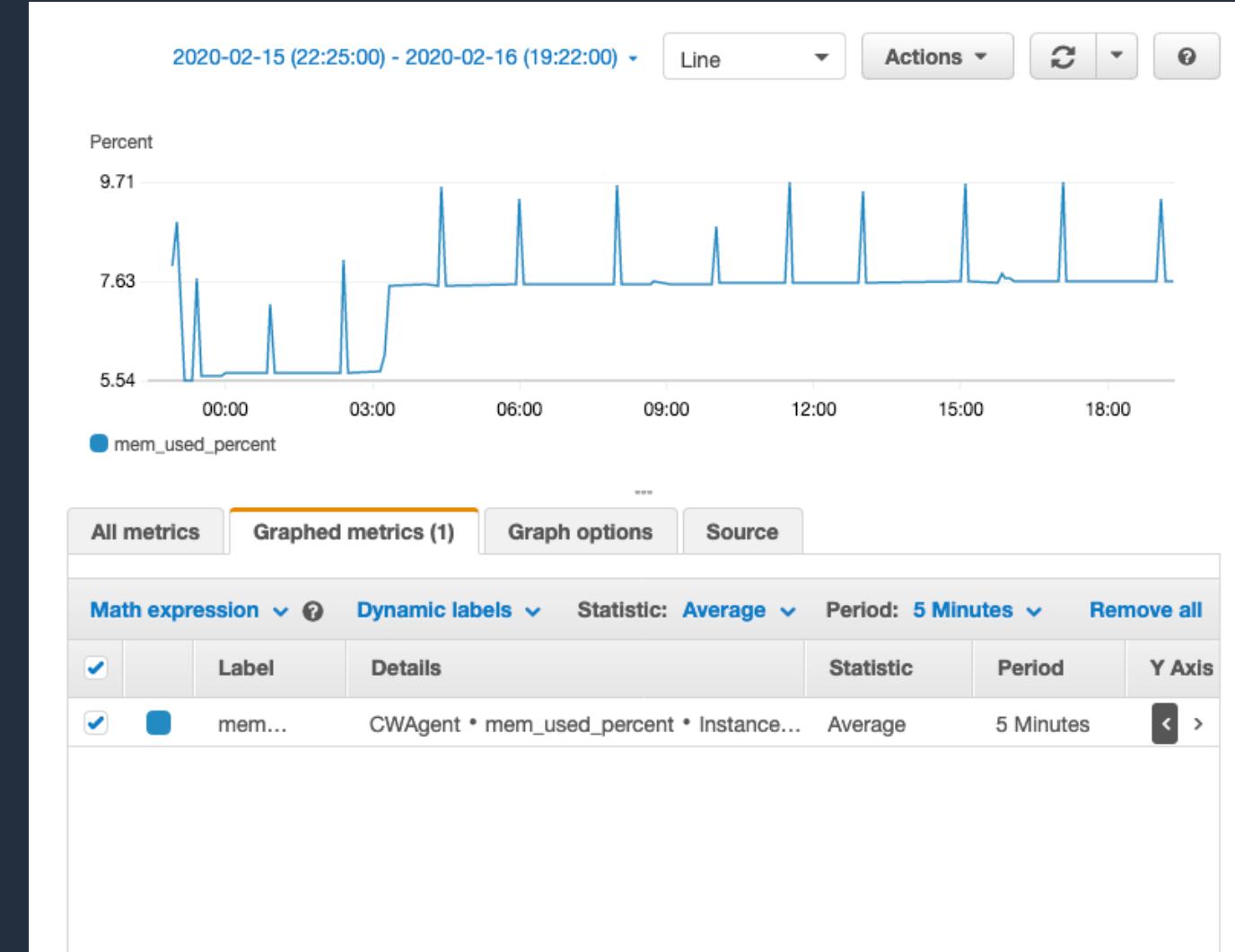
Log stream	Last event time
i-077f7e49ee1c0112c	1/10/2020, 8:00:49 PM
i-03343584efd07d2a6	11/29/2019, 8:03:35 PM
i-09bd407810ebfa83f	11/29/2019, 8:00:52 PM
i-0bf3c984cda70e7c0	9/19/2019, 9:00:35 PM

CloudWatch Metrics

Built-in metrics



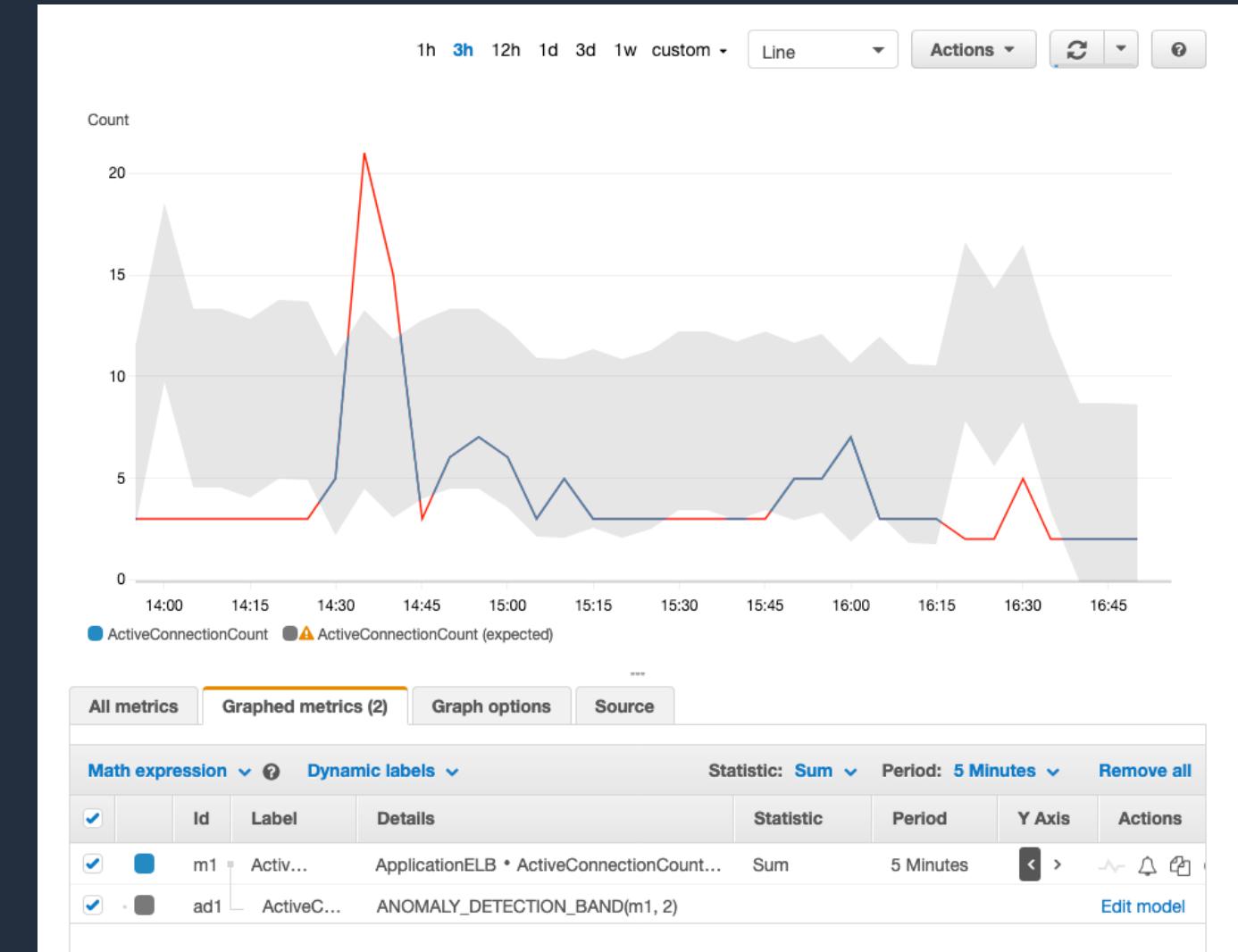
Custom metrics



Anomaly Detection

When you enable anomaly detection for a metric, CloudWatch applies machine learning algorithms to the metric's past data to create a model of the metric's expected values.

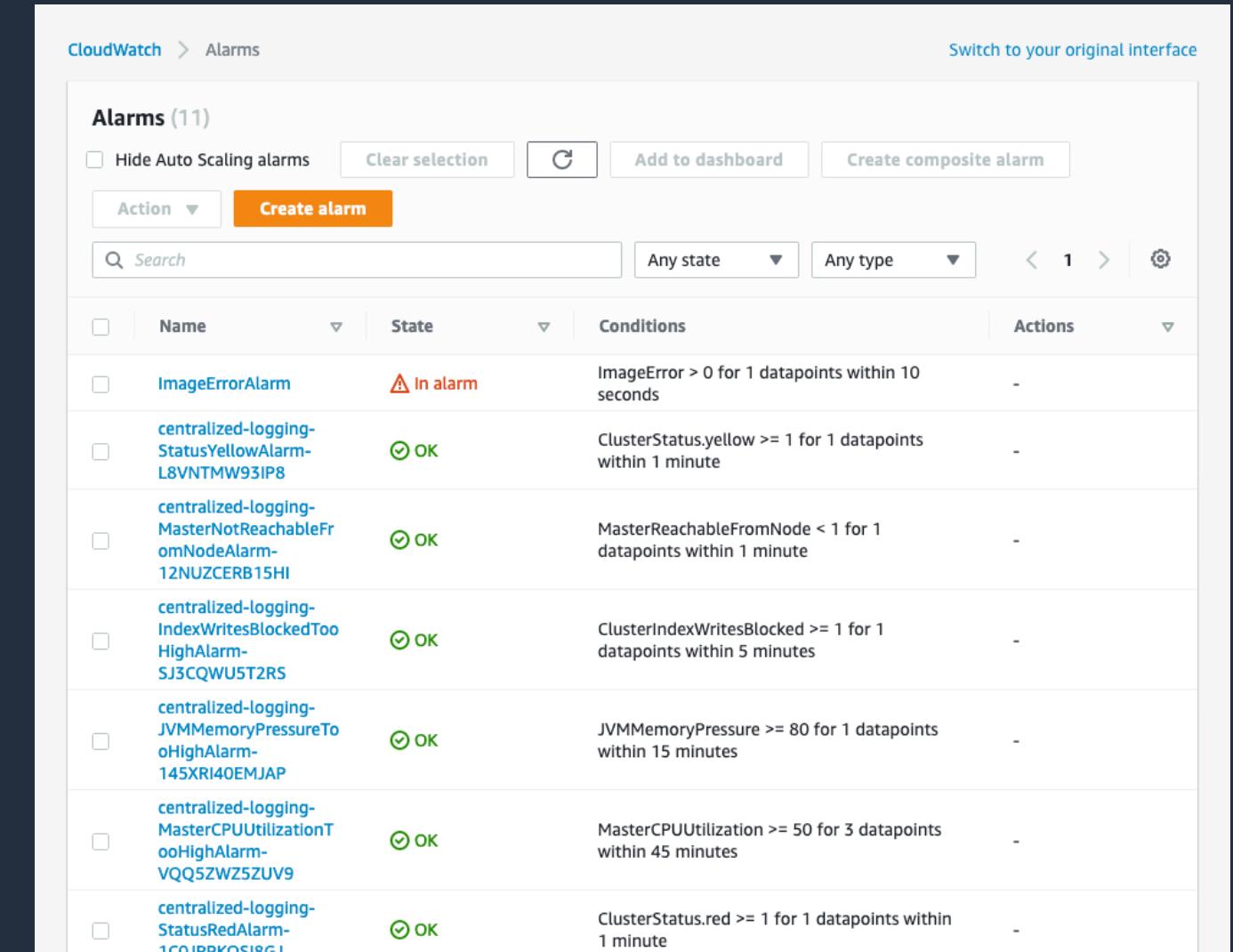
- Create alarms that auto-adjust thresholds based on natural metric patterns
- Alarm when the metric value is above or below the band, or both
- Visualize metrics with anomaly detection bands on dashboards



CloudWatch Alarms

Amazon CloudWatch alarms allow you to set a threshold on metrics and trigger an action.

- Watch a single metric or the result of a math expression
- Perform actions based on the value of metrics
 - Send a notification to an SNS topic
 - Auto Scaling action
 - EC2 Action (Stop, Terminate, Reboot or Recover)
- Add alarms to dashboards to visualize them



The screenshot shows the AWS CloudWatch Alarms console interface. At the top, there are buttons for 'Hide Auto Scaling alarms' (unchecked), 'Clear selection', a search bar, and buttons for 'Add to dashboard' and 'Create composite alarm'. Below this is a search bar and filters for 'Any state' and 'Any type'. The main area displays a table titled 'Alarms (11)' with columns for 'Action' (dropdown), 'Name', 'State', 'Conditions', and 'Actions'. The table lists 11 alarms, each with a checkbox, a name, a state indicator (e.g., 'In alarm' for ImageErrorAlarm, 'OK' for others), a condition description, and a 'More' link. The conditions listed include various metric thresholds over different time periods.

Action	Name	State	Conditions	Actions
<input type="checkbox"/>	ImageErrorAlarm	⚠ In alarm	ImageError > 0 for 1 datapoints within 10 seconds	More
<input type="checkbox"/>	centralized-logging-StatusYellowAlarm-L8VNTMW93IP8	✔ OK	ClusterStatus.yellow >= 1 for 1 datapoints within 1 minute	More
<input type="checkbox"/>	centralized-logging-MasterNotReachableFromNodeAlarm-12NUZCERB15HI	✔ OK	MasterReachableFromNode < 1 for 1 datapoints within 1 minute	More
<input type="checkbox"/>	centralized-logging-IndexWritesBlockedTooHighAlarm-SJ3CQWU5T2RS	✔ OK	ClusterIndexWritesBlocked >= 1 for 1 datapoints within 5 minutes	More
<input type="checkbox"/>	centralized-logging-JVMMemoryPressureTooHighAlarm-145XRI40EMJAP	✔ OK	JVMMemoryPressure >= 80 for 1 datapoints within 15 minutes	More
<input type="checkbox"/>	centralized-logging-MasterCPUUtilizationTooHighAlarm-VQQ5ZWZ5ZUV9	✔ OK	MasterCPUUtilization >= 50 for 3 datapoints within 45 minutes	More
<input type="checkbox"/>	centralized-logging-StatusRedAlarm-1C0IRPKOSI8GJ	✔ OK	ClusterStatus.red >= 1 for 1 datapoints within 1 minute	More

CloudWatch Events

Provides a near real-time stream of system events that describe changes to your AWS resources.

Write rules to indicate which events are of interest to your application and what automated actions to take when a rule matches an event.

Rules > ChangInstanceSize Actions ▾

Summary

ARN ⓘ arn:aws:events:eu-west-1:180304385487:rule/ChangInstanceSize

Schedule Cron expression 0 6 ? * 6L *

Next 10 Trigger Date(s) 1. Fri, 28 Feb 2020 06:00:00 GMT
2. Fri, 27 Mar 2020 06:00:00 GMT
3. Fri, 24 Apr 2020 06:00:00 GMT
4. Fri, 29 May 2020 06:00:00 GMT
5. Fri, 26 Jun 2020 06:00:00 GMT
6. Fri, 31 Jul 2020 06:00:00 GMT
7. Fri, 28 Aug 2020 06:00:00 GMT
8. Fri, 25 Sep 2020 06:00:00 GMT
9. Fri, 30 Oct 2020 06:00:00 GMT
10. Fri, 27 Nov 2020 06:00:00 GMT

Status Enabled

Description

Monitoring [Show metrics for the rule](#)

Targets

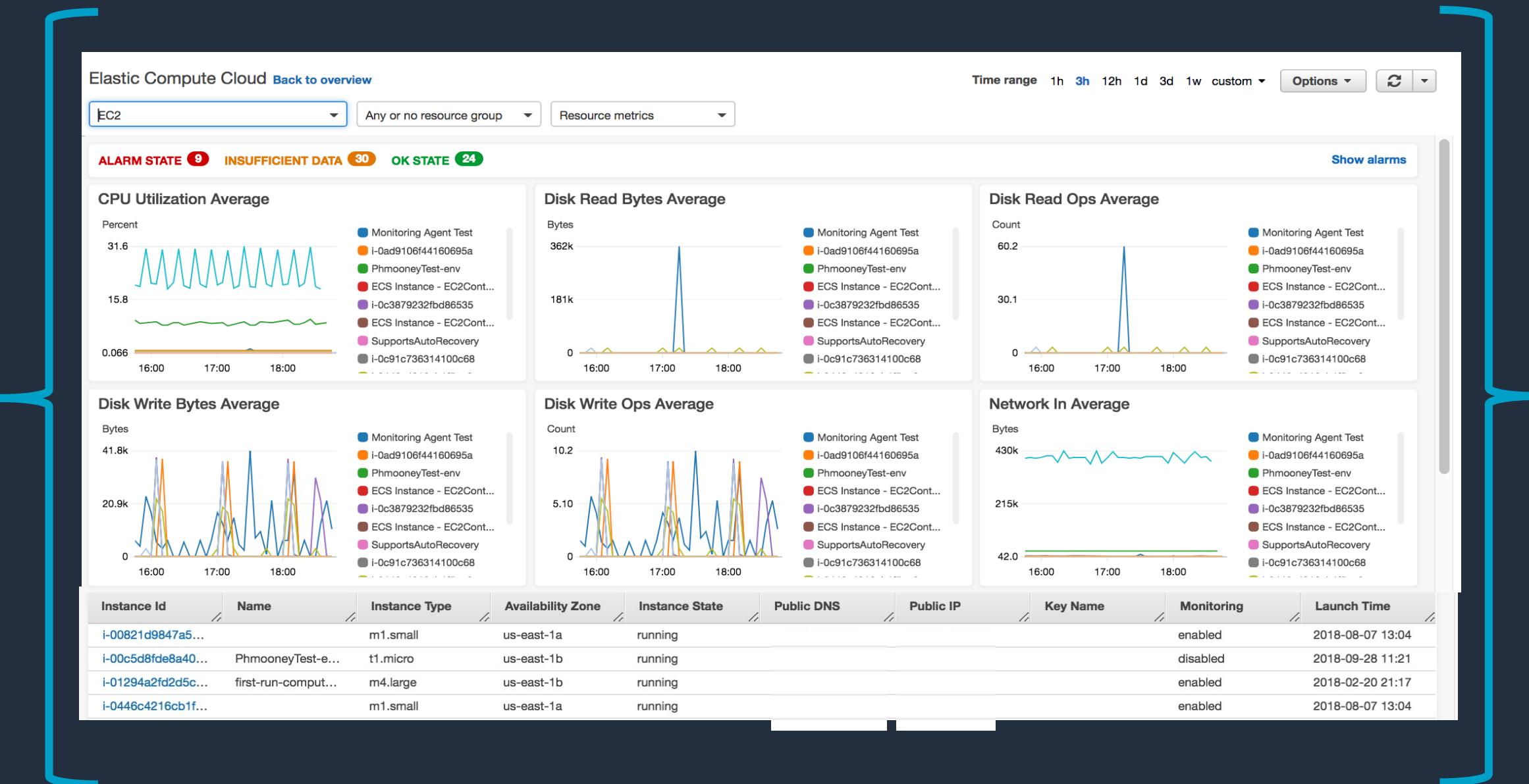
Filter:

Type	Name	Input
SSM Automation	ChangInstanceSize (version \$DEFAULT)	Constant: {"InstanceId": ["i-0cb0104ddf22a"]}

CloudWatch Automatic Dashboards

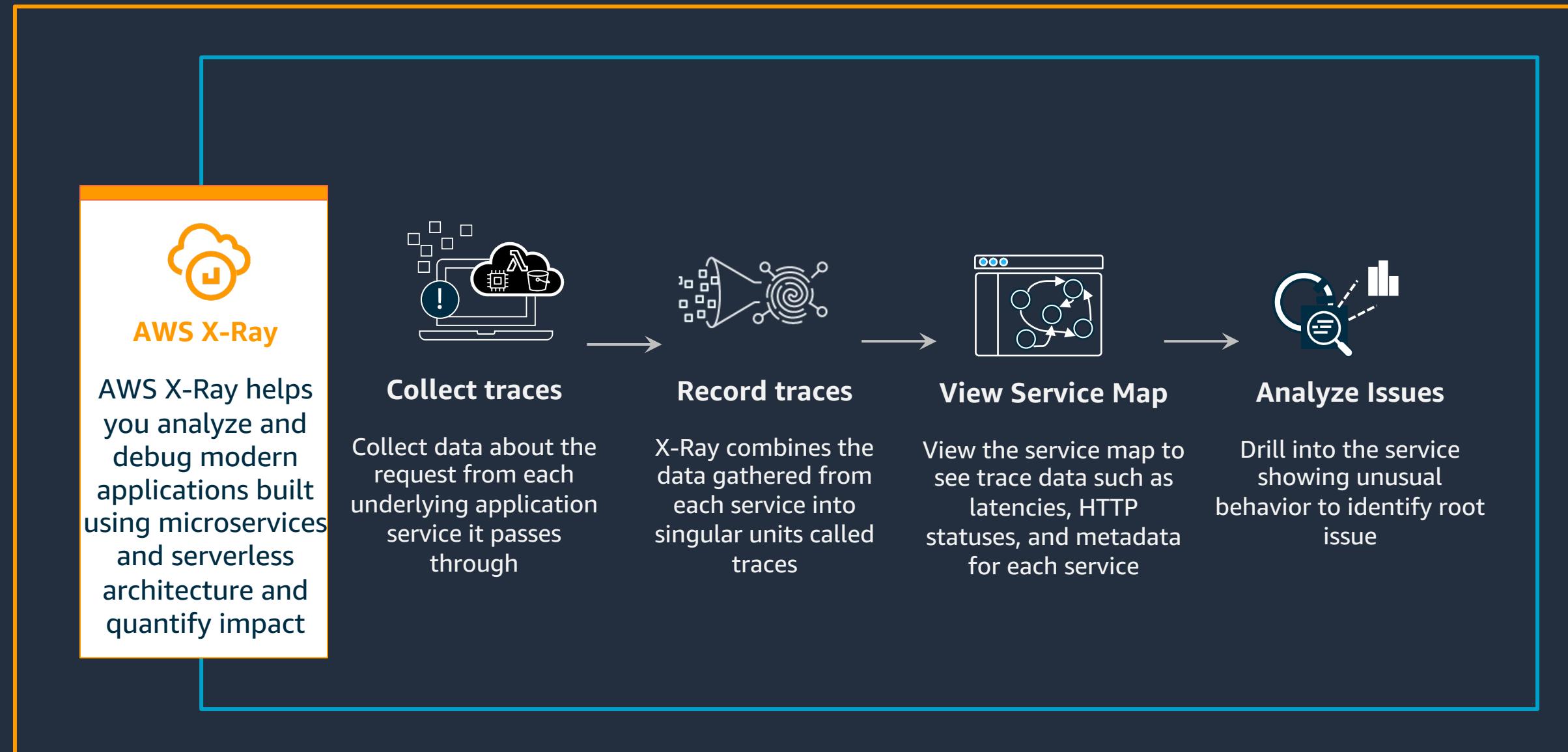
CloudWatch simplifies infrastructure monitoring with a default, getting started experience.

Dynamic, self-updating AWS infrastructure dashboards



AWS X-Ray

ANALYZE AND DEBUG PRODUCTION, DISTRIBUTED APPLICATIONS



CloudWatch Application Insights

Full stack observability for monitoring and troubleshooting your applications

CloudWatch ServiceLens

Container
Insights

Lambda
Insights

Application
Insights

Real User &
Synthetics

Contributor
Insights

X-Ray
Insights

Log Insights

ANALYTICS

Metric Insights

Amazon CloudWatch Metrics Insights

Why CloudWatch Metrics Insights?

Customer Challenges



Scale...

- Customer environments are moving towards container-based applications and microservices
- These new environments require more data to monitor



Speed...

- Short-lived resources change customer environments faster than before
- These frequently changing environments require faster monitoring and troubleshooting



Flexibility...

- Customers add context to their applications by assigning user defined labels to their metrics
- Customers require flexibility to analyze metrics by filtering and aggregating using these labels

What is CloudWatch Metrics Insights?

A fast, flexible, SQL based query engine that helps customers to analyze their operational metrics at scale, and be able to group and aggregate metrics in real time



Analyze operational
metrics at scale



Group and aggregate
metrics in real time

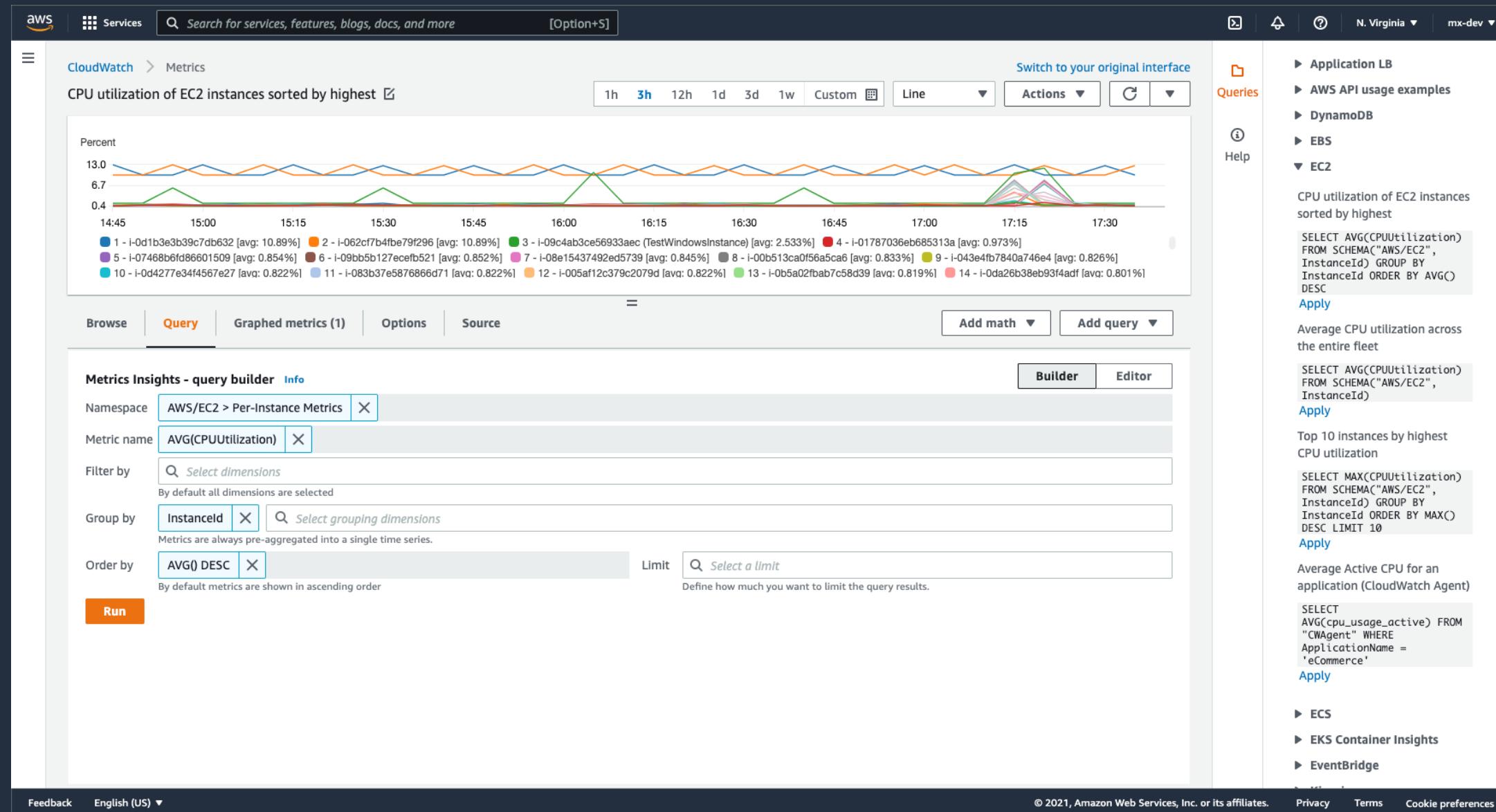


Pinpoint and
troubleshoot
issues quickly



Reduce MTTR

Metrics Insights: query CloudWatch metrics at scale



Amazon CloudWatch Synthetics

Customer challenges

Bad end-user experience (or digital experience) of your applications affects business including reputation, revenue, and retention.



of consumers say page speed impacts their willingness to buy from an online retailer.

—Unbounce report 2019

There is also a need to validate application choices with end-users.

For end-to-end visibility, customers need integrated observability tooling.

Why digital experience monitoring (DEM)?

Ensure a consistently great **customer experience**



Observe...

See what your customer sees

- Spot intermittent issues
- See when issues are introduced



Inspect...

Debug issues

- Discover performance issues
- Distributed apps means more dependencies



Respond...

Reduce mean time to recovery

- Minimize customer impact
- Fix issues/ initiate rollbacks



Validate...

Reduce risks for new features

- Controlled launches with monitoring
- Experiment to identify best choice

CloudWatch DEM features

Features for developers, DevOps engineers, and product owners to optimize their applications' end-user experience



CloudWatch Synthetics

Monitor web applications 24x7 using modular, light-weight canary scripts



CloudWatch RUM

New real user monitoring feature to get insights into actual end-user experience



CloudWatch Evidently

Safely launch new features and validate web application choices by conducting online experiments

Customer challenges

Need to identify when performance issues are affecting users

Need for continuous app monitoring from end-user perspective to spot intermittent issues and understand when issues were introduced

Once issues are identified, will need to debug them

Important to identify where in the distributed application, the performance is being impacted

What is CloudWatch Synthetics?

Monitor your endpoints every minute, 24x7 using modular canary scripts and be alerted when your application doesn't behave as expected



Website and API
endpoint monitoring

**Availability and latency
performance**



Outside-in monitoring

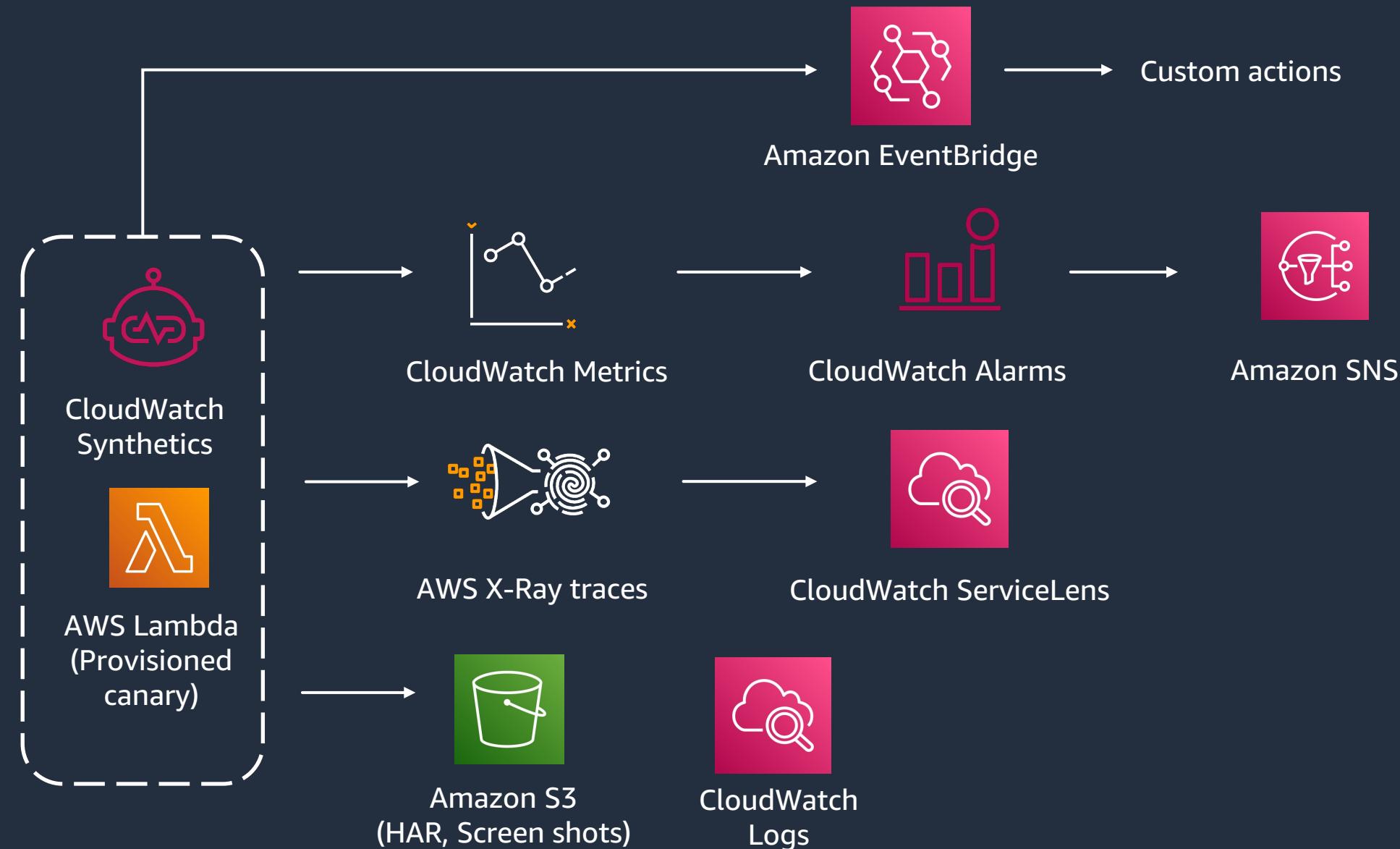
Client-side to server-side



Continuous monitoring

**Acts as a user and makes
scheduled health checks**

CloudWatch Synthetics—how it works



Easy getting started

Search for services, features, marketplace products, and docs [Option+S]

CloudWatch > Create a canary

Create canary Info

To get started, choose how you would like to create your canary.

Use a blueprint
Work from a template script

Inline Editor
Edit inline or upload your own scripts

Import from S3
Use existing scripts from S3

Blueprints

Heartbeat monitoring
Run a basic page load on a single URL.

API canary
Monitor your APIs as HTTP steps.

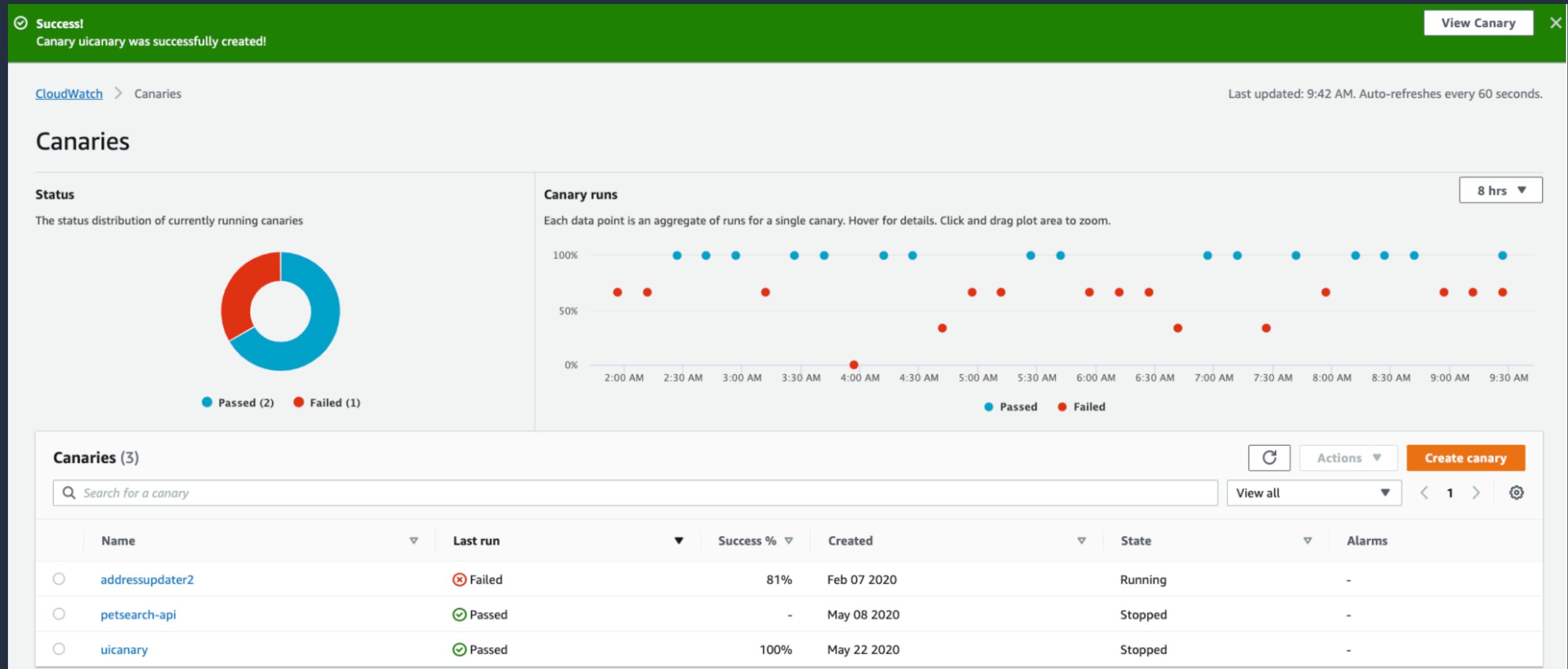
Broken link checker
Run a basic web crawler on designated URL.

Canary Recorder
Use the AWS Canary Recorder plugin.

GUI workflow builder
Create a GUI workflow with actions to perform.

Visual monitoring
Compare screenshots for every run

Visualize results



Debug using Canary run data

Steps	Screenshots	Logs	HAR File	Traces
Requests		Status code	Response size	Duration
https://www.amazon.com/alm/storefront?almBrandId=Q...ref_=nav_cs_fresh_2e88810ae9154e73ba87c8d7aad08e4b				
+	GET storefront?almBrandId=QW1hem9uiE	200	123.3 KB	743.4ms
+	GET 11EIQ5IGqaL._RC 012THT2ObnL.css,1	200	27.8 KB	13.9ms
+	GET 41KBYOkTjIL._RC 71pxb+E1-OL.css,41	200	44.7 KB	32.6ms
+	GET 11q9+KCTdOL._RC 01TrKJuJ6JL.css,0	200	4 KB	29.1ms
+	GET ueedata?staticb&id=SFCBKYPES3QHEE	200	150 B	218.6ms
+	GET nav-sprite-global-1x-hm-dsk-reorg_.t	200	11 KB	4.1ms
+	GET fresh19_stacked_color.png	200	13.3 KB	3.5ms
+	GET 51+Xe1pYFPL._RC 01j5DeZSMzL.js,31	200	23.3 KB	78.8ms
+	GET 11GnIC8wjvL.js?AUIClients/F3GLOWA	200	1.8 KB	63.1ms
+	GET ueedata?staticb&id=SFCBKYPES3QHEE	200	149 B	97.8ms
+	GET 41wII72RM+L.css?AUIClients/ACSWid	200	3.4 KB	39.7ms
+	GET halloween_storefront_hero_alt_mw1r	200	72.1 KB	135.7ms
+	GET F3VX-Fresh-dealsGraphic-type-t2-Mu	200	44.7 KB	200.5ms
...				

Amazon CloudWatch RUM

Customer challenges

Customers need to understand the actual user experience

Capture last mile issues including in DNS resolution, connection time

Ability to quantify an issue, or evaluate if it is more prevalent than expected

Correlate this data with the application monitoring

When we are alerted to issues, need for debugging to reduce customer impact and MTTR

What is CloudWatch RUM?

Helps developers and DevOps engineers optimize end-user experience through client-side data on app performance in real time



Client-side telemetry

Completes end-to-end monitoring



Correlated with resources

Client-side through transaction



Measure user impact

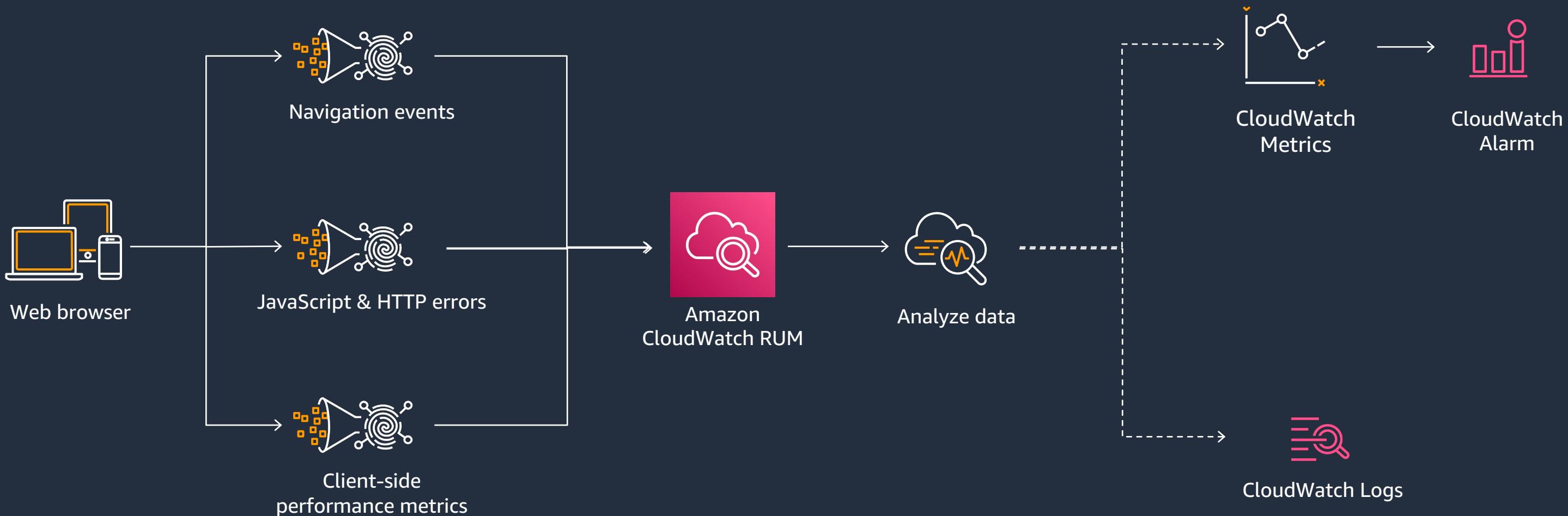
Get alerted and optimize user experience



Debugging made easy

Reduce mean time to recovery

Amazon CloudWatch RUM—how it works



Getting started

Create AppMonitor in
CloudWatch RUM

Get RUM web client
code to add to the
HTML header of your
web application

Start visualizing using
RUM dashboard

Flexibility in configuration

Session samples

Choose to collect a sample of sessions. Sampling helps reduce data storage costs.

Specify the percent of sessions you would like to collect and analyze.

Analyze % of sessions All sessions will be recorded

▼ **Configure pages - optional**

Choose to include or exclude pages.

All pages Data will be collected on all pages.

Include only these pages Data will be collected on only the pages you specify.

Exclude these pages Data will be collected on all pages excluding the ones you specify.

Include these pages
https://www.mywebstore.com/checkout*

Configure RUM data collection

Choose which data plugins to install in the RUM tracker.

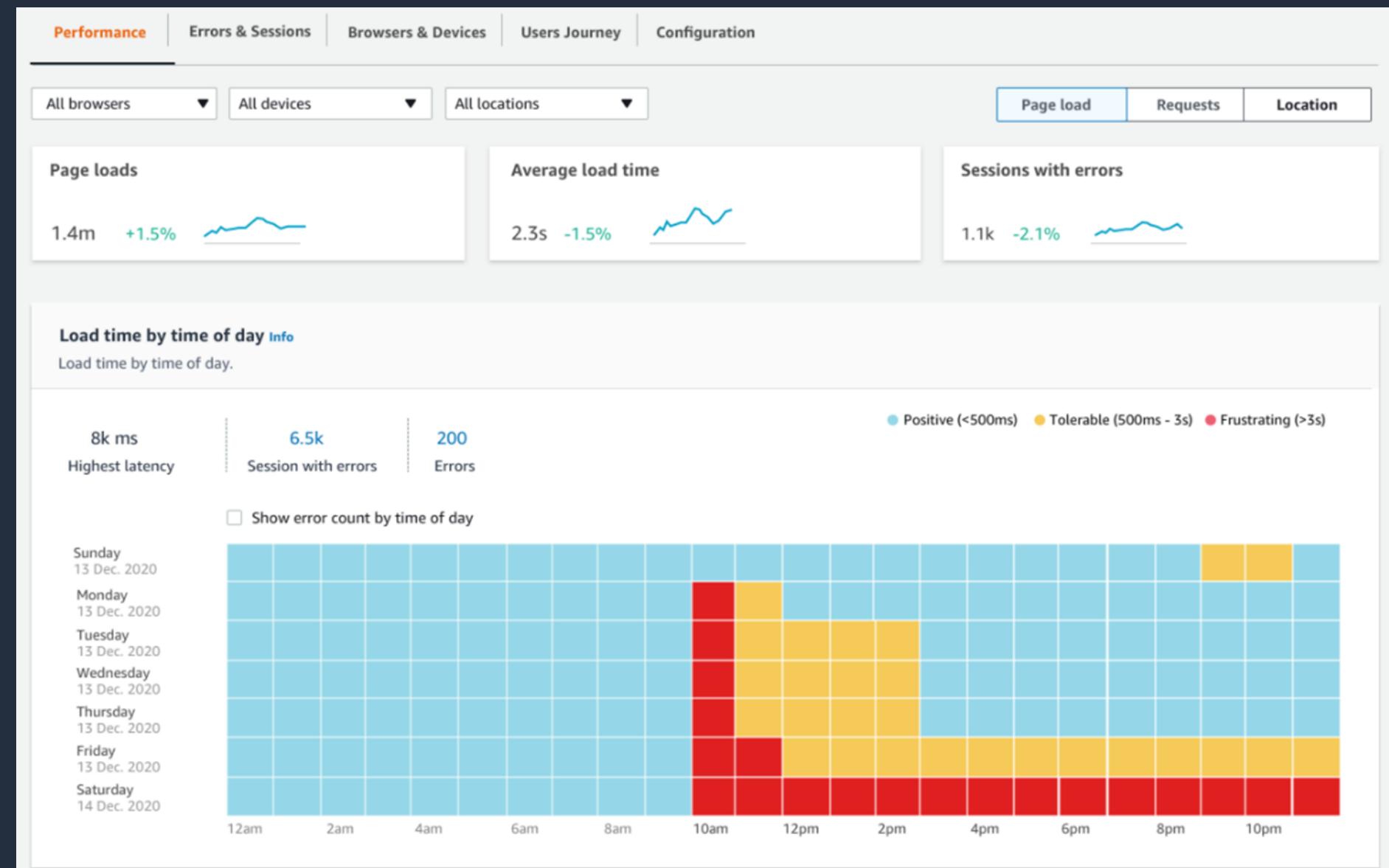
Each plugin records one or more events. Events contain a unique set of attributes about an interaction (passive or active) between the user and the application being monitored.

Performance telemetry
The RUM Agent will record timing data about how your web application and its resources are loaded and rendered. This includes Core Web Vitals. RUM will use this telemetry to give you insights into how users experience your application.

JavaScript errors
The RUM Web Client will record unhandled exceptions raised by your web application.

HTTP errors
The RUM Web Client will record HTTP errors thrown by your web application.

Visualize results using CloudWatch RUM



Amazon CloudWatch Evidently

Customer challenges

As customers innovate more and release features faster, they need to reduce their risks of unintended consequences.

- Risks including unexpected user behavior
- Performance degradation

To reduce this risk, developers often implement manual safety mitigations including manually setting up traffic to new features.

For new features, developers commonly generate variations of the new features and use A/B testing to assess user preference. However, accurately deciphering test data can be challenging and typically requires advanced statistics knowledge.

What is CloudWatch Evidently?

Launch monitoring and experimentation across the full software stack

For app developers to conduct experiments, reduce risk, and identify unintended consequences before launching features for general use

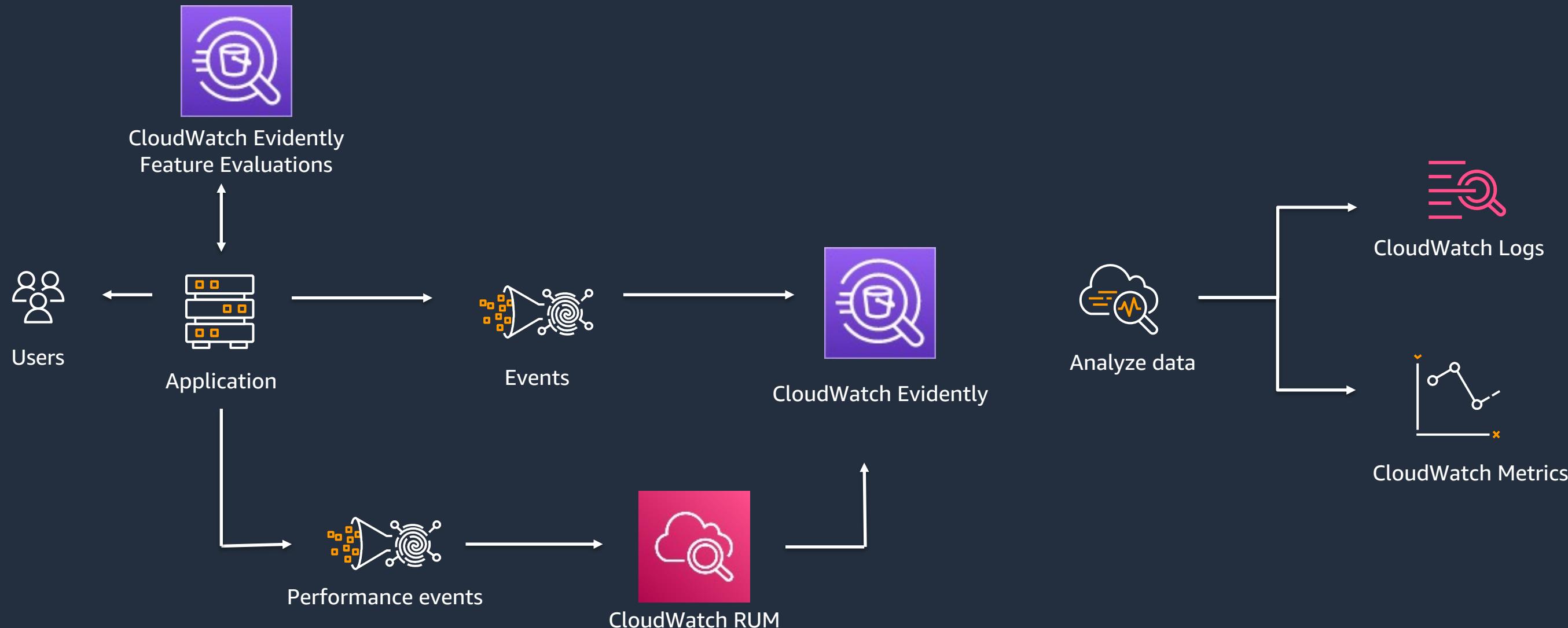


Launch monitoring
**Reduce unintended
consequences**



Experimentation
Remove guesswork

CloudWatch Evidently—how it works



Value proposition for launch monitoring



Small traffic

Limit exposure



Monitor and act

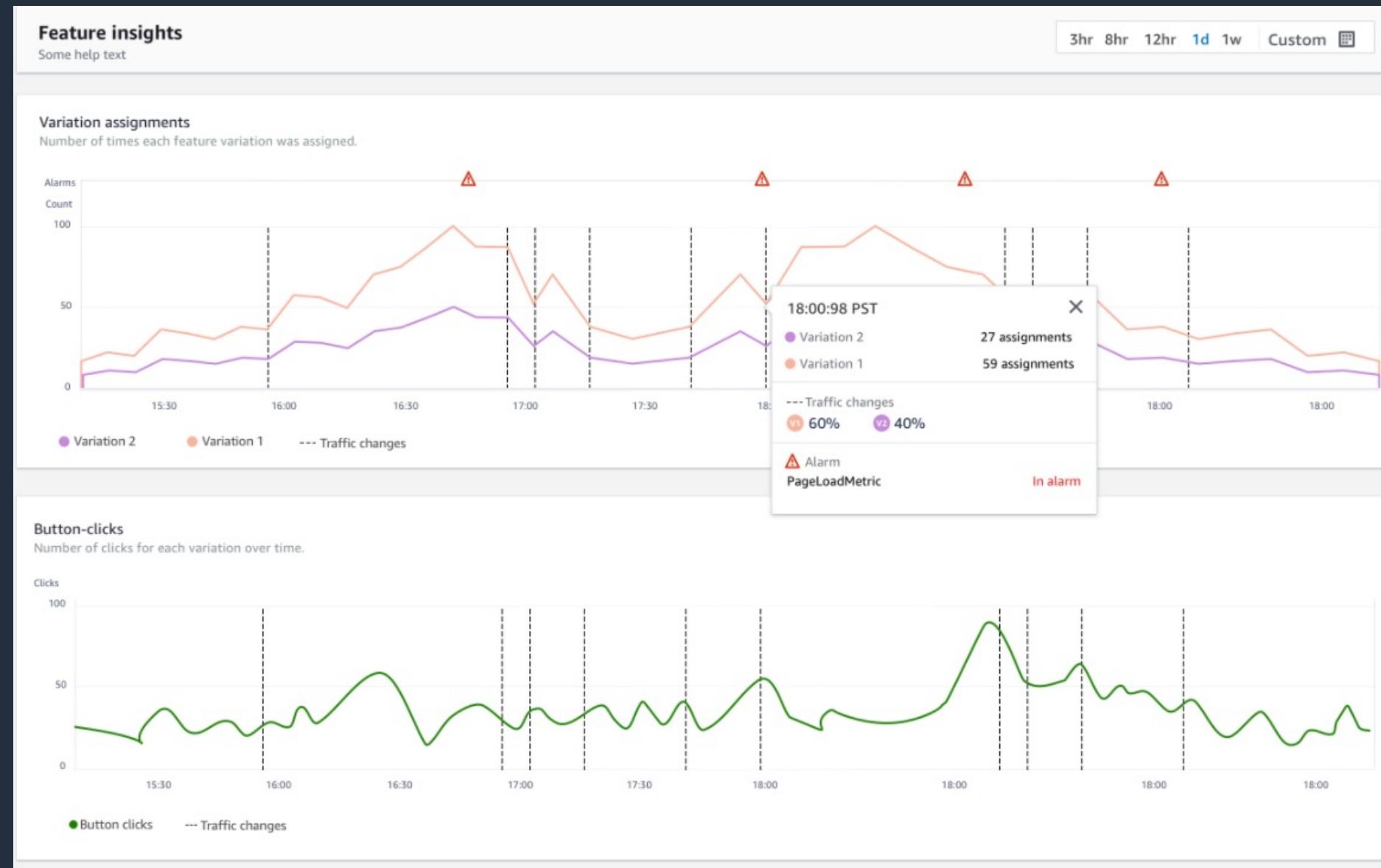
**Visualize anomalies,
optional stop switch**



Dial up/down traffic

**Include bake time
and automate**

CloudWatch Evidently: launch monitoring



Automate dial up

Launch history (1)

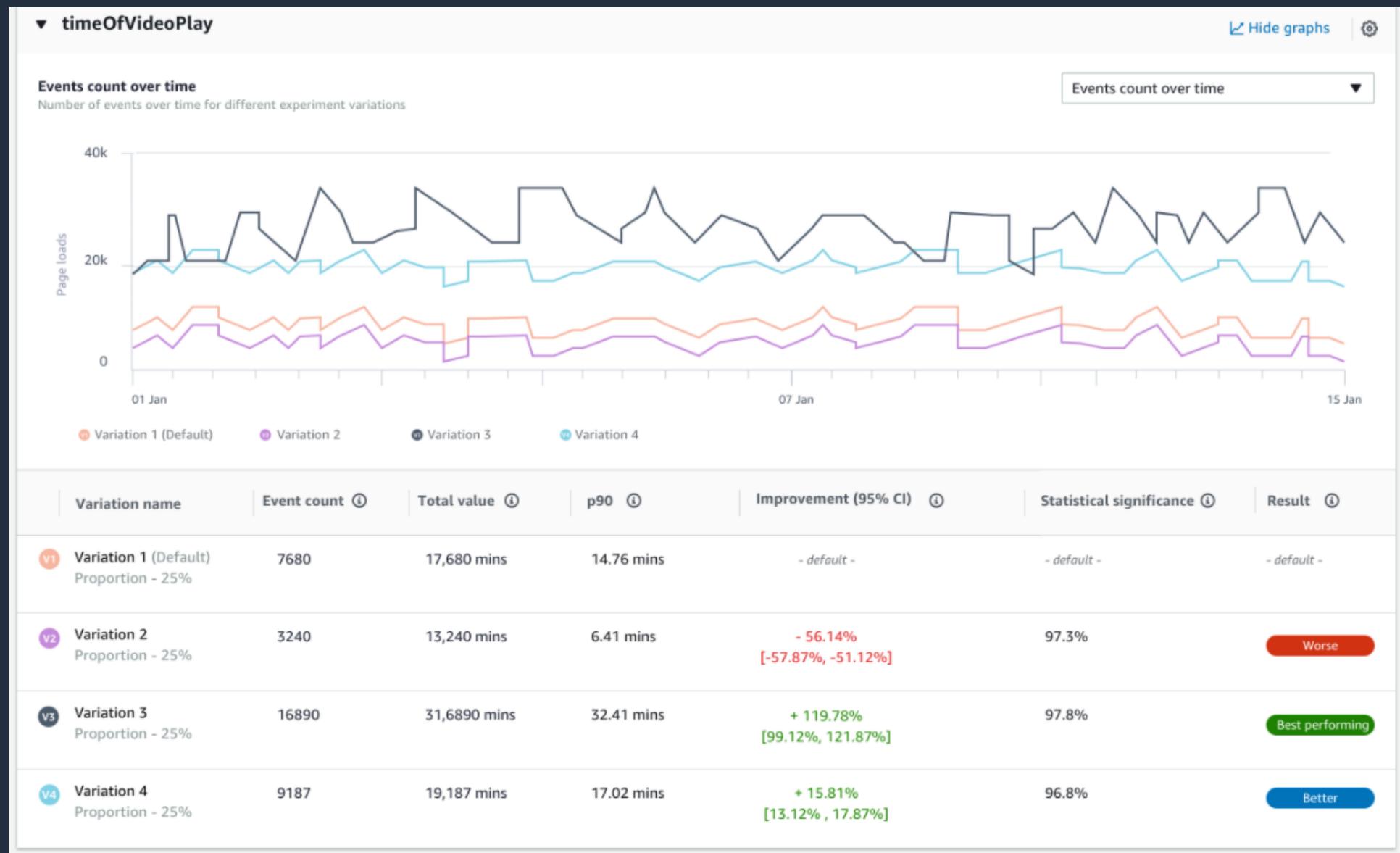
Launch history (1)				
Variation and traffic	Timestamp	User	Comments	State
 v1 50% v2 50%	5 days ago April 1, 2021, 00:09:03 am PST	ajassy	*Launch configuration defined during setup.*	 In progress

Scheduled steps (4)

Duration: 30 days | Tuesday, April 1, 2021 09:00 am PST to Friday, April 30, 2021 11:59 pm PST

Schedule	Variation and traffic	Status
Thursday, April 1, 2021 09:00 am PST 	 v1 50% v2 50%	Completed
Friday, April 9, 2021 09:00 am PST 	 v1 60% v2 40%	Completed
Thursday, April 20, 2021 09:00 am PST	 v1 75% v2 25%	Upcoming
Friday, April 30, 2021 09:00 am PST	 v1 100%	

CloudWatch Evidently experiments



Getting started

Create features
in Evidently

Instrument your
applications
with Evidently
SDK for feature
code and events
to be measured

Start launch/
experiment in
Evidently by
setting traffic
percentages

Visualize results
Evidently on
how your
variations are
performing



AWS CloudTrail & CloudTrail Insights

AWS CloudTrail

- Track user and resource activity across your AWS infrastructure and resources for governance and auditing.
- Identify and respond to unusual usage based on automated analysis.



Capture

Record activity as CloudTrail events



Store

Retain events logs in secure S3 bucket



Act

Trigger actions when important events are detected



Review

Analyze findings or recent and historical activity

AWS CloudTrail Features



**Compliance
Aid**



**Visibility
into Activity**



**Anomaly
Detection**



**Detect Data
Exfiltration**



**Automate
Security
Analysis**



**Analyze
Permissions**

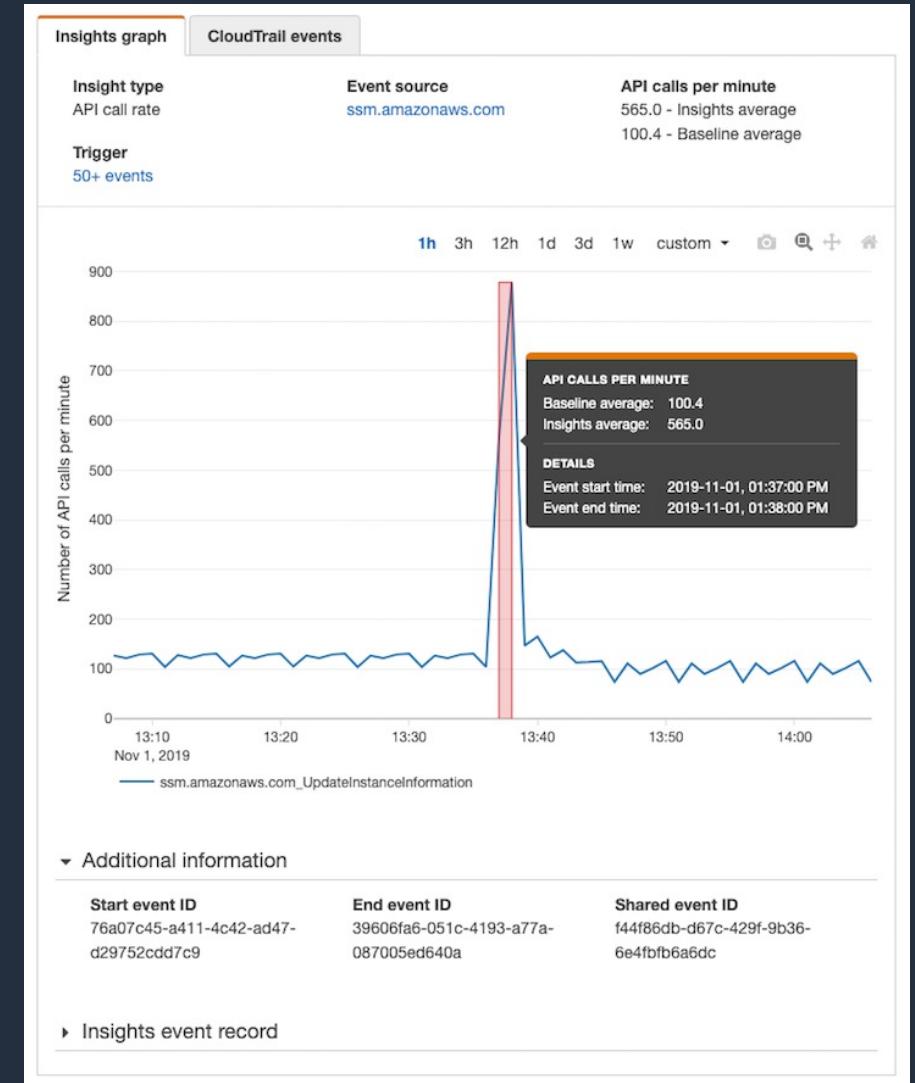


**Detect Unusual
Activity**

CloudTrail Insights



- Identify and respond to unusual operational activity
 - Unexpected spikes in resource provisioning
 - Bursts of IAM management actions
 - Gaps in periodic maintenance activity
- Automatic analysis of API calls and usage patterns
- Alerts when unusual activity is detected



What you can do with CloudTrail today

- Identify users logged in during an incident, and all actions taken during that period
- Notify when admin privileges are granted or console logins occur
- Detect access from authorized networks or IP addresses
- Identify when a file or object has changes to public access, and who made the change
- Understand top user, role, or service callers of API calls or Lambda functions
- Get alerted when you misconfigure your autoscaling script
- Comply with internal and regulatory compliance requirements with the immutable history of all AWS activity



AWS Config

AWS Config Rules

- Set up rules to check configuration changes recorded
- Use pre-built rules provided by AWS
- Author custom rules using AWS Lambda
- Invoked automatically for continuous assessment
- Use dashboard for visualizing compliance and identifying offending changes
- Community-contributed custom rules at <https://github.com/awslabs/aws-config-rules>



Amazon VPC Flow Logs

Amazon VPC Flow Logs

Stores logs in AWS CloudWatch Logs

- Can be enabled on
 - Amazon VPC, a subnet, or a network interface
 - Amazon VPC & subnet enables logging for all interfaces in the VPC/subnet
 - Each network interface has a unique log stream
- Flow logs **do not capture real-time** log streams for your network interfaces
- Filter desired result based on need
 - All, Reject, Accept
 - Troubleshooting or security related with alerting needs?
 - Think before enabling All on VPC, will you use it?

Amazon VPC Flow Logs

- Agentless
- Enable per ENI, per subnet, or per VPC
- Logged to AWS CloudWatch Logs
- Create CloudWatch metrics from log data
- Alarm on those metrics

Interface	Source IP	Source port	Protocol	Packets	Destination IP	Destination port	Bytes	Start/end time	Accept or reject
AWS account									
Event Data	eni-b30b9cd5 119.147.115.32 10.1.1.179 6000 22 6 1 40 1442975475 1442975535 REJECT OK								
▼ 2 41747	eni-b30b9cd5 169.54.233.117 10.1.1.179 21188 80 6 1 40 1442975535 1442975595 REJECT OK								
▼ 2 41747	eni-b30b9cd5 212.7.209.6 10.1.1.179 3389 3389 6 1 40 1442975596 1442975655 REJECT OK								
▼ 2 41747	eni-b30b9cd5 189.134.227.225 10.1.1.179 39664 23 6 2 120 1442975656 1442975716 REJECT OK								
▼ 2 41747	eni-b30b9cd5 77.85.113.238 10.1.1.179 0 0 1 1 100 1442975656 1442975716 REJECT OK								
▼ 2 41747	eni-b30b9cd5 10.1.1.179 198.60.73.8 512 123 17 1 76 1442975776 1442975836 ACCEPT OK								



Cost Monitoring

Tags

Key	Value
name	Jane_Doe
group	dev
costcenter	4004
use	image_svr

Key (Attribute): 127 Unicode characters

Value (Detail/Description): 255 Unicode characters

Tags per resource: 50 tags

Types of Tags

Resource Tags

- Provide the ability to organize and search within and across resources
- Filterable and Searchable
- Do not appear in Detail Billing Report

Cost Allocation Tags

- Information presented in Detailed Billing Report and Cost Explorer
- Available on certain services or limited to components within a service (e.g. S3 bucket but not objects)

AWS Cost Explorer

CONSOLE-BASED COST AND USAGE REPORTING



Filter/Group your data



Save your progress



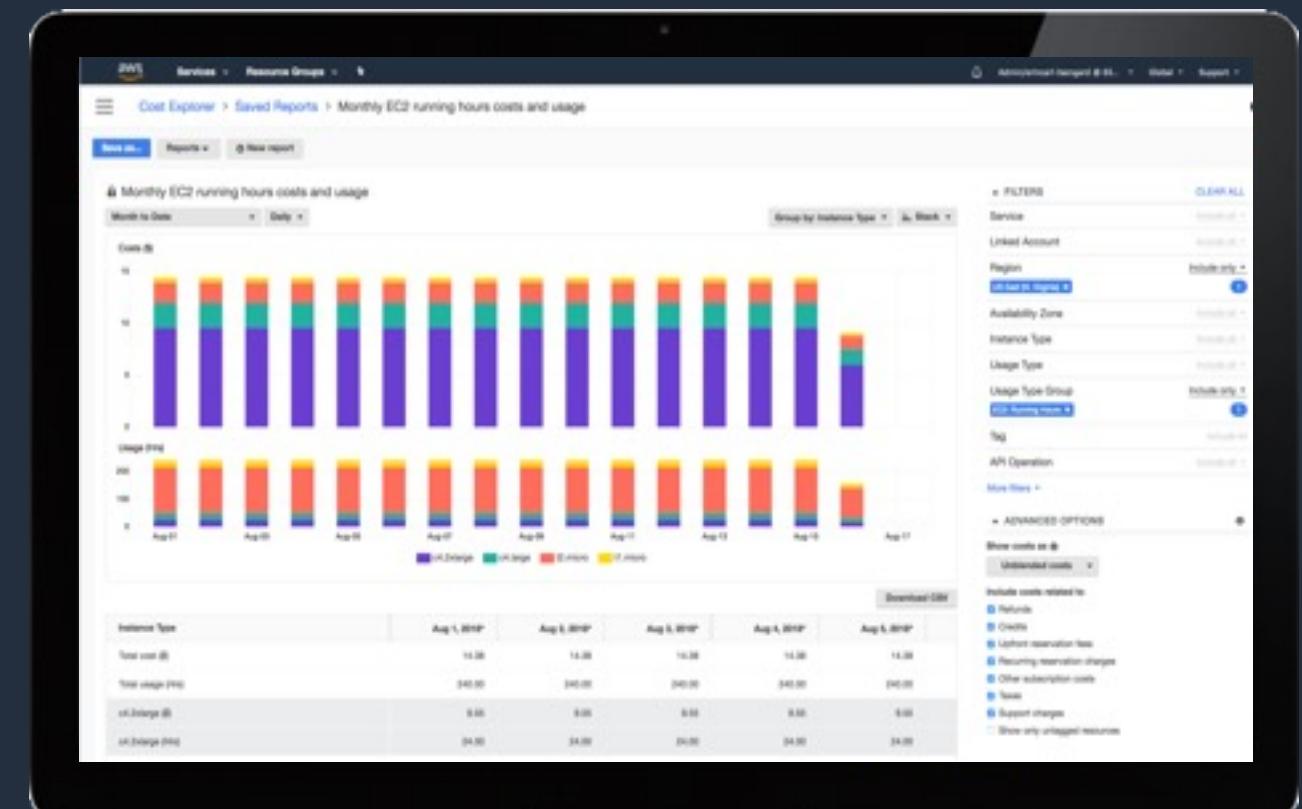
Set time interval and granularity



Forecast future costs and usage



Build custom applications

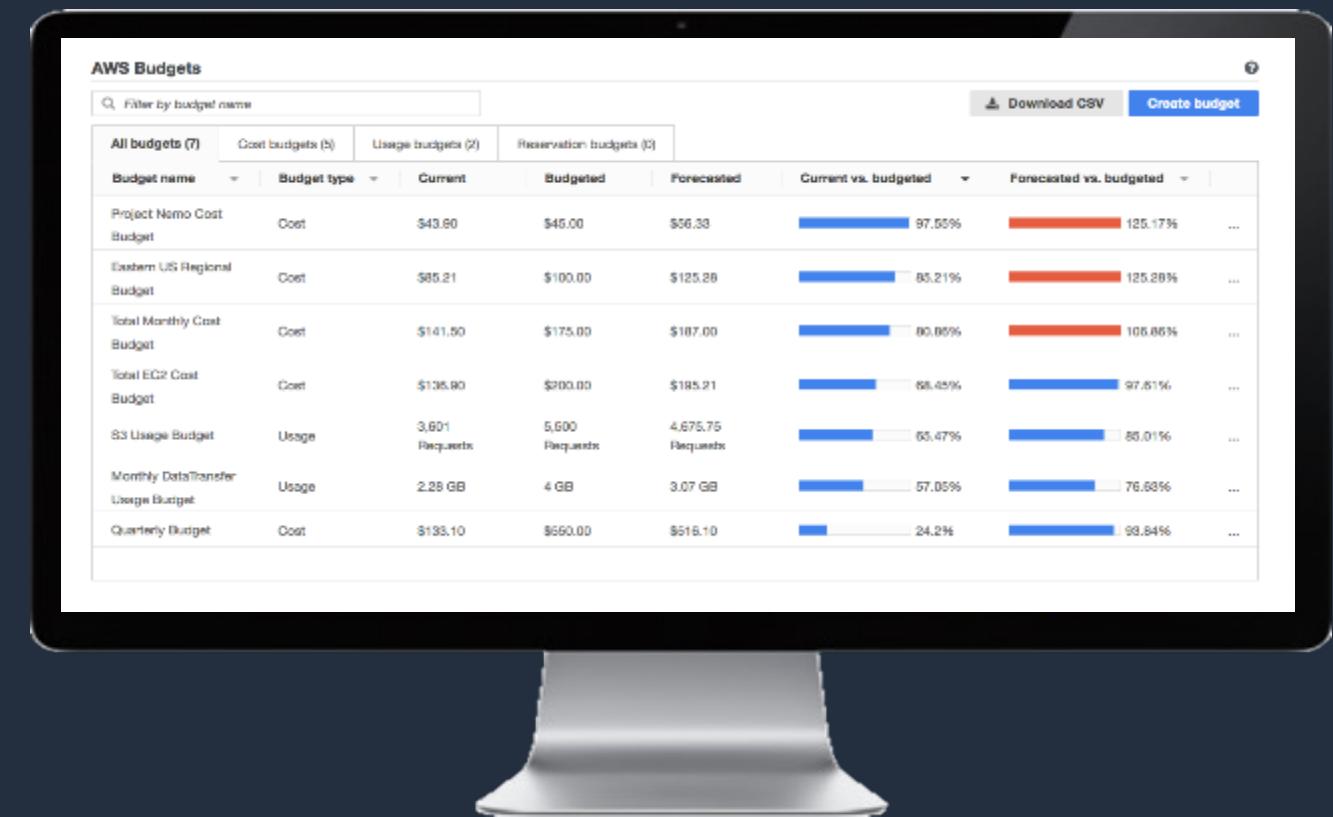


AWS Budgets

AWS Budgets gives you the ability to set custom budgets that alert you when your cost or usage exceed (or are forecasted to exceed) your budgets amount.

Benefits

- Customizable budgets
- Ongoing monitoring and alert notification
- Flexible Automation



AWS Budgets Reports

- Set up daily, weekly, or monthly AWS Budgets Reports emails
- For stakeholders with limited or no access to AWS Cost Management dashboard

Dear AWS Customer,

You requested that we provide a daily update on the status of the following budgets.

Budget Name	Budget Type	Current	Budgeted	Forecasted	Current vs. Budgeted	Forecasted vs. Budgeted
SG EC2 Product Budget	Cost	\$0.00	\$5.00	-	0.00%	-
Monthly EC2 Budget	Cost	\$148.46	\$75.00	\$501.90	197.94%	669.20%
Monthly budget for EC2	Cost	\$166.83	\$84.43	\$562.54	197.60%	666.28%
SG EC2 Usage	Cost	\$0.00	\$100.00	-	0.00%	-
e.g., My Monthly EC2 Budget 17	Cost	\$148.46	\$100.00	\$501.90	148.46%	501.90%
Monthly EC2 Budget	Cost	\$190.80	\$200.00	\$643.99	95.40%	321.99%
Monthly EC2 Costs	Cost	\$266.01	\$584.62	\$871.89	45.50%	149.14%
My Monthly EC2 Budget	Cost	\$0.00	\$1,000.00	-	0.00%	-
EC2 Data Transfer	Usage	0.12 GB	0.50 GB	0.42 GB	23.80%	84.40%
Daily EC2 Utilization	RI Utilization	100.00%	100.00%	-	100.00%	-
Daily EC2 RI Coverage	RI Coverage	20.90%	100.00%	-	20.90%	-
Daily EC2 Coverage	RI Coverage	20.90%	100.00%	-	20.90%	-

[Go to AWS Budgets Report Dashboard](#)

AWS Budgets | Alerting

▼ Alert #1

Set alert threshold

Threshold

When should this alert be triggered?

 80 % of budgeted amount

Trigger

How should this alert be triggered?

 Actual

Notification preferences - *Optional*

Select one or more notification preferences to receive alerts.

Email recipients

Specify the email recipients you want to notify when the threshold has exceeded.

Separate email addresses using commas

Maximum number of email recipients is 10.

► [Amazon SNS Alerts](#) Info

► [Amazon Chatbot Alerts](#)

Budget Notification: Total Monthly Cost Budget is in Alarm State

 no-reply-aws@amazon.com <no-reply-aws@amazon.com>

Tuesday, August 1, 2017 at 6:55 PM

To: Carlson, Erin



08/02/2017

AWS Budget Notification

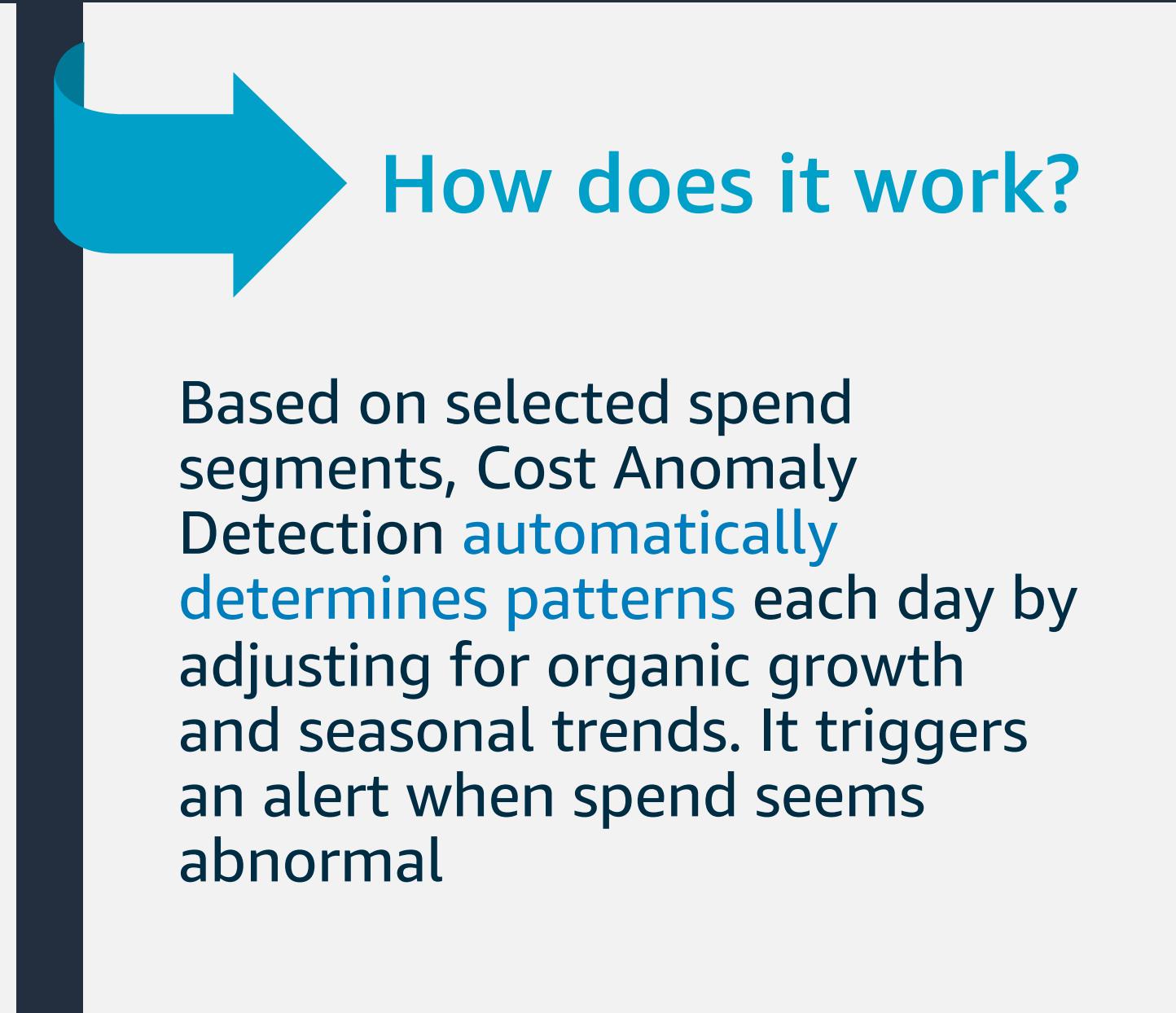
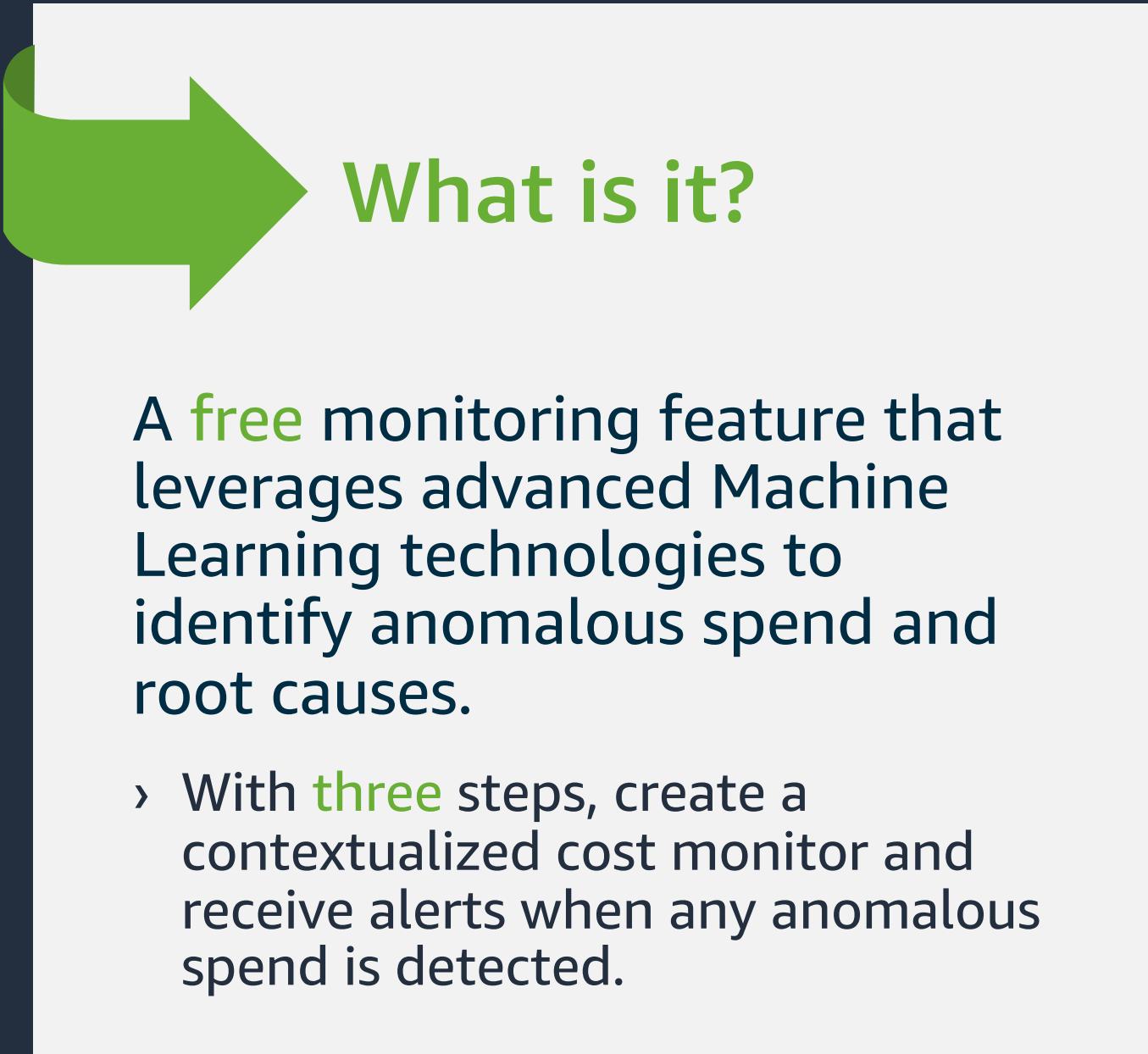
Dear AWS Customer,

You requested that we notify you when your **Forecasted Cost** for your budget "**Total Monthly Cost Budget**" is **greater than \$150.00**. Your **Forecasted Cost** for this budget is now **\$199.28**. You can find further details below and by accessing your AWS Budgets dashboard.

Budget Name	Budget Type	Budgeted Value	Notification Threshold	Forecasted Value
Total Monthly Cost Budget	Forecasted	\$150.00	> \$150.00	\$199.28

[Go to AWS Budgets Dashboard](#)

AWS Cost Anomaly Detection



AWS Cost Anomaly Detection

SAVE TIME MONITORING SPEND AND FOCUS ON DRIVING INNOVATION

Easy start

Simple setup to evaluate spend anomalies for all AWS services individually, member accounts, cost allocation tags, or AWS Cost Categories.

Automated root cause

Receive automated root cause analysis, pin-pointing potential cost drivers, such as usage type, specific AWS service, Region, and Member Account(s).

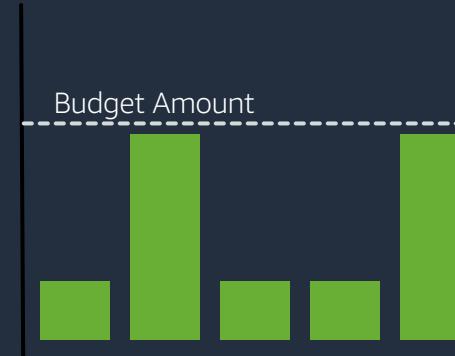
Minimize surprise bills

Stay informed with automated detection alerts, via email or SNS topic at the frequency of your choice (individual alerts or daily or weekly summary).

Not all alerts tell the same story

LEVERAGE AWS BUDGETS AND AWS COST ANOMALY DETECTION TO AVOID SURPRISES

AWS Budgets



AWS Cost Anomaly Detection

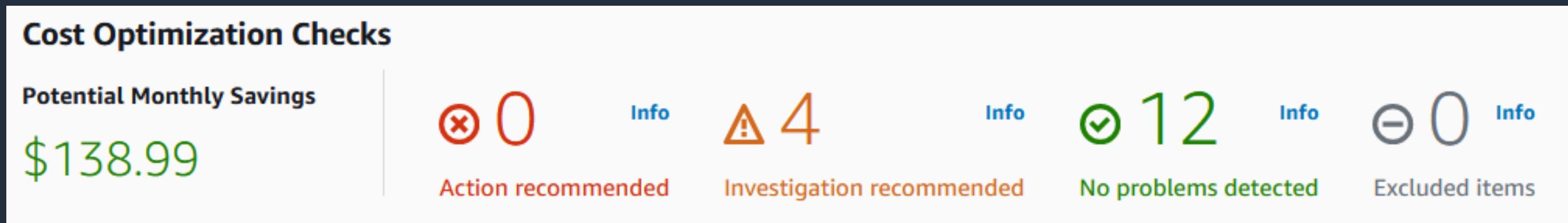


AWS Trusted Advisor



- A tool that provides guidance following AWS best practices
- All customers have access to Core checks
- Enterprise Support and Business Support customers have access to the full set of checks including Cost Optimization

AWS Trusted Advisor Cost Optimization Checks



- Underutilized resources
- Idle resources
- RI Recommendations



Q&A