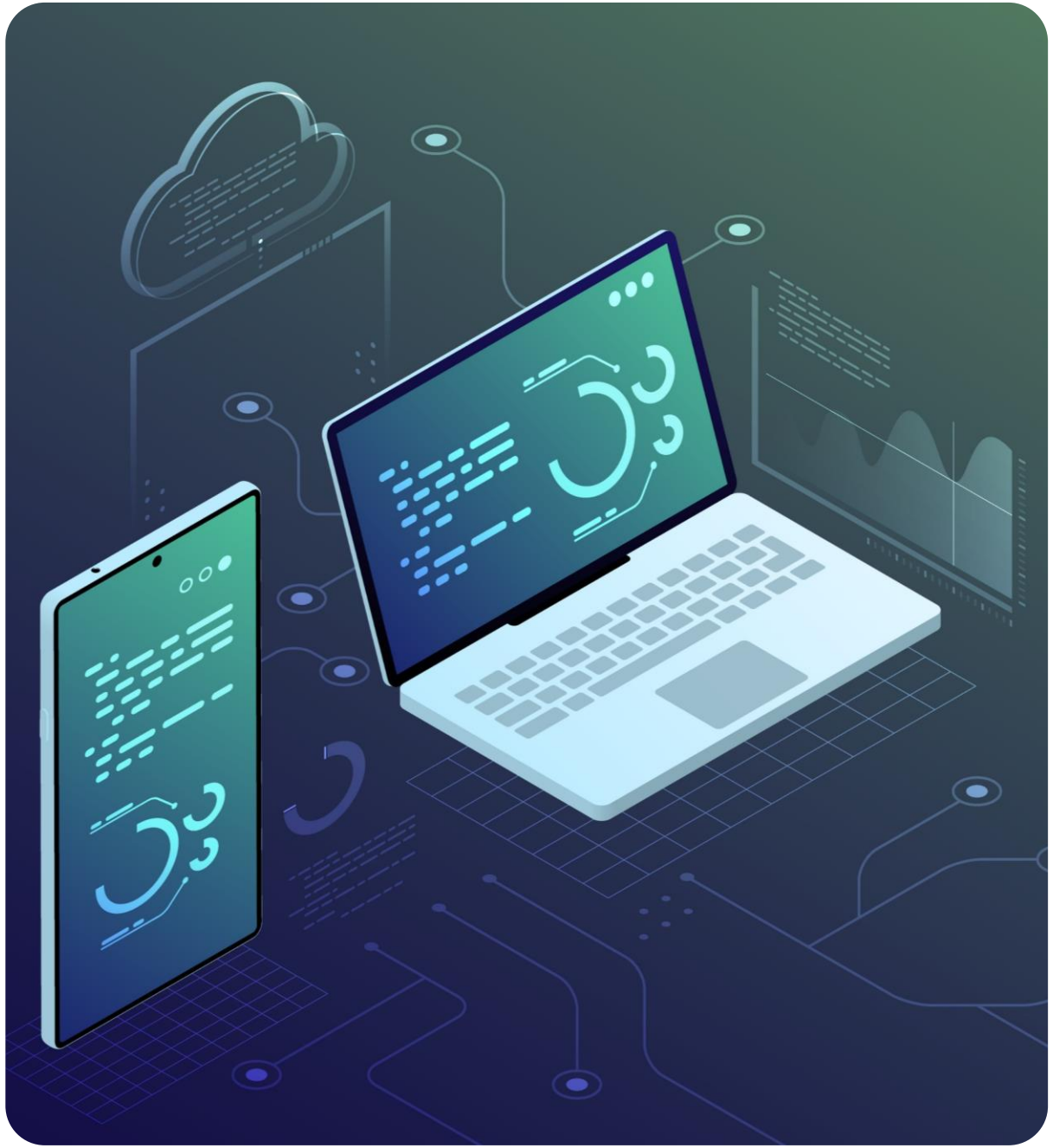
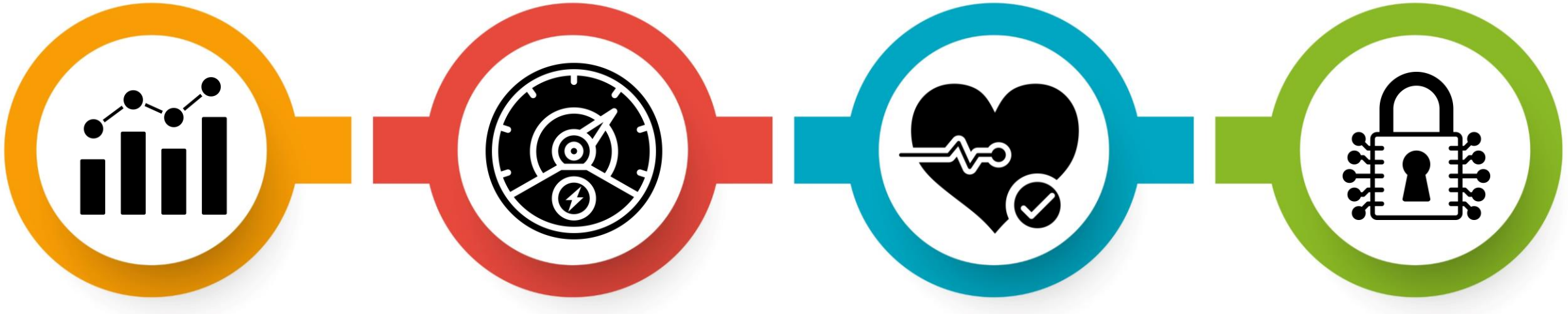
Monitoring in Cloud



Monitoring

Why monitoring is important?

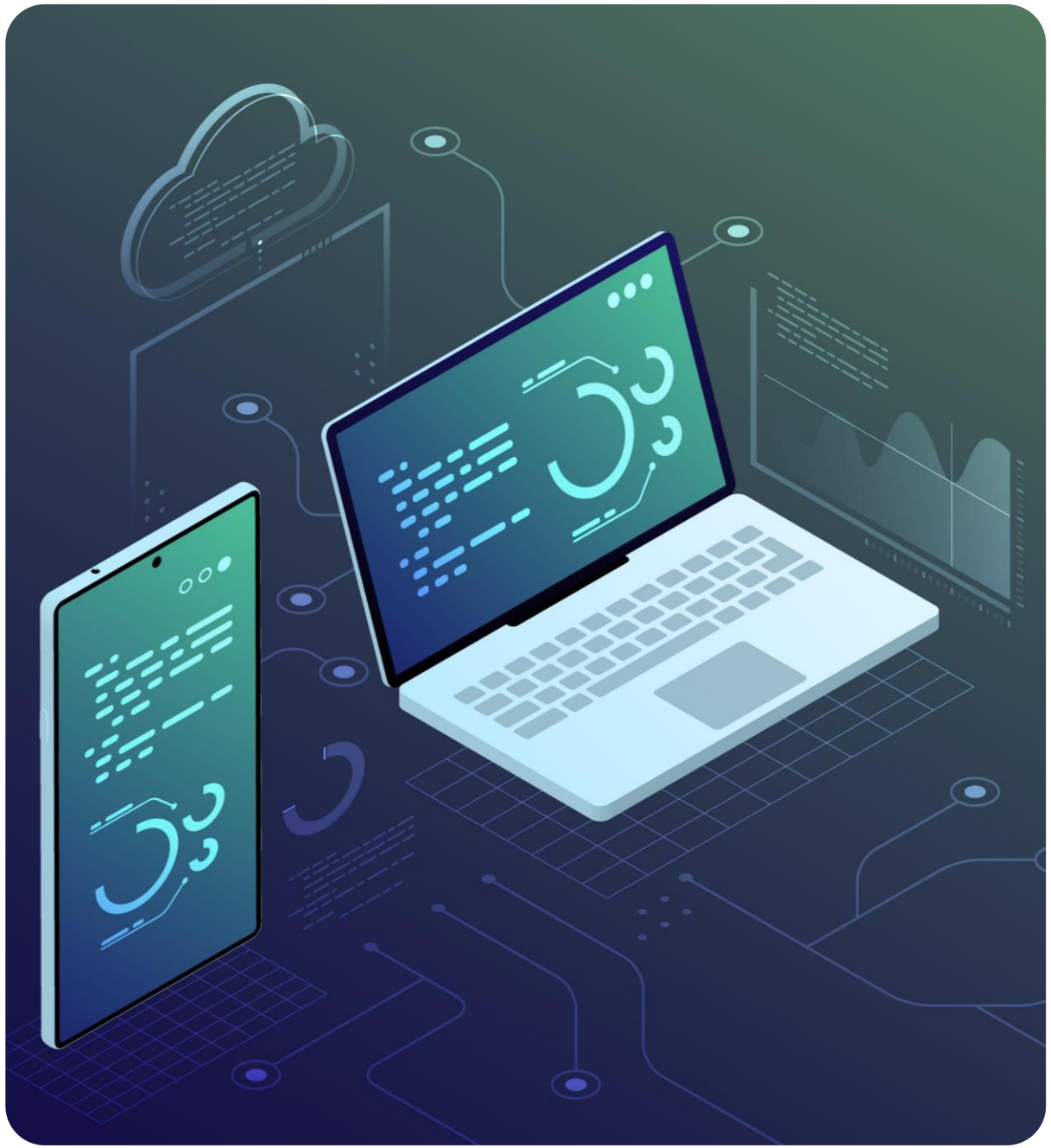


Performance

Utilization

Health

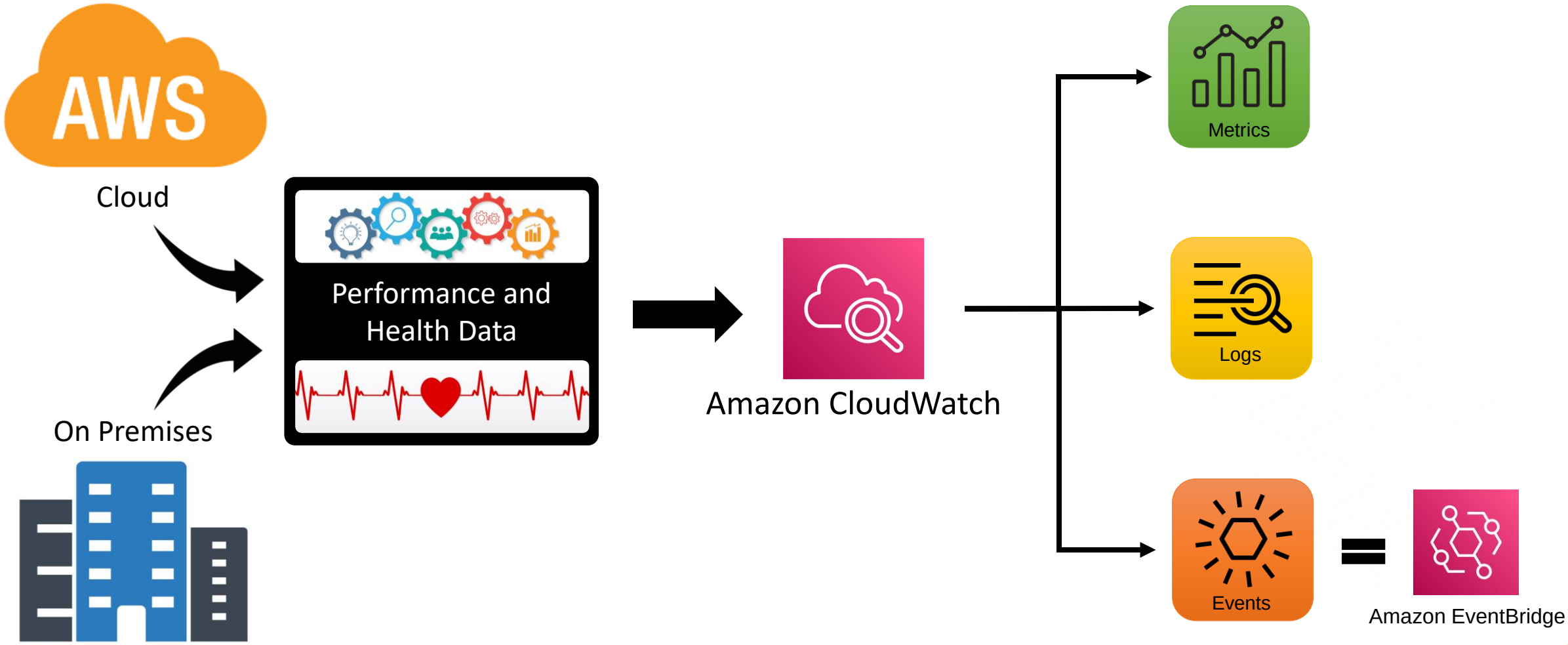
Security

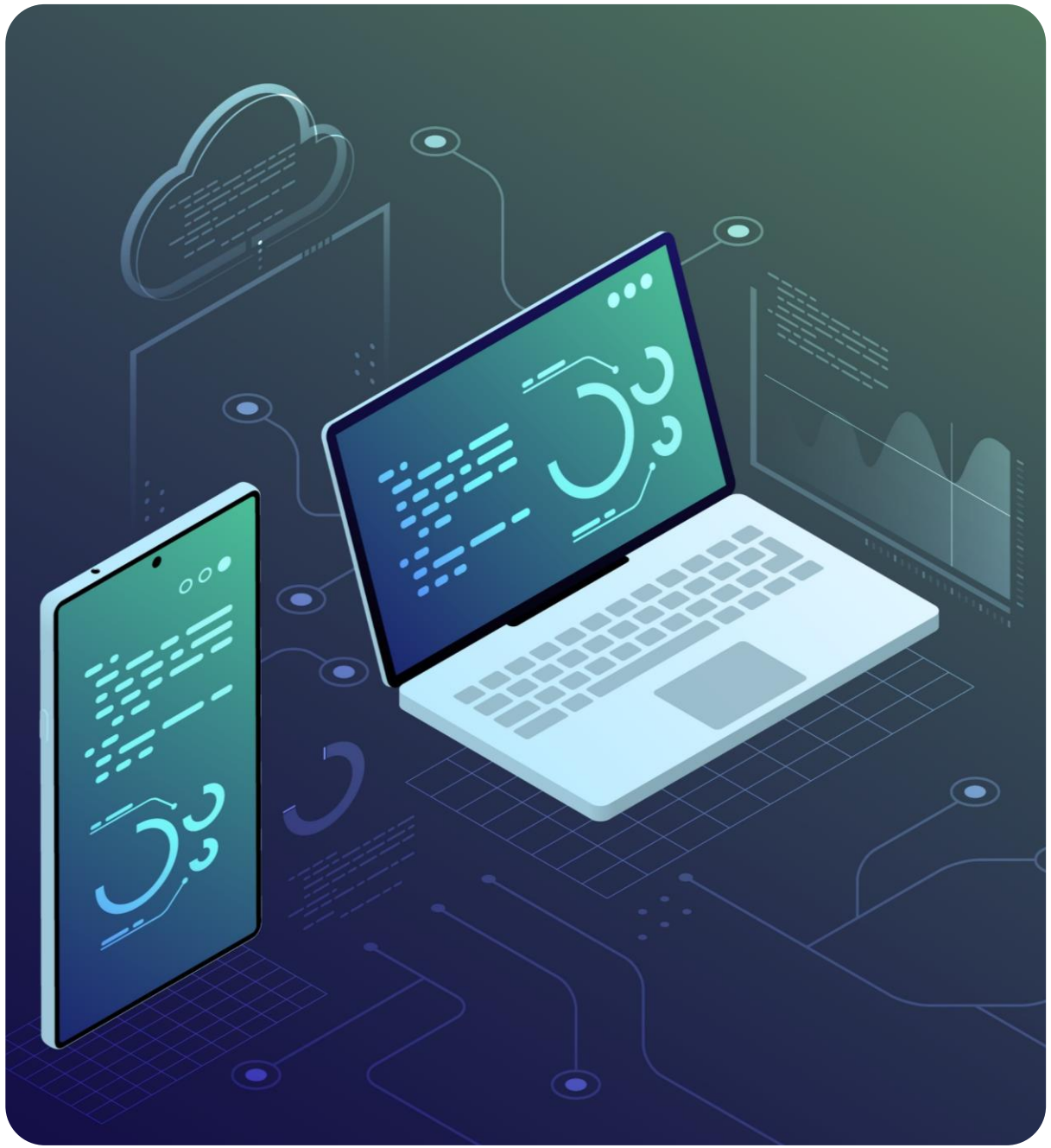


Amazon CloudWatch

Amazon CloudWatch

- Amazon CloudWatch allows you to collect, access, and correlate performance and health data of your application and infrastructure running on AWS and on-premises.



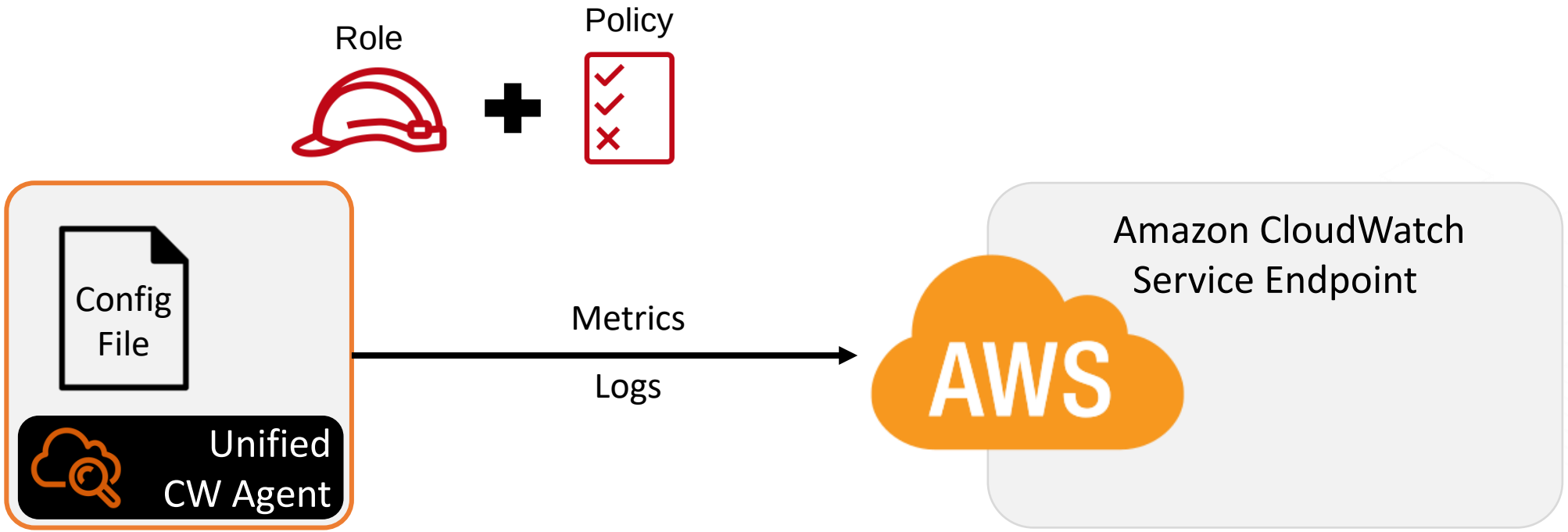


Custom Metrics

Custom Metrics

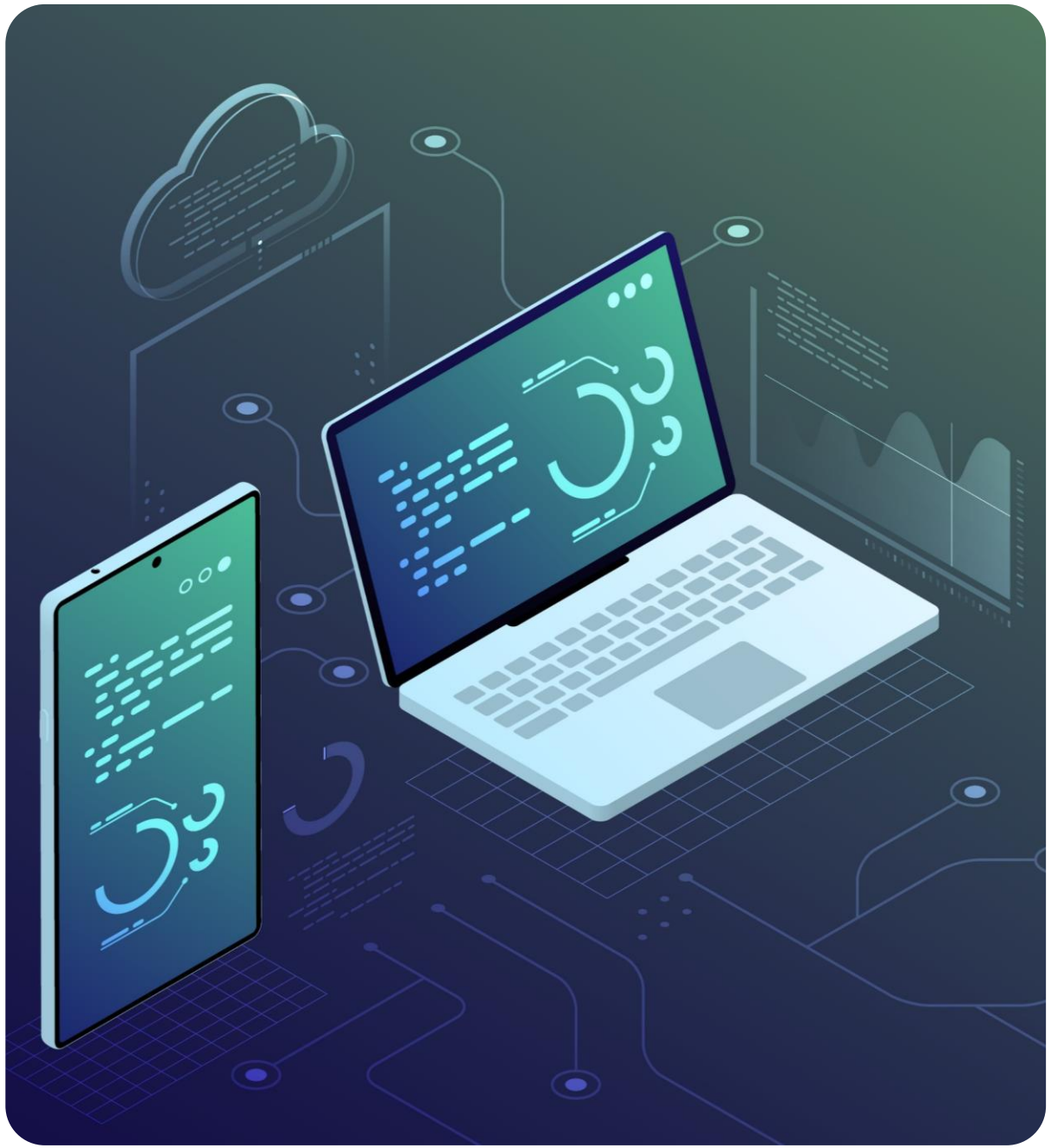
- You can publish custom metrics (your business and application metrics) to CloudWatch using the AWS CLI or an API.

- You can use the open source Unified CloudWatch agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers.



Configuring Custom Metrics

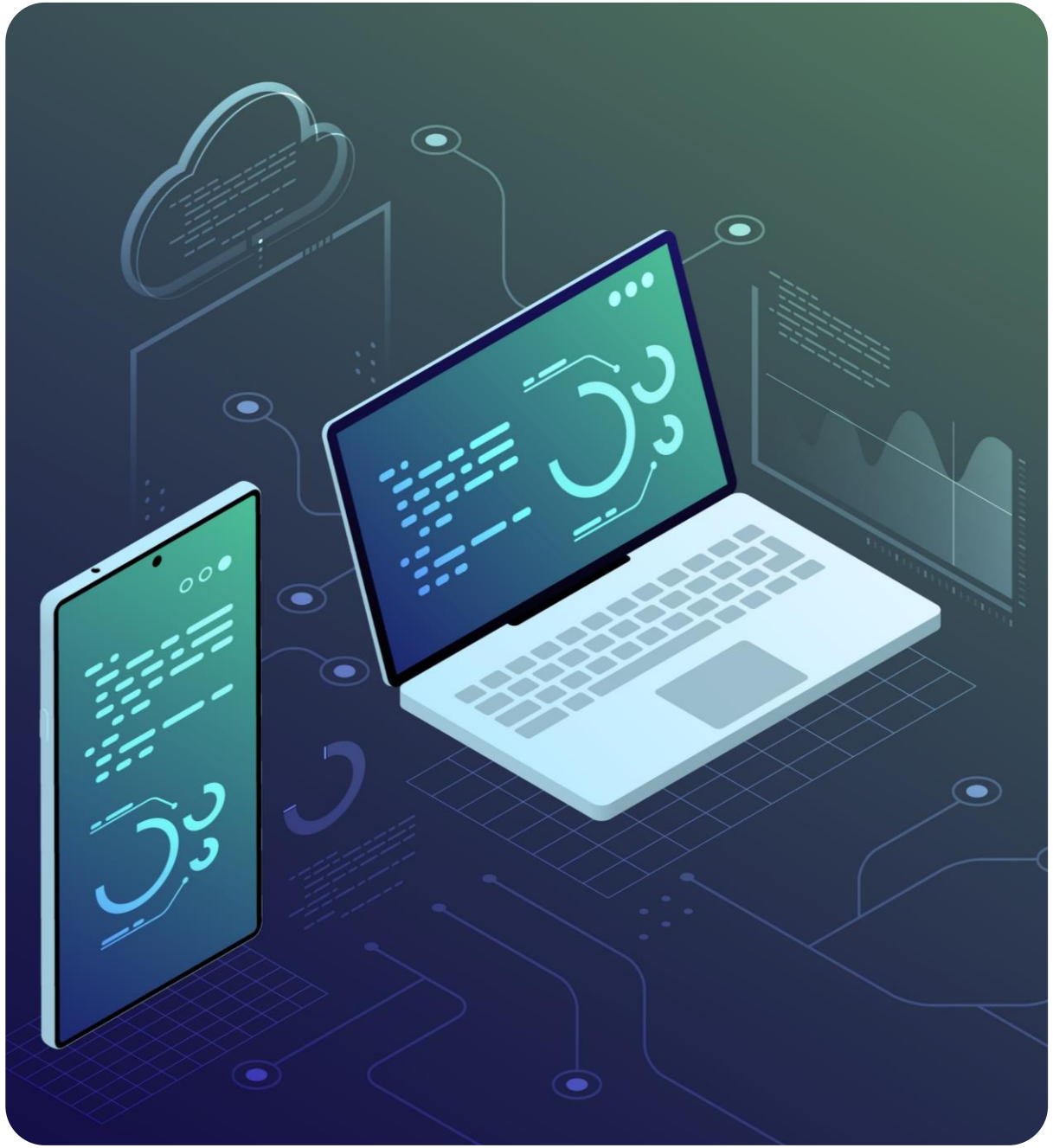
- Install Agent
  - sudo yum install amazon-cloudwatch-agent
- Configure it
  - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
- Create and associate IAM role (or user)
  - You use IAM roles on Amazon EC2 instances, and you use IAM users with on-premises servers.
- Start the agent
  - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -m ec2 -a status

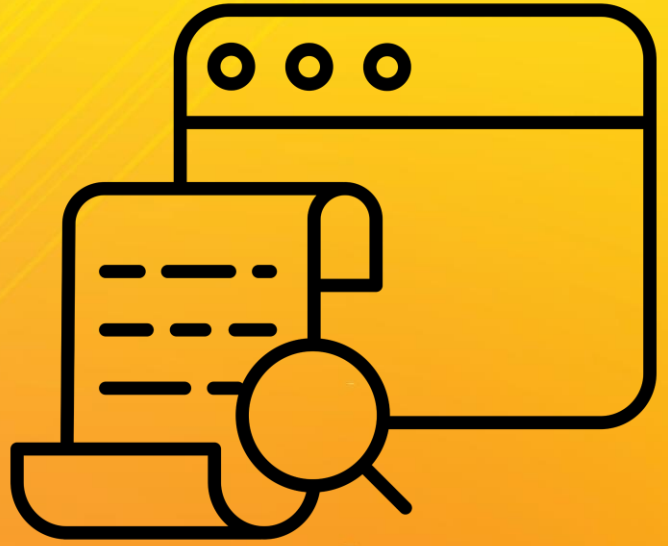


Alarms

Amazon CloudWatch Alarms

- An alarm watches a single metric over a specified time period, and performs one or more specified actions, based on the value of the metric relative to a threshold over time.
- You can use an alarm to automatically initiate actions on your behalf. The most common type of alarm action is to notify one or more people by sending a message to an Amazon Simple Notification Service topic.
- A metric alarm has the following possible states:
  - **OK** – The metric or expression is within the defined threshold.
  - **ALARM** – The metric or expression is outside of the defined threshold.
  - **INSUFFICIENT_DATA** – The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state.
- You can also add alarms to dashboards.

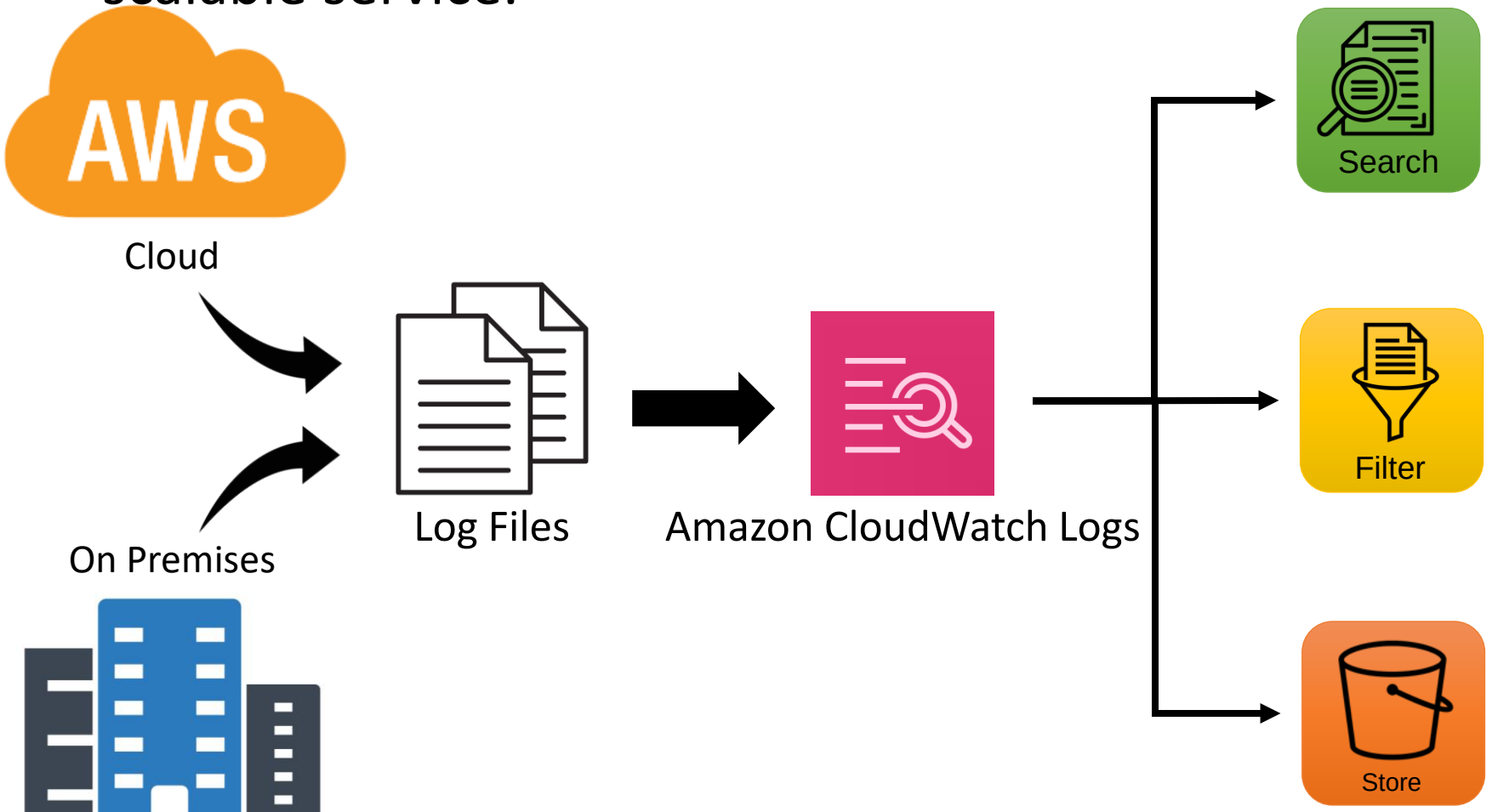




Amazon CloudWatch Logs

Amazon CloudWatch Logs

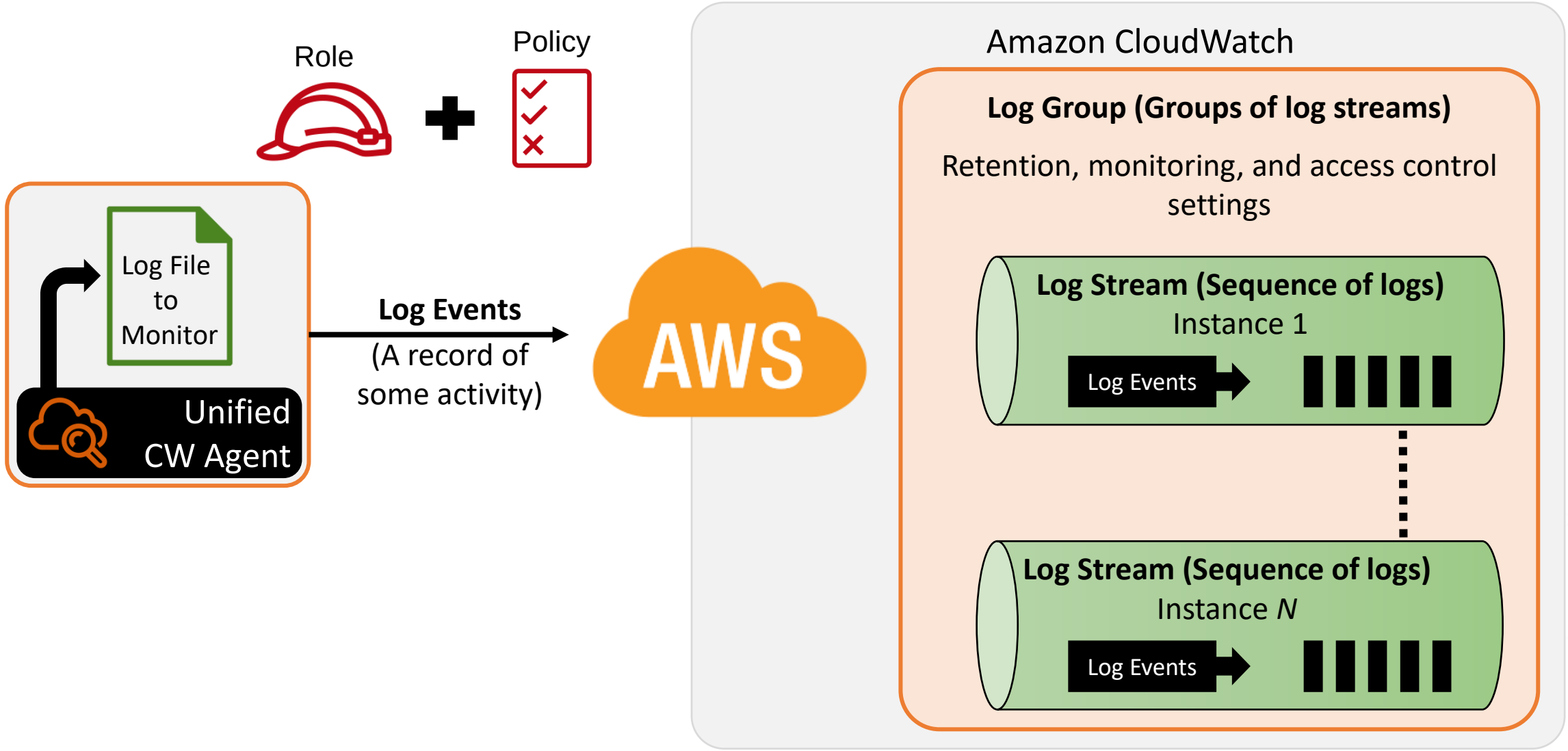
- CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service.



- You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis.

Publishing Logs

- You can publish logs to CloudWatch Logs using the unified agent.



Amazon CloudWatch Logs concepts

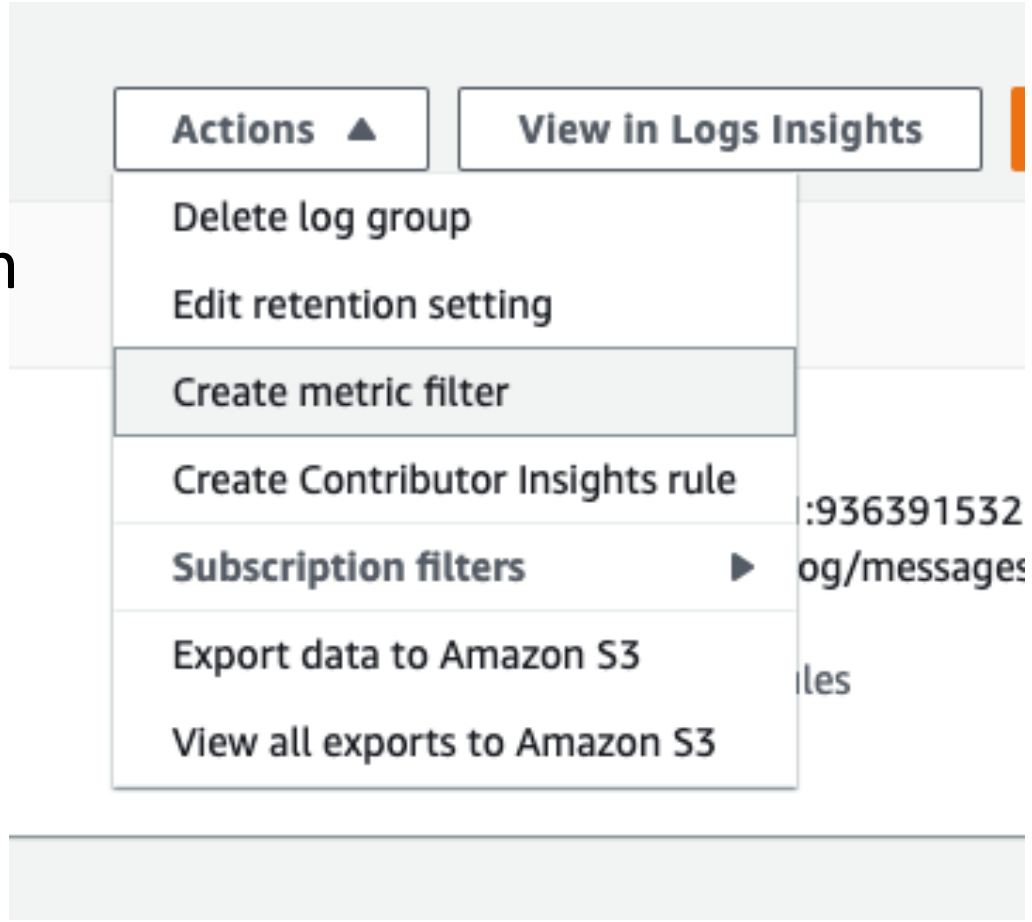
- Log events
  - A log event is a record of some activity recorded by the application or resource being monitored. The log event record that CloudWatch Logs understands contains two properties: the timestamp of when the event occurred, and the raw event message. Event messages must be UTF-8 encoded.
- Log streams
  - A log stream is a sequence of log events that share the same source. More specifically, a log stream is generally intended to represent the sequence of events coming from the application instance or resource being monitored. For example, a log stream may be associated with an Apache access log on a specific host.
- Log groups
  - Log groups define groups of log streams that share the same retention, monitoring, and access control settings. Each log stream has to belong to one log group. For example, if you have a separate log stream for the Apache access logs from each host, you could group those log streams into a single log group called MyWebsite.com/Apache/access_log.

Publishing Logs

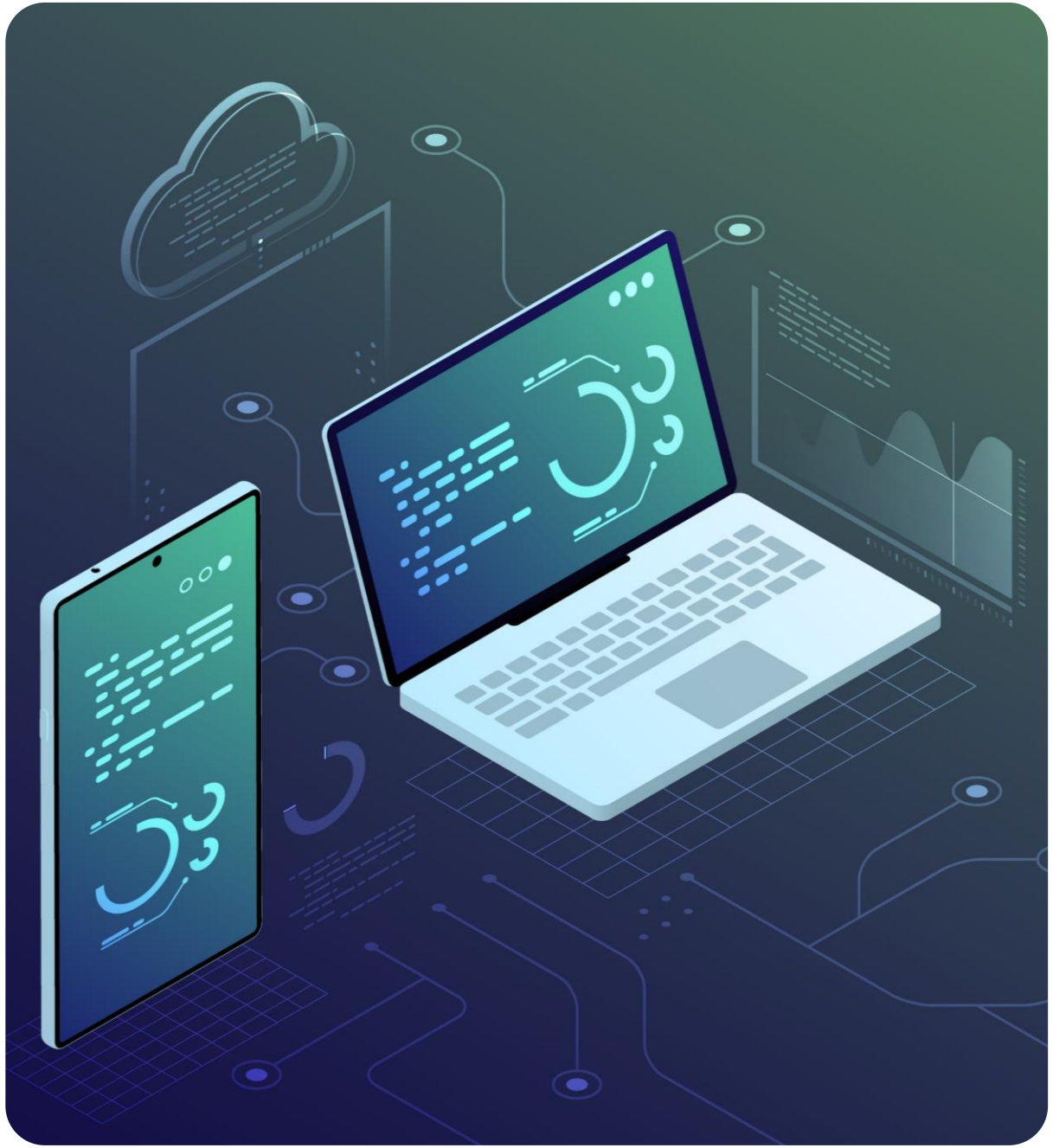
- Install Agent
  - sudo yum install amazon-cloudwatch-agent
- Configure it by providing detail of log file to monitor
  - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
- Create and associate IAM role (or user)
  - You use IAM roles on Amazon EC2 instances, and you use IAM users with on-premises servers.
- Start the agent
  - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -m ec2 -a start

CloudWatch Metric Filter

1. Create a Filter
2. Test the pattern
3. Add it to and Alarm
4. Get notified



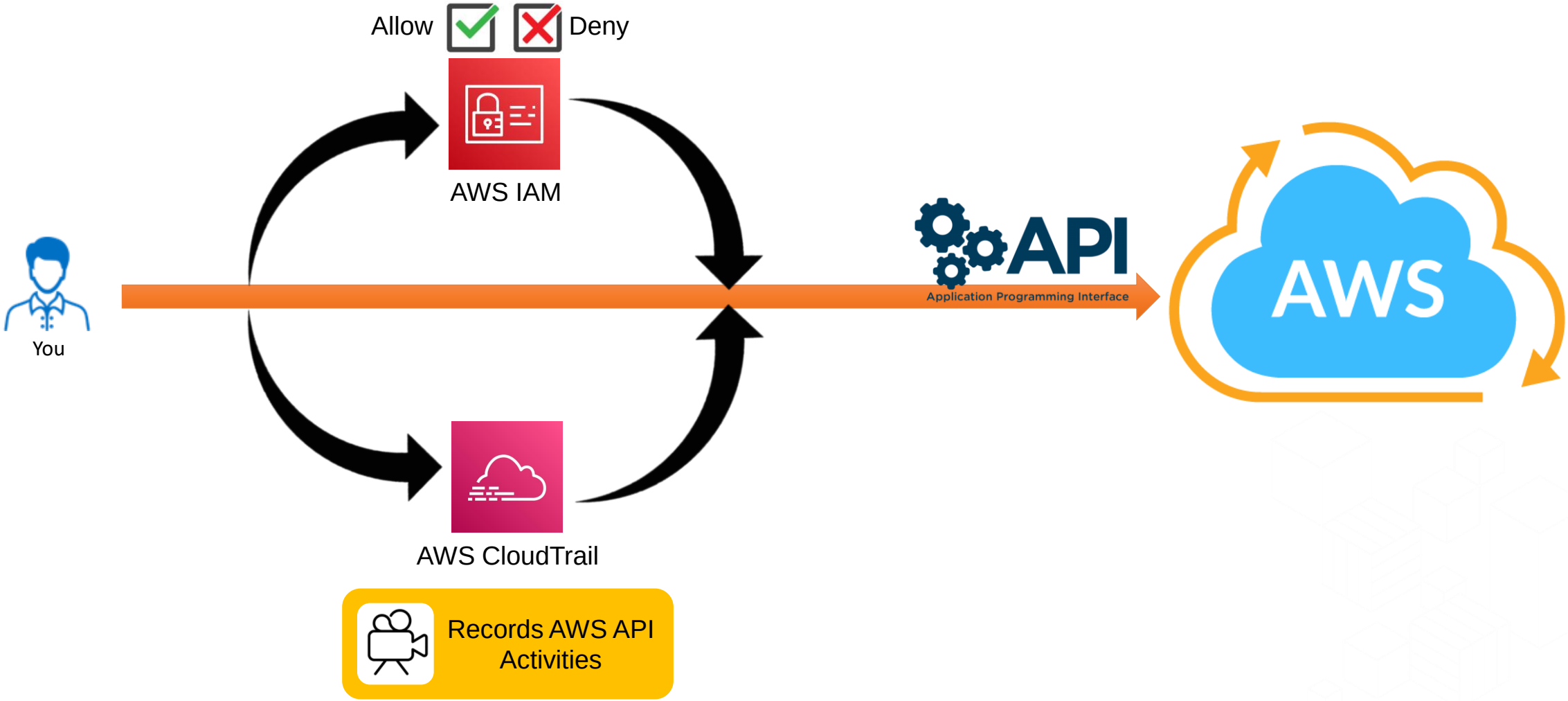
aws workshop studio



AWS CloudTrail

Security Camera

Flow of a request to AWS



AWS CloudTrail

- CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, SDKs, CLI, and other AWS services.

- CloudTrail helps identify who or what took which action, what resources were acted on, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.

- Logs API call to AWS endpoints
  - Success and Failure
  - Can store logs information in Amazon S3 bucket
  - Supports cross account, cross region

Concepts

- Events - An event in CloudTrail is the record of an activity in an AWS account.
  - There are three types of events that can be logged in CloudTrail:
    - Management events – Control Plane operations
    - Data events – Data plane operations performed on supported resource
    - CloudTrail Insights events – Capture unusual activity in your AWS account

- Trails - A trail is a configuration that helps deliver events to an S3 bucket that you specify.
  - You can also deliver and analyze events in a trail with CloudWatch Logs and CloudWatch Events.

CloudTrail Tutorial 

Best Practices

- Configure CloudTrail Logs to be delivered to a central S3 bucket in a separate AWS account.
- Configure MFA-delete on the Amazon S3 bucket storing log files.
- Configure versioning on the Amazon S3 bucket storing log files.
- Configure server-side encryption for CloudTrail log files.
- Configure log file validation for CloudTrail.