# Session 5 – AWS Security

## AWS Certified Solutions Architect – Associate

Nayef Khan, AWS Solutions Architect

Aug 20, 2021

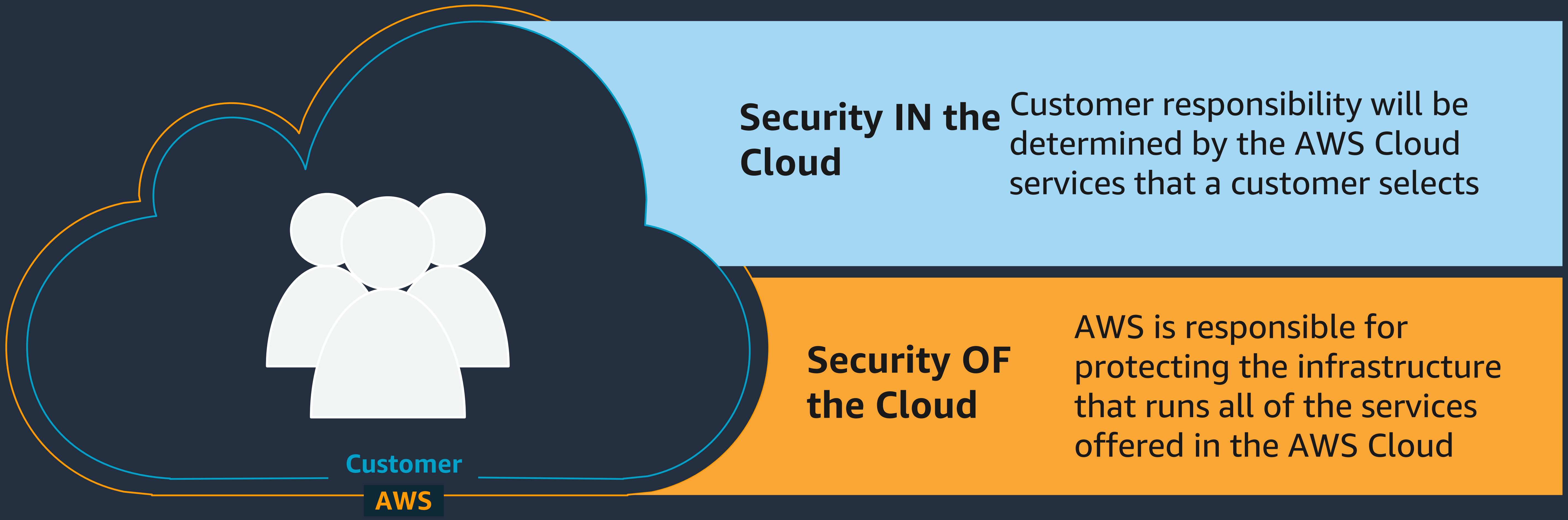
# Agenda

- Security Primer
- CloudWatch
- KMS and Cloud HSM
- WAF and Shield
- Parameter Store
- Secrets Manager
- AWS Config
- CloudTrail
- Cognito
- Practice Questions

0

# Security Primer

# Shared responsibility model



**Security IN the Cloud**

Customer responsibility will be determined by the AWS Cloud services that a customer selects

**Security OF the Cloud**

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud

# AWS security, identity, and compliance solutions

## Identity and access management

- AWS Identity and Access Management (IAM)
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager

## Detective controls

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender

## Infrastructure protection

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF – Web application firewall
- Amazon Virtual Private Cloud
- AWS PrivateLink
- AWS Systems Manager

## Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

## Incident response

- Amazon Detective
- CloudEndure DR
- AWS Config Rules
- AWS Lambda

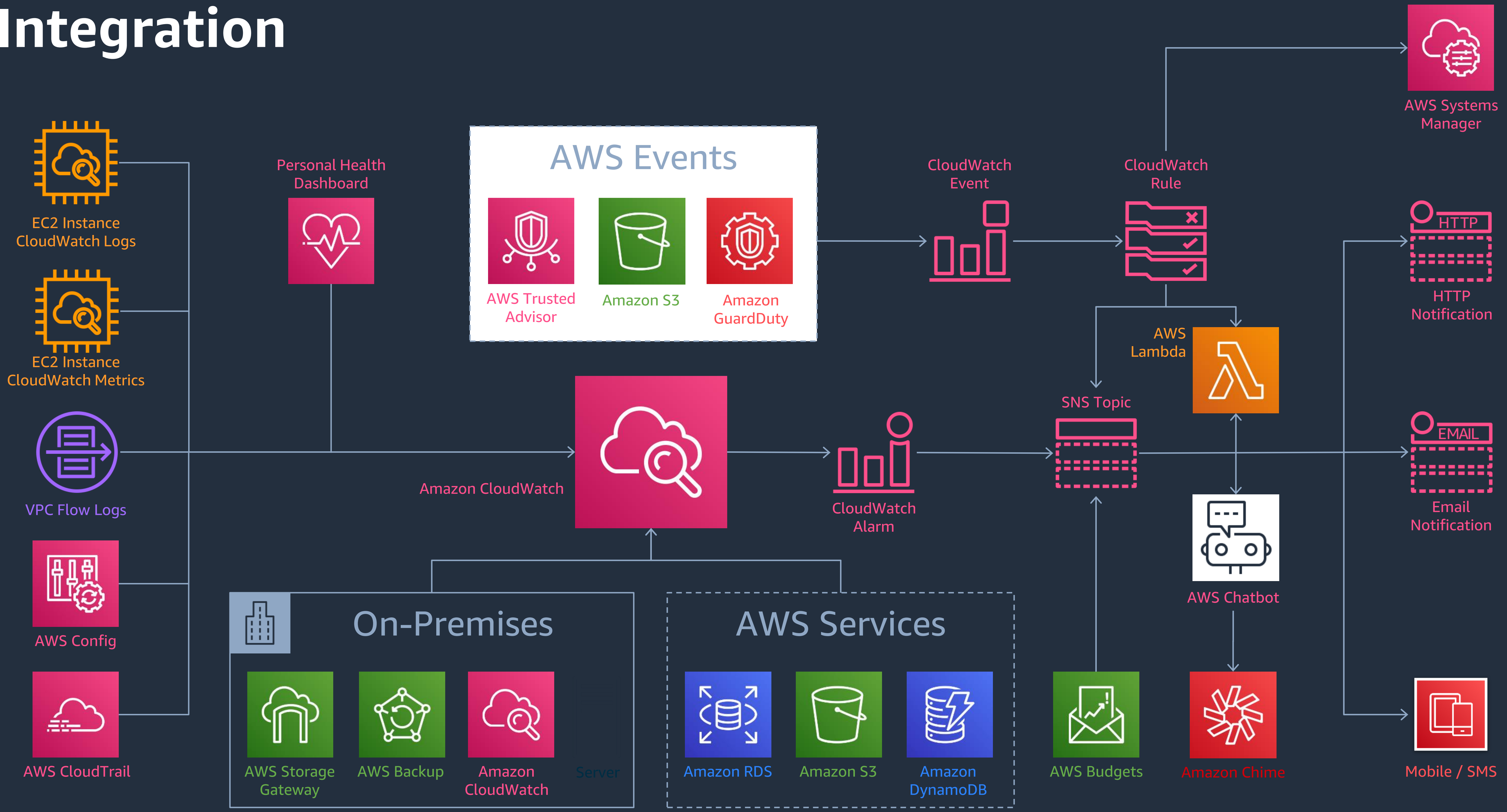
## Compliance

- AWS Artifact
- AWS Audit Manager

1

# CloudWatch

# Integration



# CloudWatch Metrics

## Built-in Metrics

Collecting metrics is time consuming. Amazon CloudWatch allows you to collect default metrics from more than 70 AWS services, such as:

- Amazon EC2
- Amazon DynamoDB
- Amazon S3
- Amazon ECS
- AWS Lambda
- Amazon API Gateway

No action is required on your part. For example, EC2 instances automatically publish CPU utilization, data transfer, and disk usage metrics to help you understand changes in state.

## Custom Metrics

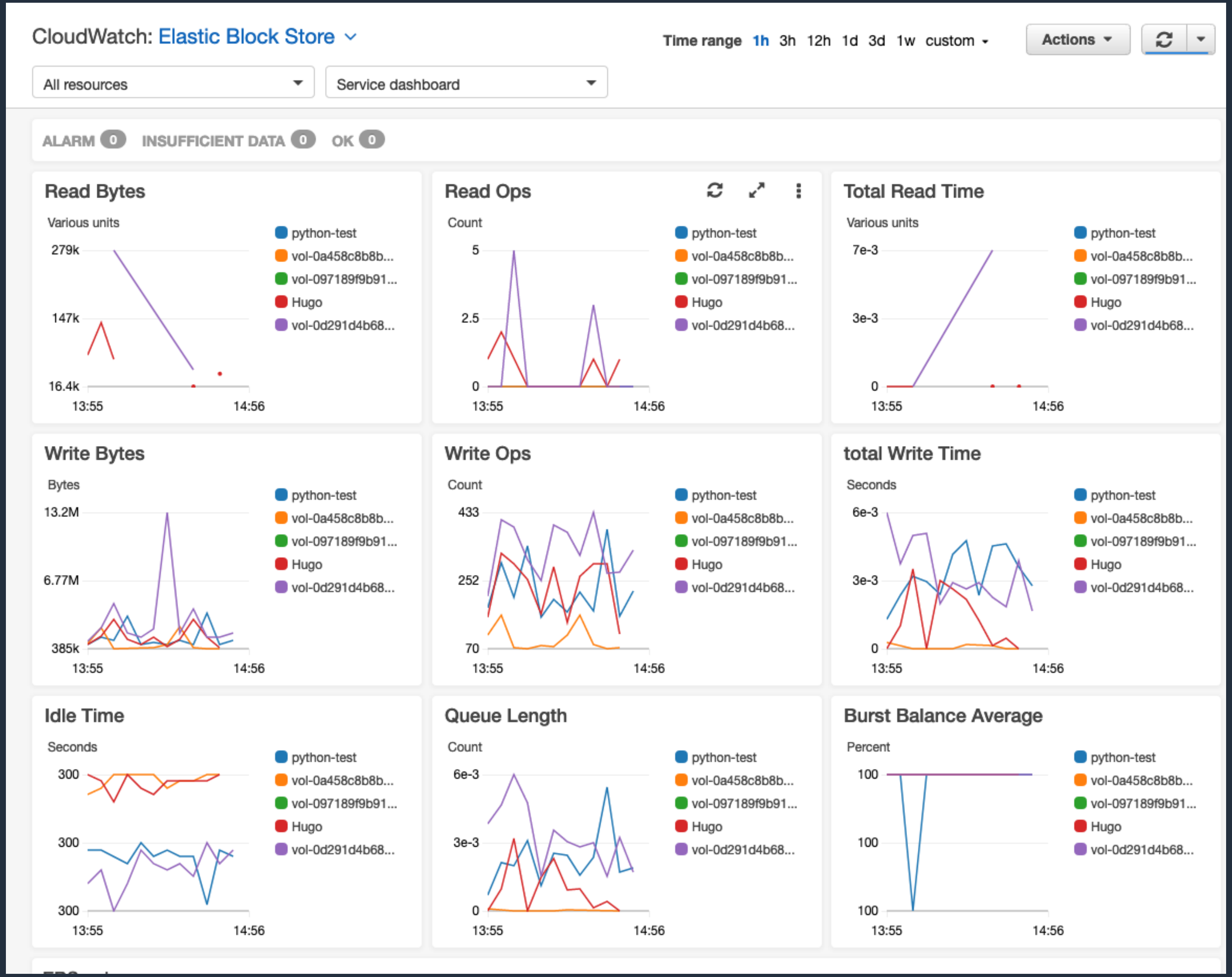
Collect custom metrics from your own applications to monitor operational performance, troubleshoot issues, and spot trends. User activity is an example of a custom metric you can collect and monitor over a period of time.

- Publish metrics using the AWS CLI or an API
- Standard resolution, with a one-minute granularity
- High resolution, with a granularity of one second
- Aggregate data before you publish to CloudWatch
- StatsD and collectd support via CloudWatch Agent

# Unified operational view with dashboards

Amazon CloudWatch dashboards enable you to create re-usable graphs and visualize your cloud resources and applications in a unified view.

- A single view for selected metrics and alarms
- Multiple AWS accounts and multiple Regions.
- An operational playbook
- A common view of critical resource and application measurements that can be shared



CloudWatch: Elastic Block Store

Time range 1h 3h 12h 1d 3d 1w custom

All resources

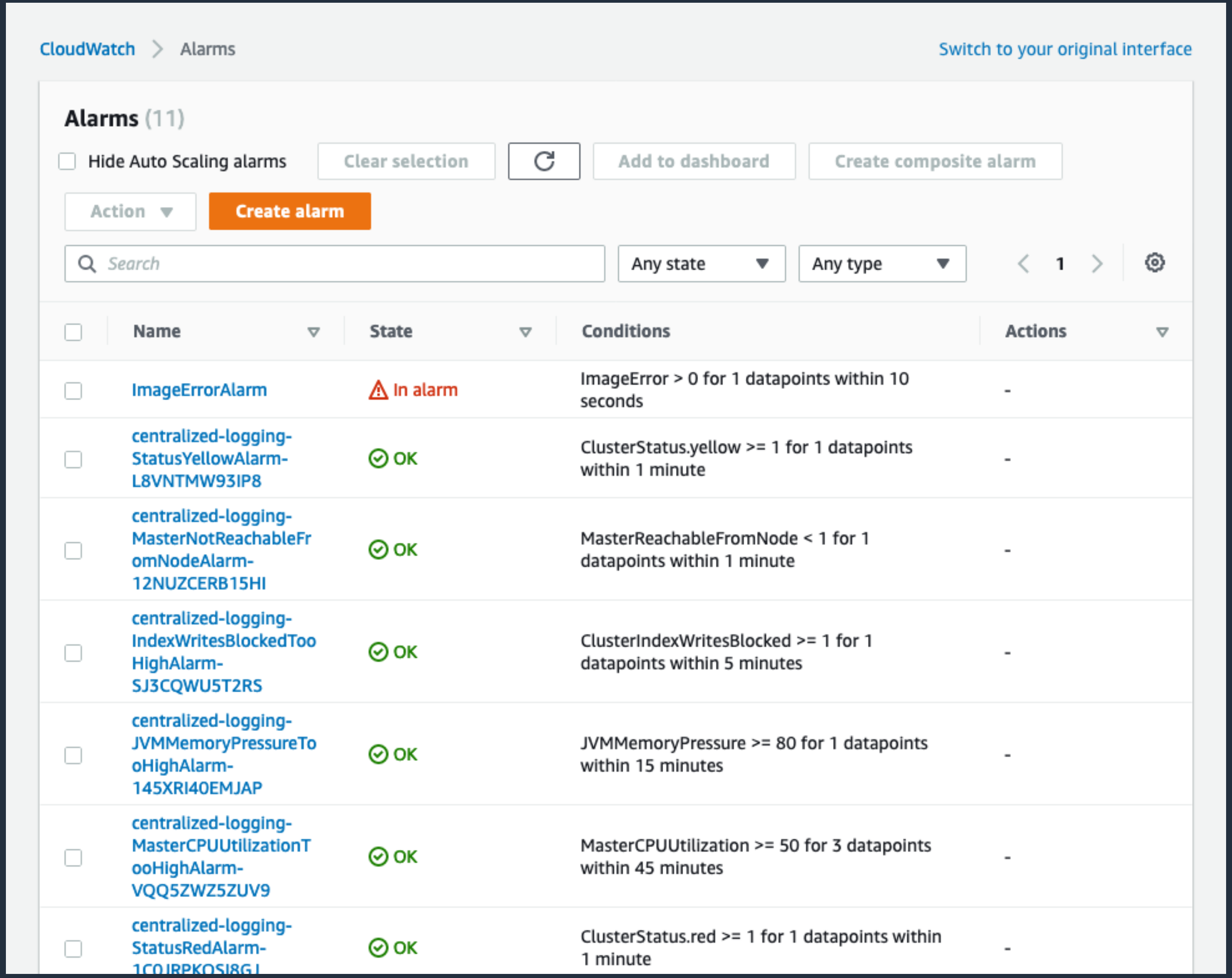
Service dashboard

ALARM 0 INSUFFICIENT DATA 0 OK 0

# High resolution 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



| □ | Name | State | Conditions | Actions |
|---|---|---|---|---|
| □ | ImageErrorAlarm | ⚠ In alarm | ImageError > 0 for 1 datapoints within 10 seconds | - |
| □ | centralized-logging-StatusYellowAlarm-L8VNTMW93IP8 | ✓ OK | ClusterStatus.yellow >= 1 for 1 datapoints within 1 minute | - |
| □ | centralized-logging-MasterNotReachableFromNodeAlarm-12NUZCERB15HI | ✓ OK | MasterReachableFromNode < 1 for 1 datapoints within 1 minute | - |
| □ | centralized-logging-IndexWritesBlockedTooHighAlarm-SJ3CQWU5T2RS | ✓ OK | ClusterIndexWritesBlocked >= 1 for 1 datapoints within 5 minutes | - |
| □ | centralized-logging-JVMMemoryPressureTooHighAlarm-145XRI40EMJAP | ✓ OK | JVMMemoryPressure >= 80 for 1 datapoints within 15 minutes | - |
| □ | centralized-logging-MasterCPUUtilizationTooHighAlarm-VQQ5ZWZ5ZUV9 | ✓ OK | MasterCPUUtilization >= 50 for 3 datapoints within 45 minutes | - |
| □ | centralized-logging-StatusRedAlarm-1COJRPKQSI8GJ | ✓ OK | ClusterStatus.red >= 1 for 1 datapoints within 1 minute | - |

# Automate response to changes

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

- Respond quickly
- Take corrective action

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

- Invoke a Lambda Function
- Notify an SNS Topic
- Create an Ops Item in Systems Manager

CloudWatch Alarms can send a notification to SNS, from there, you can trigger a Lambda function or push a message to Slack or Amazon Chime via AWS Chatbot. This allows you to do almost anything, including:

- Trigger a Systems Manager Automation
- Resize an instance
- Send a message to Chime or Slack
  - Respond with CLI commands
- Invoke disaster recovery
- Update security groups
- Automate deployments
- Instigate backups and snapshots
- Responding to security events

# Poll 1

Which of the services below can help you find underutilized EC2 instances? (Select TWO)

A) Amazon CloudWatch
B) Amazon Simple Notification Service (SNS)
C) AWS Trusted Advisor
D) Amazon CloudTrail

# Poll 2

Which of the following requires a custom Amazon CloudWatch metric to monitor?

A) Total number of HTTP requests made to an Amazon S3 bucket
B) Memory utilization on an Amazon EC2 instance
C) Disk operation activity on an Amazon EC2 instance
D) The number of connections that were not successfully established between the load balancer and the registered Amazon EC2 instances

2

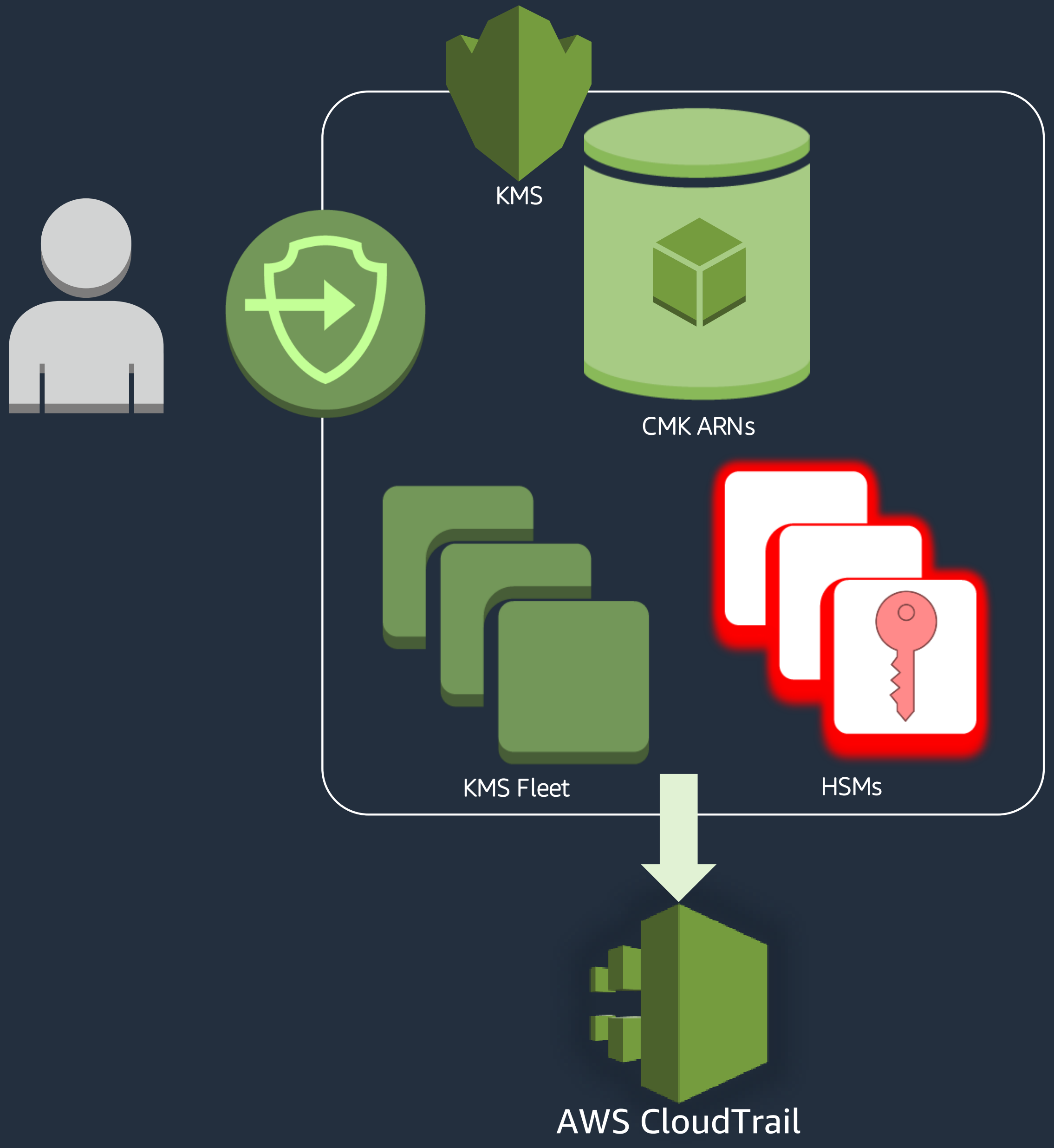
# KMS

# AWS KMS overview

Traditional **web service** with web APIs integrated with other Amazon Web Services (AWS) services

Backed by **hardware security modules (HSMs)**

Non-exportable keys called **customer master keys (CMKs)**



# Customer Master Keys and Data Keys

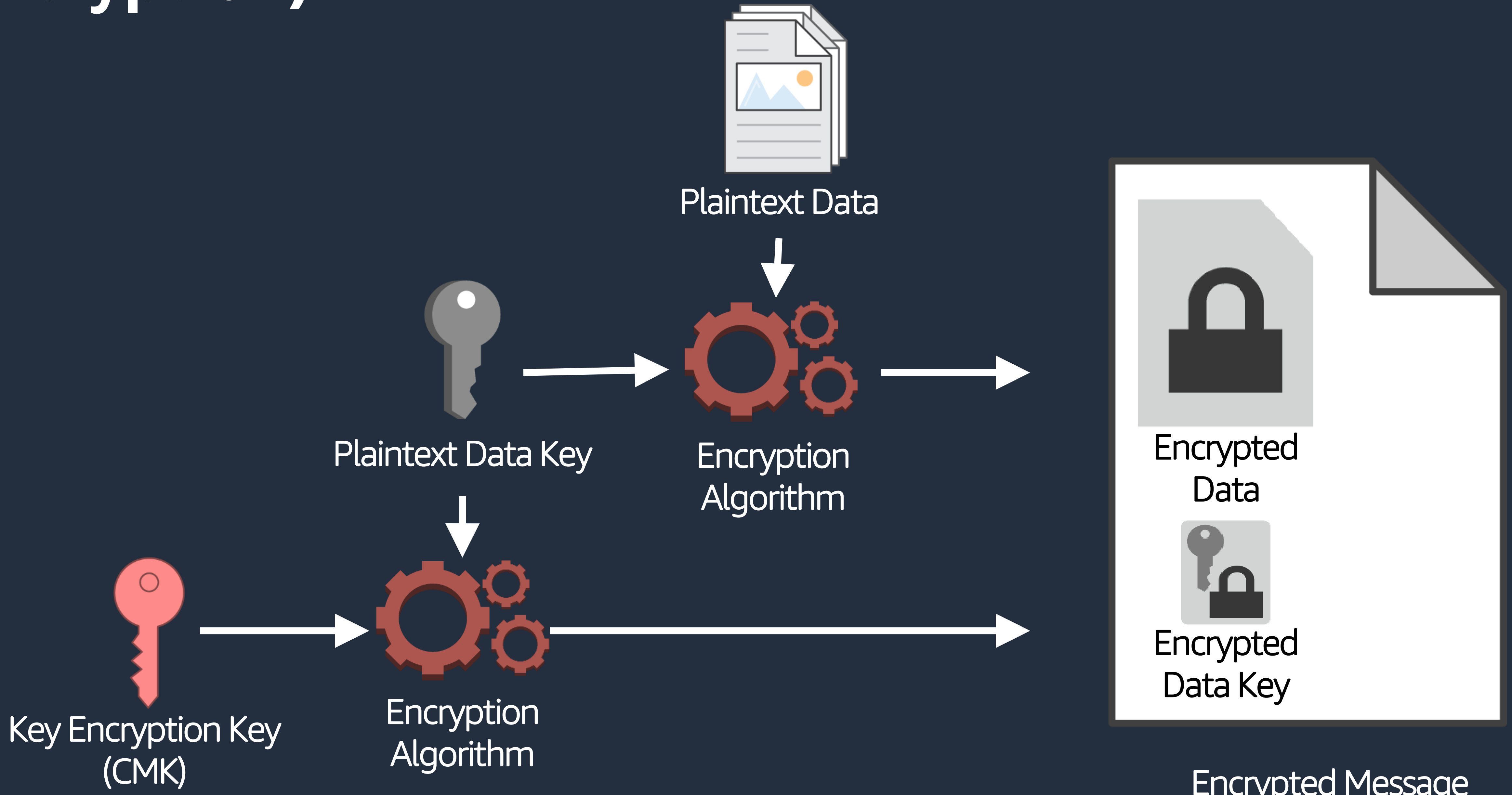
Customer Master Keys (CMKs)

- Represents the top of a key hierarchy
- Unique ARN
- Non-exportable
- Generated on HSM or imported by the customer
- Region specific, globally unique

Data Keys

- Used to encrypt your data
- Protected by CMKs
- Generated (or decrypted) by KMS

# Envelope Encryption (Encryption)



Encrypted Message

# Encryption Context

**Non-secret, plaintext** additional information

Should be **relevant to the data**

Included verbatim in **AWS CloudTrail logs**

Can be used as **conditions in IAM policies, Key Policies, and Grants**

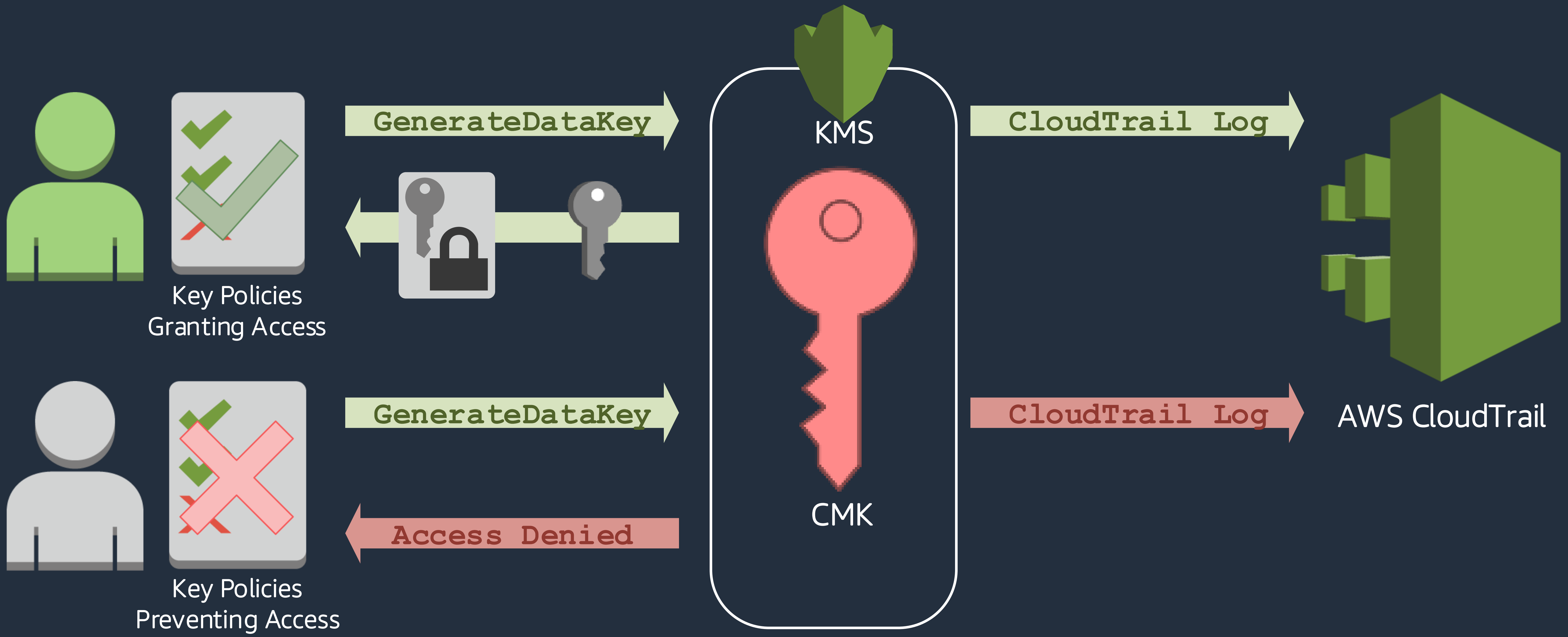
Examples:

- Document type, security classification, customer ID, datestamps, order IDs…
- Balance plaintext disclosure with audit/access control detail

```
{
  "awsRegion": "us-east-2",
  "eventName": "Decrypt",
  "eventSource": "kms.amazonaws.com",
  "eventTime": "2017-09-15T19:35:54Z",
  "requestParameters": {
    "encryptionContext": {
      "TenantID": ”123AID",
      "OrderDate": "2018-09-01",
      "OrderID": "123-4567890-011",
      "Type": "Invoice"
    }
  },
  // ...
}
```

Encryption Context

# AWS KMS authorization



3

# Cloud HSM

# AWS CloudHSM Delivers

Single-tenant FIPS 140-2 Level 3 validated HSMs in your VPC

Zero config high-availability and one-click cluster expansion

Audit logs and HSM metrics to Amazon CloudWatch

Durability of backups

4

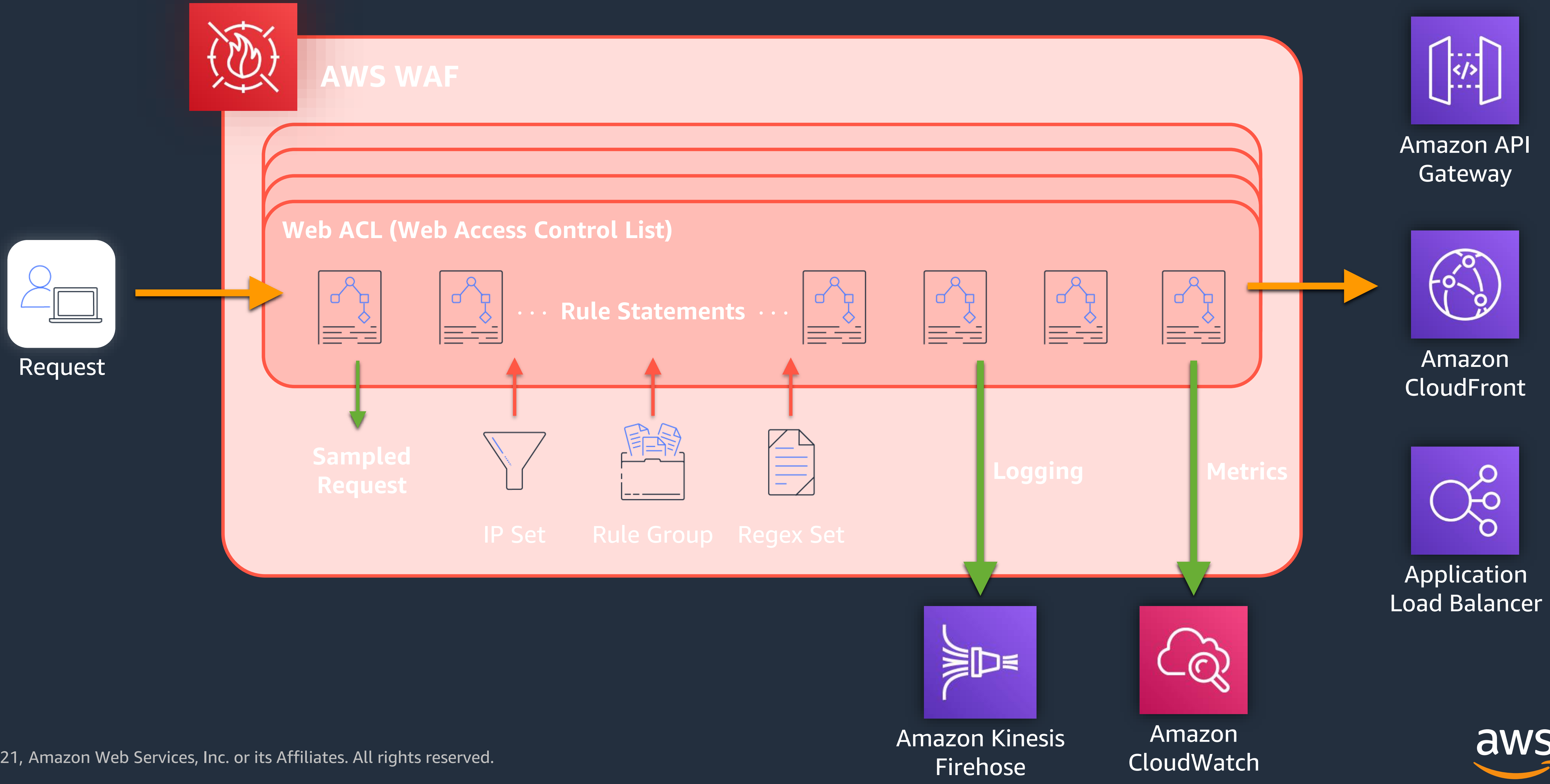
# Web Application Firewall

# What is AWS WAF?

*Highly configurable and scalable cloud-native web application firewall – giving you the first line of defense to incoming threats.*

**AWS WAF**

# Key Terminology



# Ready to use rules for AWS WAF

**Built-in rules**

- SQL injection and cross-site scripting (SQLi/XSS) attack detection

- AWS Managed Rules for AWS WAF

**CloudFormation templates**

- OWASP Top 10 Web Application Vulnerabilities
- AWS Security Automation

**Managed rules from AWS Marketplace**

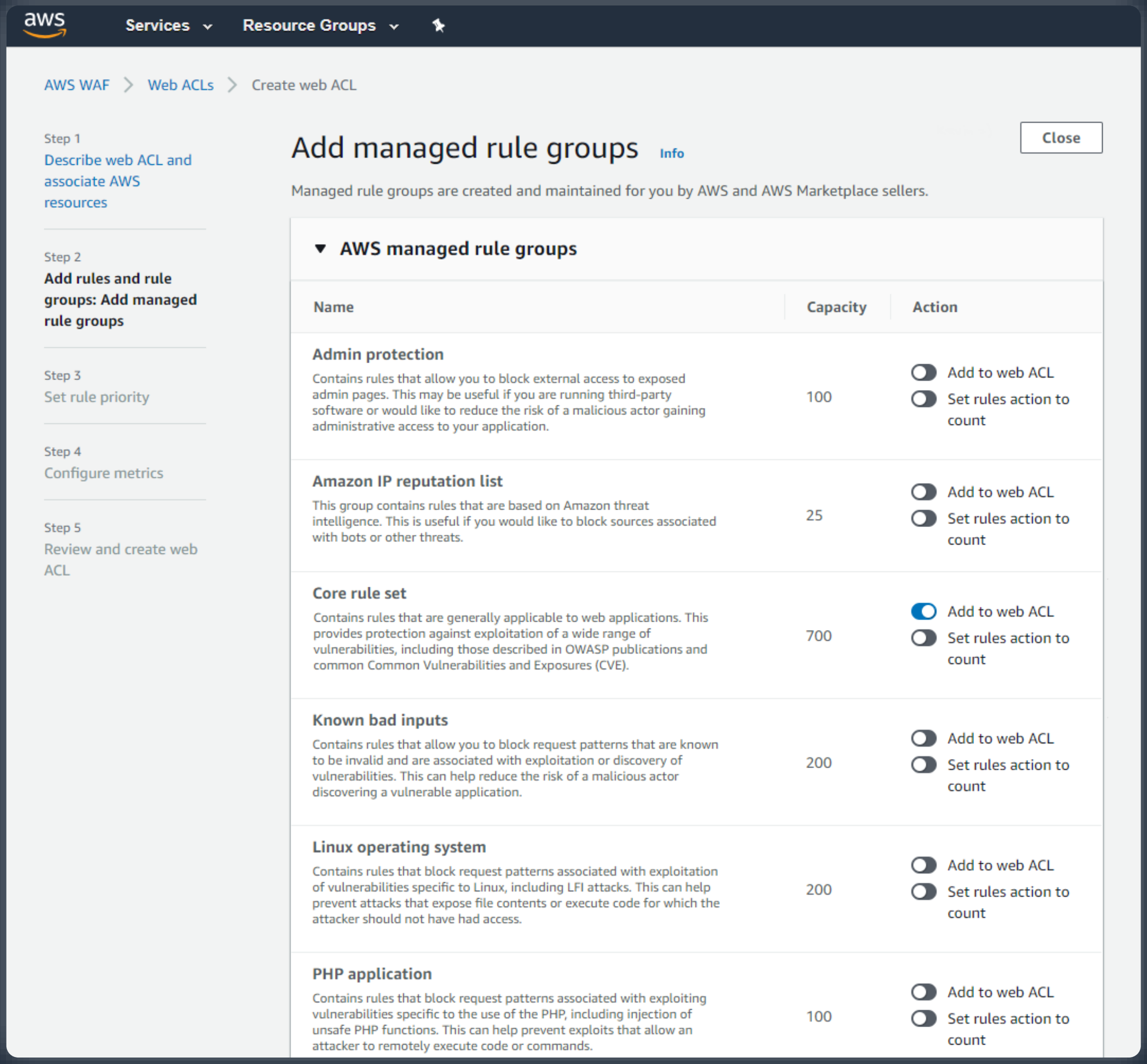
- Rules provided by security vendors that covers wide-range of web applications

# AWS Managed Rules for AWS WAF

**Set of pre-configured rules that you can deploy on your application**

- Covers common attack vectors and threats
- Curated and maintained by threat research team
- Influenced by OWASP Top 10 Web Application Security Risks

**Available to all customers at no extra charge**



Step 1
Describe web ACL and associate AWS resources

Step 2
**Add rules and rule groups: Add managed rule groups**

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

## Add managed rule groups

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers.

**▼ AWS managed rule groups**

| Name | Capacity | Action |
|---|---|---|
| **Admin protection**<br>Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. | 100 | ○ Add to web ACL<br>○ Set rules action to count |
| **Amazon IP reputation list**<br>This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats. | 25 | ○ Add to web ACL<br>○ Set rules action to count |
| **Core rule set**<br>Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications and common Common Vulnerabilities and Exposures (CVE). | 700 | ● Add to web ACL<br>○ Set rules action to count |
| **Known bad inputs**<br>Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. | 200 | ○ Add to web ACL<br>○ Set rules action to count |
| **Linux operating system**<br>Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. | 200 | ○ Add to web ACL<br>○ Set rules action to count |
| **PHP application**<br>Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands. | 100 | ○ Add to web ACL<br>○ Set rules action to count |

5

# Shield

# AWS Shield

## *A Managed DDoS Protection Service*

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.

**AWS Shield**

# AWS Shield **Standard**

| | | | |
|---|---|---|---|
| DDoS Expertise | Built-in DDoS Protection for Everyone | Enhanced Protection | 24x7 access to DDoS Response Team (DRT) |
| Visibility & Compliance | CloudWatch Metrics | Attack Diagnostics | Global threat environment dashboard |
| Economic Benefits | AWS WAF at no additional cost<br>*for protected resources* | AWS Firewall Manager at no additional cost | Cost Protection for scaling |

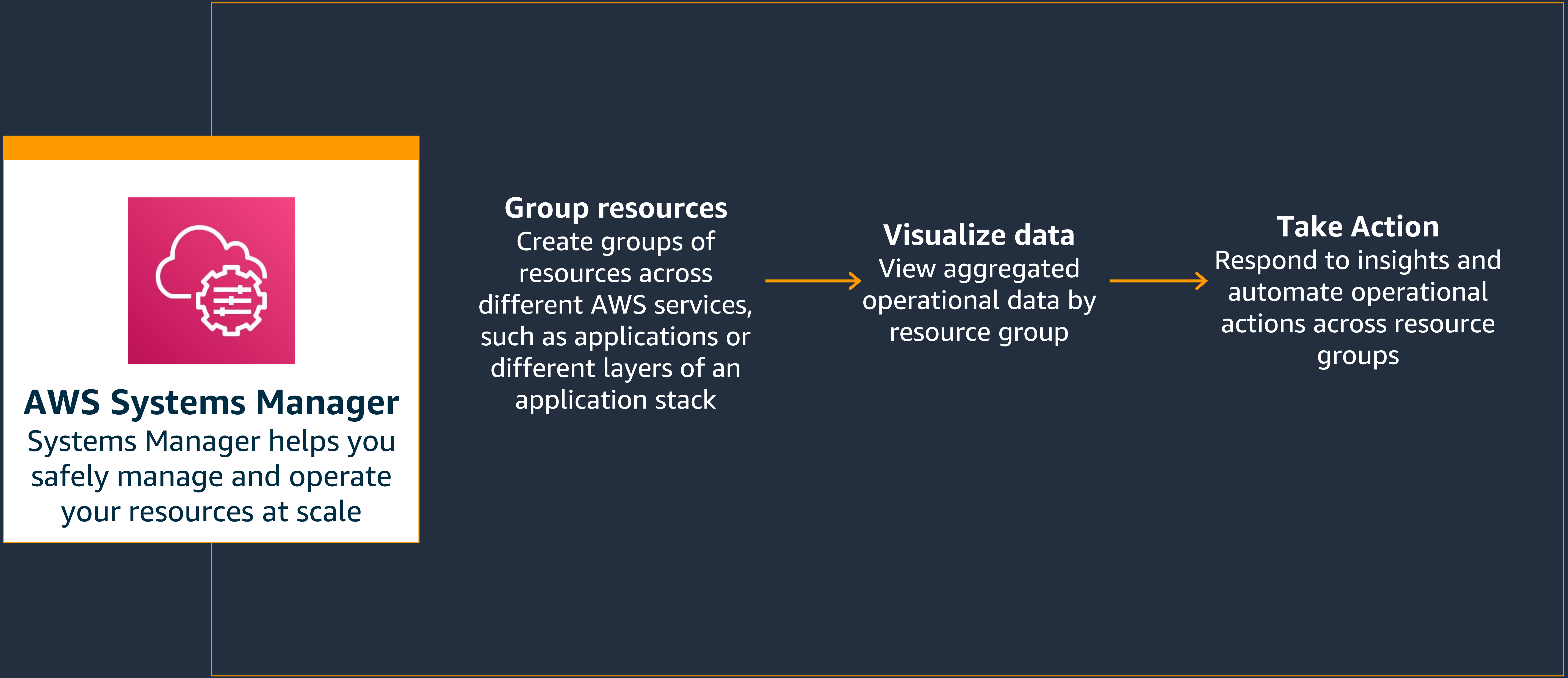
# AWS Shield **Advanced**

| | | | |
|---|---|---|---|
| DDoS Expertise | Built-in DDoS Protection for Everyone | Enhanced Protection | 24x7 access to DDoS Response Team (DRT) |
| Visibility & Compliance | CloudWatch Metrics | Attack Diagnostics | Global threat environment dashboard |
| Economic Benefits | AWS WAF at no additional cost<br>*for protected resources* | AWS Firewall Manager<br>at no additional cost | Cost Protection for scaling |

6

# Systems Manager – Parameter Store

# AWS Systems Manager



**AWS Systems Manager**

Systems Manager helps you safely manage and operate your resources at scale

**Group resources**

Create groups of resources across different AWS services, such as applications or different layers of an application stack

→

**Visualize data**

View aggregated operational data by resource group

→

**Take Action**

Respond to insights and automate operational actions across resource groups

# AWS Systems Manager Parameter Store

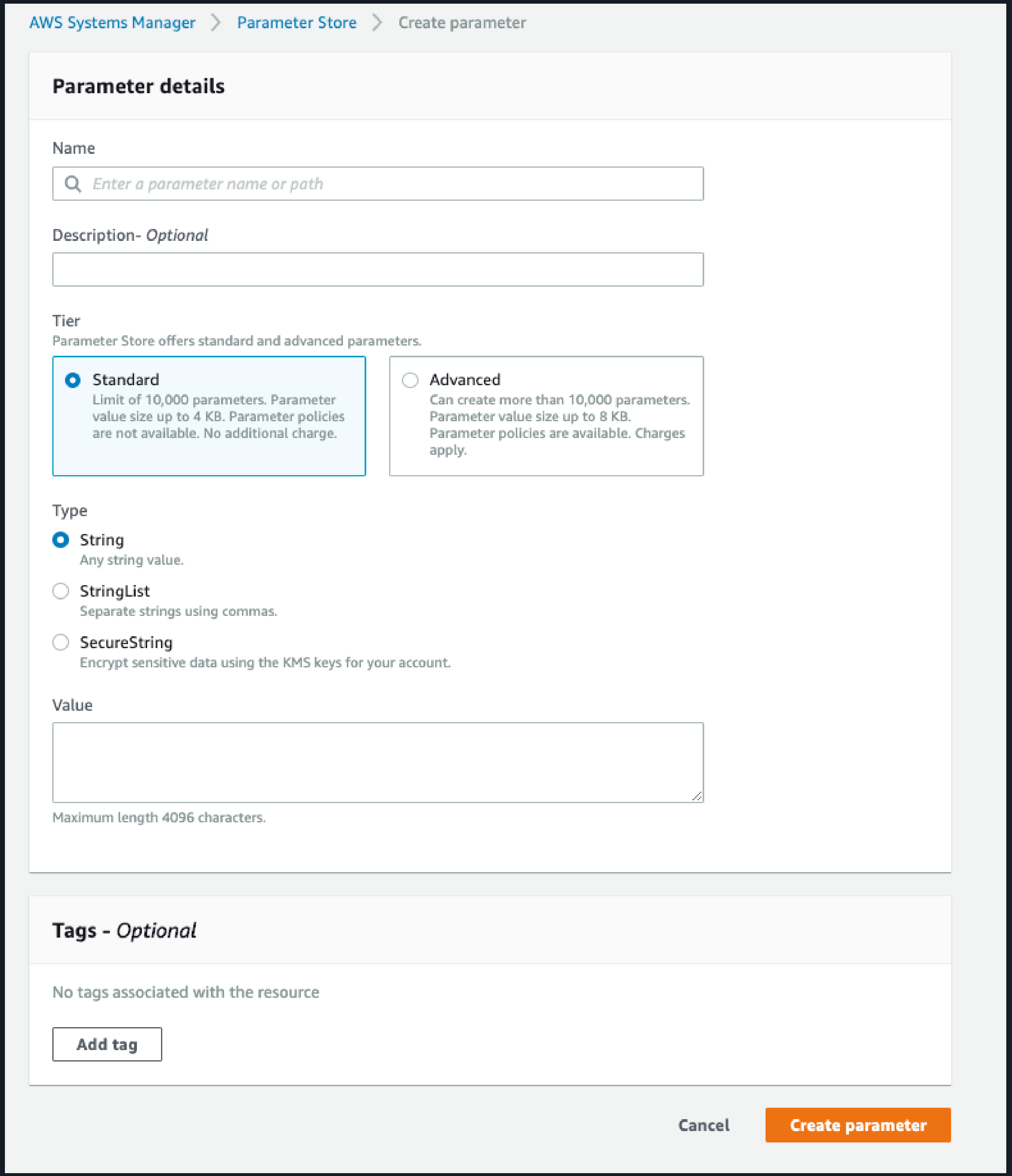
- Secure, scalable, hosted secrets management service
- Improves security posture by separating your data from your code
- Store configuration data and secure strings in hierarchies and track versions
- Control and audit access at granular levels
- Configure change notifications and trigger automated actions for both parameters and parameter policies
- Tag parameters individually, and then secure access from different levels, including operational, parameter, Amazon EC2 tag, and path levels

# Parameter

- Configuration data
  - DB connection string
  - Password
  - License key

- Types
  - String
  - String List
  - Secure String

*ssm:parameter-name*



AWS Systems Manager > Parameter Store > Create parameter

**Parameter details**

Name

*Enter a parameter name or path*

Description- *Optional*

Tier

Parameter Store offers standard and advanced parameters.

● Standard
Limit of 10,000 parameters. Parameter value size up to 4 KB. Parameter policies are not available. No additional charge.

○ Advanced
Can create more than 10,000 parameters. Parameter value size up to 8 KB. Parameter policies are available. Charges apply.

Type

● String
Any string value.

○ StringList
Separate strings using commas.

○ SecureString
Encrypt sensitive data using the KMS keys for your account.

Value

Maximum length 4096 characters.

**Tags - *Optional***

No tags associated with the resource

7

# Secrets Manager

# AWS Secrets Manager

## Lifecycle management for secrets such as database credentials and API keys.

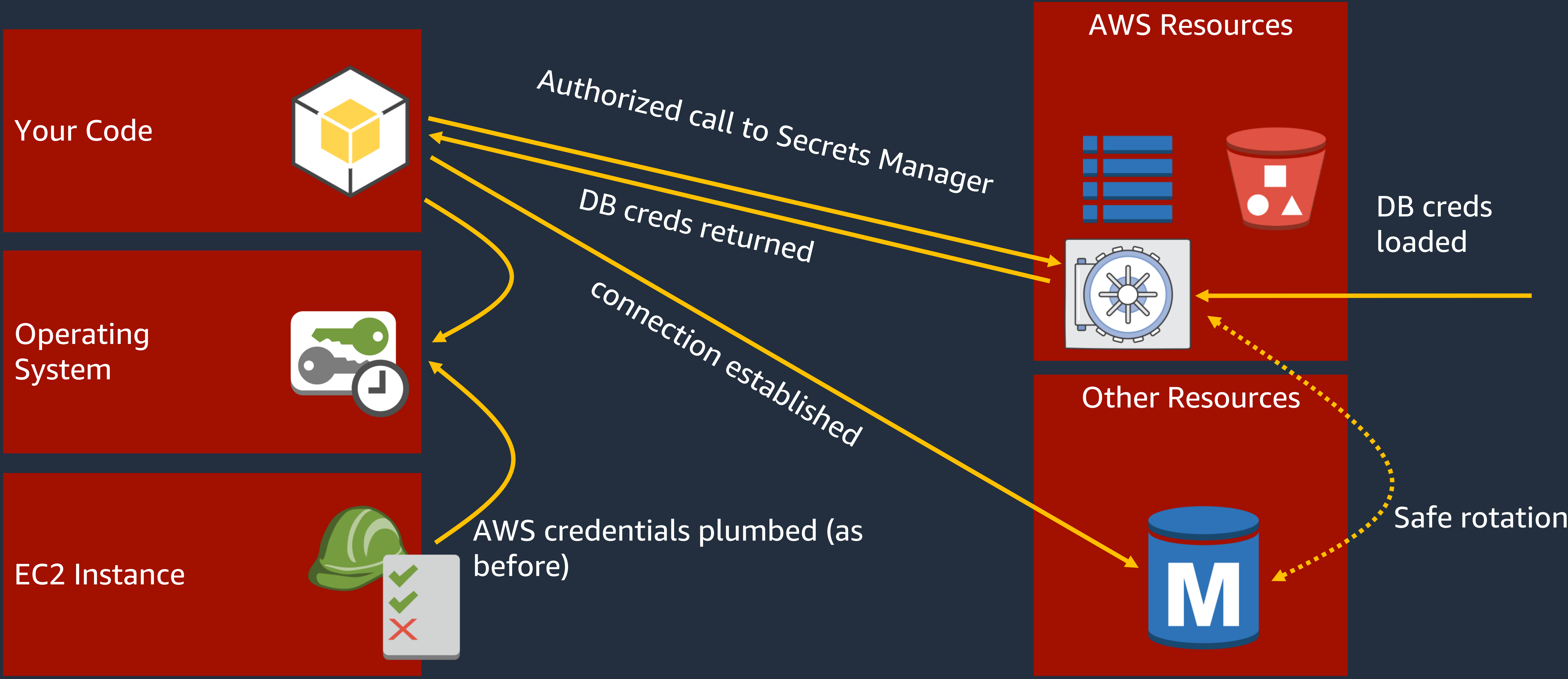
Rotate Secrets Safely

Manage access with fine-grained policies

Secure and audit secrets centrally

Pay as you go

# Retrieve Secret



Combo provides your apps a reliable, secure, auto-rotating solution for ALL credentials

# Comparing AWS Systems Manager Parameter Store

## AWS Systems Manager Parameter Store

- Secure storage for configuration data, which can include secrets.
- Reference values using the unique name specified during creation.
- Use parameters in scripts for configuration and automation.

## AWS Secrets Manager

- A service to manage the lifecycle for secrets in your organization.
- Helps you meet security and compliance requirements by rotating secrets automatically.
- Built-in integrations for Amazon RDS that can rotate database credentials on your behalf.
- Extensible via Lambda.

8

# CloudTrail

# AWS CloudTrail provides audit logs for AWS

- Capture and log user and resource activity across your AWS infrastructure and resources for governance and auditing.
- Enable compliance, operational and risk auditing.

## Capture

Record activity as CloudTrail events

## Store

Retain events logs in secure S3 bucket

## Act

Trigger actions when important events are detected

## Review

Analyze recent events and logs with Amazon Athena or CloudWatch Logs Insights

# Components of CloudTrail

| | |
|---|---|
| Audit Trails | • Configure recording events across all your AWS accounts and regions<br>• Centralize logging across your AWS Organization<br>• Create additional trails as needed for operations, support, and security needs<br>• Configure trail to select relevant events for delivery by choosing management events (all, read, write, exclude KMS), and/or data events (all or specific S3 buckets and Lambda functions) |
| Event Delivery | • Deliver events to Amazon S3, Amazon CloudWatch Logs or Amazon EventBridge<br>• Get SNS notifications when events are delivered<br>• Enable encryption using SSE or KMS<br>• Cryptographically validate whether log file was modified, deleted or unchanged |
| Search and Analytics | • Lookup recent (90-day) event history on Console or API<br>• Leverage integration with CloudWatch Logs, or Amazon Athena to query events<br>• Import logs to Amazon Elasticsearch Service, or AWS Partner Solutions for deeper analysis |
| CloudTrail Insights | • Identify unusual operational activity such as spikes in resource provisioning, or gaps in periodic maintenance activity<br>• Enable automatic analysis of events to establish baseline for normal behavior and detect anomalous patterns.<br>• Remediate operational issues using actionable information in Insights events. |

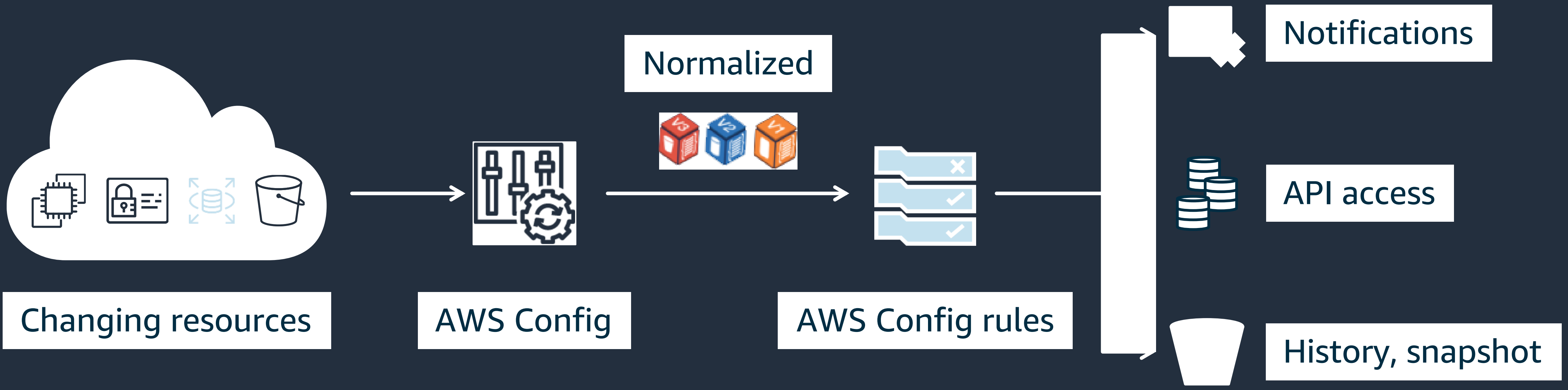
9

# Config

# AWS Config

- Native, agentless AWS capability to discover resources in your account
- Tracks configuration changes and maintains a history (up to 7 years)
- Evaluates configuration changes against compliance policies (using AWS Config rules)
- Provides aggregated view of resource configuration and compliance status across accounts and regions
- Integrates with your own CMDBs (such as ServiceNow)

**AWS Config = Continuous configuration auditor**



# AWS Config rules

Analyze configuration changes

90+ pre-built rules provided by AWS

Custom rules using AWS Lambda

GitHub repo: Community sourced rules

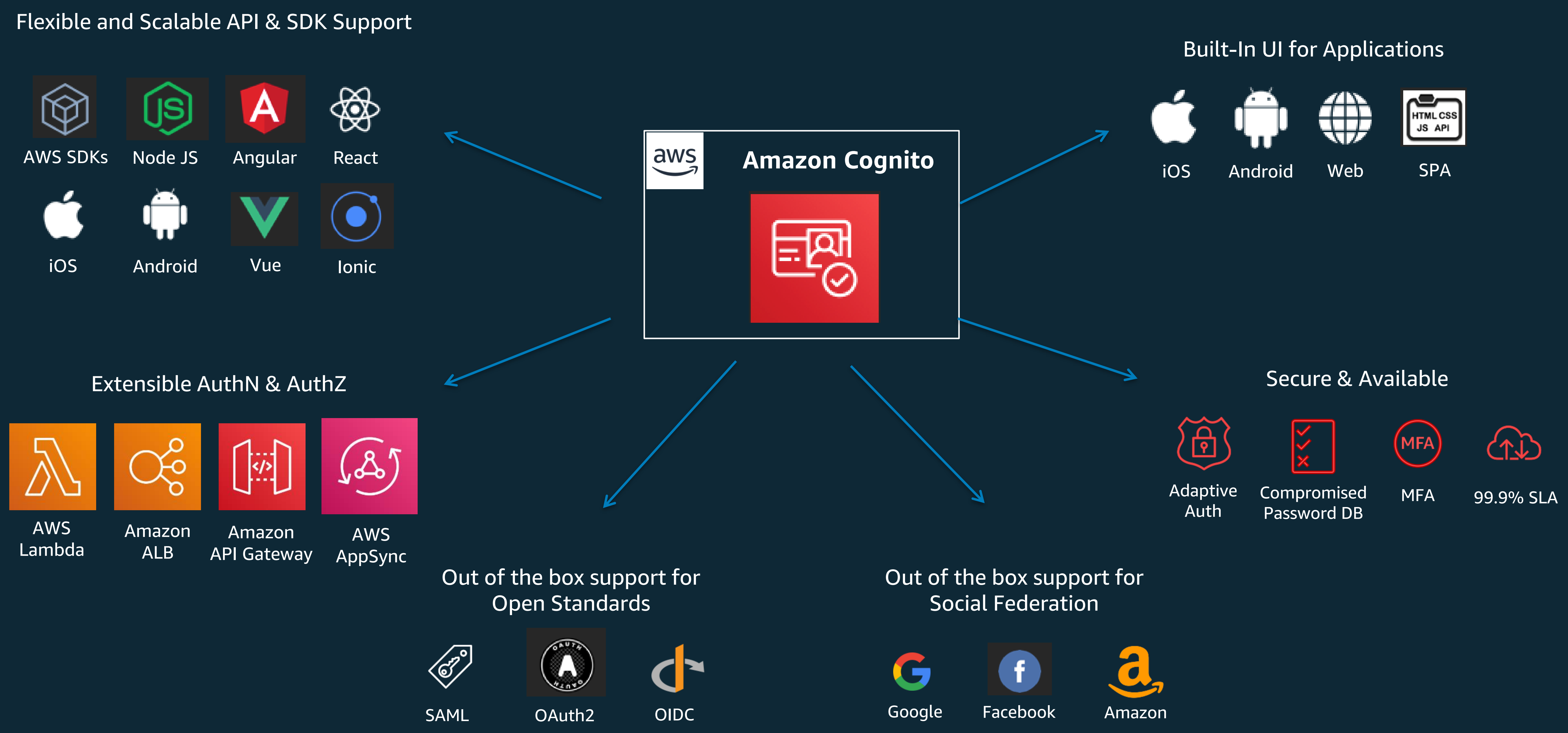
Aggregate compliance into a central account

Compliance history

# 10

# Cognito

# Cognito: Flexible and Fully Managed Application Identity



Amazon Cognito

Flexible and Scalable API & SDK Support

AWS SDKs, Node JS, Angular, React, iOS, Android, Vue, Ionic

Built-In UI for Applications

iOS, Android, Web, SPA

Extensible AuthN & AuthZ

AWS Lambda, Amazon ALB, Amazon API Gateway, AWS AppSync

Secure & Available

Adaptive Auth, Compromised Password DB, MFA, 99.9% SLA

Out of the box support for Open Standards

SAML, OAuth2, OIDC

Out of the box support for Social Federation

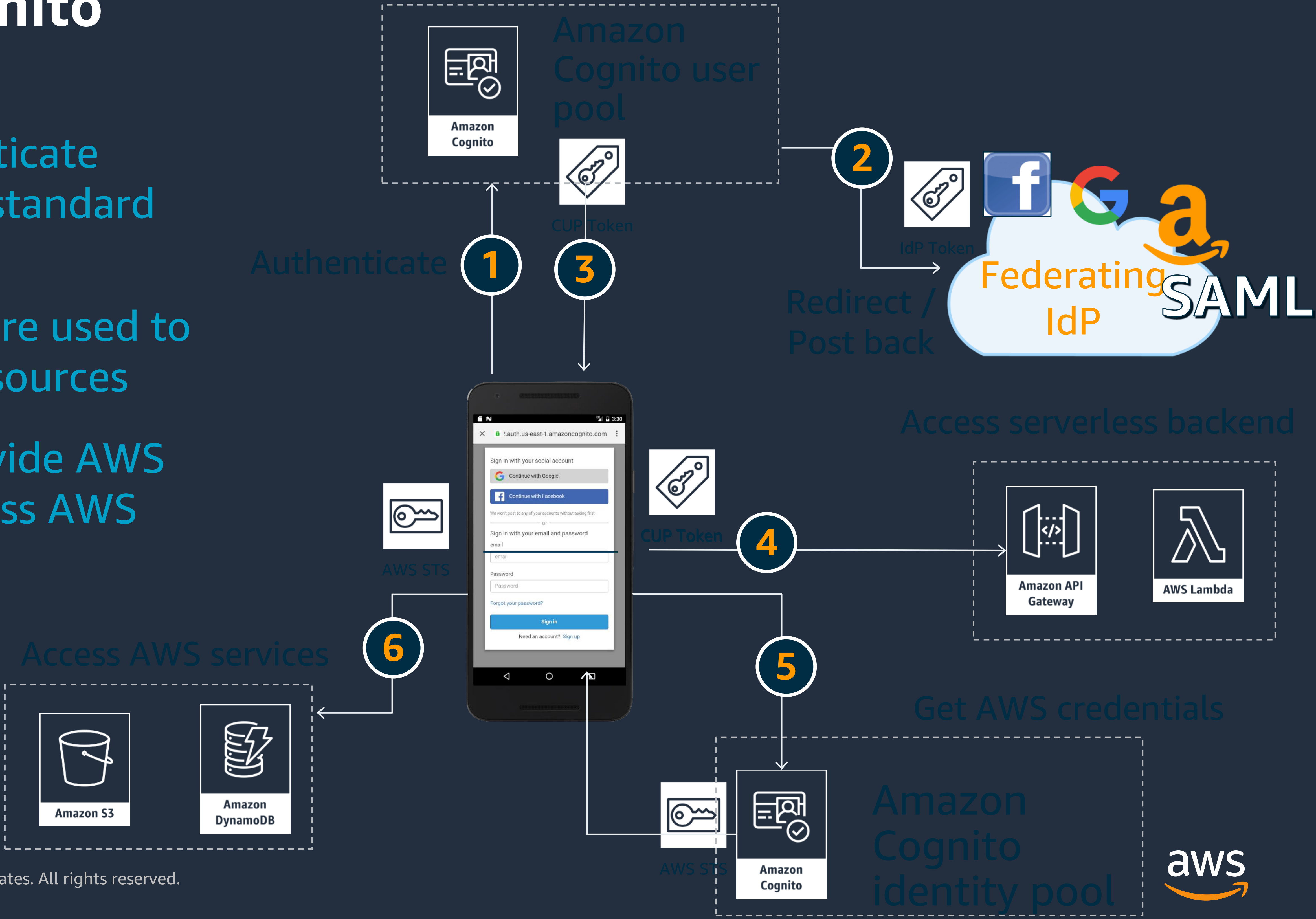
Google, Facebook, Amazon

# Amazon Cognito

User pools authenticate users and returns standard tokens

User pool tokens are used to access backend resources

Identity pools provide AWS credentials to access AWS services



Sign In with your social account

We won't post to any of your accounts without asking first

Sign in with your email and password

Need an account? Sign up

# Other Security Services

### Guard Duty

A threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads

### Amazon Inspector

An automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices

### Security Hub

Security and compliance center for AWS customers and is designed as the first stop where AWS- focused security and compliance professionals will go each day to understand their security and compliance state. Listen to your customers.

### AWS Firewall Manager

Security management service which allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization. … Finally, with AWS Firewall Manager, you can enable security groups for your Amazon EC2 and ENI resource types in Amazon VPCs.

# 11

# Practice Questions

# Poll 3

A company's security team requires that all data stored in the cloud be encrypted at rest at all times using encryption keys stored on-premises. Which encryption options meet these requirements? (Select TWO.)

A) Use Server-Side Encryption with Amazon S3 Managed Keys (SSE-S3).
B) Use Server-Side Encryption with AWS KMS Managed Keys (SSE-KMS).
C) Use Server-Side Encryption with Customer Provided Keys (SSE-C).
D) Use client-side encryption to provide at-rest encryption.
E) Use an AWS Lambda function triggered by Amazon S3 events to encrypt the data using the customer's keys

# Poll 4

You are responsible for deploying a PCI compliant, critical application on AWS. There is a need to monitor web application logs to identify any malicious activity. Which services meet these requirements? (Select THREE.)

A) Amazon CloudWatch Logs
B) Amazon VPC Flow Logs
C) Amazon Trusted Advisor
D) Amazon CloudTrail

# Poll 5

You plan to manage API keys in AWS Secrets Manager. The API keys need to be automatically rotated, per company policy. Applications get the latest version of the API credentials. How would you implement rotation of API keys?

A) Use AWS Systems Manager - Parameter Store instead, as Secrets Manager does not support it
B) Add multiple keys in Secrets Manager, and rotate them every year
C) Define and implement key rotation with an AWS Lambda function
D) Modify application to select a different key stored in Secrets Manager every 6 months

# Additional Reference Links

- Amazon CloudWatch FAQs

https://aws.amazon.com/cloudwatch/faqs/

- Amazon KMS FAQs

https://aws.amazon.com/kms/faqs/

- Secrets Manager versus Parameter Store

https://acloudguru.com/blog/engineering/an-inside-look-at-aws-secrets-manager-vs-parameter-store

# Additional Reference Links

- How AWS Services use KMS

https://docs.aws.amazon.com/kms/latest/developerguide/service-integration.html

- Amazon CloudTrail versus CloudWatch

https://medium.com/awesome-cloud/aws-difference-between-cloudwatch-and-cloudtrail-16a486f8bc95

- AWS Shield FAQs

https://aws.amazon.com/shield/faqs/

# THANK YOU!