# Fundamentals of AWS Security

Esteban Hernandez, Specialist SA for Security &
Compliance , EMEA

30/04/2019

# Strengthen your security posture

Inherit global security and compliance controls

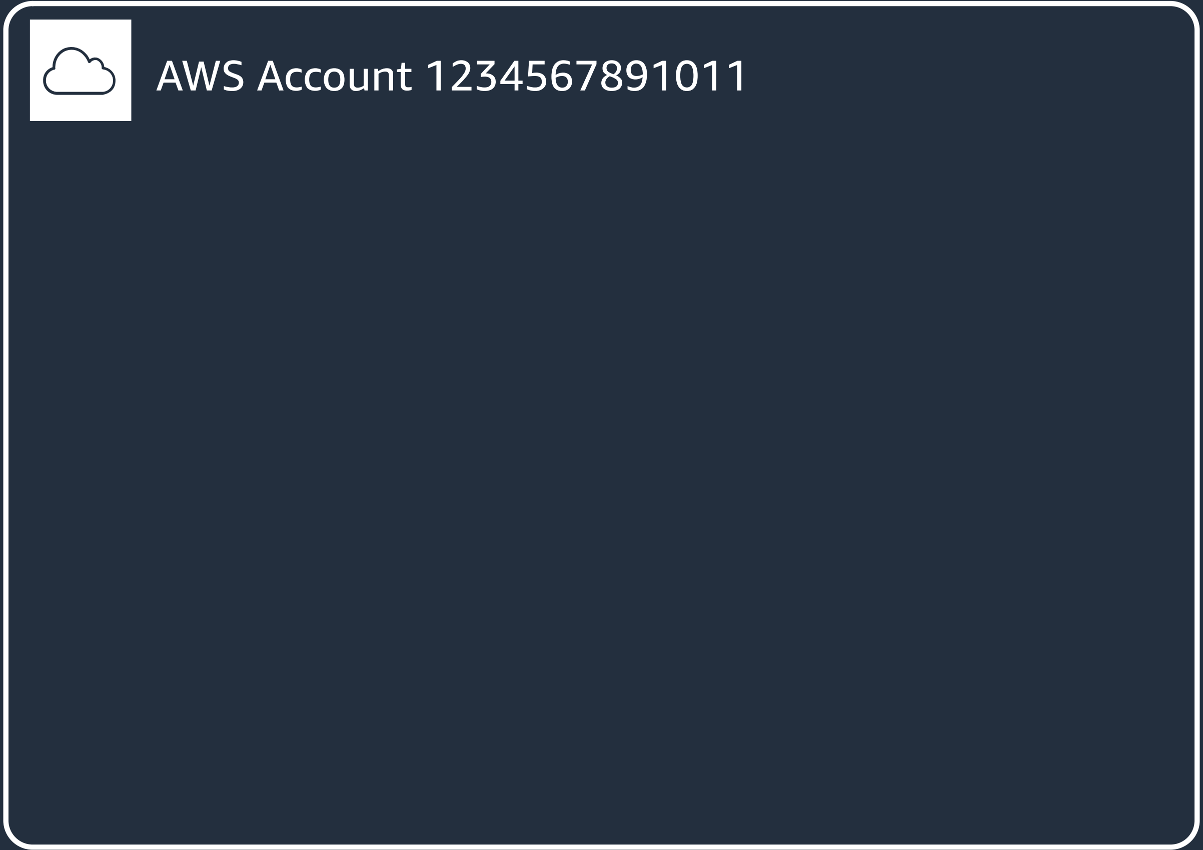
Scale with superior visibility and control

Highest standards for privacy and data security

Automate with deeply integrated security services

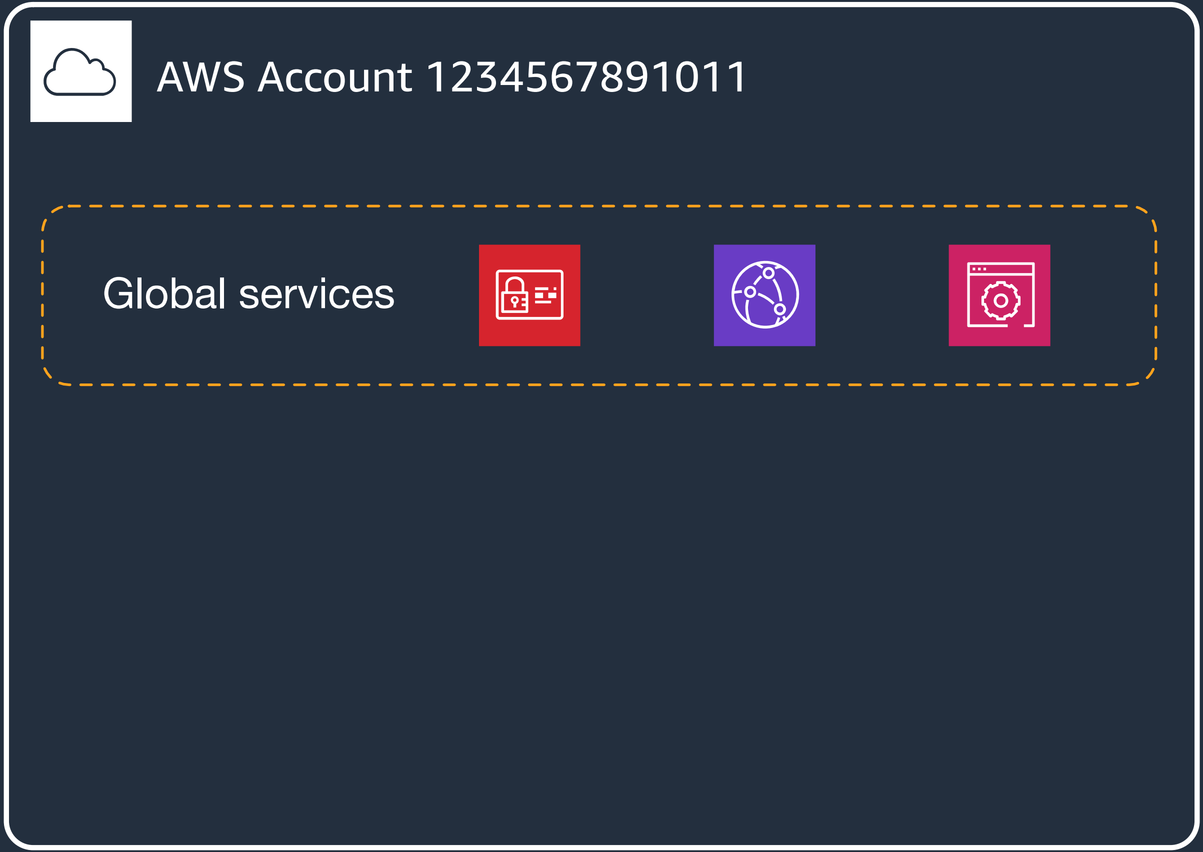
Largest network of security partners and solutions

# You have opened an AWS account, now what?



AWS Account 1234567891011

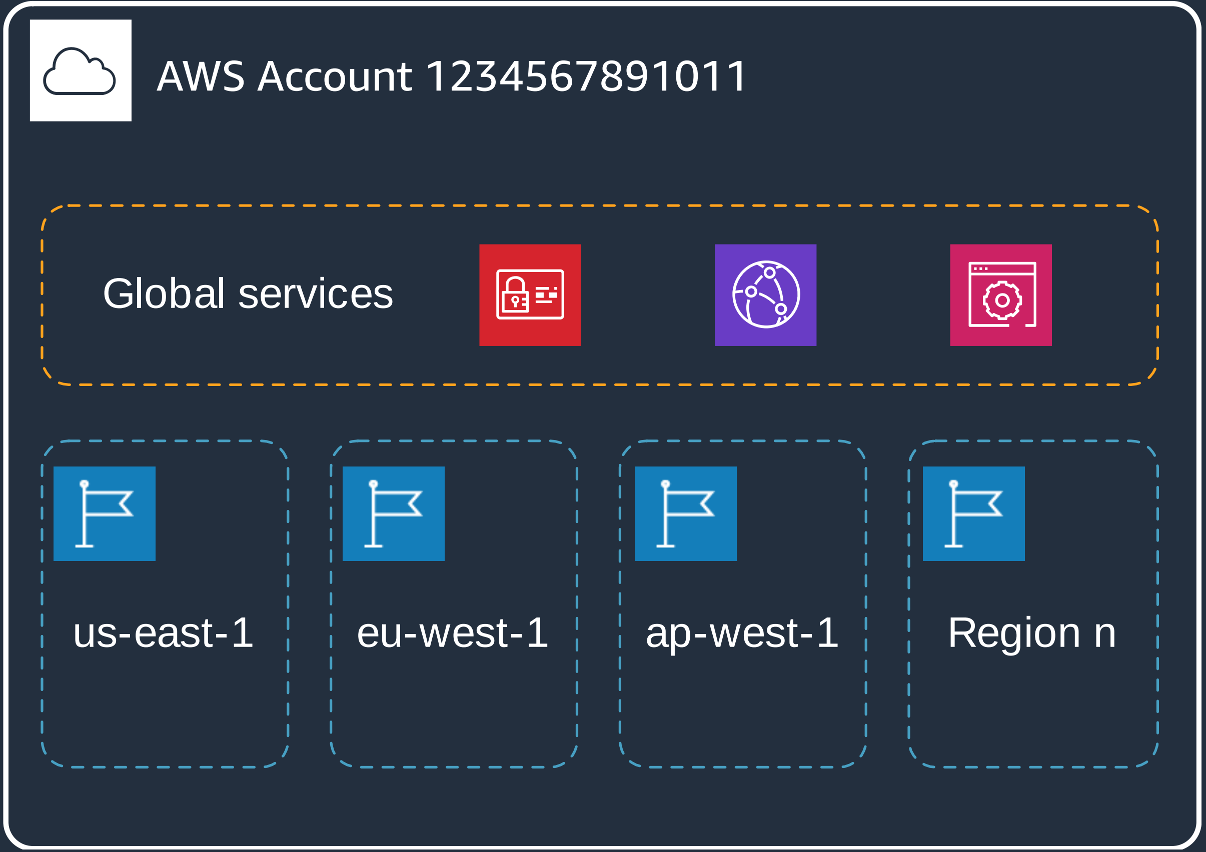
# Anatomy of an AWS account



AWS Account 1234567891011

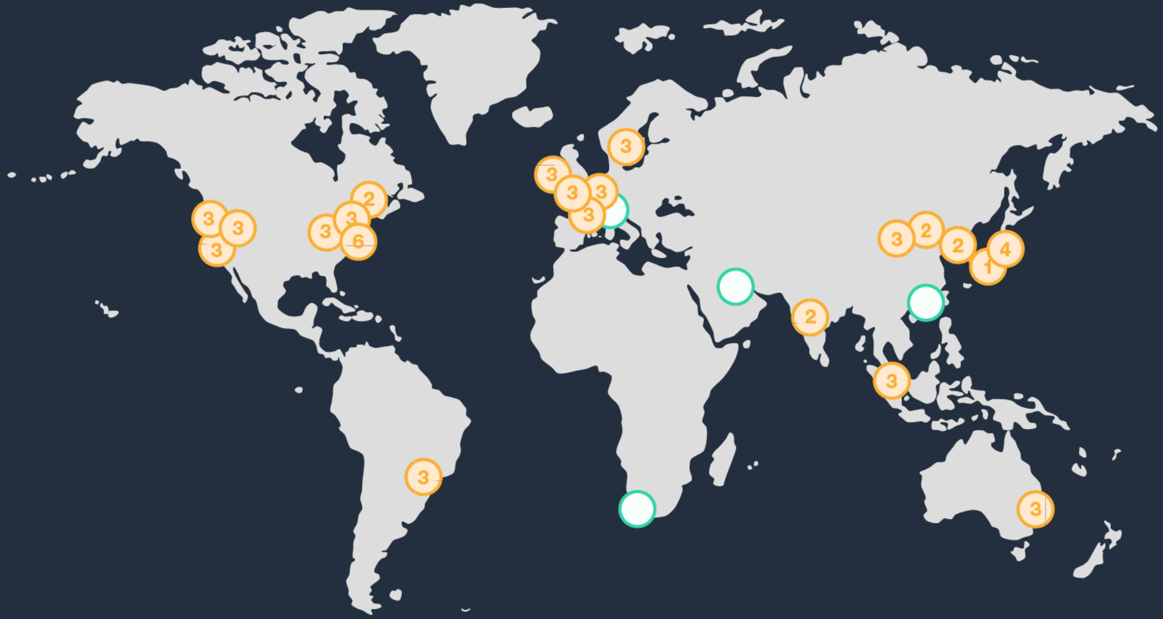
Global services

# Anatomy of an AWS account



# AWS Global Infrastructure

**20** Regions – **60** Availability Zones – **160** Points of presence



## Regions and Availability Zones

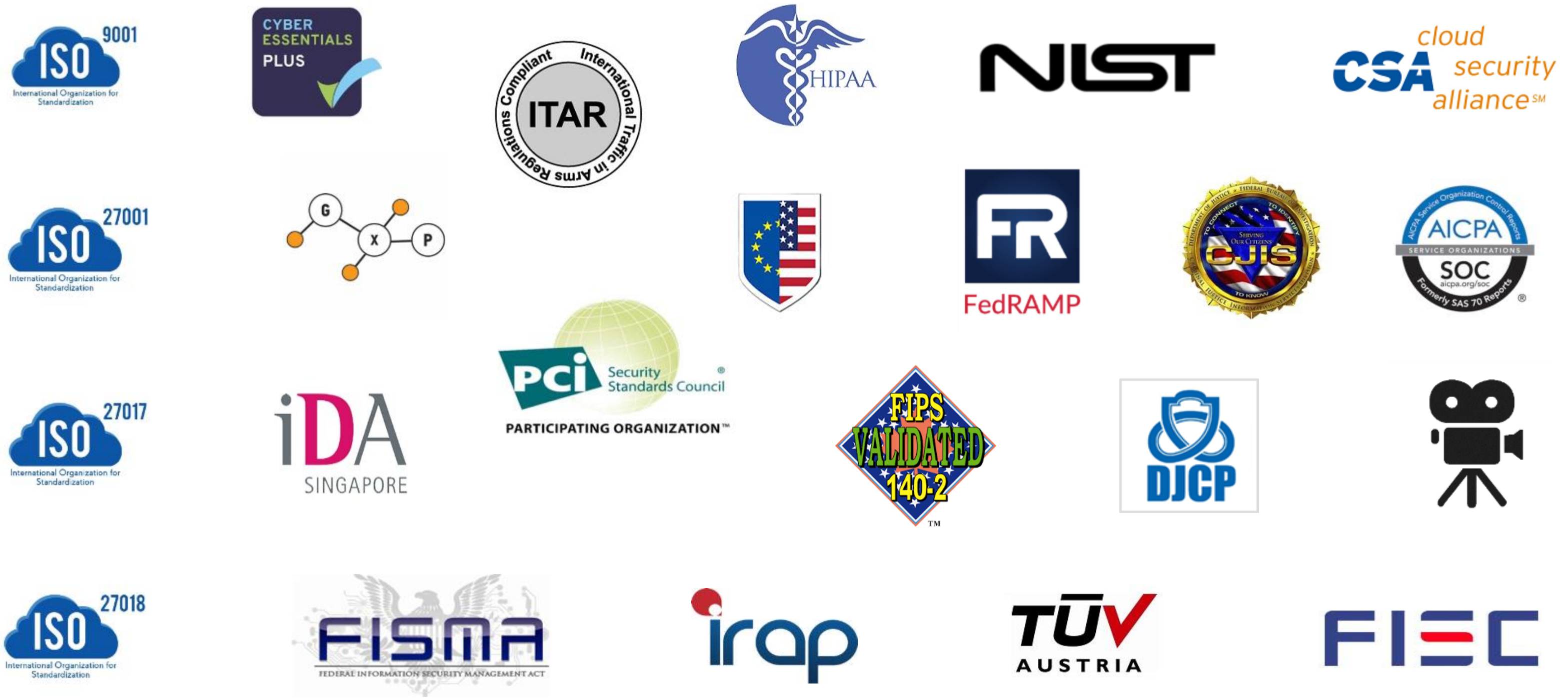
**US East**
N. Virginia (6)
Ohio (3)
**US West**
N. California (3)
Oregon (3)
**Asia Pacific**
Mumbai (2)
Seoul (2)
Singapore (3)
Sydney (3)
Tokyo (4)
Osaka-Local (1)
**Canada**
Central (2)

**China**
Beijing (2)
Ningxia (3)
**Europe**
Frankfurt (3)
Ireland (3)
London (3)
Paris (3)
Stockholm (3)
South America
São Paulo (3)
**GovCloud (US)**
US-East (3)
US-West (3)

## New Regions (coming soon)

Bahrain, Cape Town, Hong Kong SAR, Milan

# Inherit global security and compliance controls


ISO 9001
International Organization for Standardization
CYBER ESSENTIALS PLUS
ITAR
International Traffic in Arms Regulations Compliant
HIPAA
NIST
CSA cloud security alliance℠
ISO 27001
International Organization for Standardization
G X P
FR
FedRAMP
CJIS
Serving Our Citizens
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports
PCI Security Standards Council
PARTICIPATING ORGANIZATION™
ISO 27017
International Organization for Standardization
iDA SINGAPORE
FIPS VALIDATED 140-2
DJCP
ISO 27018
International Organization for Standardization
FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
irap
TÜV AUSTRIA
FISC

# AWS Compliance Program

Compliance **certifications** and **attestations** are assessed by a third-party, independent auditor and result in a **certification**, **audit report**, or **attestation of compliance**.

# AWS Compliance

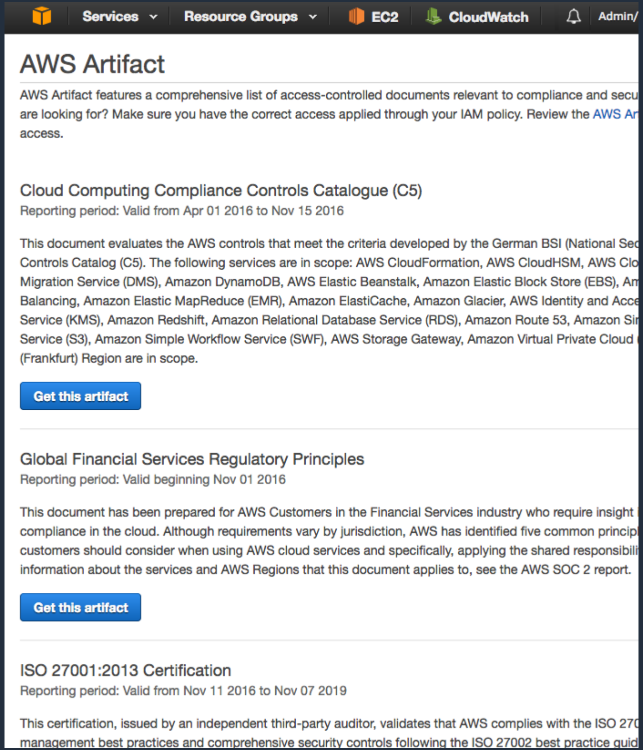
Compliance **alignments** and **frameworks** include published security or compliance requirements for a specific purpose, such as a specific industry or function.

AWS provides functionality (such as security features) and enablers (including compliance playbooks, mapping documents, and whitepapers) for these types of programmes.

# Accessing AWS Compliance Reports

AWS Artifact:

- On-demand access to AWS' compliance reports
- Globally available
- Easy identification
- Quick assessments
- Continuous monitoring
- Enhanced transparency



## AWS Artifact

AWS Artifact features a comprehensive list of access-controlled documents relevant to compliance and secu
are looking for? Make sure you have the correct access applied through your IAM policy. Review the AWS Ar
access.

### Cloud Computing Compliance Controls Catalogue (C5)

Reporting period: Valid from Apr 01 2016 to Nov 15 2016

This document evaluates the AWS controls that meet the criteria developed by the German BSI (National Sec
Controls Catalog (C5). The following services are in scope: AWS CloudFormation, AWS CloudHSM, AWS Clo
Migration Service (DMS), Amazon DynamoDB, AWS Elastic Beanstalk, Amazon Elastic Block Store (EBS), Am
Balancing, Amazon Elastic MapReduce (EMR), Amazon ElastiCache, Amazon Glacier, AWS Identity and Acce
Service (KMS), Amazon Redshift, Amazon Relational Database Service (RDS), Amazon Route 53, Amazon Si
Service (S3), Amazon Simple Workflow Service (SWF), AWS Storage Gateway, Amazon Virtual Private Cloud
(Frankfurt) Region are in scope.

Get this artifact

### Global Financial Services Regulatory Principles

Reporting period: Valid beginning Nov 01 2016

This document has been prepared for AWS Customers in the Financial Services industry who require insight
compliance in the cloud. Although requirements vary by jurisdiction, AWS has identified five common princip
customers should consider when using AWS cloud services and specifically, applying the shared responsibili
information about the services and AWS Regions that this document applies to, see the AWS SOC 2 report.

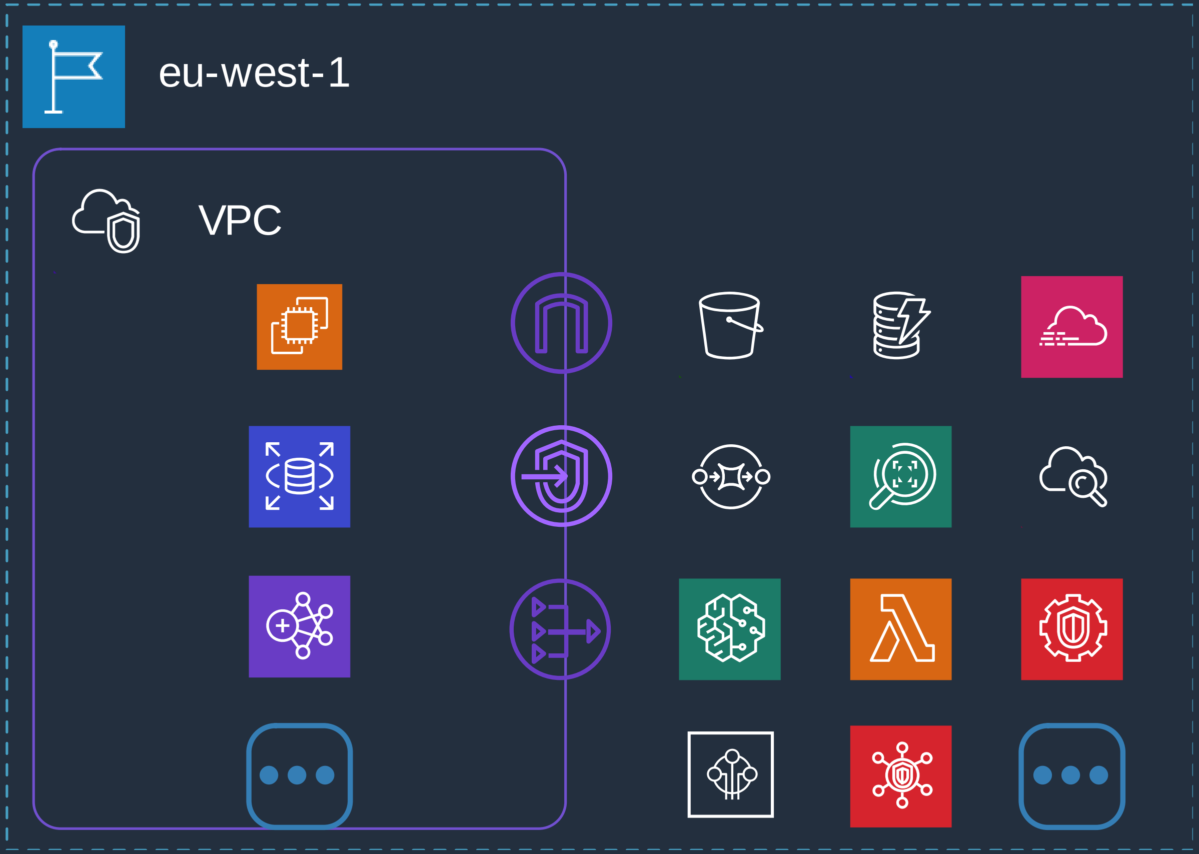
Get this artifact

### ISO 27001:2013 Certification

Reporting period: Valid from Nov 11 2016 to Nov 07 2019

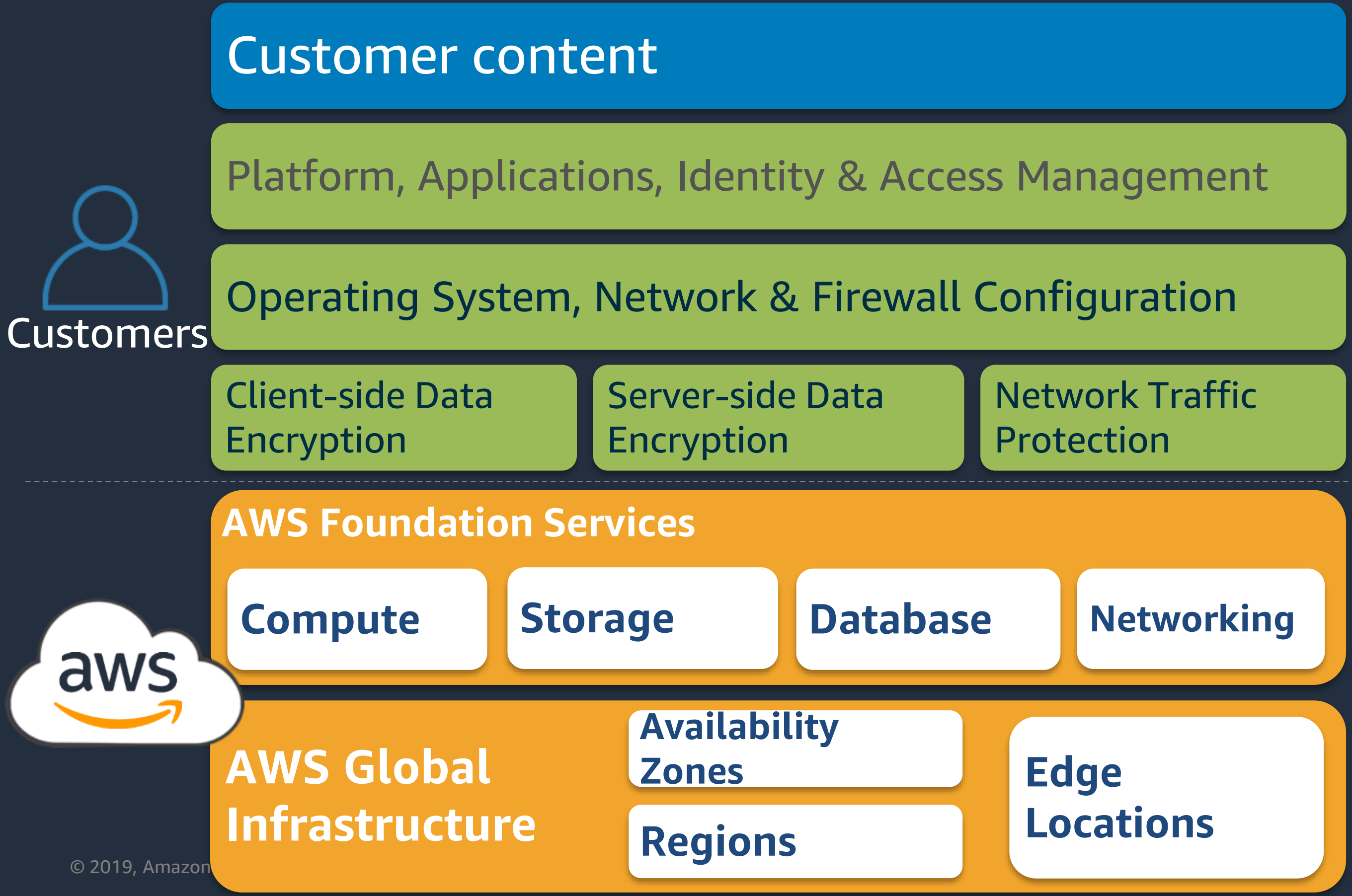
This certification, issued by an independent third-party auditor, validates that AWS complies with the ISO 270
management best practices and comprehensive security controls following the ISO 27002 best practice guid

# In a region



# The AWS Shared Responsibility Model

# AWS Shared Responsibility Model



Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Customers

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

AWS Foundation Services

Compute

Storage

Database

Networking

aws

AWS Global Infrastructure

Availability Zones

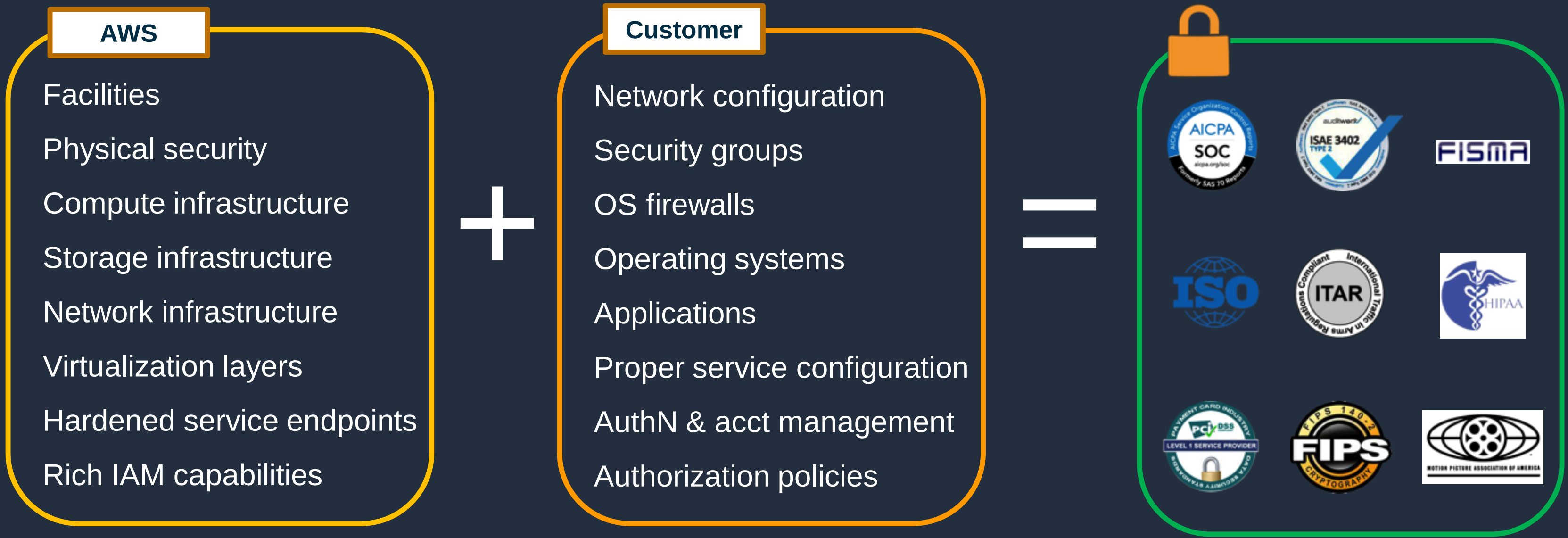
Regions

Edge Locations

Customers are responsible for their security and compliance **IN** the Cloud

AWS is responsible for the security **OF** the Cloud

# AWS Shared Responsibility Model – A deeper view



AWS

- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualization layers
- Hardened service endpoints
- Rich IAM capabilities

+

Customer

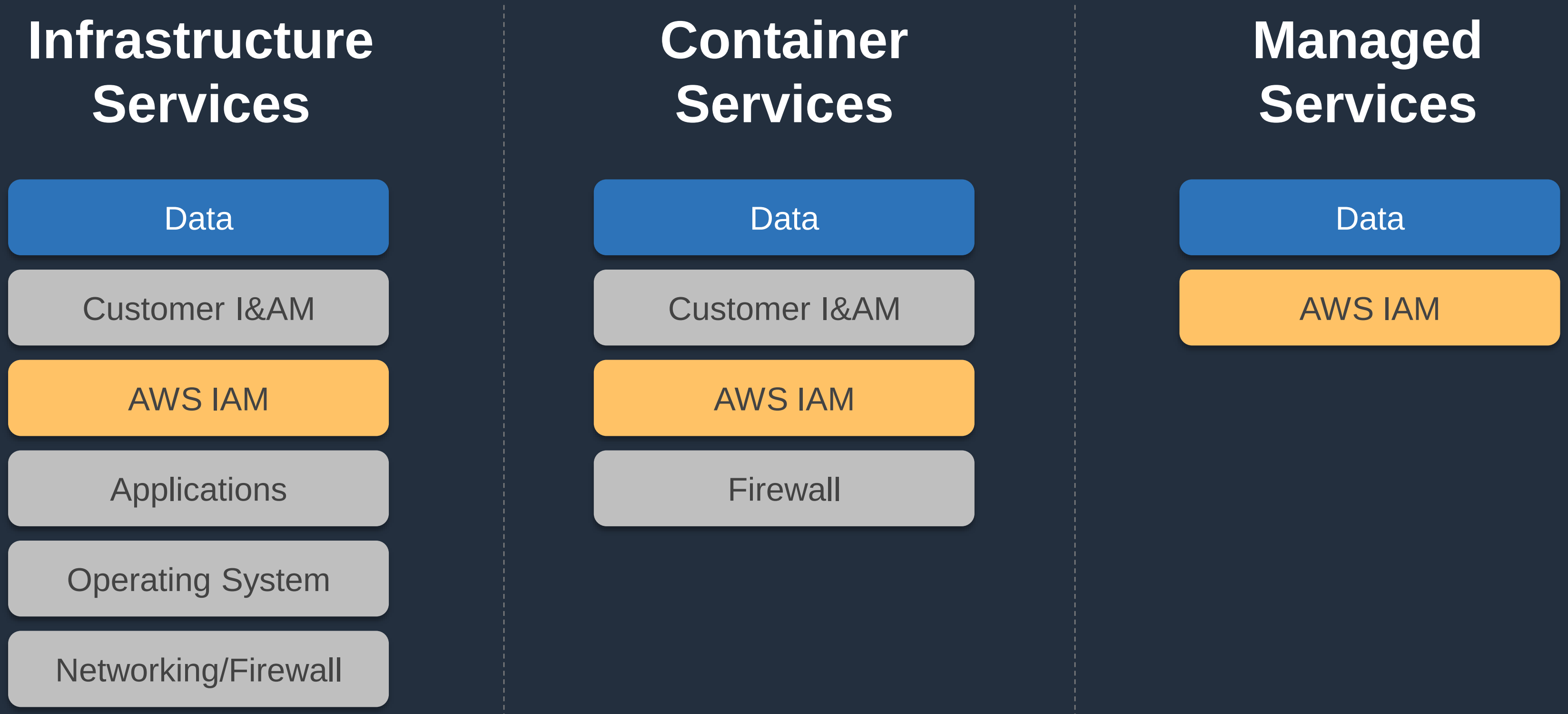
- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Applications
- Proper service configuration
- AuthN & acct management
- Authorization policies

=

AICPA SOC
ISAE 3402 TYPE II
FISMA
ISO
ITAR
HIPAA
PCI DSS LEVEL 1 SERVICE PROVIDER
FIPS 140-2 CRYPTOGRAPHY
MOTION PICTURE ASSOCIATION OF AMERICA

- Scope of responsibility depends on the type of service offered by AWS: Understanding who is responsible for what is critical to ensuring your AWS data and systems are secure!

# Summary of Customer Responsibility in the Cloud



## Infrastructure Services

- Data
- Customer I&AM
- AWS IAM
- Applications
- Operating System
- Networking/Firewall

## Container Services

- Data
- Customer I&AM
- AWS IAM
- Firewall

## Managed Services

- Data
- AWS IAM

# In short:

Your data is *your data* and you decide who can access it.

# AWS security solutions

## Identity

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

## Detective control

- AWS Security Hub
- Amazon GuardDuty
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- VPC Flow Logs

## Infrastructure security

- AWS Systems Manager
- AWS Shield
- AWS WAF – Web application firewall
- AWS Firewall Manager
- Amazon Inspector
- Amazon Virtual Private Cloud (VPC)

## Data protection

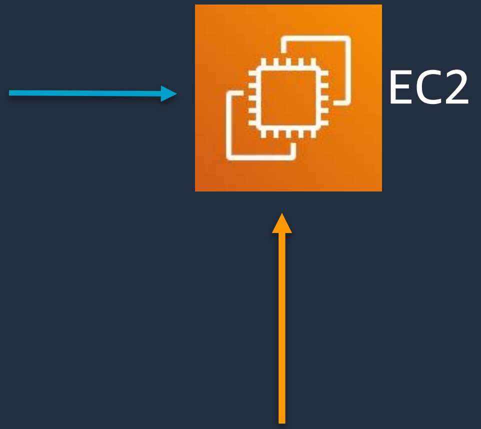
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- Amazon Macie
- Server-Side Encryption

## Incident response

- AWS Config Rules
- AWS Lambda

# Identity and Access Management

# Understanding planes of access



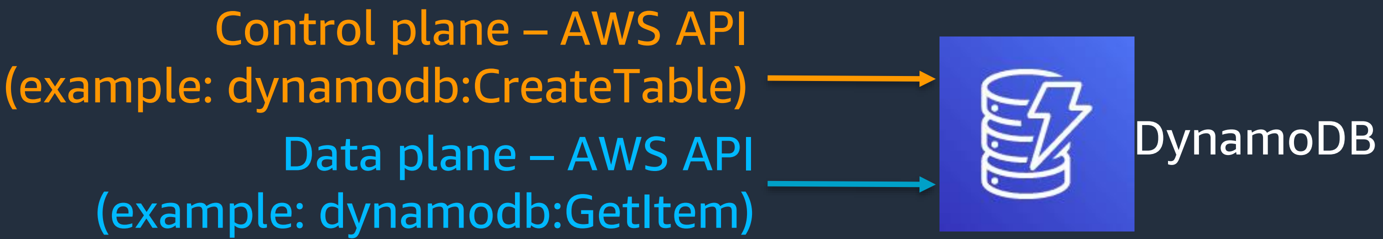
Data plane – VPC connection
(example: SSH, RDP)

EC2

Control plane – AWS API
(example: ec2:StartInstance)

Different:
- Paths
- Credentials
- Protocols

# Understanding planes of access



Control plane – AWS API
(example: dynamodb:CreateTable)

Data plane – AWS API
(example: dynamodb:GetItem)

DynamoDB

Same:

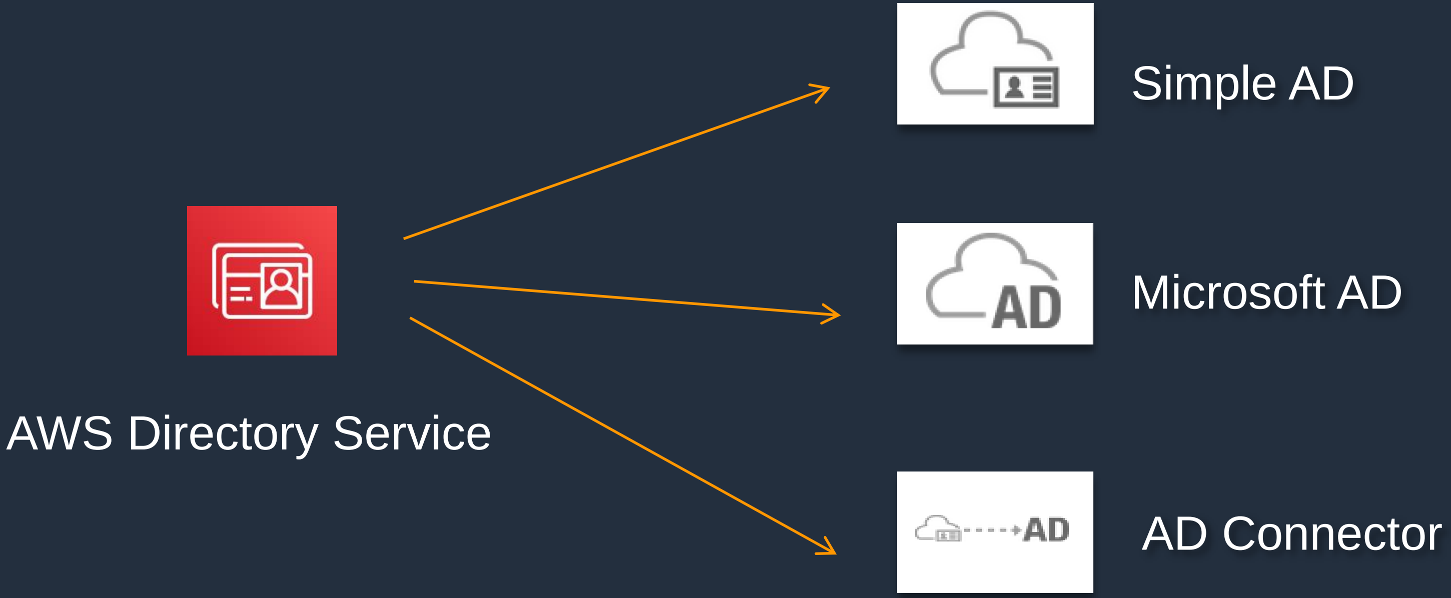
- Path
- Credential
- Protocol

# Identity & Access Management (IAM)

AWS Authentication supporting:

- Multiple options including rich SAML federation capabilities, MFA, web identities
- Clean separation of identity from proof of identity
- Roles are powerful and flexible pseudo-principals that can be assumed by other identities
  - Federation scenarios
  - Cross-account access

# AWS Directory Services – Authentication service



AWS Directory Service

Simple AD

Microsoft AD

AD Connector

# Detective Control

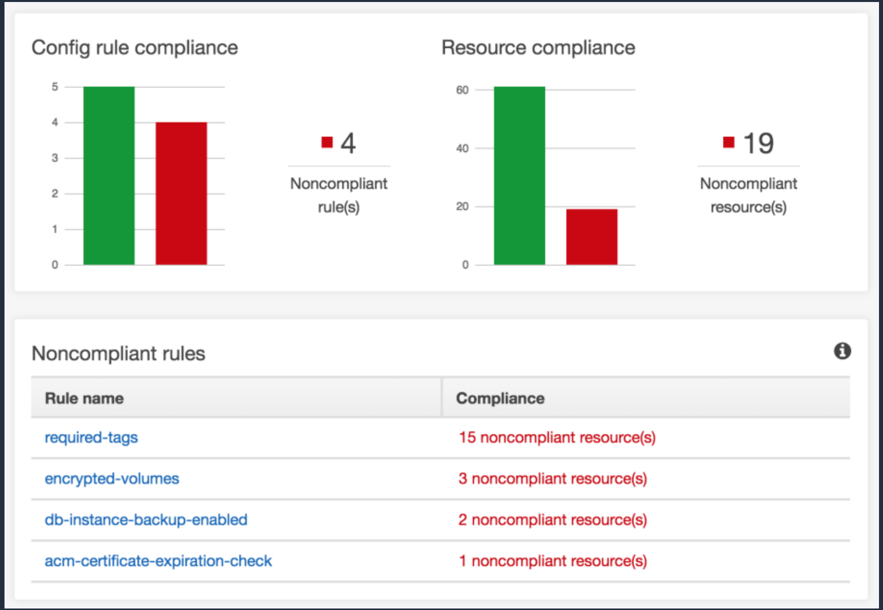
# AWS Config – Configuration monitoring

*AWS Config is a fully managed service that provides you with an inventory of your AWS resources, lets you audit the resource configuration history and notifies you of resource configuration changes.*

# Compliance change detection

Use AWS Config custom or managed rules to check for:

- CloudTrail is enabled
- Encrypted EBS volumes
- Tags
- RDS instances backup
- MFA for root account
- S3 Buckets logging
- and more



Config rule compliance

🟥 4

Noncompliant rule(s)

Resource compliance

🟥 19

Noncompliant resource(s)

Noncompliant rules

| Rule name | Compliance |
|---|---|
| required-tags | 15 noncompliant resource(s) |
| encrypted-volumes | 3 noncompliant resource(s) |
| db-instance-backup-enabled | 2 noncompliant resource(s) |
| acm-certificate-expiration-check | 1 noncompliant resource(s) |

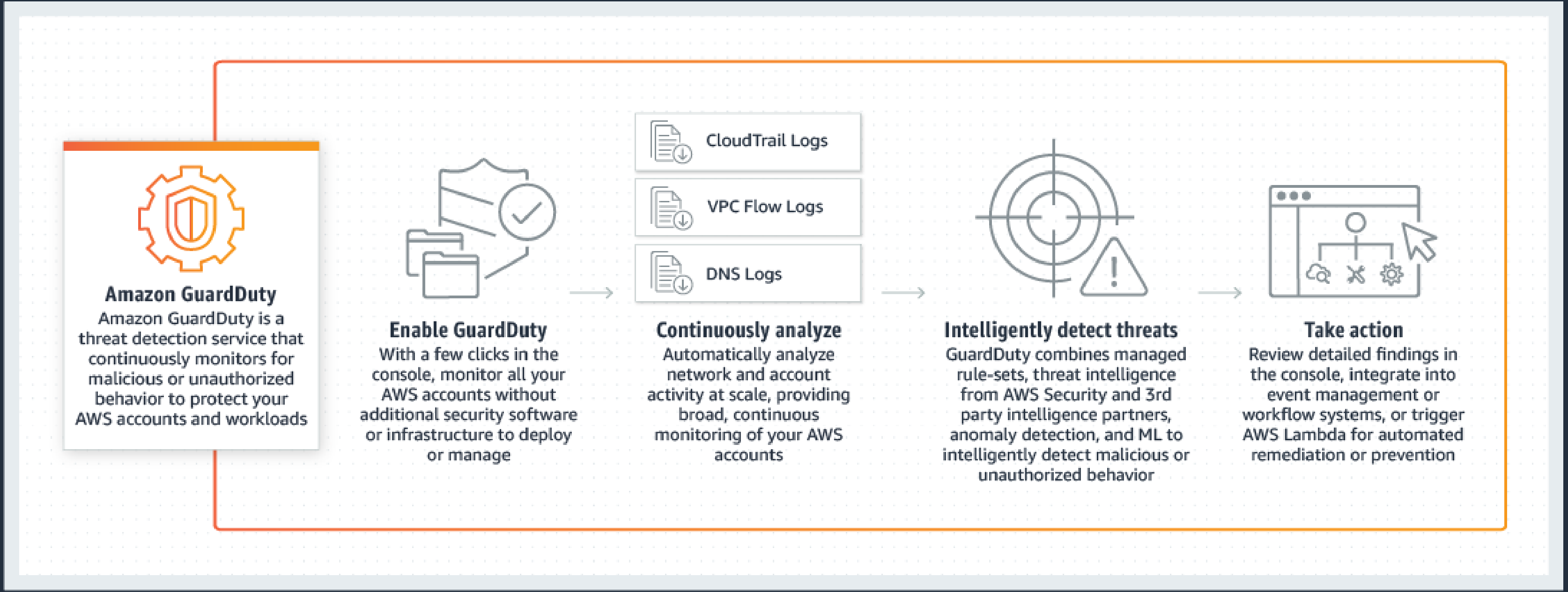
# Amazon GuardDuty

Amazon GuardDuty is a managed threat detection service that continuously monitors for **malicious** or **unauthorized** behavior to help you protect your AWS accounts and workloads.

**GuardDuty Monitors:**

- Unusual API calls.
- Potentially unauthorized deployments that indicate a possible account compromise.
- Potentially compromised instances or reconnaissance by attackers.

# Intelligent threat detection with Amazon GuardDuty



**Amazon GuardDuty**

Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to protect your AWS accounts and workloads

**Enable GuardDuty**

With a few clicks in the console, monitor all your AWS accounts without additional security software or infrastructure to deploy or manage

CloudTrail Logs

VPC Flow Logs

DNS Logs

**Continuously analyze**

Automatically analyze network and account activity at scale, providing broad, continuous monitoring of your AWS accounts

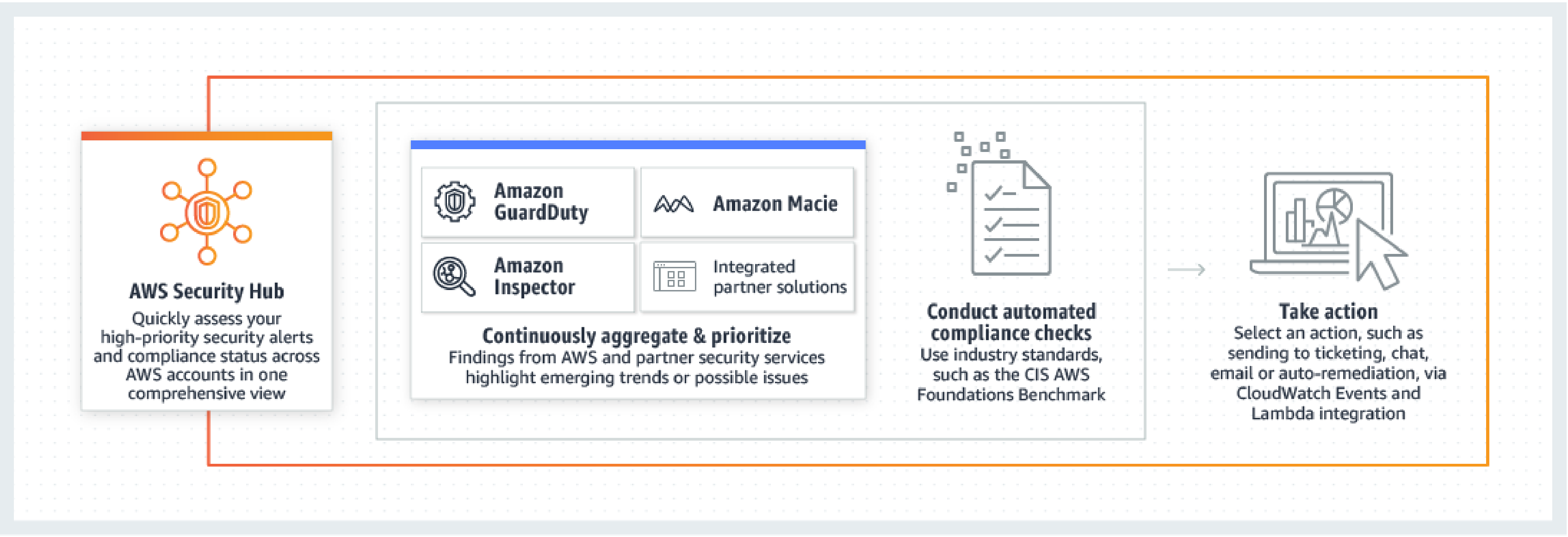
**Intelligently detect threats**

GuardDuty combines managed rule-sets, threat intelligence from AWS Security and 3rd party intelligence partners, anomaly detection, and ML to intelligently detect malicious or unauthorized behavior

**Take action**

Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

# AWS Security Hub Overview



**AWS Security Hub**

Quickly assess your high-priority security alerts and compliance status across AWS accounts in one comprehensive view

Amazon GuardDuty

Amazon Macie

Amazon Inspector

Integrated partner solutions

**Continuously aggregate & prioritize**

Findings from AWS and partner security services highlight emerging trends or possible issues

**Conduct automated compliance checks**

Use industry standards, such as the CIS AWS Foundations Benchmark

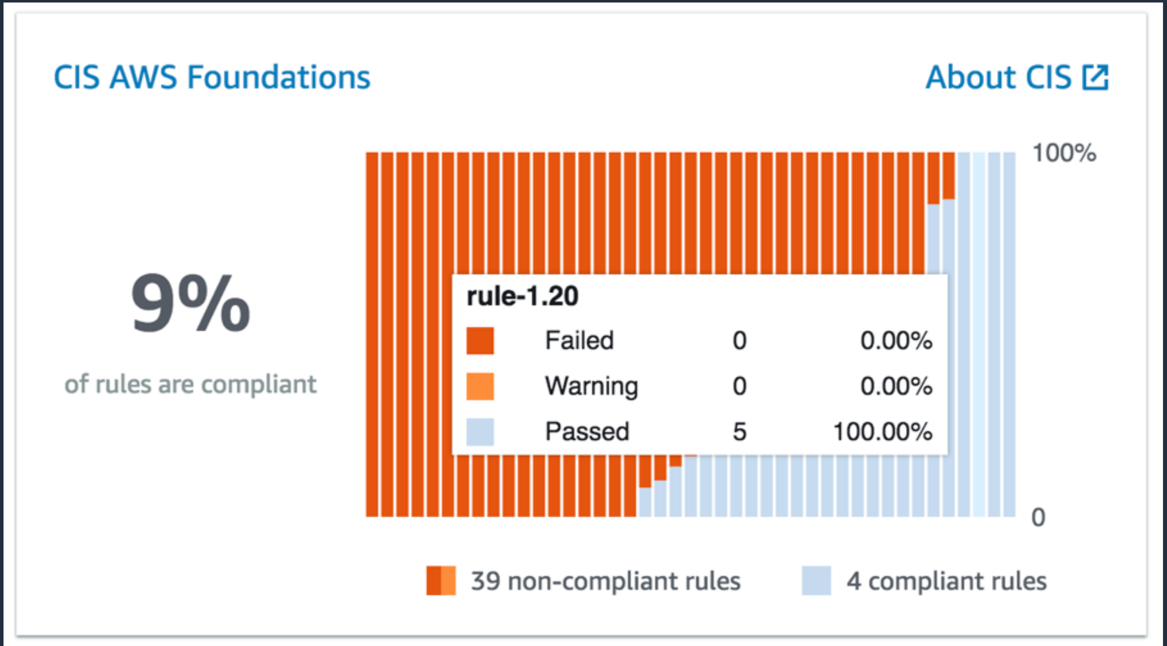
**Take action**

Select an action, such as sending to ticketing, chat, email or auto-remediation, via CloudWatch Events and Lambda integration

# AWS Security Hub: Automated Assessment Versus Standards

CIS® Center for Internet Security®

43 fully automated, nearly continuous checks



CIS AWS Foundations

About CIS

9%

of rules are compliant

rule-1.20

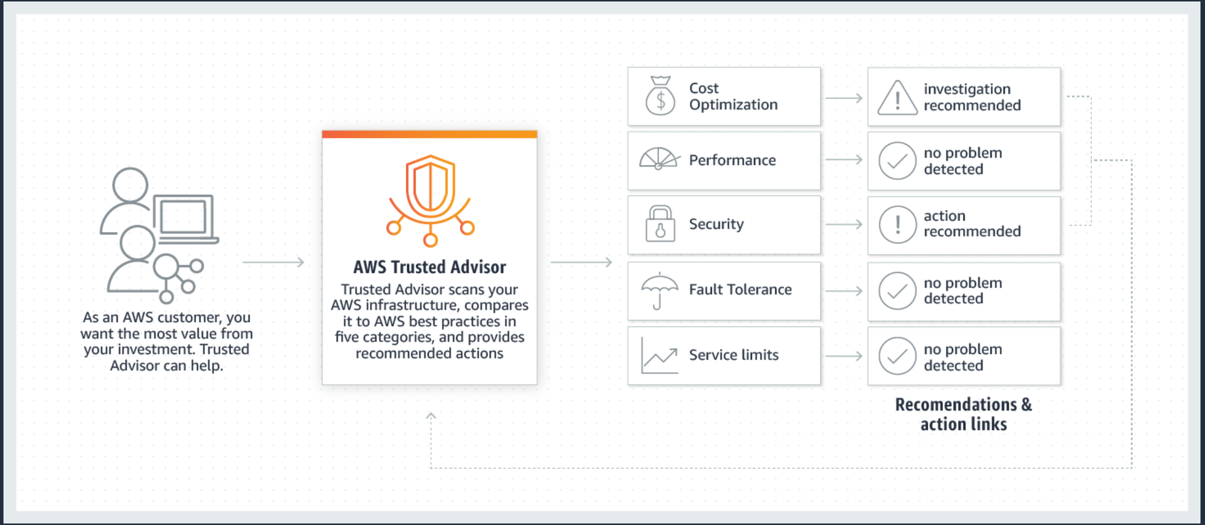
| | | | |
|---|---|---|---|
| 🟥 | Failed | 0 | 0.00% |
| 🟧 | Warning | 0 | 0.00% |
| ⬜ | Passed | 5 | 100.00% |

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark

# AWS Trusted Advisor – Real time guidance

Security configuration checks of your AWS environment:

- Open ports
- Unrestricted access
- CloudTrail Logging
- S3 Bucket Permissions
- Multi-factor auth
- Password Policy
- DB Access Risk
- DNS Records
- Load Balancer config



As an AWS customer, you want the most value from your investment. Trusted Advisor can help.

**AWS Trusted Advisor**

Trusted Advisor scans your AWS infrastructure, compares it to AWS best practices in five categories, and provides recommended actions

**Recomendations & action links**

# Detective Control - Logging and Auditing

# Full visibility and logging features

Full **visibility** of your AWS environment

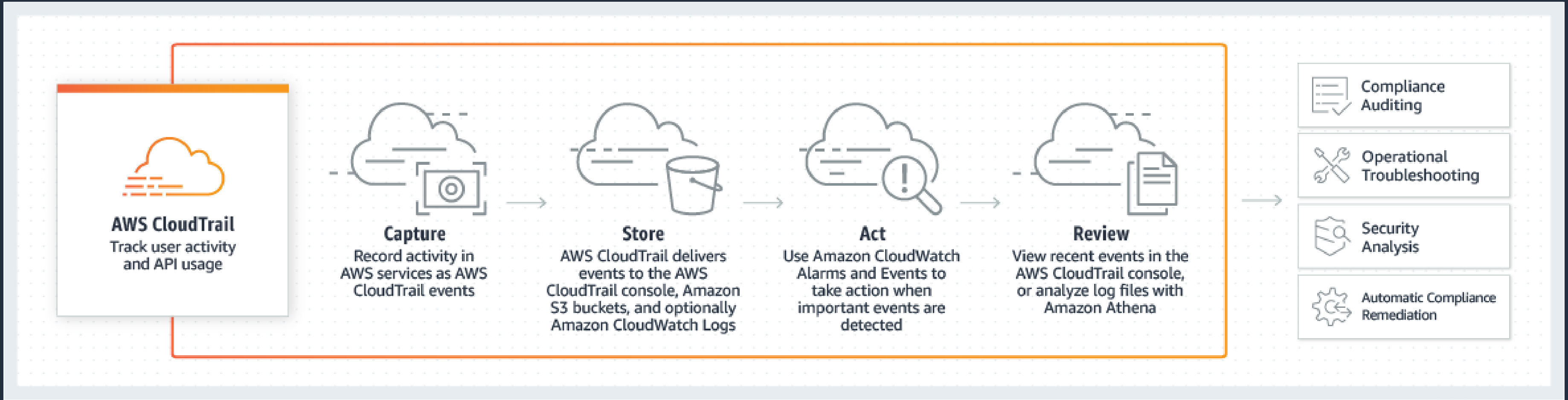
- CloudTrail will record access to API calls and save logs in your S3 buckets, no matter how those API calls were made

**Who** did **what** and **when** and from **where** (IP address)

- CloudTrail/Config support for many AWS services and growing - includes EC2, EBS, VPC, RDS, IAM and RedShift
- Edge/CDN, WAF, ELB,VPC/Network FlowLogs
- Easily Aggregate all log information
- CloudWatch Alarms

Out of the box **integration** with log analysis tools from AWS partners including Splunk, AlertLogic and SumoLogic

# Tracking of user activity and API usage with AWS CloudTrail



**AWS CloudTrail**
Track user activity and API usage

**Capture**
Record activity in AWS services as AWS CloudTrail events

**Store**
AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs

**Act**
Use Amazon CloudWatch Alarms and Events to take action when important events are detected

**Review**
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena

- Compliance Auditing
- Operational Troubleshooting
- Security Analysis
- Automatic Compliance Remediation

You are making API calls

On a growing set of services around the world…

AWS CloudTrail is continuously recording API calls

And delivering log files to you

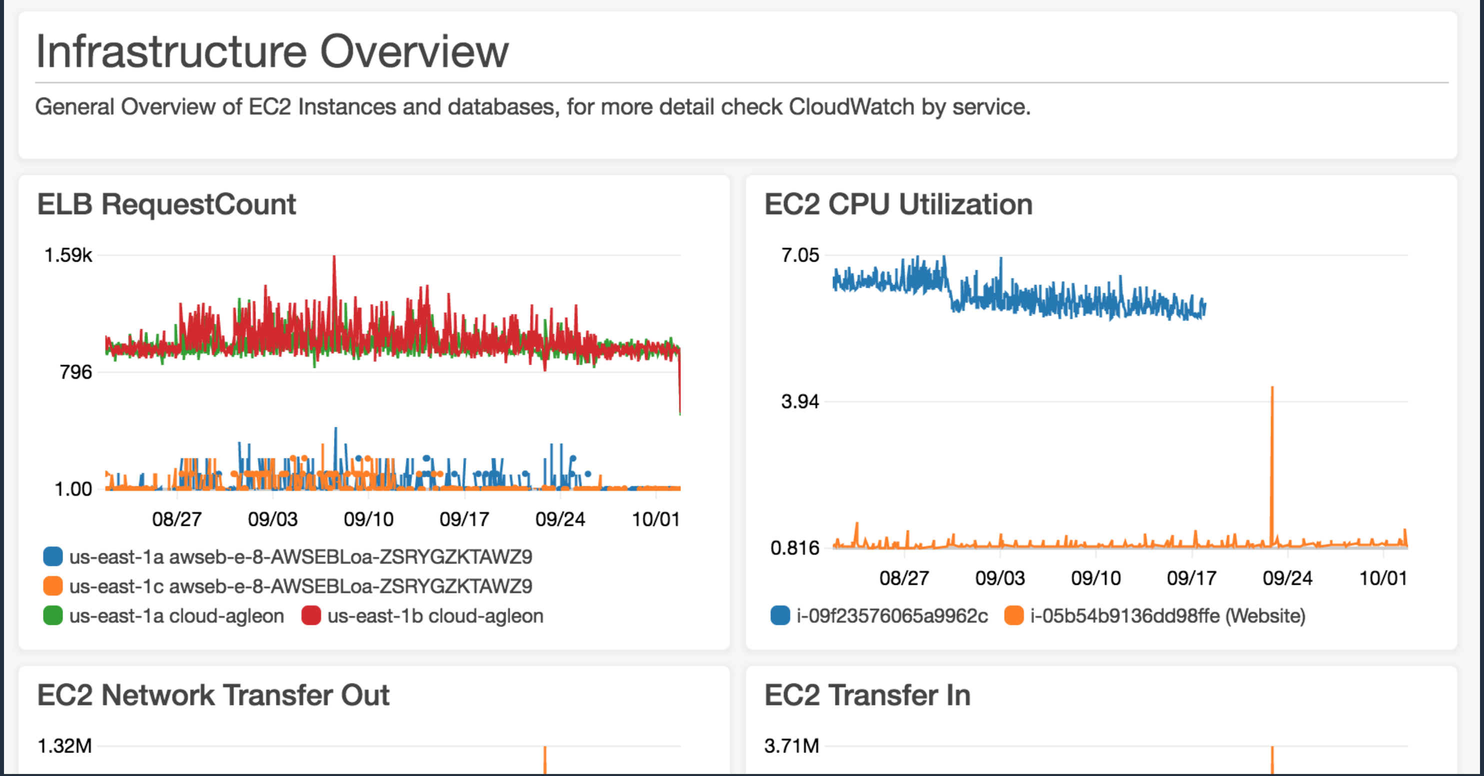
# Amazon CloudWatch – Monitoring service

CloudWatch provides visibility and metrics into every aspect of your AWS environment, metrics are actionable and can notifications, run code, etc.

Metrics include

- EC2 Instances (CPU Usage, Networking, etc)
- RDS instances (Connections, CPU, etc)
- ELB metrics (Healthy backends, Network, etc)
- Many services are included
- Support for Custom metrics

# CloudWatch Dashboards sample

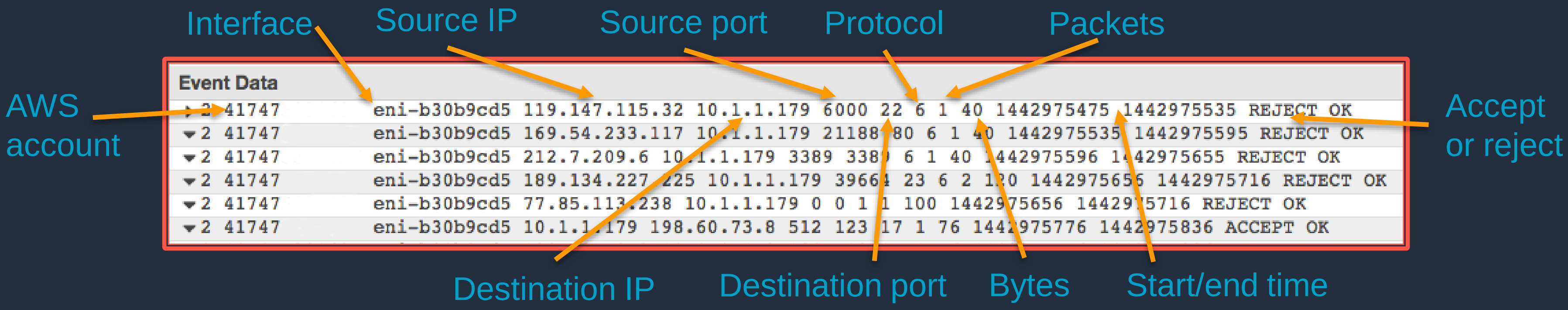


Infrastructure Overview

General Overview of EC2 Instances and databases, for more detail check CloudWatch by service.

# VPC Flow Logs

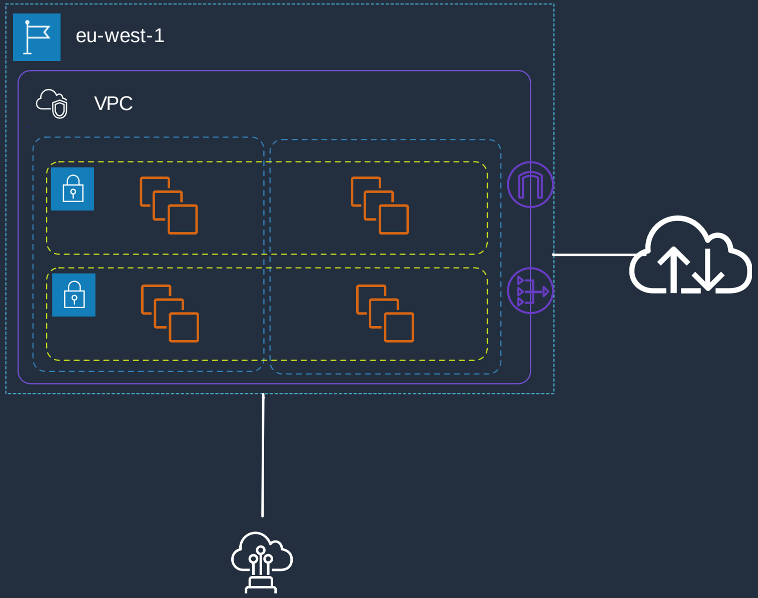
- Agentless
- Enable per ENI, per subnet, or per VPC
- Logged to AWS CloudWatch Logs
- Create CloudWatch metrics from log data
- Alarm on those metrics



```
Event Data
▸2 41747     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
```

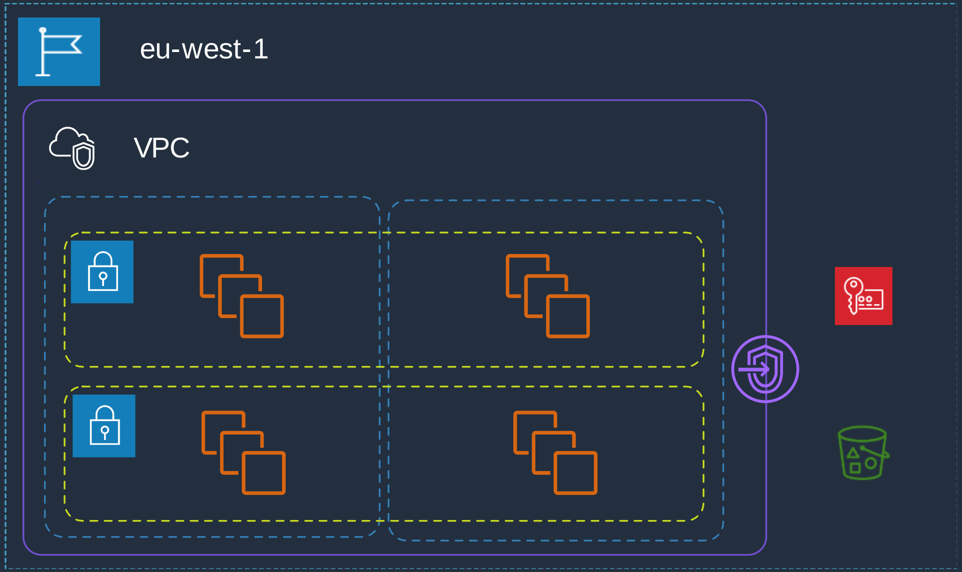
# Infrastructure Security

# Network isolation with Virtual Private Cloud



- Define your own IP address space with networks, subnets, routing
- Connect your offices with AWS using Direct Connect or VPN
- Configure Security Groups (virtual firewalls) for your instances
- Configure the Network Access Control List for control at the network layer level
- Enable private connections to AWS services using AWS Private Link
- Connect the accounts of your organization or other organizations

# Amazon VPC Endpoints



Access Amazon S3 and Amazon Dynamodb without an Internet Gateway and keep your connection private

Use cases

- Secure storage of files
- Private databases

# AWS Shield
# **Standard** & **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 at no additional cost | Cost Protection for scaling |

# AWS Shield **Standard**

**AWS Shield Standard**

## Layer 3/4 Protection for Everyone

- ✓ Automatic defense against the most common network and transport layer DDoS attacks for any AWS resource, in any AWS Region
- ✓ Comprehensive defense against all known network and transport layer attacks when using Amazon CloudFront and Amazon Route 53
- ✓ SYN Floods, UDP Floods, Reflection Attacks, etc.

**AWS WAF**

## Layer 7 Protection Available via AWS WAF

- ✓ Self-service & pay-as-you-go
- ✓ Flexible rule language

# AWS Shield Advanced:
# Enhanced Protection

## Detection

- Layer 7 attack detection
  - HTTP Floods
  - DNS Query Floods
- Baselining and Anomaly detection
- Enhanced Layer 3 attack detection

## Mitigation

- Proprietary packet filtering stacks
- Pre-configured mitigations according to resource type
- Customer defined Mitigations
- Traffic Engineering for Large DDoS Attacks
- Network ACLs executed at the border for EIPs

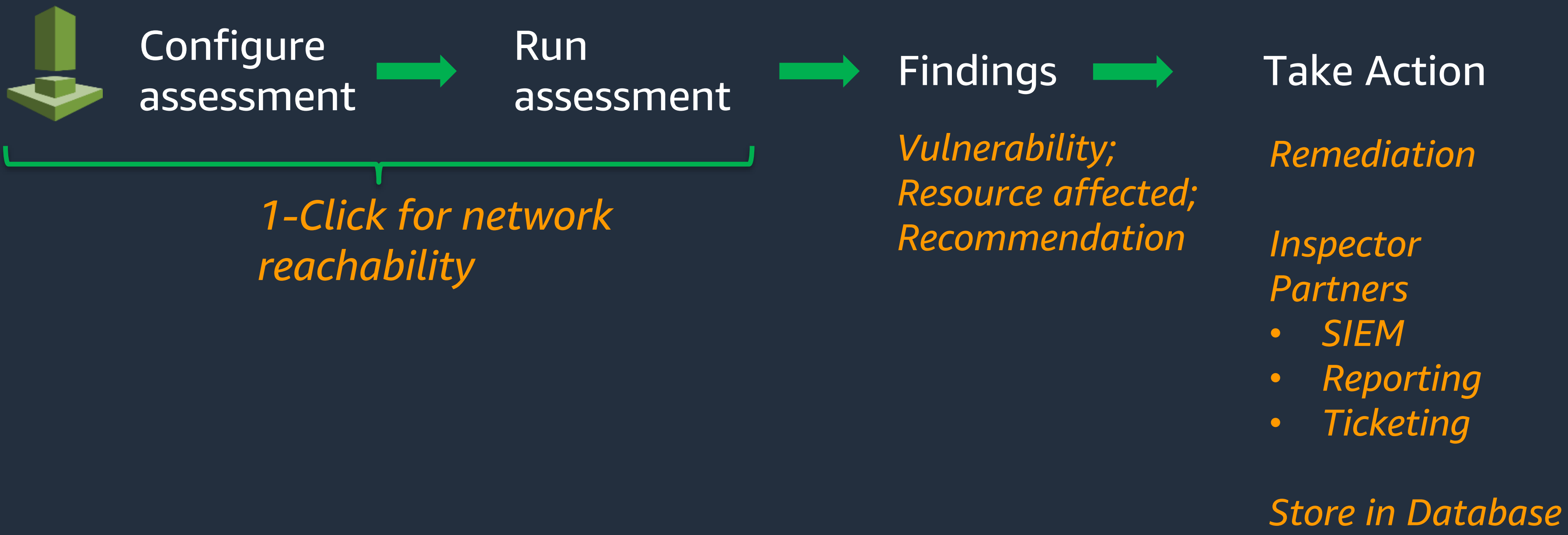
# Amazon Inspector

- Vulnerability Assessment Service
  - Built from the ground up to support DevSecOps
  - Automatable via APIs
  - Integrates with CI/CD tools
  - On-Demand Pricing model
  - Static & Dynamic Rules Packages
  - Generates Findings

# Amazon Inspector – common use cases

| | **Network Reachability**<br>***(access to instances)*** | **Host assessments**<br>***(vulnerabilities on instances)*** |
|---|---|---|
| *Before deployment* | Validate network;<br>Find unexpected exposure | Check golden AMIs;<br>DevOps pipeline |
| *Migration* | VPC configuration mistakes | Check for software changes;<br>New (zero-day) vulnerabilities |
| *Production* | Check that no exposures have opened up | Check for software changes;<br>New (zero-day) vulnerabilities |

# How to use Amazon Inspector?



Configure assessment → Run assessment → Findings → Take Action

*1-Click for network reachability*

Findings:

*Vulnerability;*
*Resource affected;*
*Recommendation*

Take Action:

*Remediation*

*Inspector Partners*

- *SIEM*
- *Reporting*
- *Ticketing*

*Store in Database*

# Penetration Testing of your AWS environment

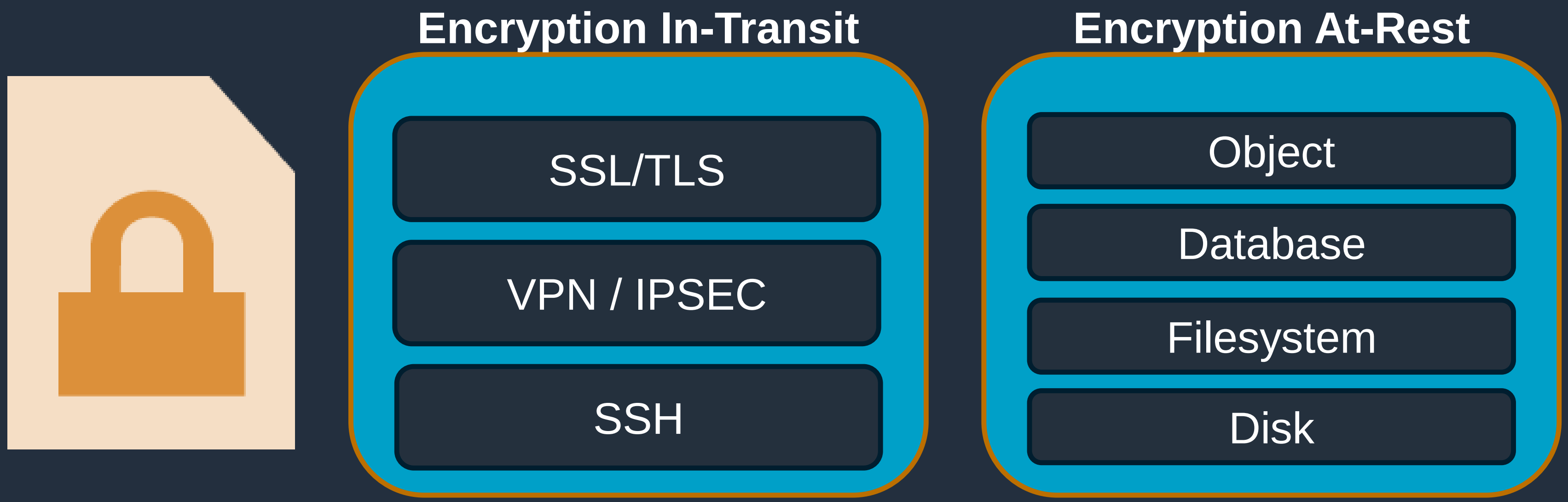
Effective immediately, AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services.

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront (Restricted, please read the policy)
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Please review the full policy at:
https://aws.amazon.com/security/penetration-testing/

# Data Privacy and Encryption

# Data Protection In-Transit and At-Rest



## Encryption In-Transit

- SSL/TLS
- VPN / IPSEC
- SSH

## Encryption At-Rest

- Object
- Database
- Filesystem
- Disk

# AWS Certificate Manager (ACM), In-Transit

- Provision trusted SSL/TLS certificates from AWS for use with AWS resources:
  - Elastic Load Balancing
  - Amazon CloudFront distributions
- AWS handles the muck
  - Key pair and CSR generation
  - Managed renewal and deployment
- Domain validation (DV) through email
- Available through AWS Management Console, AWS Command Line Interface (AWS CLI), or API

# Data Encryption At-Rest

AWS CloudHSM

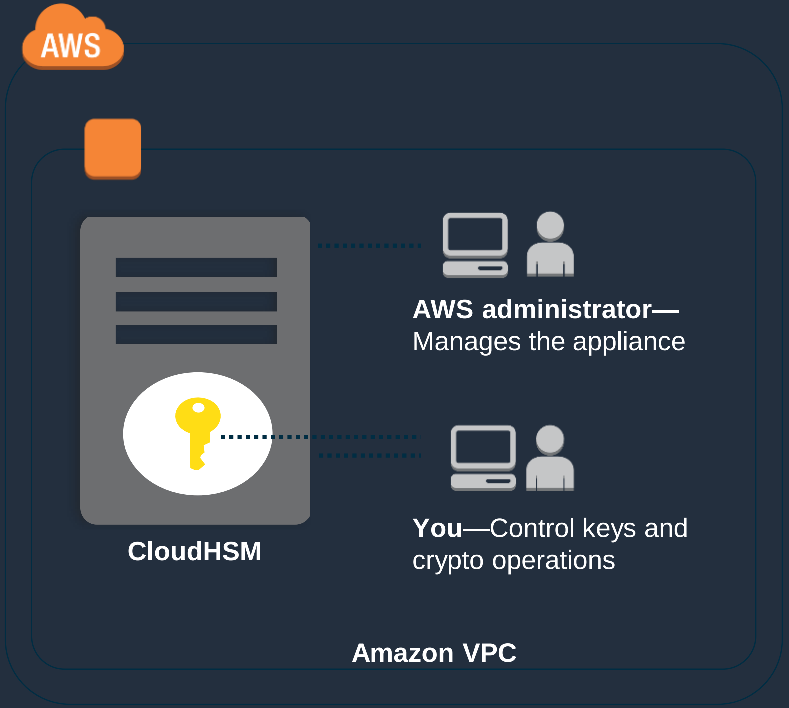
AWS
Key Management Service

# AWS Key Management Service (AWS KMS)

- Managed service that simplifies creation, control, rotation, deletion, and use of encryption keys in your applications
- Integrated with many AWS services for server-side encryption
- Integrated with AWS service clients/SDKs
    - S3, EMRFS, DynamoDB, AWS Encryption SDK
- Integrated with CloudTrail to provide auditable logs of key usage for regulatory and compliance activities
- Available in all commercial regions except China

# AWS CloudHSM

- Dedicated access to HSM appliances
- HSMs located in AWS data centers
- Managed and monitored by AWS
- Only you have access to your keys and operations on the keys
- HSMs are inside your Amazon VPC, isolated from the rest of the network
- Setup right from the console


AWS
CloudHSM
**AWS administrator—**Manages the appliance
**You**—Control keys and crypto operations
Amazon VPC

# AWS CloudHSM

Available in multiple AWS regions worldwide

Compliance

- Included in AWS PCI DSS and SOC compliance packages
- FIPS 140-2 level 3 (AWS CloudHSM)
- FIPS 140-2 level 2 (AWS CloudHSM Classic)

Typical use cases

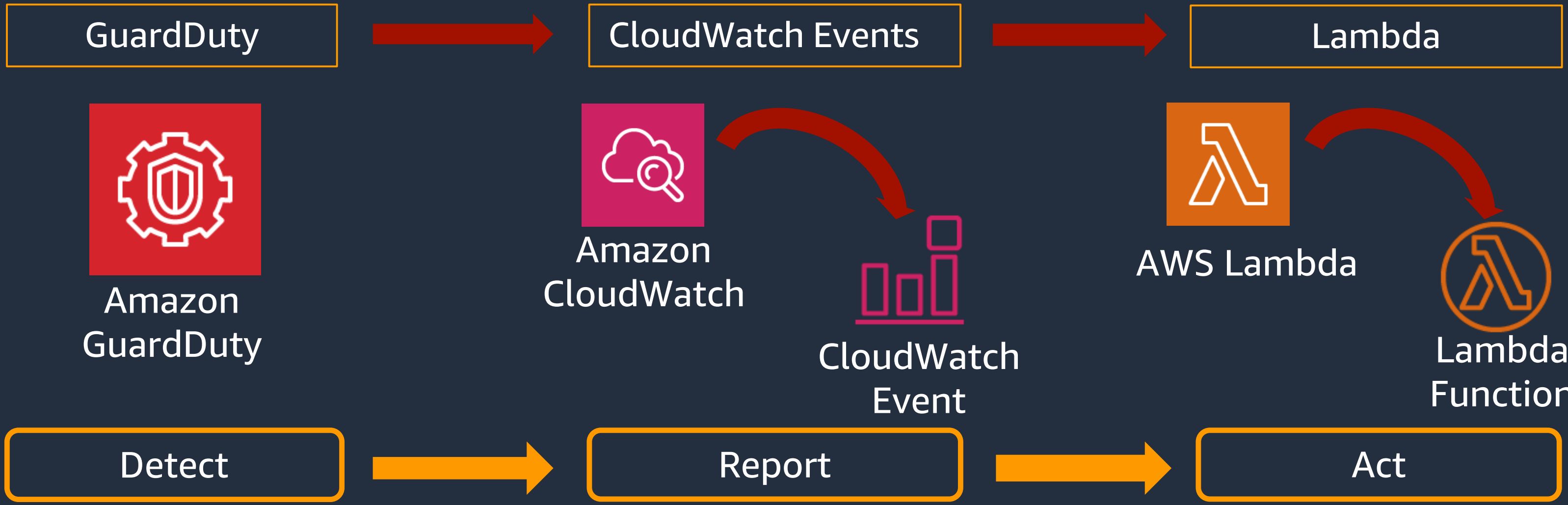
- Electronic invoicing and document signing
- Use with Amazon Redshift and RDS for Oracle
- Integrate with third-party software (Oracle, Microsoft SQL Server, Apache, SafeNet, OpenSSL)
- Build your own custom applications

# Incident Response

# Responding to Findings: *Remediation*

- Remediate a Compromised Instance
- Remediate Compromised AWS Credentials

## Automatic Remediation



# Largest ecosystem of security partners and solutions

## Infrastructure security

ALERT LOGIC

iMPERVA

ARMOR

paloalto NETWORKS

Barracuda

SOPHOS

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

f5

Symantec.

FORTINET

TREND MICRO

## Identity & access control

okta

onelogin

PingIdentity

## Data protection

gemalto security to be free

Vormetric a Thales Company

## Configuration & vulnerability analysis

ALERT LOGIC Security. Compliance. Cloud.

cavirin

CloudCheckr

CloudPassage

Dome9 SECURITY

evident.io

QUALYS CONTINUOUS SECURITY

RedLock

SAVIYNT

tenable

threat stack

turbot

## Logging & monitoring

sumologic

splunk>

ALIEN VAULT

aws

# At AWS Security is Job Zero

Designed for security

Constantly monitored

Highly automated

Highly available

Highly accredited

# Q&A

Name of presenter

# Thank you!

# Additional Resources

# AWS Quick Starts

# What are AWS Quick Starts?

AWS Quick Starts are:

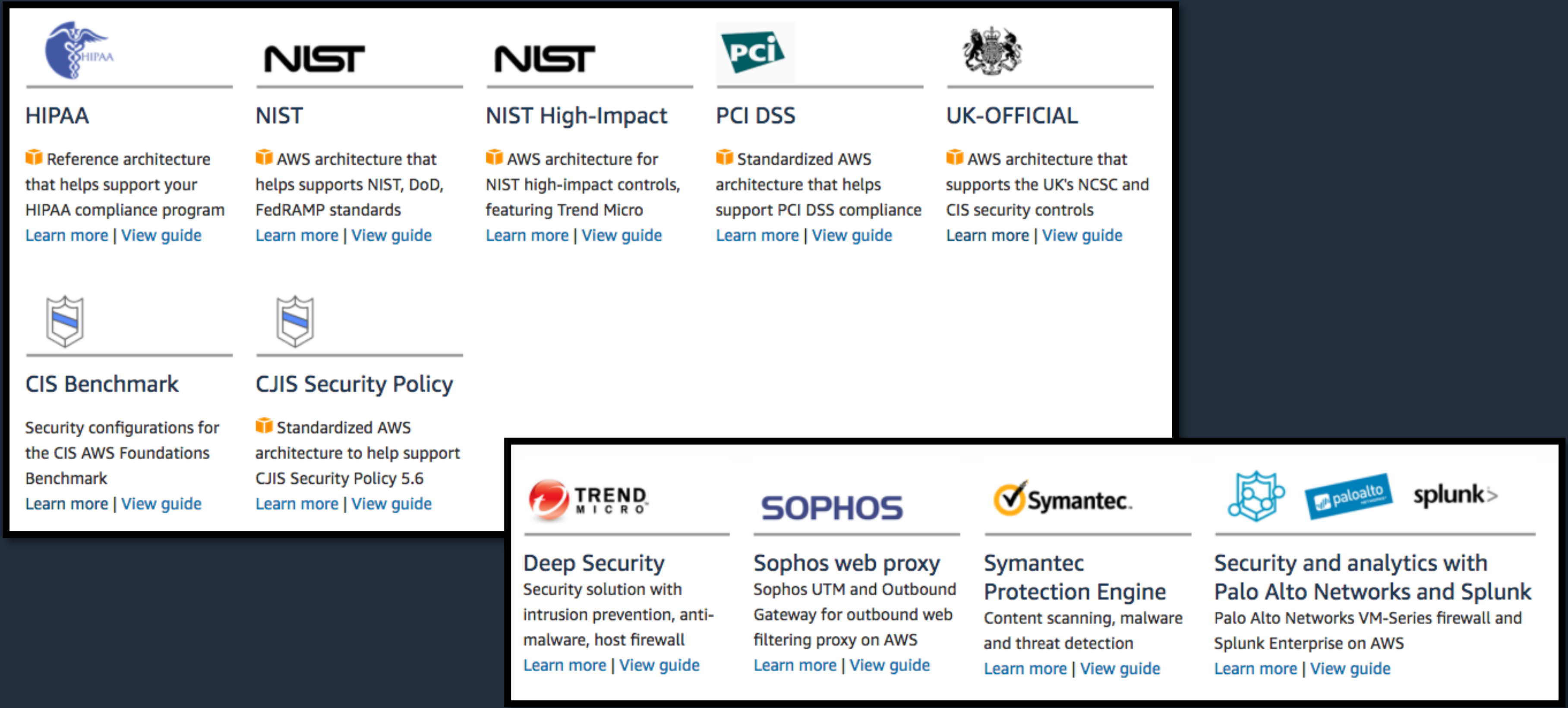
- built by AWS solutions architects and partners
- help you deploy popular solutions on AWS
- based on AWS best practices for security and high availability

Covers a wide range of topics

- DevOps; Security & Compliance
- Database & Storage; Big Data & Analytics
- Microsoft & SAP

https://aws.amazon.com/quickstart/

# Security-focused Quick Starts



### HIPAA

Reference architecture that helps support your HIPAA compliance program

Learn more | View guide

### NIST

AWS architecture that helps supports NIST, DoD, FedRAMP standards

Learn more | View guide

### NIST High-Impact

AWS architecture for NIST high-impact controls, featuring Trend Micro

Learn more | View guide

### PCI DSS

Standardized AWS architecture that helps support PCI DSS compliance

Learn more | View guide

### UK-OFFICIAL

AWS architecture that supports the UK's NCSC and CIS security controls

Learn more | View guide

### CIS Benchmark

Security configurations for the CIS AWS Foundations Benchmark

Learn more | View guide

### CJIS Security Policy

Standardized AWS architecture to help support CJIS Security Policy 5.6

Learn more | View guide

### Deep Security

Security solution with intrusion prevention, anti-malware, host firewall

Learn more | View guide

### Sophos web proxy

Sophos UTM and Outbound Gateway for outbound web filtering proxy on AWS

Learn more | View guide

### Symantec Protection Engine

Content scanning, malware and threat detection

Learn more | View guide

### Security and analytics with Palo Alto Networks and Splunk

Palo Alto Networks VM-Series firewall and Splunk Enterprise on AWS

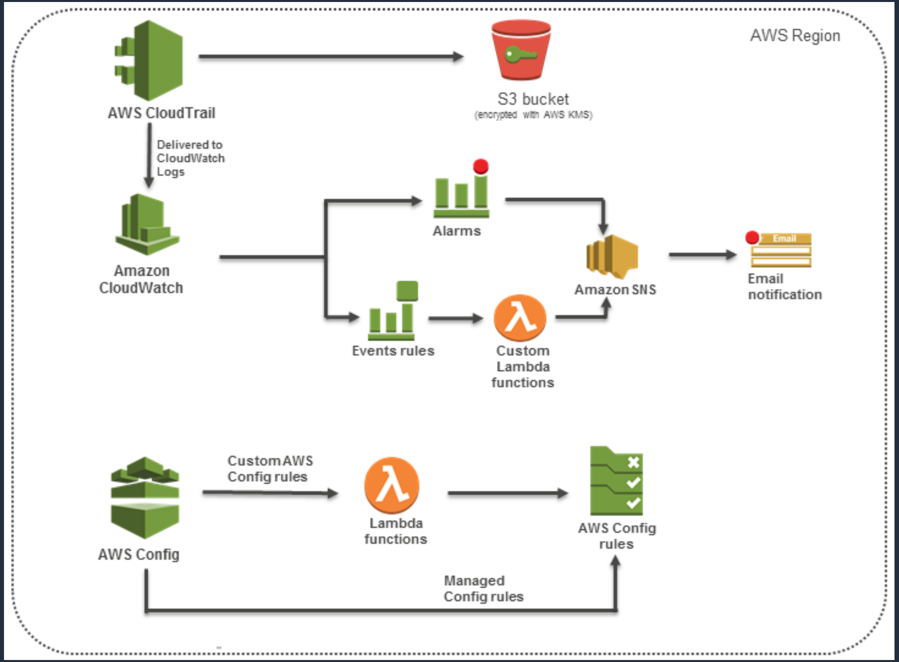
Learn more | View guide

# CIS Benchmark on AWS

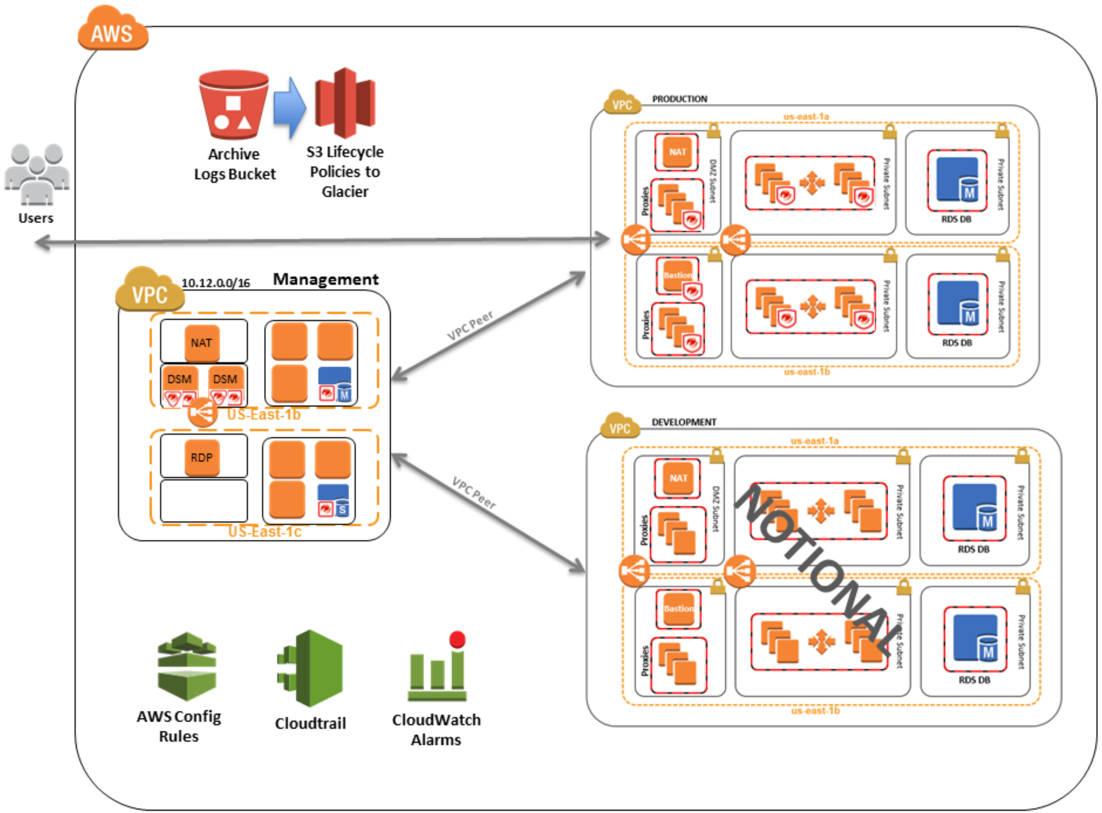
Standardized architecture for the Center for Internet Security (CIS) AWS Foundations Benchmark.

Deploys the following AWS services

- AWS Config rules
- CloudWatch alarms
- CloudWatch Events
- Lambda functions
- AWS CloudTrail
- AWS Config



# NIST High-Impact on AWS



# AWS Answers

# What is AWS Answers?

- Offers clear answers to common questions about architecting, building, and running applications on AWS
- Repository of instructional documents and solutions
- Outlines AWS best practices & provides prescriptive architectural guidance

https://aws.amazon.com/answers/

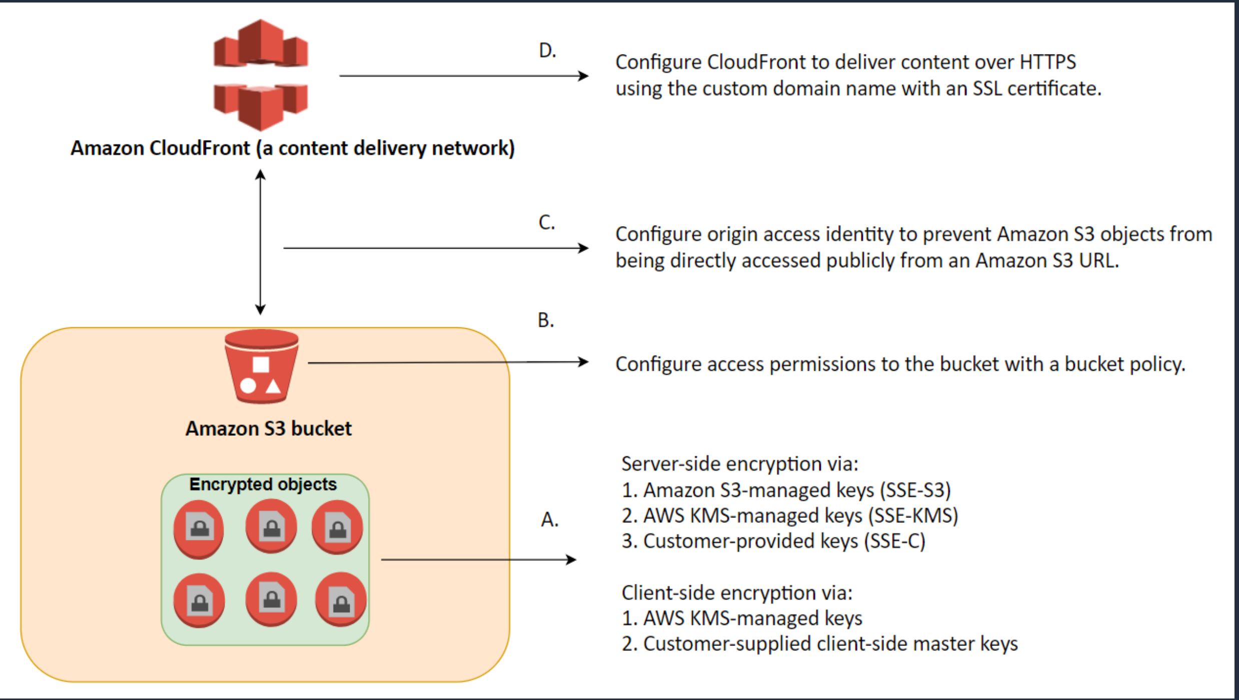
# AWS Blogs

# What are AWS Blogs?

- New service / functionality announcements
- Best practice guidance
- Customer references and case studies
- Key blogs from a security perspective:
  - AWS Security: https://aws.amazon.com/blogs/security/
  - AWS Management Tools: https://aws.amazon.com/blogs/mt/
  - AWS Architecture: https://aws.amazon.com/blogs/architecture/

**https://aws.amazon.com/blogs/**

# Securing data on S3 using bucket policies



D. Configure CloudFront to deliver content over HTTPS using the custom domain name with an SSL certificate.

C. Configure origin access identity to prevent Amazon S3 objects from being directly accessed publicly from an Amazon S3 URL.

B. Configure access permissions to the bucket with a bucket policy.

A. Server-side encryption via:
1. Amazon S3-managed keys (SSE-S3)
2. AWS KMS-managed keys (SSE-KMS)
3. Customer-provided keys (SSE-C)

Client-side encryption via:
1. AWS KMS-managed keys
2. Customer-supplied client-side master keys

[https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-your-amazon-s3-data/](https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-your-amazon-s3-data/)

# Finally, some links to remember…

AWS Cloud Security

Protect your data with cloud-powered security.

I'd like information about Security in the Cloud »

**https://aws.amazon.com/security/**

AWS Cloud Compliance

Assurance programs for finance, healthcare, government and more.

I'd like information about Compliance in the Cloud »

**https://aws.amazon.com/compliance/**