AWS RESEARCH ROADSHOW – 4 APRIL 2023

Security & Data Sovereignty on AWS

AWS Education & Research Team

Roberta Piscitelli - piscitr@amazon.com
Nikiforos Botis - nbotis@amazon.com
Pavlos Kaimakis- pkaim@amazon.com
Michael Wittel – mwittel@amazon.com
Vasilios Kotitsas – vasiliko@amazon.com
Marina Arcadieva - arcadiev@amazon.com

At AWS, cloud security is our top priority.

All AWS customers benefit from a data center and network architecture built to satisfy the requirements of the most security-sensitive organizations.

AWS Security, Identity, and Compliance Solutions

Identity and access management

- AWS Identity and Access Management (IAM)
- AWS IAM Identity Center (successor to AWS SSO)
- 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
- Amazon VPC
- 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
- Amazon EventBridge
- AWS Backup
- AWS Security Hub
- AWS Elastic Disaster Recovery

Privacy and Compliance

- AWS Artifact
- AWS Audit Manager
- Amazon CloudWatch
- AWS CloudTrail
- AWS Config
- AWS Security Hub
- AWS Systems Manager

Gain access to a world-class security team

Where would some of the world’s top security people like to work? At scale on huge challenges with huge rewards

So AWS has world-class security and compliance teams watching your back!

Every customer benefits from the tough scrutiny of other AWS customers

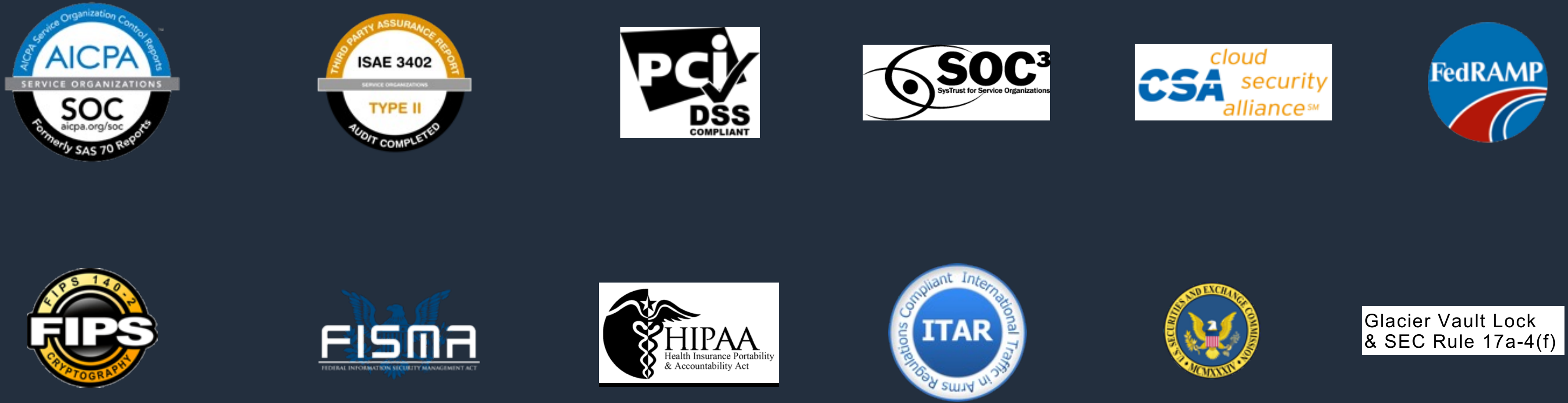
U.S. SECURITIES AND EXCHANGE COMMISSION
MCMXXXIV

CDC

GE

Pfizer

Broad Accreditations & Certifications

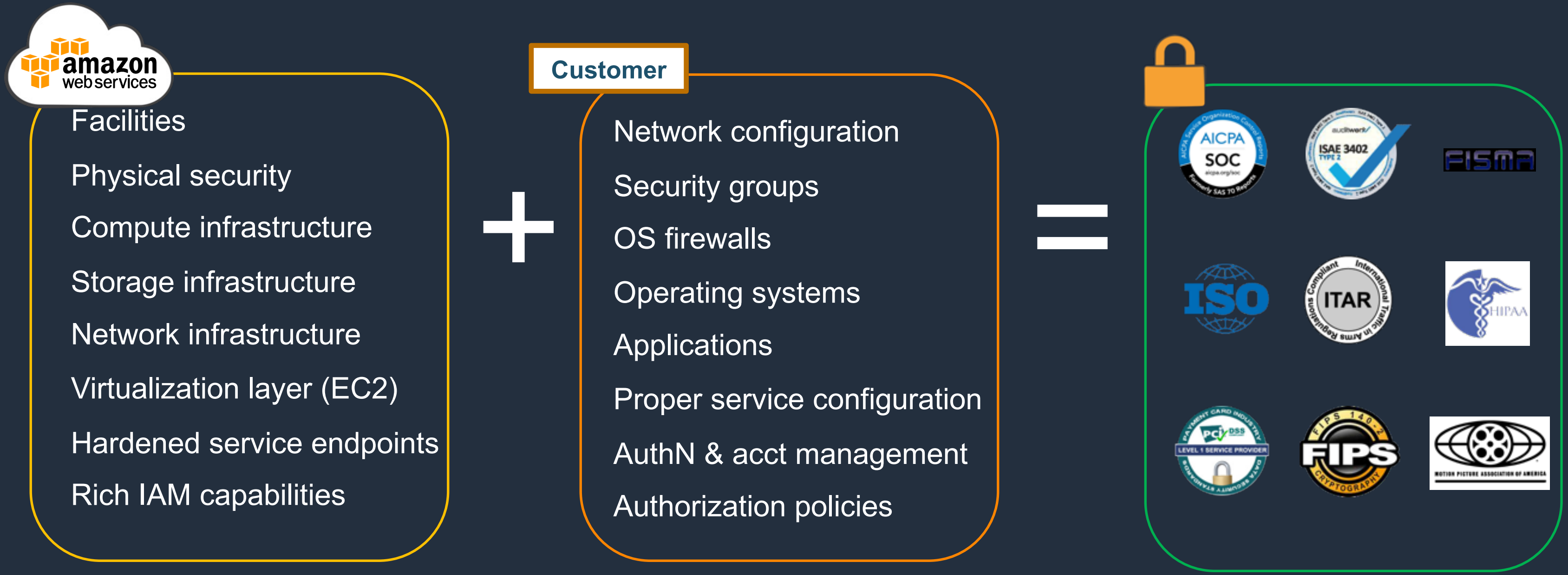

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports
THIRD PARTY ASSURANCE REPORT
ISAE 3402
SERVICE ORGANIZATIONS
TYPE II
AUDIT COMPLETED
PCI DSS COMPLIANT
SOC3
SysTrust for Service Organizations
CSA cloud security alliance
FedRAMP
FIPS 140-2
FIPS
CRYPTOGRAPHY
FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
HIPAA
Health Insurance Portability & Accountability Act
Compliant International Traffic in Arms Regulations
ITAR
U.S. SECURITIES AND EXCHANGE COMMISSION
MCMXXXIV

Glacier Vault Lock
& SEC Rule 17a-4(f)

See https://aws.amazon.com/compliance/programs/ for full list

Shared Responsibility Model

AWS Shared Responsibility Model



amazon web services

- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualization layer (EC2)
- Hardened service endpoints
- Rich IAM capabilities

+

Customer

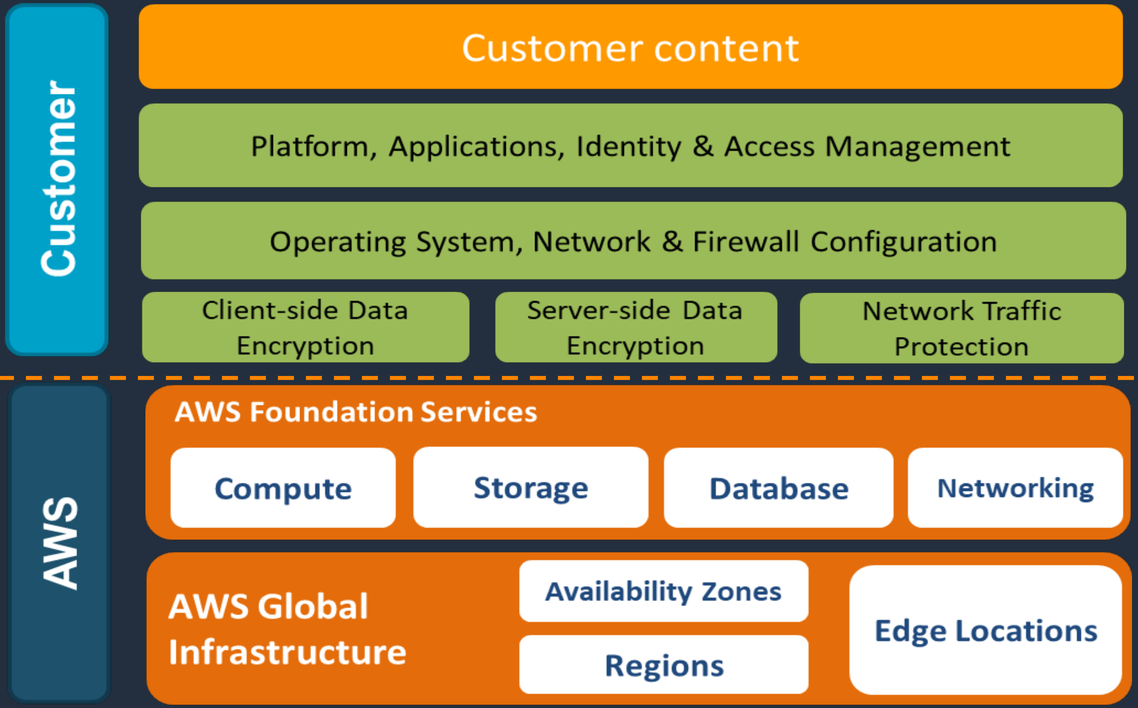
- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Applications
- Proper service configuration
- AuthN & acct management
- Authorization policies

=

AICPA SOC
ISAE 3402 TYPE 2
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: **Infrastructure, Container, Abstracted Services**
- Understanding who is responsible for what is critical to ensuring your AWS data and systems are secure!

Shared Responsibility Model



Customer

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

AWS

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

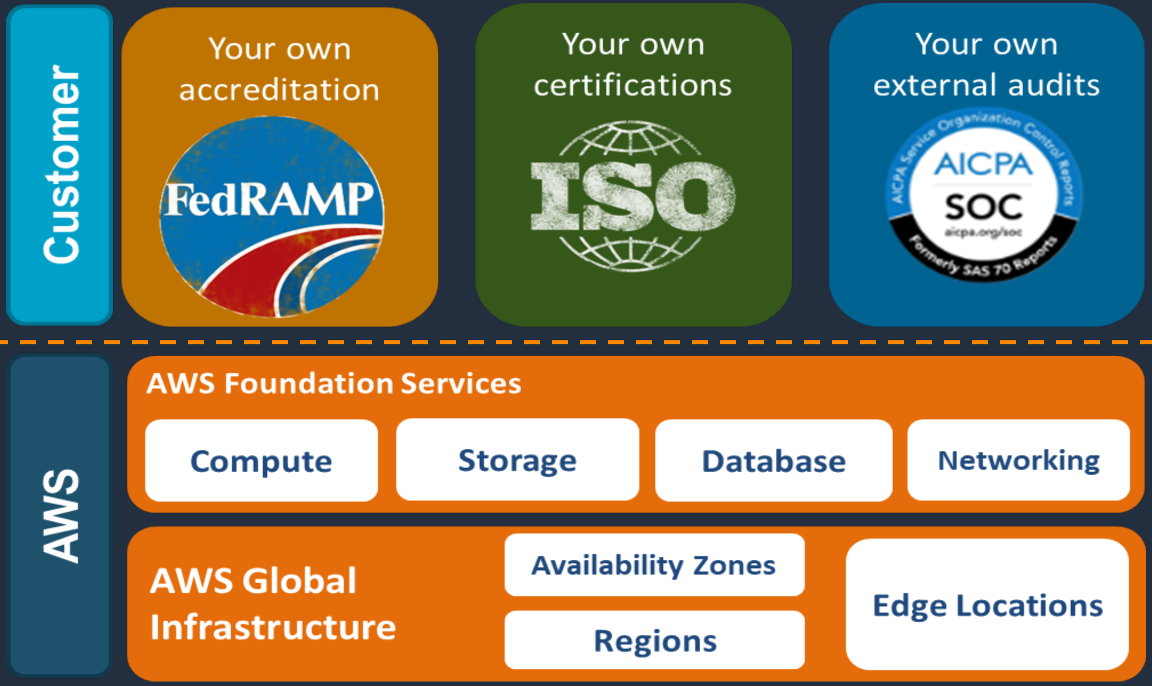
Regions

Edge Locations

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

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

Meet your own security objectives



Customer

Your own accreditation

Your own certifications

Your own external audits

AWS

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

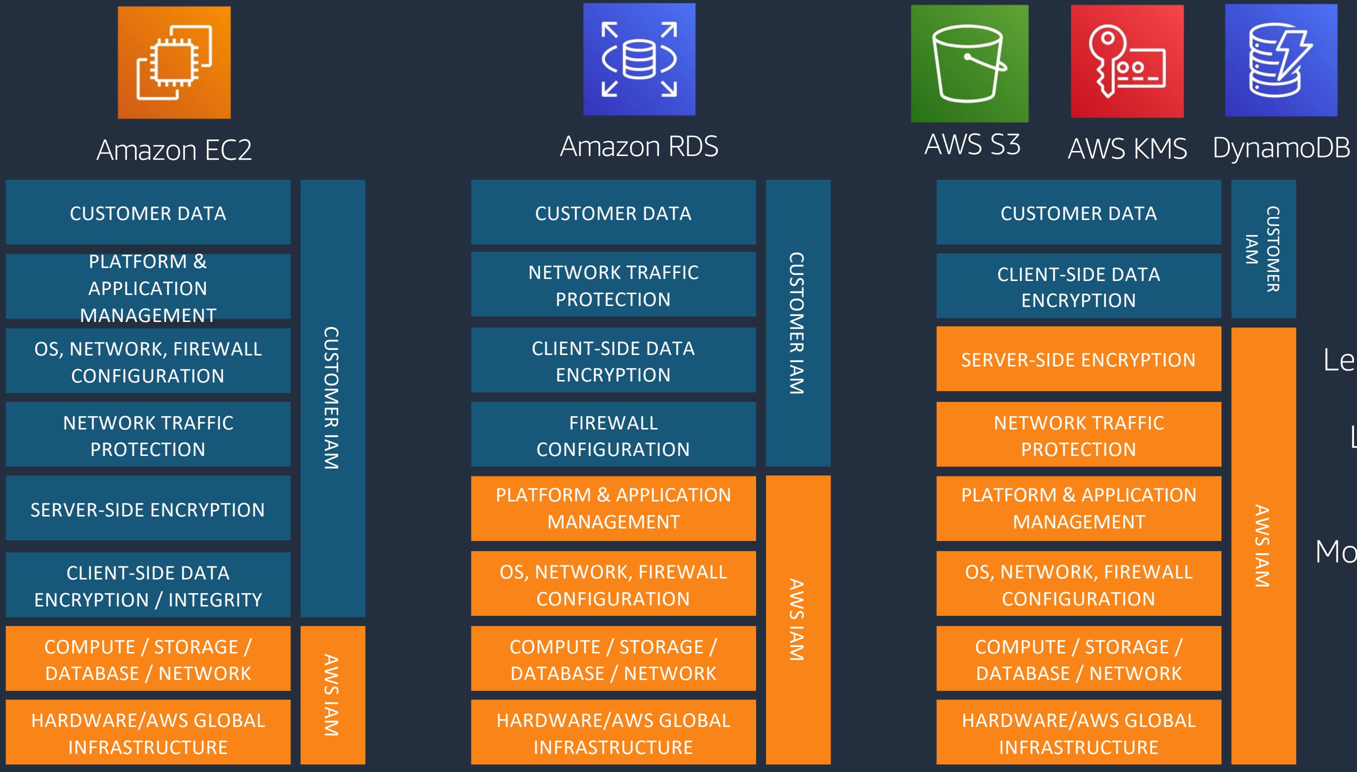
Customer scope and effort is reduced

Better results through focused efforts

Built on AWS consistent baseline controls

The Line Varies ...

More Customizable
+
More Customer
Responsibility



Amazon EC2

CUSTOMER DATA

PLATFORM & APPLICATION MANAGEMENT

OS, NETWORK, FIREWALL CONFIGURATION

NETWORK TRAFFIC PROTECTION

SERVER-SIDE ENCRYPTION

CLIENT-SIDE DATA ENCRYPTION / INTEGRITY

COMPUTE / STORAGE / DATABASE / NETWORK

HARDWARE/AWS GLOBAL INFRASTRUCTURE

CUSTOMER IAM

AWS IAM

Amazon RDS

CUSTOMER DATA

NETWORK TRAFFIC PROTECTION

CLIENT-SIDE DATA ENCRYPTION

FIREWALL CONFIGURATION

PLATFORM & APPLICATION MANAGEMENT

OS, NETWORK, FIREWALL CONFIGURATION

COMPUTE / STORAGE / DATABASE / NETWORK

HARDWARE/AWS GLOBAL INFRASTRUCTURE

CUSTOMER IAM

AWS IAM

AWS S3 AWS KMS DynamoDB

CUSTOMER DATA

CLIENT-SIDE DATA ENCRYPTION

SERVER-SIDE ENCRYPTION

NETWORK TRAFFIC PROTECTION

PLATFORM & APPLICATION MANAGEMENT

OS, NETWORK, FIREWALL CONFIGURATION

COMPUTE / STORAGE / DATABASE / NETWORK

HARDWARE/AWS GLOBAL INFRASTRUCTURE

CUSTOMER IAM

AWS IAM

Less Customizable
+
Less Customer
Responsibility
+
More Best Practices
built-in

Infrastructure
Services

Container
Services

Abstracted
Services

AWS Responsibilities

Physical Security of Data Center

- **Amazon has been building large-scale data centers for many years.**
- **Important attributes:**
  - Non-descript facilities
  - Robust perimeter controls
  - Strictly controlled physical access
  - Two or more levels of two-factor authentication
- **Controlled, need-based access.**
- **All access is logged and reviewed.**
- **Separation of Duties**
  - Employees with physical access don’t have logical privileges.

AWS Responsibilities

EC2 Security

- **Host (hypervisor) operating system**
  - Individual SSH keyed logins via bastion host for AWS admins
  - All accesses logged and audited
- **Guest (EC2 Instance) operating system**
  - Customer controlled (customer owns root/admin)
  - AWS admins cannot log in
  - Customer-generated keypairs
- **Stateful firewall**
  - Mandatory inbound firewall, default deny mode
  - Customer controls configuration via Security Groups

Network Security

- IP Spoofing prohibited at host OS level.
- Packet sniffing (promiscuous mode) is ineffective (protected at hypervisor level).
- Unauthorized Port Scanning a violation of TOS and is detected/blocked.
- Inbound ports blocked by default.

AWS Responsibilities

Configuration Management

- Most updates are done in such a manner that they will not impact the customer.
- Changes are authorized, logged, tested, approved, and documented.
- AWS will communicate with customers, either via email, the AWS Service Health Dashboard (http://status.aws.amazon.com/), or the AWS Personal Health Dashboard (https://phd.aws.amazon.com/) when there is a potential for service being affected.

Built for "Continuous Availability"

- **Scalable, fault tolerant services.**
- **All availability zones (AZs) are always on.**
  - There is no "Disaster Recovery Datacenter"
  - All managed to the same standards
- **Robust Internet connectivity**
  - Each AZ has redundant, Tier 1 ISP Service Providers
  - Resilient network infrastructure

Identity and Access Management

What is Identity Management?

"…the management of individual **principals**, their **authentication**, **authorization**, and **privileges**

…with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks."

(Wikipedia)

Identity and access management

Define, enforce, and audit user permissions across AWS services, actions, and resources

AWS Identity and Access Management (IAM)

Securely manage access to AWS services and resources

AWS IAM Identity Center (successor to AWS SSO)

Centrally manage workforce access to multiple AWS accounts and business apps

AWS Directory Service

Managed Microsoft Active Directory in AWS

Amazon Cognito

Add user sign-up, sign-in, and access control to your web and mobile apps

AWS Organizations

Policy-based management for multiple AWS accounts

AWS Resource Access Manager

Simple, secure service for sharing AWS resources

AAA with AWS

Authenticate	Authorize	Audit
IAM Username/Password Access Key (+ MFA) Federation	IAM Policies	CloudTrail

Considerations for Layers of Principals

Applications

- Identities: Application Users, Application Administrators

Operating Systems

- Identities: Developers, and/or Systems Engineers

Amazon Web Services

- Identities: Developers, Solutions Architects, Testers, Software/Platform
- Interaction of AWS Identities:
  - Provisioning/deprovisioning EC2 instances and EBS storage.
  - Configuring Elastic Load Balancers.
  - Accessing S3 Objects or data in DynamoDB.
  - Accessing data in DynamoDB.
  - Interacting with SQS queues.
  - Sending SNS notifications.

AWS Principals

Account Owner ID (Root Account)

- Access to all subscribed services.
- Access to billing.
- Change Account settings, change AWS support plan, close AWS account.
- Register as a seller, sign up for GovCloud.

IAM Users, Groups and Roles

- Access to specific services.
- Access to console and/or APIs.
- Access to Customer Support (Business and Enterprise).

Temporary Security Credentials

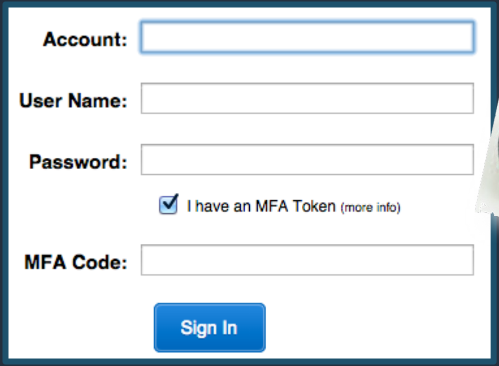
- Access to specific services.
- Access to console and/or APIs.

AWS Identity Authentication

AUTHENTICATION: HOW DO WE KNOW YOU ARE WHO YOU SAY YOU ARE?

AWS Management Console

Login with **Username/Password** with optional **MFA** (recommended)



Account:

User Name:

Password:

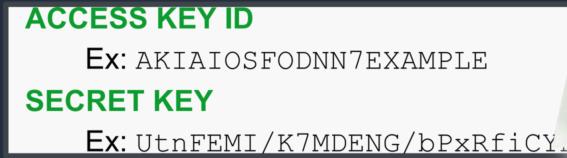
☑ I have an MFA Token (more info)

MFA Code:

For time-limited access: **a Signed URL can** provide temporary access to the Console

API access

Access API using **Access Key + Secret Key**, with optional MFA



ACCESS KEY ID

Ex: `AKIAIOSFODNN7EXAMPLE`

SECRET KEY

Ex: `UtnFEMI/K7MDENG/bPxRfiCY`

For time-limited access: Call the AWS Security Token Service (STS) to get a temporary AccessKeyId + SecretAccessKey + SessionToken

AWS Authorization and Privileges

AUTHORIZATION: WHAT ARE YOU ALLOWED TO DO?

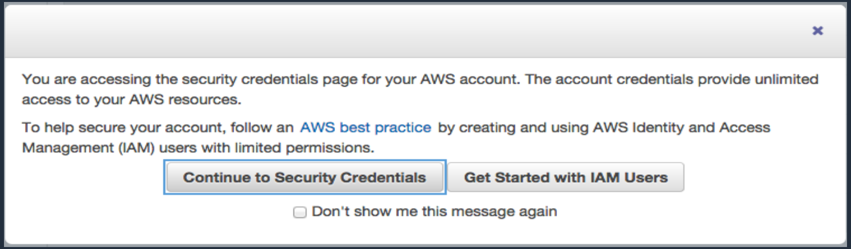
Account Owner (Root)

- Privileged for all actions.

Note: *Always associate the account owner ID with an MFA device and store it in a secured place!*

IAM Policies

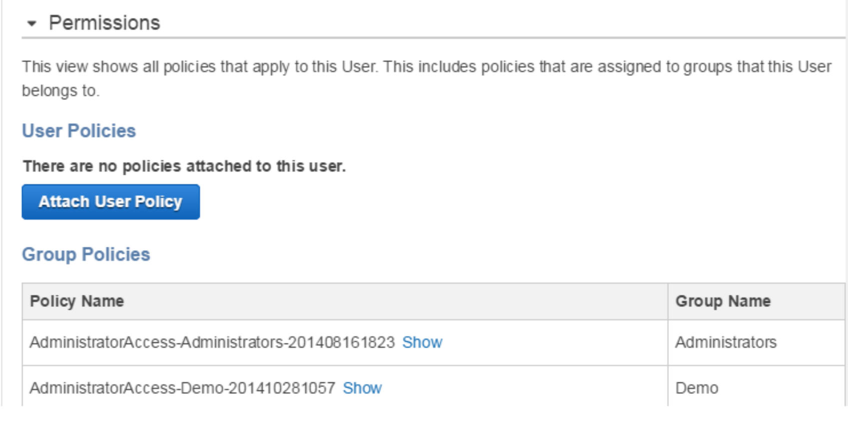
- Privileges defined at User and Resource Level



You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an AWS best practice by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

Continue to Security Credentials
Get Started with IAM Users
□ Don't show me this message again



Permissions

This view shows all policies that apply to this User. This includes policies that are assigned to groups that this User belongs to.

User Policies

There are no policies attached to this user.

Group Policies

Policy Name	Group Name
AdministratorAccess-Administrators-201408161823 Show	Administrators
AdministratorAccess-Demo-201410281057 Show	Demo

Data Protection

Data protection

In addition to using automatic data encryption and management services, you can employ more features

for data protection

(including data management, data security, and encryption key storage)

Amazon Macie

Discover and protect your sensitive data at scale

AWS Key Management Service (AWS KMS)

Easily create and control the keys used to encrypt your data

AWS CloudHSM

Managed hardware security module on the AWS Cloud

AWS Certificate Manager

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services

AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle

AWS VPN

Extend your on-premises networks to the cloud and securely access them from anywhere

Server-Side Encryption

Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys

Encryption

PROTECTING DATA IN-TRANSIT & AT-REST (AND IN-USE).

Encryption In-Transit

- HTTPS
- SSL/TLS
- VPN / IPSEC
- SSH

Encryption At-Rest

- Object
- Database
- Filesystem
- Disk

More Details about encryption can be found in this whitepaper: Encrypting Data-at-Rest and -in-Transit

Encryption at Rest

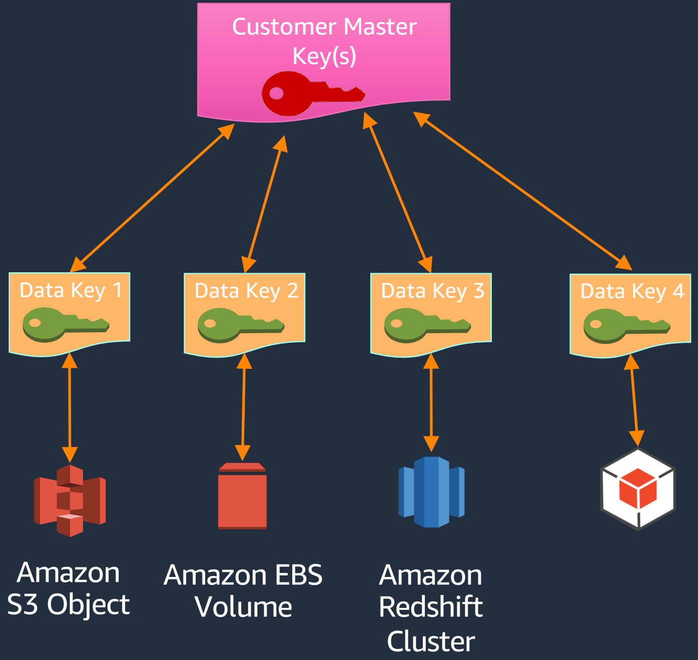
Volume Encryption	EBS Encryption	Filesystem Tools	AWS Marketplace/Partner		
Object Encryption	S3 Server Side Encryption (SSE)	S3 SSE w/ Customer Provided Keys	Client-Side Encryption		
Database Encryption	RDS MSSQL TDE	RDS ORACLE TDE/HSM	RDS MYSQL KMS	RDS PostgreSQL KMS	Redshift Encryption

AWS Certificate Manager

A service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

AWS Key Management Service

MANAGED SERVICE TO CREATE AND MANAGE CRYPTOGRAPHIC KEYS AND CONTROL THEIR USE ACROSS A WIDE RANGE OF AWS SERVICES AND IN YOUR APPLICATIONS.

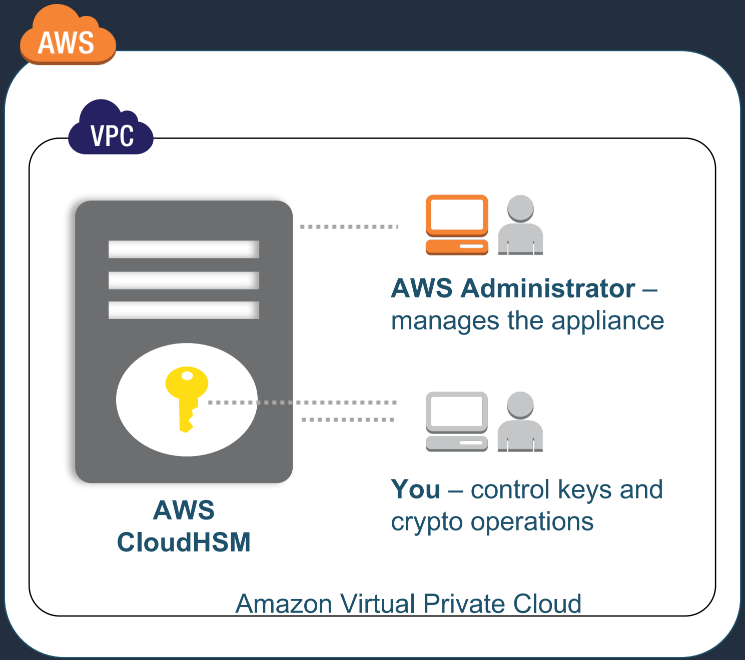


AWS CloudHSM

HELP MEET COMPLIANCE REQUIREMENTS FOR DATA SECURITY BY USING A DEDICATED HARDWARE SECURITY MODULE APPLIANCE WITH AWS.

- Dedicated, single-tenant hardware device
- Can be deployed as HA and load balanced

- Customer use cases:
  - Oracle TDE
  - MS SQL Server TDE
  - Setup SSL connections
  - Digital Rights Management (DRM)
  - Document Signing


AWS
VPC
AWS Administrator – manages the appliance
You – control keys and crypto operations
AWS CloudHSM
Amazon Virtual Private Cloud

Detective Controls

Detective controls

Gain the visibility you need to spot issues before they impact your business, improve your security posture, and reduce the risk profile of your environment

AWS Security Hub

Centrally view and manage security alerts & automate compliance checks.

Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads.

Amazon Inspector

Automates security assessments to help improve the security and compliance of applications deployed on AWS.

Amazon CloudWatch

Complete visibility of your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes.

AWS Config

Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, and security analysis.

AWS CloudTrail

Track user activity and API usage to enable governance, compliance, and operational and risk auditing of your AWS account.

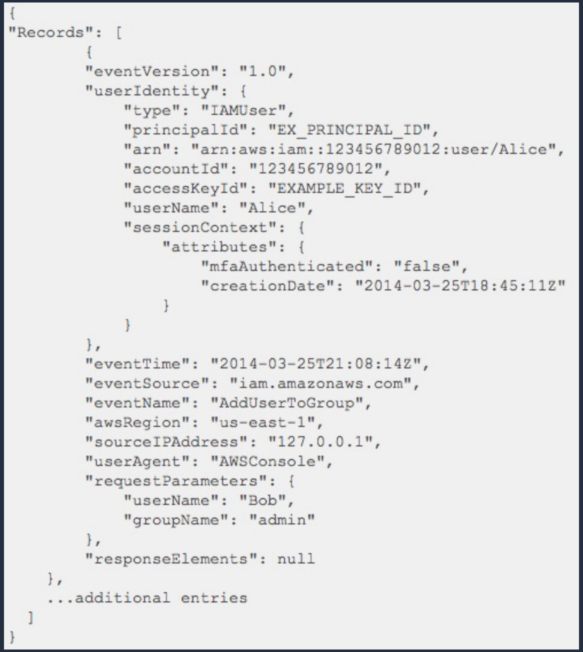
VPC Flow Logs

Capture info about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs.

AWS CloudTrail

CLOUDTRAIL PROVIDES EVENT HISTORY OF YOUR AWS ACCOUNT ACTIVITY, INCLUDING ACTIONS TAKEN THROUGH THE AWS MANAGEMENT CONSOLE, AWS SDKS, COMMAND LINE TOOLS, AND OTHER AWS SERVICES.

Who?	When?	What?	Where to?	Where from?
Bill	3:27pm	Launch Instance	us-west-2	72.21.198.64
Alice	8:19am	Added Bob to admin group	us-east-1	127.0.0.1
Steve	2:22pm	Deleted DynamoDB table	eu-west-1	205.251.233.176



```
{
"Records": [
        {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-03-25T18:45:11Z"
                }
            }
        },
        "eventTime": "2014-03-25T21:08:14Z",
        "eventSource": "iam.amazonaws.com",
        "eventName": "AddUserToGroup",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "AWSConsole",
        "requestParameters": {
            "userName": "Bob",
            "groupName": "admin"
        },
        "responseElements": null
    },
    ...additional entries
  ]
}
```

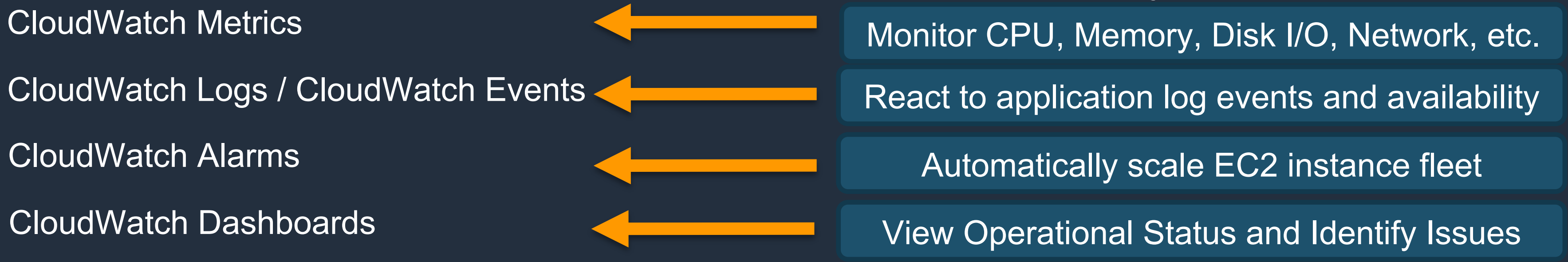
AWS CloudWatch

MONITORING SERVICES FOR AWS RESOURCES AND AWS-BASED APPLICATIONS.

What does it do?

- Collect and Track Metrics
- Monitor and Store Logs
- Set Alarms (react to changes)
- View Graphs and Statistics

How can you use it?



CloudWatch Metrics ← Monitor CPU, Memory, Disk I/O, Network, etc.

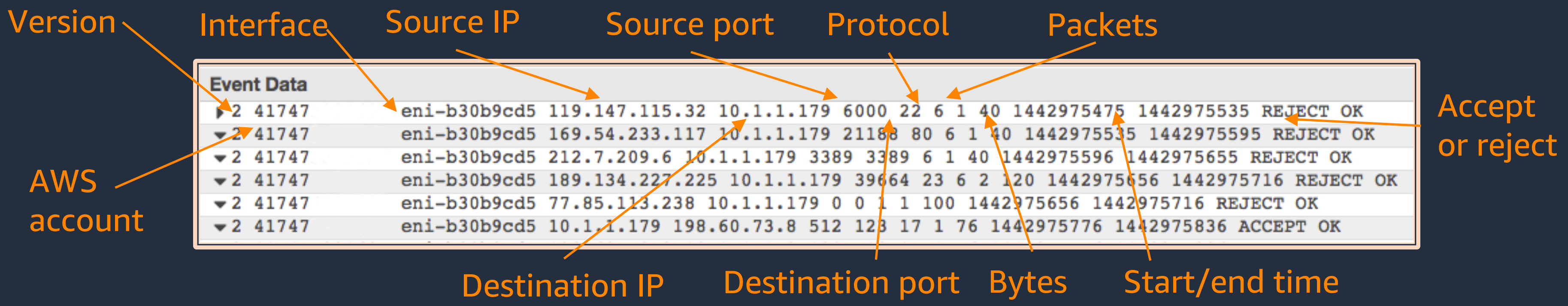
CloudWatch Logs / CloudWatch Events ← React to application log events and availability

CloudWatch Alarms ← Automatically scale EC2 instance fleet

CloudWatch Dashboards ← View Operational Status and Identify Issues

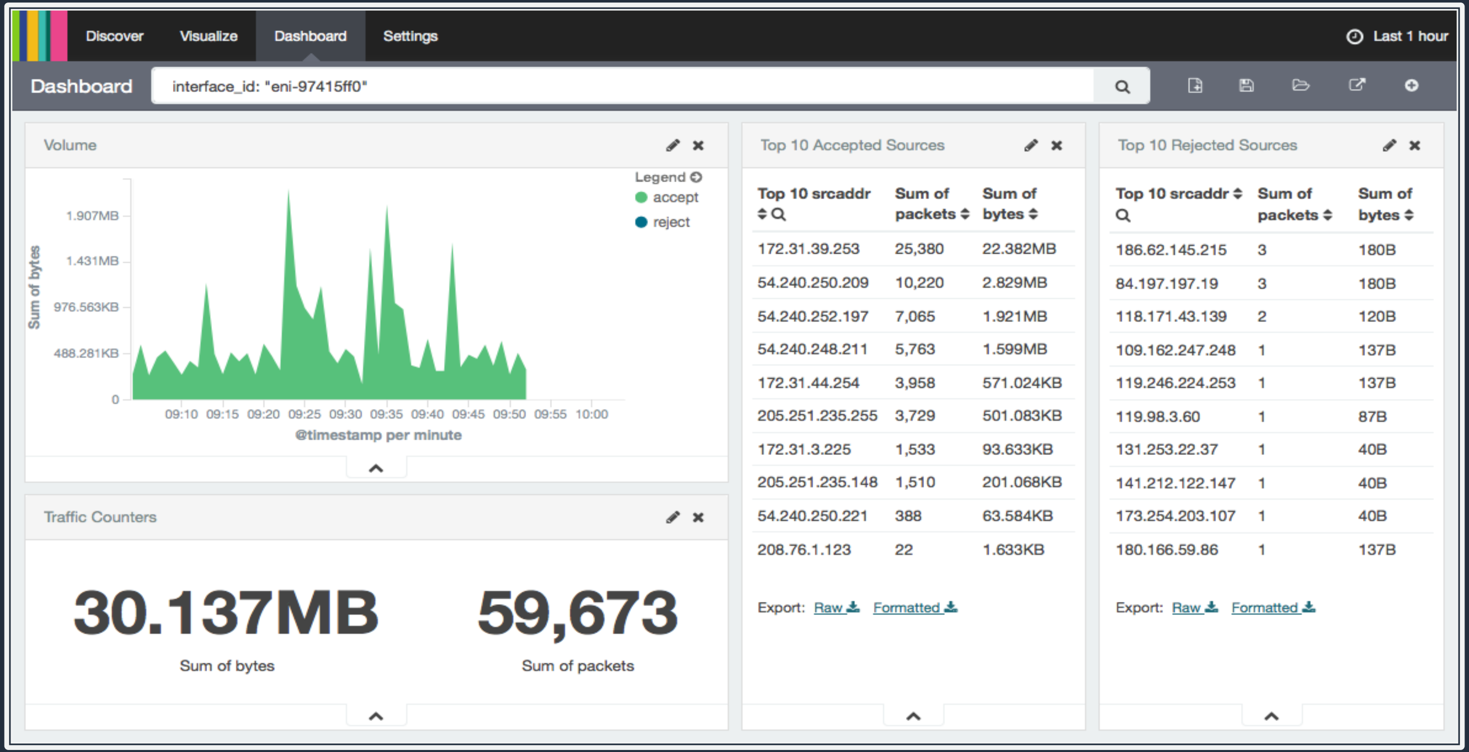
VPC Flow Logs

- 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
```

VPC Flow Logs



interface_id: "eni-97415ff0"

Traffic Counters

30.137MB
Sum of bytes

59,673
Sum of packets

Top 10 Accepted Sources

Top 10 srcaddr	Sum of packets	Sum of bytes
172.31.39.253	25,380	22.382MB
54.240.250.209	10,220	2.829MB
54.240.252.197	7,065	1.921MB
54.240.248.211	5,763	1.599MB
172.31.44.254	3,958	571.024KB
205.251.235.255	3,729	501.083KB
172.31.3.225	1,533	93.633KB
205.251.235.148	1,510	201.068KB
54.240.250.221	388	63.584KB
208.76.1.123	22	1.633KB

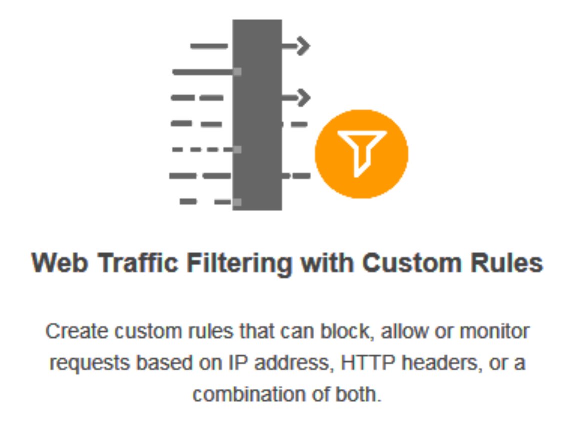
Export: Raw Formatted

Top 10 Rejected Sources

Top 10 srcaddr	Sum of packets	Sum of bytes
186.62.145.215	3	180B
84.197.197.19	3	180B
118.171.43.139	2	120B
109.162.247.248	1	137B
119.246.224.253	1	137B
119.98.3.60	1	87B
131.253.22.37	1	40B
141.212.122.147	1	40B
173.254.203.107	1	40B
180.166.59.86	1	137B

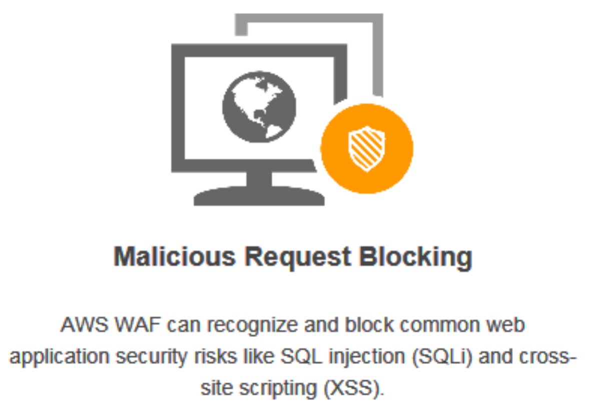
Export: Raw Formatted

AWS WAF (Web Application Firewall)



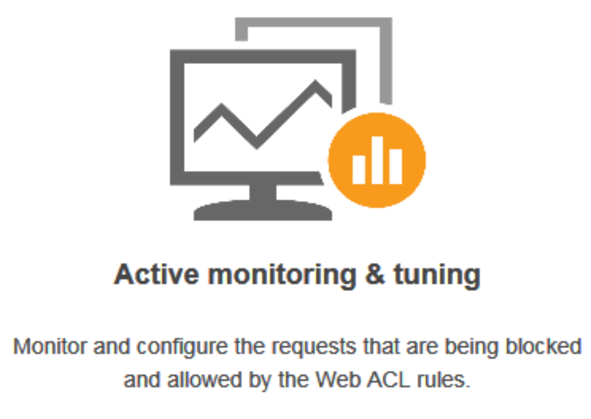
Web Traffic Filtering with Custom Rules

Create custom rules that can block, allow or monitor requests based on IP address, HTTP headers, or a combination of both.



Malicious Request Blocking

AWS WAF can recognize and block common web application security risks like SQL injection (SQLi) and cross-site scripting (XSS).

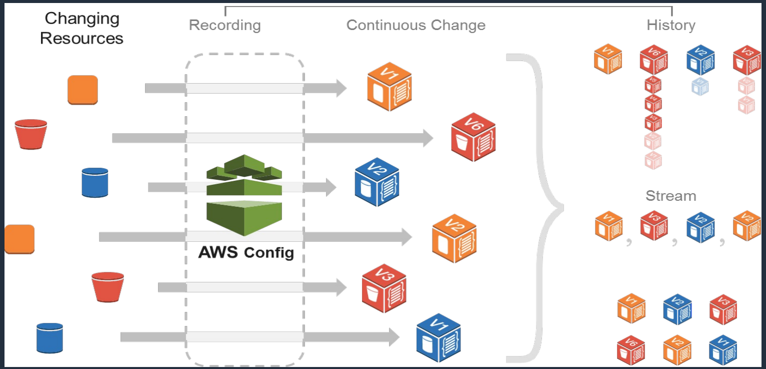


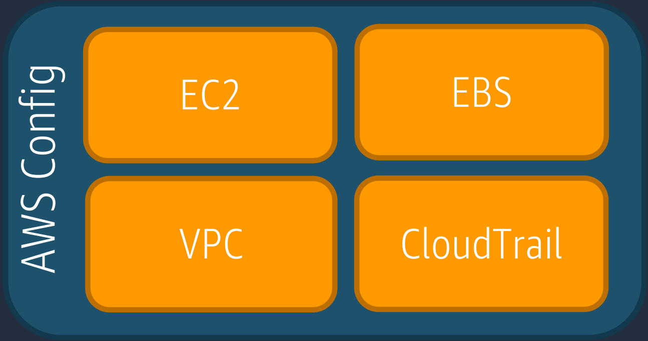
Active monitoring & tuning

Monitor and configure the requests that are being blocked and allowed by the Web ACL rules.

AWS Config

MANAGED SERVICE FOR TRACKING AWS INVENTORY AND CONFIGURATION, AND CONFIGURATION CHANGE NOTIFICATION.





AWS Config

EC2

EBS

VPC

CloudTrail

Security Analysis

Audit Compliance

Change Management

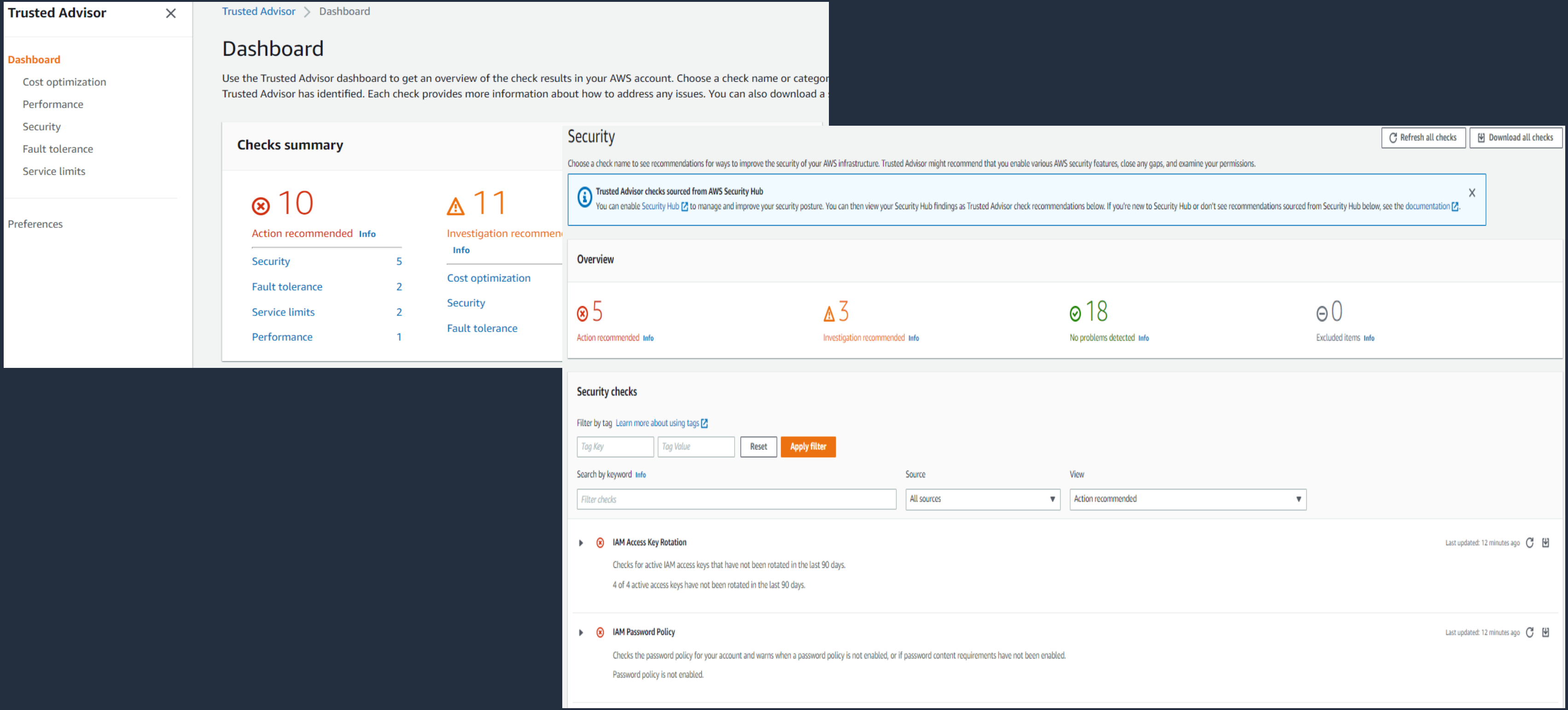
Troubleshooting

Discovery

Additional Best Practices

AWS Trusted Advisor

LEVERAGE TRUSTED ADVISOR TO ANALYZE YOUR AWS RESOURCES FOR BEST PRACTICES FOR AVAILABILITY, COST, PERFORMANCE AND SECURITY.



Dashboard

Use the Trusted Advisor dashboard to get an overview of the check results in your AWS account. Choose a check name or categor
Trusted Advisor has identified. Each check provides more information about how to address any issues. You can also download a

Checks summary

⊗ 10 Action recommended Info

Security	5
Fault tolerance	2
Service limits	2
Performance	1

⚠ 11 Investigation recommen Info

Cost optimization
Security
Fault tolerance

Security

Choose a check name to see recommendations for ways to improve the security of your AWS infrastructure. Trusted Advisor might recommend that you enable various AWS security features, close any gaps, and examine your permissions.

Trusted Advisor checks sourced from AWS Security Hub
You can enable Security Hub to manage and improve your security posture. You can then view your Security Hub findings as Trusted Advisor check recommendations below. If you're new to Security Hub or don't see recommendations sourced from Security Hub below, see the documentation.

Overview

⊗ 5 Action recommended Info
⚠ 3 Investigation recommended Info
✓ 18 No problems detected Info
⊖ 0 Excluded items Info

Security checks

Filter by tag Learn more about using tags

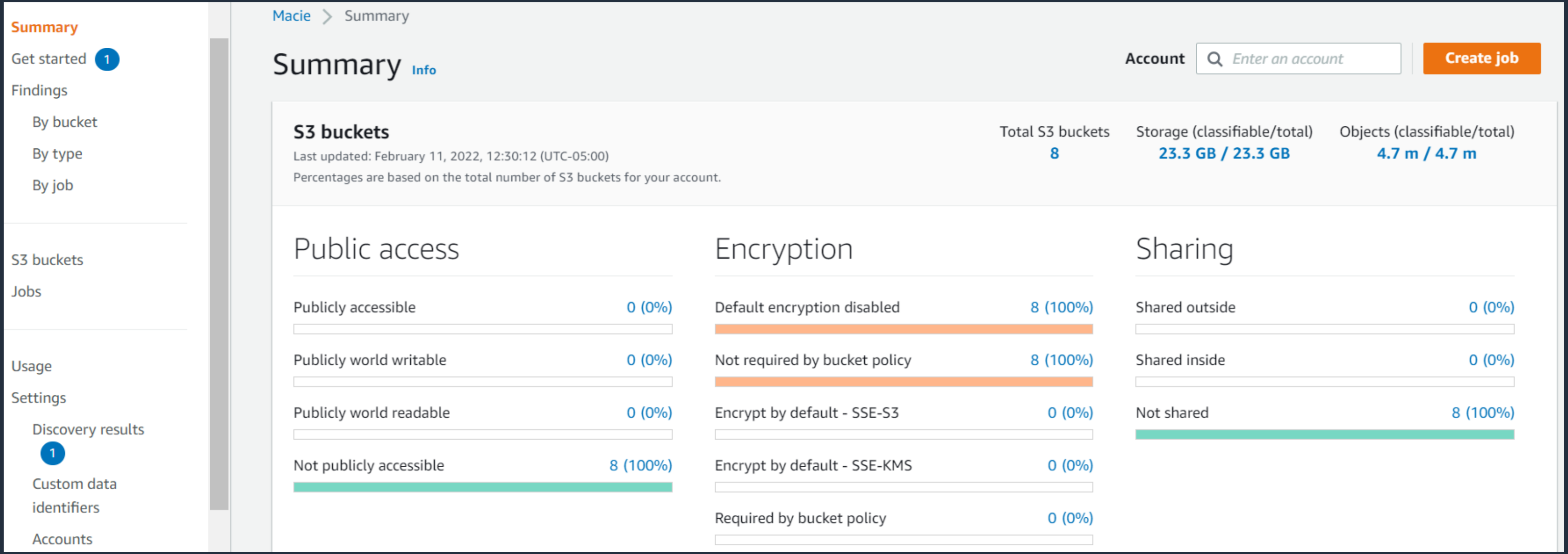
Search by keyword Info: Filter checks
Source: All sources ▼
View: Action recommended ▼

⊗ IAM Access Key Rotation — Last updated: 12 minutes ago
Checks for active IAM access keys that have not been rotated in the last 90 days.
4 of 4 active access keys have not been rotated in the last 90 days.

⊗ IAM Password Policy — Last updated: 12 minutes ago
Checks the password policy for your account and warns when a password policy is not enabled, or if password content requirements have not been enabled.
Password policy is not enabled.

Amazon Macie

LEVERAGE AMAZON MACIE TO HELP PREVENT DATA LOSS IN AWS.



Summary Info

S3 buckets

Last updated: February 11, 2022, 12:30:12 (UTC-05:00)

Percentages are based on the total number of S3 buckets for your account.

Total S3 buckets	Storage (classifiable/total)	Objects (classifiable/total)
8	23.3 GB / 23.3 GB	4.7 m / 4.7 m

Public access

Publicly accessible	0 (0%)
Publicly world writable	0 (0%)
Publicly world readable	0 (0%)
Not publicly accessible	8 (100%)

Encryption

Default encryption disabled	8 (100%)
Not required by bucket policy	8 (100%)
Encrypt by default - SSE-S3	0 (0%)
Encrypt by default - SSE-KMS	0 (0%)
Required by bucket policy	0 (0%)

Sharing

Shared outside	0 (0%)
Shared inside	0 (0%)
Not shared	8 (100%)

AWS Marketplace Security Partners

Infrastructure Security

- CISCO
- f5
- CITRIX
- SOPHOS
- Barracuda
- FORTINET
- intel Security
- paloalto networks
- Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.
- IMPERVA

Logging & Monitoring

- ALERTLOGIC Security Compliance Cloud
- splunk>
- sumologic
- CloudPassage
- loggly

Identity & Access Control

- okta
- CIPHERGRAPH networks
- Elastic SSO
- conjur
- onelogin

Configuration & Vulnerability Analysis

- QUALYSGUARD
- TREND MICRO
- tenable network security
- RAPID7
- evident.io

Data Protection

- gemalto security to be free
- Vormetric Data Security Simplified
- HYTRUST Cloud Under Control
- KeyNexus
- Townsend SECURITY
- druva

Sovereign-by-Design

An AWS approach

1. Control over the location of your data

2. Verifiable control over data access

Sovereign by design

3. The ability to encrypt everything everywhere

4. Resilience of the cloud

Encryption everywhere

AWS Key Management Service (AWS KMS)

AWS CloudHSM

Ability to encrypt all your data, whether in transit, at rest, or in memory

All services support encryption; most services support encryption with customer managed keys that are inaccessible to AWS

AWS KMS, CloudHSM, and XKS provide customers the ability to manage their keys and encrypt all their data to meet regulatory requirements

AWS Sovereignty Pledge:

We commit to continue to innovate and invest in additional controls for sovereignty and encryption features so that our customers can encrypt everything everywhere with encryption keys managed inside or outside the AWS Cloud.

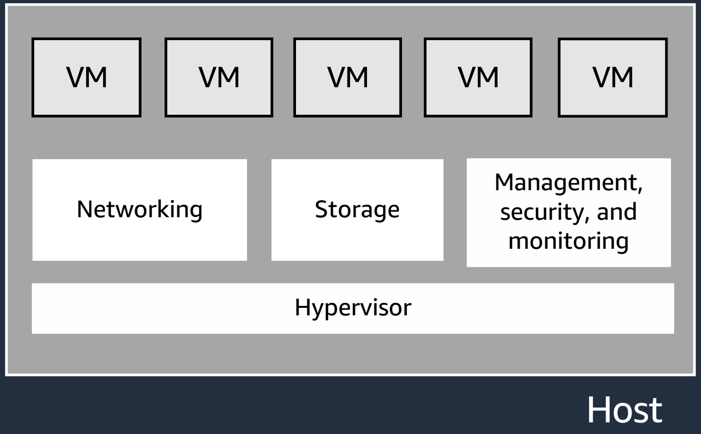
Security standards and compliance certifications

AWS supports more security standards and compliance certifications than any other offering, including FedRAMP, GDPR, C5, CISPE, and NIST 800-171, helping customers satisfy compliance requirements for virtually every regulatory agency around the globe

Access to data

AWS prohibits – and its systems are designed to prevent – remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by customers, is required to prevent fraud and abuse, or to comply with law

Reinventing virtualization for the cloud



VM VM VM VM VM

Networking

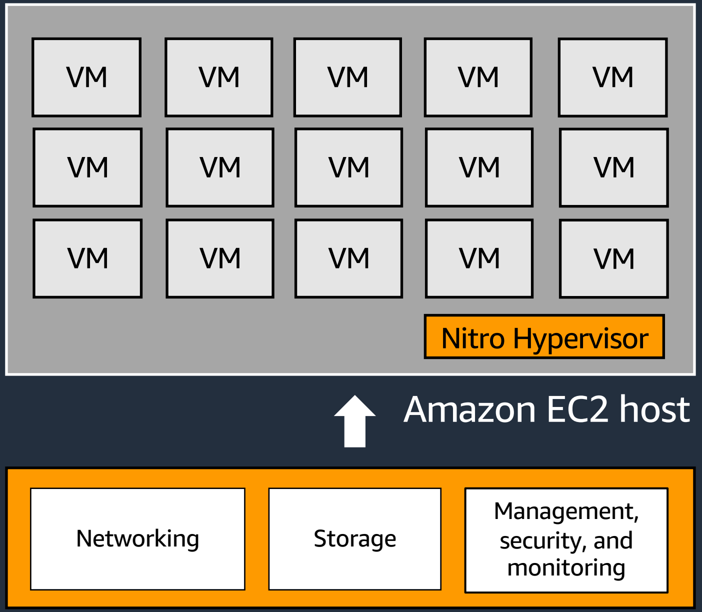
Storage

Management, security, and monitoring

Hypervisor

Host

Classical virtualization



VM VM VM VM VM

VM VM VM VM VM

VM VM VM VM VM

Nitro Hypervisor

Amazon EC2 host

Networking

Storage

Management, security, and monitoring

AWS Nitro System

AWS Nitro System

Nitro Cards

- Local NVMe storage
- Elastic block storage
- Networking, monitoring, and security

Nitro Security Chip

- Integrated into motherboard
- Protects hardware resources

Nitro Hypervisor

- Lightweight hypervisor
- Memory and CPU allocation
- Bare metal-like performance

The Security Overview of the AWS Nitro System whitepaper

- Detailed review of the security design of the three primary components of the AWS Nitro System:
  - Nitro Cards,
  - Nitro Security Chip
  - Nitro Hypervisor
- Deep dive on the AWS Nitro System integrity protections, tenant isolation model, and no operator access design

https://a.co/hYWhsH9

In summary

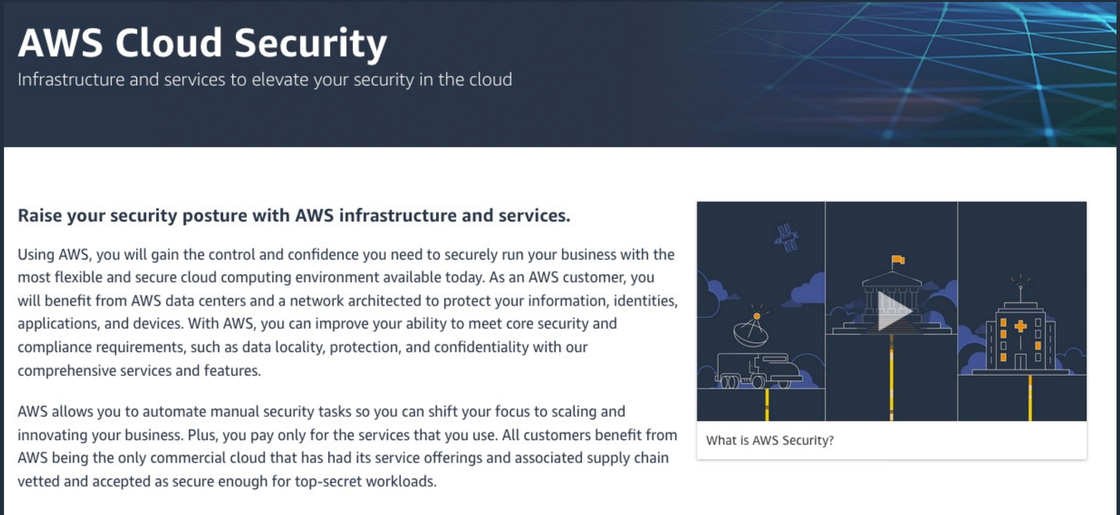
Technical measures

Process measures

Contractual measures

AWS Security Center

COMPREHENSIVE SECURITY PORTAL TO PROVIDE A VARIETY OF SECURITY NOTIFICATIONS, INFORMATION AND DOCUMENTATION.



AWS Cloud Security

Infrastructure and services to elevate your security in the cloud

Raise your security posture with AWS infrastructure and services.

Using AWS, you will gain the control and confidence you need to securely run your business with the most flexible and secure cloud computing environment available today. As an AWS customer, you will benefit from AWS data centers and a network architected to protect your information, identities, applications, and devices. With AWS, you can improve your ability to meet core security and compliance requirements, such as data locality, protection, and confidentiality with our comprehensive services and features.

AWS allows you to automate manual security tasks so you can shift your focus to scaling and innovating your business. Plus, you pay only for the services that you use. All customers benefit from AWS being the only commercial cloud that has had its service offerings and associated supply chain vetted and accepted as secure enough for top-secret workloads.

What is AWS Security?

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

Security Whitepapers

- Overview of Security Process
- AWS Risk and Compliance
- AWS Security Best Practices

Security Bulletin

Security Resources

Vulnerability Reporting

Penetration Testing

Requests

Report Suspicious Emails

Under the AWS Shared Responsibility Model

AWS RESPONSIBILITY? OR CUSTOMER RESPONSIBILITY?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Preventing packet sniffing at the hypervisor level

Patching the operating system with the latest security patches

Shredding disk drives before they leave a datacenter

Securing the internal network inside the AWS datacenters

Installing camera systems to monitor the physical datacenters

Toggling on the Server-side encryption feature for S3 buckets

Under the AWS Shared Responsibility Model

AWS RESPONSIBILITY? OR CUSTOMER RESPONSIBILITY?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Preventing packet sniffing at the hypervisor level

Patching the operating system with the latest security patches

Shredding disk drives before they leave a datacenter

Securing the internal network inside the AWS datacenters

Installing camera systems to monitor the physical datacenters

Toggling on the Server-side encryption feature for S3 buckets

Thank you!

AWS Education & Research Team

Roberta Piscitelli - piscitr@amazon.com
Nikiforos Botis - nbotis@amazon.com
Pavlos Kaimakis - pkaim@amazon.com
Michael Wittel -.mwittel@amazon.com
Vasilios Kotitsas - vasiliko@amazon.com
Marina Arcadieva - arcadiev@amazon.com