



Security Essentials & Best Practices



Overview

Overview of the AWS cloud security concepts such as the AWS Security Center, Shared Responsibility Model, and Identity and Access Management.



AWS Security

What are your perceptions on cloud security?

At AWS, cloud security is job zero.

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

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



Broad Accreditations & Certifications



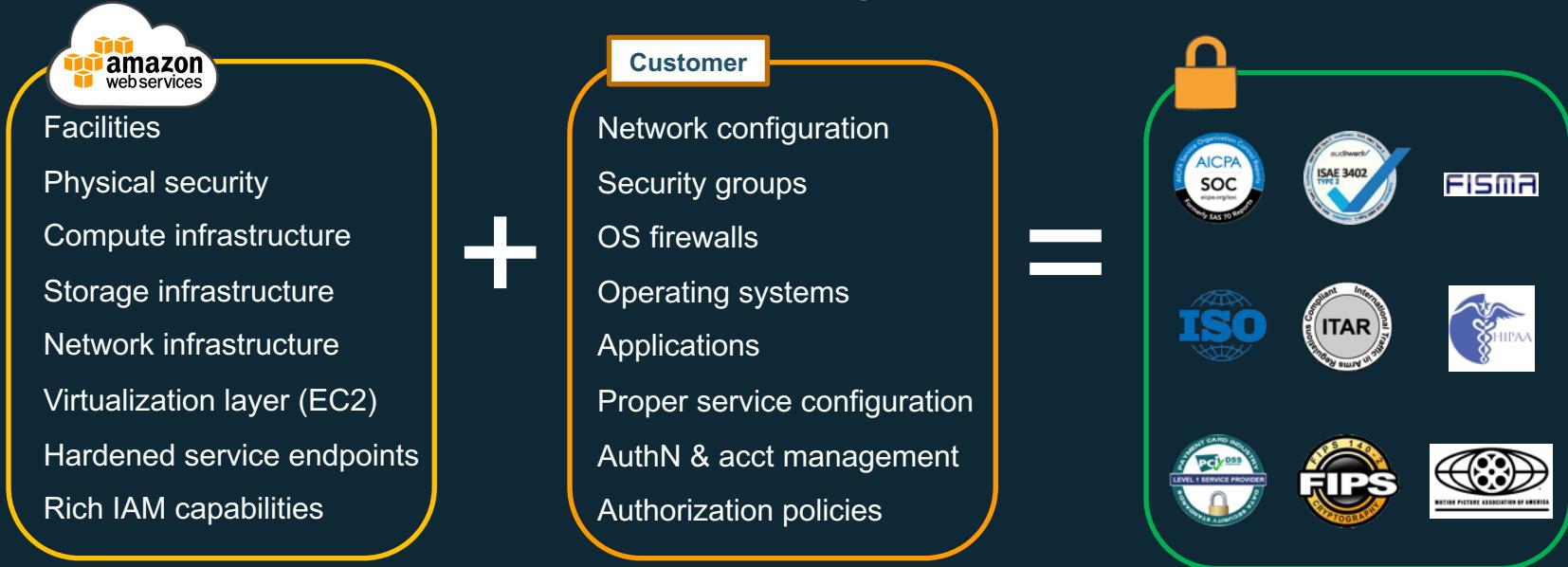
Glacier Vault Lock
& SEC Rule 17a-4(f)

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



Shared
Responsibility Model

AWS Shared Responsibility Model



- 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



Customer scope and effort is reduced

Better results through focused efforts

AWS

AWS Foundation Services

Compute

Storage

Database

Networking

Built on AWS consistent baseline controls

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

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

AWS Responsibilities

Disk Management

- Proprietary disk management prevents customers from accessing each other's data.
- Disks wiped prior to use.
- Disks can also be encrypted by the customer for additional security.

Storage Device Decommissioning

- All storage devices go through process using techniques from:
 - DoD 5220.22-M ("National Industrial Security Program Operating Manual").
 - NIST 800-88 ("Guidelines for Media Sanitization").
- Ultimately devices are:
 - Degaussed.
 - Physically destroyed.

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

Patching the operating system with the latest security patches

Installing camera systems to monitor the physical datacenters

Preventing packet sniffing at the hypervisor level

Shredding disk drives before they leave a datacenter

Toggling on the Server-side encryption feature for S3 buckets

Securing the internal network inside the AWS datacenters



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)

AAA with AWS

Authenticate

IAM Username/Password
Access Key
(+ MFA)
Federation

Authorize

IAM Policies

Audit

CloudTrail

Considerations for Layers of Principals

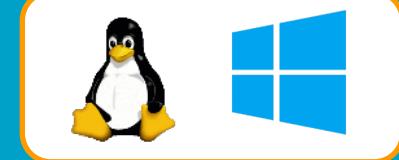
Applications

- 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.

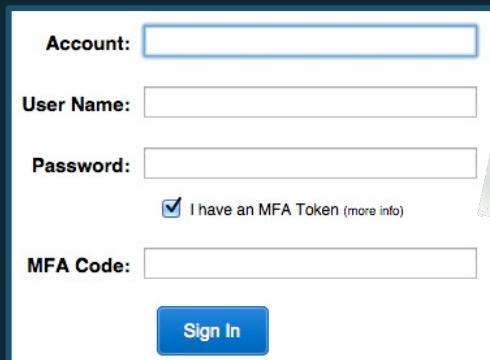


AWS Identity Authentication

Authentication: How do we know you are who you say you are?

AWS Management Console

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



The form contains the following fields:
Account: [Input Field]
User Name: [Input Field]
Password: [Input Field]
 I have an MFA Token ([more info](#))
MFA Code: [Input Field]

Sign In

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: UtnPfEMI/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?

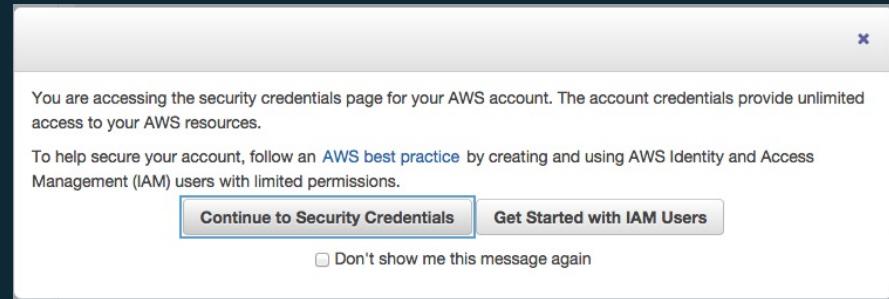
Account Owner (Root)

- 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



▼ 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.

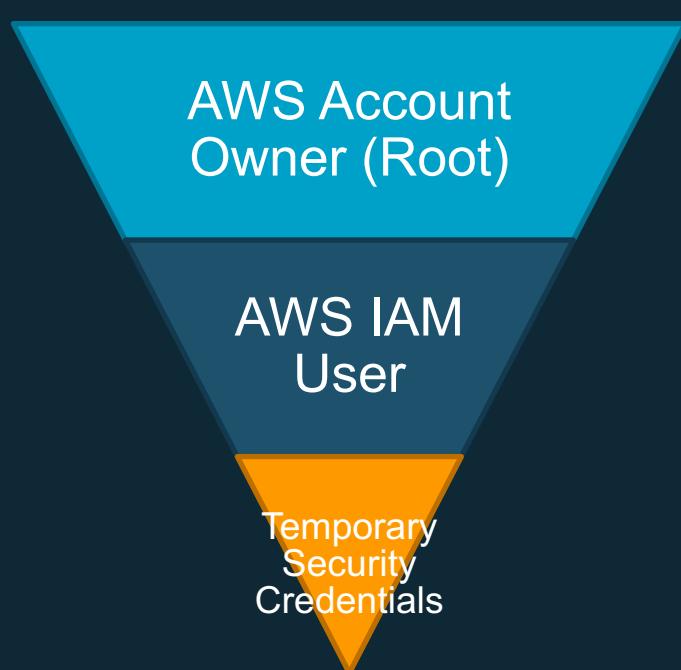
[Attach User Policy](#)

Group Policies

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

AWS IAM Hierarchy of Privileges

Enforce principle of least privilege with Identity and Access Management (IAM) users, groups, and policies and temporary credentials.



Permissions	Example
Unrestricted access to all enabled services and resources.	Action: * Effect: Allow Resource: * (implicit)
Access restricted by Group and User policies	Action: ['s3:*', 'sts:Get*'] Effect: Allow Resource: *
Access restricted by generating identity and further by policies used to generate token	Action: ['s3:Get*'] Effect: Allow Resource: 'arn:aws:s3:::mybucket/*'

AWS Identity and Access Management (IAM)

Securely control access to AWS services and resources for your users.

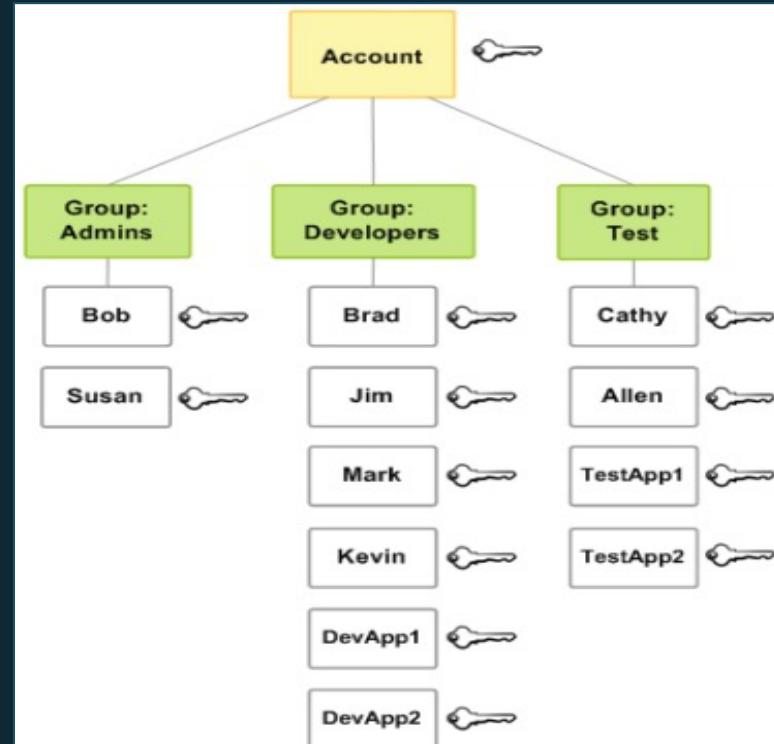
Username/
User

Manage groups
of users

Centralized
Access Control

Optional Configurations:

- Password for console access.
- Policies for controlling access AWS APIs.
- Two methods to sign API calls:
 - X.509 certificate
 - Access/Secret Keys
- Multi-factor Authentication (MFA)



Identity and Access Management

Common approaches for Applications and Operating Systems

Local User Databases

- Local Password (passwd) files
- Local Windows admin accounts
- User Databases



LDAP Directories

- On-premise accessed over VPN.
- Replicated to AWS (read-only or read/write)
- Federated (one-way trusts, ADFS).
- Managed Samba-based directories via AWS Directory Services.





AWS Directory Service

Managed service for Active Directory

Use your existing Corporate Credentials for

- AWS-based applications
- AWS Management Console



Microsoft AD

Based on Microsoft Active Directory in Windows Server 2012 R2. Supports adding trust relationships with on-premises domains. Extend your schema using MS AD



Simple AD

A Microsoft Active-Directory compatible directory powered by Samba 4.



AD Connector

Connect to your on-premises Active Directory. Integrates with existing RADIUS MFA solutions.



Encryption

How are you currently encrypting your data?

Encryption

Protecting data in-transit and at-rest.



Encryption In-Transit

HTTPS

SSL/TLS

VPN / IPSEC

SSH

Encryption At-Rest

Object

Database

Filesystem

Disk

*Details about encryption can be found in the AWS Whitepaper,
[“Securing Data at Rest with Encryption”](#).*

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

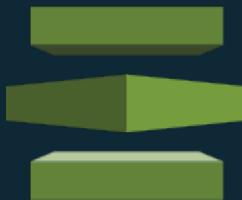
RDS
ORACLE
TDE/HSM

RDS
MYSQL
KMS

RDS
PostgreSQL
KMS

Redshift
Encryption

AWS Certificate Manager

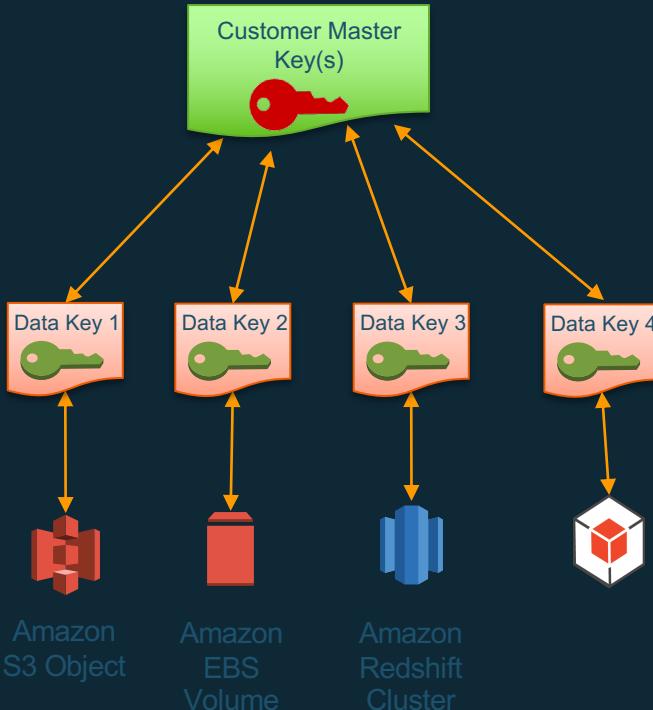


A service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

AWS Key Management Service



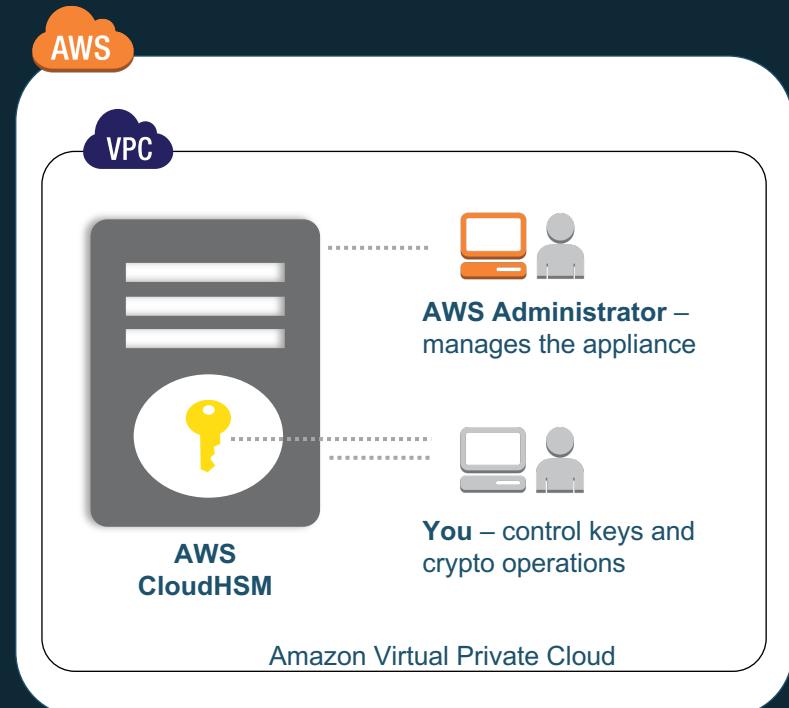
Managed service to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications.



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





Configuration Management

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?

Monitor CPU, Memory, Disk I/O, Network, etc.

CloudWatch Metrics

React to application log events and availability

CloudWatch Logs / CloudWatch Events

Automatically scale EC2 instance fleet

CloudWatch Alarms

View Operational Status and Identify Issues

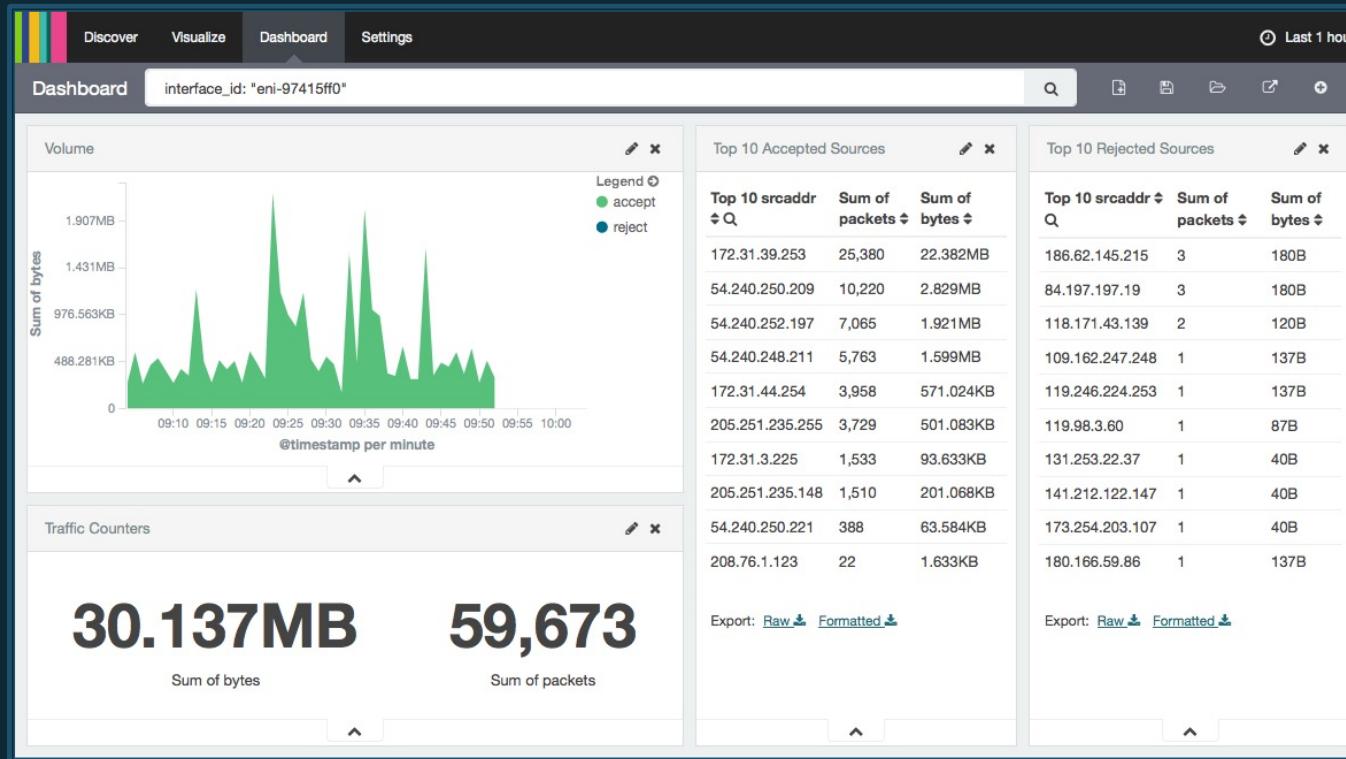
CloudWatch Dashboards

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

Version	Interface	Source IP	Source port	Protocol	Packets	
AWS account	Event Data					Accept or reject
▼ 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	1 100 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



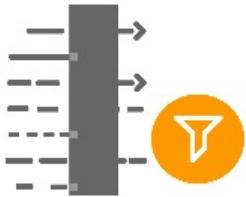
- Amazon Elasticsearch Service
- Amazon CloudWatch Logs subscriptions

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



AWS WAF



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).

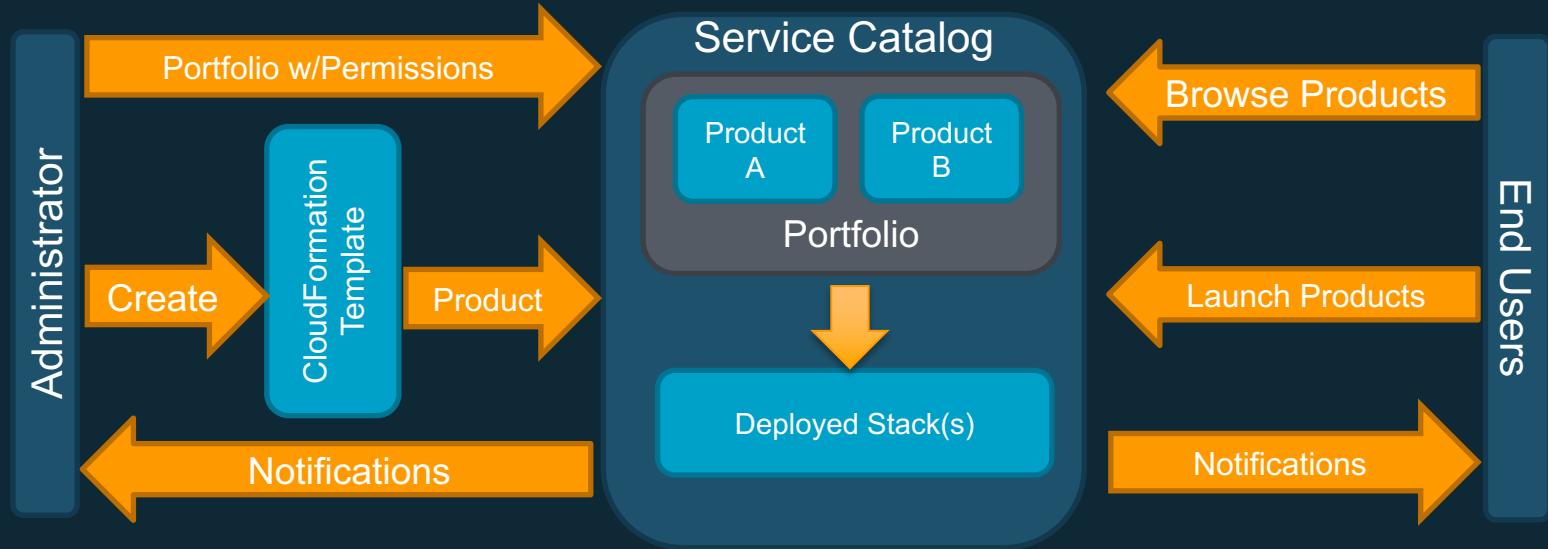


Active monitoring & tuning

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

AWS Service Catalog

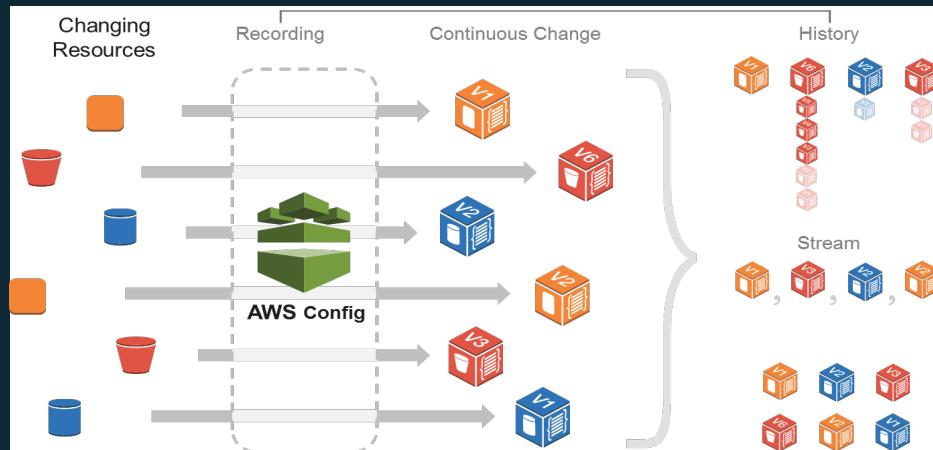
Self-service portal for creating and managing resources in AWS.



- Create and manage approved catalogs of resources.
- End users browse and launch products via self-service portal.
- Control user access to applications or AWS resources per compliance needs.
- Extensible via API to existing self-service frameworks.

AWS Config

Managed service for tracking AWS inventory and configuration, and configuration change notification.



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.

Trusted Advisor Dashboard

Welcome to the AWS Trusted Advisor console! For more information, see [Meet AWS Trusted Advisor](#).

[Download](#) [CSV](#) [Help](#)

Cost Optimization	Performance	Security	Fault Tolerance
2 ✓ 5 ▲ 0 ! 0 excluded items \$331.20 Potential monthly savings	6 ✓ 2 ▲ 0 ! 0 excluded items	4 ✓ 1 ▲ 4 ! 1 excluded items	8 ✓ 3 ▲ 2 ! 0 excluded items

Security

[Download](#) [CSV](#) [Help](#)

4 ✓ 1 ▲ 4 !
1 excluded items

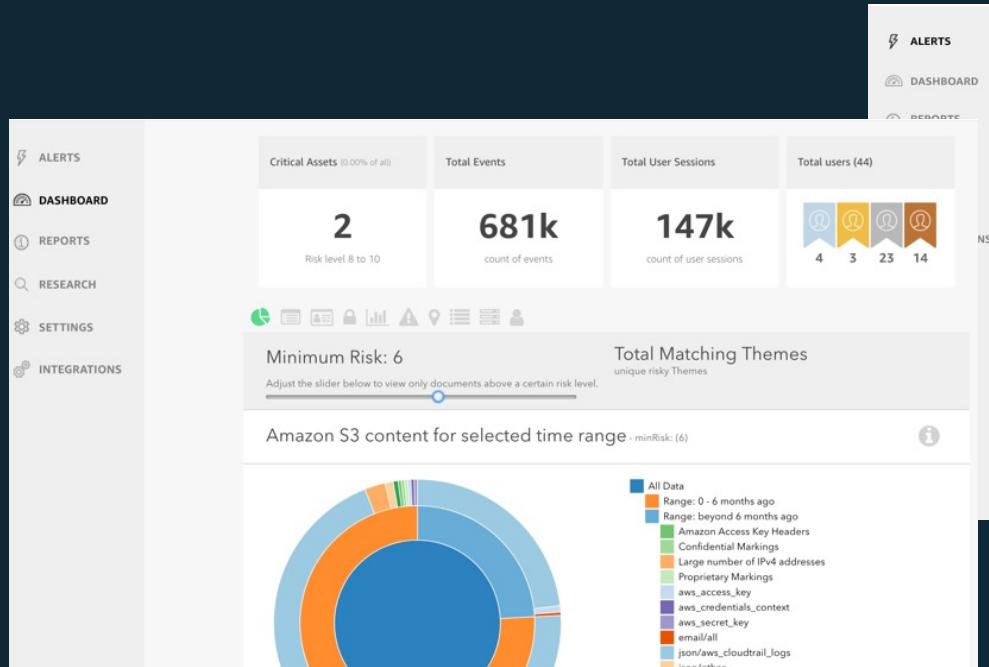
[View](#) [All checks](#)

Security Checks

Security Groups - Specific Ports Unrestricted Updated: Dec 22, 2014 6:32 AM
Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports. 44 of 124 security group rules allow unrestricted access to a specific port.
Security Groups - Unrestricted Access Updated: Dec 22, 2014 6:24 AM
Checks security groups for rules that allow unrestricted access to a resource. 47 of 124 security group rules have a source IP address with a /0 suffix. 1 items have been excluded.
Amazon S3 Bucket Permissions Updated: Dec 22, 2014 6:24 AM
Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions.

Amazon Macie

Leverage Amazon Macie to help prevent data loss in AWS.



The interface displays a list of alerts categorized by type:

- All (204)
- Audit (0)
- Admin (0)
- Insider (0)
- Login (0)
- DLP Match (0)
- IP Match (0)
- Location Anomaly (0)
- Anonymous Proxy (0)
- Privilege Escalation (0)
- DLP (203)
- Behavioral Anomaly (1)
- Custom Alert (203)
- Predictive (1)

Three specific alerts are shown in a grid:

- S3 Bucket uses IAM policy to grant read rights to Everyone** (100): Last seen 11 minutes ago, 0 comments, 0 views. Triggered by CUSTOM_ALERT and DLP.
- S3 Bucket uses IAM policy to grant read rights to Everyone** (100): Last seen 21 minutes ago, 0 comments, 0 views. Triggered by CUSTOM_ALERT and DLP.
- Access Denied In Secure Account** (50): Last seen 30 minutes ago, 0 comments, 0 views. Triggered by CUSTOM_ALERT and DLP.

AWS Marketplace Security Partners

Infrastructure Security



Logging & Monitoring



Identity & Access Control



Configuration & Vulnerability Analysis



Data Protection



Enforce consistent security on your hosts

Configure and harden EC2 instances based on security and compliance needs.



Host-based Protection Software

Restrict Access Where Possible

Launch with IAM Role

User administration

Whitelisting and integrity

Malware protection

Vulnerability management

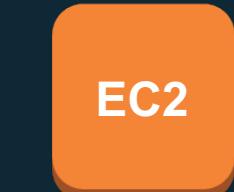
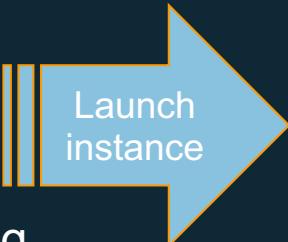
Audit and logging

Hardening

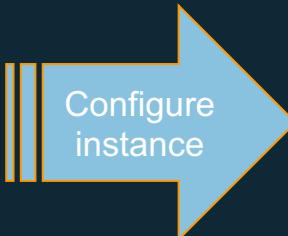
Operating system



AMI catalog

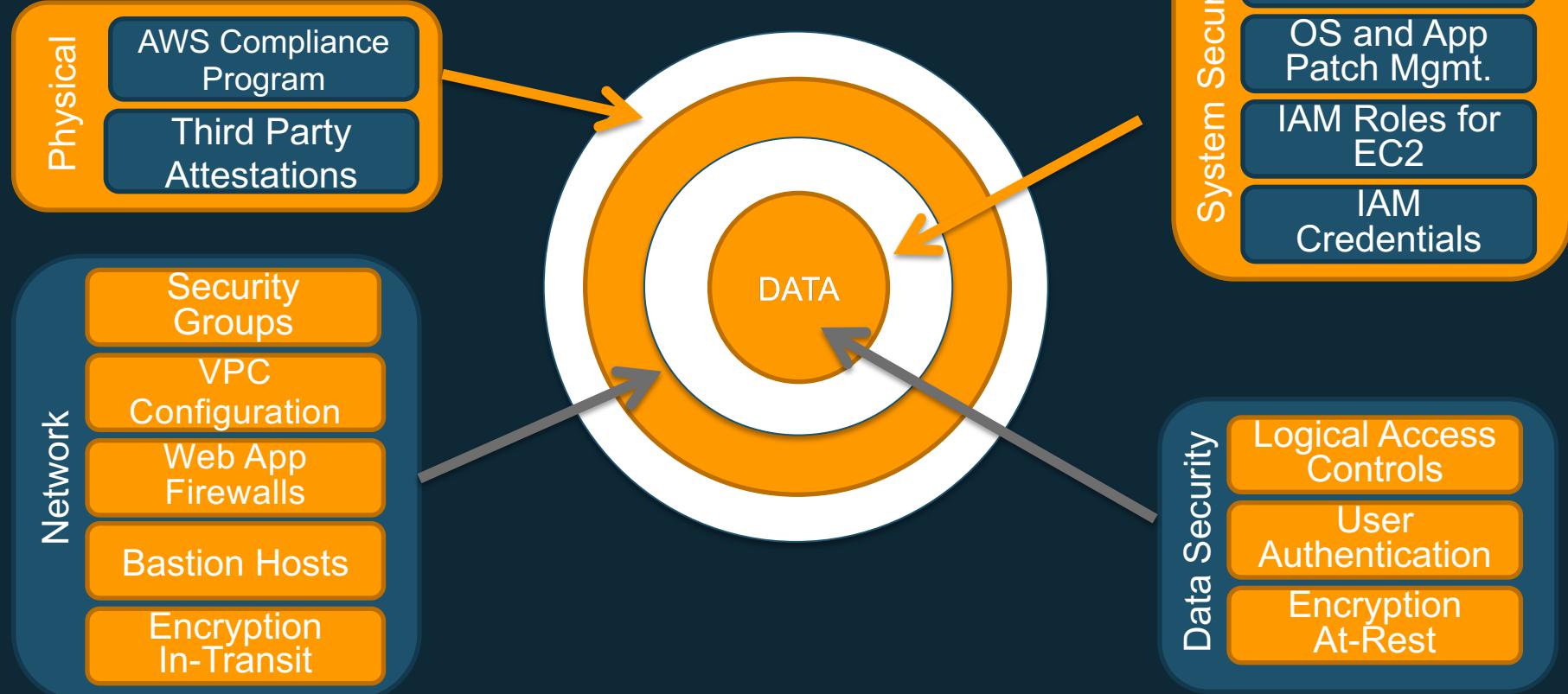


Running instance



Your instance

Defense-in-Depth



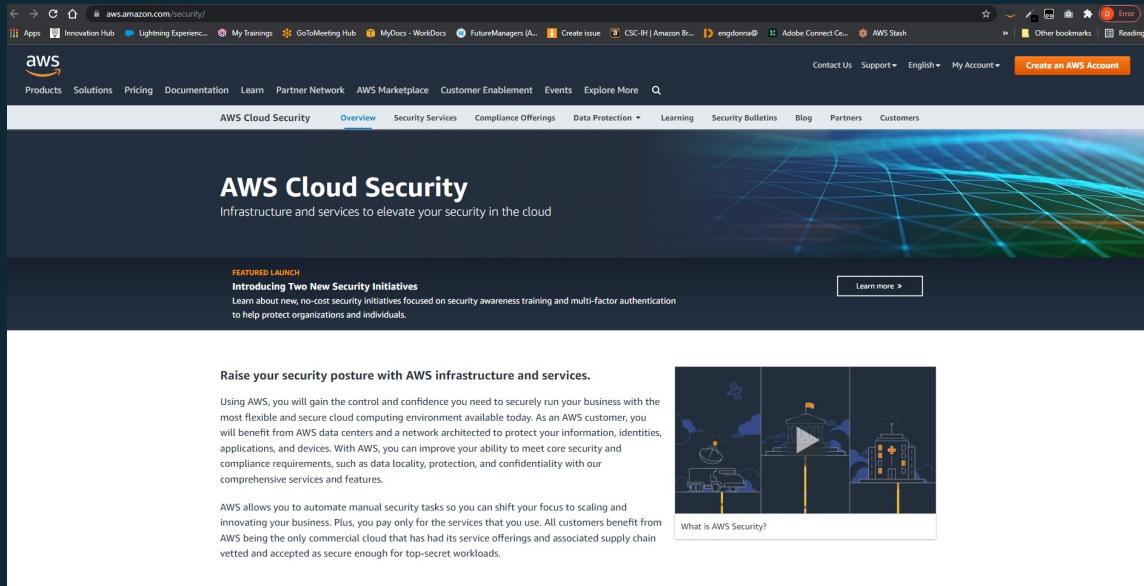


AWS Security Center

AWS Security Center

Comprehensive security portal to provide a variety of security notifications, information and documentation.

<http://aws.amazon.com/security>

A screenshot of the AWS Security Center homepage. The top navigation bar includes links for Innovation Hub, Lightning Experience, My Trainings, GoToMeeting Hub, MyDocs - WorkDocs, FutureManagers, Create issue, CSC-IH | Amazon Br..., engforma®, Adobe Connect Ce..., AWS Stash, Contact Us, Support, English, My Account, and Create an AWS Account. Below the navigation is a secondary menu with links for AWS Cloud Security (selected), Overview, Security Services, Compliance Offerings, Data Protection, Learning, Security Bulletins, Blog, Partners, and Customers. The main content area features a dark background with a blue grid pattern. A section titled "AWS Cloud Security" with the subtitle "Infrastructure and services to elevate your security in the cloud" is displayed. Below this is a "FEATURED LAUNCH" section for "Introducing Two New Security Initiatives". A call-to-action button labeled "Learn more >" is present. The bottom half of the page contains two columns of text and images. The left column discusses raising security posture with AWS infrastructure and services, mentioning AWS's flexible and secure environment, and how it can help protect organizations and individuals. The right column discusses automating manual security tasks to focus on scaling and innovating. A video player icon with the text "What is AWS Security?" is shown.

Security Whitepapers

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

Security Services

Compliance Offerings

Data Protection

Learning

Security Bulletins

Report Suspicious Emails

Security Resources

<http://aws.amazon.com/security/security-resources/>

Developer Information, Articles and Tutorials,
Security Products, and Whitepapers

Security Learning

Security in the cloud is similar to security in your on-premises data centers — only without the costs of maintaining facilities and hardware. In the cloud, you don't have to manage physical servers or storage devices. Instead, you use software-based security tools to monitor and protect the flow of information into and out of your cloud resources. For this reason, cloud security is a [Shared Responsibility](#) between the customer and AWS, where customers are responsible for "security in the cloud" and AWS is responsible for "security of the cloud."

The AWS cloud allows you to scale and innovate while maintaining a secure environment. As an AWS customer, you will benefit from data centers and network architecture designed to meet the requirements of the most security-sensitive organizations. AWS infrastructure is custom-built for the cloud and is monitored 24x7 to help protect the confidentiality, integrity, and availability of our customers' data. [Browse this page](#) to learn more about key topics, areas of research, and training opportunities for cloud security on AWS.

[Whitepapers, Technical Guides, and Reference Materials](#) | [Security Documentation](#) | [Provable Security: Research and Insights](#) | [Training](#) | [AWS Security Control Domains](#) | [International Content](#)

AWS Security Blog

<http://blogs.aws.amazon.com/security/>

Subscribe to the blog – it's a great way to stay up-to-date on AWS security and compliance.

AWS Security Blog



Manage your AWS Directory Service credentials using AWS Secrets Manager

by Ashwin Bhargava and Satya Vajrapu | on 28 SEP 2021 | in Advanced (300), AWS Directory Service, AWS Secrets Manager, Security, Identity, & Compliance | [Permalink](#) | [Comments](#) | [Share](#)

AWS Secrets Manager helps you protect the secrets that are needed to access your applications, services, and IT resources. With this service, you can rotate, manage, and retrieve database credentials, API keys, OAuth tokens, and other secrets throughout their lifecycle. The secret value rotation feature has built-in integration for services like Amazon Relational Database Service [...]

[Read More](#)



AWS achieves FedRAMP P-ATO for 18 additional services in the AWS US East/West and AWS GovCloud (US) Regions

by Alexis Robinson | on 27 SEP 2021 | in Announcements, AWS GovCloud (US), Federal, Foundational (100), Government, Public Sector, Security, Identity, & Compliance | [Permalink](#) | [Comments](#) | [Share](#)

We're pleased to announce that 18 additional AWS services have achieved Provisional Authority to Operate (P-ATO) by the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB). The following are the 18 additional services with FedRAMP authorization for the US federal government, and organizations with regulated workloads: Amazon Cognito lets you add user [...]

[Read More](#)



137 AWS services achieve HITRUST certification

by Sonali Valdya | on 27 SEP 2021 | in Announcements, Compliance, Foundational (100), Security, Identity, & Compliance | [Permalink](#) | [Comments](#) | [Share](#)

We're excited to announce that 137 Amazon Web Services (AWS) services are certified for the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) for the 2021 cycle. The full list of AWS services that were audited by a third-party auditor and certified under HITRUST CSF is available on our Services in Scope by Compliance [...]

[Read More](#)

AWS Compliance

List of compliance, assurance programs and resources:

[http://aws.amazon.com/compliance/.](http://aws.amazon.com/compliance/)



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



27018



Questions