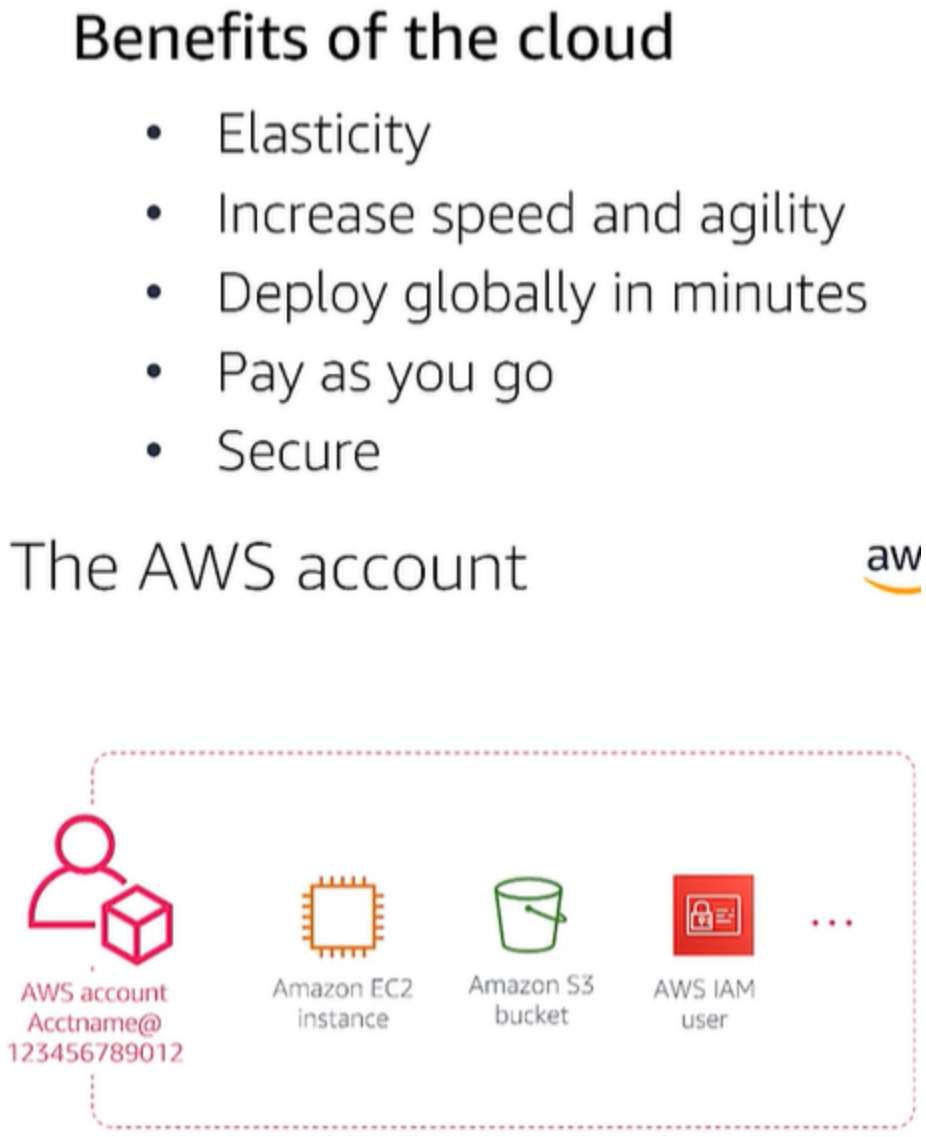
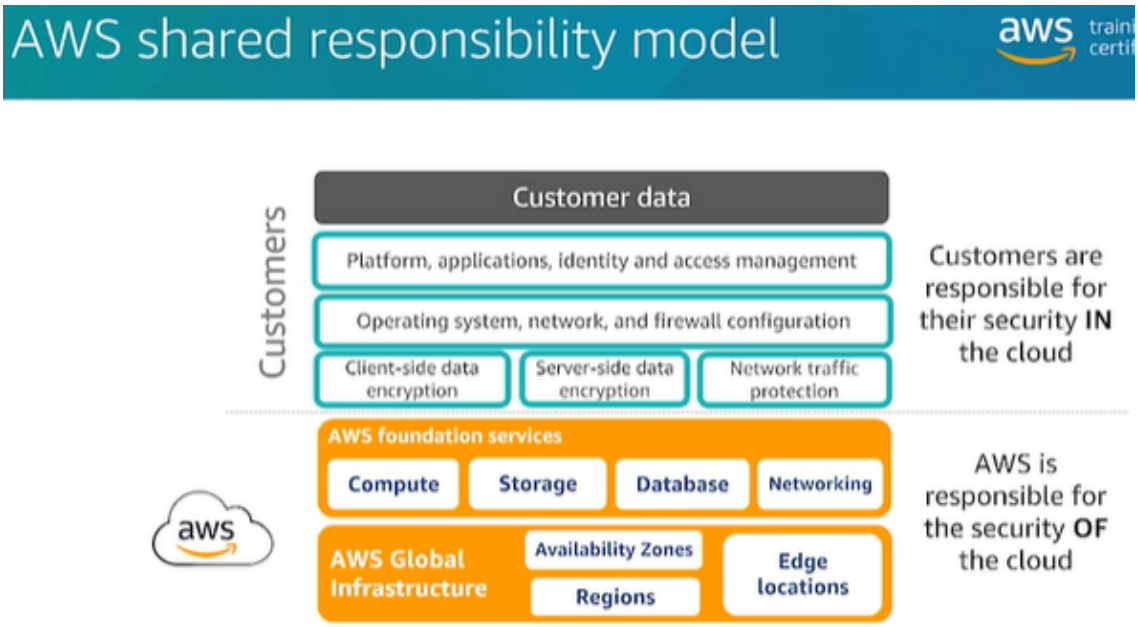
Security Learning Plan

- **AWS Foundations: Securing Your AWS Cloud**
  - Intro

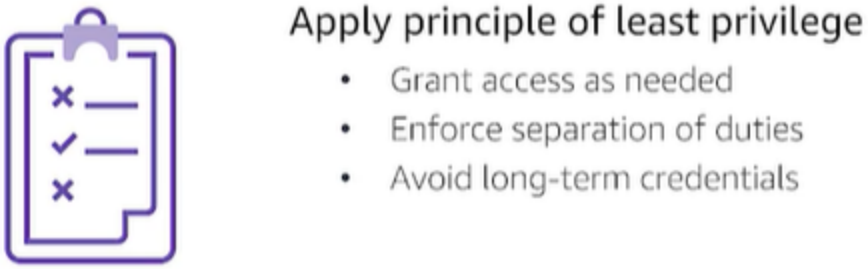


Everything starts at the account level:

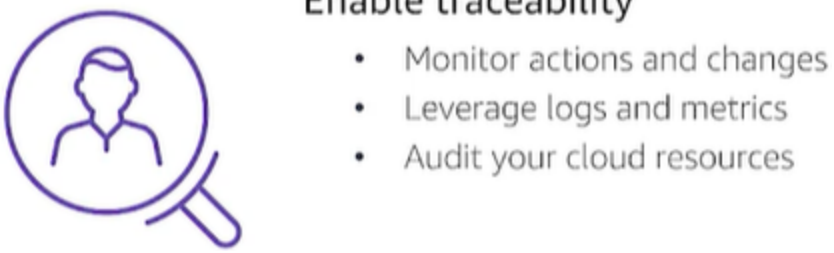


▼ Secure Design Principles

1. Least Privilege



2. Traceability



3. Secure all layers

Secure all layers

- Take a defense in depth approach
- Use different AWS services

4. Automate

Automate security

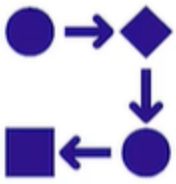
- Automate security routine tasks with APIs
- Turn infrastructure into code

5. protect data

Protect data in transit and at rest

- Use encryption and access controls
- Classify your data with tagging
- Leverage VPN and TLS connections

6. prepare for security events



Prepare for security events

- Mitigate the impact of security incidents
- Create processes to isolate incidents and restore operations

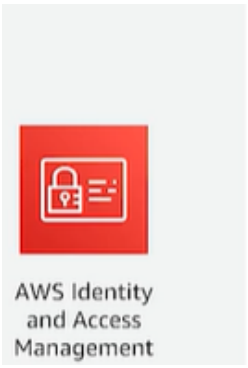
7. minimize attack surface

Minimize attack surface

- Be ready to scale and absorb the attack
- Safeguard exposed resources

▼ What is your Security Posture?

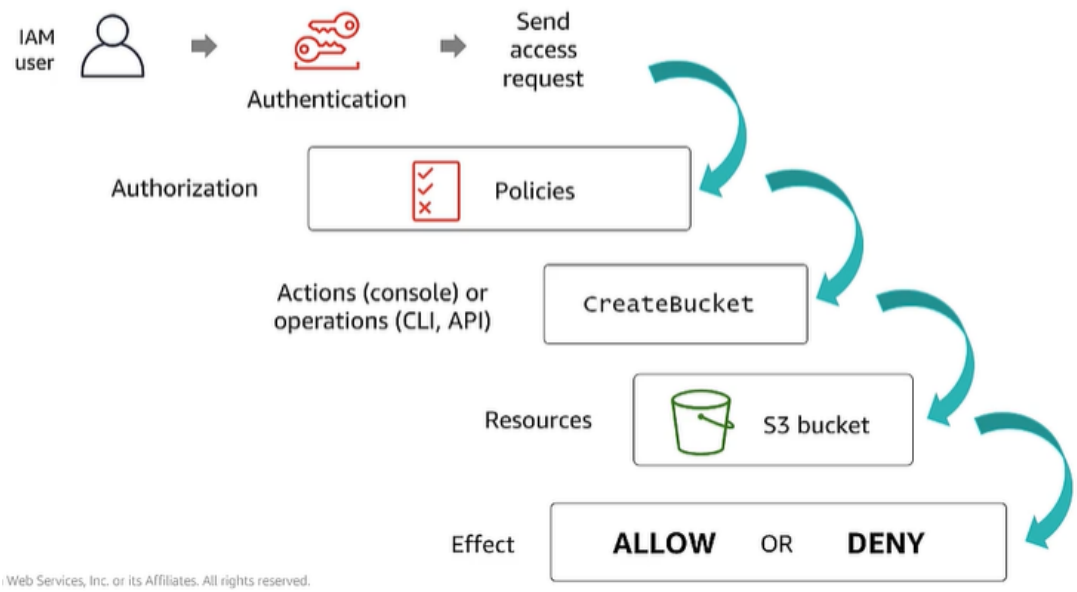
1. Authentication: Who are you?



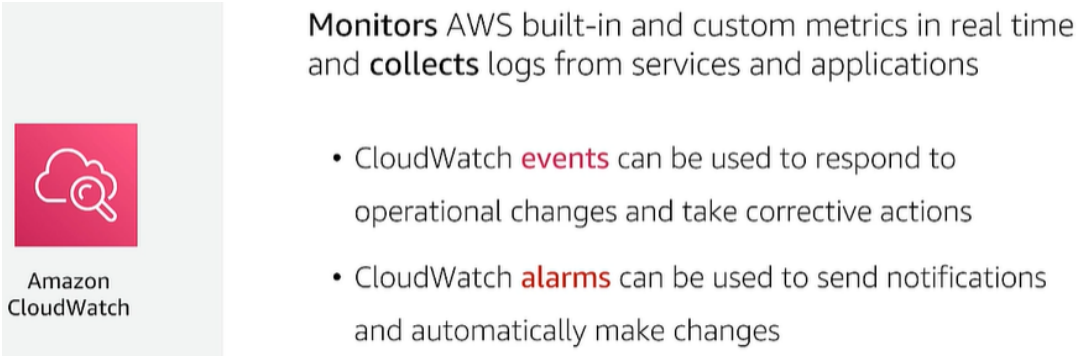
Control access to your AWS resources for users, groups, and roles

- User name and password when accessing the AWS Management Console
- Secret and access keys when using the AWS CLI or AWS SDKs, or making direct API calls

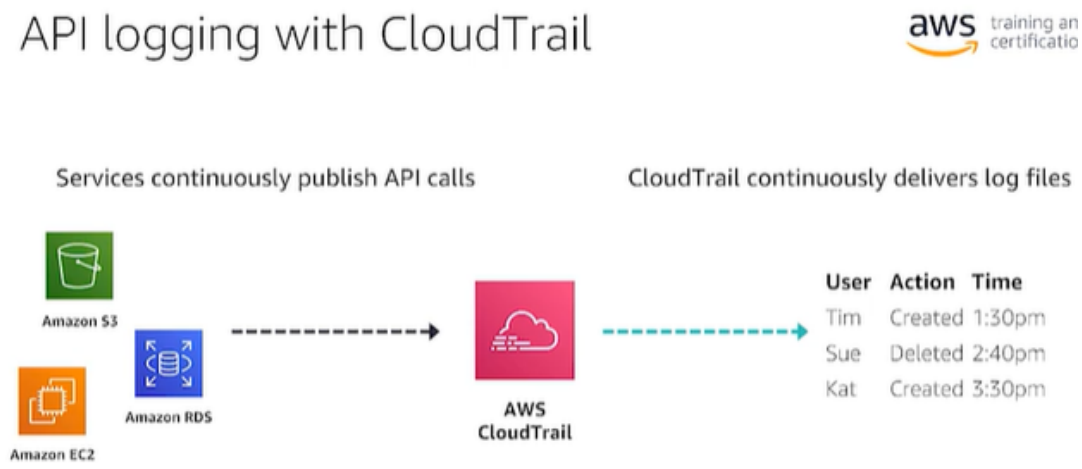
2. Authorization: What can you do or not do?



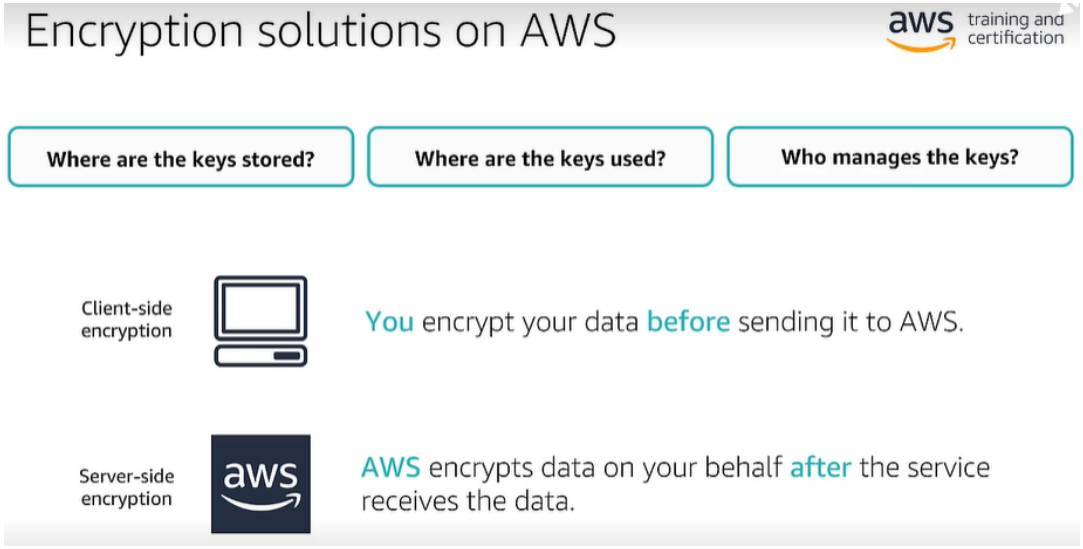
3. Monitoring: How much did you?

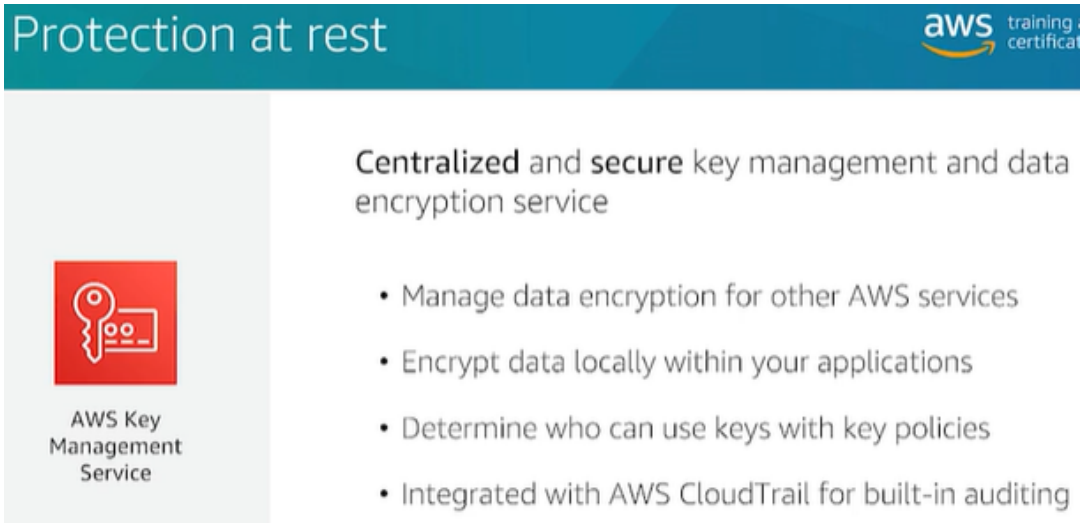


4. Audit: What did you actually do?



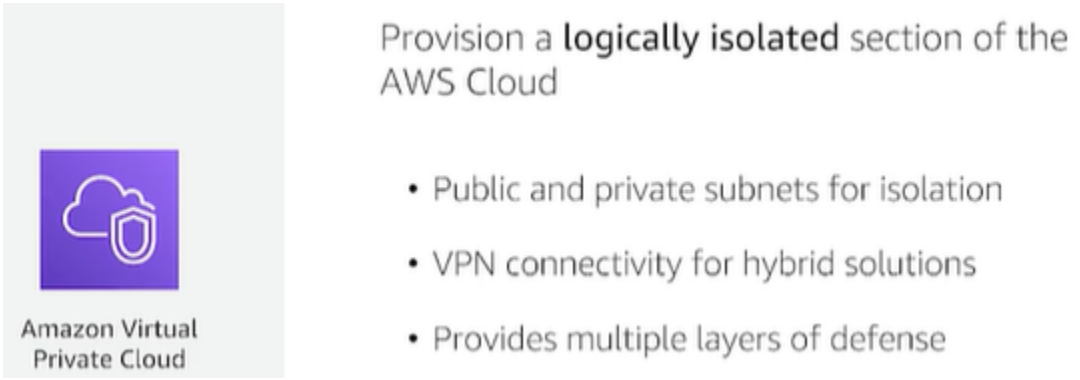
5. Encryption: Is your data encrypted at rest and in transit?

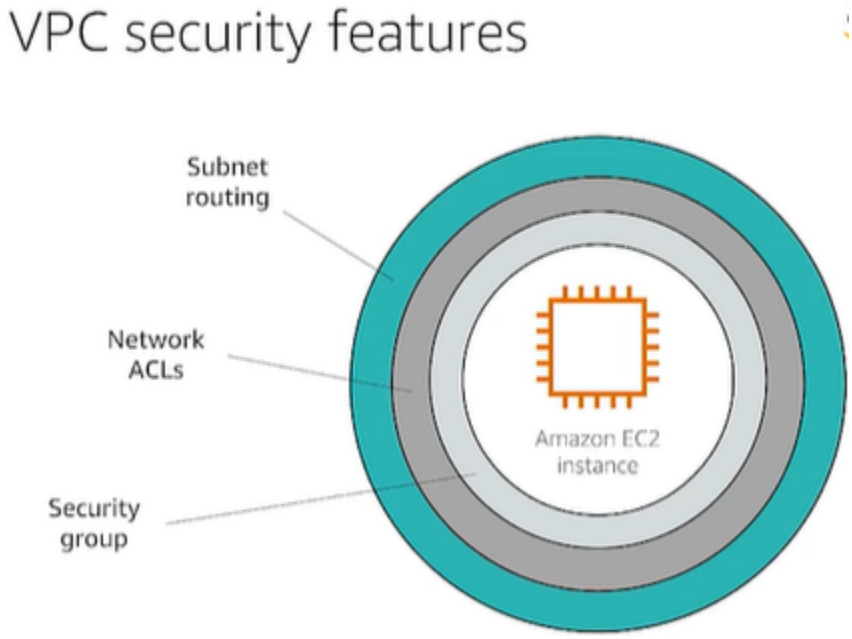




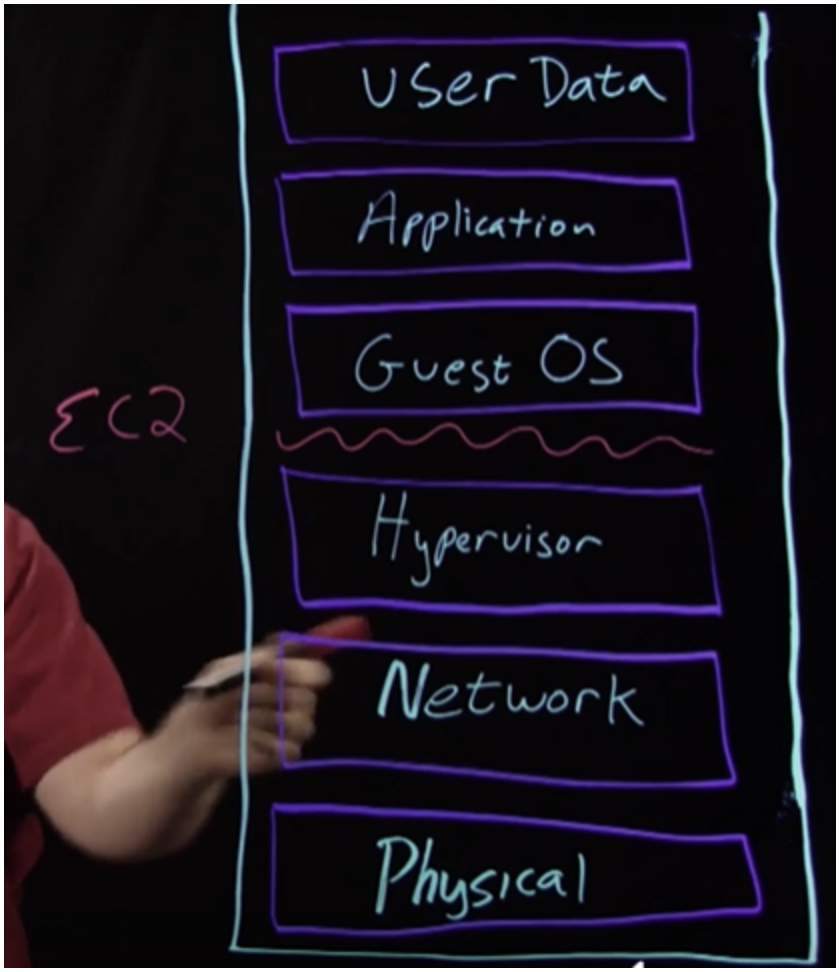
- Authenticate network communications with TLS or IPsec
- Manage SSL/TLS certificates by using AWS Certificate Manager
- Enforce encryption in transit by only allowing HTTPS traffic

6. Data path: What network controls do you have?





▼ **AWS Shared Responsibility Model**



▼ **Getting Started with AWS Security, Identity, and Compliance**

▼ Intro

The challenges of on-premises workloads

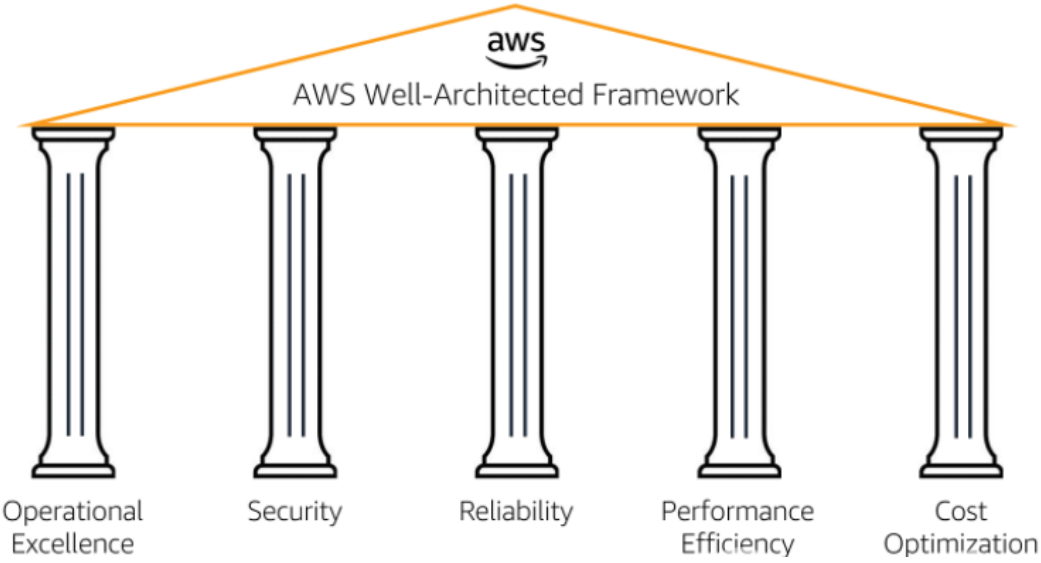
Today's businesses can decide between on-premises and cloud solutions for nearly every element of their IT services. On-premises solutions have a few advantages over cloud-based solutions, but the disadvantages are growing as cloud computing matures. The following are some of the major challenges of on-premises workloads:

- **Maintenance –** With an on-premises system, you are responsible for maintaining server hardware and software, data backups, storage, and disaster recovery. This maintenance can be an issue for smaller companies that have limited budgets and technical resources.
- **Cost –** A system built from the ground up requires significant effort and comes at a hefty cost. This cost includes the initial investment and the maintenance and operating costs that the company will have to incur on an ongoing basis.
- **Mobility –** On-premises systems can be accessed remotely but often require third-party support for access and authentication. This support increases the risk of security and communication failures.
- **Scalability –** If a company with on-premises servers experiences an increase in computing needs, it has no choice but to invest in expensive new infrastructure. If the company's needs later decrease to previous levels, it is burdened with excess capacity.

The AWS Well-Architected Framework

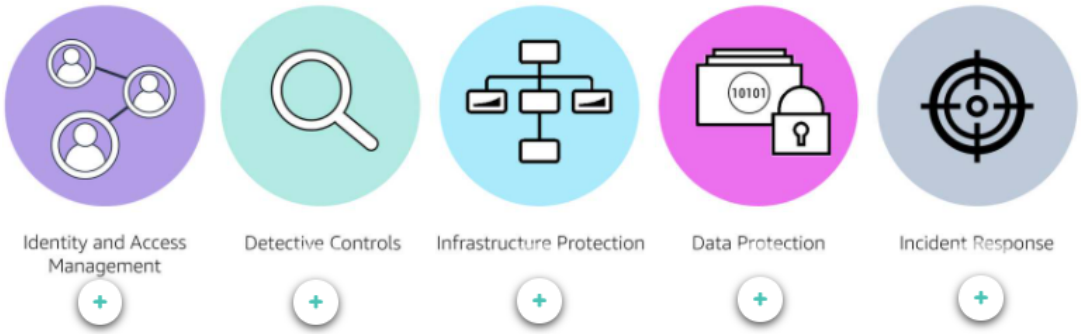
The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS. By using the AWS Well-Architected Framework, you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement. AWS believes that having well-architected systems greatly increases the likelihood of business success.

The framework is based on five pillars. Select each of the following markers for more information:



The security pillar

The security pillar signifies the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies. The security pillar is made up of five different areas for security in the cloud. All AWS security services can be categorized by these five areas. Select each of the following markers for more information on the different security pillar areas.



In this course, we cover the AWS services found under the Security, Identity, and Compliance section of the AWS Management Console.

▼ IAM

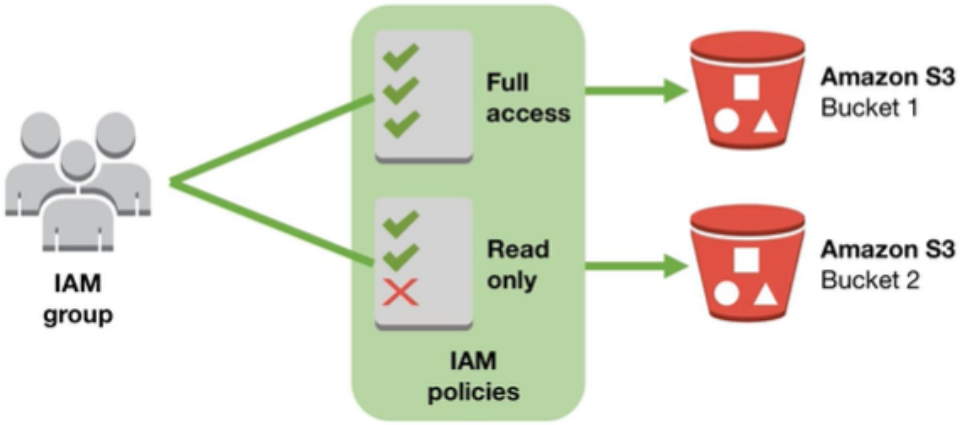
▼ Intro

AWS services for identity and access management

You can use the following AWS services to protect credentials and allow for user authentication and authorization.

- **Amazon Cognito** +
- **AWS Directory Service** +
- **AWS Identity and Access Management (IAM)** +
- **AWS Single Sign-On** +

IAM Policies are JSON documents used to describe permissions within AWS.



IAM Policies are JSON documents used to describe permissions within AWS.

```
"Sid":  "Stmt1505076701000",
"Effect":  "Allow",
"Action":  [
    "s3:DeleteObject",
    "s3:GetObject"
],
"Condition":  {
    "IpAddress":  {
        "aws:SourceIP":  "10.14.8.0/24"
    }
},
"Resource":  [
    "arn:aws:s3:::billing-marketing",
    "arn:aws:s3:::billing-sales"
]
```

Who/what is authorized

Which task(s) are allowed

Which condition(s) need to be met for authorization

Resources to which authorized tasks are performed

IAM Role

- IAM users, applications, and services may assume IAM roles
- Uses an IAM policy for permissions

1. Manage IAM users and their access
2. Manage IAM roles and their permissions
3. Manage federated users and their permissions

▼ Cognito

Two Ways to Federate with Amazon Cognito

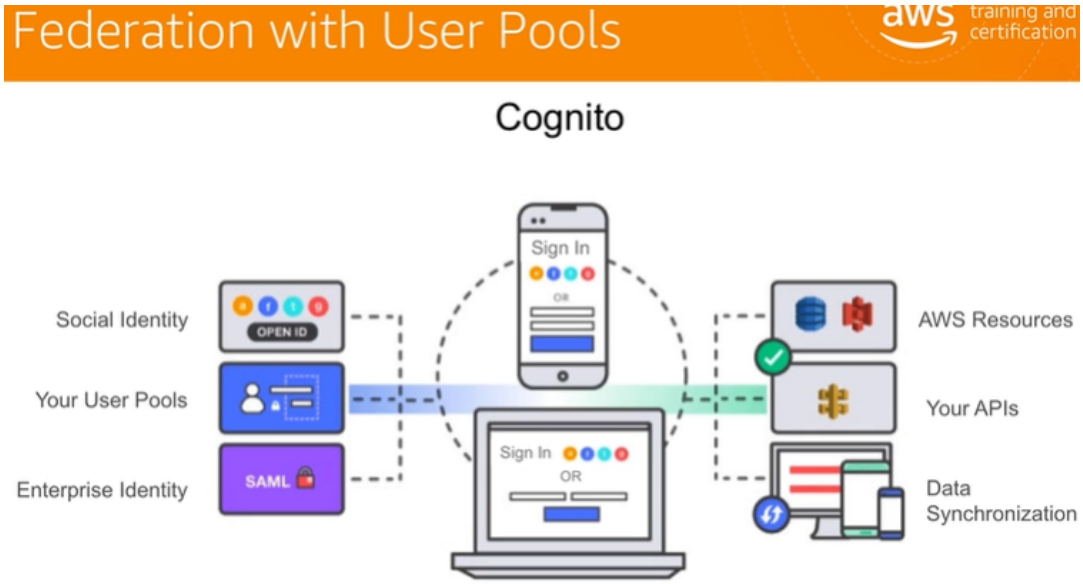
aws training certifica

Cognito User Pools

- Handles the IdP interactions for you
- Provides profiles to manage users
- Provides OpenID Connect and OAuth2.0 standard tokens
- Priced per monthly active user

Cognito Identity Pools

- Provides AWS credentials for accessing resources on behalf of users
- Supports rules to map users to different IAM roles
- Free

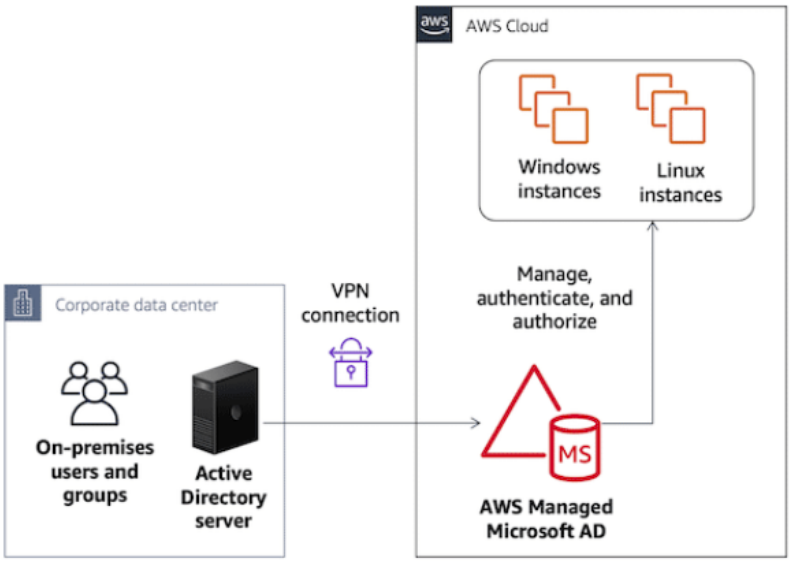


▼ AWS Directory Service for User Federation

Directory Service provides multiple directory choices for customers who want to use existing Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP)-aware applications in the cloud. You can choose directory services with the features and scalability that best meet your needs.

Use case: extend your on-premises Active Directory to the AWS Cloud

If you already have an Active Directory infrastructure and want to use it when migrating Active Directory aware workloads to the AWS Cloud, AWS Managed Microsoft AD can help. You can use Active Directory trusts to connect AWS Managed Microsoft AD to your existing Active Directory. This means your users can access Active Directory aware and AWS applications with their on-premises Active Directory credentials without needing you to synchronize users, groups, or passwords.



▼ Detective Controls

▼ Intro

Monitoring for security

The shared responsibility model requires you to monitor and manage your environment at the operating system and higher layers. You probably already do this on premises or in other environments, so you can adapt your existing processes, tools, and methodologies for use in the cloud. Security monitoring starts by answering the following questions:

- [ ] What are the key performance indicators?
- [ ] How should you measure them?
- [ ] What are the thresholds for these metrics?
- [ ] What is the escalation process?

AWS services for detective controls

AWS provides a suite of services that will monitor and combat threats through unified security and compliance, managed threat detection, application security analysis, and the ability to investigate potential security issues.

AWS Security Hub +

Amazon GuardDuty +

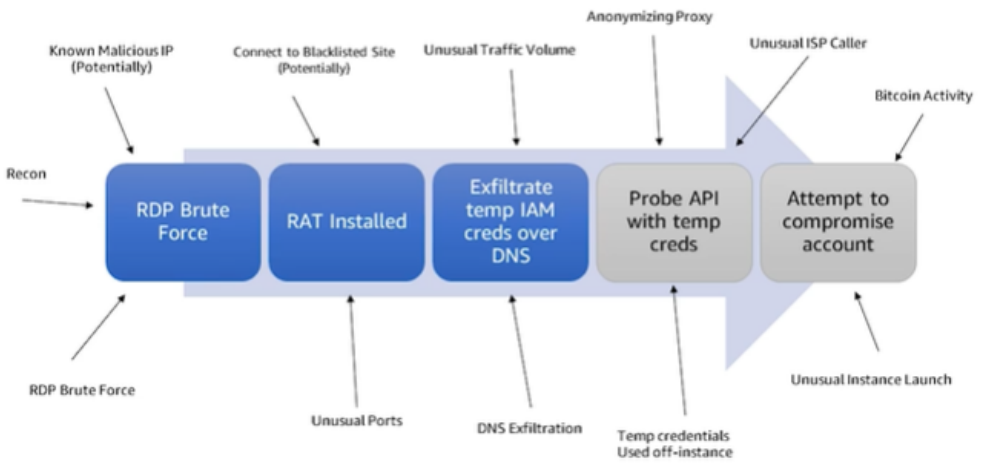
Amazon Inspector +

Amazon Detective +

Amazon Macie +

▼ GuardDuty for Threat Detection

What can the service detect?



Detecting Known Threats

- Threat Intelligence
- GuardDuty consumes feeds from various sources
  - AWS Security
  - Commercial feeds from CrowdStrike & Proofpoint
  - Open source feeds
  - Customer provided threat intel
- Known malware infected hosts
- Anonymizing Proxies
- Sites hosting malware & hacker tools
- Crypto-currency mining pools and wallets
- Great catch-all for suspicious & malicious activity

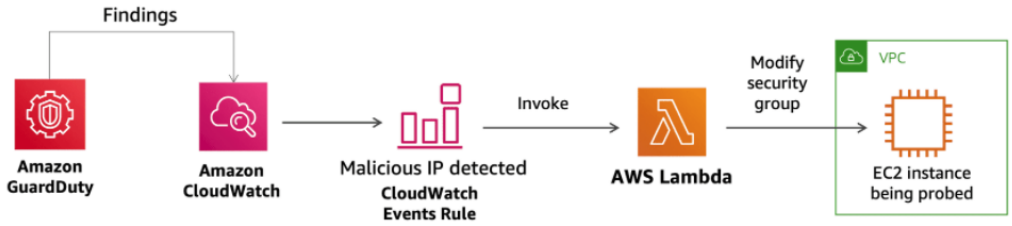
Detecting Unknown Threats

Anomaly Detection

- Algorithms to detect unusual behavior
  - Inspecting signal patterns for signatures
  - Profiling normal and looking at deviations
  - Machine Learning Classifiers
- Larger R&D Effort:
  - Highly skilled Data Scientists to study data
  - Develop theoretical detection models
  - Experiment with implementations
  - Testing, Tuning & Validation

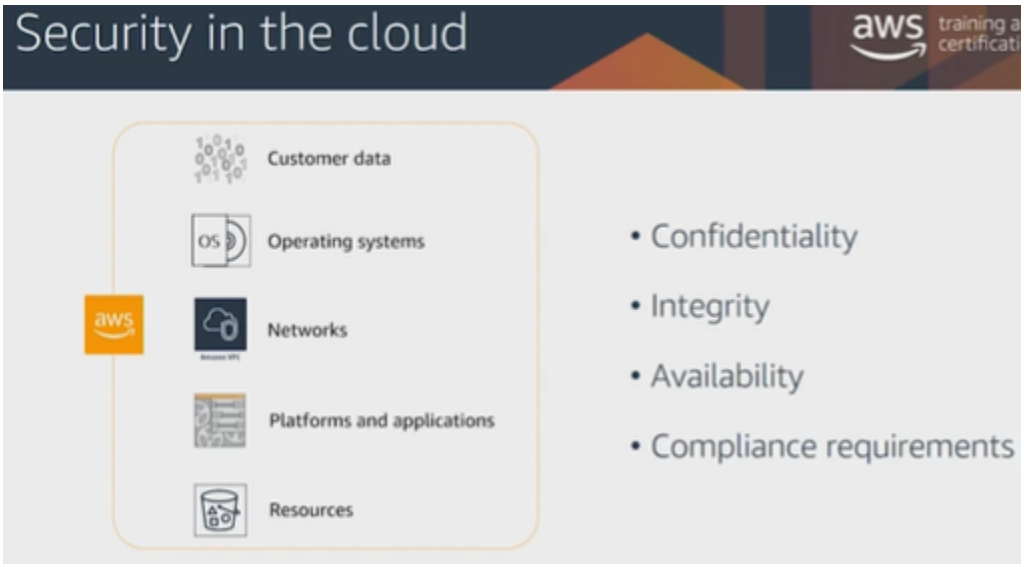
Use case: automatically remediating findings

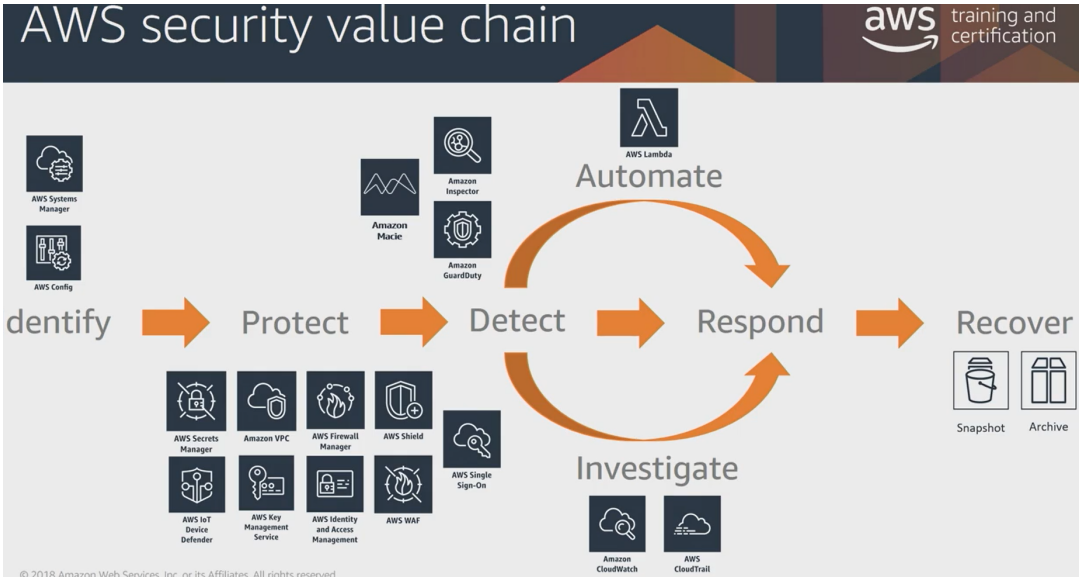
If you get a GuardDuty finding indicating that a known malicious IP is probing one of your Amazon Elastic Compute Cloud (Amazon EC2) instances, you can address it through an Amazon CloudWatch Events rule that triggers an AWS Lambda function to automatically modify your security group/network access control list (network ACL) rules and restrict access on that port.

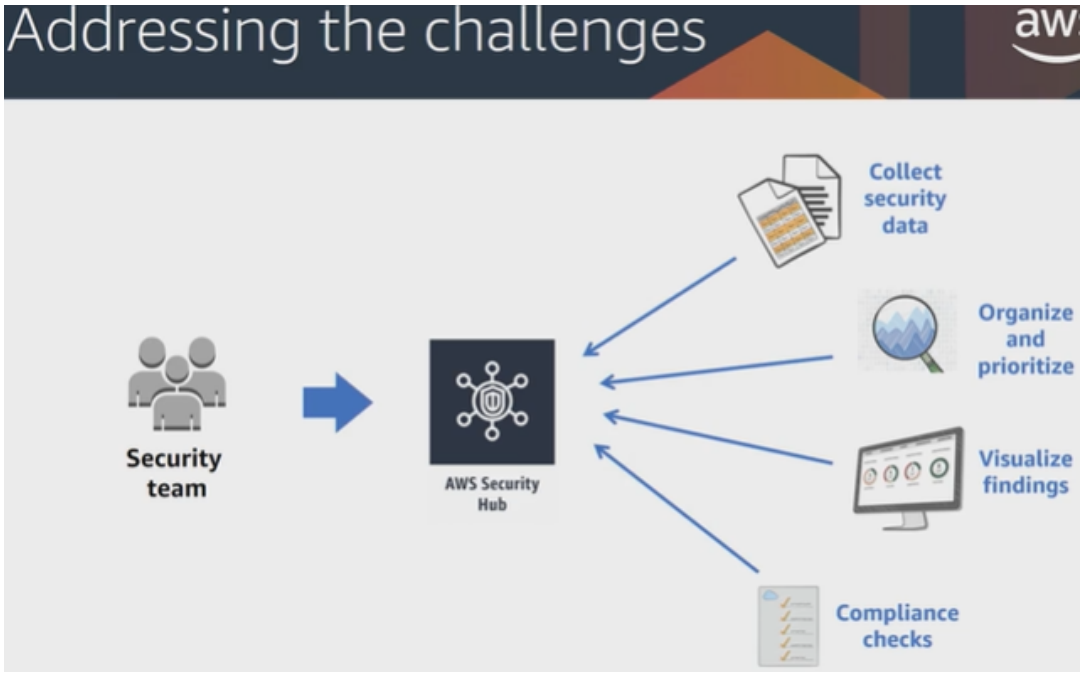


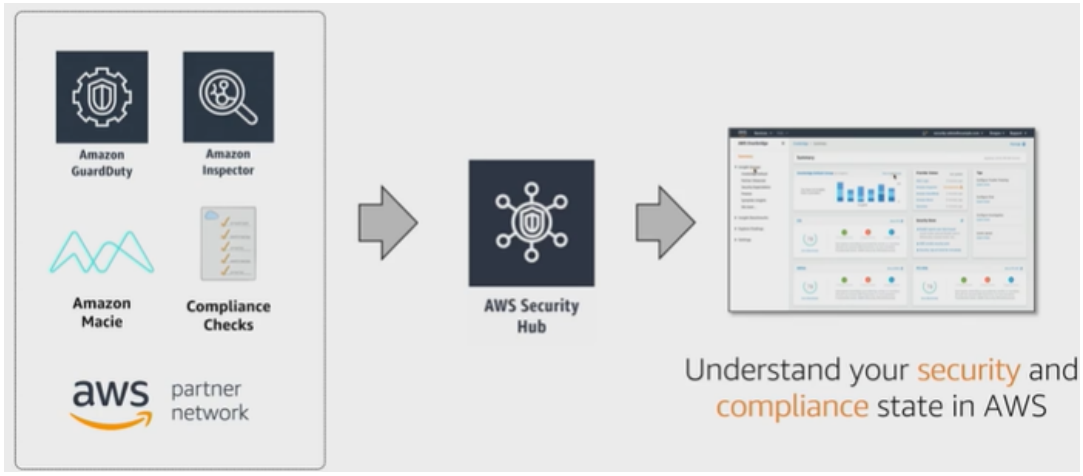
Cloud Security Tip #2 - You need to take action when you see GuardDuty findings. Your own incident response policy determines the actions to take. For each finding, ensure that you have determined what your required response actions should be.

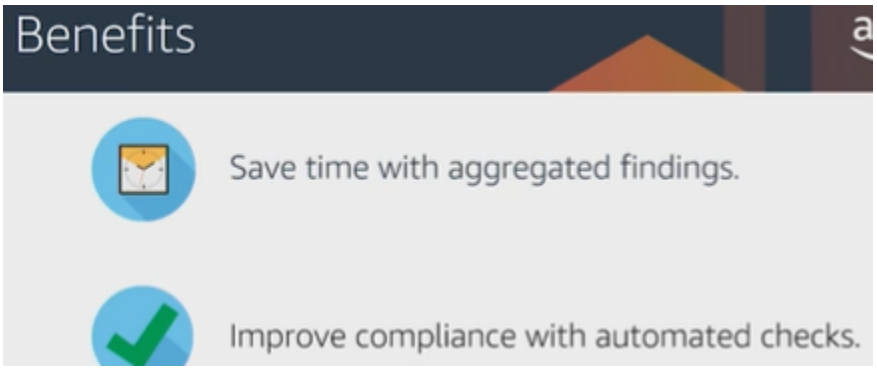
▼ AWS Security Hub for Prioritizing Findings

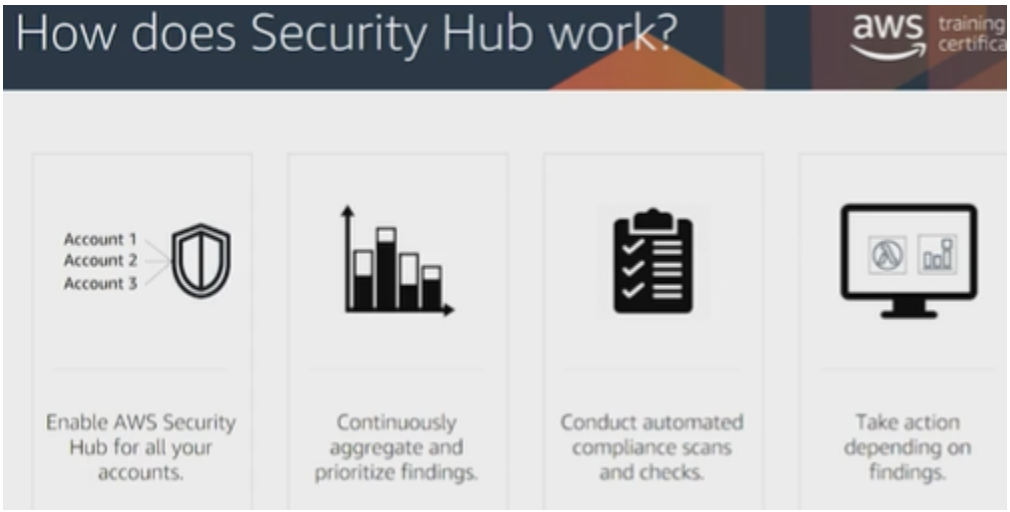

Security in the cloud
aws training a certificati
Customer data
Operating systems
Networks
Platforms and applications
Resources
• Confidentiality
• Integrity
• Availability
• Compliance requirements


AWS security value chain
aws training and certification
AWS Systems Manager
AWS Config
Amazon Macie
Amazon Inspector
Amazon GuardDuty
AWS Lambda
Automate
dentify
Protect
Detect
Respond
Recover
AWS Secrets Manager
Amazon VPC
AWS Firewall Manager
AWS Shield
AWS Single Sign-On
AWS IoT Device Defender
AWS Key Management Service
AWS Identity and Access Management
AWS WAF
Investigate
Amazon CloudWatch
AWS CloudTrail
Snapshot
Archive
© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.


Addressing the challenges
Collect security data
Organize and prioritize
Visualize findings
Compliance checks
Security team
AWS Security Hub


Amazon GuardDuty
Amazon Inspector
Amazon Macie
Compliance Checks
aws partner network
AWS Security Hub
Understand your security and compliance state in AWS

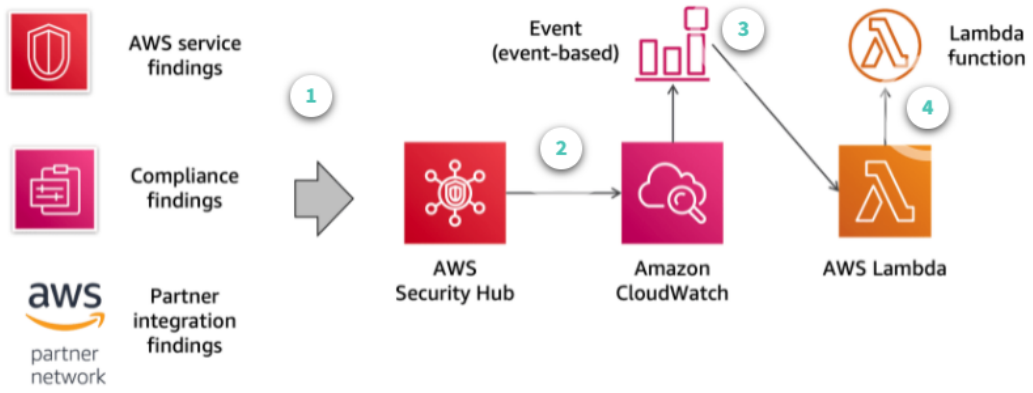

Benefits
Save time with aggregated findings.
Improve compliance with automated checks.


How does Security Hub work?
aws training
Account 1
Account 2
Account 3
Enable AWS Security Hub for all your accounts.
Continuously aggregate and prioritize findings.
Conduct automated compliance scans and checks.
Take action depending on findings.


Key takeaways
aws
Understand and manage your overall AWS security and compliance posture.
Collect and process security findings from multiple accounts within a region.
Evaluate your compliance against regulatory and best practice frameworks.
Identify and prioritize the most important issues by grouping and correlating security findings with Insights.

Use case: automated response and remediation

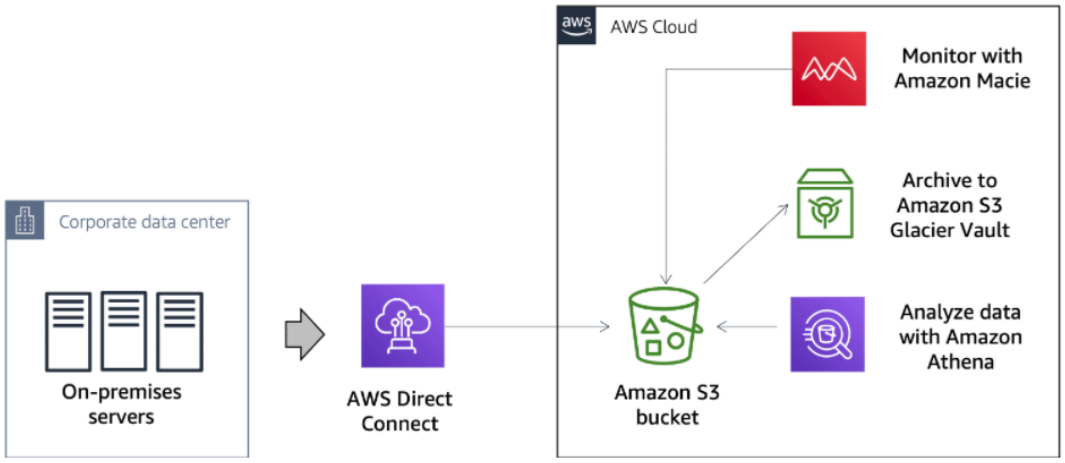
Select each of the following numbered markers for more information.



Cloud Security Tip #3 - Security Hub provides a view of the compliance posture of your AWS accounts using the CIS Benchmarks. One of these checks looks for IAM users with access keys more than 90 days old. If you need to use access keys rather than roles, you should rotate them regularly. If your users access AWS via user federation, then you can remove the need to issue AWS access keys for your users. Users authenticate to the identity provider (IdP) and assume an IAM role in the target AWS account. The result is that long-term credentials are not needed, and your user will have short-term credentials associated with an IAM role.

▼ Amazon Macie for Data Monitoring

Macie enables you to identify business-critical data and analyze access patterns and user behavior. It continuously monitors new data in your AWS environment and uses artificial intelligence to understand access patterns of historical data by automatically accessing user activity, applications, and service accounts. With Macie, you may create your own security alerts and custom policy definitions.



Here is an example of a corporation using AWS Direct Connect to create a hybrid connection to AWS. All production data is being sent to AWS for storage, archiving due to compliance requirements, and analysis via Amazon Athena. With the addition of Macie, data is now being monitored and classified for the following:

- Anonymous access via the analysis of AWS CloudTrail logs and events
- PII artifacts inside a public Amazon S3 bucket
- Amazon S3 buckets and objects with certain keywords
- Amazon S3 objects containing certain type of data

▼ Infrastructure Protection

▼ Intro

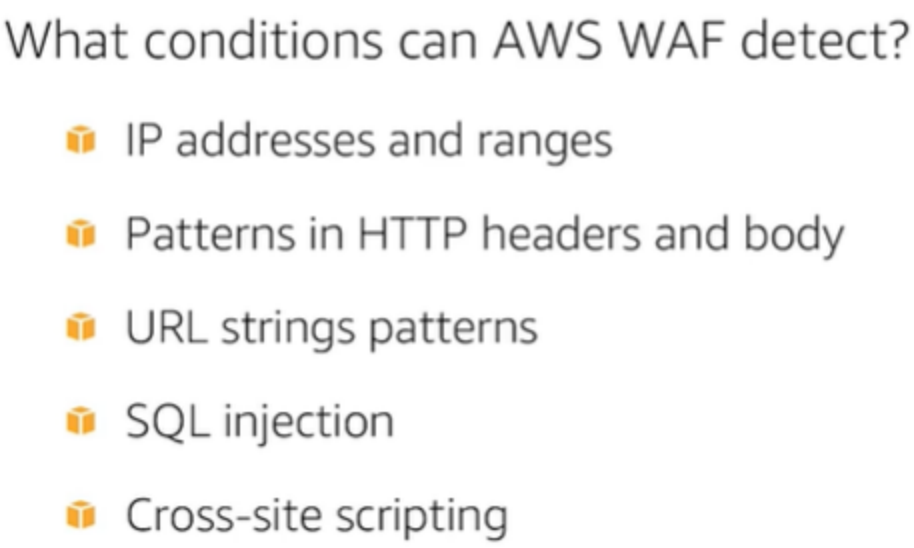
Cloud Security Tip #6 - Security groups are a key way that you can enable network access to resources you have provisioned on AWS. Ensuring that only the required ports are open and the connection is enabled from known network ranges is a foundational approach to security.

AWS services for infrastructure protection

AWS provides a suite of services for infrastructure protection. The following are some of them.

- **AWS Shield** +
- **AWS WAF** +
- **AWS Firewall Manager** +

▼ WAF for Traffic Filtering



Service features and benefits

- AWS WAF protects web applications from attacks by filtering traffic based on rules that you create. For example, you can filter any part of the web request, such as IP addresses, HTTP headers, HTTP body, or URI strings.
- With Managed Rules for AWS WAF, you can quickly get started and protect your web application or APIs against common threats.
- AWS WAF gives near-real-time visibility into your web traffic. You can use this visibility to create new rules or alerts in Amazon CloudWatch.
- AWS WAF protects applications deployed on Amazon CloudFront as part of your content delivery network (CDN) solution, the Application Load Balancer that fronts all your origin servers, or Amazon API Gateway for your APIs.
- AWS WAF provides a customizable, self-service offering, and pricing is based on how many rules you deploy and how many web requests your web application receives.

▼ Shield for DDoS Protection

AWS Shield is a managed DDoS protection service that safeguards applications running on AWS. A DDoS attack is an attack in which multiple compromised systems attempt to flood a target, such as a network or web application, with traffic. A DDoS attack can prevent legitimate users from accessing a service and can cause the system to crash due to the overwhelming traffic volume.

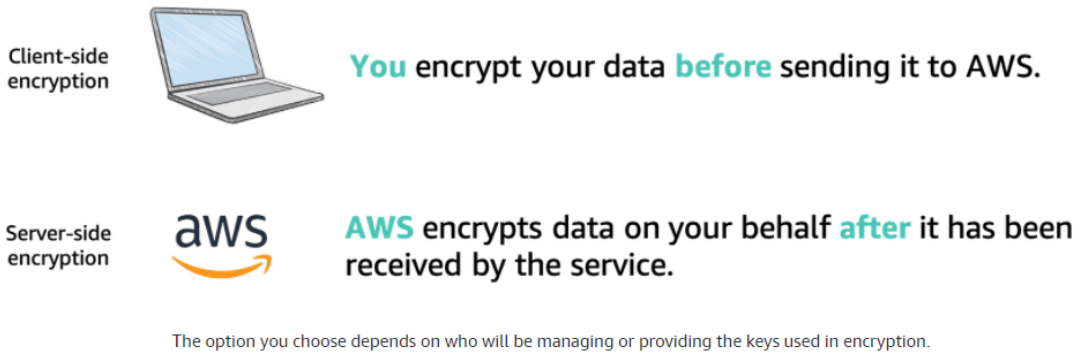
AWS provides two levels of protection against DDoS attacks:

- AWS Shield Standard (enabled by default and comes with no additional cost)
- AWS Shield Advanced

	AWS Shield Standard	AWS Shield Advanced
Always-on detection	✓	✓
Automatic inline mitigation	✓	✓
Layer 3 and 4 protection	✓	✓
Expanded DDoS attack protection		✓
24/7 DDoS response team		✓
Cost protection for DDoS spikes		✓
Access to real-time reports		✓

▼ Data Protection

▼ Intro

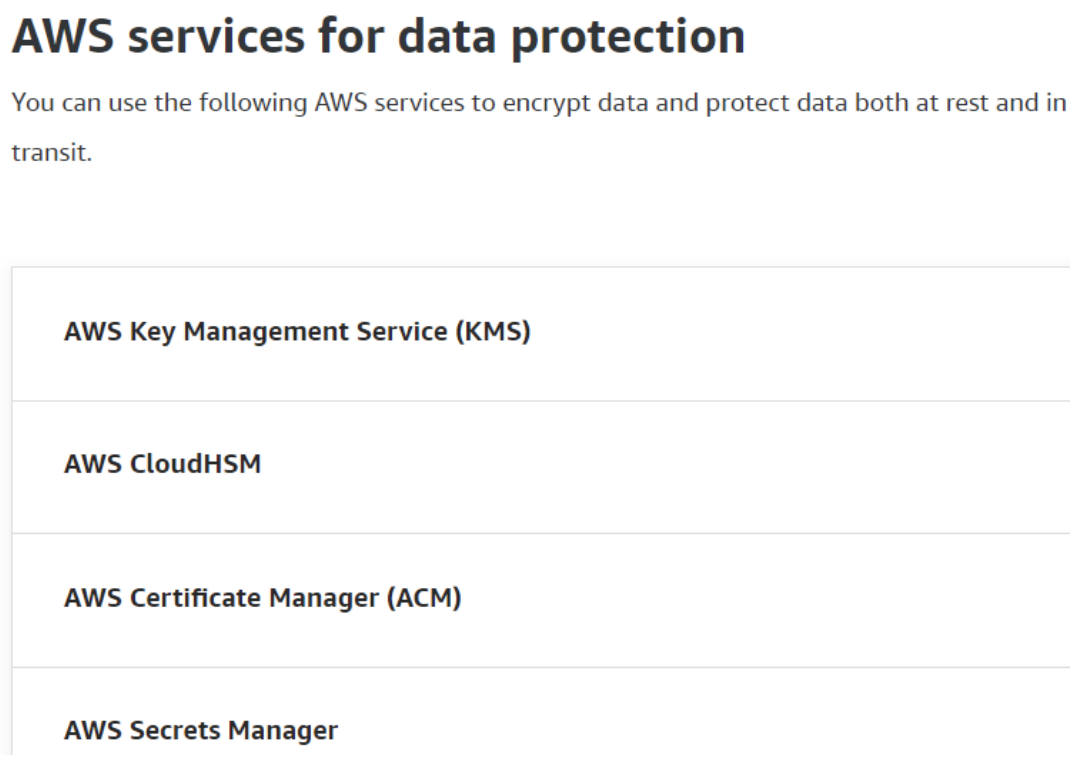


In Transit:

AWS services provide HTTPS endpoints using TLS for communication, thus providing end-to-end encryption when communicating with the AWS APIs.

Use AWS to generate, deploy, and manage public and private certificates used for TLS encryption in web-based workloads.

Use IPsec with VPN connectivity into AWS to facilitate the encryption of traffic.

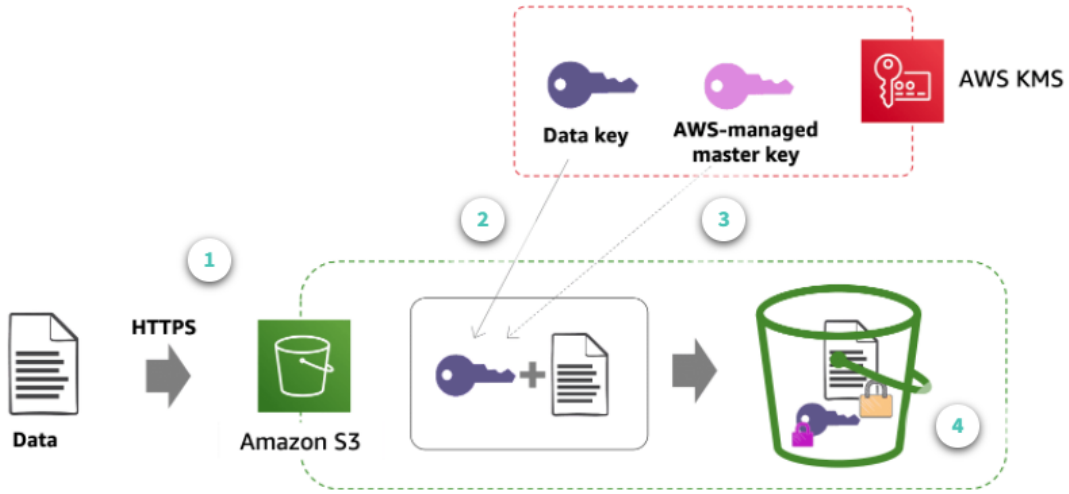


▼ AWS KMS

AWS KMS allows you to centrally manage and securely store your keys. You can use these keys from within your applications and supported AWS cloud services to protect your data. The keys never leaves AWS KMS, which reduces the risk of having your data key compromised. You submit data to AWS KMS to be encrypted or decrypted under keys that you control. You set usage policies on these keys that determine which users can use them to encrypt and decrypt data. All requests to use these keys are logged in AWS CloudTrail so that you can understand who used which key and when.

Server-side encryption example

Select each of the following numbered markers for more information.



Types of CMKs

AWS KMS can use two types of CMKs when encrypting data keys: AWS managed and customer managed. The following table summarizes the key differences and similarities between AWS managed CMKs and customer managed CMKs.

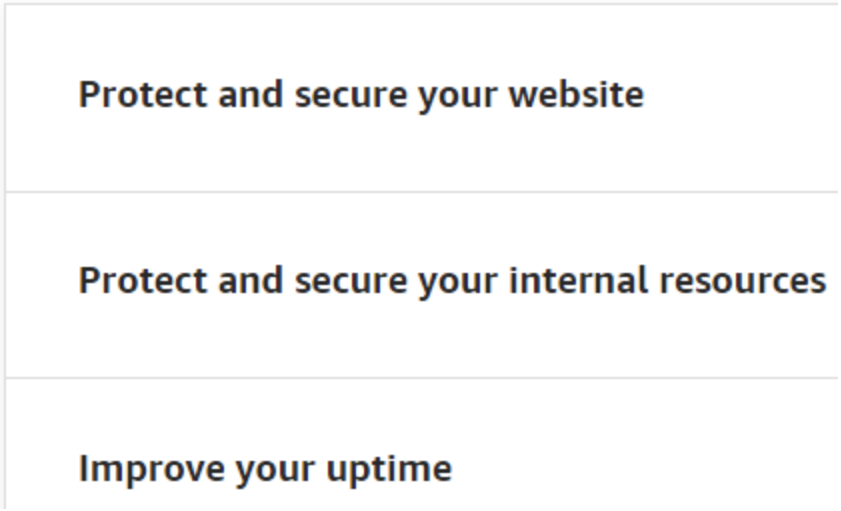
	AWS managed CMK	Customer managed CMK
Creation	AWS generated on the customer's behalf	Customer generated
Rotation	Once every 3 years automatically	Once a year automatically through opt-in or manually on-demand
Deletion	Can't be deleted	Can be deleted
Scope of use	Limited to a specific AWS service	Controlled via AWS KMS or AWS Identity and Access Management (IAM) policy
Key access policy	AWS managed	Customer managed
User access management	AWS IAM policy	AWS IAM policy

▼ AWS Certificate Manager for Securing Communications

Service features and benefits

- ACM manages the renewal and deployment process for the certificates used with ACM integrated services, such as Elastic Load Balancing and Amazon API Gateway.
- With AWS Certificate Manager Private Certificate Authority APIs, ACM enables you to automate the creation and renewal of private certificates for on-premises resources, Amazon Elastic Compute Cloud (Amazon EC2) instances, and Internet of Things (IoT) devices.
- ACM removes many of the time-consuming and error-prone steps to acquire a SSL/TLS certificate for your website or application.
- With ACM, there is no need to generate a key pair or certificate signing request (CSR), submit a CSR to a certificate authority, or upload and install the certificate once received.
- With ACM, there is no additional charge for provisioning public or private SSL/TLS certificates you use with ACM integrated services.

Common use cases



▼ AWS Secrets Manager for Credentials Management

Service features and benefits

- Secrets Manager helps you meet your security and compliance requirements by enabling you to rotate secrets safely without the need for code deployments.
- With Secrets Manager, you can manage access to secrets using fine-grained AWS Identity and Access Management (IAM) policies and resource-based policies.
- Secrets Manager offers built-in integration for Amazon Relational Database Service (Amazon RDS), Amazon Redshift, and Amazon DocumentDB (with MongoDB compatibility) and automatically rotates these database credentials on your behalf.
- Using Secrets Manager, you can secure secrets by encrypting them with encryption keys that you manage using AWS KMS.
- Secrets Manager also integrates with AWS logging and monitoring services for centralized auditing.
- With Secrets Manager, you pay for the number of secrets managed in Secrets Manager and the number of Secrets Manager API calls made.

▼ IR

▼ Rethinking IR

Using APIs for automation

In AWS, you can use APIs to automate many of the routine tasks that need to be performed during incident response. For example, using a single command, you can isolate an instance by changing the security groups associated with the instance.

Performing forensics on data volumes

Forensics often requires capturing the disk image or as-is configuration of an operating system. You can use Amazon Elastic Block Store (Amazon EBS) snapshots and the Amazon Elastic Compute Cloud (Amazon EC2) APIs to capture the data and state of systems under investigation.

Operating in a clean room

AWS CloudFormation can be used to quickly create a new, trusted environment in which to conduct deeper investigation. AWS

CloudFormation can deploy preconfigured instances in an isolated environment. These instances may contain all the necessary tools forensic teams need to determine the cause of the incident.

Coordinating AWS services into serverless workflows

AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. Workflows are made up of a series of steps, with the output of one step acting as the input into the next. Step Functions can be used to design and run workflows that stitch together services such as AWS Lambda and AWS CloudFormation to respond to an incident in the cloud.

▼ AWS Config for Responding to Incidents

Service features and benefits

With AWS Config, you are able to continuously monitor and record configuration changes of your AWS resources.

AWS Config allows you to continuously audit and assess the overall compliance of your AWS resource configurations with your organization’s policies and guidelines.

With AWS Config, you are able to track the relationships among resources and review resource dependencies prior to making changes.

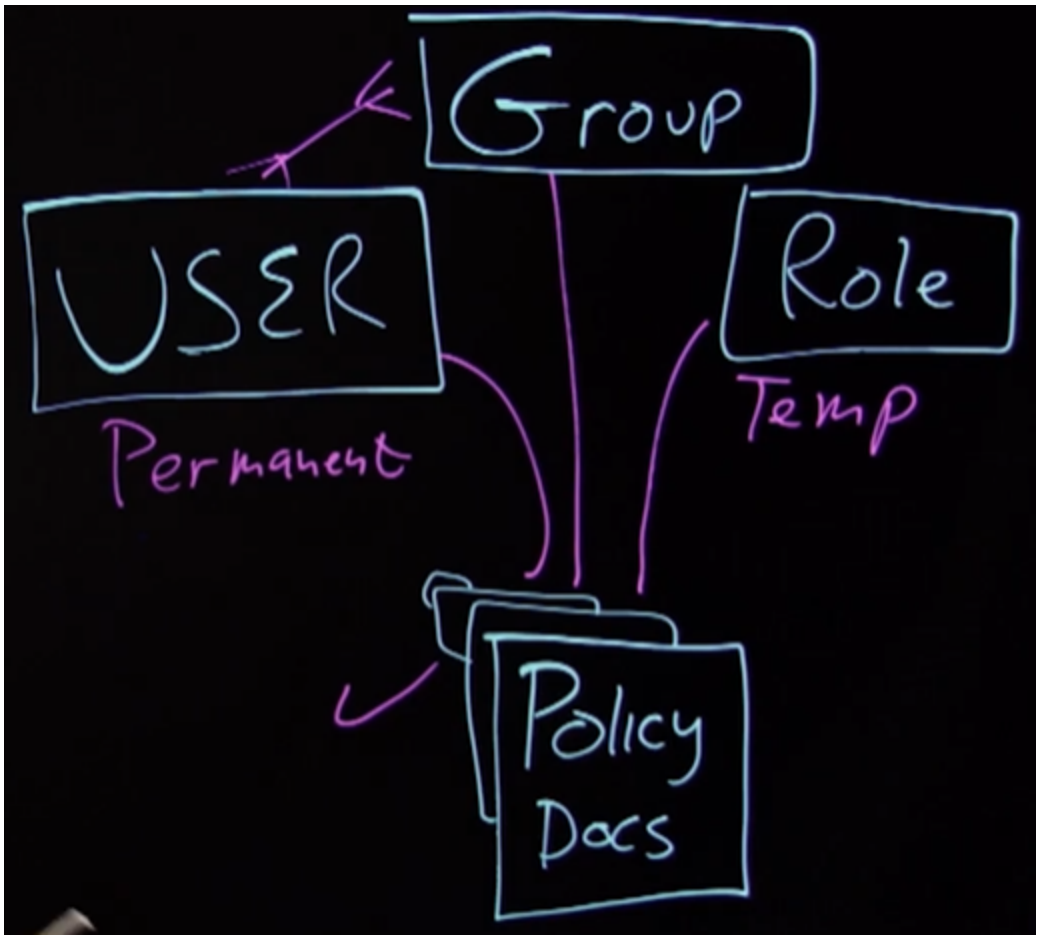
AWS Config enables you to capture a comprehensive history of your AWS resource configuration changes to simplify troubleshooting of your operational issues.

▼ **Authentication and Authorization with AWS Identity and Access Management**

Everything is an API

User - permissions are permament

Role - permissions are temporary



▼ **AWS Well-Architected**

Key points

- Make informed decisions about architecture in the cloud, and understand the potential impact of those decisions.
- Understand what a cloud-native architecture would look like by leveraging design principles.
- Questions are the starting point – Think actively about "what if" and failure scenarios.

Operational Excellence Pillar:

Key points

- ✓ Understand business priorities.
- ✓ Design for operations.
- ✓ Evaluate operational readiness.
- ✓ Understand workload and operational health.
- ✓ Prepare for and respond to events.
- ✓ Learn from your experience, share learnings, and make improvements.

Security Pillar:

Key points

- Protecting information, systems, and assets
- Keeping root account credentials protected
- Encrypting data at rest and in transit on AWS, if applicable, in multiple ways
- Ensuring that only authorized, authenticated users are able to access your resources
- Using detective controls to detect or identify a security breach

Reliability Pillar

The Reliability pillar encompasses the ability of a workload to perform its intended function correctly and consistently when it's expected to.

- Foundations
- Workload architecture
- Change management
- Failure management

Performance Pillar

Key points

- Use computing resources efficiently to meet system requirements.
- Select appropriate resource types.
- Benchmark and load test.
- Monitor performance.
- Optimize location of resources, data, and processing.

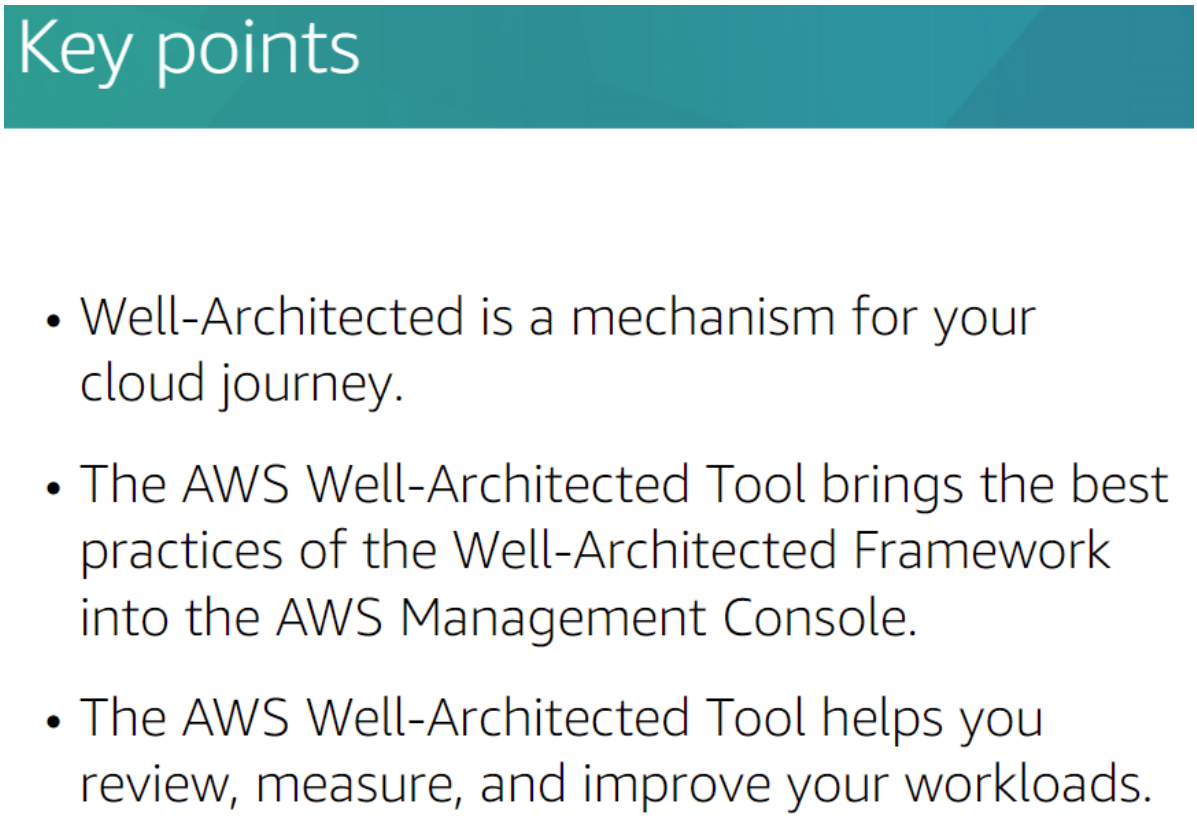
Cost Pillar

Key points

- Avoiding or eliminating unneeded cost or suboptimal resources
- Measuring overall workload efficiency
- Managing demand and supply resources
- Using savings plans to reduce cost
- Measuring overall efficiency
- Learning about new services and features

Well Architected Review

Well Architected Tool



▼ **Exam Readiness: AWS Certified Security Specialty**

▼ IR

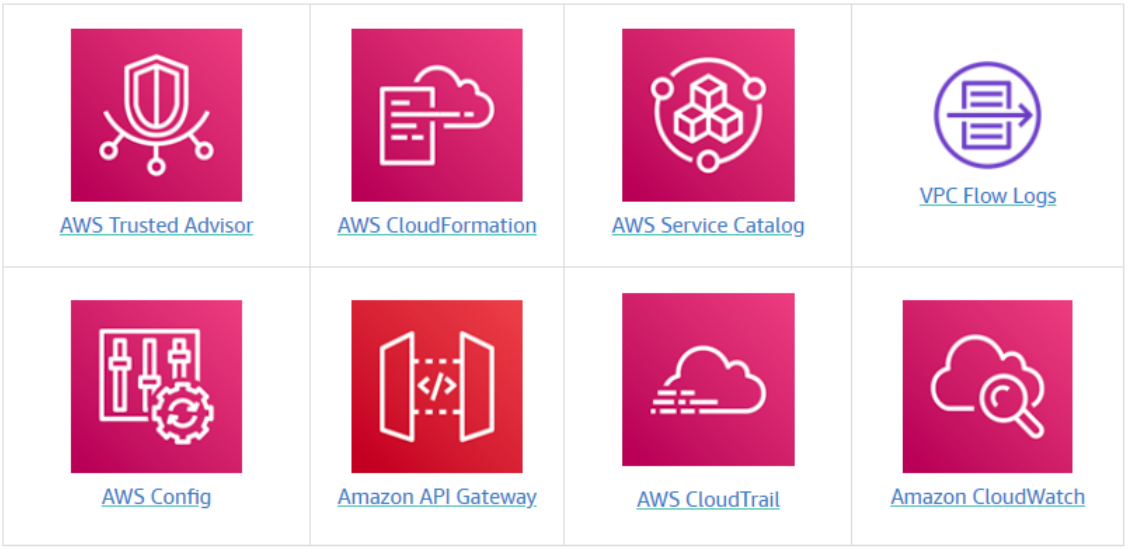
For the exam, you should know how to:

1 Evaluate the suspected compromised instance or exposed access keys given an AWS abuse notice.

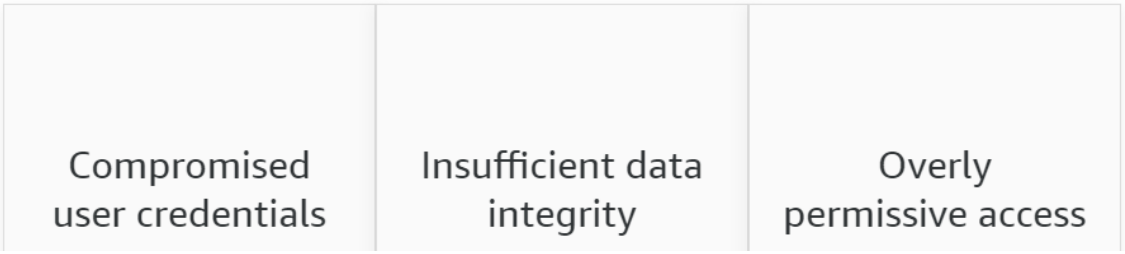
2 Verify that the incident response plan includes relevant AWS services.

3 Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.

AWS tools for incident response



Common incidents



▼ Logging and Monitoring

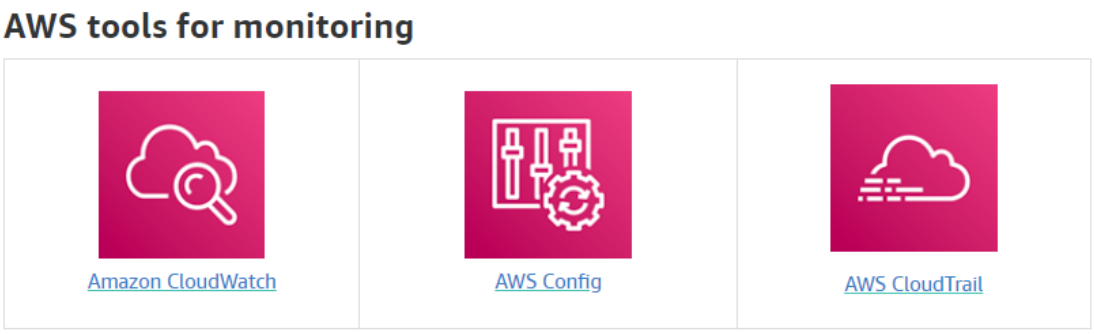
For the exam, you should know how to:

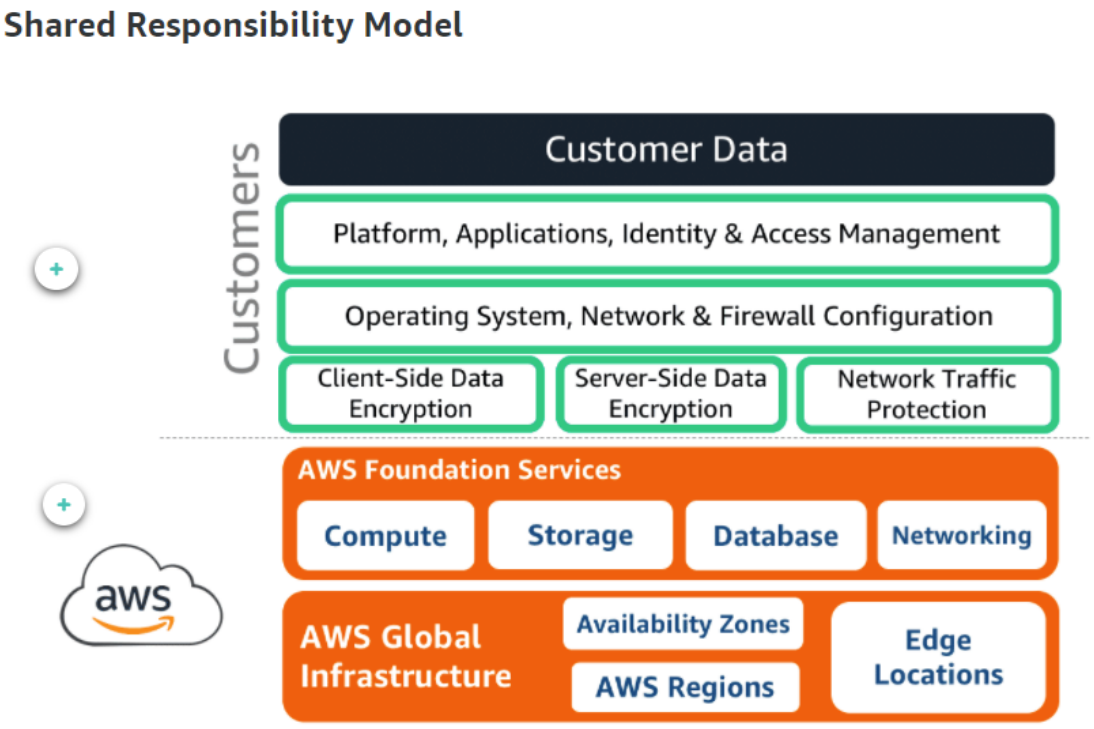
1 Design and implement security monitoring and alerting.

2 Troubleshoot security monitoring and alerting.

3 Design and implement a logging solution.

4 Troubleshoot logging solutions.





▼ Infrastructure Security

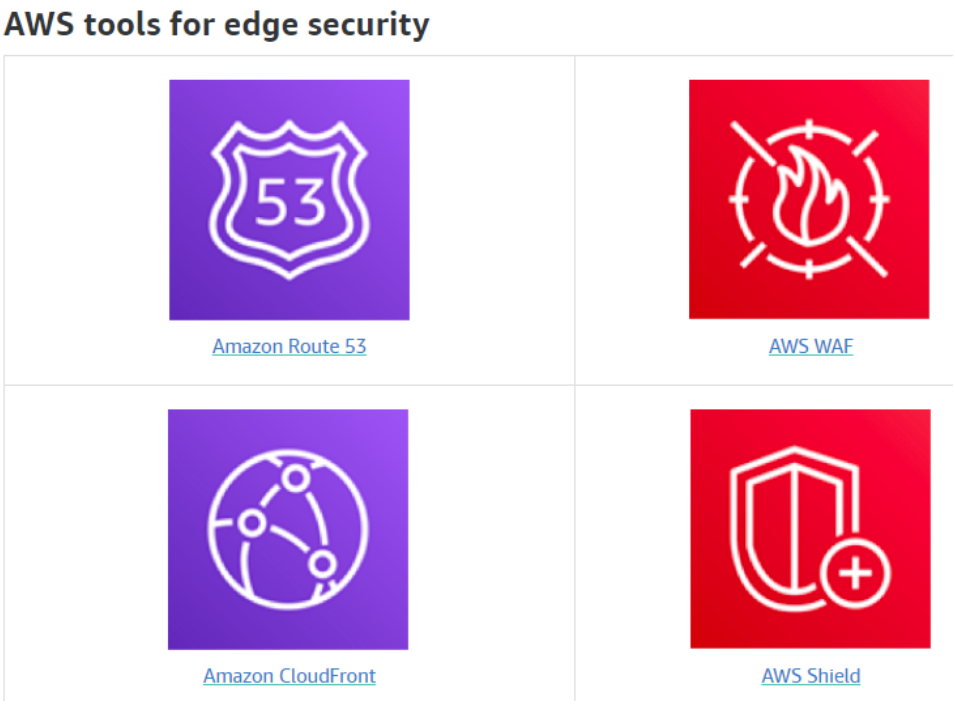
For the exam, you should know how to:

1 Design edge security on AWS.

2 Design and implement a secure network infrastructure.

3 Troubleshoot a secure network infrastructure.

4 Design and implement host-based security.



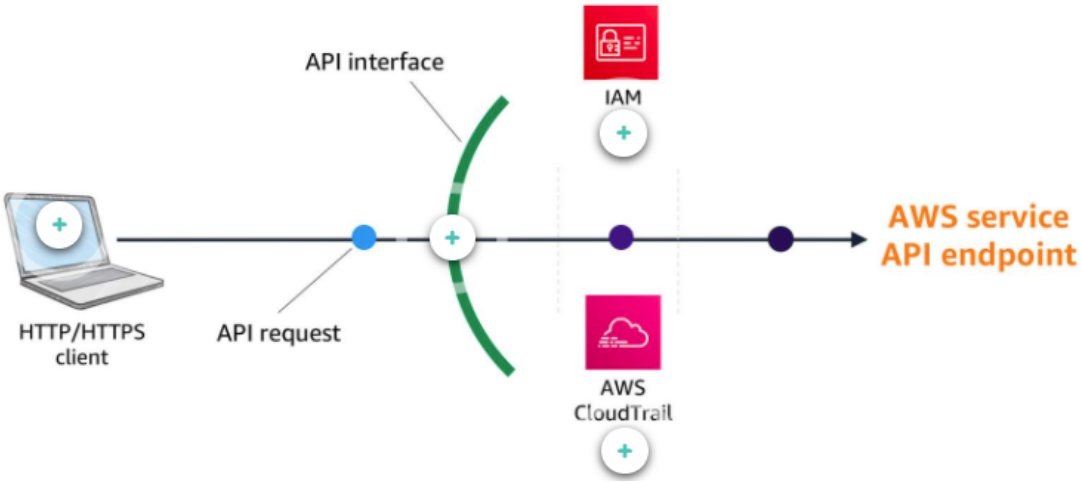
▼ IAM

For the exam, you should know how to:

1 Design and implement a scalable authorization and authentication system to access AWS resources.

2 Troubleshoot an authorization and authentication system to access AWS resources.

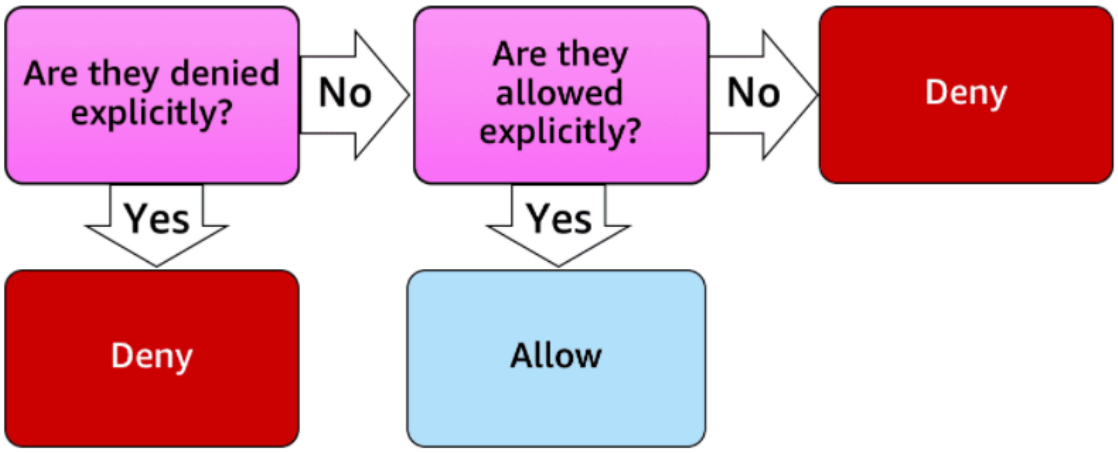
API request flow



Access policy types

AWS-managed	Customer-managed	inline

How IAM determines permissions


Are they denied explicitly?
No
Are they allowed explicitly?
No
Deny
Yes
Yes
Deny
Allow

Effect	Specifies whether the statement results in an allow or an explicit deny.	YES
Action	Describes the specific action or actions that will be allowed or denied.	YES
Resource	Specifies the object or objects that the statement covers.	YES
Condition	Specifies conditions for when a policy is in effect.	NO
Principle	Specifies the entity that is allowed or denied access to a resource. Used for resource-based or trust policies.	NO

Example IAM access policy

```
{
 "Version": "2012-10-17",
 "Statement": {
  "Effect": "Allow",
  "Action": ”sqs:GetQueueAttributes",
  "Resource": "*",
  "Condition" : {
   "DateGreaterThan" : {"aws:CurrentTime" : "2018-08-16T12:00:00Z"},
   "DateLessThan": {"aws:CurrentTime" : "2018-08-16T15:00:00Z"},
   "IpAddress" : {"aws:SourceIp" : ["192.0.2.0/24", "203.0.113.0/24"]}
  }
 }
```

▼ Data Protection

For the exam, you should know how to:

1 Design and implement key management.

2 Troubleshoot key management.

3 Design and implement a data encryption solution for data at rest and data in transit.

AWS tools for data protection

Amazon RDS

Amazon DynamoDB

AWS Secrets Manager

Amazon S3 Glacier

Amazon S3 Glacier Vault

Encryption primer