Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud

simplilearn

Cloud

Caltech | Center for Technology & Management Education

AWS SysOps Administrator – Associate Level

Security and Compliance

Learning Objectives

By the end of this lesson, you will be able to:

- Configure IAM and its policies
- Work with CloudTrail
- Upload objects to S3 buckets without AWS credentials or authorization.
- Configure Infrastructure protection strategy tools

A Day in the Life of an AWS Administrator

You are employed as an administrator in a company. Your company is considering moving its infrastructure to the cloud but is concerned about security. You've been asked to recommend a few security solutions available in AWS that meet the following criteria so that the organization may make a migration decision.

- They'd like an entity that can be attached to any AWS resource and define access permissions for that resource.
- The company doesn't want to give out long-term credentials (such usernames and passwords or access keys) to any server, therefore they'll need a solution that can provide temporary rights for applications to utilize when calling other AWS resources.

A Day in the Life of an AWS Administrator

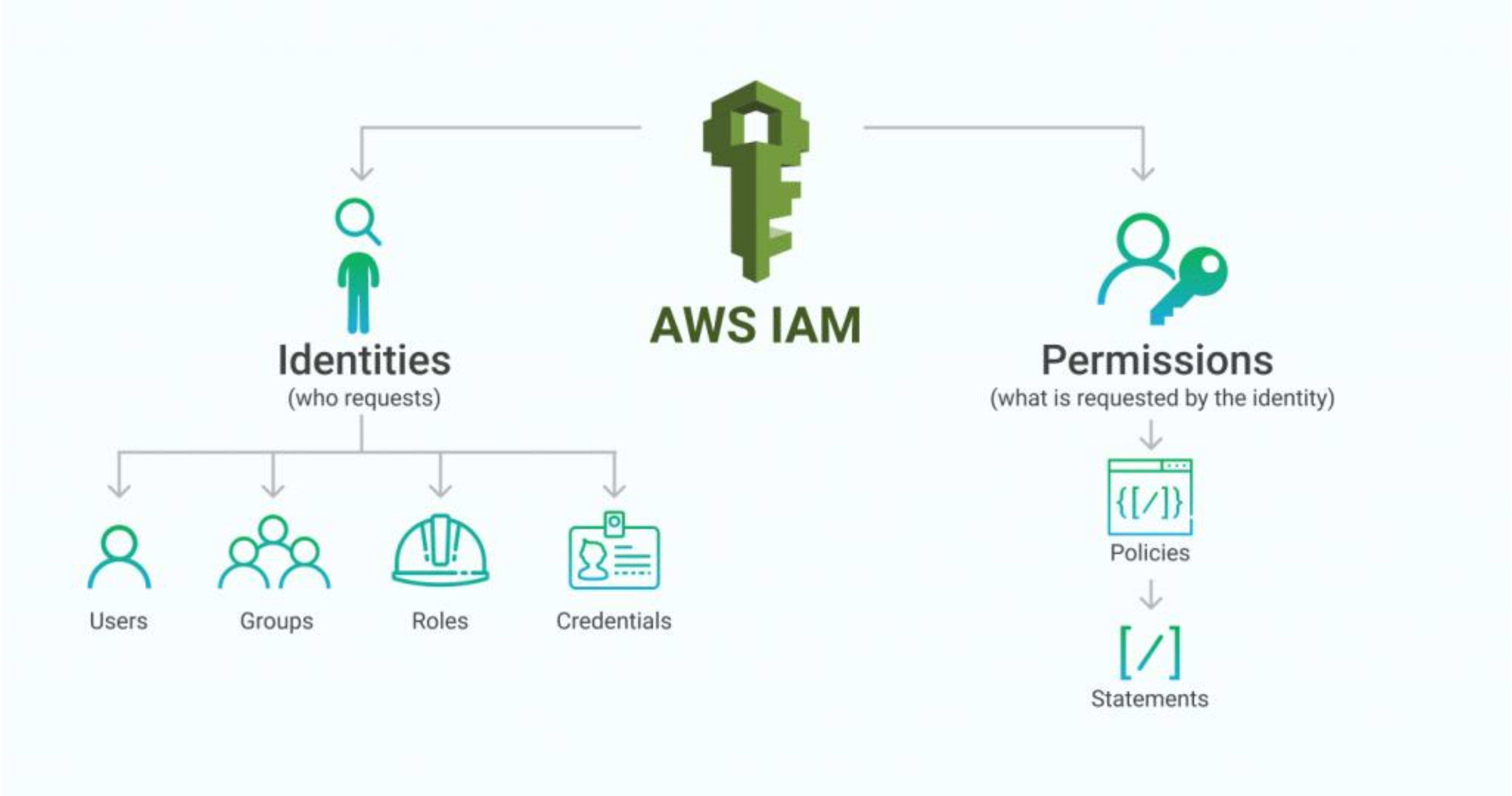
- They'd also want to look after the AWS account's governance, compliance, operational audits, and risk auditing.
- They also want to ensure that the security and compliance of the applications they've installed on AWS are up to standard.

To achieve all the above along with some additional features, you will be learning a few concepts in this lesson that will help you find solutions for the above-given scenario.

AWS Identity and Access Management (IAM)

IAM

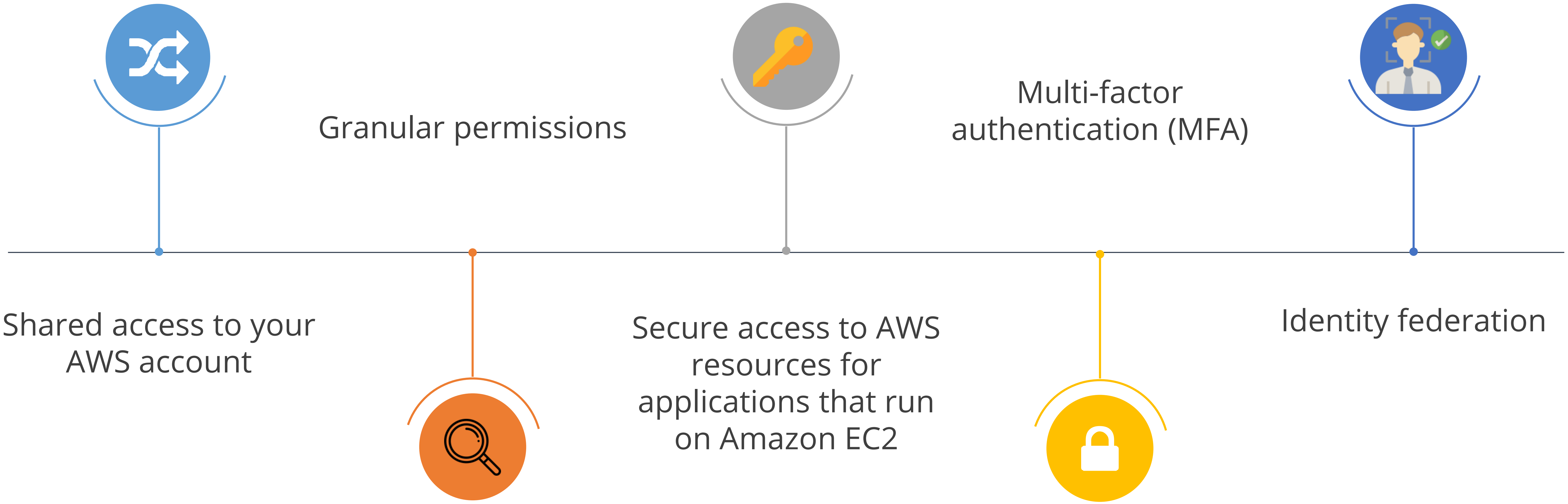
AWS Identity and Access Management (IAM) is a web service that allows the user to control the authorization of AWS resources.



IAM controls the authentication and authorization of the resources.

IAM Features

IAM provides the following features:



Shared access to your AWS account

Granular permissions

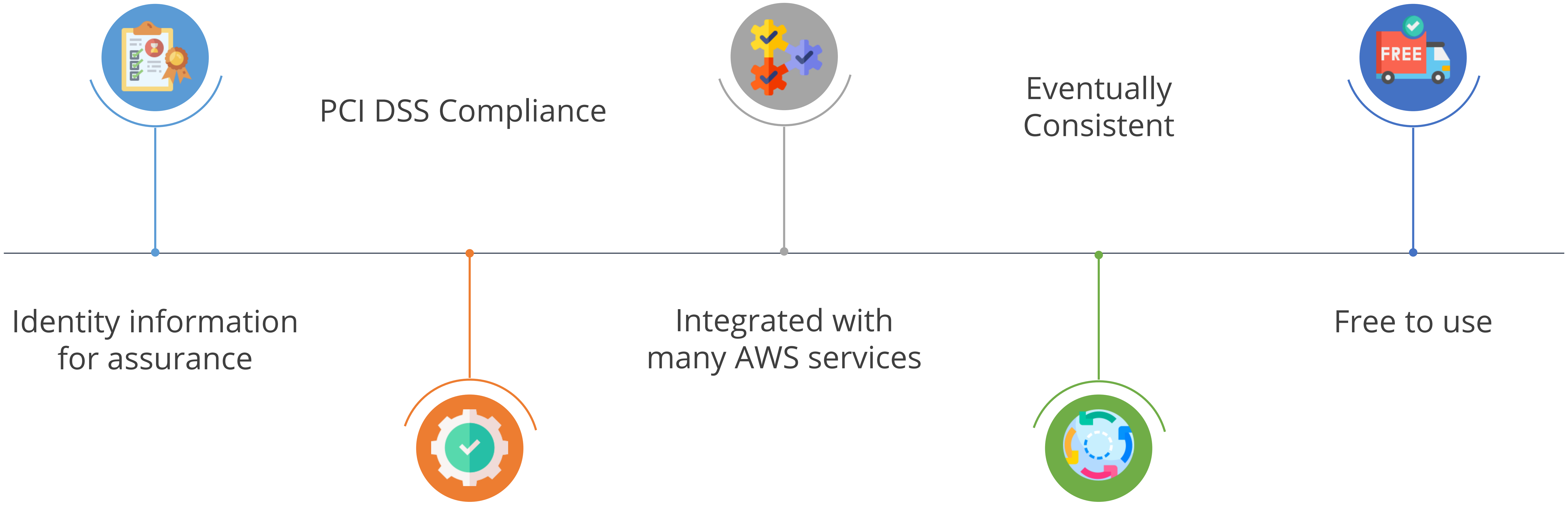
Secure access to AWS resources for applications that run on Amazon EC2

Multi-factor authentication (MFA)

Identity federation

IAM Features

IAM provides the following features:



Identity information for assurance

PCI DSS Compliance

Integrated with many AWS services

Eventually Consistent

Free to use

Password Policy

The following policy allows full access to view and edit the account password policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "FullAccessPasswordPolicy",
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountPasswordPolicy",
                "iam:DeleteAccountPasswordPolicy",
                "iam:UpdateAccountPasswordPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Assisted Practice

Custom IAM Policy

Duration: 10 Min.

Problem Statement:

You are given a project to create a Custom IAM Policy that is an entity that, when attached to an identity or resource, defines their permissions.

Assisted Practice: Guidelines

Steps to create and configure a custom IAM policy:

1. Login to AWS lab

2. Select **IAM** from **Services**

3. Select a policy from the menu on the left

4. Create a custom IAM policy

Multi-Factor Authentication

MFA provides additional security by requiring users to submit unique authentication from an AWS-supported MFA method in addition to their standard sign-in details when accessing AWS websites or services.

IAM Roles

An IAM role is an IAM identity that users can create in their account that has specific permissions and policies.

With IAM Roles, the user can:

- Delegate access to users, applications, or services
- Delegate access to AWS resources

IAM Roles

Assisted Practice

Roles and Instances

Duration: 10 Min.

Problem Statement:

You are given a project to create a Role and attach it to an EC2 instance to appropriately grant access permissions to an application that performs AWS API requests running on your EC2 instances. With IAM roles, you can avoid sharing long-term credentials and protect your instances against unauthorized access.

Assisted Practice: Guidelines

Steps to create and integrate roles and policies with S3 bucket:

1. Create an EC2 instance

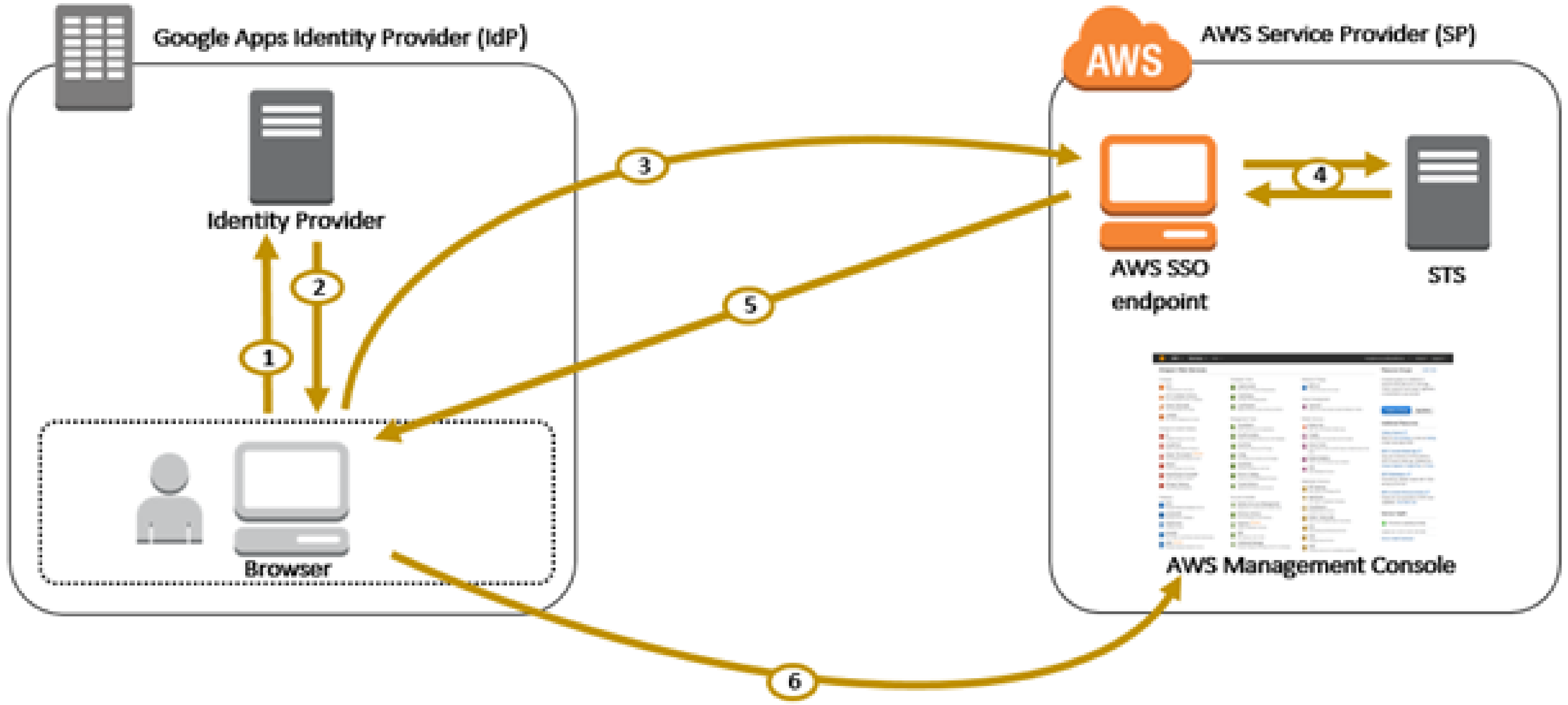
2. Create an IAM role

3. Connect EC2 instance

4. Attach the instance with the IAM role

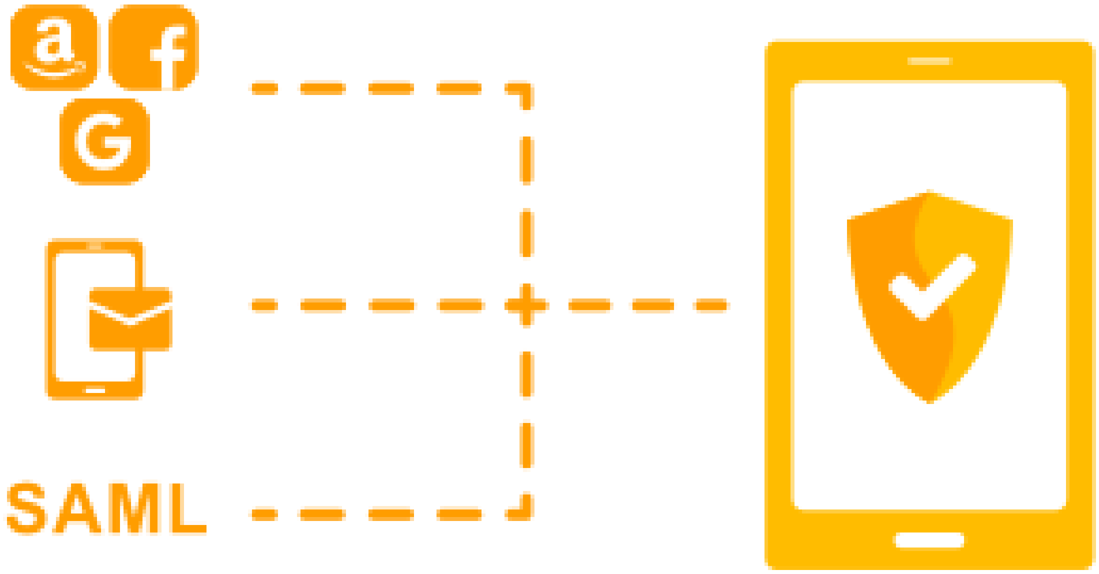
SAML

SAML 2.0 (Security Assertion Markup Language) is an open federation standard that enables an identity provider (IdP) to authenticate users and provide authentication and authorization information to a service provider (SP).



Federated Identity

Federated Identities (Amazon Cognito identity pools) allow you to build unique identities for your users and connect them to identity providers.



With an identity pool, the user can generate temporary or limited-access AWS credentials for other AWS services.

IAM Policy

There are two types of policies:

Identity-based policies

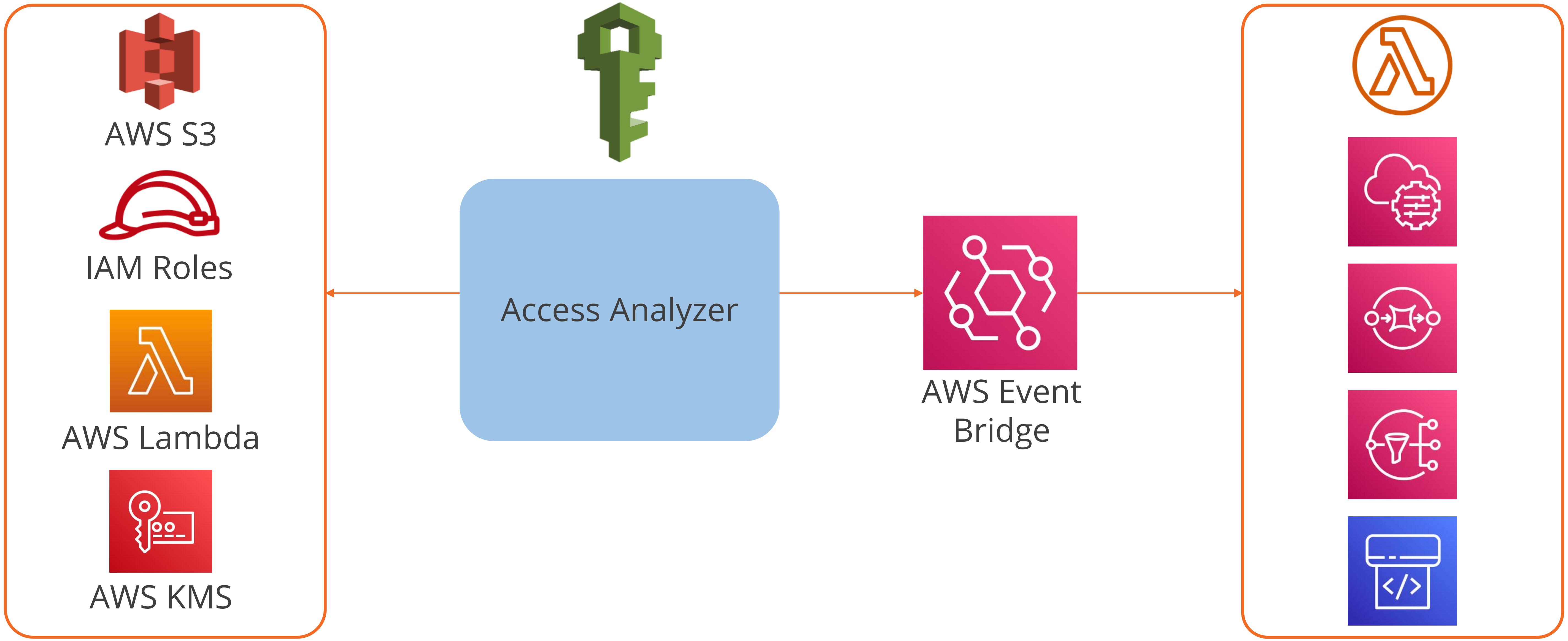
- Identity-based policies can be attached directly to identities such as users, groups, and roles.
- These policies define the permissions such as allow or deny for the identities.

Resource-based policies

- Resource-based policies are attached to AWS resources such as Amazon S3, Amazon EC2, and more.
- These policies define the permissions such as allow or deny for the AWS resources.

IAM Access Analyzer

IAM Access Analyzer identifies the resources that are shared with third parties by analyzing the resource-based policies in the AWS environment using logic-based reasoning.



IAM Policy Simulator

IAM policy simulator helps in testing and troubleshooting identity-based policies, IAM permissions boundaries, organizations' service control policies (SCPs), and resource-based policies.

Features

- Test policies that are attached to IAM users, user groups, or roles in your AWS account
- Test and troubleshoot the effect of permissions boundaries on IAM entities
- Test policies that are attached to AWS resources
- Test new policies that are not yet attached to a user, user group, or role by typing or copying them into the simulator

AWS Security and Compliance Policy Tools

Compliance Frameworks

The AWS Compliance Program provides detailed information about AWS security and compliance in the cloud.

The three major compliance frameworks are given below:

ISO 27001

ISO/IEC 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidelines.

- AWS performs the following operations:
  1. Evaluates the information security risks, taking into account the impact of threats and vulnerabilities
  2. Designs the suite of information security controls and risk management for customers

- AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014 and is managed by third-party auditors.
- It doesn't have any impact on the services used by the end user.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a US government program for security assessment, authorization, and continuous monitoring of cloud products and services.

- FedRAMP is important because it provides:

1. Consistency and confidence in the security of cloud solutions
2. Transparency between the US government and cloud providers
3. Real-time continuous monitoring
4. Automation and reuse of assessments and authorizations

- AWS FedRAMP compliance doesn’t result in increase in service cost.

Source: https://aws.amazon.com/compliance/fedramp/

HIPAA and HITECH

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a legislation that is designed to make it easy for US workers to retain health insurance coverage when they change or lose their jobs.

Health Information Technology for Economic and Clinical Health (HITECH) act is an expansion of HIPAA which includes a set of federal standards to protect the security and privacy of the Protected Health Information (PHI).

- AWS aligns the HIPAA risk management program with FedRAMP and NIST 800-53, which are higher security standards that map to the HIPAA Security Rule.
- HIPAA or HITECH doesn’t restrict end users from using any AWS services.

Source: https://aws.amazon.com/compliance/hipaa-compliance/

NIST

The National Institute of Standards and Technology (NIST) 800-53 security controls are generally applicable to the US Federal Information System.

- The Federal Information System typically follows the formal assessment and authorization process to ensure protection of confidentiality, integrity, and availability of information and information system.

- The NIST Cybersecurity Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by any organization.

- AWS Cloud infrastructure and services have been validated by third-party testing performed against the NIST 800-53 Revision 4 controls.

Source: https://aws.amazon.com/compliance/nist/

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council.

- PCI DSS applies to all entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD), including merchants, processors, acquirers, issuers, and service providers.
- The PCI DSS Attestation of Compliance (AOC) and Responsibility Summary is available to customers by using AWS Artifact, a self-service portal for on-demand access to AWS compliance reports.
- The compliance assessment was conducted by Coalfire Systems Inc., an independent Qualified Security Assessor (QSA).

Source: https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

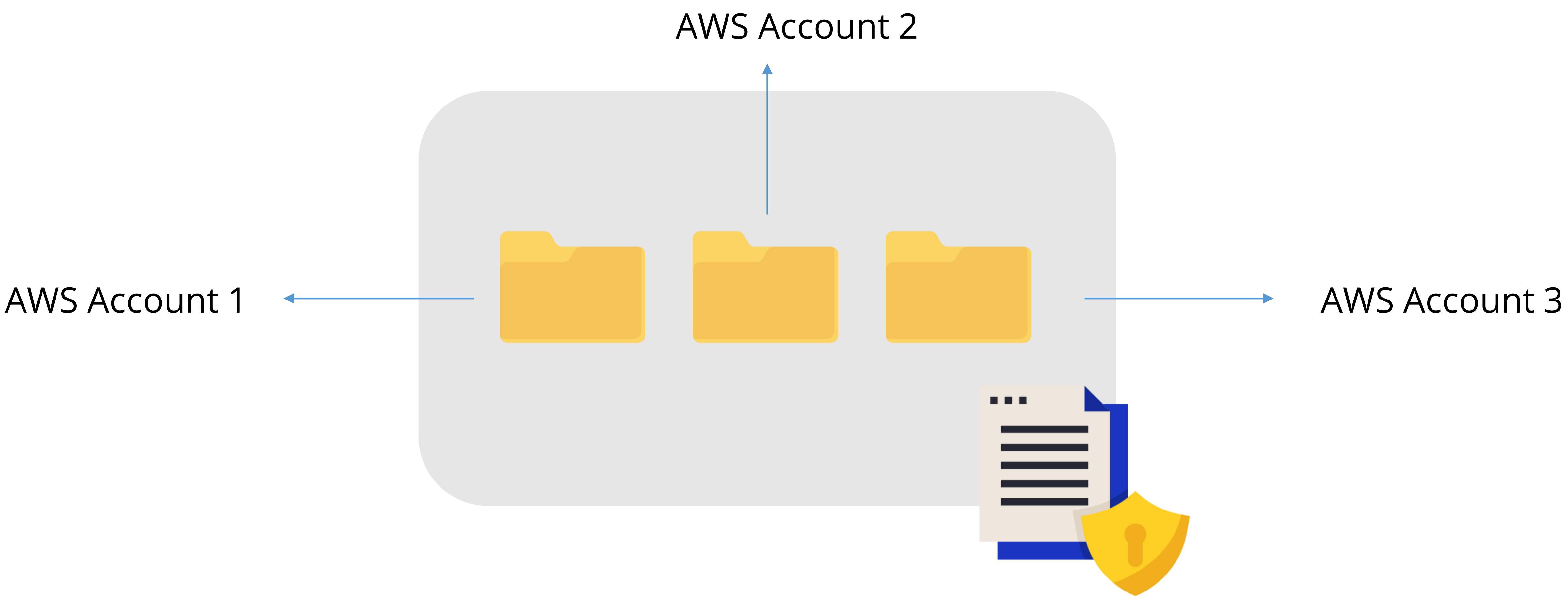
Service Control Policies

SCPs are a sort of organizational policy that users can use to manage permissions in the organization.

SCPs provide centralized management of the maximum available permissions for all accounts in the organization.

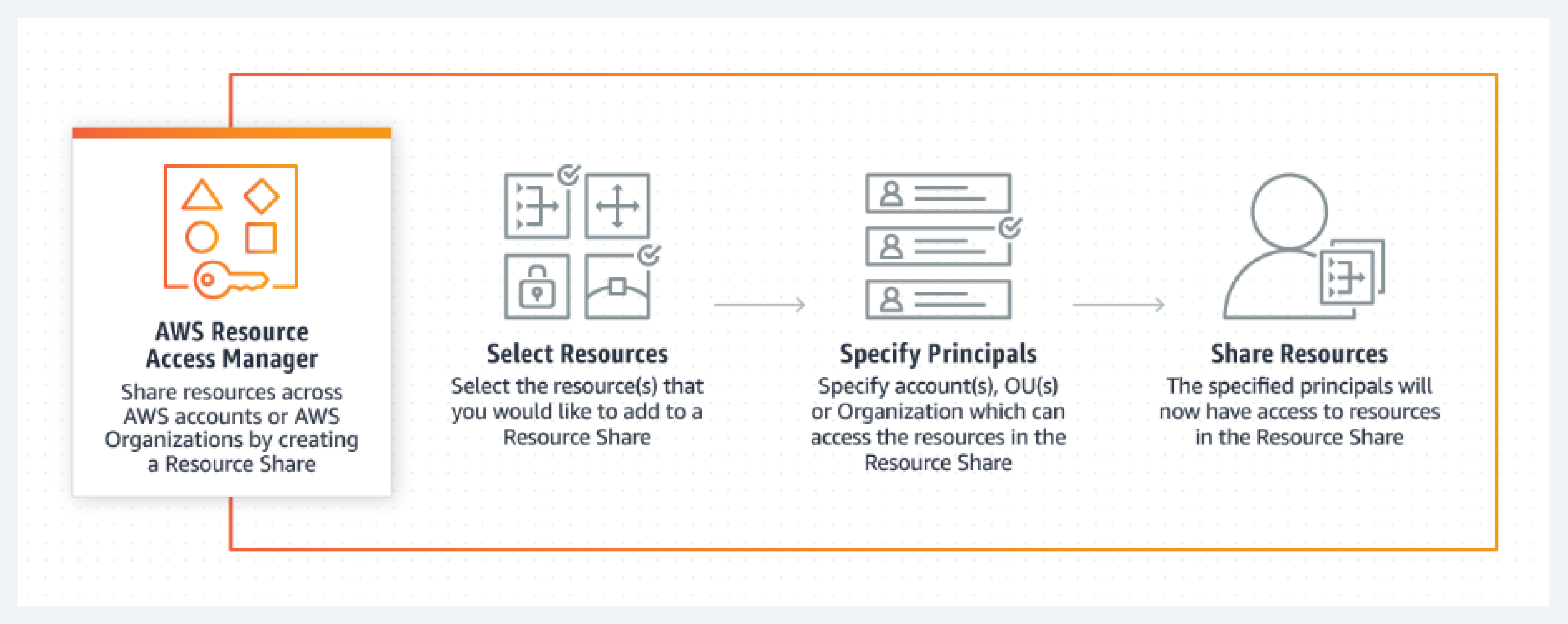
AWS Resource Access Manager

AWS Resource Access Manager or AWS RAM allows you to share your AWS resources securely with any AWS account. Users can create AWS resources centrally in a multi-account environment.



AWS RAM

The following diagram shows the working of AWS RAM:



AWS Resource Access Manager

Share resources across AWS accounts or AWS Organizations by creating a Resource Share

Select Resources

Select the resource(s) that you would like to add to a Resource Share

Specify Principals

Specify account(s), OU(s) or Organization which can access the resources in the Resource Share

Share Resources

The specified principals will now have access to resources in the Resource Share

Source: aws.amazon.com

AWS Trusted Advisor

Trusted Advisor examines the AWS setup and gives recommendations where there are chances to save money, increase system availability and performance, or eliminate security breaches.

Trusted Advisor incorporates best practices learned from supporting hundreds of thousands of AWS customers.

AWS Trusted Advisor Plans

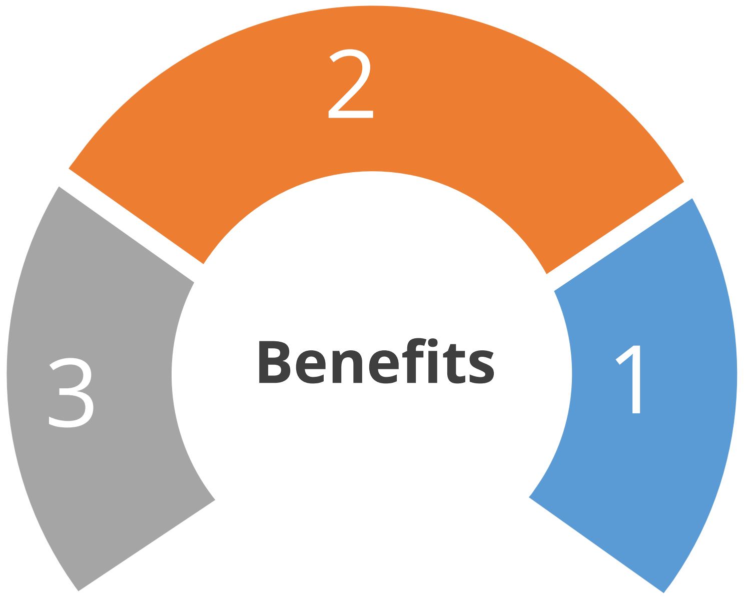
There are two types of plans available in AWS Trusted Advisor:

Basic or Developer Support plan

Business or Enterprise Support plan

AWS Control Tower

AWS Control Tower is the simplest way to set up and manage a secure, multi-account AWS environment known as a landing zone.



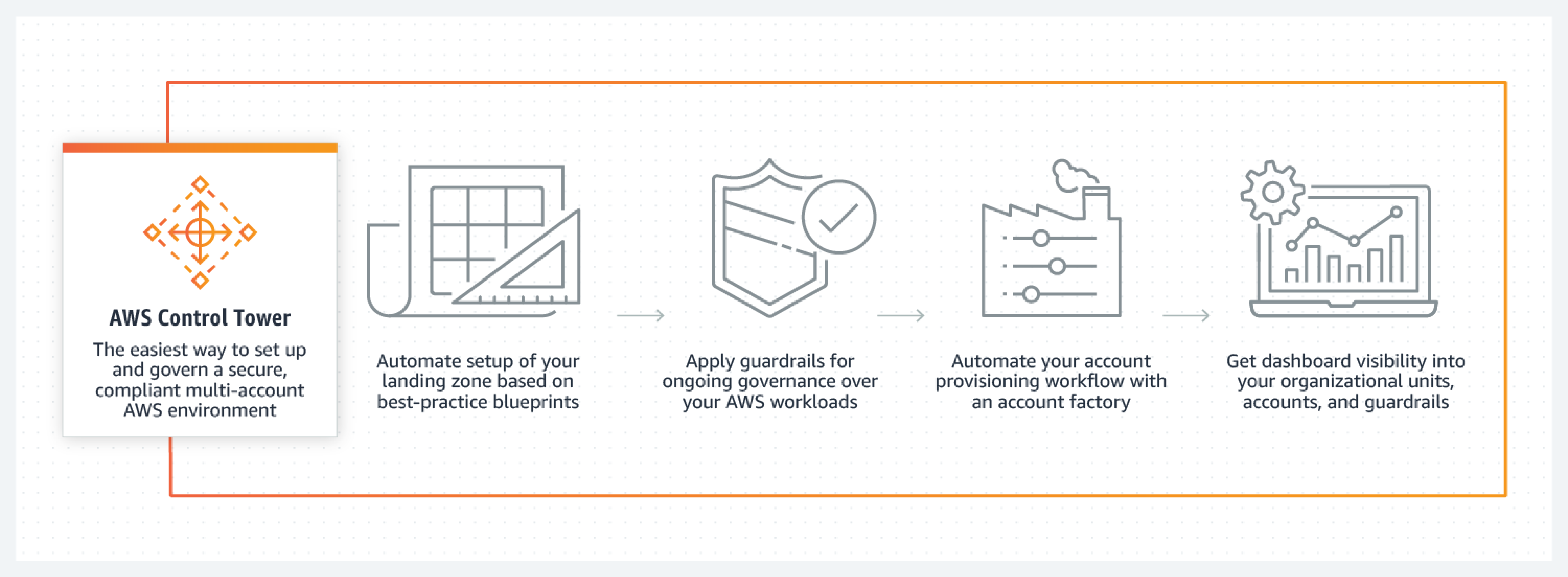
Automate ongoing policy management

View policy-level summaries of AWS environment

Quickly setup and configure a new AWS environment

AWS Control Tower

The following diagram shows the working of AWS Control Tower:



AWS Control Tower

The easiest way to set up and govern a secure, compliant multi-account AWS environment

Automate setup of your landing zone based on best-practice blueprints

Apply guardrails for ongoing governance over your AWS workloads

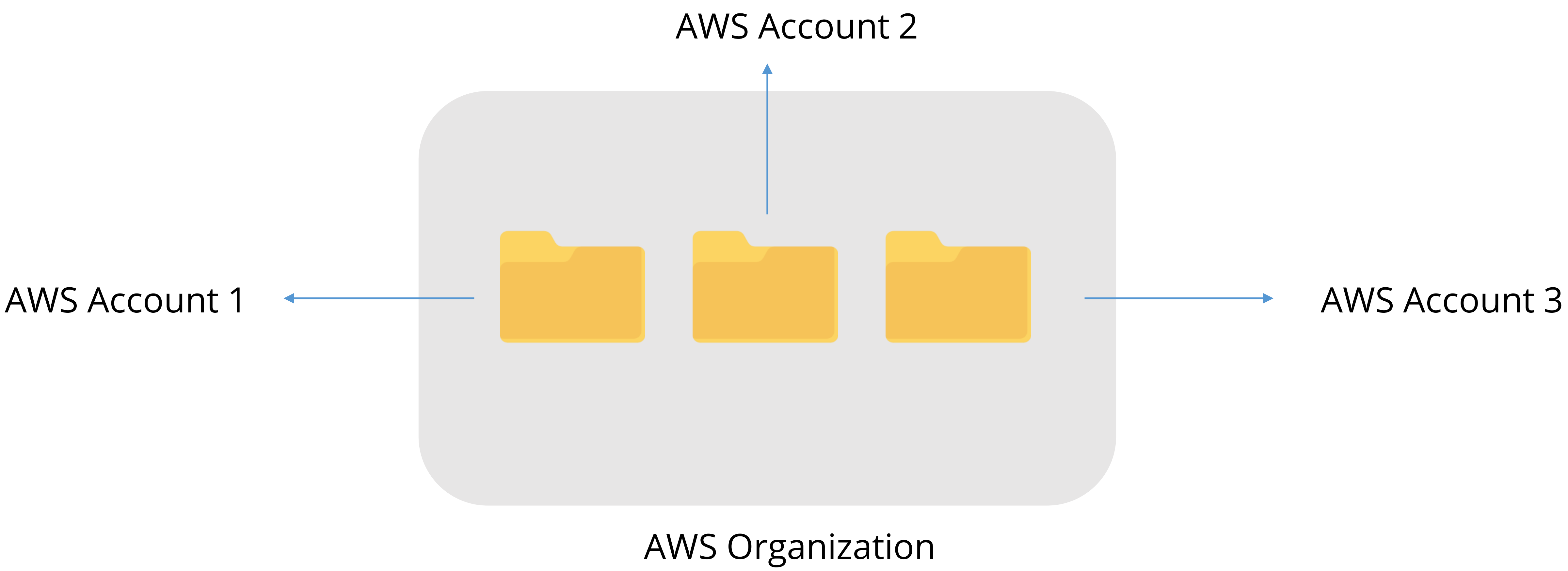
Automate your account provisioning workflow with an account factory

Get dashboard visibility into your organizational units, accounts, and guardrails

Source: https://aws.amazon.com

AWS Organization

AWS Organization is an account management service that allows users to consolidate multiple AWS accounts into a group called an organization that they can create and manage centrally.



AWS Organization

AWS Organization is used with AWS RAM to share resources across a group of AWS accounts. It helps to centrally manage billing, control access, compliance, and security across the member AWS accounts of the organization.

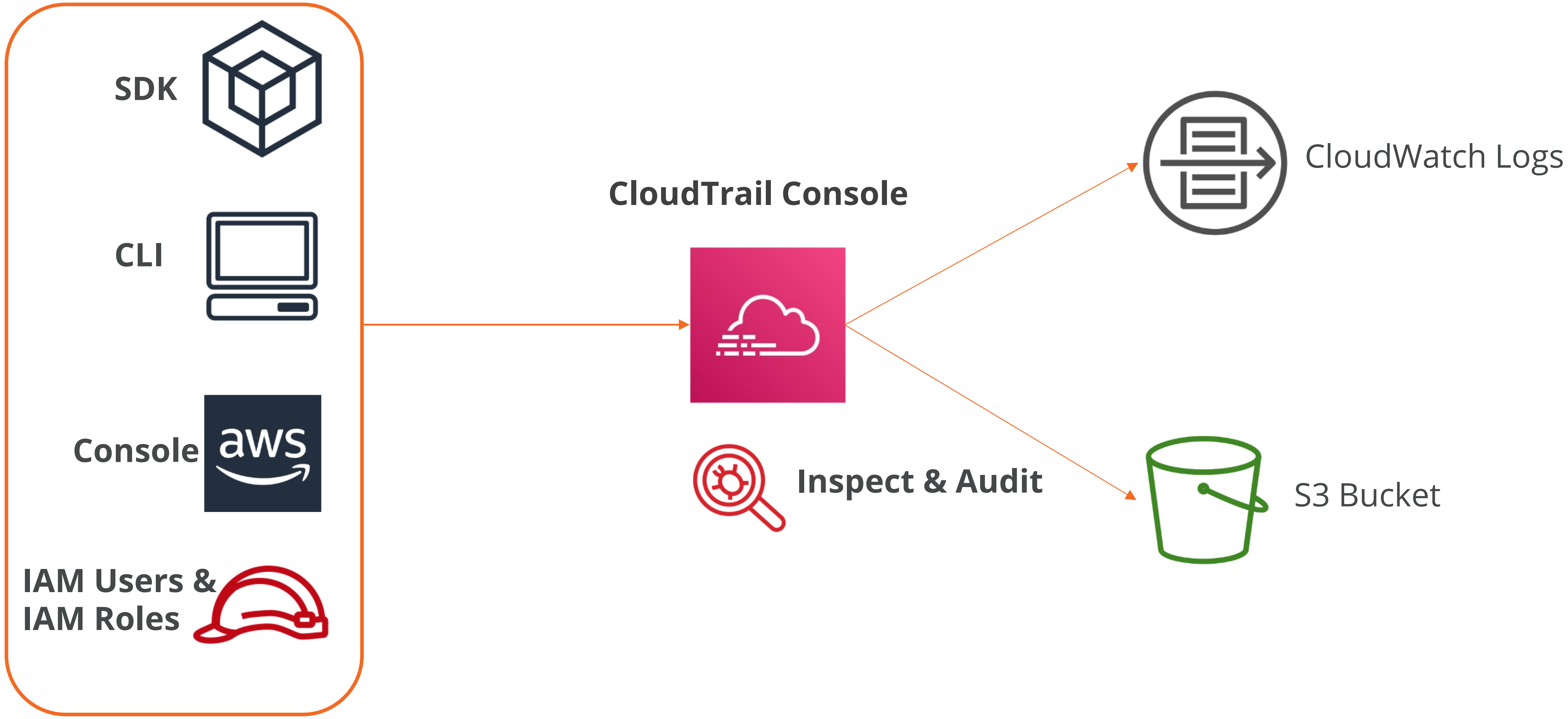
Points to Remember

- Accounts are grouped into logical groups called Organizational Units (OUs).
- The parent container for all the accounts in all OUs is called the root.
- The OU that contains the member AWS accounts is called the custom OU.
- The OU that contains the log archive account and details such as what resources are being shared among the accounts is called the core.

AWS CloudTrail

CloudTrail Overview

AWS CloudTrail is a service that provides AWS account governance, compliance, audit, and risk management.



CloudTrail - Validating Logs

CloudTrail log file integrity validation can help the user to verify whether a log file was updated, deleted, or kept unchanged after CloudTrail distributed it.

This functionality is designed with industry-standard techniques, including SHA-256 for hashing and SHA-256 plus RSA for digital login.

CloudTrail - Turning It On

There are three ways to enable CloudTrail log files:

- AWS Management Console
- AWS CLI
- CloudTrail API

CloudTrail - Turning It On

AWS Management Console

To enable the log file with the AWS CloudTrail console, choose **Yes** for the **Enable log file validation** option while creating or updating a trail.

AWS CLI

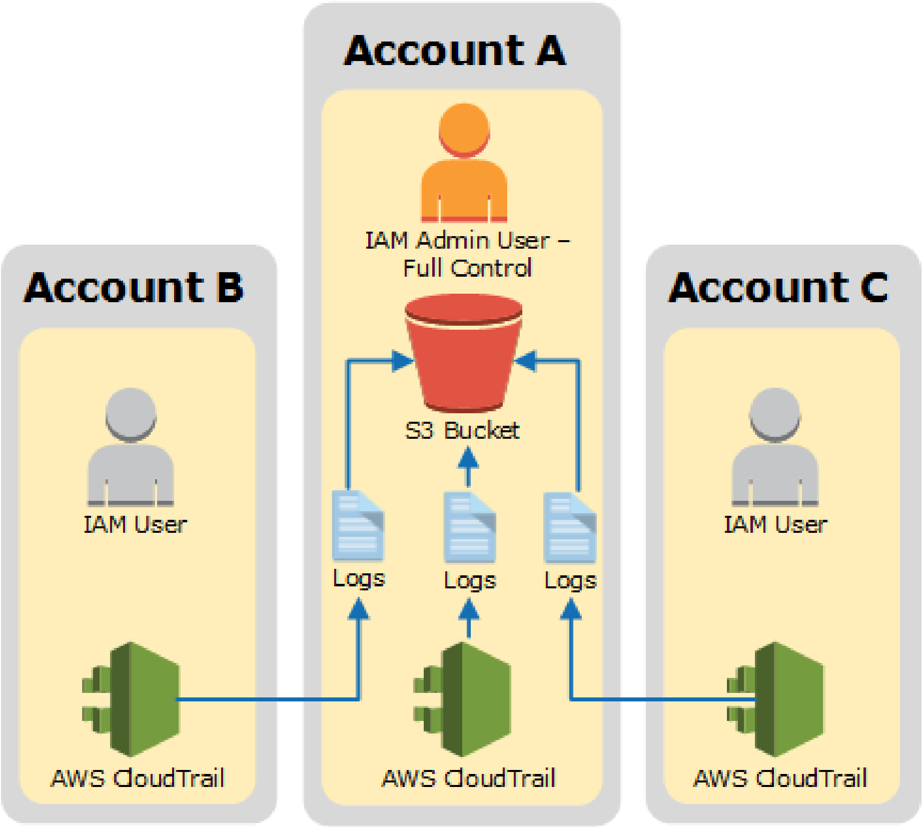
To enable log file with the AWS CLI, use **--enable-log-file-validation** command with create-trail or update-trail commands.

CloudTrail API

To enable log file integrity validation with the CloudTrail API, set **EnableLogFileValidation -> True** while updating or creating.

Protecting Logs

AWS is responsible for securing the global infrastructure that maintains the AWS Cloud. Users are responsible for keeping control of the content stored on this infrastructure.



AWS shared repository model applies to protect logs in CloudTrail.

Protecting Logs

These are the ways to apply for data protection in AWS CloudTrail:

- Use Multi-Factor Authentication (MFA) with each account
- Use SSL/TLS to communicate with AWS resources
- Set up API and user activity logging with AWS CloudTrail
- Use AWS encryption solutions, along with all default security controls within AWS services
- Use advanced managed security services such as Amazon Macie

Assisted Practice

AWS CloudTrail

Duration: 10 Min.

Problem Statement:

You are given a project to demonstrate CloudTrail that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

Assisted Practice: Guidelines

Steps to create and configure CloudTrail:

1. Login to AWS lab
2. Select **CloudTrail** from **Services**
3. Create a trail
4. Select the S3 bucket to store log files

Security in S3

Pre-signed URLs with S3

Users have the option to share objects via a pre-signed URL or allow their customers to upload objects to S3 buckets without AWS credentials or authorization.

Limiting pre-signed URL capabilities:

- Users can build AWS Identity and Access Management (IAM) policies that require a specific network path if they wish to restrict the use of pre-signed URLs and all S3 access to specific network paths.
- If you're using Amazon S3's public endpoint, use **aws:SourceIp**.
- If you're connecting to Amazon S3 through a VPC endpoint, use **aws:SourceVpc** or **aws:SourceVpce**.

S3 – Restrict IP Addresses

To restrict the IP addresses for Amazon S3 buckets, follow these steps:

- Create a unique CloudFront user called an Origin Access Identity (OAI) and link it to your distribution.
- Configure your S3 bucket permissions so that CloudFront can use the OAI to access and deliver files in your bucket.
- Make sure that users cannot access a file in the S3 bucket by using a direct URL.

This will allow users to access your files through CloudFront, not directly from the S3 bucket.

S3 – Restrict IP Addresses

The following code is a bucket policy that restricts traffic to the bucket unless the request is from a particular VPC endpoint (**aws:sourceVpce**):

```
{ "Id": "VPCe",
"Version": "2012-10-17",
"Statement": [
{ "Sid": "VPCe",
"Action": "s3:*",
"Effect": "Deny",
"Resource":
[ "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
"arn:aws:s3:::DOC-EXAMPLE-BUCKET/*" ],
"Condition":
{ "StringNotEquals": { "aws:SourceVpce":
[ "vpce-1111111", "vpce-2222222" ] } },
"Principal": "*" } ] }
```

S3 – Origin Access Identity (OAI)

OAI is a special CloudFront user which helps to access and deliver the files of a bucket.

A user can create a CloudFront OAI in two different ways:

CloudFront Console

Can simultaneously create an OAI and add it to the distribution

CloudFront API

Creates an OAI, which can be included later in the distribution

S3 Encryption

Amazon S3 default encryption is used to set the default encryption behavior for an S3 bucket. This is done so that all the new objects are encrypted when they are stored in the bucket.

The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or customer master keys (CMKs) stored in AWS Key Management Service (AWS KMS).

S3 Encryption

When you use server-side encryption, Amazon S3 encrypts an object before saving it to the disk and decrypts it when you download the objects.

Assisted Practice

Bucket Policy with Wildcards

Duration: 10 Min.

Problem Statement:

You are given a project to implement the bucket policies to grant other Amazon Web Services accounts or IAM users access permissions for the bucket and the objects in it.

Assisted Practice: Guidelines

Steps to implement bucket policies with wildcards:

1. Configure IAM role and create an S3 bucket
2. Launch an EC2 instance
3. Attach an S3 bucket policy with wildcards

Infrastructure Protection Strategy Tools

AWS Hypervisor

Hypervisor or virtual machine monitor (VMM) is the software, firmware, or hardware that creates and runs a VM.

- The computer on which the hypervisor runs is called the host machine, and all other VMs are called guest machines.
- EC2 currently runs on Xen hypervisor.
- It can have either paravirtualization (PV) or hardware virtual machines (HVM).
- The VMs on the hypervisor are unaware that the processing time is shared between all the VMs.
- PV is a faster and lighter form of virtualization.

AWS Service Quotas

Service Quotas is an AWS service that allows users to manage their quotas for several AWS services from a single location.

A user can request a quota increase through the Service Quotas console in addition to checking up quota values.

AWS KMS Overview

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for the user to create and control Customer Master Keys (CMKs).

AWS KMS

CMKs are encryption keys used to encrypt the data.

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM) manages the complexity of creating, storing, and renewing public and private SSL/TLS certificates and keys that protect the AWS websites and applications.

- Free public certificates for ACM-integrated services
- Managed certificate renewal
- Get certificates easily

AWS VPN Overview

AWS Virtual Private Network connects the on-premises networks, remote offices, client devices, and the AWS global network in a secure manner.

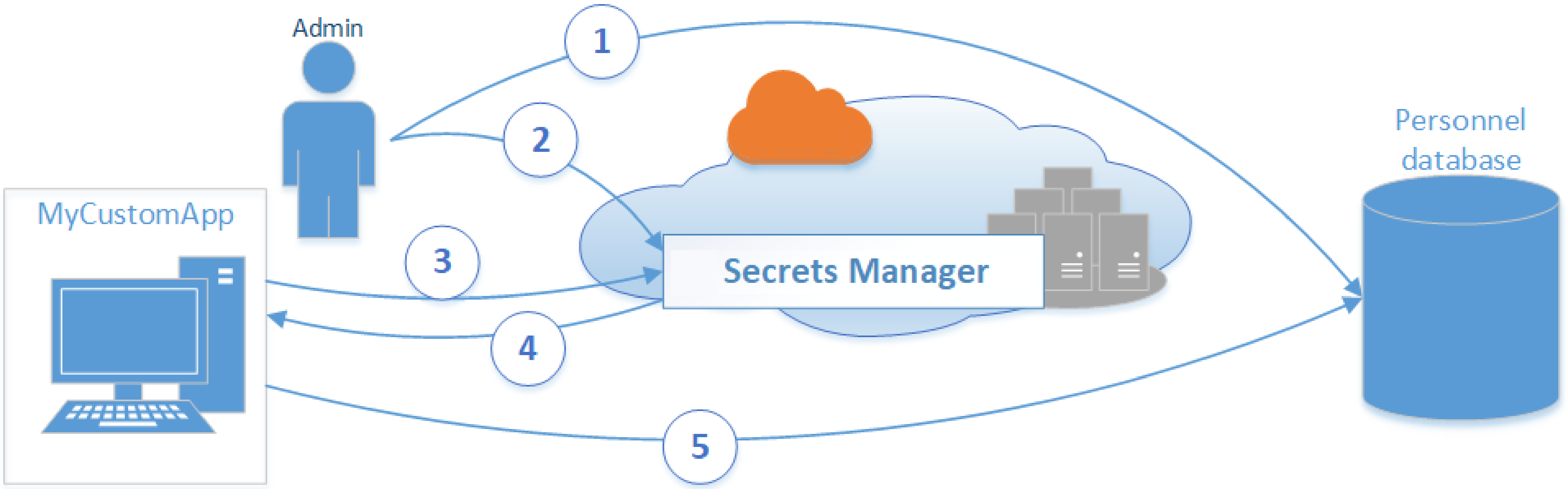
Systems Manager

AWS Systems Manager is a tool that provides visibility and control of the entire AWS infrastructure to the user.

- It integrates with Cloudwatch which allows user to view the dashboard, operational date, or reporting bugs.
- It also includes Run command to automate operational tasks such as security patching.
- It also organizes the inventory by grouping resources by application or environment.

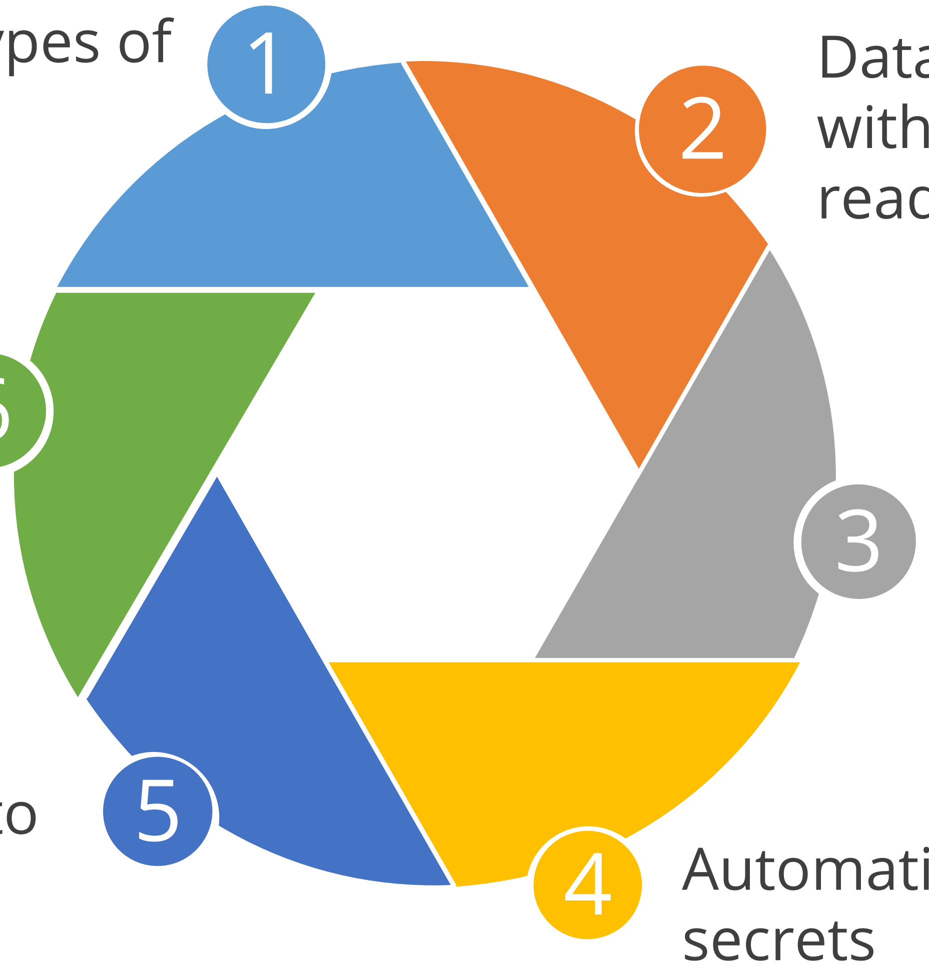
AWS Secret Manager

Secrets Manager is a service that makes it simple to rotate, manage, and recover hard-coded credentials, API keys, and other secrets at any point in their lifecycle.



Secret Manager Features

These are the features of AWS Secret Manager:



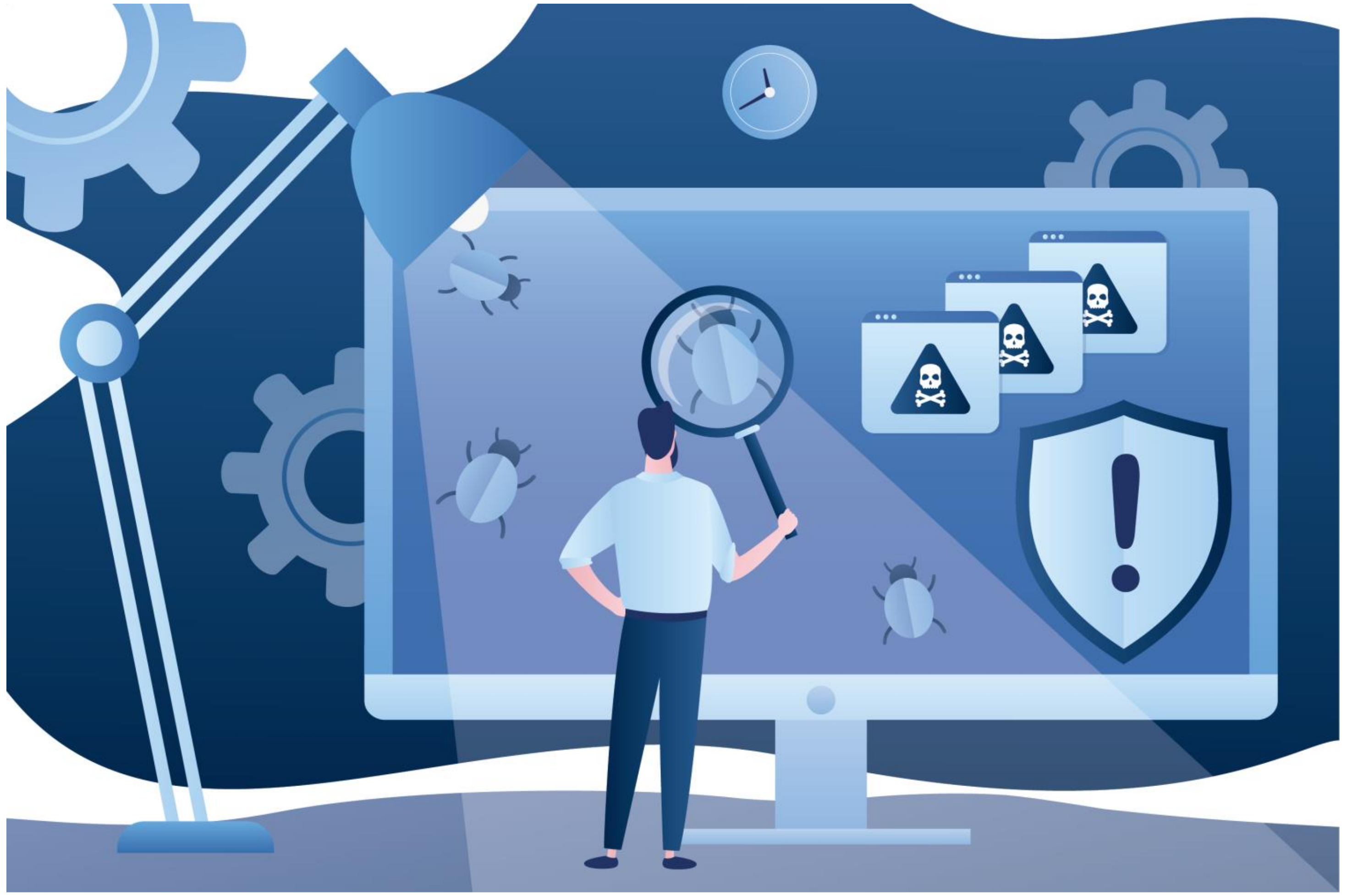
1. Storing different types of secrets
2. Databases and other services with fully configured and ready-to-use rotation support
3. Encrypting your secret data
4. Automatically rotating your secrets
5. Control access to secrets
6. Programmatically retrieve encrypted secret values at runtime

AWS Security Hub

AWS Security Hub gives a complete view of your AWS security state and assists you in comparing your environment to security industry standards and practices.

AWS GuardDuty

Amazon GuardDuty is a threat detection service that watches for harmful activity and unauthorized behavior to secure the AWS accounts, workloads, and data stored in Amazon S3.



Amazon Inspector

Amazon Inspector is an automated security evaluation service that aids in the security and compliance of AWS-hosted applications.

Inspector checks applications for exposure, vulnerabilities, and deviations from recommended practices automatically.

Amazon Inspector Vs Trusted Advisor

These are the difference between Amazon Inspector and Trusted Advisor:

Inspector	Trusted Advisor
Applies to the content of multiple EC2 instances	Applies to the AWS account and AWS services
No impact on performance	Improves performance by checking service limits
No cost recommendations	Recommendations to optimize cost
Amazon Elastic Compute Cloud (Amazon EC2) instances configuration	AWS account and administrators
Requires an agent	Does not require an agent

SRM

Shared responsibility model (SRM) states which security entities and dependencies are managed by AWS and what is the role of the customers in securing their data.

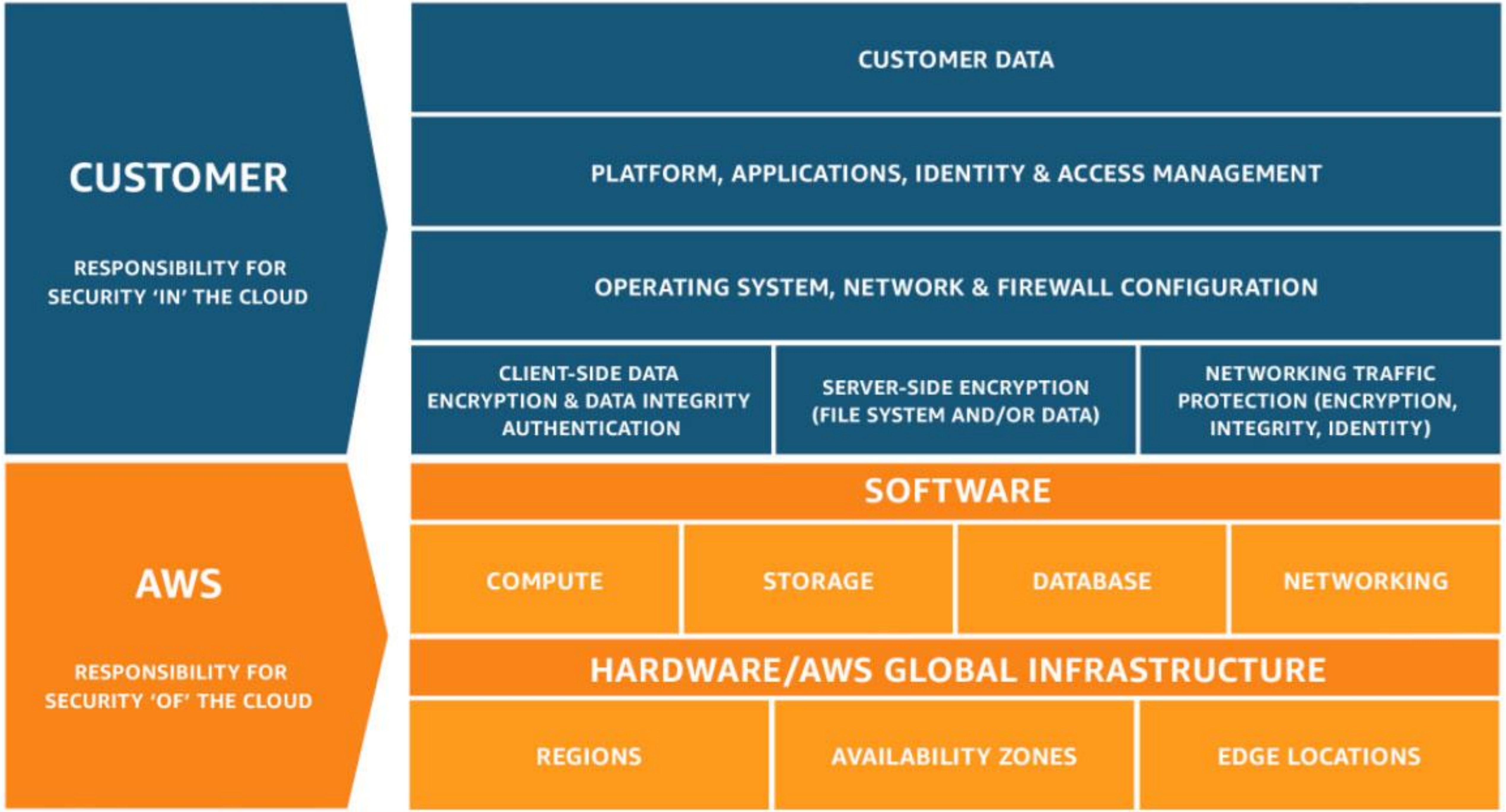
- It reduces the customer’s operational dependencies, as AWS operates, manages, and controls all components of the platform.

- Responsibility is divided into two parts:

  - **Security of the cloud (by AWS):** AWS ensures the security of the infrastructure on which all the services are running including, hardware, software, and networking facilities.

  - **Security in the cloud (by customer):** The customer is responsible for securing data using the services present in AWS by determining the amount of configurations to be set for used services.

SRM Division



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

Assisted Practice

AWS Config with S3

Duration: 10 Min.

Problem Statement:

Create and assign SSM run command for S3.

Assisted Practice: Guidelines

Steps to use AWS config with S3:

1. Selecting S3 bucket
2. Creating config rules for S3

Key Takeaways

- AWS Identity and Access Management (IAM) is a web service that allows the user to control the authorization of AWS resources.
- AWS Offers Multi Factor Authentication for additional security.
- AWS Organization is an account management service that allows users to consolidate multiple AWS accounts into a group.
- AWS CloudTrail is a service that provides AWS account governance, compliance, audit, and risk management.
- Hypervisor or virtual machine monitor (VMM) is the software, firmware, or hardware that creates and runs a VM.

Lesson-End Project

Duration: 60 min.

Implementing CloudTrail Using AWS IAM

Problem Statement:
Create and configure CloudTrail with an attached custom policy and control access to the log files.

Background of the problem statement:
The AWS team wants to implement CloudTrail that has an attached Read and Write custom policy and configured control access to the log files.