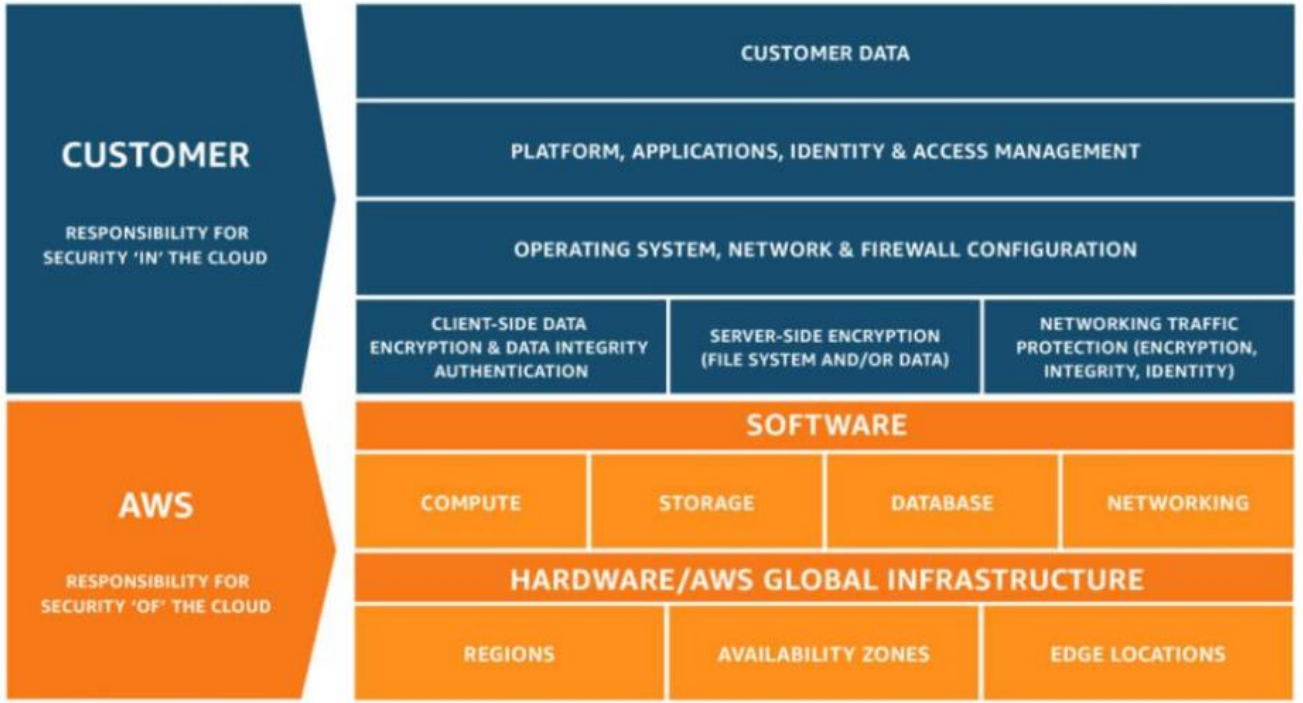
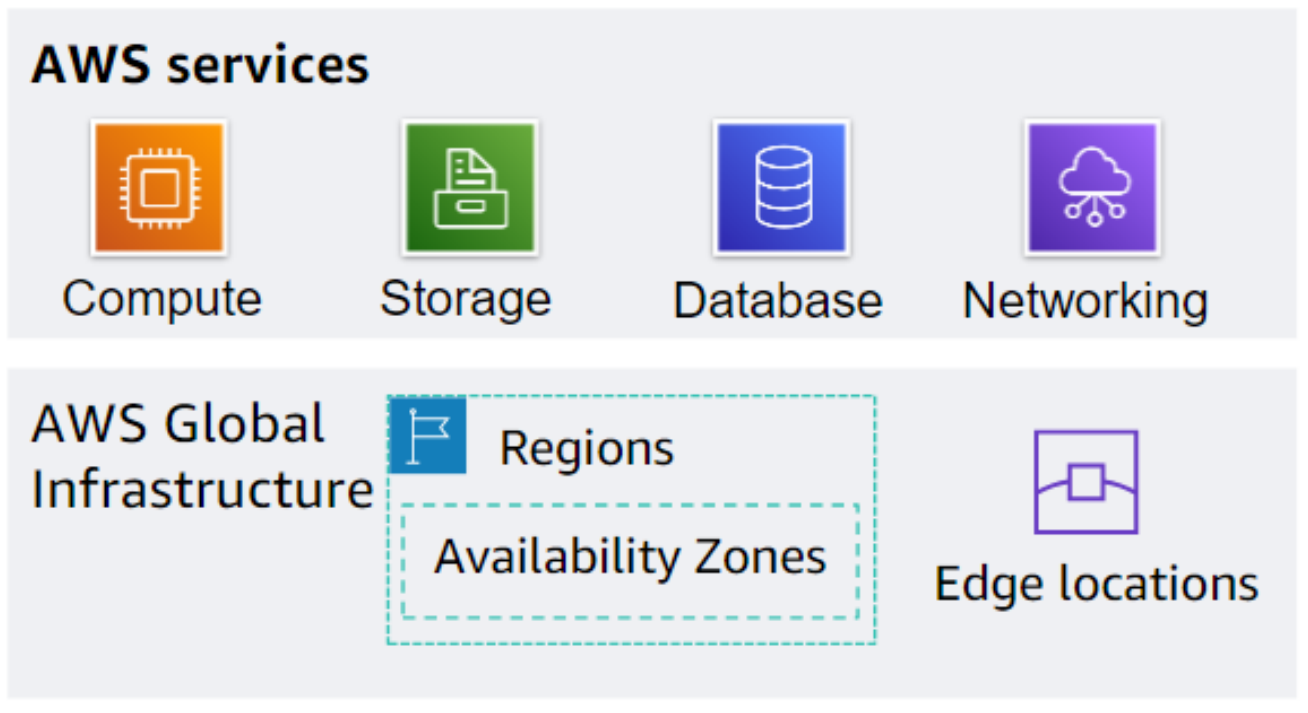
CLOUD SECURITY

By: Alayna Lee

SHARED RESPONSIBILITY MODEL

AWS has security responsibilities, and the user has some responsibilities



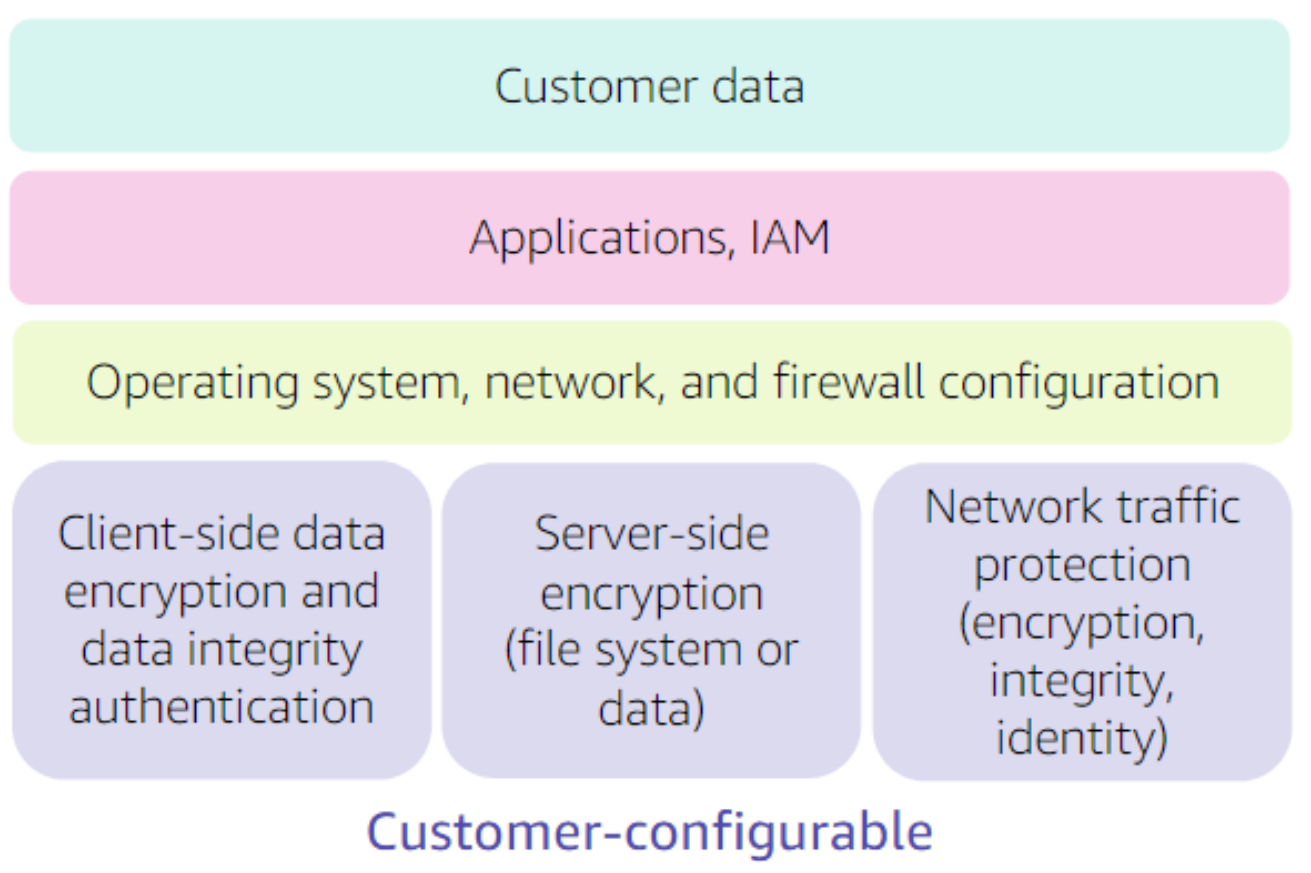


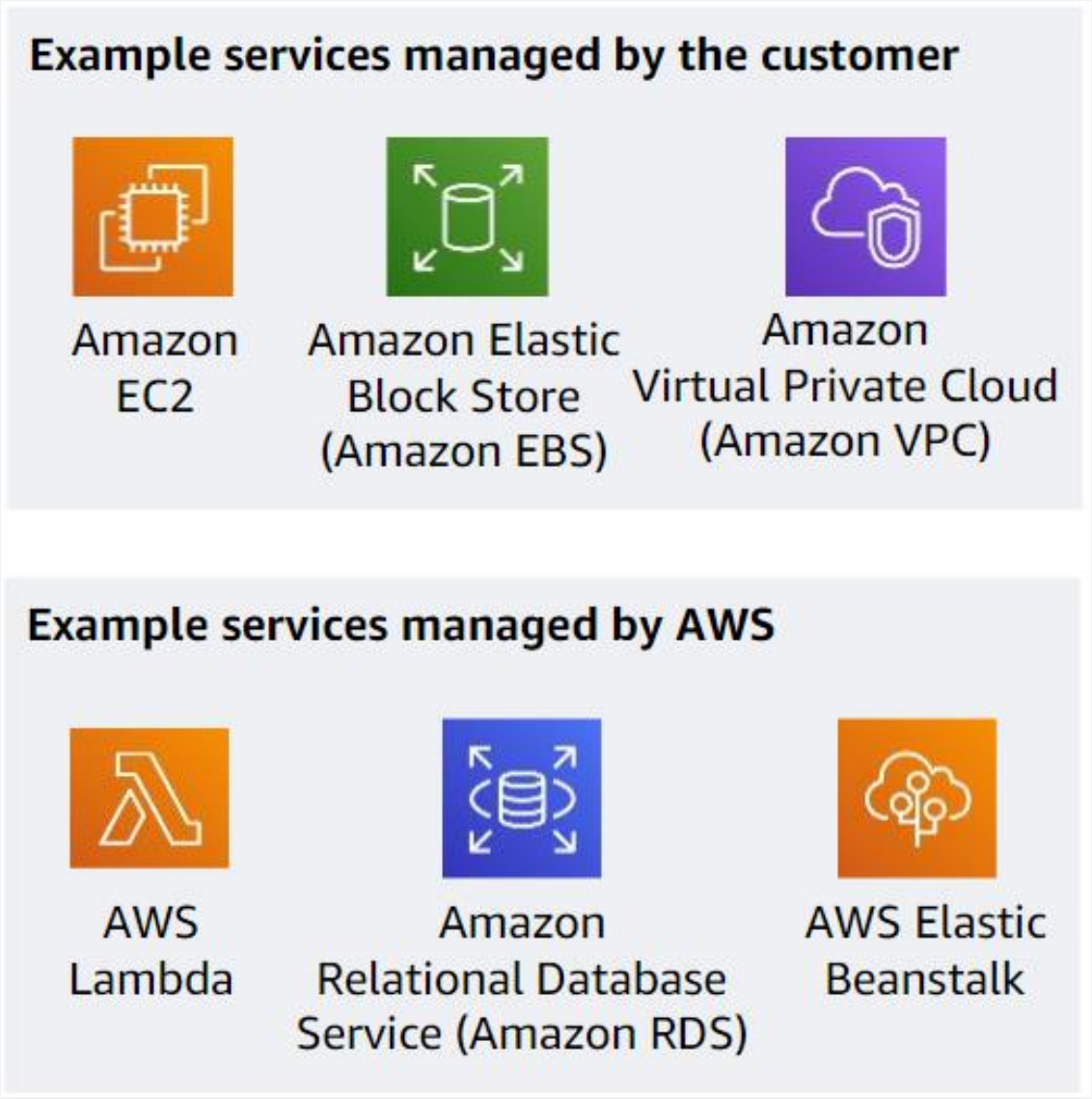
AWS SECURITY (IN DEPTH)

- AWS is responsible for the things ON the cloud
- HARDWARE:
  - Data centers
  - Edge zones
  - Availability zones
- SOFTWARE:
  - Computing
  - Storage
  - Database
  - Networking

CUSTOMERS SECURITY (IN DEPTH)

- The costumer is responsible for the things IN the cloud
- Customer data
- Applications + polices/access
- OS, networking, firewall configuration





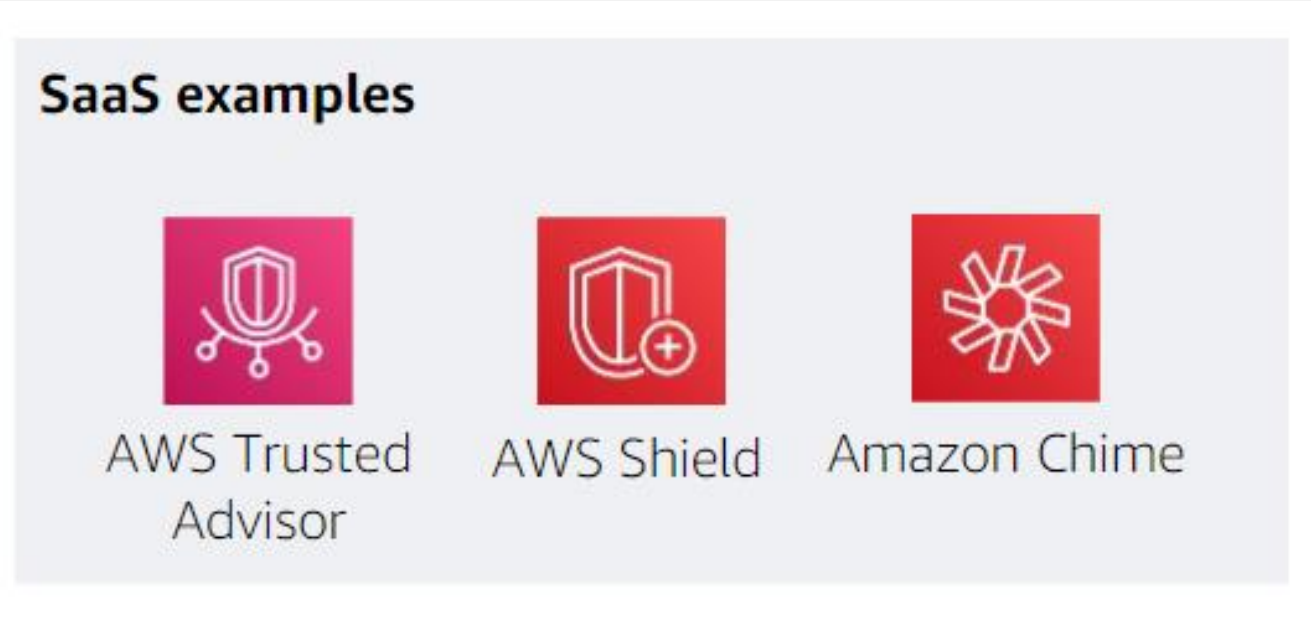
PAAS AND PAAS

- Infrastructure as a service
- Allows users to have more control over their services

- Platform as a service
- AWS handles and manages most of the service so that the user can focus more on the coding and data

SAAS

- Software as a service
- This provides full out of the box solutions for the user.
- User does not need to manage any of the infrastructure

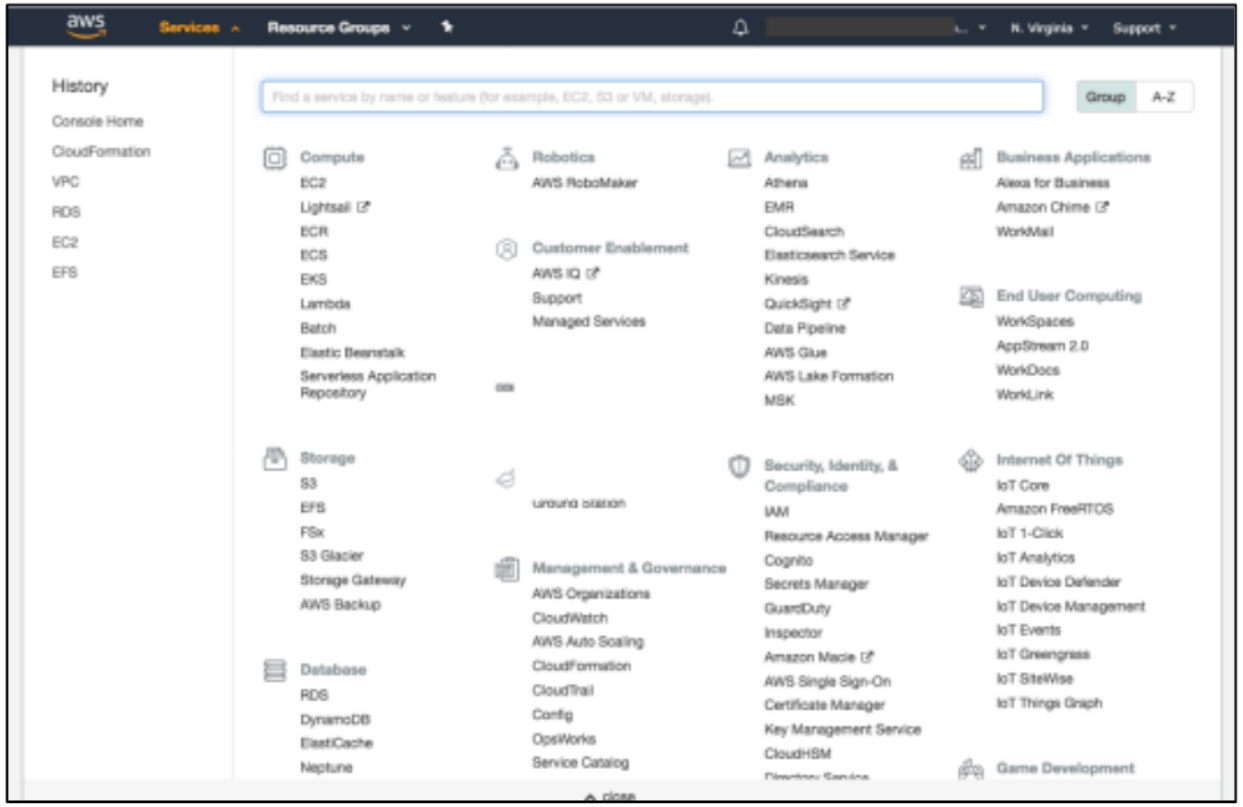


AWS IDENTITY AND ACCESS MANAGEMENT SERVICE

- This is one of the first services you will need to use when starting your AWS account
- This allows user to create polices and roles to assign to each account
- Polices allow account to either access or deny access to different services in the cloud
- Each role can be assigned to an account and can be customized based on the users needs

TYPES OF IAM ACCESS

- Programmatic Access
  - Requires Access Key ID
  - Provides CLI and SDK access
- AWS Management Console Access
  - 12-diget Account ID
  - IAM user or password



IAM MFA

Provides extra security by requesting an authentication code to grant user access

IAM POLICIES, GROUPS, AND ROLES

IAM polices are documents that can be assigned to a user, group, or role

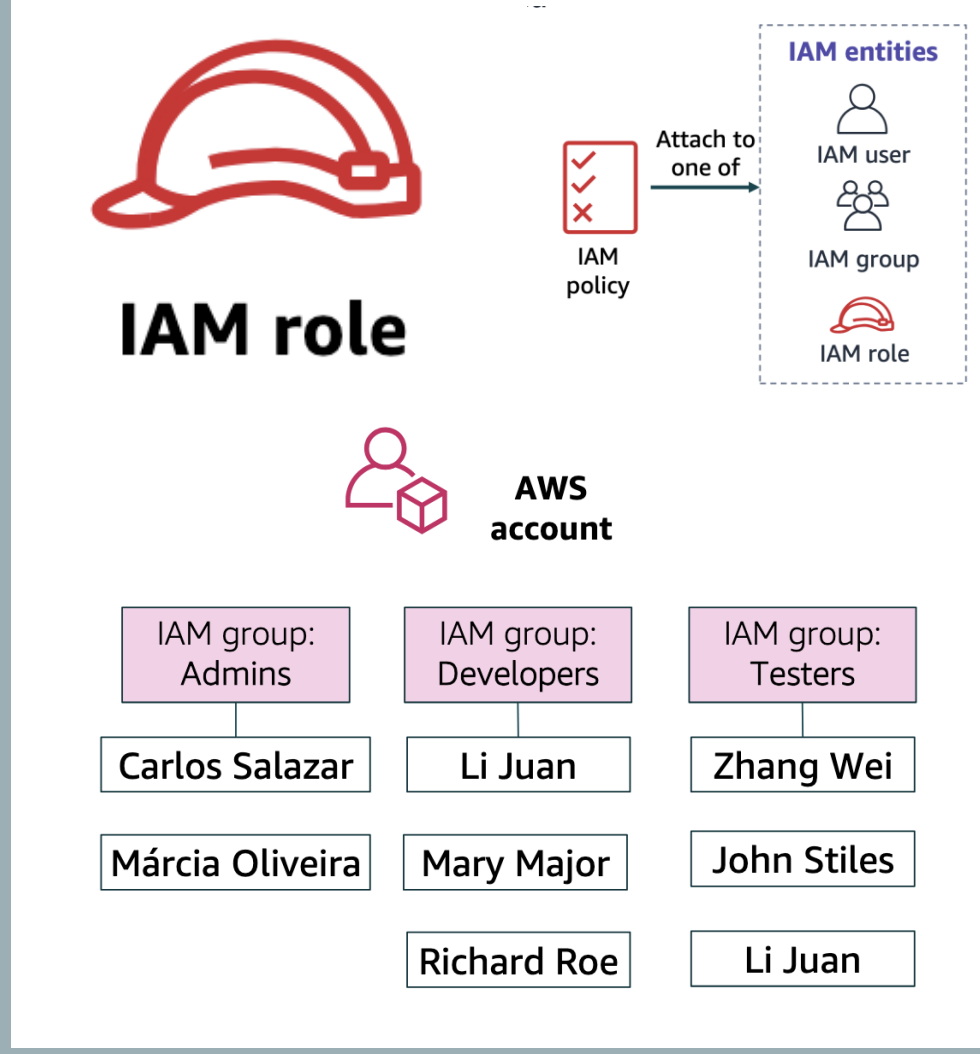
- Allows users to gain access to certain roles

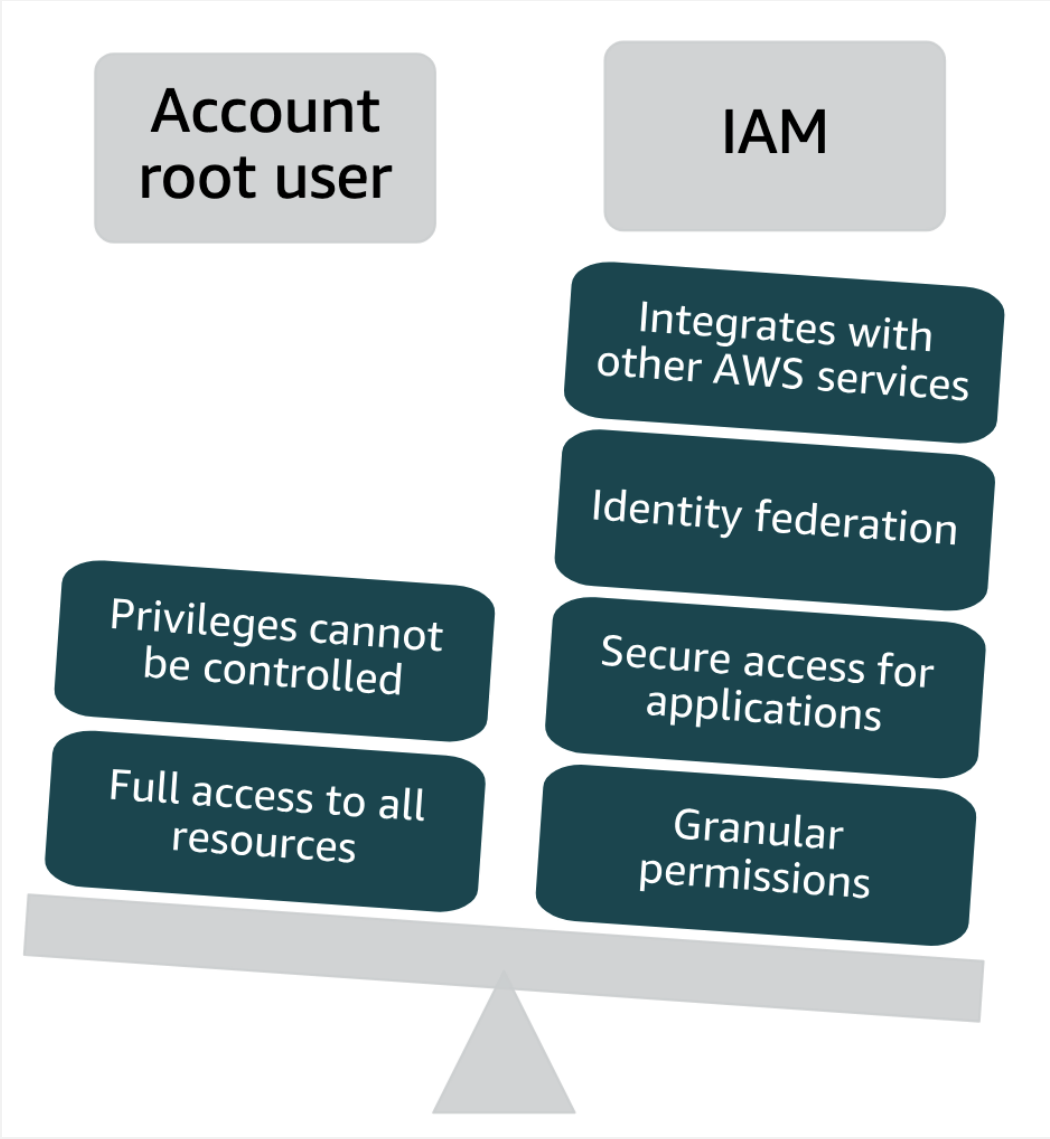
IAM groups is a collection of IAM users that can be grouped together and assigned a policy

- User can be assigned to multiple groups

IAM roles are IAM identities with specific permissions

- Different from IAM users because it can be assigned to multiple users





IAM ROOT ACCOUNT

- This account has full access to all services and resources
- Its not recommended to use this account on a day-to-day basis to avoid unnecessary changes
- Instead, AWS recommends that users make their own IAM user

SECURING NEW AWS ACCOUNT

- Ways to secure your AWS account:
- Multi-step authentication
- AWS CloudTrail tracks all users activity
- Billing Reports provides billing reports

AWS ORGANIZATION

This service allows the user to manage multiple AWS accounts

It also groups the accounts into different organizational units (OUs) that you can attach different polices to

This service also integrates and supports IAM

SCPs is like IAM, but SCPs specify the maximum permissions

AWS KEY MANAGEMENT SERVICE

- Allows users to create and manage encryption keys.
- Integrates with AWS CloudTrail and logs all user's activity
- Allows user to create custom master keys (CMKs) which grant user's access to encrypted data

Amazon Cognito

AWS COGNITO

Allows users to add a sign-in, sign-up, and helps moderate access control on your web applications

AWS SHIELD

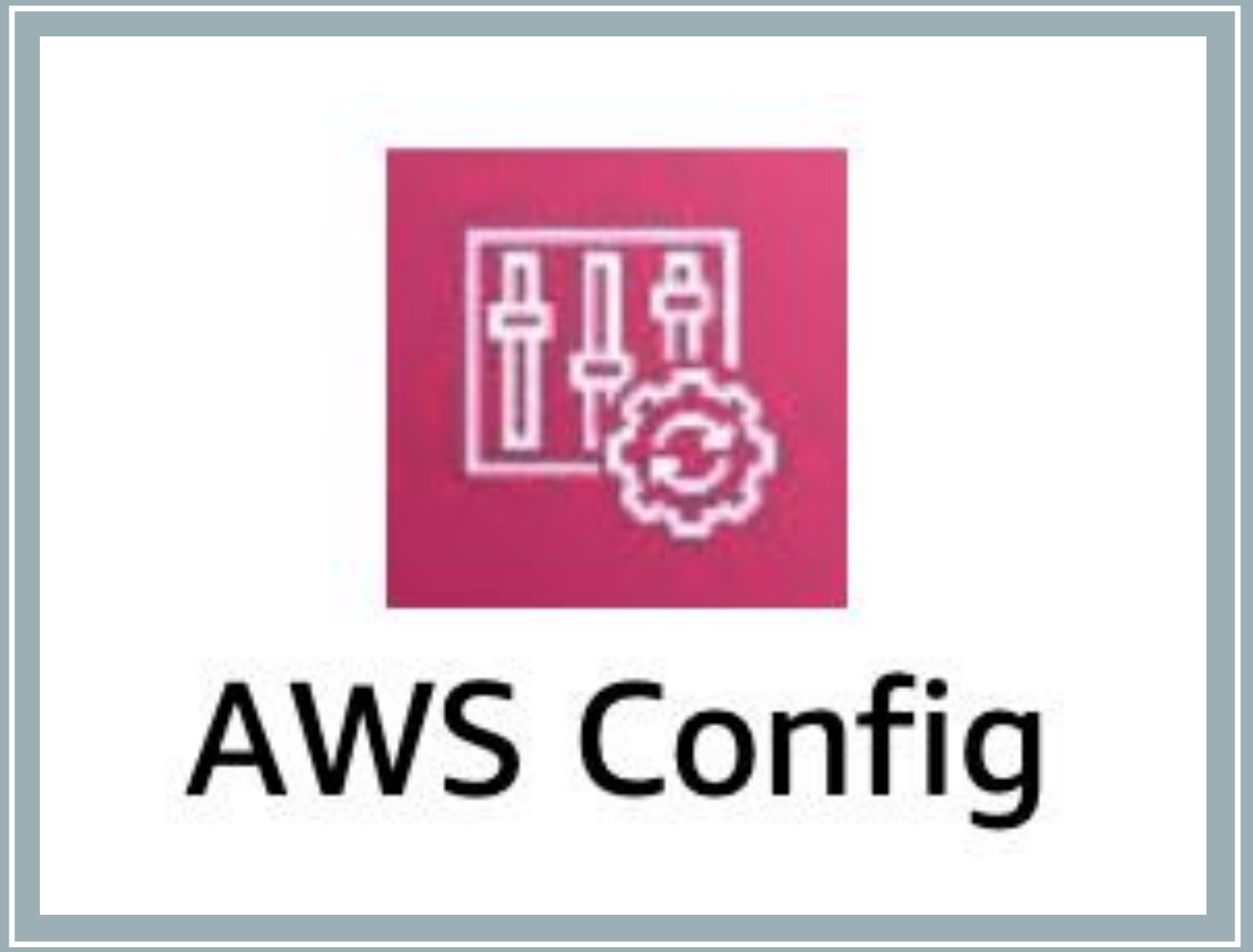
- This service is a distributed denial of service (DDoS) protection service.
- This service is used to minimize latency and downtime
- Advance shield is an addition to AWS Shield, and it provides extra protection against larger attacks.

ENCRYPTION OF DATA AT REST OR IN TRANSIT

- Data at rest is data that is being stored and it encodes data with a secret key.
- Data in transit is data that is being moved across a network.
- This can be secured by the TLS or the HTTPS which makes a tunnel for your data

AWS CONFIG

Used to monitor configurations, and simplifies compliance auditing and security analysis



AWS ARTIFACT

- This service provides resources for compliance-related information
- You can access AWS Artifact through the management console
- This service also provides access to security and compliance reports