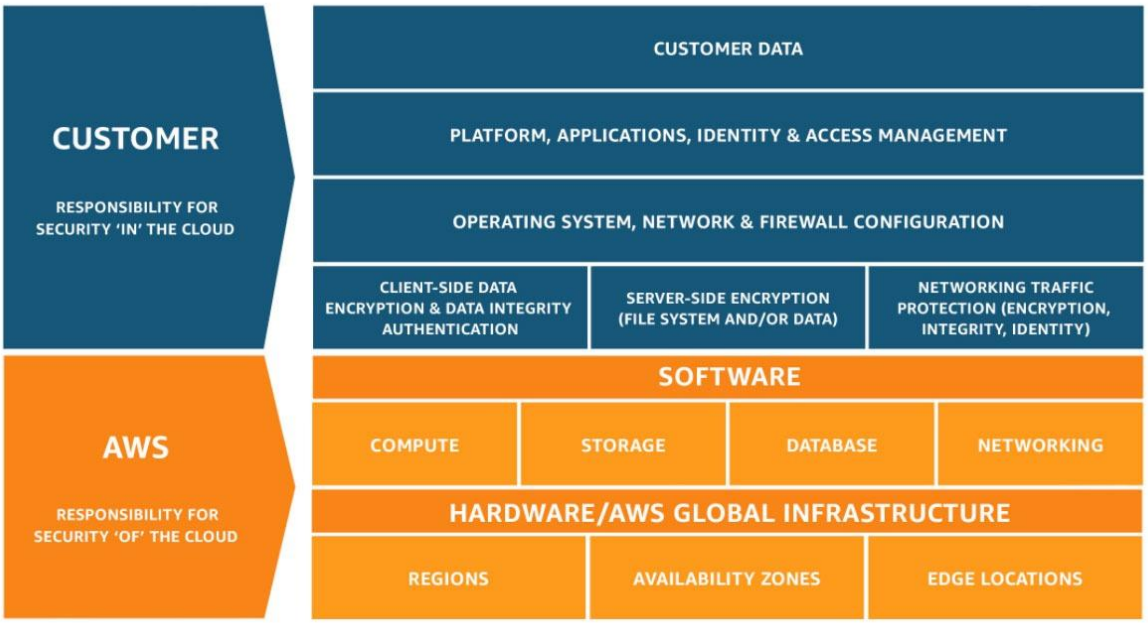
MODULE 4: AWS Cloud Security

1. AWS cloud Security

AWS shared responsibility model:

- Customer is responsible for security in the cloud
- AWS is responsible for the security of the cloud.



AWS Responsibilities:

- Physical security of data centres: controlled and need based access.
- Hardware and Software infrastructure : Host operating systems access, logging and auditing
- Network infrastructure : intrusion detection
- Virtualisation infrastructure: Instance isolation

Customer responsibilities:

- Amazon EC2
- Instances OS
- Applications
- Security groups configurations
- OS or host based firewall
- Network Configuration
- Account Management

Services characteristics and security responsibilities:

- Iaas: customer has more flexibility over configuring networking and settings. Customers are responsible for managing more aspects of security. Customer configures the access controls

- Paas: customer doesn't need to manage the underlying infrastructure. AWS handles the OS, database patching, firewall configuration and disaster recovery. Customers can focus on managing code or data.
- Saas: Software is centrally hosted. Licence on a subscription model or pay as you go basis. Services are typically accessed via web browser, mobile app or API. Customers do not need to manage the infrastructure that supports the service.

AWS IAM

- Used for managing access to AWS resources.
- Free of cost

IAM Components:

- IAM User: a person or application that can authenticate with an AWS account.
- IAM Group: A collection of IAM Users that are granted identical authorisation.
- IAM Policy: its a document which defines which resources can be accessed and the level of access to each resource
- IAM Role: useful mechanism to grant set of permission for making aWS service request

When you define an IAM user, you select what type of access this user is permitted to use.

Types of access:

- Programmatic access: access key ID, secret access key - authentication. It provides AWS CLI and AWS SDK access.
- Management console access : authentication - 12 digit account ID, IAM username and password. MFA is also used here and we get an authentication code every time you login.

IAM MFA:

- It provides increased security
- In addition to username and password, it requires an authentication code to access AWS services.
- Access permitted: IAM User, IAM group, IAM roles have full access to read IAM policy but they can't write IAM policies.
- Full access of EC2 and read only for S3 bucket.

IAM Authorisation:

- Assign permission by reading an IAM policy. Permission determines which resources and operations are allowed and best practises for IAM authorisation is the principle of least privilege.

IAM Policy is a document which defines permissions.
Types of IAM policies:

- Identity based : attach a policy to any IAM entity. Actions that may or may not be performed by the entity. A single policy can be attached to multiple entities and a single entity can have multiple policies attached to it.
- Resource based: it is attached to a resource like S3 Bucket.

IAM Group:

- It a collection of IAM users
- A group is used to grant the same permissions to multiple users.
- A user can belong to multiple group
- There is no default group
- Group cannot be nested.

IAM Roles:

- IAM Role is an IAM Identity with specific permission
- It is similar to IAM user as it attaches permission policies to it.
- It is different from IAM users as it is not uniquely associated.
- Roles provided temporary security credentials
- Examples: An application that runs on EC2 instance and need access to an S3 bucket

1. Securing a new AWS Account

AWS Root User Vs AWS IAM User

- Best practises is to always use the AWS IAM User instead of AWS Root User.
- AWS Root User: privileges can't be controlled in account root. Full access to all resources.
- AWS IAM: User It integrates with other AWS services. Identity federation, secure access for applications, granular permissions.

How to secure new AWS account:

- Stop using Root user asap
- Enabling MFA
- Use AWS cloudtrail
- Enable billing report

Best practises to secure AWS account:

- Secure logins with MFA.
- Delete account root user's access key
- Create individual IAM users and grant permission according to the principle of least privilege.
- Use group to assign permission to IAM users

- Configure a strong password policy
- Monitor account activity using AWS cloudtrail
- Delegate using Roles instead of sharing credentials

2. Securing account:

- AWS Organisation enables you to consolidate multiple AWS accounts so that you can centrally manage.

Securing features of AWS Organisations :

- Group AWS accounts into OU and attach different access policies to each OU.
- Integration and support for IAM.
- Use service control policies to establish control over the AWS services
- SCP offers centralised control over accounts. It ensures that the account complies with access control guidelines.

AWS KMS

Features :

- It enables you to create and manage encryption keys
- It enables you to control the use of encryption across AWS services and in your application.
- It integrates with AWS cloudtrail to log all keys usage

AMAZON COGNITO

- Adds user signup sign in an access control to your web and mobile application.
- It scales to millions of users
- It support sign in with social indemnity provider via SAML 2.0 (security Assertion Markup Language)

AWS Shield

- It is managed by DDOS protection services.
- It safeguard application running on AWS
- Provides always on detection
- No additional cost - AWS Shield Standard
- Paid - AWS Shield Advanced
- It is used to minimise application downtime and latency

3. Securing Data

AWS supports encryption for data at rest. (data stored physically)

You can encrypt data stores in any service that is supported by AWS KMS which includes S3, EBS, EFS, RDS.

Encryption of data in transit:

- Transport Layer Security is an open standard protocol.
- AWS certificate manager provides a way to manage deploy, and renew TLS certificate
- AWS services supports data in transit encryption

Securing S3 objects and buckets

Newly created S3 buckets and objects are private and protected by default

Working to ensure compliance:

- AWS engages with certifying bodies and independent auditors to provide customers with detailed information about the policies, processes, and controls that are established and operated by AWS.

Certifications and attestation
Laws, regulation and privacy
Alignment and frameworks.

AWS Config:

- Assess, audit and evaluates the configuration of AWS resources
- It reviews configuration changes
- It simplifies compliance auditing and security analysis

AWS Artefact :

- It is resource for compliance related information
- It provides access to security and compliance reports and select online agreements
- You can access directly from AWS management Console