Basics of Securing Your Cloud

Security on the cloud consists of - a) Infrastructure Structure Security b) DDoS Mitigation c) Data Encryption d) Inventory & Configuration e) Monitoring and Logging

Security on the cloud consists of -

1. Infrastructure Structure Security
2. DDoS Mitigation
3. Data Encryption
4. Inventory & Configuration
5. Monitoring and Logging

Infrastructure Structure Security

Several security capabilities and services to increase privacy and control network access. These include: Network firewalls built into the VPC and web application firewall capabilities using WAF will let you create private networks, and control access to your instances and applications Encryption in transit with TLS across all services Connectivity options that enable private, or dedicated, connections from your office or on-premises environment

DDoS Mitigation

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic. Availability is of paramount importance in the cloud. Customers benefit from DDoS protection services and technologies built from the ground up to provide resilience in the face of DDoS attacks. Some services like auto scaling also are designed with an automatic response to DDoS help minimize time to mitigate and reduce impact.

Data Encryption

AWS offers you the ability to add an additional layer of security to your data

at rest in the cloud, providing scalable and efficient encryption features. This includes:

Data encryption capabilities available in AWS storage and database services, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift.

Flexible key management options, including AWS Key Management Service, allowing you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your keys.

Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS.

Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to satisfy compliance requirements.

Inventory & Configuration

The Cloud range of tools allow you to move fast while still ensuring that your cloud resources comply with organizational standards and best practices. This includes:

A security assessment service like Amazon Inspector, that automatically assesses applications for vulnerabilities or deviations from best practices, including impacted networks, OS, and attached storage.

Deployment tools to manage the creation and decommissioning of AWS resources according to organization standards.

Inventory and configuration management tools, including AWS Config, that identify AWS resources and then track and manage changes to those resources over time.

Template definition and management tools, including CloudFormation to create standard, preconfigured environments.

Monitoring and Logging

The cloud provides tools and features that enable you to see exactly what's happening in your environment. This includes:

Deep visibility into API calls , including who, what, who, and from where calls were made.

Log aggregation options, streamlining investigations and compliance reporting.

Alert notifications through CloudWatch when specific events occur or thresholds are exceeded.

These tools and features give you the visibility you need to spot issues before they impact the business and allow you to improve security posture, and reduce the risk profile, of your environment.

Identity and Access Control

Cloud Providers offer you capabilities to define, enforce, and manage user access policies across services. This includes services like: AWS Identity and Access Management (IAM) lets you define individual user accounts with permissions across AWS resources.

AWS Multi-Factor Authentication for privileged accounts, including options for hardware-based authenticators AWS Directory Service allows you to integrate and federate with corporate directories to reduce administrative overhead and improve end-user experience.

AWS provides native identity and access management integration across many of its services plus API integration with any of your own applications or services.

Most cloud providers like Azure and AWS are ISO1, ISO2, ISO3, PCI, HIPPA, SOC, FedRAMP compliant.