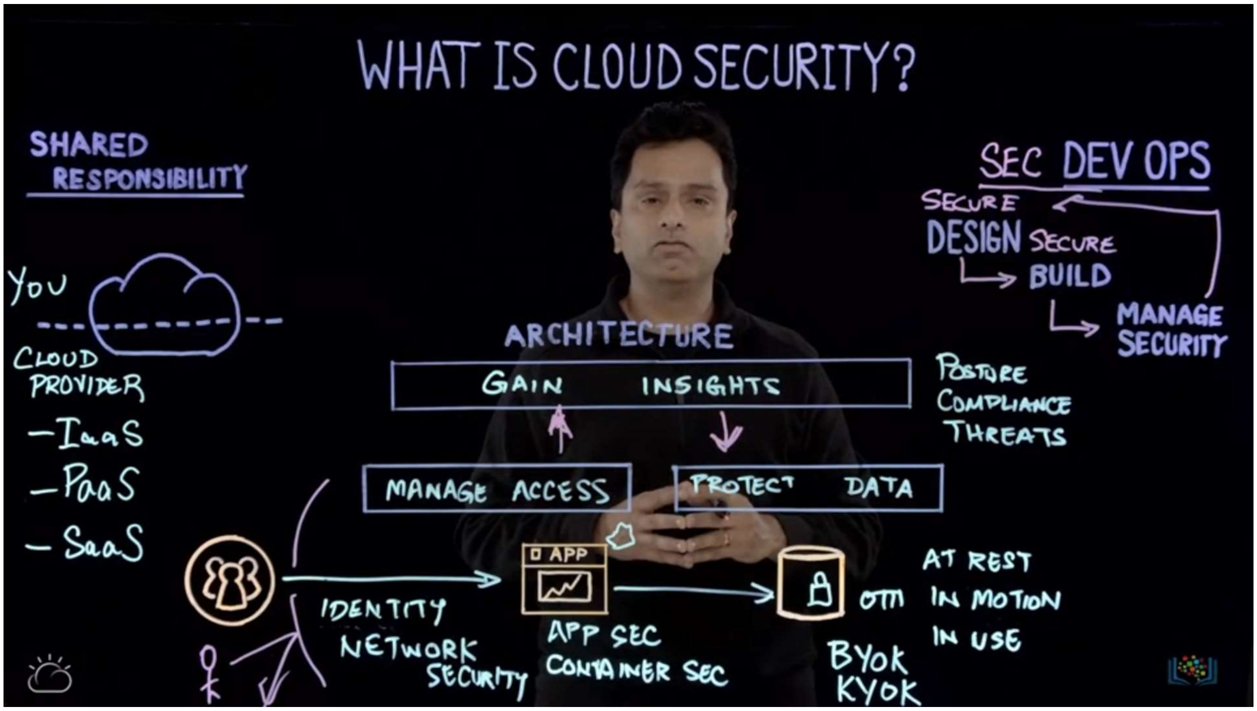
4/14

Cloud Security



Cloud security concerns

1. Data Loss and Leakage
2. Unauthorized access
3. Insecure interfaces and api s

Data Protection States

1. Encryption at Rest
    a. Protects stored data
    b. Multiple encryption options:
        i. Ex. block and file storage
        ii. Ex. build-in for object storage
        iii. Database encryption
2. Encryption in Transit
    a. Protects data while transmitting
    b. Includes encrypted before transmission
    c. Authenticates endpoints
    d. Decrypts data on arrival
        i. EX. Secure Sockets Layer, Transport Layer Security
3. Encryption in Use
    a. Protects data in use in memory
    b. Allows computations to be performed on encrypted text without decryption

Cloud Monitoring

There needs to be active monitoring of all connected systems and cloud-based services to maintain visibility of all data exchanges between public, private, and hybrid cloud environments. This ensures that the cloud provides a trusted platform that can securely integrate with your enterprise data centers.

Summary

- Cloud security refers to the policies, technological procedures, services, and solutions designed to secure the enterprise applications and data on cloud against insider threats, data breaches, compliance issues, and organized security threats.

- Cloud security is a shared responsibility between the cloud provider and the user organization.

- Security architecture and methods for achieving continuous security need to be embedded through the life cycle of an application to ensure that the application runs on a safe platform, the code is free from vulnerabilities, and the operational risks are understood.

- Identity and Access Management, also known as access control, helps authenticate and authorize users, and provide user-specific access to cloud resources, services, and applications.

- As part of their Identity and Access Management services, most cloud providers offer users the ability to define access groups and create access policies that define permissions for users on account resources.

- Cloud encryption, often referred to as the last line of defense, not only encrypts data, but also provides robust data access control, key management, and certificate management.

- Data needs encryption in three states -

    - Encryption at rest; protecting data while it is stored

    - Encryption in transit; protecting data while it is transmitted from one location to another

    - Encryption in use; protecting data when it is in use in memory

- There needs to be active monitoring of all connected systems and cloud-based services to maintain visibility of all data exchanges between public, private, and hybrid cloud environments. This ensures that the cloud provides a trusted platform that can securely integrate with your enterprise data centers.