

# Cloud Data Security for CCSP

---

## DATA SECURITY TECHNOLOGIES



**Kevin Henry**

CISM CISSP CCSP

[kevin@kmhenrymanagement.com](mailto:kevin@kmhenrymanagement.com)



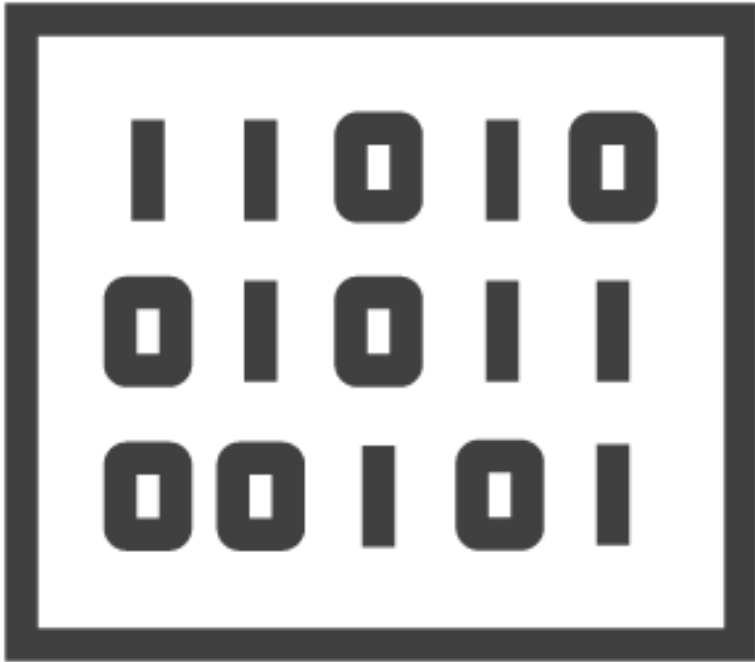
# Cloud Data Security

## Agenda:

**Cloud Data Security Concepts**

**Cloud Data Security  
Technologies**

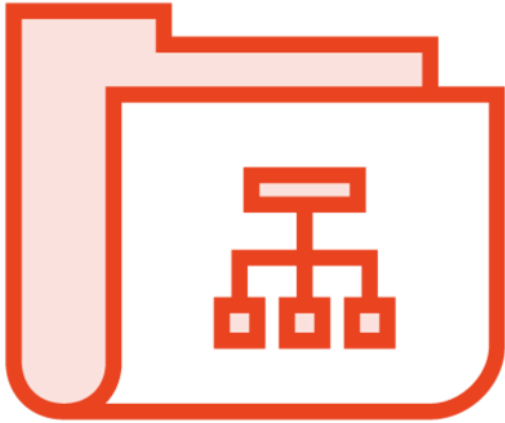




## Data storage

- Ephemeral
  - Virtual machines
- RAW storage
- Long-term storage

# Data Storage Types

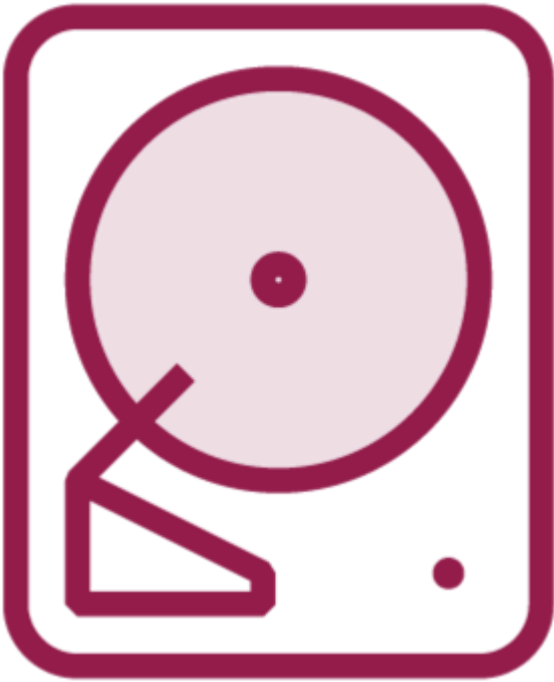


Volume



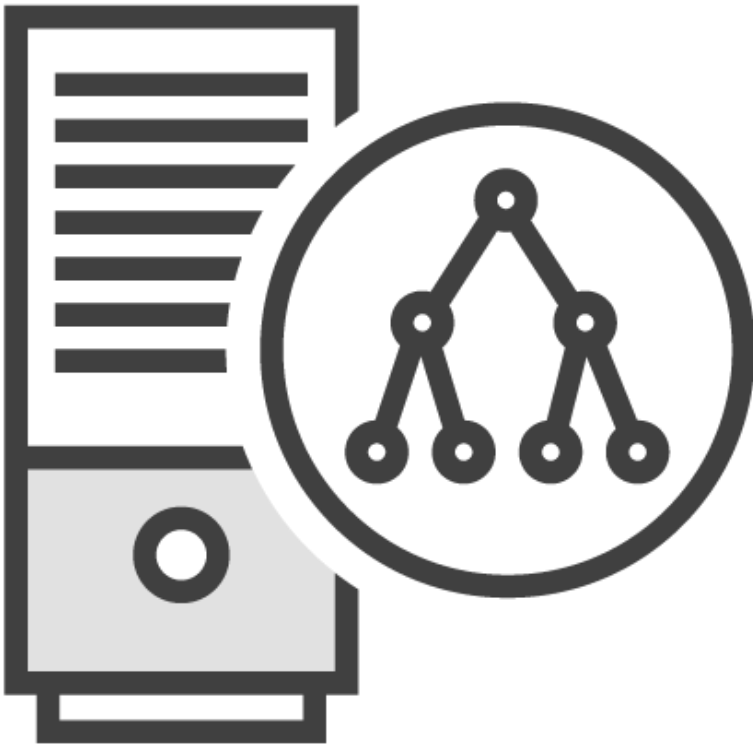
Object

# Block Storage



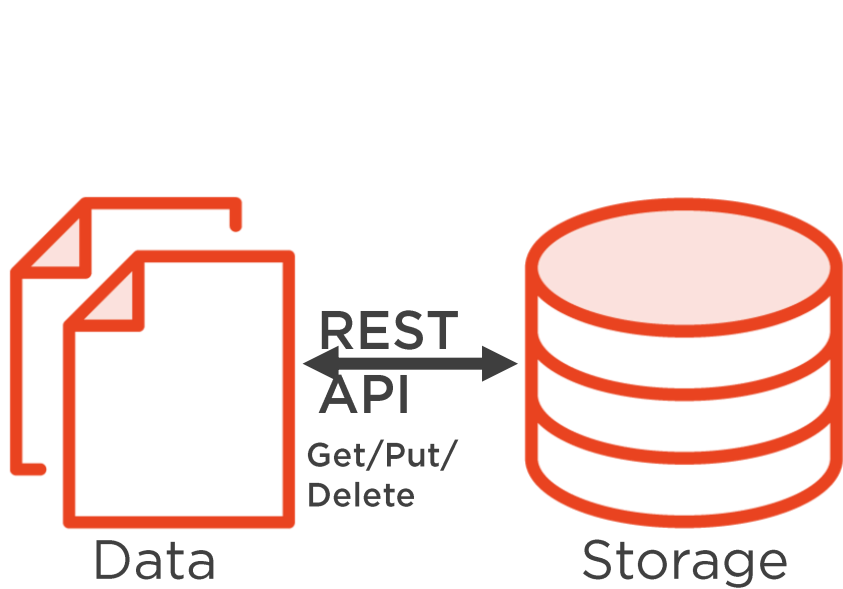
- Files and file folders
- Data stored in blocks on specified hardware
  - Tracks and Sectors
- Expensive, poor scalability
- Accessed through applications and operating systems

# File Storage



- Data stored as files in a hierarchical structure e.g., directory
- Accessed through applications and operating system
- Not very scalable as number of files increases
- Good for transactional activity
  - Database

# Object Storage

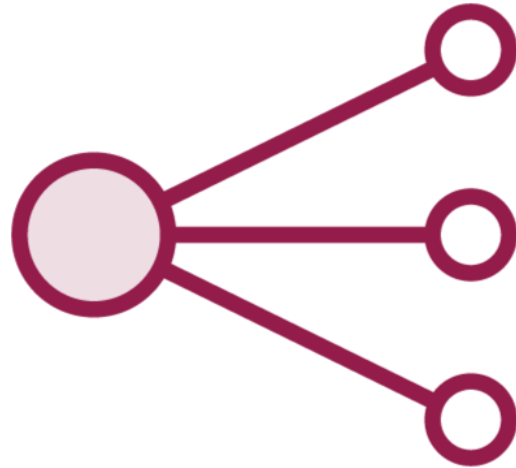


- Data stored as objects that include metadata
- Good for Cloud services
- May be stored in containers
- Accessed through http-based Restful APIs
- Flat storage, not tree or directory
- Meta data is searchable
- Easy replication and integrity checking using hash values

# Object Storage Benefits



Data can be accessed from anywhere using multiple types of devices and applications



Load balancing and hardware abstraction



Faster search and retrieval



Storage systems act as a valet in a parking lot

- Can better optimize data
- Scalable
- Less expensive
- Good for videos, images, blogs





# Metadata



- Data that describes data
- Can be searched
  - Find all data in a certain category

# Example of Object



Name: Kuwait-evening.jpg

Resolution: 600x800

Date: Jan 1, 2020

Time:

GPS location:

ID #: 3A5TS

Metadata

Integrity



# Cloud Data Protection

---





## The key to data protection is:

- Access Control
  - Only allow authorized entities (personnel or processes) to perform authorized functions
    - Time
    - Attributes

# Threats to Data



## Storage

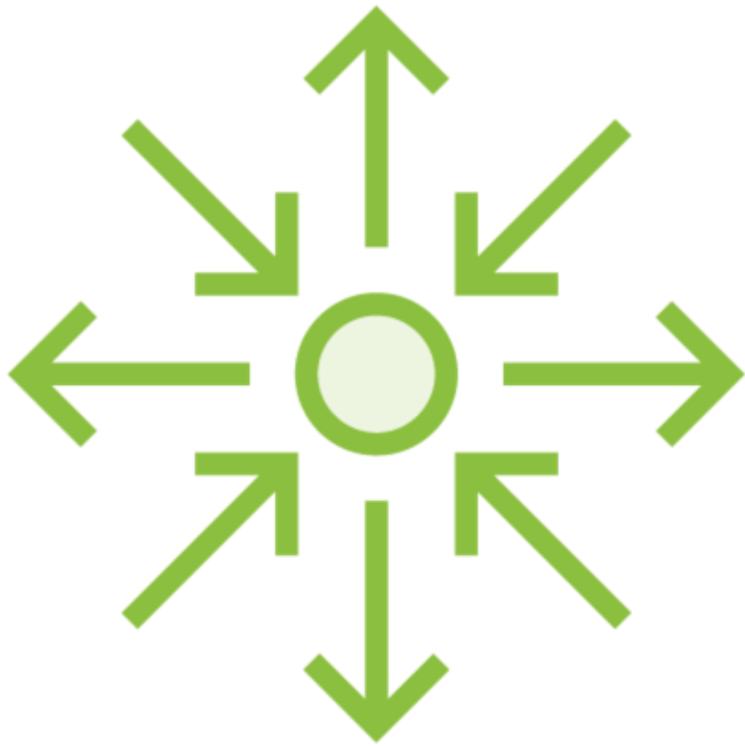
- Disclosure
- Alteration
- Loss



## Transmission

- Man-in-the-middle

# Data Protection

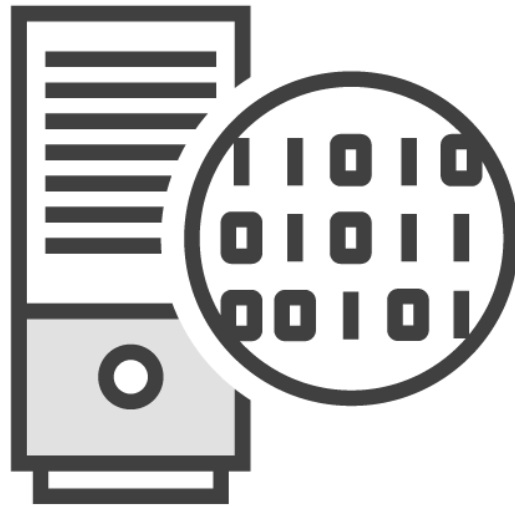


- Transmission
  - Virtual Private Networks
    - TLS
    - IPSec
    - WPA3

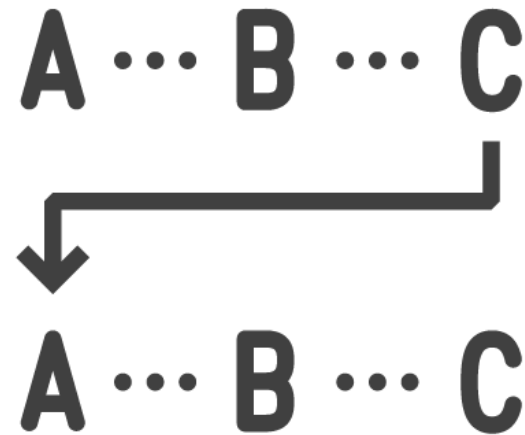
# Data Protection – Storage



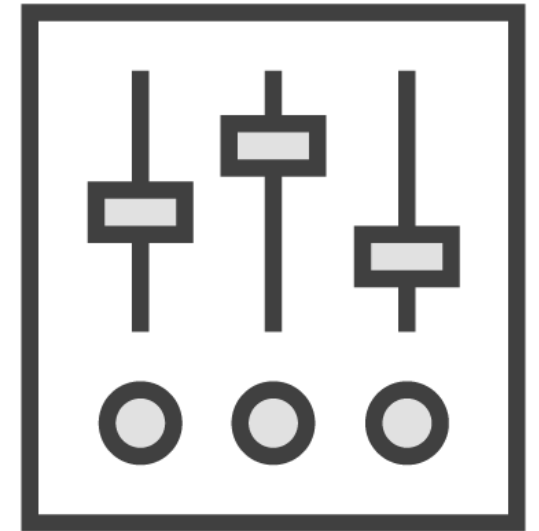
Replication



Encryption



Hashing



Access controls

# DLP



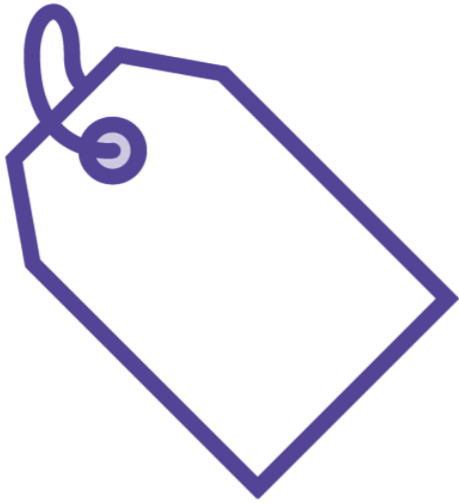
## Data Loss (or Leakage) Prevention

- Prevents data from:
  - Leaking out of an organization
  - Being improperly disclosed within an organization



# DLP Operations

Identifies sensitive data based on:



Labels



Key words



Strings

# DRM / IRM



## Digital Rights Management /Information Rights Management

- Protection of data that does go outside of the organization
  - Encryption
  - Logging
  - Expiry
  - Restrictions on replication
    - Print
    - Forward
    - Copy

# Encryption and Key Management

---



# Protection of Data - Encryption

Encryption provides the benefits of protecting data:



Confidentiality



Integrity



Access control



Authentication



Non-repudiation

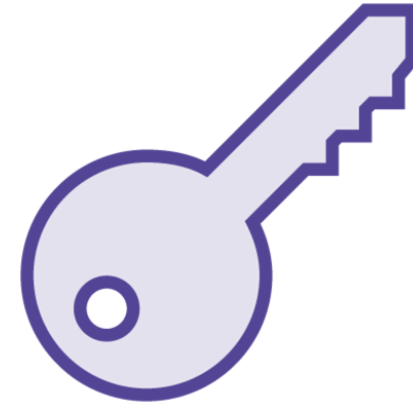
# Symmetric Encryption Algorithms

## Protection of data:



Bulk data

- Storage
- Transmission



**Requires careful key management**

- Key creation
- Key storage
- Key distribution

# Who Holds the Keys?



## SaaS

- Keys controlled by the CSP
  - Transmission
  - Storage

# Who Holds the Keys?



## PaaS

- Keys controlled by the Cloud Consumer but perhaps also by the CSP
  - Transmission
  - Storage
    - Application
    - Database
      - Transparent encryption
      - Built-in encryption

# Who Holds the Keys?



## IaaS

- Keys controlled by the Cloud Consumer
  - Transmission
  - Storage



# Key Management



## Key Recovery

- Escrow
  - Dual control
- Split knowledge (multi-party)
- Hardware Security Module (HSM)
  - May be software
- Outsourced key management
  - PKI (Public Key Infrastructure)
  - CASB (Cloud Access Security Broker)

# Asymmetric Encryption

Used to:



Distribute or negotiate  
symmetric keys



Digital signatures

- Message authenticity
- Proof of origin

# Key Points Review



**Encryption is a valuable tool to protect data, but:**

- It requires careful key management
- Training of users and administrators
- Correct configuration

# Hashing

---



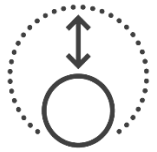
# Hashing



## A critical piece in the security chain

- Provides a way to ensure:
  - Authenticity
  - Integrity
  - Protection of secrets
    - Not really cryptography since it is a one-way function

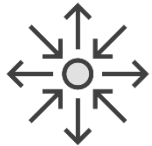
# Hashing Benefits



Very sensitive to changes to a document, file, database or other entity



Fast



Freely available



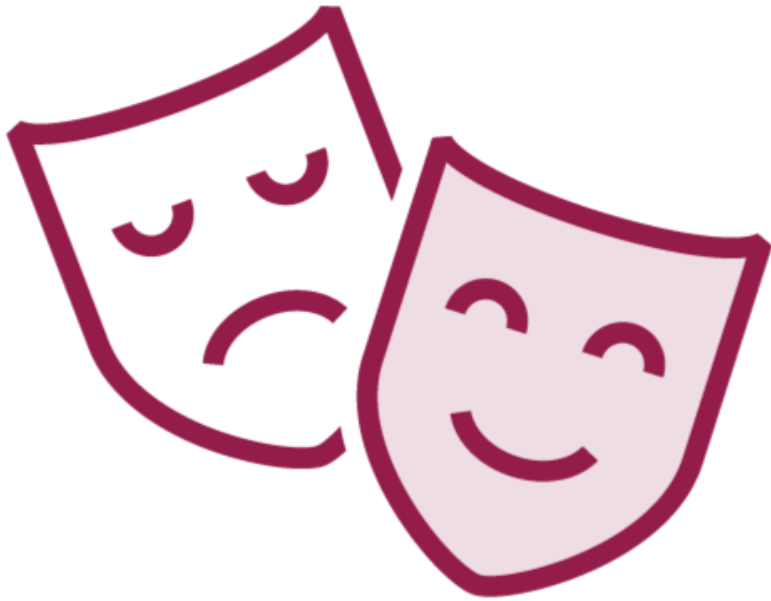
Essential for the Cloud due to the need to protect the integrity of transmitted and stored data



Combined with asymmetric encryption to create digital signatures



# Masking and Obfuscation



## Hiding sensitive data

- Replacing payment card numbers with meaningless values
  - Dots, hash
- Used to protect data in the Use or Sharing phases
- Real data is still available in back end
- Used when displaying data or putting it into a report

# Anonymization



**Replacing sensitive (e.g. PII) data making data non-personal**

- Random substitution
- Algorithmic substitution

**Risk of de-anonymization**



# Implementing Masking and Anonymization in the Cloud



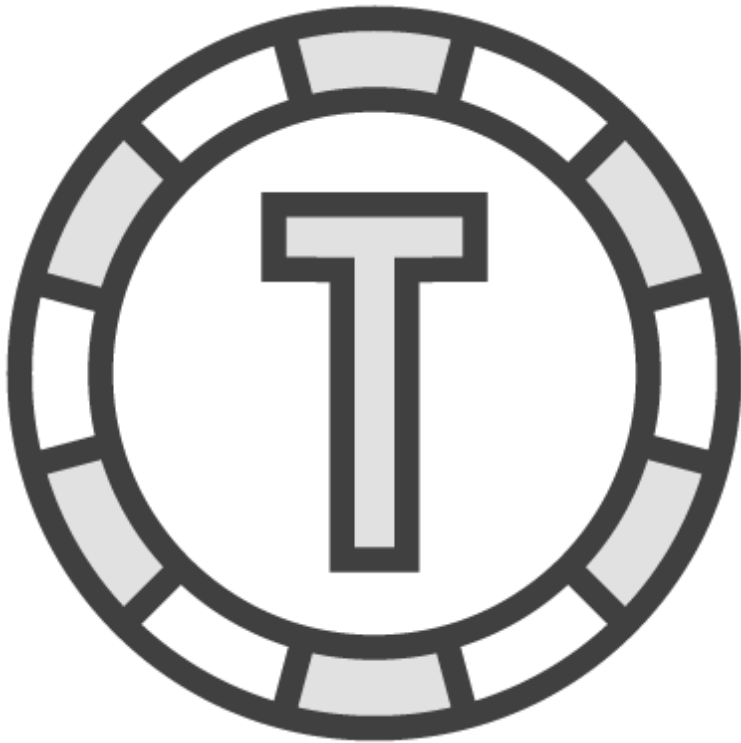
**Can be in SaaS applications by the CSP**

**Can be built-into applications running on PaaS**

- May be managed by the Cloud Consumer

**Responsibility of the Cloud Consumer in IaaS**

# Tokenization



Replacing sensitive data with another unique value that can be cross-referenced back to the original value

Often done by a third party to hide sensitive data from unauthorized use

- Payment card data processed by a third party

# Key Points Review



The protection of data in the Cloud is the ultimate responsibility of the Data Owner – usually the Cloud Consumer

Data must be protected at all times using tools such as IRM, DLP and cryptographic functions



# Cloud Data Event Management

---



# Event Management



**Many Cloud deployments are not being monitored for compliance**

- Log reviews
- Access controls
- Encryption
- Destruction of old equipment

# Log Review



## Too much data – not enough time

- Cost for storage
- Performance impact



## Need skills



## Need tools

- Analysis

# Event Sources



IP Address



Geolocation



Identification



# Cloud-based Investigations



## **Requires a liaison between the Consumer and Provider**

- Formal agreement
  - Law enforcement
  - Regulators
- Data availability
  - Logs
  - Timelines
  - Format



# Security Operation Center (SOC)



**May be provided internally, by the cloud provider or as a third-party service**

- Central point of monitoring/control
- Skilled resources
  - Experienced Staff
  - Learn from others' experiences

# Investigation in the Cloud



## Approach varies depending on deployment model

- SaaS – all control resides with the CSP
  - Except access control management
- PaaS – split responsibility
- IaaS – mostly the responsibility of the Cloud Consumer

# Investigation Requirements



**Ability to track all activity and  
associate to an identifier**



**Preservation of log integrity**

- Access controls
- Hash values
- Storage on separate system

# Data Discovery



- Support for investigations
  - Requirement to comply with regulations
    - Logs
    - Monitoring

# Chain of Custody



**Unbroken record of all activities associated with evidence throughout the evidence lifecycle**

- Harder to provide in the Cloud
  - Evidence provided by a third party
    - Skill and trustworthiness of provider
  - Defined procedures
  - Non-disclosure agreements

# Summary



This course examined the importance of securing data in a cloud environment.

This includes:

- Data classification
- Controls
- Logs

This requires securing data throughout the data lifecycle

