Domain 9 Data Security

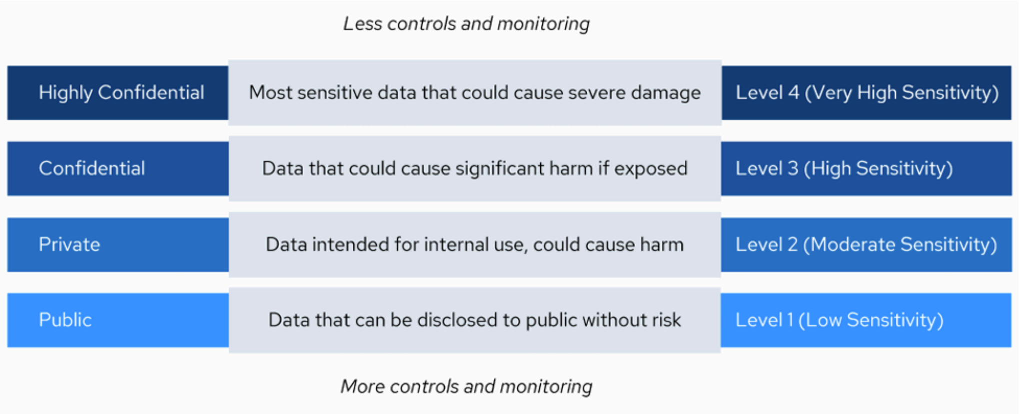
- Understanding and implementing data classification practices help organizations align with operational and compliance strategies.
- **Object Storage**:
  - Each file is represented as an object, including the data itself, metadata, and a unique identifier.
  - Cannot be modified after creation.
  - Redundancy and availability are the responsibility of the cloud provider.
- **Volume Storage:**
  - Customers reserve a fixed block of storage and attach it to an existing workload.
  - known for its low latency, flexibility, and legacy support.
  - Customer responsibility.
- **Database Storage:**

  - **Relational databases**: SQL databases, store data in structured tables with rows and columns. / Amazon RDS, Google Cloud SQL, Microsoft Azure SQL Database, and Oracle Database services. / MySQL, Oracle, PostgreSQL, and SQL Server.
  - **Non-relational databases**: NoSQL databases, store data in flexible formats like documents or key-value pairs. / Amazon DynamoDB, Google Cloud Datastore, Oracle NoSQL Cloud DB, andAzure CosmosDB. / Handle large amounts of unstructured data efficiently.

  Logging services like Amazon CloudWatch, Google Cloud Logging, Oracle Events, and Azure Monitor, which store and analyze log data from applications and infrastructure.
- Cloud storage may also be offered as SaaS, such as Google Drive, Dropbox, Microsoft OneDrive, Box, and others.

Data Security Tools and Techniques:

- **Data Classification**:



Less controls and monitoring

Highly Confidential	Most sensitive data that could cause severe damage	Level 4 (Very High Sensitivity)
Confidential	Data that could cause significant harm if exposed	Level 3 (High Sensitivity)
Private	Data intended for internal use, could cause harm	Level 2 (Moderate Sensitivity)
Public	Data that can be disclosed to public without risk	Level 1 (Low Sensitivity)

More controls and monitoring

Figure 23: Data Classification Scale

- **Identity and Access Management**
- **Access Policies**
- **Encryption and Key Management** (Key management systems securely store these keys, ensuring they remain separate from the CSP, either within their infrastructure or on an external Key Management Server (KMS)).
- **Data Loss Prevention**: by discovering, classifying, and enforcing security policies to prevent unauthorized sharing or exfiltration. / more commonly used for SaaS applications.

Cloud Data Encryption at Rest:

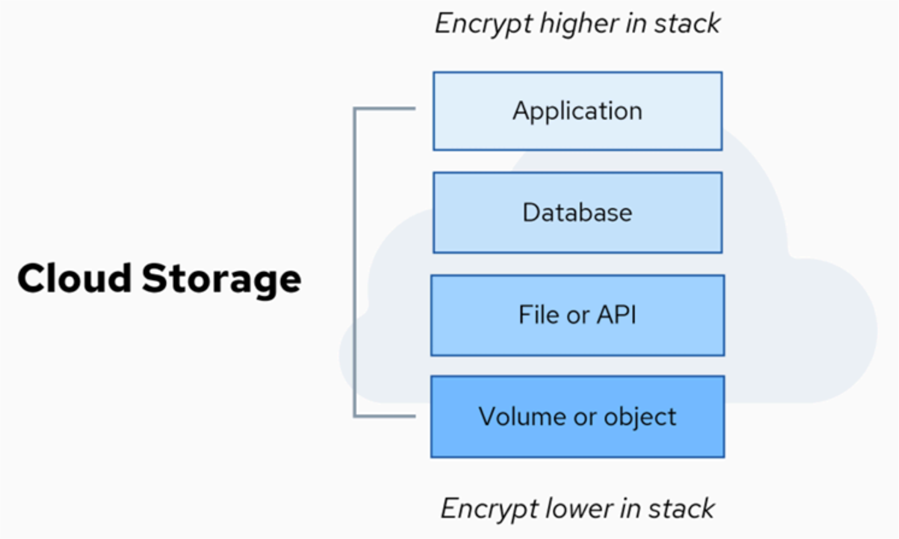


Figure 24: Cloud Data Encryption Layers

Data encryption protects stored data from breaches.

Encryption Layers

1. **Application-Level Encryption:** Encrypts data before storage (e.g., credit card info).
2. **File/API Encryption:** Encrypts specific files or API-accessed data.
3. **Database Encryption:** Secures entire databases or specific tables/columns.
4. **Object Storage Encryption:** Encrypts cloud objects (e.g., S3, Azure Blob).
5. **Volume Encryption:** Protects virtual disks and **backups**.

Cloud Data Key Management Strategies

6. **Client-Side Encryption:** Customers **encrypt data before uploading**.
7. **Server-Side Encryption:** Cloud provider encrypts data automatically.
8. **Customer-Managed Keys:** Customers control keys via **KMS services**.
9. **Customer-Provided Keys (BYOK):** Users **generate and manage encryption keys**.
10. **Application-Level Encryption:** Encrypts data **within the application itself**.

Encryption Best Practices

✓ Use **Key Management Services (KMS)** for security.
✓ Consider **SaaS encryption limitations**.
✓ Enforce **IAM policies on encryption keys**.
✓ Use **separate keys for different services**.
✓ Align encryption with **threat models**.

Data Security Posture Management (DSPM)

- **Monitors and evaluates** data security risks.
- **Identifies sensitive data** and **assesses access control policies**.
- Helps visualize **who has access** and **suggests security improvements**.

Object Storage Security

- **Misconfigurations in object storage** (AWS S3, Azure Blob) create security risks.
- Use **IAM roles, encryption (KMS), and CDNs** to **reduce exposure**.
- Continuous monitoring via **CSPM and DSPM** is essential.

Data Security for Artificial Intelligence (AI)

AI systems require **special security measures** to prevent **data leaks and adversarial attacks**.

AI as a Service (AIaaS)

- AI platforms like **ChatGPT, Claude, Vertex AI** require:
  ✓ **Understanding data retention policies**.
  ✓ **Assessing security against adversarial threats**.
  ✓ **Aligning with regulatory compliance**.