Azure Storage Security & Compliance

Protecting Sensitive Data in the Cloud

Agenda

1. ## Introduction to Azure Storage

   Understanding its core services and capabilities.

2. ## Azure Storage Service Encryption (SSE)

   Automatic data protection at rest.

3. ## Azure Key Vault & Customer-Managed Keys (CMK)

   Enhancing control over encryption keys.

4. ## Azure Role-Based Access Control (RBAC)

   Granular permission management.

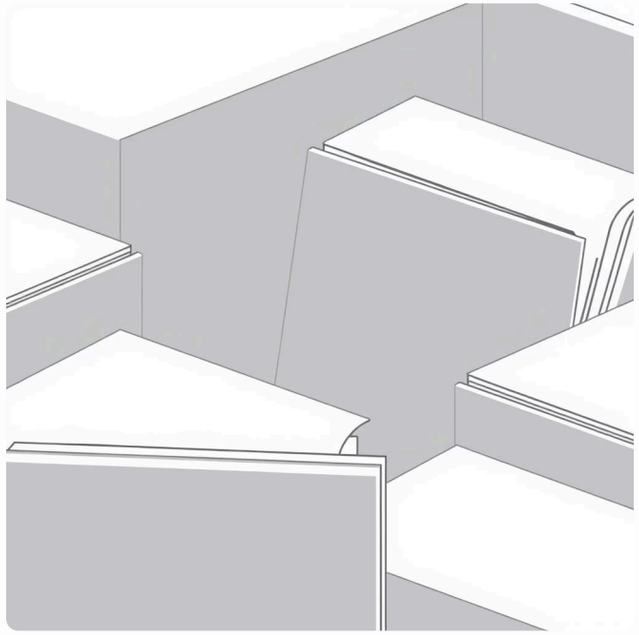
5. ## Implementation Steps & Best Practices

   A practical guide to securing your data.

Azure Storage: Core Services

Azure Blob Storage

Ideal for storing large amounts of unstructured data, such as documents (PDFs, Word files), images, videos, and backups. Optimized for scale and performance.



Azure Files

Provides fully managed file shares in the cloud, accessible via SMB (Server Message Block) protocol. Perfect for lift-and-shift scenarios for enterprise applications.

Azure Queues & Tables

Azure Queues: A service for storing large numbers of messages, enabling asynchronous communication between application components.

Azure Tables: A NoSQL datastore for storing structured, non-relational data, offering high availability and scalability.

Azure Storage Service Encryption (SSE)

SSE is a built-in Azure feature that automatically encrypts all data stored at rest in Azure Storage. This protects your data from unauthorized access by encrypting it before persisting it to disk.

- **Automatic:** Encryption is handled by Azure, requiring no configuration or code changes from the user.
- **Transparent:** Data is encrypted as it's written and decrypted as it's read, with no performance impact.
- **Secure by default:** All new storage accounts have SSE enabled.

Enhancing Security with Azure Key Vault & CMK

Why Azure Key Vault?

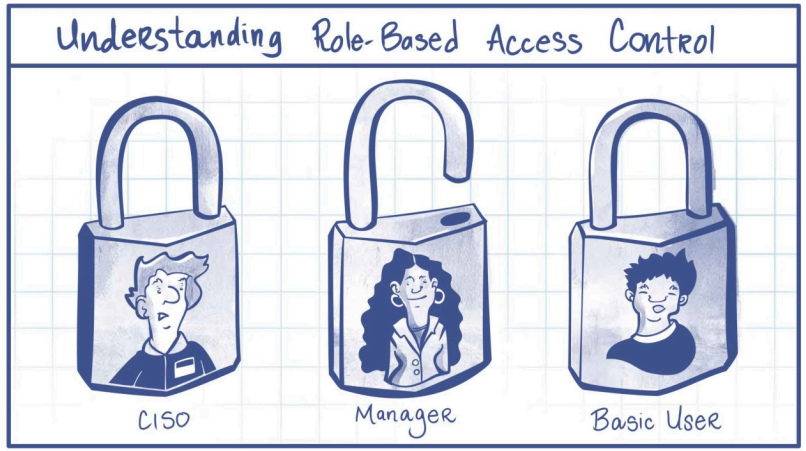
Azure Key Vault is a cloud service for securely storing and accessing secrets, such as API keys, passwords, certificates, and encryption keys. For HIPAA compliance and other regulatory requirements, it's crucial to have full control over your encryption keys.

Customer-Managed Keys (CMK)

While SSE uses Microsoft-managed keys by default, CMK allows you to manage and control your own encryption keys in Azure Key Vault. This adds an extra layer of control:

- **Key Lifecycle Management:** Create, rotate, and revoke keys as needed.
- **Separation of Duties:** Distinguish between data ownership and key management.
- **Enhanced Compliance:** Meet stringent regulatory standards like HIPAA, GDPR, and PCI DSS.

Granular Access Control with Azure RBAC



Azure Role-Based Access Control (RBAC) allows you to manage who has access to Azure resources and what they can do with those resources. This is essential for maintaining a strong security posture.

- **Principle of Least Privilege:** Grant only the necessary permissions to users and services.
- **Built-in Roles:** Utilize predefined roles like "Storage Blob Data Contributor" or "Storage Blob Data Reader."
- **Custom Roles:** Create Custom roles for specific requirements.
- **Assignment Scope:** Apply permissions at the subscription, resource group, or individual resource level (e.g., a specific Blob container).

Implementation Steps

1. Create Resources

Deploy an Azure Storage Account and an Azure Key Vault instance.

2. Generate Customer-Managed Key

In Azure Key Vault, create or import a new encryption key (CMK). Configure access policies for the Storage Account to use this key.

3. Configure Storage Account for CMK

Link your Azure Storage Account to the Customer-Managed Key in the "Encryption" settings, selecting "Customer-managed keys."

4. Create Blob Container & Upload Files

Within your Storage Account, create a container and upload your documents (e.g., PDFs, Word files). Data will be encrypted using your CMK.

5. Implement RBAC

Assign appropriate Azure RBAC roles (e.g., "Storage Blob Data Reader") to specific users or service principals to control access.

Benefits of This Approach

Enhanced Data Security

Leveraging SSE with CMK ensures your data is encrypted at rest, and you maintain control over the encryption keys, adding a critical layer of protection.

Reduced Risk of Unauthorized Access

Granular RBAC policies minimize the blast radius of potential breaches by limiting access to sensitive data to only authorized entities.

Operational Efficiency

Automated encryption and streamlined access management reduce manual overhead while maintaining high security standards.