Azure Cosmos DB security

Azure COSMOS DB security overview

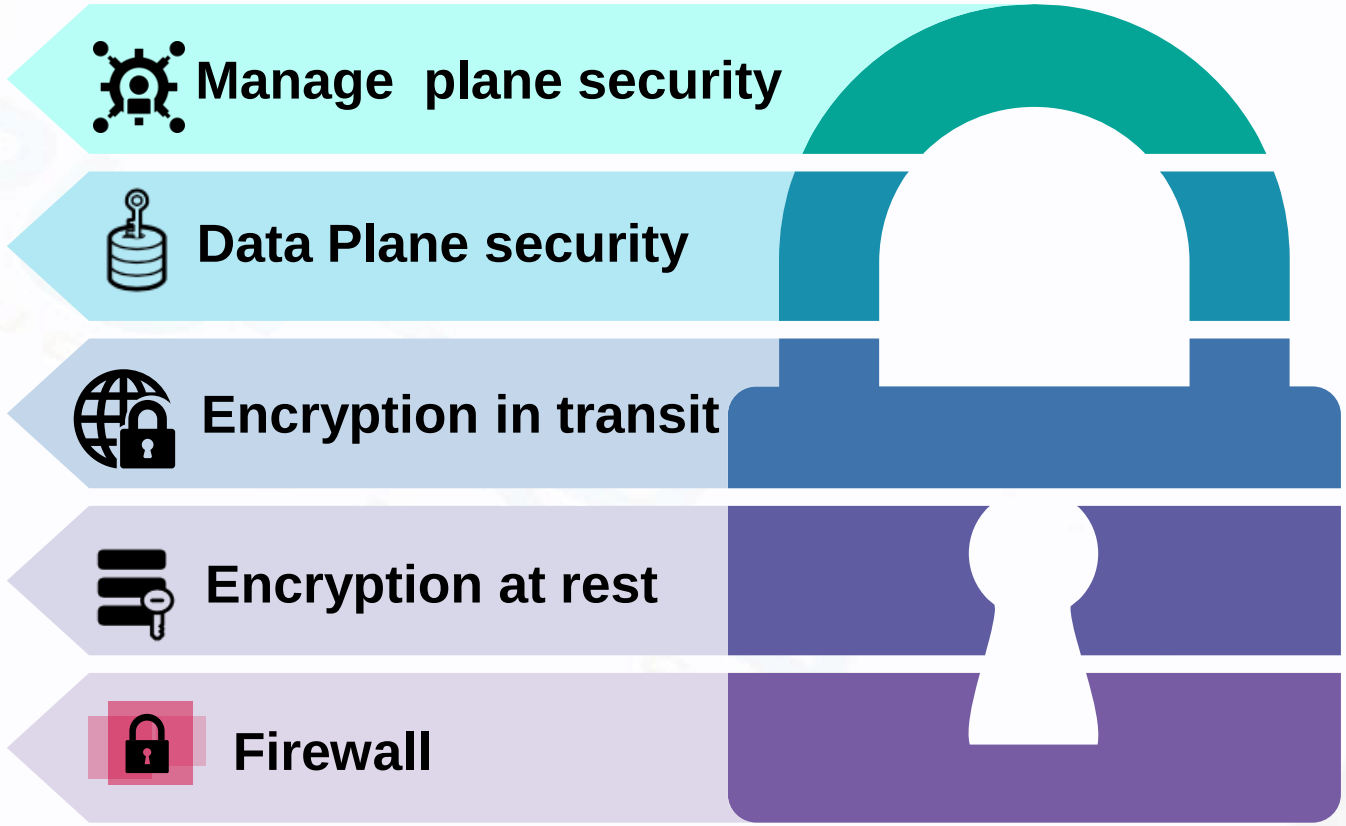
Securing your COSMOS DB account

Securing access to your data

Encryption in transit

Encryption at rest

Secure network level access



Management plane security

Management plane refers to the access to Azure COSMOS accounts, databases, containers and throughput.

- DocumentDB Accounts Contributor - Can manage Azure Cosmos DB accounts.
- Cosmos DB Account Reader - Can read Azure Cosmos DB account data.
- Cosmos Backup Operator - Can submit restore request for an Azure Cosmos database or a container.
- Cosmos DB Operator - Can provision Azure Cosmos accounts, databases, and containers but cannot access the keys that are required to access the data.

Data plane security

Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources.

Master Keys

- Provide access to accounts, databases, users, and permissions.
- Cannot be used to provide granular access to containers and documents.
- Are created during the creation of an account.
- Can be regenerated at any time.

Resource Tokens

- Provide access to specific containers, partition keys, documents, attachments, stored procedures, triggers, and UDFs.
- Are created when a user is granted permissions to a specific resource.
- Are time bound with a customizable validity period. The default valid timespan is one hour. Token lifetime, however, may be explicitly specified, up to a maximum of five hours.
- Provide a safe alternative to giving out the master key.

Resource tokens usage approach