Security – Azure Synapse Service

Eshant Garg

Data Engineer, Architect, Advisor

eshant.garg@gmail.com

Introduction

Source: Microsoft

Advance Data Security

Vulnerability assessment	• Discover track and remediate potential database vulnerabilities.
Data discovery & Classification	• Identify and label sensitive data for monitoring and alerting
Advanced Threat Protection	• Analyzes your SQL Server logs to detect unusual behavior and potentially harmful attempts

Auditing

- Tracks Database events and writes them to an audit logs

- Auditing allows to monitor, analyze and investigate database activities to identify potential threats or suspected abuse and security violations

Network Security

- Firewall rules allow or block IP addresses

- Uses port 1433

- Server firewall rules only

- Connections encrypted by default

Transparent Data Encryption

- By default, data in motion is always encrypted using TLS (Transport Layer Security)

- Encrypts and decrypts data at rest

- Uses AES-256 encryption algorithm

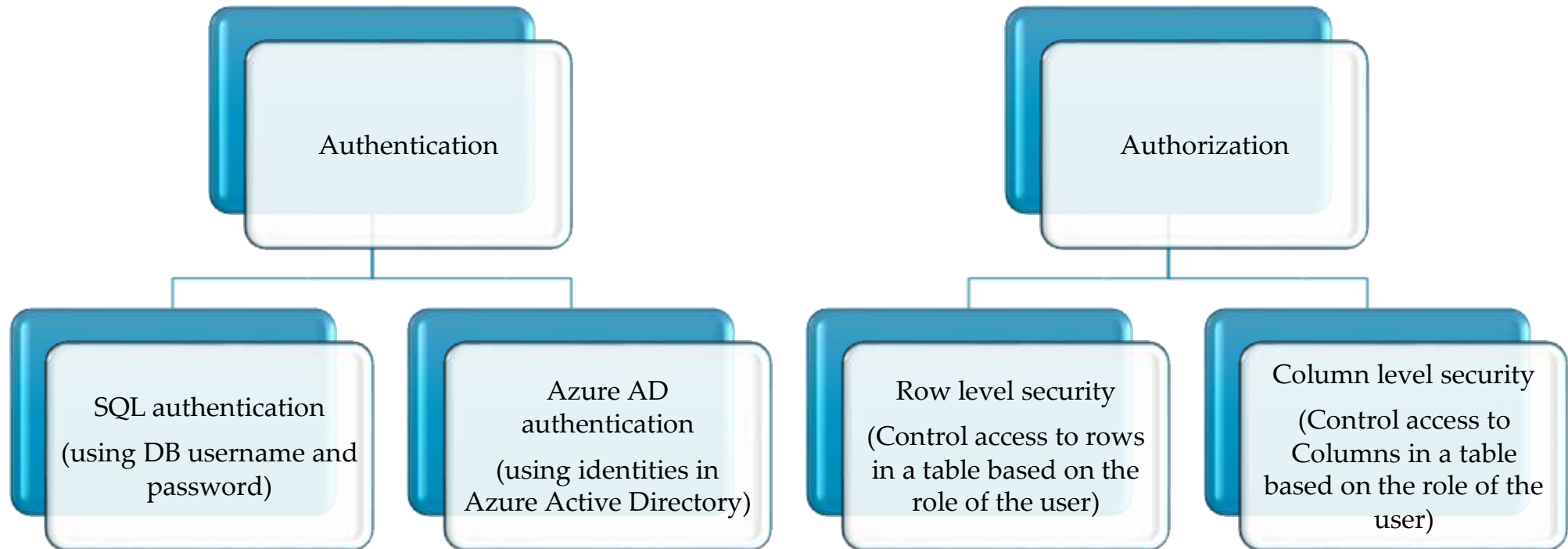- Encryption keys are stored in Azure key vault

Dynamic Data Masking(DDM)

- **Limit exposure to sensitive data by masking**
  - **Full** – entire column is masked
  - **Partial** – show starting and/or ending characters of the column data, mask the rest with custom string
  - **Email** – show the first character of the column data, mask the rest with xxx@xxxx.com
  - **Random** – entire column is replaced by random values

- **Reveals masked data to queries**
  - Data in the database is not changed

- **Enforced a the database level**
  - No impact at the application level

Access Management

Authentication

Authorization

SQL authentication (using DB username and password)

Azure AD authentication (using identities in Azure Active Directory)

Row level security (Control access to rows in a table based on the role of the user)

Column level security (Control access to Columns in a table based on the role of the user)

Row level security – use cases

- Hospital allows nurses to view data of their patients only

- Bank restrict financial data on role basis

- Multi-tenant application enforce a logical separation for each tenant in a single table

Column level security – use cases

- Financial firm allows only account managers to have access to customer social security numbers (SSN), phone, and other PII.

- Health care provider allows only doctors and nurses to have access to sensitive medical records.

Summary

Source: Microsoft