DP201 - Designing an Azure Data Platform Solution

Lab 4 – Azure Security Design Considerations

Exercise 1

Task 1: Defence in depth approach

Use the table below to document the security requirements for AdventureWorks. You can use requirements as identified from the AdventureWorks case study. You should also suggest security requirements that are missed but should be considered to ensure that AdventureWorks has proper security coverage.

Below are some examples of the requirements that could be identified.

Requirement	Defence in Depth Category
Only internal access allowed to the Azure SQL Data Warehouse	Identity & Access
The connected bicycle must have secure connections to 1st and 3rd party applications	Physical Security Network Access
Bots conversation history storage	
Use Azure Active Directory integration in the first instance	Identity & Access
Restrict Access to services based on IP Address	Network Perimeter
Encrypt data in Rest	Encryption
Use Shared Access Signatures for access to data stores required by external vendors.	Identity & Access
Enable database auditing to monitor data access	Identity & Access
Use Azure Key Fault to safeguard keys and secrets	Physical Security Identity & Access
Protect data in transit	Encryption
Use Role Based Access control	Identity & Access
Limit administrative access to services and resources	Identity & Access Compute
Ensure Application Level Security for third party applications	Application