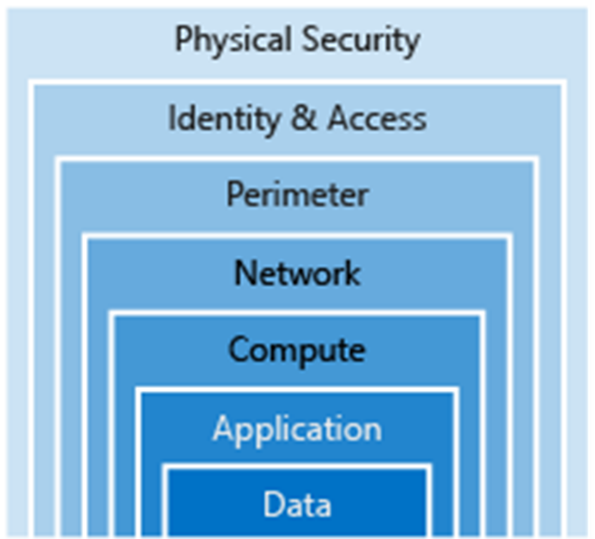
# **DP200 - Implementing a Data Platform Solution**

## Lab 8 – Securing Azure Data Platforms

### Exercise 1: Introduction to security

Below is a diagram that represents the layered support to security:



From the course content, case study and the scenarios taken in the course so far, spend 10 minutes in a group identify the layers of security that you have impacted so far to secure AdventureWorks in the labs. Find three examples.

|  |  |  |
| --- | --- | --- |
| Task | High level security task | Layer |
| 1 | Public/Private access levels to blob | Data |
| 2 | SAS/ storage account keys to access blob | Data |
| 3 | Access to Azure Data Warehouse/Azure Synapse Analytics | Data, Identity & Access |
| 4 | AAD app | Application |
| 5 | Azure Web App, and Twitter API security | Application |
| 6 | Azure DataWarehouse Firewall | Network |
| 7 | Secrets in API config | Identity & Access |
| 8 | RBAC for all Azure resources | Identity & Access |

Which security layers have we not dealt with in this course? Can you make a suggestion of what you would do in this area?

|  |  |  |
| --- | --- | --- |
| # | Layer | Suggestion |
| 1 | Physical Security | Encourage users to keep complex password meeting security standards |
| 2 | Perimeter | Restrict anonymous access wherever possible. Avoid access to external organization/ domain if possible |
| 3 | Compute | Use RBAC to resources like Azure Databricks, Cosmos DB, etc. |