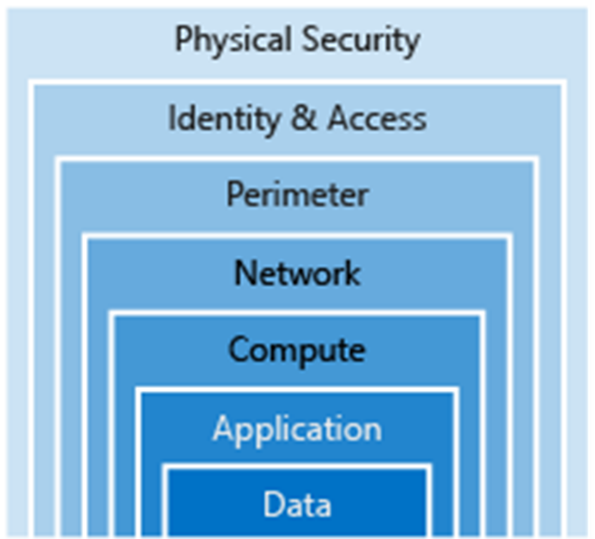
# **DP200 - Implementing a Data Platform Solution**

## 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 | Set access levels to blob containers | Data |
| 2 | Use Storage Account Keys to control access to Azure Blob or Data Lake Storage | Data |
| 3 | Create an application registration in Azure Active Directory | Application |
| 4 | Access Control (IAM) management of application Ids | Identity & Access |
| 5 | Use Azure Sign in to connect Visual Studio code with Cosmos DB | Identity & Access |
| 6 | Config and app.config file with a accountEndpoint  and account key for access | Identity & Access |
| 7 | Define a user name and password for access to SQL Database and SQL Data Warehouse | Identity & Access |
| 8 | Configure a SQL Service Fiewall | Network |
| 9 | Create a Database scoped credential | Identity & Access |
| 10 | Creating Event Hub Shared access policies | Identity & Access |
| 11 | Application accounts security (Telecom datagenerator or Twitter API) | Application |

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 | Consider the physical security of staff laptops that hold data |
| 2 | Perimeter | Work with the infrastructure Engineers to configure Perimeter security of the network. NAT, Vnet security etc. |
| 3 | Compute | Work with Azure Engineers to restrict the permission to Compute resources such as Databricks |