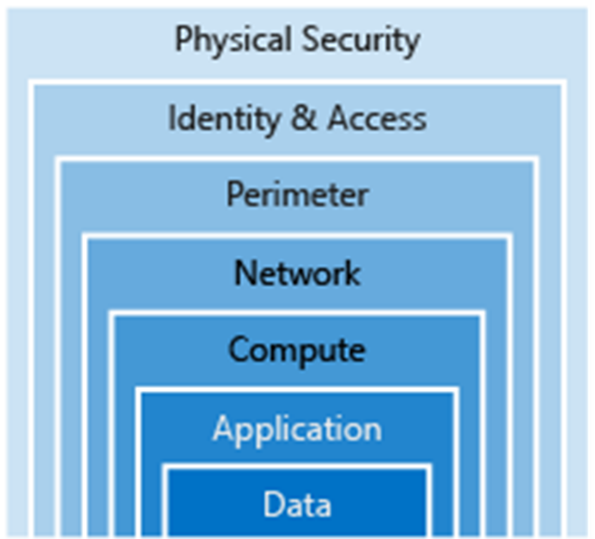
# **DP200 - 实施数据平台解决方案**

## 实验室 8 - 确保 Azure 数据平台安全

### 练习 1：安全性介绍

下面的图表表示对安全性的分层支持：



从到目前为止的课程内容、案例研究和课程场景中，以小组为单位花 10 分钟确定到目前为止你已经影响到的安全层，以确保实验室中的 AdventureWorks 的安全。找三个示例。

|  |  |  |
| --- | --- | --- |
| 任务 | 高级安全任务 | 层 |
| 1 | 将访问级别设置为 blob 容器 | 数据 |
| 2 | 使用存储帐户密钥来控制对 Azure Blob 或 Data Lake Storage 的访问 | 数据 |
| 3 | 在 Azure Active Directory 中创建应用程序注册 | 应用程序 |
| 4 | 应用程序 ID 的访问控制 (IAM) 管理 | 身份和访问 |
| 5 | 使用 Azure 登录，将 Visual Studio 代码与 Cosmos DB 连接 | 身份和访问 |
| 6 | Config 和 app.config 文件（带有 accountEndpoint 和  帐户密钥以供访问） | 身份和访问 |
| 7 | 定义用于访问 SQL 数据库和 SQL 数据仓库的用户名和密码 | 身份和访问 |
| 8 | 配置 SQL Service 防火墙 | 网络 |
| 9 | 创建数据库范围的凭证 | 身份和访问 |
| 10 | 创建事件中心共享访问策略 | 身份和访问 |
| 11 | 应用程序帐户安全性 (Twitter API) | 应用程序 |

在本课程中我们没有处理哪些安全层？你能否就这方面的做法提出建议？

|  |  |  |
| --- | --- | --- |
| # | 层 | 建议 |
| 1 | 物理安全性 | 考虑持有数据的员工笔记本电脑的物理安全性 |
| 2 | 外围 | 与基础结构工程师合作，配置网络的外围安全性。NAT、Vnet 安全性等。 |
| 3 | 计算 | 与 Azure 工程师合作以限制计算资源（如 Databricks）的权限 |