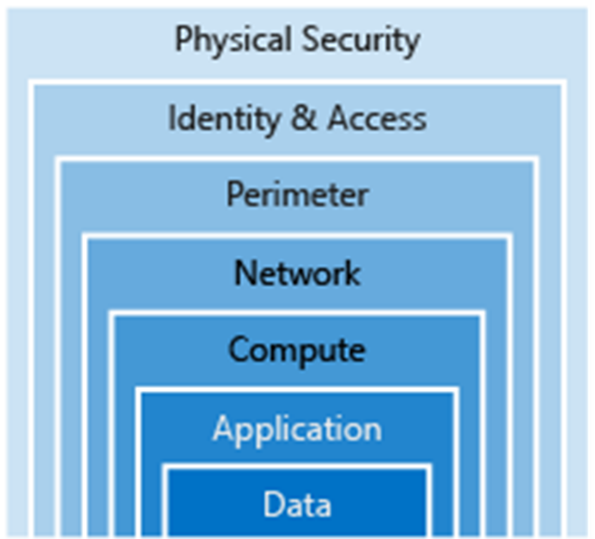
# **DP200 - 데이터 플랫폼 솔루션 구현**

## 랩 8 – Azure 데이터 플랫폼 보안

### 연습 1: 보안 소개

다음은 보안에 대한 계층화된 지원을 나타내는 다이어그램입니다.



과정 내용, 사례 연구 및 지금까지 수행된 시나리오에서 10분 동안 그룹별로 지금까지 랩에서 AdventureWorks를 보호하기 위해 영향을 준 보안 계층을 식별합니다. 세 가지 예제를 찾습니다.

|  |  |  |
| --- | --- | --- |
| 작업 | 높은 수준의 보안 작업 | 계층 |
| 1 | BLOB 컨테이너에 대한 액세스 수준 설정 | 데이터 |
| 2 | 스토리지 계정 키를 사용하여 Azure Blob 또는 Data Lake Storage에 대한 액세스를 제어합니다. | 데이터 |
| 3 | Azure Active Directory에서 애플리케이션 등록 만들기 | 애플리케이션 |
| 4 | 애플리케이션 ID의 IAM(액세스 제어) 관리 | ID 및 액세스 |
| 5 | Azure 로그인을 사용하여 Visual Studio Code를 Cosmos DB와 연결합니다. | ID 및 액세스 |
| 6 | accountEndpoint가 있는 Config 및 app.config 파일  액세스용 계정 키 | ID 및 액세스 |
| 7 | SQL Database 및 SQL Data Warehouse에 액세스할 수 있는 사용자 이름 및 암호 정의 | ID 및 액세스 |
| 8 | SQL 서비스 방화벽 구성 | 네트워크 |
| 9 | 데이터베이스 범위 별 자격 증명 만들기 | ID 및 액세스 |
| 10 | 이벤트 허브 공유 액세스 정책 만들기 | ID 및 액세스 |
| 11 | 애플리케이션 계정 보안(트위터 API) | 애플리케이션 |

이 과정에서 다루지 않은 보안 계층은 무엇인가요? 이 영역에서 무엇을 할 것인지 제안할 수 있나요?

|  |  |  |
| --- | --- | --- |
| # | 계층 | 제안 사항 |
| 1 | 물리적 보안 | 데이터를 보유한 직원 랩톱의 물리적 보안 고려 |
| 2 | 경계 | 인프라 엔지니어와 협력하여 네트워크의 경계 보안을 구성합니다. NAT, Vnet 보안 등 |
| 3 | 컴퓨팅 | Azure 엔지니어와 협력하여 Databricks와 같은 리소스 컴퓨팅 권한을 제한합니다. |