7- Defense in Depth

---

1. physical security
2. access and control
3. perimeter security
4. network security
5. compute security
6. application security
7. data security

Physical security

Microsoft maintains physical security at the data centers.

Access and identity

provided by Azure Active Directory
Eg: Conditional Access, MFA and identity protection

---

perimeter security

one example of the service at this layer is Azure DDoS which defends against Denial-of-service.

---

network security

An example at this layer is Network Security Groups, which are essentially firewall rules for your Azure networks.

compute security

To ensure that their Operating Systems are regularly patched. Fortunately, many of the compute services take care of this for you. But if you are using VM’s, you need to take care of this yourselves.

Application Security

Ensure your developers write your applications in a secure manner.

Data Security

This is what attackers are usually trying to access.

- Azure offers a variety of data security features, such as
  - Encryption
  - Advanced Threat protection in Azure SQL Database.