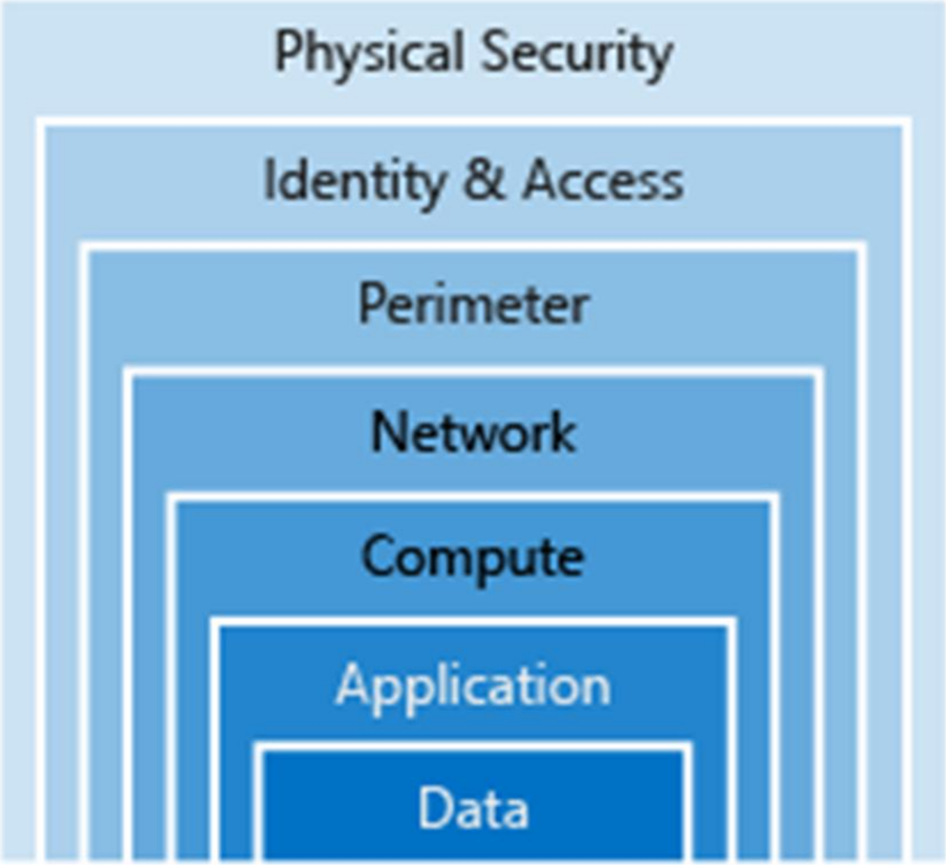
Microsoft

DP-201T04: Security Design Considerations

Lesson Objectives

- Take a defense in depth approach to securing your architecture.
- How to protect your identities.
- Technologies to protect your Azure infrastructure.
- Use encryption to secure your data.
- Protect your architecture at the network level.
- Leverage application security best practices

Defence in Depth Approach.



Identity Management

Identifying users that access your resources is an important part of security design.

Identity as a security layer

Customers and employees alike expect to be able to access services from anywhere at any time, which has driven the development of identity protocols that can work at internet scale across many disparate devices and operating systems.

Single sign-on

With single sign-on, users only need to remember one ID and one password. Access across database systems or applications is granted to a single identity tied to a user

SSO with Azure Active Directory

Azure Active Directory (AD) is a cloud-based identity service. It has built-in support for synchronizing with your existing on-premises Active Directory or can be used stand-alone. This means that all your applications, whether on-premises, in the cloud (including Office 365), or even mobile can share the same credentials.

Infrastructure Protection

Role Based Access Control

Roles are defined as collections of access permissions. Security principals are mapped to roles directly or through group membership.

Roles and management groups

Roles are sets of permissions that users can be granted to. Management groups add the ability to group subscriptions together and apply policy at an even higher level.

Privileged Identity Management

Azure AD Privileged Identity Managemen (PIM) is an additional paid-for offering that provides oversight of role assignments, self-service, and just-in-time role activation

Providing identities to services

An Azure service can be assigned an identity to ease the management of service access to other Azure resources.

Service principals

A Service Principal is literally named. It is an identity that is used by a service or application. Like other identities, it can be assigned roles

Managed identities

When you create a managed identity for a service, you create an account on the Azure AD tenant. Azure infrastructure will automatically take care of authentication

Encryption

Encryption at rest

Data at rest is the data that has been stored on a physical medium. This could be data stored on the disk of a server, data stored in a database, or data stored in a storage account.

Encryption in transit

Data in transit is the data actively moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers.

Encryption on Azure.

Raw Encryption

Enables the encryption of:

- Azure Storage
- V.M. Disks
- Disk Encryption

Database Encryption

Enables the encryption of databases using:

- Transparent Data Encryption

Encrypting Secrets

Azure Key Vault is a centralized cloud service for storing your application secrets.

.

Network Security

Network security is protecting the communication of resources within and outside of your network. The goal is to limit exposure at the network layer across your services and systems

Internet protection

A great first place to start is to assess the resources that are internet-facing, and only allow inbound and outbound communication where necessary. Identify all resources that are allowing inbound network traffic of any type, and ensure they are necessary and restricted to only the ports/protocols required.

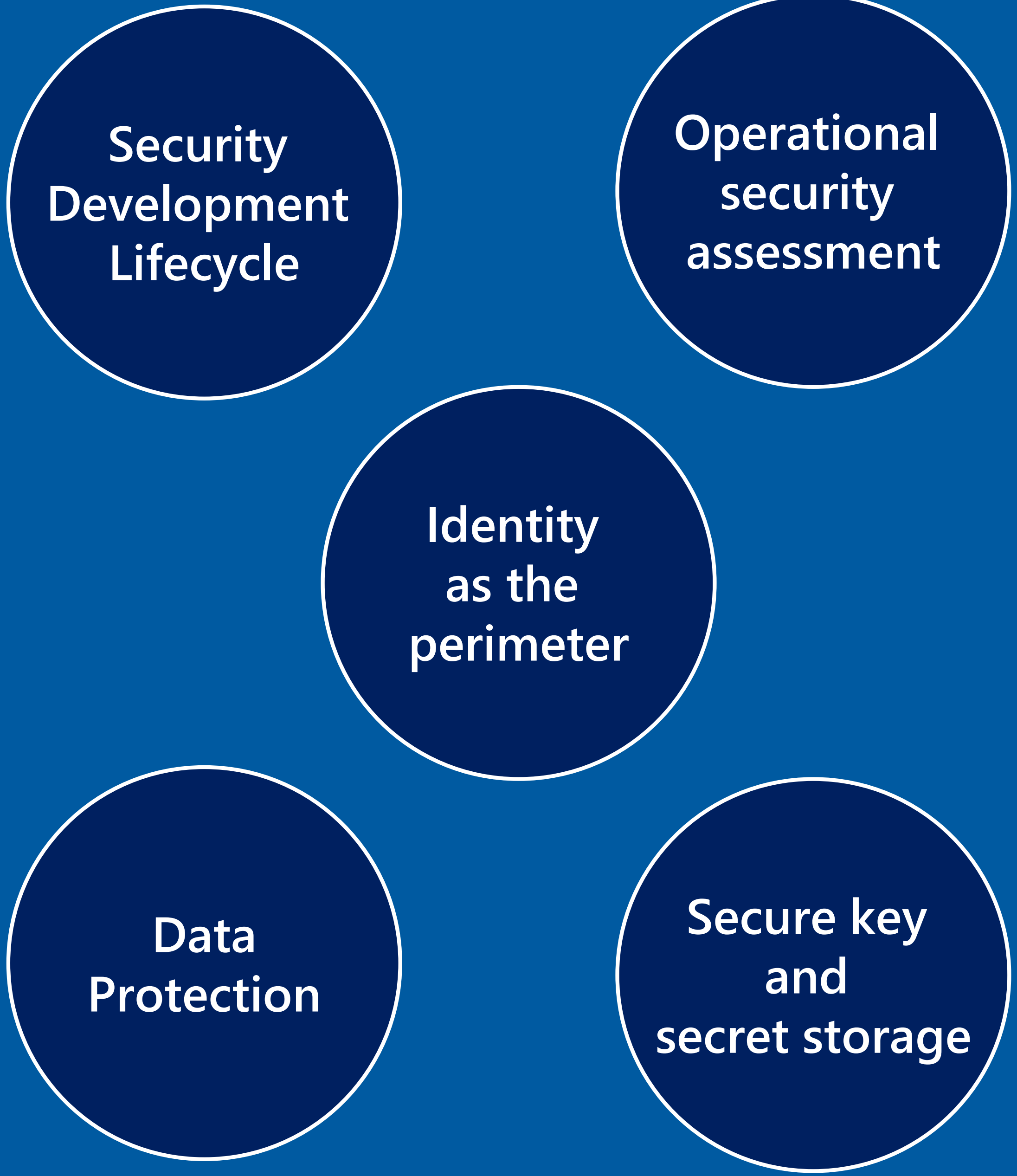
Virtual network security

To isolate Azure services to only allow communication from virtual networks, use VNet service endpoints. With service endpoints, Azure service resources can be secured to your virtual network.

Network integration

VPN connections are a common way of establishing secure communication channels between networks, and this is no different when working with virtual networking on Azure. Connection between Azure VNets and an on-premises VPN device is a great way to provide secure communication.

Application Security



Security Development Lifecycle

Operational security assessment

Identity as the perimeter

Data Protection

Secure key and secret storage

Lab: Azure Data Platform Security Design Considerations

Lab overview

The students will explore the range of security options that are available to provide a defence in depth approach to securing the AdventureWorks environment. This will include investigating the available network protection options that are available, as well as the authentication mechanisms that are support by each service. The students will also understand the encryption options that are available and demonstrate an understanding of network level and application level protection.

Lab objectives

After completing this lab, you will be able to:

1. Defense in Depth Security Approach
2. Identity Management

Lab scenario

You have recently been hired as a senior data engineer at AdventureWorks and are working with a consultant and architects to design a security approach for cloud data platform solution that meets the organizations technical and business requirements.

Working in a group, you will be performing a security assessment of the architectures that have been defined so that there is a defense in depth approach to securing the environment. Firstly, you will create a document to show the aspects of the architecture that require securing. You will then specify the identity management approach that is required.

It is important that you should be able to justify your choices as a team, and you are encouraged to use references from Microsoft such as Microsoft documentation, or blogs from Microsoft to provide evidence that supports your choices.

At the end of this lab, you will have defined:

1. Defense in Depth Security Approach
2. Identity Management

Lab review

- Exercise 1 – Explore the answers given by each group. What was the common ground? What were the differences?

- Exercise 2 – Who should be involved in the design process for authentication?

- Are there other security areas that should be considered in depth?

Module Summary ❯

In this module, you have learned about:

- Take a defense in depth approach to securing your architecture.
- How to protect your identities.
- Technologies to protect your Azure infrastructure.
- Use encryption to secure your data.
- Protect your architecture at the network level.
- Leverage application security best practices

Next steps ❯

After the course, use the Azure Security Center to keep track of security updates to the products that you are interested in.