

AZ-305

Tag 3

# Designing Microsoft Azure Infrastructure Solutions

Guten Morgen!



# AZ-305 Agenda

Module 01 Design a governance solution

Module 02 Design a compute solution

Module 03 Design a non-relational data storage solution

✓ NFS ✓

Module 04 Design a data storage solution for relational data

✓

Module 05 Design a data integration solution

✓

Module 06 Design an application architecture solution

✓

Service Bus  
Queue

---

Module 07 Design Authentication and Authorization Solutions

Module 08 Design a solution to log and monitor Azure resources

Log Analytics

Module 09 Design a network infrastructure solution

Module 10 Design a business continuity solution

Module 11 Design a migration solution

07

# Design Authentication and Authorization Solutions



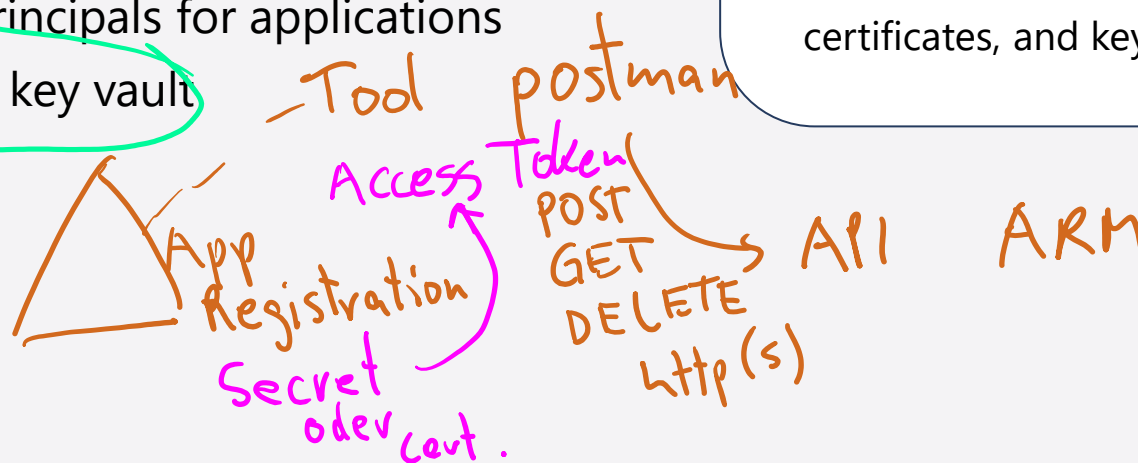
# Learning Objectives

- Design for identity and access management
- Design for Microsoft Entra ID
- Design for Microsoft Entra B2B
- Design for Azure Active Directory B2C
- Design for conditional access *MFA free*
- Design for identity protection *P1*
- Design for access reviews
- Design service principals for applications
- Design for Azure key vault
- Case study
- Learning recap

AZ-305: Design Identity, Governance, and Monitoring Solutions (25-30%)

## Design Authentication and Authorization Solutions

- Recommend an authentication solution
- Recommend an identity management solution
- Recommend a solution for authorizing access to Azure resources
- Recommend a solution to manage secrets, certificates, and keys



# Design for identity and access management



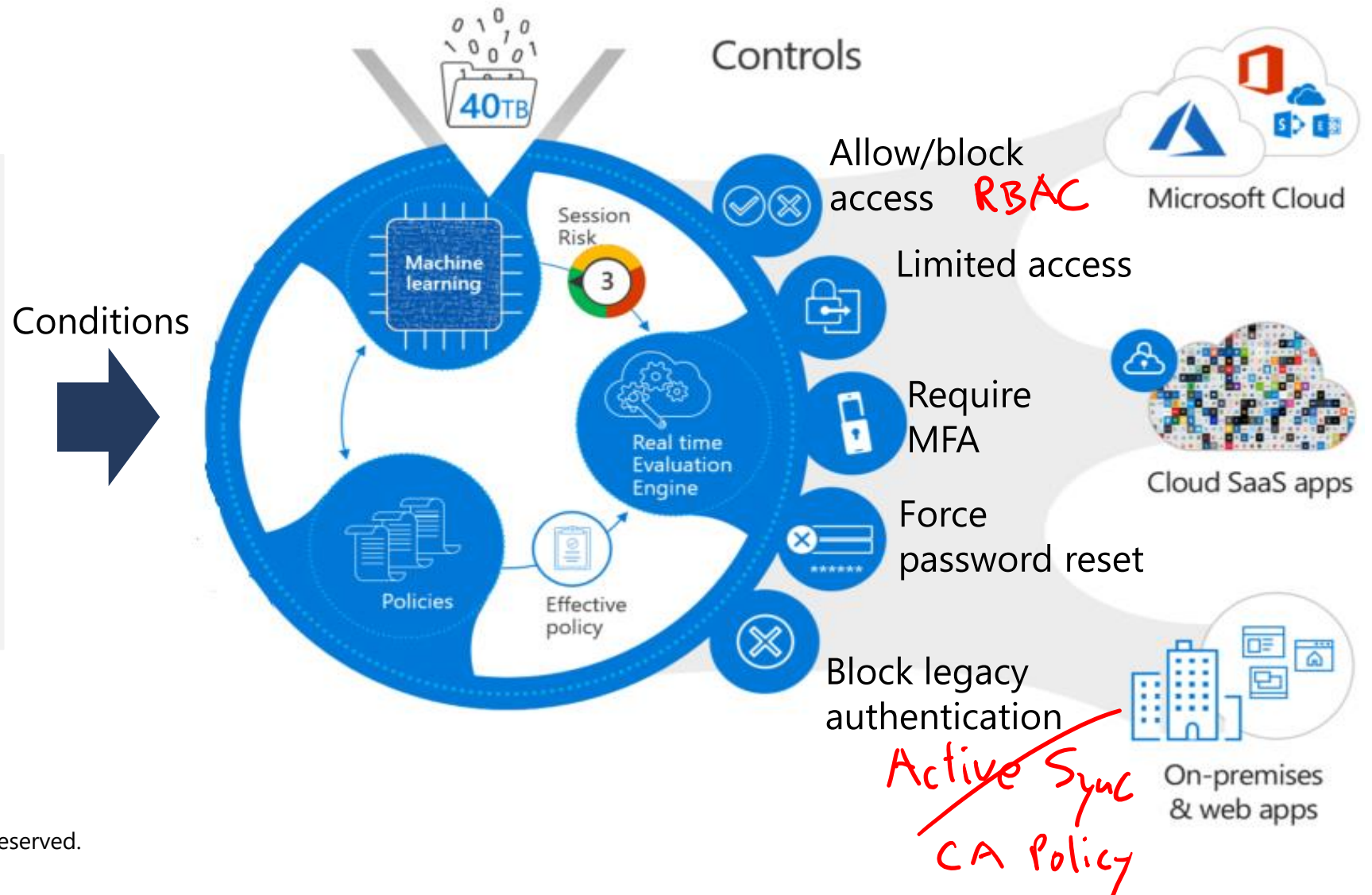


# Follow the Zero Trust model guidelines

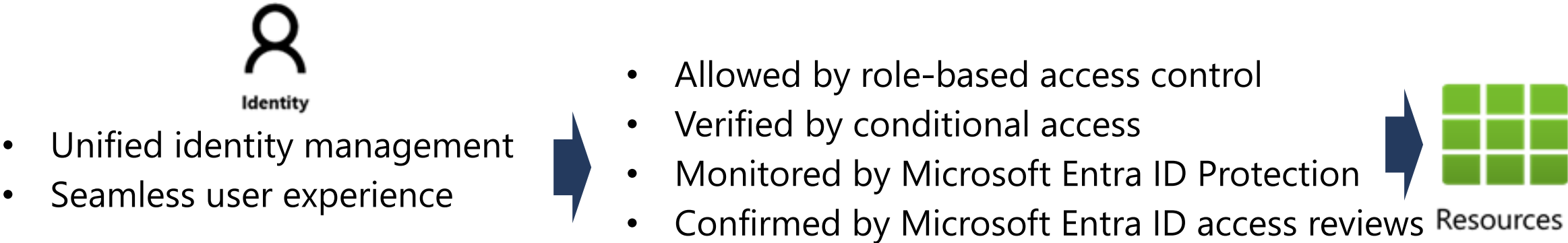
- Never trust, always verify.
- Assume Breach

- Employee and partner user and roles
- Trusted and compliant devices
- Physical and virtual location
- Client apps and authentication method

OAuth 2.0



# What is identity and access management



If you need this	Use this
Provide identity and access management for employees in a cloud or hybrid environment.	Microsoft <span>Entra ID</span> <span>△ Tenant</span>
Collaborate with <span>guest users</span> and external business partners like suppliers and vendors.	Microsoft Entra B2B
Control how customers sign up, sign in, and manage their profiles when they use your applications.	<span>Azure AD Business to Consumer (B2C)</span>

# Design for Microsoft Entra ID

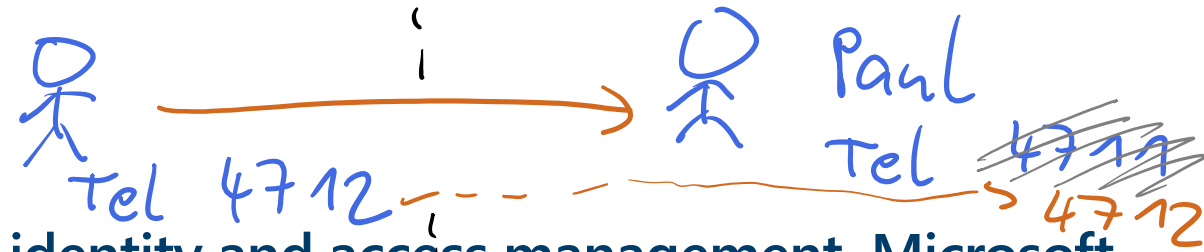




# When to use Microsoft Entra ID

Microsoft Entra ID is a cloud-based solution for identity and access management. Microsoft Entra ID is a multitenant, cloud-based directory, and identity management service.

- Centralize identity management
- Establish a single Microsoft Entra tenant
- Use Microsoft Entra Connect, or Microsoft Entra Connect Sync for hybrid identity sync



M 365

On-premises Identities

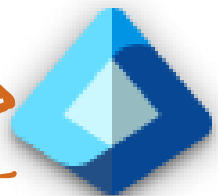
Azure Identities



Active Directory Domain Services

Tool (MS IDManager)

Microsoft Entra Connect  
write back

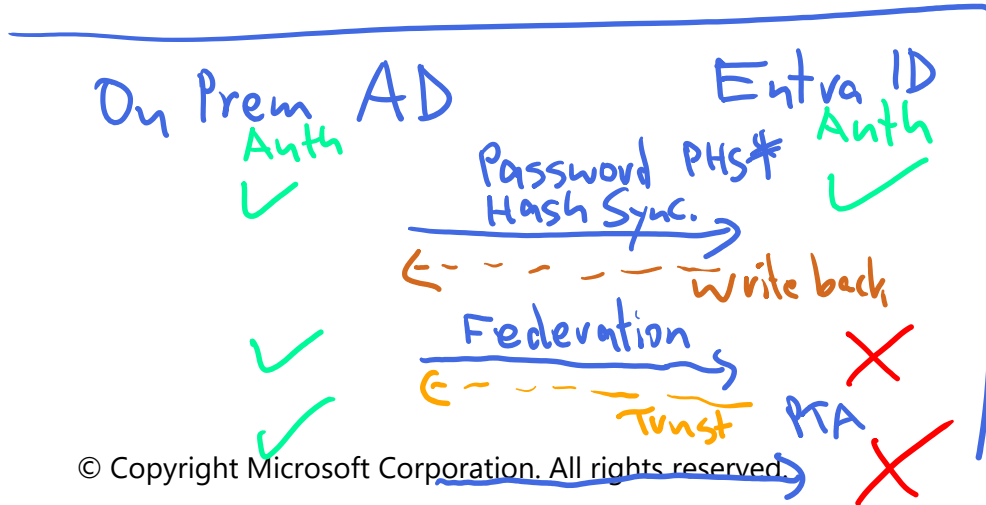


Microsoft Entra ID

- Internal users
- On-premises users
- Guest users (B2B)

Kerberos :88  
~~NTLM~~

:443  
O Auth 2.0  
O ID Connect



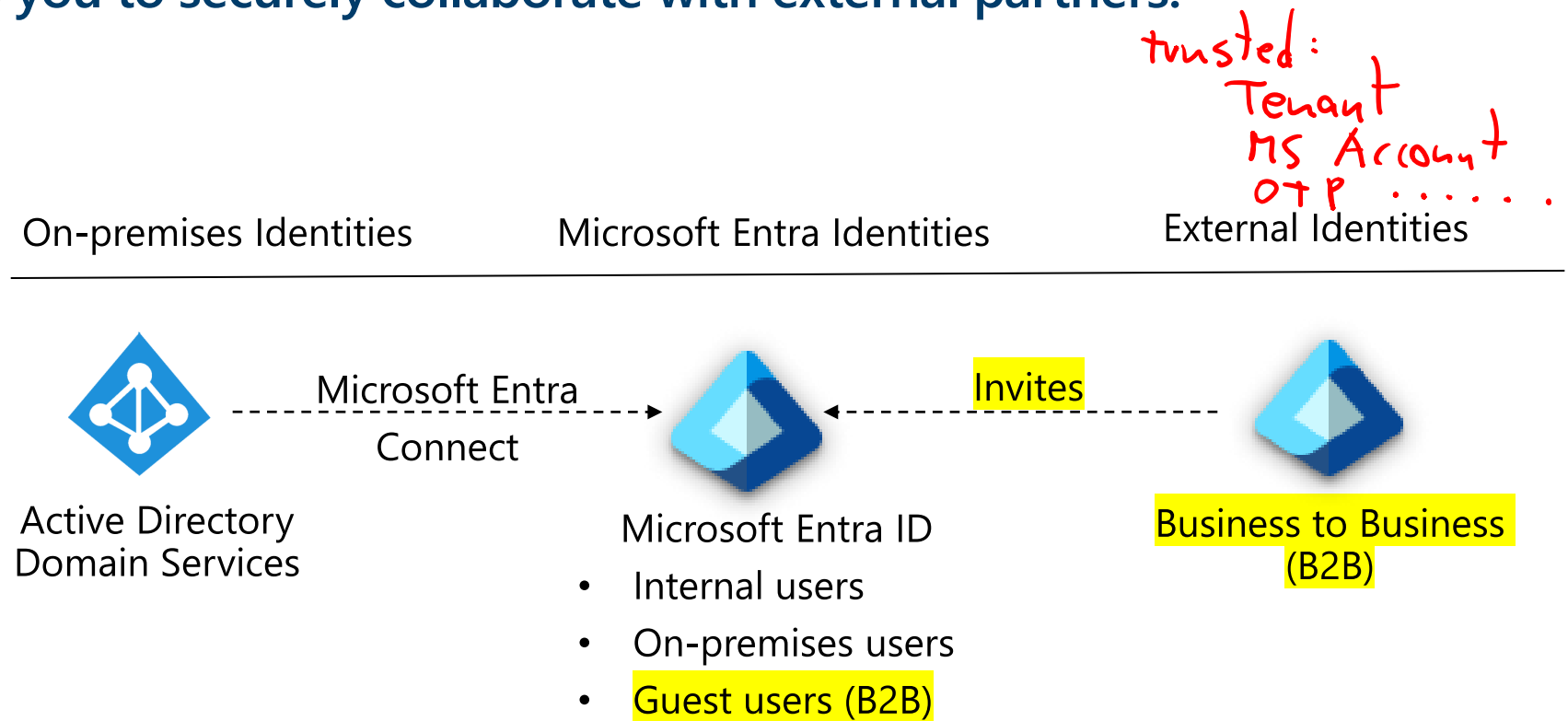
# Design for Microsoft Entra Business to Business



# When to use Microsoft Entra Business to Business (B2B)

Microsoft Entra B2B enables you to securely collaborate with external partners.

- Integrate with identity providers
- Use conditional access policies to intelligently grant or deny access
- Require MFA for guest users



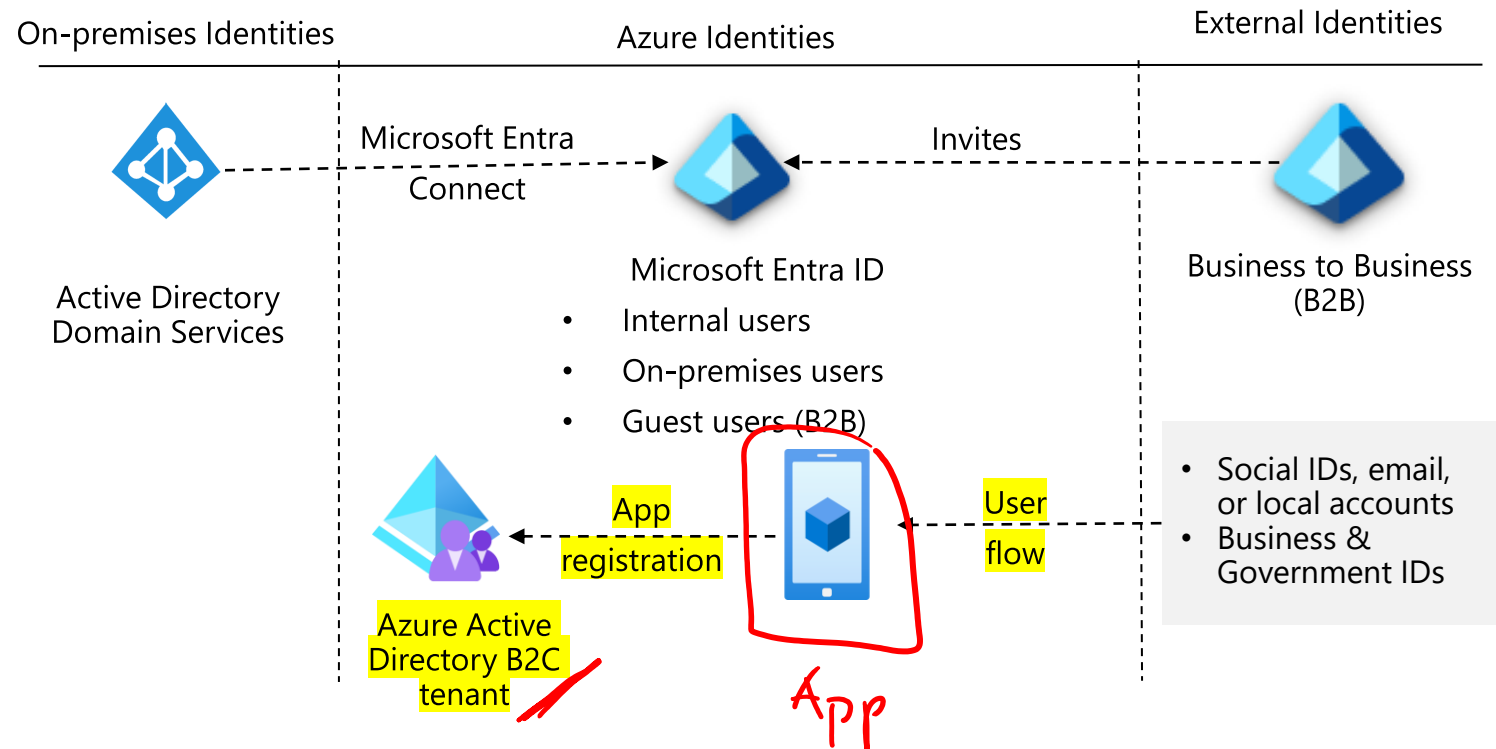
# Design for Azure AD Business to Customer



# When to use Azure AD Business to Customer (B2C)

Azure AD B2C is a tenant to manage customer identities and their application access.

- Integrate with external user stores
- Provide single sign-on access with a user-provided identity
- Create a custom-branded identity solution
- Use policies to configure user journeys
- Use progressive profiling to gradual collect user information
- Pass user data to a 3<sup>rd</sup> party for validation





# Compare solutions (activity)



- Customers cannot be viewed by other users
- Users are managed in a separate Microsoft Entra tenant
- Users need to be able to self-signup for accounts
- Users manage their own profiles
- Users can come from SAML and WS-Fed based identity providers

Business to  
Business

OR

Business to  
Consumer

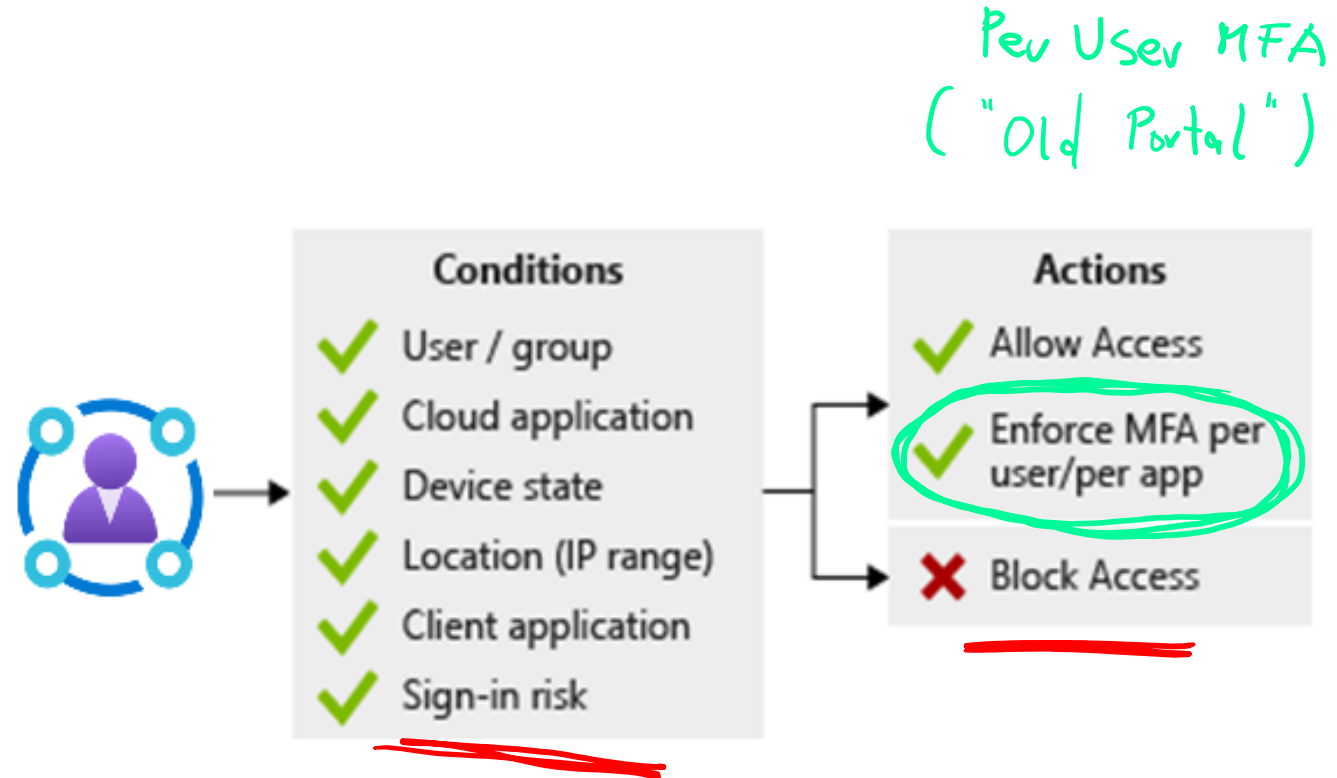
# Design for conditional access



# When to use conditional access

Conditional Access is a Microsoft Entra tool that allows (or denies) access to resources.

- Use to enable multifactor authentication
- Require managed devices
- Access only approved client applications
- Exclude countries from which you never expect a sign in
- Respond to potentially compromised accounts.
- Completely block access
- Block legacy authentication protocols.
- Test using the report-only mode



# Design for identity protection



# When to use identity protection

P1

P2

P1M

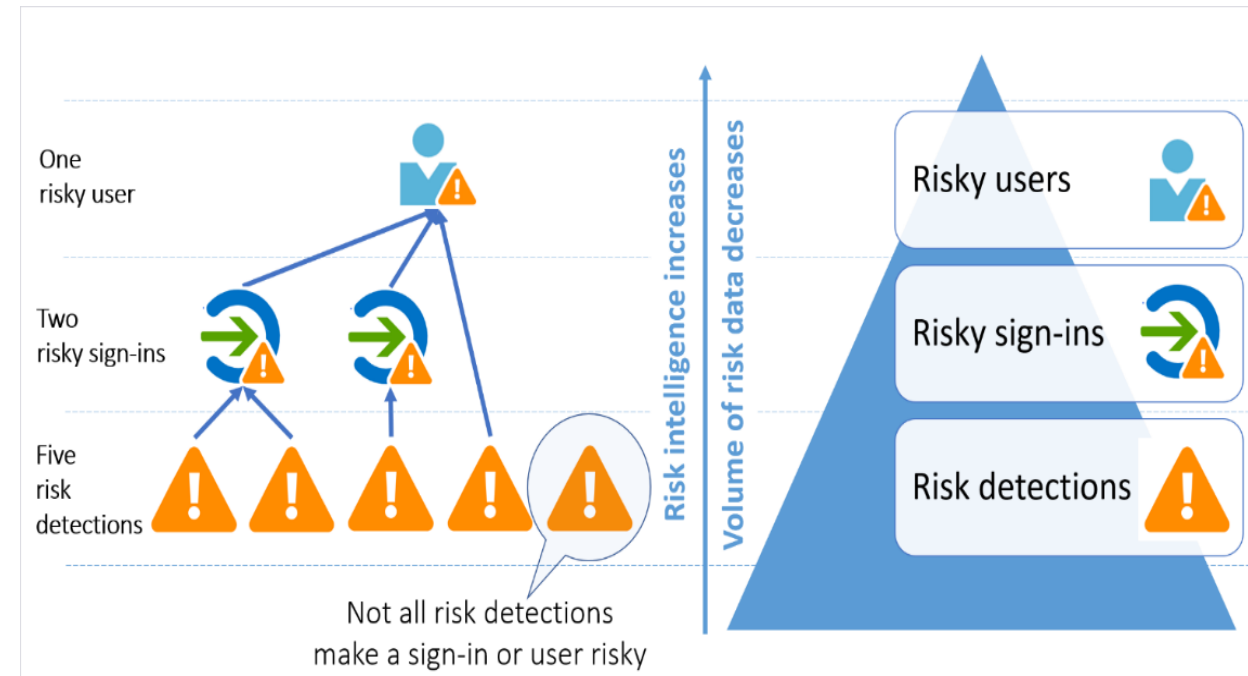
Priv. ID Mngt

Request  
Role ✓  
Time

Identity protection is a Microsoft Entra tool that automates the detection and remediation of identity-based risks.

- Configure the policies and actively review the results
- Set the sign-in risk policy to Medium and above and allow self-remediation options
- Set the user risk policy threshold to High
- Allow for excluding users - emergency access or break-glass administrator accounts
- Send data to Conditional Access or other security information and event management (SIEM) tool

Sentinel





# Design for access reviews

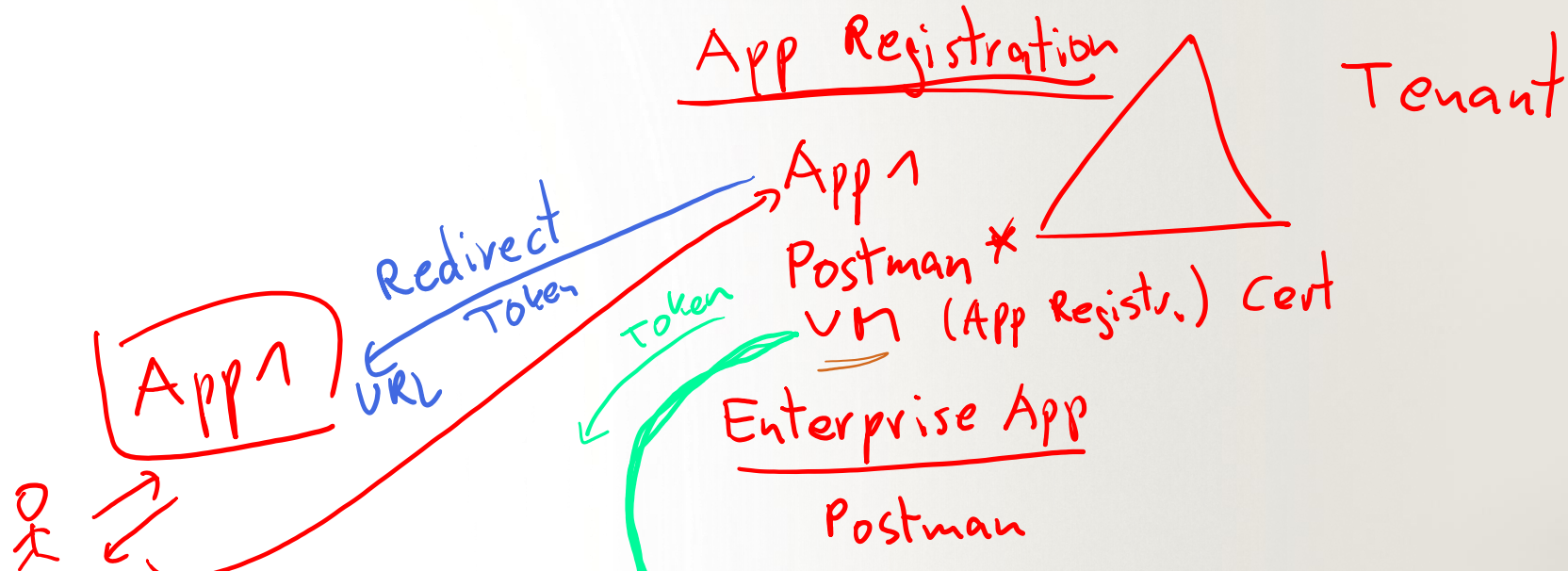


# When to use access reviews

Access reviews are a Microsoft Entra tool to review user access and ensure they should have continued access to resources.

- Determine the purpose of the access review
- Engage the right stakeholders
- Create an access review plan
- Determine who will conduct the reviews
- Decide who can self-attest access
- Determine what resource types will be reviewed
- Start small – pilot your plan – keep people informed

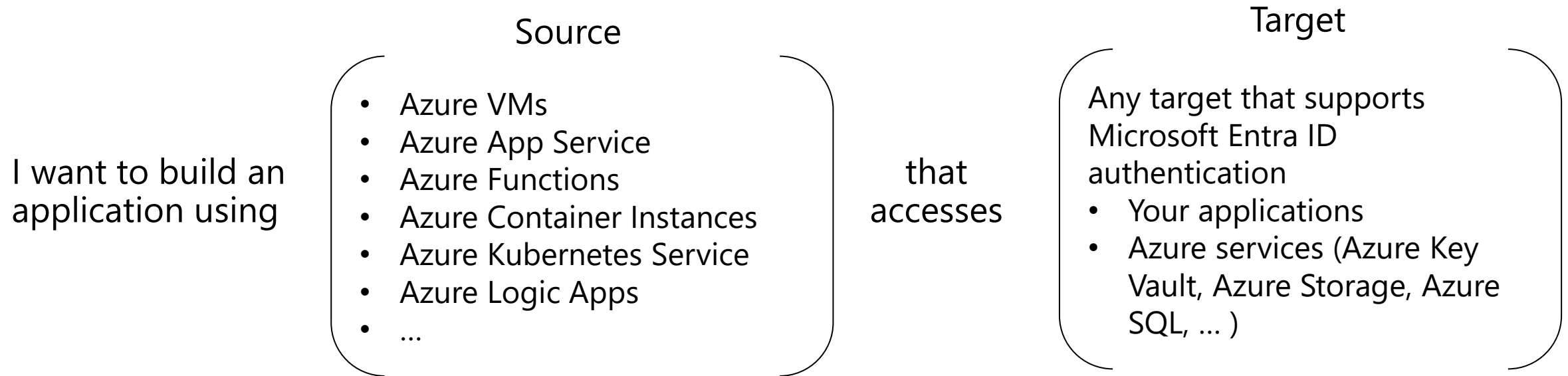




# Design service principals for applications

# Design managed identities

Managed identities provide an identity for application authentication.



- The source is an Azure resource
- The target supports Microsoft Entra ID authentication and Azure RBAC
- No credential rotation or certificate management

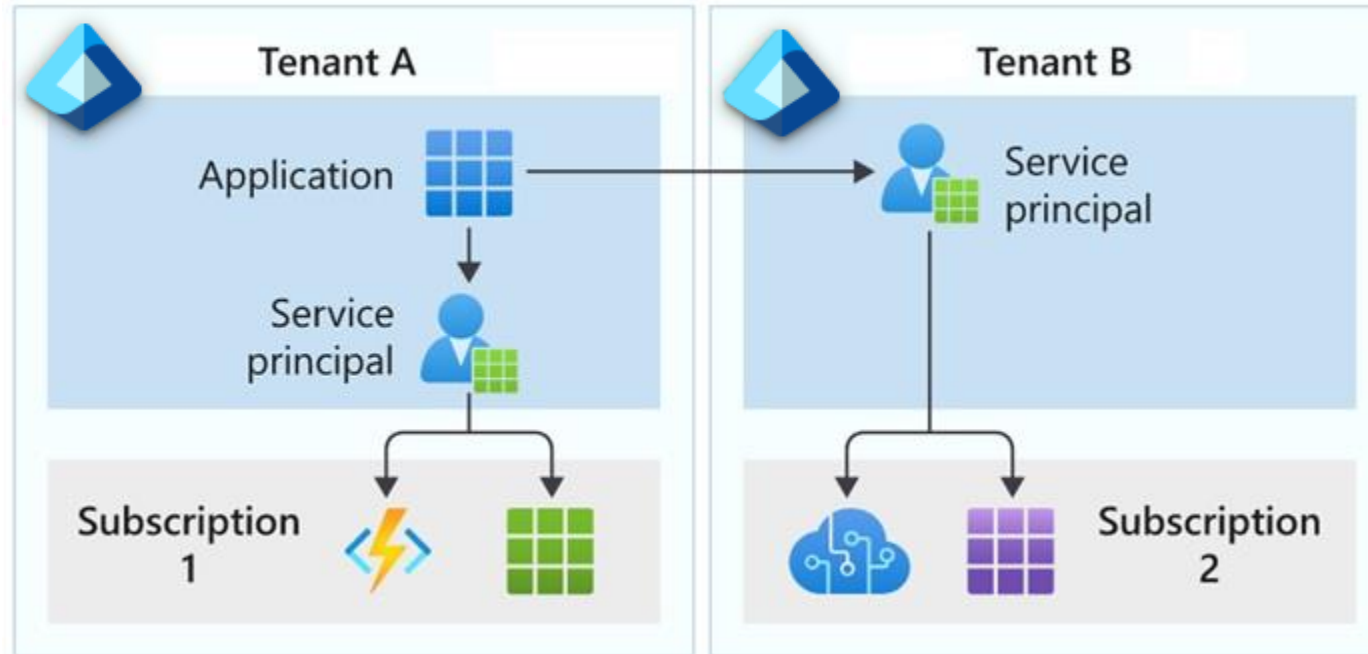
# Select managed identities

Property	System-assigned managed identity	User-assigned managed identity
Creation	<ul style="list-style-type: none"><li>Created as part of an Azure resource</li></ul>	<ul style="list-style-type: none"><li>Created as a stand-alone Azure resource</li></ul>
Life cycle	<ul style="list-style-type: none"><li>Shared life cycle with the Azure resource</li></ul>	<ul style="list-style-type: none"><li>Independent life cycle</li><li>Must be explicitly deleted</li></ul>
Sharing across Azure resources	<ul style="list-style-type: none"><li>Cannot be shared</li><li>Can only be associated with a single Azure resource</li></ul>	<ul style="list-style-type: none"><li>Can be shared</li><li>Can be associated with more than one Azure resource</li></ul>
Common use cases	<ul style="list-style-type: none"><li>Workloads that are contained within a single Azure resource</li><li>Workloads for which you need independent identities.</li><li>For example, an application that runs on a single virtual machine</li></ul>	<ul style="list-style-type: none"><li>Workloads that run on multiple resources and which can share a single identity</li><li>Workloads that need pre-authorization to a secure resource as part of a provisioning flow.</li><li>Workloads where resources are recycled frequently, but permissions should stay consistent.</li></ul>



# Select application service principals

The local representation, or application instance, of an object in a single tenant or directory



Useful when Managed Identities cannot be used

Authentication is performed by the application using a secret or certificate

Often used to authenticate external applications to Azure resources

# Best practices for requesting permissions

When building an app that uses Microsoft Entra ID to provide sign-in and access tokens for secured endpoints, there are a few good practices you should follow.



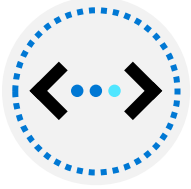
When registering an application in Microsoft Entra ID, consider business and security needs of admin consent versus user consent

---



Only ask for the permissions required for implemented app functionality. Don't request user consent for permissions that you haven't yet implemented for your application.

---



In addition, when requesting permissions for app functionality, you should request the least-privileged access.

---



Apps should gracefully handle scenarios where the user doesn't grant consent to the app when permissions are requested.

Standard  
Premium

Soft  
Hard

# Design for Azure key vault



# Design for Azure Key Vault

Azure Key Vault provides a secure storage area for managing all your app secrets so you can properly encrypt your data in transit or while it's being stored.

## Why use Key Vault?

- Separation of sensitive app information from other configuration and code, reducing the risk of accidental leaks.
- Restricted secret access with access policies tailored to the apps and individuals that need them. *pro Region!*
- Centralized secret storage, allowing required changes to happen in only one place.
- Access logging and monitoring to help you understand how and when secrets are accessed.
- Implementing Customer Managed Keys for Azure services

## When to consider multiple Key Vaults:

- RBAC vs Policies
- Performance

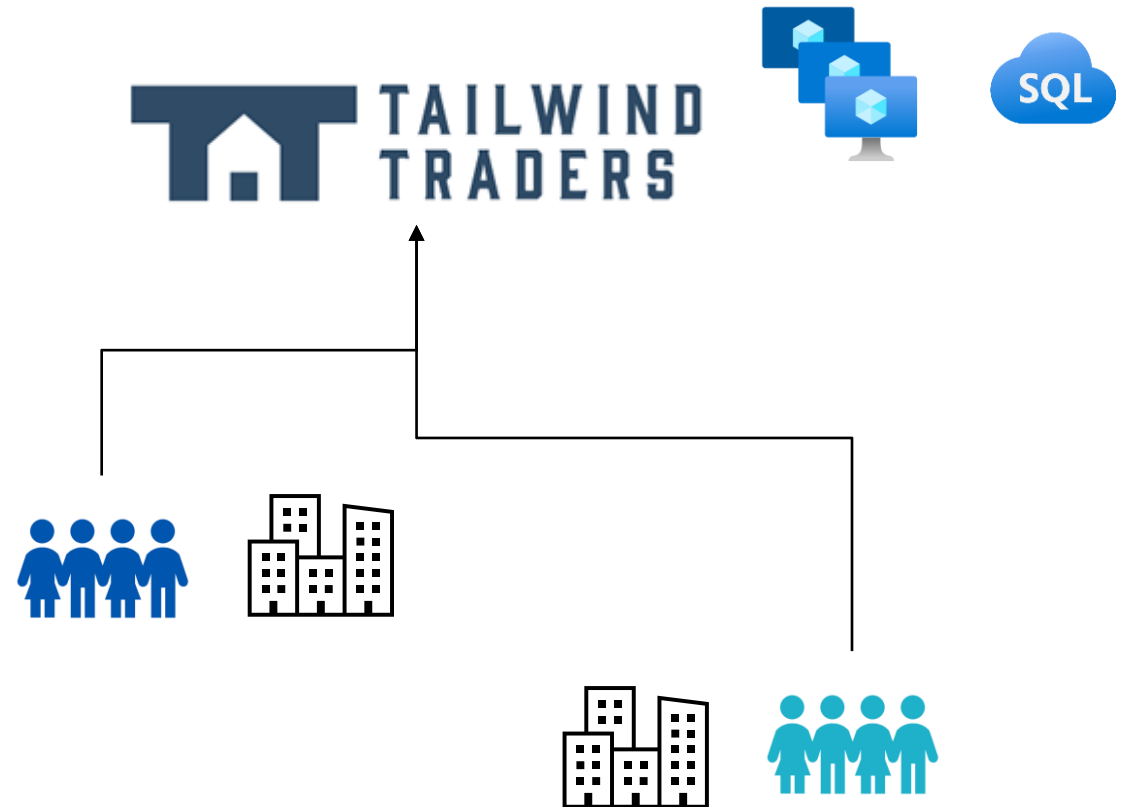
# Case study and review



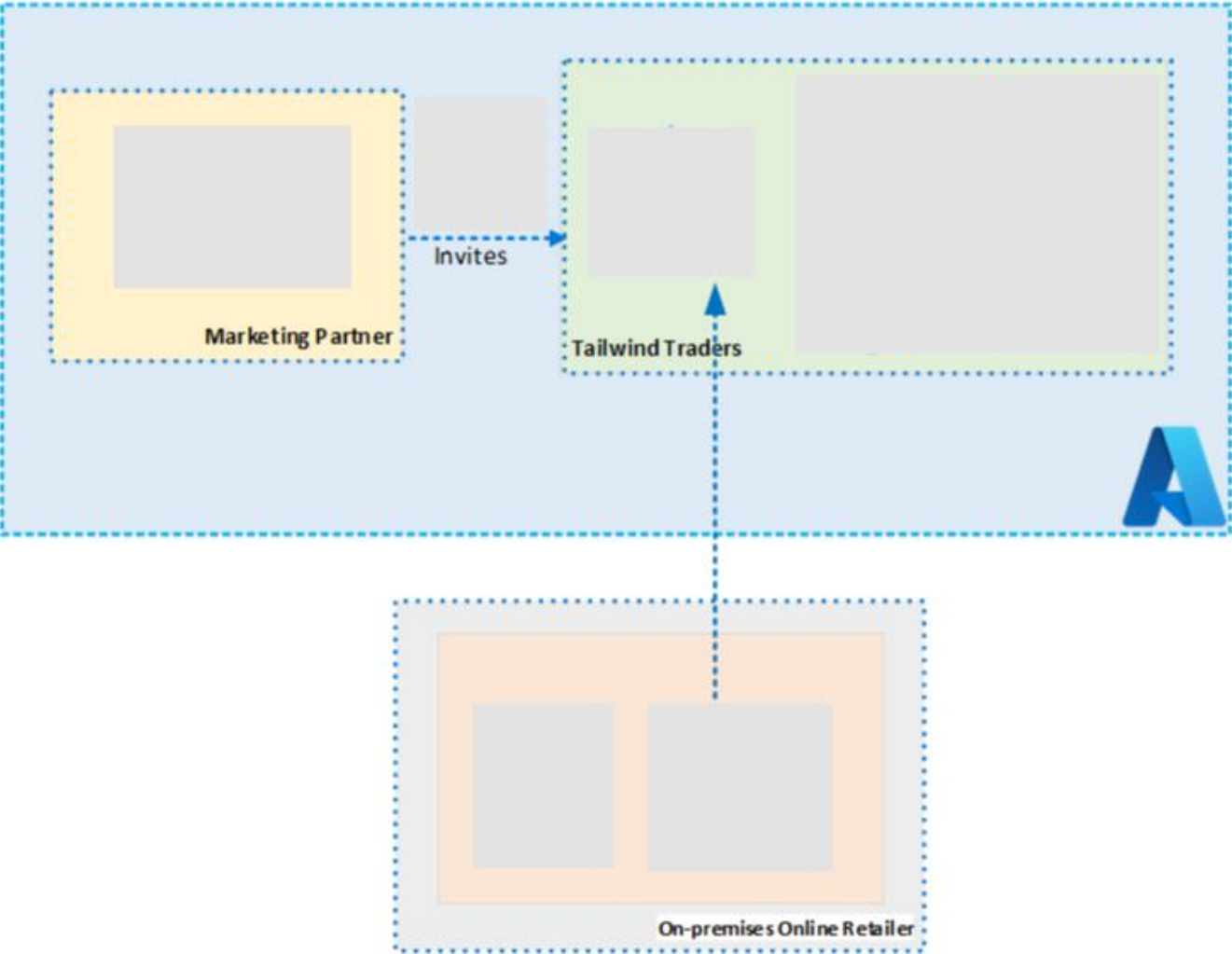


# Case Study – Authentication and authorization

1. A company acquisition will add 75 employees – new user accounts
2. New employees are in different geographic regions – new identity protection policies
3. New application with a SQL database – access solution



# Instructor – New Employee Accounts



ADDS



Microsoft  
Entra  
Connect



Conditional  
Access



Identity  
Protection



B2B

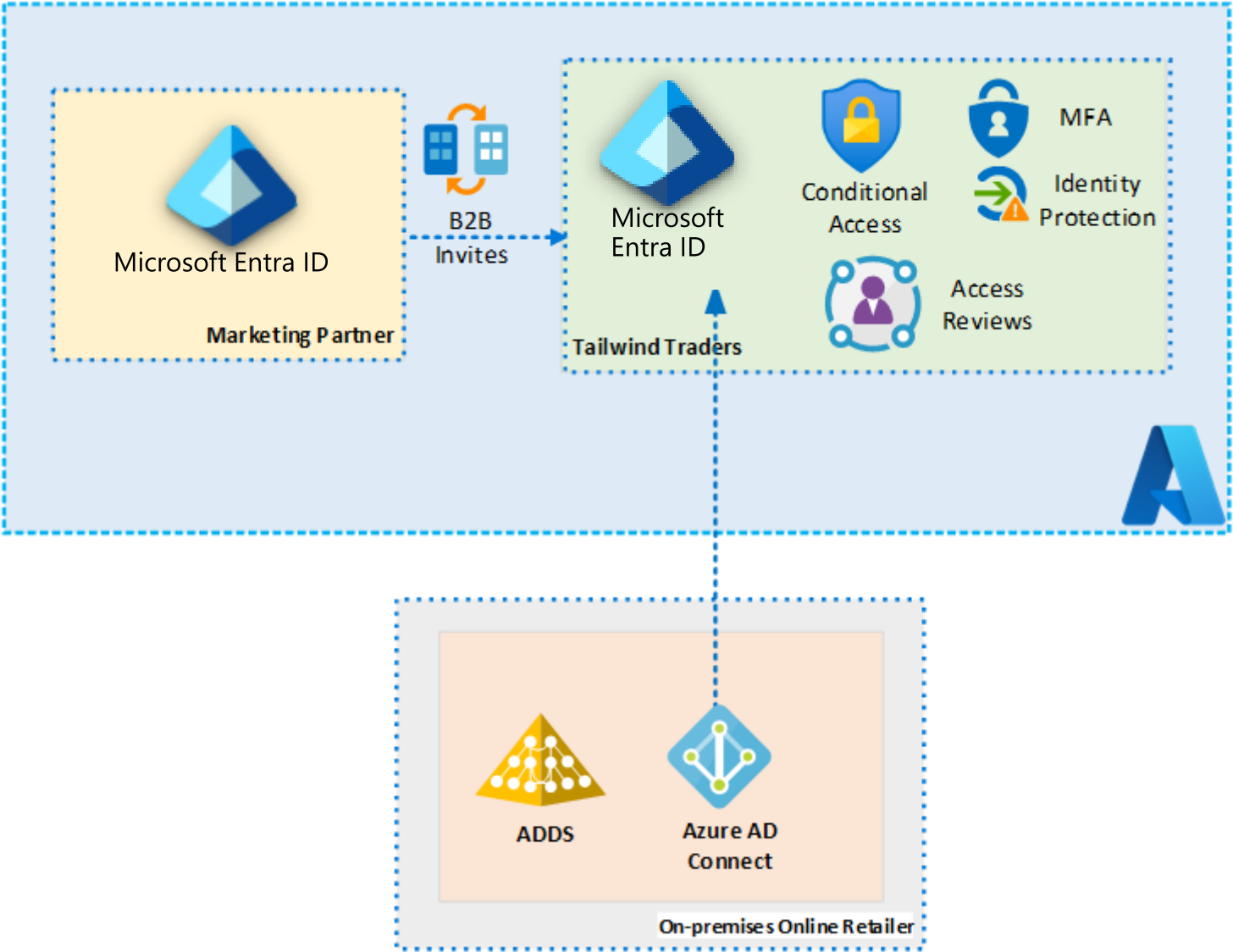


MFA

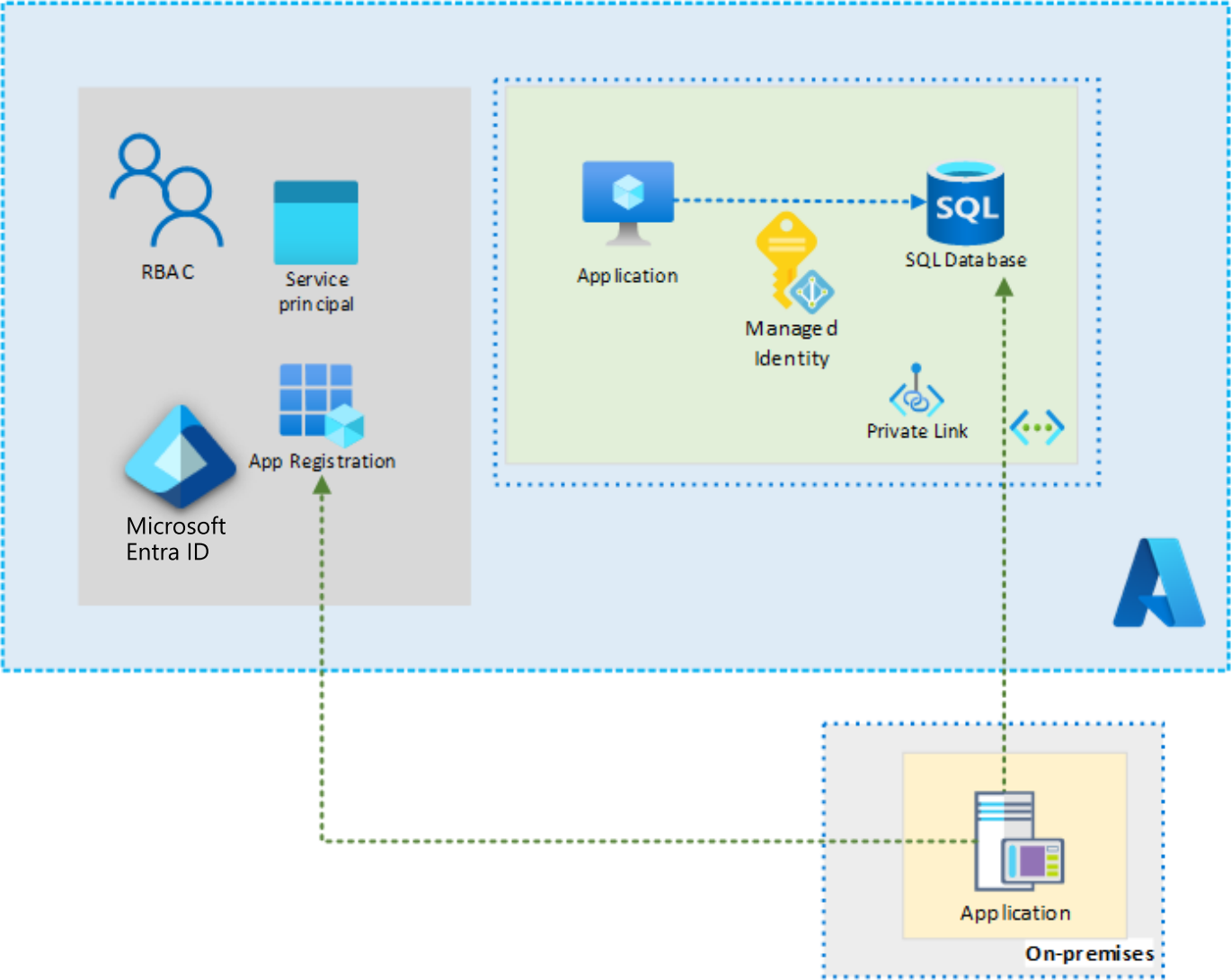


Microsoft  
Entra ID

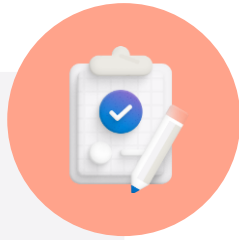
# Instructor – New Employee Accounts (completed)



# Instructor – New Identity Solution Features



# Learning recap – authentication and authorization solutions



Check your  
knowledge  
questions and  
review

- [Enable secure external collaboration for your applications with Azure AD B2B](#)
- [Enable secure external access to apps for external users with Azure AD B2C](#)
- [Configure and manage secrets in Azure key vault](#)
- [Manage secrets in your server apps with Azure key vault](#)
- [Authenticate apps to Azure services by using service principals and managed identities for Azure resources](#)

# End of presentation

