

AZ-305

Tag 3

# Design Microsoft Azure Infrastructure Solutions

Guten Morgen!

# AZ-305 Agenda

12<sup>30</sup> - 13<sup>30</sup>

Module 01 Design a governance solution ✓

Module 02 Design a compute solution ✓

Module 03 Design a non-relational data storage solution

Module 04 Design a data storage solution for relational data

Module 05 Design a data integration solution

Module 06 Design an application architecture solution

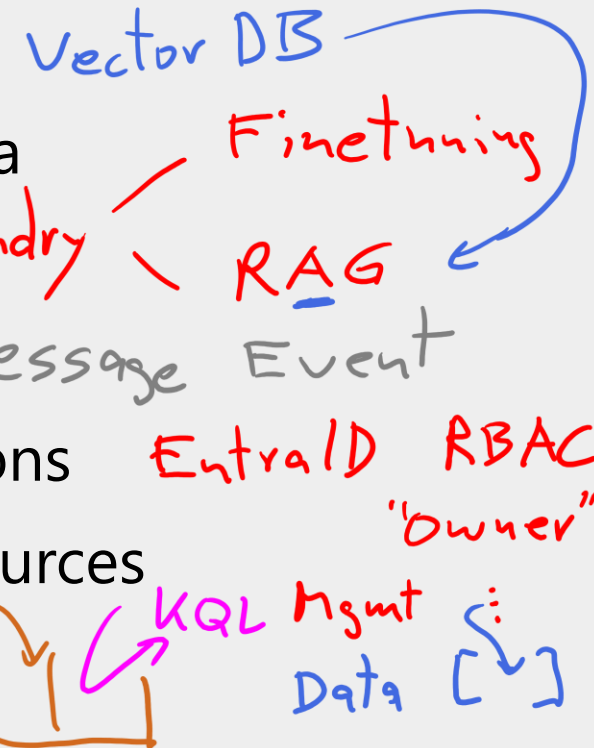
Module 07 Design Authentication and Authorization Solutions

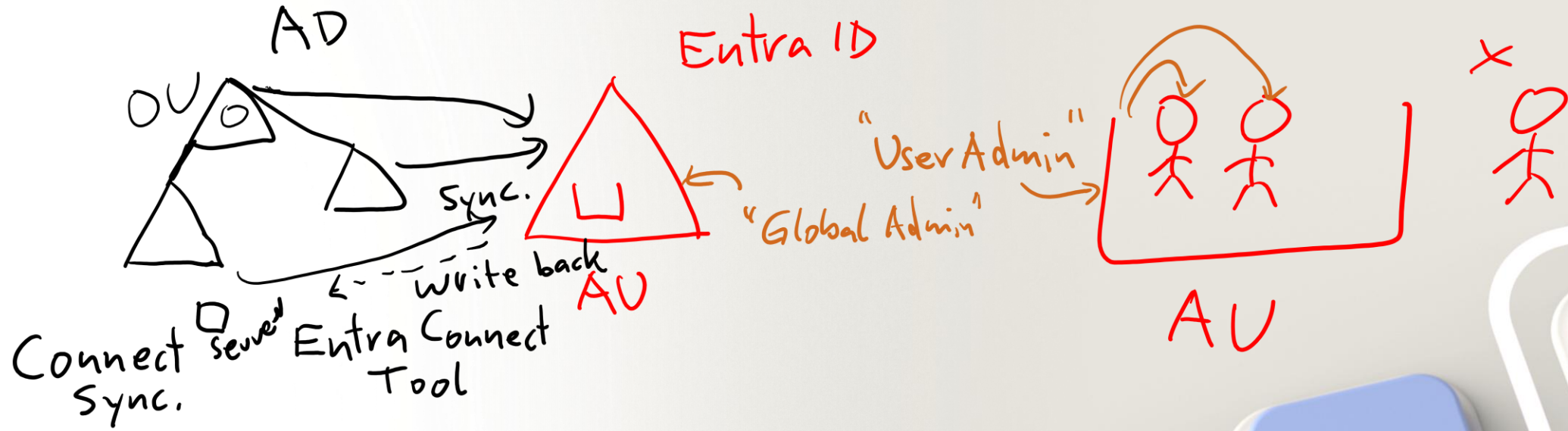
Module 08 Design a solution to log and monitor Azure resources

Module 09 Design a network infrastructure solution

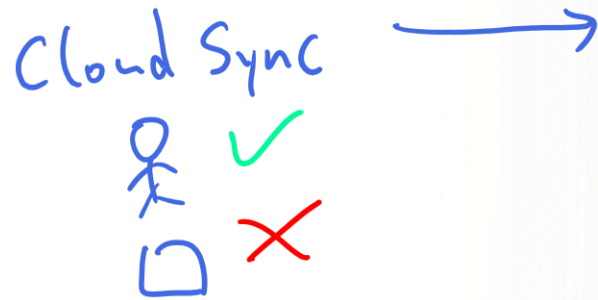
Module 10 Design a business continuity solution

Module 11 Design a migration solution





# 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 Microsoft Entra External ID
- Design for conditional access
- Design for identity protection
- 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

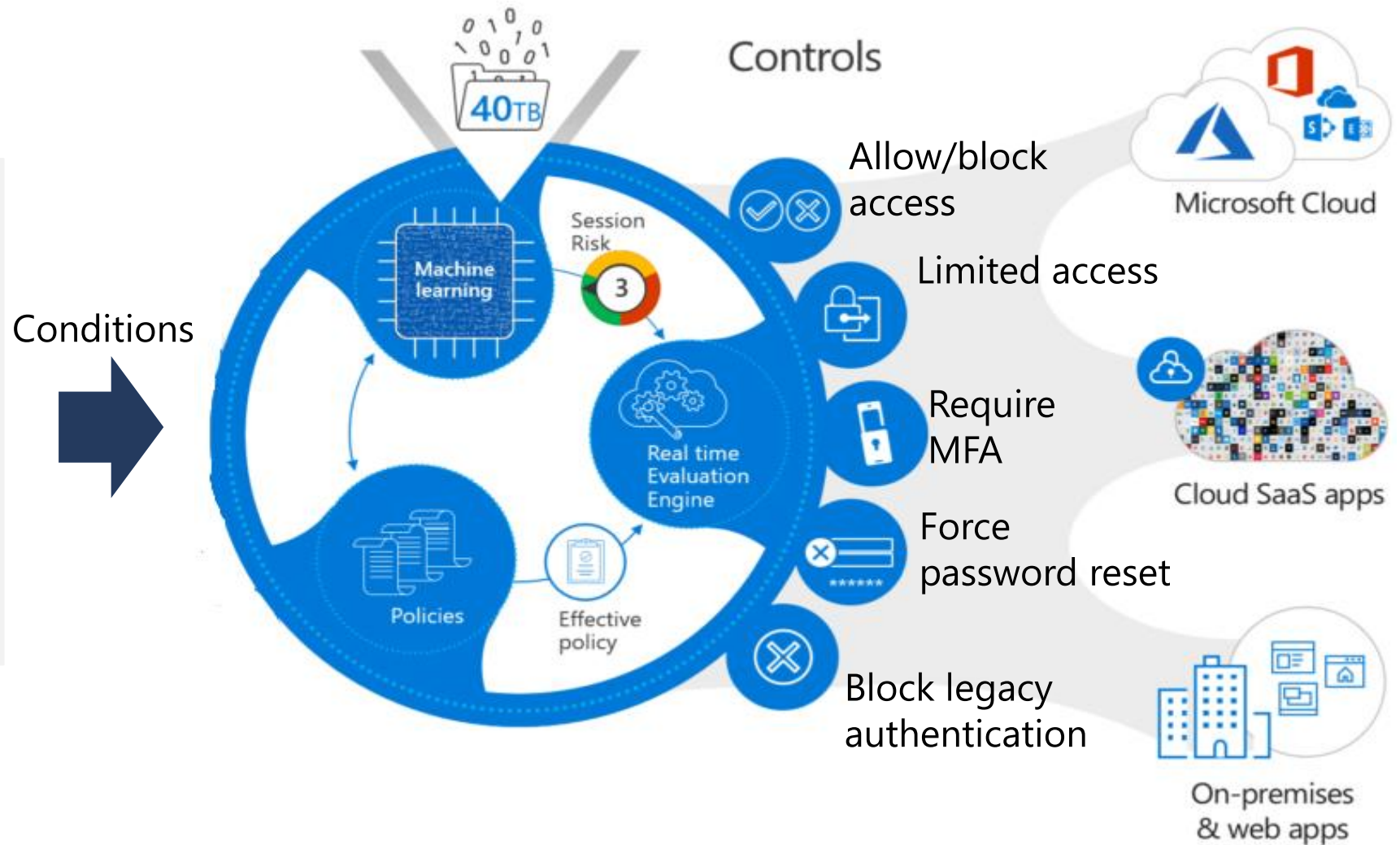




# Follow the Zero Trust model guidelines

Never trust, always verify.

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



# What is identity and access management



Identity

- Unified identity management
- Seamless user experience



- Allowed by role-based access control
- Verified by conditional access
- Monitored by Microsoft Entra ID Protection
- Confirmed by Microsoft Entra ID access reviews



Resources

If you need this	Use this
Provide identity and access management for employees in a cloud or hybrid environment.	Microsoft Entra ID
Collaborate with guest users 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.	Microsoft Entra External ID

# Design for Microsoft Entra ID



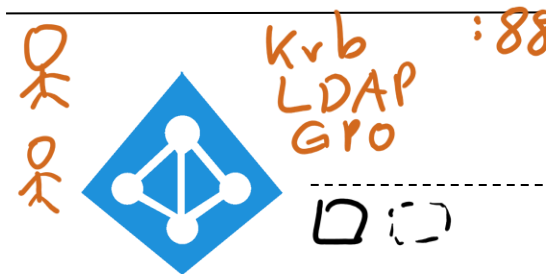


# When to use Microsoft Entra ID

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 Sync, or Microsoft Entra Cloud Sync for hybrid identity synchronization

On-premises Identities



Active Directory Domain Services

AD

Azure Identities

Microsoft Entra Connect



Microsoft Entra ID

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

Auth  
? Intune

Wer kann authentif?

	AD	Entra ID
PHS	✓	✓
WS-Fed	✓	✗
PTA	✓	✗

Krb  
NTLM2 Hash  
RC4

PHS  
WS-Fed

RC4

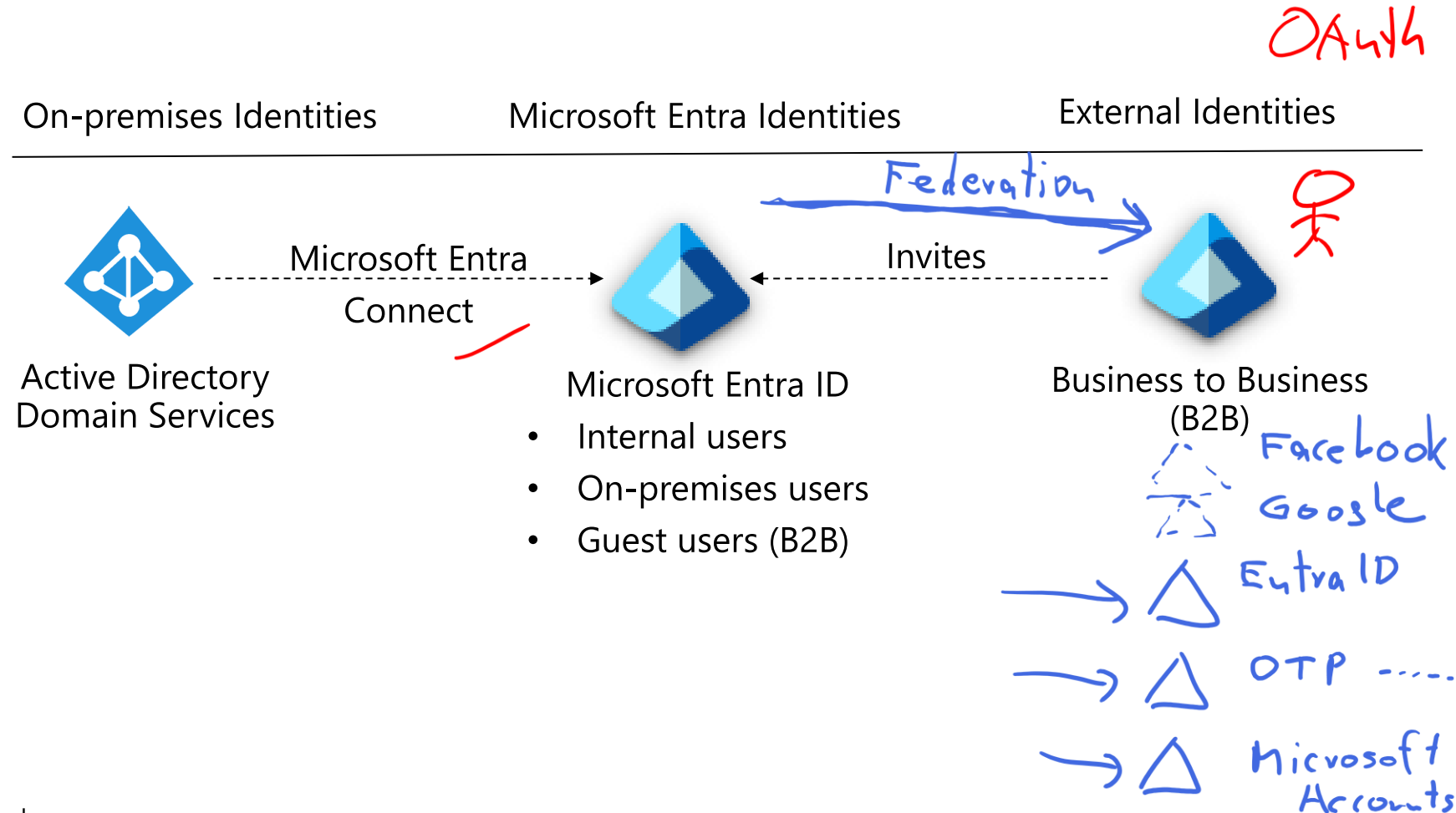
# Design for Microsoft Entra Business to Business



# 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 Microsoft Entra External ID



# When to use Microsoft Entra External ID

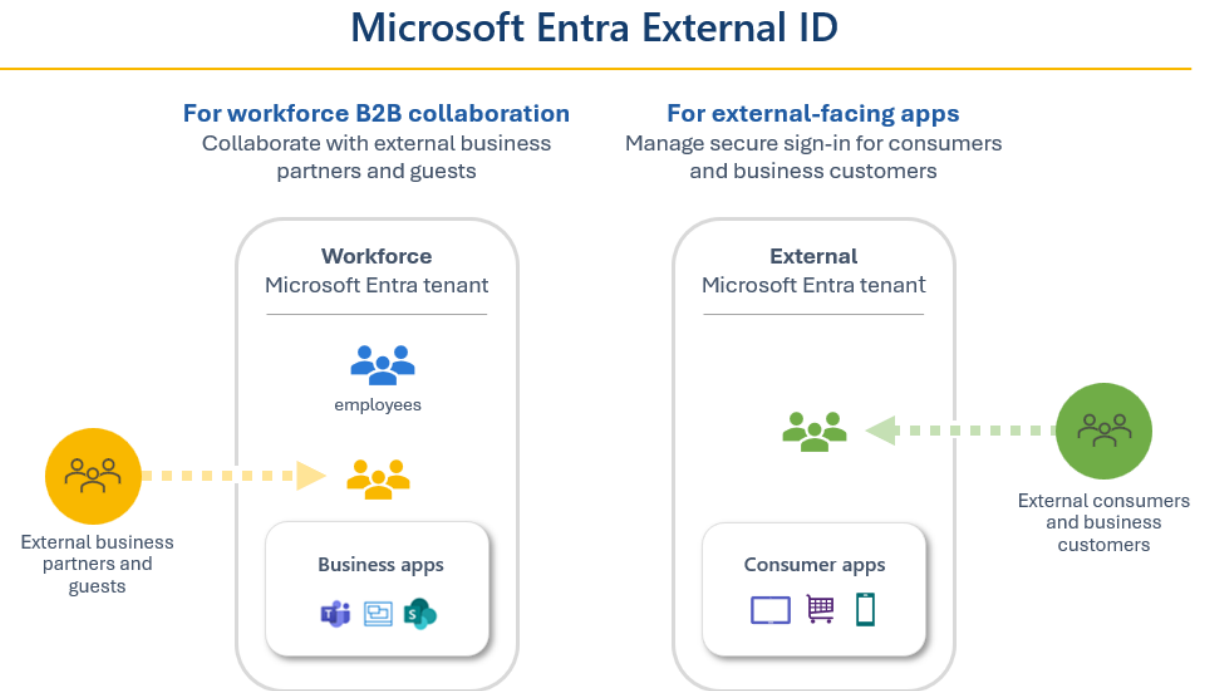
## Solutions for working with people outside of your organization

- **Workforce tenant collaboration**

- Business partners and other external users
- Guests can securely access your business applications through invitations or self-service sign-up

- **External tenant collaboration**

- External ID secures your applications
- Consumers and business customers can securely access your business applications through invitations or self-service sign-up





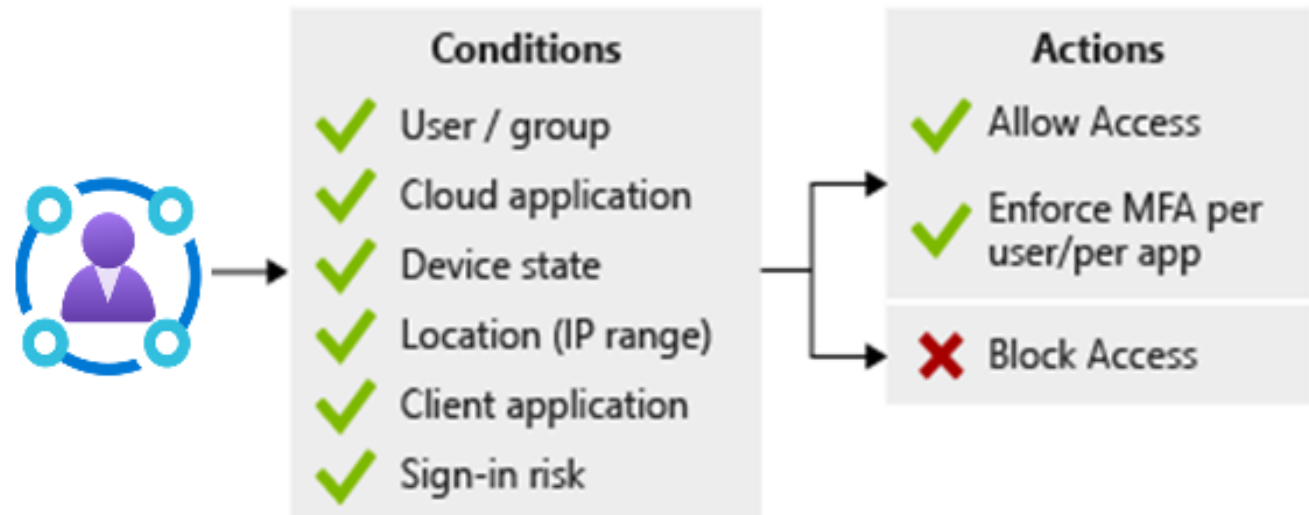
# Design for conditional access



# 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 areas 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



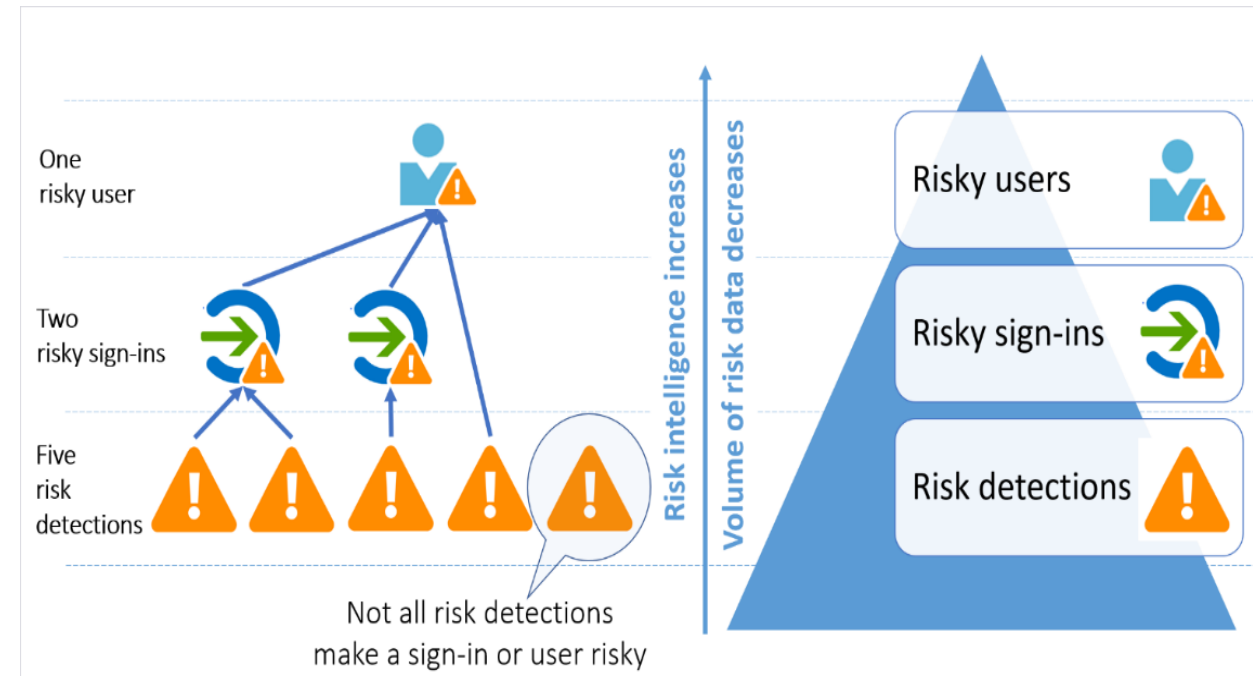
# Design for identity protection



# When to use identity protection

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



# 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

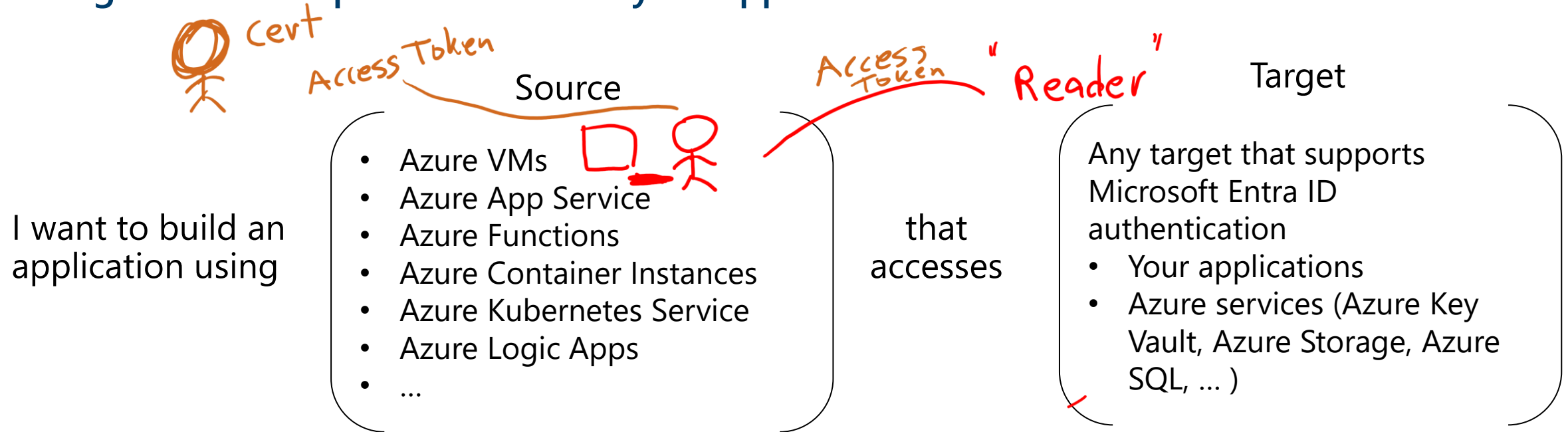


# Design service principals for applications



# 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

1:1

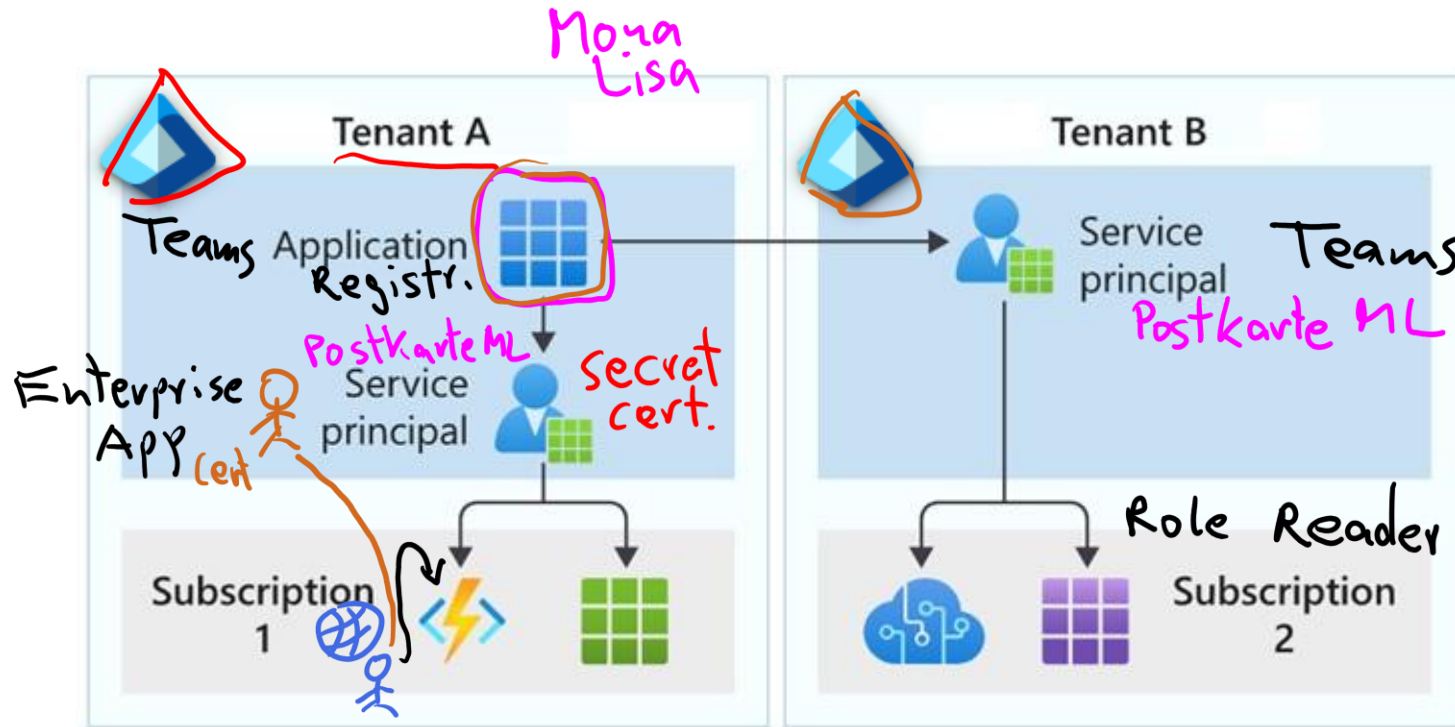


1 : N

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.



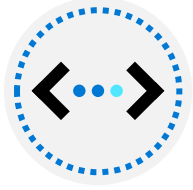
When registering an application in Microsoft Entra ID, consider business and security needs of admin consent versus user consent

---



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.

---

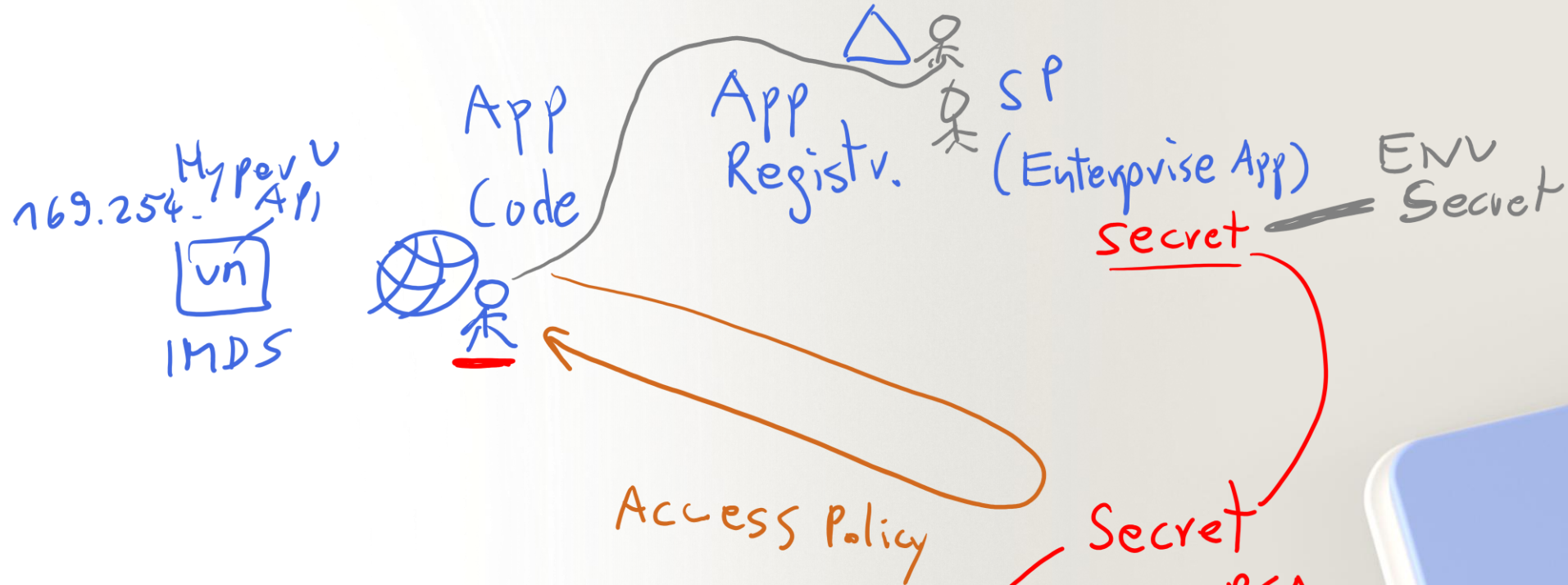


In addition, when requesting permissions for app functionality, you should request the least-privileged access.

---



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



# Design for Azure key vault

Secret  
Key RSA  
EC  
Cert

entangled

# 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?

- Separate of sensitive app information
- Restricted secret access with access policies
- Centralized secret, key, and certificate storage
- Access logging and monitoring
- Implement customer managed keys

## When to consider multiple Key Vaults:

- RBAC vs Policies
- Performance



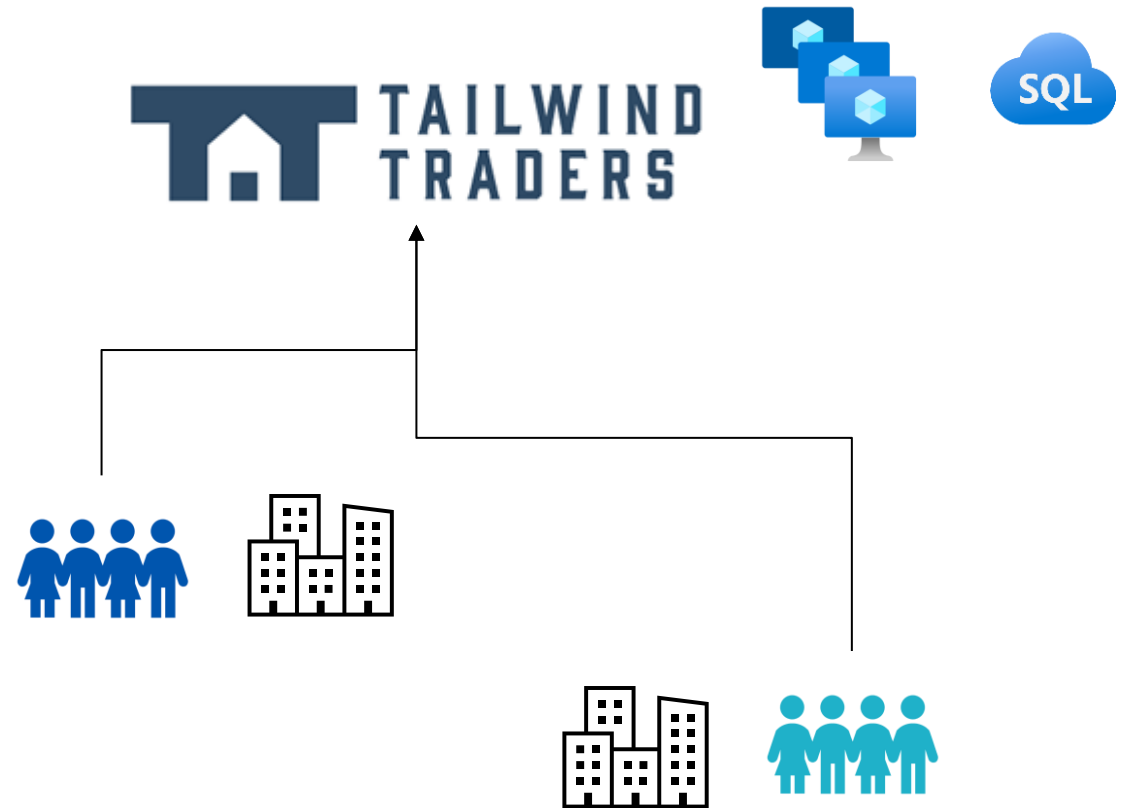
Secrets  
Keys  
Certificates

# Case study and review



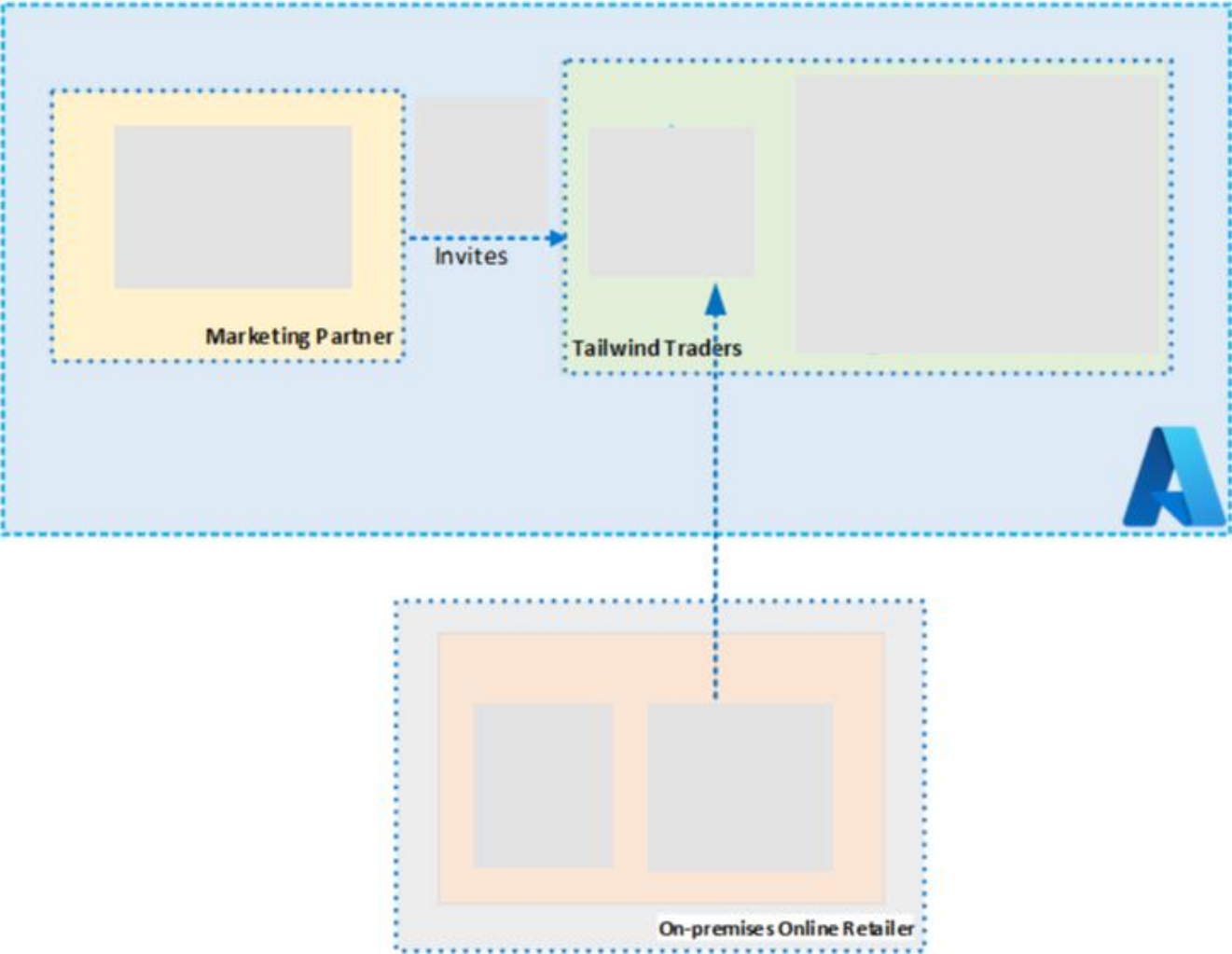
# Case Study – Authentication and authorization

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

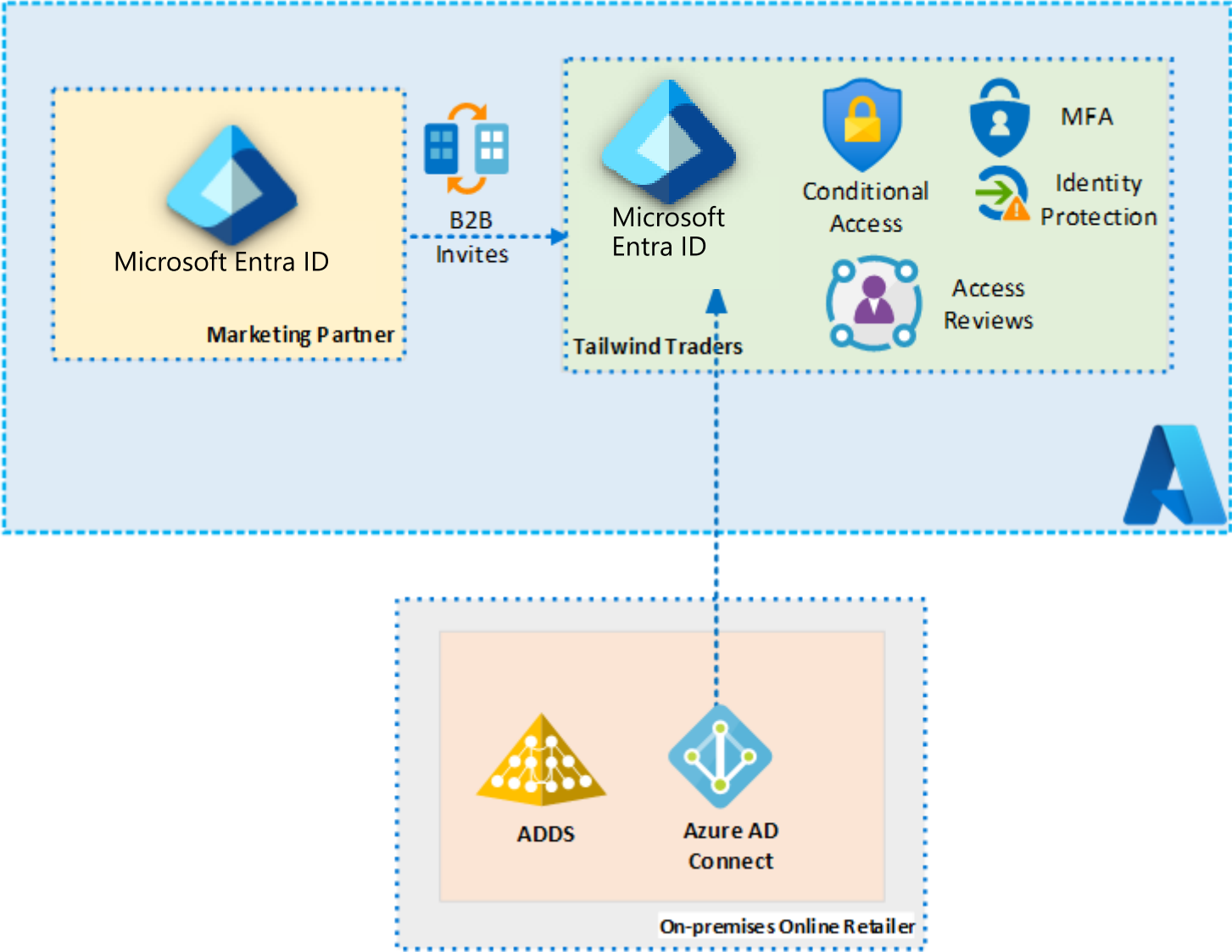


MFA

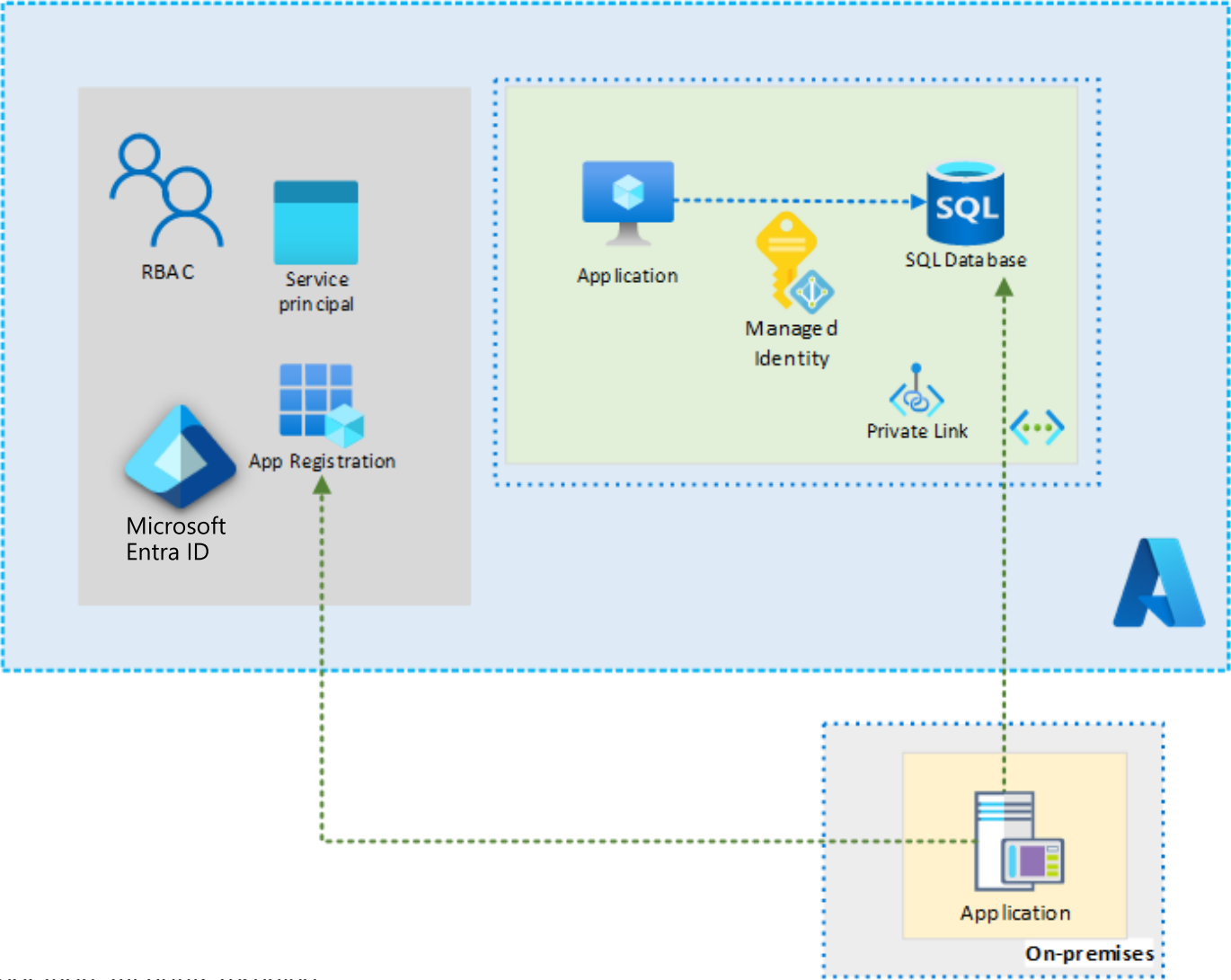


Microsoft  
Entra ID

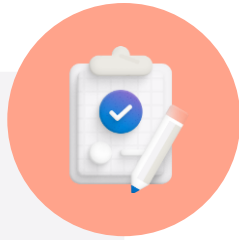
# Instructor – New Employee Accounts (completed)



# Instructor – New Identity Solution Features



# Learning Recap – Authentication and authorization solutions



Check your  
knowledge  
questions and  
review

## Reference modules

- [Understand Microsoft Entra ID](#)
- [Plan, implement, and administer conditional access](#)
- [Design, develop, and manage access reviews](#)
- [Configure and manage secrets in Azure key vault](#)
- [Manage secrets in your server apps with Azure key vault](#)

# End of presentation

