Identity and Access Management Solutions for Microsoft 365

Vlad Catrinescu

Microsoft MVP

@vladcatrinescu https://VladTalksTech.com

Overview

Identity concepts

- Authentication and Authorization
- Modern Authentication

Introduction to Microsoft Active Directory

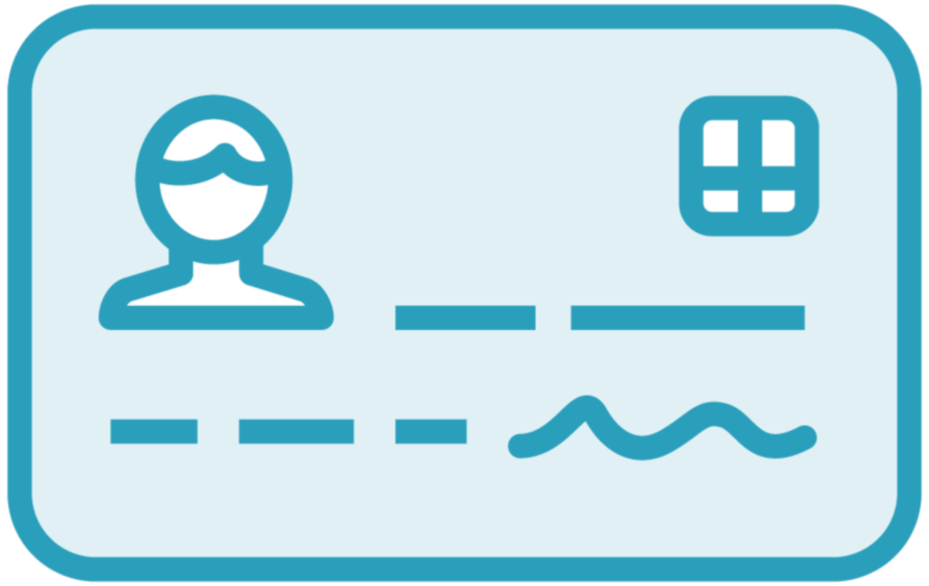
- And Azure Active Directory!
- Hybrid identities

Azure Active Directory authentication methods

Conditional Access

Identity Concepts

Authentication and Authorization



Authentication and authorization are very different processes

Authentication is validating that users are whom they claim to be

Authorization is the process of giving the user permissions for a specific resource

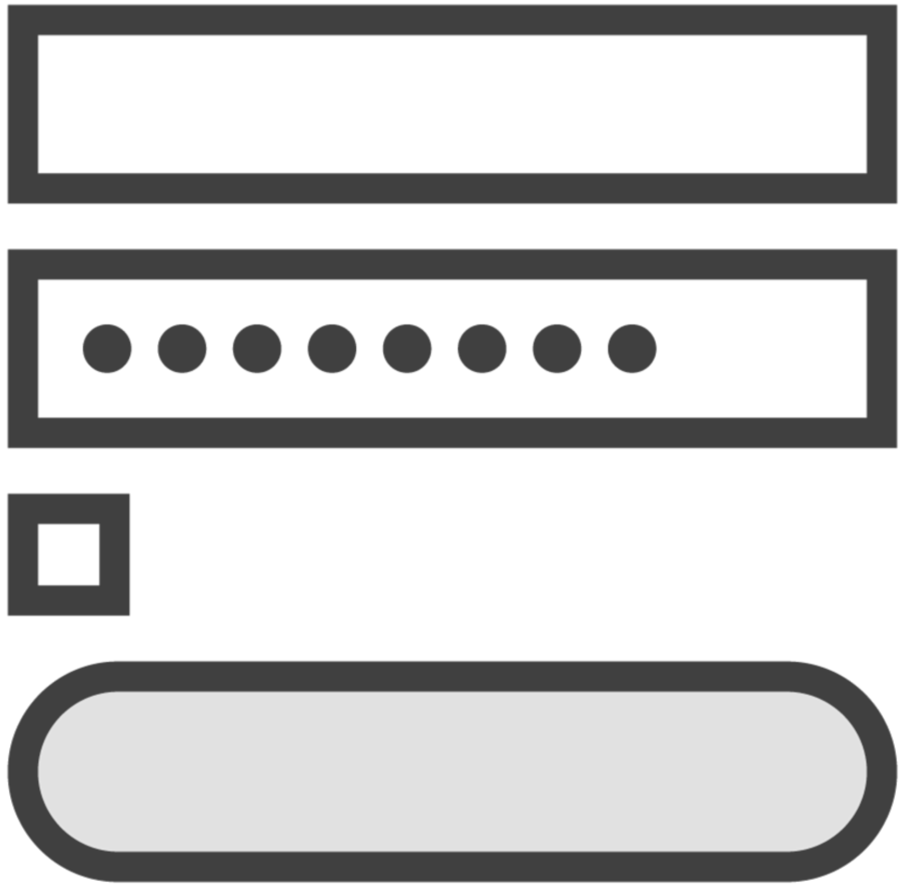
Authentication

Traditionally done by username and password

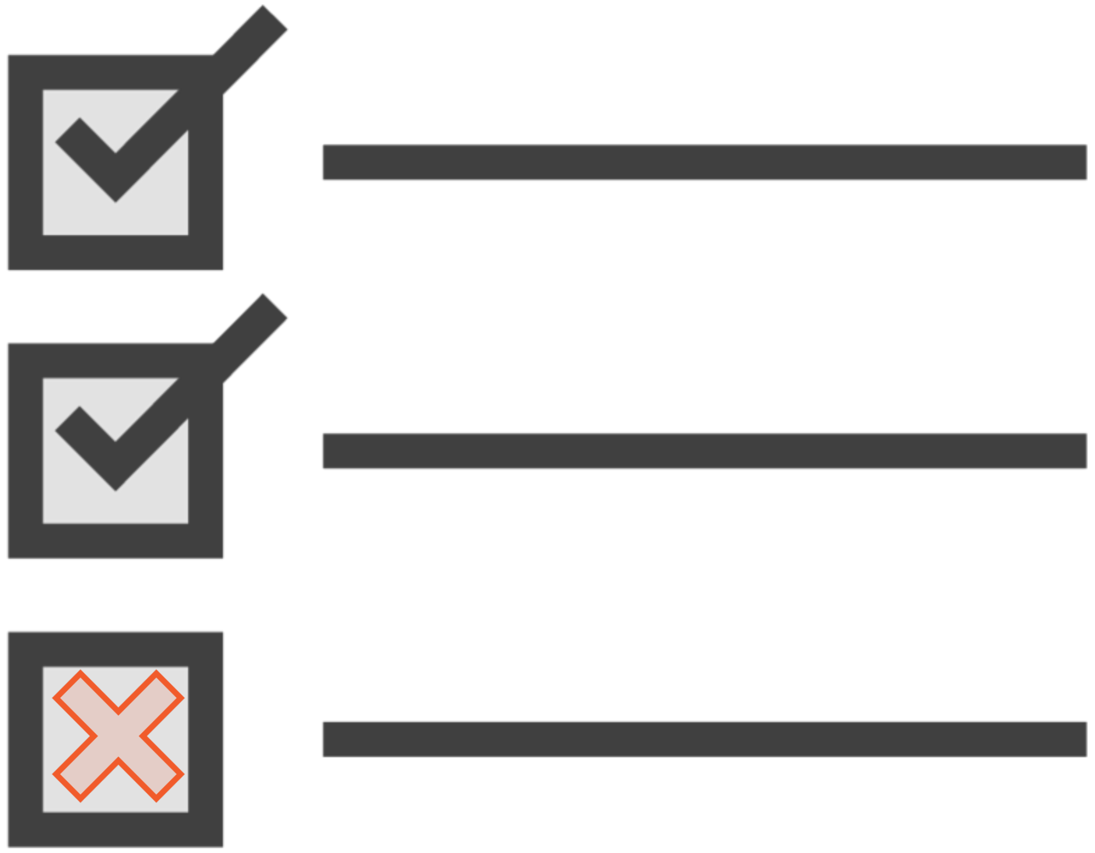
- Single Factor Authentication

Authentication confirms you are who you say you are

Authentication is always done before authorization



Authorization



Determines what permissions you have

Authentication and Authorization

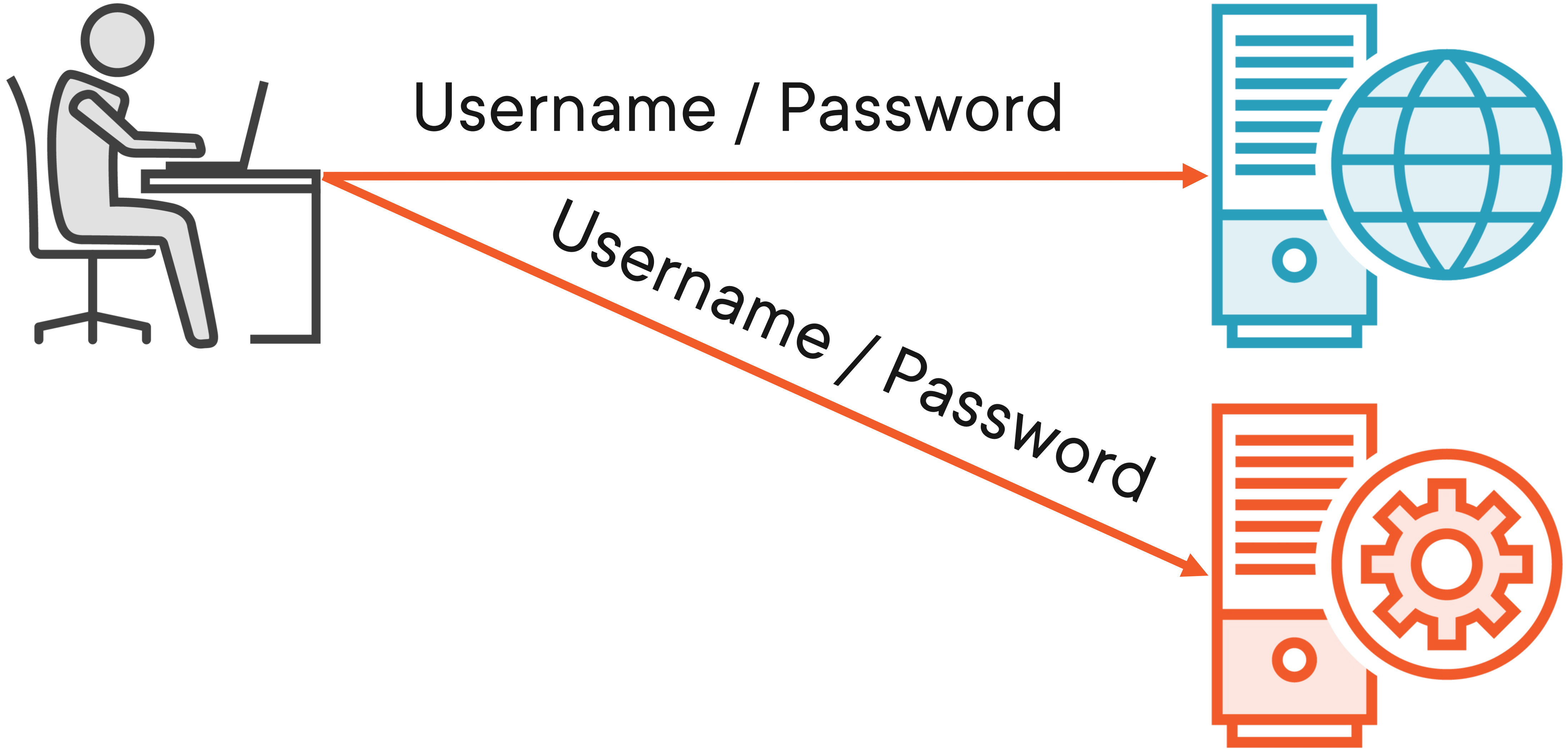
Authentication
Confirms users are who they say they are

Authorization
Checks if users are allowed to access a resource

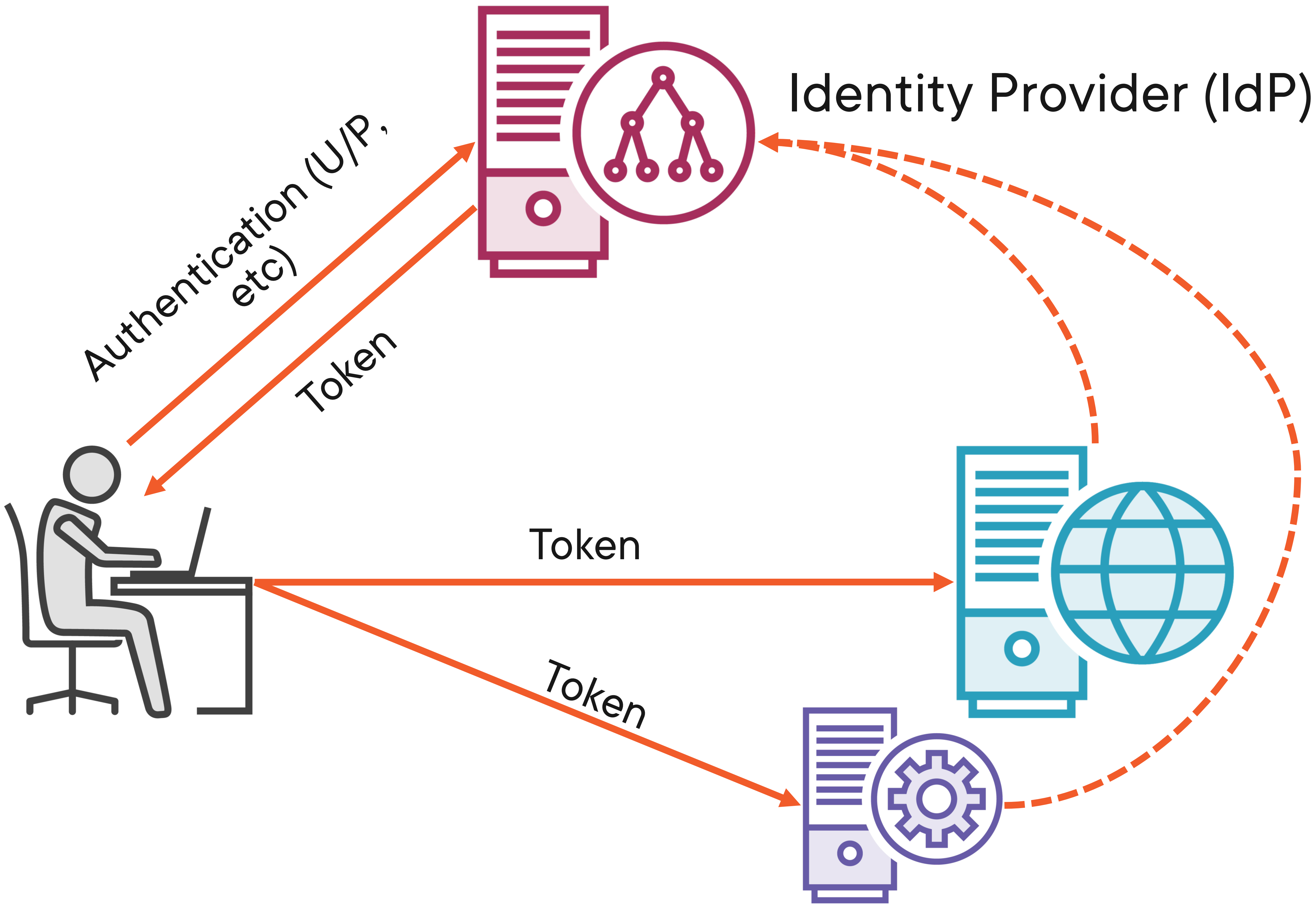
Modern Authentication

Modern Authentication is a Microsoft umbrella term for authentication & authorization methods between client and server

Before Modern Authentication



Modern Authentication



The Identity Provider

The Identity Provider is at the center of modern authentication

An Identity Provider offers authentication, authorization, and auditing services

A modern Identity Provider offers Single Sign On (SSO)

Introduction to Microsoft Active Directory

Introduction to Directory Services

Customizable information store

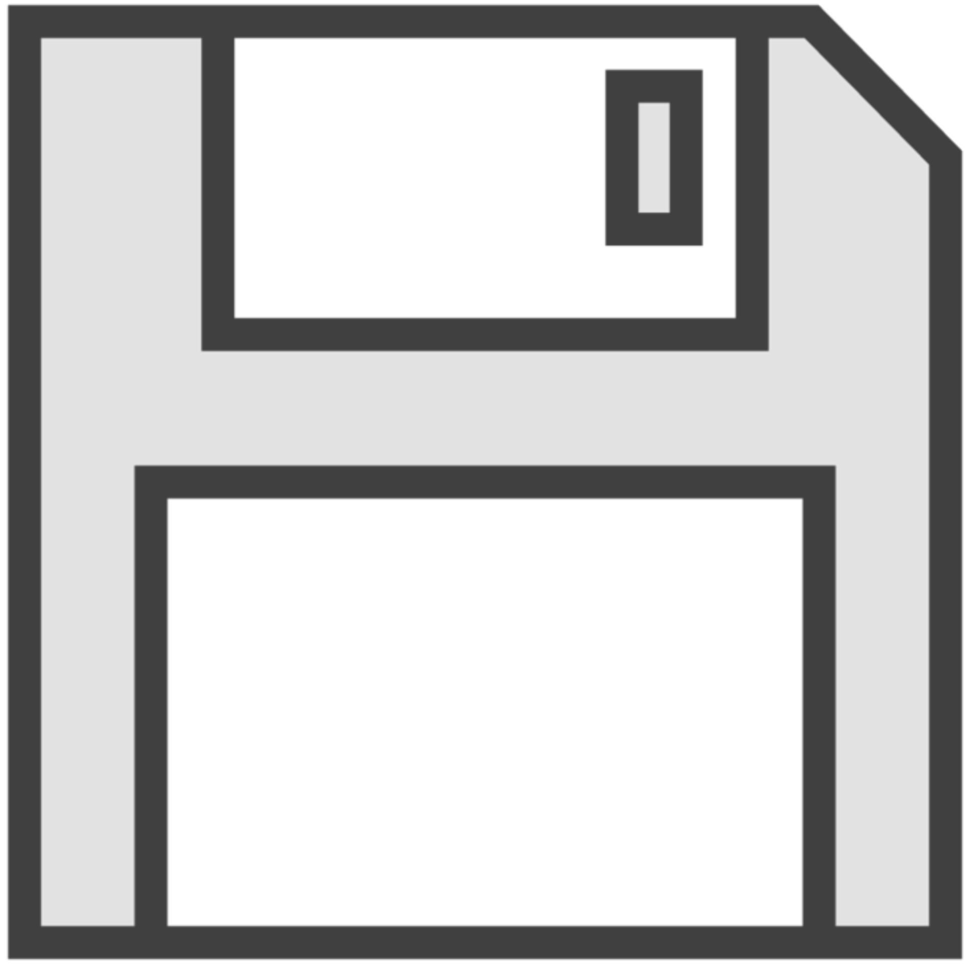
Functions as a single point where users can locate resources across the network

- Users & Groups
- Devices
- Printers
- & more

Single point for administrators to manage all those objects

Active Directory Domain Services (AD DS)

- AD DS Introduced by Microsoft with Windows 2000
  - For On-Premises Networks
- Central component in organizations with on-premises IT Infrastructure
- Azure Active Directory is the next evolution of Microsoft identity solutions
  - Cloud based



Azure Active Directory (Azure AD)

Microsoft’s cloud-based identity and access management service

- Part of the Microsoft Entra suite of services

Provide a single identity system for cloud and on-premises applications

- Internal and external users

Each Microsoft cloud subscription uses Azure AD

- Microsoft 365 / Office 365
- Azure
- Dynamics 365

Azure AD Identities

Users

Groups

Service Principals (Applications)

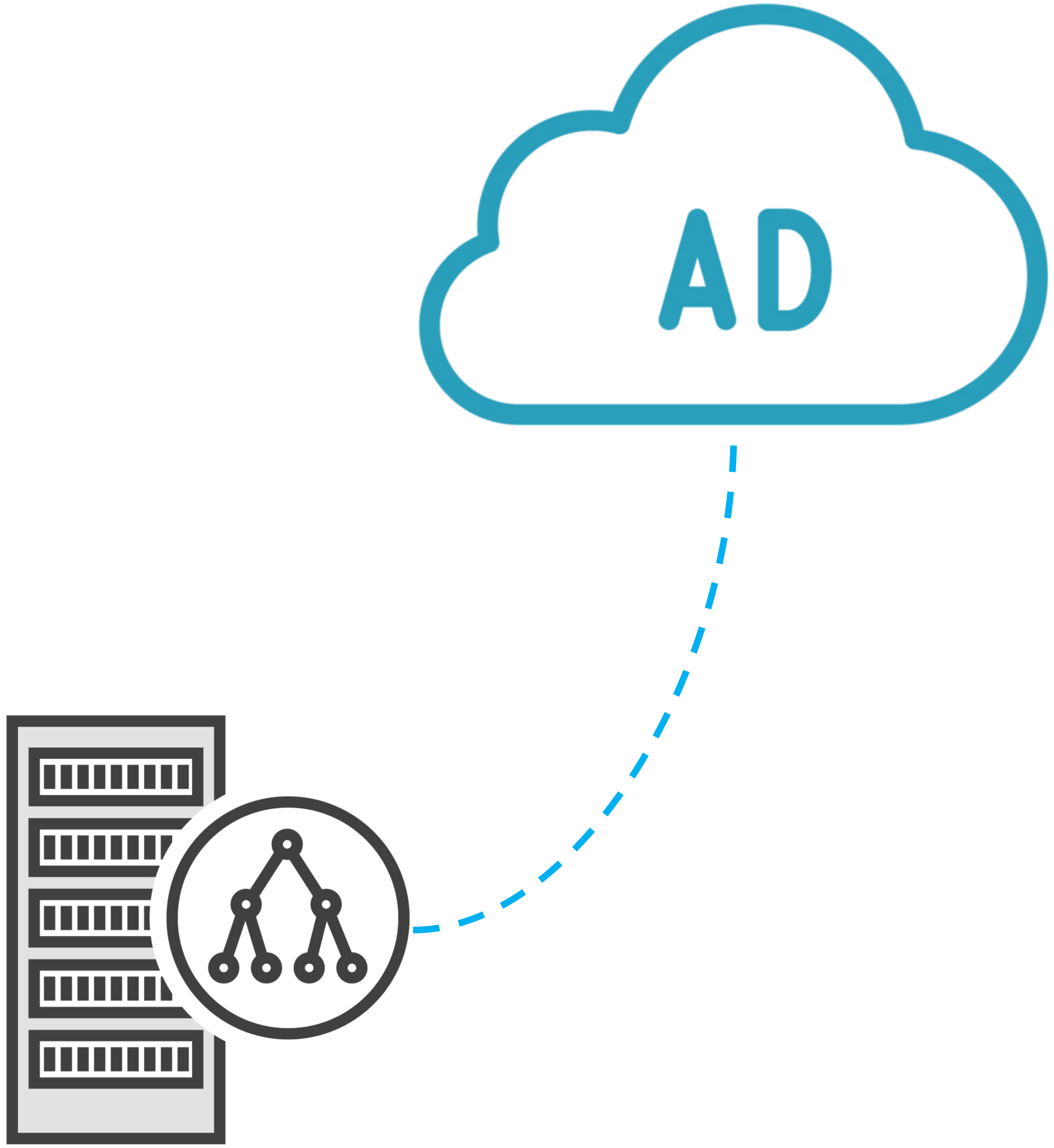
Managed Identities

Devices

A Note on Licensing

- Azure AD has multiple licensing tiers / editions
- Some features we will talk about require premium licensing
- Licensing always changes
  - Make sure to always check the latest information
    - https://azure.microsoft.com/en-ca/pricing/details/active-directory/

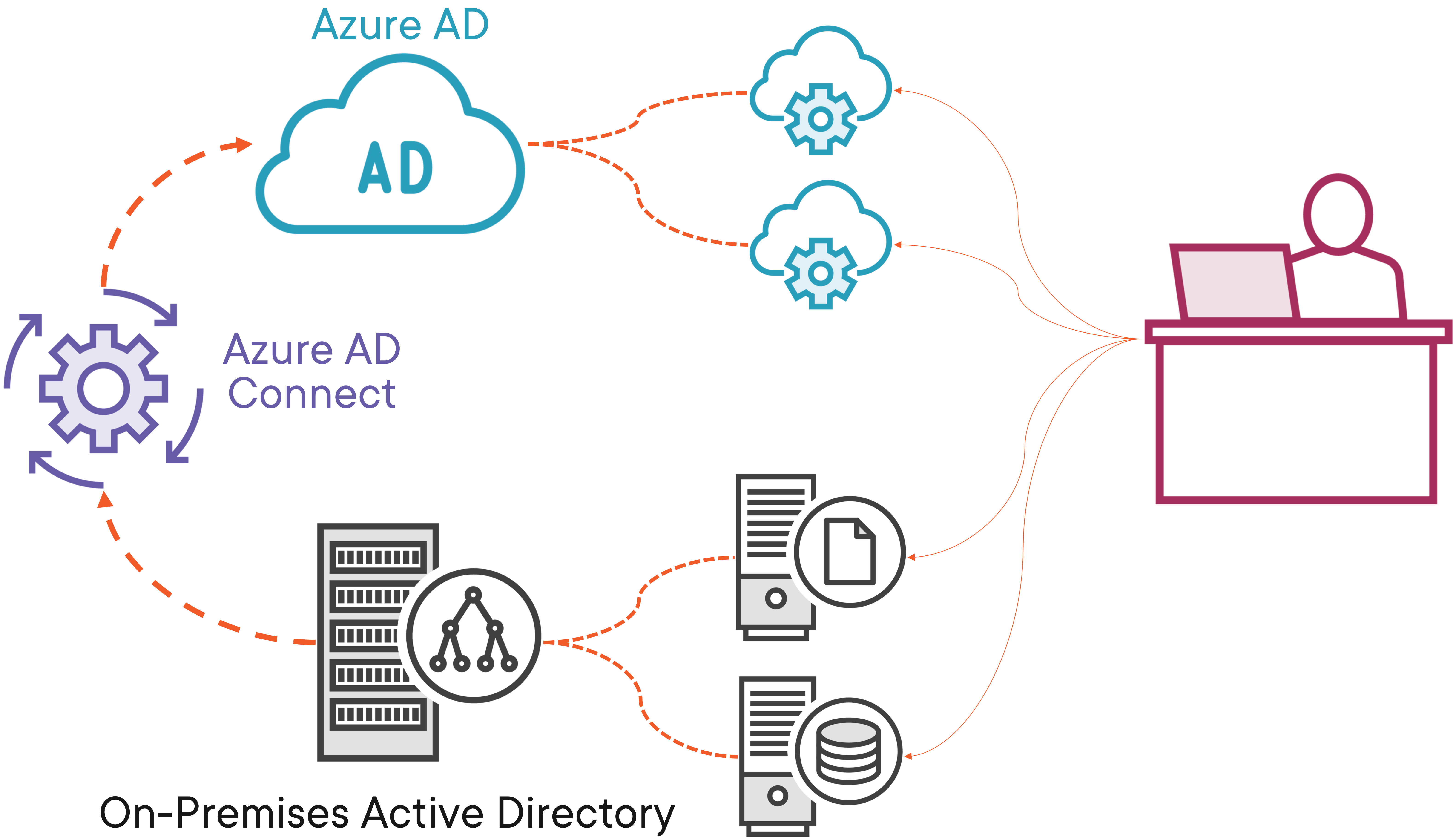
Hybrid Identities



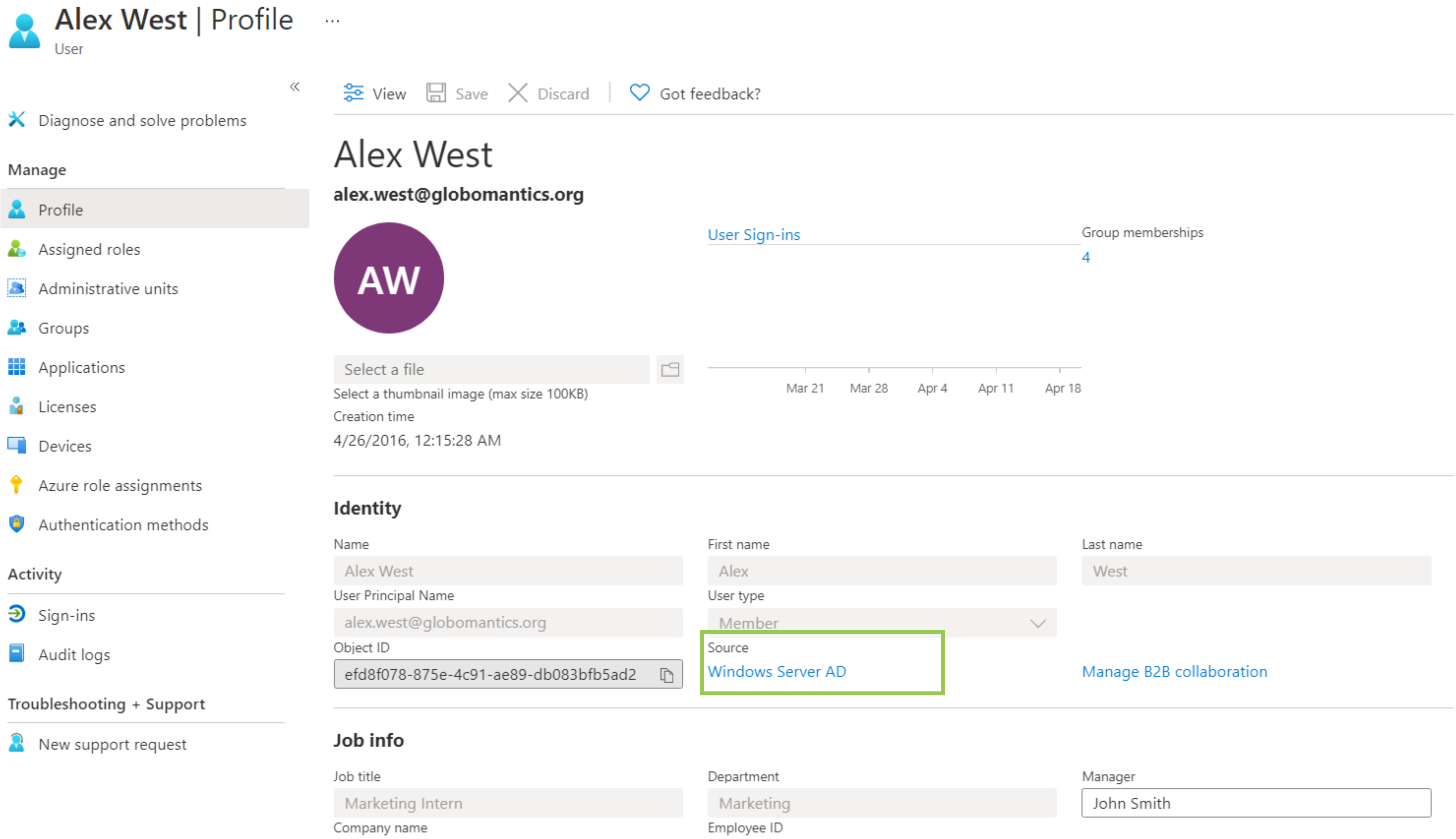
Most enterprises started with an on-premises infrastructure

- And used Active Directory Domain Services
- Most enterprises still have an on-premises infrastructure
  - File Shares
  - Collaboration (Ex: SharePoint Server)
  - Line of Business Applications

Hybrid Identities – High Level



Hybrid Identity User



Alex West

alex.west@globomantics.org

Group memberships
4

Select a thumbnail image (max size 100KB)

Creation time
4/26/2016, 12:15:28 AM

Identity

Name: Alex West

First name: Alex

Last name: West

User Principal Name: alex.west@globomantics.org

User type: Member

Object ID: efd8f078-875e-4c91-ae89-db083bfb5ad2

Source: Windows Server AD

Job info

Job title: Marketing Intern

Department: Marketing

Manager: John Smith

Company name

Employee ID

Terminology

Accounts that only exist in Azure AD

Cloud-Only

Cloud-Sourced

Cloud-Mastered

Accounts that are synced from On-Prem

Directory synchronized user

Azure AD Authentication Methods

Authentication

Authentication is the process of verifying an identity to be legitimate

Traditionally we have used passwords

- Passwords are not perfect
  - Users re-use passwords across services
  - Good passwords are difficult to remember
    - Decreasing productivity

Some Statistics around Passwords

80%

Of data breaches in 2019 were caused by password compromise
https://enterprise.verizon.com/resources/reports/dbir/

65%

Of people reuse passwords across multiple sites
https://services.google.com/fh/files/blogs/google_security_infographic.pdf

13%

Of people use the same password for all passworded accounts and devices
https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Multi-Factor Authentication (MFA)

MFA requires more than one form of verification

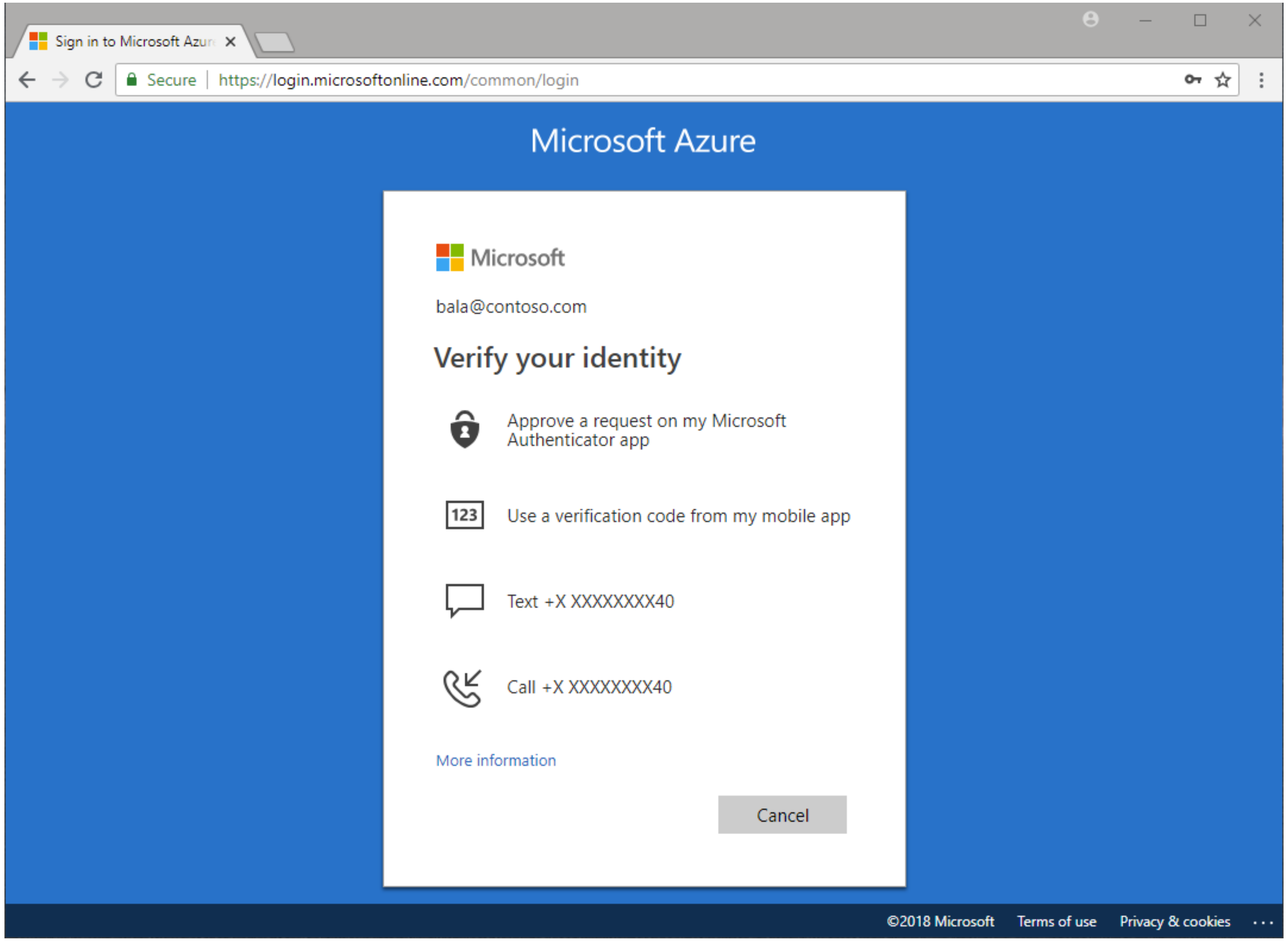
- Something you know (Ex: password)
- Something you have (phone, hardware key)
- Something you are (biometrics)

Microsoft studies show that enabling MFA can reduce the risk of identity compromise by as much as 99.9%*

This is always the first thing to enable in order to provide greater protection to user identities

https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

- Supported forms of additional verification
  - Microsoft authenticator app
  - OATH Hardware token
  - SMS
  - Voice Call
- Administrators can disable certain methods
- SMS / Voice Call are considered the least secure MFA methods
  - But still way better than no MFA!



Sign in to Microsoft Azur
Secure
https://login.microsoftonline.com/common/login

Microsoft Azure

Microsoft

bala@contoso.com

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

Text +X XXXXXXXX40

Call +X XXXXXXXX40

More information

Cancel

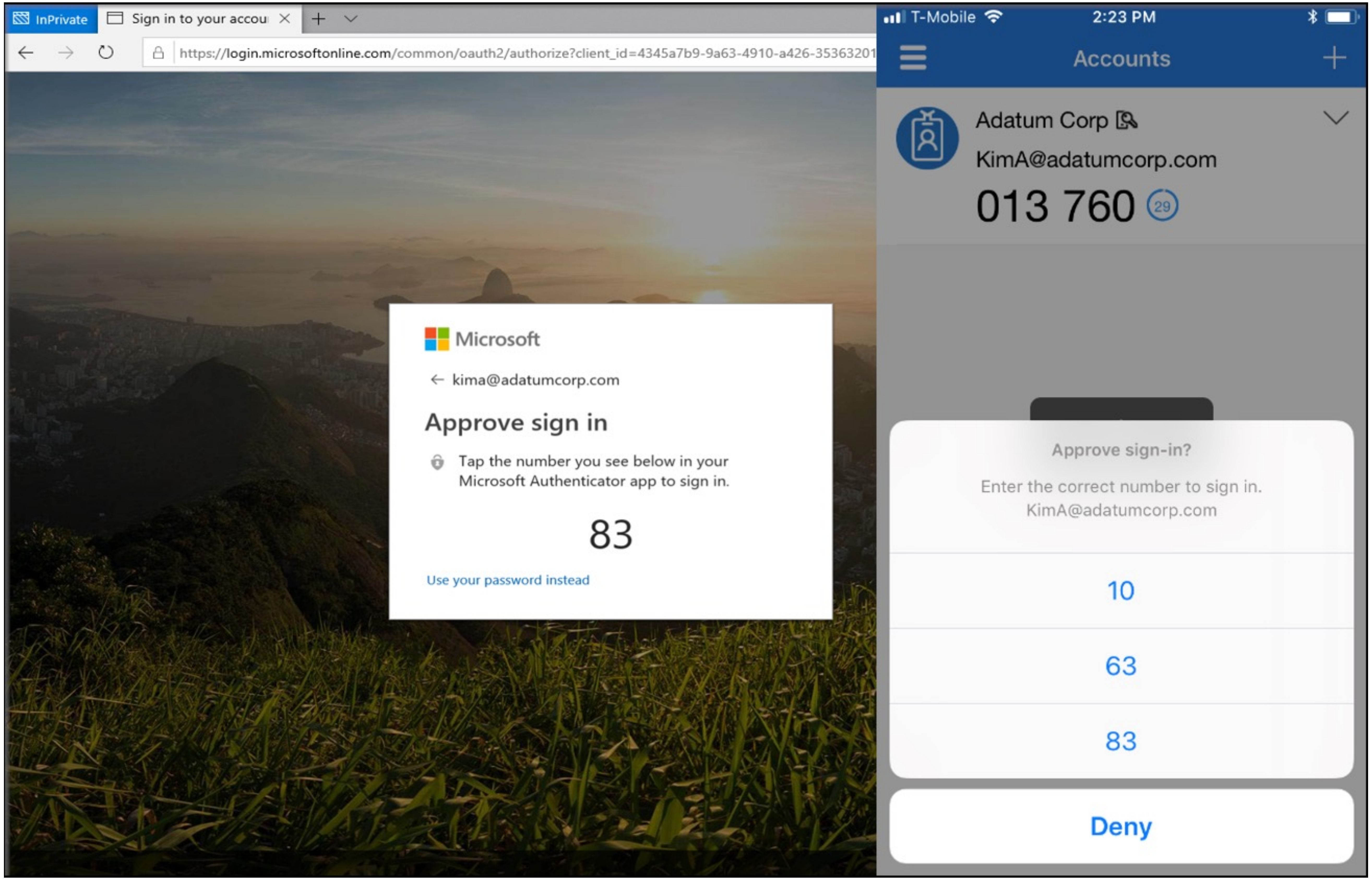
©2018 Microsoft Terms of use Privacy & cookies ...

Image Source
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Passwordless

- Based on something you are
  - Rather than something you know
- Passwordless options
  - Microsoft Authenticator Fingerprint Scan
  - FIDO2 Security Key
  - Windows Hello

Passwordless Prompt



InPrivate
Sign in to your accou
https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201
T-Mobile
2:23 PM
Accounts

Microsoft

kima@adatumcorp.com

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

83

Use your password instead

Adatum Corp

KimA@adatumcorp.com

013 760 29

Approve sign-in?

Enter the correct number to sign in.
KimA@adatumcorp.com

10

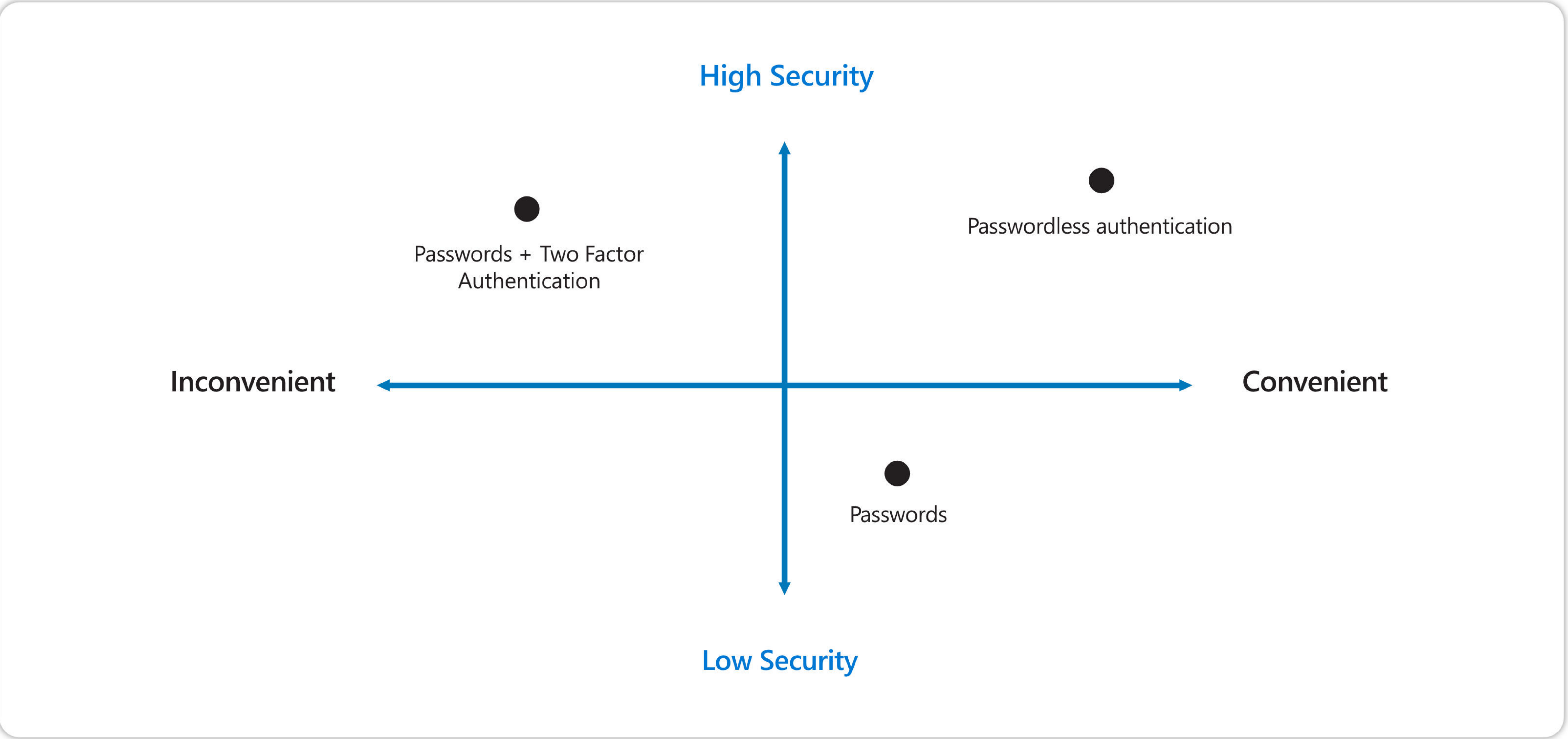
63

83

Deny

:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone

Passwordless as Positioned by Microsoft



High Security
Passwords + Two Factor Authentication
Passwordless authentication
Inconvenient
Convenient
Passwords
Low Security

https://www.microsoft.com/en-us/security/business/identity-access-management/passwordless-authentication

Demo

Multi Factor Authentication

Passwordless Authentication

Conditional Access

Azure AD Conditional Access

Additional layer of security between authentication and authorization

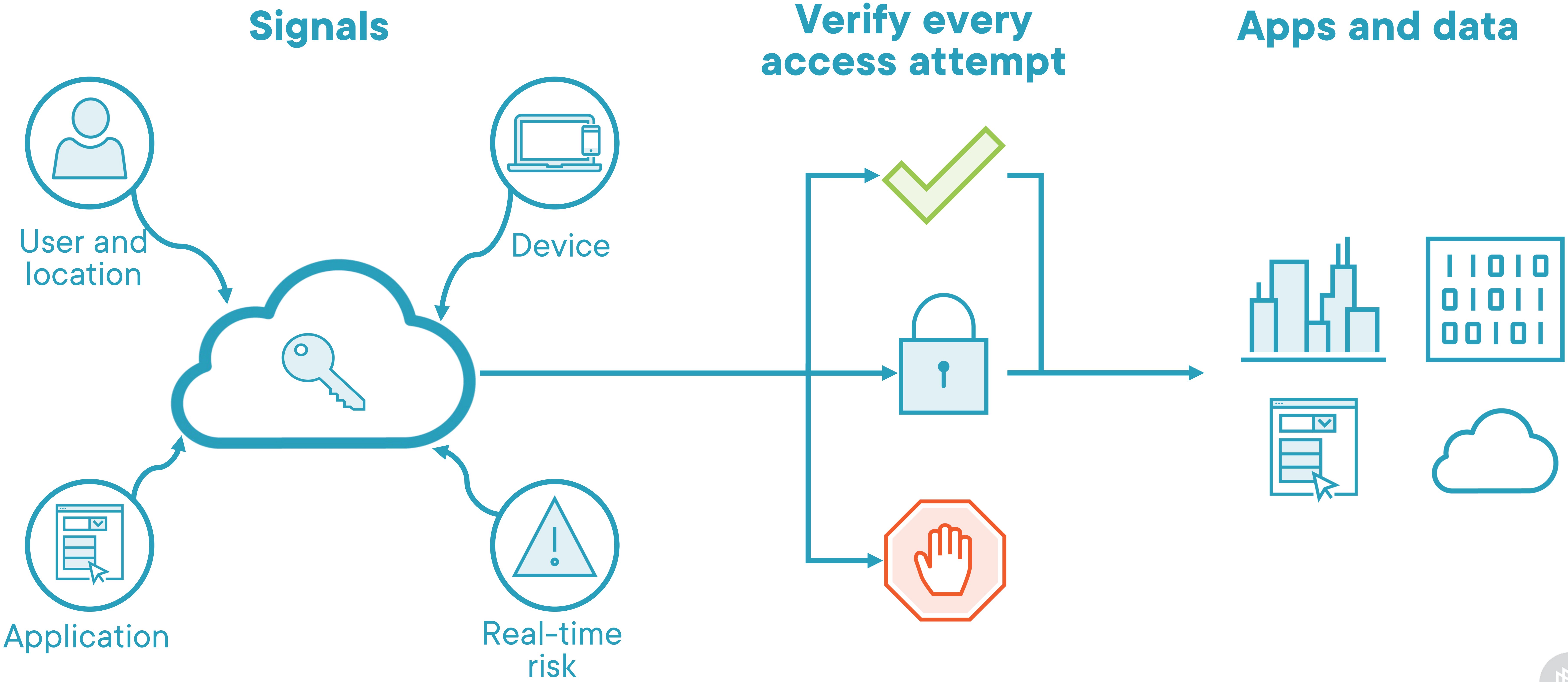
Conditional access policies evaluate every access attempt and decide if

- Grant access
- Block access
- Require one or more conditions to be met
  - Require MFA
  - Require device to be marked as compliant

Conditional access is implemented trough policies created by each organization

- Can be applied to users or applications

Azure AD Conditional Access



Signals

Verify every access attempt

Apps and data

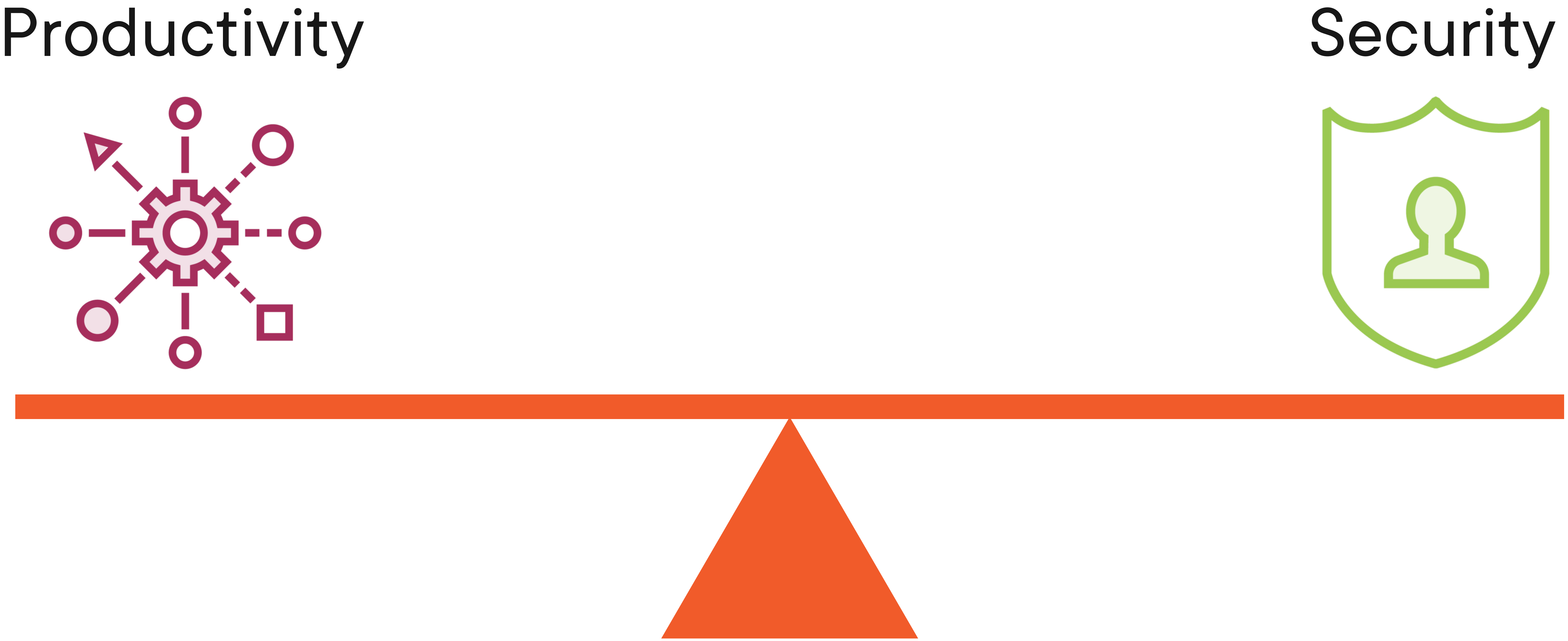
User and location

Device

Application

Real-time risk

Conditional Access Allows You to Find a Balance



Productivity

Security

Example Conditional Access Policies

If a user wants to access SharePoint Online from a trusted network after authenticating on a compliant device

- Grant Access

If a user wants to access a collaboration SharePoint site from an untrusted network

- Prompt MFA

Any user that logs in that has an administrative role

- Prompt MFA

Example Conditional Access Policies

A user authenticates at home on a mangled device and trusted network and browses the intranet

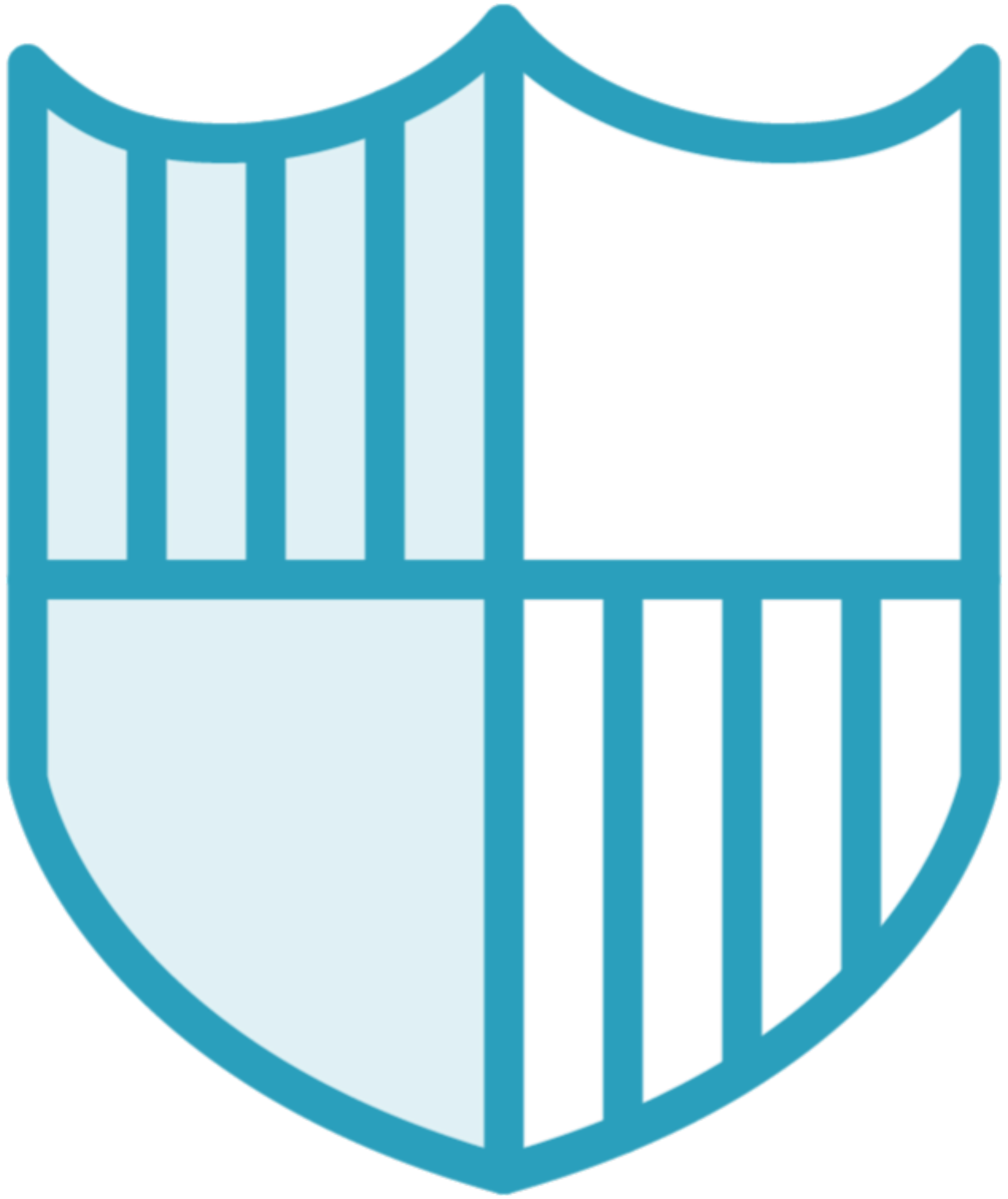
- Allowed

Same user tries to access the SharePoint site where employee files are stored

- Ask for MFA prompt

A user tries to access SharePoint Online from another country

- Block access



Demo

Azure Active Directory Conditional Access

Conclusion

Identity Concepts

- Authentication and Authorization
- Modern Authentication

Introduction to Microsoft Active Directory

- And Azure Active Directory!
- Hybrid identities

Azure AD authentication methods

- Multi Factor Authentication (MFA)
- Passwordless

Conditional Access

Up Next:
Threat Protection Solutions for Microsoft 365