



# Microsoft Academyadi

la partecipazione che ti premia





# Microsoft Academyadi

la partecipazione che ti premia

Solo per riprese social evento 😊

Wifi Network: Showroom - guest  
Password Wifi: microsoft2019





# Microsoft Academyadi

la partecipazione che ti premia

**MWP Academy - Day 1**

**Identity and Access Management:  
road to a password-less world**

Michele Sensalari

[michele@sensalari.com](mailto:michele@sensalari.com)



# Michele



- ❑ Senior Consultant – Speaker – Trainer (22 anni)
- ❑ Dipendente 50% su tecnologie Microsoft Dipartimento di Informatica – Università degli Studi di Milano
- ❑ Freelance 50/70%
- ❑ Mi occupo di: AD, SCCM, W10, Win Server, AzureAD, O365, M365, Azure, Enterprise Mobility & Security
- ❑ Speaker da 12 anni di WPC e da 5 responsabile agenda ITPRO e Security
- ❑ Certificato MCT, MCSE, MCSA, MCITP
- ❑ Contatti:
  - ❑ [michele@sensalari.com](mailto:michele@sensalari.com)
  - ❑ [michele.sensalari@overneteducation.it](mailto:michele.sensalari@overneteducation.it)
  - ❑ Twitter: @ilsensa7
  - ❑ Linkedin: <https://www.linkedin.com/in/michele-sensalari-4988b7/>

# Agenda – Day 1

- Introduzione alla MWP Academy
- Microsoft 365 Plans
- Password
- Azure Active Directory
- Azure AD Conditional Access
- Self Service Password Reset
- MFA
- Microsoft Authenticator App
- Passwordless
- Azure AD Identity Protection
- Azure Advanced Threat Protection
- Azure AD Privileged Identity Management
- Cloud App Security
- .....

# Introduzione alla MWP Academy

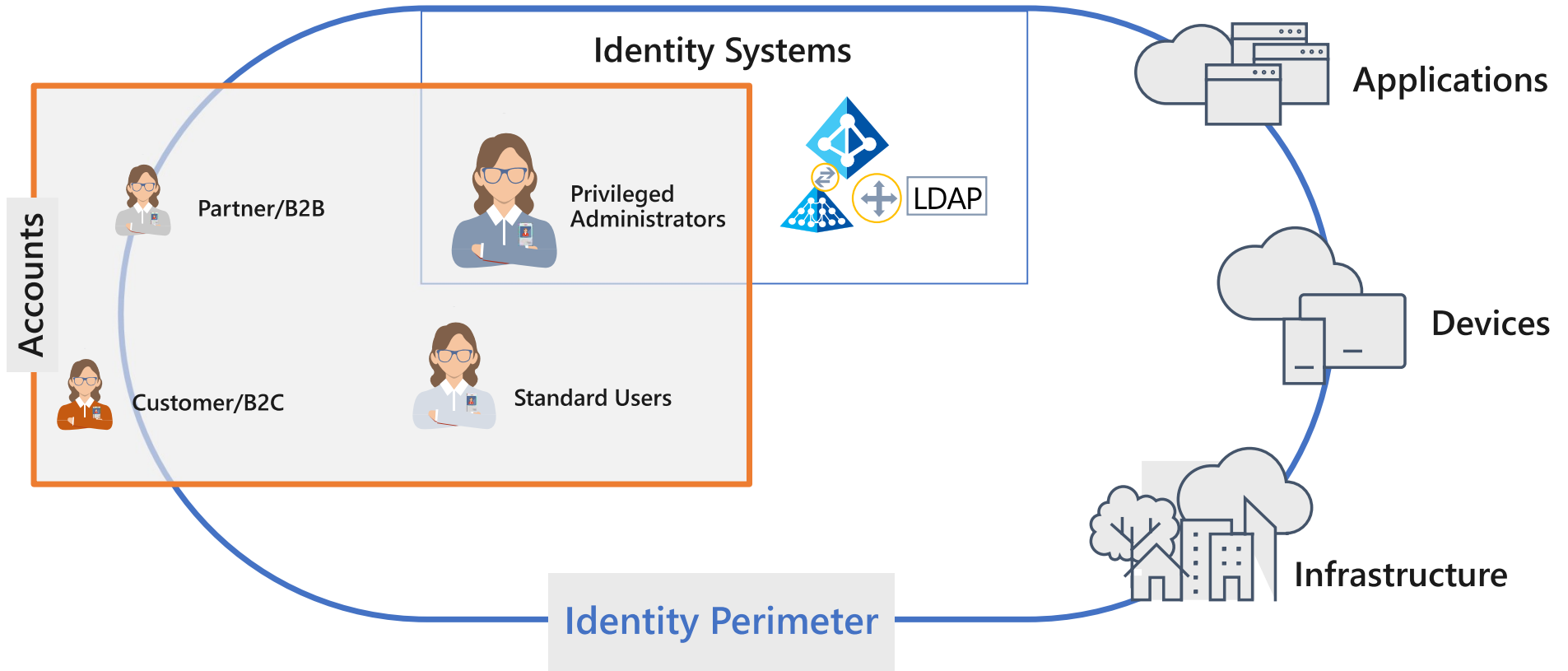


# Programma e contenuti

- ❑ **29 Gennaio:** Identity and Access Management: road to a password-less world– Michele Sensalari
- ❑ **25 Febbraio:** Deploy and manage a Modern Desktop – Michele Sensalari
- ❑ **24 Marzo:** Manage and Secure Non-Microsoft Device with Azure Intune– Michele Sensalari
- ❑ **28 Aprile:** Microsoft Teams Fundamentals - Alessandro Appiani (Michele)
- ❑ **26 Maggio:** Microsoft Teams Deployment & Communications– Alessandro Appiani (Michele)
- ❑ **23 Giugno:** Protect your data with Microsoft Information Protection– Michele Sensalari



# Identity and access management





# Microsoft a leader in the Gartner MQ for Access Management

Azure Active Directory (Azure AD) is a universal identity and access management platform that provides the right people the right access to the right resources. It safeguards identities and simplifies access for users. Users sign in once with a single identity to access all the apps they need—whether they're on-premises apps, Microsoft apps, or third-party cloud apps. Microsoft was recognized for high scores in market understanding and customer experience.



Password.....



# Worst Passwords of 2018-2019

## TOP 2018

- |    |           |      |          |
|----|-----------|------|----------|
| 1. | 123456    | 9.   | qwerty   |
| 2. | password  | 10.  | iloveyou |
| 3. | 123456789 | 11.  | princess |
| 4. | 12345678  | 12.  | admin    |
| 5. | 12345     | 13.  | welcome  |
| 6. | 111111    | 14.  | 666666   |
| 7. | 1234567   | 15.  | abc123   |
| 8. | sunshine  | 100. | ....     |

## TOP 2019

- |    |           |      |            |
|----|-----------|------|------------|
| 1. | 123456    | 9.   | 111111     |
| 2. | 123456789 | 10.  | 123123     |
| 3. | qwerty    | 11.  | abc123     |
| 4. | password  | 12.  | qwerty123  |
| 5. | 1234567   | 13.  | 1q2w3e4r   |
| 6. | 12345678  | 14.  | admin      |
| 7. | 12345     | 15.  | qwertyuiop |
| 8. | iloveyou  | 100. | merlin     |

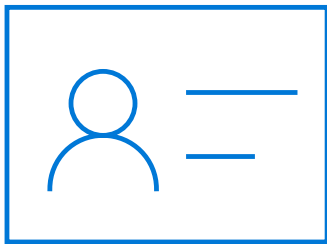
<https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/>

<https://www.teamsid.com/1-50-worst-passwords-2019/>

# Key Identity Trends

## Credential theft

81%



Over 81% of reported incidents in 2018 involved **use of stolen user credentials**.

## Identity as a Service

40%



By 2022, 40% of global midsize and larger enterprises will use identity and access management as a service (IDaaS) capabilities to **fulfill most of their identity and access management (IAM) needs**.

## Cloud-Based Attacks

300%



Cloud-based user account **attacks have increased 300%** from 2017 to 2018.

# Your Pa\$\$word doesn't matter

Attack	Also known as	Frequency	Mechanism	User assists attacker by	Does your password matter?
<b>Credential Stuffing</b>	Breach replay, list cleaning	Very high – 20+M accounts probed daily in MSFT ID systems	<b>Very easy:</b> Purchase creds gathered from breached sites with bad data at rest policies, test for matches on other systems. List cleaning tools are readily available.	Being human. Passwords are hard to think up. <b>62% of users admit reuse.</b>	<b>No</b> – attacker has exact password.
<b>Phishing</b>	Man-in-the-middle, credential interception	Very high. 0.5% of all inbound mails.	<b>Easy:</b> Send emails that promise entertainment or threaten, and link user to doppelganger site for sign-in. Capture creds. Use Modlishka or similar tools to make this very easy.	Being human. People are curious or worried and ignore warning signs.	<b>No</b> – user gives the password to the attacker
<b>Password spray</b>	Guessing, hammering, low-and-slow	Very high – accounts for at least 16% of attacks. Sometimes 100s of thousands broken per day. Millions probed daily.	<b>Trivial:</b> Use easily acquired user lists, attempt the same password over a very large number of usernames. Regulate speed and distributed across many IPs to avoid detection. Tools are readily and cheaply available. See below.	Being human. Using common passwords such as <b>qwerty123</b> or <b>Estate2018!</b>	<b>No</b> , unless it is in the handful of top passwords attackers are trying.

# Your Pa\$\$word doesn't matter

Attack	Also known as	Frequency	Mechanism	User assists attacker by	Does your password matter?
<b>Brute force</b>	Database extraction, cracking	Very low.	Varies: Penetrate network to extract files. Can be easy if target organization is weakly defended (e.g. password only admin accounts), more difficult if appropriate defenses of database, including physical and operation security, are in place. Perform hash cracking on password. Difficulty varies with encryption used. See below.	None.	<b>No</b> , unless you are using an unusable password (and therefore, a password manager) or a really creative passphrase. See below.
<b>Other: Keystroke logging, Local discovery, Extortion</b>		Low	<a href="https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984">https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984</a>		

# Solution....GO PASSWORDLESS...BUT....

## Roadmap

Require unique passwords

Enable password-less credentials

Adopt modern authentication

Block basic authentication

Eliminate passwords

# Microsoft 365 Plans





# Microsoft 365 Plans

Microsoft 365 E3	Microsoft 365 E5
Office 365 E3 Windows 10 Enterprise E3 Enterprise Mobility + Security E3	Office 365 E5 Windows 10 Enterprise E5 Enterprise Mobility + Security E5

Service area	Feature	Office 365 Business Premium	Microsoft 365 Business	Microsoft 365 E3	Microsoft 365 E5
<b>Licenses available</b>	Maximum number of users	300	300	Unlimited	Unlimited
<b>Office apps</b>	Office	Business	Business	ProPlus	ProPlus
<b>Email &amp; calendar</b>	Outlook, Exchange Online	50 GB	50 GB	unlimited	unlimited
<b>File storage</b>	OneDrive for Business	1 TB per user	1 TB per user	unlimited	unlimited

<https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/licensing-microsoft-365-in-smb#feature-comparison-office-365-business-premium-and-microsoft-365-plans>

# Microsoft 365 Plans

Service area	Feature	Office 365 Business Premium	Microsoft 365 Business	Microsoft 365 E3	Microsoft 365 E5
Threat protection	Microsoft Advanced Threat Analytics, Device Guard, Credential Guard, AppLocker, Enterprise Data Protection	No	No	Yes	Yes
	Office 365 Advanced Threat Protection	No	Yes	No	Yes
	Windows Defender Advanced Threat Protection	No	No	No	Yes
	Office 365 Threat Intelligence	No	No	No	Yes

# Microsoft 365 Plans

Service area	Feature	Office 365 Business Premium	Microsoft 365 Business	Microsoft 365 E3	Microsoft 365 E5
<b>Identity management</b>	Self-service password reset for hybrid Azure Active Directory accounts, Azure MFA, Conditional Access	No	Yes	Yes	Yes
	Azure AD: Cloud App Discovery, Azure AD Connect Health, SSO for more than 10 apps	No	No	Yes	Yes
	Azure Active Directory Plan 2	No	No	No	Yes

# Microsoft 365 Plans

Service area	Feature	Office 365 Business Premium	Microsoft 365 Business	Microsoft 365 E3	Microsoft 365 E5
<b>Device &amp; app management</b>	Microsoft Intune, Windows AutoPilot	No	Yes	Yes	Yes
	Shared computer activation, Windows Virtual Desktop	No	Yes	Yes	Yes
	Microsoft Desktop Optimization Pack, VDA	No	No	Yes	Yes
<b>Information protection</b>	Office 365 data loss prevention, Azure Information Protection Plan 1	No	Yes	Yes	Yes
	Azure Information Protection Plan 2, Microsoft Cloud App Security, Office 365 Cloud App Security	No	No	No	Yes

Office 365 E3

Office 365 ProPlus	Exchange Online Plan 2	SharePoint Online Plan 2	OneDrive for Business Plan 2
Office Mobile	Exchange Online Protection	Yammer Enterprise	MyAnalytics
Office Online	Data Loss Prevention	PowerApps for Office 365	Flow for Office 365
Sway	eDiscovery	Retention Policy	Stream for Office 365
Skype for Business Plan 2	Microsoft Teams	Forms	Delve
Meeting Broadcast	Planner	Audit Logging	Kaizala Pro

Office 365 E3

Enterprise Mobility + Security E3 (EMS E3)

Intune MDM & MAM	Azure Information Protection Plan 1	Advanced Threat Analytics	Azure Rights Management
System Center Config Manager	System Center Endpoint Protection	Windows Server CAL Rights	Windows Rights Management
Conditional Access	Multi-Factor Auth (MFA) inc. Server	Microsoft Identity Manager	Azure AD B2B <small>5 guests per user</small>
App Proxy, including PingAccess	Cloud App Discovery	3 <sup>rd</sup> Party MFA Integration	Terms of Use
Advanced Security Reports & Alerts	Single-Sign-On to other SaaS	Azure AD Connect Health	Enterprise State Roaming
Shared Account Password Roll-Over	Self-Service Password Reset in AD	Self-Service Group Management	Group-Based Access Management

Azure AD Premium Plan 1

Enterprise Mobility + Security E3 (EMS E3)

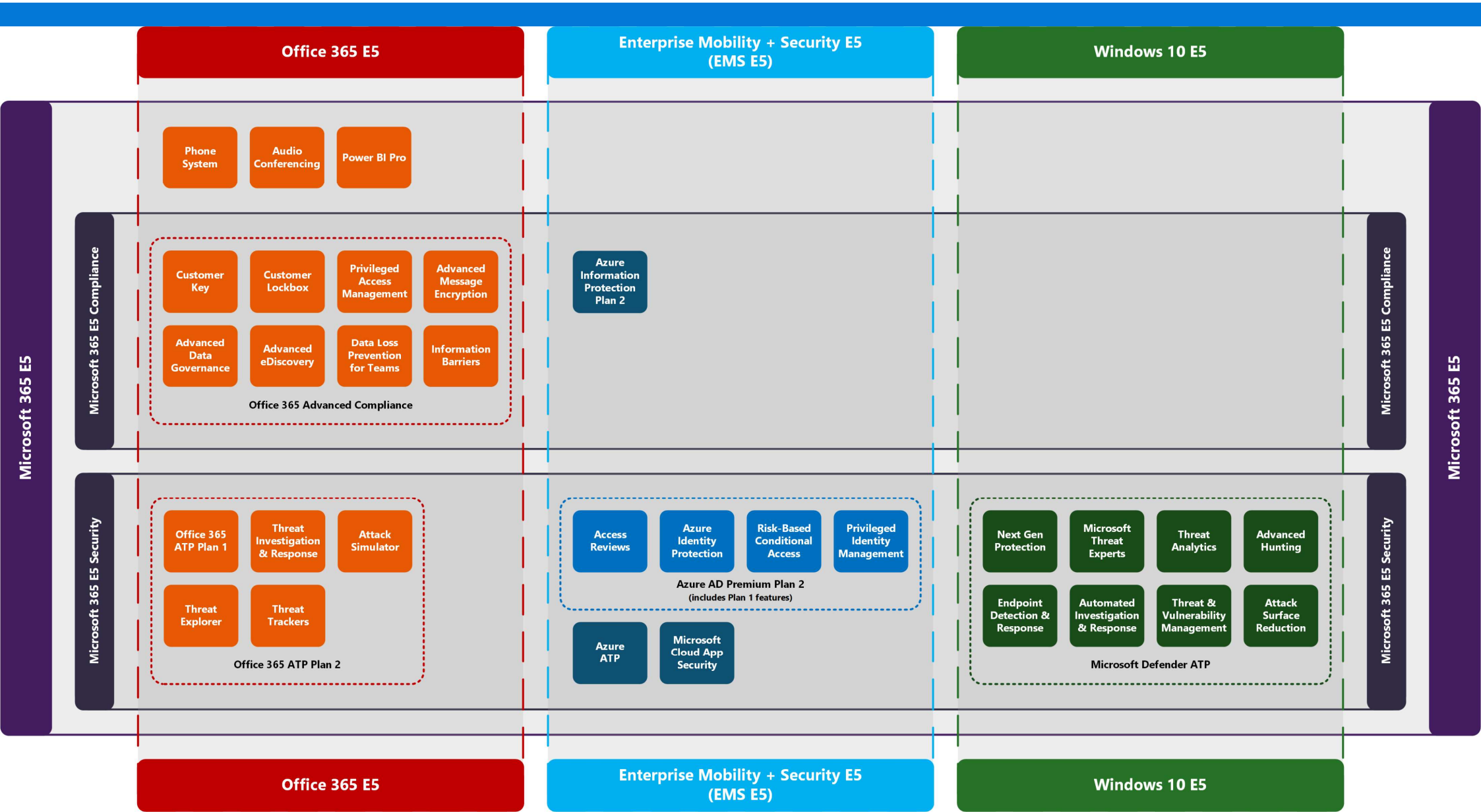
Windows 10 E3

App-V	AppLocker	Azure AD Join	BitLocker
Conditional Access	Cortana Management	Credential Guard	Device Guard
MDM & MAM	MDOP	Microsoft Store for Business	User Experience Virtualisation
Windows Defender Antivirus	Windows Hello Management	Windows Information Protection	Windows to Go
BitLocker to Go	BranchCache	Voice, Pen, Touch, Ink, and Gesture	Windows Analytics
Direct Access	Domain Join	Windows Update for Business	Windows Virtual Desktop

Windows 10 E3

Microsoft 365 E3

Microsoft 365 E3



# Azure Active Directory



# What is Azure Active Directory?

Azure AD is a multi-tenant, cloud-based directory and identity management service

Centralized directory store

Used by Azure and Office 365

Contains all the identities of users in your organization



Manage all your identities in the cloud




Govern access to all your apps in one place



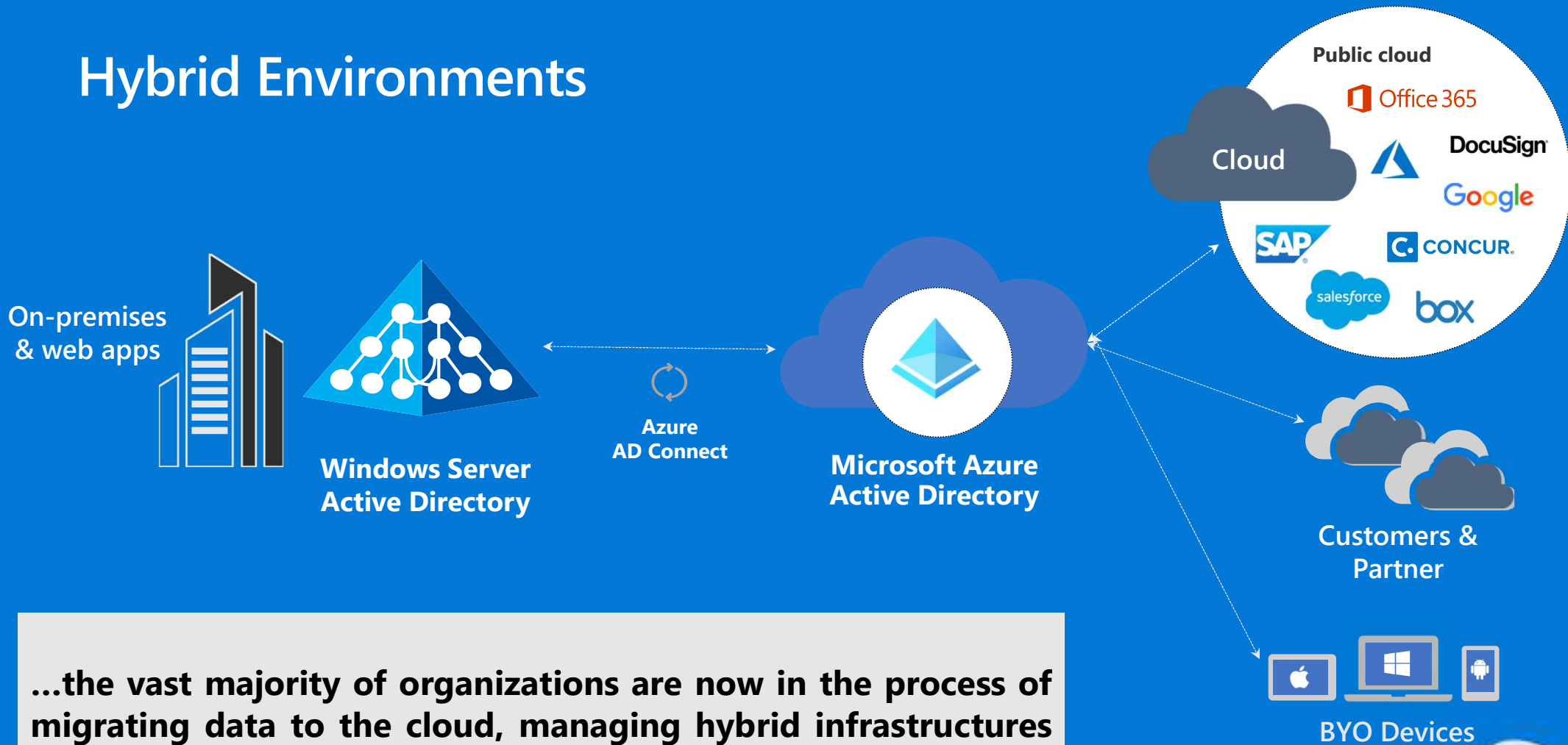
Employ industry-leading security



# What is Azure Active Directory?

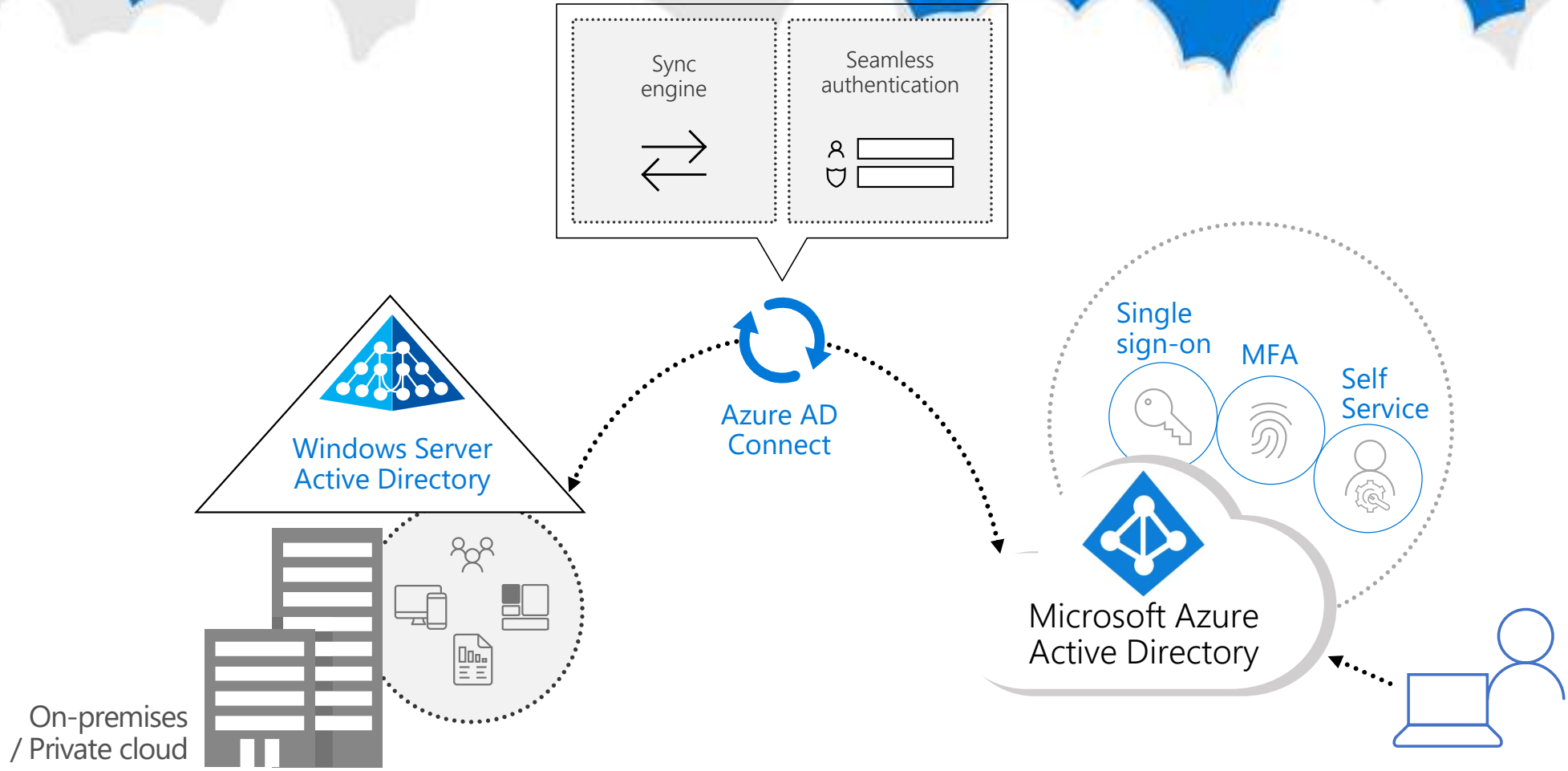
- ❖ Single sign-on to any cloud or on-premises web app: Use a single identity for on-premises and cloud resources
  - ❖ A full suite of identity management capabilities including multi-factor authentication, device registration, self-service password management, privileged account management, RBAC, monitoring, auditing, and alerting
  - ❖ Extend AD to the cloud
  - ❖ Compatible with iOS, Mac OS X, Android, and Windows devices
  - ❖ Protect on-premises web applications with secure remote access
  - ❖ Help protect sensitive data and applications
  - ❖ Azure AD is primarily an identity solution, and designed for HTTP and HTTPS communications
  - ❖ Queried using the REST API over HTTP and HTTPS. Instead of LDAP.
  - ❖ Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization). Instead of Kerberos
  - ❖ Includes federation services, and many third-party services (such as Facebook)
  - ❖ Azure AD users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs)
- 

# Hybrid Environments



**...the vast majority of organizations are now in the process of migrating data to the cloud, managing hybrid infrastructures in a complicated balance of legacy network components and traditional applications.”** Michael Xie, Forbes Magazine

# Azure AD Connect



# Authentication options in Azure AD

## Cloud authentication

Cloud-only

Password Hash Sync +  
Seamless SSO

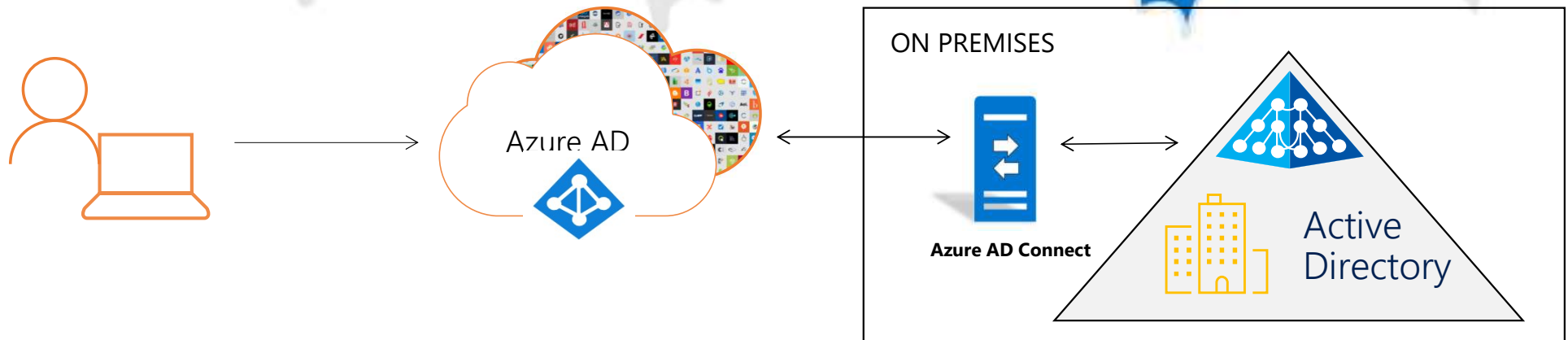
Pass-through authentication  
+ Seamless SSO

## Federated authentication

AD FS

Third party federation  
providers

# Password Hash Sync



## Great user experience

- Same passwords for cloud-based and on-premises apps
- Disaster recovery option incase other authN methods are unavailable

## Secure and compliant

- Only non-reversible hashes are stored in the cloud
- Leaked credential report available
- Integrated with Smart Lockout, Identity Protection and Conditional Access

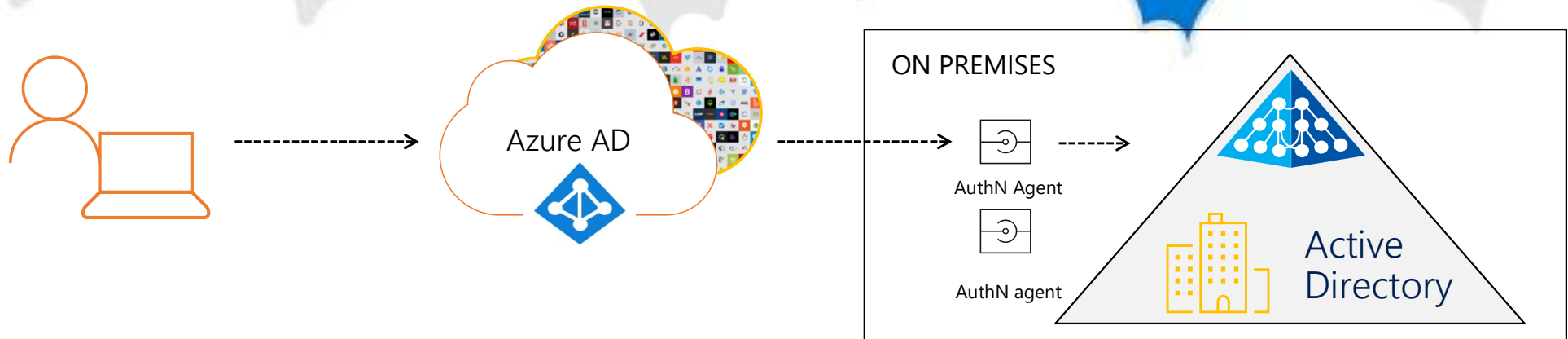
## Easy to deploy & administer

- No on-premises agent needed
- Small on-premises footprint

# Password Hash Sync

- Azure Active Directory uses 1000 iterations of SHA256 over the salted password to generate our per user, per password hash.
- If the incoming password is synchronized from on-premises, Azure AD receive a hash of that on-premises password then re-hash using the same scheme.
- In addition to this, the database in which the passwords are stored is encrypted (encryption also scrambles data, but the data can be recovered with a key), and then stored on an encrypted drive using Bitlocker.

# Pass thru Authentication



## Great user experience

- Same passwords for cloud-based and on-premises apps
- Integrated with Self-Service Password Reset

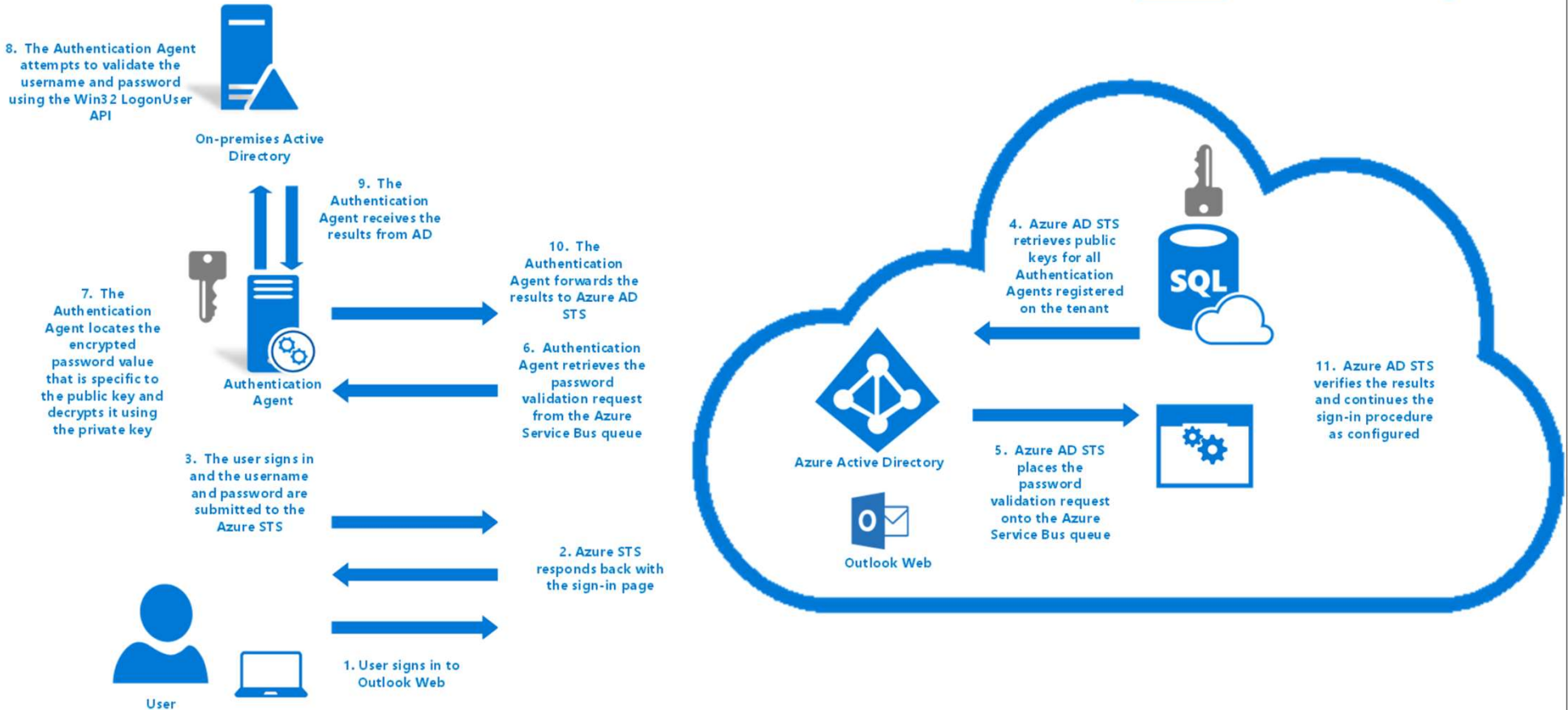
## Secure and compliant

- Passwords remain on-premises
- No DMZ and no inbound firewall requirements
- Integrated with Smart Lockout, Identity Protection and Conditional Access

## Easy to deploy & administer

- Agent-based deployment
- High availability out-of-the-box
- No complex on-premises deployments or network config
- Zero management overhead

# Pass thru Authentication



Authentication Agents are persistently connected to the Service Bus queue, one of the available Authentication Agents retrieves the password validation request

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-security-deep-dive>

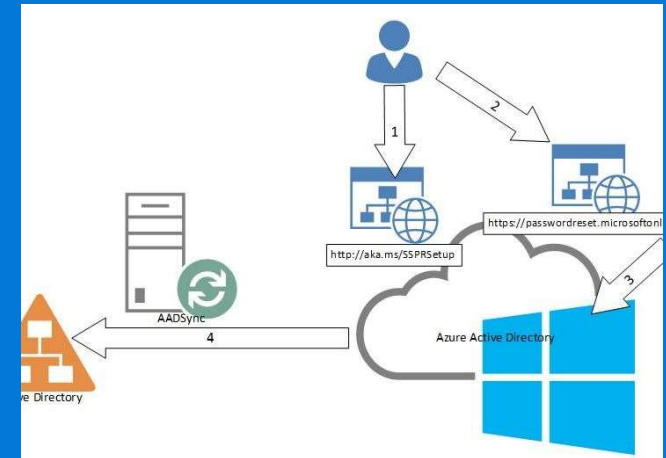


# Password WriteBack

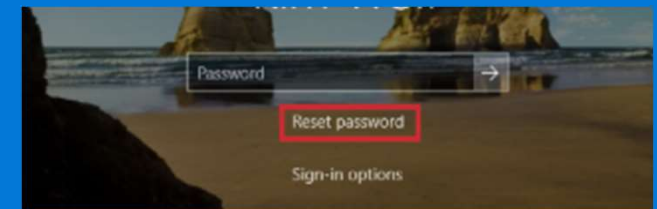
- Password writeback is a feature enabled with Azure AD Connect that allows password changes in the cloud to be written back to an existing on-premises directory in real time.
- Password writeback is supported in environments that use:
  - Active Directory Federation Services
  - Password hash synchronization
  - Pass-through authentication
- <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

# Self-Service Password Management

- Self-service password reset (SSPR) allows users to reset their own password without requiring intervention by an administrator
- SSPR is not enabled by default
- To reset a password, users must authenticate their identity first
- If an administrator wants to use SSPR, they must use two verification methods, and they are not able to use security questions
- If you purchase Azure AD Premium, it includes the ability to write back passwords. This enables you to implement self-service password reset for synchronized identities and federated identities



<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>



<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-windows>

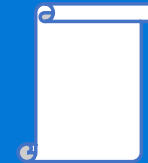
**Require unique passwords**

# Azure AD Password Protection



# Azure AD Password Protection

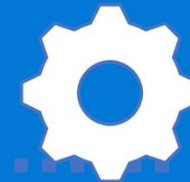
- Protects your organization by detecting and blocking known weak passwords and their variants
- It can also block additional weak terms that are specific to your organization.
- Enhance the password quality of your organizations.
- Thwarting "password spray" attacks type.
- Stop users to use guessable passwords.
- Permit the use On-Premises of the:
  - Microsoft Global Banned Password List
  - Custom Banned Password list



Banned  
Password Lists



Proxy  
Service



DC Agent  
Service



Password  
Filter



# Design Principles

- **Active Directory:**
  - **No Active Directory schema changes:** The software uses the existing Active Directory container and serviceConnectionPoint schema objects.
  - **No minimum DFL/FFL:** The software works with every supported Active Directory domain or forest functional level (DFL/FFL).
  - **No Service Account:** The software doesn't create or require accounts in the Active Directory domains that it protects.
- **Network**
  - Support a **proxy architecture** using the Azure AD Password Protection Proxy Service.
  - Domain controllers never have to communicate directly with the Internet.
  - No new network ports are opened on domain controllers where the Azure AD Password Protection DC Agent is installed.
- **Functional**
  - User clear-text passwords never leave the domain controller, either during password validation operations or at any other time.
  - The software is not dependent on other Azure AD features. Incremental deployment is supported.

Custom banned passwords

Enforce custom list ⓘ  Yes  No

Custom banned password list ⓘ

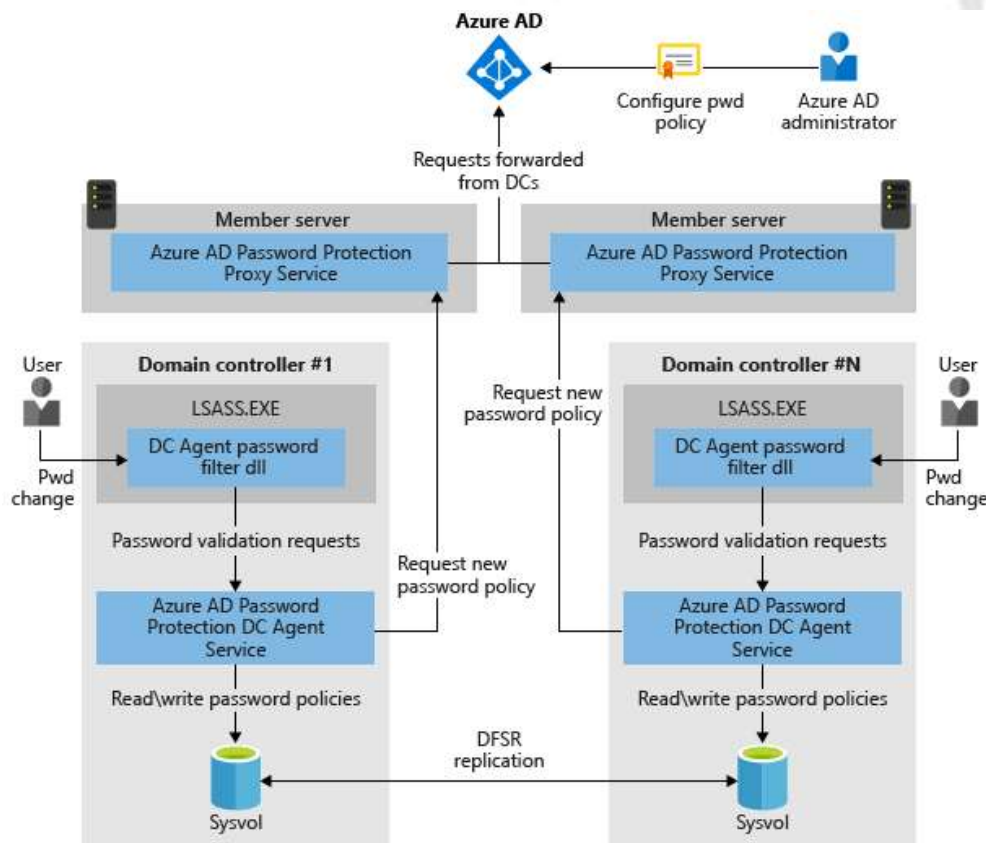
Medicina  
Sciroppo  
Pastiglie  
Comprese  
Bustine

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ  Yes  No

Mode ⓘ  Enforced  Audit

# Architecture



The **Password filter DLL**, receives password validation requests from the **Operating System** and forwards them to the **DC agent service** running locally on the Domain Controller.

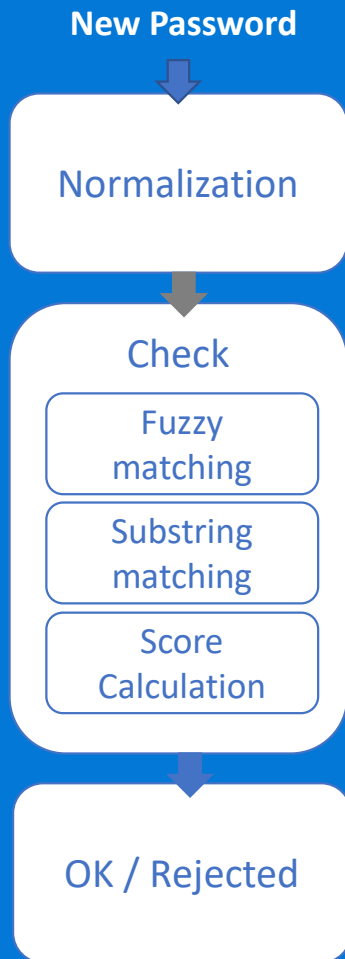
## DC agent service:

- Receives password validation requests from the Password filter DLL, processes them using the current **locally available password policy**, and returns the result
- Once per hour calls the **Azure AD password protection proxy service** to retrieve new versions of the password policy

## Proxy Service:

- Runs on **domain-joined machines in the current Active Directory forest**.
- The **Main task** is to **forwards requests** from domain controllers to **Azure AD** and **returns the response** from Azure AD back to the domain controllers.
- **Must be registered**, with two PowerShell cmdlets, on **Azure AD** and in the **Active Directory forest**

# Password evolution Process



Normalization

Original letter	Substituted letter
'0'	'o'
'1'	'l'
'\$'	's'
'@'	'a'

Fuzzy matching

Contoso**s** = Contoso  
Conto**s** = Contoso  
**s**Contoso = Contoso

Score Calculation

Substring matching

Michele123abcd = Michele

MicheleContosoKO  
[Matteo] + [Contoso] + (K) + (O) = 4

MicheleContosoOK!  
[Matteo] + [Contoso] + (O) + (K) + (!) = 5

# Azure AD Password Protection License

	Azure AD password protection with global banned password list	Azure AD password protection with custom banned password list
Cloud-only users	Azure AD Free	Azure AD Premium P1 or P2
Users synchronized from on-premises Windows Server Active Directory	Azure AD Premium P1 or P2	Azure AD Premium P1 or P2



MFA



# Implementing Multi-Factor Authentication

- Multi-factor Authentication (MFA) in Microsoft 365 helps increase security by requesting users to provide a username and a password while signing in and then use a second authentication method.
- The second authentication method might be acknowledging a phone call, text message, or an app notification on their smartphone
- You can also enable users who authenticate from a federated, on-premises directory for multi-factor authentication.
- The tenant administrator enables MFA in the Microsoft 365 admin center

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

Allow users to create app passwords to sign in to non-browser apps  
 Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27  
192.168.1.0/27  
192.168.1.0/27

verification options [\(learn more\)](#)

Methods available to users:

Call to phone  
 Text message to phone  
 Notification through mobile app  
 Verification code from mobile app or hardware token

remember multi-factor authentication [\(learn more\)](#)

Allow users to remember multi-factor authentication on devices they trust  
Days before a device must re-authenticate (1-60):

# Multi-Factor Authentication

- Any two of more of the following factors:
  - Something you know: a password or pin
  - Something you have: a phone, smartcard, or hardware token
  - Something you are: facial recognition, fingerprint, or other biometric



Hardware token



Microsoft Authenticator



Certificates



Phone




Smartcard

You can reduce your odds of being compromised by up to 99.9% by implementing multi-factor authentication (MFA).

*Source: [Microsoft 2018 Security Research](#)*

# MFA – How to enable

- **Enabled by changing user state** - This is the traditional method for requiring two-step verification and is discussed in this article. It works with both Azure MFA in the cloud and Azure MFA Server. Using this method requires users to perform two-step verification **every time** they sign in and overrides Conditional Access policies.
  - **Enabled by Conditional Access policy** - This is the most flexible means to enable two-step verification for your users. Enabling using Conditional Access policy only works for Azure MFA in the cloud and is a premium feature of Azure AD.
  - **Enabled by Azure AD Identity Protection** - This method uses the Azure AD Identity Protection risk policy to require two-step verification based only on sign-in risk for all cloud applications. This method requires Azure Active Directory P2 licensing.
- 

# Changing user state

Status	Description
Disabled	The default state for a new user not enrolled in Azure MFA.
Enabled	The user has been enrolled in Azure MFA, but has not registered. They receive a prompt to register the next time they sign in.
Enforced	The user has been enrolled and has completed the registration process for Azure MFA.

Microsoft Azure bmath@contoso.com | ?

## multi-factor authentication

[users](#) [service settings](#)

Before you begin, take a look at the [multi-factor auth deployment guide](#).

View:   Multi-Factor Auth status:

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Bill Mathers	bmath@contoso.com	Disabled
<input type="checkbox"/>	Bill Mathers	billmath@billmathfabrikam.onmicrosoft.com	Disabled
<input type="checkbox"/>	Britta Simon	bsimon@billmathfabrikam.onmicrosoft.com	Enforced
<input type="checkbox"/>	John Smith	jsmith@billmathfabrikam.onmicrosoft.com	Disabled
<input type="checkbox"/>	Lola Jacobson	ljacobson@billmathfabrikam.onmicrosoft.com	Enabled

Select a user

# OATH tokens for Azure MFA

- Azure AD supports the use of OATH-TOTP SHA-1 tokens of the 30-second or 60-second variety
- The following are the pre-requirements to complete this configuration:
  - Azure AD Premium P1 or P2 license
  - Token2 hardware token(s)
  - A CSV file for your token device(s). You can request the CSV file after successful delivery.
- Import CSV



```
upn,serial number,secret key,timeinterval,manufacturer,model  
guInara@token2.onmicrosoft.com,60234567,1234567890abcdef1234567890abcdef,30,Token2,c101
```

**MFA Server - OATH tokens**

Overview

Manage

- Account lockout
- Block/unblock users
- Caching rules
- Fraud alert
- Notifications
- OATH tokens**

Upload Download Refresh

To get started, select the Upload button above and choose a CSV file. For more information, view the public documentation.

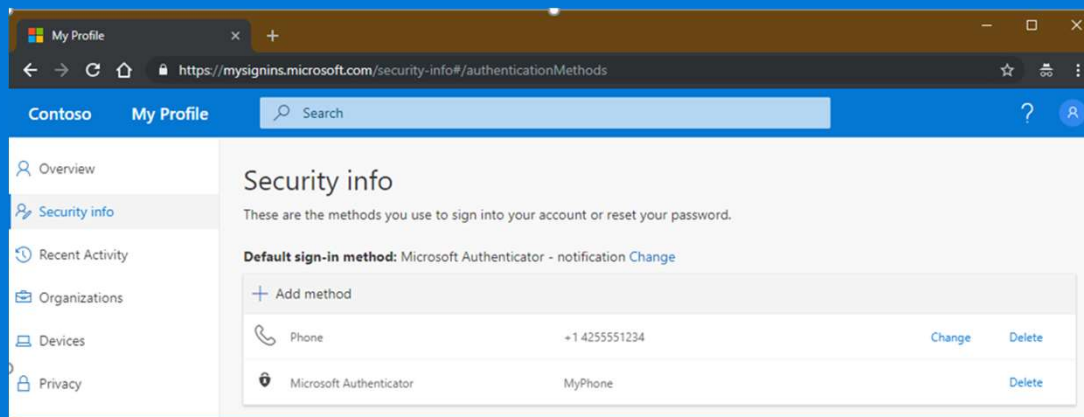
Username  Show

**NAME**

No results

# Combined security information registration (preview)

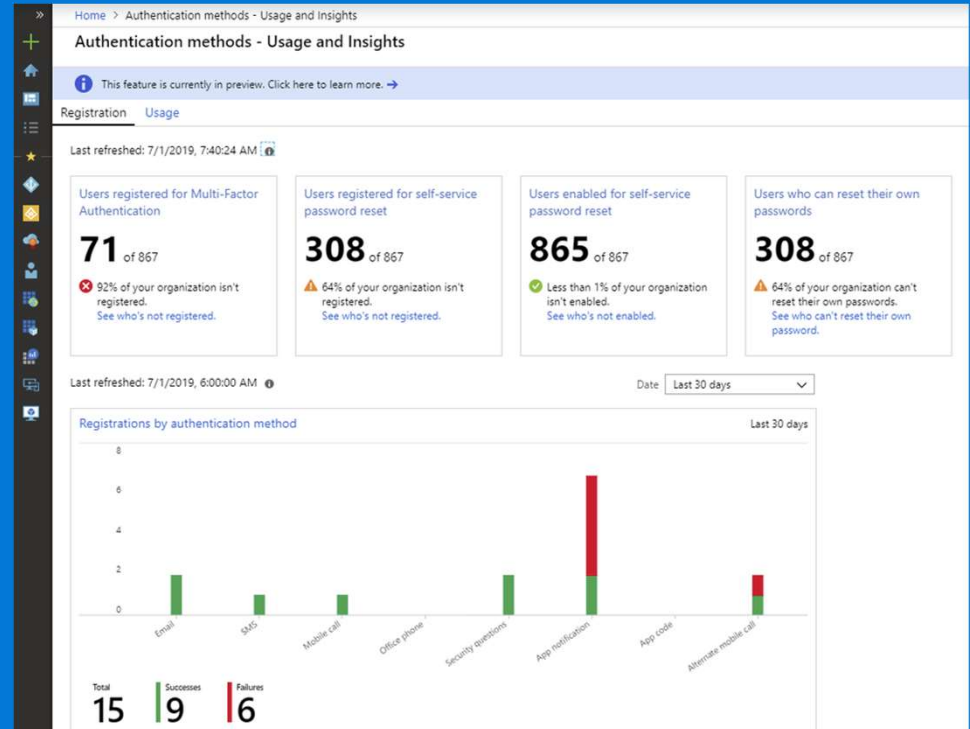
Before combined registration, users registered authentication methods for Azure Multi-Factor Authentication and self-service password reset (SSPR) separately. People were confused that similar methods were used for Multi-Factor Authentication and SSPR but they had to register for both features. Now, with combined registration, users can register once and get the benefits of both Multi-Factor Authentication and SSPR.



	Register	Change	Delete
Microsoft Authenticator	Yes (maximum of 5)	No	Yes
Other authenticator app	Yes (maximum of 5)	No	Yes
Hardware token	No	No	Yes
Phone	Yes	Yes	Yes
Alternate phone	Yes	Yes	Yes
Office phone	No	No	No
Email	Yes	Yes	Yes
Security questions	Yes	No	Yes
App passwords	Yes	No	Yes

# Authentication Methods–Usage & Insights

- One of the most common requests is to have the ability to understand who is and is not registered for both MFA and SSPR. In the **Registration** section of the Authentication Methods Registration report, you can see:
  - how many of your users are registered for MFA and SSPR.
  - how many users are enabled to use SSPR,
  - how many of these users have actually registered so they can reset their own passwords.
- This data is calculated by looking at each user to see which methods they've registered and whether they are enabled for SSPR. You can drill down and see the status of each user by clicking one of the tiles.





# Security Defaults

## One-click method

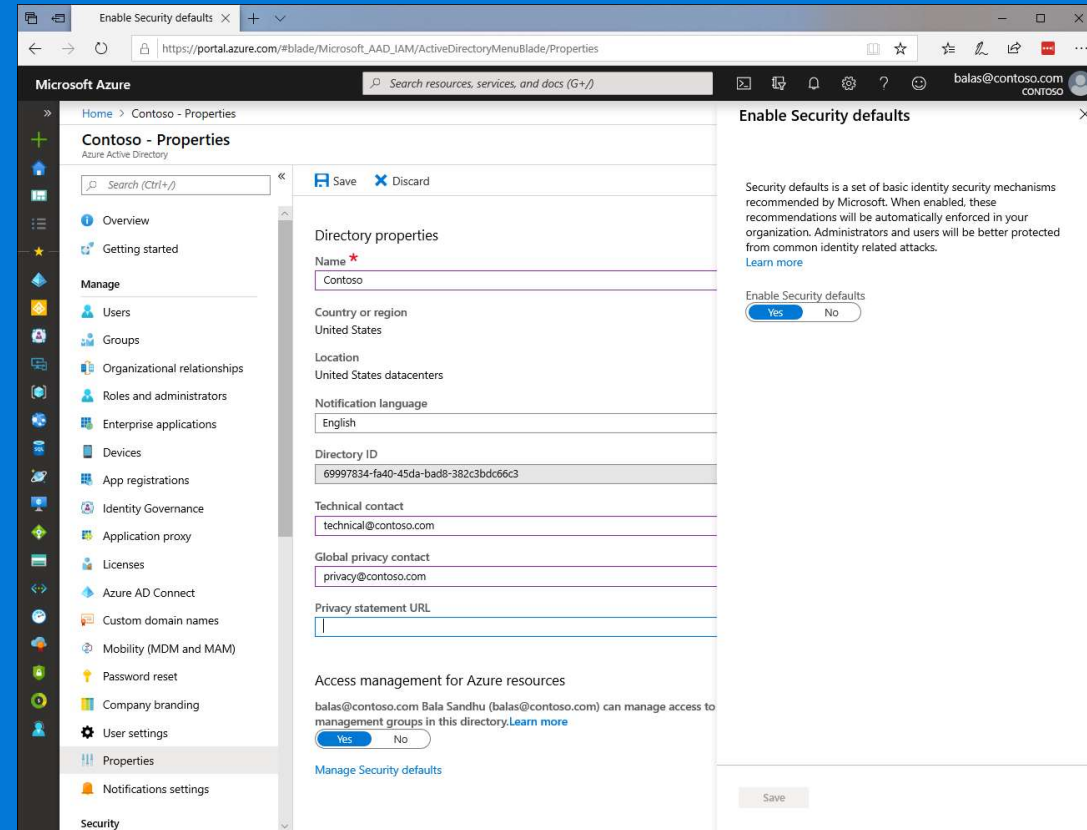
Enables MFA for all users AND blocks legacy auth tenant wide

It's FREE!!!

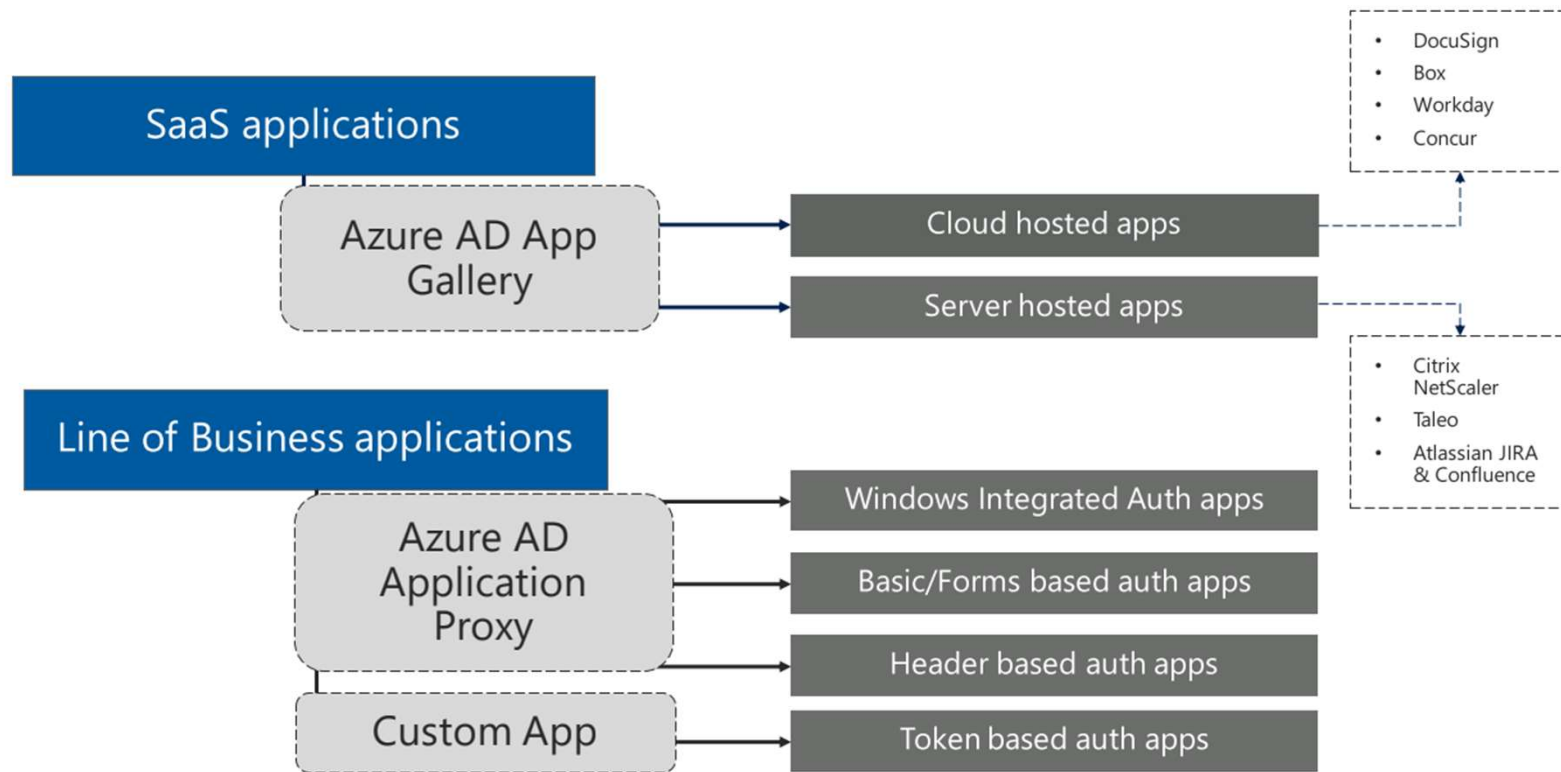
## Secure by default

New tenants will have security defaults enabled by default:

- Requiring all users and admins to register for MFA.
- Challenging users with MFA - mostly when they show up on a new device or app, but more often for critical roles and tasks.
- Disabling authentication from legacy authentication clients, which can't do MFA.

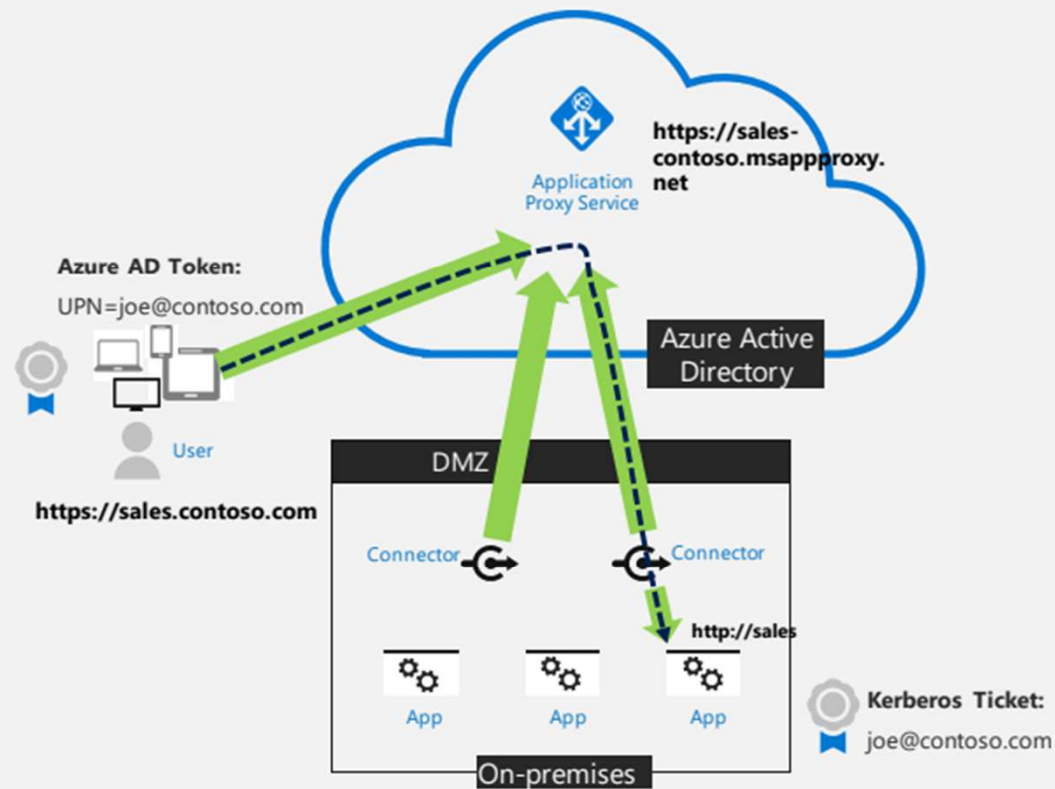


# Azure AD Enterprise Applications



# Azure AD Application Proxy

1. Make the internal hosted apps accessible to the workforce without VPN
2. Azure AD protected External URL
3. Azure AD authentication or Pre-Auth option for authentication
4. Ability to Translate Header
5. Ability to translate Body



Home > Enterprise applications > Application proxy > Add your own on-premises application

### Add your own on-premises application

Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Application Proxy

**Basic Settings**

- Name: Contoso Sales Leads
- Internal Uri: https://salesleads
- External Uri: https://contososalesleads-jeevancontoso.msappproxy.net/
- Pre Authentication: Azure Active Directory
- Connector Group: Default

**Additional Settings**

- Backend Application Timeout: Default
- Translate URLs In:
  - Headers: Yes
  - Application Body: Yes

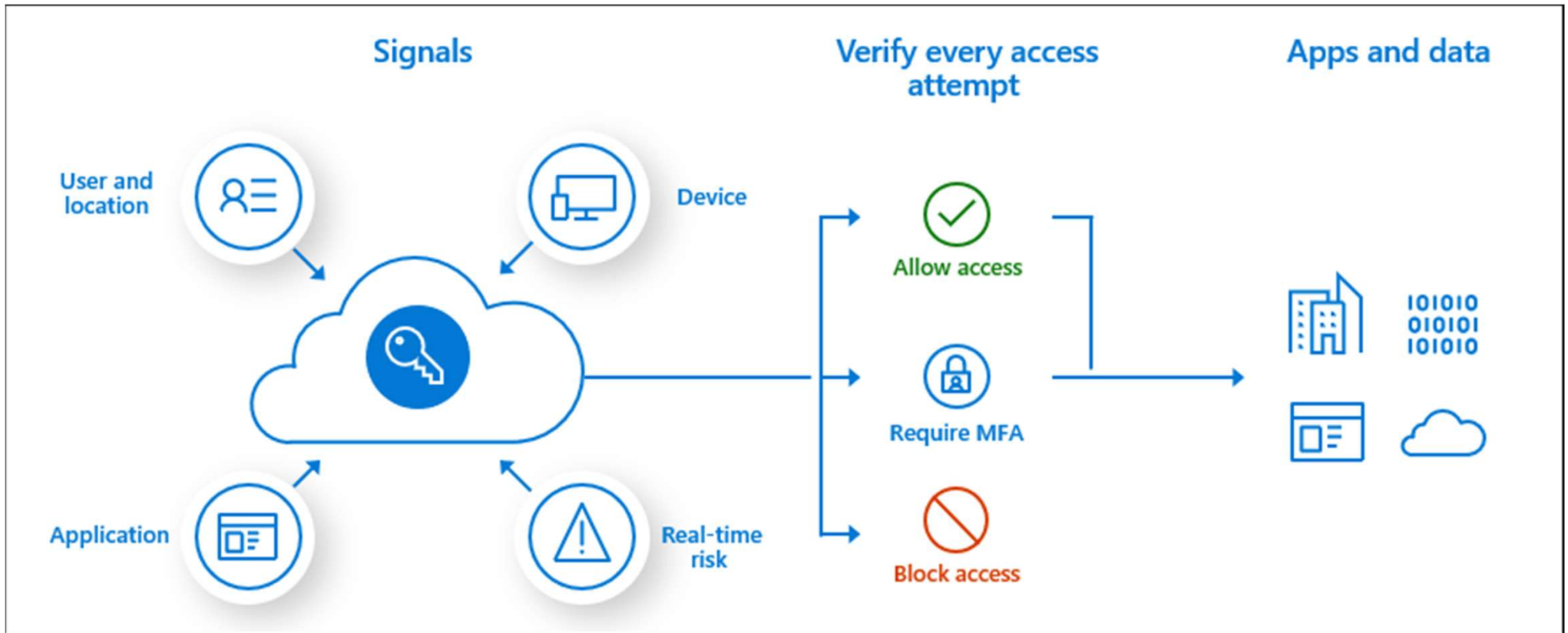
**Adopt modern authentication**

**Block basic authentication**

# Azure AD Conditional Access



# Azure AD Conditional Access



# Configuring Conditional Access



Corporate resources



Access Decisions

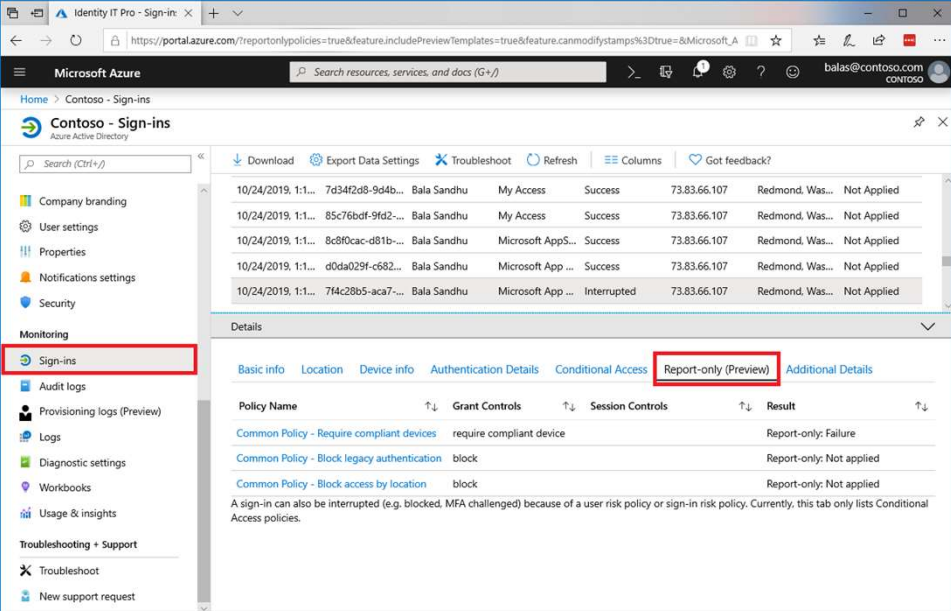


Device & Identity Signals

# What is Conditional Access report-only mode?

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

- Conditional Access policies can be enabled in report-only mode.
- During sign-in, policies in report-only mode are evaluated but not enforced. Results are logged in the **Conditional Access** and **Report-only (Preview)** tabs of the Sign-in log details.
- Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.



Date	User	App	Status	IP	Location	Result
10/24/2019, 1:1...	7d34f2d8-9d4b...	Bala Sandhu	My Access	Success	73.83.66.107	Redmond, Was... Not Applied
10/24/2019, 1:1...	85c76bdf-9fd2...	Bala Sandhu	My Access	Success	73.83.66.107	Redmond, Was... Not Applied
10/24/2019, 1:1...	8c8f0cac-d81b...	Bala Sandhu	Microsoft AppS...	Success	73.83.66.107	Redmond, Was... Not Applied
10/24/2019, 1:1...	d0da029f-c682...	Bala Sandhu	Microsoft App ...	Success	73.83.66.107	Redmond, Was... Not Applied
10/24/2019, 1:1...	7f4c28b5-aca7...	Bala Sandhu	Microsoft App ...	Interrupted	73.83.66.107	Redmond, Was... Not Applied

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only>

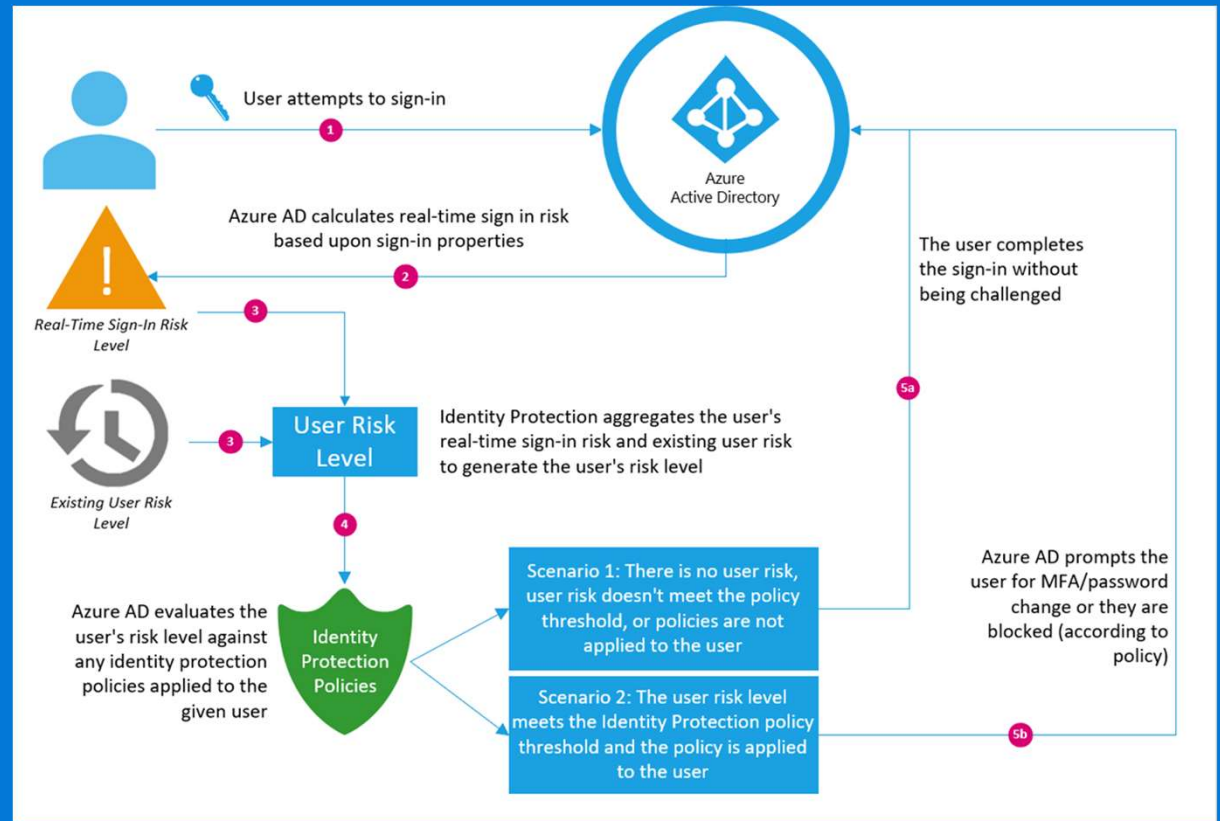
# Azure AD Identity Protection

A decorative border at the bottom of the slide consisting of stylized, overlapping clouds in white and light gray.



# Azure AD Identity Protection

- Proactively prevent compromised identities from being abused
- Automatically mitigate risk when suspicious activity is detected
- Investigate risky users and sign-ins to address potential vulnerabilities
- Be alerted when a user's risk reaches a specified threshold
- Export risk detection data to third-party utilities for further analysis.



# How does Identity Protection work?

A user is considered at risk if..



A sign-in to Azure AD is considered risky.

examples: unfamiliar sign-in properties, anonymous IP address



An activity done in an application after sign-in is suspicious

examples: user sets up forwarding rules, user sends spam.



The user's credentials are known to be compromised

example: reused credentials found on data breach.

# Sign-in risk

- A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.
- These risks can be calculated in real-time or calculated offline using Microsoft's internal and external threat intelligence sources including security researchers, law enforcement professionals, security teams at Microsoft, and other trusted sources

Risk detection	Detection type	Description
Anonymous IP address	Real-time	This risk detection type indicates sign-ins from an anonymous IP address (for example, Tor browser or anonymous VPN). These IP addresses are typically used by actors who want to hide their login telemetry (IP address, location, device, etc.) for potentially malicious intent.
Atypical travel	Offline	<p>This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior. Among several other factors, this machine learning algorithm takes into account the time between the two sign-ins and the time it would have taken for the user to travel from the first location to the second, indicating that a different user is using the same credentials.</p> <p>The algorithm ignores obvious "false positives" contributing to the impossible travel conditions, such as VPNs and locations regularly used by other users in the organization. The system has an initial learning period of the earliest of 14 days or 10 logins, during which it learns a new user's sign-in behavior.</p>
Malware linked IP address	Offline	This risk detection type indicates sign-ins from IP addresses infected with malware that is known to actively communicate with a bot server. This detection is determined by correlating IP addresses of the user's device against IP addresses that were in contact with a bot server while the bot server was active.
Unfamiliar sign-in properties	Real-time	<p>This risk detection type considers past sign-in history (IP, Latitude / Longitude and ASN) to look for anomalous sign-ins. The system stores information about previous locations used by a user, and considers these "familiar" locations. The risk detection is triggered when the sign-in occurs from a location that's not already in the list of familiar locations. Newly created users will be in "learning mode" for a period of time in which unfamiliar sign-in properties risk detections will be turned off while our algorithms learn the user's behavior. The learning mode duration is dynamic and depends on how much time it takes the algorithm to gather enough information about the user's sign-in patterns. The minimum duration is five days. A user can go back into learning mode after a long period of inactivity. The system also ignores sign-ins from familiar devices, and locations that are geographically close to a familiar location.</p> <p>We also run this detection for basic authentication (or legacy protocols). Because these protocols do not have modern properties such as client ID, there is limited telemetry to reduce false positives. We recommend our customers to move to modern authentication.</p>
Admin confirmed user compromised	Offline	This detection indicates an admin has selected 'Confirm user compromised' in the Risky users UI or using riskyUsers API. To see which admin has confirmed this user compromised, check the user's risk history (via UI or API).
Malicious IP address	Offline	This detection indicates sign-in from a malicious IP address. An IP address is considered malicious based on high failure rates because of invalid credentials received from the IP address or other IP reputation sources.
Suspicious inbox manipulation rules	Offline	This detection is discovered by Microsoft Cloud App Security (MCAS). This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This may indicate that the user's account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.
Impossible travel	Offline	This detection is discovered by Microsoft Cloud App Security (MCAS). This detection identifies two user activities (is a single or multiple sessions) originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second, indicating that a different user is using the same credentials.

# User risk

- A user risk represents the probability that a given identity or account is compromised.
- These risks are calculated offline using Microsoft's internal and external threat intelligence sources including security researchers, law enforcement professionals, security teams at Microsoft, and other trusted sources.

Risk detection	Description
Leaked credentials	This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials. This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling the credentials on the black market. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they are checked against Azure AD users' current valid credentials to find valid matches.
Azure AD threat intelligence	This risk detection type indicates user activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.

# Investigate risk

## Risky sign-ins

The risky sign-ins report contains filterable data for up to the past 30 days (1 month).

With the information provided by the risky sign-ins report, administrators can find:

- Which sign-ins are classified as at risk, confirmed compromised, confirmed safe, dismissed, or remediated.
- Real-time and aggregate risk levels associated with sign-in attempts.
- Detection types triggered
- Conditional Access policies applied
- MFA details
- Device information
- Application information
- Location information

Administrators can then choose to take action on these events. Administrators can choose to:

- Confirm sign-in compromise
- Confirm sign-in safe

## Risky users

With the information provided by the risky users report, administrators can find:

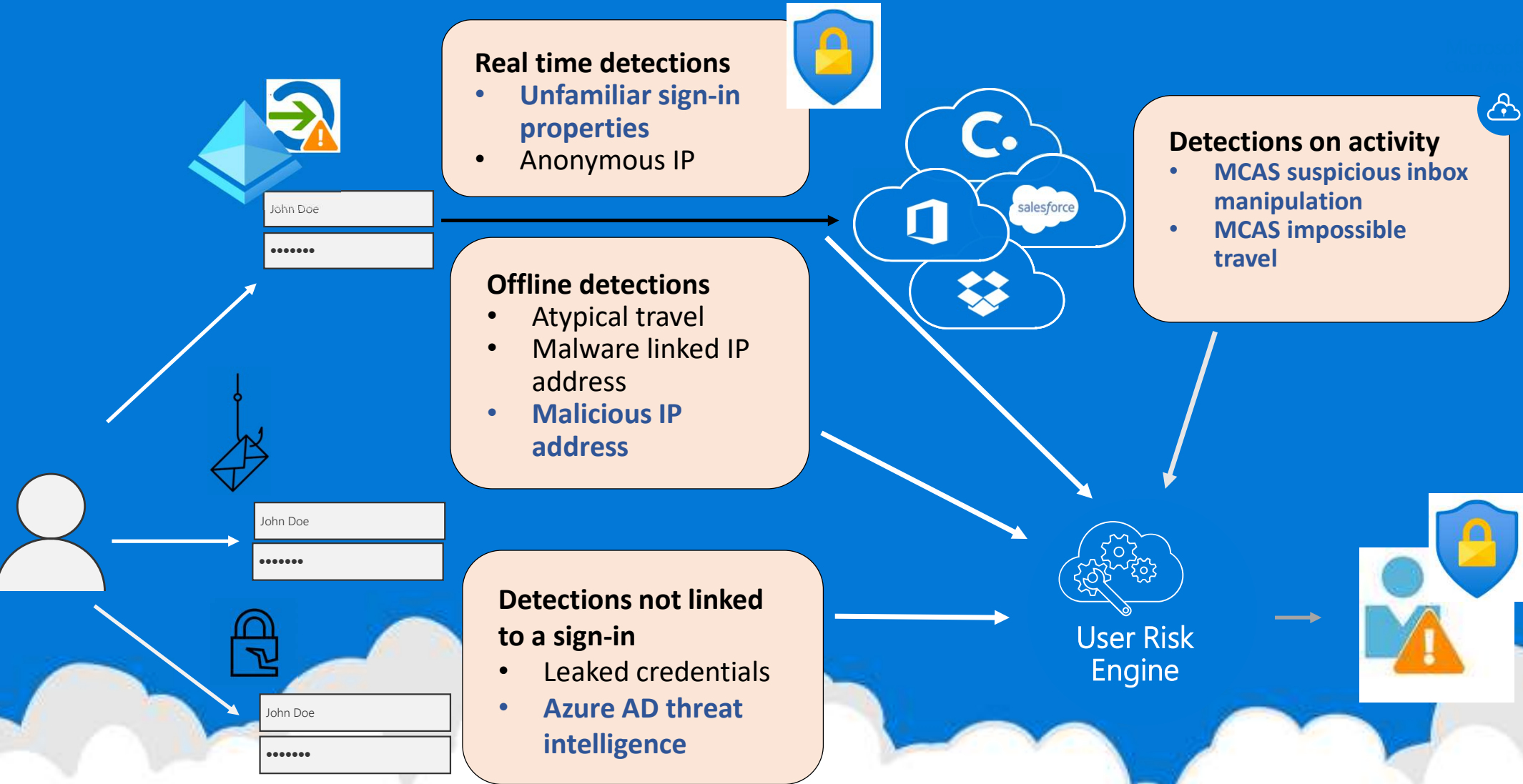
- Which users are at risk, have had risk remediated, or have had risk dismissed?
- Details about detections
- History of all risky sign-ins
- Risk history

Administrators can then choose to take action on these events. Administrators can choose to:

- Reset the user password
- Confirm user compromise
- Dismiss user risk
- Block user from signing in
- Investigate further using Azure ATP

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk>

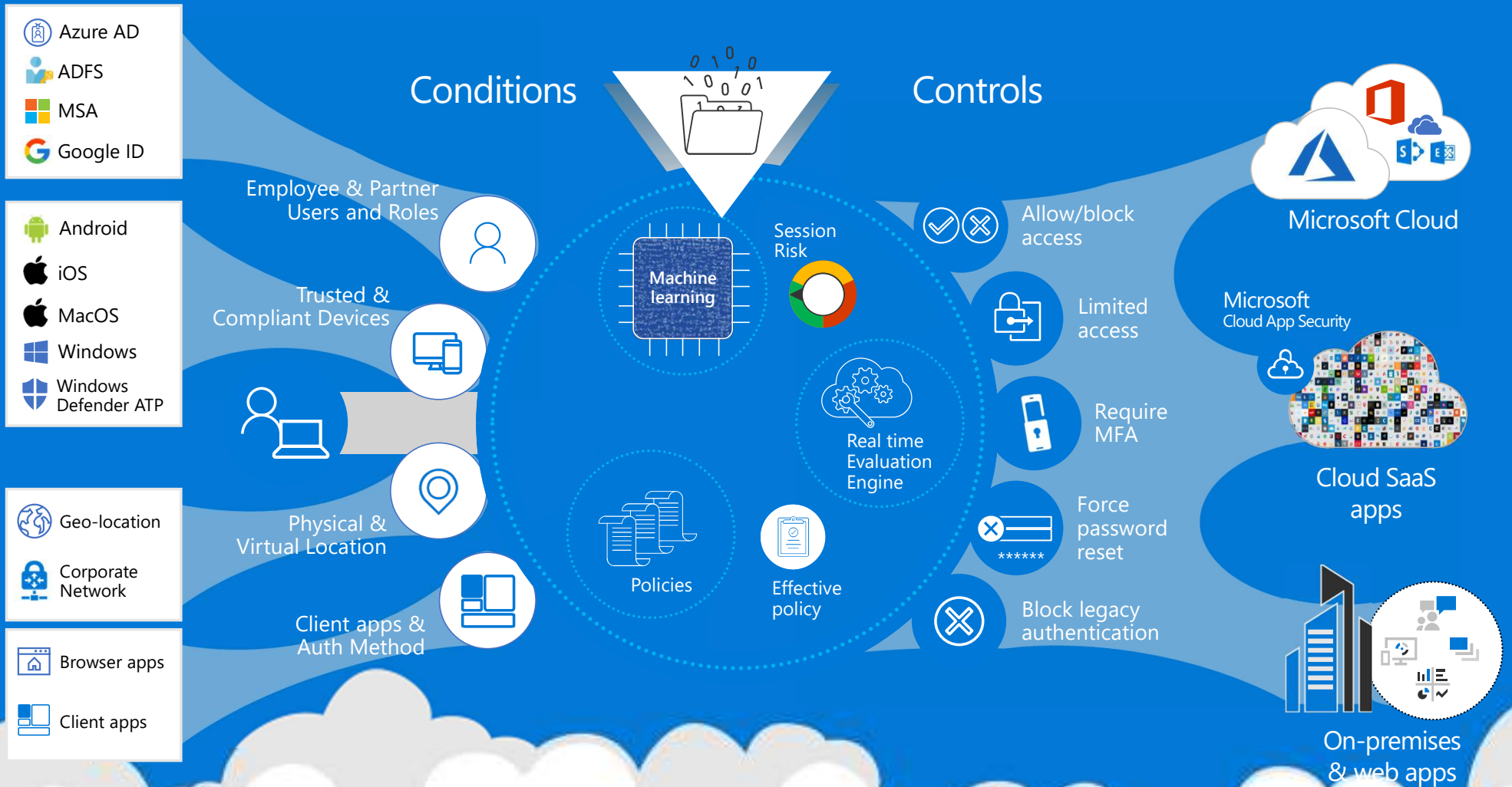
# Risk detections and risk engine



# Azure AD Identity Protection License Requirements

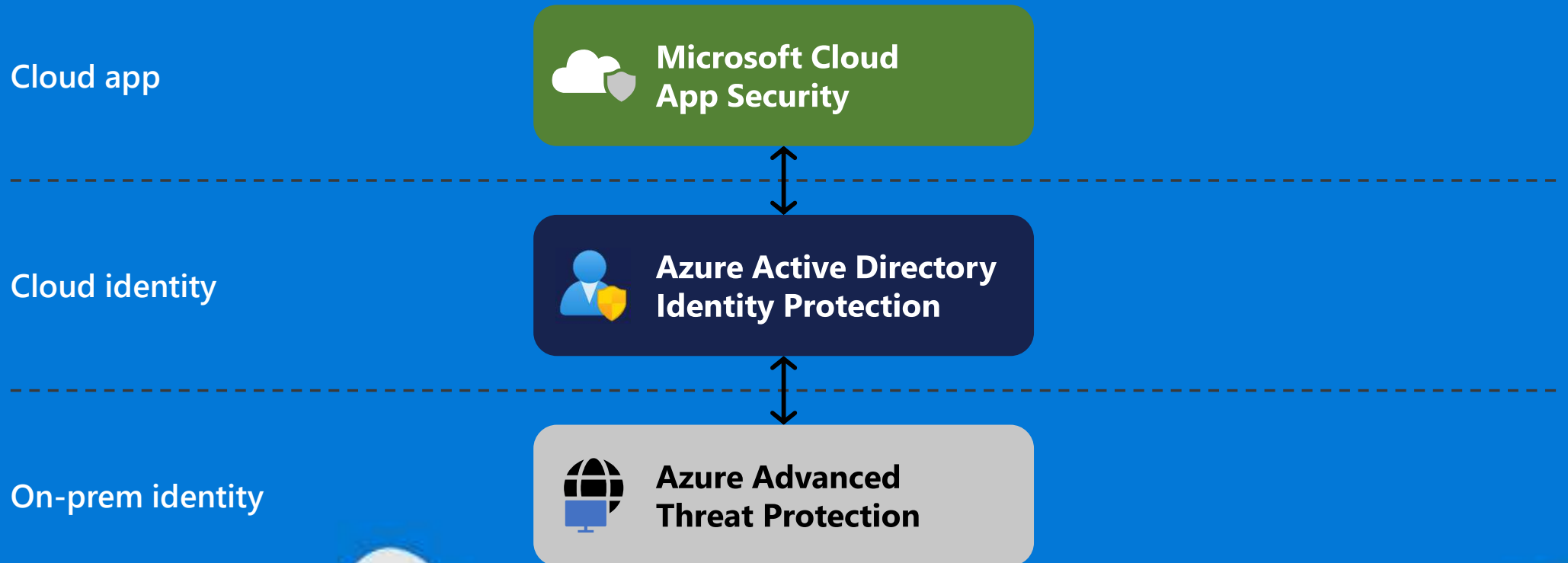
Capability	Details	Azure AD Premium P2	Azure AD Premium P1	Azure AD Basic/Free
Risk policies	User risk policy (via Identity Protection)	Yes	No	No
Risk policies	Sign-in risk policy (via Identity Protection or Conditional Access)	Yes	No	No
Security reports	Overview	Yes	No	No
Security reports	Risky users	Full access	Limited Information	Limited Information
Security reports	Risky sign-ins	Full access	Limited Information	Limited Information
Security reports	Risk detections	Full access	Limited Information	No
Notifications	Users at risk detected alerts	Yes	No	No
Notifications	Weekly digest	Yes	No	No
	MFA registration policy	Yes	No	No

# Conditional Access + Identity Protection





# End-to-end Identity Protection



# In-session detections across your app ecosystem

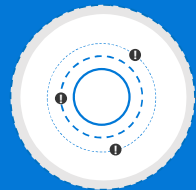
## Cloud App Security (require M365 E5)

Malware in cloud apps  
Malicious OAuth applications  
Multiple failed login attempts  
Suspicious inbox rules

Unusual file share activity  
Unusual file download  
Unusual file deletion activity  
Ransomware activity  
Data exfiltration to unsanctioned apps  
Activity by a terminated employee

Indicators of a  
compromised session

Malicious use of  
a privileged user



Threat delivery  
and persistence

Malicious use of  
an end-user account

Activity from suspicious IP addresses  
Activity from anonymous IP addresses  
Activity from an infrequent country  
Impossible travel between sessions  
Logon attempt from a suspicious user agent

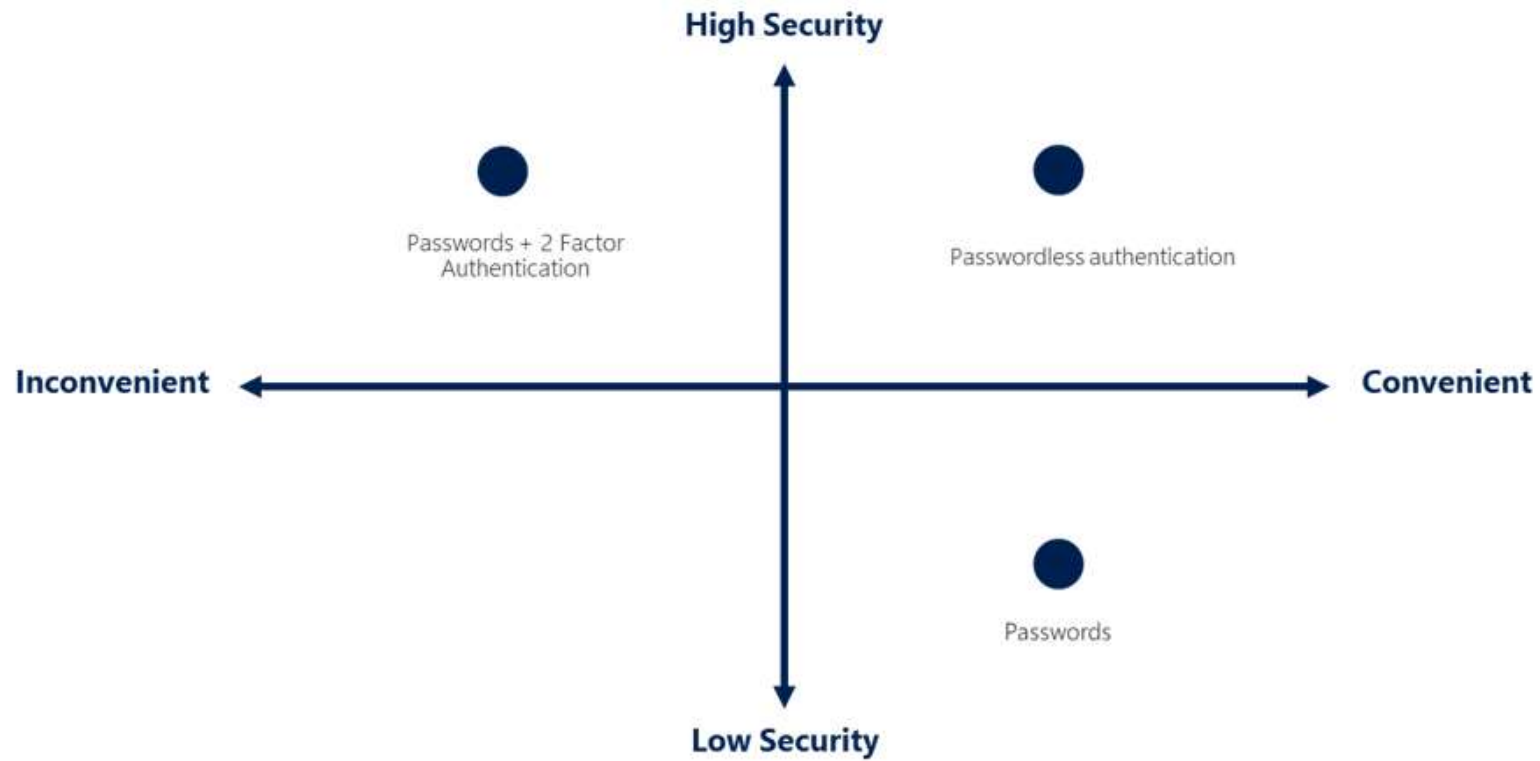
Unusual impersonated activity  
Unusual administrative activity  
Unusual multiple delete VM activity

**Eliminate Password**

**Adopt Passwordless Solutions**



# Passwordless authentication options



# Passwordless foundation

Windows Hello

- ✓ Strong Credentials
- ✓ Registration of Windows Devices

Microsoft Authenticator

- ✓ Authenticator app
- ✓ Registration of Mobile Devices

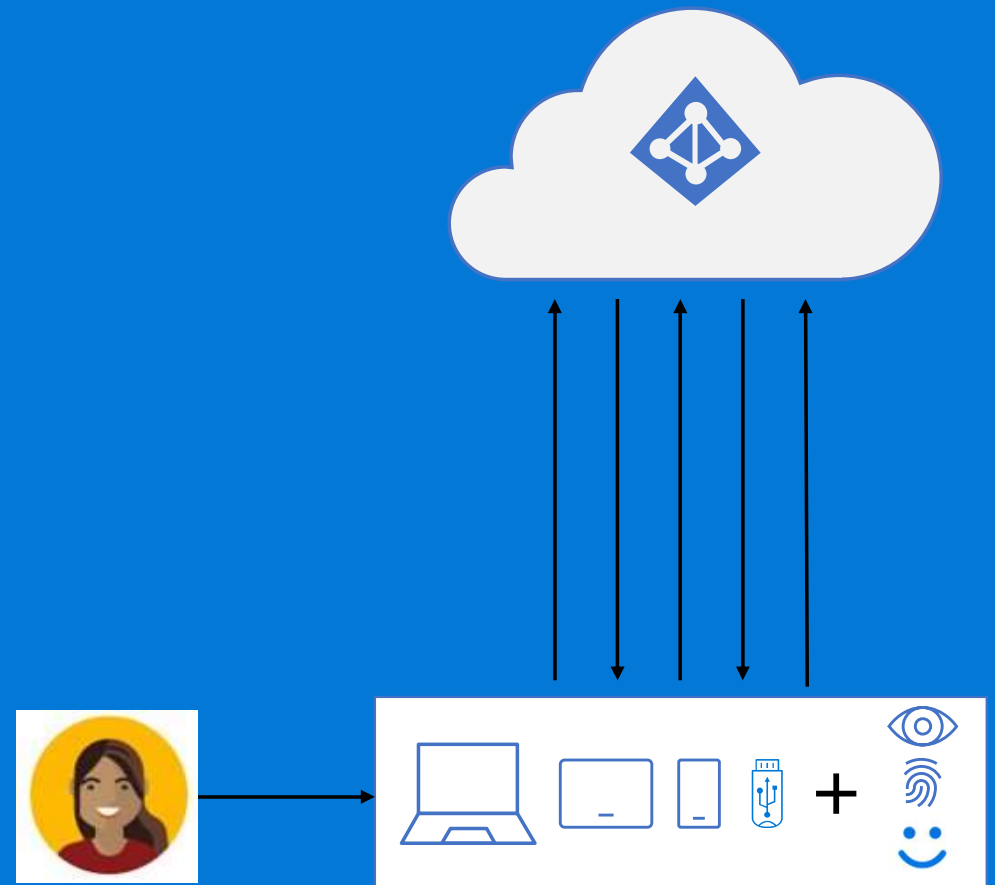
FIDO2 Security Keys

- ✓ Windows 10 Build 1809+
- ✓ Azure AD Joined Devices

# Secure Authentication Flow

A simple, common architecture

- FIDO2: standard based Passwordless authentication
- Based on public-key technology
- Private-keys are securely stored on the device
- Requires a local gesture (e.g., biometric, PIN)
- Private-keys are bound to a single device and never shared



# Windows Hello for Business

Microsoft's premier  
passwordless experience

2016  
Available since

FIDO2  
Certified

9.3K enterprise deployments  
with over 1.7M MAD



# Windows Hello for Business

## Description

Windows Hello for Business replaces passwords with **strong multi-factor authentication** on Windows 10 platforms. This authentication consists of a new type of user credential that's linked to a device and uses a **biometric or PIN**. It lets you sign in with your **face, iris scan, fingerprint, or a PIN**, and enables you to authenticate to enterprise applications, content, and resources **without a password being stored on your device or in a network at all**. The biometric data is only used locally and never leaves the device.

## How it works

The Windows Hello provisioning process generates a cryptographic key pair bound to the **Trusted Platform Module (TPM) on a device**. Access to these keys and obtaining a signature to validate user ownership of the private key is enabled only by the PIN or biometric gesture. Taking place during Windows Hello enrollment, the **two-step verification creates a trusted relationship between the identity provider and the user**. When a user makes the gesture through the device, the provider is able to verify the identity from the combination of Hello keys and the gesture. This activates an authentication token that allows Windows 10 to access resources and services

**3 Deployment Type: Cloud Only, Hybrid, On-Premises**



# Microsoft Authenticator passwordless sign-in

Microsoft's passwordless anywhere solution

2018

Available in public  
preview

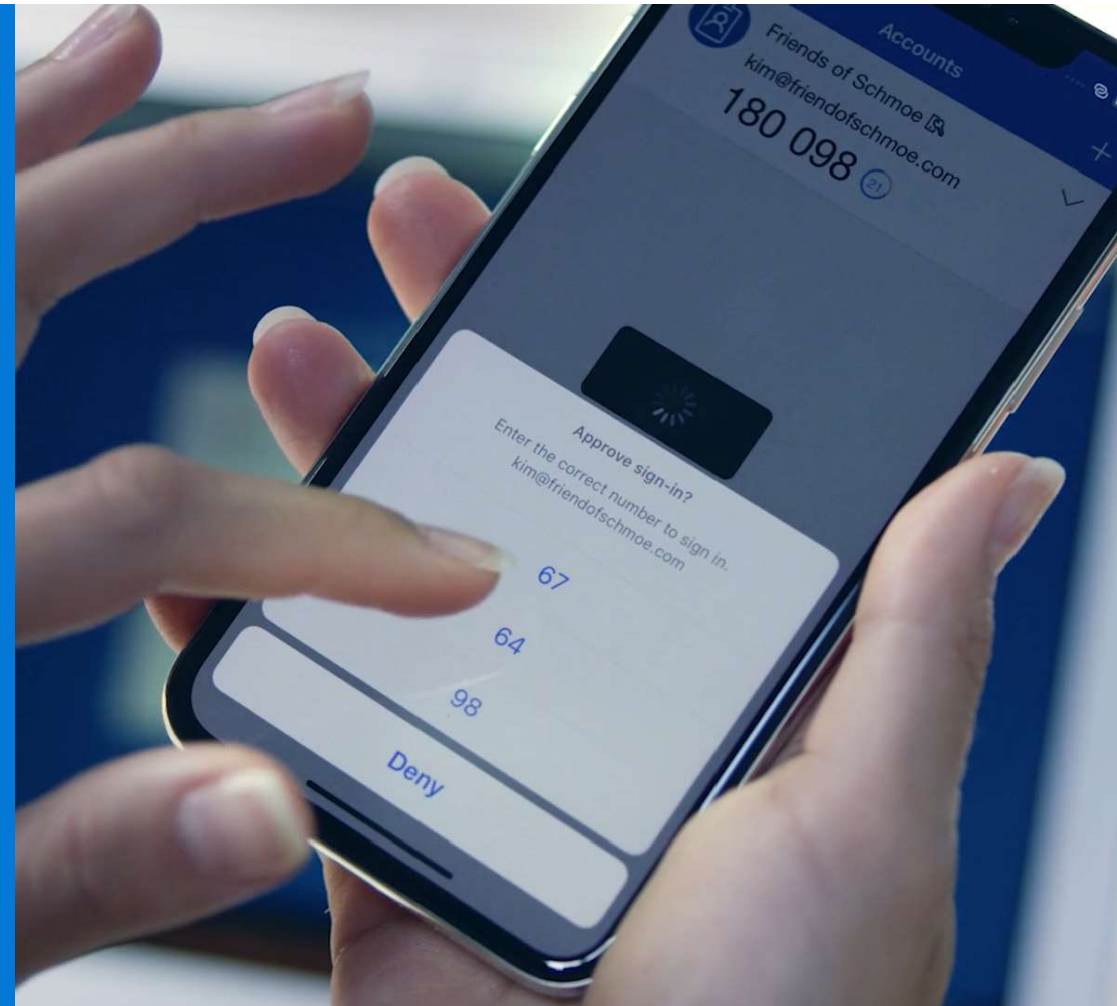
~50K MAU

for passwordless  
sign-in

---

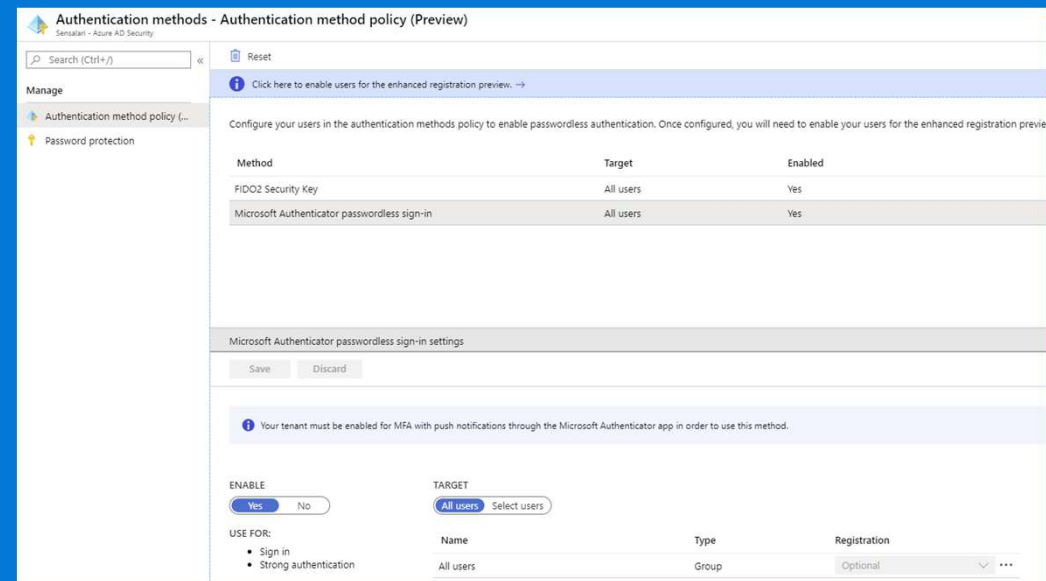
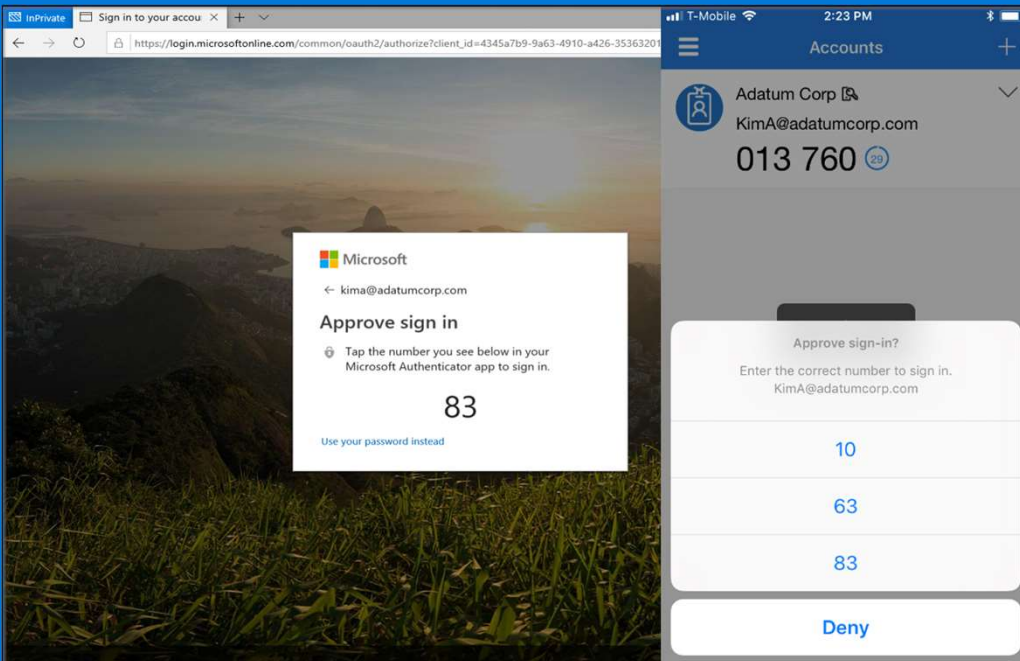
16M+ users of App

50M downloads



# MS Auth App Passwordless

Instead of seeing a prompt for a password after entering a username, a person who has enabled phone sign-in from the Microsoft Authenticator app will see a message telling them to tap a number in their app. In the app, the user must match the number, choose Approve, then provide their PIN or biometric, then the authentication will complete.



# FIDO2 security keys

Microsoft's passwordless solution for shared devices

Currently only for Azure AD Joined devices

July 2019

Available in public  
preview

750+

enterprises  
expressed interest

---

2K+ tenants have enabled  
feature and registered keys



# Passwordless with FIDO2 security keys

Open standards that allow innovative offerings from partners, serving broad range of user needs

USB/NFC Key



USB Biometric Key

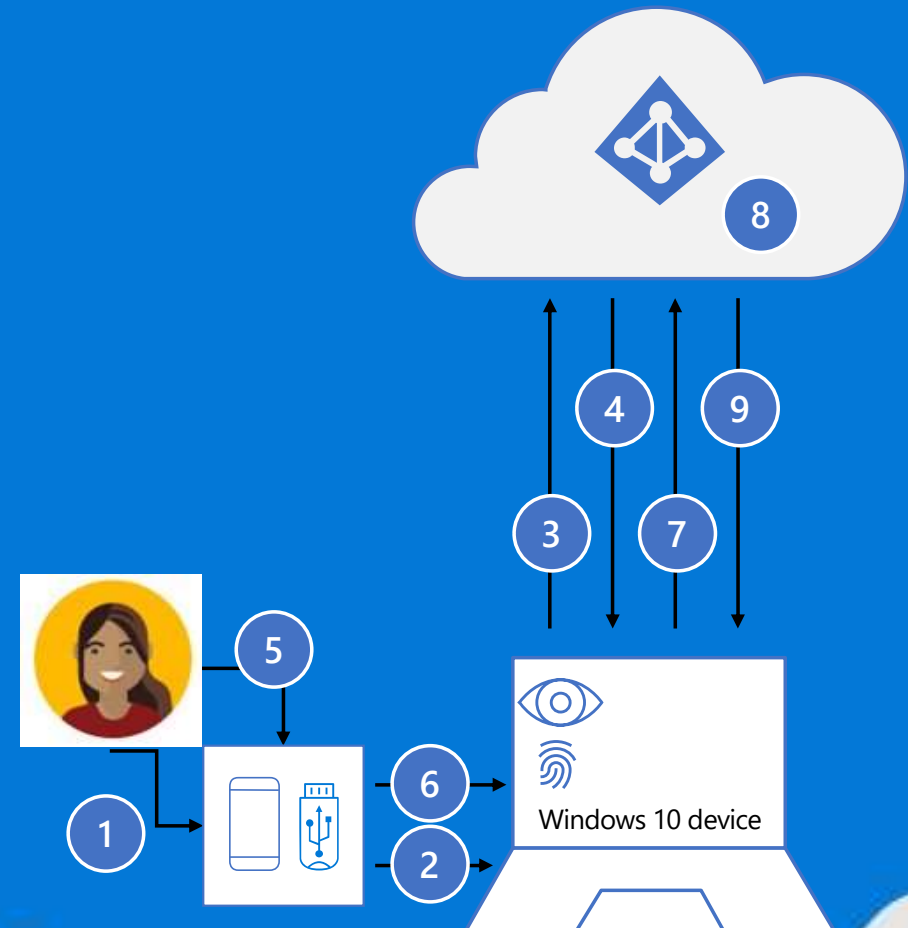


NFC Badge



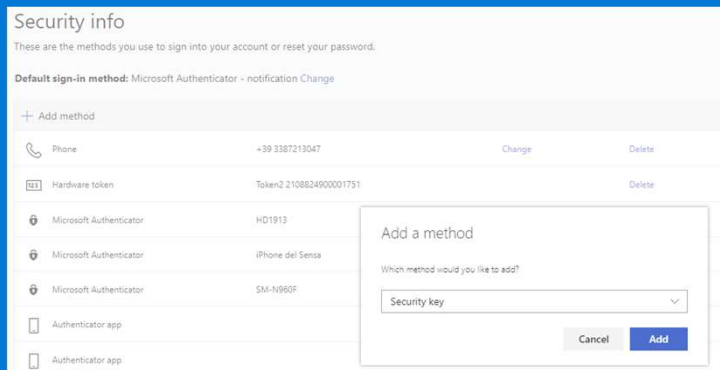
# Strong Authentication with FIDO2 security key

- 1 User plugs FIDO2 security key into computer
- 2 Windows detects FIDO2 security key
- 3 Windows device sends auth request
- 4 Azure AD sends back nonce
- 5 User completes gesture to unlock private key stored in security key's secure enclave
- 6 FIDO2 security key signs nonce with private key
- 7 PRT token request with signed nonce is sent to Azure AD
- 8 Azure AD verifies FIDO key signature
- 9 Azure AD returns PRT to enable access to cloud resources

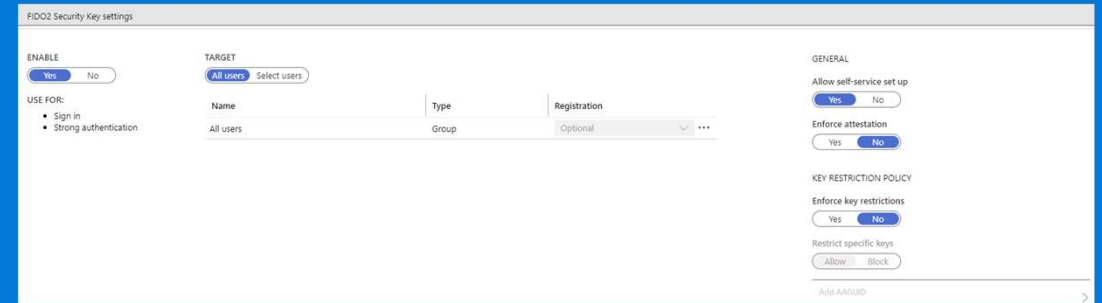


# Enable password-less sign-in with security keys

## Step 1- Configure the authentication method



## Step 3 - Configure security keys as a sign-in option



## Step 2 -Register security key as sign-in method (require Combined security information registration )

1. Open the Azure portal and navigate to **Microsoft Intune > Device configuration > Profiles** to open the **Devices configuration - Profiles** blade
2. On the **Devices configuration - Profiles** blade, click **Create profile** to open the **Create profile** blade
3. On the **Create profile** blade, provide the following information and click **Create**
  - **Name:** Provide a valid name
  - **Description:** (Optional) Provide a valid description
  - **Platform:** Windows 10 and later
  - **Profile type:** Identity protection
  - **Settings:** See step 4
4. On the **Windows Hello for Business** blade, select **Enable** with **Use security keys for sign-in** and click **OK**;



This setting requires Windows 10, version 1903, or later, and is not dependent on configuring Windows Hello for Business

# Upcoming

FIDO2 public preview expanding to Hybrid environments  
(Early 2020)

What will be included?



Passwordless sign-in using  
FIDO2 security keys

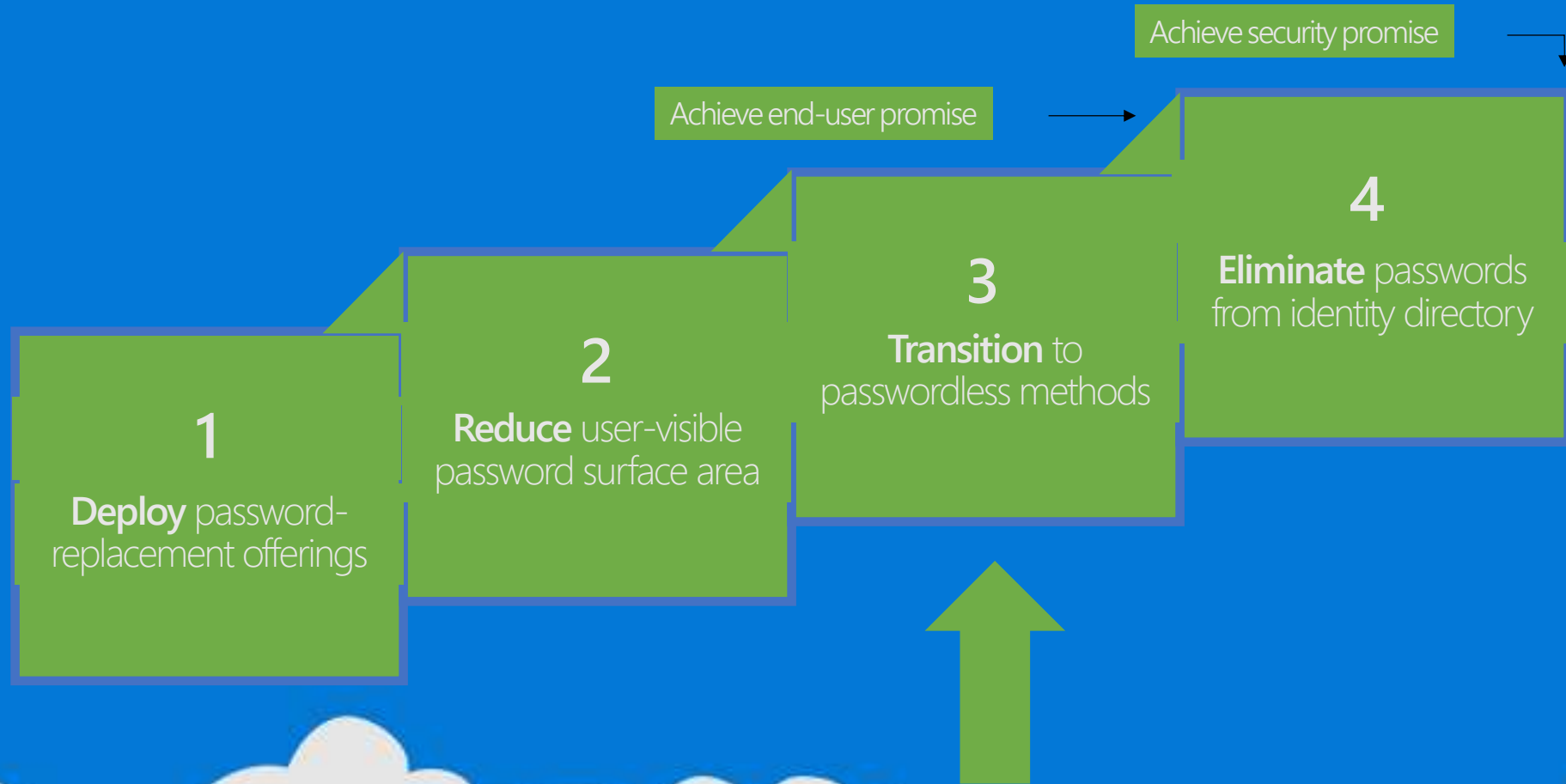


- Azure Active Directory Joined  
(AADJ)  
- Hybrid AADJ Windows 10  
devices



Seamless SSO to Cloud and on-  
premises resources

# Microsoft Passwordless Journey

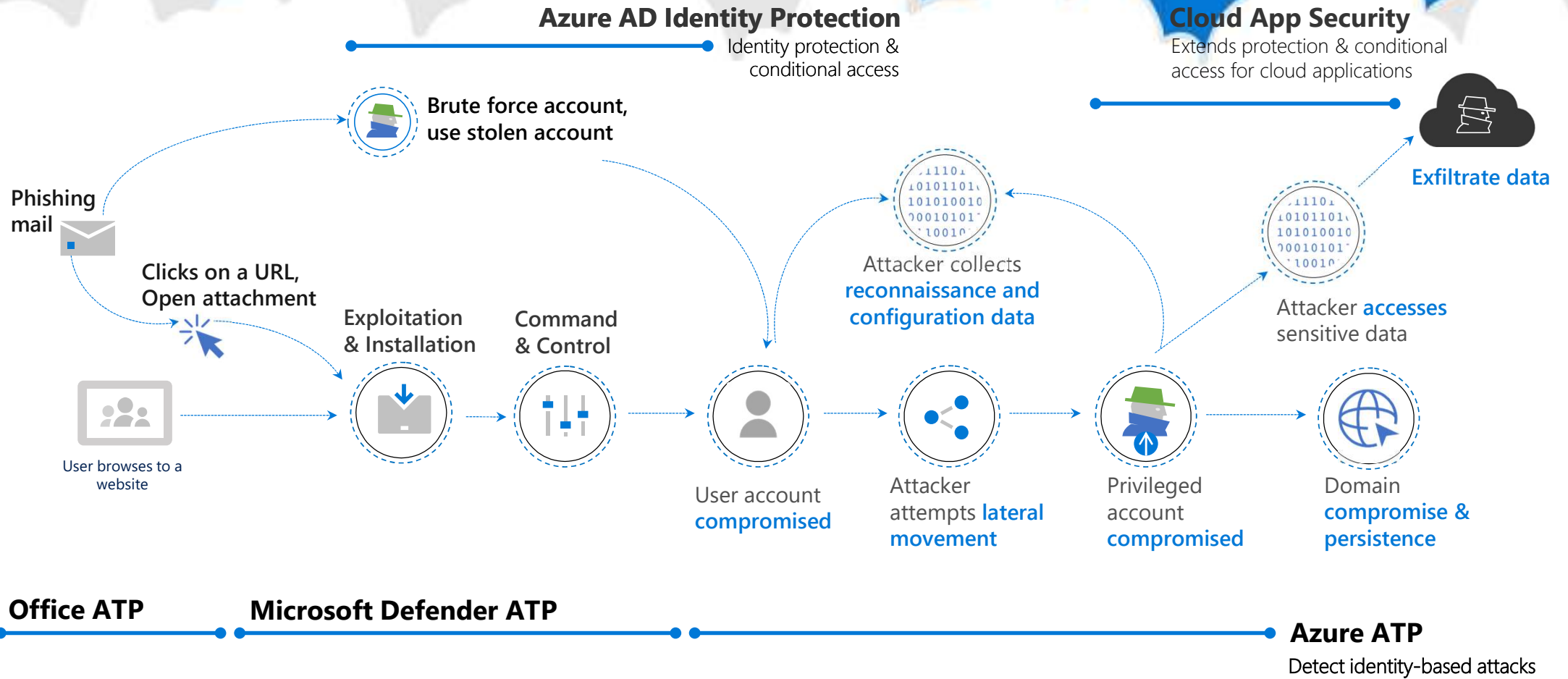




# Protect, Detect and Responde



# Maximize detection during attack stages



# Empower your defenders with Azure ATP

## PREVENT

### Improve Security Posture

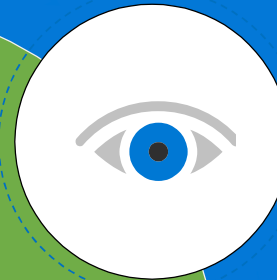
Automate updates and configuration



## DETECT

### More Visibility, Less Alerts

Focus on what's important and reduce noise

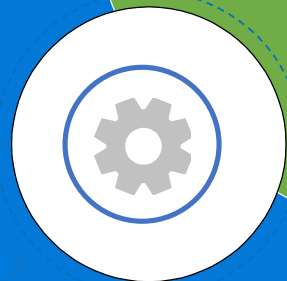


Cloud Scale,  
Continuous Updates

## RESPOND

### Reduce Mean Time To Response

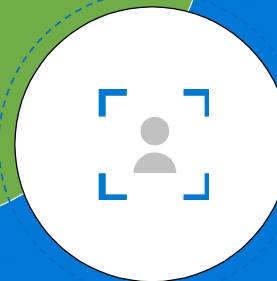
Automate responses and integrate with existing tools



## INVESTIGATE

### Uncover Complex Threats

Understand the entire attack and Identify Suspicious users



# Azure ATP Data Sources and Technologies

## NETWORK TRAFFIC ANALYTICS

Inspect network traffic:  
NTLM, Kerberos, LDAP,  
RPC, DNS, SMB

## SECURITY EVENTS & ACTIVE DIRECTORY DATA

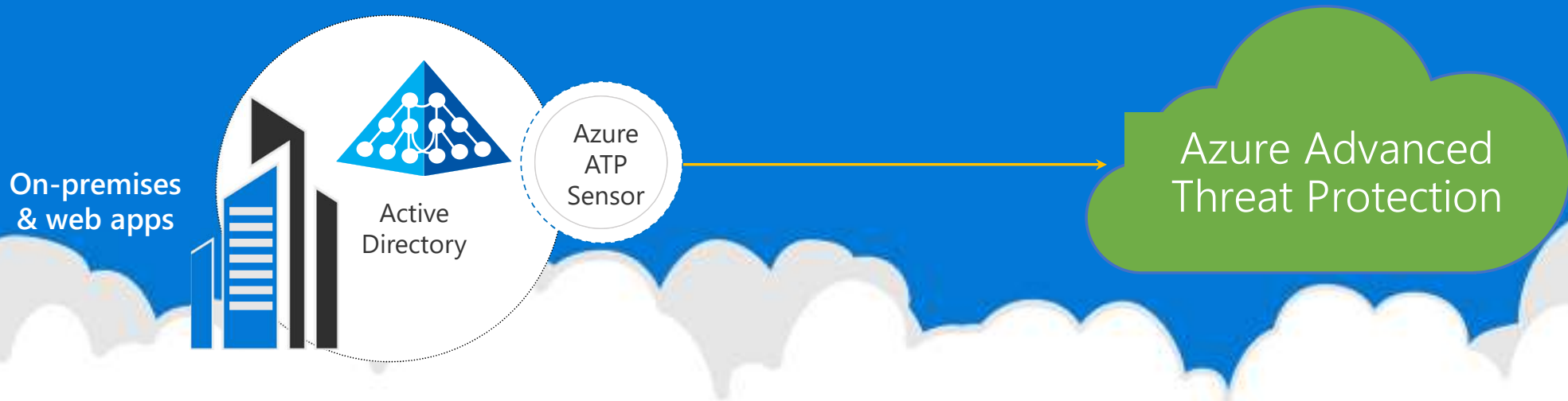
Inspect events, event  
tracing and profile active  
directory entities

## USER BEHAVIOR ANALYTICS

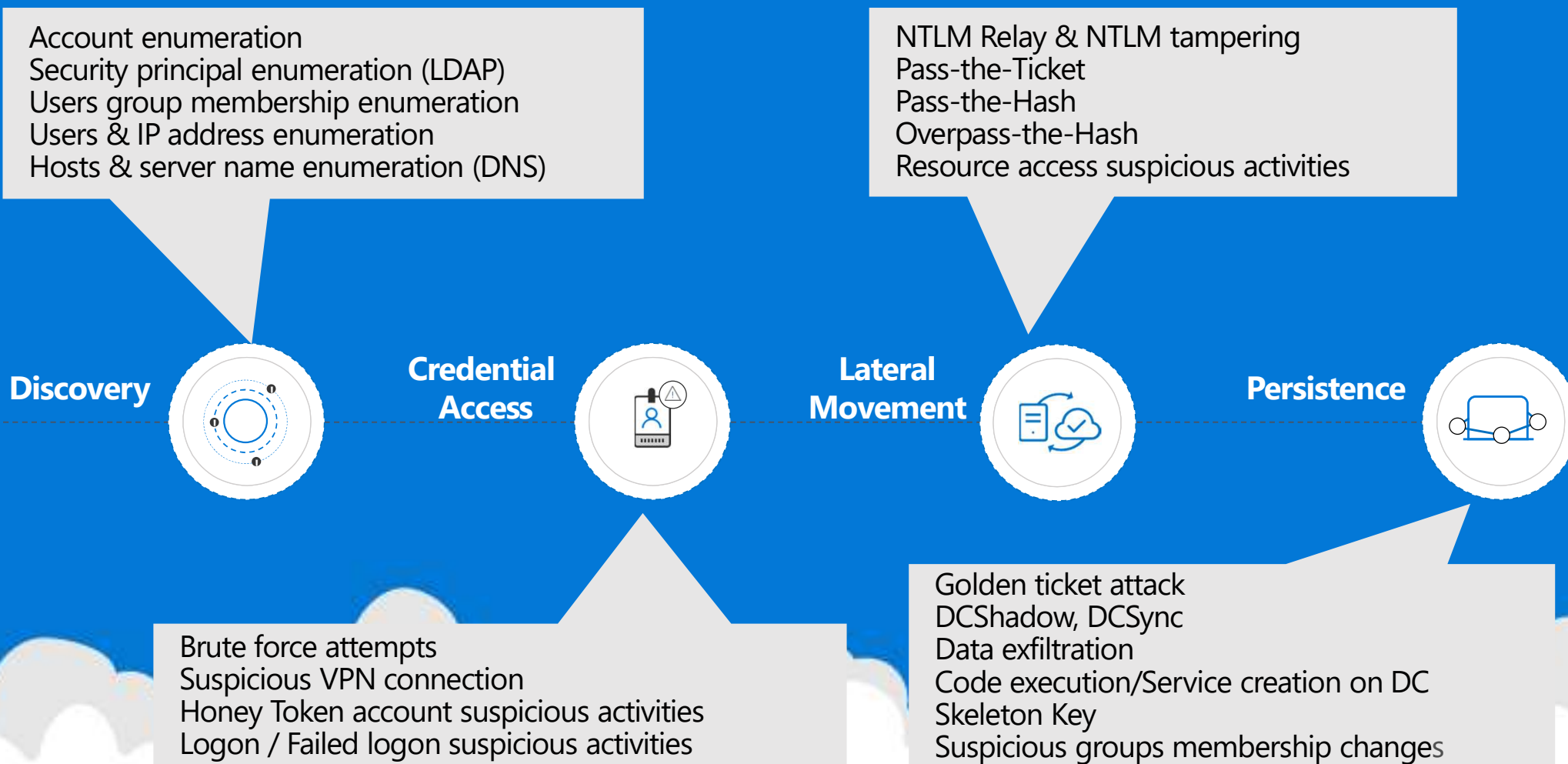
Profile users & entities  
behavior, identify  
behavior anomalies

## CLOUD BASED REAL-TIME DETECTIONS

Data enrichment and  
correlation in the cloud, for  
real time detections



# Detect identity-based attacks throughout the kill chain



# Azure ATP & Hybrid Environments

## Azure ATP

Protect, detect, investigate and respond to compromised users and lateral movements in **On-premises environments**



## Microsoft Cloud App Security & Azure AD Identity Protection

A complete identity protection for the **hybrid organization**.

# Extend Detections across cloud apps with Microsoft Cloud App Security and Azure AD Identity Protection

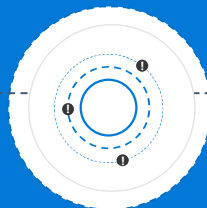
Users with leaked credentials  
Activity from suspicious IP addresses  
Activity from anonymous IP addresses  
Activity from an infrequent country  
Impossible travel between sessions  
Logon from a suspicious user agent

Unusual file share activity  
Unusual file download  
Unusual file deletion activity  
Ransomware activity  
Data exfiltration to unsanctioned apps  
Activity by a terminated employee

Compromised session



Threat delivery and persistence



Malicious use of an end-user account



Malicious use of a privileged user



Malware implanted in cloud apps  
Malicious OAuth application  
Multiple failed login attempts to app  
Suspicious inbox rules (delete, forward)

Unusual impersonated activity  
Unusual administrative activity  
Unusual multiple delete VM activity

# Alerts investigation & management

Alerts

RESOLUTION STATUS: OPEN, DISMISSED, RESOLVED

CATEGORY: Select risk category...

SEVERITY: [Yellow] [Orange] [Red]

APP: Select apps...

USER NAME: Jeff Leatherman (jeffv@igniteaat...)

POLICY: Select policy...

Advanced

1 - 10 of 10 alerts

Alert	Resolution	Severity	Date
Risky sign-in: Anonymous IP address 197.231.221.211 LR Jeff Leatherman	Microsoft Azure OPEN	Medium	6 days ago
Suspicious VPN connection Jeff Leatherman	OPEN	Medium	2 months ago
Abnormal access to protected data 84.59.125.30 Jeff Leatherman			2 months ago
Suspicious inbox forwarding 185.220.101.45 Jeff Leatherman	Microsoft Excha... OPEN	Medium	2 months ago
Risky sign-in: Unfamiliar sign-in properties DE 185.220.102.6 Jeff Leatherman			2 months ago
Leaked credentials Jeff Leatherman	OPEN	High	2 months ago

On-Premises (source: Azure ATP)

Cloud (source: Microsoft Cloud App Security)

Cloud (source: Azure AD Identity Protection)



# Hunting – based on user activity log

Activity log Investigate in Web traffic log

QUERIES: Select a query...  
APP: Select apps...  
USER NAME: Jeff Leatherman (jeffl@mcast...)  
RAW IP ADDRESS: Enter IP address...  
ACTIVITY TYPE: Select activity...  
LOCATION: Select countries/regions...  
Save as Advanced

1 - 20 of 76 activities New policy from search Filter Download View

Activity	User	App	IP address	Location	Device	Date
Run command: SAMR query QueryUser user Jeff Leather...	Jeff Leatherman	Active Directory	10.0.8.7	—	Jeff-DSK	Mar 6, 2019, 6:02 AM
Access file: file https://mcastest9.sharepoint.com/sites/Dr...	Jeff Leatherman (jeffl@mcastest9.onmicr...	Microsoft ShareP...	5.29.115.84	—	—	—
WACTokenShared	Jeff Leatherman (jeffl@mcastest9.onmicr...	Microsoft ShareP...	5.29.115.84	Israel	Windows	Mar 5, 2019, 11:59 PM
Log on	Jeff Leatherman	Active Directory	10.0.8.8	—	Financeserv53	Mar 5, 2019, 11:59 PM
Credentials validation	Jeff Leatherman	Active Directory	N/A	—	—	—
Add member to group: user jeffl@mcastest9.onmicrosoft...	Jeff Leatherman	Office 365	N/A	—	—	Mar 5, 2019, 11:59 PM
Add member to group: user jeffl@mcastest9.onmicrosoft...	Jeff Leatherman	Office 365	N/A	—	—	Mar 5, 2019, 11:59 PM
MemberAdded: user jeffl@mcastest9.onmicrosoft.com	Jeff Leatherman	Microsoft Teams	N/A	—	—	Mar 5, 2019, 11:59 PM
Log on	Jeff Leatherman	Microsoft Teams	5.29.115.84	Israel	Windows	Mar 5, 2019, 11:53 PM

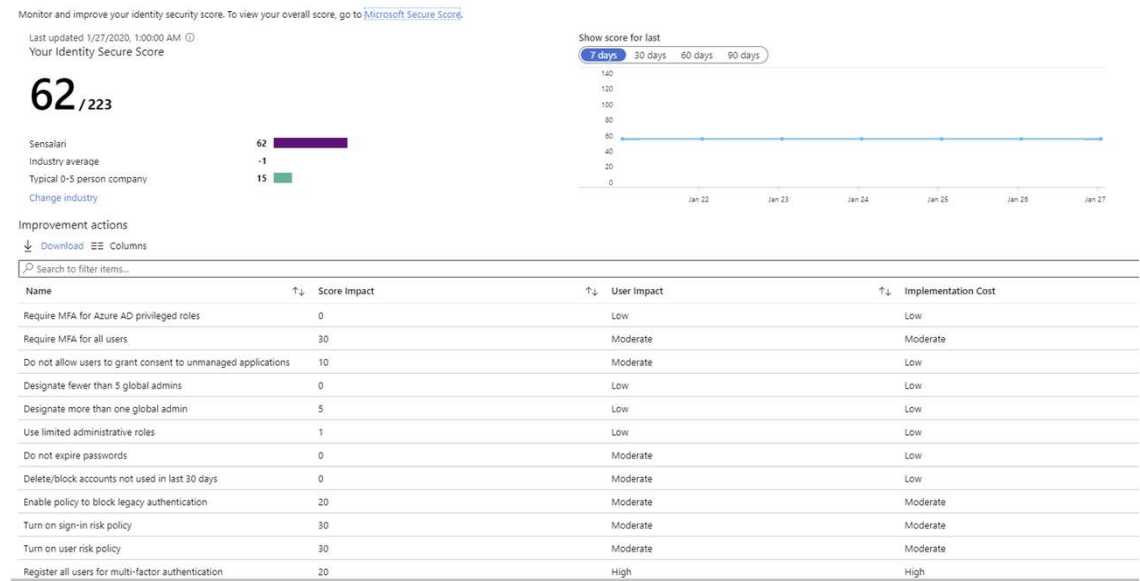
**On-Premises (source: Azure ATP)** (points to the 'Access file' and 'WACTokenShared' rows)

**Cloud (source: Microsoft Cloud App Security)** (points to the 'Log on' and 'Add member to group' rows)

# Azure AD Identity Score

The identity secure score is number between 1 and 223 that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security. Each improvement action in identity secure score is tailored to your specific configuration.

- The score helps you to:
  - Objectively measure your identity security posture
  - Plan identity security improvements
  - Review the success of your improvements
- Every 48 hours, Azure looks at your security configuration and compares your settings with the recommended best practices.



# Reducing number of global admins

1. Understand what permissions are needed
2. Identify the appropriate Azure AD RBAC role
3. Move user to one of 50+ built-in roles **or build you own!**

Application Administrator

Application Developer

Azure DevOps Administrator

Global Reader

Helpdesk Administrator

Billing Administrator

Compliance Administrator

Privileged Authentication Administrator

Exchange Administrator

Reports Reader

Authentication Administrator

Conditional Access Administrator

Azure Information Protection Administrator

+ 35 built-in!

**Custom Role**

# Privileged Identity Management

Require Premium P2 edition or M365 E5

Discover, restrict, and monitor privileged identities

Enforce on-demand, just-in-time administrative access when needed

Manage access to resources in Azure AD, Azure Resources (Preview), and other Microsoft Online Services like Office 365 or Microsoft Intune

Provides more visibility through alerts, audit reports and access reviews



Global Administrator



Billing Administrator



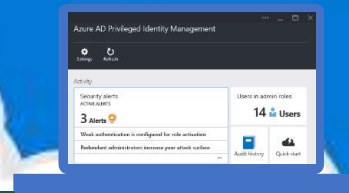
Exchange Administrator



User Administrator



Password Administrator



# Privileged Identity Management benefits

Reduces exposure to attacks targeting admins

Removes unneeded permanent admin role assignments

Limits the time a user has admin privileges

Ensures MFA validation prior to admin role activation

Simplifies delegation

Separates role administration from other tasks

Adds roles for read-only views of reports and history

Asks users to review and justify continued need for admin role

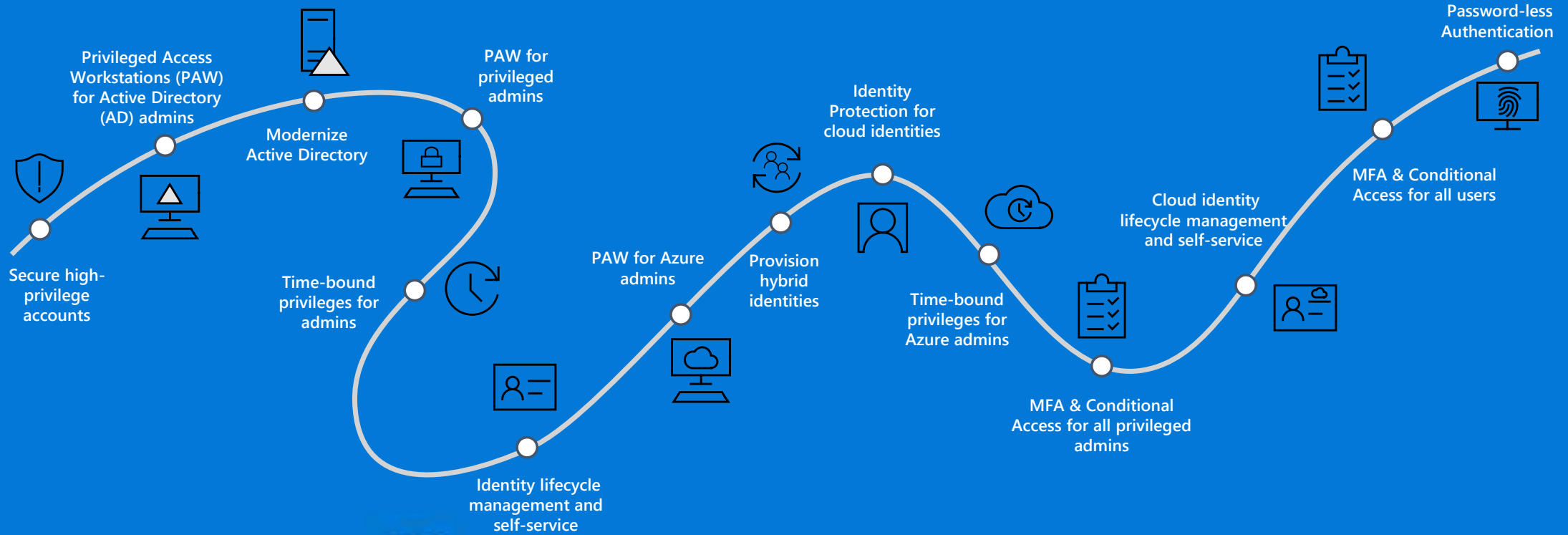
Increases visibility and finer-grained control

Enables least privilege role assignments

Alerts on users who haven't used their role assignments

Simplifies reporting on admin activity

# Modern Identity Journey



GRAZIE!

