



1st AID for EID

How to prevent lateral movement to Entra ID
when your Active Directory has fallen

Christopher Brumm
Engaged Speaker and Entra Fan

Agenda

- Who is Chris?
- Why should I care?
- What should I do?
 - To prevent Full Compromise of Entra ID?
 - To protect my user accounts in Entra ID?
- How can I prepare myself?

Christopher Brumm

Cyber Security Architect @ glueckkanja AG

- ✕ @cbrhh
- in /in/christopherbrumm
- 🏠 chris-brumm.medium.com
- 🏢 www.glueckkanja.com



Okay let's assume a situation where your Active Directory is compromised

Hopefully you have deployed good defense tools like

- Microsoft Defender for Identity
 - > to detect AD based threats
- Microsoft Defender for Endpoint
 - > to detect OS based threats and contain systems

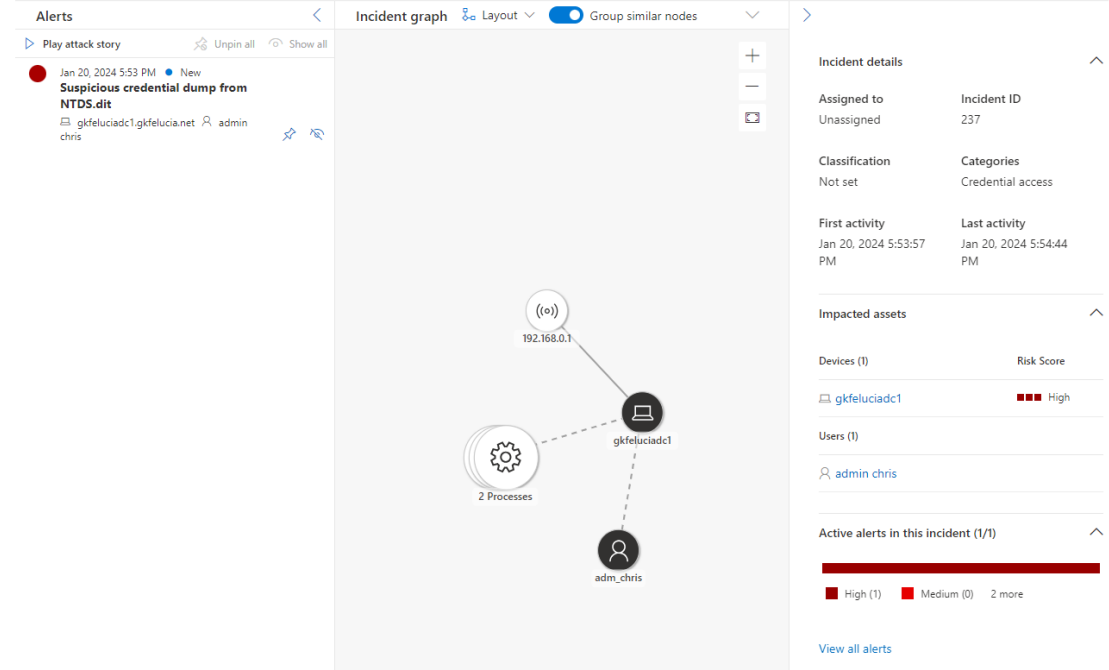
and hopefully you've managed already to isolate the suspicious systems.

Independent from that: If the attacker had a Domain Admin account or something similar **you have a problem and need to contain this Active Directory.**

Suspicious credential dump from NTDS.dit on one endpoint

High Active Unassigned MDE-Management

Attack story Alerts (1) Assets (2) Investigations (0) Evidence and Response (4) Summary



But wait! Is this really a realistic scenario?

Attackers are focussing (currently) on OnPrem environments

It is easier to attack and much harder to protect

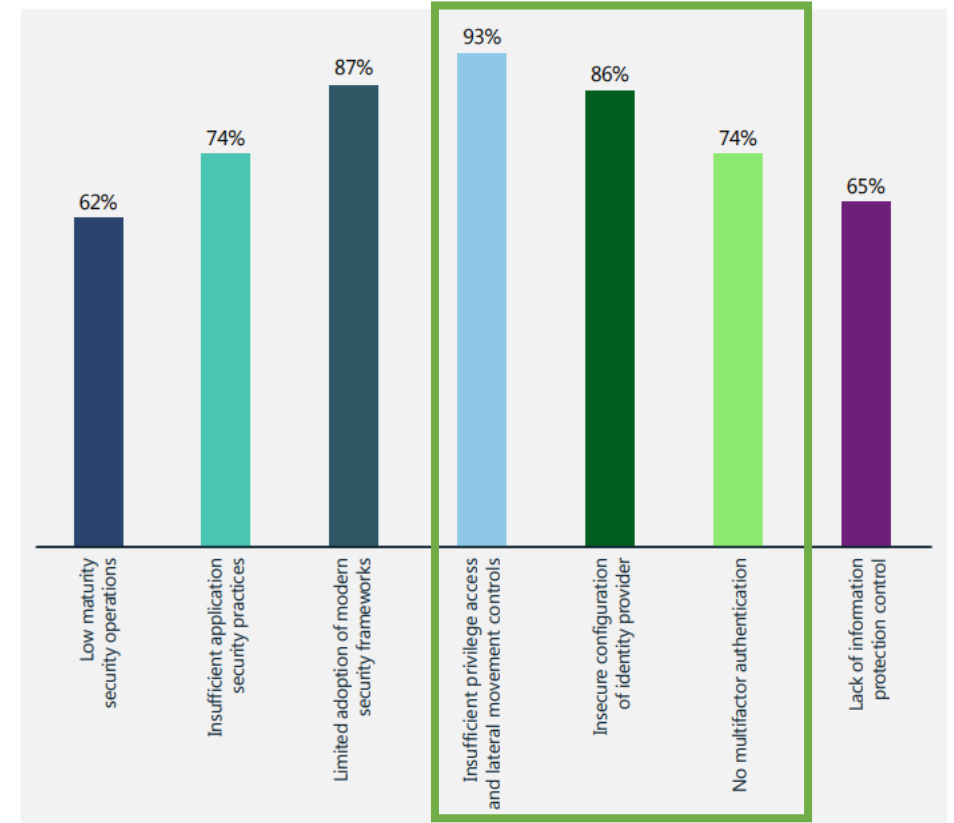
Human-operated ransomware has raised by more than 200% *

Almost every (bigger) company using Entra ID has a hybrid identity environment.

This means:
AD DS is connected via Entra ID Connect

And it means:
There are multiple lateral movement pathes to Entra ID

Summary of most common findings in ransomware response engagements



The most common finding among ransomware incident response engagements was insufficient privilege access and lateral movement controls.

The biggest threat to Entra ID is the connected Active Directory

*Regarding the Microsoft Digital Defense Report 2023

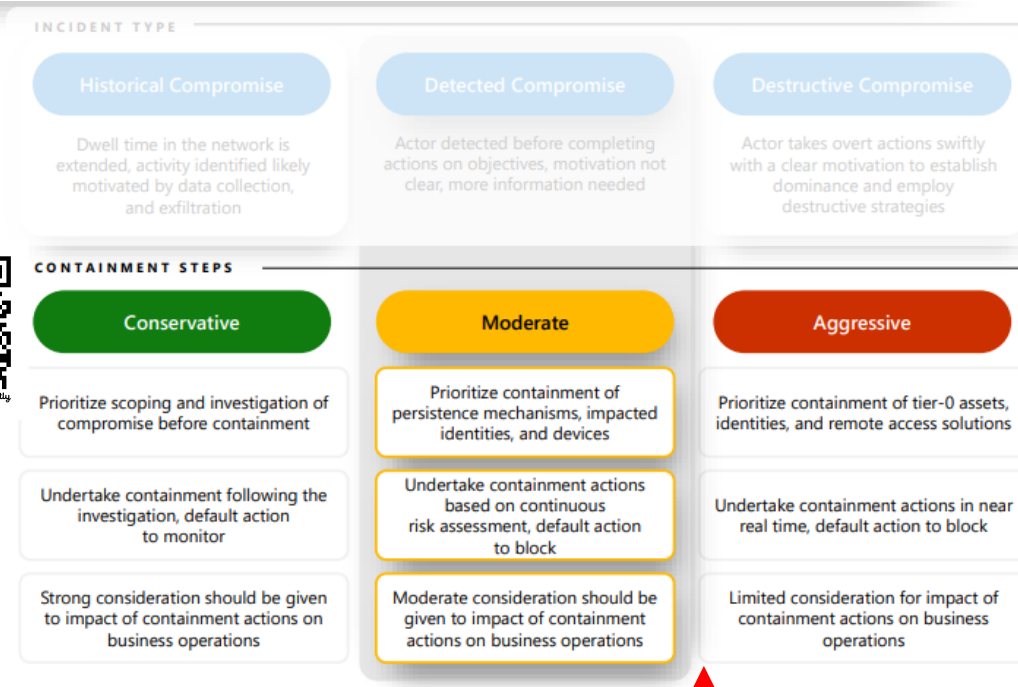
What is important now?

Containment is important!

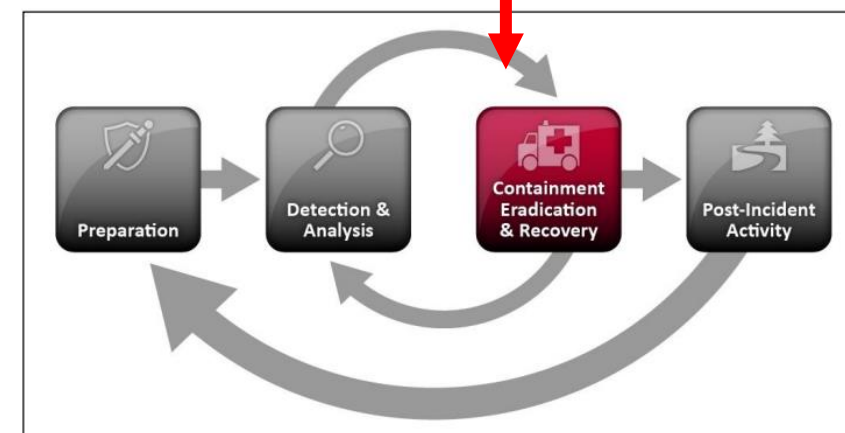
Active Directory plays a central role in many environments and there are various ways for attackers to expand their influence.

From a defender's point of view, I suggest severing the following connections for containment:

- Connections to other forests and partners
- Connections to the OT environment
- Connections to the backup system
- Connections to Entra ID



We are here!

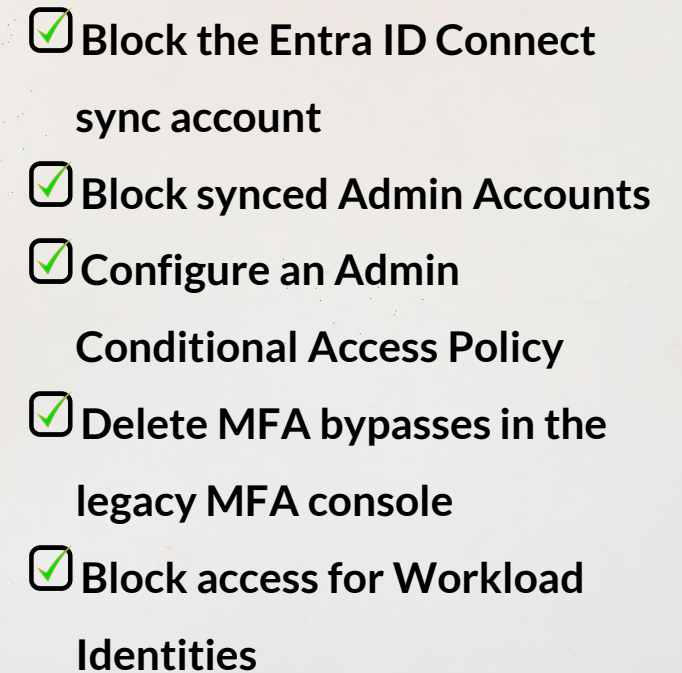


To Do List

1. Prevent full compromise of Entra ID
2. Protect User Accounts in Entra ID
3. search for traces of attackers and establish security monitoring in Entra ID
4. Continue hardening of Entra ID

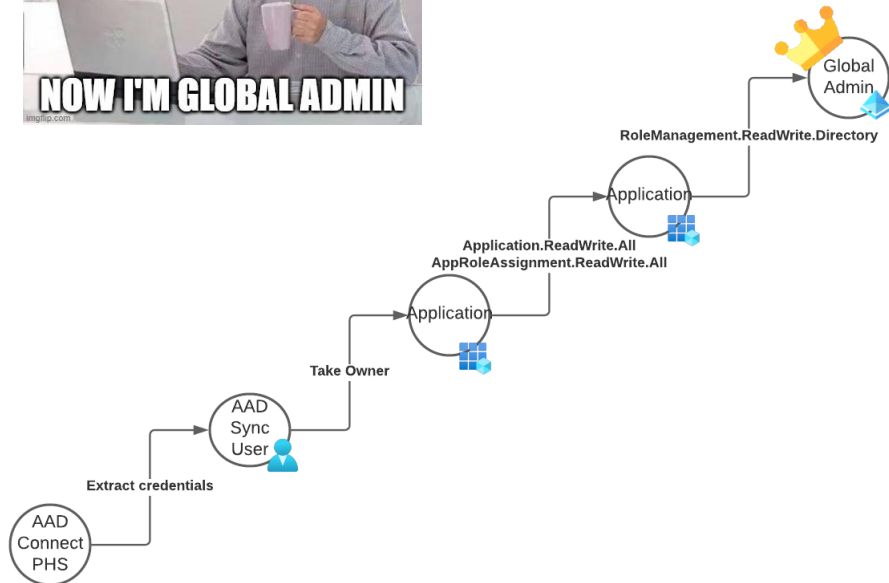
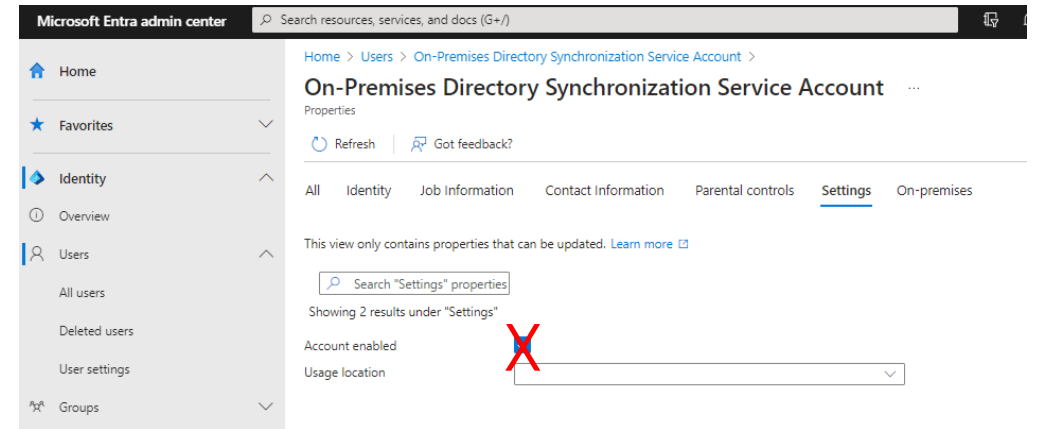


Prevent full compromise of Entra ID

- 
- ☒ Block the Entra ID Connect sync account
 - ☒ Block synced Admin Accounts
 - ☒ Configure an Admin Conditional Access Policy
 - ☒ Delete MFA bypasses in the legacy MFA console
 - ☒ Block access for Workload Identities

Block the Entra ID Connect sync account

Fabian







More details on this

Fabian Bader
From on-prem to Global Admin
without password reset



Let's take care for the Admins!

	ADMIN ACCOUNT
	+ MFA + SIGN-IN FREQ.
	+ DEVICE COMPLIANCE ENFORCEMENT
	+ FIDO/WH4B + PAW ENFORCEMENT



Demo – find and handle synced accounts

More details on this

Thomas Naunheim
Blog



Conditional Access and MFA for Admins!

Minimum Admin Policy

Use the Conditional Access [template Require MFA for administrators](#)

Please add session controls!

And you want to extend the scoped roles in the template to all privileged roles

-> see [this table](#)

Session ×

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

☐ Use app enforced restrictions ⓘ

ⓘ This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. [Learn more](#)

☐ Use Conditional Access App Control ⓘ

☒ Sign-in frequency ⓘ

☒ Periodic reauthentication

10 ✓

Hours ▼

☐ Every time

☒ Persistent browser session ⓘ

Persistent browser session

Never persistent ▼

MFA Hardening

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

no entries!

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

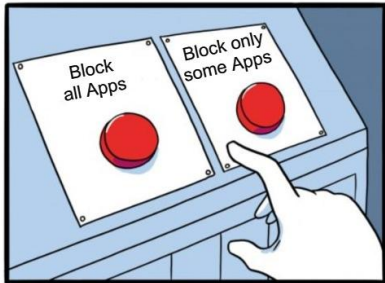
- Methods available to users:
- ☐ Call to phone
- ☐ Text message to phone
- ☒ Notification through mobile app
- ☒ Verification code from mobile app or hardware token

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

- ☐ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)
- Number of days users can trust devices for 90

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. [Learn more about reauthentication prompts.](#)

Handling Workload Identities



„I don't have detailed insights on the permissions of all of my Workload Identities.“

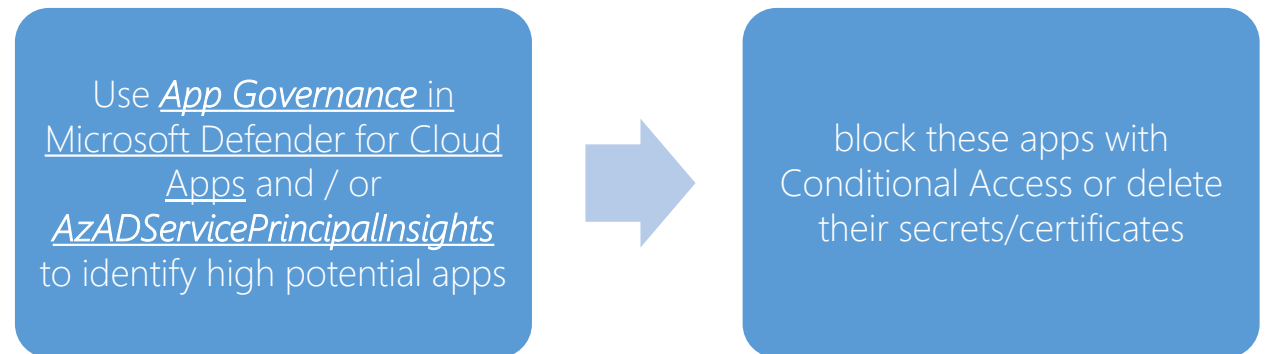


„I know the apps and their identities in my environment and I'm familiar with the tooling“

The aggressive approach



The moderate approach



Workload Identity Permissions

More details on this

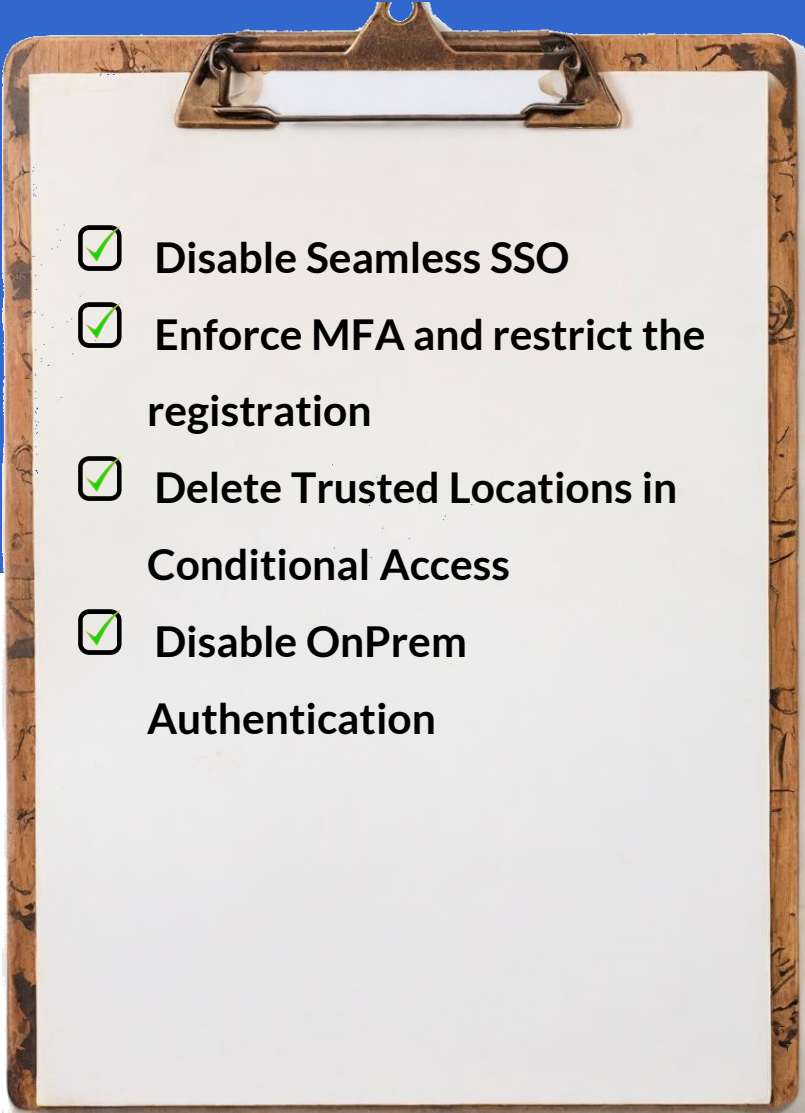
App Governance
in Microsoft Defender for
Cloud Apps



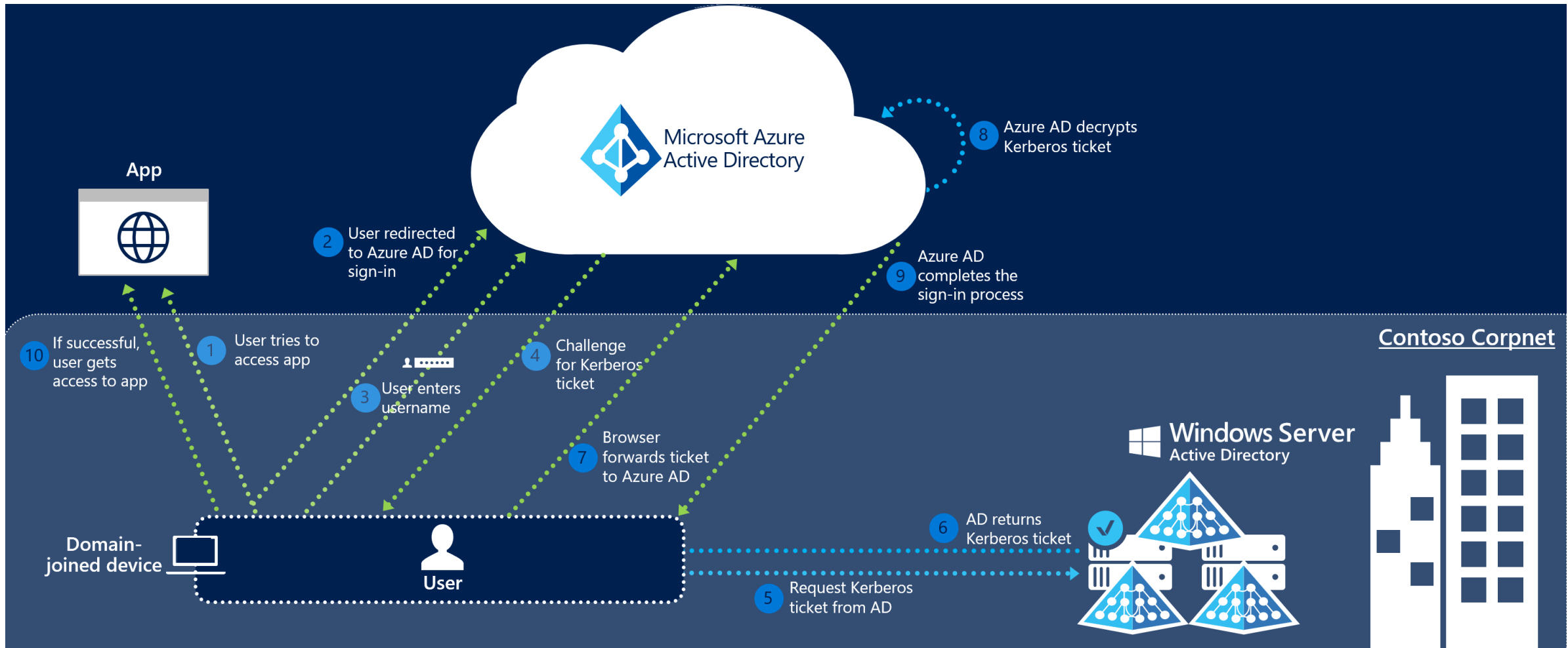
AzADServicePrincipalInsights
by Julian Hayward



Protect User Accounts in Entra ID

- 
- ☒ Disable Seamless SSO
 - ☒ Enforce MFA and restrict the registration
 - ☒ Delete Trusted Locations in Conditional Access
 - ☒ Disable OnPrem Authentication

The problem with Seamless SSO



Demo: SSSO and AADInternals

More details on this

Dr. Nestori Syynimaa
Unnoticed sidekick: Getting
access to cloud as an on-
prem admin



Dirk-jan Mollema
I'm in your cloud, reading
everyone's emails - hacking
Azure AD via Active Directory



How much time do I have?

- Active Directory has no built-in feature to ensure random generated or „hard-to-guess“ passwords
- All not random generated passwords can be seen as instantly breached.
- Bonus: In most environments (especially in those in incidents) there are still a lot of old protocols and algorithms active...

Consider all your passwords as breached and focus on MFA!

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

 [Learn how we made this table at hivesystems.io/password](https://hivesystems.io/password)

MFA Enforcement + Registration

Grant

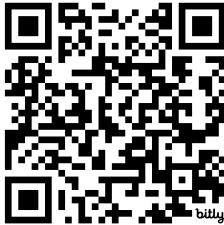
Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multifactor authentication

Consider using the CA templates



Select what this policy applies to

User actions

Select the action this policy will apply to

☒ Register security information

☐ Register or join devices

☒ Create a dedicated CA policy to enforce MFA

☒ Exclude only the Breakglass Account

☒ Don't exclude trusted locations!

☒ Create a dedicated CA policy for the User Action

☒ Enforce Trusted Device or MFA

☒ Use TAP for onboarding

Disable OnPrem Authentication

Active Directory Federation Services

```
#Install required module
Install-Module Microsoft.Graph -Scope CurrentUser

# Get a Token
Connect-MGGraph -Scopes "Domain.ReadWrite.All", "Directory.AccessAsUser.All"

# Check Status
Get-MgDomain -DomainId yourdomain.com

# Migrate to Managed
Update-MgDomain -DomainId <domain name> -AuthenticationType "Managed"

# Check Status
Get-MgDomain -DomainId yourdomain.com
```



Pass Through Authentication

```
# Install and Import the module
Install-Module AADInternals
Import-Module AADInternals

# Get a Token (as Global Admin or Hybrid Auth Admin)
$pt=Get-AADIntAccessTokenForPTA -UseDeviceCode

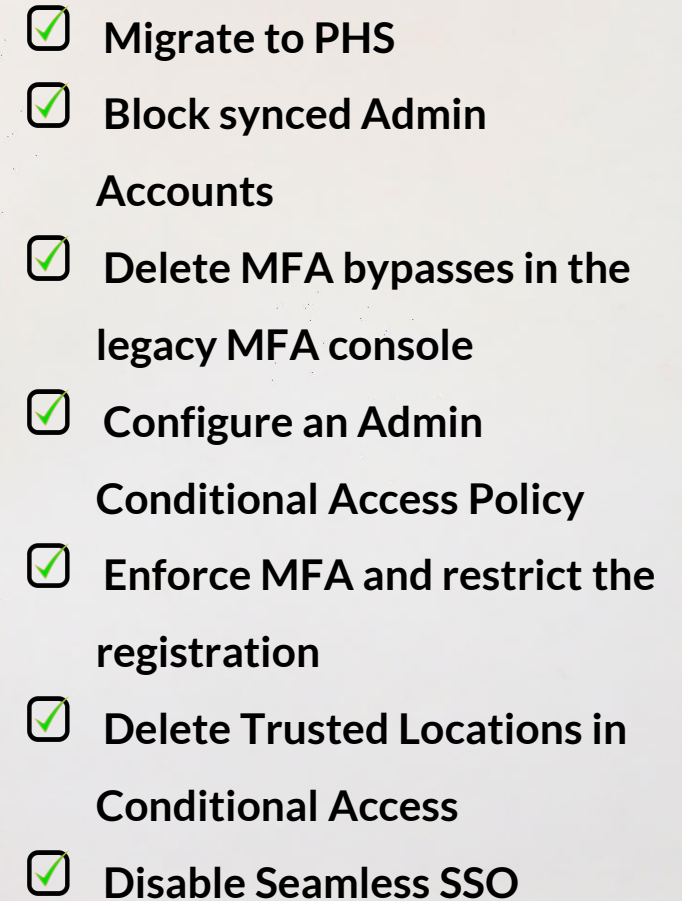
# Disable PTA
Set-AADIntPassThroughAuthenticationEnabled -AccessToken $pt -Enable $false
```



There is no glory in prevention!

Christian Drosten, Virologist, March 2020

Things you should prepare today

- 
- ☒ Migrate to PHS
 - ☒ Block synced Admin Accounts
 - ☒ Delete MFA bypasses in the legacy MFA console
 - ☒ Configure an Admin Conditional Access Policy
 - ☒ Enforce MFA and restrict the registration
 - ☒ Delete Trusted Locations in Conditional Access
 - ☒ Disable Seamless SSO

Sponsors



Vielen Dank für's Zuhören!
