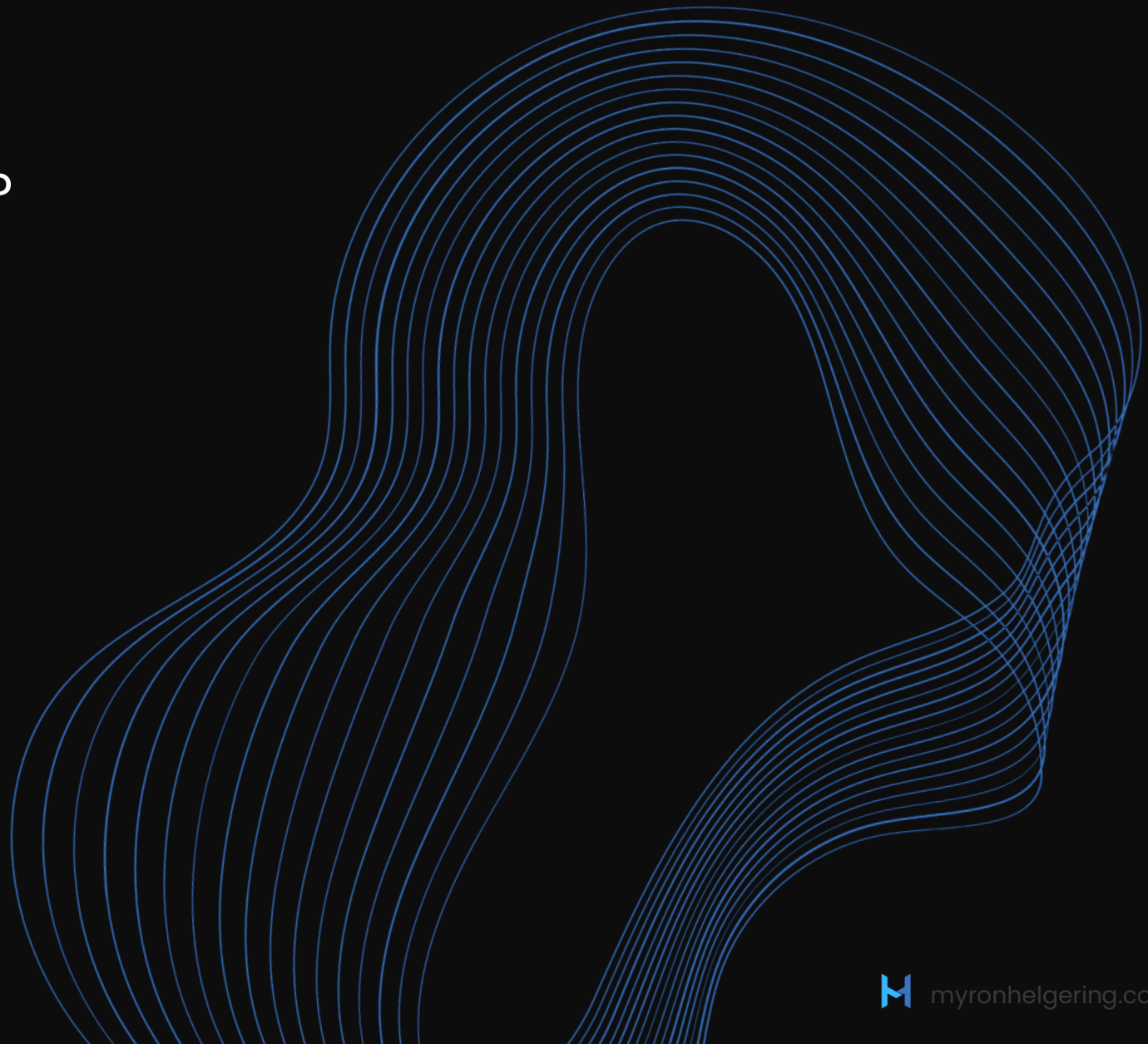
SESSION

7 Methods to Prevent Data Leakage from Personal Devices

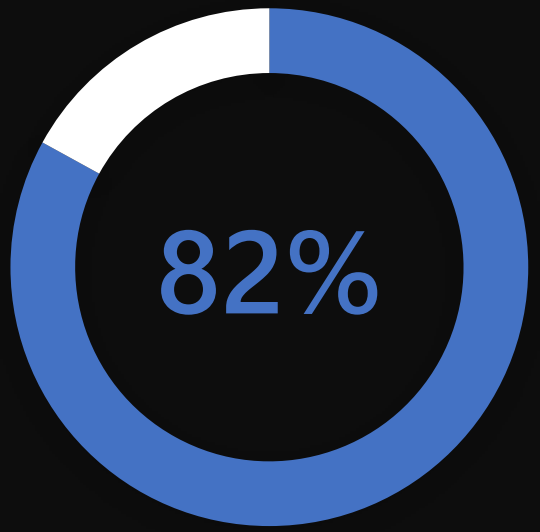
5 September 2023 @ Pink Elephant

Agenda

- Why is it important?
- Method 1, 2, 3, 4 ,5
- Method 6 [DEMO]
- Method 7 [DEMO]
- Summary

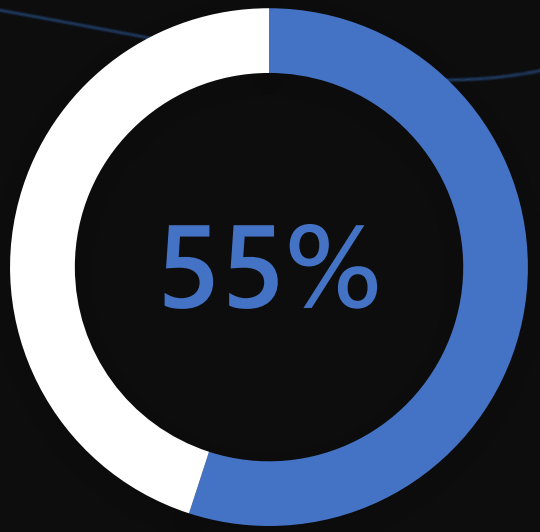


Numbers on personal devices



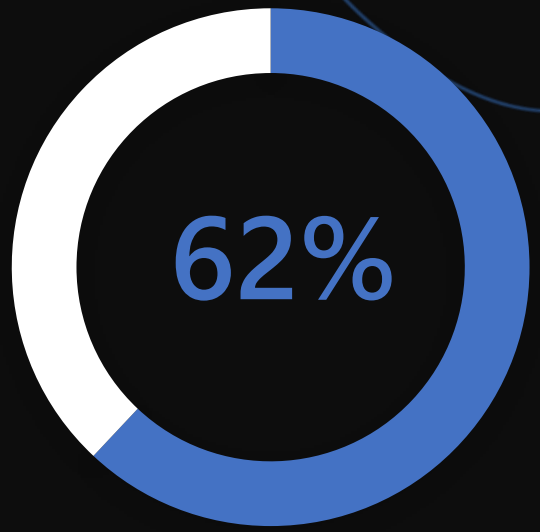
of companies allow the use of personal devices for work

Cybersecurity Insiders report 2021



of employees work from personal devices

Gartner research 2021

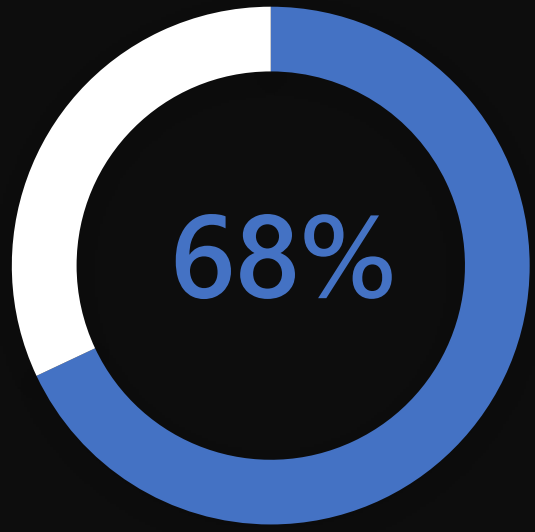


Of companies see data leakage as their top BYOD risk

Cybersecurity Insiders report 2021

Challenges dealing with personal devices

- Not up-to-date
- No insights on vulnerabilities
- No policies to harden security
- No hard drive encryption
- Cannot wipe data when stolen/lost or employee leave



of companies report improved employee productivity

Cybersecurity Insiders report 2021

MYRON HELGERING

MICROSOFT SECURITY & COMPLIANCE

- Microsoft Security Engineer @ 2source4
- Working with M365 since 2013
- Blogger @ myronhelgering.com
- Snowboarding, traveling & fantasy geek

@MyronHelgering

in/myronhelgering

myronhelgering.com

Method 1
Do nothing...

- Let employees be productive
- Allow personal devices
- No technical measures
- Accept risks

I would **not** recommend this.

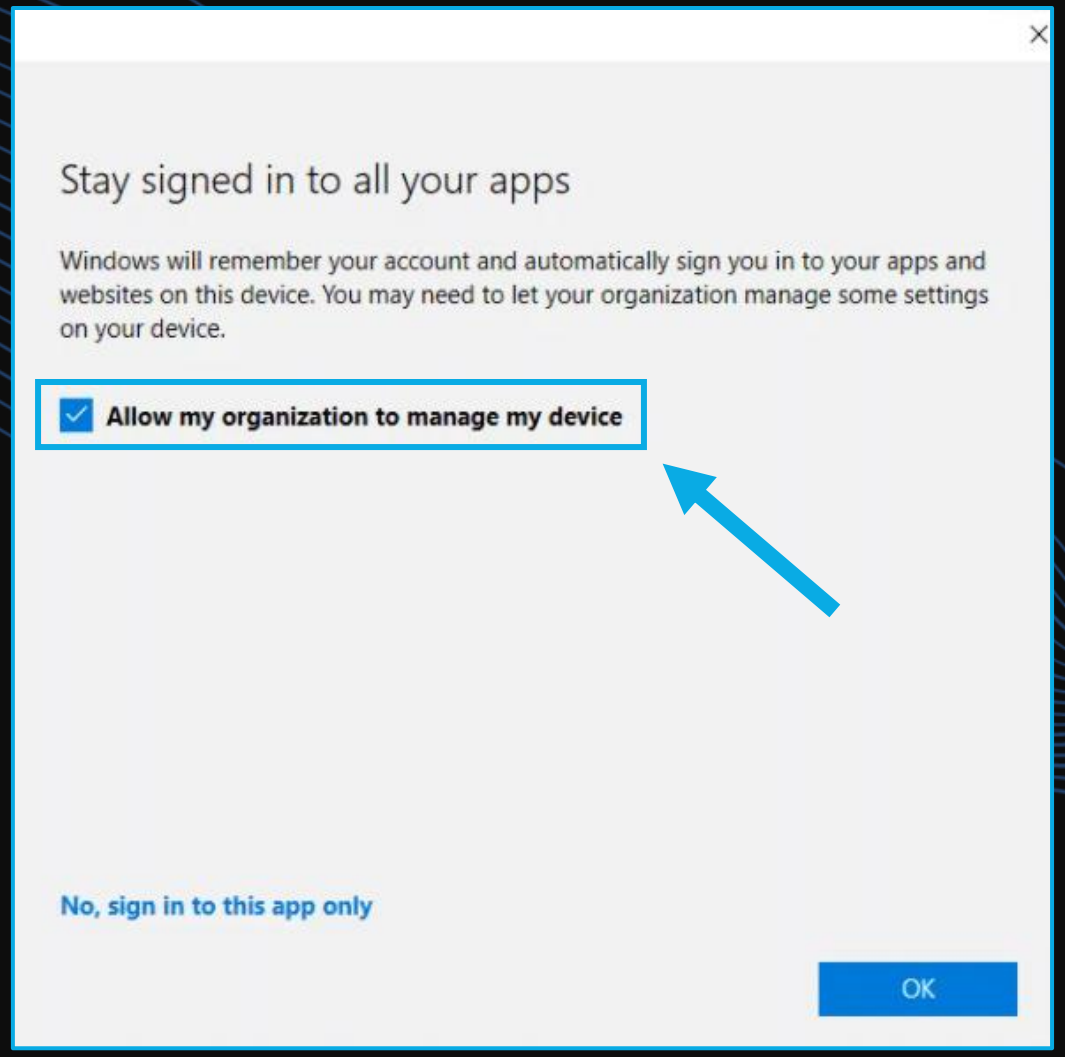
Example of doing nothing

Method 2
Require enrollment

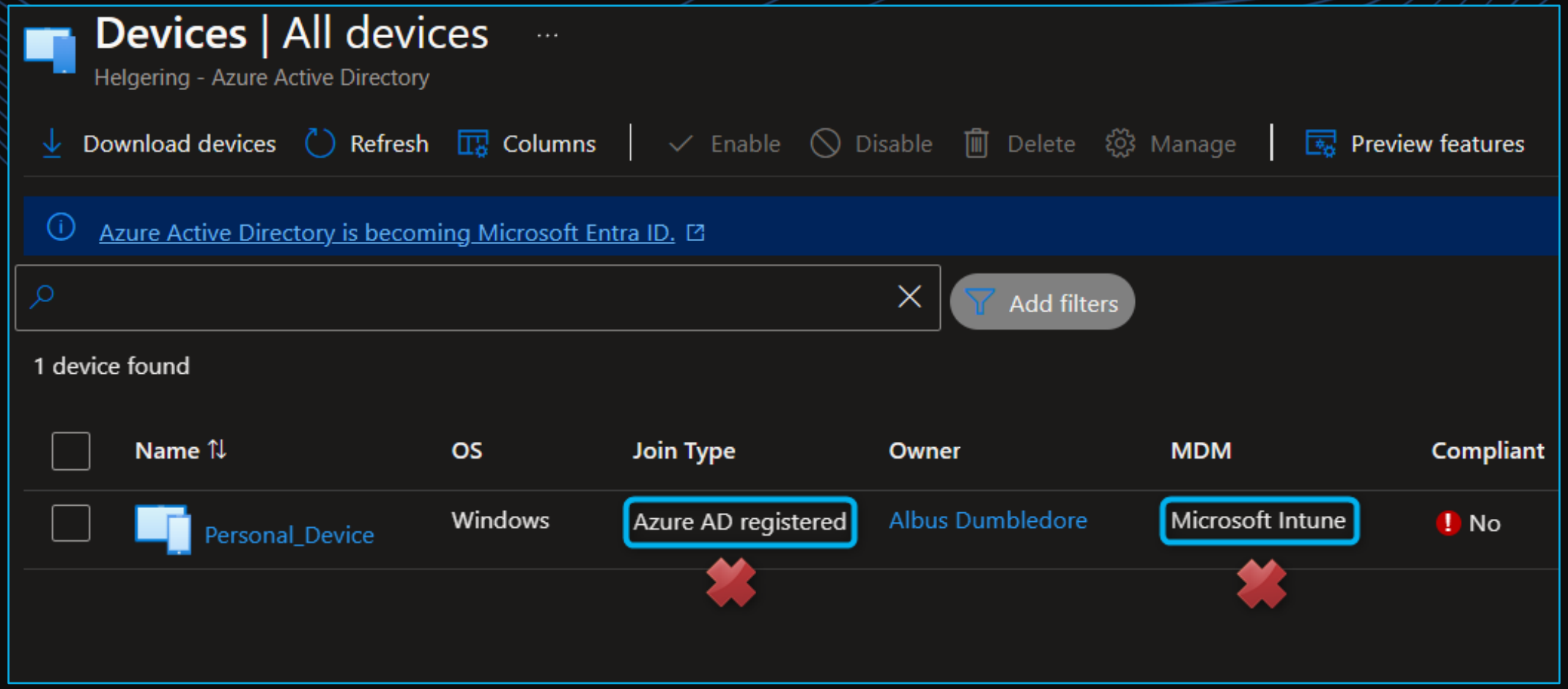
- Full control over personal devices
- Secure, and ability to wipe
- Ability to deploy policies
- Be a terrible ruler

I would **not** recommend this.

Enrollment during Office sign-in



What happened here...



Enrollment Restrictions

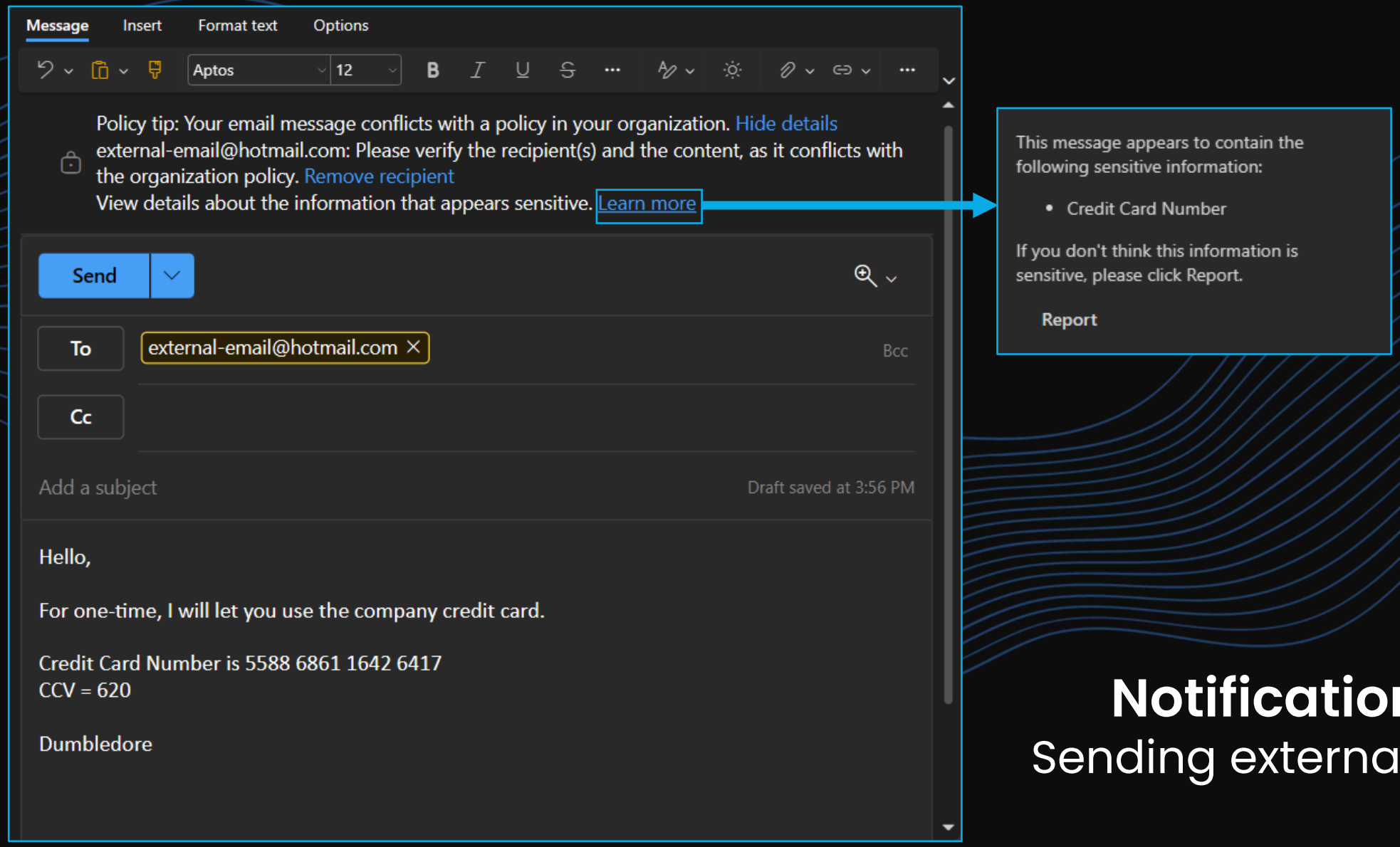
Type	Platform	versions	Personally owned
Android Enterprise (work profile)	Allow / Block	Allow min/max range: Min Max	Allow / Block
Android device administrator	Allow / Block	Allow min/max range: Min Max	Allow / Block
iOS/iPadOS	Allow / Block	Allow min/max range: Min Max	Allow / Block
macOS	Allow / Block	Restriction not supported	Allow / Block
Windows (MDM) ⓘ	Allow / Block	Allow min/max range: Min Max	Allow / Block

Example of require enrollment

Method 3
Data Loss Prevention

- Protect sensitive (precious) information
- Prevent data loss across;
  - M365 services
  - Office apps
  - Windows & MacOS endpoints
  - Other cloud apps (third party)
  - On-premises file shares

Great method for sensitive data, but **not applicable** for personal devices.

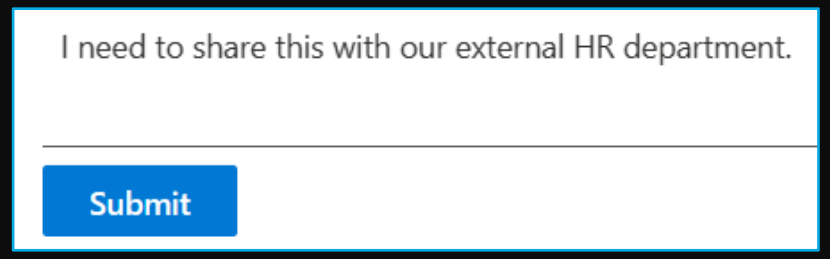


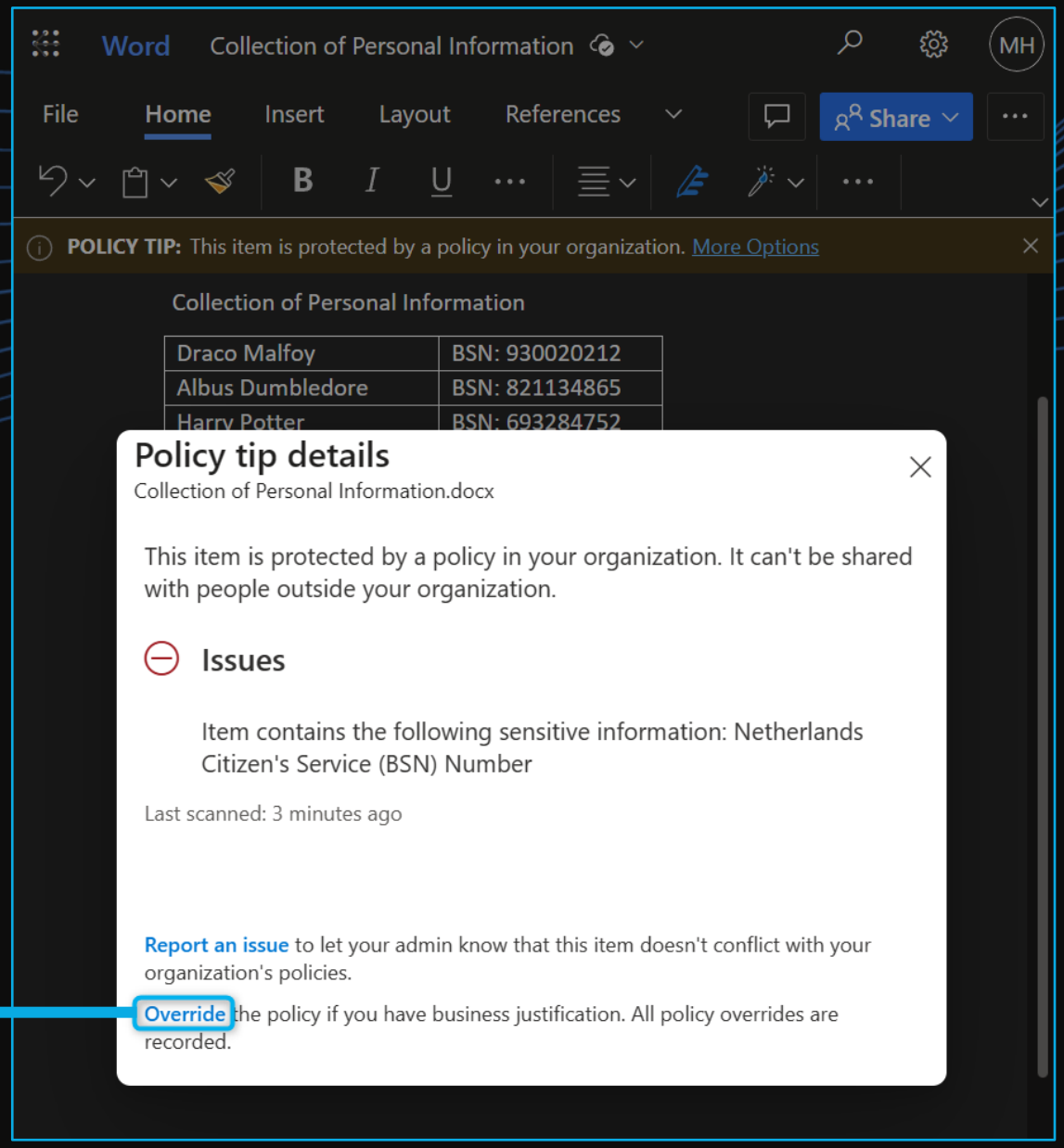
Notification only

Sending external email

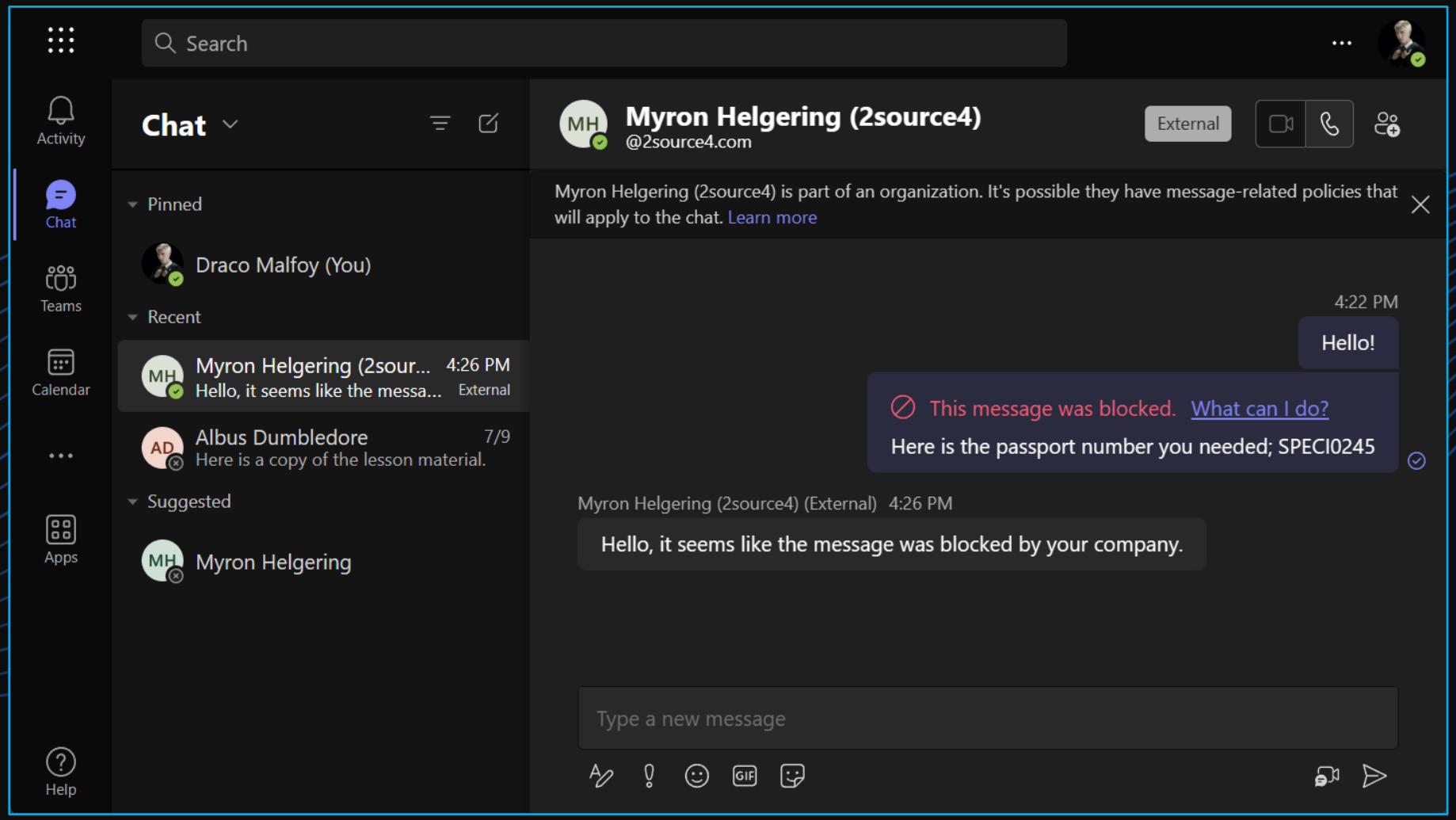
Block with Override

External file sharing



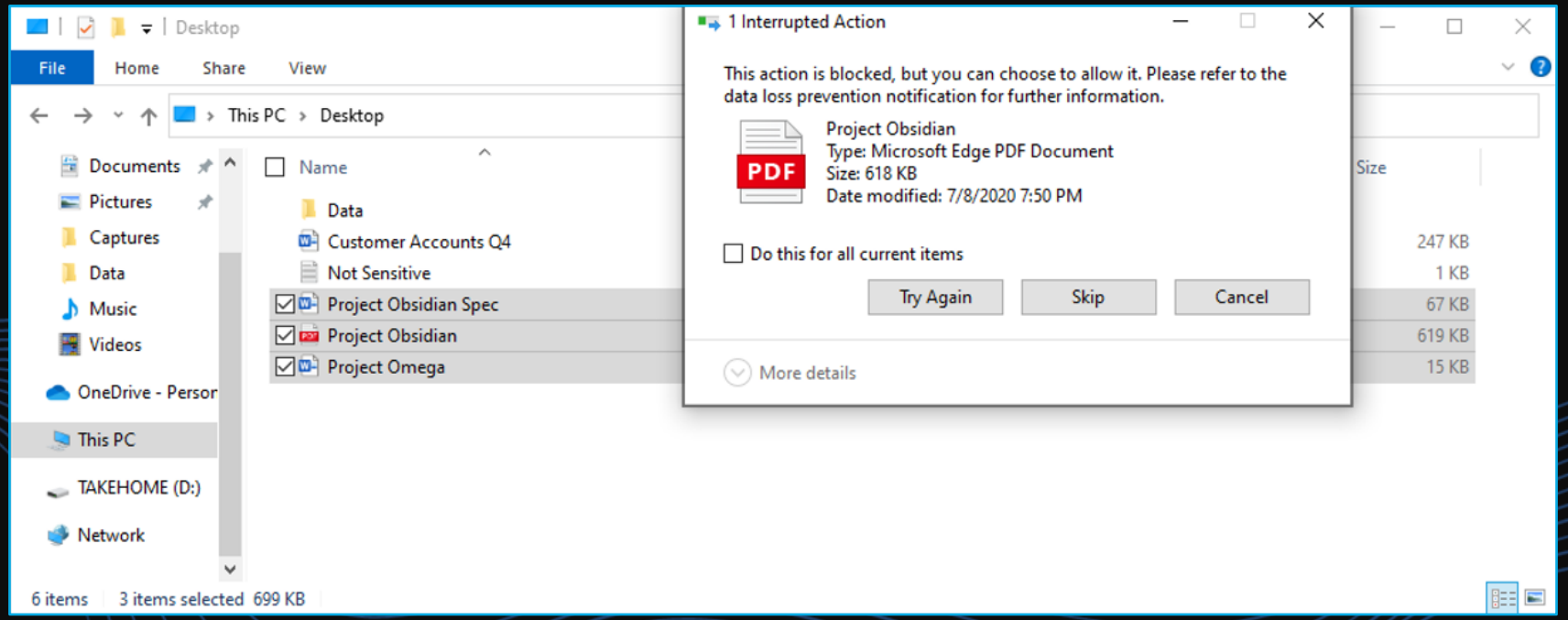


Block External chat message



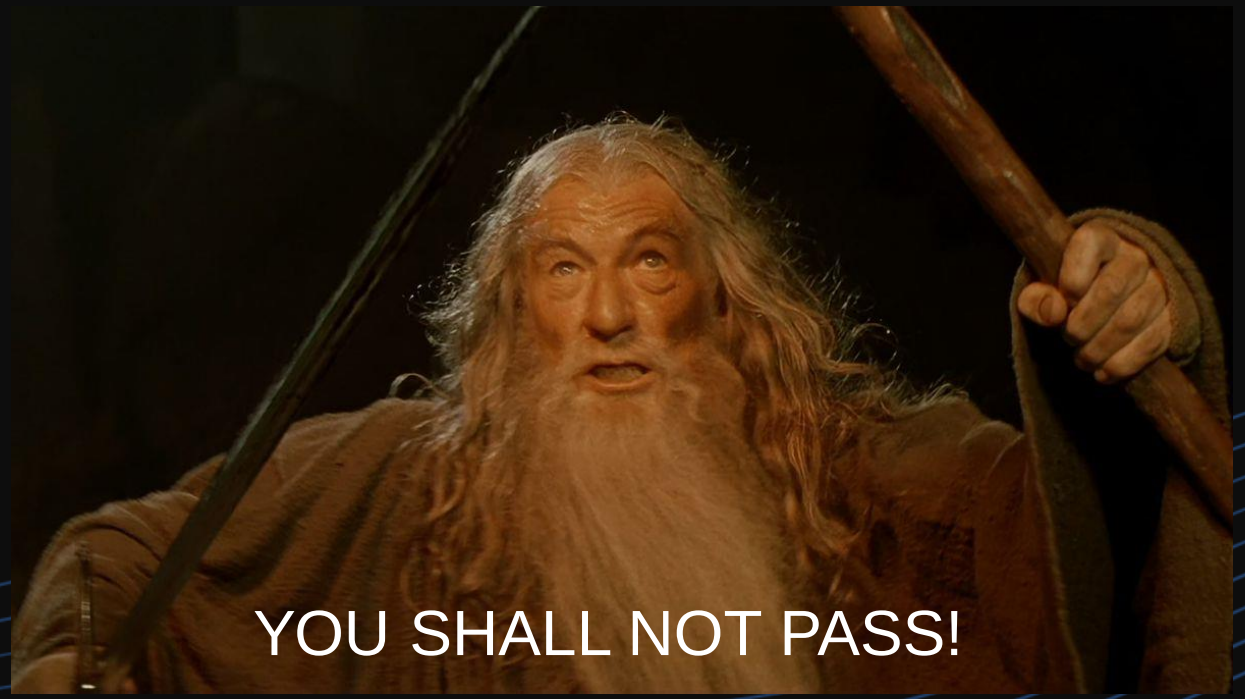
Block with override

Copy to USB (Endpoint DLP)



Method 4
Block access

- Block all access
- Secure
- Not always user-friendly

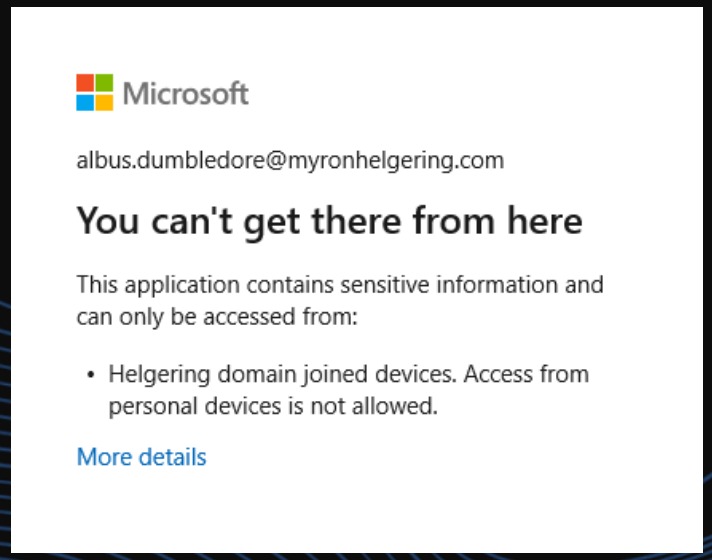


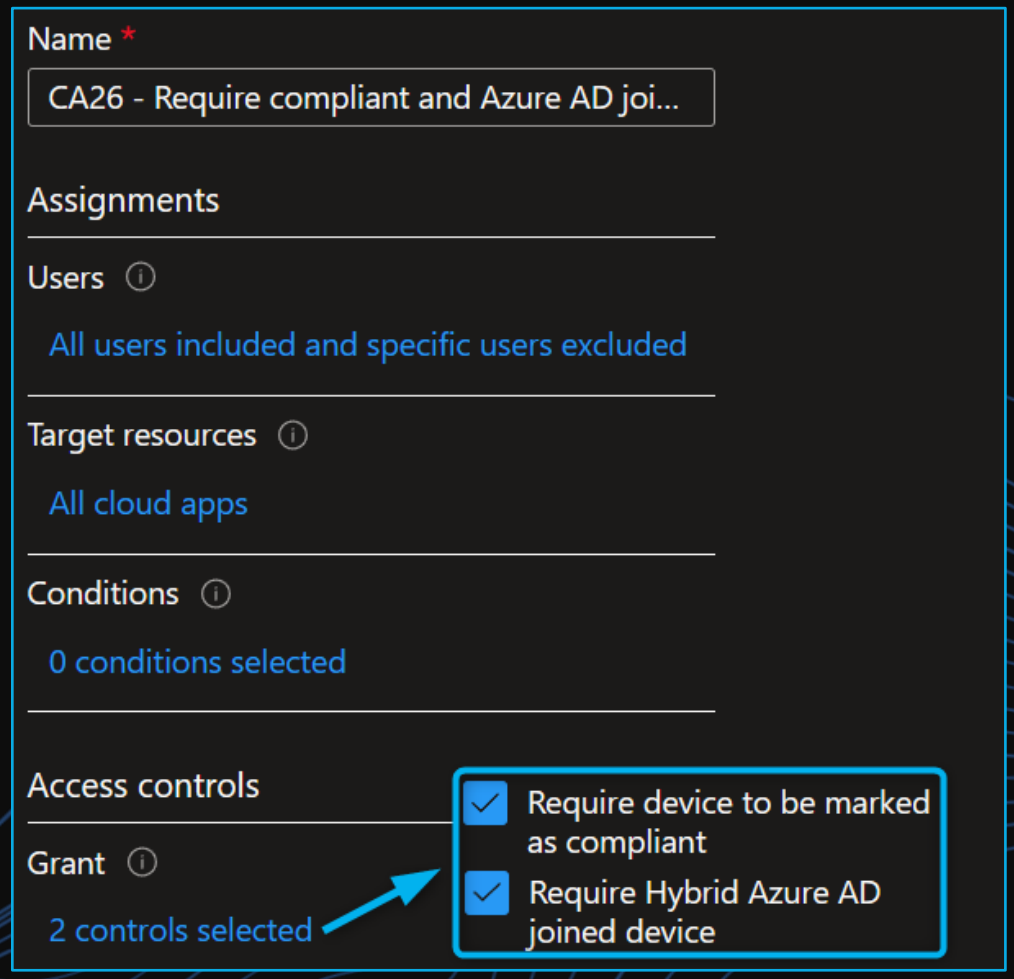
Good method, but not suitable for most organizations.

Conditional Access policy

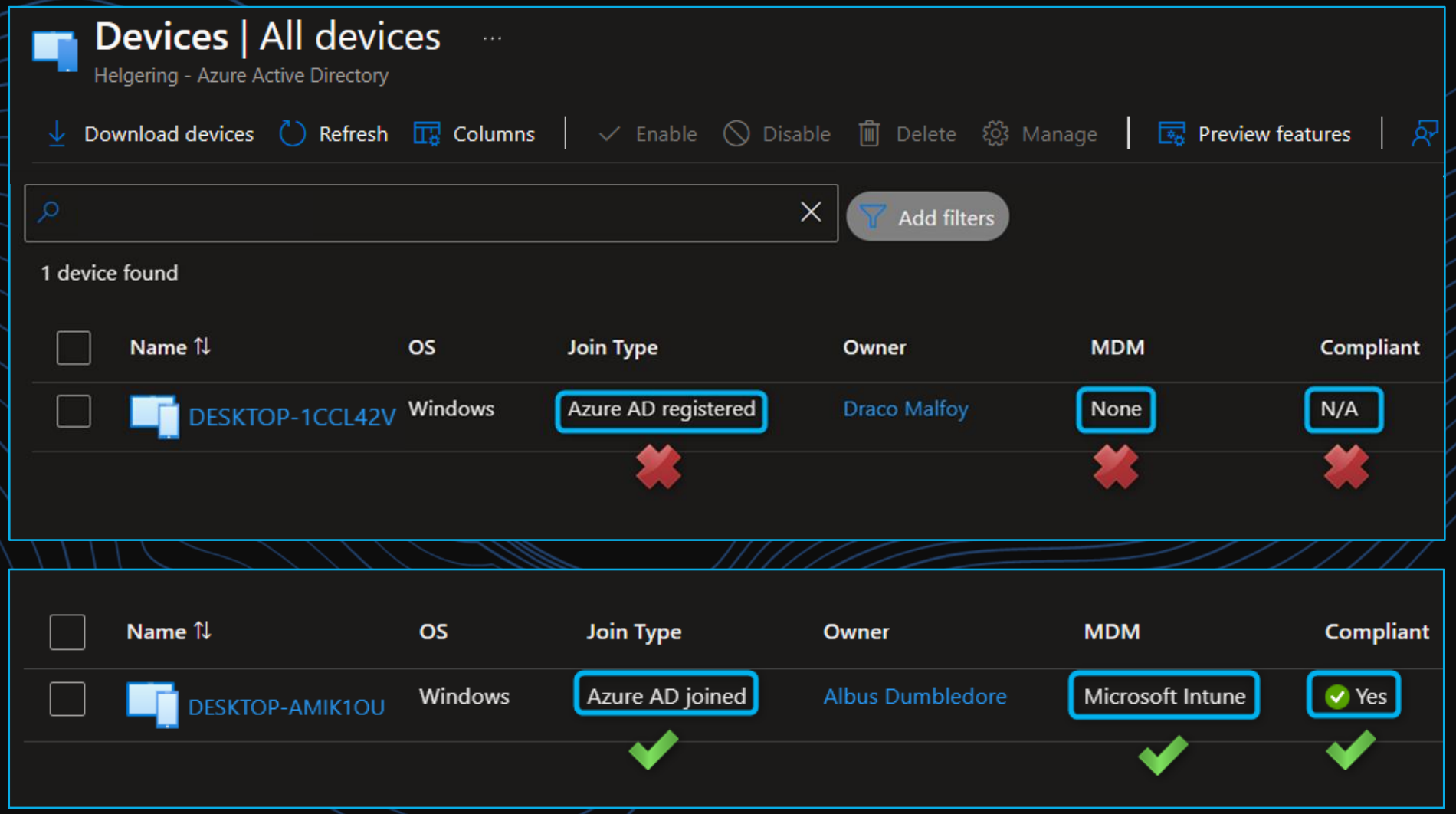
Some things to consider;

- Exclude guest, service, break-glass accounts
- Exclude VDI/RDS IP-addresses
- Target Office365 apps, more or all cloud apps

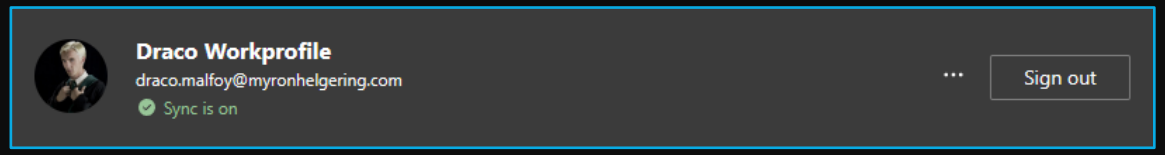




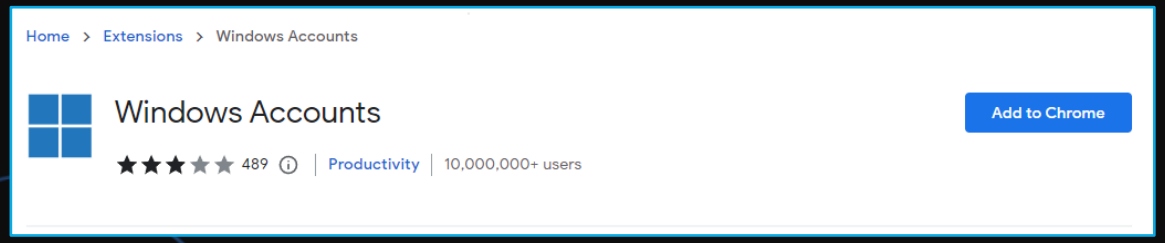
Check if devices are compliant and enrolled



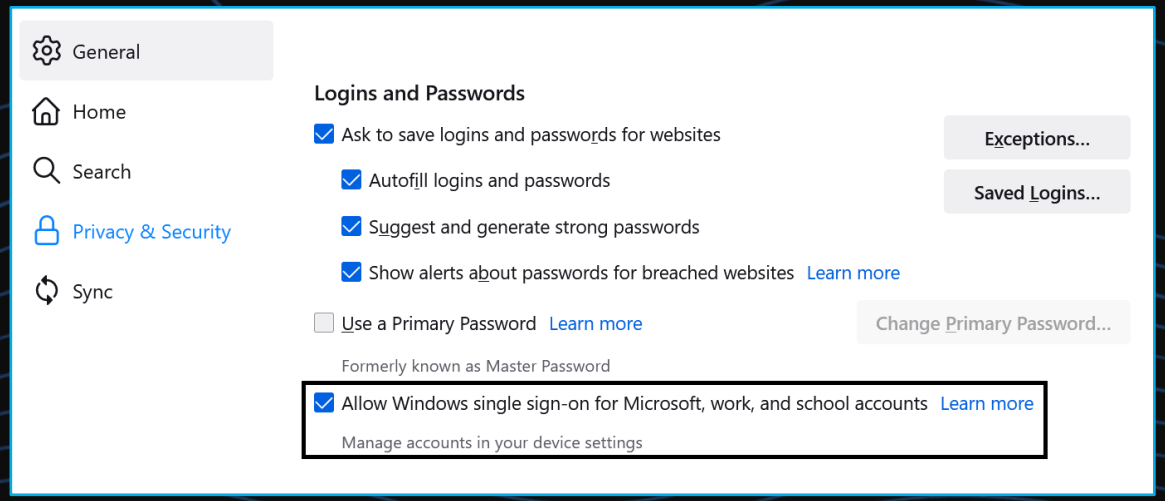
Single Sign On



Microsoft Edge



Google Chrome

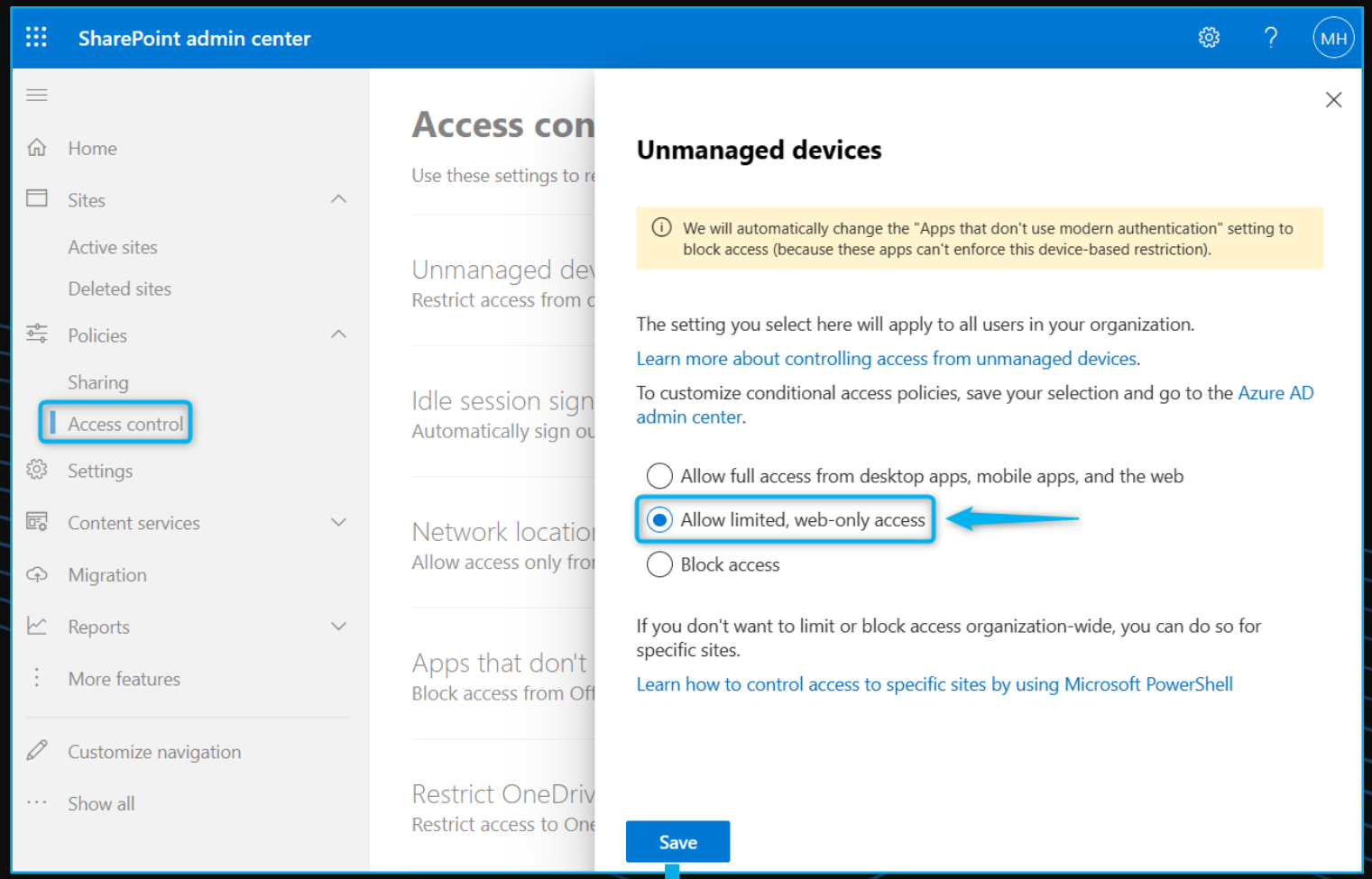


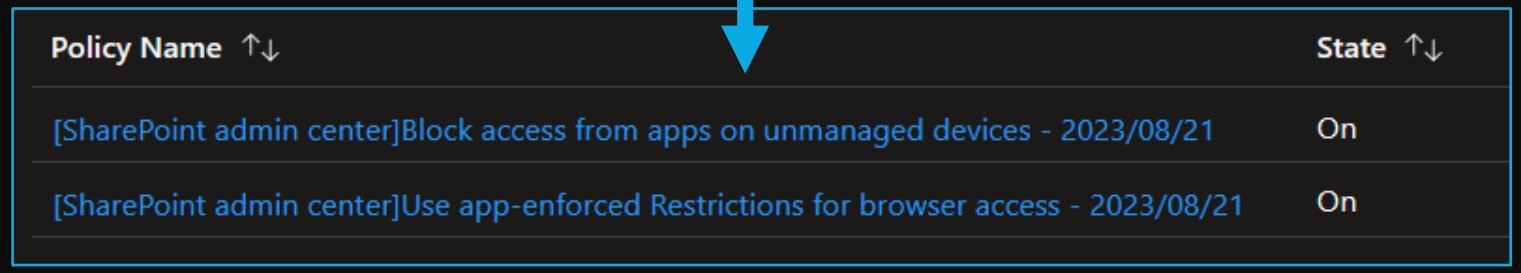
Mozilla Firefox

Method 5
App-enforced restrictions

- Block desktop app access
- Enforce web-only access
- Restrict download, print & sync

Good method, but it is lacking some important features and restrictions.



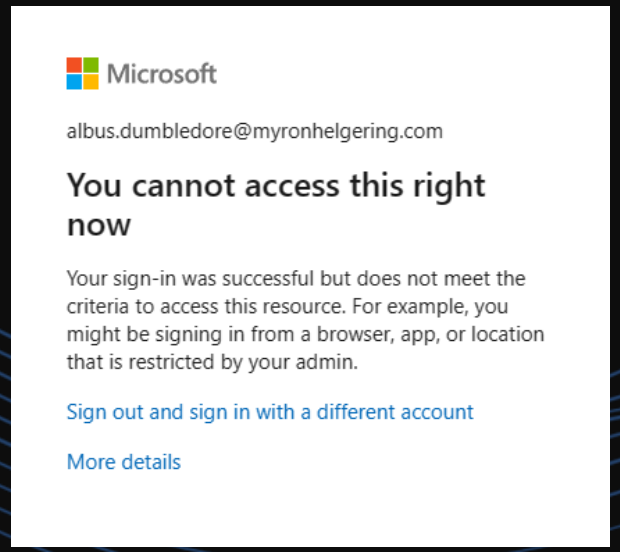


Enable in SharePoint Admin Center

Conditional Access policies are created

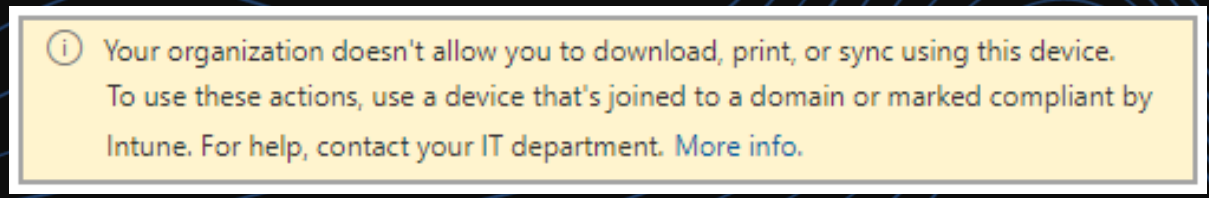
Policy 1
Block access from apps on unmanaged devices

- Block access from desktop apps on unmanaged devices
- Applies to SharePoint Online by default, but more apps can be added

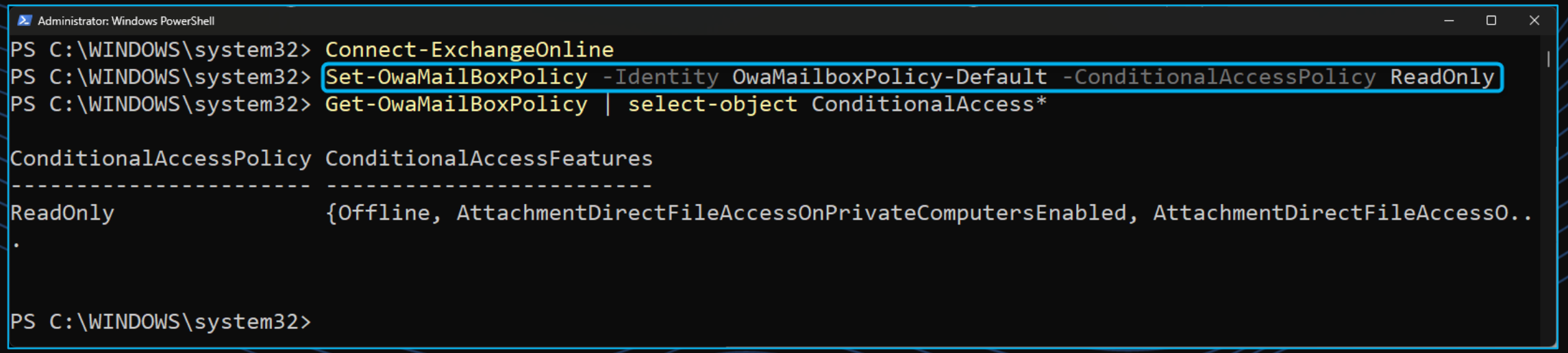


Policy 2
Use app-enforced restrictions for browser access

- Enforces limited web access on unmanaged devices
- Blocks download, print, or syncing
- Can only apply to SharePoint Online and **Exchange Online**



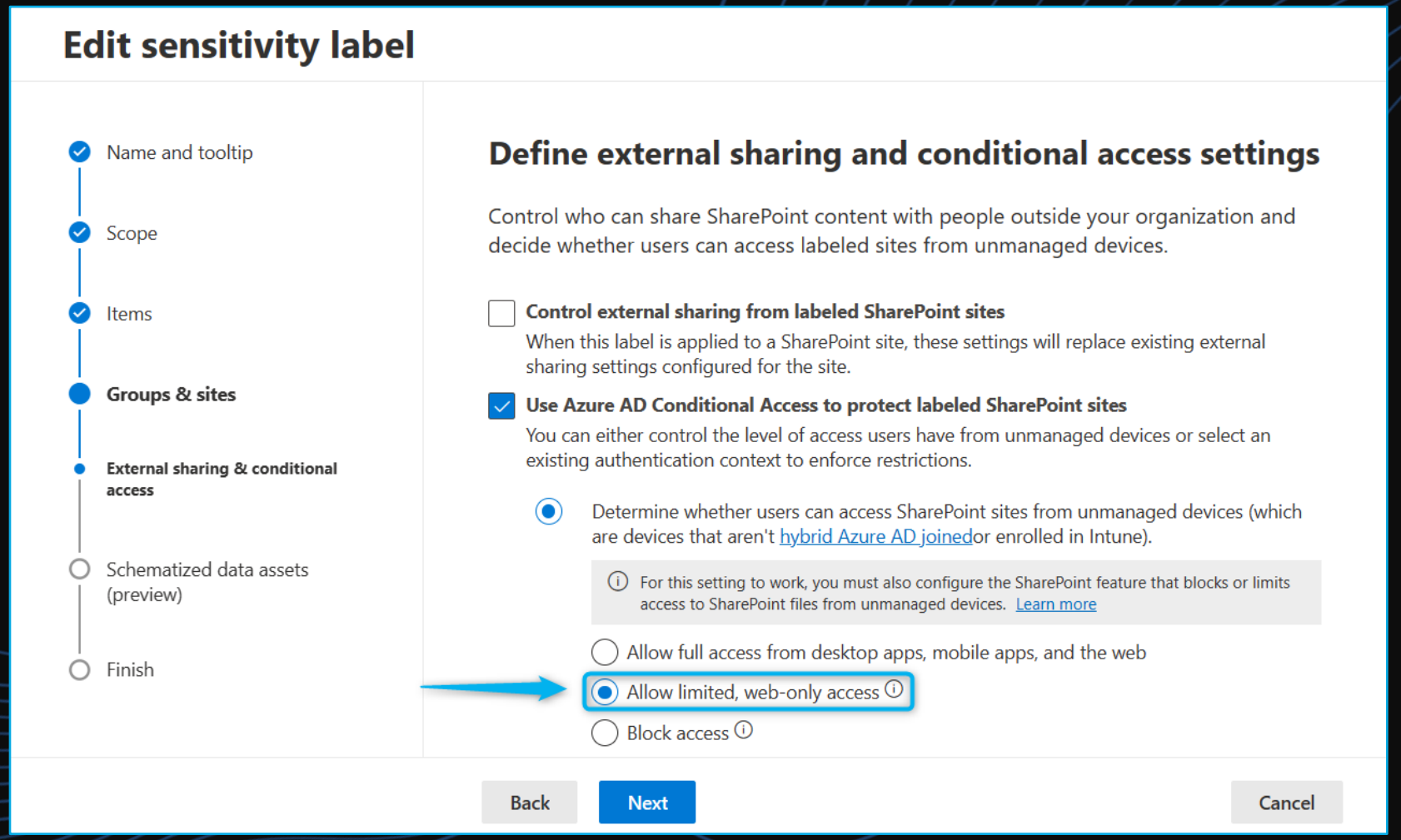
Enable App-Enforced Restrictions for Exchange Online with PowerShell



Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly

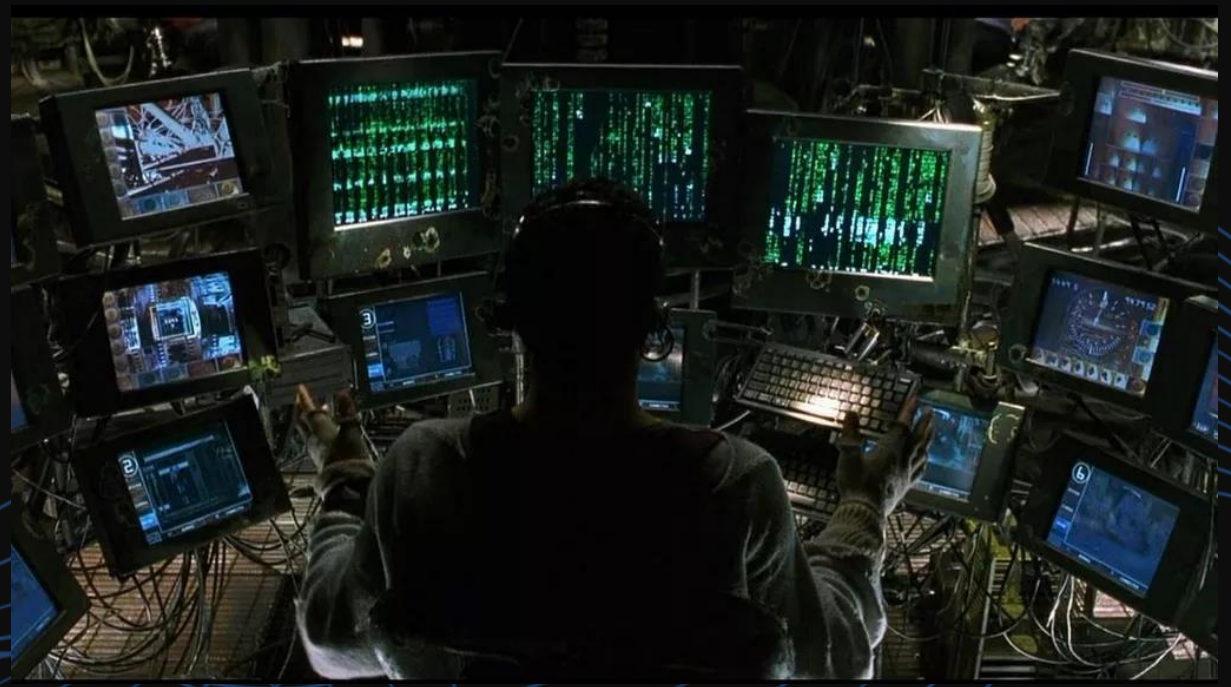
Sensitivity Labels

- Target locations with sensitive data only
- Applies to M365 Groups, SharePoint Sites, and Teams



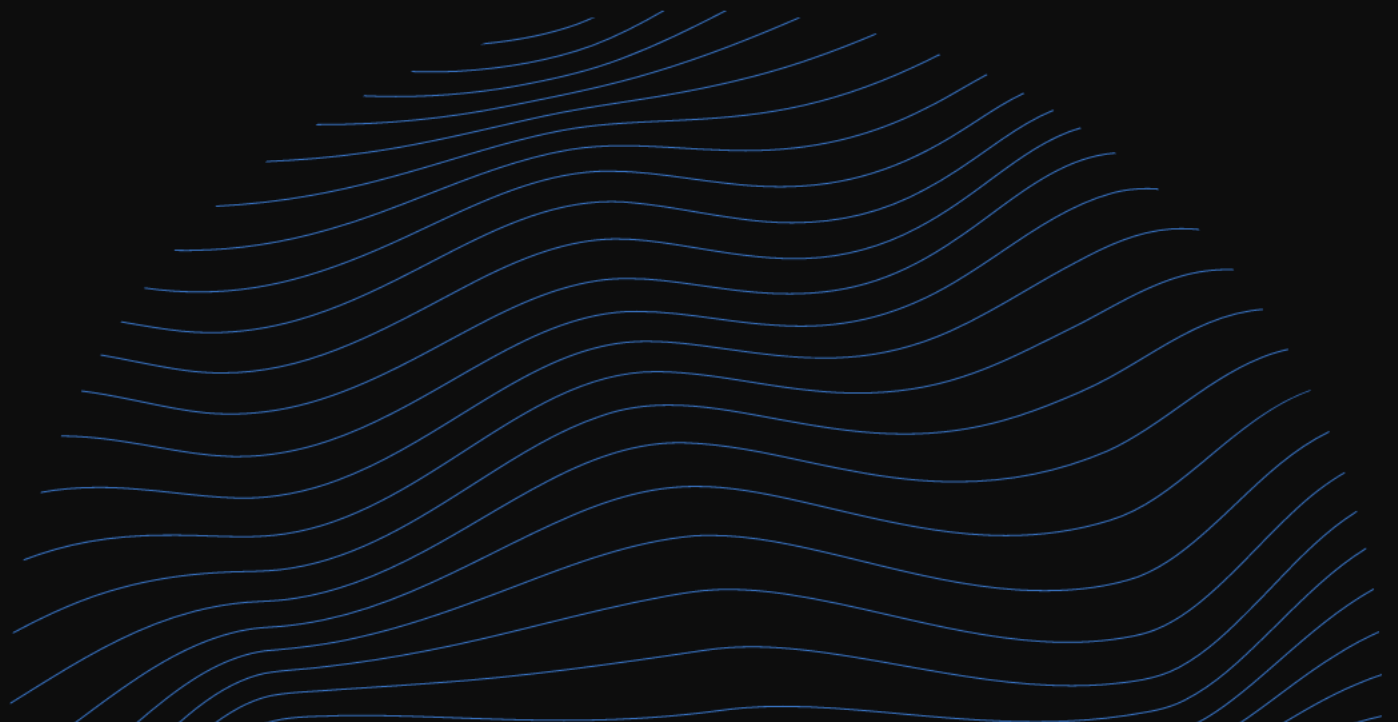
Method 6
Session Monitoring

- Enforce web session monitoring
- Restrict download, print, cut, copy, and more!
- Supports more cloud apps



Good method but combine it with blocking desktop app access.

Session Monitoring
DEMO



Method 7
App Protection Policies

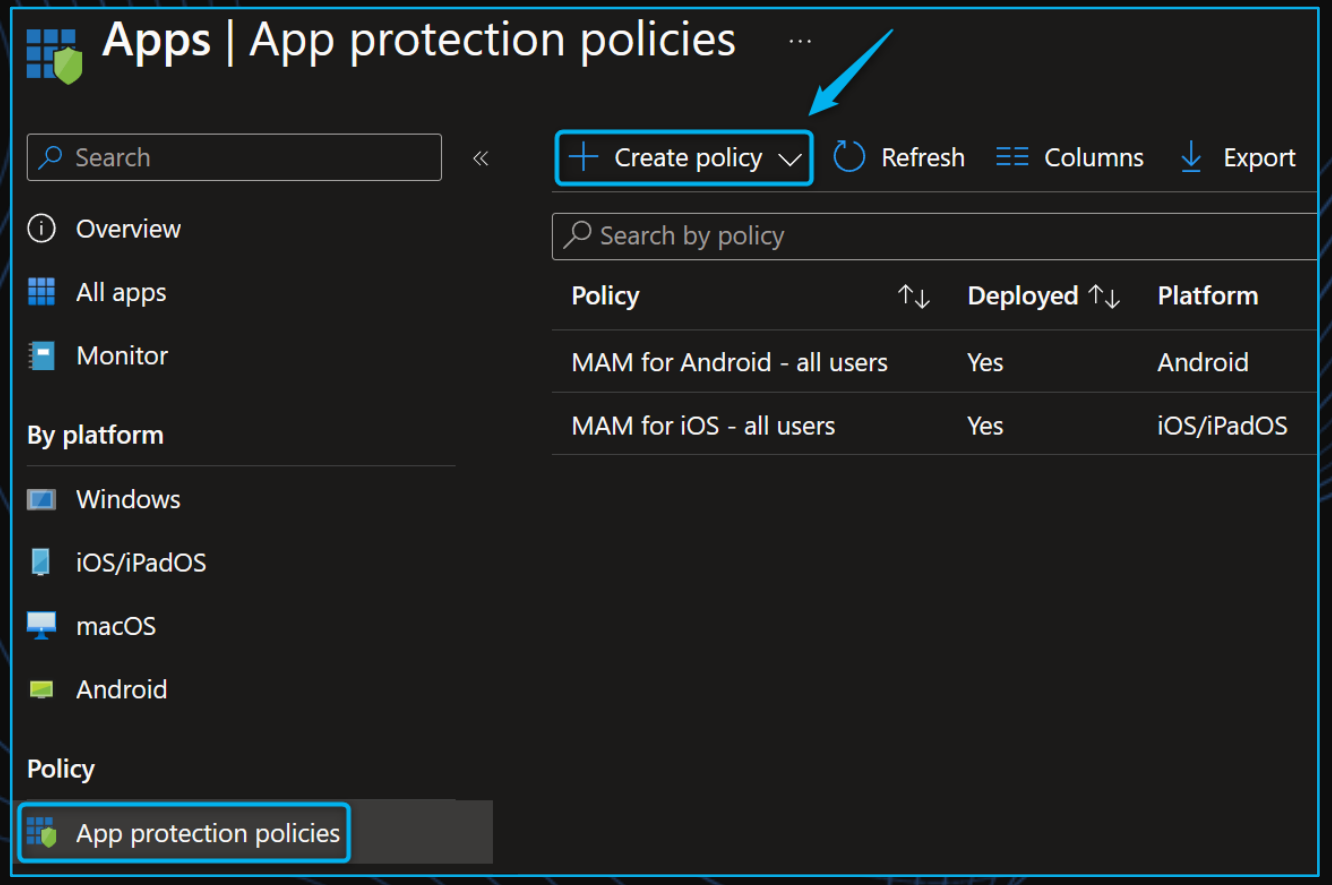
- Apply data protection controls
- Manage and wipe app data only
- Set specific device conditions
- Ensure secure authentication

Great method in theory, it protects corporate data, while respecting personal data.

MAM for Android & iOS

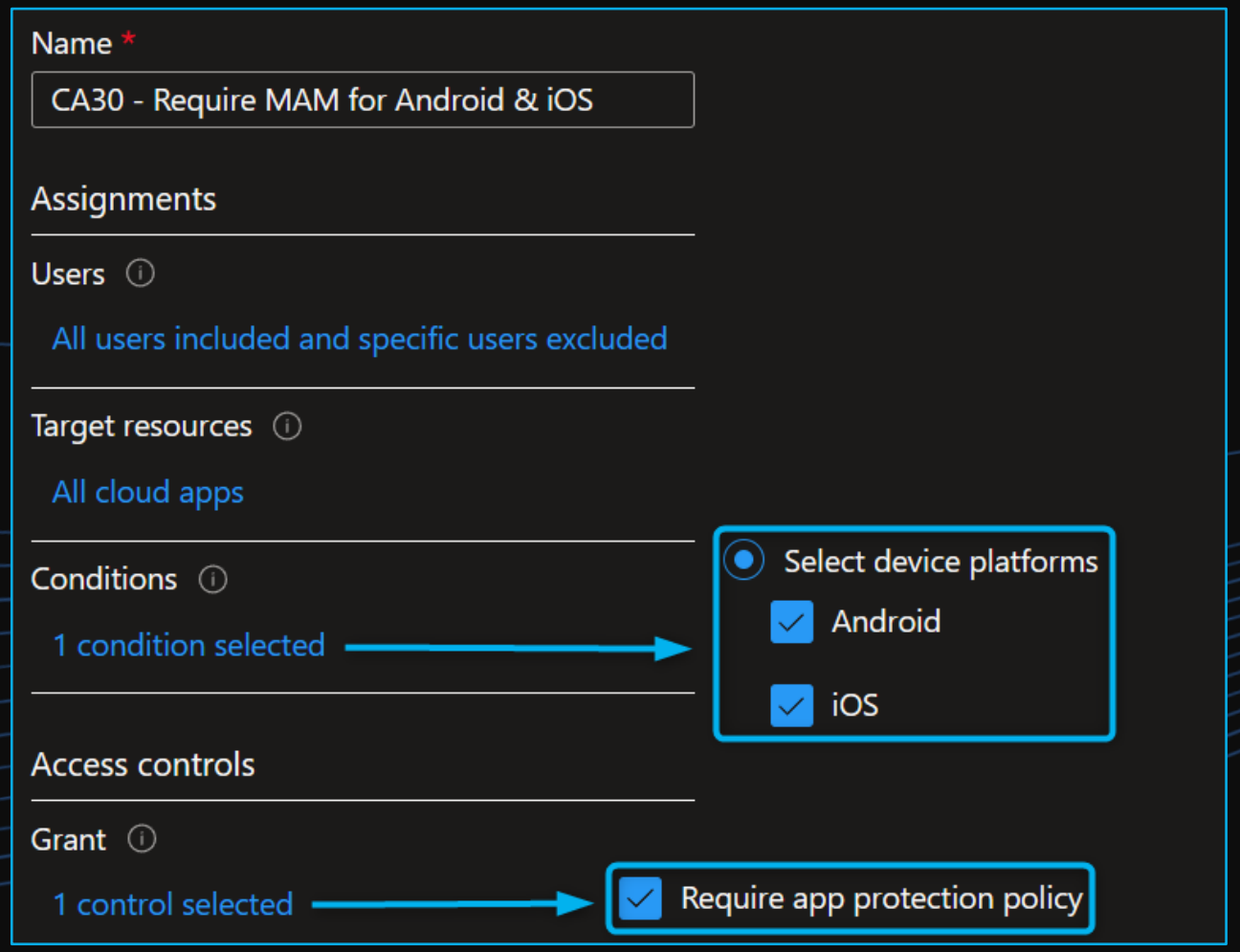
App Protection policy settings

- No cut/copy/paste between apps
- No printing or downloading
- No screenshots (Android only)
- Encrypt app data
- Secure authentication (PIN/biometric)
- Set max threat level (MTD connector)
- Block access for specific OS versions, manufacturers, or jailbroken devices

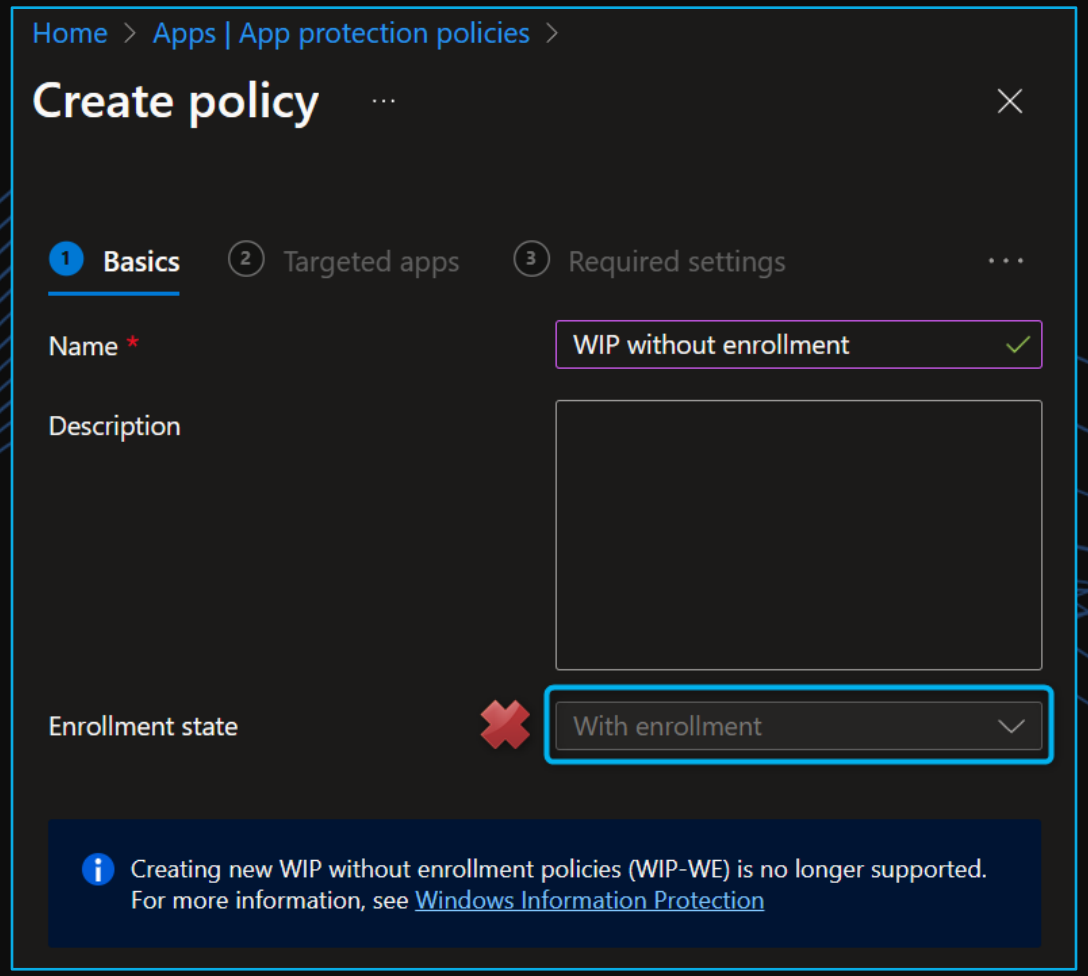


Require MAM with CA policy

- Authenticator app for iOS
- Company Portal app for Android



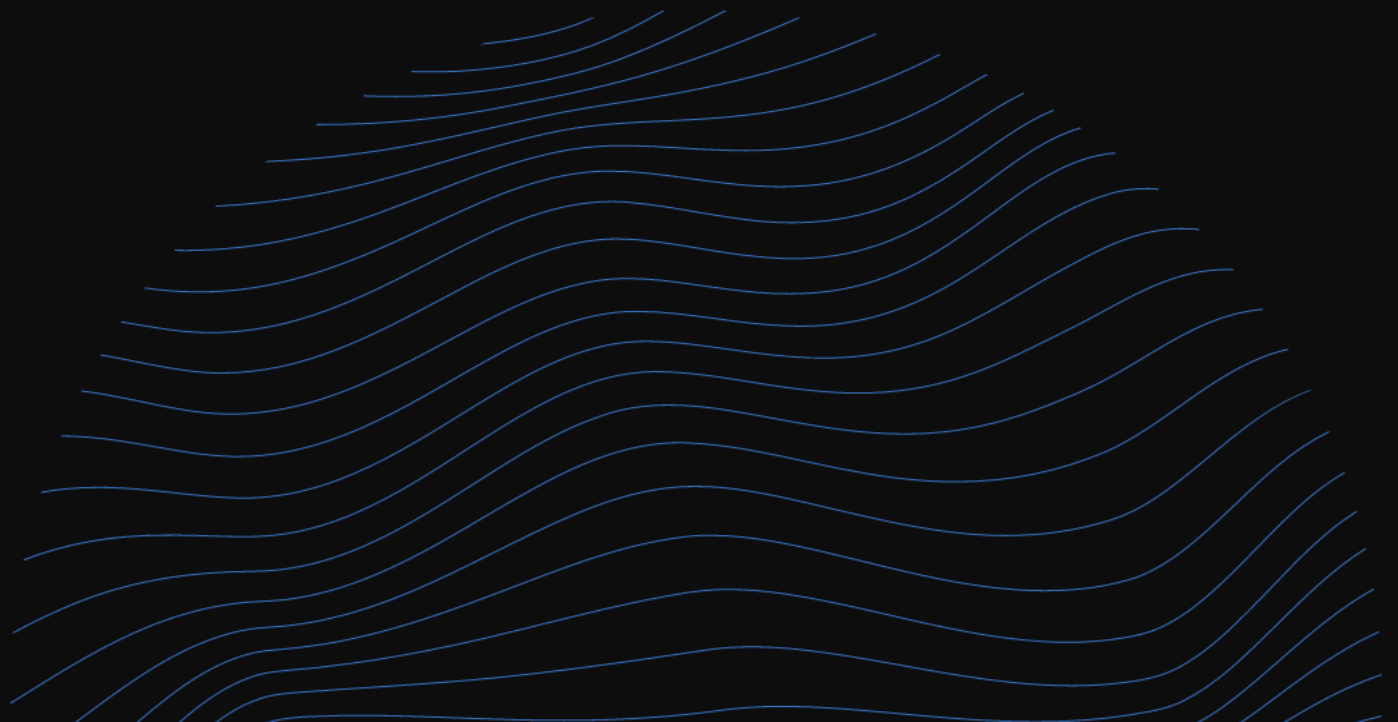
Windows Information Protection



- Barrier between corporate and personal data
- Users can use MS Office desktop apps and sync (encrypted) data with OneDrive
- No longer supported for unmanaged devices

MAM for Windows (NEW)

DEMO



What to expect in the future?

Summary

1. Don't do nothing
2. Don’t require MDM enrollment for personal devices

3. Use Data Loss Prevention for most sensitive data
4. Consider blocking personal devices, at least for admins.

Or choose at least one balanced method;

5. Enforce app-enforced restrictions (with CA)
6. Enforce session monitoring (with MS Defender)
7. Enforce app protection policies (with MAM)

Blog posts

- Enforce Limited web-only access with Conditional Access
- Enforce Limited web-only access with Sensitivity Labels
- Enforce Limited web-only access with Session policies
- First look at MAM for Windows
- Quick Guide: Enable Sigle Sign On for Chrome and Firefox

@MyronHelgering in/myronhelgering myronhelgering.com

Thank you!

 @MyronHelgering

 in/myronhelgering

 myronhelgering.com