

SESSION

7 Methods to Prevent Data Leakage from Personal Devices



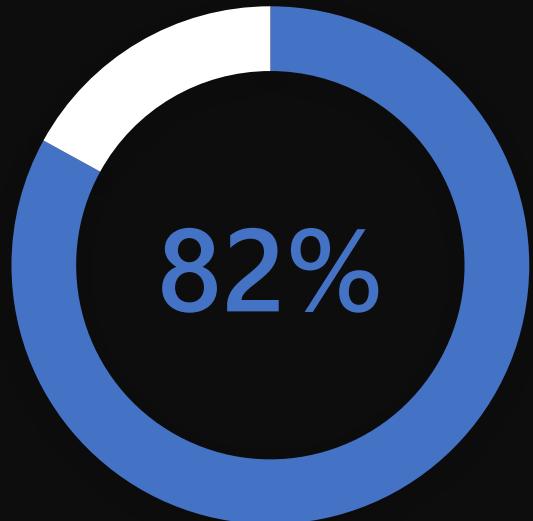
5 September 2023 @ Pink Elephant

Agenda

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

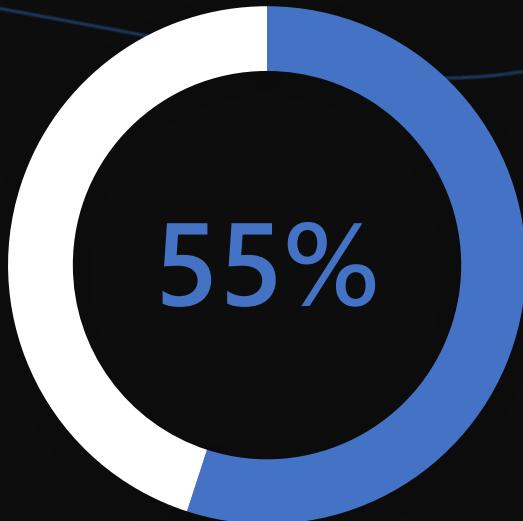


Numbers on personal devices



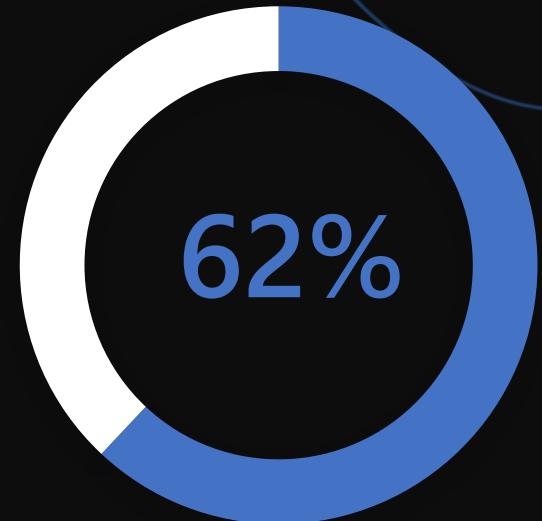
of companies allow
the use of personal
devices for work

Cybersecurity Insiders report 2021



of employees
work from
personal devices

Gartner research 2021

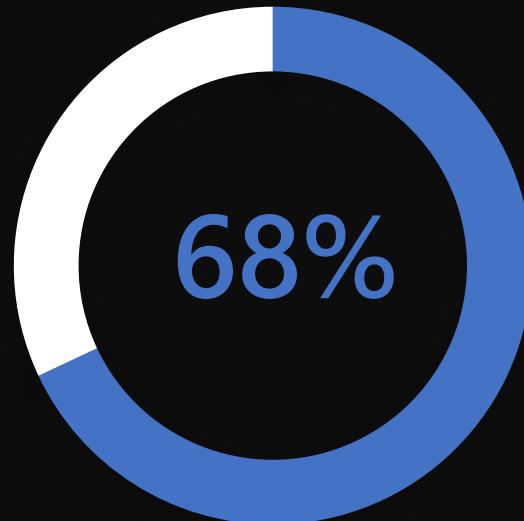


Of companies see
data leakage as
their top BYOD risk

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



- 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



MASSACHUSETTS
EYE AND EAR
Bold Science. Life-Changing Cures.

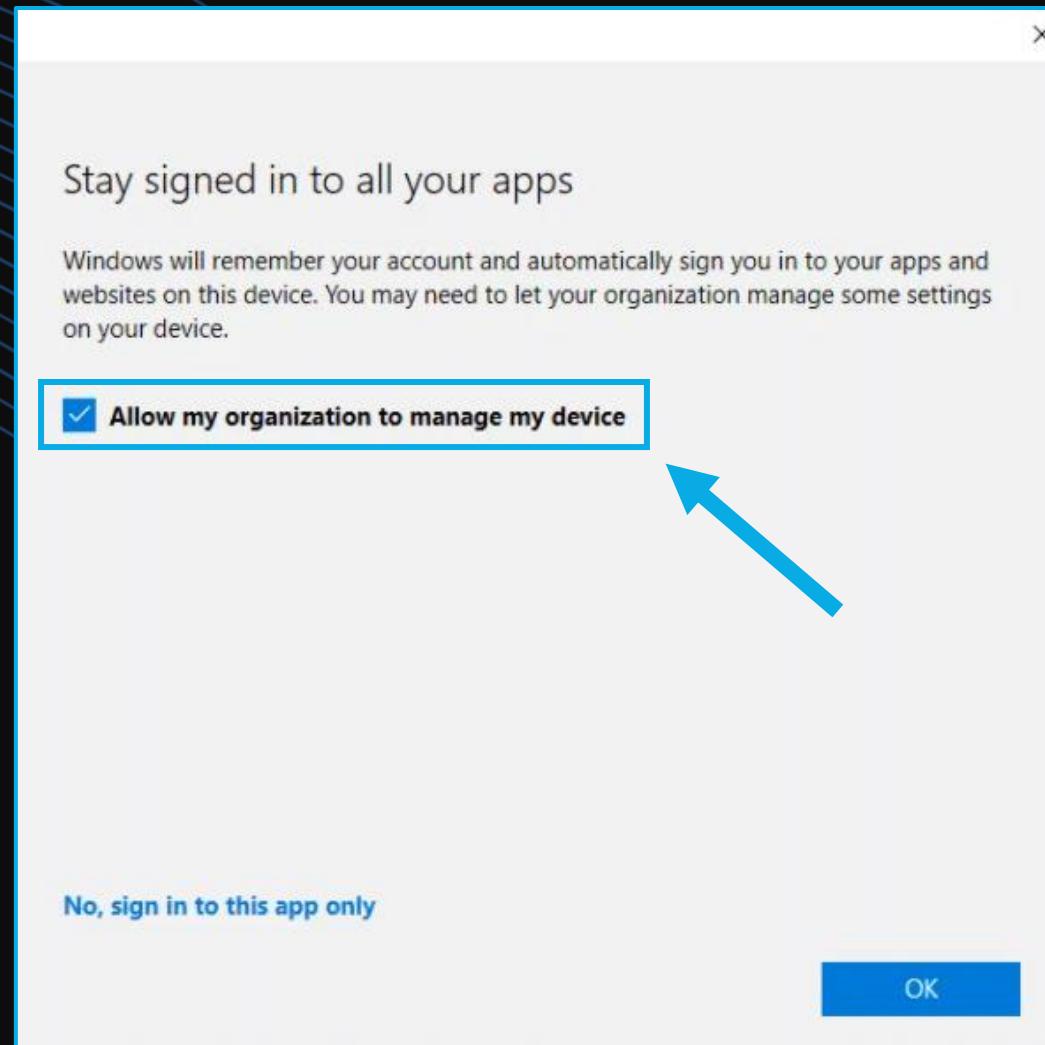
Method 2 Require enrollment



- 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...

 **Devices | All devices** ...
Helgering - Azure Active Directory

 Download devices  Refresh  Columns |  Enable  Disable  Delete  Manage |  Preview features

 [Azure Active Directory is becoming Microsoft Entra ID.](#) 

   Add filters

1 device found

<input type="checkbox"/>	Name ↑	OS	Join Type	Owner	MDM	Compliant
<input type="checkbox"/>	 Personal_Device	Windows	Azure AD registered	Albus Dumbledore	Microsoft Intune	 No

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

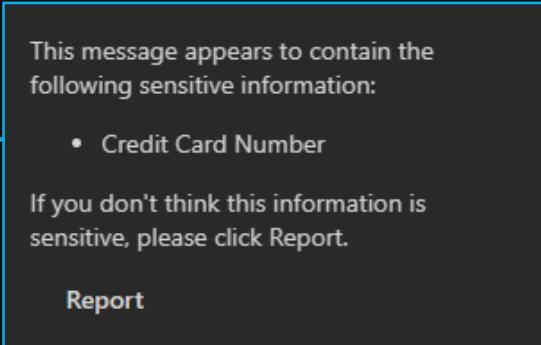
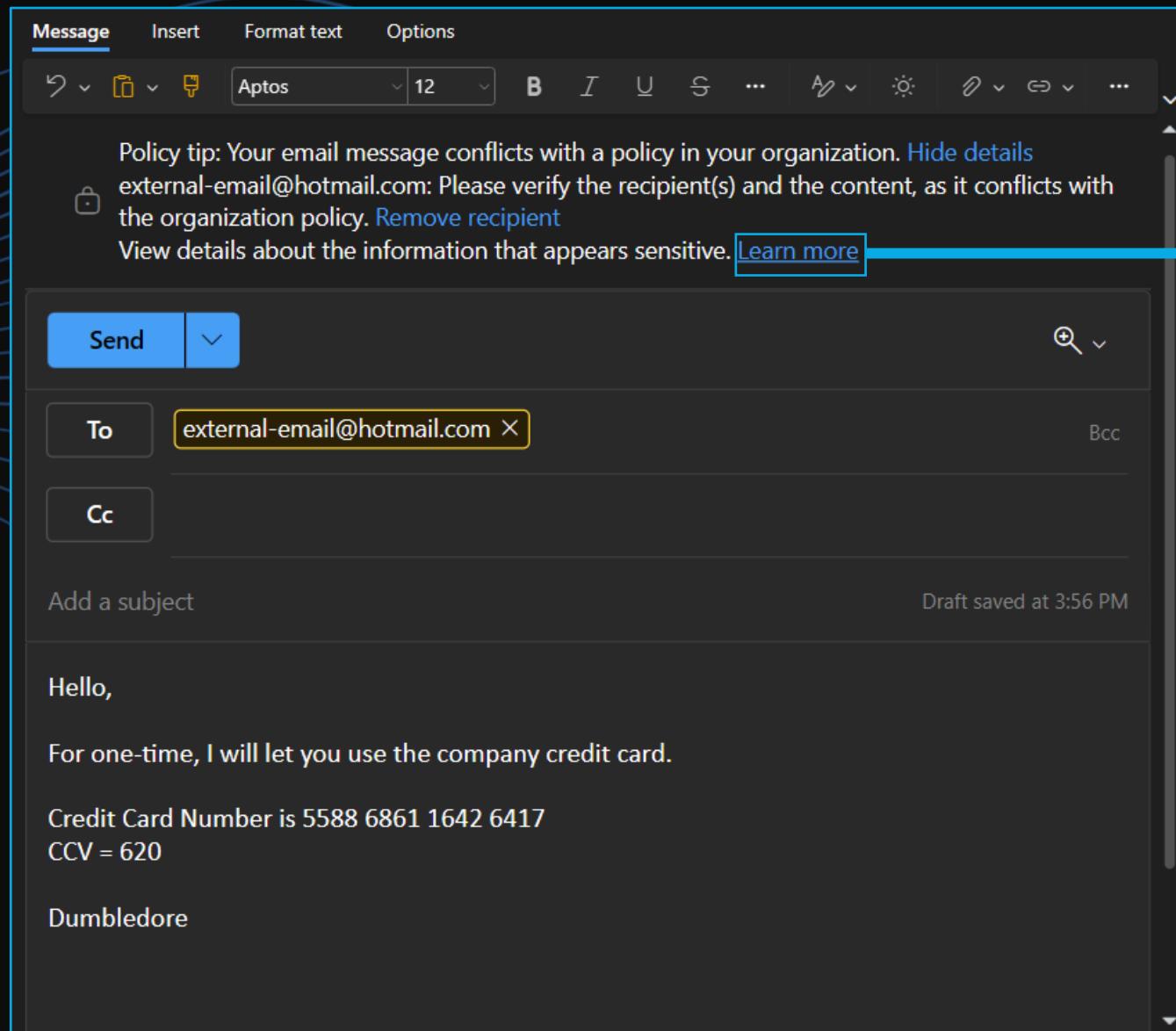


Method 3 Data Loss Prevention

- 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.



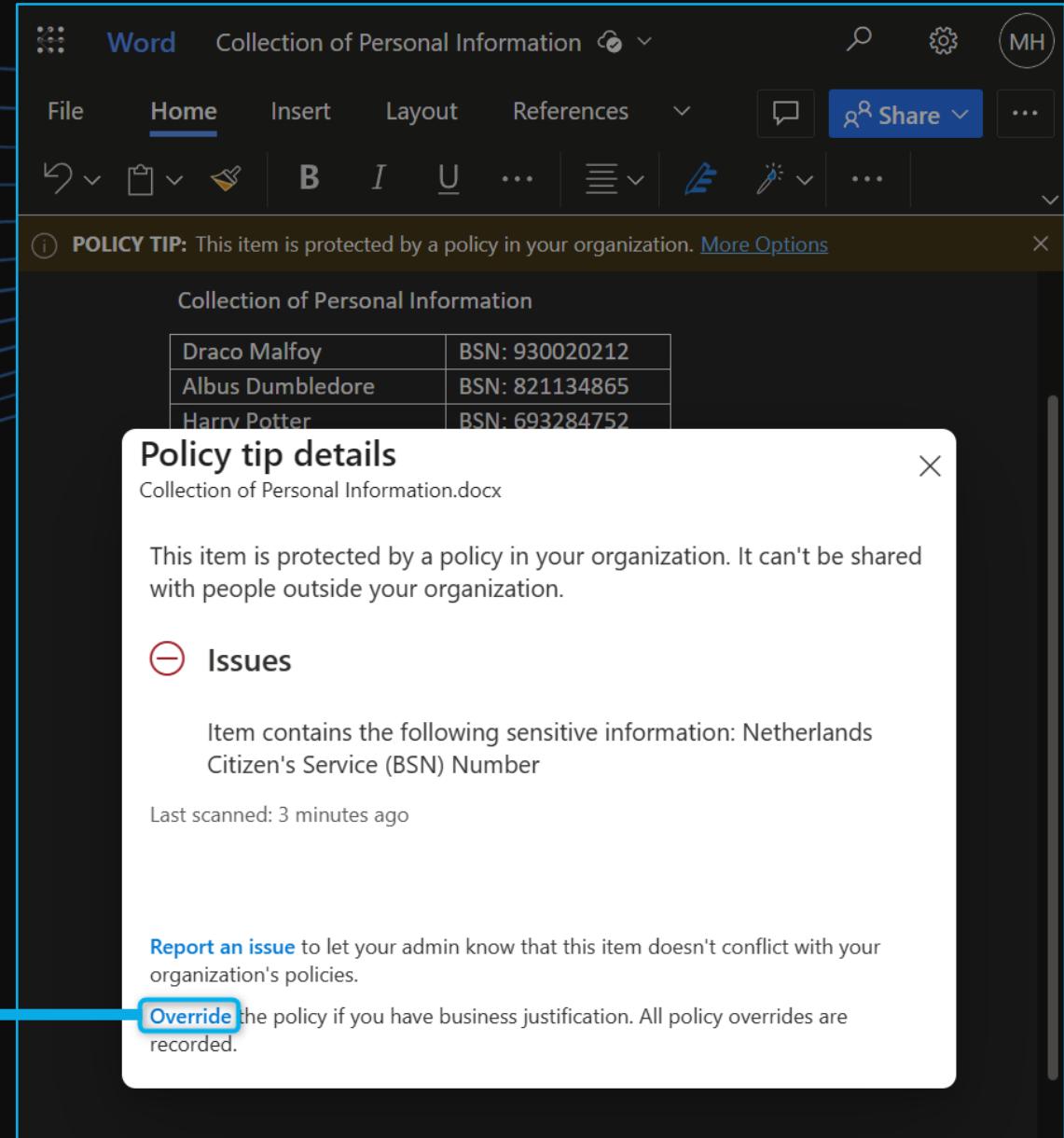
Notification only Sending external email

Block with Override

External file sharing

I need to share this with our external HR department.

Submit

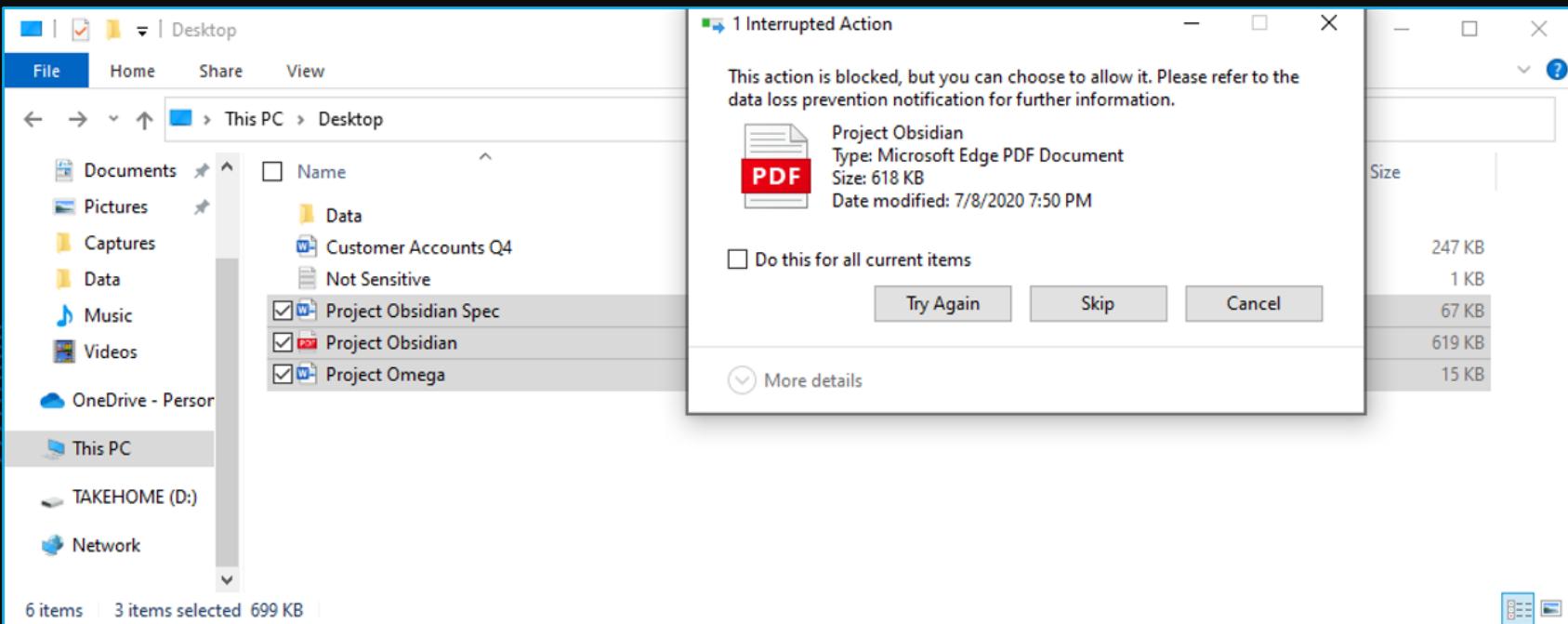


Block External chat message

The screenshot shows the Microsoft Teams Chat interface. On the left, there's a sidebar with icons for Activity, Chat (which is selected), Teams, Calendar, ..., Apps, and Help. The main area shows a conversation with "Myron Helgering (2source4)" (External). A message from Myron at 4:26 PM says, "Hello, it seems like the message was blocked by your company." A purple callout bubble over this message states, "This message was blocked. [What can I do?](#)" and "Here is the passport number you needed; SPECI0245". Below this, another message from Myron at 4:26 PM says, "Hello!". The Teams interface includes a search bar, pinned and recent chats, and a message input field at the bottom.

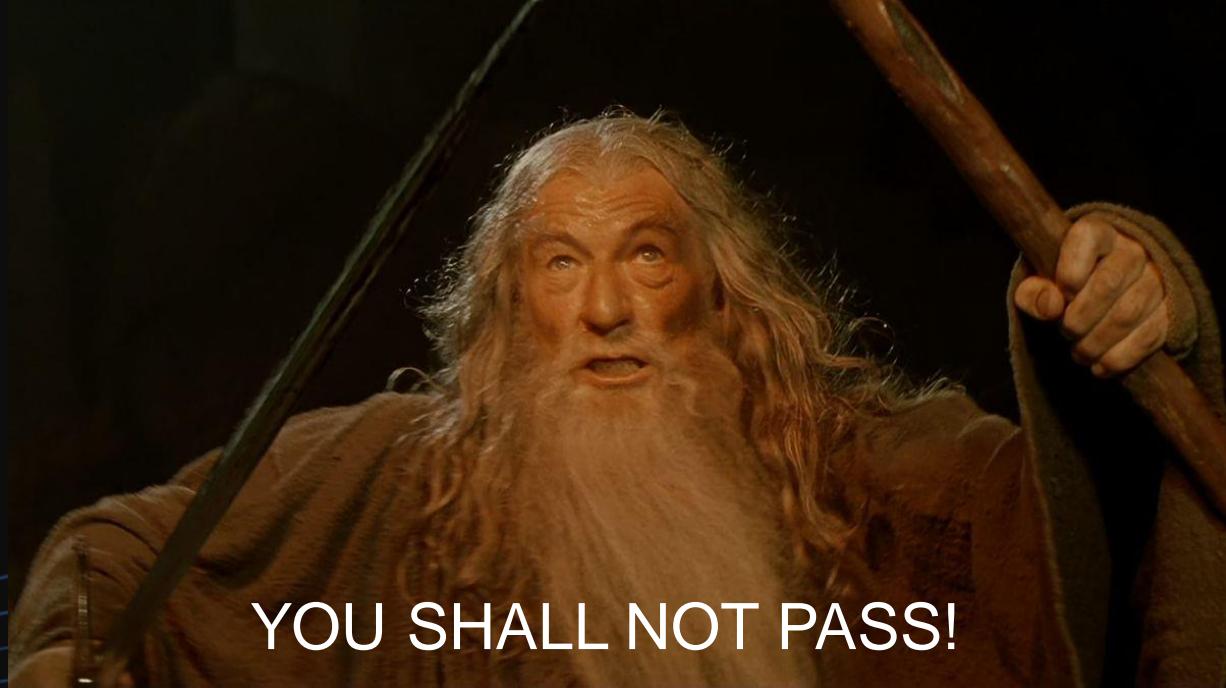
Block with override

Copy to USB (Endpoint DLP)



Method 4 Block access

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



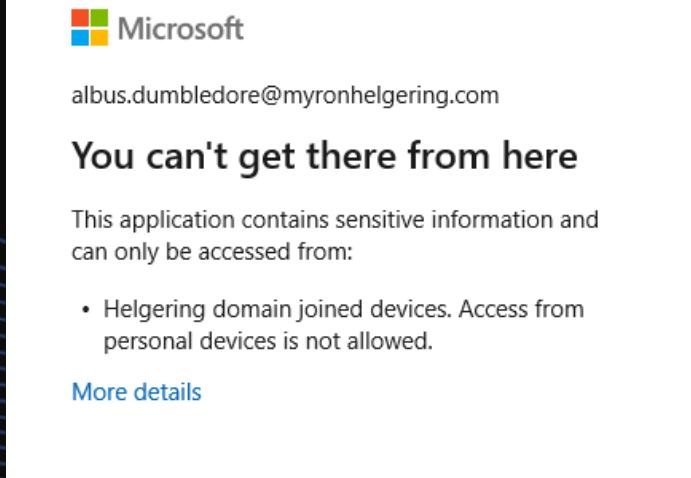
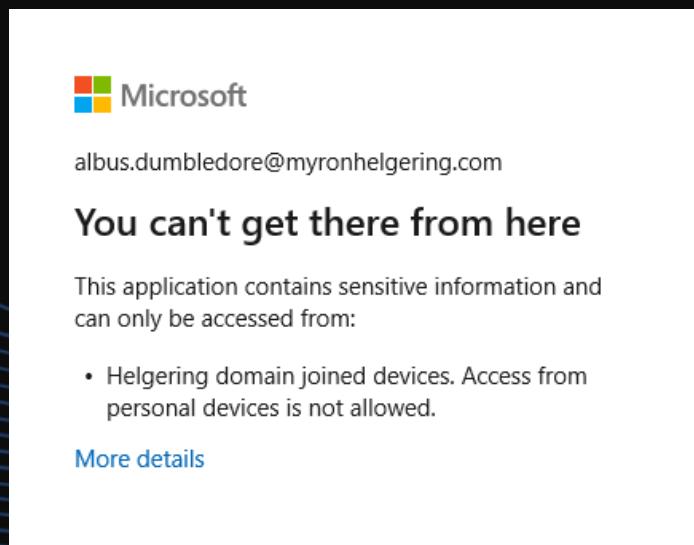
YOU SHALL NOT PASS!

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

Devices | All devices

Helgering - Azure Active Directory

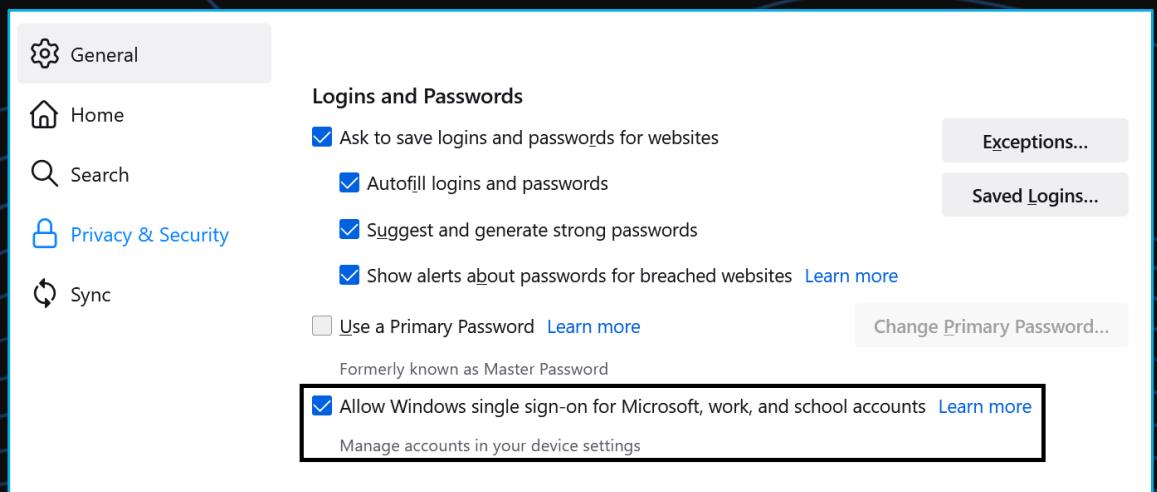
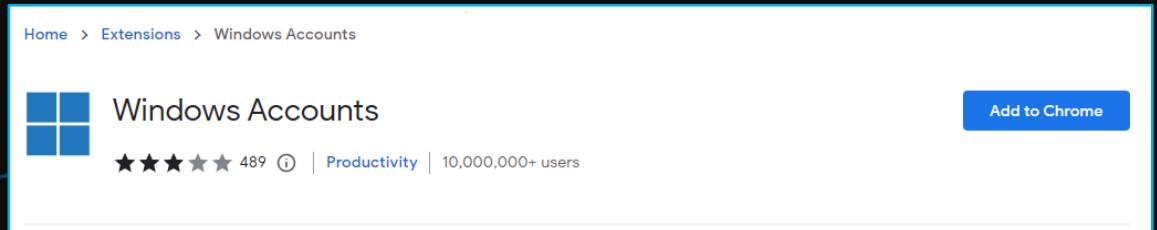
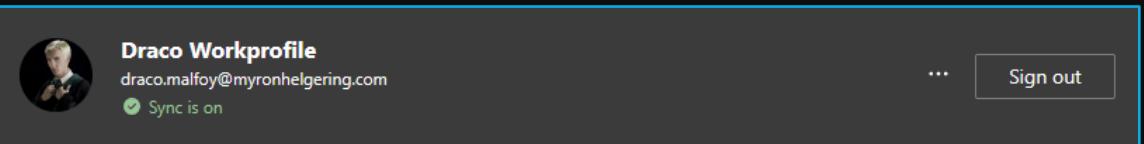
Download devices Refresh Columns Enable Disable Delete Manage Preview features Add filters

1 device found

Name ↑	OS	Join Type	Owner	MDM	Compliant
DESKTOP-1CCL42V	Windows	Azure AD registered	Draco Malfoy	None	N/A

Name ↑	OS	Join Type	Owner	MDM	Compliant
DESKTOP-AMIK1OU	Windows	Azure AD joined	Albus Dumbledore	Microsoft Intune	Yes

Single Sign On



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.



Balanced as all things should be

SharePoint admin center

- Home
- Sites
 - Active sites
 - Deleted sites
- Policies
- Sharing
- Access control**
- Settings
- Content services
- Migration
- Reports
- More features
- Customize navigation
- Show all

Access control

Unmanaged devices

Use these settings to restrict access from unmanaged devices.

Unmanaged devices

Restrict access from devices that don't use modern authentication.

Idle session sign-out

Automatically sign out users after 15 minutes of inactivity.

Network location

Allow access only from specific locations.

Apps that don't use modern authentication

Block access from Office 365 and Microsoft 365 apps.

Restrict OneDrive

Restrict access to OneDrive.

We will automatically change the "Apps that don't use modern authentication" setting to block access (because these apps can't enforce this device-based restriction).

The setting you select here will apply to all users in your organization.

[Learn more about controlling access from unmanaged devices.](#)

To customize conditional access policies, save your selection and go to the Azure AD admin center.

Allow full access from desktop apps, mobile apps, and the web

Allow limited, web-only access

Block access

If you don't want to limit or block access organization-wide, you can do so for specific sites.

[Learn how to control access to specific sites by using Microsoft PowerShell](#)

Save

Policy Name ↑↓	State ↑↓
[SharePoint admin center]Block access from apps on unmanaged devices - 2023/08/21	On
[SharePoint admin center]Use app-enforced Restrictions for browser access - 2023/08/21	On

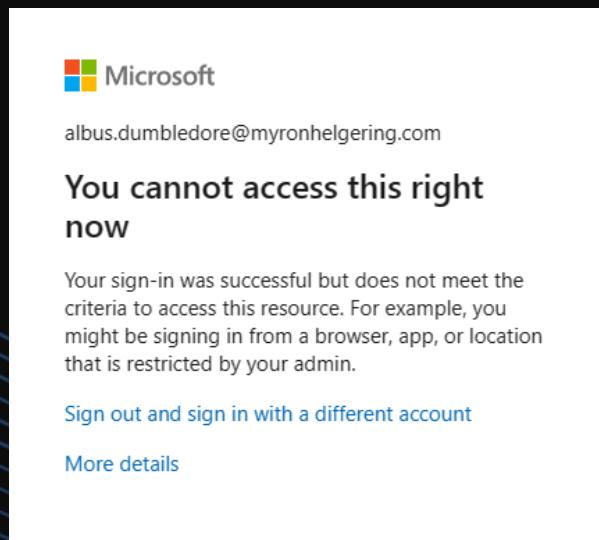
Enable in SharePoint Admin Center

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



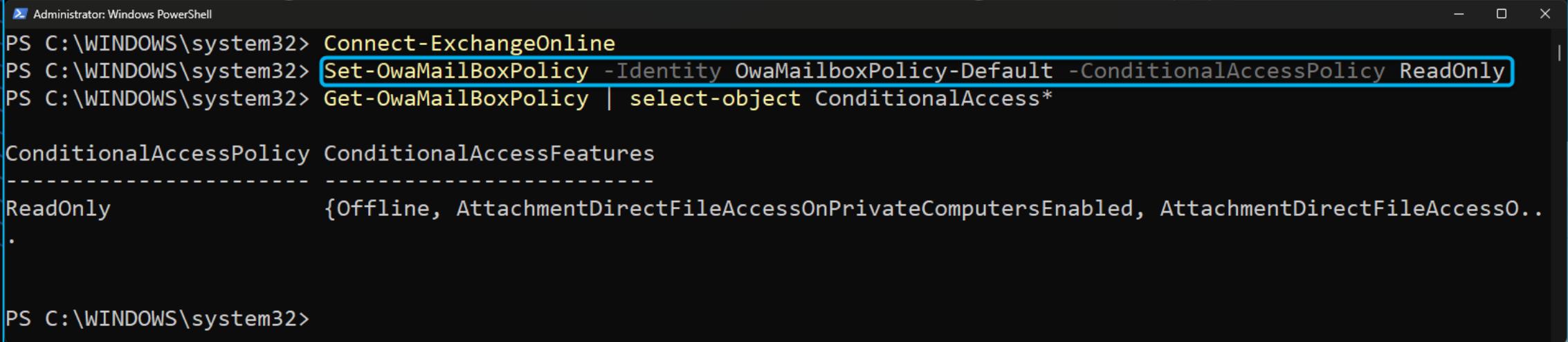
Policy 2

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

 Your organization doesn't allow you to download, print, or sync using this device. To use these actions, use a device that's joined to a domain or marked compliant by Intune. For help, contact your IT department. [More info.](#)

Enable App-Enforced Restrictions for Exchange Online with PowerShell



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Connect-ExchangeOnline
PS C:\WINDOWS\system32> Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly
PS C:\WINDOWS\system32> Get-OwaMailBoxPolicy | select-object ConditionalAccess*
ConditionalAccessPolicy ConditionalAccessFeatures
-----
ReadOnly {Offline, AttachmentDirectFileAccessOnPrivateComputersEnabled, AttachmentDirectFileAccessO...
.
.

PS C:\WINDOWS\system32>
```

Set-OwaMailBoxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly

Sensitivity Labels

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

Edit sensitivity label

Progress bar:

- Name and tooltip
- Scope
- Items
- Groups & sites**
- External sharing & conditional access
- Schematized data assets (preview)
- Finish

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Use Azure AD Conditional Access to protect labeled SharePoint sites
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [hybrid Azure AD joined](#) or enrolled in Intune).
(i) For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#)

Allow full access from desktop apps, mobile apps, and the web

Allow limited, web-only access (i)

Block access (i)

[Back](#) [Next](#) [Cancel](#)

Method 6 Session Monitoring

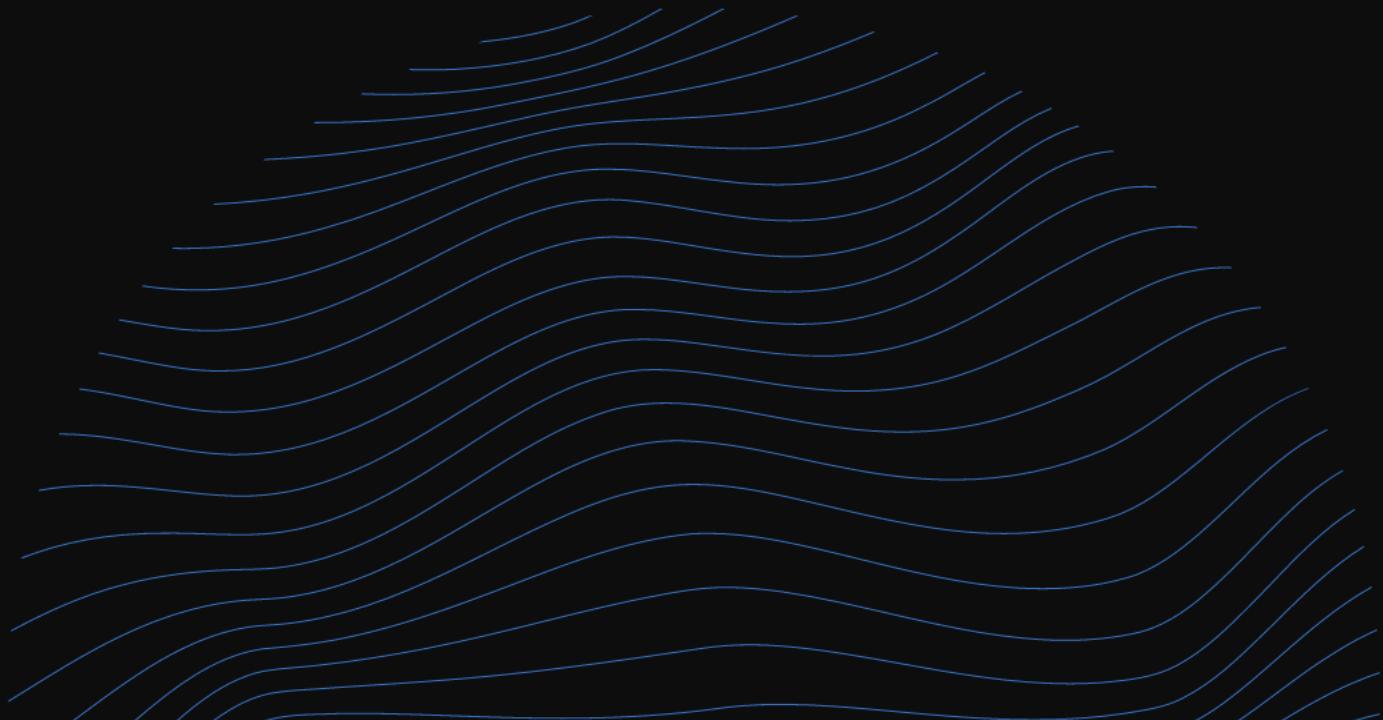
- Enforce web session monitoring
- Restrict download, print, cut, copy, and more!
- Supports more cloud apps



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

Apps | App protection policies

+ Create policy

Policy	Deployed	Platform
MAM for Android - all users	Yes	Android
MAM for iOS - all users	Yes	iOS/iPadOS

Search

Overview

All apps

Monitor

By platform

Windows

iOS/iPadOS

macOS

Android

App protection policies

Require MAM with CA policy

- Authenticator app for iOS
- Company Portal app for Android

Name *****
CA30 - Require MAM for Android & iOS

Assignments

Users **(i)**
All users included and specific users excluded

Target resources **(i)**
All cloud apps

Conditions **(i)**
1 condition selected → Select device platforms
 Android
 iOS

Access controls

Grant **(i)**
1 control selected → Require app protection policy

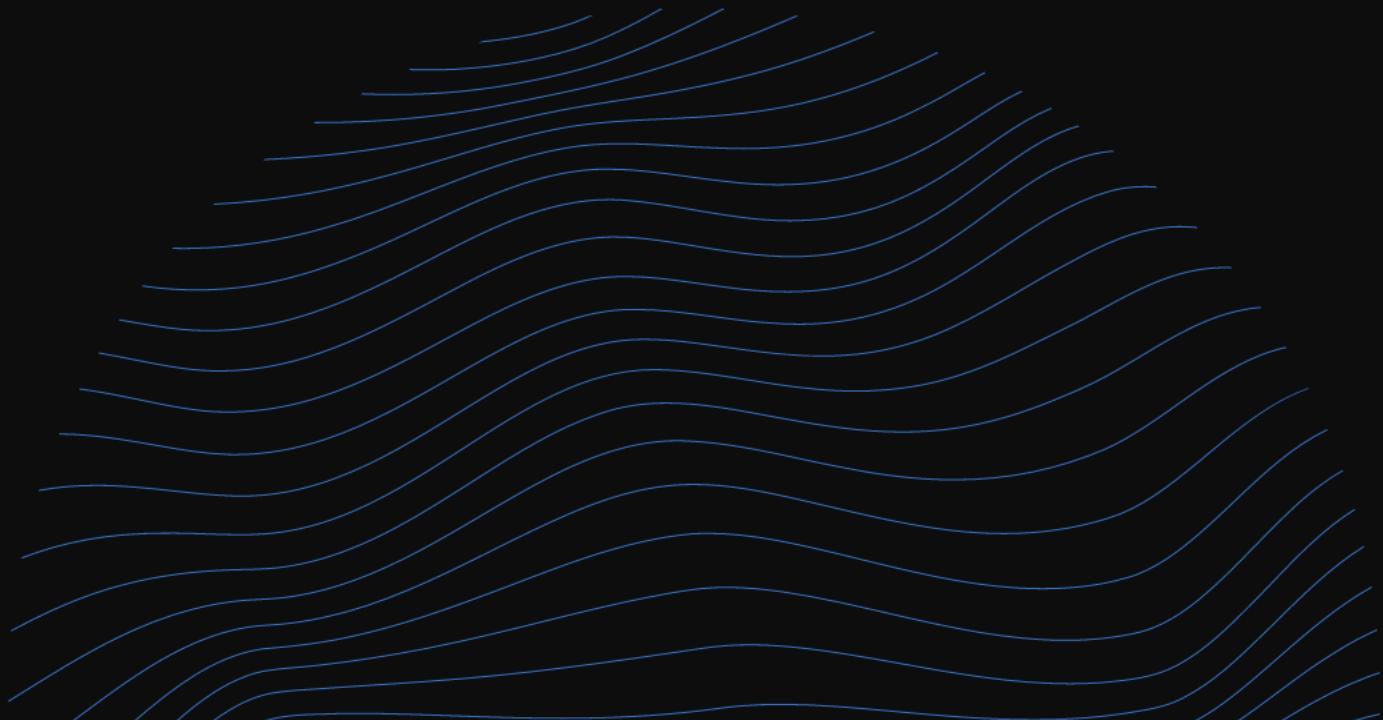
Windows Information Protection

The screenshot shows the 'Create policy' dialog in the Microsoft Endpoint Manager admin center. The title bar says 'Home > Apps | App protection policies > Create policy'. The tabs at the top are 'Basics' (selected), 'Targeted apps', and 'Required settings'. The 'Basics' tab has three steps: 'Name *' (WIP without enrollment), 'Description' (empty), and 'Enrollment state' (With enrollment). A note at the bottom says: 'Creating new WIP without enrollment policies (WIP-WE) is no longer supported. For more information, see 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 Single Sign On for Chrome and Firefox



@MyronHelgering



in/myronhelgering



myronhelgering.com

Thank you!



@MyronHelgering



in/myronhelgering



myronhelgering.com