Session:

Date 18 April: 16:30

Protecting corporate data on personal Windows devices - Your options

Peter van der Woude

MODERN ENDPOINT MANAGEMENT

Welcome to:

MODERN
ENDPOINT
MANAGEMENT

SUMMIT 2024

APRIL 17 - 19

GOLD PARTNERS

controlUP

Microsoft

THANK YOU PARTNERS

GOLD PARTNERS

controlUP

Microsoft

SILVER PARTNERS

adaptiva

LIQUIT
Part of RECAST SOFTWARE

PATCH MY PC

TANIUM

Rimo3

BRONZE PARTNERS

Synapsys

About me

SPEAKER

Peter van der Woude

www.petervanderwoude.nl

@pvanderwoude

/peterwoude

MODERN ENDPOINT MANAGEMENT SUMMIT EMEA 2024

Protecting corporate data on personal Windows devices - Your options

Agenda

Why is it important to protect corporate data on personal devices

What are the options for protecting corporate data on personal Window devices

A closer look at the details of MAM for Windows

How do the different options for protecting corporate data compare

Why is it important to protect corporate data on personal devices


Prevention


Visibility


CROQUIS DE MANZANA ESC. 1:1000
CALCULO DE MODULOS DE ESTACIONAMIENTO
DETALLE DE ESCALERA PRINCIPAL - PLANTA-
ESC.: 1:20
SILUETA Y BALANCE DE SUPERFICIES
Comply


Protect

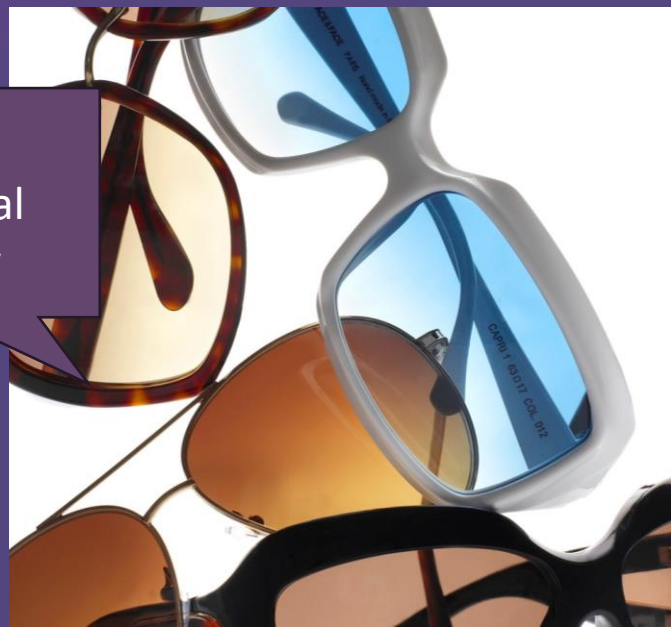
Why is it important?

Comply with regulations

Visibility into data

Prevent data loss

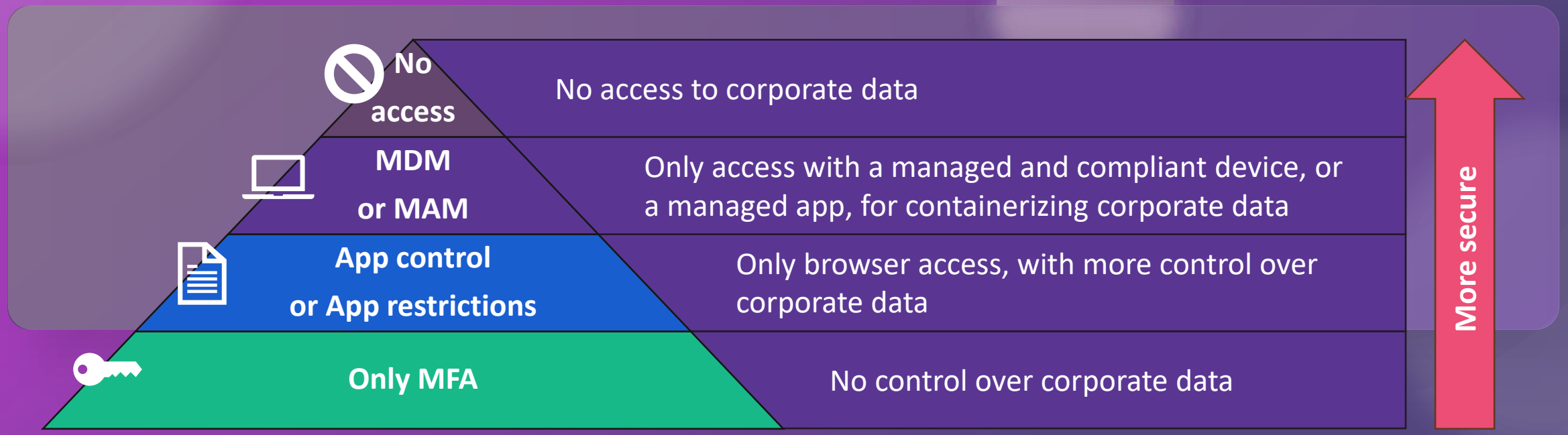
Protect intellectual property



What are the options for protecting corporate data on personal devices

Protecting corporate data on personal devices

All options rely on Conditional Access for enforcement



Overview inspired by: The Underwhelming MAM for Edge and What Else We Can Do - ITProMentor

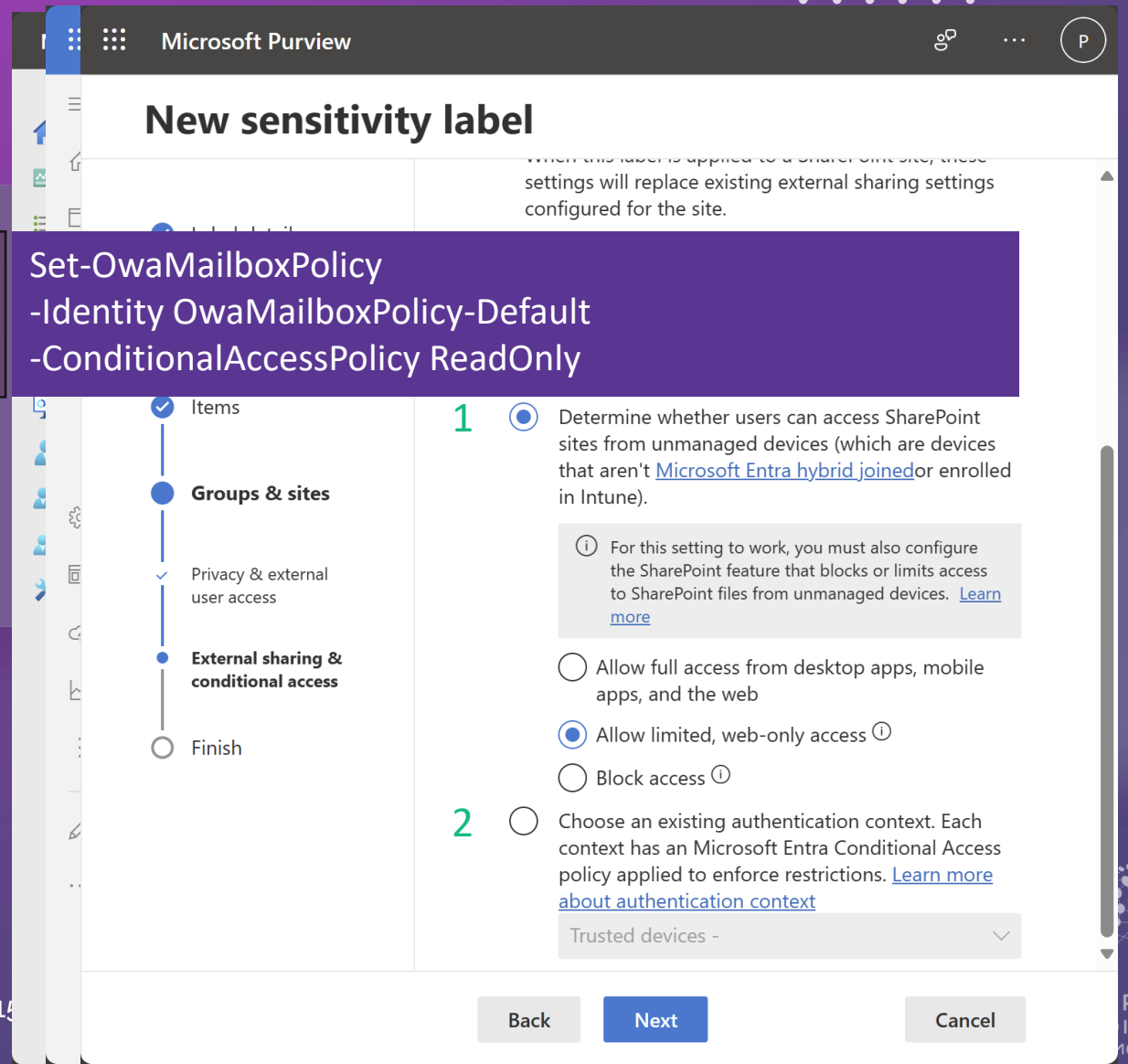
MODERN ENDPOINT MANAGEMENT

Specifically for personal Windows devices

What are the realistic options?

Conditional Access with App Enforced Restrictions

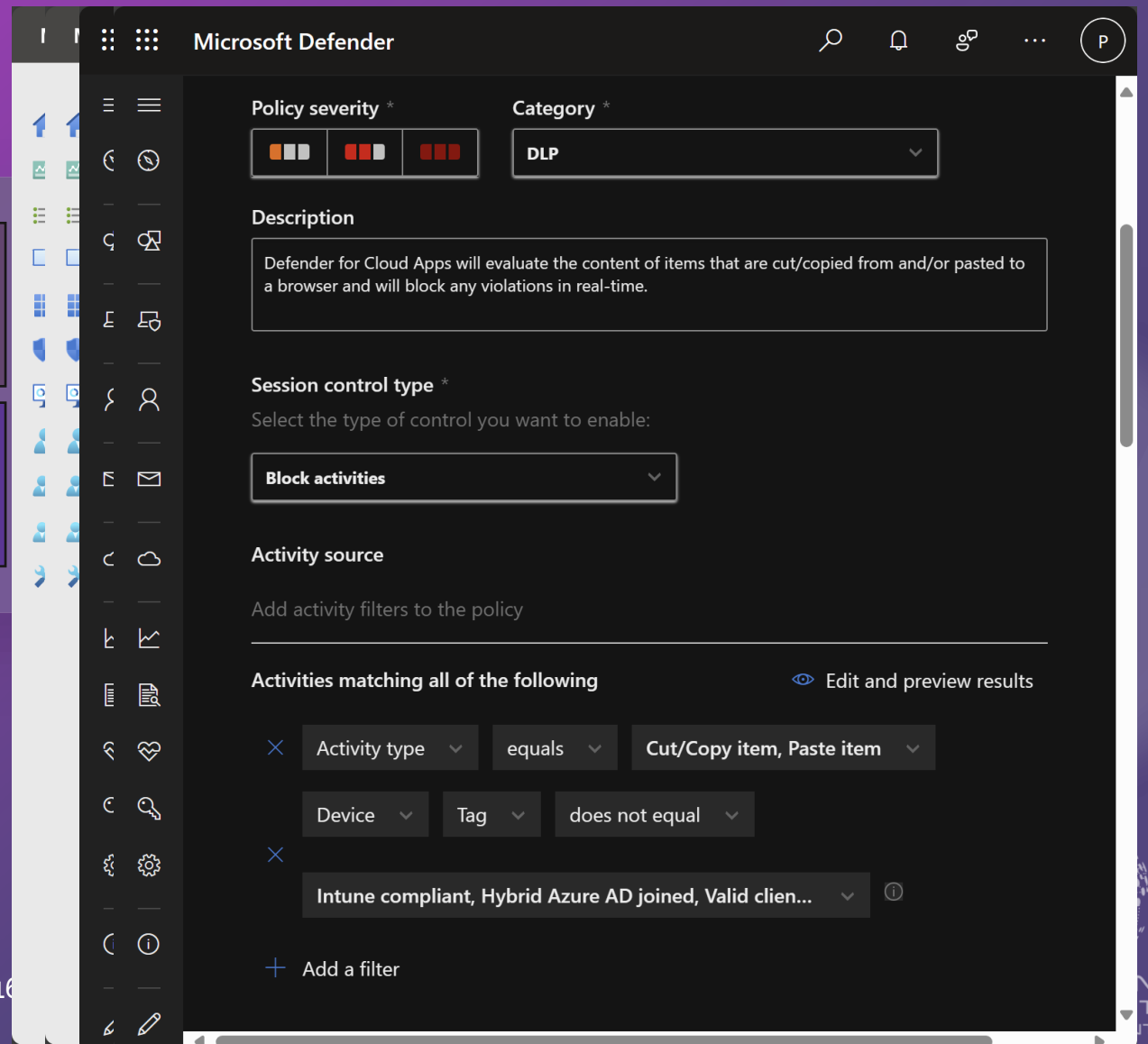
Set-OwaMailboxPolicy
-Identity OwaMailboxPolicy-Default
-ConditionalAccessPolicy ReadOnly



Specifically for personal Windows devices

What are the realistic options?

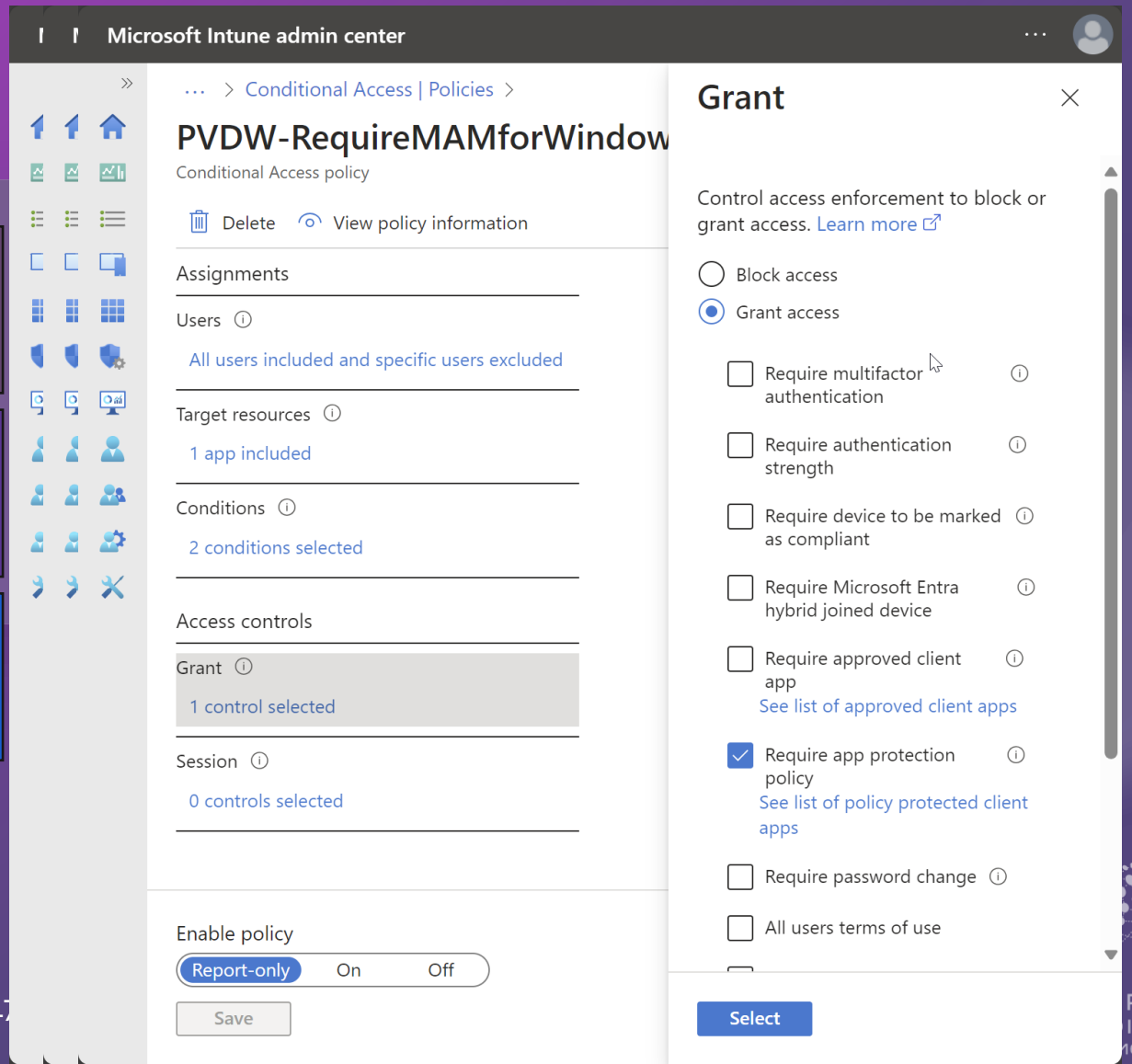
- Conditional Access with App Enforced Restrictions
- Conditional Access with App Control (Defender for Cloud Apps)



Specifically for personal Windows devices

What are the realistic options?

- Conditional Access with App Enforced Restrictions
- Conditional Access with App Control (Defender for Cloud Apps)
- Conditional Access with App Protection Policies (MAM for Windows)



Combining technologies

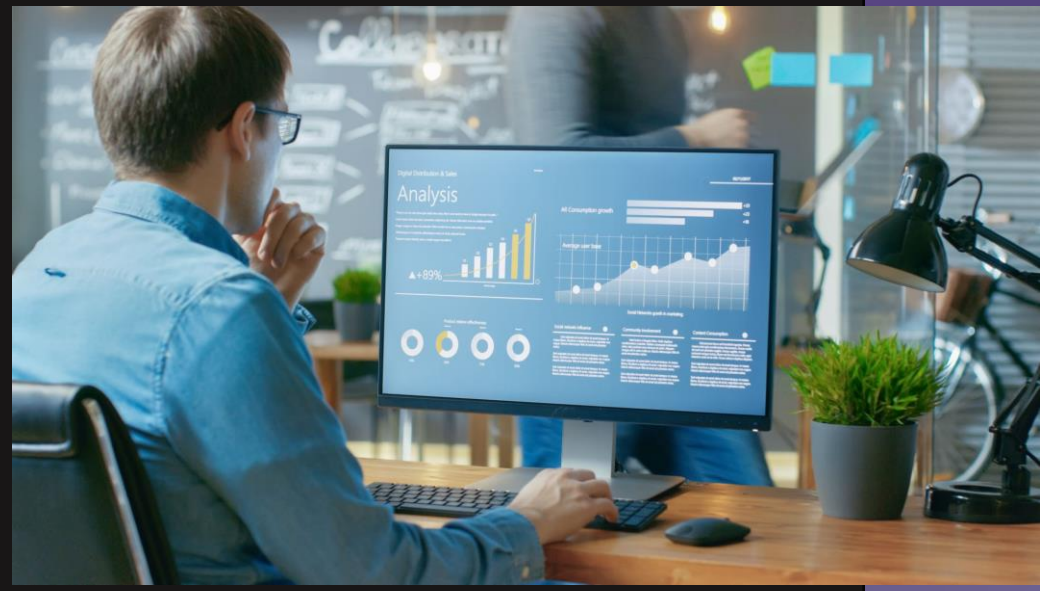
The most obvious combinations

Option 1	Option 2
 Conditional Access with App Enforced Restrictions	 Conditional Access with App Control (Defender for Cloud Apps)
 Conditional Access with App Protection Policies (MAM for Windows)	 Conditional Access with App Protection Policies (MAM for Windows)

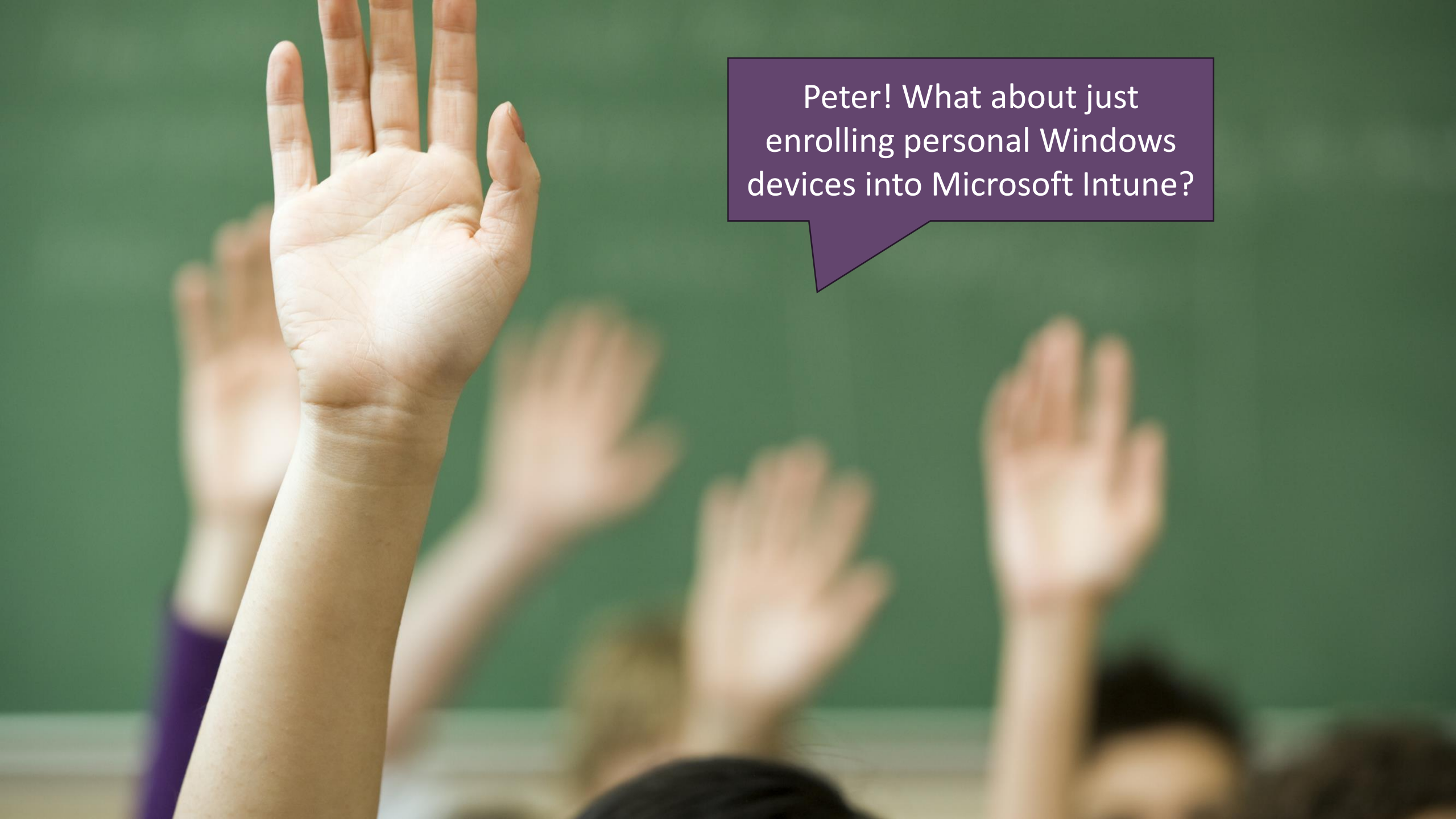
Combining technologies

Main reasons for combining technologies

- More granularity
  - Differentiate between data sensitivity
  - Differentiate between device state
  - Differentiate between sites
- Protect local data (including remote wipe)
- Configure important browser settings
- Best of both worlds



MODERN ENDPOINT MANAGEMENT


Peter! What about just enrolling personal Windows devices into Microsoft Intune?

Should you allow personal Windows devices?

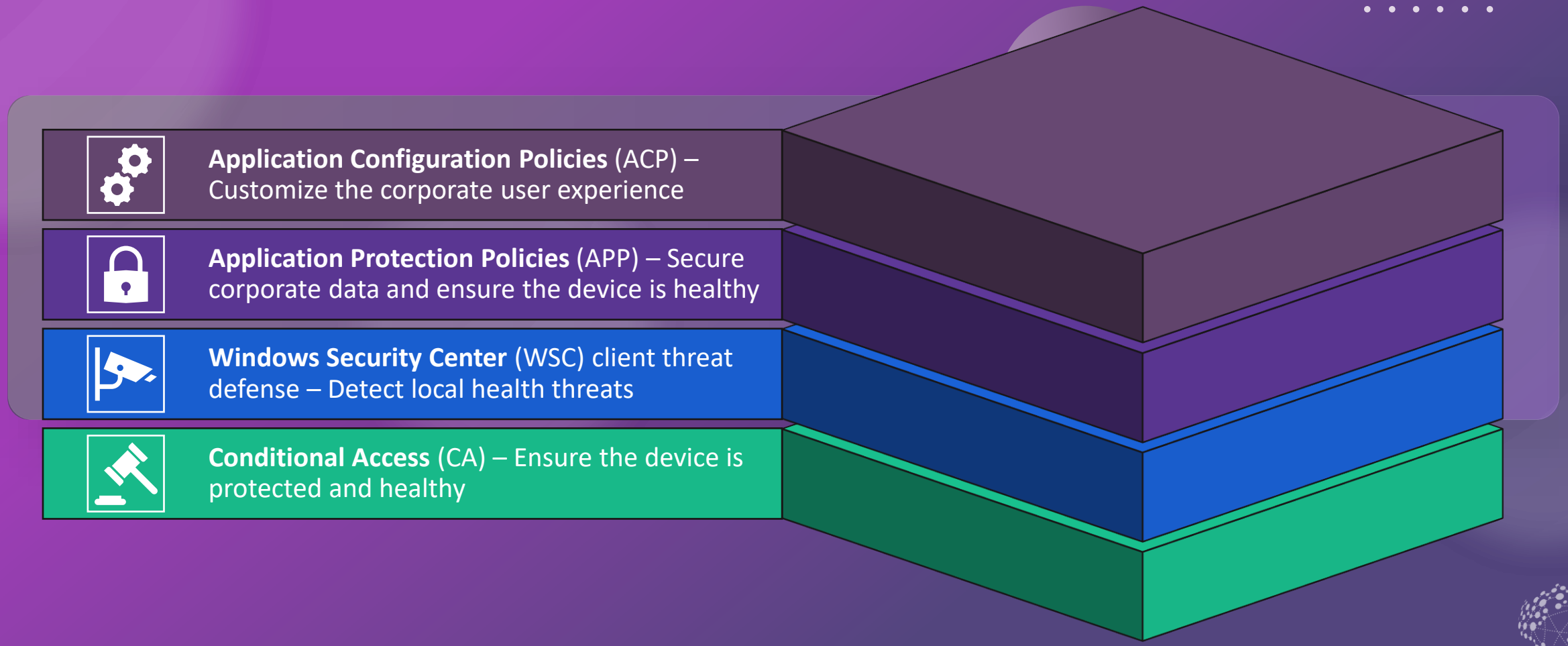
Note: I might be slightly biased by now

Summary

Ultimately, it's a business decision, BUT
it will be a security nightmare,
with potential legal challenges,
…and a suboptimal user experience

A closer look at MAM for Windows (for Edge)

Layers of MAM for Windows

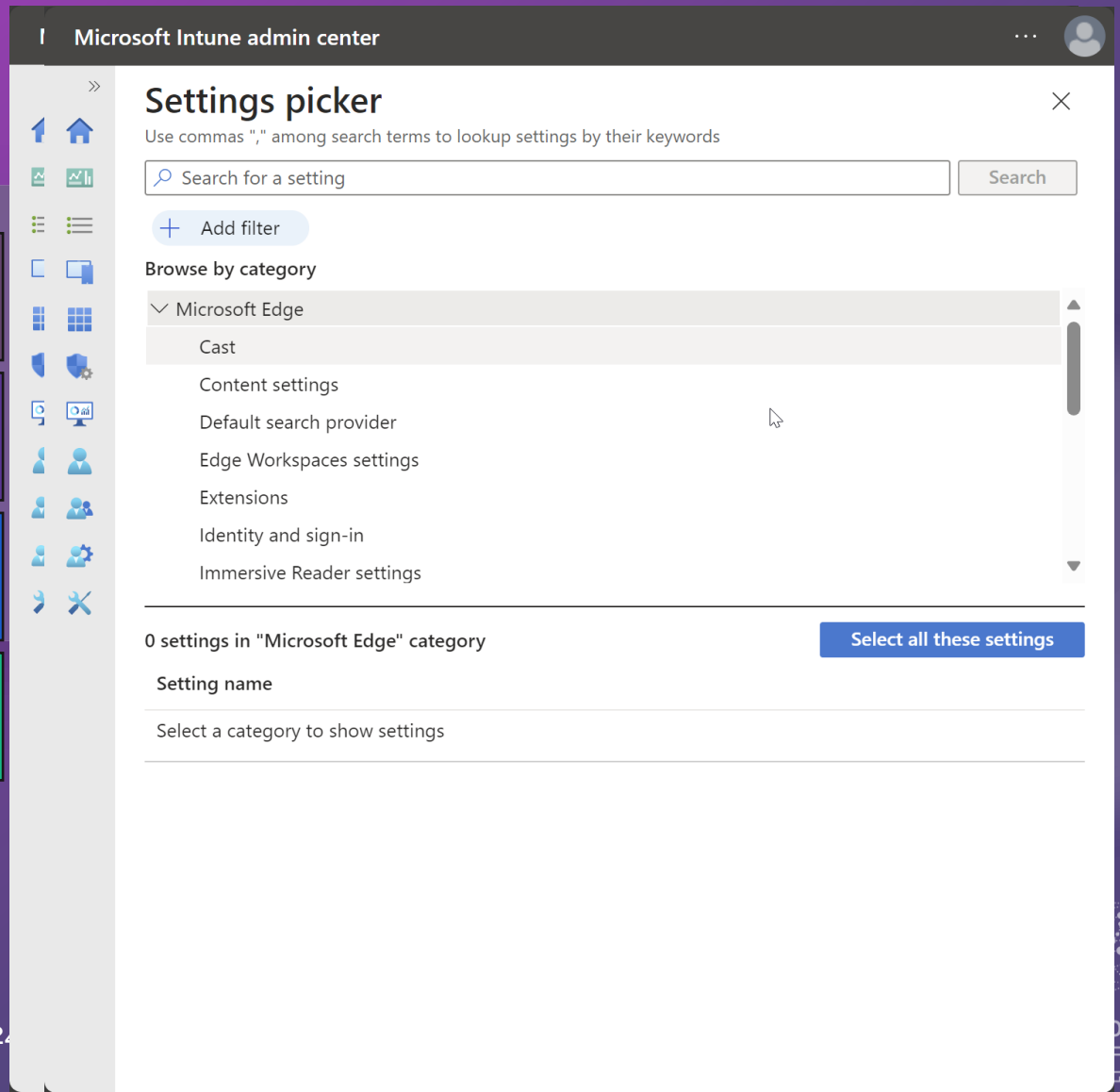


MODERN ENDPOINT MANAGEMENT

Customizing the user experience

Important configuration options

- Create a policy for managed apps
- Select the required app
- Configure the required settings
- Configure the assignment



Protecting corporate data

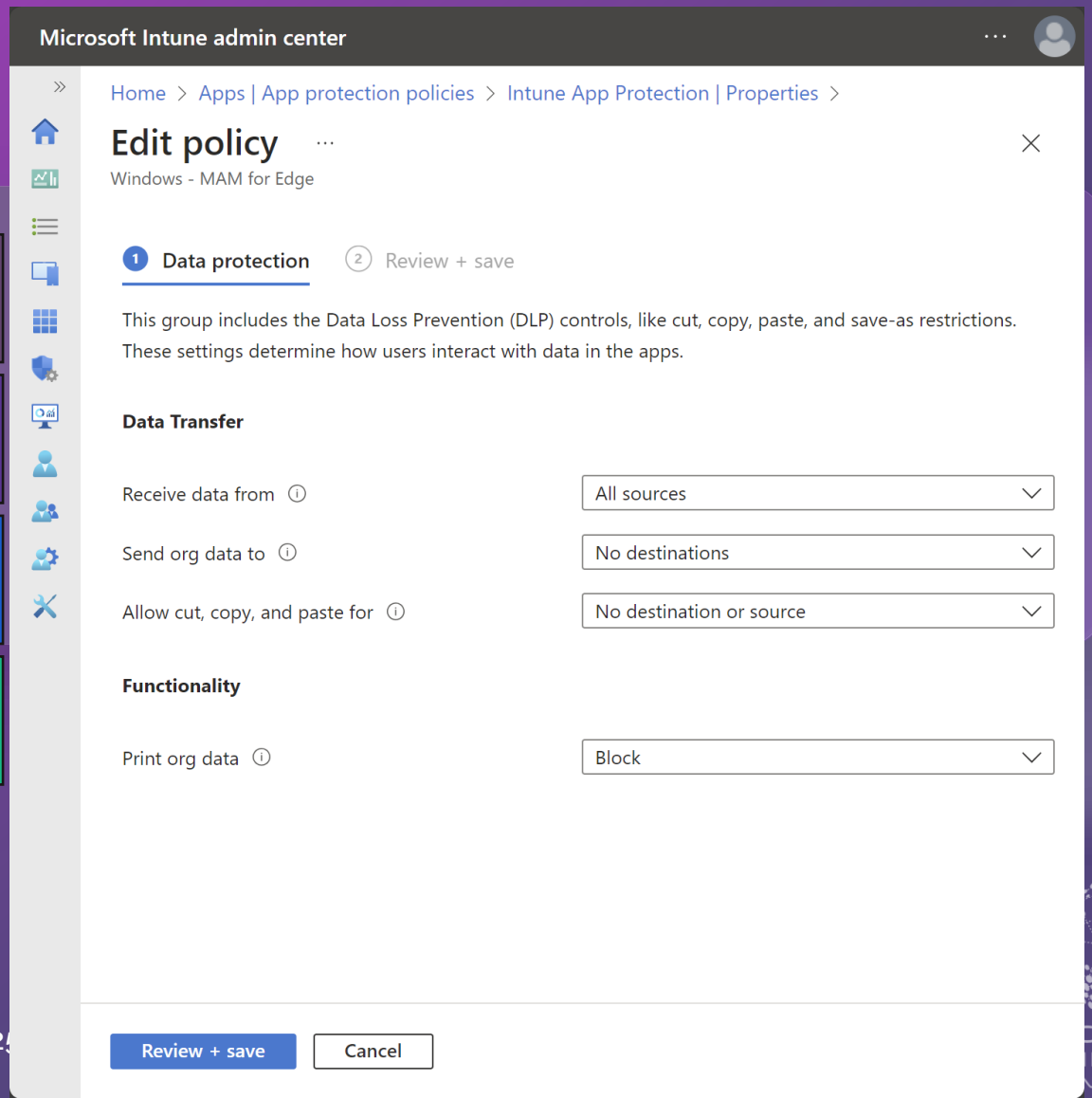
Data protection options

Receive data from – Configure the sources that users can receive data from

Send org data to – Configure the destinations that users can send corporate data to

Allow cut, copy, and paste for – Configure the sources and destinations users can cut or copy or paste org data for

Print org data – Configure if users are allowed to print corporate data, or not

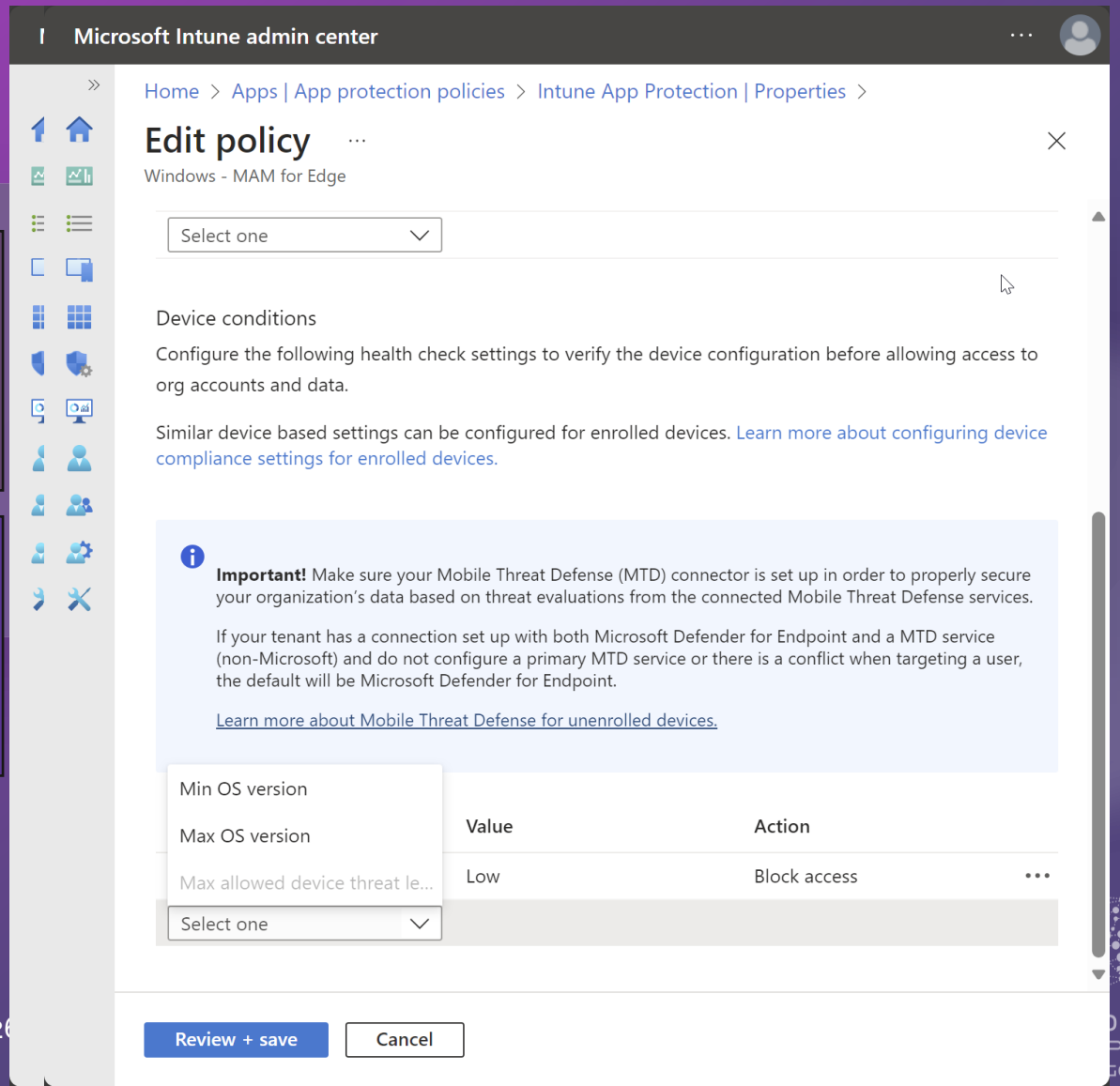


Protecting corporate data

Health checks configuration options

Configure the health check settings to verify the application configuration before allowing access to corporate accounts and data

Configure the health check settings to verify the device configuration before allowing access to corporate accounts and data

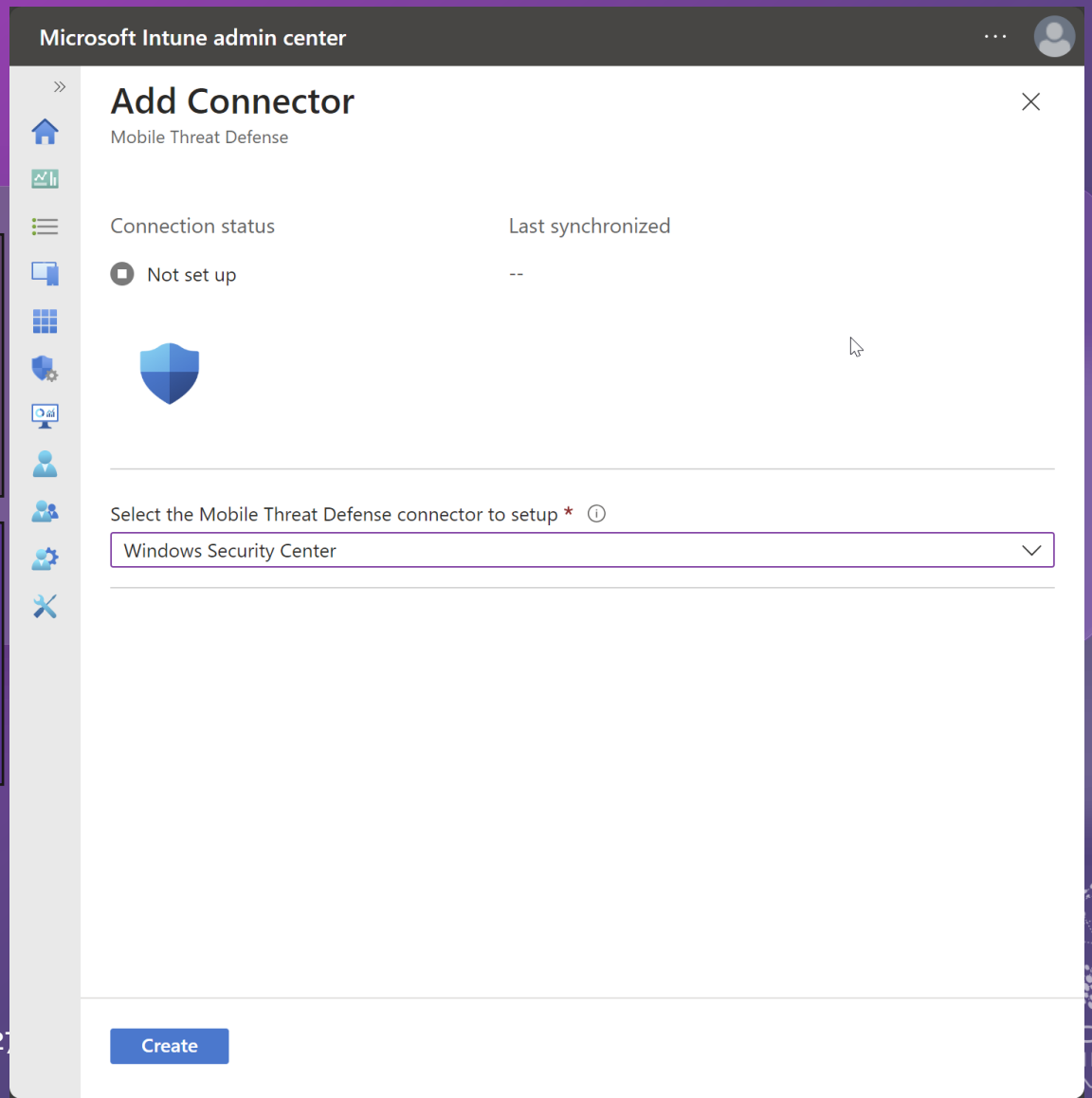


Detecting local health threats

Mobile threat defense connector options

Configure the **Mobile Threat Defense** connector that integrates directly with APP for information about local threats

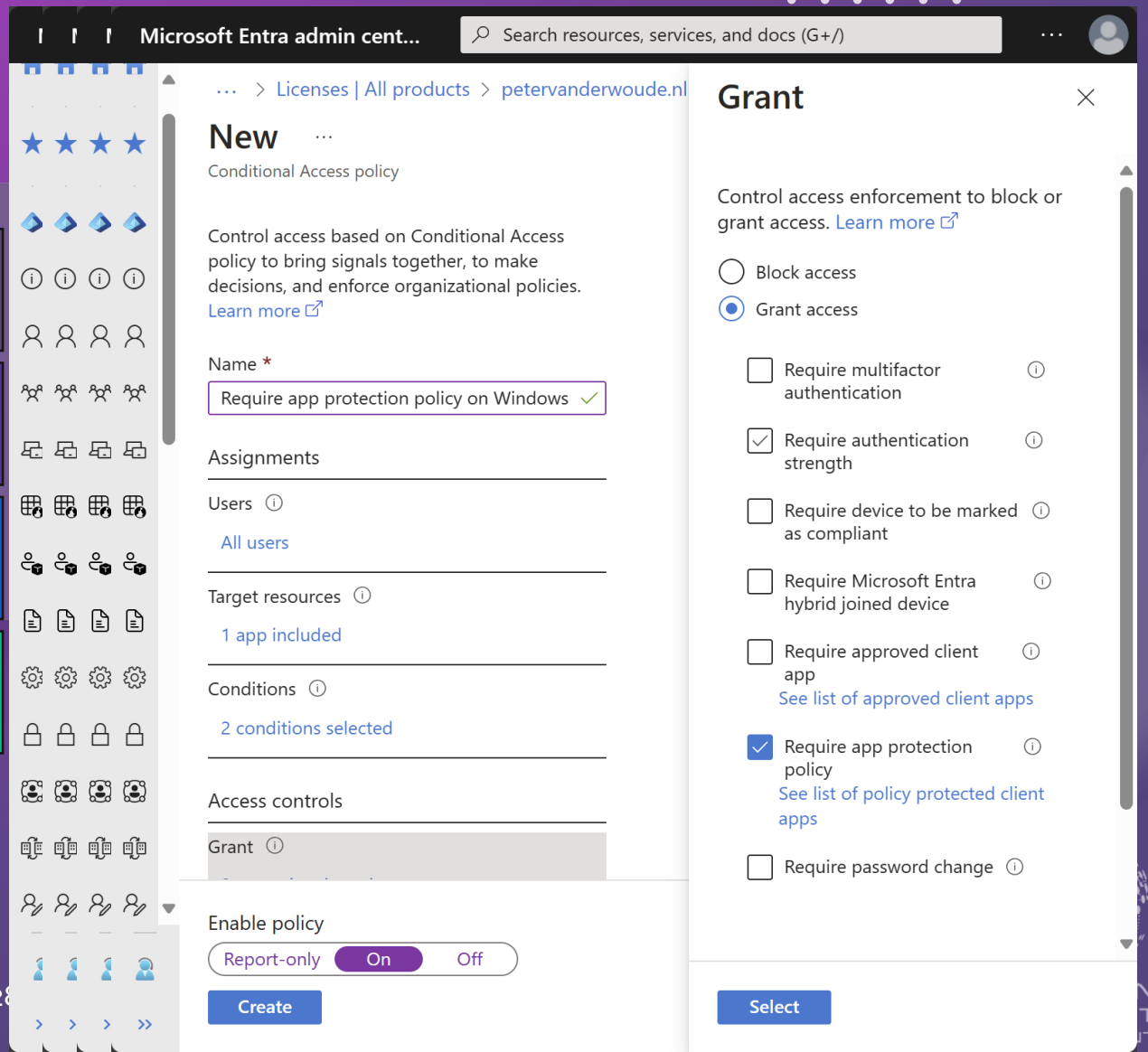
The health state includes user, app, and device identifiers, a predefined health state, and the time of last health state update



Ensuring device is protected

Conditional Access configuration options

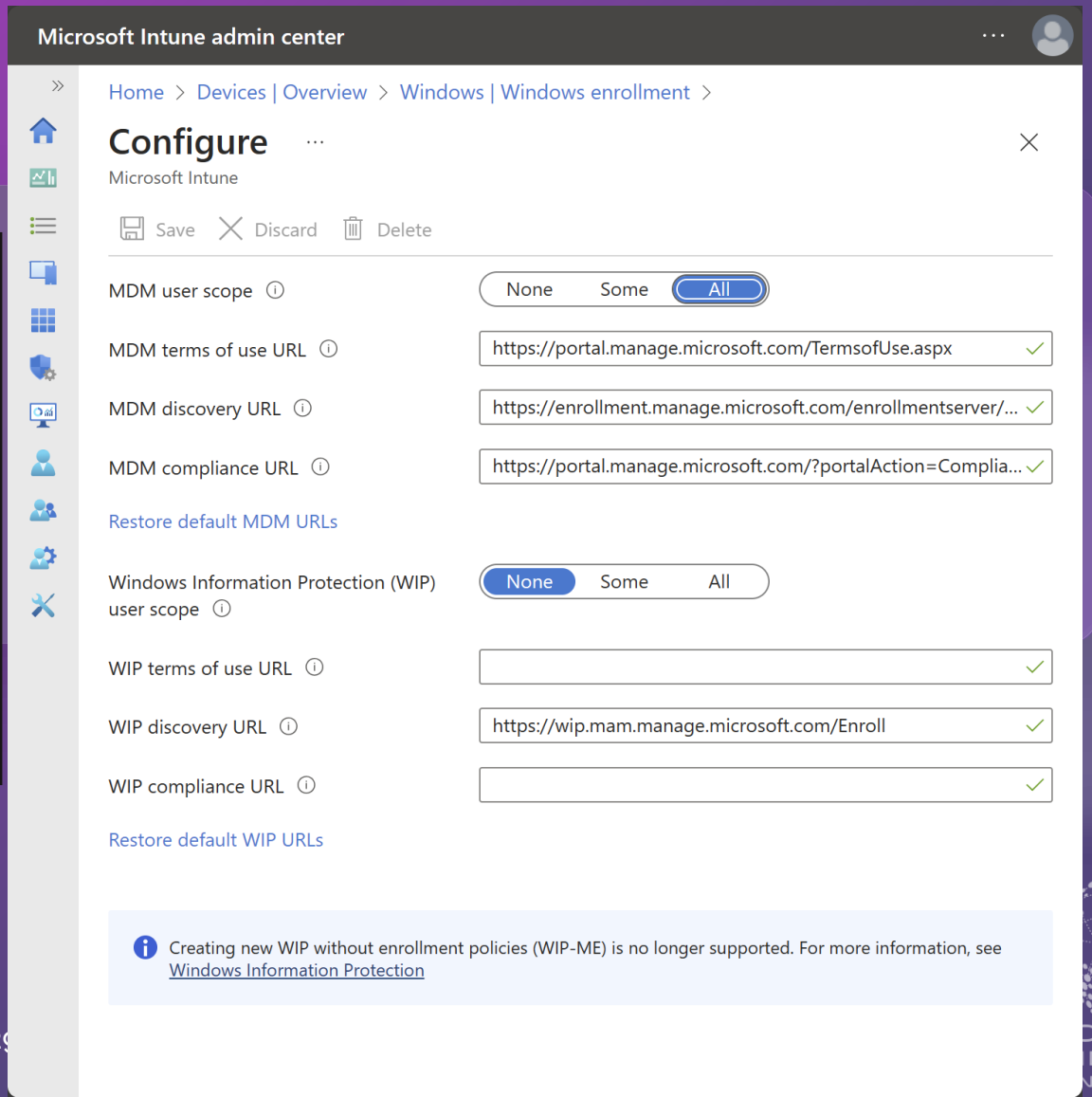
- Assignment to **All users** with the required exclusions
- Targeted resources to **Office 365**
- Conditions for **Windows** as platform and **Browser** as client apps
- Access control **Require app protection policy** with additional requirements



Important (non-)configurations

Configurations that are **definitely NOT** required

You do **NOT** have to configure the **MAM user scope**. For clarity Microsoft renamed this to **Windows Information Protection user scope**.



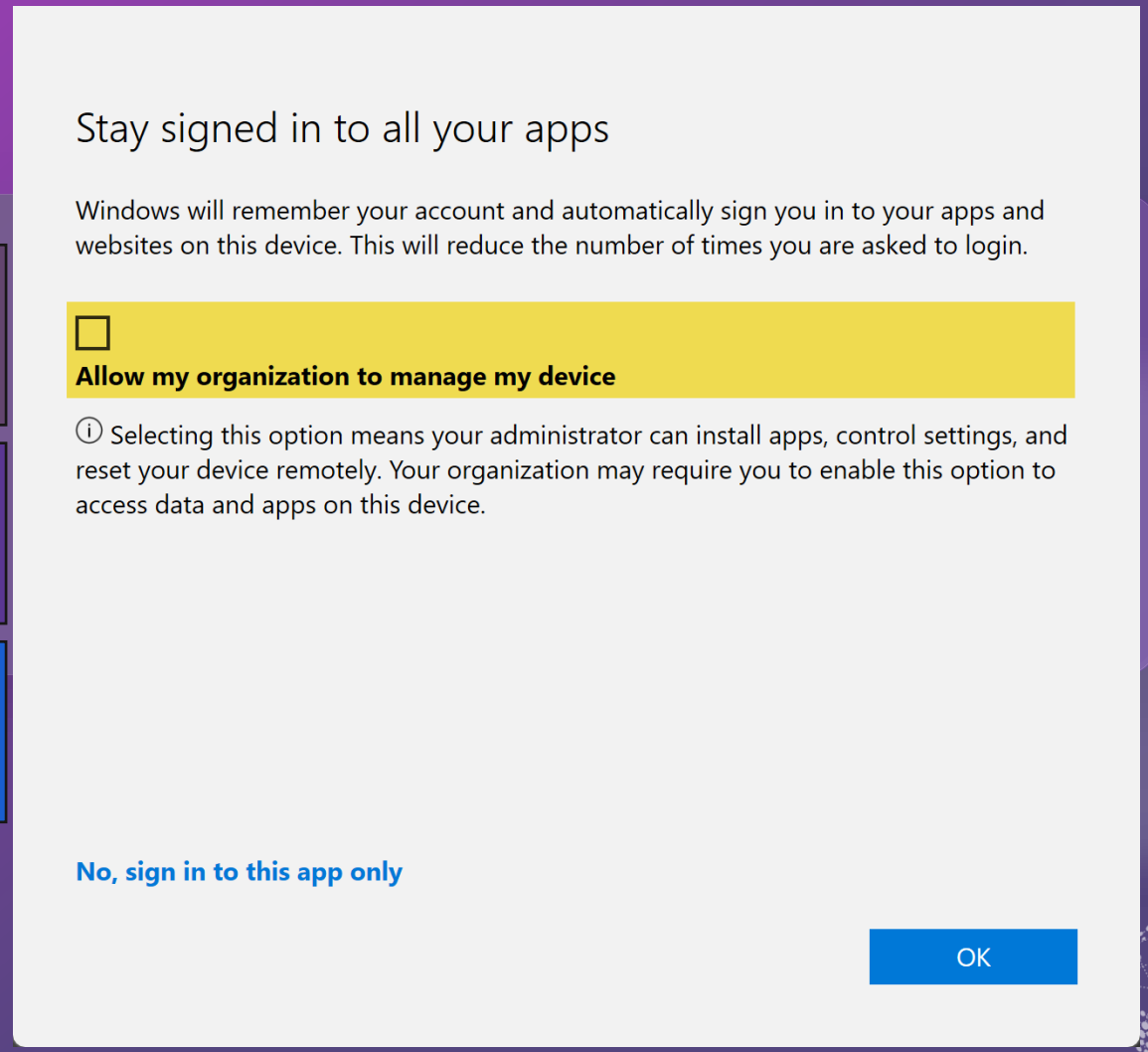
User experience

Experience for the end user

You should **NOT** check the box with **Allow my organization to manage my device**

When a device is managed through MDM, the MAM enrollment is blocked

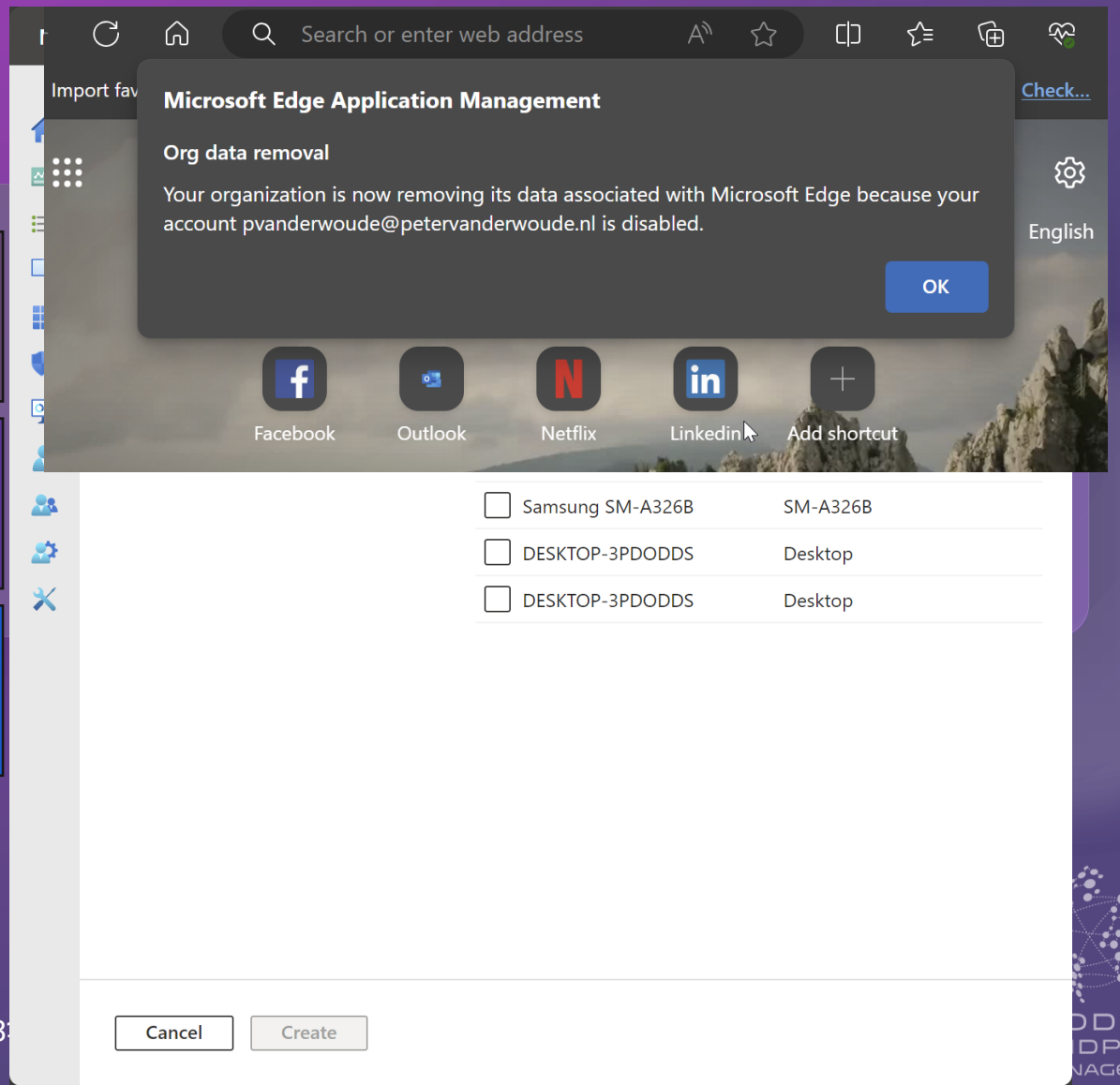
When a device becomes managed, after MAM enrollment, the applicable policies are no longer applied



App selective wipe

Selective wipe options

- Selectively remove company data when a device is lost or stolen, or if the employee leaves the company.
- Use a wipe request to remove company data from the device.
- Monitor the status of the wipe request to see if the action was successful.



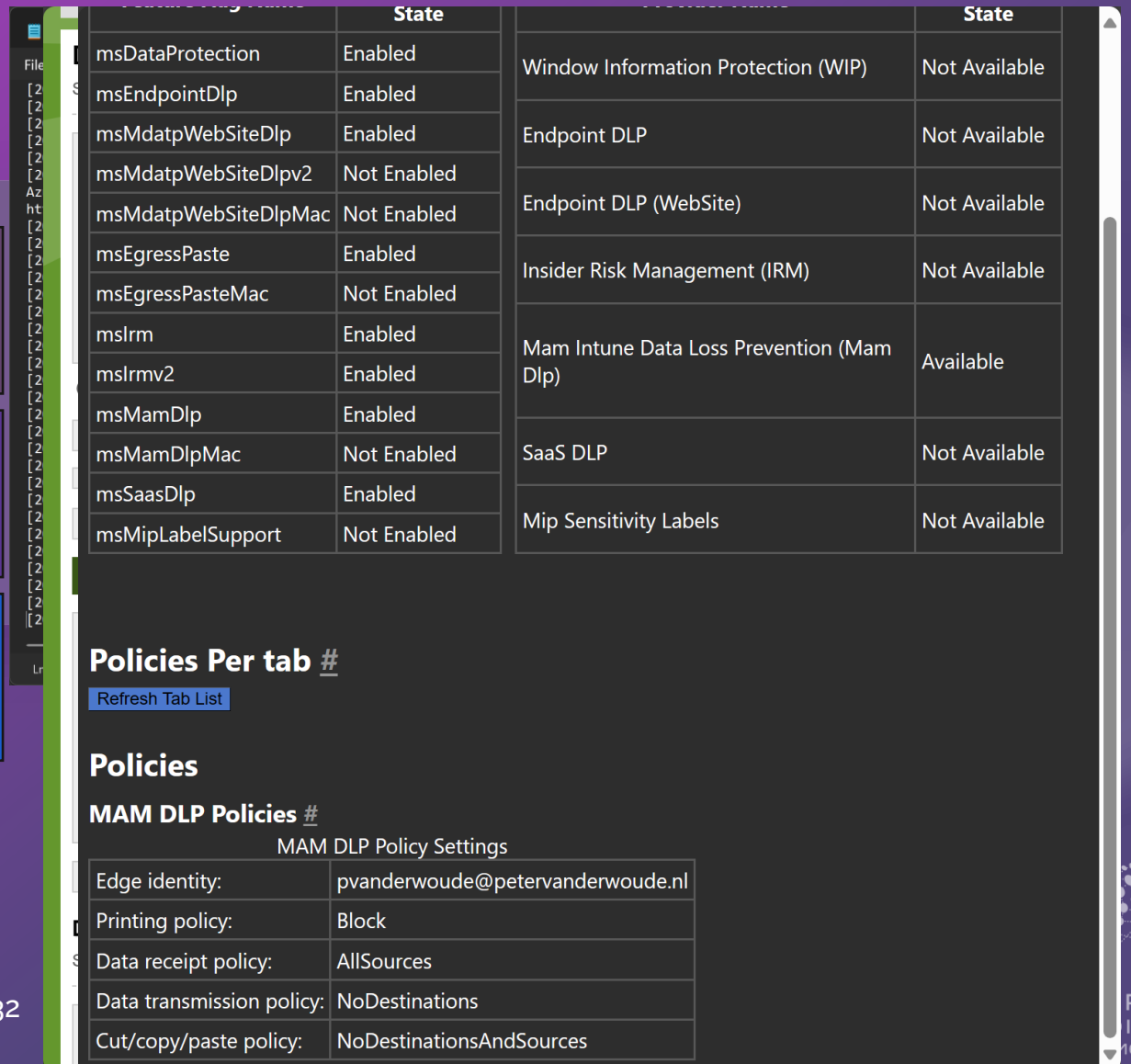
Troubleshooting

Most common options for troubleshooting

%userprofile%\AppData\Local\Microsoft\Edge\User Data\MamLog.txt

%userprofile%\AppData\Local\Microsoft\Edge\User Data\MamCache.json

edge://edge-dlp-internals/



	State
msDataProtection	Enabled
msEndpointDlp	Enabled
msMdatpWebSiteDlp	Enabled
msMdatpWebSiteDlpv2	Not Enabled
msMdatpWebSiteDlpMac	Not Enabled
msEgressPaste	Enabled
msEgressPasteMac	Not Enabled
msIrm	Enabled
msIrmv2	Enabled
msMamDlp	Enabled
msMamDlpMac	Not Enabled
msSaasDlp	Enabled
msMipLabelSupport	Not Enabled

	State
Window Information Protection (WIP)	Not Available
Endpoint DLP	Not Available
Endpoint DLP (WebSite)	Not Available
Insider Risk Management (IRM)	Not Available
Mam Intune Data Loss Prevention (Mam Dlp)	Available
SaaS DLP	Not Available
Mip Sensitivity Labels	Not Available

Policies Per tab #

Refresh Tab List

Policies

MAM DLP Policies #

MAM DLP Policy Settings

Edge identity:	pvanderwoude@petervanderwoude.nl
Printing policy:	Block
Data receipt policy:	AllSources
Data transmission policy:	NoDestinations
Cut/copy/paste policy:	NoDestinationsAndSources

How do the different options compare for personal devices

How do they compare?

Most basic components for comparing

	App enforced restrictions	App protection	App control
Enrollment	N/a	App enrollment	N/a
Management	N/a	App management	N/a
Data protection	Session controlled	App level	Session controlled
Supported apps	SharePoint, OneDrive and Exchange	All Cloud apps	All Cloud apps when connected
Supported browser	Microsoft Edge, Google Chrome, Mozilla Firefox	Microsoft Edge	Microsoft Edge, Google Chrome, Mozilla Firefox
Required license	Microsoft 365 E3	Microsoft 365 E3	Microsoft 365 E5
Admin experience	Straight forward	Straight forward	More complex
User experience	Straight forward	More complex	Straight forward