

**Session:**

**Date 18 April: 16:30**

# **Protecting corporate data on personal Windows devices - Your options**

—Peter van der Woude—



# Welcome to:



MODERN  
ENDPOINT  
MANAGEMENT

## SUMMIT 2024

APRIL 17 - 19

GOLD PARTNERS

control  UP

 Microsoft

# THANK YOU PARTNERS

## GOLD PARTNERS



## SILVER PARTNERS



## BRONZE PARTNERS



# About me

SPEAKER

## Peter van der Woude

 [www.petervanderwoude.nl](http://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 Windows 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

A close-up photograph of a medical syringe and a glass vial on a reflective surface. The syringe is partially filled with a light-colored liquid and has a dark plunger. The vial is clear glass with a dark cap. In the top right corner, there is a solid purple rectangular callout bubble containing the word "Prevention" in white, sans-serif font.

Prevention

Visibility



## Comply





Protect



# Why is it important?

Comply with regulations

Prevent data loss

Visibility into data

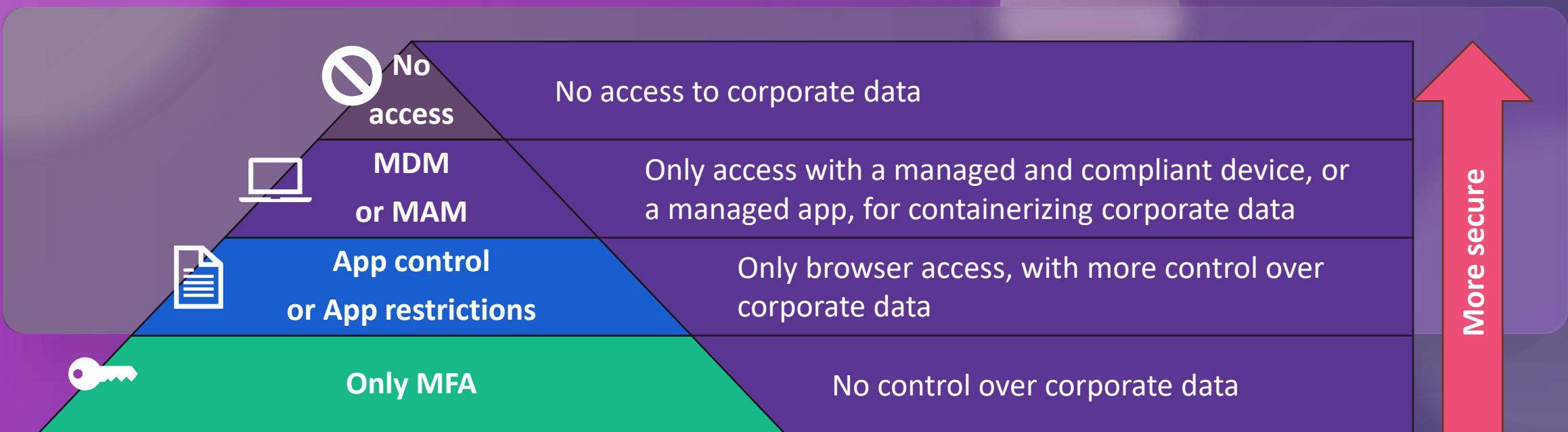
Protect intellectual property



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](#)

# Specifically for personal Windows devices:

What are the realistic options?



## Conditional Access with App Enforced Restrictions

Microsoft Purview

### New sensitivity label

settings will replace existing external sharing settings configured for the site.

Set-OwaMailboxPolicy  
-Identity OwaMailboxPolicy-Default  
-ConditionalAccessPolicy ReadOnly

Items

Groups & sites

Privacy & external user access

External sharing & conditional access

Finish

1  Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [Microsoft Entra hybrid joined](#) or enrolled in Intune).  
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 ①

Block access ①

2  Choose an existing authentication context. Each context has an Microsoft Entra Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)

Trusted devices -

Back Next Cancel

# 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)

The screenshot shows the Microsoft Defender policy configuration interface. The top navigation bar includes search, filter, and settings icons. The main area is titled "Microsoft Defender" and displays a policy configuration page.

**Policy severity \***: Three levels are shown: Low (green), Medium (yellow), and High (red).

**Category \***: DLP (Data Loss Prevention) is selected.

**Description**: Defender for Cloud Apps will evaluate the content of items that are cut/copied from and/or pasted to a browser and will block any violations in real-time.

**Session control type \***: Block activities is selected.

**Activity source**: Add activity filters to the policy.

**Activities matching all of the following**:  
Activity type: Cut/Copy item, Paste item  
Device: Intune compliant, Hybrid Azure AD joined, Valid client...  
Tag: does not equal  
Intune compliant, Hybrid Azure AD joined, Valid client...

**Add a filter**: A button to add more filtering criteria.

# 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)

Microsoft Intune admin center

... > Conditional Access | Policies > PVDW-RequireMAMforWindows Conditional Access policy

Delete [View policy information](#)

Assignments

Users [All users included and specific users excluded](#)

Target resources [1 app included](#)

Conditions [2 conditions selected](#)

Access controls

Grant [1 control selected](#)

Session [0 controls selected](#)

Enable policy [Report-only](#) [On](#) [Off](#)

Block access  Grant access

Require multifactor authentication

Require authentication strength

Require device to be marked as compliant

Require Microsoft Entra hybrid joined device

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

Require app protection policy  
[See list of policy protected client apps](#)

Require password change

All users terms of use

Select

# Combining technologies

The most obvious combinations

## Option 1



Conditional Access with App Enforced Restrictions



Conditional Access with App Protection Policies (MAM for Windows)

## Option 2



Conditional Access with App Control (Defender for Cloud Apps)



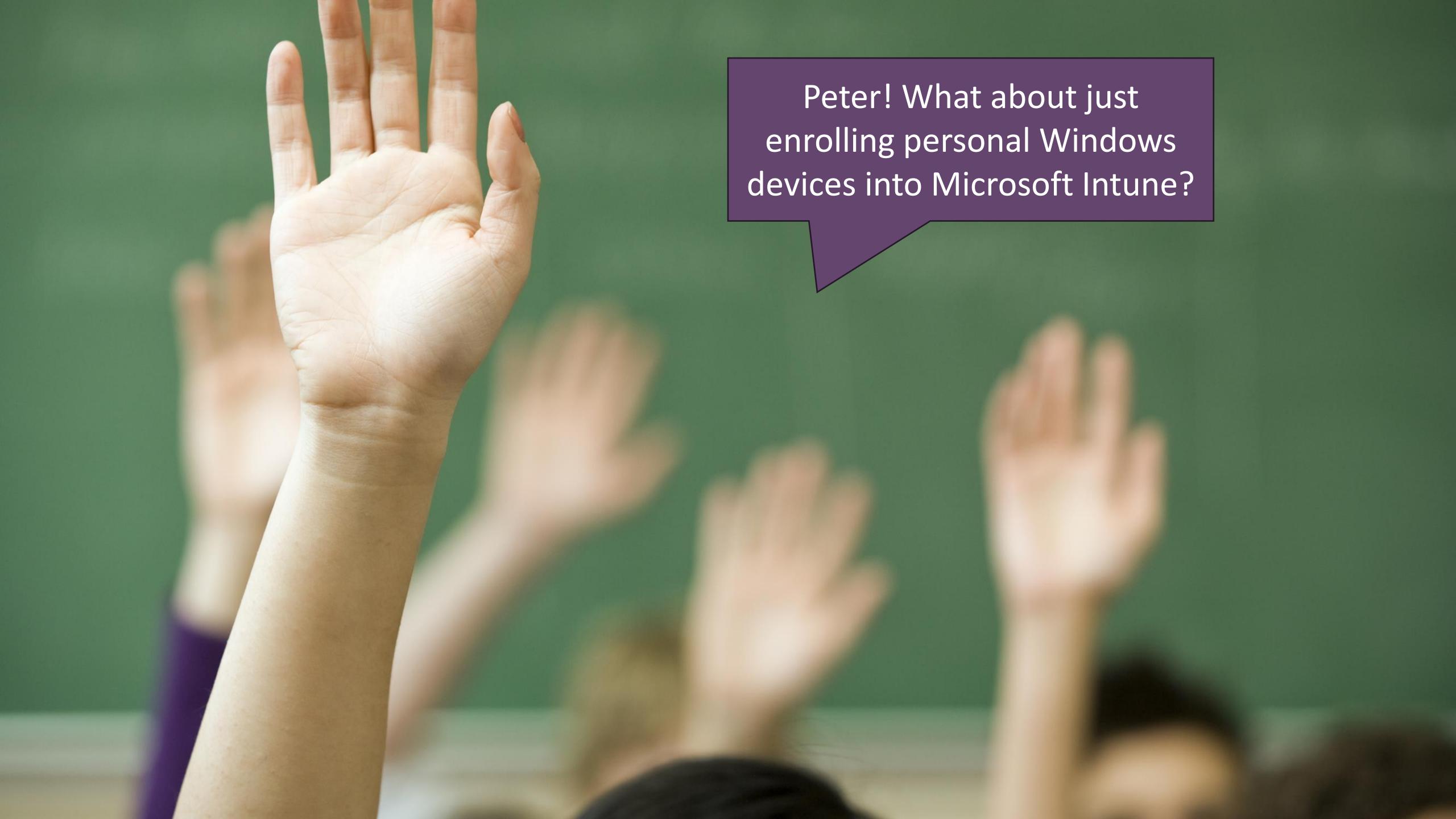
Conditional Access with App Protection Policies (MAM for Windows)

# 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





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

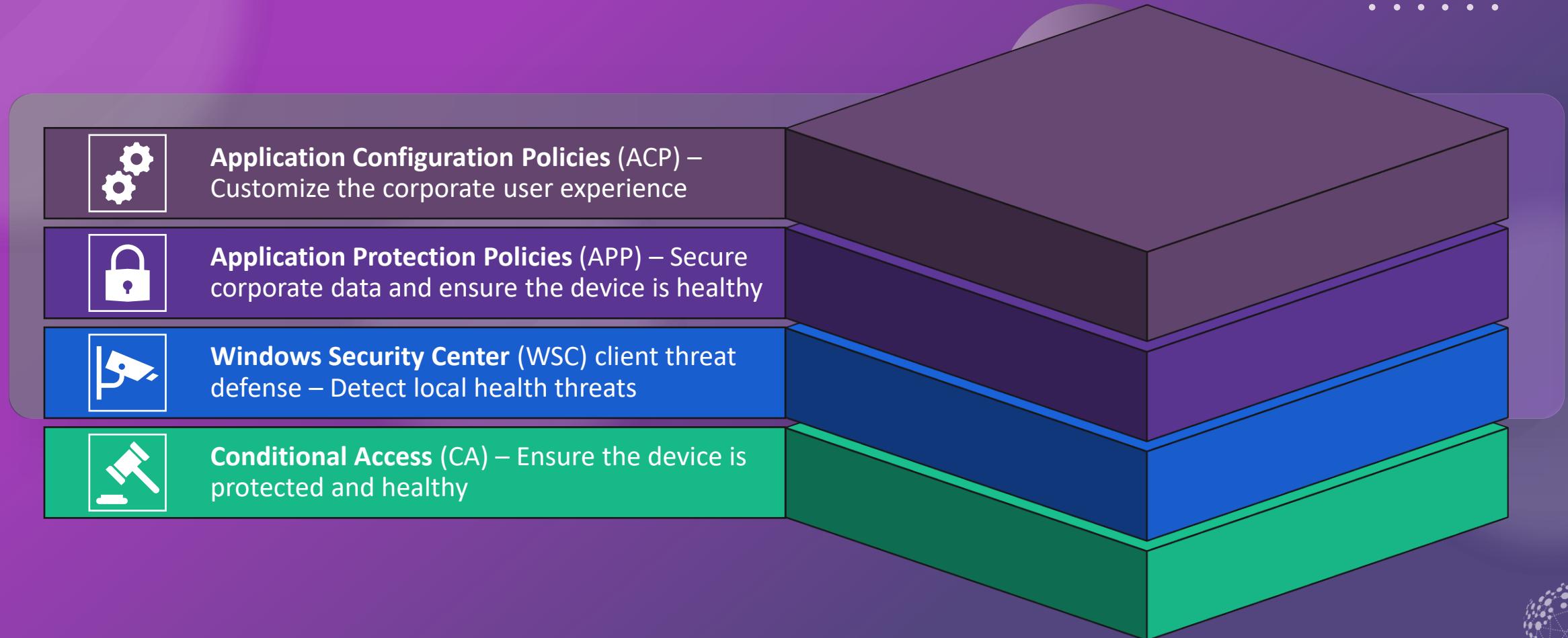
## Summary

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



# Customizing the user experience

## Important configuration options

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

Microsoft Intune admin center

### Settings picker

Use commas "," among search terms to lookup settings by their keywords

Search for a setting  Search

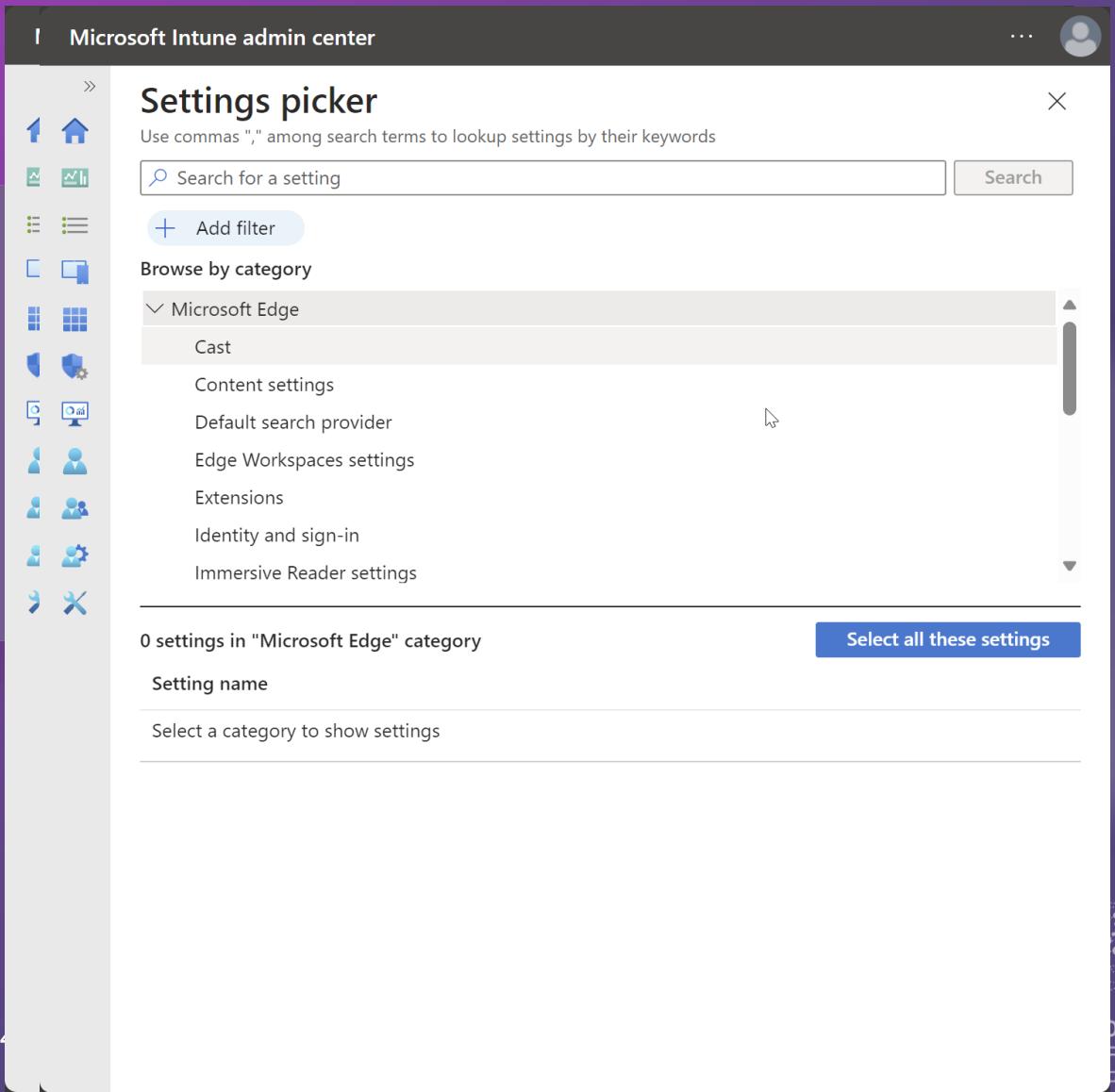
+ Add filter

Browse by category

- Microsoft Edge
  - Cast
  - Content settings
  - Default search provider
  - Edge Workspaces settings
  - Extensions
  - Identity and sign-in
  - Immersive Reader settings

0 settings in "Microsoft Edge" category Select all these settings

Setting name  
Select a category to show settings



# 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

Microsoft Intune admin center

Home > Apps | App protection policies > Intune App Protection | Properties >

Edit policy ...

Windows - MAM for Edge

1 Data protection    2 Review + save

This group includes the Data Loss Prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps.

**Data Transfer**

Receive data from ⓘ All sources

Send org data to ⓘ No destinations

Allow cut, copy, and paste for ⓘ No destination or source

**Functionality**

Print org data ⓘ Block

Review + save Cancel

# 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

Microsoft Intune admin center

Home > Apps | App protection policies > Intune App Protection | Properties >

### Edit policy

Windows - MAM for Edge

Select one

Device conditions

Configure the following health check settings to verify the device configuration before allowing access to org accounts and data.

Similar device based settings can be configured for enrolled devices. [Learn more about configuring device compliance settings for enrolled devices.](#)

**Important!** Make sure your Mobile Threat Defense (MTD) connector is set up in order to properly secure your organization's data based on threat evaluations from the connected Mobile Threat Defense services.

If your tenant has a connection set up with both Microsoft Defender for Endpoint and a MTD service (non-Microsoft) and do not configure a primary MTD service or there is a conflict when targeting a user, the default will be Microsoft Defender for Endpoint.

[Learn more about Mobile Threat Defense for unenrolled devices.](#)

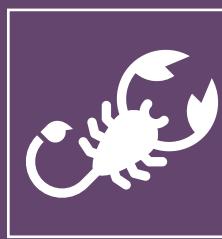
Min OS version	Value	Action
Max OS version	Low	Block access
Max allowed device threat le...		

Select one

Review + save Cancel

# 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

Microsoft Intune admin center

Add Connector

Mobile Threat Defense

Connection status Last synchronized

Not set up --

Select the Mobile Threat Defense connector to setup \*

Windows Security Center

Create

# 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

Microsoft Entra admin center | ... > Licenses | All products > petervanderwoude.nl

Search resources, services, and docs (G+)

New Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Assignments

Users [\(i\)](#)  
All users

Target resources [\(i\)](#)  
1 app included

Conditions [\(i\)](#)  
2 conditions selected

Access controls

Grant [\(i\)](#)

Enable policy

Block access  
 Grant access

Require multifactor authentication  
 Require authentication strength  
 Require device to be marked as compliant  
 Require Microsoft Entra hybrid joined device  
 Require approved client app  
[See list of approved client apps](#)  
 Require app protection policy  
[See list of policy protected client apps](#)  
 Require password change

Create Select

# 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**.

Microsoft Intune admin center

Home > Devices | Overview > Windows | Windows enrollment >

## Configure

MDM user scope  None  Some  All  
https://portal.manage.microsoft.com/TermsofUse.aspx

MDM terms of use URL  None  Some  All  
https://enrollment.manage.microsoft.com/enrollmentserver/...

MDM discovery URL  None  Some  All  
https://portal.manage.microsoft.com/?portalAction=Complia...

MDM compliance URL  None  Some  All  
https://wip.mam.manage.microsoft.com/Enroll

Restore default MDM URLs

Windows Information Protection (WIP) user scope  None  Some  All

WIP terms of use URL  None  Some  All  
https://wip.mam.manage.microsoft.com/Enroll

WIP discovery URL  None  Some  All  
https://wip.mam.manage.microsoft.com/Enroll

WIP compliance URL  None  Some  All  
https://wip.mam.manage.microsoft.com/Enroll

Restore default WIP URLs

**Info** Creating new WIP without enrollment policies (WIP-ME) is no longer supported. For more information, see [Windows Information Protection](#)

# User experience

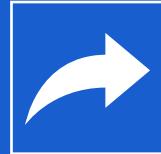
Experience for the end user



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

Stay signed in to all your apps

Windows will remember your account and automatically sign you in to your apps and websites on this device. This will reduce the number of times you are asked to login.



**Allow my organization to manage my device**

ⓘ Selecting this option means your administrator can install apps, control settings, and reset your device remotely. Your organization may require you to enable this option to access data and apps on this device.

[No, sign in to this app only](#)

OK



# 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.

A screenshot of the Microsoft Edge browser window. A modal dialog box titled "Microsoft Edge Application Management" is displayed, stating "Org data removal" and "Your organization is now removing its data associated with Microsoft Edge because your account pvanderwoude@petervanderwoude.nl is disabled." At the bottom right of the modal is an "OK" button. Below the modal, the Edge interface shows a toolbar with icons for Facebook, Outlook, Netflix, and LinkedIn, and a list of devices: Samsung SM-A326B (SM-A326B), DESKTOP-3PDODDS (Desktop), and DESKTOP-3PDODDS (Desktop). At the bottom of the screen are "Cancel" and "Create" buttons. The overall theme is modern endpoint management.

# 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/

Setting	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
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

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

