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

Start 13:00

Peter van der Woude

Albert Hoitingh

Protecting corporate data on personal Windows devices - Your options

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Sprekers

Peter van der Woude

Principal Consultant
Security MVP (Intune)

Albert Hoitingh

Principal Consultant
Security MVP (Microsoft
Information Protection)

What are we going to discuss?

- 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 Windows MAM and Defender for Cloud Apps
- How do the different options for protecting corporate data compare

Why is it important to protect corporate data on personal devices

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Prevention

Visibility

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

Comply

Protect

Prevent data loss

Visibility into data

Comply with regulations

CROQUIS DE MANZANA ESC. 1:1000
CALCULO DE MODULOS DE ESTACIONAMIENTO

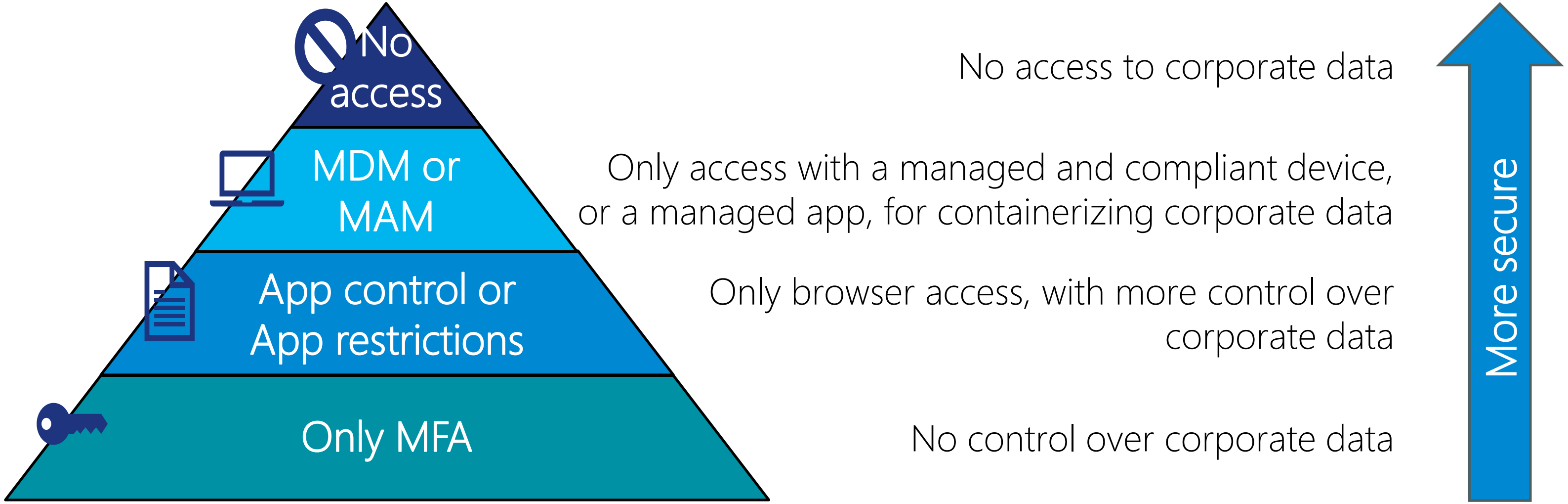
Protect intellectual property

What are the options for protecting corporate data on personal devices

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Protecting corporate data on personal devices

All options rely on Conditional Access for enforcement



No access to corporate data

Only access with a managed and compliant device, or a managed app, for containerizing corporate data

Only browser access, with more control over corporate data

No control over corporate data

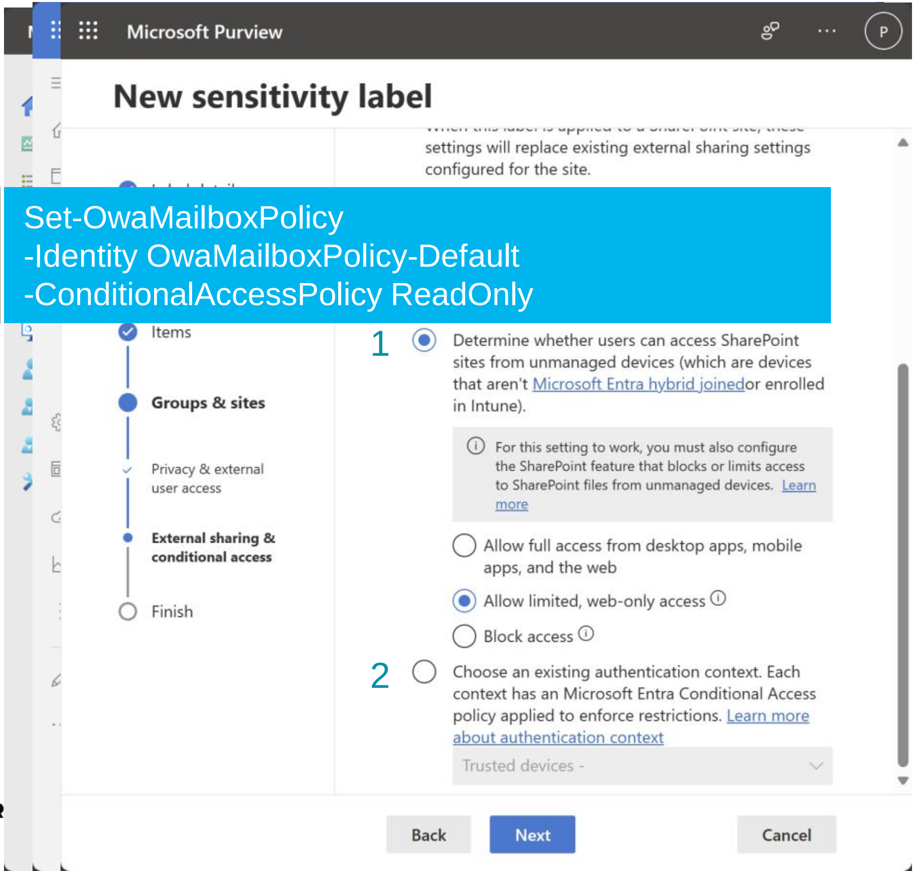
Overview inspired by: [The Underwhelming MAM for Edge and What Else We Can Do - ITProMentor]()

Specifically for personal Windows devices

What are the realistic options?

Conditional Access with App Enforced Restrictions

```
Set-OwaMailboxPolicy
-Identity OwaMailboxPolicy-Default
-ConditionalAccessPolicy ReadOnly
```



Microsoft Purview

New sensitivity label

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

- ✓ 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 joinedor 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 ⓘ

○ Block access ⓘ

2 ○ Choose an existing authentication context. Each context has an Microsoft Entra Conditional Access policy applied to enforce restrictions. Learn more about authentication context

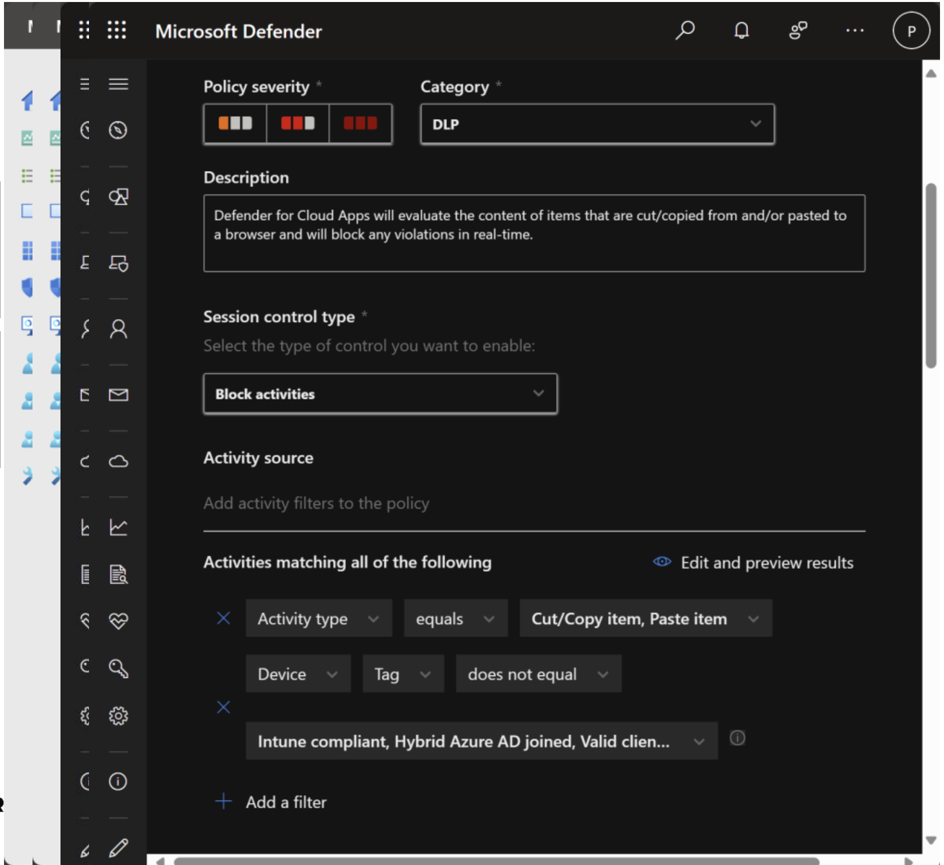
Trusted devices -

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)



Policy severity *

Category * DLP

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 *

Select the type of control you want to enable:

Block activities

Activity source

Add activity filters to the policy

Activities matching all of the following

Edit and preview results

Activity type equals Cut/Copy item, Paste item

Device Tag does not equal Intune compliant, Hybrid Azure AD joined, Valid clien...

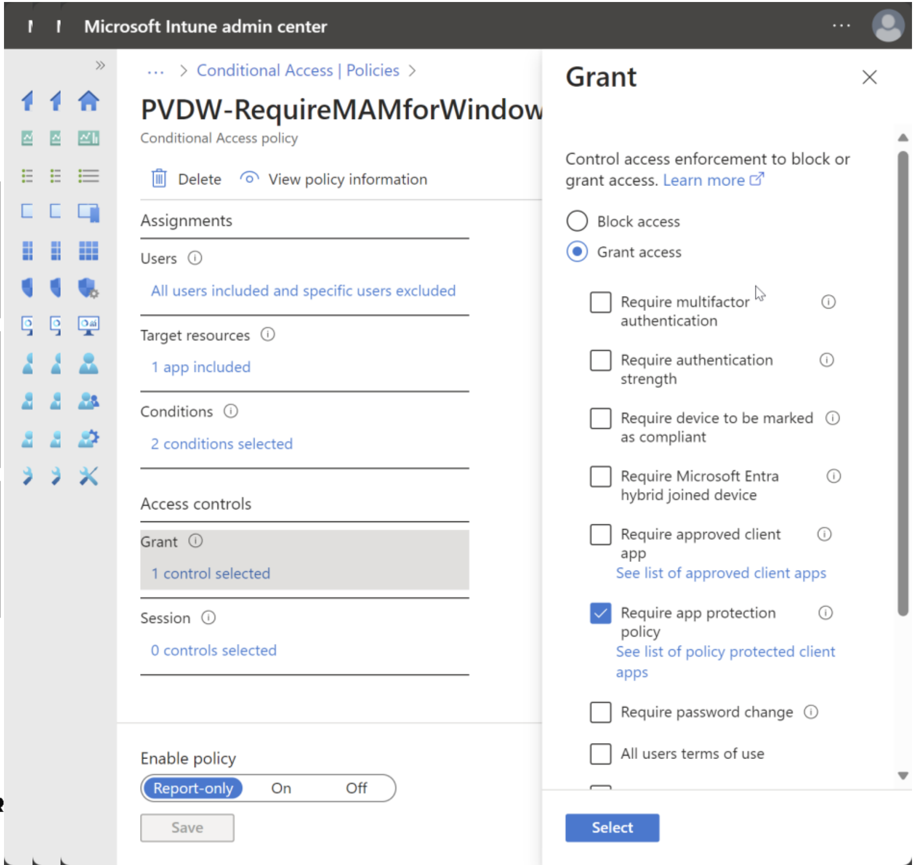
Add a filter

rubrik DELL Technologies SquaredUp infinity INTER

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-RequireMAMforWindow

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

Save

Grant

Control access enforcement to block or grant access. Learn more

○ 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

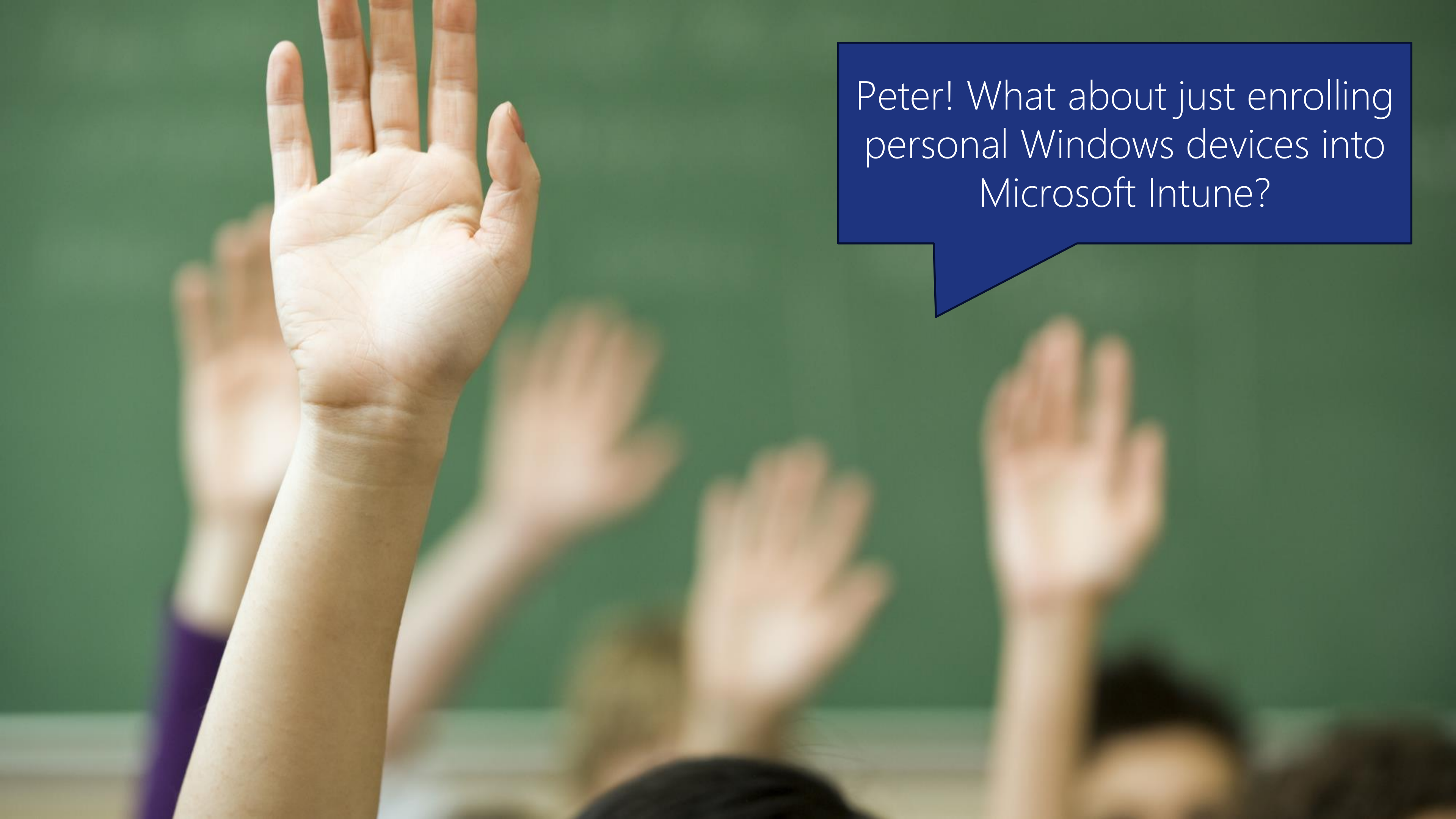
The most obvious combinations

Option 1	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 (incl. remote wipe)
- Configure important browser settings
- Best of both worlds



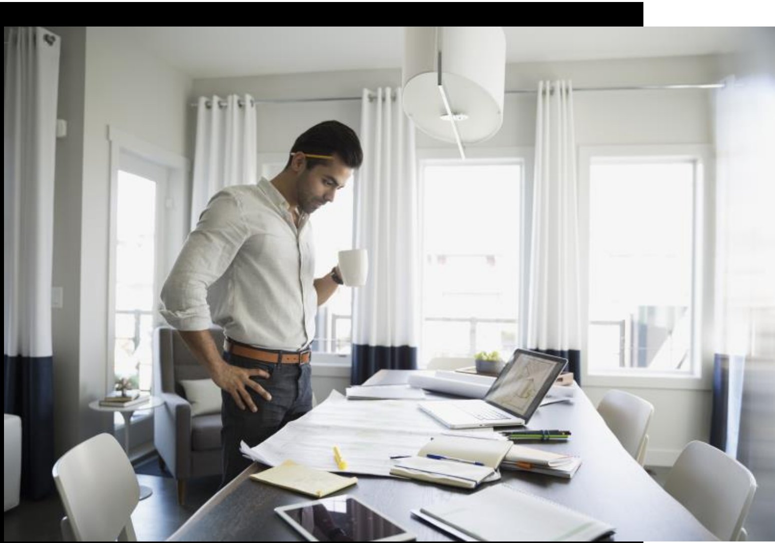
Peter! What about just enrolling personal Windows devices into Microsoft Intune?

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



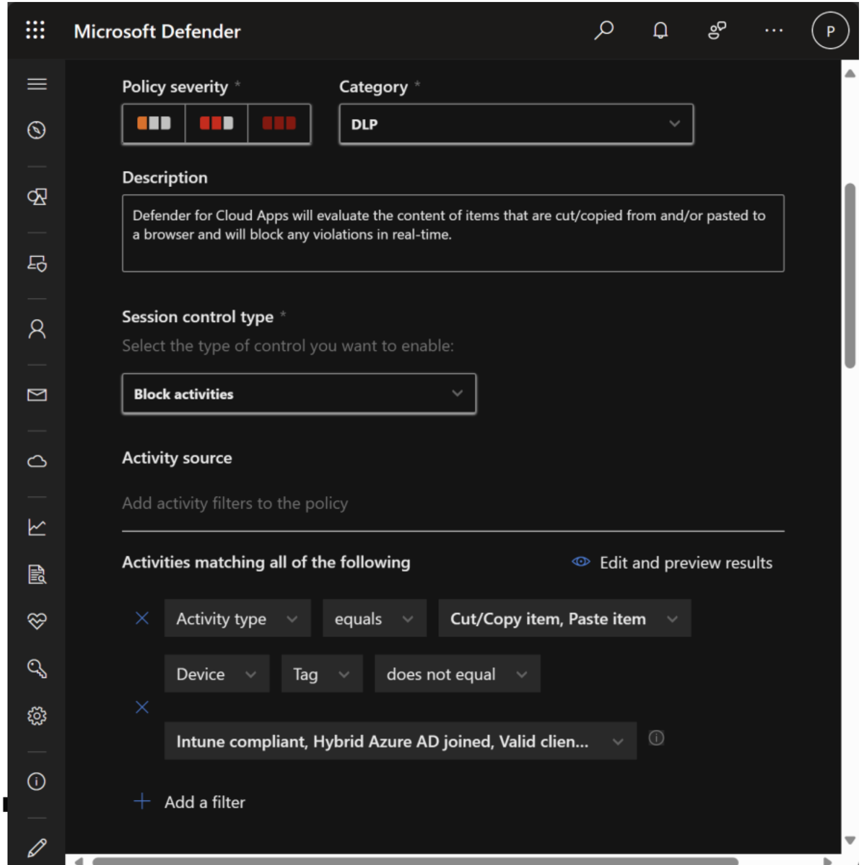
A closer look at Microsoft Defender for Cloud Apps

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)

rubrik DELL Technologies SquaredUp infinity INTERSTELL



Policy severity *

Category *
DLP

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 *

Select the type of control you want to enable:

Block activities

Activity source

Add activity filters to the policy

Activities matching all of the following

Activity type equals Cut/Copy item, Paste item

Device Tag does not equal Intune compliant, Hybrid Azure AD joined, Valid clien...

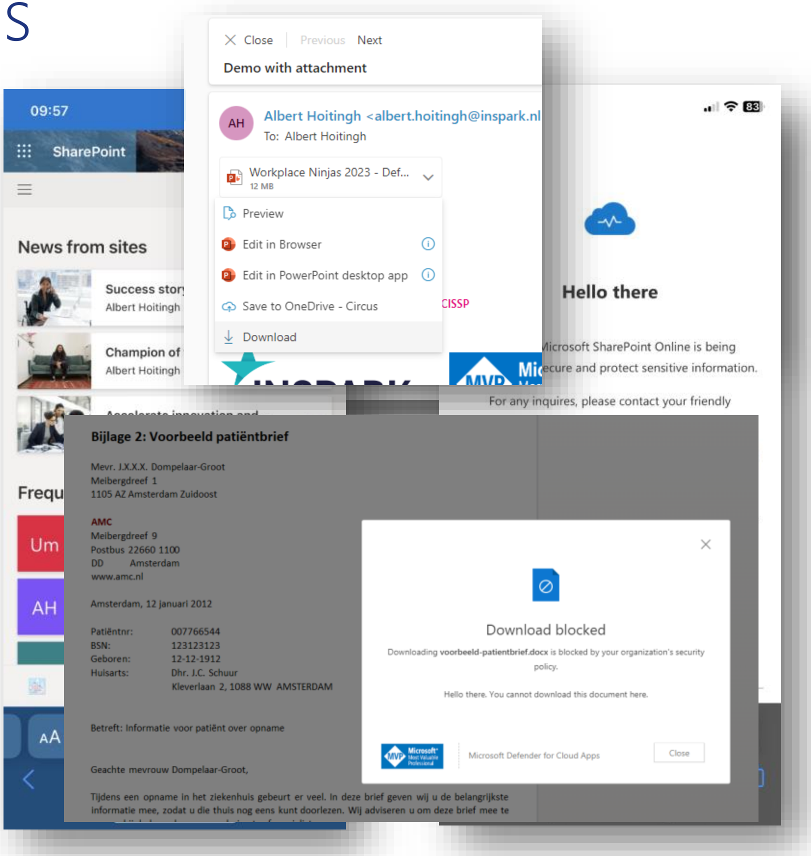
Specifically for devices

Using session based checks

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 SharePoint Online is being ... ecure and protect sensitive information.

For any inquires, please contact your friendly

Bijlage 2: Voorbeeld patiëntbrief

Mevr. J.X.X.X. Dompelaar-Groot
Meibergdreef 1
1105 AZ Amsterdam Zuidoost

AMC
Meibergdreef 9
Postbus 22660 1100
DD Amsterdam
www.amc.nl

Amsterdam, 12 januari 2012

Patiëntnr:	007766544
BSN:	123123123
Geboren:	12-12-1912
Huisarts:	Dhr. J.C. Schuur Kleverlaan 2, 1088 WW AMSTERDAM

Betreft: Informatie voor patiënt over opname

Geachte mevrouw Dompelaar-Groot,

Tijdens een opname in het ziekenhuis gebeurt er veel. In deze brief geven wij u de belangrijkste informatie mee, zodat u die thuis nog eens kunt doorlezen. Wij adviseren u om deze brief mee te

Download blocked

Downloading **voorbeeld-patientbrief.docx** is blocked by your organization's security policy.

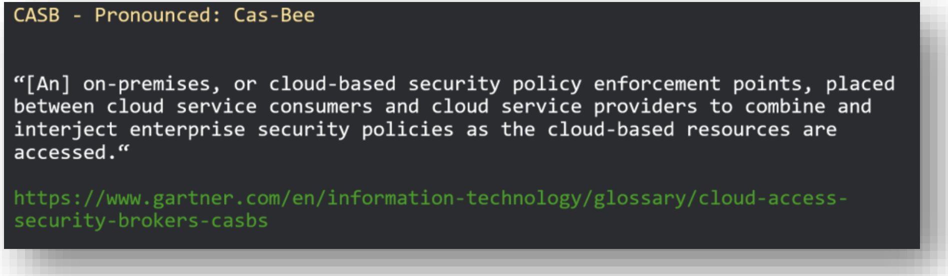
Hello there. You cannot download this document here.

rubrik · DELL Technologies · SquaredUp · infinity · INTERSTELLAR · kpn Partner Network · INSPARK · cegeka

Microsoft Defender for Cloud Apps

Four important functions

- Discover and assess risks
- Protect information
- Control access
- Discover threats



```
CASB - Pronounced: Cas-Bee

“[An] on-premises, or cloud-based security policy enforcement points, placed
between cloud service consumers and cloud service providers to combine and
interject enterprise security policies as the cloud-based resources are
accessed.“

https://www.gartner.com/en/information-technology/glossary/cloud-access-
security-brokers-casbs
```

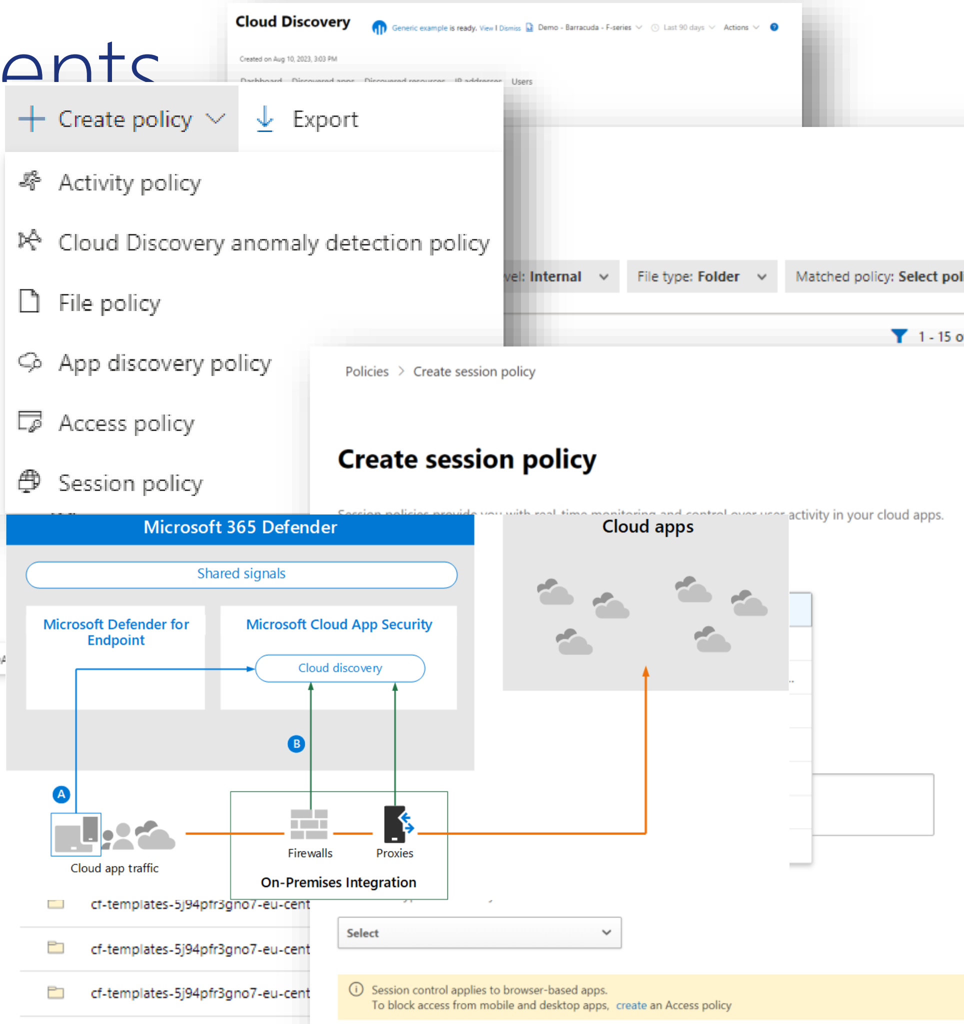
Three components

Defender for Cloud Apps

Cloud discovery

Insights and logs

Policies



Policies > Create session policy

Create session policy

Session policies provide you with real-time monitoring and control over user activity in your cloud apps.

Session control applies to browser-based apps.
To block access from mobile and desktop apps, create an Access policy

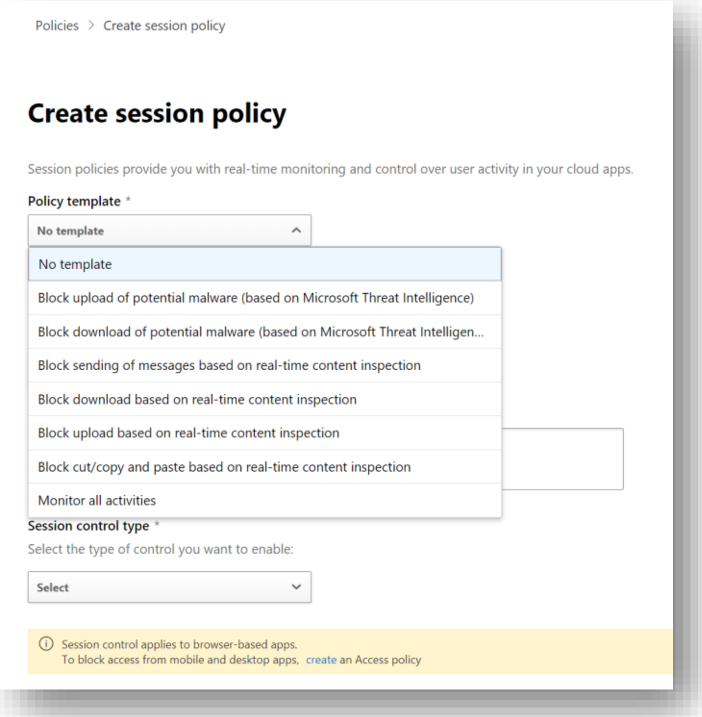
Focus for today

Session policies

Cloud discovery

Insights and logs

Policies



Policies > Create session policy

Create session policy

Session policies provide you with real-time monitoring and control over user activity in your cloud apps.

Policy template *

No template

- No template
- Block upload of potential malware (based on Microsoft Threat Intelligence)
- Block download of potential malware (based on Microsoft Threat Intelligen...
- Block sending of messages based on real-time content inspection
- Block download based on real-time content inspection
- Block upload based on real-time content inspection
- Block cut/copy and paste based on real-time content inspection
- Monitor all activities

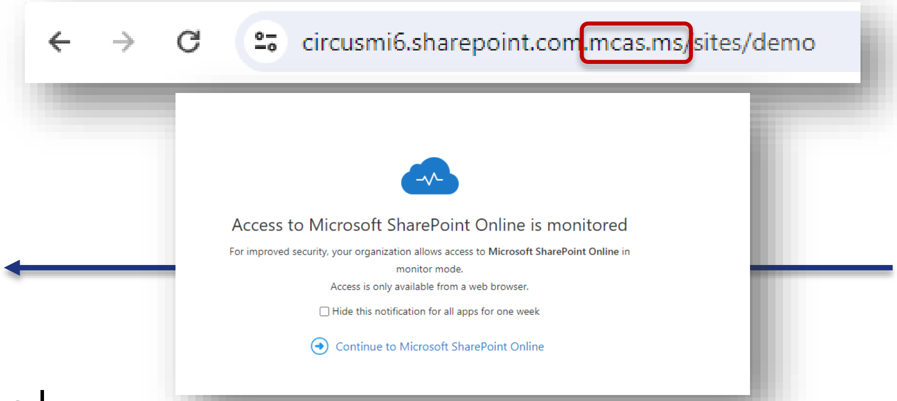
Session control type *

Select the type of control you want to enable:

Select

ⓘ Session control applies to browser-based apps.
To block access from mobile and desktop apps, create an Access policy

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka



circusmi6.sharepoint.com.mcas.ms/sites/demo

Access to Microsoft SharePoint Online is monitored

For improved security, your organization allows access to **Microsoft SharePoint Online** in monitor mode.

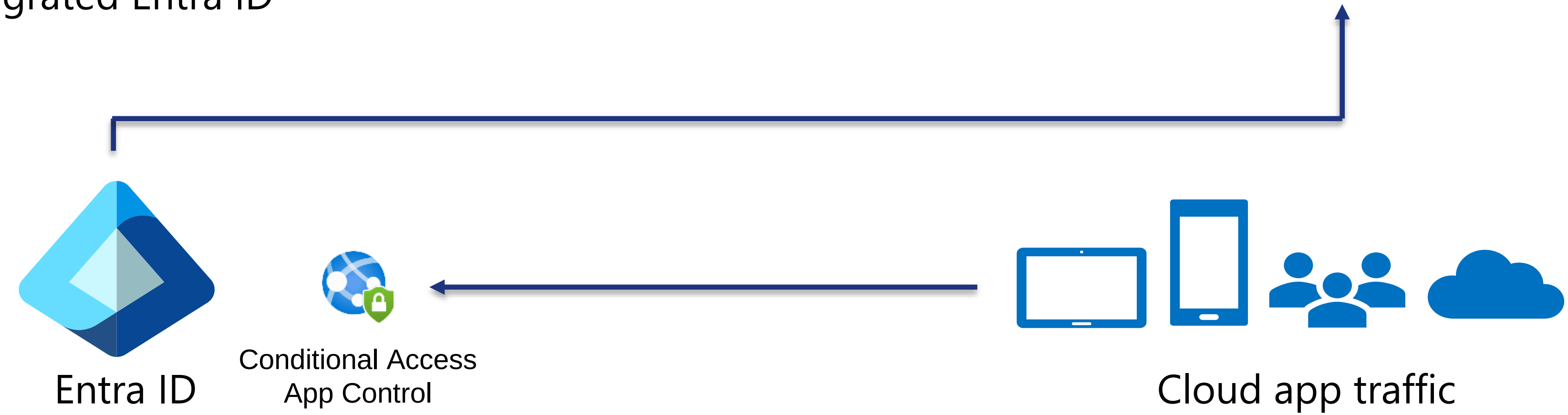
Access is only available from a web browser.

□ Hide this notification for all apps for one week

Continue to Microsoft SharePoint Online

Connected SaaS apps | integrated Entra ID

Microsoft Defender for Cloud Apps

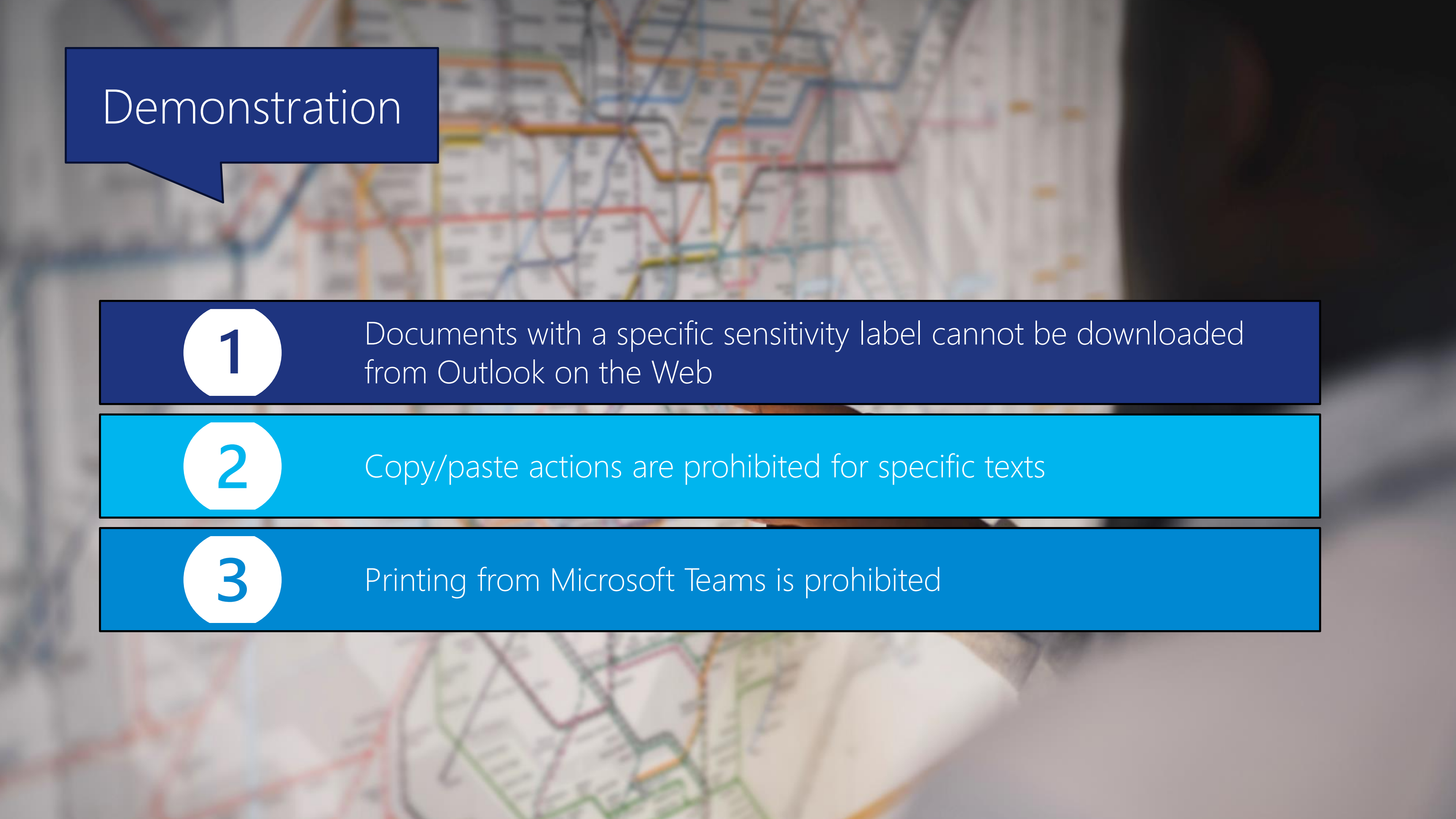


Entra ID

Conditional Access App Control

Cloud app traffic

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka



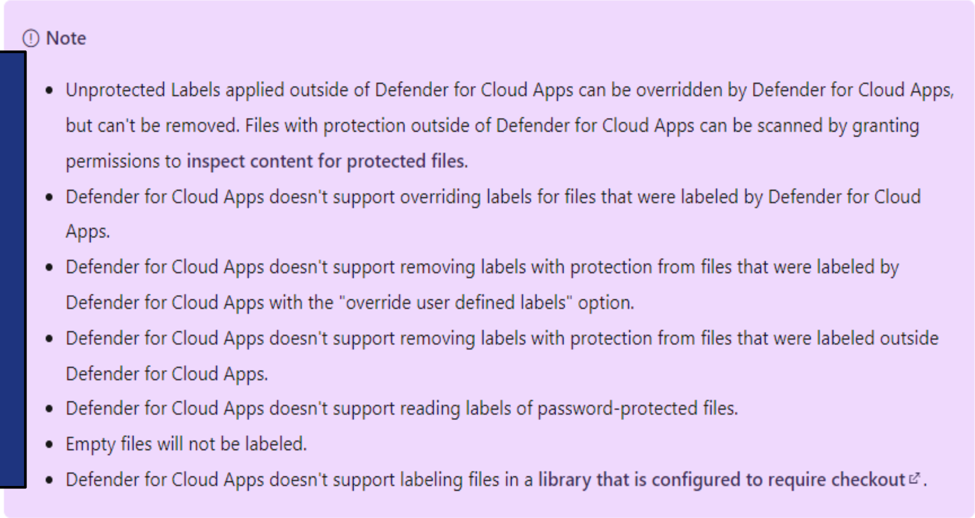
Demonstration

1. Documents with a specific sensitivity label cannot be downloaded from Outlook on the Web
2. Copy/paste actions are prohibited for specific texts
3. Printing from Microsoft Teams is prohibited

Information protection

Beware the small-print

⚠ Existing files are only scanned when these have been modified. There is a limit of 100 "Apply label" actions per app/tenant/day. MDfCA requires "All users" or "Everyone in the org" permissions in the label.



ⓘ Note

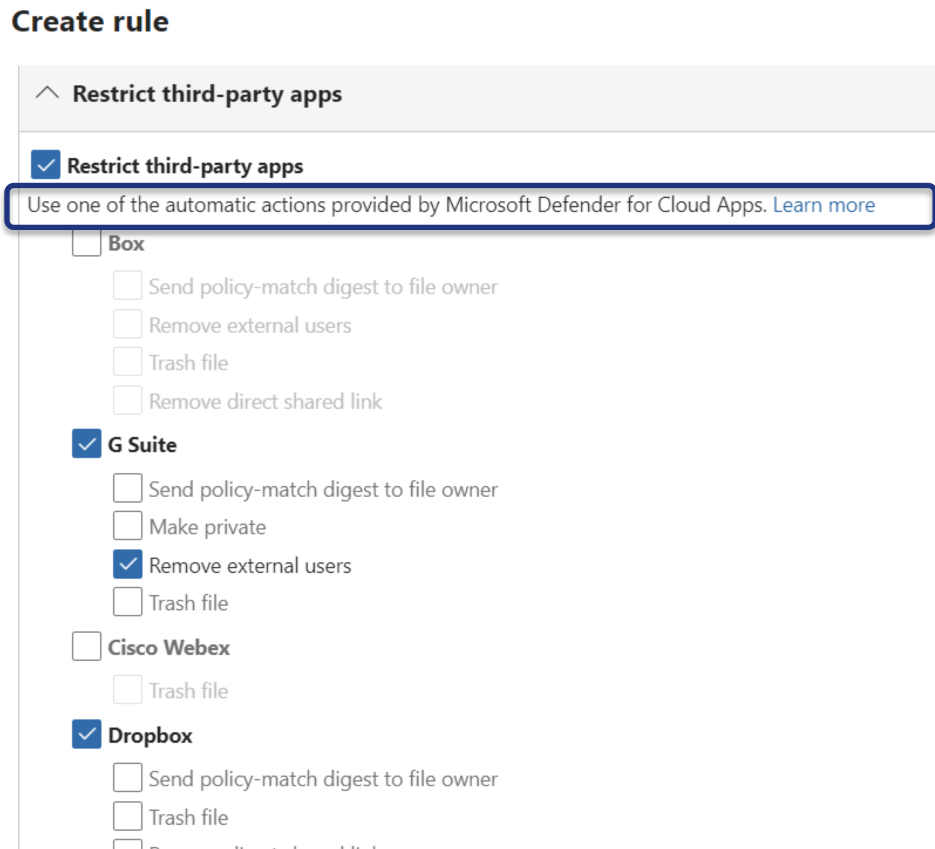
- Unprotected Labels applied outside of Defender for Cloud Apps can be overridden by Defender for Cloud Apps, but can't be removed. Files with protection outside of Defender for Cloud Apps can be scanned by granting permissions to inspect content for protected files.
- Defender for Cloud Apps doesn't support overriding labels for files that were labeled by Defender for Cloud Apps.
- Defender for Cloud Apps doesn't support removing labels with protection from files that were labeled by Defender for Cloud Apps with the "override user defined labels" option.
- Defender for Cloud Apps doesn't support removing labels with protection from files that were labeled outside Defender for Cloud Apps.
- Defender for Cloud Apps doesn't support reading labels of password-protected files.
- Empty files will not be labeled.
- Defender for Cloud Apps doesn't support labeling files in a library that is configured to require checkout.

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Microsoft Purview DLP

Two management portals

⚠ File policies can be configured using Microsoft Purview DLP. File policies and session policies are not the same.



Create rule

^ Restrict third-party apps

☑ Restrict third-party apps

Use one of the automatic actions provided by Microsoft Defender for Cloud Apps. Learn more

□ Box
- □ Send policy-match digest to file owner
- □ Remove external users
- □ Trash file
- □ Remove direct shared link

☑ G Suite
- □ Send policy-match digest to file owner
- □ Make private
- ☑ Remove external users
- □ Trash file

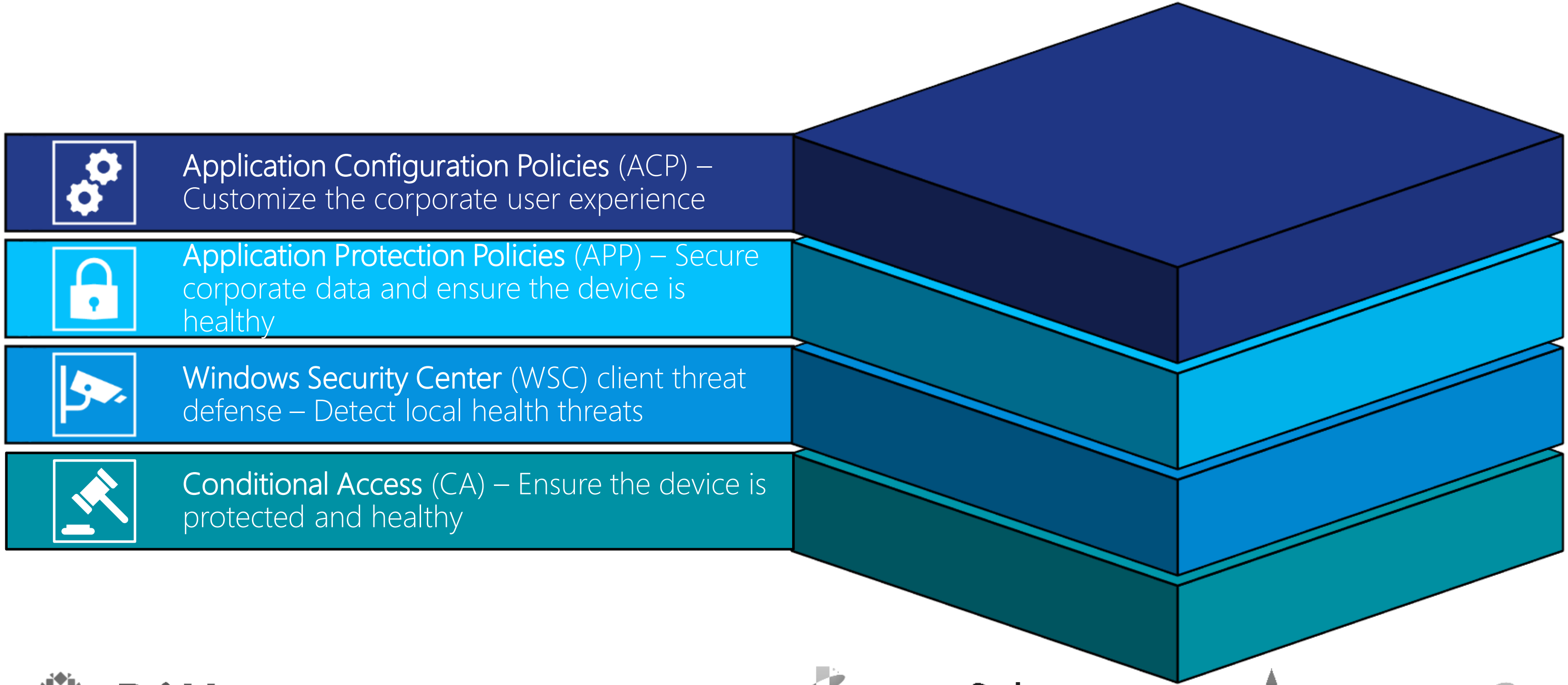
□ Cisco Webex
- □ Trash file

☑ Dropbox
- □ Send policy-match digest to file owner
- □ Trash file

rubrik DELL Technologies SquaredUp infinity INTER

A closer look at Windows MAM (for Edge)

Layers of Windows MAM



Application Configuration Policies (ACP) – Customize the corporate user experience

Application Protection Policies (APP) – Secure corporate data and ensure the device is healthy

Windows Security Center (WSC) client threat defense – Detect local health threats

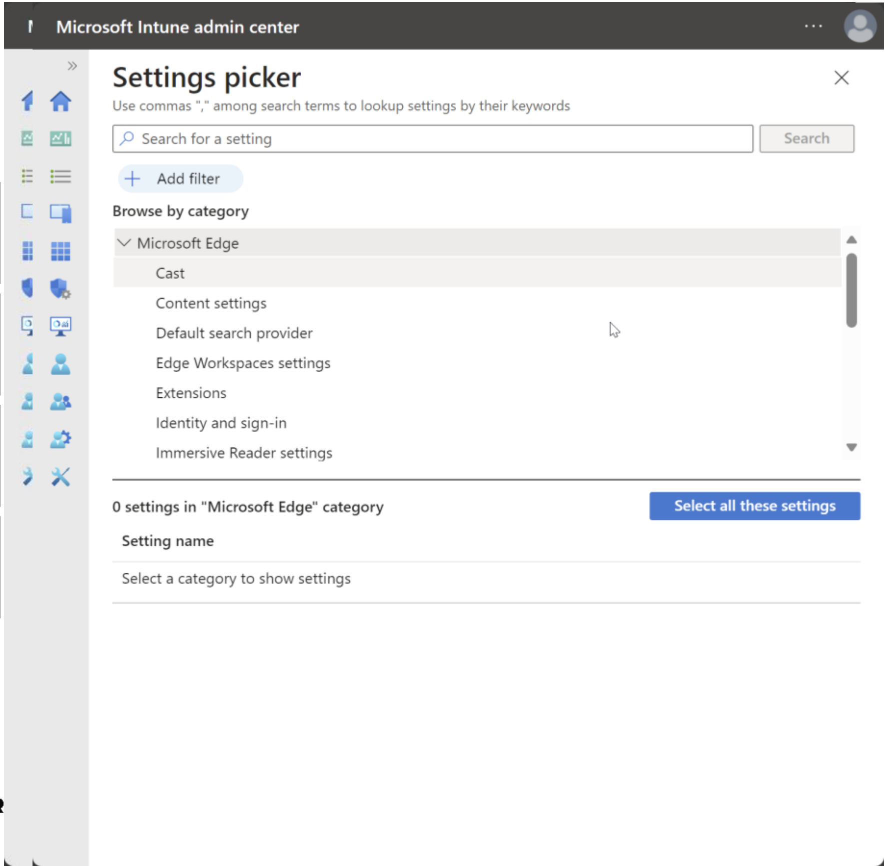
Conditional Access (CA) – Ensure the device is protected and healthy

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

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

Demonstration

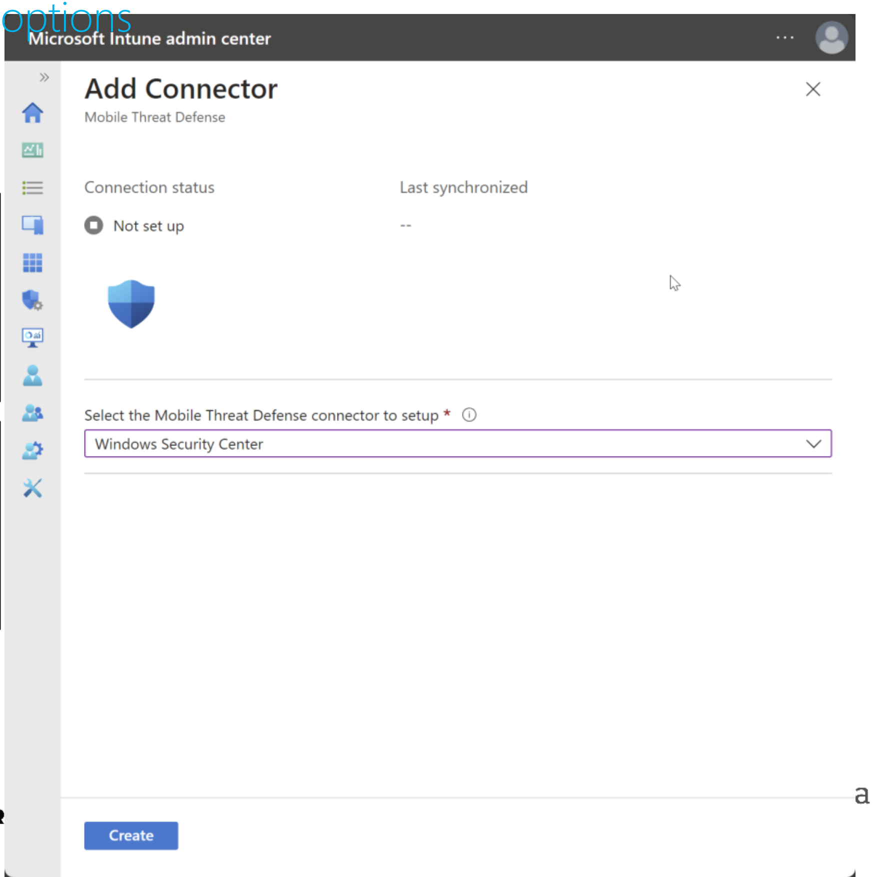
1. Basics of app protection for Windows
2. Combining app protection with Defender for Cloud Apps
3. Looking at the user experience

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: Not set up

Last synchronized: --

Select the Mobile Threat Defense connector to setup *: Windows Security Center

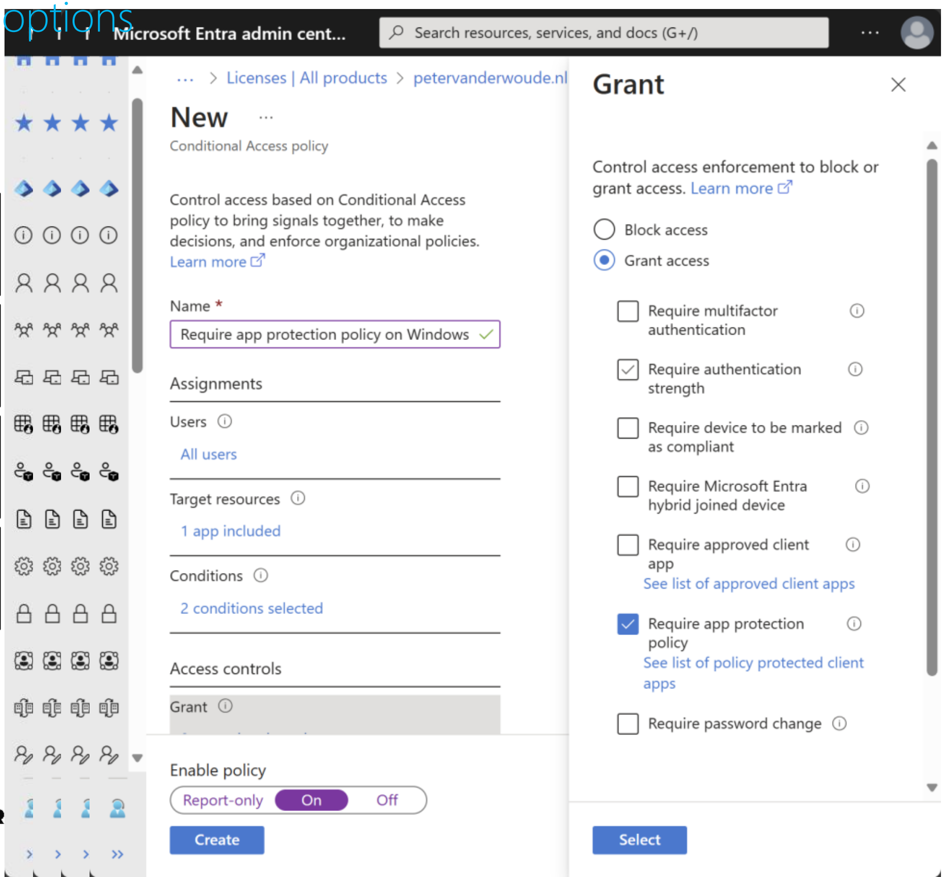
rubrik DELL Technologies SquaredUp infinity INTER

a

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 cent...

Search resources, services, and docs (G+/)

... > Licenses | All products > petervanderwoude.nl

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 *

Require app protection policy on Windows

Assignments

Users ⓘ

All users

Target resources ⓘ

1 app included

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

Enable policy

Report-only | **On** | Off

Create

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

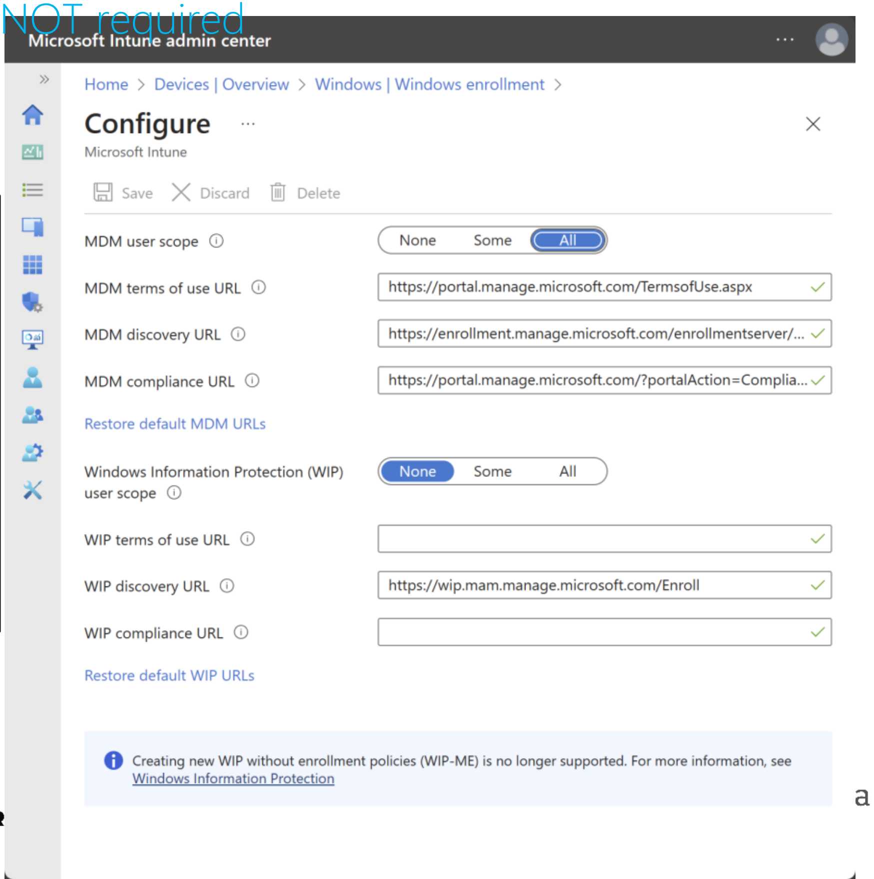
- □ Require multifactor authentication ⓘ
- ☑ Require authentication strength ⓘ
- □ Require device to be marked as compliant ⓘ
- □ Require Microsoft Entra hybrid joined device ⓘ
- □ Require approved client app ⓘ
  See list of approved client apps
- ☑ Require app protection policy ⓘ
  See list of policy protected client apps
- □ Require password change ⓘ

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

Microsoft Intune

MDM user scope: None / Some / [✓ All]

MDM terms of use URL: https://portal.manage.microsoft.com/TermsofUse.aspx ✓

MDM discovery URL: https://enrollment.manage.microsoft.com/enrollmentserver/... ✓

MDM compliance URL: https://portal.manage.microsoft.com/?portalAction=Complia... ✓

Restore default MDM URLs

Windows Information Protection (WIP) user scope: [✓ None] / Some / All

WIP terms of use URL: ✓

WIP discovery URL: https://wip.mam.manage.microsoft.com/Enroll ✓

WIP compliance URL: ✓

Restore default WIP URLs

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

a

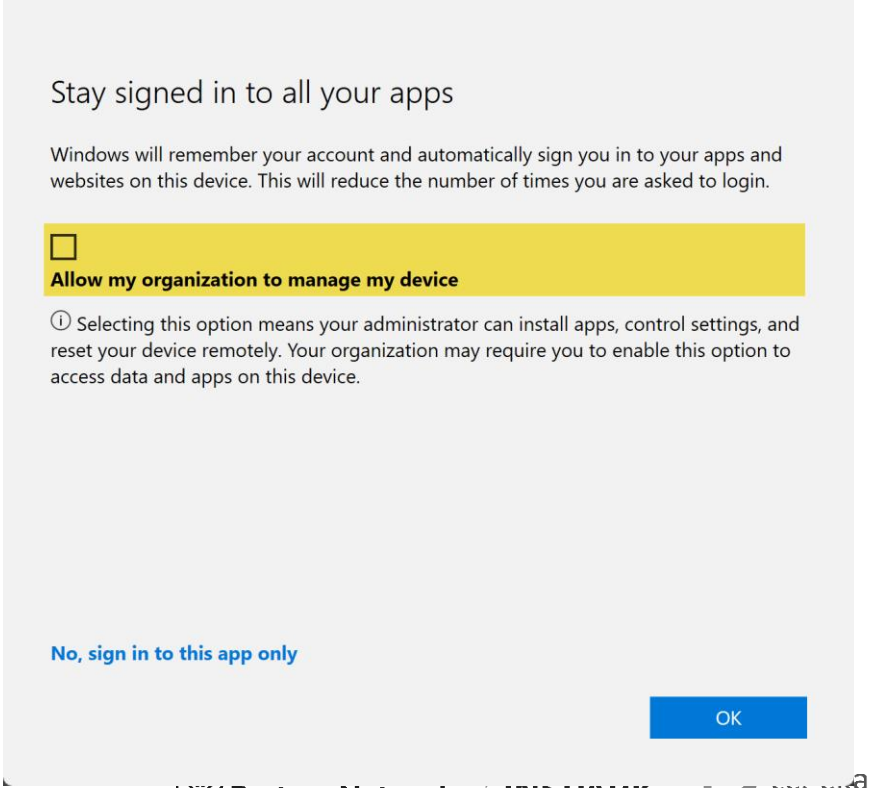
User experience

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.

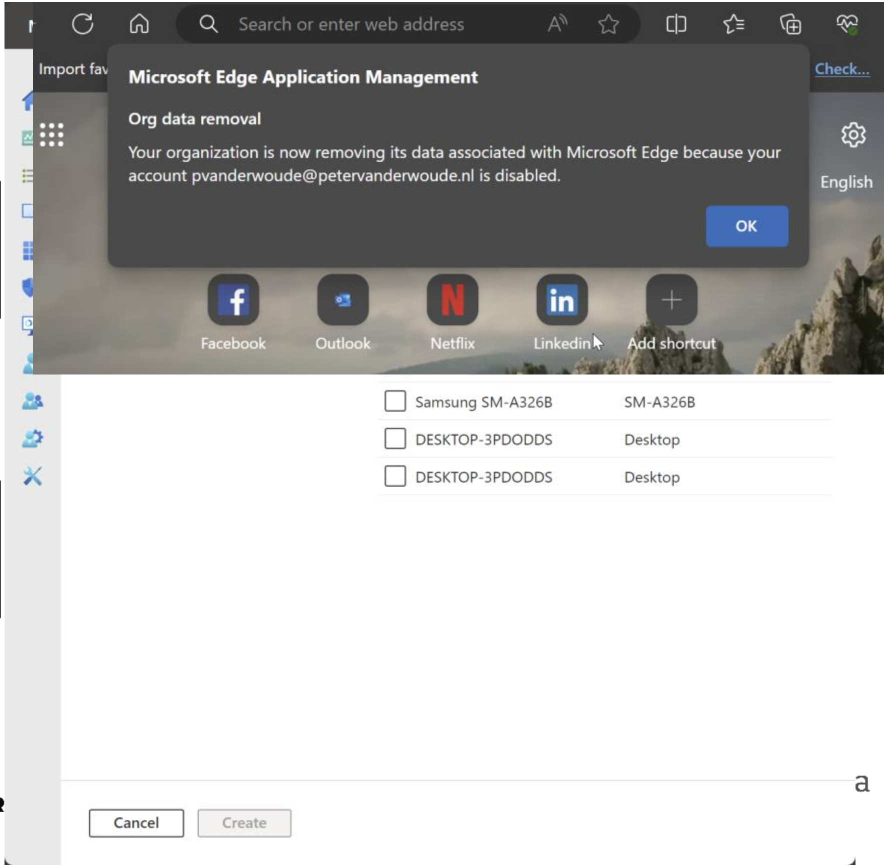
App selective wipe

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.



Microsoft Edge Application Management

Org data removal

Your organization is now removing its data associated with Microsoft Edge because your account pvanderwoude@petervanderwoude.nl is disabled.

□ Samsung SM-A326B	SM-A326B
□ DESKTOP-3PDODDS	Desktop
□ DESKTOP-3PDODDS	Desktop

How do the different options compare for personal devices

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

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

Please evaluate this session in the App.

THANK YOU

Are there any questions?

Next session 14:00 – 14:50

AppControl for Business