Why Microsoft Purview Projects Fail

(and How to Avoid It)

MC2MC

CONNECT

Ewelina Paczkowska

- Solution Architect at Threatscape
- Microsoft Security MVP in MS Purview
- M365 Security & Compliance user group co-organiser

@welkasworld.com

@WelkasWorld

@WelkasWorld

@WelkasWorld

@/ewelinapaczkowska

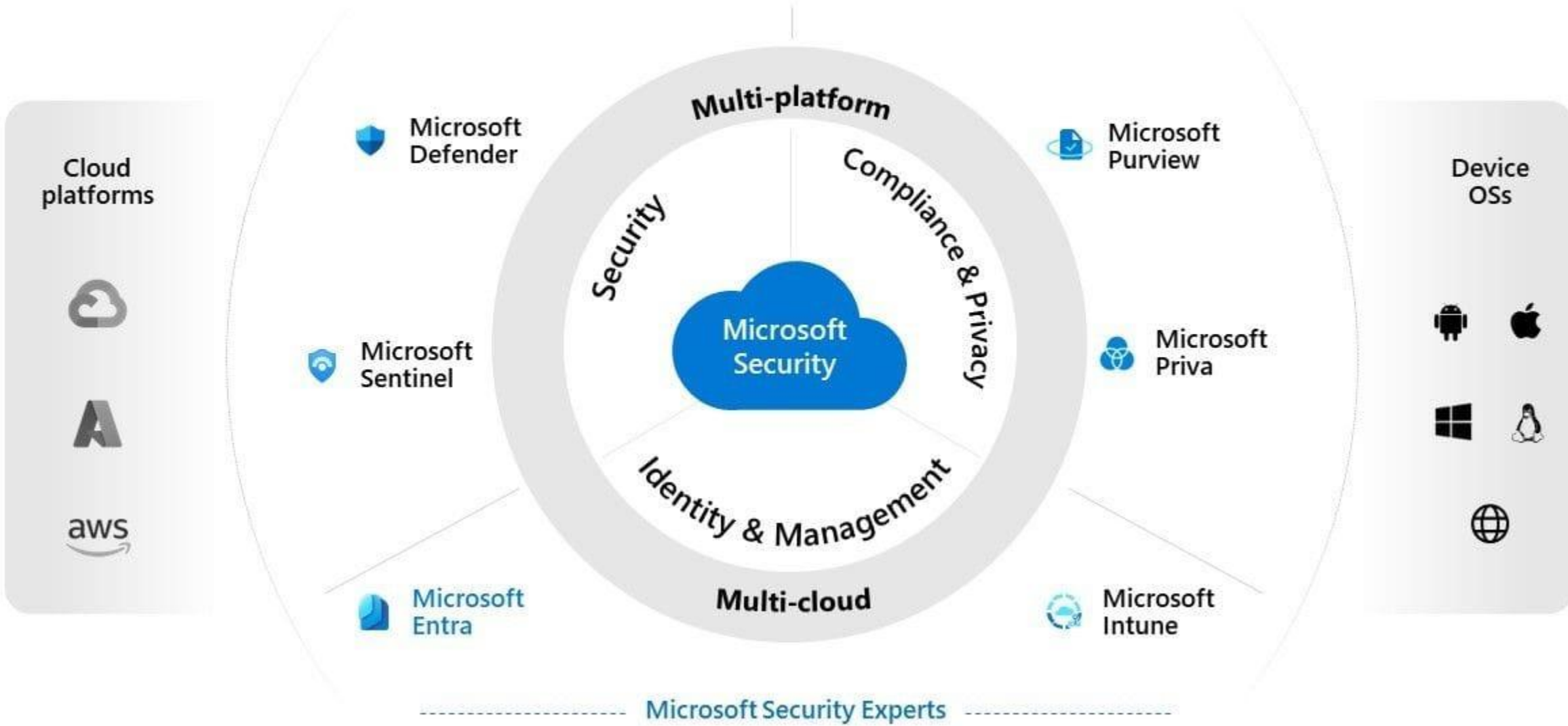
www.welkasworld.com

MC2MC
CONNECT

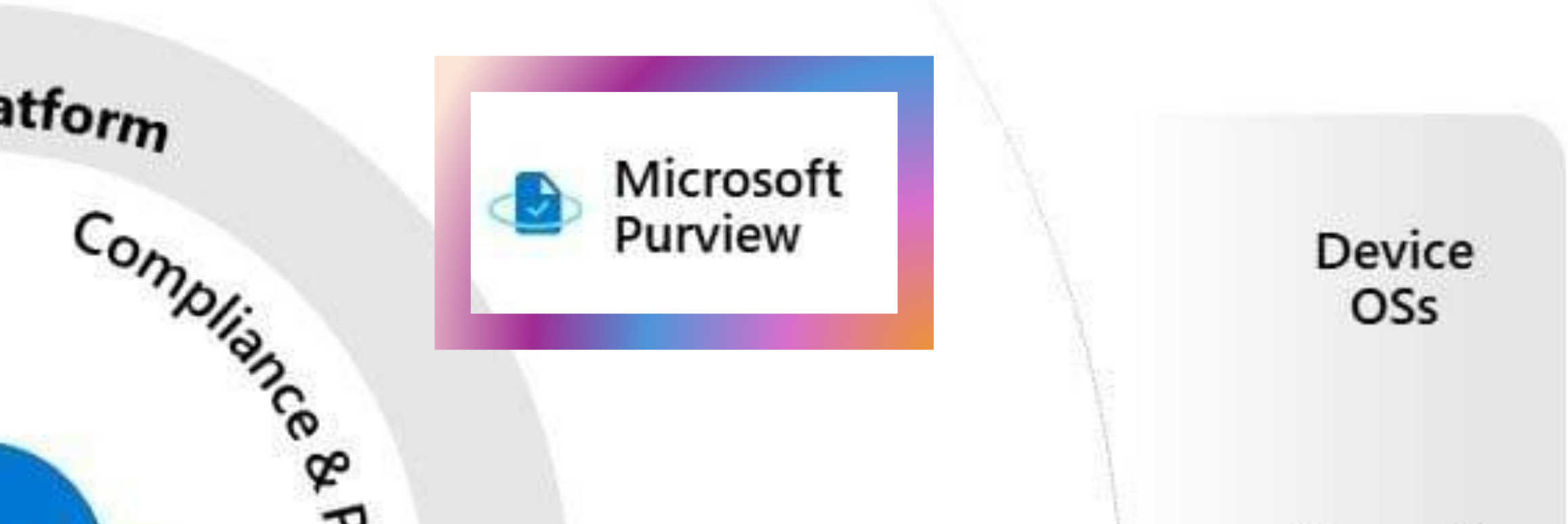
Agenda

- Field notes and lessons learned
- Latest advice for an evergreen service
- No-nonsense, straight to the point
- Real world lessons
- How to ensure project success

Microsoft Security Product Portfolio



Portfolio



MICROSOFT PURVIEW

Microsoft Purview

Microsoft Purview is a unified data governance and compliance platform.

Microsoft Purview helps you:

- Discover where your data lives
- Classify what’s sensitive
- Protect it across Microsoft 365 and beyond
- Comply with regulations

Microsoft Purview

Risk and Compliance

For risk, compliance, and legal teams

Data Security

For information and cybersecurity teams

Data Governance

For data consumers, data engineers, data officers

MC2MC
CONNECT

Microsoft Purview

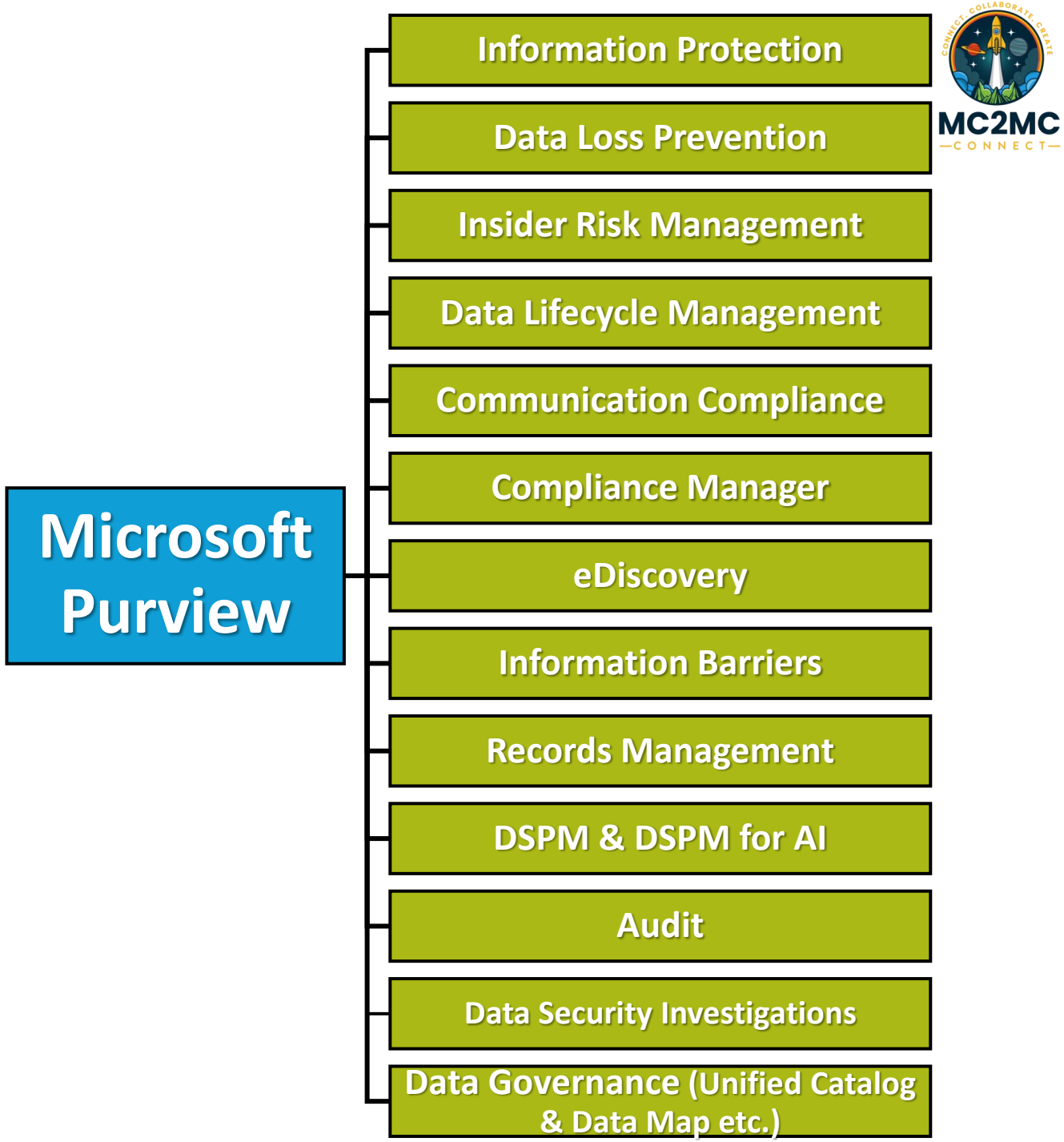
Risk and Compliance

Data Security

Data Governance

MICROSOFT PURVIEW

PRODUCTS & SOLUTIONS



Field notes and lessons learned

Notes from the field

Purview is not another tool you switch on and walk away from.

It is a full-on transformation.

If you change how data is labelled, accessed, protected…

… that has ripple effects across your entire organisation

The technical side is not the hard part.

It’s the non-technical prerequisites that make or break a Purview rollout.

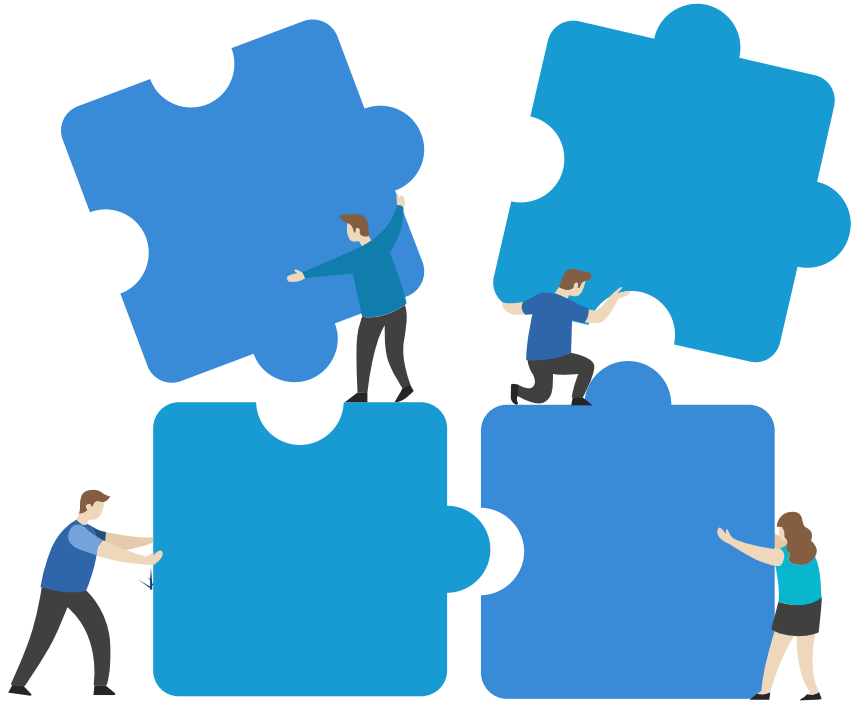
1. Management buy-in

No management buy-in

If one influential executive hates it – it’s a game over

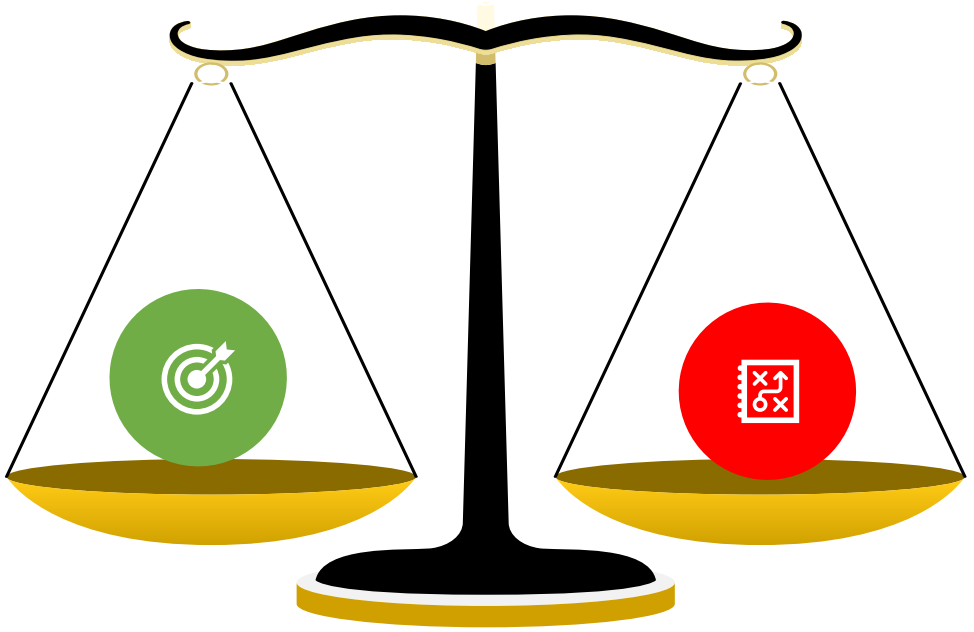
No team collaboration

Purview only works if everyone feeds into the design



Poor balance of security vs usability

If people can’t do their job – they will bypass security



No user training or awareness

End users need to understand what they're doing and why

No dedicated resource

- Someone needs to take ownership/ responsibility
- Purview should not be the responsibility of only the IT teams
- Dedicated resource

Lessons learned

- ✅ Get management buy-in
- ✅ Focus on team collaboration
- ✅ Balance security with usability
- ✅ Prioritise user training and awareness campaigns
- ✅ Have a dedicated resource managing Purview

2. Technical prerequisites

A64 | 1 E5 Compliance value shown. Includes additional value.

Microsoft 365 Compliance Licensing Comparison

Note: A dot (●) indicates that the rights to benefit from the feature are specifically conveyed through the license. Microsoft 365 E5 Compliance, Microsoft 365 E5 Information Protection and Governance, Microsoft 365 E5 Insider Risk Management, and Microsoft 365 E5 eDiscovery and Audit are supplemental (add-on) licenses that have pre-requisite license requirements and convey only the rights to benefit from advanced (E5) features only, and not the rights to benefit from underlying features (e.g. Microsft 365 E3 features), which must be licensed separately.

Solution	Feature	Microsoft 365 E5 Compliance[2] (See footnote regarding blank cells in this column)	Microsoft 365 E5/A5 Info Protection & Governance[3]	Microsoft 365 E5 Insider Risk Management[4]	Micro eDisc
	Customer Key for Office 365	●	●		
	Bring Your Own Key (BYOK) for customer-managed key provisioning life cycle[13]	●	●		
	Hold Your Own Key (HYOK) that spans Azure Information Protection and Active Directory (AD) Rights Management for highly regulated scenarios	●	●		
	Endpoint DLP	●	●		
Insider Risk Management	Insider Risk Management	●		●	
	Communication Compliance (incl. Supervision policies)	●		●	
	Information Barriers	●		●	
	Customer Lockbox	●		●	
	Privileged Access Management	●		●	
Discover & Respond	Content Search				
	Core eDiscovery (incl. Hold and Export)				
	Advanced eDiscovery	●			
	Custodian management (mapping content to custodian)	●			
	Custodian communications	●			
	Deep crawling/indexing	●			
	Review data (query data, tags, smart tags, dashboard) and annotate (redact)	●			

M365 Compliance Licensing

http://learn.microsoft.com/en-us/office365/servicedescriptions/downloads/microsoft-365-compliance-licensing-comparison.xlsx

> **Tip**
>
> When you compare the minimum versions in the tables with the versions you have, remember the common practice of release versions to omit leading zeros.
>
> For example, you have version 4.2128.0 and read that 4.7.1+ is the minimum version. For easier comparison, read 4.7.1 (no leading zeros) as 4.**0007**.1 (and not 4.** 7000**.1). Your version of 4.2128.0 is higher than 4.0007.1; so, your version is supported.

Sensitivity label capabilities in Word, Excel, and PowerPoint

The numbers listed are the minimum Office application versions required for each capability.

> **Note**
>
> For Windows and the Semi-Annual Enterprise Channel, the minimum supported version numbers might not yet be released. Learn more.

Expand table

Capability	Windows	Mac	iOS	Android	Web

New sensitivity label

- Label details
- **Scope**
- Items
- Groups & sites
- Finish

Define the scope for this label

Labels can be applied to data assets and containers (like SharePoint sites and Teams). Let us know where you want this label to be used so we can show you the related protection settings. Learn more about label scopes

Files & other data assets

Label files and data assets in Microsoft 365, Microsoft Fabric (includes Power BI), Microsoft Azure.

Emails

Label messages sent from all versions of Outlook.

Meetings

Label calendar events and meetings schedules in Outlook and Teams.

Parent label will automatically inherit meeting scope from sub labels

Groups & sites

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, SharePoint sites, and Loop workspaces.

To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.

Back Next Cancel

New sensitivity label

- Label details
- **Scope**
- Items
- Groups & sites
- Finish

Define the scope for this label

Labels can be applied to data assets and containers (like SharePoint sites and Teams). Let us know where you want this label to be used so we can show you the related protection settings. Learn more about label scopes

- **Files & other data assets**
  Label files and data assets in Microsoft 365, Microsoft Fabric (includes Power BI), Microsoft Azure.
- **Emails**
  Label messages sent from all versions of Outlook.
- **Meetings**
  Label calendar events and meetings schedules in Outlook and Teams.

  ⓘ Parent label will automatically inherit meeting scope from sub labels

- Groups & sites
  Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, SharePoint sites, and Loop workspaces.

  ⓘ To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.

Back Next Cancel

Home
Solutions
Learn
Settings
Compliance Manager
Data Loss Prevention
Information Protection
Insider Risk Managem...
Communi... Compliance

Settings
Account
Roles and scopes
Data connectors
Device onboarding
Optical character recognition (OCR)

Solution settings
Communication Compliance
Compliance Manager
Data Catalog
Data Lifecycle Management
Data Loss Prevention
eDiscovery
Information Protection
Insider Risk Management
Records Management

Information Protection settings

Co-authoring for files with sensitivity labels
Information protection scanner

Co-authoring for files with sensitivity labels

This setting allows users in your organization to co-author in Office desktop documents that are encrypted by using sensitivity labels. To support this new capability, all users must have the latest Microsoft 365 Apps for enterprise and label metadata must be upgraded for all labeled documents that aren't encrypted. Learn more about this one-time setting

Prerequisites

- Sensitivity labels must be enabled for files in OneDrive and SharePoint. If this isn't already done, we'll enable this for you when you turn on co-authoring.
- Minimum versions of apps to support the new labeling metadata.
- Latest Microsoft 365 Apps for enterprise.
- Any labeling apps or solutions you've deployed use the minimum supported version of the MIP SDK.
- Any scripts or tools you're using that read from or write to the labeling metadata for documents are updated to use the new metadata format and location.

Learn more about these prerequisites

What to expect after turning this on

- When existing labeled and unencrypted documents are opened and saved, the sensitivity label information that's currently stored as a custom property is copied and saved to a new format in a new metadata location.

☐ Turn on co-authoring for files with sensitivity labels

When you turn this on, we'll also enable sensitivity labels for files in OneDrive and SharePoint if it's not already enabled. Learn more

⚠ To turn this switch off, you'll need to use PowerShell. Before turning off, make sure you understand the consequences to understand how turning off will impact labeled content in your organization. Learn more

Home
Solutions
Compliance Manager
Data Loss Prevention
Information Protection
Insider Risk Managem...
Communi... Compliance
...

Information Protection
Overview
Reports
Recommendations
Sensitivity labels
Policies
Label publishing policies
Auto-labeling policies
Protection policies (preview)
Classifiers
Explorers
Diagnostics

Related solutions

Auto-labeling policies

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. Learn more about role group permissions.

View role groups

Set up billing to continue auto-labeling assets in non-Microsoft 365 sources. Support for non-Microsoft 365 data sources has switched to our pay-as-you-go billing model. Existing policies that include these data sources will continue to work for a short time, but you can't edit them or create new ones for these sources until you link an Azure subscription for pay-as-you-go billing. Learn more about pay-as-you-go billing

Get started

Automatically apply sensitivity labels to sensitive emails, files, and other data assets. In addition to these policies, you can automatically apply labels to Office client apps by editing the "Auto-labeling" settings for a specific label. Learn more about auto-labeling

Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn on here, but note that additional configuration is required for Multi-Geo environments. Learn more

Turn on now

Protect PDFs with Auto-labeling

Turn on PDF protection for files in SharePoint and OneDrive.

Home
Solutions
Compliance Manager
Data Loss Prevention
Information Protection
Insider Risk Managem...
Communi... Compliance
...

Information Protection

Overview
Reports
Recommendations
Sensitivity labels
Policies
Label publishing policies
Auto-labeling policies
Protection policies (preview
Classifiers
Explorers
Diagnostics

Related solutions

you'll only be able to
ssions.
View role groups

s. Support for non-Microsoft
ies that include these data
new ones for these sources until
-as-you-go billing
Get started

ta assets. In addition to these
the "Auto-labeling" settings

he files that have encrypted
n on here, but note that
Turn on now

MC2MC CONNECT

Home
Solutions
Settings
Compliance Manager
Data Loss Prevention
Information Protection
Insider Risk Managem...
...

Settings
Account
Roles and scopes
Data connectors
Device onboarding
Devices
Onboarding
Offboarding
Optical character recognition (OCR)
Solution settings
Communication Compliance
Compliance Manager
Data Catalog

Onboarding

Select operating system to start onboarding process:

Windows 10

To onboard devices to the compliance center, choose your preferred deployment method, download articles provided for each method.

Deployment method

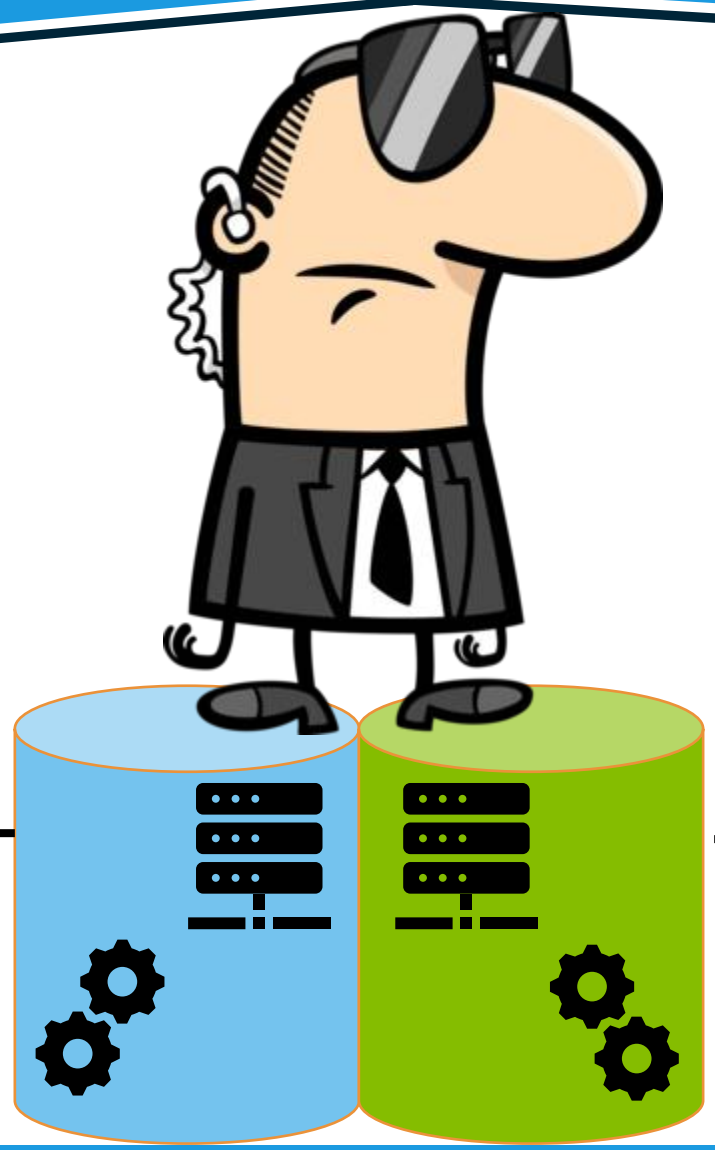
Mobile Device Management / Microsoft ...

Instructions for onboarding devices using Mobile Device Management tools.
Although this article describes onboarding devices to Microsoft Defender for Endpoint, the instructions

Download package

MDE/ Purview onboarding

1 AGENT

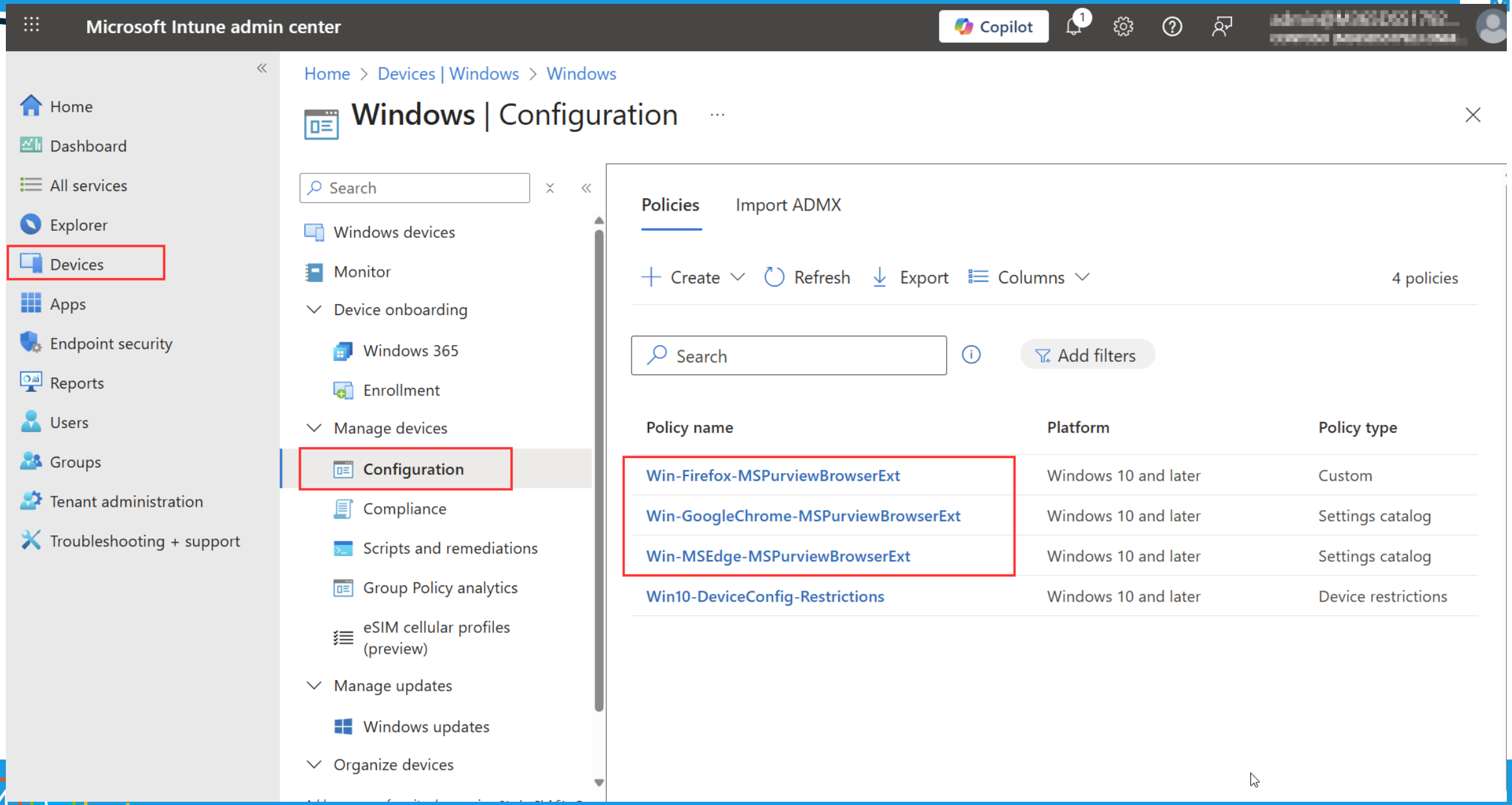


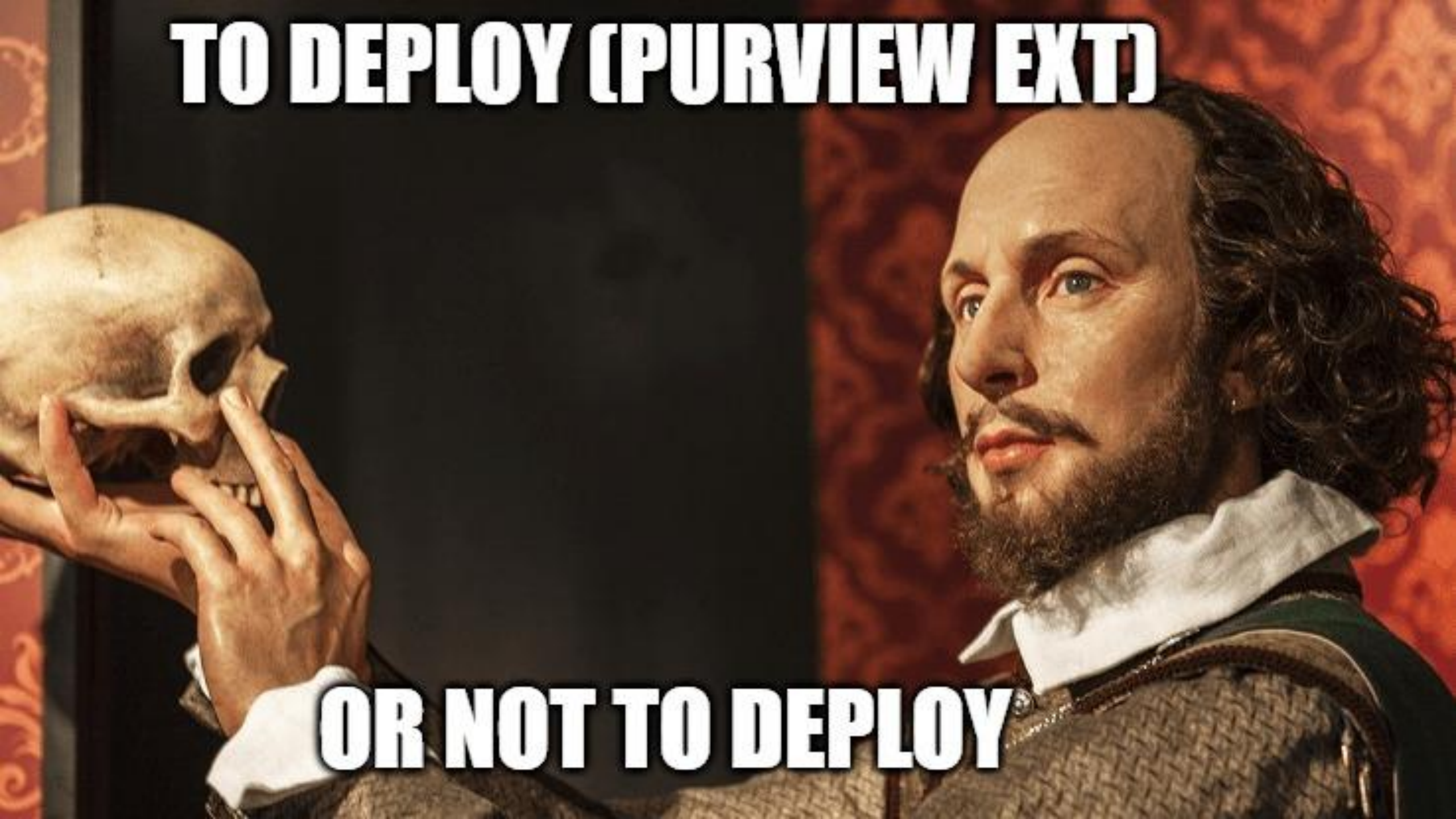
2 SERVICES

MDE (anti-malware protection)

DLP/IRM (DLP protection)

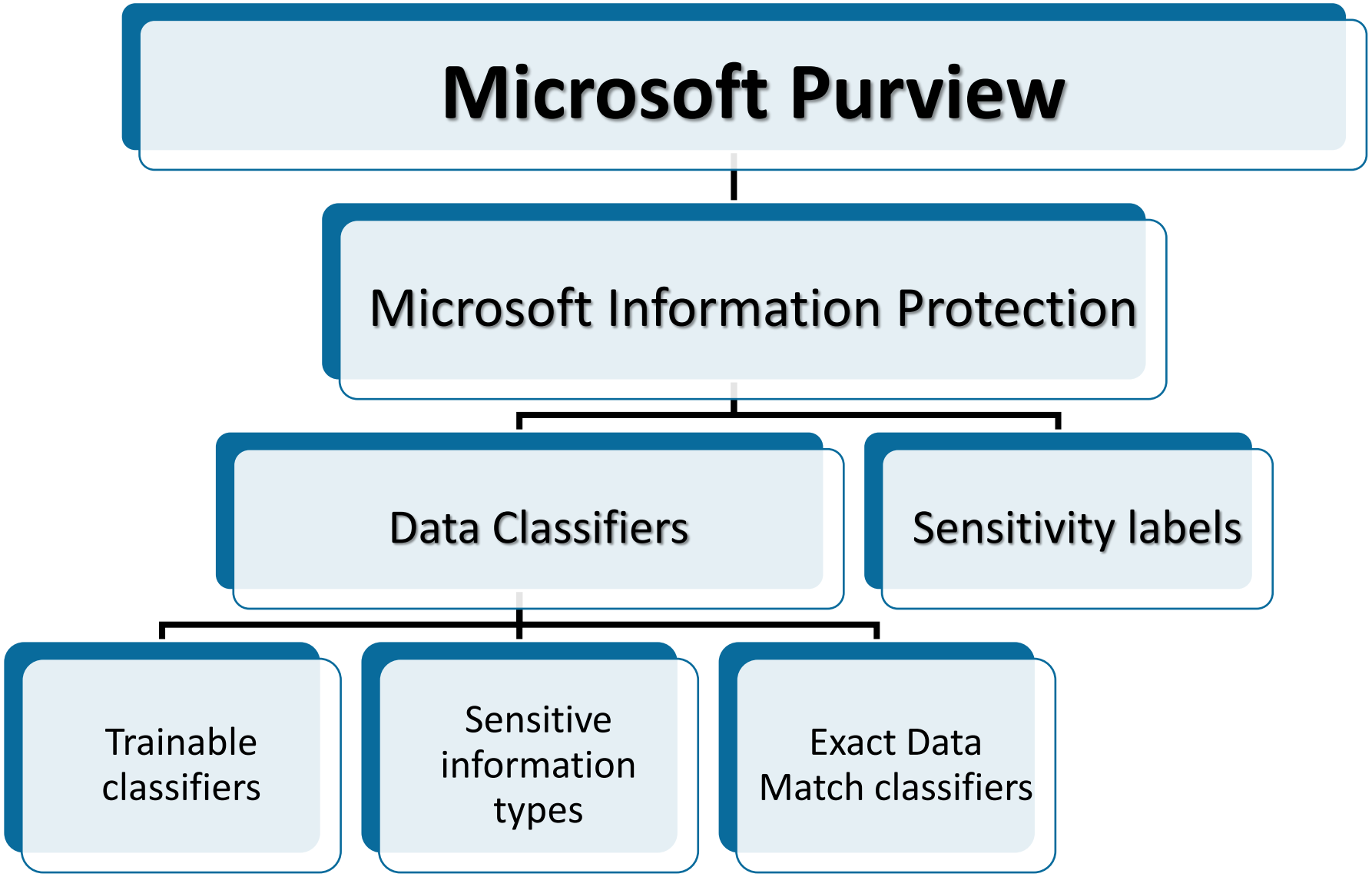
Purview web browser extension




TO DEPLOY (PURVIEW EXT)
OR NOT TO DEPLOY

	DLP	IRM	DSPM for AI
Microsoft Edge	Windows: Not required macOS: Not required	Windows: Not required macOS: Not required + Not supported for browsing to other AI sites	Windows: Required macOS: Not supported
Google Chrome	Windows: Required macOS: Not required	Windows: Required macOS: Not required + Not supported for browsing to other AI sites	Windows: Required macOS: Not supported
Firefox	Windows: Required macOS: Not required	Windows: Required macOS: Not required + Not supported for browsing to other AI sites	Windows: Required macOS: Not supported

Microsoft Purview hierarchy



Home
Solutions
Agents
Learn
Settings
Data Loss Prevention
Information Protection

Information Protection
Overview
Reports
Recommendations
Sensitivity labels
Policies
Classifiers
Trainable classifiers
Sensitive info types
EDM classifiers
On-demand classification
Collection policies
Explorers
Diagnostics

Related solutions
Data Security Investigations (preview)

Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

+ Create sensitive info type | + Create Fingerprint based SIT | Refresh | 334 items | Search

Filters: Supported platforms: Any | Type: Any | Publisher: Any | Add filter

Name	Supported platforms	Type	Publisher
Company Credit Card Number	All	Entity	Contoso
Mark 8 Project	All	Entity	Contoso
Top Secret	All	Entity	Contoso
Project Olivine	All	Entity	Contoso
Proseware Merger	All	Entity	Contoso
Project Obsidian	All	Entity	Contoso
Contoso Employee Onboarding	All	Fingerprint	M365DS517923.o...
ABA Routing Number	All	Entity	Microsoft Corpor...
Argentina National Identity (DNI) Number	All	Entity	Microsoft Corpor...

Lessons learned

- ✅ Inventory your Office 365 apps
- ✅ Inventory existing label integrations
- ✅ Know your license
- ✅ Prerequisite check ahead of deployment
- ✅ Several of them may already be satisfied
- ✅ Focus on getting the data classification right before further deployment

3. Encryption and label permissions


ENCRYPTION

The advantage of sensitivity label encryption

Encryption travels with an email or a file regardless where it goes.

Search

Copilot

MC2MC CONNECT

Edit sensitivity label

- Label details
- Scope
- **Items**
- Groups & sites
- Finish

Choose protection settings for the types of items you selected

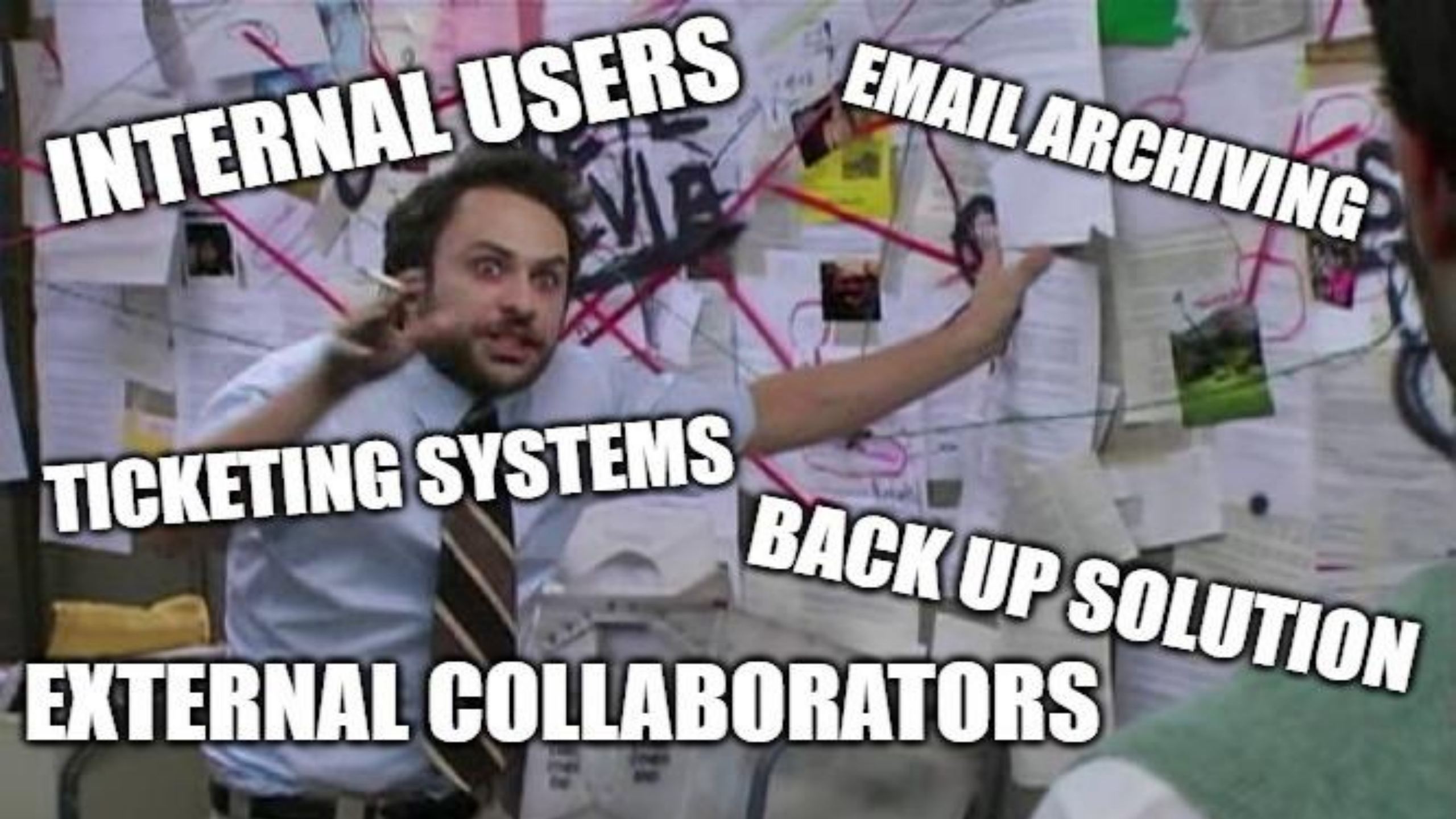
The protection settings you configure will be enforced when the label is applied to items in Microsoft 365.

- [x] **Control access**
  Control who can access and view labeled items.
- [ ] **Apply content marking**
  Add custom headers, footers, and watermarks to labeled items.

Back | Next | Cancel

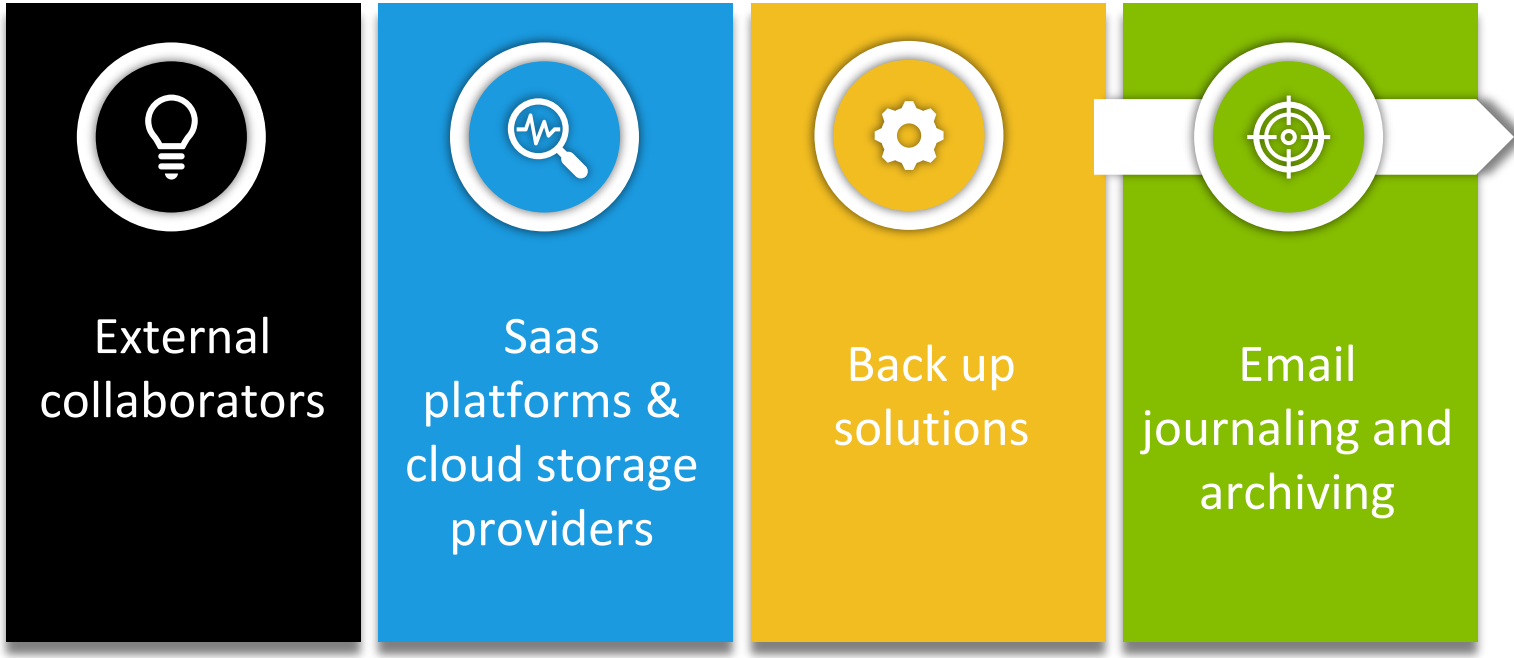
Lack of universal support for encryption

Not all platforms and applications can handle encrypted content, especially older software and certain cloud services.


INTERNAL USERS
EMAIL ARCHIVING
TICKETING SYSTEMS
BACK UP SOLUTION
EXTERNAL COLLABORATORS

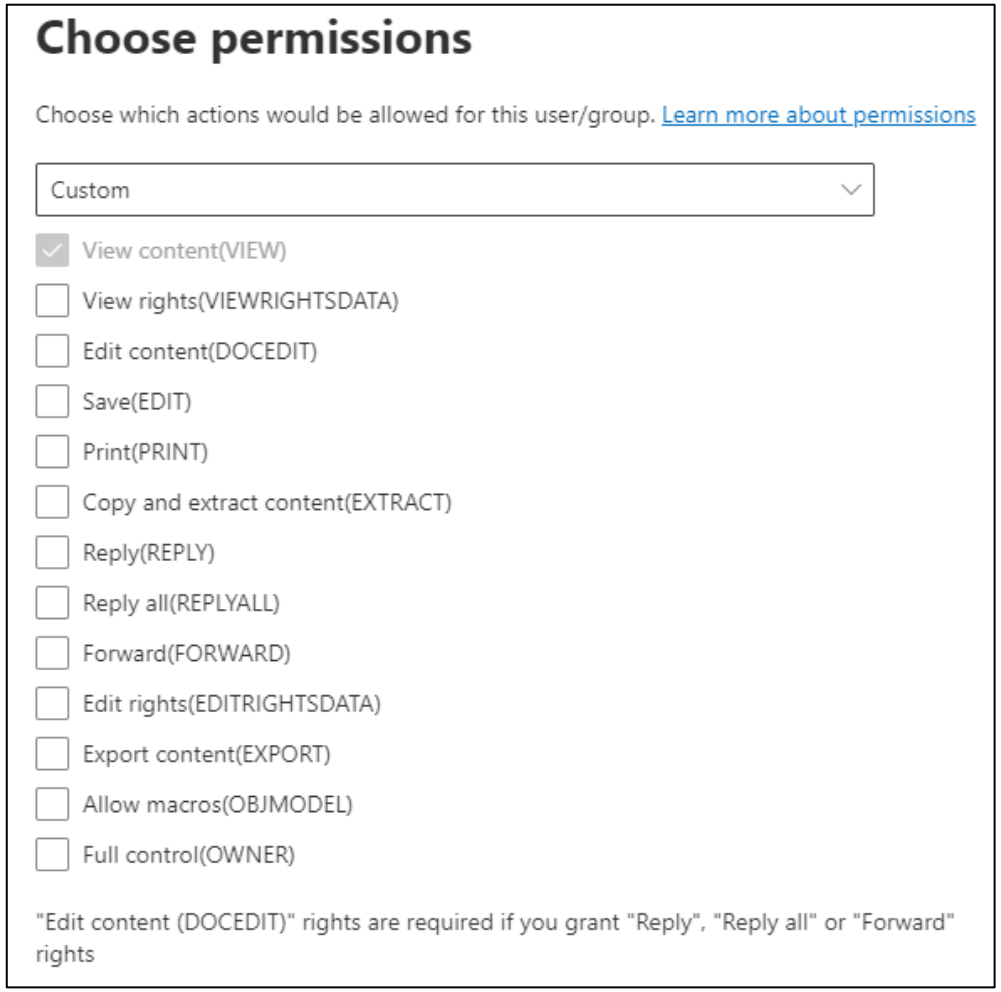
Lack of universal support for encryption

Not all platforms and applications can handle encrypted content, especially older software and certain cloud services.

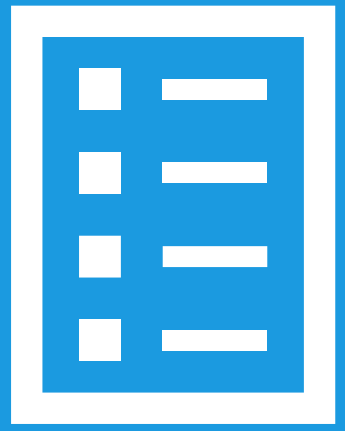


Pre-defined sensitivity label permission levels

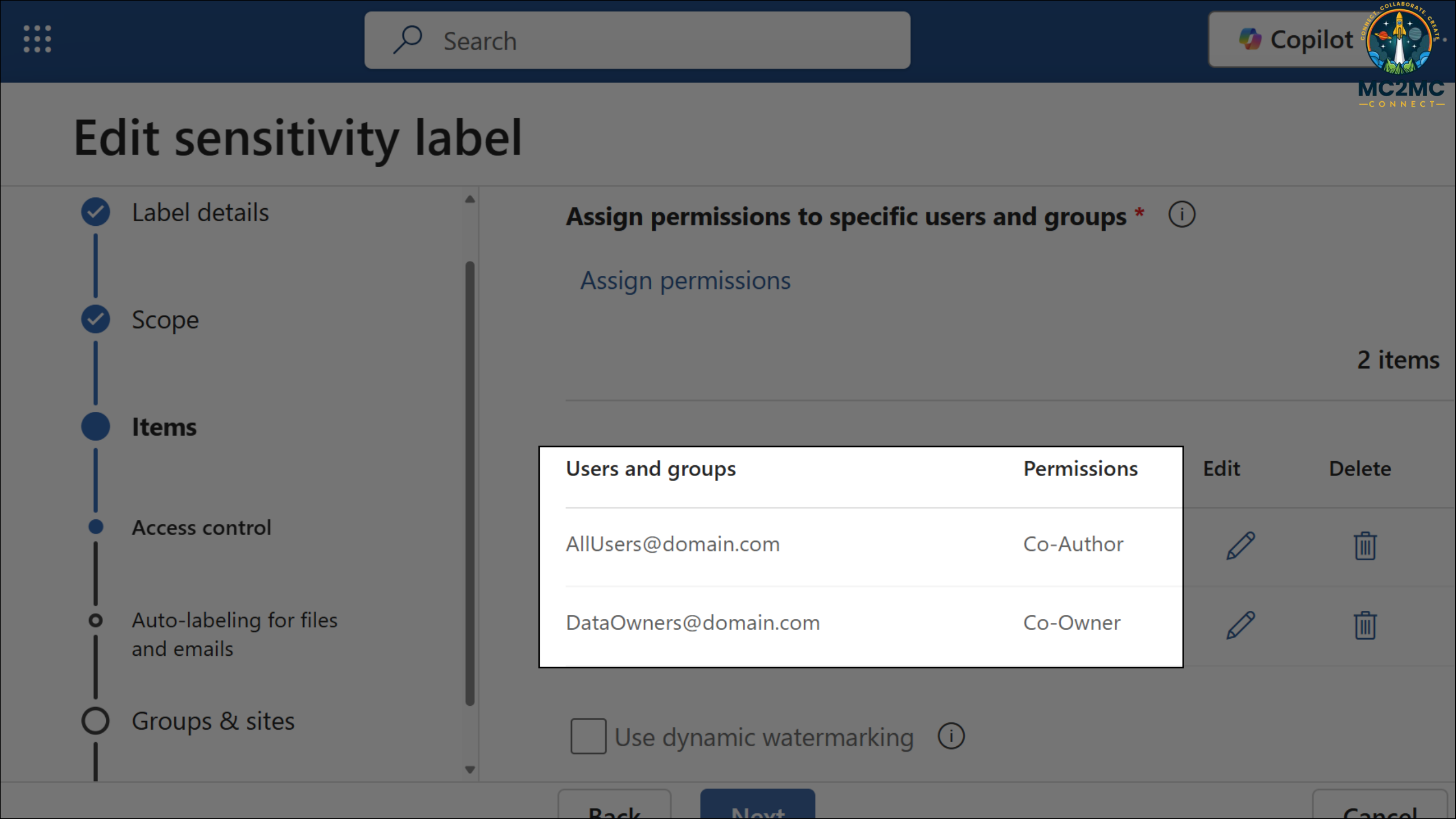
Specific permissions are granted to labelled content = Azure Rights Management



Built-in permission templates



	Owner	Editor	Restricted Editor	Viewer	
View	✅	✅	✅	✅	Email and Files
Open	✅	✅	✅	✅	
Read	✅	✅	✅	✅	
Save	✅	✅	✅	🚫	
Edit content & Edit	✅	✅	✅	🚫	
Copy (Extract)	✅	✅	🚫	🚫	
View rights	✅	✅	✅	✅	
Change rights	✅	🚫	🚫	🚫	
Allow Macros	✅	✅	✅	✅	
Save As, Export	✅	🚫	🚫	🚫	
Print	✅	✅	🚫	🚫	
Reply	✅	✅	✅	🚫	Email Only
Reply All	✅	✅	✅	🚫	
Forward	✅	✅	✅	🚫	
Full Control	✅	🚫	🚫	🚫	


Search
Copilot
MC2MC
CONNECT
Edit sensitivity label
Label details
Scope
Items
Access control
Auto-labeling for files and emails
Groups & sites
Assign permissions to specific users and groups *
Assign permissions
2 items
Users and groups
Permissions
Edit
Delete
AllUsers@domain.com
Co-Author
DataOwners@domain.com
Co-Owner
Use dynamic watermarking
Back
Next
Cancel

- You need to bulk decrypt files for auditing, legal, or other compliance reasons.

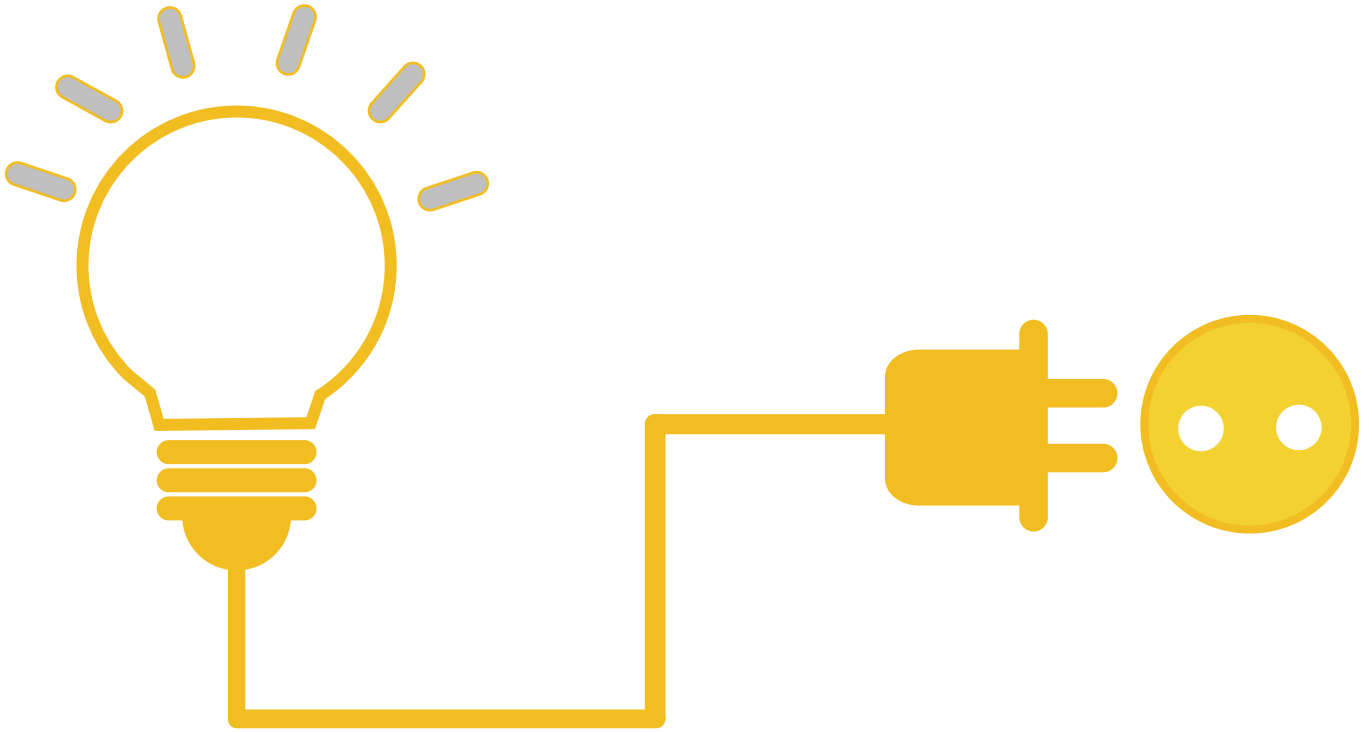
Configuration for the super user feature

By default, the super user feature is not enabled, and no users are assigned this role. It is enabled for you automatically if you configure the Rights Management connector for Exchange, and it is not required for standard services that run Exchange Online, Microsoft Sharepoint Server, or SharePoint in Microsoft 365.

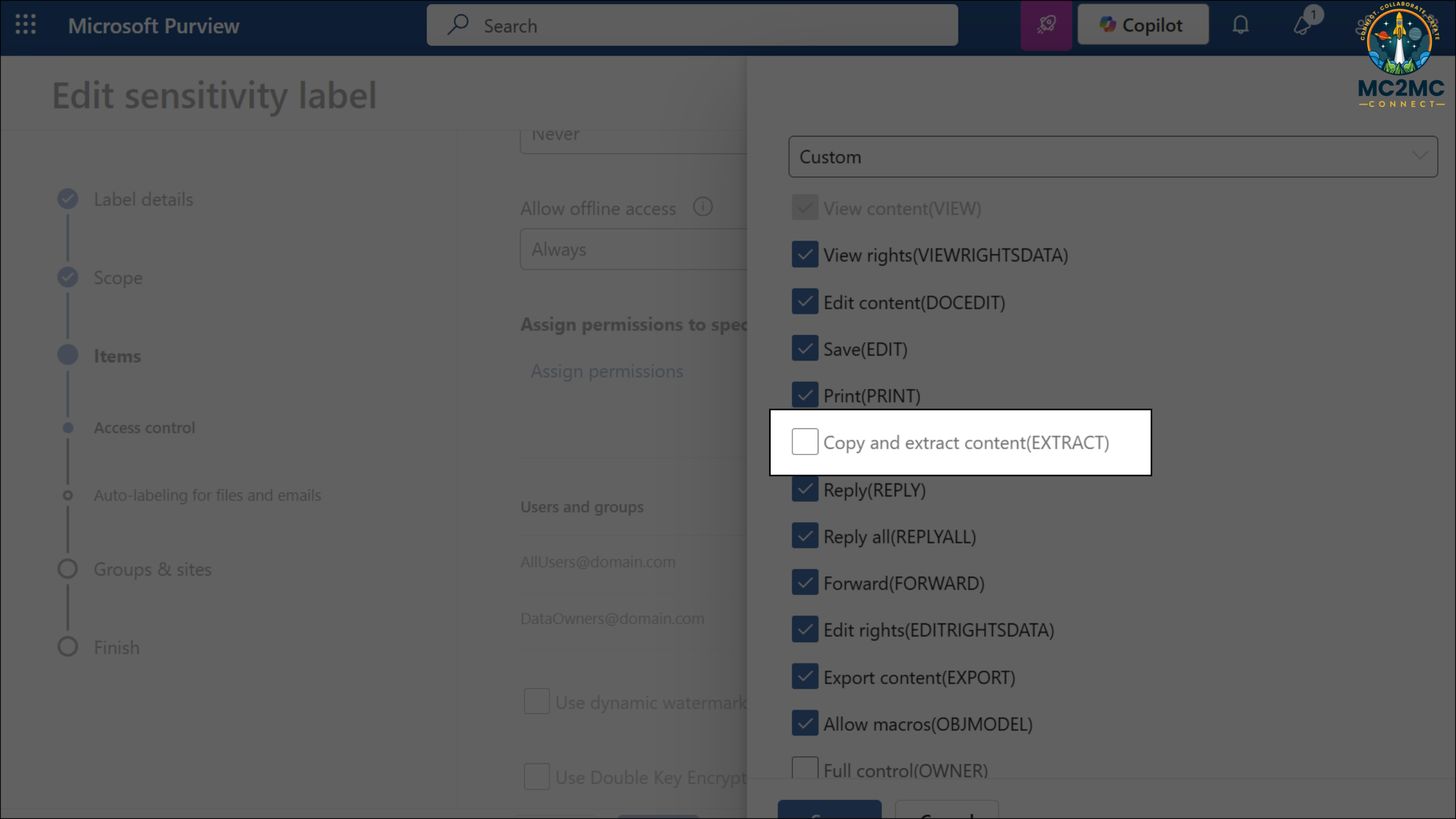
If you need to manually enable the super user feature, use the PowerShell cmdlet Enable-AipServiceSuperUserFeature, and then assign users (or service accounts) as needed by using the Add-AipServiceSuperUser cmdlet or the Set-AipServiceSuperUserGroup cmdlet and add users (or other groups) as needed to this group.

Microsoft 365 Copilot and access to encrypted content

Azure Rights Management permission



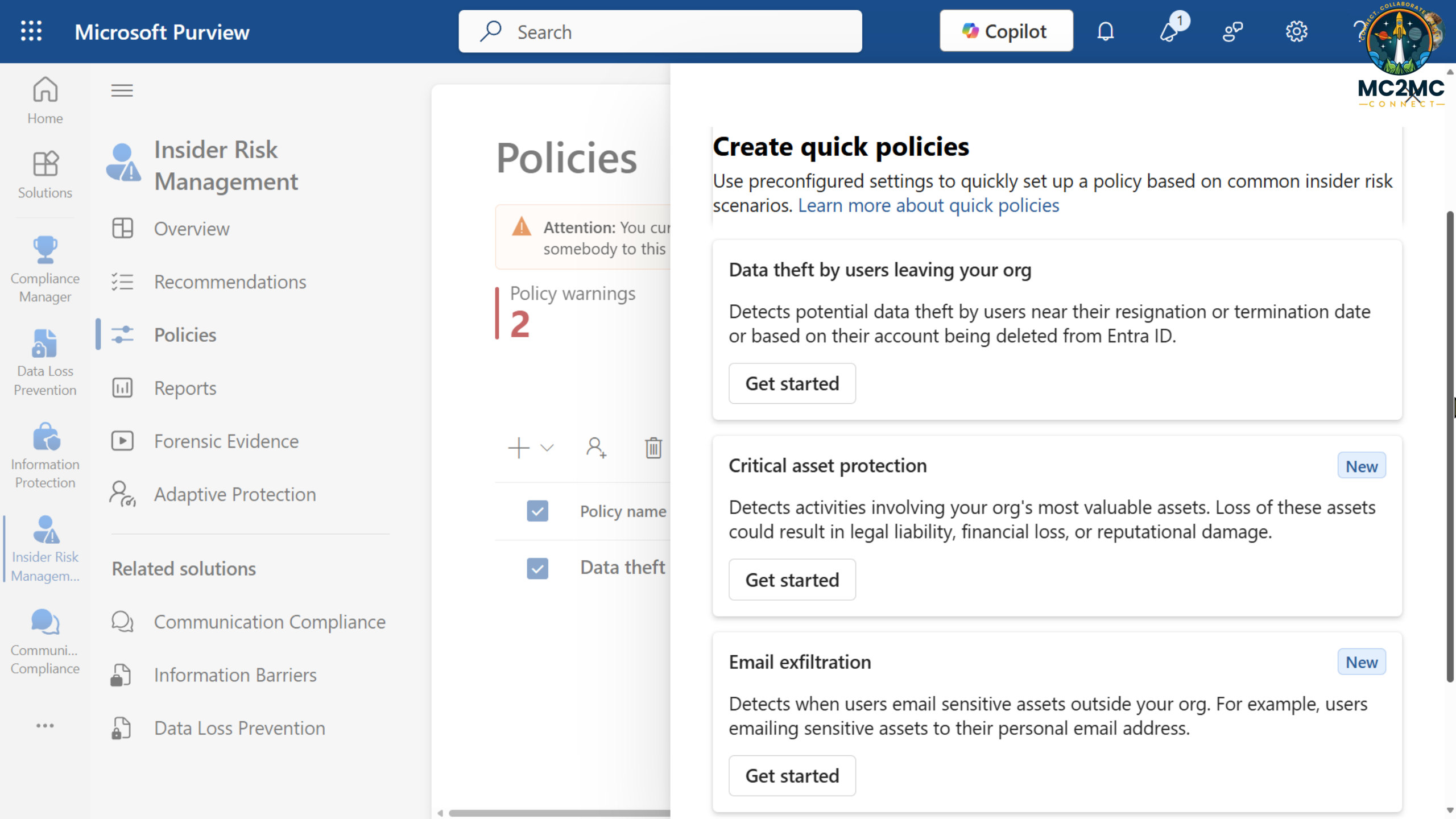
Copy and extract content (EXTRACT)


Microsoft Purview
Search
Copilot
MC2MC
CONNECT
Edit sensitivity label
Never
Label details
Allow offline access
Scope
Always
Items
Assign permissions to spec
Assign permissions
Access control
Auto-labeling for files and emails
Users and groups
Groups & sites
AllUsers@domain.com
DataOwners@domain.com
Finish
Use dynamic watermark
Use Double Key Encrypt
Custom
View content(VIEW)
View rights(VIEWRIGHTSDATA)
Edit content(DOCEDIT)
Save(EDIT)
Print(PRINT)
Copy and extract content(EXTRACT)
Reply(REPLY)
Reply all(REPLYALL)
Forward(FORWARD)
Edit rights(EDITRIGHTSDATA)
Export content(EXPORT)
Allow macros(OBJMODEL)
Full control(OWNER)

Lessons learned

- ✅ Encryption travels with data
- ✅ Plan for compatibility issues and exceptions
- ✅ Grant appropriate permissions
- ✅ Assign data owners with Co-Owner permissions
- ✅ Use the AIP Super User feature for bulk decryption
- ✅ Remove [EXTRACT] permission from highly sensitive data

4. Audit mode


Microsoft Purview
Search
Copilot
Home
Solutions
Compliance Manager
Data Loss Prevention
Information Protection
Insider Risk Managem...
Communi... Compliance
Insider Risk Management
Overview
Recommendations
Policies
Reports
Forensic Evidence
Adaptive Protection
Related solutions
Communication Compliance
Information Barriers
Data Loss Prevention
Policies
Attention: You cur
somebody to this
Policy warnings
2
Policy name
Data theft
Create quick policies
Use preconfigured settings to quickly set up a policy based on common insider risk scenarios. Learn more about quick policies
Data theft by users leaving your org
Detects potential data theft by users near their resignation or termination date or based on their account being deleted from Entra ID.
Get started
Critical asset protection
New
Detects activities involving your org's most valuable assets. Loss of these assets could result in legal liability, financial loss, or reputational damage.
Get started
Email exfiltration
New
Detects when users email sensitive assets outside your org. For example, users emailing sensitive assets to their personal email address.
Get started

Info to label
Name
Label
Admin units
Locations
Policy rules
Policy mode
Finish

Decide if you want to test out the policy now or later

To help you determine whether the label will be applied to the correct items, you'll need to run the policy in simulation mode before turning it on. You can do this right away or wait until later.

- (●) **Run policy in simulation mode**
  We'll gather items that match the policy but labels won't be applied yet. It's highly recommended that you review these items to decide whether the policy needs to be refined or if it's ready to be turned on.
  - [ ] Automatically turn on policy if not modified after 7 days in simulation.
    The 7-day period will restart each time the policy is modified while in simulation.
- ( ) **Leave policy turned off**
  Your settings will be saved, but the policy will be inactive until you run it in simulation mode and then turn it on.

Create rule

Actions

Use actions to protect content when the conditions are met.

Audit or restrict activities on devices

When specific activities are detected on devices with protected files containing sensitive information, you can choose whether to only audit the activity, block it entirely, or block it and allow users to override the restriction.
Learn more restricting device activity

Service domain and browser activities

Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.

- [x] Upload to a restricted cloud service domain or access from an unallowed browsers — Audit only

+ Choose different restrictions for sensitive service domains

Save Cancel

Edit rule

When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

- [x] Copy to clipboard — Audit only
  - + Choose different copy to clipboard restrictions
- [x] Copy to a removable USB device — Audit only
  - + Choose different removable USB device restrictions
- [x] Copy to a network share
  - + Choose different network share restrictions
- [x] Print — Audit only

Audit only
Block with overr...
Block
Allow
Off

Save Cancel

Data Loss Prevention
Overview
Policies
Alerts
Classifiers
Explorers
Data explorer
Content explorer (classic)
Activity explorer
Related solutions
Information Protection
Insider Risk Management

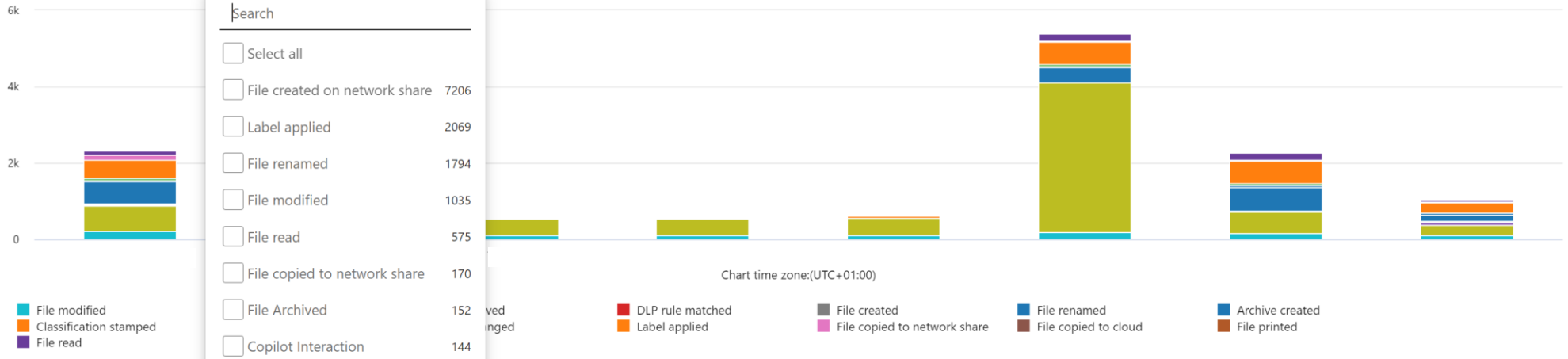
Activity explorer

Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, SharePoint, OneDrive, and endpoint devices. Support for more locations is coming soon. Learn more

Copilot | Show me the top 5 activities from the past week | Filter and investigate activities | Find files used in specific activities

Selected filter set: None | Save

Date: | Activity: Any | Location: Any | User: Any | Sensitivity label: Any | Add filter | Reset all



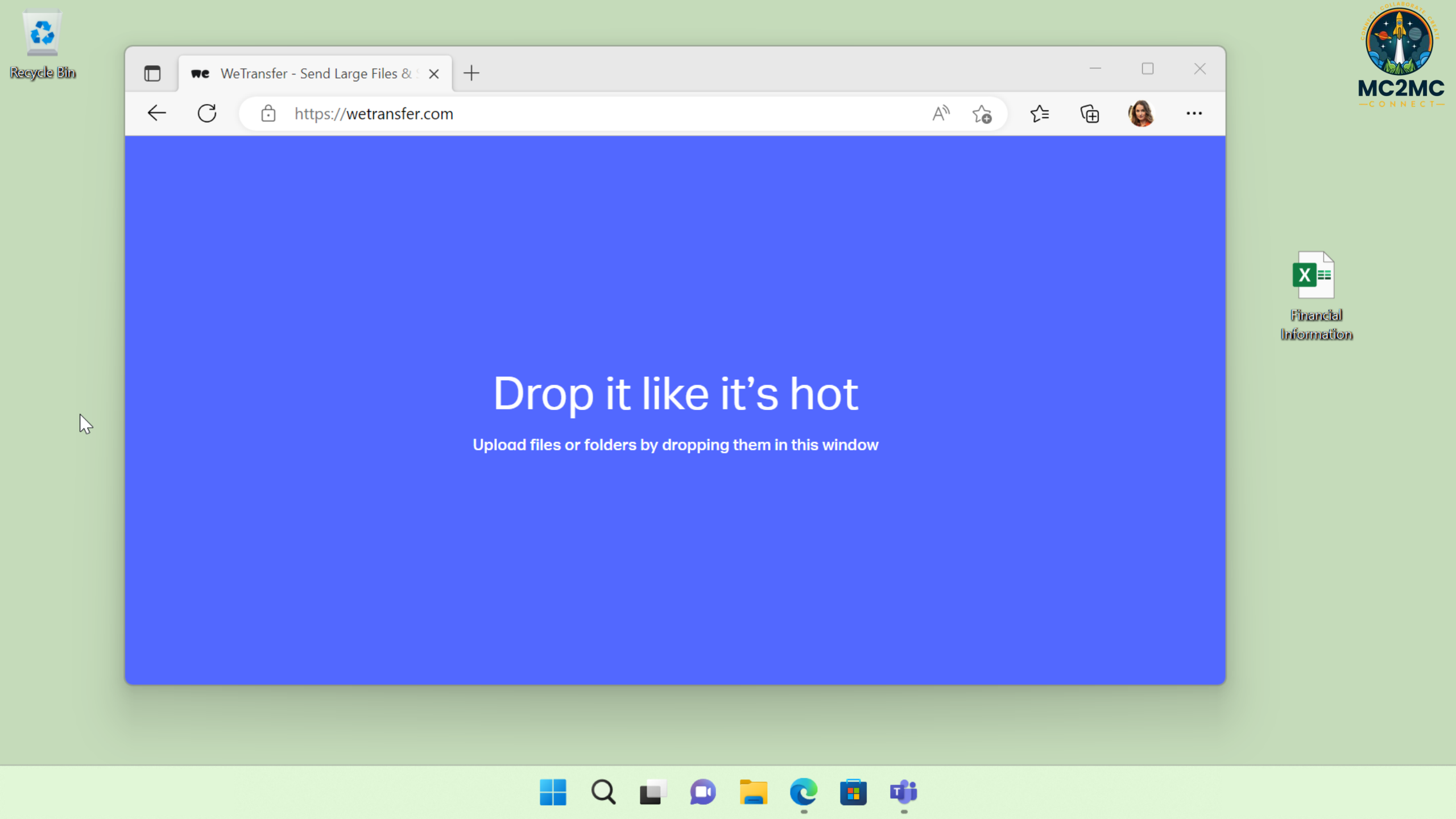
Search

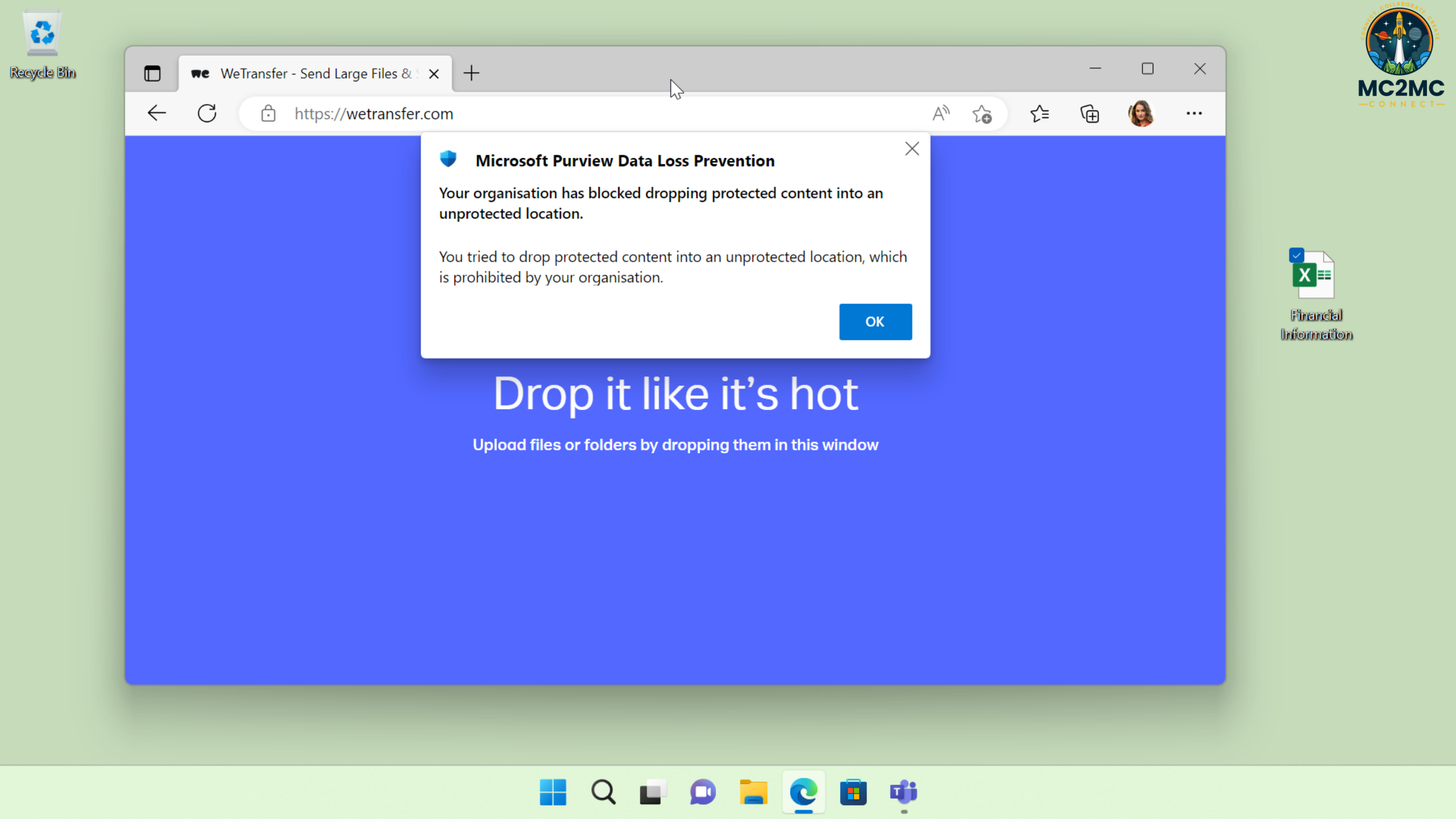
- Select all
- File created on network share 7206
- Label applied 2069
- File renamed 1794
- File modified 1035
- File read 575
- File copied to network share 170
- File Archived 152
- Copilot Interaction 144
- Archive created 119
- File created 76
- Classification stamped 63
- File copied to cloud 23
- Label changed 10
- File printed 1
- DLP rule matched 1

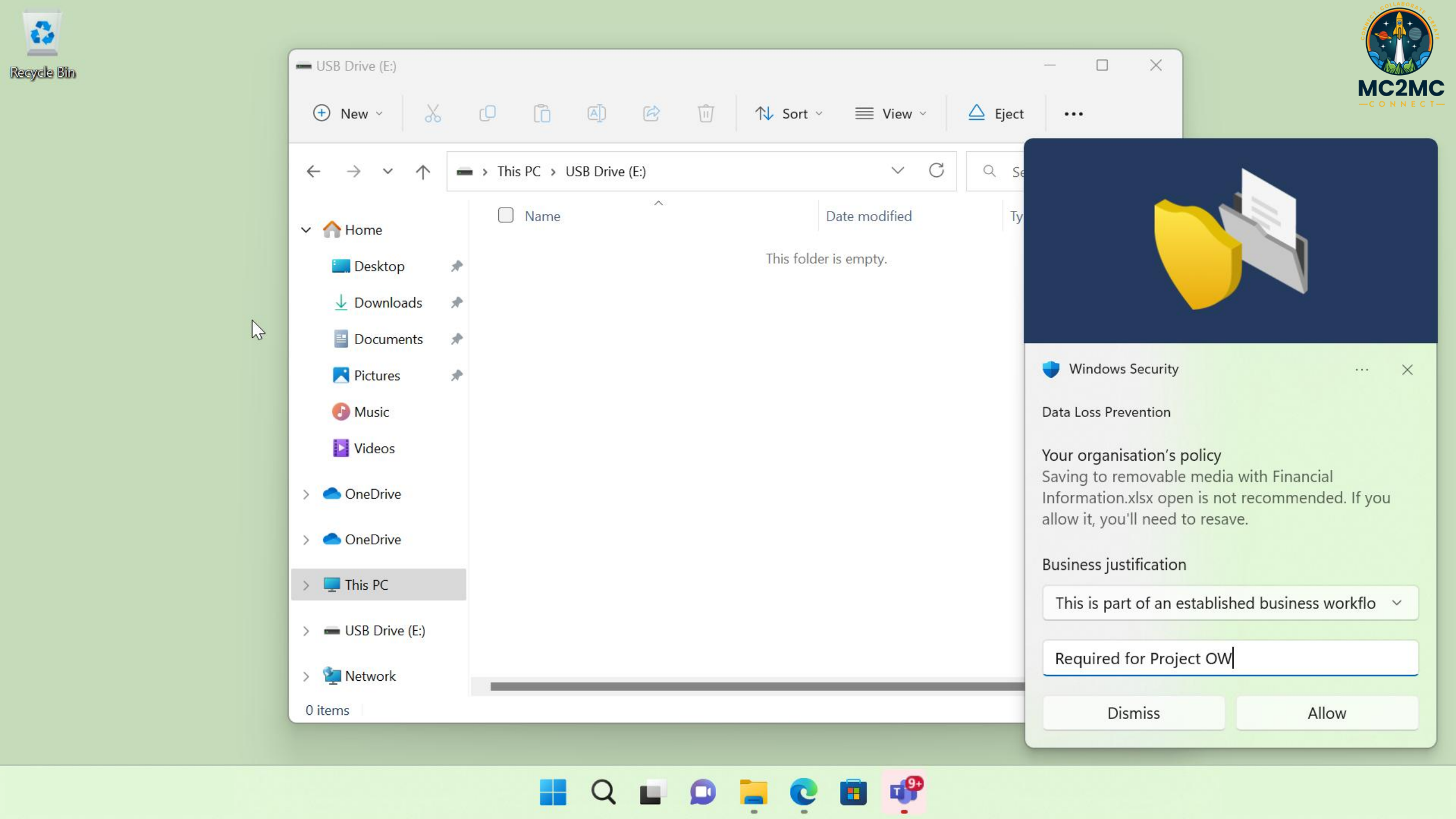
Apply

Export | Refresh | 13440 items | Customize columns

Activity	Location	User	Happened	Policy	Rule
File renamed	Endpoint devices				
File created on networ	Endpoint devices				
Label applied	Exchange				
File modified	Endpoint devices				
File renamed	Endpoint devices				
File renamed	Endpoint devices				
File renamed	Endpoint devices				


Recycle Bin
WeTransfer - Send Large Files &
https://wetransfer.com
Drop it like it's hot
Upload files or folders by dropping them in this window
Financial Information
MC2MC
CONNECT

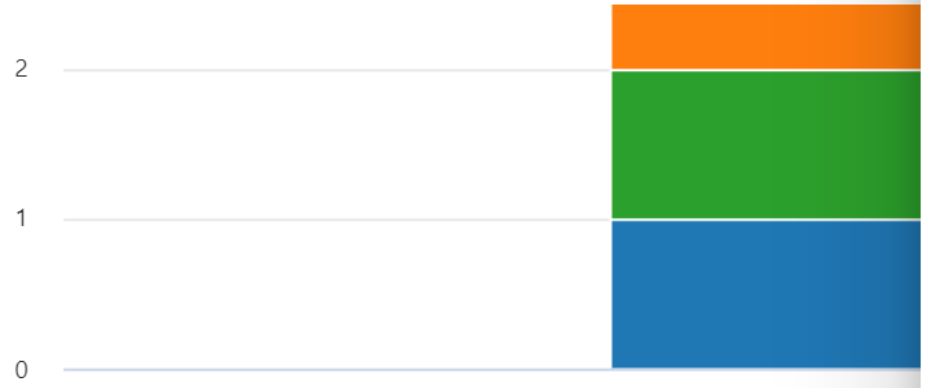

Recycle Bin
WeTransfer - Send Large Files &
https://wetransfer.com
Microsoft Purview Data Loss Prevention
Your organisation has blocked dropping protected content into an unprotected location.
You tried to drop protected content into an unprotected location, which is prohibited by your organisation.
OK
Drop it like it's hot
Upload files or folders by dropping them in this window
Financial Information
MC2MC
CONNECT


Recycle Bin
USB Drive (E:)
New
Sort
View
Eject
This PC
USB Drive (E:)
Name
Date modified
This folder is empty.
Home
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
OneDrive
This PC
USB Drive (E:)
Network
0 items
Windows Security
Data Loss Prevention
Your organisation's policy
Saving to removable media with Financial Information.xlsx open is not recommended. If you allow it, you'll need to resave.
Business justification
This is part of an established business workflo
Required for Project OW
Dismiss
Allow
MC2MC
CONNECT

Contoso Electronics Microsoft Purview

Built-in filters Reset Filters

Date: Activity: FilePrinted, FileD



File copied to removable media File created File copie

Export Refresh

Activity	File
File copied to removabl...	C:\Users\AdeleVance\Desktop\Finan
File copied to cloud	C:\Users\AdeleVance\Desktop\Finan
File created	C:\Users\AdeleVance\AppData\Loca

File copied to cloud

Activity details

Activity
File copied to cloud

Happened

Client IP

Enforcement mode
Block

Originating domain
pnl1-excel.officeapps.live.com

Target domain
wetransfer.com

About this item

File
Financial Information.xlsx

User
AdeleV@MS .OnMicrosoft.com

File extension
xlsx

File size
9.2 MB

Sensitive info type
Credit Card Number +5 more

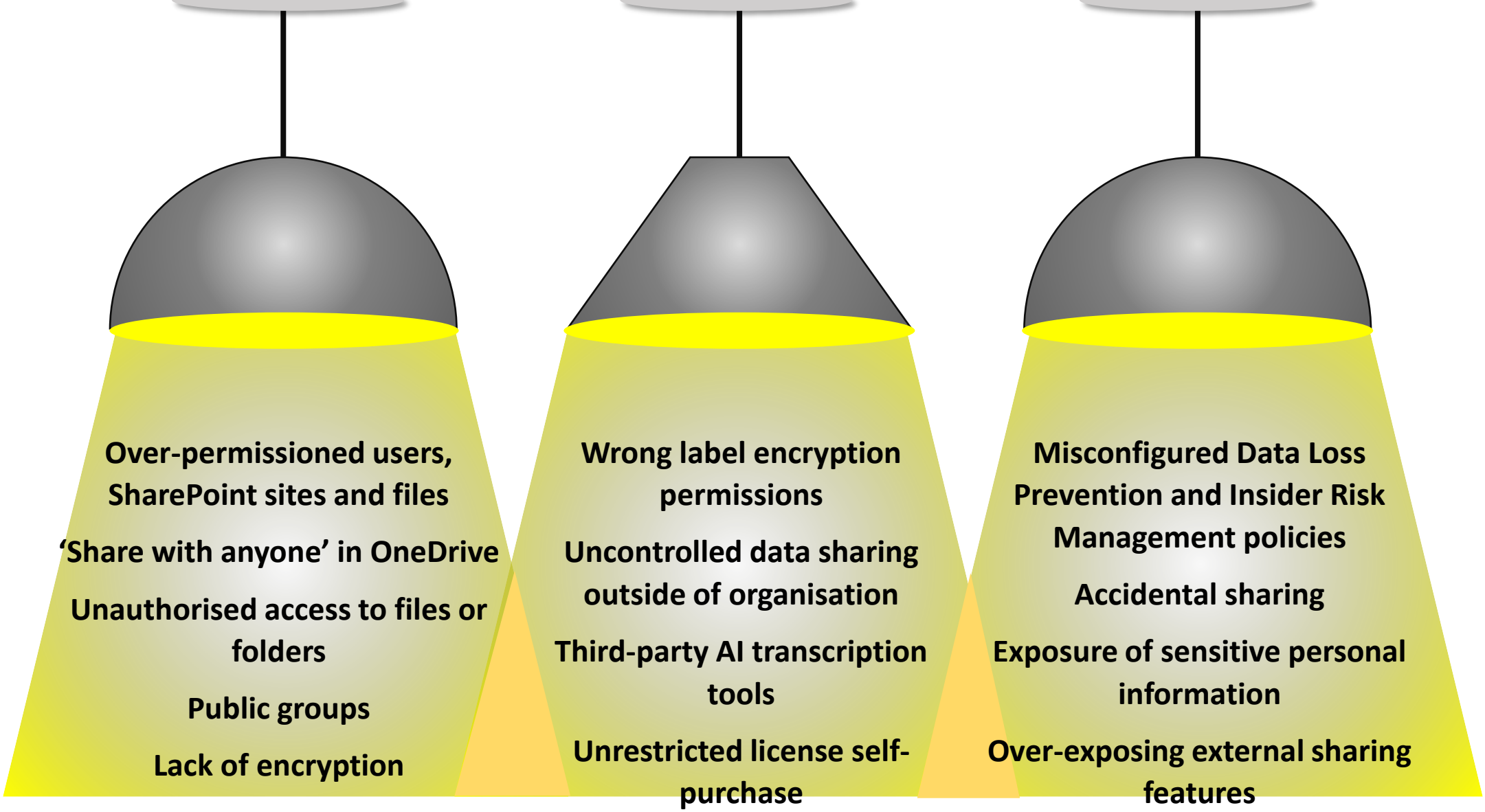
Policy
Default policy for devices

Rule

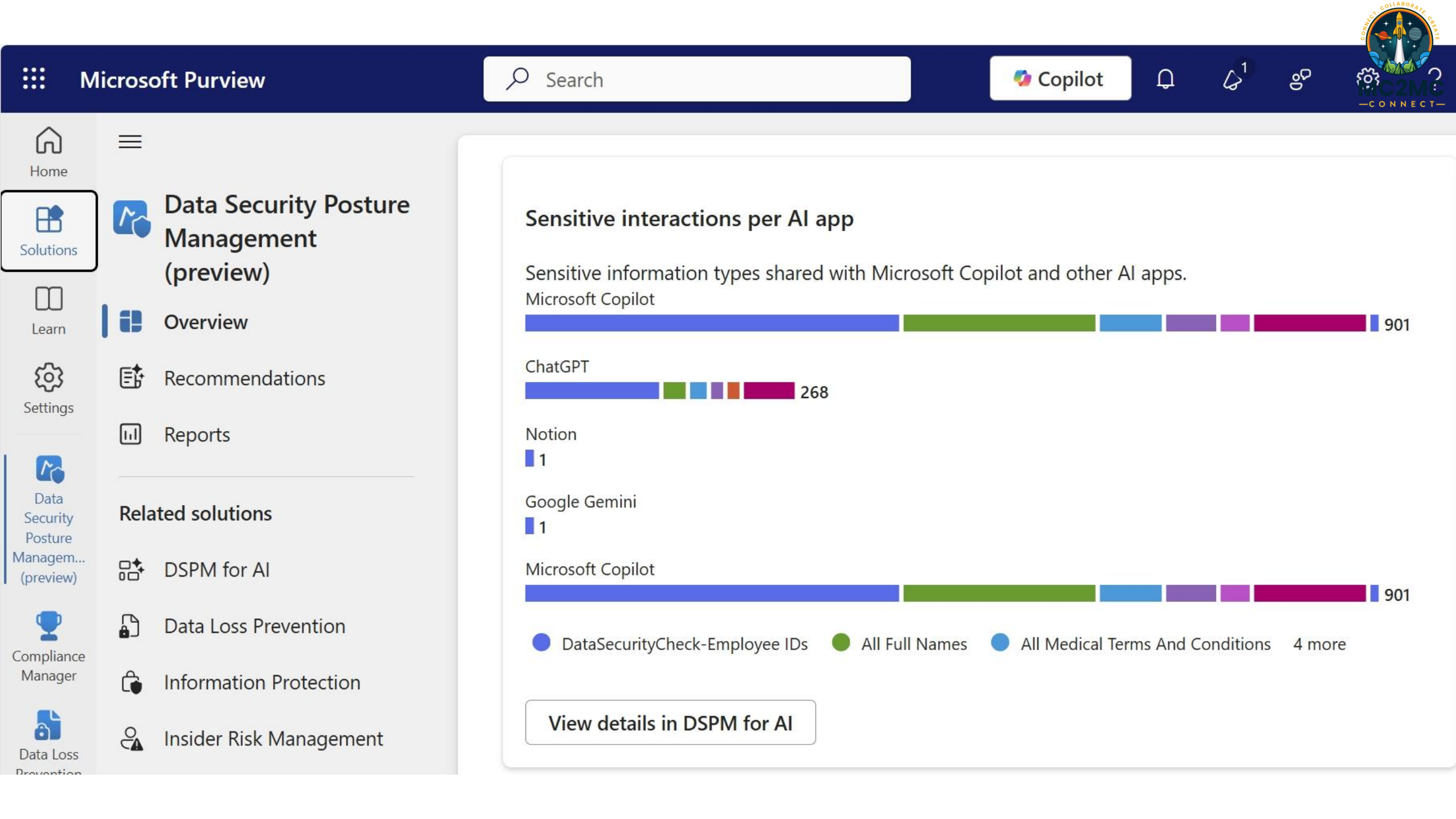
Lessons learned

- ✅ Get the data
- ✅ Make the decisions
- ✅ Audit > Simulate > Block with override
- ✅ Provides tremendous value for IR teams too

5. Shadow AI



Microsoft 365 Copilot


Microsoft Purview
Search
Copilot
Home
Solutions
Learn
Settings
Data Security Posture Managem... (preview)
Compliance Manager
Data Loss
Data Security Posture Management (preview)
Overview
Recommendations
Reports
Related solutions
DSPM for AI
Data Loss Prevention
Information Protection
Insider Risk Management
Sensitive interactions per AI app
Sensitive information types shared with Microsoft Copilot and other AI apps.
Microsoft Copilot
901
ChatGPT
268
Notion
1
Google Gemini
1
Microsoft Copilot
901
DataSecurityCheck-Employee IDs
All Full Names
All Medical Terms And Conditions
4 more
View details in DSPM for AI

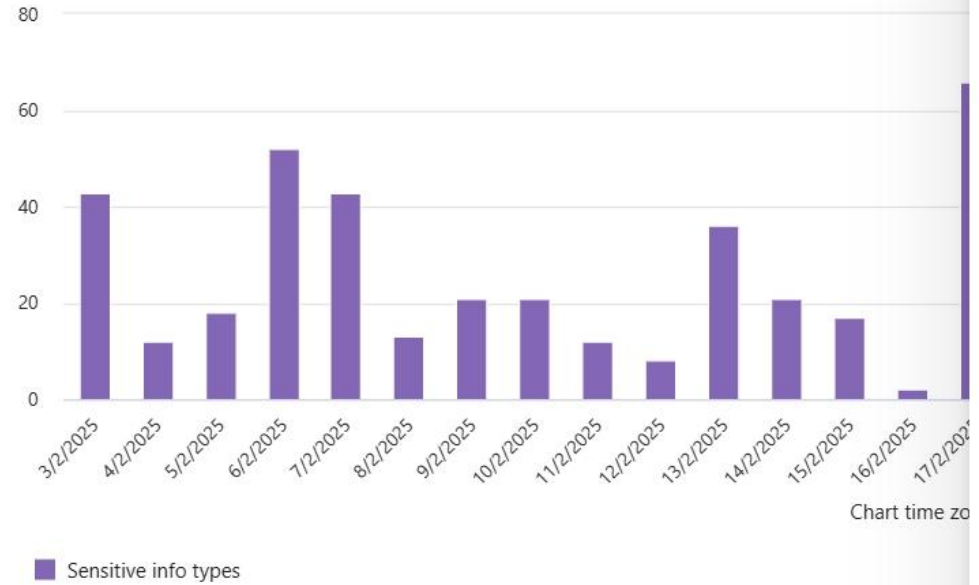
Home
Solutions
Learn
Settings
Data Security Posture Managem... (preview)
DSPM for AI
Data Loss Prevention
Insider Risk Managem...

DSPM for AI
Overview
Recommendations
Reports
Policies
Activity explorer
Data assessments Preview

Activity explorer

Review AI activity including AI interactions (prompts and response), activity with s

Filters: Timestamp: 3/2/2025-3/3/2025 | Activity type: Sensitive info types | AI app | App accessed in: Any | User: Any | User risk level: Any | Sensitive info typ | Scope: Any | Reset all



Export Selected Items

Activity type	User	User risk level	Timestar
Sensitive info types	[redacted]		3 Mar 20

Sensitive info types

Activity details

Activity type
Sensitive info types

Timestamp
3 Mar 2025 10:12

Record ID
75a2fb67-8680-4f64-b677-848c8abf60e9

About this user

User
[redacted]

View more user details in insider risk management

App details

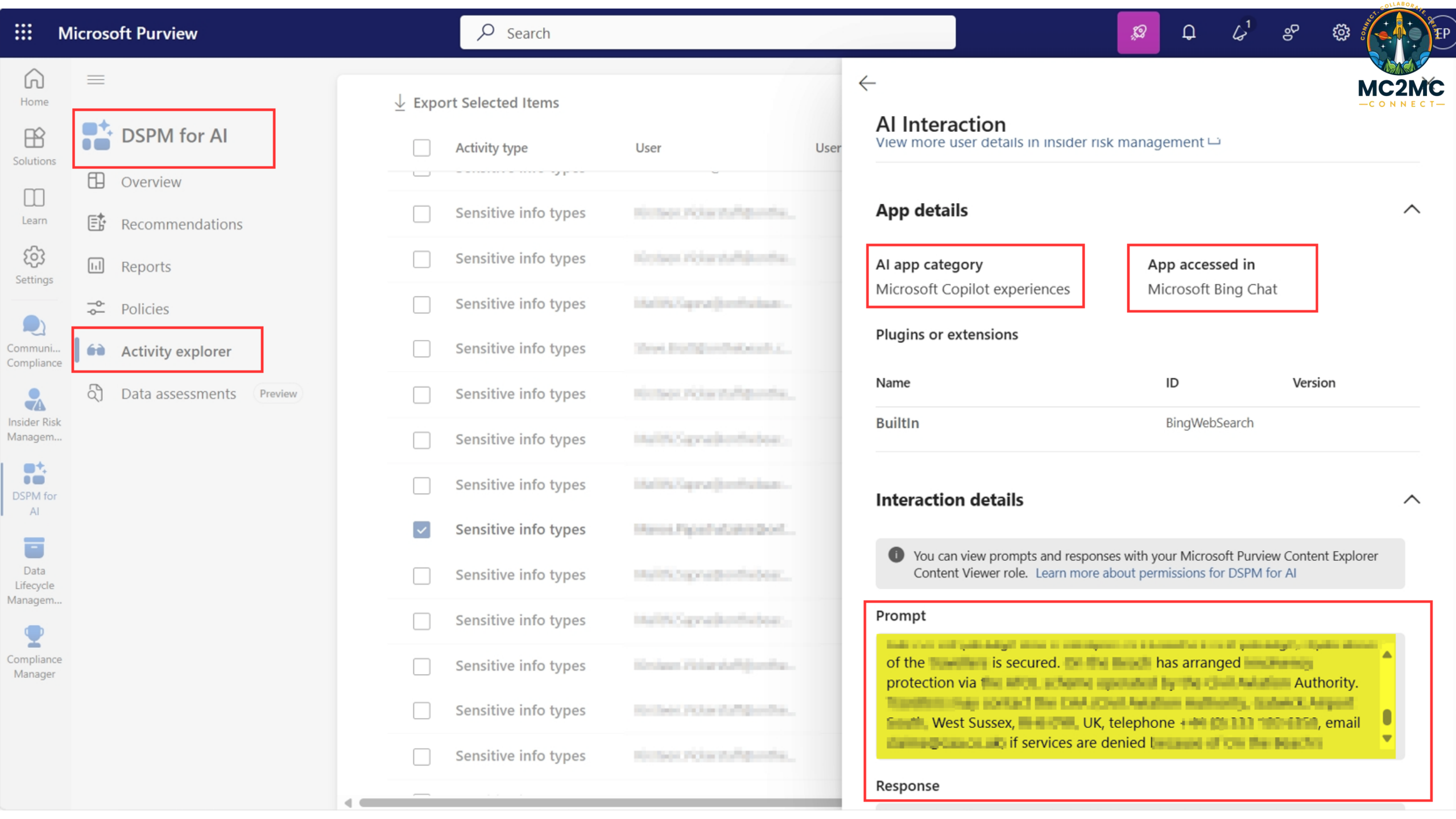
AI app category
Microsoft Copilot experiences

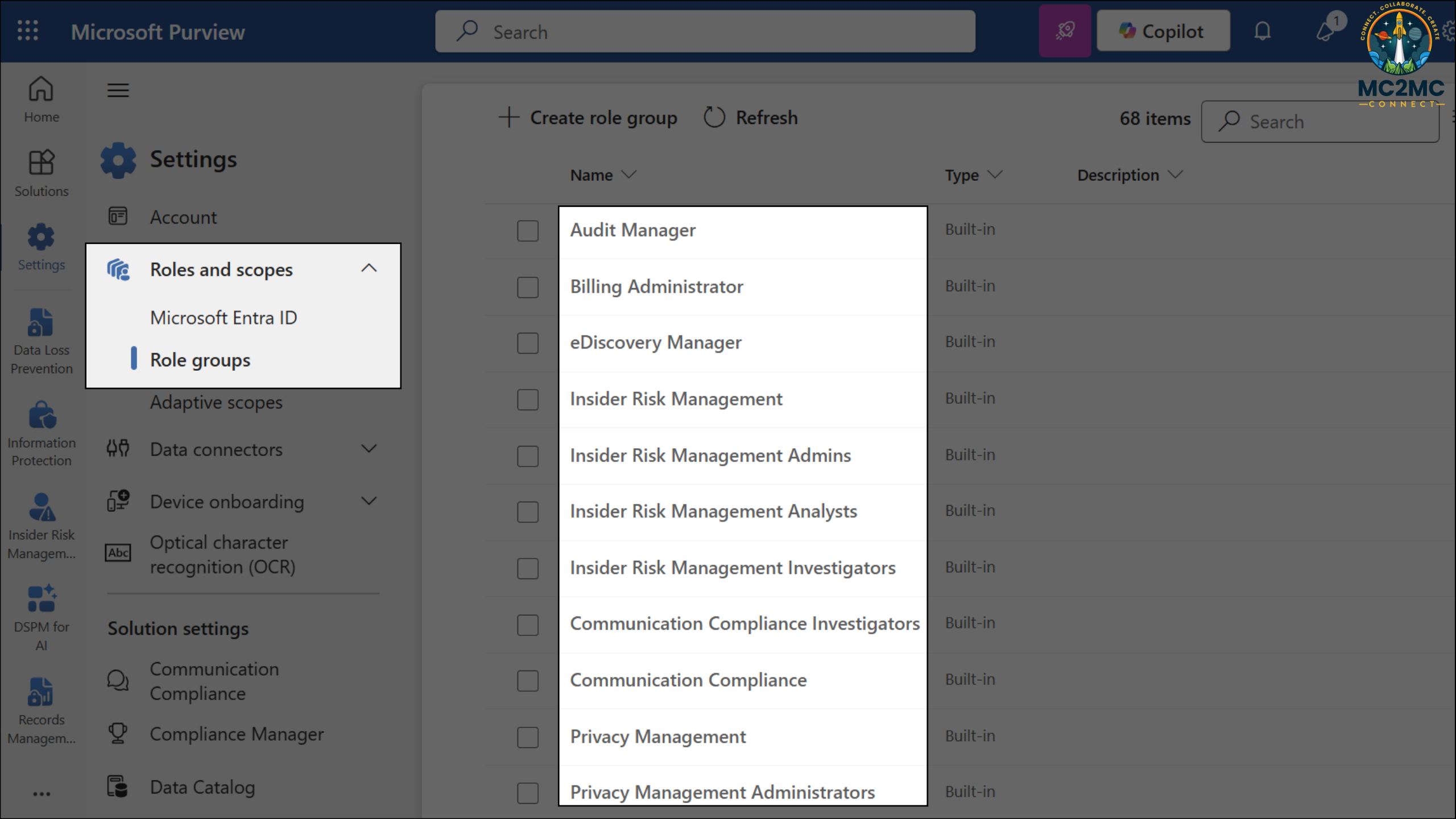
App accessed in
Microsoft 365 Copilot Chat

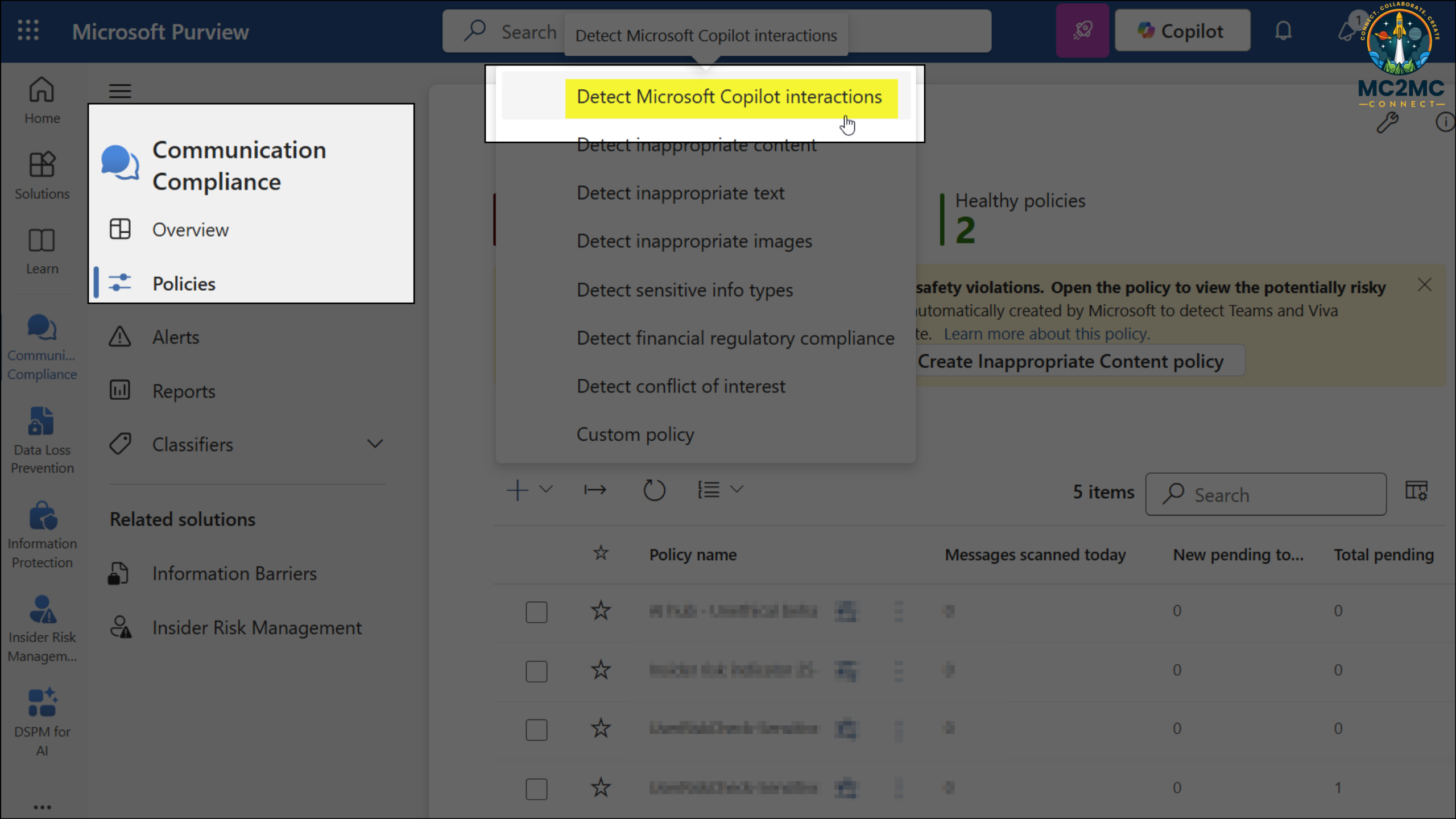
Interaction details

Interaction data
View related AI interaction activity

Sensitive info types detected
HR


Microsoft Purview
Search
Home
Solutions
Learn
Settings
Communi... Compliance
Insider Risk Managem...
DSPM for AI
Data Lifecycle Managem...
Compliance Manager
DSPM for AI
Overview
Recommendations
Reports
Policies
Activity explorer
Data assessments
Preview
Export Selected Items
Activity type
User
Sensitive info types
AI Interaction
View more user details in insider risk management
App details
AI app category
Microsoft Copilot experiences
App accessed in
Microsoft Bing Chat
Plugins or extensions
Name
ID
Version
BuiltIn
BingWebSearch
Interaction details
You can view prompts and responses with your Microsoft Purview Content Explorer Content Viewer role. Learn more about permissions for DSPM for AI
Prompt
Response


Microsoft Purview
Search
Copilot
MC2MC
CONNECT
Home
Solutions
Settings
Data Loss Prevention
Information Protection
Insider Risk Managem...
DSPM for AI
Records Managem...
...
Settings
Account
Roles and scopes
Microsoft Entra ID
Role groups
Adaptive scopes
Data connectors
Device onboarding
Optical character recognition (OCR)
Solution settings
Communication Compliance
Compliance Manager
Data Catalog
Create role group
Refresh
68 items
Search
Name
Type
Description
Audit Manager
Billing Administrator
eDiscovery Manager
Insider Risk Management
Insider Risk Management Admins
Insider Risk Management Analysts
Insider Risk Management Investigators
Communication Compliance Investigators
Communication Compliance
Privacy Management
Privacy Management Administrators
Built-in


Microsoft Purview
Search
Detect Microsoft Copilot interactions
Copilot
Detect Microsoft Copilot interactions
Detect inappropriate content
Detect inappropriate text
Detect inappropriate images
Detect sensitive info types
Detect financial regulatory compliance
Detect conflict of interest
Custom policy
Home
Solutions
Learn
Communi... Compliance
Data Loss Prevention
Information Protection
Insider Risk Managem...
DSPM for AI
Communication Compliance
Overview
Policies
Alerts
Reports
Classifiers
Related solutions
Information Barriers
Insider Risk Management
Healthy policies
2
safety violations. Open the policy to view the potentially risky
utomatically created by Microsoft to detect Teams and Viva
te. Learn more about this policy.
Create Inappropriate Content policy
5 items
Search
Policy name
Messages scanned today
New pending to...
Total pending
0
0
0
0
0
0
0
1
MC2MC
CONNECT

- Policy template
- Name and description
- Admin units
- Users and groups
- Content to prioritize
- Triggering event
- Indicators
- Finish

Data theft

Data theft by departing users

Data leaks

Data leaks

Data leaks by risky users

Data leaks by priority users

Risky AI usage (preview)

Risky AI usage (preview)

Security policy violations (preview)

Security policy violations (preview)

Security policy violations by departing users (preview)

Security policy violations by risky users (preview)

Security policy violations by

Risky AI usage (preview)

Detects potentially risky or sensitive content in Microsoft Copilot experiences, Enterprise AI apps and web versions of other AI apps.

Prerequisites

Communication compliance policy detecting inappropriate content in messages OPTIONAL RECOMMENDED

You'll be able to create a communication compliance policy when selecting the triggering event later in this wizard, .

HR data connector OPTIONAL RECOMMENDED

Configure to periodically import resignation and termination date details for your organization. Set up HR Connector

Devices onboarded OPTIONAL

- **Microsoft Purview extension** REQUIRED

  Microsoft Insider risk extension (on Edge browser) or Microsoft Purview extension (on Chrome browser) must be

Next

Cancel

- Template or custom policy
- Name
- Admin units
- **Locations**
- Policy settings
- Policy mode
- Finish

Exchange email	Turn on location to scope	
SharePoint sites	Turn on location to scope	
OneDrive accounts	Turn on location to scope	
Teams chat and channel messages	Turn on location to scope	
Devices	Turn on location to scope	
Instances	Turn on location to scope	
On-premises repositories	Turn on location to scope	
Fabric and Power BI workspaces	Turn on location to scope	
Microsoft 365 Copilot (preview)	All users & groups	Edit

Back Next Cancel

Template or custom policy
Name
Admin units
Locations
Policy settings
Advanced DLP rules
Policy mode
Finish

Create rule

Content contains

Group name *

Default

Sensitivity labels

Confidential

Add

Evaluate predicate for (available for Exchange workload only)

Message or attachment Message only Attachments only

Create group

Add condition Add group

Actions

Use actions to protect content when the conditions are met.

Prevent Copilot from processing content (preview)

Content that matches your conditions won't be used by Copilot to generate responses. This action is supported for specific content that's processed across various Copilot experiences. Lear

Prevent Copilot from processing content

Lessons learned… Purview & beyond

- ✅ AI tools are here to stay
- ✅ Get Copilot and AI-ready
- ✅ Review user access to data sources
- ✅ Follow the principle of least privilege
- ✅ Use PIM for Purview RBAC roles
- ✅ Deploy policies to manage AI & oversharing risks
- ✅ Enable secure collaboration settings

6. Safe deployment practices

Secure by default with Microsoft Purview and protect against oversharing

Foundational

Start with recommended labels

Activities

- Start with default labels and protection at file and site level
- Turn on data security pre-requisites and adv. analytics
- Train users on managing exceptions
- Turn on DLP for labeled content

Outcomes

- M365 new/updated content protected

Efforts

- 1 week

Managed

Address files with highest sensitivity

Activities

- Manually configure priority sites default library labeling
- Autolabeling for credentials and contextual conditions
- Turn on DLP for content that is not labeled
- Turn on Adaptive Protection and data leak behavioral rules

Outcomes

- M365 priority content protected

Efforts

- 2 weeks

Optimized

Expand to your entire M365 data estate

Activities

- Auto-label sensitive files on clients (low thresholds)
- Simulate auto-labeling sensitive files at rest
- Reduce false positives with advanced classifiers
- Automate and improve M365 protection to historical and in use data

Outcomes

- M365 historical content protected

Efforts

- 2 weeks iteration

Strategic

Operate, expand, and retroactive actions

Activities

- Operational review of user labeling behaviors
- Iterate with new labeling scenarios
- Set up accountability chain and lifecycle management
- Extend protection to Azure SQL and non-M365 storage

Outcomes

- Protection beyond M365

Efforts

- Situational

Last updated: August 14, 2024

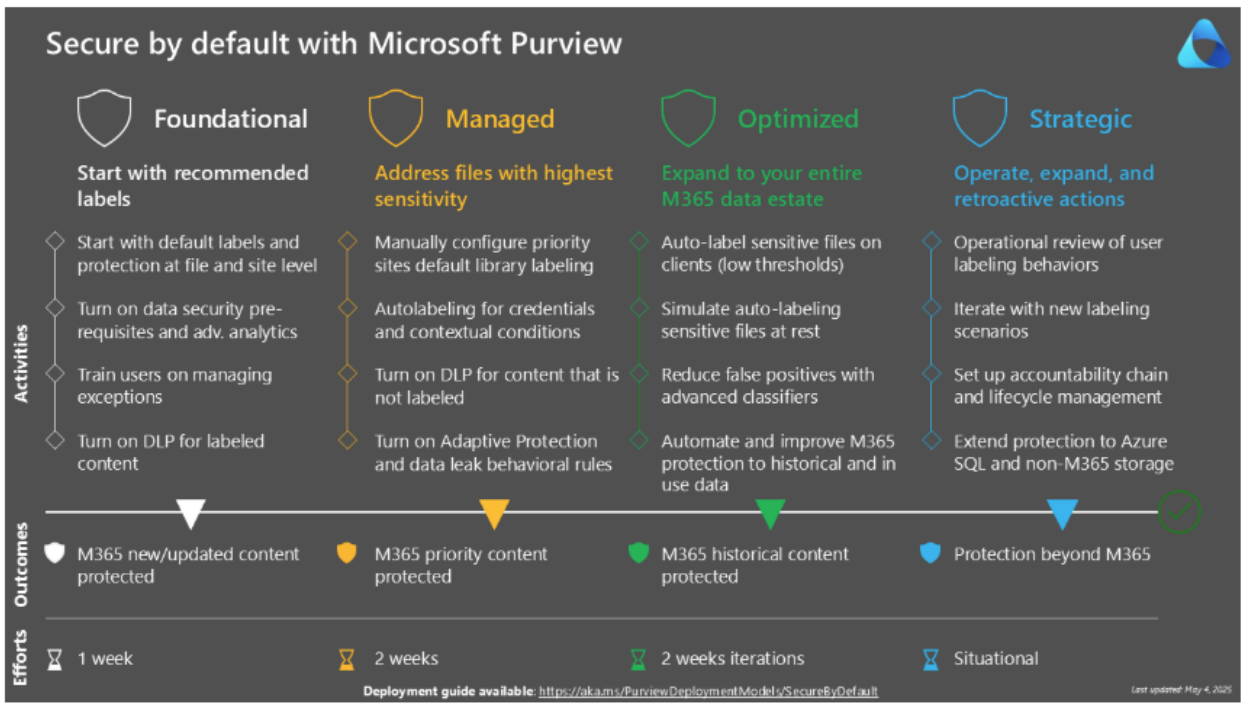
Microsoft Purview deployment blueprint

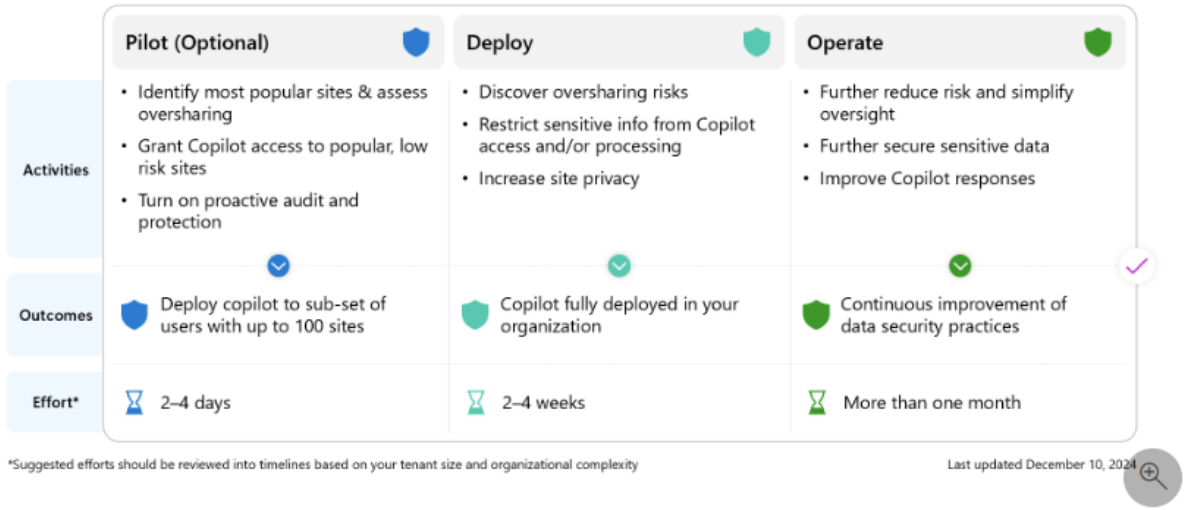
The blueprint provides:

- a recommended label taxonomy to get your organization started
- options for end users to manage exceptions, if encryption prevents them from working effectively
- help to enable your organization to augment its data security rapidly

It's important to review and adapt this blueprint based on your existing deployment, data security objectives, and experience. There are more options to help you deploy in stages. You're in complete control of your deployment experience.

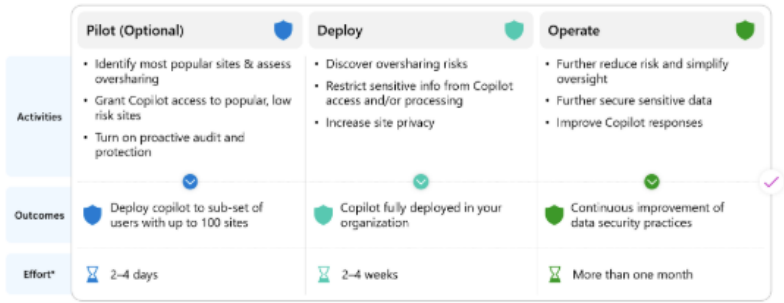
> **Note**
>
> This blueprint is closely aligned with Microsoft's internal strategy. Learn more about Microsoft labeling deployment at: How we're using sensitivity labels to make Microsoft more secure





Download the blueprint and documentation

Expand table

Deployment model	Description
	Use this deployment model to assist organizations in identifying and mitigating oversharing risks. **This model includes** • Blueprint with high level activities and presentation PDF | PowerPoint

Published Feb 5, 2020 • 8 min read

Advancing safe deployment practices

By Mark Russinovich, Chief Technology Officer, Deputy Chief Information Security Officer, and Technical Fellow, Microsoft Azure

SHARE

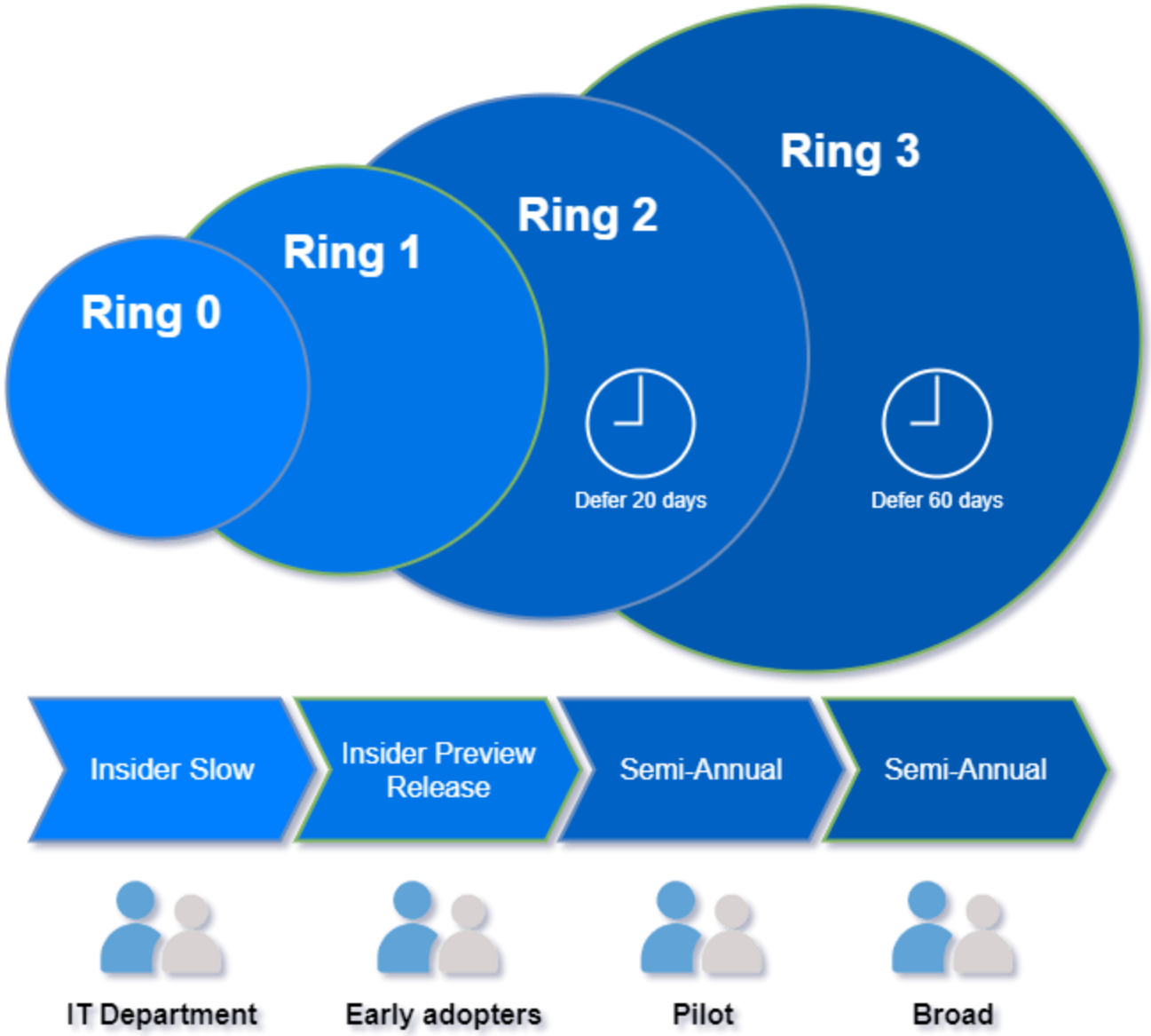
AUDIENCE

Business decision makers

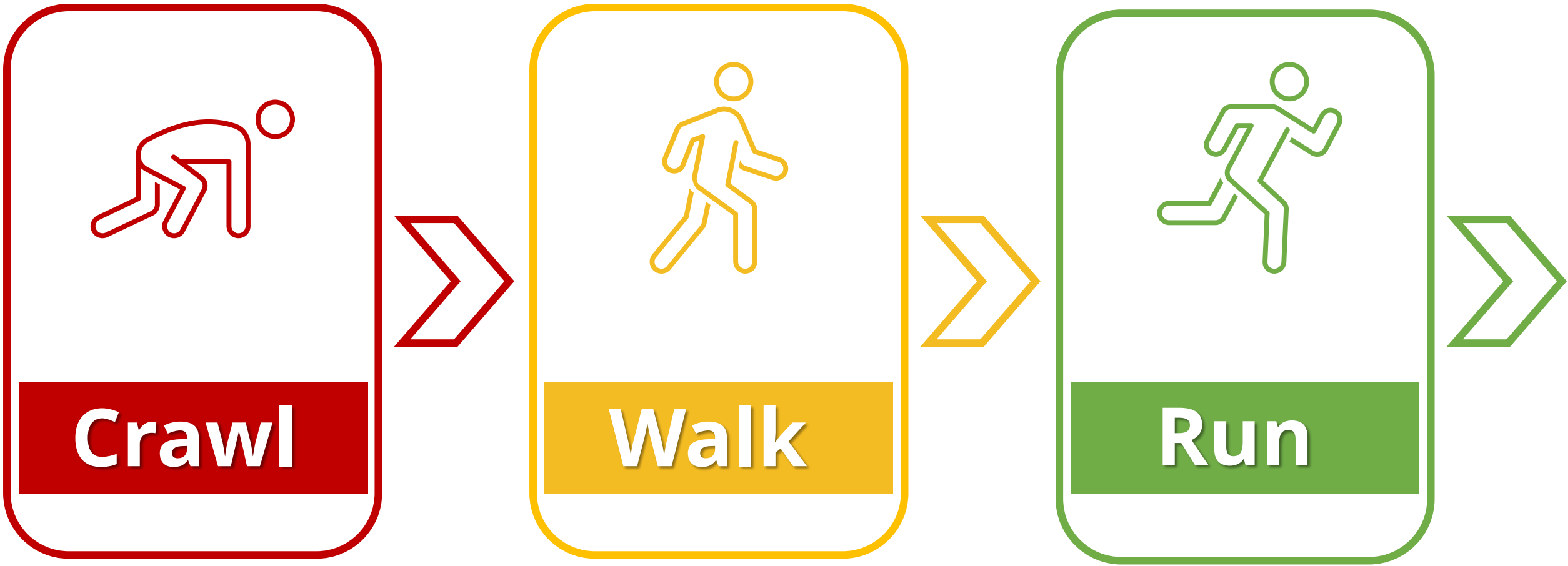
IT decision makers

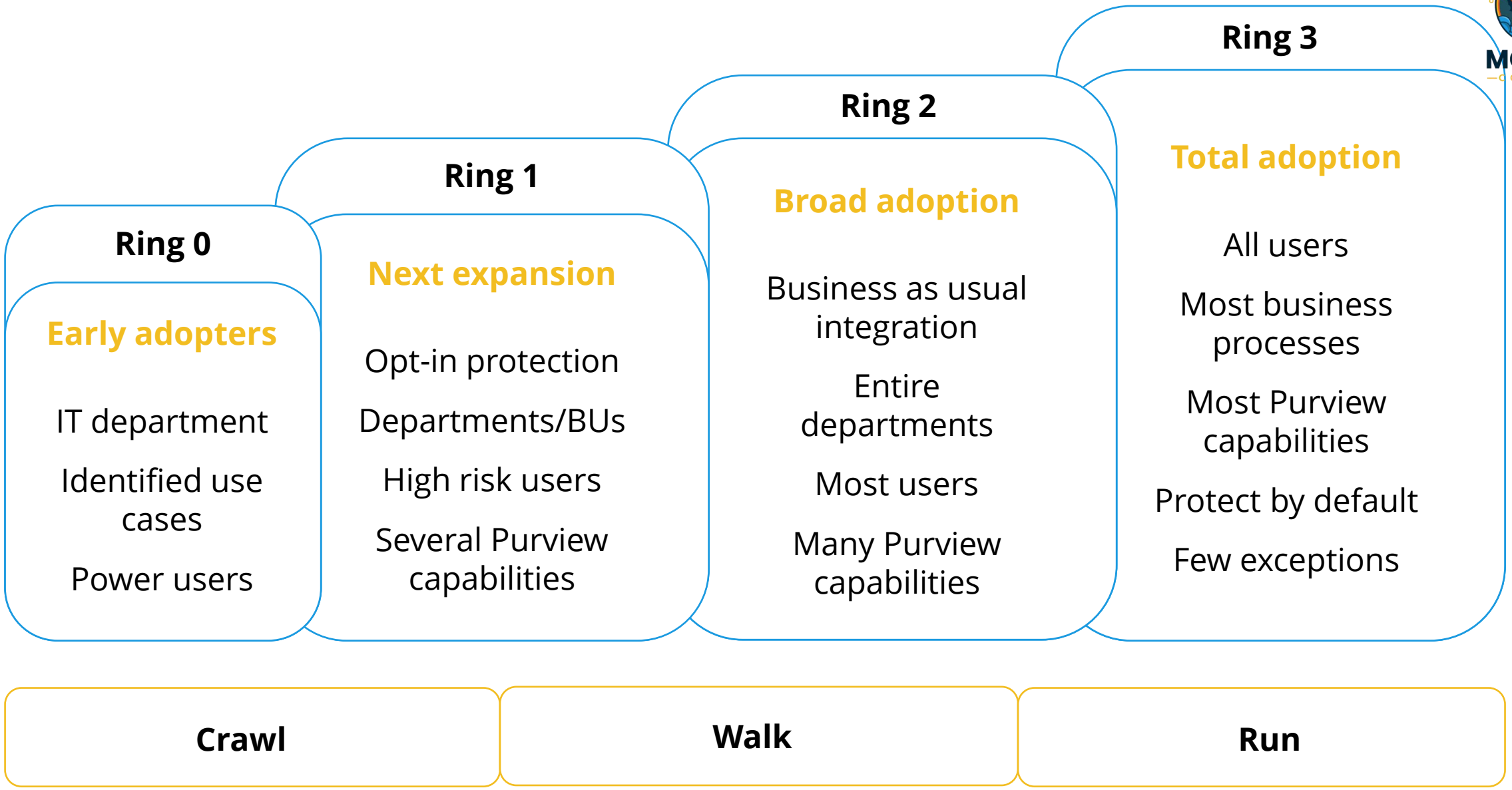
more

"What is the primary cause of service reliability issues that we see in Azure, other than small but common hardware failures? Change. One of the value propositions of the cloud is that it's continually improving, delivering new capabilities and features, as well as security and reliability enhancements. But since the platform is continuously evolving, change is inevitable. This requires a very different approach to ensuring quality and stability than the box product or traditional IT approaches — which is to test for long periods of time, and once something is deployed, to avoid changes. This post is the fifth in the series I kicked off in my July blog post that shares insights into what we're doing to ensure that Azure's reliability supports your most mission critical workloads. Today we'll describe our **safe deployment practices**, which is how we manage change automation so that all code and configuration updates go through well-defined stages to catch regressions and bugs before they reach customers, or if they do make it past the early stages, impact the smallest number possible. **Cristina del Amo Casado** from our Compute engineering team authored this posts, as she has been driving our safe deployment


Ring 0
Ring 1
Ring 2
Ring 3
Defer 20 days
Defer 60 days
Insider Slow
Insider Preview Release
Semi-Annual
Semi-Annual
IT Department
Early adopters
Pilot
Broad

Microsoft Purview




Ring 0
Early adopters
IT department
Identified use cases
Power users
Ring 1
Next expansion
Opt-in protection
Departments/BUs
High risk users
Several Purview capabilities
Ring 2
Broad adoption
Business as usual integration
Entire departments
Most users
Many Purview capabilities
Ring 3
Total adoption
All users
Most business processes
Most Purview capabilities
Protect by default
Few exceptions
Crawl
Walk
Run

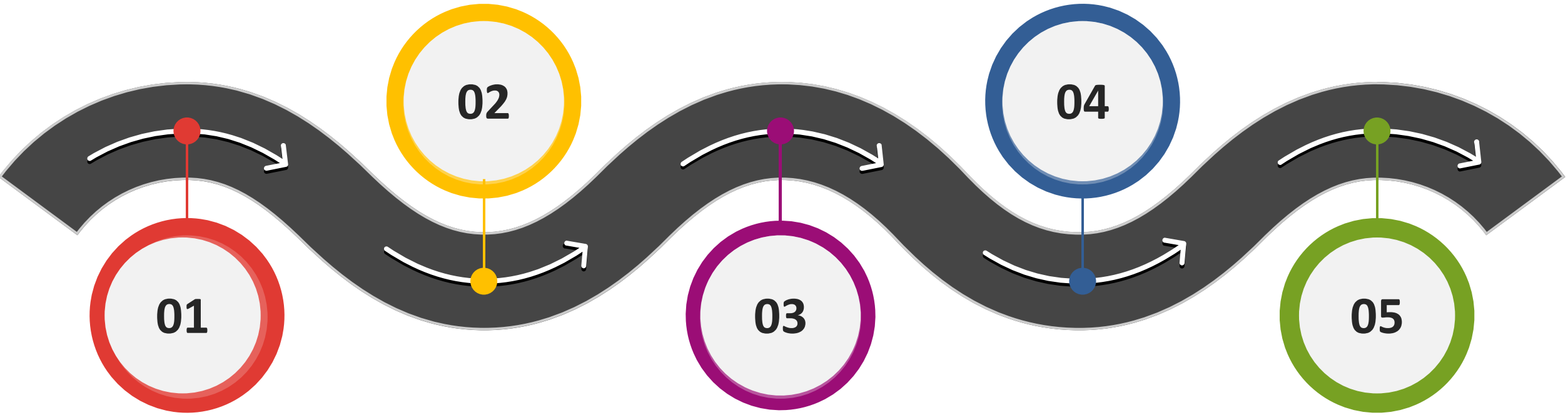
Summary

- ✓ Start with the people, not the portal
- ✓ Know the capabilities
- ✓ Win business buy-in
- ✓ Purview is not set it & forget it so have a dedicated resource managing it
- ✓ Safe deployment practices (SDP)

Conclusions

- Microsoft Purview is not plug and play
- Microsoft Purview is only as good as your planning, deployment, and tuning
- Progress, not perfection
- Start with prerequisites, right licensing, pilot/ audit mode
- Continuous monitoring & adjustment is key

Road Map for Microsoft Purview implementation



Audit

Audit all activities

Information Protection

Data discovery, data classification, sensitivity labels

Data Loss Prevention

Prevent data loss

Insider Risk Management

Stop data leaks and data theft

Data Lifecycle Management

Manage stale data

We would love your feedback!

Session feedback available in home feed of the app after the session

Q & A

MC2MC

CONNECT

Thank you

MC2MC

CONNECT