

Ewelina Paczkowska

# BUILDING EFFECTIVE DATA LOSS PREVENTION POLICIES WITH MICROSOFT PURVIEW

## WELKA'S WORLD



# WHO AM I?

**NAME:** Ewelina Paczkowska

**NICKNAME:** Welka

**LOCATION:**  

**JOB:** Solution Architect at Threatscape

**UG:** M365 Security & Compliance

*(meetup.com/m365sandcug)*

BLOG

[www.welkasworld.com](http://www.welkasworld.com)

in

@ewelinapaczkowska

X

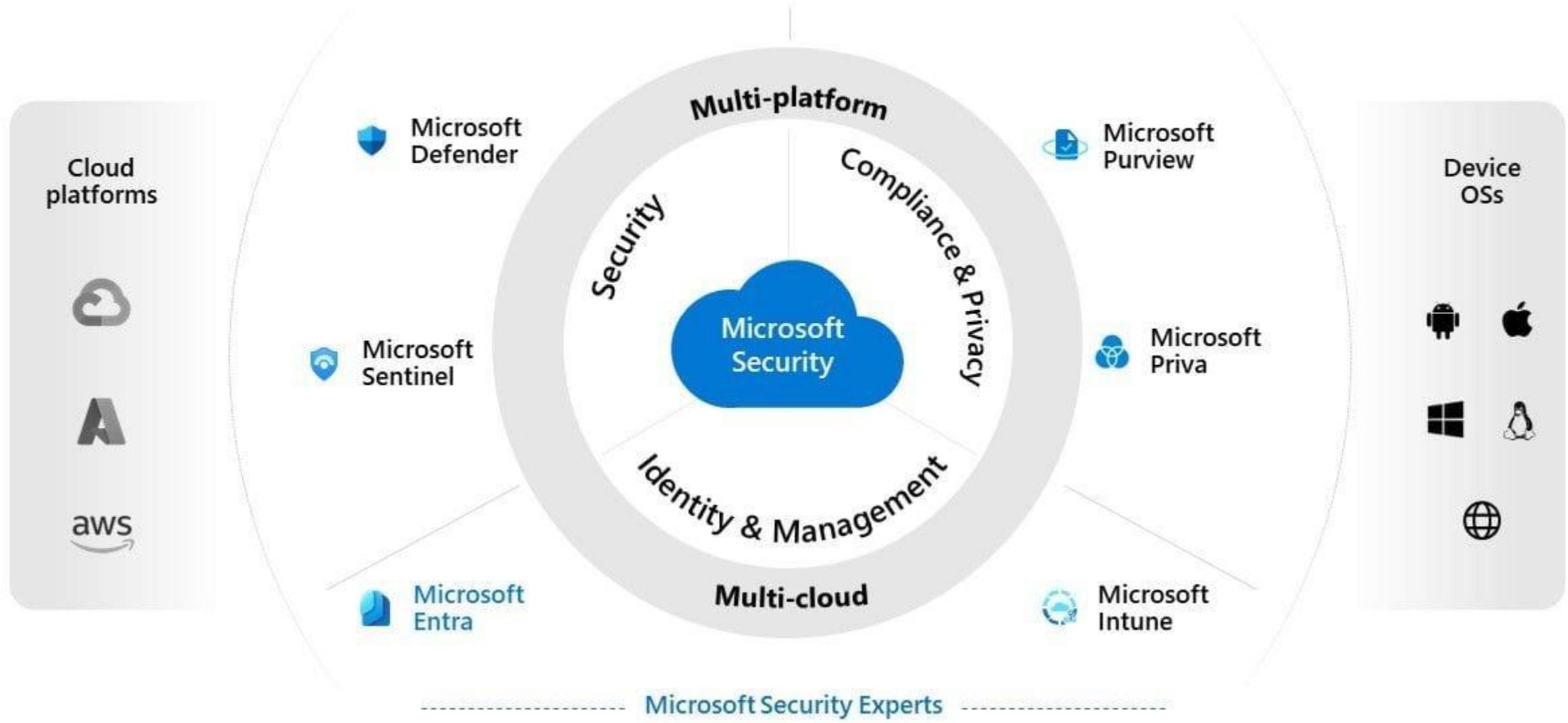
@WelkasWorld



# AGENDA

- Microsoft Security portfolio overview
- Microsoft Purview introduction
- Data Loss Prevention (DLP) deep dive
- Demos
- Best practices & common mistakes
- Conclusions and Q&A

# Microsoft Security Product Portfolio



# Portfolio

Platform

Compliance & F



Device  
OSs

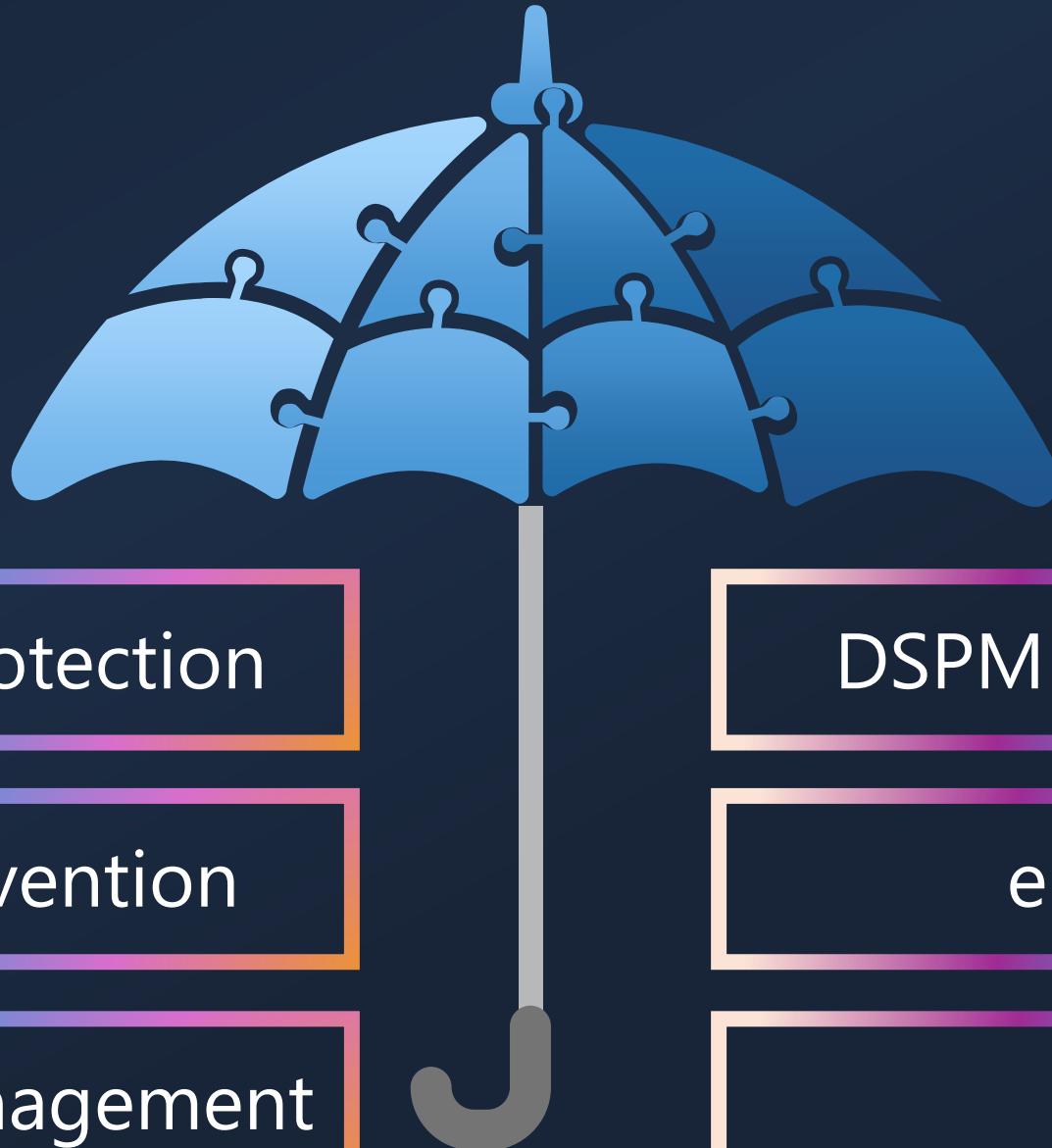
# MICROSOFT PURVIEW

**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





Information Protection

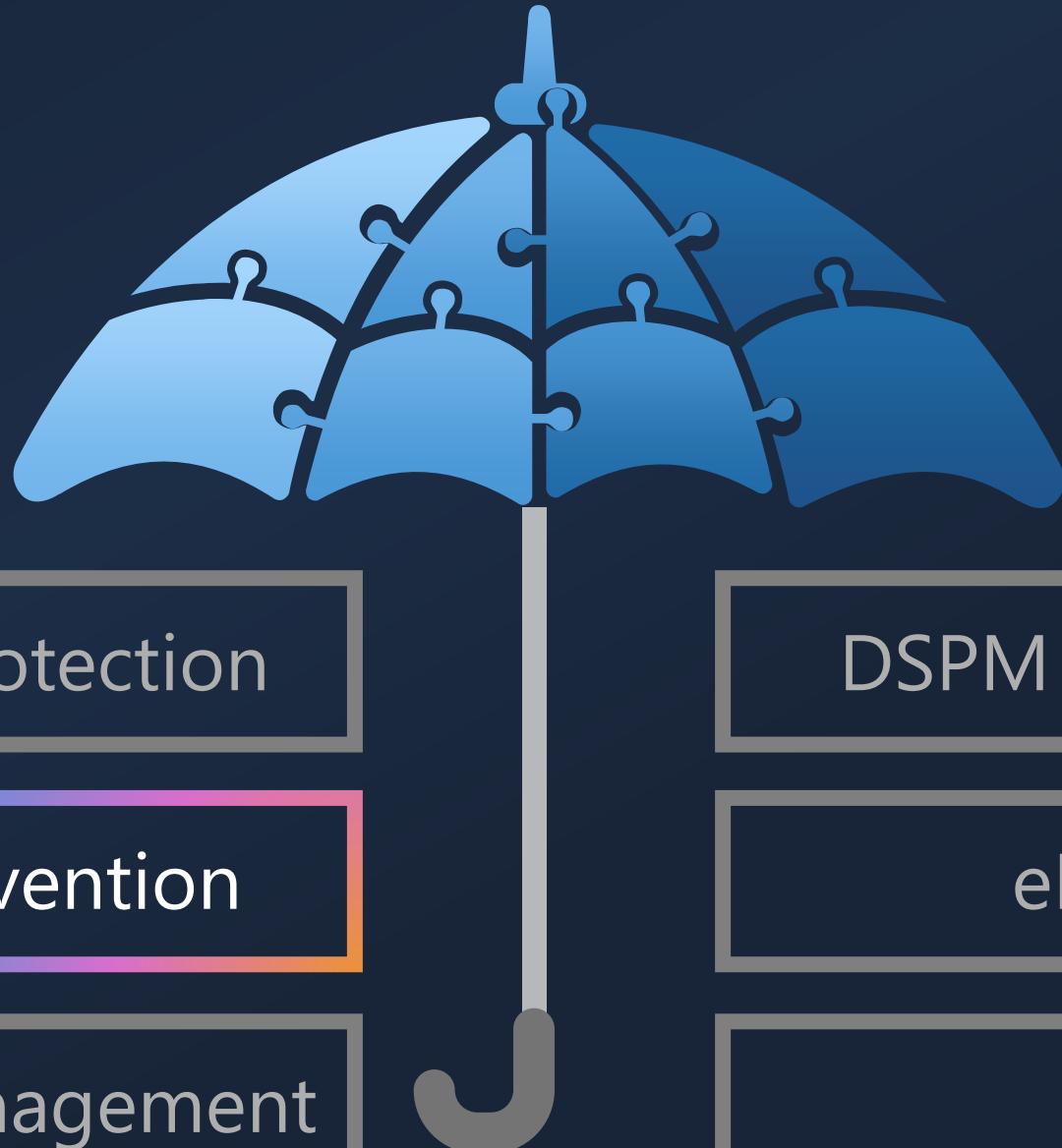
Data Loss Prevention

Insider Risk Management

DSPM & DSPM for AI

eDiscovery

Audit



Information Protection

Data Loss Prevention

Insider Risk Management

DSPM & DSPM for AI

eDiscovery

Audit

# Data Loss Prevention

# DATA LOSS PREVENTION

**Data Loss Prevention (DLP)** is a technology within Microsoft Purview that identifies, monitors, and protects sensitive data from being shared or leaked outside an organization without permission.



# WHY DLP MATTERS?

- Protects sensitive data in emails, Teams, endpoints, and cloud apps
- Shields you from leaks, fines, and insider threats
- Helps meet GDPR, HIPAA, PCI-DSS compliance



# HOW DLP WORKS

- **Detection:** Sensitive info types, trainable classifiers, EDMs, sensitivity labels
- **Enforcement:** audit, warn (block with override), block
- **Coverage:** Exchange, SharePoint, OneDrive, Teams, Endpoints (device + browser), Cloud Apps, Copilot, Fabric, On-prem



# Data Loss Prevention

## Licensing

# DLP LICENSING

- **Business Premium/ Microsoft 365 E3 (or equivalent)** - Core DLP for Exchange, SharePoint, OneDrive
- **Microsoft 365 E5 (or equivalent)** - includes Endpoint DLP, DLP for Teams, MDA integration
- **Other equivalents / add-on SKUs**, e.g. Compliance add-ons (Purview suite), may provide parts of features

**1** E5 Compliance value shown. Includes additional va

Microsoft 365 Compliance Licensing Comparison

©2020 Microsoft Corporation. All rights reserved. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. This document." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. This document does not provide you with any legal rights to any intellectual property product. Some information relates to pre-released product which may be substantially modified before it's commercially released.

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 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. Microsoft 365 E3 features), which must be licensed separately.

Solution	Feature	<input checked="" type="checkbox"/> (See footnote <a href="#">1</a> regarding blank cells in this column)	Microsoft 365 E5 Compliance <sup>2</sup>	Microsoft 365 E5/A5 Info Protection & Governance <sup>3</sup>	Microsoft 365 E5 Insider Risk Management <sup>4</sup>	Microsoft 365 eDiscovery
Key Management	<a href="#">Customer Key for Office 365</a>	●	●			
	<a href="#">Bring Your Own Key (BYOK) for customer-managed key provisioning life cycle<sup>13</sup></a>	●	●			
	<a href="#">Hold Your Own Key (HYOK) that spans Azure Information Protection and Active Directory (AD) Rights Management for highly regulated scenarios</a>	●	●			
	<a href="#">Endpoint DLP</a>	●		●		
Insider Risk Management	<a href="#">Insider Risk Management</a>	●			●	
	<a href="#">Communication Compliance (incl. Supervision policies)</a>	●			●	
	<a href="#">Information Barriers</a>	●			●	
	<a href="#">Customer Lockbox</a>	●			●	
	<a href="#">Privileged Access Management</a>	●			●	
Discover & Respond	<a href="#">Content Search</a>					
	<a href="#">Core eDiscovery (incl. Hold and Export)</a>					
	<a href="#">Advanced eDiscovery</a>	●				
	<a href="#">Custodian management (mapping content to custodian)</a>	●				
	<a href="#">Custodian communications</a>	●				
	<a href="#">Deep crawling/indexing</a>	●				
	<a href="#">Review data (query data, tags, smart tags, dashboard) and annotate (redact)</a>	●				

# Data Loss Prevention

## Prerequisites



# PREREQUISITES

- Onboard your devices to Microsoft Purview (via Microsoft Defender for Endpoint)
- Deploy Microsoft Purview browser extension for non-native browsers (Chrome, Firefox, etc.)
- Install Microsoft Purview Information Protection On-premises Scanner for file servers/SharePoint Server
- Integrate with Defender for Cloud Apps (optional)

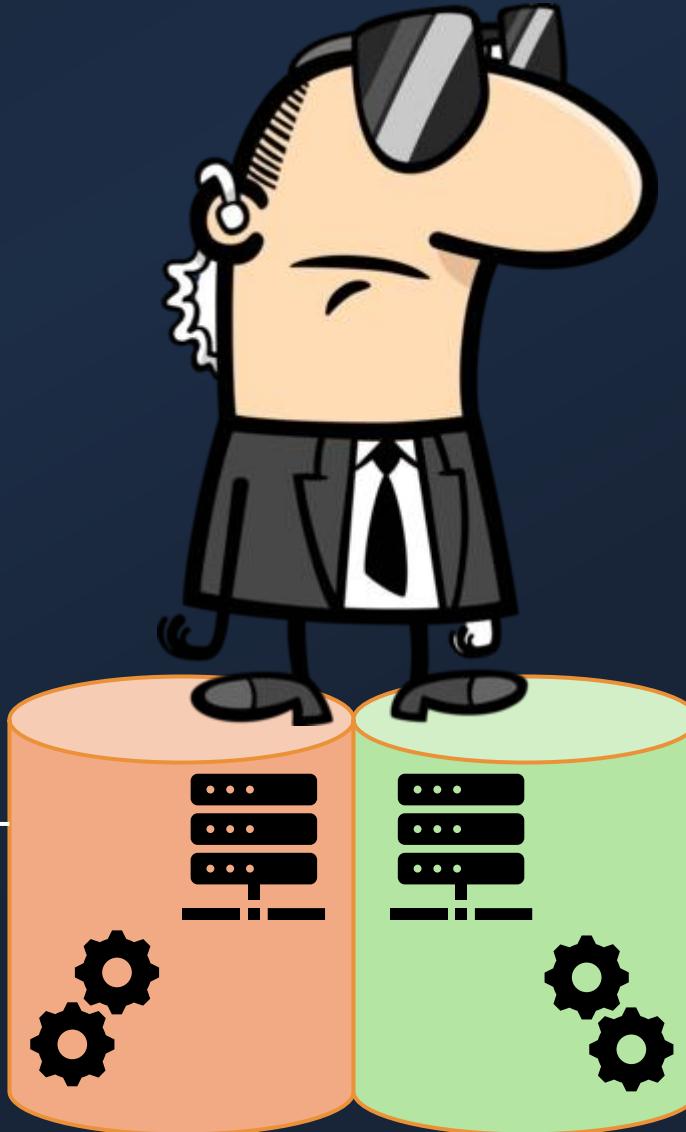
# Data Loss Prevention

## Device onboarding

# MDE/ Purview onboarding

1 AGENT

2 SERVICES



MDE (anti-malware  
protection)

DLP/IRM (DLP  
protection)

- [!\[\]\(2488868bbf8d1ed0fe423a2a454e7f41\_img.jpg\) Home](#)
- [!\[\]\(72830f677403653777b92f3d415cb189\_img.jpg\) Solutions](#)
- [!\[\]\(f5620ad1f0b83a47248ce0e4564f16d1\_img.jpg\) Agents](#)
- [!\[\]\(9ab676b7c21b5d301aba823950f7128e\_img.jpg\) Learn](#)
- [!\[\]\(c5da13620c9e780fd8e01562585c283a\_img.jpg\) Settings](#)
- [!\[\]\(11db8983fb3598ca1a71f8e0b4aba3fe\_img.jpg\) Data Loss Prevention](#)
- [!\[\]\(83e3b0f858286941d49c35def071742c\_img.jpg\) Information Protection](#)
- [!\[\]\(52246e3267bae2bf359bb668cbd4d49e\_img.jpg\) Device onboarding](#)
- [!\[\]\(68addc2288f303e6a8a2cf7ae1092993\_img.jpg\) Devices](#)
- [!\[\]\(68d5a403957a539116af527c327e1735\_img.jpg\) Onboarding](#)
- [!\[\]\(d4de1faff8fb26e640acc4ca6493d912\_img.jpg\) Offboarding](#)
- [!\[\]\(1ac262b2e9eed26c286e8a9709746368\_img.jpg\) Optical character recognition \(OCR\)](#)
- [!\[\]\(d66de2025d2b86130a0d1141f9976ba8\_img.jpg\) Solution settings](#)
- [!\[\]\(5ef0ab68a0dbcfe70621f0ed38669d1c\_img.jpg\) Communication](#)
- [!\[\]\(7fc40e753dddee72245d1fb38e042804\_img.jpg\) Compliance](#)
- [!\[\]\(751074dfa6ae4e6f04776a1cd444bae2\_img.jpg\) Compliance Manager](#)
- [!\[\]\(b2ea189526089337533d196396a159d2\_img.jpg\) Data Catalog](#)
- [!\[\]\(1189f1d6f491e1f6030d78cc9b514717\_img.jpg\) Data Lifecycle Management](#)
- [!\[\]\(5941928ff6b11a8427bba7052ded6269\_img.jpg\) Data Loss Prevention](#)
- [!\[\]\(e5aea5fbaf5cb4630f3d7f971f40471f\_img.jpg\) eDiscovery](#)

# Onboarding

Select operating system to start onboarding process:

Windows 10

To onboard devices to the compliance center, choose your preferred deployment method, download the related configuration package, and follow the guidance in the articles provided for each method.

Deployment method

Local script (for up to 10 machines)

Local script (for up to 10 machines)

Group Policy

Microsoft Endpoint Configuration Manager

Mobile Device Management / Microsoft

Intune

VDI onboarding scripts for non-persistent devices

o 10 devices. If you want to onboard more than that, choose a different deployment method.  
[a local script](#)

devices to Microsoft Defender for Endpoint, the instructions are the same for onboarding to the

## Endpoints

## Email &amp; collaboration

## Cloud apps

## SOC optimization

## Reports

## Learning hub

## Trials

## More resources

## System

## Audit

## Data management

## Permissions

## Health

## Settings

## Customize navigation

Settings &gt; Endpoints

## Endpoints

## General

## Advanced features

Licenses

Email notifications

Auto remediation

## Permissions

Roles

Device groups

## Rules

Alert suppression

Indicators

Isolation exclusion rules

with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.

**Microsoft Intune connection**

Connects to Microsoft Intune to enable sharing of device information and enhanced policy enforcement.

Intune provides additional information about managed devices for secure score. It can use risk information to enforce [conditional access](#) and other security policies.

**Authenticated telemetry**

Keep authenticated telemetry turned on to prevent spoofing telemetry into your dashboard

**Preview features**

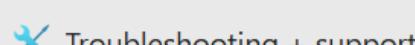
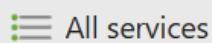
Allow access to preview features. Turn on to be among the first to try upcoming features.

**Save preferences**

&lt;

[Home](#) > [Endpoint security | Endpoint detection and response](#) > [EP-MDE\\_Onboarding](#) >

Home



## Edit Policy

...

Endpoint detection and response

[Configuration settings](#)[Review](#) Search settings by setting name (i)

### Microsoft Defender for Endpoint



Microsoft Defender for  
Endpoint client  
configuration package  
type

 Configured

.....

Onboarding blob from  
Connector



Sample Sharing



Not configured



[Deprecated] Telemetry  
Reporting Frequency



Not configured

[Next](#)

## Settings

[Account](#)[Roles and scopes](#)[Data connectors](#)[Device onboarding](#)[Devices](#)[Onboarding](#)[Offboarding](#)[Optical character  
recognition \(OCR\)](#)

### Solution settings

[Communication  
Compliance](#)[Compliance Manager](#)[Data Catalog](#)[Data Lifecycle  
Management](#)[Data Loss Prevention](#)[eDiscovery](#)[Information Protection](#)[Insider Risk Management](#)

# Devices

No devices onboarded yet

To onboard devices for use in compliance solutions, you first need to turn on device onboarding.

[Turn on device onboarding](#)

**Settings**

Account

 Roles and scopes ▼ Data connectors ▼ Device onboarding ^ **Devices**

Onboarding

Offboarding

 Optical character  
recognition (OCR)**Solution settings** Communication  
Compliance

Compliance Manager

Data Catalog

 Data Lifecycle  
Management

Data Loss Prevention

eDiscovery

Information Protection

Insider Risk Management

# Devices

**No devices onboarded yet**

To onboard devices for use in compliance solutions, you first need to turn on device onboarding.

[Turn on device onboarding](#)

## Turn on device onboarding



When you turn this on, any devices that already onboarded to Microsoft Defender for Endpoint (MDE) will appear in the device list here.

Regardless of whether you already have onboarded devices, you'll be able to onboard new ones from the "Onboarding" page.

[OK](#)[Cancel](#)

# Devices

## Device monitoring is being turned on

This might take awhile, so refresh the page often to check progress.

When it's turned on, any devices that are already onboarded to Microsoft Defender for Endpoint (MDE) will appear in the device list.

If devices weren't already onboarded, you can get started from the "Onboarding" page.

## Settings

### Account

### Roles and scopes

### Data connectors

### Device onboarding

#### Devices

Onboarding

Offboarding

Optical character  
recognition (OCR)

### Solution settings

Communication  
Compliance

Compliance Manager

Data Catalog

Data Lifecycle  
Management

Data Loss Prevention

eDiscovery

Information Protection

Insider Risk Management

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Settings

DSPM for AI

Data Loss Prevention

Devices

Onboarding

Offboarding

Optical character recognition (OCR)

Solution settings

Communication Compliance

Compliance Manager

Data Catalog

Data Lifecycle Management

# Devices

Activity from these onboarded devices can be reviewed in features such as activity explorer or monitored by compliance solutions such as insider risk management and data loss prevention (DLP). [Learn more](#)

Export Turn off Windows device monitoring Turn off macOS device monitoring

Search

Filter Reset Filters

Days look back: 30 Configuration status: Any Policy sync status: Any OS: Any OS version: Any +2 more

Device name	Configuration status	Policy sync status	Last seen	OS
ep-win-11	✓ Updated	✓ Updated	Oct 27, 2025 6:28 PM	Windows11

# Devices

Activity from these onboarded devices can be reviewed in features such as activity explorer or monitoring prevention (DLP). [Learn more](#)

[Export](#)[Turn off Windows device monitoring](#)[Turn off macOS device monitoring](#)[Filter](#) [Reset](#) Days look back: **30**Configuration status: **Any**Policy sync status: **Any**OS: **Any**

Device name

Configuration status

Policy sync status

ep-win-11

Updated

Updated

**ep-win-11**

Configuration updated

DLP policy sync updated

## Configuration status

### Real time protection/RTP

Enabled

### Behavior monitoring/BM

Enabled

## DLP policy sync details

Policy updates can take up to 2 hours to reflect on this dashboard, and the device must be online for the update to happen. Check the device's last seen time before updating. Also, note that all policies sync across all devices, but will only be enforced for users assigned to them upon logging in to those devices.

[View all policies on this device](#)

## Device details

Need to collect device logs to help address support cases? Learn how to collect logs for [Windows](#) or [MacOS](#) devices

Need to verify if your policy synced to the device? Learn how to verify for policy sync or correct file classification for [Windows](#) or [MacOS](#) devices

### Last seen

Oct 27, 2025 6:28 PM

### OS

Windows11 x64  
Release 23H2 Build 22631.4890

### Antimalware Engine Version

1.1.25090.3001

### Antimalware Client Version

4.18.25090.3009

### Endpoint DLP status

Enabled

### MDATP device ID

aabf98b3033fce859fdd1822ceba8c924031efc

# Data Loss Prevention

Microsoft Purview Information  
Protection scanner (on-prem)



Home



Roles and scopes



Solutions

Data connectors



Agents

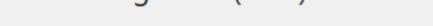
Device onboarding



Learn

Optical character recognition (OCR)

recognition (OCR)



Settings

Solution settings

Communication Compliance

Compliance Manager

Data Catalog



Data Loss

Prevention

Data Lifecycle Management



Information

Protection

Protection

Data Loss Prevention

eDiscovery

Information Protection

Insider Risk Management

Records Management

# Information Protection settings

Co-authoring for files with sensitivity labels

## Information protection scanner

### Information protection scanner

Use the scanner to discover, classify, and protect files stored in network shares and on-premises SharePoint document libraries and folders. [Learn more about the scanner](#)

Clusters Nodes Content scan jobs

⟳ Refresh + Add ⤵ Export

3 items

Search

Name	Cluster name	Schedule	Enforce
H drive	H Shared Drive	Always	Yes
S drive	S Drive Shares	Always	Yes
srv001	srv-001	Always	Yes

# Data Loss Prevention

Microsoft Purview browser  
extension

# Windows | Configuration

[Windows devices](#)[Monitor](#)[Device onboarding](#)[Windows 365](#)[Enrollment](#)[Manage devices](#)[Configuration](#)[Compliance](#)[Scripts and remediations](#)[Group Policy analytics](#)[eSIM cellular profiles  
\(preview\)](#)[Manage updates](#)[Windows updates](#)[Organize devices](#)

## Policies Import ADMX

[Create](#)[Refresh](#)[Export](#)[Columns](#)

4 policies

[Search](#)[Add filters](#)

### Policy name

### Platform

### Policy type

[Win-Firefox-MSPurviewBrowserExt](#)

Windows 10 and later

Custom

[Win-GoogleChrome-MSPurviewBrowserExt](#)

Windows 10 and later

Settings catalog

[Win-MSEdge-MSPurviewBrowserExt](#)

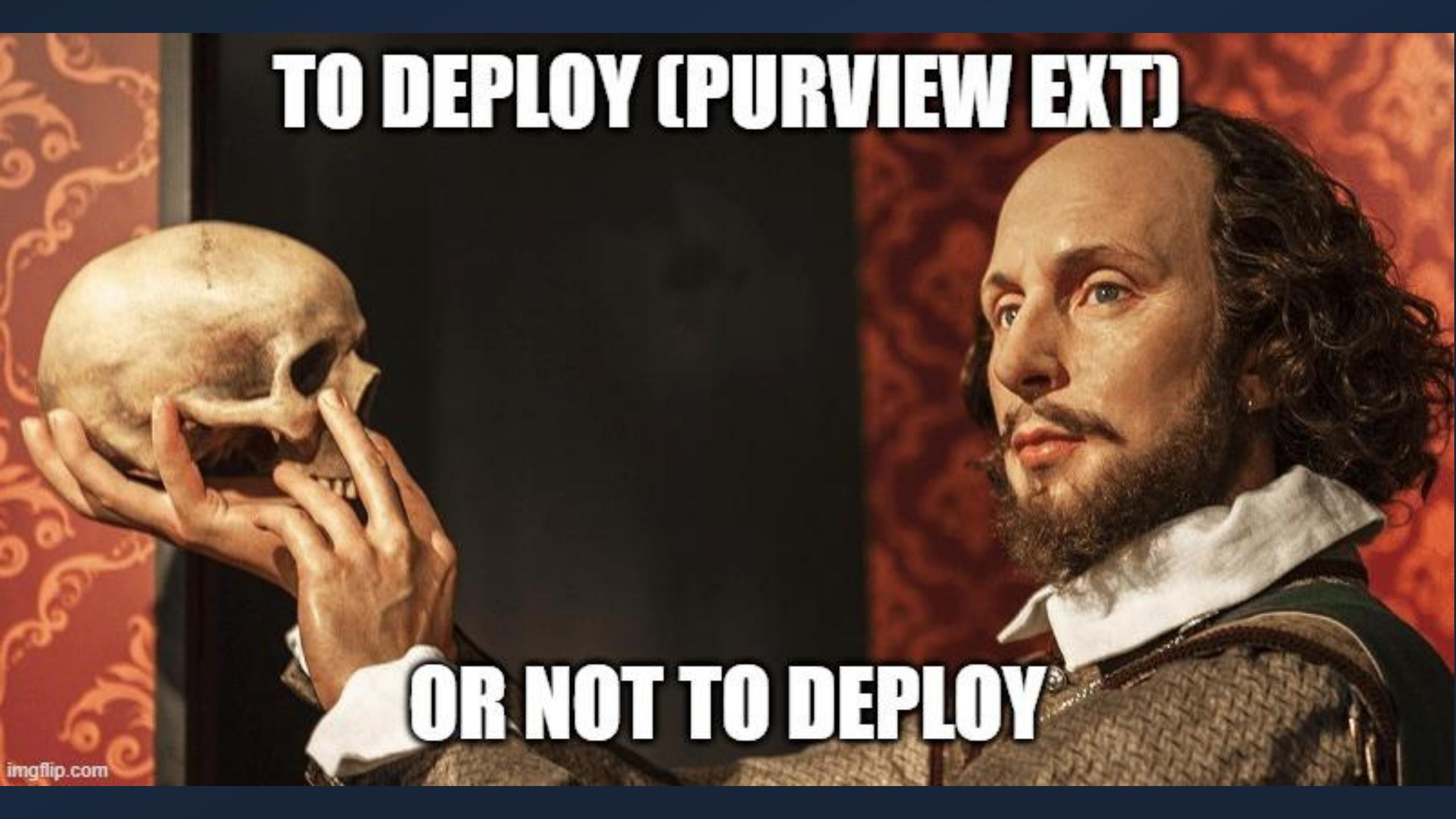
Windows 10 and later

Settings catalog

[Win10-DeviceConfig-Restrictions](#)

Windows 10 and later

Device restrictions

A painting of William Shakespeare in Elizabethan attire, holding a human skull. He is looking thoughtfully at the skull with his right hand. The background is dark, and there is a red patterned curtain on the left.

**TO DEPLOY (PURVIEW EKT)**

**OR NOT TO DEPLOY**

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

# Data Loss Prevention

Other prerequisites (optional)



## 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
<input type="checkbox"/> Company Credit Card Number	All	Entity	Contoso
<input type="checkbox"/> Mark 8 Project	All	Entity	Contoso
<input type="checkbox"/> Top Secret	All	Entity	Contoso
<input type="checkbox"/> Project Olivine	All	Entity	Contoso
<input type="checkbox"/> Proseware Merger	All	Entity	Contoso
<input type="checkbox"/> Project Obsidian	All	Entity	Contoso
<input type="checkbox"/> Contoso Employee Onboarding	All	Fingerprint	M365DS517923.o...
<input type="checkbox"/> ABA Routing Number	All	Entity	Microsoft Corpor...
<input type="checkbox"/> Argentina National Identity (DNI) Number	All	Entity	Microsoft Corpor...

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Settings

Data Loss Prevention

Information Protection

Sensitivity labels

Overview

Reports

Recommendations

Policies

Classifiers

- Trainable classifiers
- Sensitive info types
- EDM classifiers
- On-demand classification
- Collection policies

Explorers

Diagnostics

Related solutions

- Data Security Investigations (preview)
- Data Lifecycle Management
- Data Loss Prevention

## Sensitivity labels

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

*(i) Migrate to the modern label scheme. Start the migration process now to take advantage of a simplified label scheme. This new scheme replaces parent labels with 'label groups', allowing you to better organize labels by reducing them to just standalone labels and sublabels within a group. [Learn more about the modern label scheme](#)*

[Get started](#)

+ Create a label    Publish labels    Export    Refresh

8 items

	Name	Priority	Scope	Created by	Last modified
<input type="checkbox"/>	Project Obsidian	0	Files & other data assets, E...	MOD Administrator	Sep 19, 2025 1:25:11 PM
<input type="checkbox"/>	Proseware Merger	1	Files & other data assets, E...	MOD Administrator	Sep 19, 2025 1:25:12 PM
<input type="checkbox"/>	Personal	2	Files & other data assets, E...	Microsoft Corpor...	Sep 19, 2025 8:05:35 PM
<input type="checkbox"/>	Public	3	Files & other data assets, E...	Microsoft Corpor...	Sep 19, 2025 8:05:39 PM
<input type="checkbox"/>	General	4	Files & other data assets, E...	Microsoft Corpor...	Sep 19, 2025 8:05:45 PM
<input type="checkbox"/>	Confidential	7	Files & other data assets, E...	Microsoft Corpor...	Sep 19, 2025 8:05:56 PM
<input type="checkbox"/>	Highly Confidential	11	Files & other data assets, E...	Microsoft Corpor...	Sep 19, 2025 8:06:12 PM
<input type="checkbox"/>	Top Secret	16	Files & other data assets	MOD Administrator	Oct 26, 2025 7:18:31 PM

The screenshot shows the Microsoft Purview Information Protection interface. The 'Sensitivity labels' section is highlighted with a red box. The table lists eight sensitivity labels: Project Obsidian (Priority 0), Proseware Merger (Priority 1), Personal (Priority 2), Public (Priority 3), General (Priority 4), Confidential (Priority 7), Highly Confidential (Priority 11), and Top Secret (Priority 16). The 'General', 'Confidential', 'Highly Confidential', and 'Top Secret' labels are grouped under a parent label, indicated by a greater-than symbol (>) before their names.

Home

Solutions

Agents

Learn

Settings

Data Loss Prevention

Information Protection

≡

## 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](#)

# Data Loss Prevention settings

## Endpoint DLP settings

[Email templates](#)[Analytics](#)[Just-in-time protection](#)[Always-on diagnostics \(preview\)](#)[Power Automate](#)[Aggregate DLP alerts by user](#)[Integrations](#)

## Endpoint DLP settings

These settings apply to all existing and new DLP policies that protect content on endpoint Windows and Mac devices. [Learn more about these settings](#)

Support for some of these settings differs between Windows and Mac devices. [Learn about the differences](#)

## Advanced classification scanning and protection

## Advanced label-based protection for all files on devices

## File path exclusions for Windows

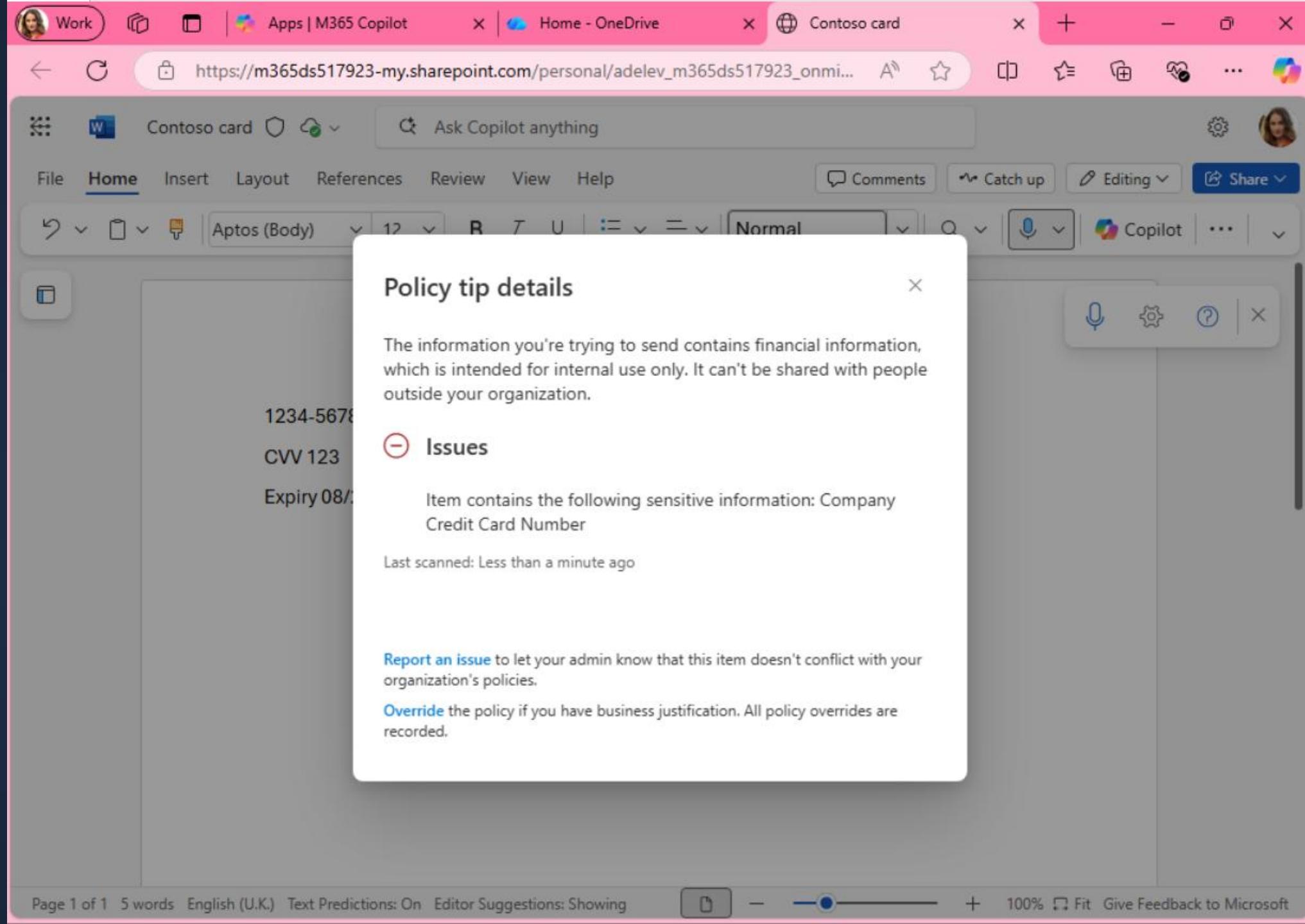
## File path exclusions for Mac

## Setup evidence collection for file activities on devices



# DEMO 1: Setting Up a Purview DLP Policy & End-User Experience

- Goal: Create a DLP policy for sensitive data (e.g. credit card numbers / PII)
- Steps to show:
  - Select locations (Exchange, SharePoint, OneDrive, Teams, Endpoint)
  - Choose sensitive info types or custom classifier
  - Define restrictions (block, warn, audit) and policy tips / notifications
  - Enforce policy, test in simulation mode first
- End user experience: what happens when a user triggers a policy tip, block, or override



Work Apps | M365 Copilot Home - OneDrive Contoso card

https://m365ds517923-my.sharepoint.com/personal/adelev\_m365ds517923\_onmi...

Contoso card Ask Copilot anything

File Home Insert Layout Refe

Aptos (Body)

Policy tip details

The information you're trying to send contains financial information, which is intended for internal use only. It can't be shared with people outside your organization.

**- Issues**

Item contains the following sensitive information: Company Credit Card Number

Expiry 08/ Last scanned: About a minute ago

[Report an issue](#) to let your admin know that this item doesn't conflict with your organization's policies.

Override the policy if you have business justification. All policy overrides are recorded.

I have my manager's permission

Submit

Work Apps | M365 Copilot Home - OneDrive Contoso card

https://m365ds517923-my.sharepoint.com/personal/adelev\_m365ds517923\_onmi...

Contoso card Ask Copilot anything

File Home Insert Layout Refe

Aptos (Body)

Policy tip details

The information you're trying to send contains financial information, which is intended for internal use only. It can't be shared with people outside your organization.

Issues

1234-5678  
CVV 123  
Expiry 08/

Item contains the following sensitive information: Company Credit Card Number

Last scanned: About a minute ago

Report an issue to let your admin know that this item doesn't conflict with your organization's policies.

Override the policy if you have business justification. All policy overrides are recorded.

I have my manager's permission

✓ It may take a few minutes to override the policy. Please reopen the file and try sharing again later.

Catch up Editing Share

Copilot

Page 1 of 1 5 words English (U.K.) Text Predictions: On Editor Suggestions: Showing

100% Fit Give Feedback to Microsoft

about:blank



## Data Loss Prevention notification



Contoso Ltd

To: Adele Vance

Reply Reply all Forward

Sun 10/26/2025 2:46 PM

 Required details  
Outlook Item

The information you're trying to send contains the following sensitive information

- **Message is sent to people outside your organization.**
- **Message contains the following sensitive information: Company Credit Card Number**

, which is intended for internal use only.

Please:

- Remove the external recipient(s), or
- override the restriction, only if applicable.

If you believe this is in error, please forward this message to the IT Helpdesk.

---

### IT Diagnostics

Policy Name: DLP-Exchange-AllUsers-SharingFinancialInfo-BlockWithOverride  
Rule Name: Exchange-AllUsers-FinancialInfo-BlockWithOverride-LowVol-EXT

## Data Loss Prevention notification Contoso card



Contoso Ltd

To: Adele Vance



Reply

Reply all

Forward



Sun 10/26/2025 2:52 PM

This message is from a trusted sender.

The information you're trying to send contains the following sensitive information \*\*\*\*, which is intended for internal use only. Please:

- Remove the external recipient(s), or
- override the restriction, only if applicable.

If you believe this is in error, please forward this message to the IT Helpdesk.

### IT Diagnostics

- Policy Name: DLP-OneDrive-AllUsers-SharingFinancialInfo-BlockWithOverride
- Rule Name: OneDrive-AllUsers-FinancialInfo-BlockWithOverride-LowVol-EXT
- Item is shared with people outside your organization
- Item contains the following sensitive information: Company Credit Card Number

Unshare File ▾

Report Issue ^

Report to admin that the file doesn't conflict with your organization's policies

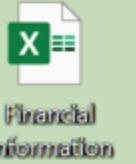
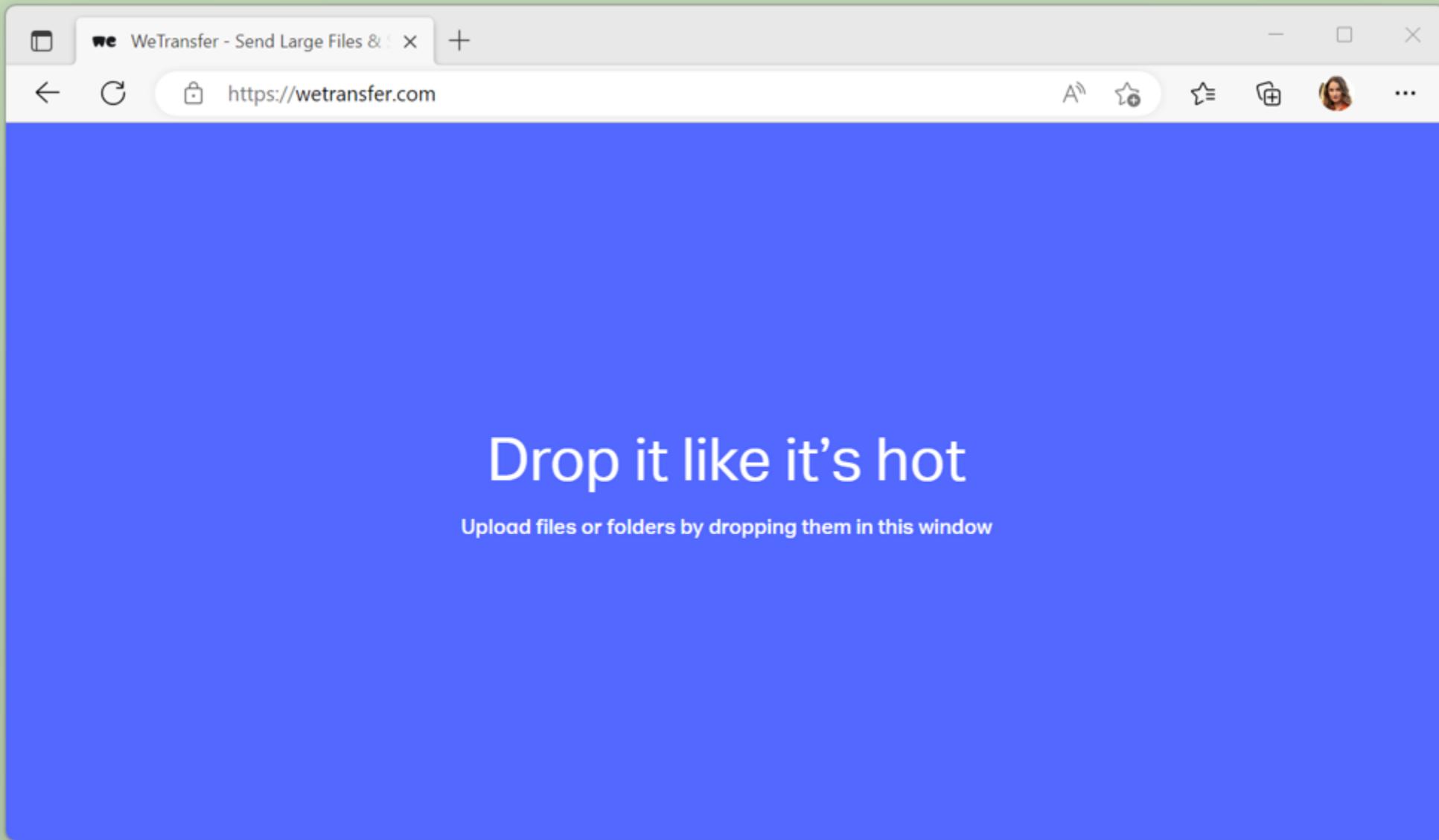
Justification

Confirm

Confirm to report unable to take action



## Recycle Bin



14:07



Recycle Bin

we 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

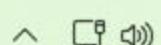
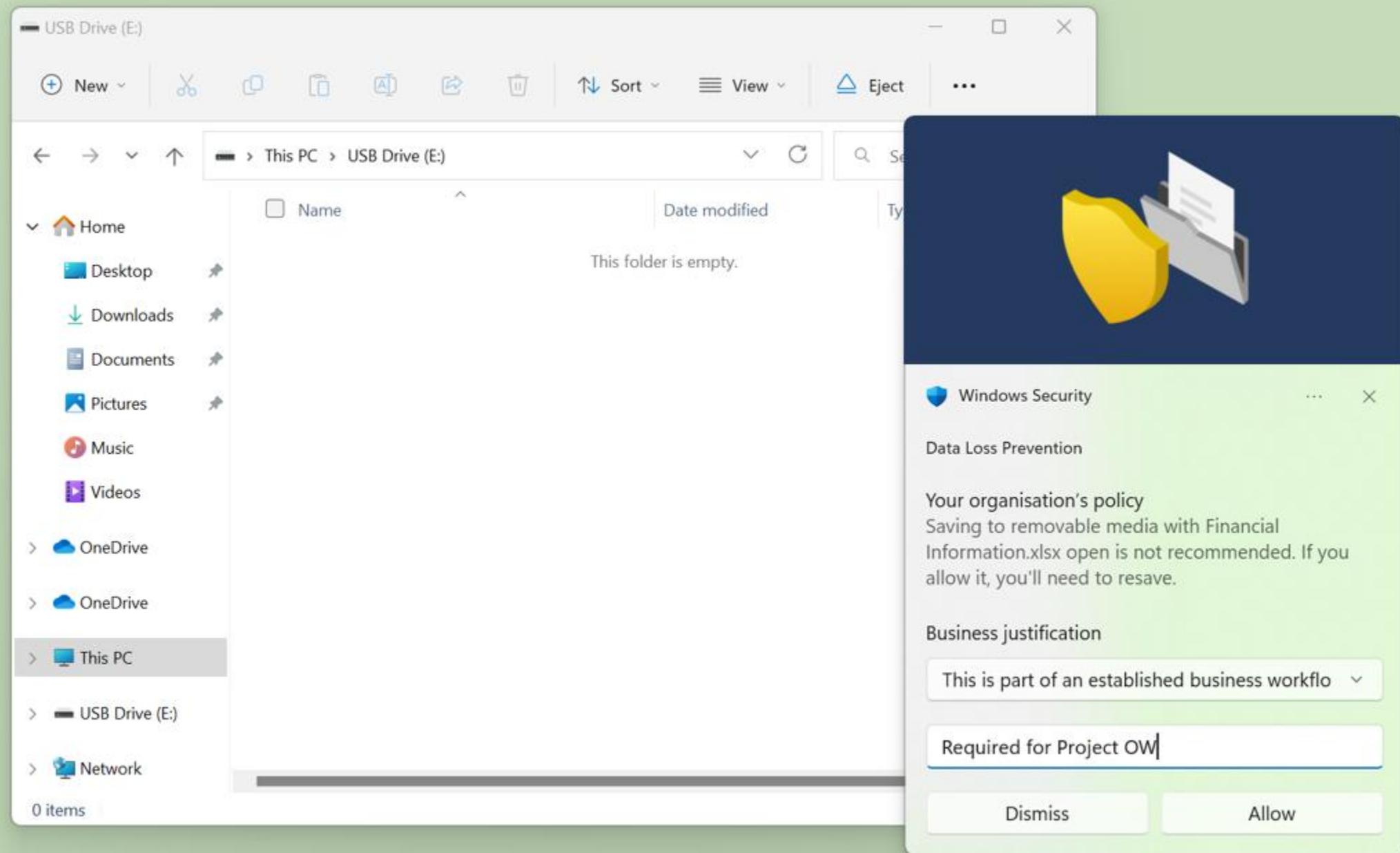
**Drop it like it's hot**

Upload files or folders by dropping them in this window

Financial  
Information



## Recycle Bin



14:11



Aptos (Body) 12 A A B I U H A Normal

### Summary by Copilot

Generate

This document is confidential



Microsoft Purview is a comprehensive set of solutions that helps your organization govern, protect, and manage data wherever it lives. Microsoft Purview solutions provide integrated coverage and help address the fragmentation of data across organizations, the lack of visibility that hampers data protection and governance, and the blurring of traditional IT management roles.

Microsoft Purview combines solutions and services into a unified platform that helps your organization:

- Gain visibility into data across your organization
- Safeguard and manage sensitive data across its lifecycle, wherever it lives
- Govern data seamlessly in new, comprehensive ways
- Manage critical data risks and regulatory requirements

Network 3  
Internet access

Confidential info

Ask Copilot anything

File Home Insert Layout References Review View Help

Comments Catch up Editing Share

Aptos (Body) 12 Normal

This document is confidential

Microsoft Purview is a comprehensive set of solutions that helps your organization govern, protect, and manage data wherever it lives. Microsoft Purview solutions provide integrated coverage and help address the fragmentation of data across organizations, the lack of visibility that hampers data protection and governance, and the blurring of traditional IT management roles.

Microsoft Purview combines solutions and services into a unified platform that helps your organization:

- Gain visibility into data across your organization
- Safeguard and manage sensitive data across its lifecycle, wherever it lives
- Govern data seamlessly in new, comprehensive ways
- Manage critical data risks and regulatory requirements

(Ctrl)

please summarise my document

Copilot

You asked for a summary of your document, "Confidential info.docx". Upon reviewing the file, I found that it contains only the following message:

"Can't provide more information in accordance with your Organization's security policies". [Confidential info](#)

This means the document does not include any additional content or details to summarise. If you have another file or specific content you would like summarised, please let me know and

Explain typical security policies for confidential files

Suggest how to handle restricted documents in reports

AI-generated content may be incorrect

Chat | M365 Copilot    Home - OneDrive    Confidential info

https://m365.cloud.microsoft/chat

Work Web Try GPT-5

# Hi, how can I help?

I have a document in my OneDrive titled "Confidential info", could you please summarise the document for me?

+ ↗

Create an FAQ based on doc

Jump-start a draft

Help me learn about topic

Boost your knowledge

Create a professional-looking background that highlights ico...

Bespoke Teams backgrounds

What's the latest from person, organised by emails, chats, and...

Stay informed

List key points from file

Understand the main points

When's my next one-on-one with person?

Find your next check-in

Network 3 Internet access

Chat | M365 Copilot    Home - OneDrive    Confidential info

https://m365.cloud.microsoft/chat

Unable to Summarise Confidential OneDrive Document

Work Web Try GPT-5

Today

I have a document in my OneDrive titled "Confidential info", could you please summarise the document for me?

Copilot

I found your document titled [Confidential info](#) in OneDrive, but I'm unable to access its contents due to your organisation's security policies. Confidential info

If you'd like, you can copy and paste the text here or upload a screenshot, and I'll help you summarise it. Let me know how you'd prefer to proceed.

Sources >

Help me paste the document text here Explain how to upload a screenshot

Message Copilot

+

AI-generated content may be incorrect

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Settings

DSPM for AI

Data Loss Prevention

Information Protection

**Data Loss Prevention**

Overview

Policies

**Alerts**

Classifiers

Explorers

Diagnostics

**Related solutions**

Data Security Investigations (preview)

Information Protection

Insider Risk Management

Alerts

If your role group permissions are restricted to a specific set of users, you'll only be able to view alerts for those users. [Learn more about role group permissions.](#)

Did you know you can now manage your DLP alerts in the Microsoft Defender portal? Alerts are automatically combined into incidents, which provide a comprehensive view into potential policy violations and advanced tools for investigation and remediation.

[Learn more about incidents](#) [Go to Incidents page](#)

Export Refresh

4 items [Customize columns](#)

Filter Reset Filters

Time range: 27/9/2025-27/10/2025 User: Any Alert status: Any Alert severity: Any

<input type="checkbox"/>	Alert name	Severity	Status	Time detected	Users	Location
<input type="checkbox"/>	DLP policy match for Microsoft 365 Copilot	Low	Active	27 Oct 2025 18:59	test_ep@T...	ExtendedApplic...
<input type="checkbox"/>	Sensitive info found in 'Confidential info.do...	Low	Active	27 Oct 2025 18:59	(User) Test Ewelina	ExtendedApplic...
<input type="checkbox"/>	DLP policy match for Microsoft 365 Copilot	Low	Active	27 Oct 2025 18:28	test_ep@T...	ExtendedApplic...
<input type="checkbox"/>	Sensitive info found in 'Confidential info.do...	Low	Active	27 Oct 2025 18:28	(User) Test Ewelina	ExtendedApplic...
<input type="checkbox"/>	DLP policy match for Microsoft 365 Copilot	Low	Active	27 Oct 2025 18:27	test_ep@T...	ExtendedApplic...
<input type="checkbox"/>	Sensitive info found in 'Confidential info.do...	Low	Active	27 Oct 2025 18:27	(User) Test Ewelina	ExtendedApplic...

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Alerts

Classifiers

Explorers

Diagnostics

Related solutions

Data Security Investigations (preview)

Information Protection

Insider Risk Management

# Alerts

If your role group permissions are restricted to a specific set of users, you'll only be able to view alert

Did you know you can now manage your DLP alerts in the Microsoft Defender portal? Alerts are automatically generated for policy violations and advanced tools for investigation and remediation.

Export Refresh

Filter Reset Filters

Time range: 27/9/2025-27/10/2025 User: Any Alert status: Any

Alert name	Severity	Status
DLP policy match for Microsoft 365 Copilot	Low	Act
Sensitive info found in 'Confidential info.docx'	Low	Act
DLP policy match for Microsoft 365 Copilot	Low	Act
Sensitive info found in 'Confidential info.docx'	Low	Act
DLP policy match for Microsoft 365 Copilot	Low	Act
Sensitive info found in 'Confidential info.docx'	Low	Act

Event: Sensitive info found in 'Confidential info.docx'

27 Oct 2025 18:58

### Impacted entities

ID	Location
1545c180-4c65-4fbb-8de8-e1861b3ee8f2	Copilot.M365

### Time of activity

27 Oct 2025 18:58

### Policy details

DLP policy matched	Rule matched
DLP-Copilot-SharingConfidentialInfo(Labelled)-Block	Copilot-SharingConfidentialInfo(Labelled)-Block

### Sensitive info types detected

None

### Trainable classifiers detected

None

### Actions taken

GenerateAlert, RestrictAccess

### User override policy

No

### Override justification text

None

Actions Update alert status

# Alerts

(i) If your role group permissions are restricted to a specific set of users, you'll only be able to view alerts for those users.

💡 Did you know you can now manage your DLP alerts in the Microsoft Defender portal? Alerts are automatically generated for sensitive information violations and advanced tools for investigation and remediation.

⤵ Export ⟳ Refresh

Filter ✖ Reset ✖ Filters

Time range: **27/9/2025-27/10/2025** ▼

User: **Any** ▼

Alert status: **Any** ▼

<input type="checkbox"/>	Alert name	Severity	Start time
<input type="checkbox"/>	DLP policy match for Microsoft 365 Copilot	<span style="color: #999;">■■■</span> Low	Action
<input checked="" type="checkbox"/>	Sensitive info found in 'Confidential info.docx'	<span style="color: #999;">■■■</span> Low	Action
<input type="checkbox"/>	DLP policy match for Microsoft 365 Copilot	<span style="color: #999;">■■■</span> Low	Action
<input type="checkbox"/>	Sensitive info found in 'Confidential info.docx'	<span style="color: #999;">■■■</span> Low	Action
<input type="checkbox"/>	DLP policy match for Microsoft 365 Copilot	<span style="color: #999;">■■■</span> Low	Action
<input type="checkbox"/>	Sensitive info found in 'Confidential info.docx'	<span style="color: #999;">■■■</span> Low	Action
<input type="checkbox"/>	DLP policy match for Microsoft 365 Copilot	<span style="color: #999;">■■■</span> Low	Action
<input type="checkbox"/>	Sensitive info found in 'Confidential info.docx'	<span style="color: #999;">■■■</span> Low	Action

## Event: Sensitive info found in 'Confidential info.docx'

↗ View all events

Details Source Metadata

**EventId:** "1545c180-4c65-4fbb-8de8-e1861b3ee8f2"

**Workload:** "ExtendedApplications"

**Time:** "2025-10-27T18:58:01Z"

**Location:** "Copilot.M365"

**Id:** "1545c180-4c65-4fbb-8de8-e1861b3ee8f2"

**Name:** "Confidential info.docx"

**PolicyMatch:** "DLP-Copilot-SharingConfidentialInfo(Labelled)-Block"

**PolicyId:** "5e5f9af4-740f-4f1b-8e4d-946ff1b063ad"

**RuleId:** "a227910b-a3a0-465d-a5fe-a9aa612de8a6"

**RuleMatch:** "Copilot-SharingConfidentialInfo(Labelled)-Block."

**SITDetected:** []

**TrainableClassifier:** []

**ActionTaken:** "GenerateAlert, RestrictAccess"

**UserOverride:** "No"

**DetectedValuesForSITS:** []

**OtherMatchedConditions:** []

Actions ▼

Update alert status

## Event: Sensitive info found in 'Confidential info.docx'

[View all events](#)

Details    Source    **Metadata**

**EventId:** "1545c180-4c65-4fbb-8de8-e1861b3ee8f2"

**Workload:** "ExtendedApplications"

**Time:** "2025-10-27T18:58:01Z"

**Location:** "Copilot.M365"

**Id:** "1545c180-4c65-4fbb-8de8-e1861b3ee8f2"

**Name:** "Confidential info.docx"

**PolicyMatch:** "DLP-Copilot-SharingConfidentialInfo(Labelled)-Block"

**PolicyId:** "5e5f9af4-740f-4f1b-8e4d-946ff1b063ad"

**RuleId:** "a227910b-a3a0-465d-a5fe-a9aa612de8a6"

**RuleMatch:** "Copilot-SharingConfidentialInfo(Labelled)-Block."

**SITDetected:** []

**TrainableClassifier:** []

**ActionTaken:** "GenerateAlert, RestrictAccess"

**UserOverride:** "No"

**DetectedValuesForSITS:** []

Send email notification

Copy event link

**Actions** ↗

Update alert status

### Update alert status

ⓘ This is not an event level action. This will update the status of the actual alert.

#### Status

Active

Active

Investigating

Dismissed

Resolved

### Update alert status

ⓘ This is not an event level action. This will update the status of the actual alert.

#### Status

Active

#### Assign to

Start typing to find users

#### Comments

Add comments about this alert

## Data Loss Prevention

Overview

Policies

Alerts

Classifiers

▼

Explorers

^

Data explorer

Content explorer (classic)

Activity explorer

Diagnostics

## Related solutions

Data Security Investigations (preview)

Information Protection

Insider Risk Management

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](#)



Show me the top 5 activities from the past week

Filter and investigate [activities](#)Find [files](#) used in specific activitiesSelected filter set: **None** ▾

Save

Date: 27/9/2025-27/10/2025

Activity: Any

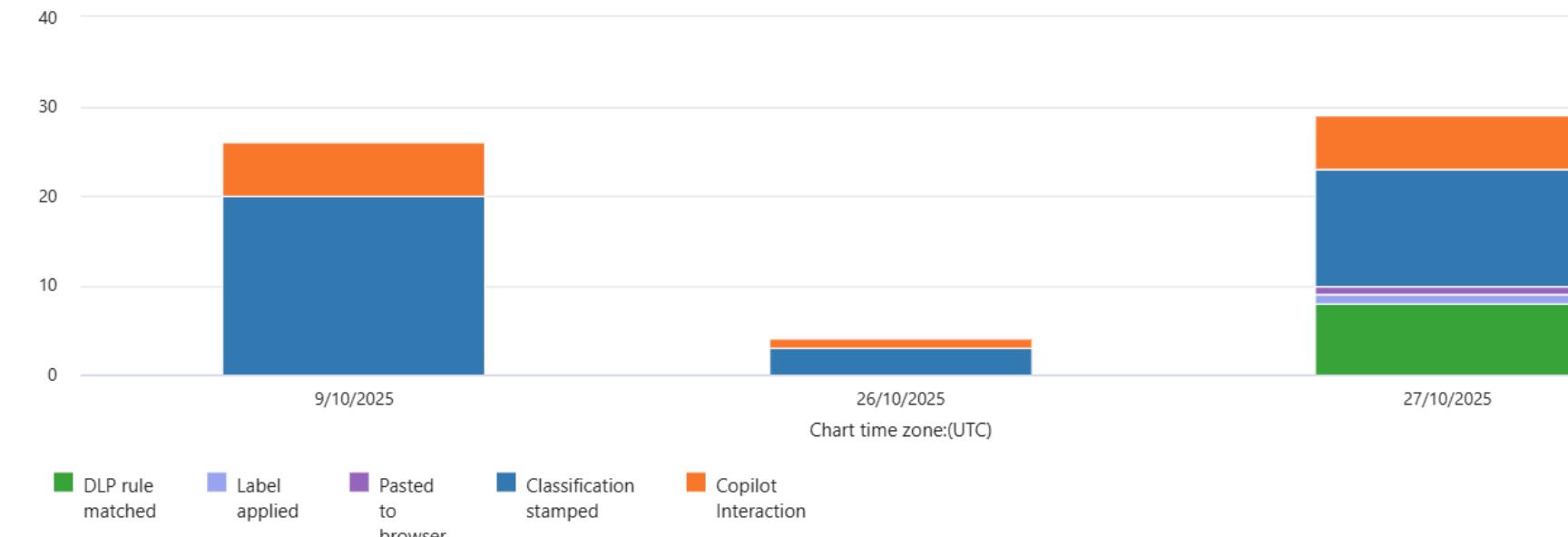
Location: Any

User: Any

Sensitivity label: Any

Add filter

Reset all



Export



Refresh

59 items Customize columns



## Data Loss Prevention

[Overview](#)[Policies](#)[Alerts](#)[Classifiers](#)[Explorers](#)[Data explorer](#)[Content explorer \(classic\)](#)[Activity explorer](#)[Diagnostics](#)

### Related solutions

[Data Security Investigations \(preview\)](#)[Information Protection](#)[Insider Risk Management](#)[Export](#) [Refresh](#)

59 items

[Customize](#)

Activity	File	Location	Enforcement plane	User
<input type="checkbox"/> Label applied	https://[REDACTED]-my.sharepoint.com/...	OneDrive		test_ep@[REDACTED]
<input type="checkbox"/> DLP rule matched		Microsoft 365 Copilot		test_ep@[REDACTED]
<input type="checkbox"/> DLP rule matched		Microsoft 365 Copilot		9ed87649-[REDACTED]
<input type="checkbox"/> DLP rule matched		Microsoft 365 Copilot		9ed87649-[REDACTED]
<input type="checkbox"/> DLP rule matched		Microsoft 365 Copilot		test_ep@[REDACTED]
<input type="checkbox"/> DLP rule matched		Microsoft 365 Copilot		test_ep@[REDACTED]
<input type="checkbox"/> DLP rule matched	https://[REDACTED]-my.sharepoint.com/...	Microsoft 365 Copilot		test_ep@[REDACTED]
<input type="checkbox"/> DLP rule matched		Microsoft 365 Copilot		test_ep@[REDACTED]
<input type="checkbox"/> DLP rule matched		Microsoft 365 Copilot		test_ep@[REDACTED]
<input type="checkbox"/> Pasted to browser		Endpoint devices		test_ep@[REDACTED]
<input type="checkbox"/> Classification stamped	1761591485337	Copilot		test_ep@[REDACTED]
<input type="checkbox"/> Classification stamped	1761591485108	Copilot		test_ep@[REDACTED]
<input type="checkbox"/> Copilot Interaction		Copilot		test_ep@[REDACTED]
<input type="checkbox"/> Classification stamped	1761589666721	Copilot		test_ep@[Threatscapelabs.c...



[Home](#)[Exposure management](#)[Investigation & response](#)[Incidents & alerts](#)[Incidents](#)[Alerts](#)[Hunting](#)[Actions & submissions](#)[Partner catalog](#)[Threat intelligence](#)[Assets](#)

# Incidents

[Alert service settings](#)[Email notification](#)

Most recent incidents and alerts

[Export](#)[Copy list link](#)[Refresh](#)

1 Week

8 Incidents



Search for name or ID



Customize columns

Filter set: [Save](#)

Status: New, In progress



Alert severity: High, Medium, Low

[Add filter](#)[Reset all](#)

	Incident name	Incident Id	Tags	Severity
<input type="checkbox"/>	DLP-Copilot-SharingConfidentialInfo(Labelled)-Block.	2045		<span style="color: #ff8080;">■■■</span> Low
<input type="checkbox"/>	DLP-Copilot-SharingConfidentialInfo(Labelled)-Block. involving one user	2043		<span style="color: #ff8080;">■■■</span> Low
<input type="checkbox"/>	DLP-Copilot-SharingConfidentialInfo(Labelled)-Block. involving one user	2044		<span style="color: #ff8080;">■■■</span> Low
<input type="checkbox"/>	DLP-Copilot-SharingConfidentialInfo(Labelled)-Block.	2042		<span style="color: #ff8080;">■■■</span> Low
<input type="checkbox"/>	Custom - Activity - Log on from an outdated browser involving one user	2036		<span style="color: #ff8080;">■■■</span> Low

Part of incident: DLP-Copilot-SharingConfidentialInfo(Labelled)-Block. involving one user [View incident page](#)

test\_ep



## DLP-Copilot-SharingConfidentialInfo(Labelled)-Block.

■■■ Low | ● Unknown | ● New

[Manage alert](#) [Move alert to another incident](#) ...

### Alert state

Classification	Assigned to
Not Set	Unassigned
<a href="#">Set Classification</a>	

### Alert details

Alert ID	Category
dl5fc55f71-6efc-6bad-f200-08de158ae384	Exfiltration

MITRE ATT&CK Techniques	Detection source
-	Microsoft Data Loss Prevention

Service source	Detection technology
Microsoft Data Loss Prevention	-

Generated on	First activity
27 Oct 2025 18:59:22	27 Oct 2025 18:58:00

Last activity	Workspace
27 Oct 2025 18:59:00	-



# DATA POLICY IN POWER PLATFORM

A **data policy** in **Microsoft Power Platform** is a rule set that controls how data flows in apps and automations, defining which data sources are business vs non-business to prevent accidental leaks.



# HOW IT EXTENDS DLP

- Brings DLP principles to apps, flows, and dashboards
- Blocks risky connector usage before data leaves approved sources
- Aligns with broader Microsoft 365 DLP for unified protection



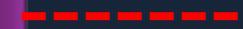
# POWER PLATFORM DATA POLICY

**Microsoft Purview**

**Power Platform**

Data Loss Prevention (DLP)

Data policies (DLP)



# DEMO 2: Setting up a Power Platform data policy

- Goal: Create a data policy to protect business data in Power Apps, Power Automate, and Power BI, Copilot Studio, etc.
- Steps to show:
  - Classify connectors as business or blocked
  - Define custom connector patterns
  - Select environments and apps where the policy applies



## Security



Overview

Settings

Data and privacy

Identity and access

Threat detection

Compliance

Products

Power Pages



...



Admin  
centers

## Data protection and privacy

Make sure personal information is handled, stored, and protected securely; prevent unauthorized access to data; and protect apps and cloud workloads from network-based cyberattacks. [Learn more](#)

### Customer-managed encryption key

Manage the key that encrypts your Power Platform data, preventing outside access to your customer data and meeting your data protection requirements.

### Advanced connector policies (preview)

Choose which certified connectors, actions, triggers, and MCP servers to allow.

### Data policy

Set up guardrails for environment and tenant-wide connectors to reduce data exfiltration risks.

### Azure Virtual Network policies

Protect items made in Power Platform inside your virtual network without exposing them over the public internet.



Feedback



Search for settings, pages, and more



Home



Actions



Manage



Security



Copilot

...



Admin

centers

## Security



← Back + New Policy

Search

Overview

Settings

Data and privacy

Identity and access

Threat detection

Compliance

Products

Power Pages

### Data policies

Create and manage connector policies to protect data within your org (tenant). [Learn more](#)

Name	Scope	Applied to	Created by
DLP-PowerPlatform-Conr	Org (tenant)	All environments	Administrator

## Assign connectors ⓘ

[Business \(7\)](#)   [Non-business \(1519\) | Default](#)   [Blocked \(25\)](#)

Search connector

Blocked connectors can't be used where this policy is applied.

⋮	Name ↑ ↴	Blockable ↴	Endpoint configu... ↴	Class ↴	Publisher ↴	About ↴
	Box	⋮ Yes	No	Standard	Microsoft	<a href="#">Learn about Box</a>
	Dropbox	⋮ Yes	No	Standard	Microsoft	<a href="#">Learn about Dropbox</a>
	Face API	⋮ Yes	No	Standard	Microsoft	<a href="#">Learn about Face API</a>
	Facebook	⋮ Yes	No	Standard	Microsoft	<a href="#">Learn about Facebook</a>
	Facebook channel in Copilot Studio	⋮ Yes	No	Built-In	Microsoft	
	FedEx	⋮ Yes	No	Premium	Microsoft	<a href="#">Learn about FedEx</a>
	FedEx Dataworks	⋮ Yes	No	Premium	Microsoft	<a href="#">Learn about FedEx Dataworks</a>
	FedEx Supply Chain Returns	⋮ Yes	No	Premium	Microsoft	<a href="#">Learn about FedEx Supply Chain Returns</a>

# BEST PRACTICES & COMMON MISTAKES

Business  
Strategy  
Planning

Technical

# Data Loss Prevention

Best practices

Home

## Data Loss Prevention



Solutions



Agents

## Overview

Policies

Alerts

Classifiers



Explorers



Diagnostics



## Related solutions

Data Security  
Investigations (preview)

Information Protection

Insider Risk Management



Customize columns

Priority

Mode

On

On

On

On

On

In simulation without notifications

On

On

On

On

On

# Business / Strategy / Planning

- Secure management buy-in & align stakeholders early
- Ensure resources are ready to manage DLP/Purview
- Define sensitive data & compliance obligations upfront
- Pilot first - use audit/simulation before full enforcement
- Use clear naming conventions for policies & rules
- Train users - make policies and sensitive data awareness clear
- Plan for change - adjust policies based on reports, false positives, and new scenarios

# Technical

- ✓ Onboard & configure devices before enabling endpoint DLP
- ✓ Deploy browser extensions & on-prem scanners
- ✓ Use classification & labeling
- ✓ Test, tune, then enforce
- ✓ Leverage the full platform for protection
- ✓ Monitor alerts & adjust
- ✓ Balance policy tips vs. blocks for user experience
- ✓ Know your license & product limitations

# Data Loss Prevention

Common mistakes

# Business / Strategy / Planning

- ✗ Poor planning -> misaligned, complex policies
- ✗ No dedicated DLP resources
- ✗ Failing to classify data -> protecting the unknown
- ✗ Overly strict policies -> productivity loss & workarounds
- ✗ Ignoring licensing -> surprise limitations
- ✗ Bad naming conventions -> confusion & management issues

# Technical

- ✗ Skipping prerequisites -> coverage gaps
- ✗ Generic policies -> lost granularity, rule conflicts
- ✗ Duplicate / unclear naming -> errors & conflicts
- ✗ Not enabling endpoint / server DLP -> gaps in scope
- ✗ Overusing overrides -> policy fatigue
- ✗ Misconfigured thresholds -> false positives or missed detections
- ✗ Ignoring alerts -> you don't know what's working

# Technical

- ✖ Not protecting Teams files -> must include SharePoint & OneDrive
- ✖ Misunderstanding policy & rule priority -> wrong actions applied
- ✖ Ignoring condition order -> rules fail unexpectedly
- ✖ Not using AND / OR logic -> limited or incorrect rule behavior
- ✖ Incorrect nested groupings -> complex rules break

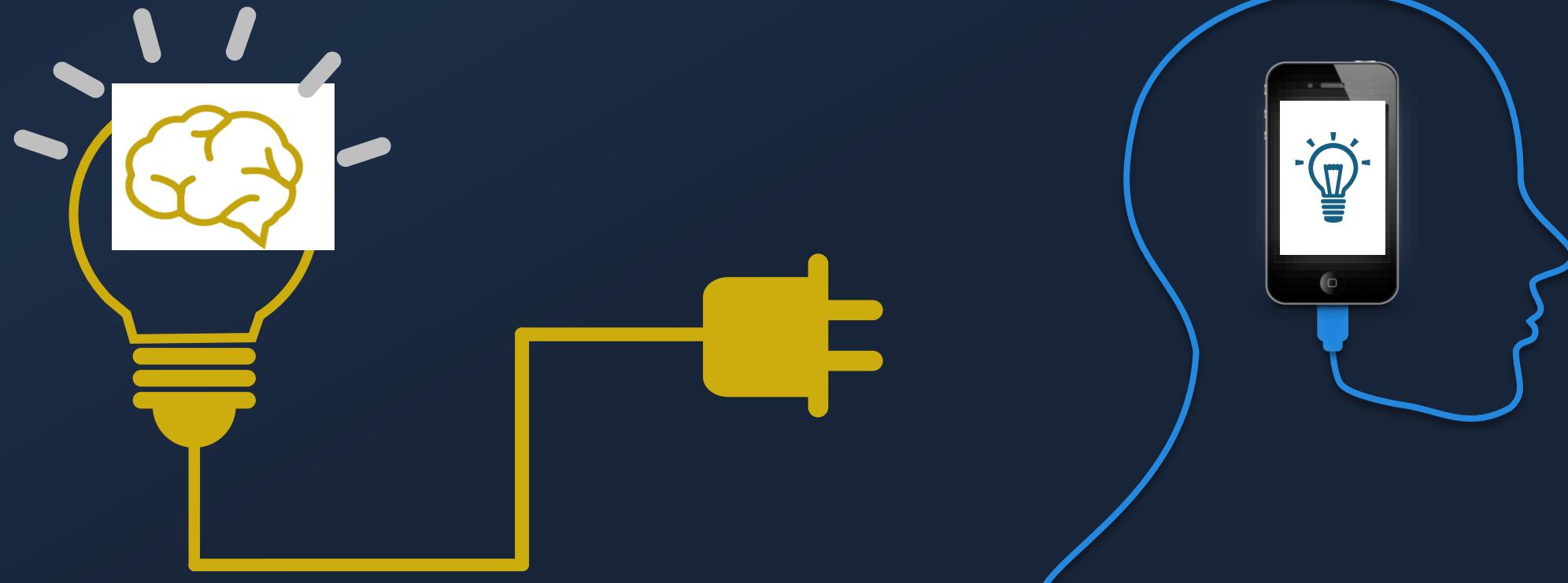
# CONCLUSIONS

- Secure management-buy in
- Start with the people, not with the portal



# CONCLUSIONS

- Microsoft Purview DLP is not plug and play
- Microsoft Purview DLP is powerful but only as good as your planning, deployment, and tuning



# CONCLUSIONS

- Progress not perfection
- Start with prerequisites, right licensing, pilot / audit mode



# CONCLUSIONS

- Use best practices to avoid common mistakes - both strategy/business and technical sides matter
- Continuous monitoring & adjustment is key



# SUMMARY OF CONCLUSIONS

- Secure management-buy in early
- Start with the people, not with the portal
- Microsoft Purview DLP is not plug and play
- Microsoft Purview DLP is powerful but only as good as your planning, deployment, and tuning
- Progress nor perfection
- Start with prerequisites, right licensing, pilot / audit mode
- Use best practices to avoid common mistakes - both strategy/business and technical sides matter
- Continuous monitoring & adjustment is key
- Leverage the entire platform



# THE LIFE OF A DLP PRO

POLICIES DON'T PROTECT DATA - PEOPLE AND PLANNING DO.

A DLP POLICY IS ONLY AS STRONG AS THE STRATEGY BEHIND IT.

DON'T AIM FOR PERFECTION - AIM FOR PROGRESS AND PROTECTION

FOR EVERY DLP OOPS, THERE'S A POST ON WELKA'S WORLD!

# REFERENCES

- [Common mistakes you may be making with Data Loss Prevention \(Welka's World\)](#)
- [Learn about data loss prevention \(MS Learn\)](#)
- [Microsoft 365 Compliance Licensing Comparison](#)
- [Microsoft Purview device onboarding](#)
- [Get started with the Microsoft Purview extension for Chrome | Microsoft Learn](#)
- [Get started with the Microsoft Purview extension for Firefox | Microsoft Learn](#)
- [How to deploy Microsoft Purview DSPM for AI to secure your AI apps | Microsoft Community Hub](#)
- [Learn about investigating data loss prevention alerts](#)
- [Learn about the Microsoft 365 Copilot policy location](#)
- [Power Platform data policy](#)

# Q&A



# THANK YOU!

BLOG

[www.welkasworld.com](http://www.welkasworld.com)



@ewelinapaczkowska



@WelkasWorld

