










Purview Quick Start blueprint

Blueprint



Lightweight guide to mitigate data leakage

Protect confidential data across M365 estate

	Good 	Better 	Best 
Activities	<ul style="list-style-type: none">• Create sensitivity and sub labels: Define and publish a 'Confidential/AllEmployees' label for files and SharePoint sites• Set default label: Automatically apply 'Confidential/AllEmployees' label to new files created in M365• Apply basic DLP policy: Block sharing of labeled content via SharePoint, OneDrive and Exchange• Enable Audit logging: Track user and admin activity across M365	<ul style="list-style-type: none">• Create custom SITs: Detect and classify data unique to your organization, like internal project codes, intellectual property• Configure client-side auto-labeling: Use custom-built SITs and auto-apply labels in Office apps as users create or edit content• Enable Teams and Endpoint DLP: Create policies to block sensitive files from USB copy, printing, sharing externally, etc.• Apply email protection: Use DLP to block emails with custom-built SITs and auto-label the email to inherit highest sensitivity from any attached or linked files	<ul style="list-style-type: none">• Encrypt files: Apply encryption to content labeled with high-sensitivity sub-labels or containing critical SITs• Extend service-side auto-labeling: Auto-label existing files and emails in transit across SharePoint, OneDrive, Exchange• Run Insider Risk Mgmt Analytics: Identify top risks and receive recommendations on pre-built policies to configure• Enable Adaptive Protection: Dynamically adjust DLP and Conditional Access policies based on user's risky activity
Outcomes	 Establish foundational data security with minimal configuration	 Expand protection to endpoints and automate classification	 Continuous improvement of data security practices
Effort*	 1-2 weeks	 2-4 weeks	 1-2 weeks

*Suggested efforts should be reviewed into timelines based on your tenant size and organizational complexity

Good

Protect your sensitive information

- Create sensitivity labels
- Create sensitivity sub-labels
- Order labels by priority
- Publish sensitivity labels
- Set as default label
- Enable OneDrive and SharePoint labels
- Enable Audit logging

Block sharing of sensitive information

- Create and deploy DLP policies across:
 - Exchange
 - SharePoint
 - OneDrive

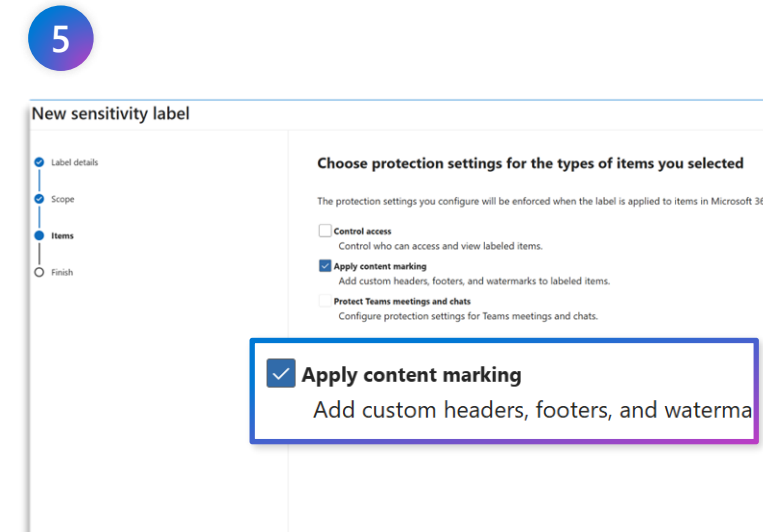
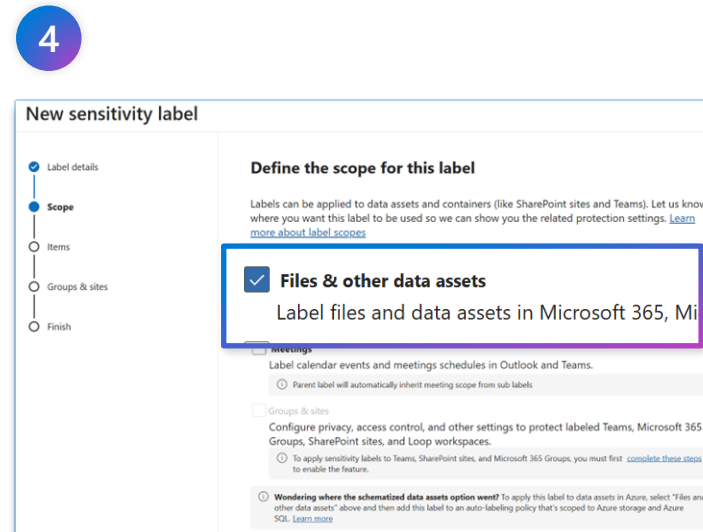
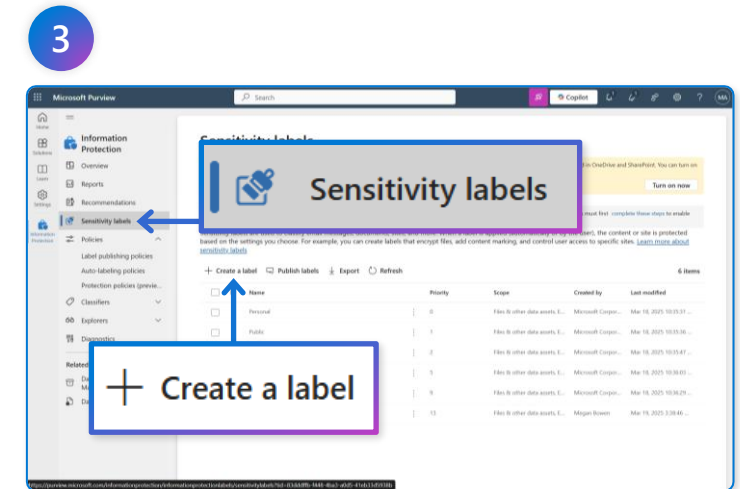
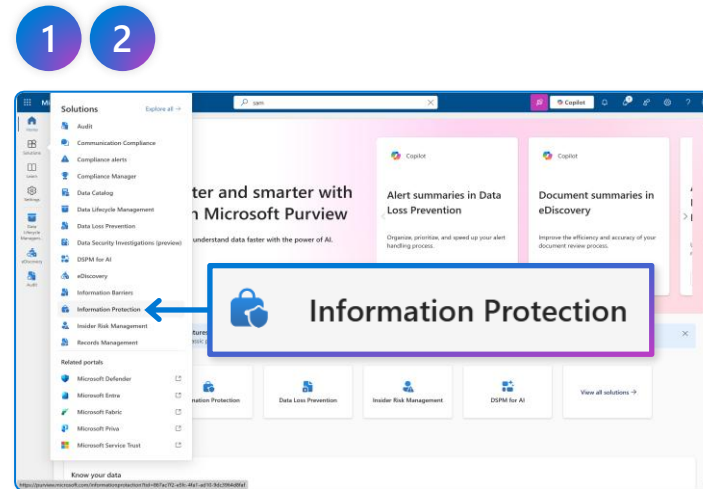
Create sensitivity labels

Sensitivity labels help classify and protect content across M365. You can define parent labels (e.g. Confidential) and sub-labels (e.g. AllEmployees) to restrict access, apply encryption and content marking.

Available with Business Premium or above

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Information Protection**
- 3) Select **Sensitivity labels > + Create a label**
- 4) Define:
 - **Label 1 name:** Confidential, General
 - **Label 2 name:** General
 - **Scope:** files and other data assets
- 5) Configure **protection settings**:
 - **Add content marking**



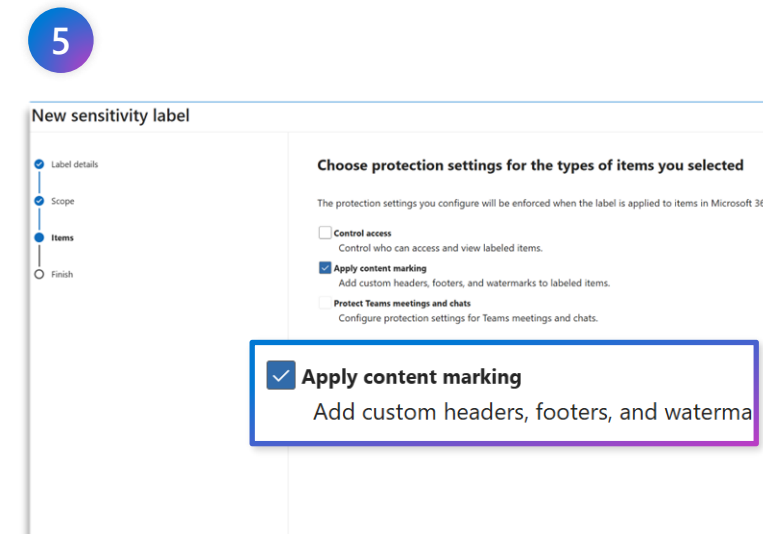
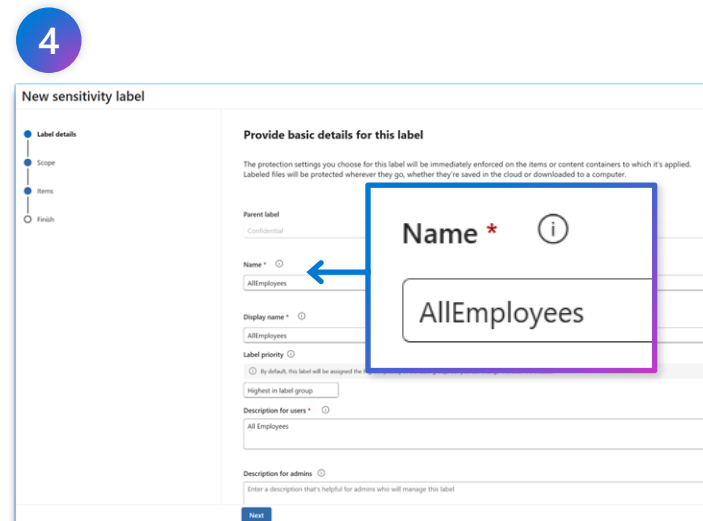
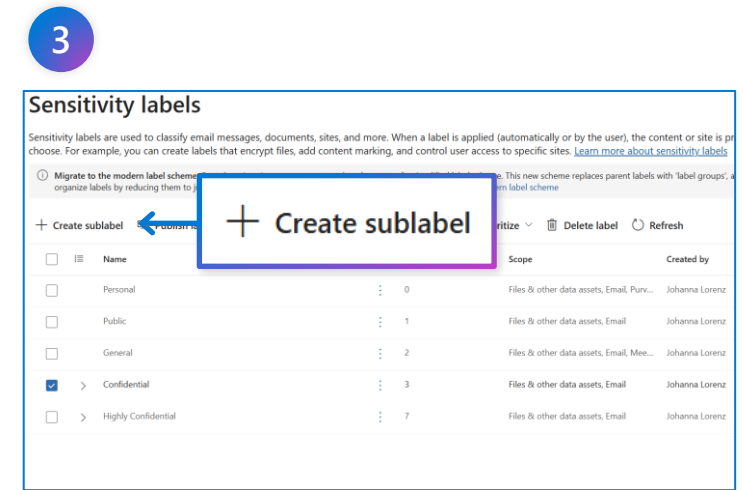
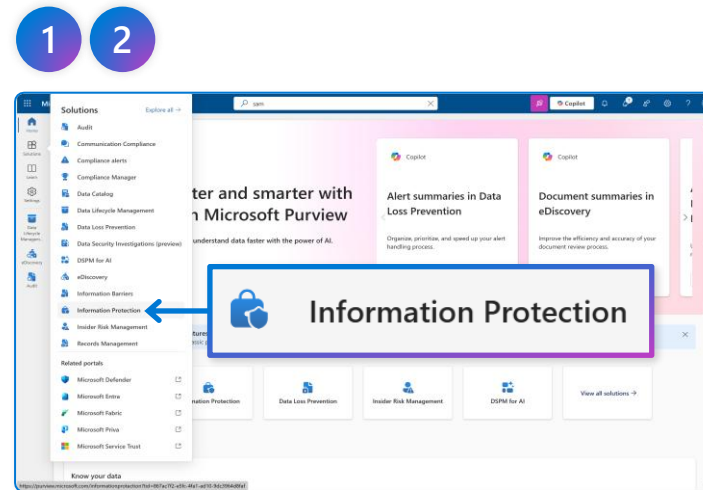
Create sensitivity sub-labels

Sub-labels allow you to apply more granular protection within a broader classification, tailored with access controls, encryption or usage restrictions. This helps balance security with productivity, ensuring the right level of protection for different types of sensitive data.

Available with Business Premium or above

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Information protection**
- 3) Select a Sensitivity label > **+Create sub-label**
- 4) Define:
 - Name: **AllEmployees**
 - Scope to: files and SharePoint sites
- 5) Configure protection settings:
 - Add content marking



Order labels by priority

Label priority determines which sensitivity label is applied when multiple labels match the same content. The highest priority label wins – typically the one with the most restrictive protections. This ensures more sensitive labels override less sensitive ones.

Available with Business Premium or above

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Information protection**
- 3) Select **Sensitivity labels** > Look at Priority
- 4) Select a label and select **Reprioritize**
 - Move less sensitive or default labels down (closer to 0)
 - Move highly sensitive labels up numerically

1

2

3

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. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

4

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. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

Reprioritize

- Move to top (lowest priority)
- Move up
- Move down
- Move to bottom (highest priority)
- Assign priority

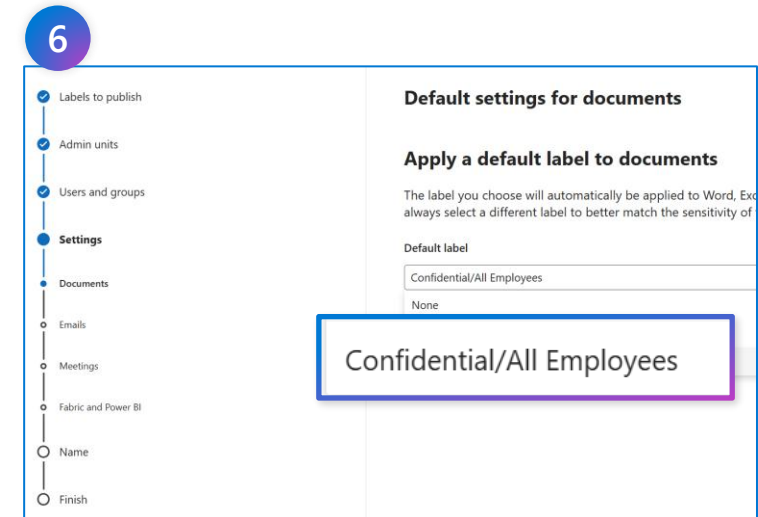
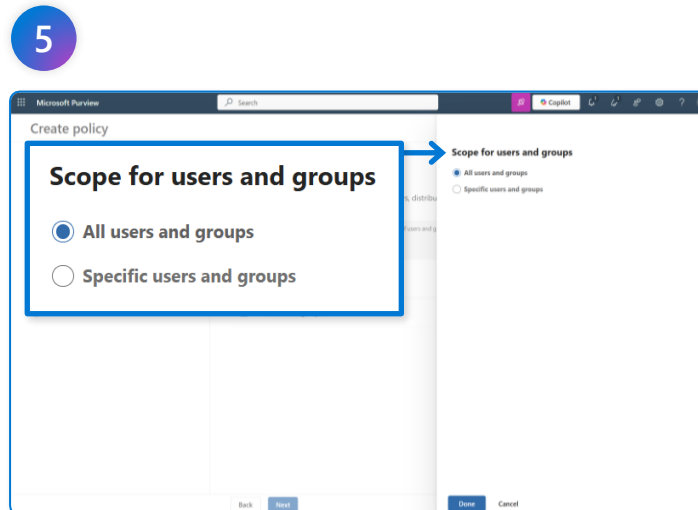
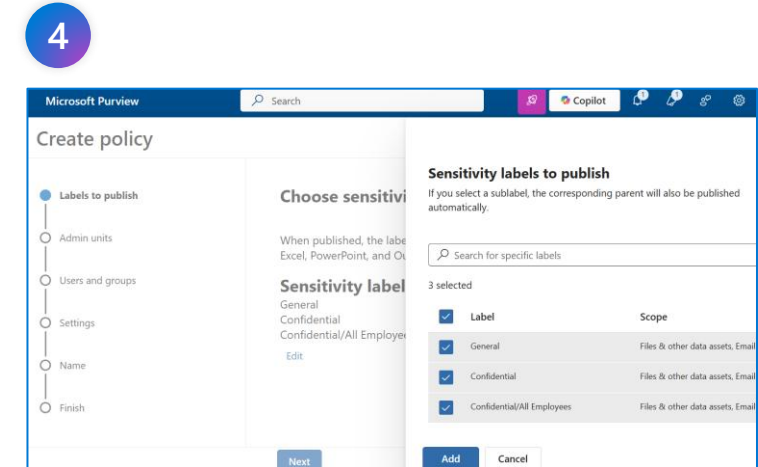
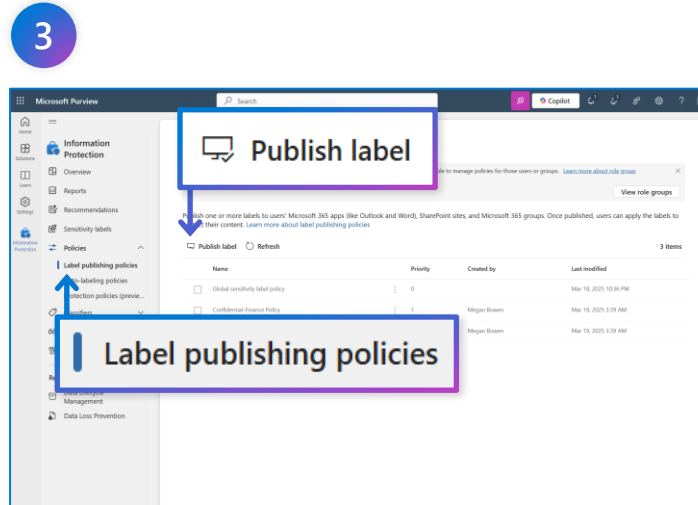
Publish sensitivity labels

Publishing your labels ensures users can see and use them. Automatically applying labels helps scale protection across Teams, SharePoint and OneDrive.

Available with Business Premium or above

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Information protection**
- 3) Select **Policies > Label publishing policies > Publish label**
- 4) Select sensitivity labels to publish, **Add**
- 5) Publish to **All users and groups**
- 6) Apply **default label to documents**, with Confidential/AllEmployees label
- 7) Name your policy



Enable OneDrive and SharePoint labels

Recognize and enforce sensitivity labels on files stored in SharePoint and OneDrive. This allows documents to inherit labels from libraries.

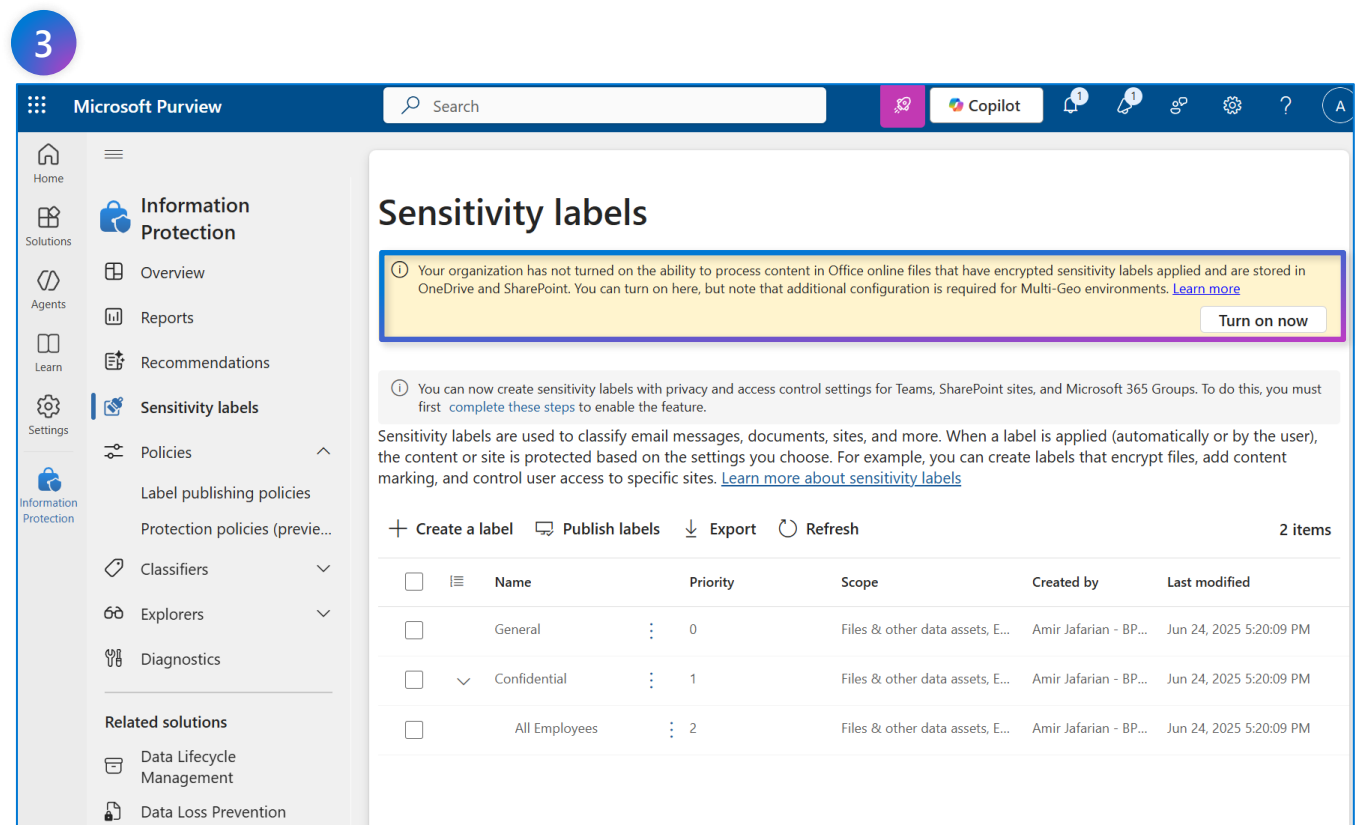
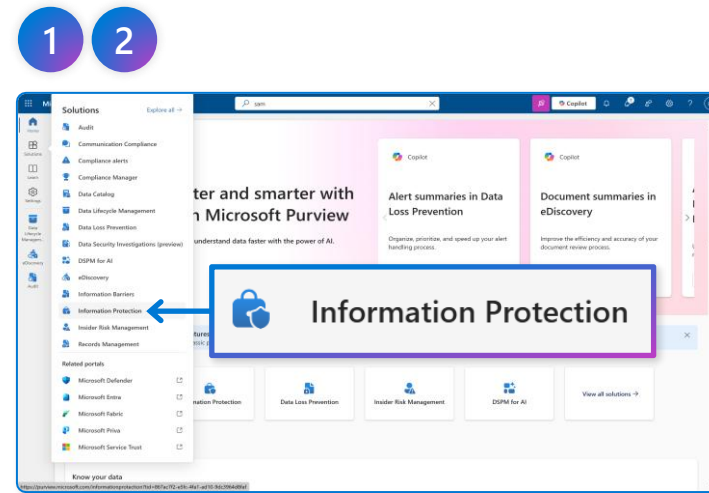
Available with Business Premium or above

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Information protection**
- 3) Under **Sensitivity labels** > If you see the following message, Select **"Turn on now"**:

"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."

Note: If you do not see this banner, the feature is likely already enabled.



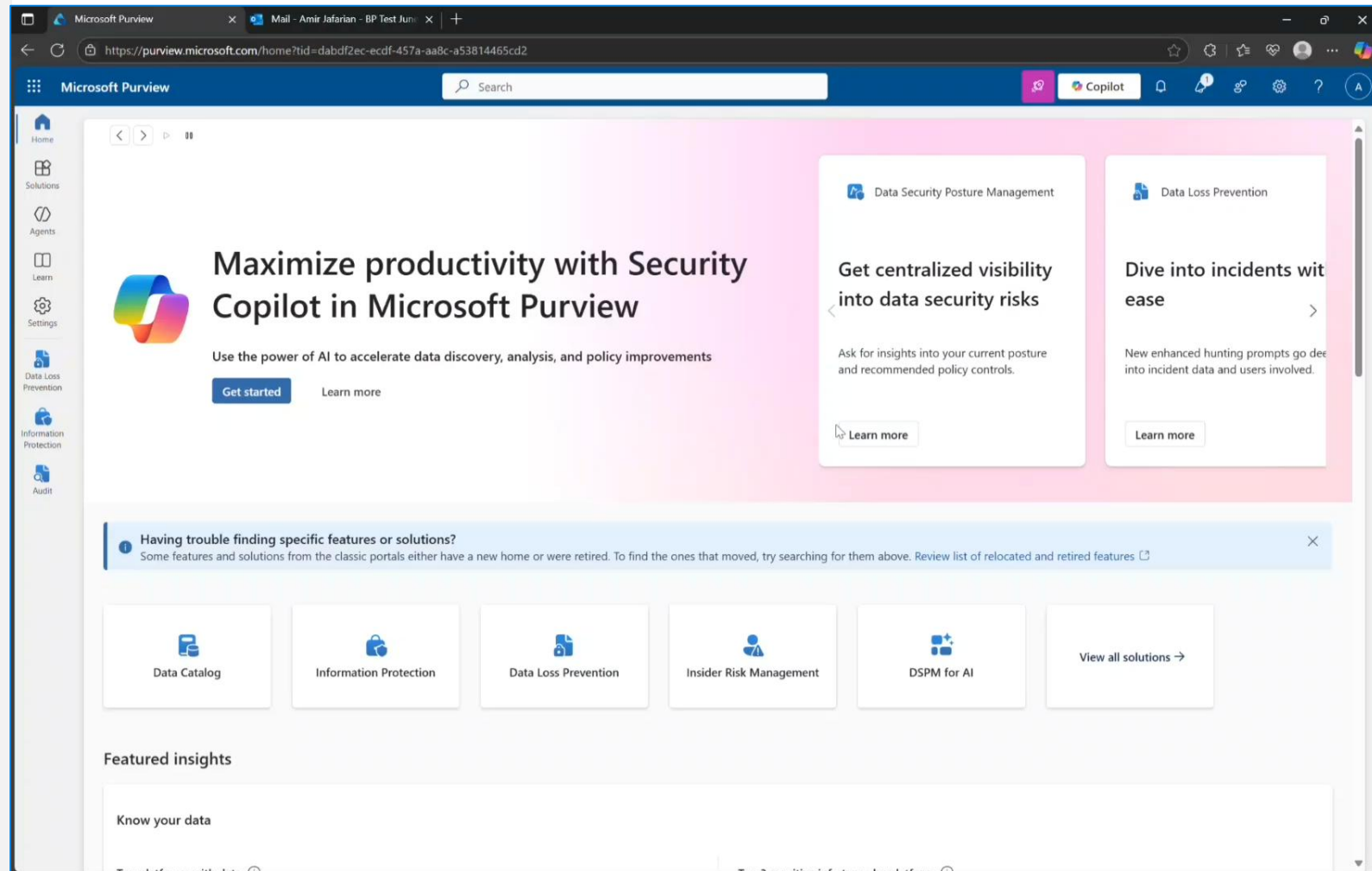
Create and deploy DLP policies

Create Microsoft Purview DLP policies for Exchange, SharePoint, and OneDrive to prevent sharing of labeled content. These policies help enforce internal-only access by blocking external sharing, forwarding, or downloading of sensitive files and emails — ensuring consistent protection across Microsoft 365.

Available with Business Premium or above

How to do it

- 1) Go to purview.microsoft.com > Go to **Solutions** > **Data Loss Prevention**
- 2) Go to Policies > **+Create policy** > **Data stored in connected sources**
- 3) Choose template: **Custom policy** and name Policy
- 4) Choose locations: Policy 1: **Exchange email**; Policy 2: **SharePoint sites, OneDrive accounts** [Best practice is to have separate DLP policy for Exchange]
- 5) Create rule and define:
 - Conditions: content is labeled **Confidential/AllEmployees**
 - Actions: Block sharing with people **outside the organization**
- 6) Select Policy mode: **Turn on the policy immediately**



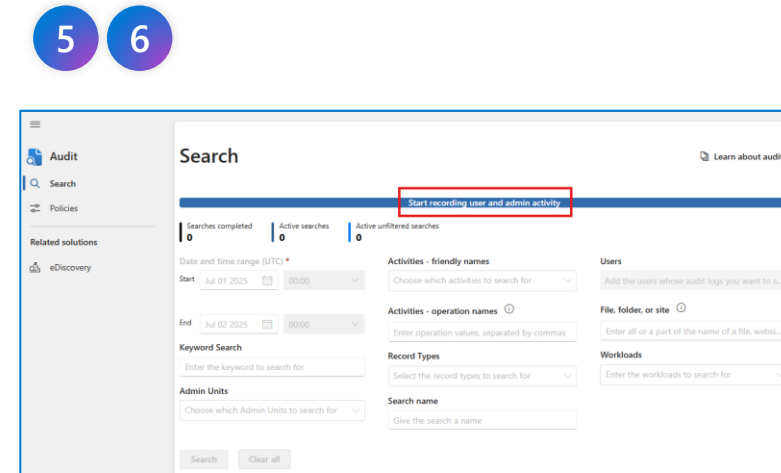
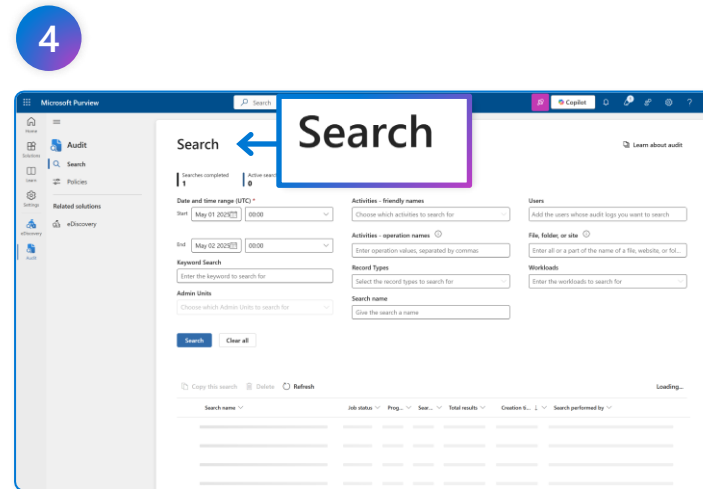
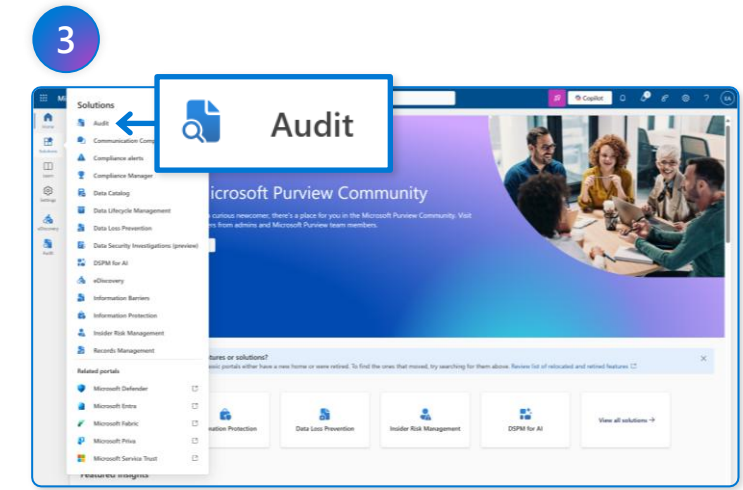
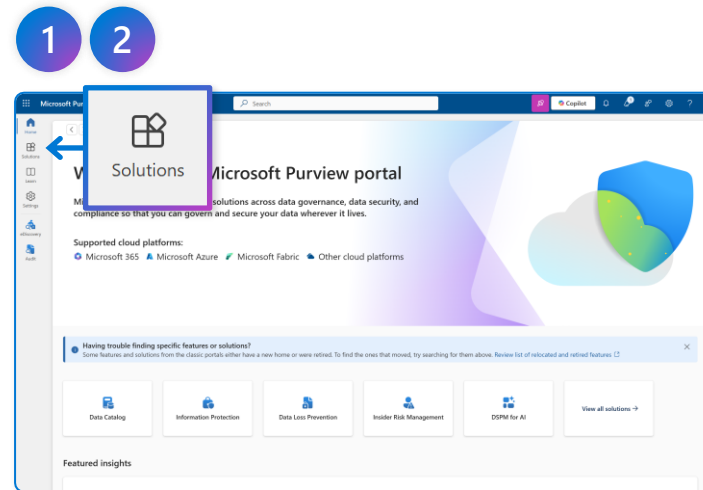
Enable audit logging

Audit logs track user and admin activity, including Copilot interactions. Even though auditing is usually turned on by default, confirming it's active ensures no gap in visibility.

Available with Business Premium or above

How to do it

- 1) Go to purview.microsoft.com
- 2) In the left-hand navigation, select **Solutions**
- 3) In the Solutions catalog, click **Audit**
- 4) If audit logging is already enabled, you will see the **Search** interface
- 5) If it's not enabled, click **Start recording user and admin activity** at the top of the page
- 6) Wait up to 60 minutes for auditing to activate



Better

Protect your sensitive information

- Create sensitivity labels
- Create sensitivity sub-labels
- Publish sensitivity labels
- Set as default label
- Enable OneDrive and SharePoint labels
- Enable Audit logging
- **Create custom sensitive info types (SIT)**
- **Configure client-side auto-labeling**

Block the sharing of sensitive information

- Create and deploy DLP policies across:
 - Exchange
 - SharePoint
 - OneDrive
 - **Teams**
 - **Endpoints**
- **Apply email protection**

Create custom sensitive info types

Custom sensitive information types (SITs) allow you to detect and classify data unique to your organization – such as internal IDs, project codes, proprietary source code – and use them in auto-labeling or DLP policies.

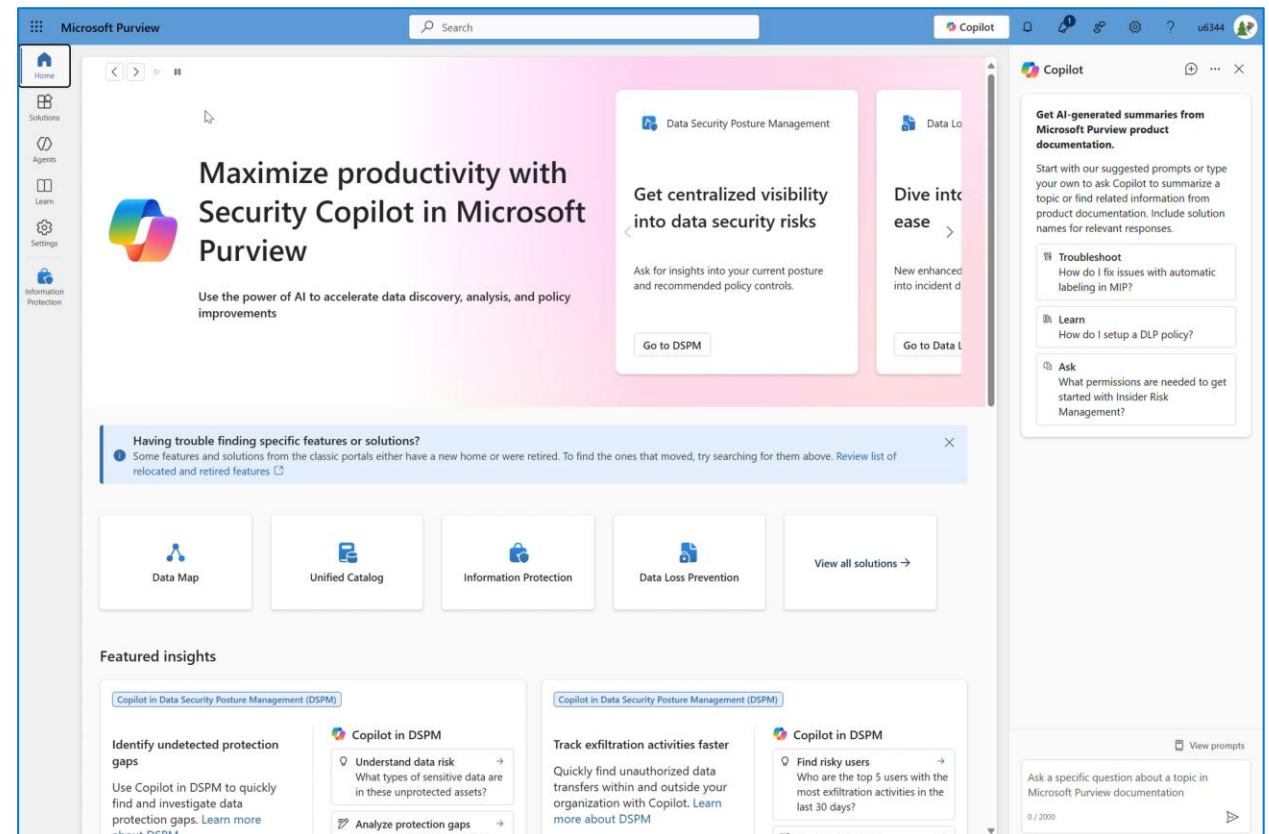
Available with IPG or above

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solution > Information protection**
- 3) Go to **Classifiers > Sensitive info types**
- 4) Click **+Create info type**
- 5) Define:
 - **Name and description**
 - **Confidence levels**
 - **Primary element:** keyword list, regex, or function
 - **Character proximity**
 - **Supporting elements** (e.g. proximity keywords)
- 6) **Save and publish**

Examples of custom sensitive info types:

Name	Pattern Type	Example match
Employee ID	Regex	EMP-123456
Internal Project Code	Keyword list	Project Falcon, Orion, Phoenix
Proprietary source code	Regex + keyword	Code snippets containing 'internal_use=true' near class or function
Credit Card Number	Function	Built-in function detects patterns like 4111 1111 1111 1111 (Visa)



Configure client-side auto-labeling

Client-side auto-labeling helps classify and protect content as users create or edit it in M365 apps like Word, Excel and Outlook. This ensures consistent labeling without relying on manual user action.

Available with IPG or above

How to do it

1) Go to purview.microsoft.com > Solutions > Information protection

2) Go to Sensitivity Labels > Select the Confidential/AllEmployees label and Edit label

3) Under Auto-labeling for files and emails > Toggle On

4) Add condition > Content contains > Add custom sensitive information types

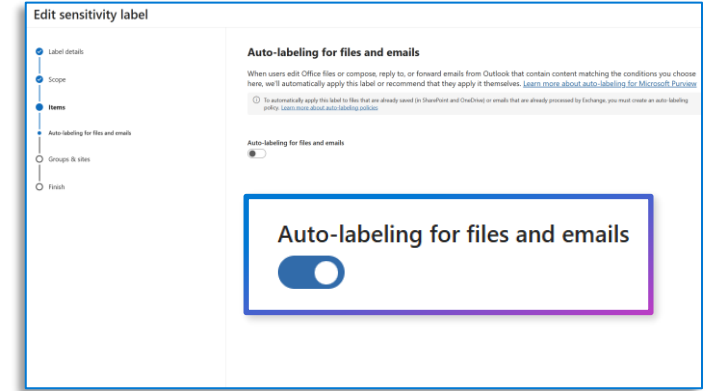
5) Change 'When content matches these conditions from Automatically apply the label > Recommend that users apply the label

6) Save label

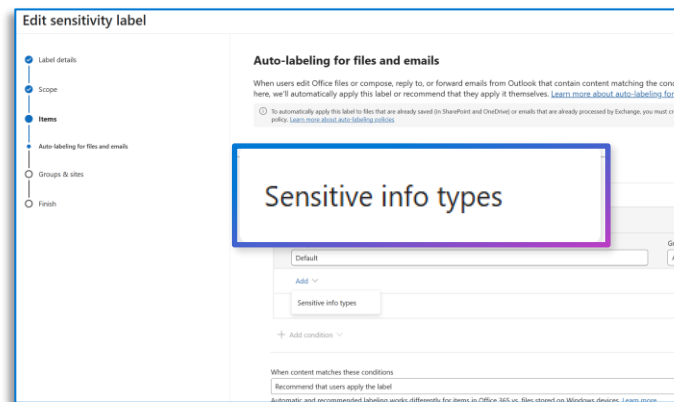
2



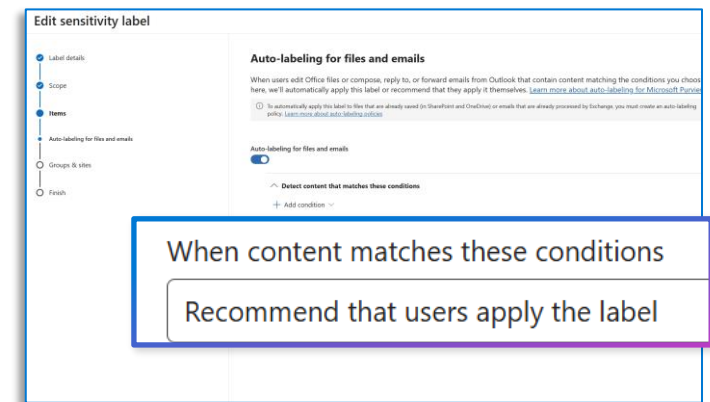
3



4



5



Create DLP policy for endpoints

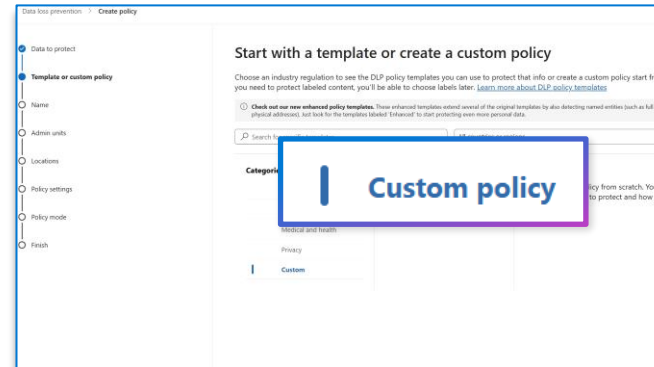
Endpoint DLP helps prevent sensitive data from being copied to USB drives, printed, or uploaded to unapproved apps. This protects data on Windows 10/11 devices enrolled with Microsoft Purview.

Available with IPG or above

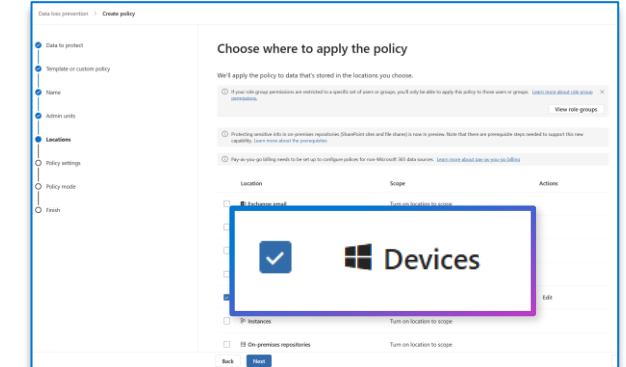
How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Data Loss Prevention**
- 3) Go to **Policies > +Create policy > Data stored in connected sources**
- 4) Choose template: **Custom policy**
- 5) Name policy and choose **devices** as the location
- 6) **Create rule** and define:
 - Conditions: content contains **custom SITs** or **Confidential/AllEmployees** sensitivity label
 - Actions: Audit or restrict activities on devices: **block copy to USB, print, clipboard or browser upload**
- 7) Run in simulation mode or turn on and **submit**

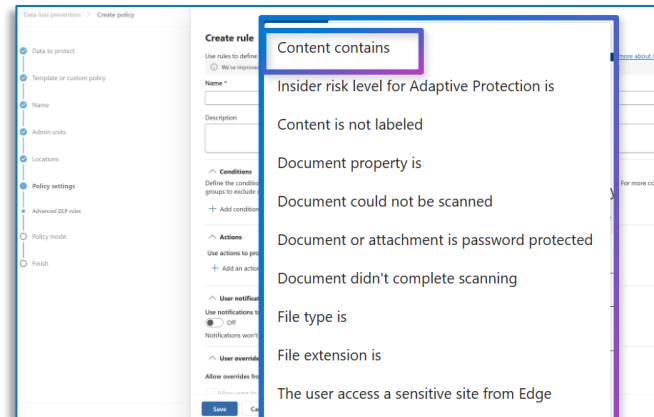
4



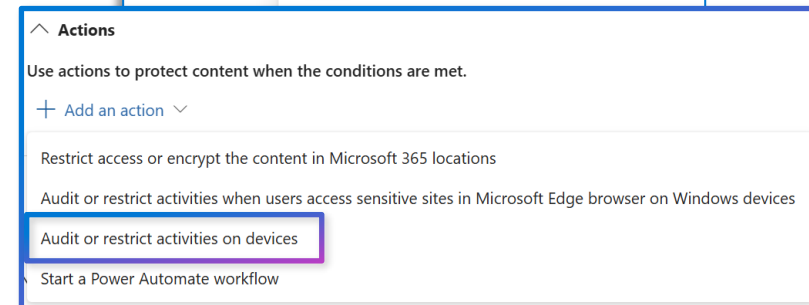
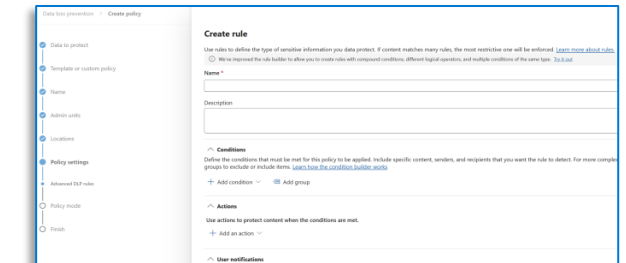
5



6



6



Create DLP policy for Teams

Prevent sensitive data from being shared in chat or channel messages with external users or guests. This protects communications and documents in Microsoft Teams environments by automatically blocking or deleting messages and restricting access to sensitive files.

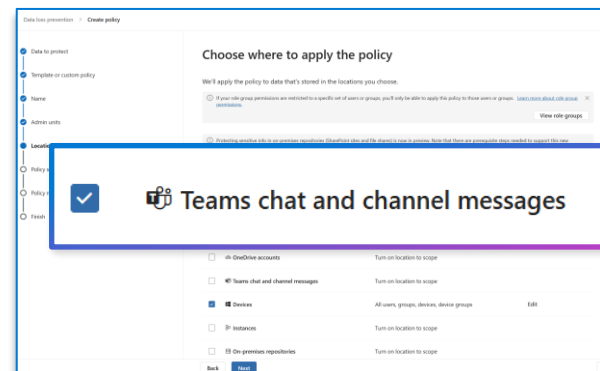
Available with IPG or above

How to do it

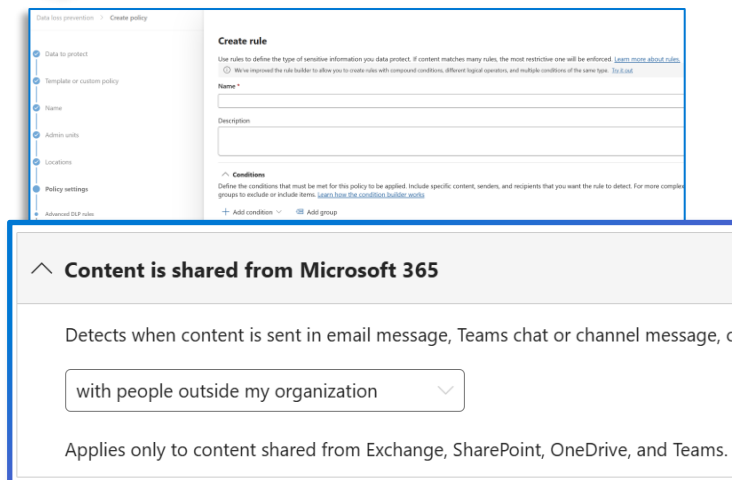
- 1) Go to purview.microsoft.com > Solutions > Data Loss Prevention
- 2) Go to Policies > +Create policy > Data stored in connected sources > Choose template: Custom policy
- 3) Name policy and choose **Teams chat and channel messages** as the location
- 4) Create rule and select **Conditions > Content contains custom SITs or Confidential/AllEmployees sensitivity label**
- 5) Add **Condition > Content is shared from M365** and select **with people outside my organization**
- 6) Add **Action > Restrict access or encrypt the content in M365 locations > Block only people outside your organization**

- 7) Run in simulation mode or turn on and **submit**

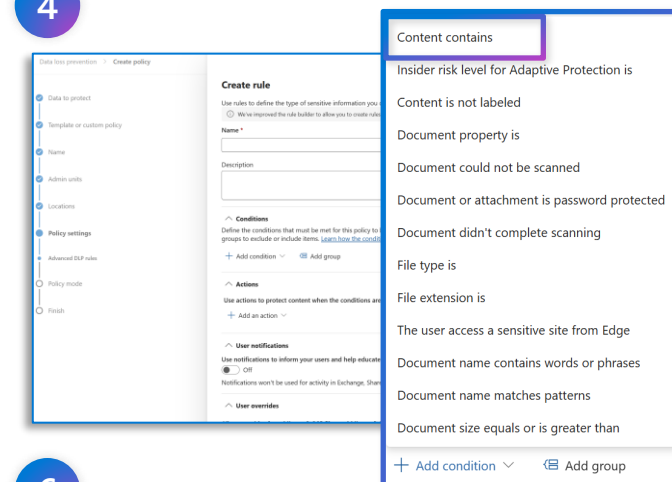
3



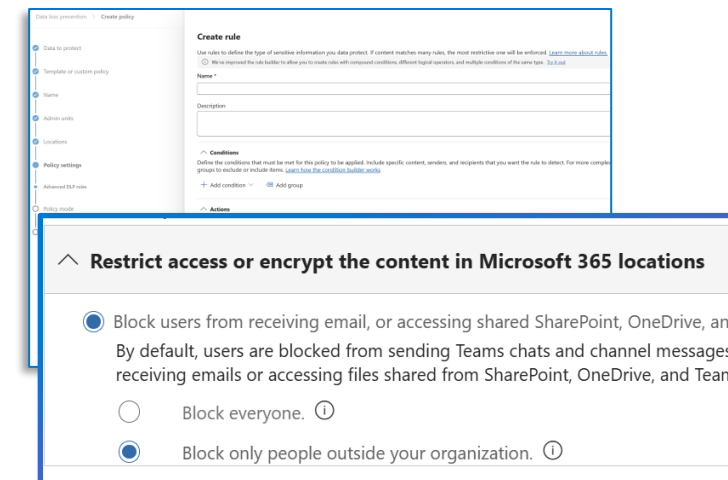
5



4



6



Apply DLP to email with custom SITs and label inheritance

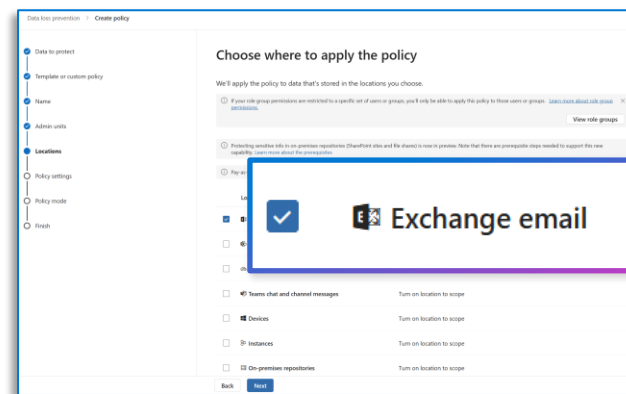
DLP can detect sensitive information in emails and attachments, block or restrict email messages, and enable email label inheritance so the email automatically adopts the most restrictive sensitivity label found on attached or linked files.

Available with IPG or above

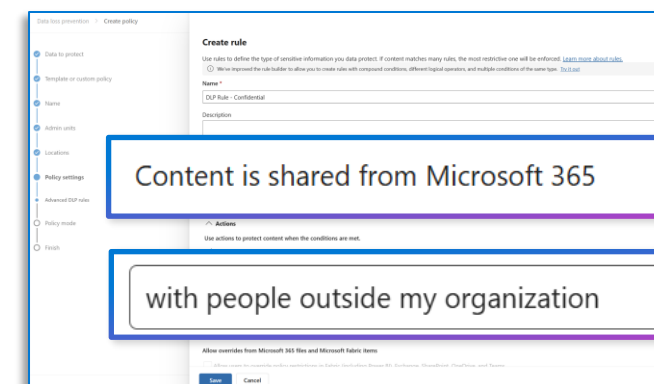
How to do it

- 1) Go to purview.microsoft.com, Solutions > Data Loss Prevention
- 2) +Create policy > Data stored in connected sources
- 3) Choose template: Custom policy and name policy
- 4) Choose **Exchange mail** as location. Best practice is to have Email be it's own DLP policy/workload
- 5) Choose conditions: **Content is shared from M365** and then select detects 'with people outside my org'
- 6) Choose conditions: **Content contains** and then add sensitivity labels All Employees
- 7) Under actions, Select **Restrict Access or encrypt the content in M365 locations**
- 8) Select Run the policy in simulation mode and click 'Turn the policy on if it's not edited within 15 days

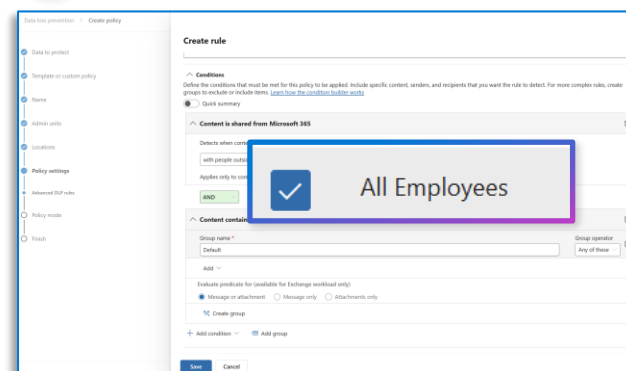
4



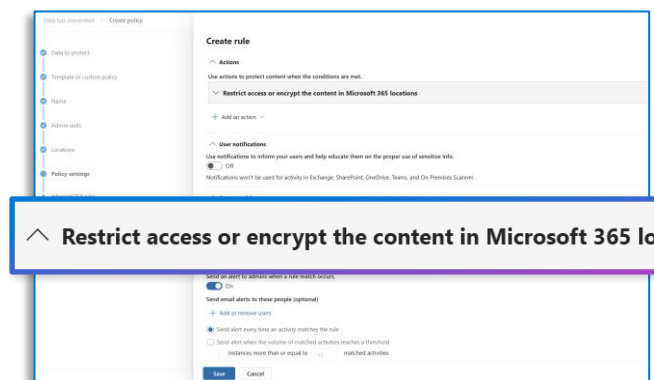
5



6



7



Best

Protect your sensitive information

- Create sensitivity labels
- Create sensitivity sub-labels
- Publish sensitivity labels
- Set as default label
- Enable OneDrive and SharePoint labels
- Enable Audit logging
- Create custom sensitive info types (SITs)
- Configure client-side auto-labeling
- **Add encryption to files**
- **Extend service-side auto-labeling**

Block the sharing of sensitive information

- Create and deploy DLP policies across:
 - Exchange
 - SharePoint
 - OneDrive
 - Teams
 - Endpoints
- Apply email protection

Detect risky activities

- **Enable Insider Risk 'Data Leaks' policy**
- **Enable Adaptive Protection for dynamic DLP policies**
- **Enable Adaptive Protection for dynamic Conditional Access policies**

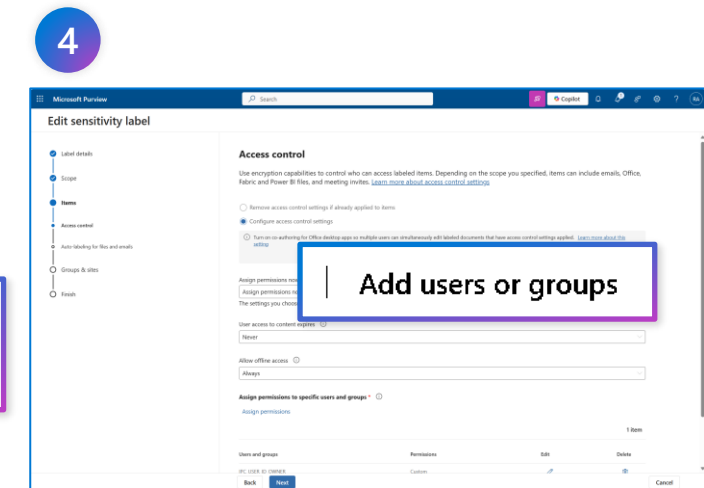
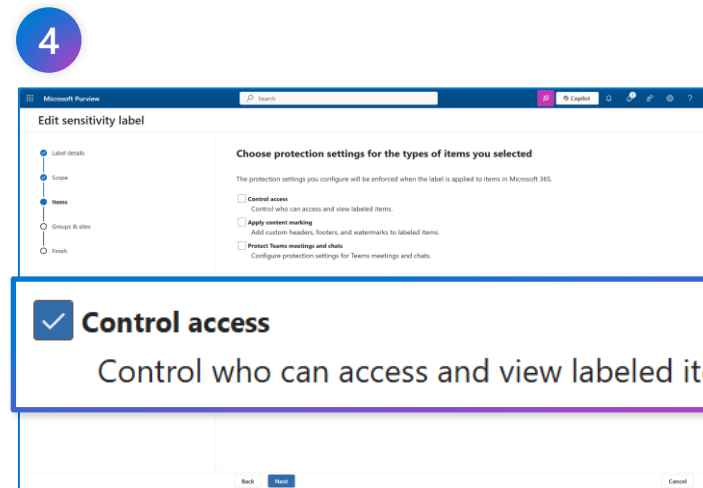
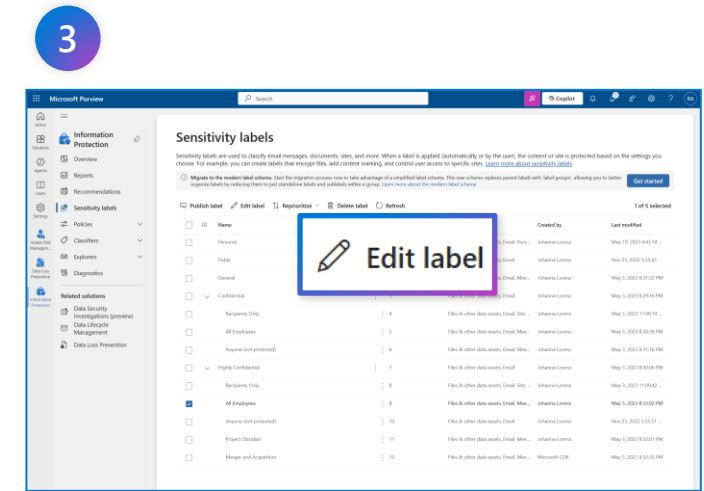
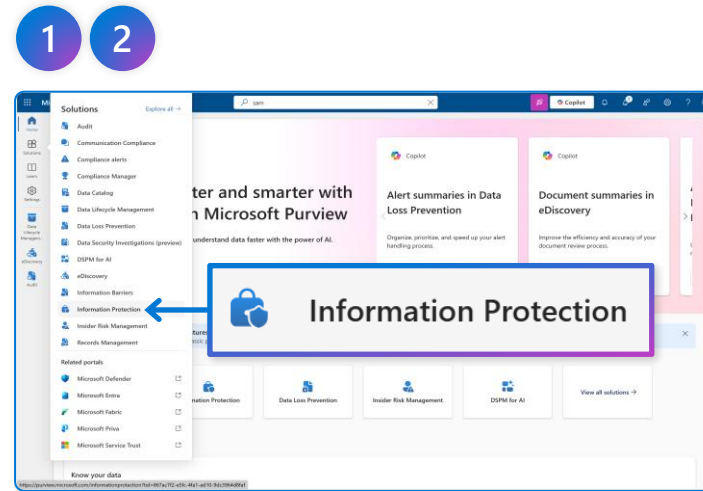
Apply encryption to labeled content

Sensitivity labels can automatically apply encryption to files that are labeled or match custom SITs. This ensures only authorized users can access the content – even if it's shared externally.

Available with IPG or above

How to do it

- 1) Go to purview.microsoft.com
- 2) Go to **Solutions > Information protection**
- 3) Select **Sensitivity labels > Choose high-sensitivity sub-labels > Edit label**
- 4) Under **items**, select **control access**:
 - Choose **Assign permissions now**
 - Set expiration, offline access
 - Assign permissions to users or groups
- 6) Save label



Extend auto-labeling to M365 services

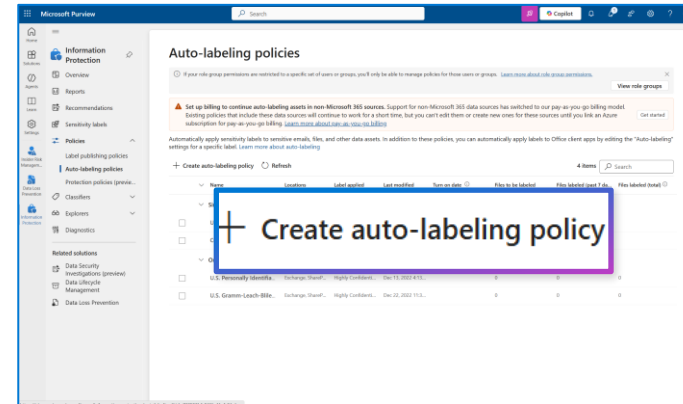
Service-side auto-labeling ensures that existing files in SharePoint and OneDrive, as well as emails in transit through Exchange, are automatically labeled based on content.

Available with IPG or above

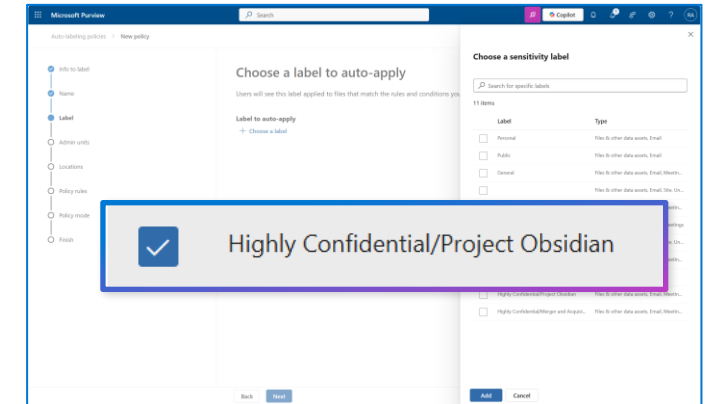
How to do it

- 1) Go to purview.microsoft.com > Solutions > Information protection
- 2) Select Policy > Auto-labeling policy > Create auto-labeling policy
- 3) Name policy and choose Label to auto-apply
- 4) Choose locations: Exchange, SharePoint, OneDrive
- 5) Define conditions:
 - Content contains: add custom SITs
- 6) Choose policy mode: Run policy in simulation mode and automatically apply after 7 day period
- 7) Review and create policy

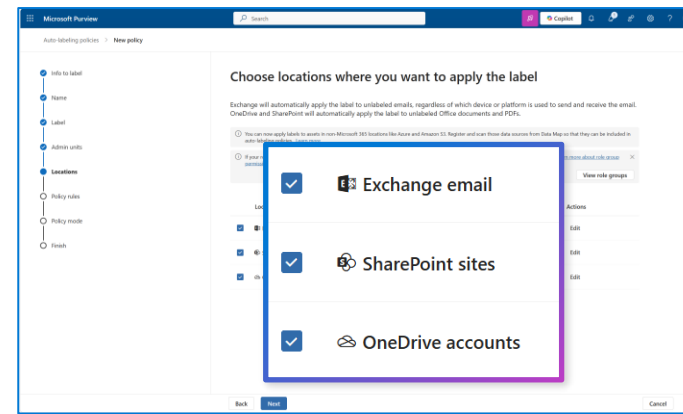
2



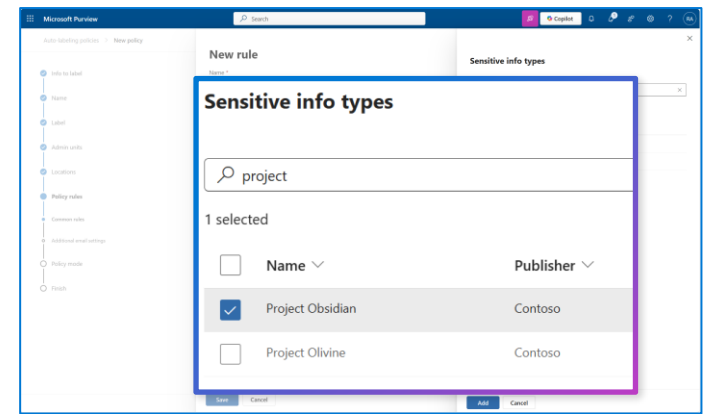
3



4



5



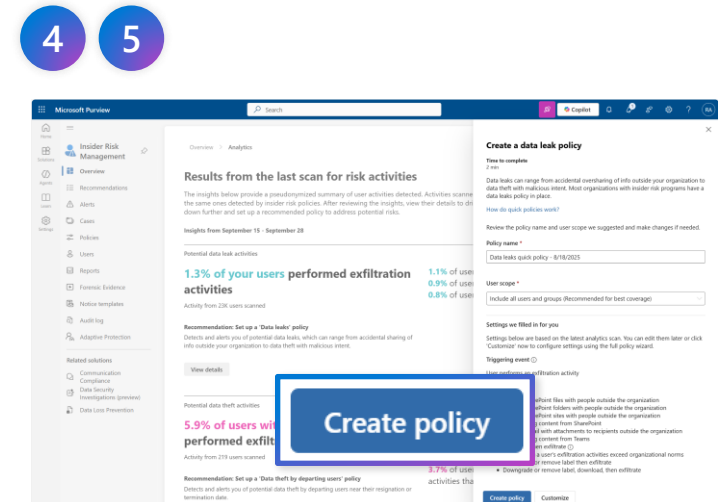
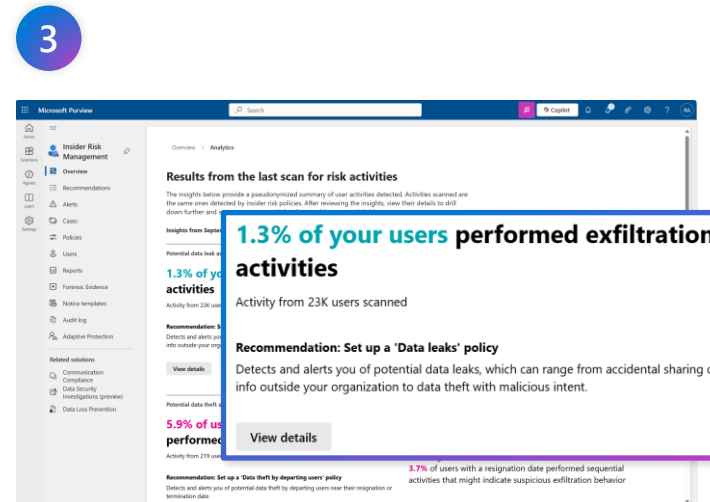
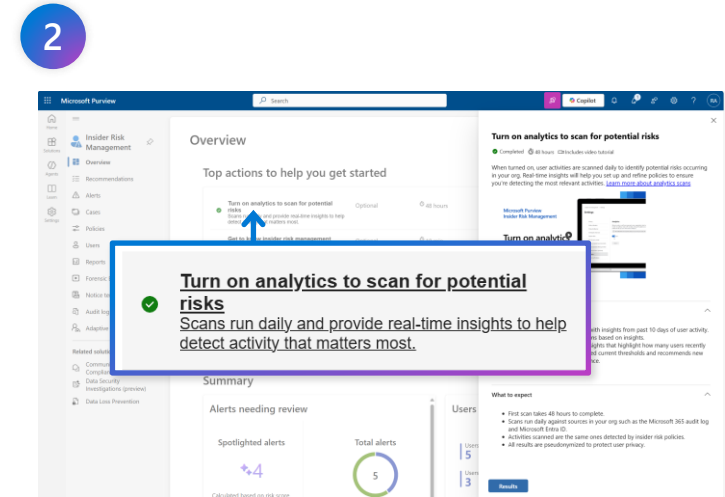
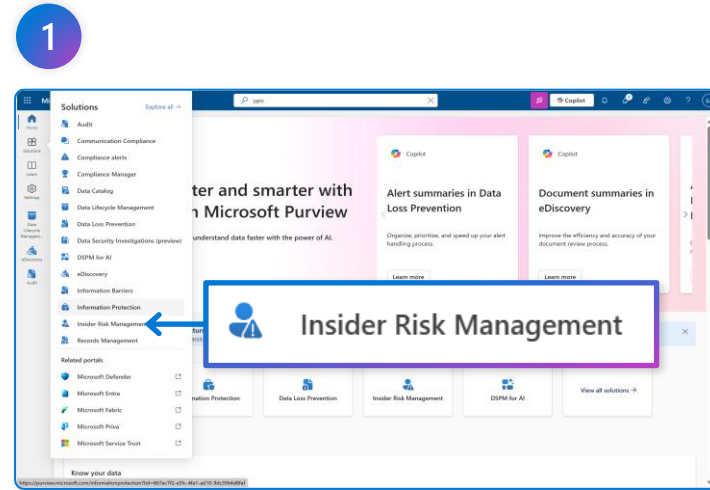
Run Insider Risk Management Analytics to identify top risks

Leverage IRM Analytics to detect risky user activities – such as data leaks, exfiltration, or policy violations – and receive recommendations using built-in templates to address these risks.

Available with E5C or above

How to do it

- 1) Go to purview.microsoft.com > Solutions > Insider Risk Management
- 2) Under Overview > Turn on analytics to scan for potential risks > 'Turn on Analytics'
- 3) Review results and click View details to get recommended policies based on your top risks.
- 4) Name your policy and define:
 - Users or groups to monitor
 - If needed, customize triggers (e.g. DLP alerts, labels changes, file downloads)
- 5) Click Create policy



Enable Adaptive Protection in DLP policies to dynamically protect data

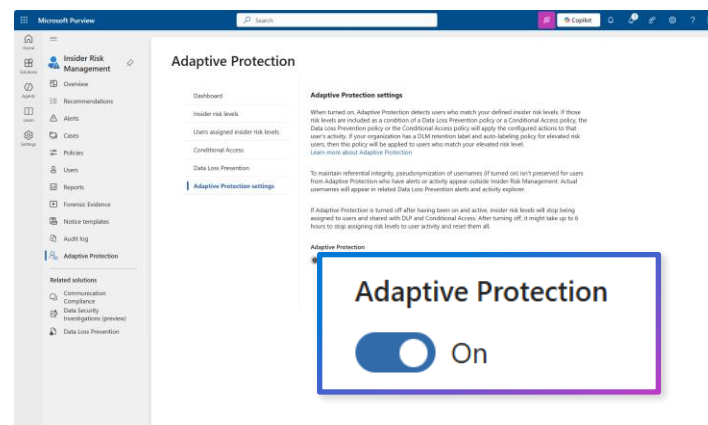
Create adaptive DLP policies to help balance data security with user productivity, by allowing low risk users to take certain actions while blocking high risk users from doing so.

Available with E5C or above

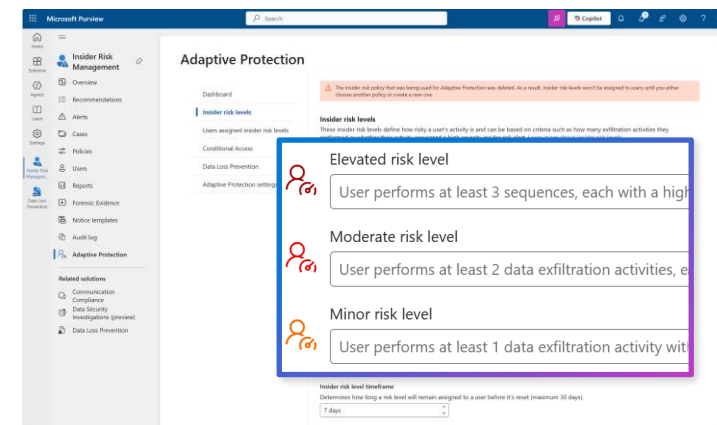
How to do it

- 1) Go to purview.microsoft.com > Solutions > Insider Risk Management
- 2) Select **Adaptive Protection** > **Adaptive Protection settings** and toggle On
- 3) Under **Insider risk levels**, Select associated **Insider risk policy** and adjust pre-configured thresholds for **Minor**, **Moderate**, **Elevated** risk to align with your risk tolerance
- 4) Now go to **Solutions** > **Data Loss Prevention** and edit a policy that you want to turn dynamic
- 5) Under **Policy settings** > **Create rule** > **Add condition** > select **Insider risk level for Adaptive Protection** is and select **Elevated** risk level
- 6) Edit **Actions** to **Block** file activities for elevated risk users

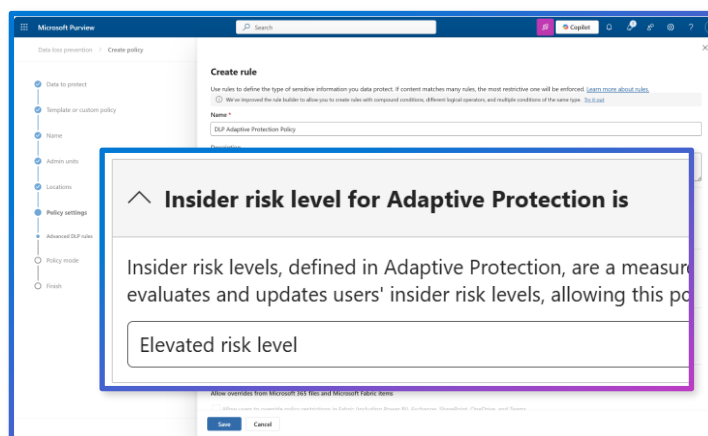
1



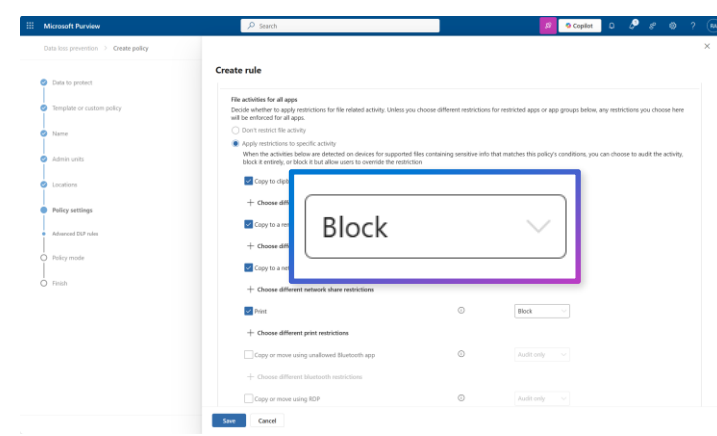
2



3



2



Enable Adaptive Protection for dynamic Conditional Access policy

Create adaptive policies so that when a user is flagged as high risk, Conditional Access policies can dynamically restrict access to sensitive SharePoint sites and OneDrive content.

Available with E5C or above

How to do it

- 1) Go to purview.microsoft.com > Solutions > Insider Risk Management
- 2) Go to Adaptive Protection > and select Conditional Access
- 3) Select Create Policy which will redirect you to create a Conditional Access policy in Entra admin center
- 4) Select condition Insider risk > and Toggle On
- 5) Select Target resources> and select SharePoint and OneDrive
- 6) Under Access controls, select Block access
- 7) Enable policy and select Report-only or On and Save

2 **3**

4

5 **6**

7

Conditional Access

+ Create policy

Insider risk

Control access for users who are assigned specific risk levels from Adaptive Protection, a Microsoft Purview Insider Risk Management feature. Insider risk levels are determined based on a user's risky data related activities. [Learn more](#)

Configure ☒ Yes ☐ No

Select the risk levels that must be assigned to enforce the policy

☒ Elevated ☐ Moderate ☐ Minor

Target resources

1 app included

Access controls

Grant ☐ Block access

Enable policy

Report-only On Off

Save