Zero to Hero: Adaptive Protection with Insider Risk Management and Conditional Access

EWELINA PACZKOWSKA

Solution Architect at Threatscape

Co-organiser of M365 Security & Compliance User Group
www.meetup.com/m365sandcug

Ewelina Paczkowska

@/ewelinapaczkowska

www.welkasworld.com

@WelkasWorld

@WelkasWorld

@WelkasWorld.com

Insider Risk Management

Definition

Compliance solution that helps organisations detect and mitigate insider threats, such as data leaks and IP theft.

Conditional Access

Definition

Zero Trust policy engine that uses signals to make decisions and enforce organisational policies. It is based on if-then statements; if a user wants to access a resource, then they must complete an action.

Adaptive Protection

Definition

Adaptive protection uses machine learning to identify critical risks and proactively and automatically apply protection controls from Data Loss Prevention (DLP), Data Lifecycle Management (DLM), and Conditional Access (CA).

Minor Risk

- No risky activity

✅ No additional controls

Moderate Risk

- Resigns
- Works on sensitive project
- No risky activity

⛔ BYOD and USB blocked
📄 Require terms of use

High Risk

- Resigns
- Works on sensitive project
- Risky activities detected

✋ Revoke access pending review

Process flow

1. Configure global Insider Risk settings

2. Create/ edit Insider Risk Management policy

3. Configure insider risk level settings

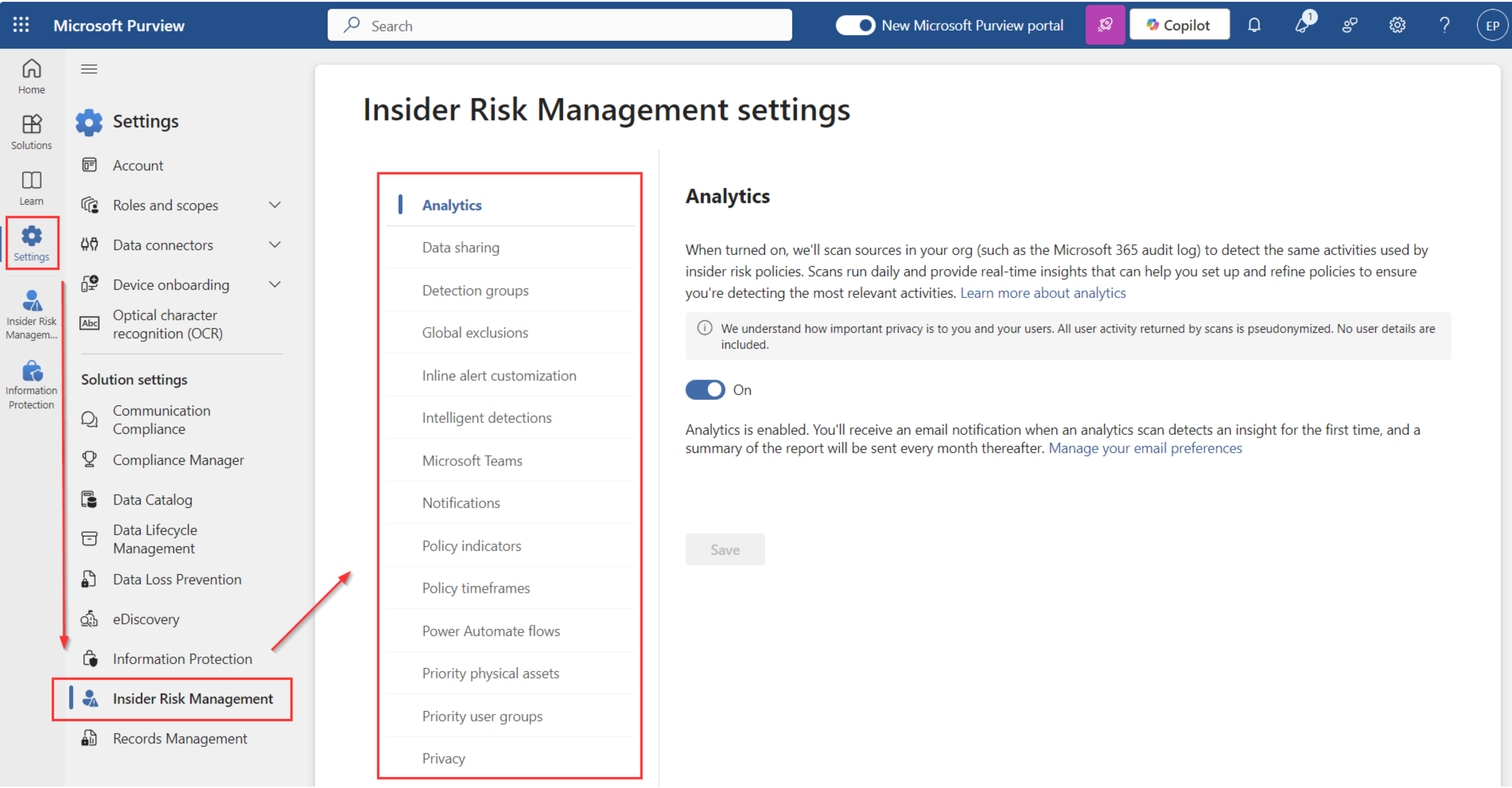
4. Customise an insider risk level for your policy

5. Create/ edit a Conditional Access policy

6. Turn on Adaptive Protection

Step 1

1. Configure global Insider Risk settings
2. Create/ edit Insider Risk Management policy
3. Configure insider risk level settings
4. Customise an insider risk level for your policy
5. Create/ edit a Conditional Access policy
6. Turn on Adaptive Protection



Insider Risk Management settings

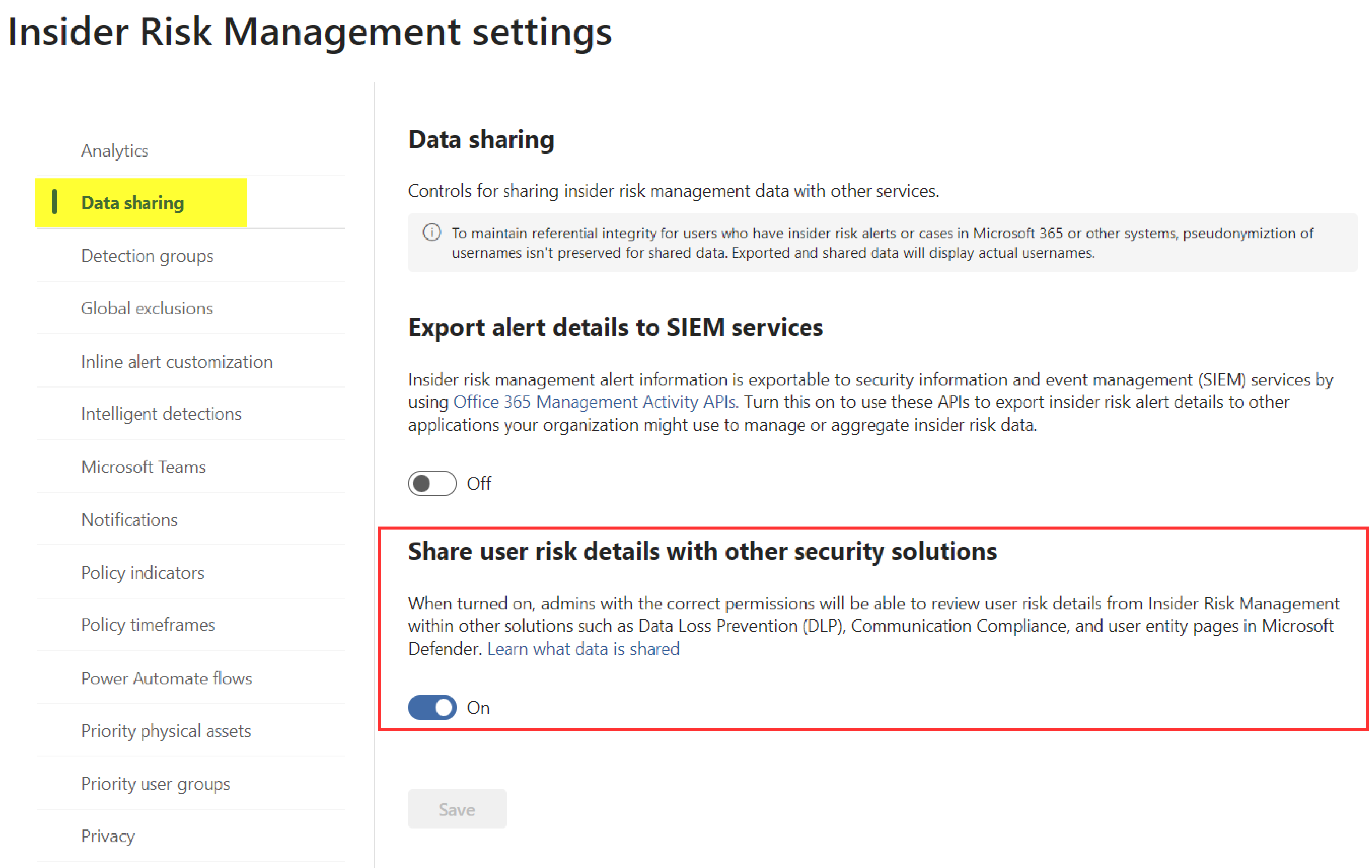
Analytics

When turned on, we'll scan sources in your org (such as the Microsoft 365 audit log) to detect the same activities used by insider risk policies. Scans run daily and provide real-time insights that can help you set up and refine policies to ensure you're detecting the most relevant activities. Learn more about analytics

ⓘ We understand how important privacy is to you and your users. All user activity returned by scans is pseudonymized. No user details are included.

● On

Analytics is enabled. You'll receive an email notification when an analytics scan detects an insight for the first time, and a summary of the report will be sent every month thereafter. Manage your email preferences



Insider Risk Management settings

Data sharing

Controls for sharing insider risk management data with other services.

ⓘ To maintain referential integrity for users who have insider risk alerts or cases in Microsoft 365 or other systems, pseudonymiztion of usernames isn't preserved for shared data. Exported and shared data will display actual usernames.

Export alert details to SIEM services

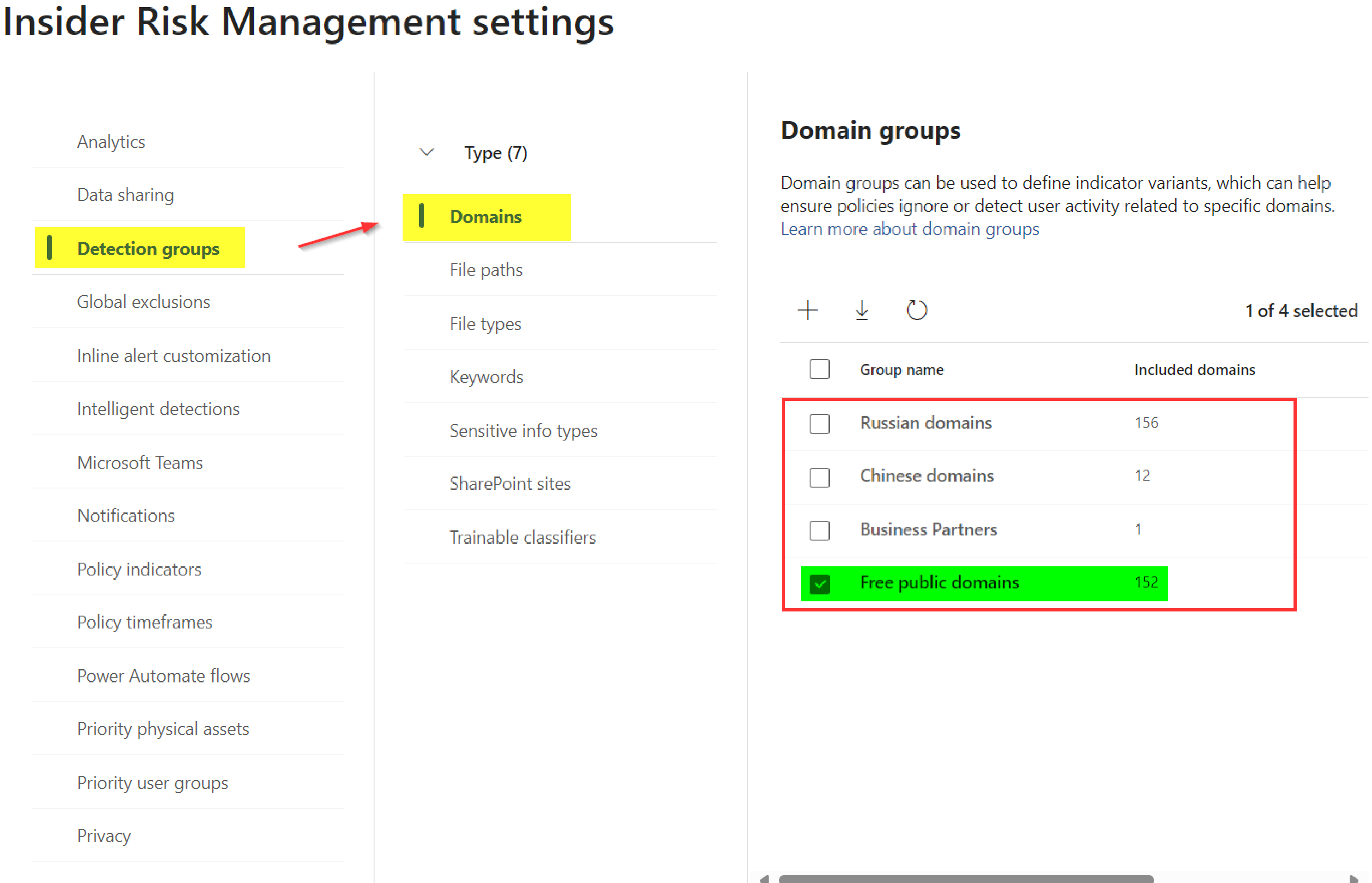
Insider risk management alert information is exportable to security information and event management (SIEM) services by using Office 365 Management Activity APIs. Turn this on to use these APIs to export insider risk alert details to other applications your organization might use to manage or aggregate insider risk data.

○ Off

Share user risk details with other security solutions

When turned on, admins with the correct permissions will be able to review user risk details from Insider Risk Management within other solutions such as Data Loss Prevention (DLP), Communication Compliance, and user entity pages in Microsoft Defender. Learn what data is shared

● On



Insider Risk Management settings

- Analytics
- Data sharing
- **Detection groups**
- Global exclusions
- Inline alert customization
- Intelligent detections
- Microsoft Teams
- Notifications
- Policy indicators
- Policy timeframes
- Power Automate flows
- Priority physical assets
- Priority user groups
- Privacy

Type (7)

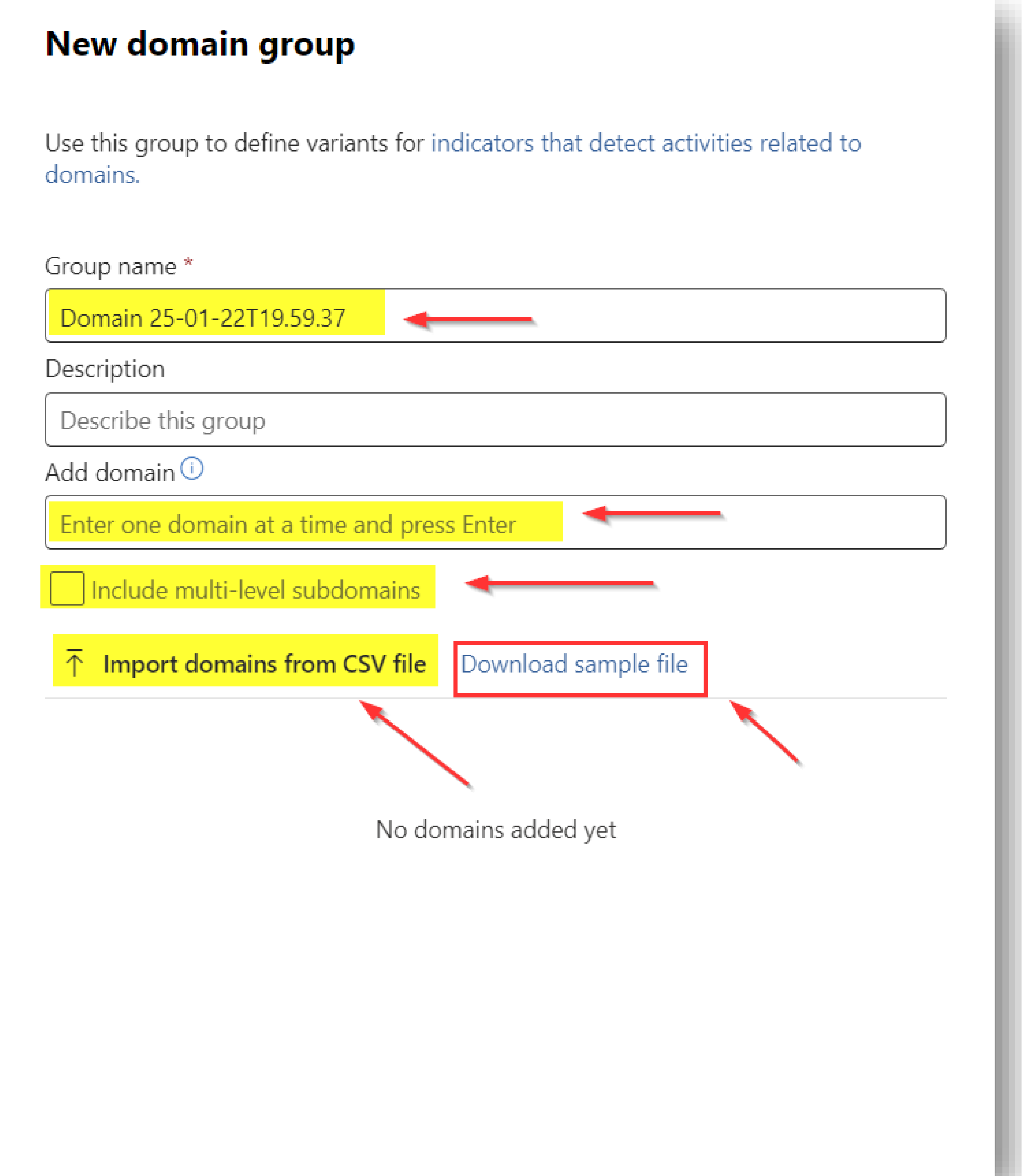
- **Domains**
- File paths
- File types
- Keywords
- Sensitive info types
- SharePoint sites
- Trainable classifiers

Domain groups

Domain groups can be used to define indicator variants, which can help ensure policies ignore or detect user activity related to specific domains. Learn more about domain groups

1 of 4 selected

□	Group name	Included domains
□	Russian domains	156
□	Chinese domains	12
□	Business Partners	1
☑	Free public domains	152



New domain group

Use this group to define variants for indicators that detect activities related to domains.

Group name *

Domain 25-01-22T19.59.37

Description

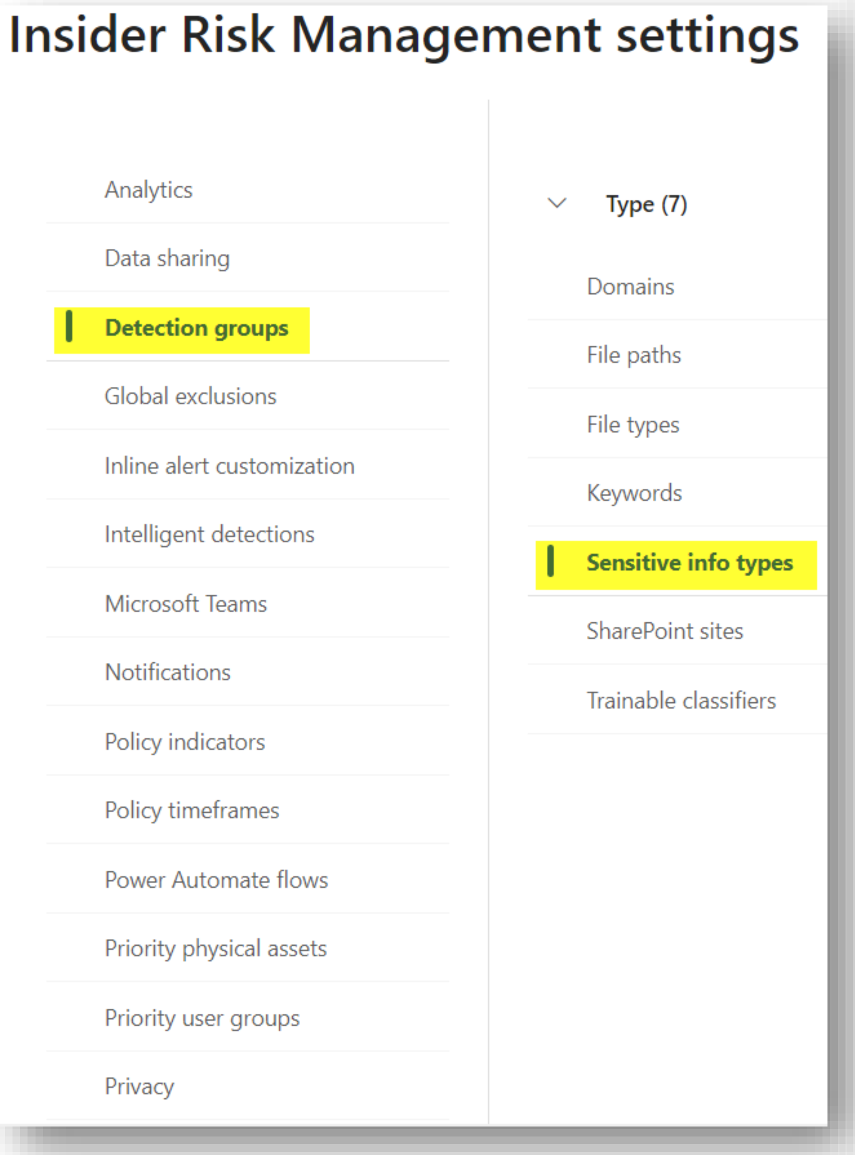
Describe this group

Add domain ⓘ

Enter one domain at a time and press Enter

□ Include multi-level subdomains

No domains added yet

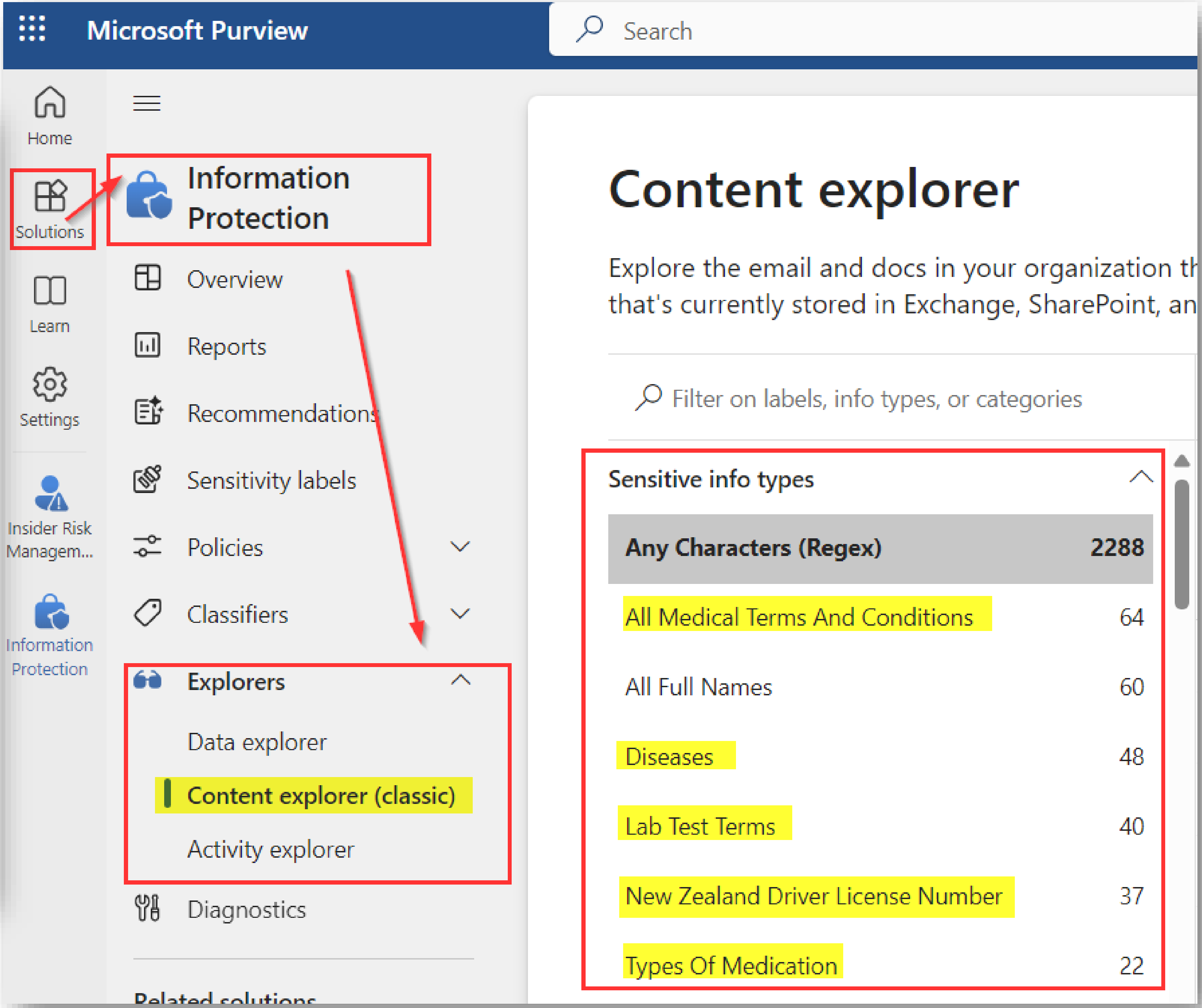


Insider Risk Management settings

- Analytics
- Data sharing
- **Detection groups**
- Global exclusions
- Inline alert customization
- Intelligent detections
- Microsoft Teams
- Notifications
- Policy indicators
- Policy timeframes
- Power Automate flows
- Priority physical assets
- Priority user groups
- Privacy

Type (7)

- Domains
- File paths
- File types
- Keywords
- **Sensitive info types**
- SharePoint sites
- Trainable classifiers



Microsoft Purview

Search

Home
Solutions
Learn
Settings
Insider Risk Managem...
Information Protection

Information Protection

- Overview
- Reports
- Recommendations
- Sensitivity labels
- Policies
- Classifiers
- Explorers
  - Data explorer
  - **Content explorer (classic)**
  - Activity explorer
- Diagnostics

Related solutions

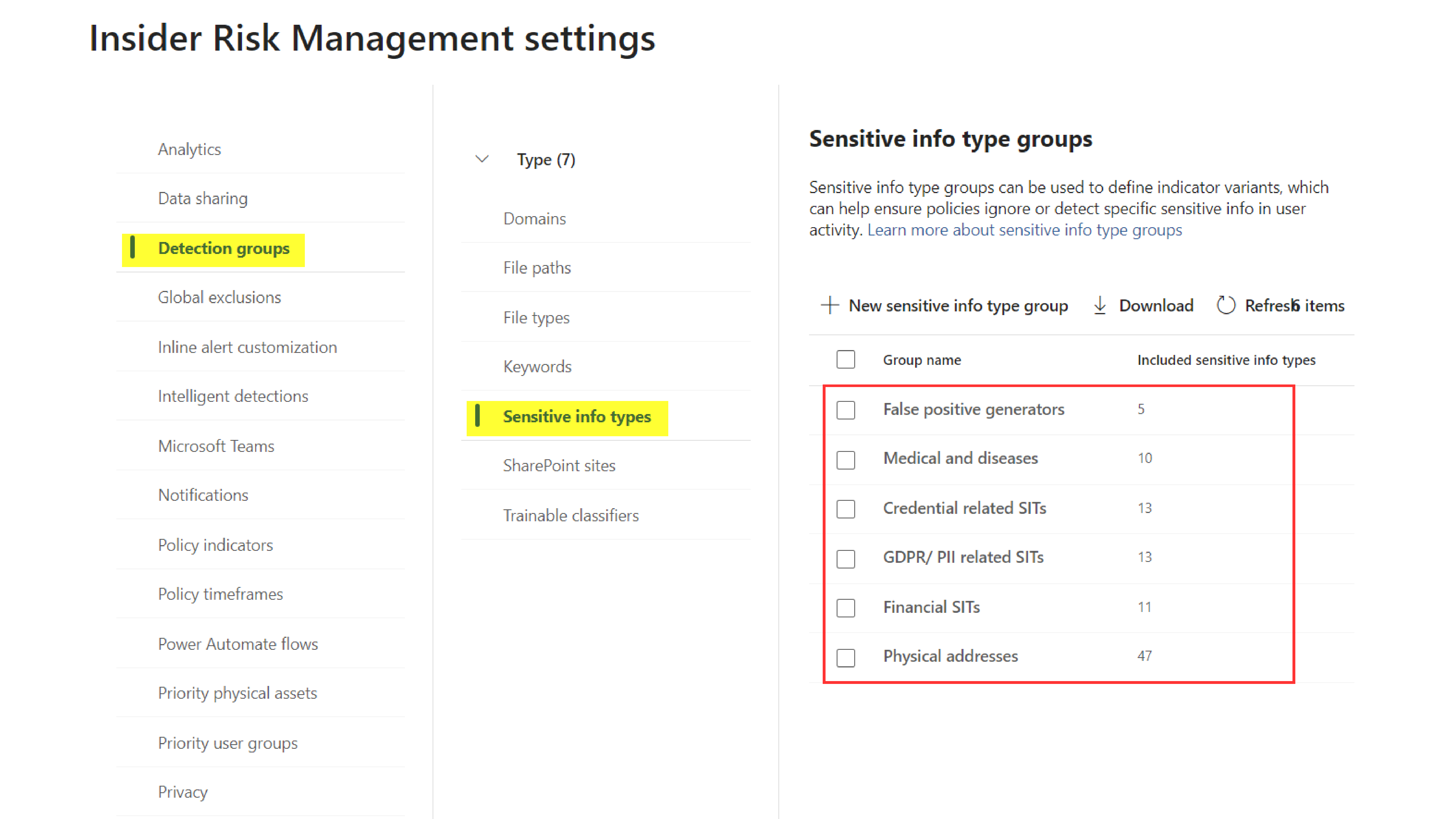
Content explorer

Explore the email and docs in your organization th that's currently stored in Exchange, SharePoint, an

Filter on labels, info types, or categories

Sensitive info types

Any Characters (Regex)	**2288**
All Medical Terms And Conditions	64
All Full Names	60
Diseases	48
Lab Test Terms	40
New Zealand Driver License Number	37
Types Of Medication	22

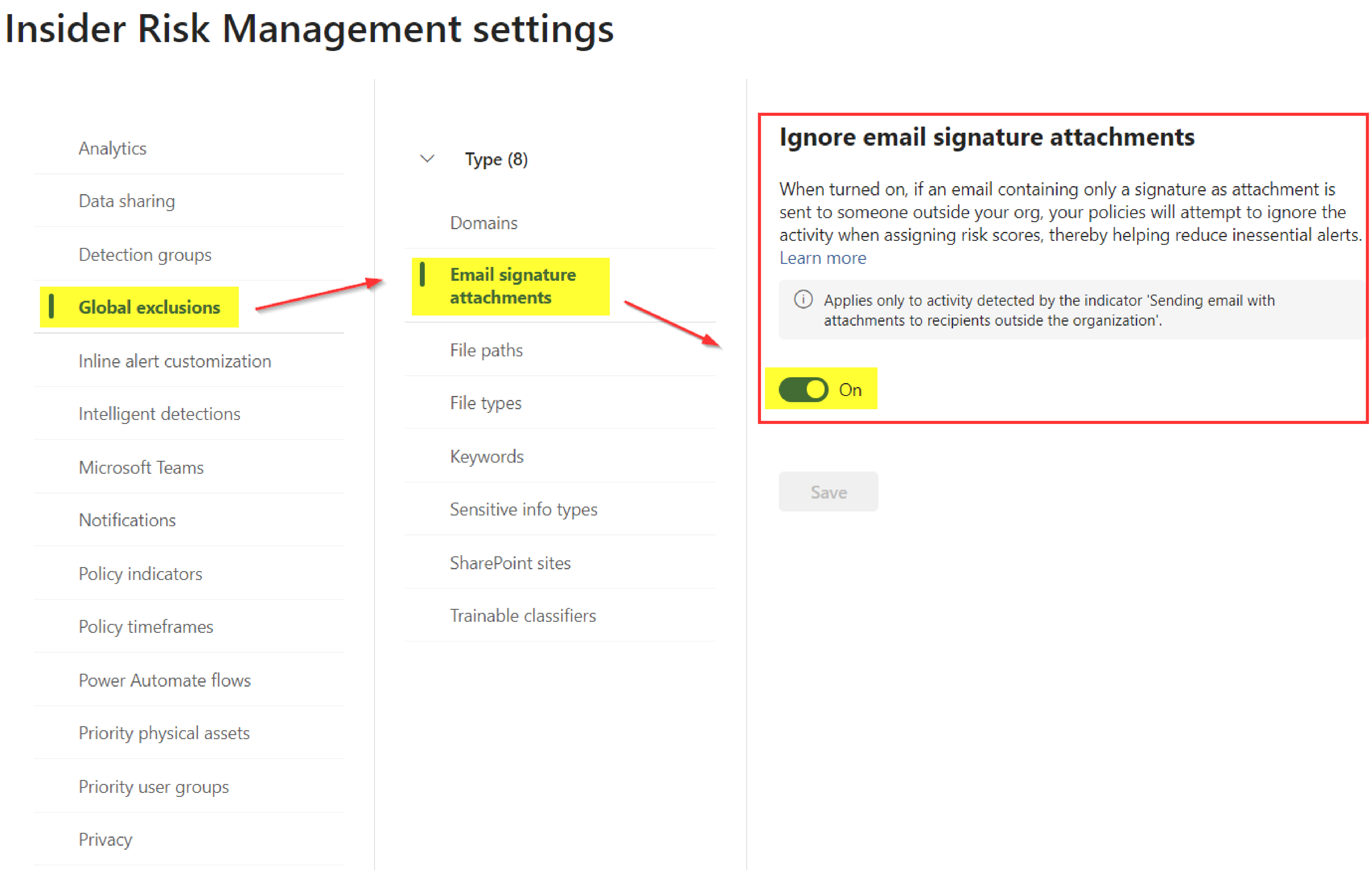


Insider Risk Management settings

Sensitive info type groups

Sensitive info type groups can be used to define indicator variants, which can help ensure policies ignore or detect specific sensitive info in user activity. Learn more about sensitive info type groups

□	Group name	Included sensitive info types
□	False positive generators	5
□	Medical and diseases	10
□	Credential related SITs	13
□	GDPR/ PII related SITs	13
□	Financial SITs	11
□	Physical addresses	47



Insider Risk Management settings

- Analytics
- Data sharing
- Detection groups
- **Global exclusions**
- Inline alert customization
- Intelligent detections
- Microsoft Teams
- Notifications
- Policy indicators
- Policy timeframes
- Power Automate flows
- Priority physical assets
- Priority user groups
- Privacy

Type (8)

- Domains
- **Email signature attachments**
- File paths
- File types
- Keywords
- Sensitive info types
- SharePoint sites
- Trainable classifiers

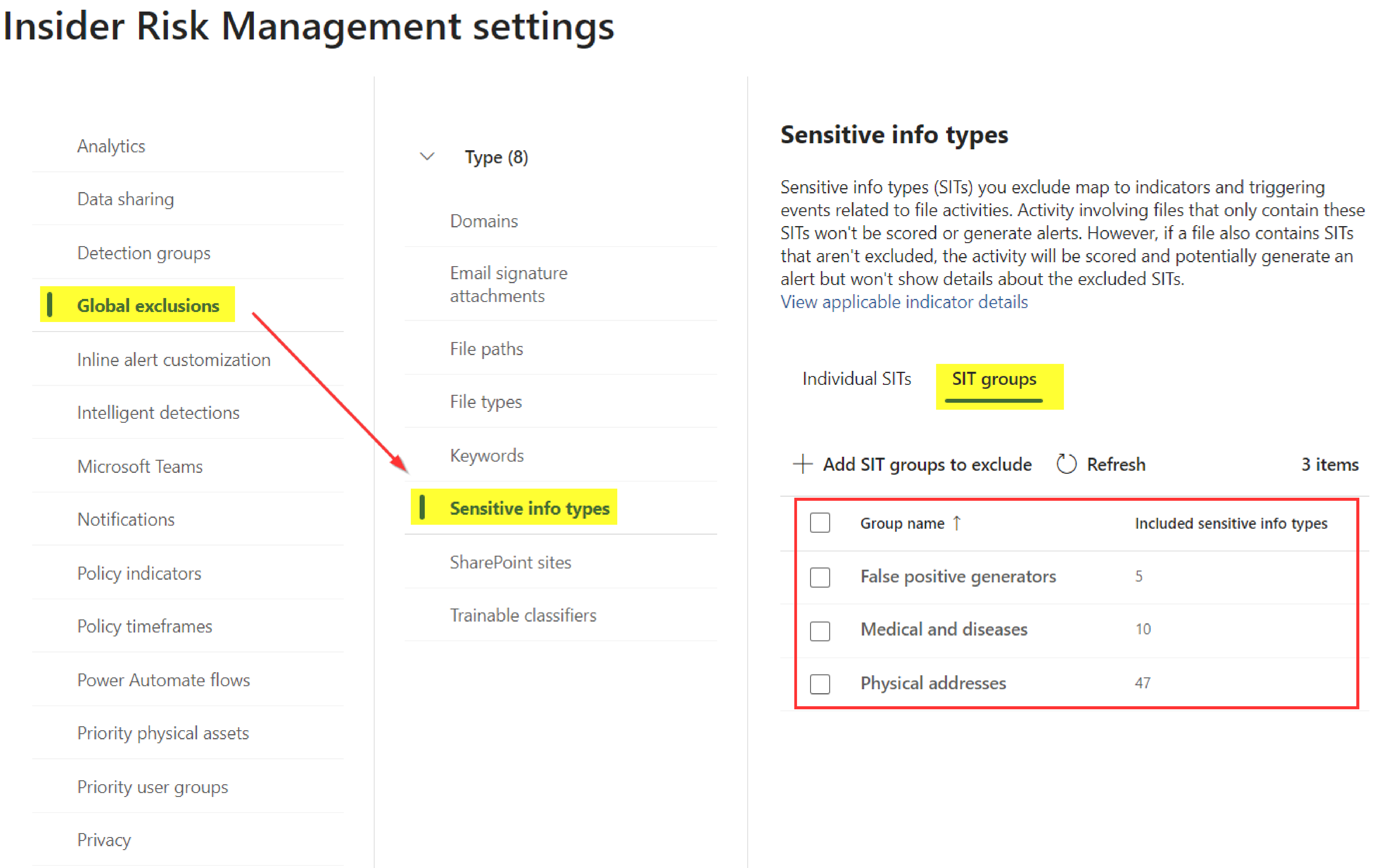
Ignore email signature attachments

When turned on, if an email containing only a signature as attachment is sent to someone outside your org, your policies will attempt to ignore the activity when assigning risk scores, thereby helping reduce inessential alerts. Learn more

ⓘ Applies only to activity detected by the indicator 'Sending email with attachments to recipients outside the organization'.

● On

Save



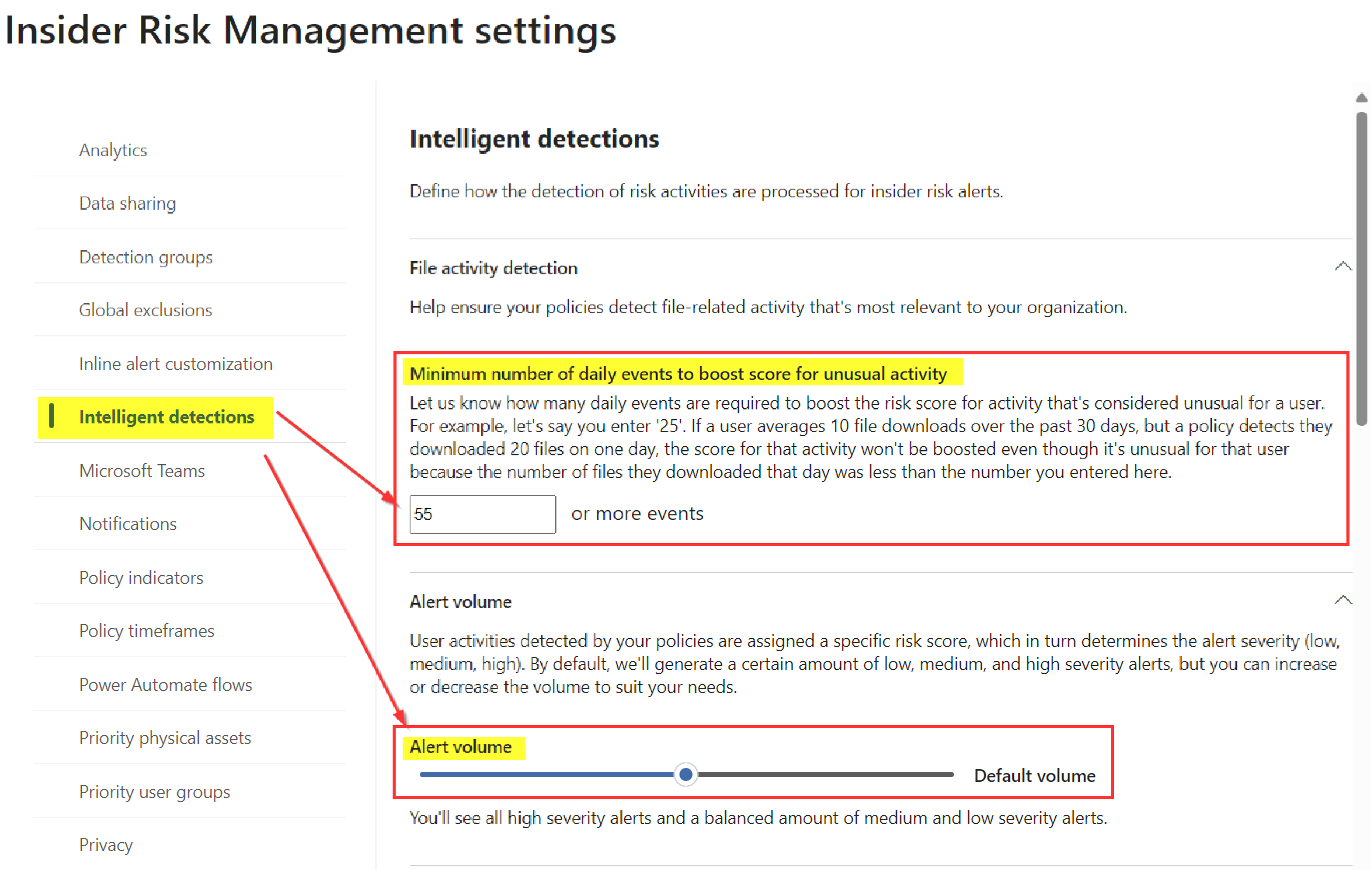
Insider Risk Management settings

Sensitive info types

Sensitive info types (SITs) you exclude map to indicators and triggering events related to file activities. Activity involving files that only contain these SITs won't be scored or generate alerts. However, if a file also contains SITs that aren't excluded, the activity will be scored and potentially generate an alert but won't show details about the excluded SITs.

View applicable indicator details

□	Group name ↑	Included sensitive info types
□	False positive generators	5
□	Medical and diseases	10
□	Physical addresses	47



Insider Risk Management settings

Intelligent detections

Define how the detection of risk activities are processed for insider risk alerts.

File activity detection

Help ensure your policies detect file-related activity that's most relevant to your organization.

Minimum number of daily events to boost score for unusual activity

Let us know how many daily events are required to boost the risk score for activity that's considered unusual for a user. For example, let's say you enter '25'. If a user averages 10 file downloads over the past 30 days, but a policy detects they downloaded 20 files on one day, the score for that activity won't be boosted even though it's unusual for that user because the number of files they downloaded that day was less than the number you entered here.

55 or more events

Alert volume

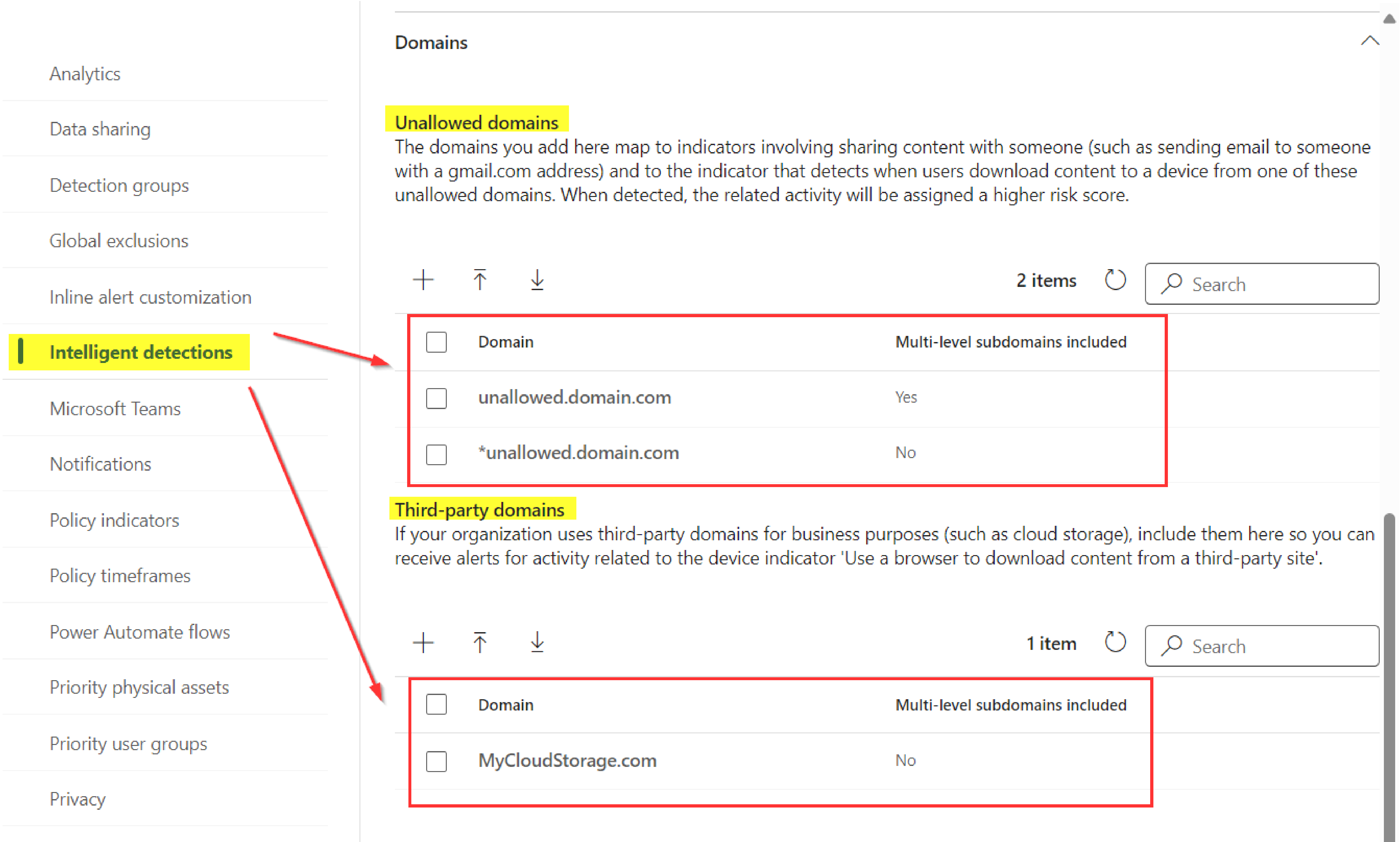
User activities detected by your policies are assigned a specific risk score, which in turn determines the alert severity (low, medium, high). By default, we'll generate a certain amount of low, medium, and high severity alerts, but you can increase or decrease the volume to suit your needs.

Alert volume

Default volume

You'll see all high severity alerts and a balanced amount of medium and low severity alerts.

Insider Risk Management settings



Domains

Unallowed domains

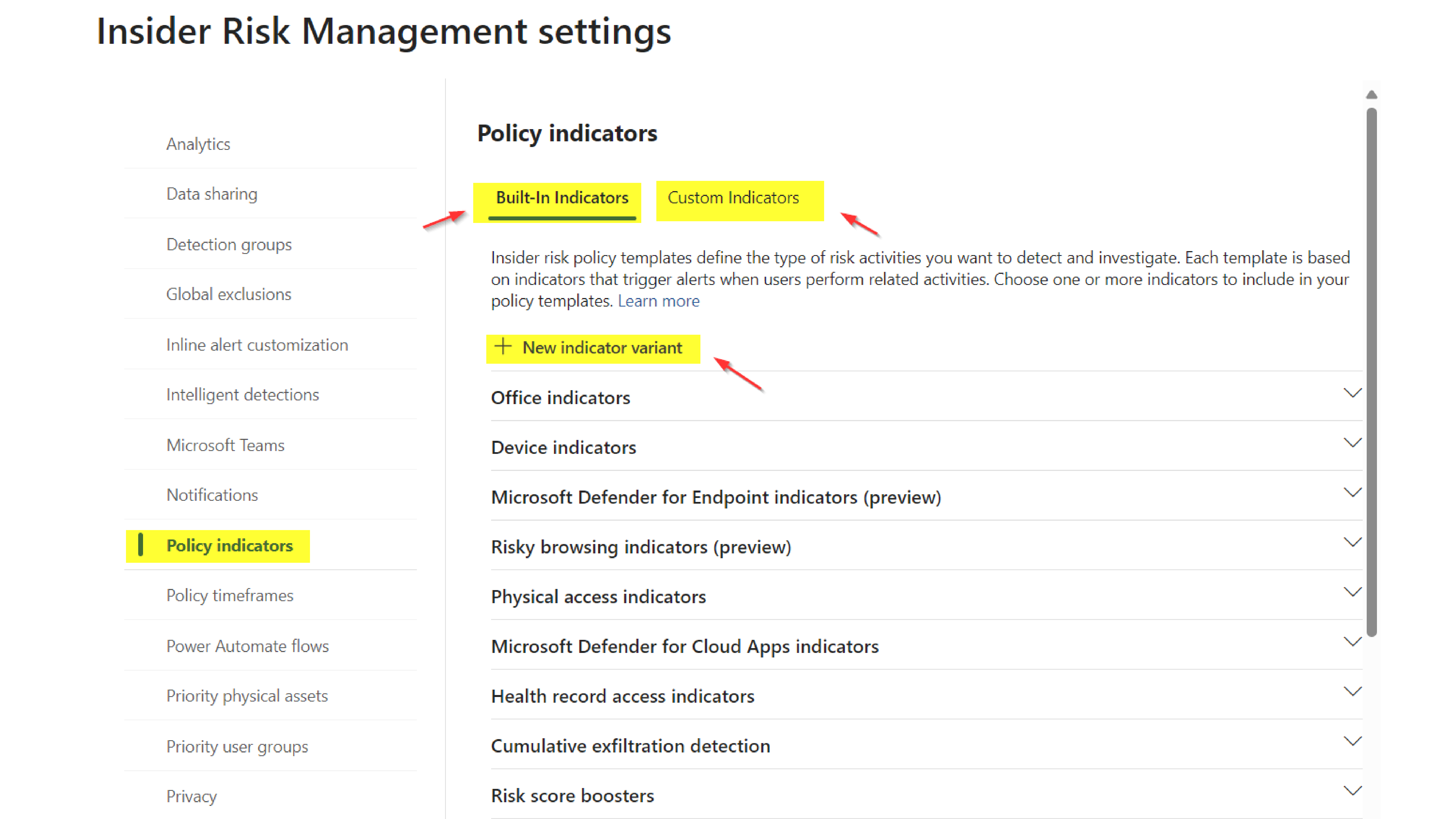
The domains you add here map to indicators involving sharing content with someone (such as sending email to someone with a gmail.com address) and to the indicator that detects when users download content to a device from one of these unallowed domains. When detected, the related activity will be assigned a higher risk score.

□	Domain	Multi-level subdomains included
□	unallowed.domain.com	Yes
□	*unallowed.domain.com	No

Third-party domains

If your organization uses third-party domains for business purposes (such as cloud storage), include them here so you can receive alerts for activity related to the device indicator 'Use a browser to download content from a third-party site'.

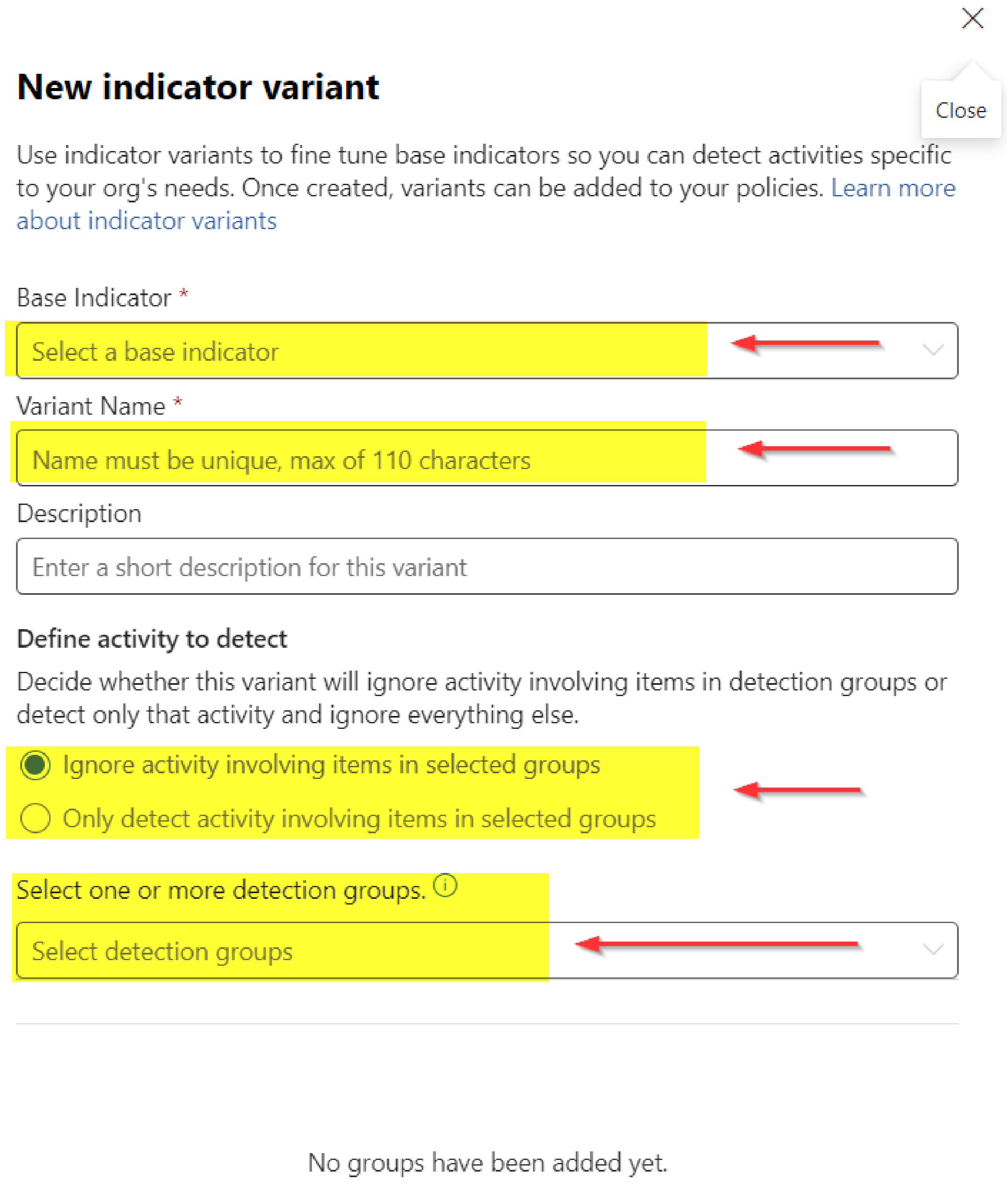
□	Domain	Multi-level subdomains included
□	MyCloudStorage.com	No



Insider Risk Management settings

Policy indicators

Insider risk policy templates define the type of risk activities you want to detect and investigate. Each template is based on indicators that trigger alerts when users perform related activities. Choose one or more indicators to include in your policy templates. Learn more



New indicator variant

Use indicator variants to fine tune base indicators so you can detect activities specific to your org's needs. Once created, variants can be added to your policies. Learn more about indicator variants

Base Indicator *

Select a base indicator

Variant Name *

Name must be unique, max of 110 characters

Description

Enter a short description for this variant

Define activity to detect

Decide whether this variant will ignore activity involving items in detection groups or detect only that activity and ignore everything else.

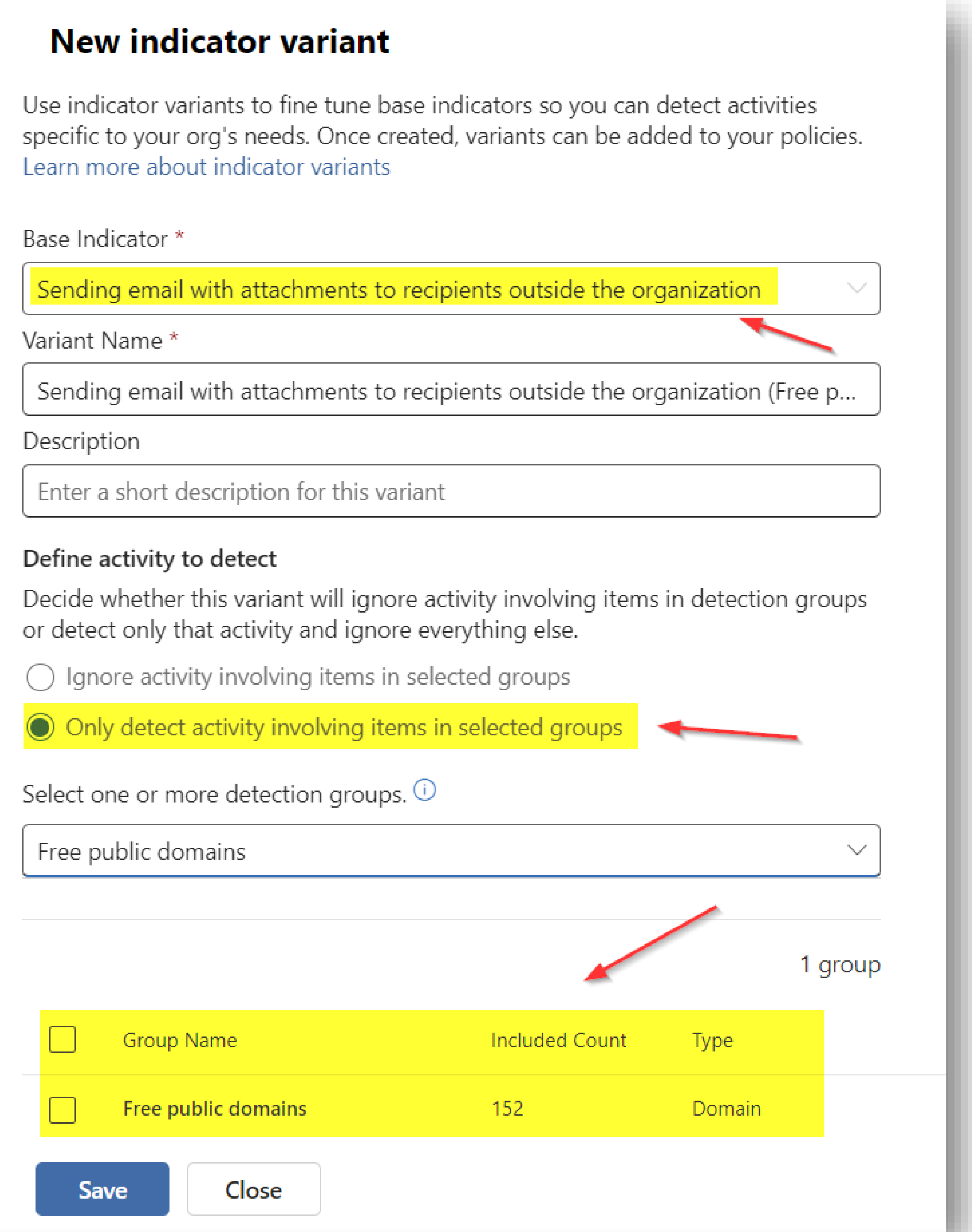
● Ignore activity involving items in selected groups

○ Only detect activity involving items in selected groups

Select one or more detection groups. ⓘ

Select detection groups

No groups have been added yet.



New indicator variant

Use indicator variants to fine tune base indicators so you can detect activities specific to your org's needs. Once created, variants can be added to your policies.
Learn more about indicator variants

Base Indicator *

Sending email with attachments to recipients outside the organization

Variant Name *

Sending email with attachments to recipients outside the organization (Free p...

Description

Enter a short description for this variant

Define activity to detect

Decide whether this variant will ignore activity involving items in detection groups or detect only that activity and ignore everything else.

○ Ignore activity involving items in selected groups

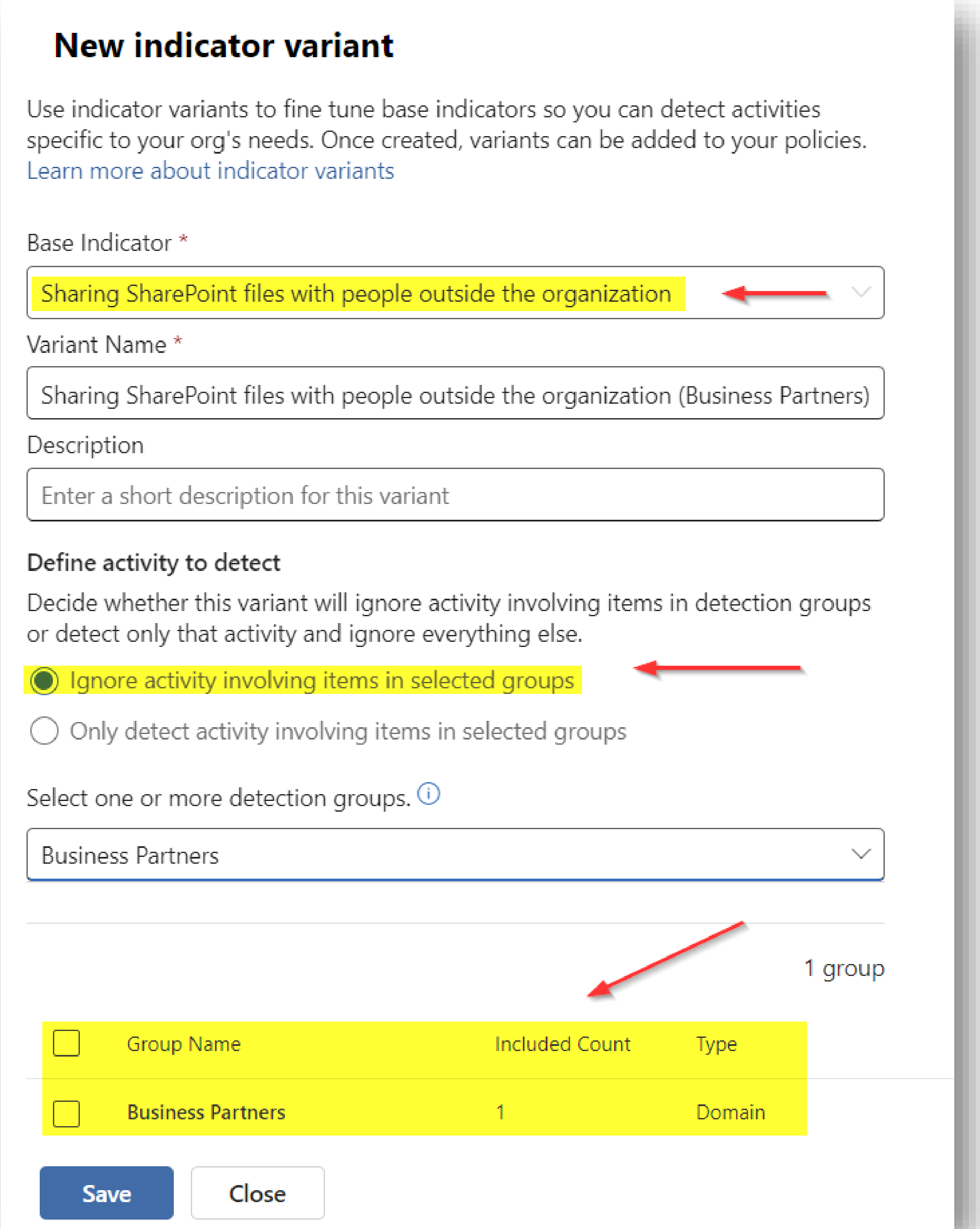
● Only detect activity involving items in selected groups

Select one or more detection groups. ⓘ

Free public domains

1 group

□	Group Name	Included Count	Type
□	**Free public domains**	152	Domain



New indicator variant

Use indicator variants to fine tune base indicators so you can detect activities specific to your org's needs. Once created, variants can be added to your policies.
Learn more about indicator variants

Base Indicator *

Sharing SharePoint files with people outside the organization

Variant Name *

Sharing SharePoint files with people outside the organization (Business Partners)

Description

Enter a short description for this variant

Define activity to detect

Decide whether this variant will ignore activity involving items in detection groups or detect only that activity and ignore everything else.

● Ignore activity involving items in selected groups

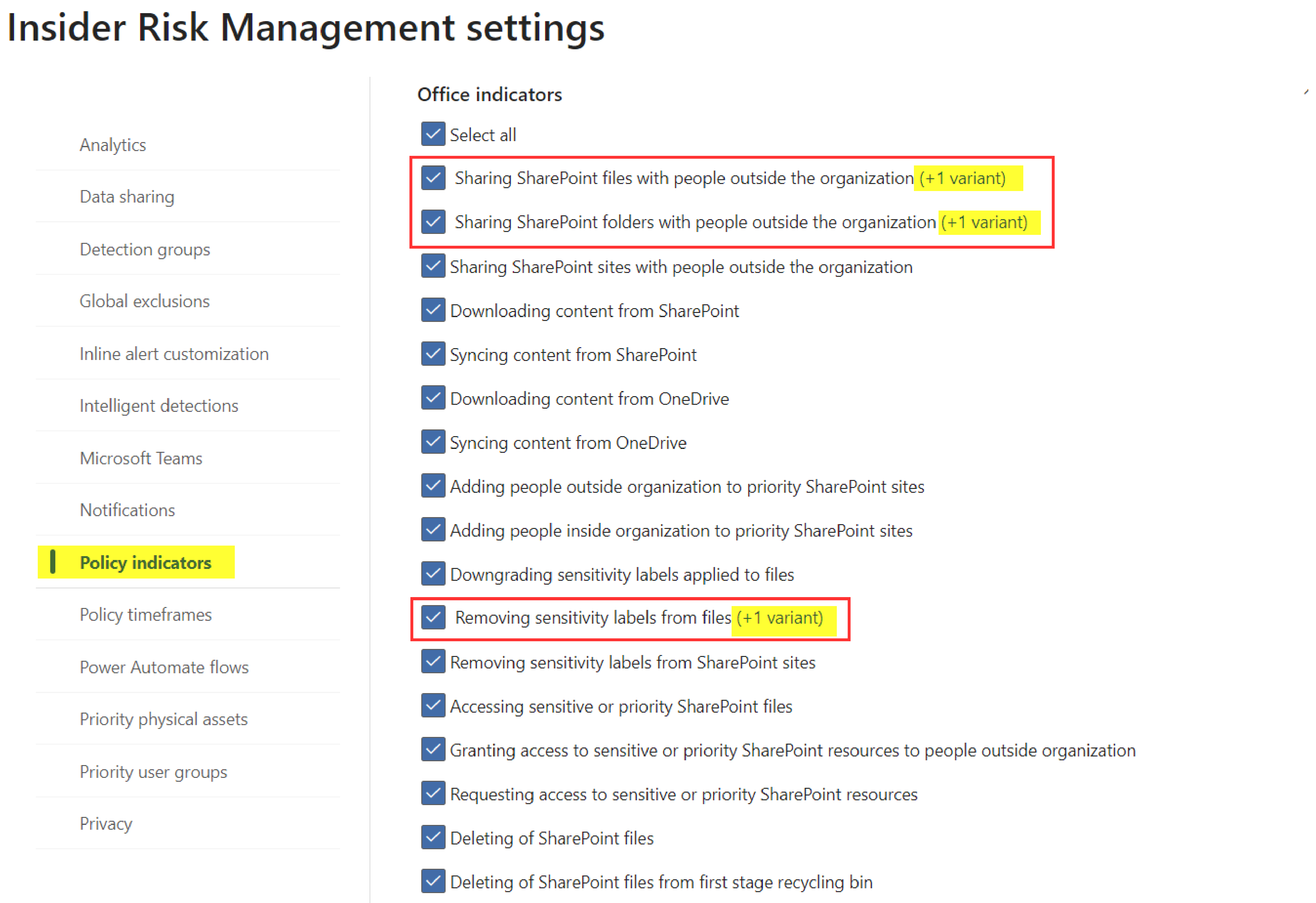
○ Only detect activity involving items in selected groups

Select one or more detection groups. ⓘ

Business Partners

1 group

□	Group Name	Included Count	Type
□	**Business Partners**	1	Domain



Insider Risk Management settings

- Analytics
- Data sharing
- Detection groups
- Global exclusions
- Inline alert customization
- Intelligent detections
- Microsoft Teams
- Notifications
- **Policy indicators**
- Policy timeframes
- Power Automate flows
- Priority physical assets
- Priority user groups
- Privacy

Office indicators

☑ Select all

☑ Sharing SharePoint files with people outside the organization (+1 variant)

☑ Sharing SharePoint folders with people outside the organization (+1 variant)

☑ Sharing SharePoint sites with people outside the organization

☑ Downloading content from SharePoint

☑ Syncing content from SharePoint

☑ Downloading content from OneDrive

☑ Syncing content from OneDrive

☑ Adding people outside organization to priority SharePoint sites

☑ Adding people inside organization to priority SharePoint sites

☑ Downgrading sensitivity labels applied to files

☑ Removing sensitivity labels from files (+1 variant)

☑ Removing sensitivity labels from SharePoint sites

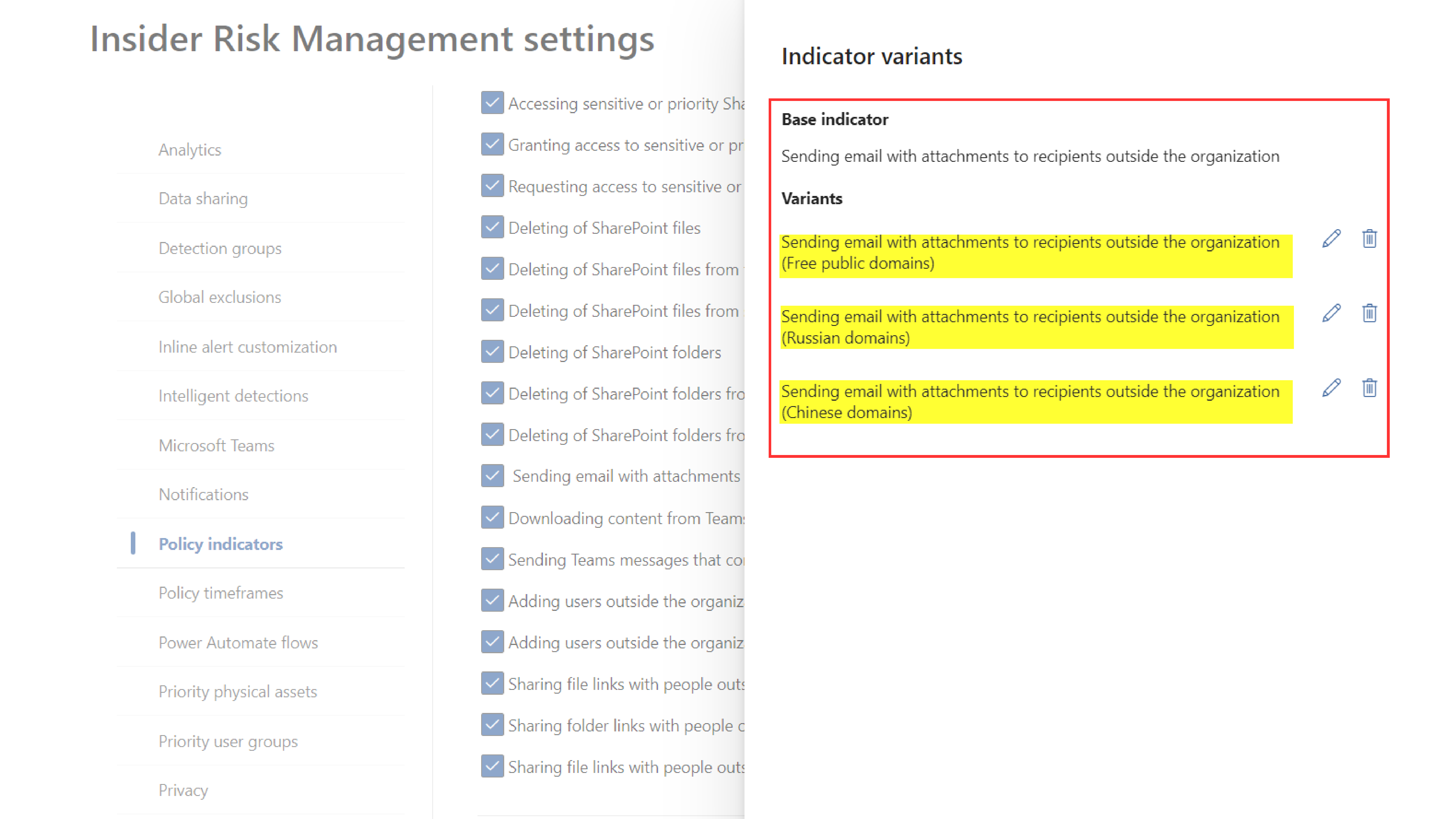
☑ Accessing sensitive or priority SharePoint files

☑ Granting access to sensitive or priority SharePoint resources to people outside organization

☑ Requesting access to sensitive or priority SharePoint resources

☑ Deleting of SharePoint files

☑ Deleting of SharePoint files from first stage recycling bin



Insider Risk Management settings

- Analytics
- Data sharing
- Detection groups
- Global exclusions
- Inline alert customization
- Intelligent detections
- Microsoft Teams
- Notifications
- **Policy indicators**
- Policy timeframes
- Power Automate flows
- Priority physical assets
- Priority user groups
- Privacy

☑ Accessing sensitive or priority Sha

☑ Granting access to sensitive or pr

☑ Requesting access to sensitive or

☑ Deleting of SharePoint files

☑ Deleting of SharePoint files from

☑ Deleting of SharePoint files from

☑ Deleting of SharePoint folders

☑ Deleting of SharePoint folders fro

☑ Deleting of SharePoint folders fro

☑ Sending email with attachments

☑ Downloading content from Teams

☑ Sending Teams messages that co

☑ Adding users outside the organiz

☑ Adding users outside the organiz

☑ Sharing file links with people outs

☑ Sharing folder links with people o

☑ Sharing file links with people outs

Indicator variants

Base indicator

Sending email with attachments to recipients outside the organization

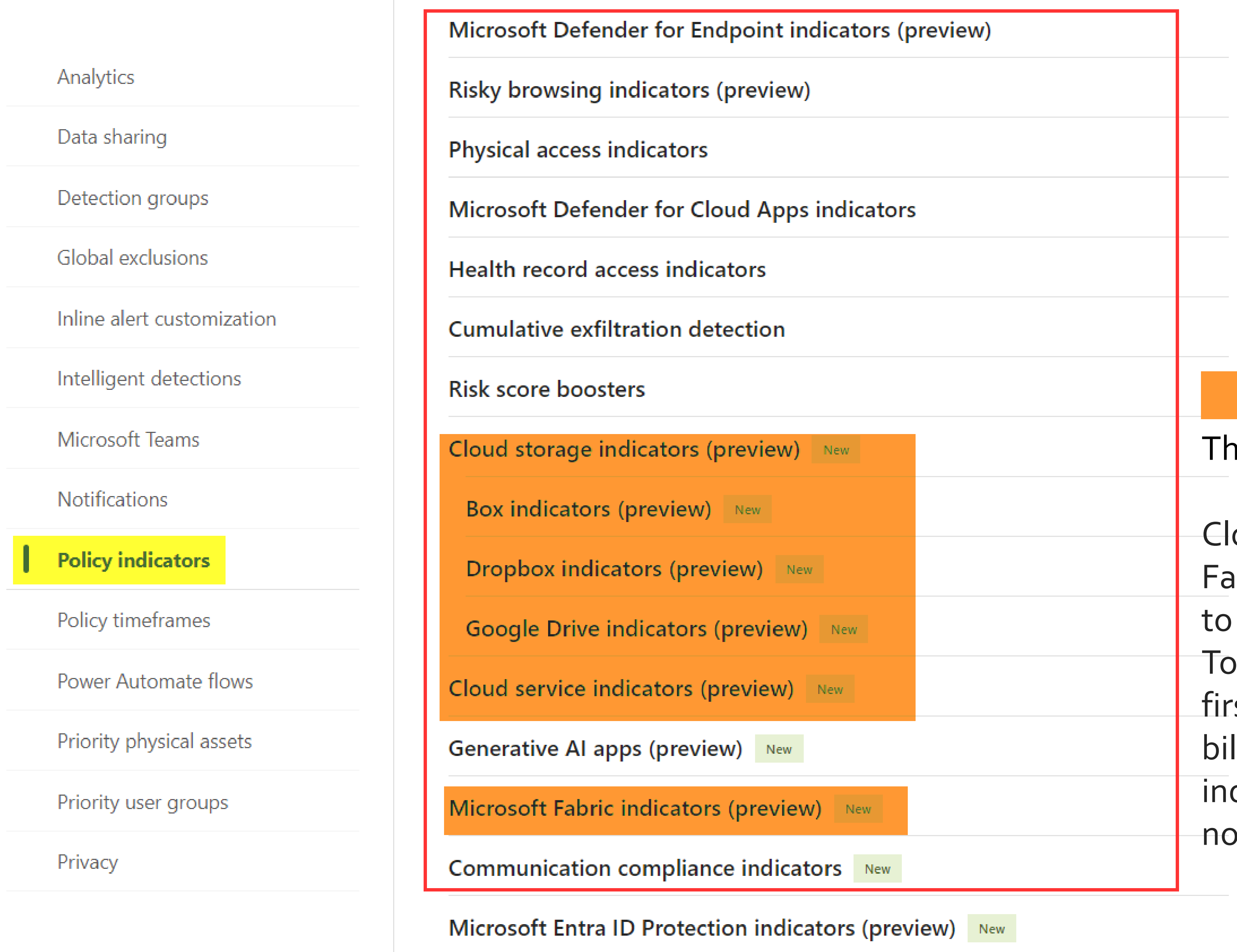
Variants

Sending email with attachments to recipients outside the organization (Free public domains)

Sending email with attachments to recipients outside the organization (Russian domains)

Sending email with attachments to recipients outside the organization (Chinese domains)

Insider Risk Management settings



Analytics

Data sharing

Detection groups

Global exclusions

Inline alert customization

Intelligent detections

Microsoft Teams

Notifications

Policy indicators

Policy timeframes

Power Automate flows

Priority physical assets

Priority user groups

Privacy

Microsoft Defender for Endpoint indicators (preview)

Risky browsing indicators (preview)

Physical access indicators

Microsoft Defender for Cloud Apps indicators

Health record access indicators

Cumulative exfiltration detection

Risk score boosters

Cloud storage indicators (preview) New

Box indicators (preview) New

Dropbox indicators (preview) New

Google Drive indicators (preview) New

Cloud service indicators (preview) New

Generative AI apps (preview) New

Microsoft Fabric indicators (preview) New

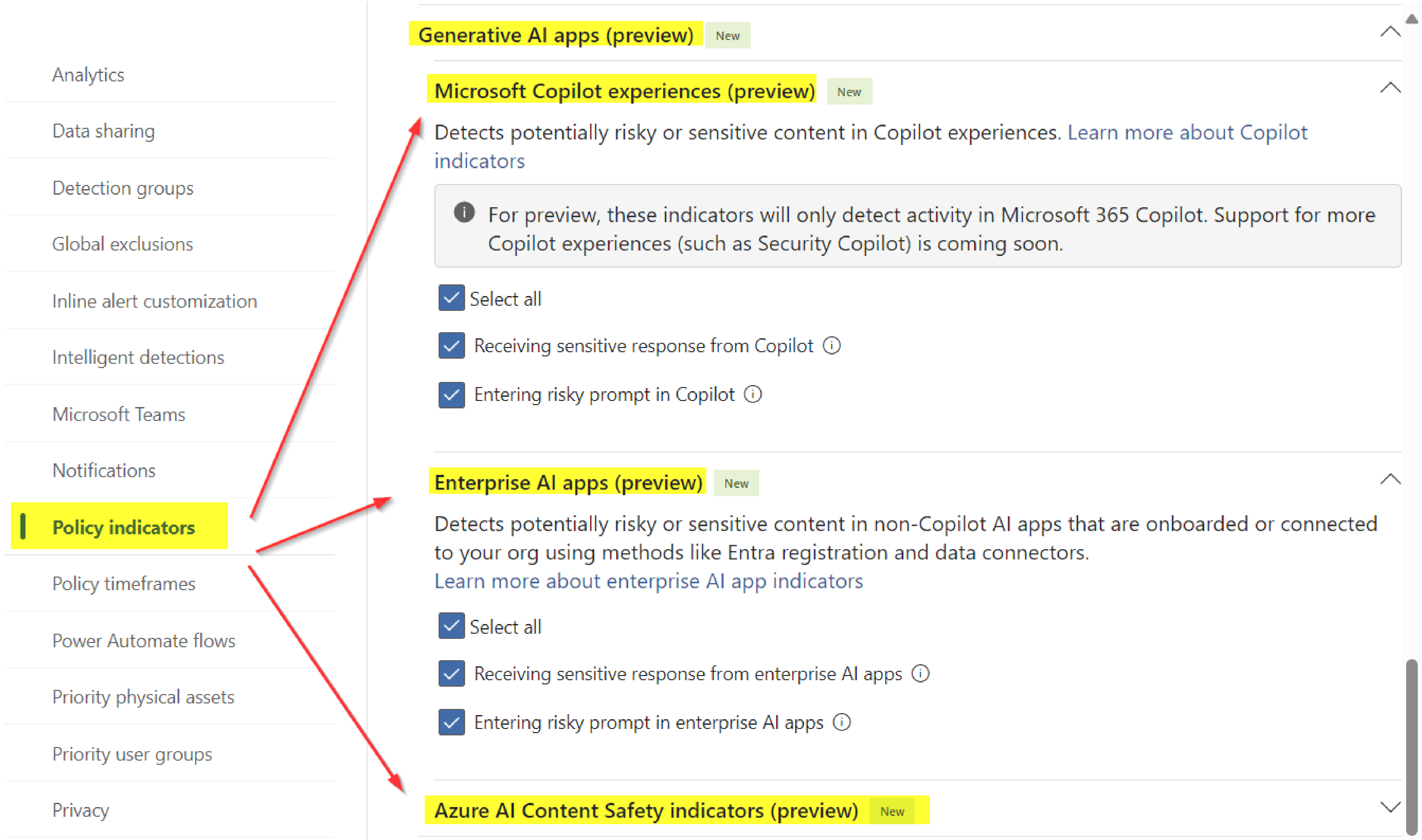
Communication compliance indicators New

Microsoft Entra ID Protection indicators (preview) New

These are pay-as-you-go indicators.

Cloud service, cloud storage, and Fabric indicators have transitioned to a pay-as-you-go pricing model. To use these indicators, you must first link an Azure subscription for billing. You'll only pay for the indicators used — no upfront costs, no commitment.

Insider Risk Management settings



- Analytics
- Data sharing
- Detection groups
- Global exclusions
- Inline alert customization
- Intelligent detections
- Microsoft Teams
- Notifications
- **Policy indicators**
- Policy timeframes
- Power Automate flows
- Priority physical assets
- Priority user groups
- Privacy

Generative AI apps (preview) New

Microsoft Copilot experiences (preview) New

Detects potentially risky or sensitive content in Copilot experiences. Learn more about Copilot indicators

For preview, these indicators will only detect activity in Microsoft 365 Copilot. Support for more Copilot experiences (such as Security Copilot) is coming soon.

☑ Select all

☑ Receiving sensitive response from Copilot ⓘ

☑ Entering risky prompt in Copilot ⓘ

Enterprise AI apps (preview) New

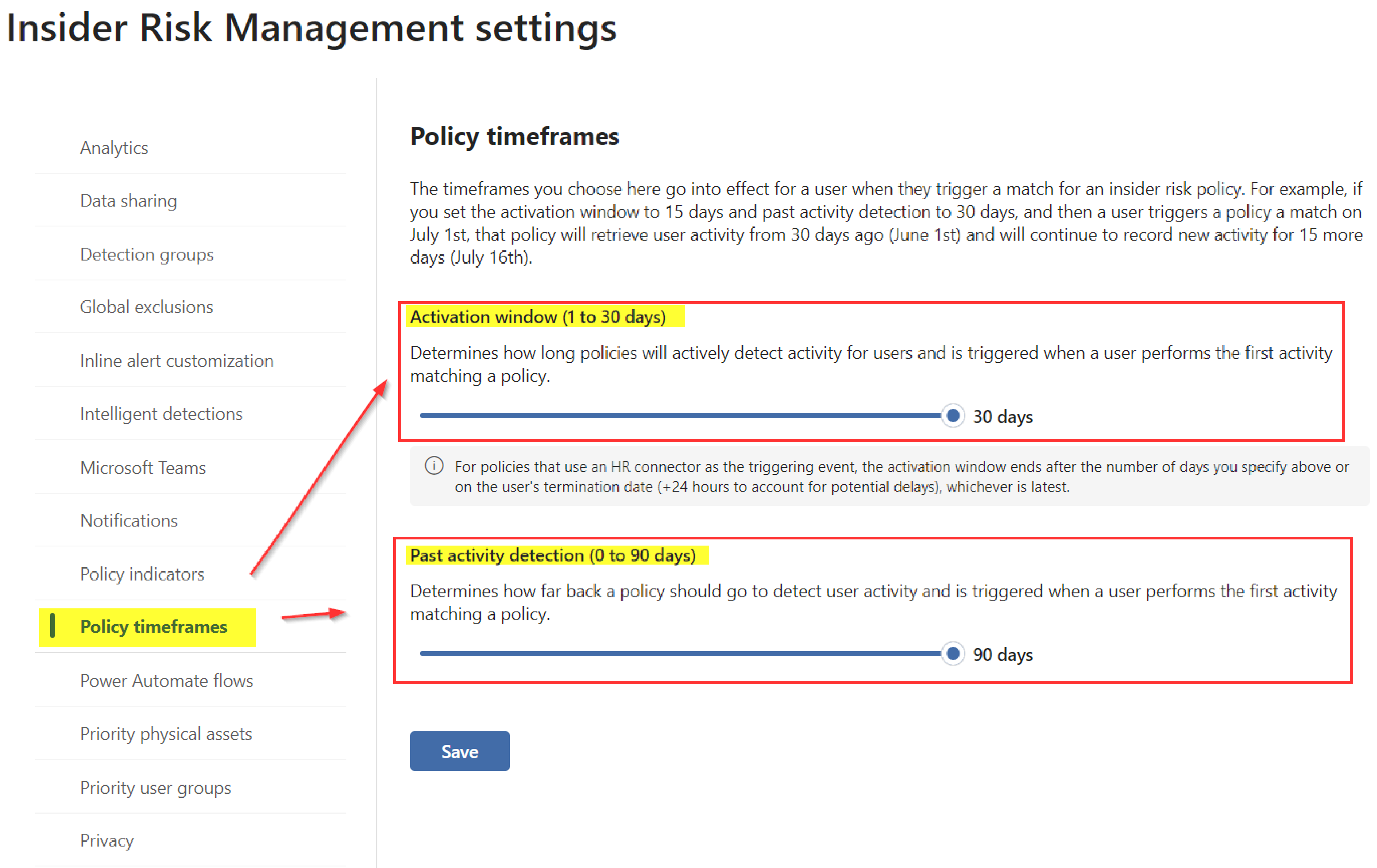
Detects potentially risky or sensitive content in non-Copilot AI apps that are onboarded or connected to your org using methods like Entra registration and data connectors.
Learn more about enterprise AI app indicators

☑ Select all

☑ Receiving sensitive response from enterprise AI apps ⓘ

☑ Entering risky prompt in enterprise AI apps ⓘ

Azure AI Content Safety indicators (preview) New



Insider Risk Management settings

Policy timeframes

The timeframes you choose here go into effect for a user when they trigger a match for an insider risk policy. For example, if you set the activation window to 15 days and past activity detection to 30 days, and then a user triggers a policy a match on July 1st, that policy will retrieve user activity from 30 days ago (June 1st) and will continue to record new activity for 15 more days (July 16th).

Activation window (1 to 30 days)

Determines how long policies will actively detect activity for users and is triggered when a user performs the first activity matching a policy.

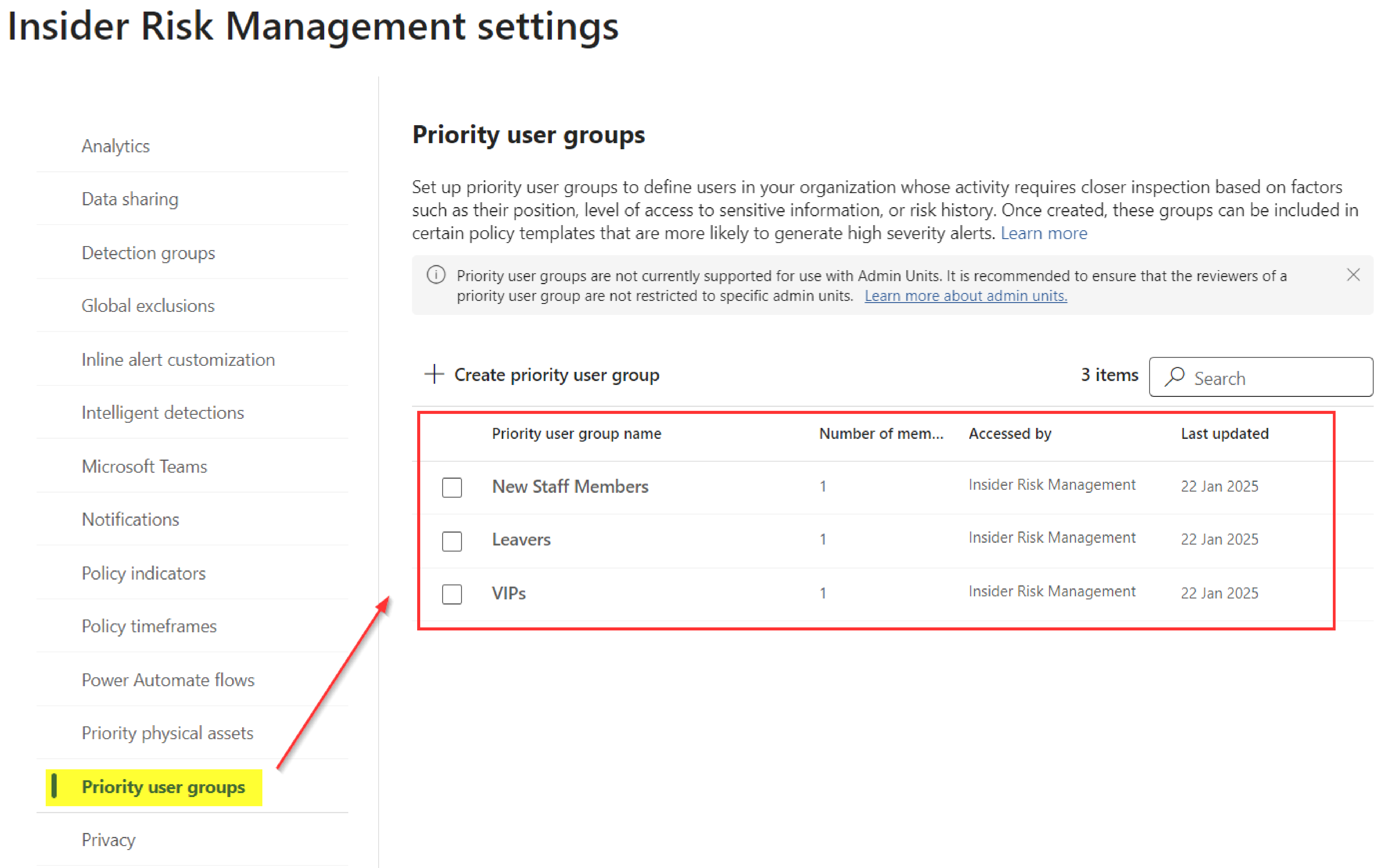
30 days

ⓘ For policies that use an HR connector as the triggering event, the activation window ends after the number of days you specify above or on the user's termination date (+24 hours to account for potential delays), whichever is latest.

Past activity detection (0 to 90 days)

Determines how far back a policy should go to detect user activity and is triggered when a user performs the first activity matching a policy.

90 days



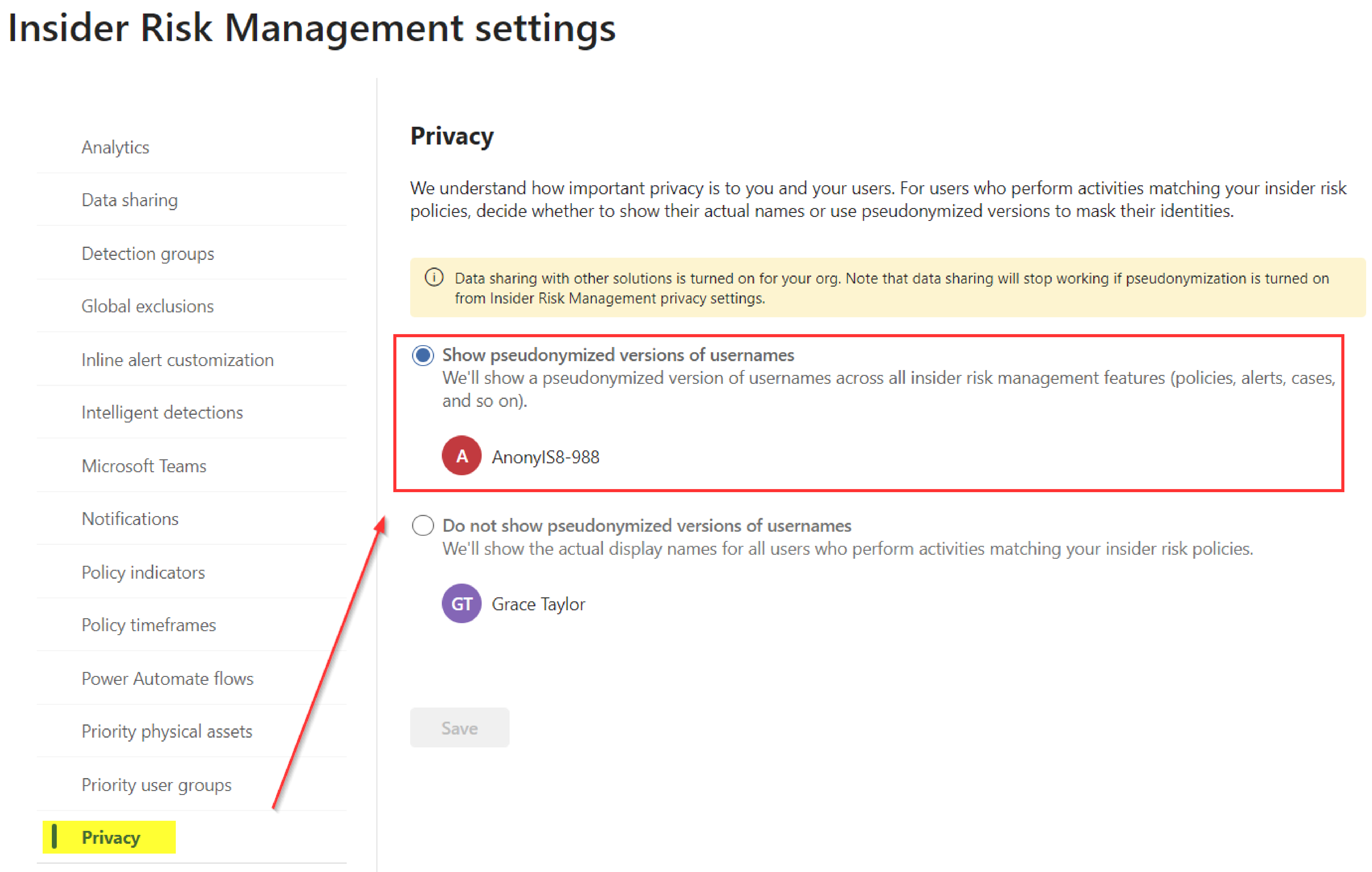
Insider Risk Management settings

Priority user groups

Set up priority user groups to define users in your organization whose activity requires closer inspection based on factors such as their position, level of access to sensitive information, or risk history. Once created, these groups can be included in certain policy templates that are more likely to generate high severity alerts. Learn more

ⓘ Priority user groups are not currently supported for use with Admin Units. It is recommended to ensure that the reviewers of a priority user group are not restricted to specific admin units. Learn more about admin units.

	Priority user group name	Number of mem...	Accessed by	Last updated
□	New Staff Members	1	Insider Risk Management	22 Jan 2025
□	Leavers	1	Insider Risk Management	22 Jan 2025
□	VIPs	1	Insider Risk Management	22 Jan 2025



Insider Risk Management settings

Privacy

We understand how important privacy is to you and your users. For users who perform activities matching your insider risk policies, decide whether to show their actual names or use pseudonymized versions to mask their identities.

ⓘ Data sharing with other solutions is turned on for your org. Note that data sharing will stop working if pseudonymization is turned on from Insider Risk Management privacy settings.

● **Show pseudonymized versions of usernames**
We'll show a pseudonymized version of usernames across all insider risk management features (policies, alerts, cases, and so on).

A AnonyIS8-988

○ **Do not show pseudonymized versions of usernames**
We'll show the actual display names for all users who perform activities matching your insider risk policies.

GT Grace Taylor

Step 2

1 Configure global Insider Risk settings

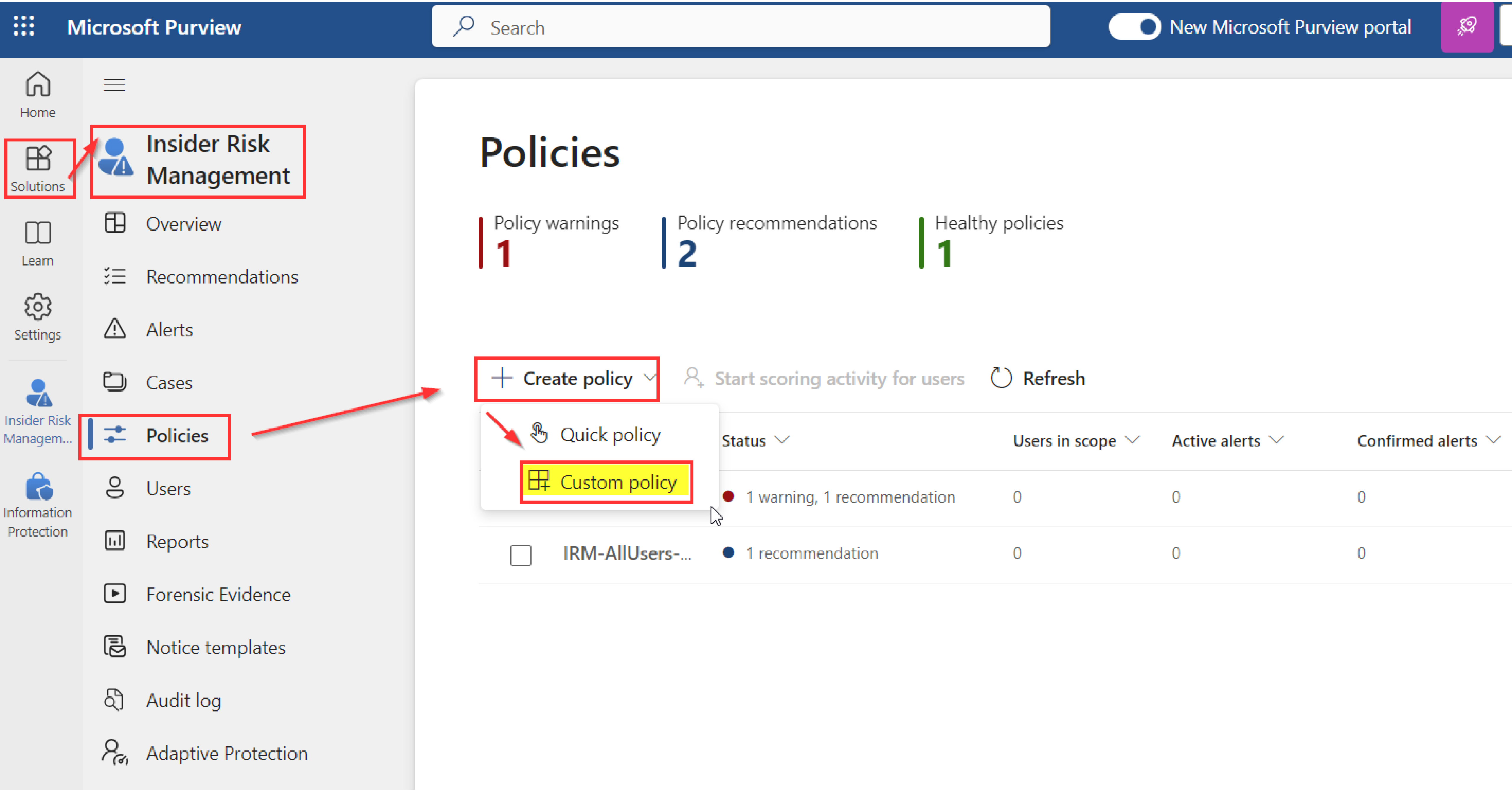
2 Create/ edit Insider Risk Management policy

3 Configure insider risk level settings

4 Customise an insider risk level for your policy

5 Create/ edit a Conditional Access policy

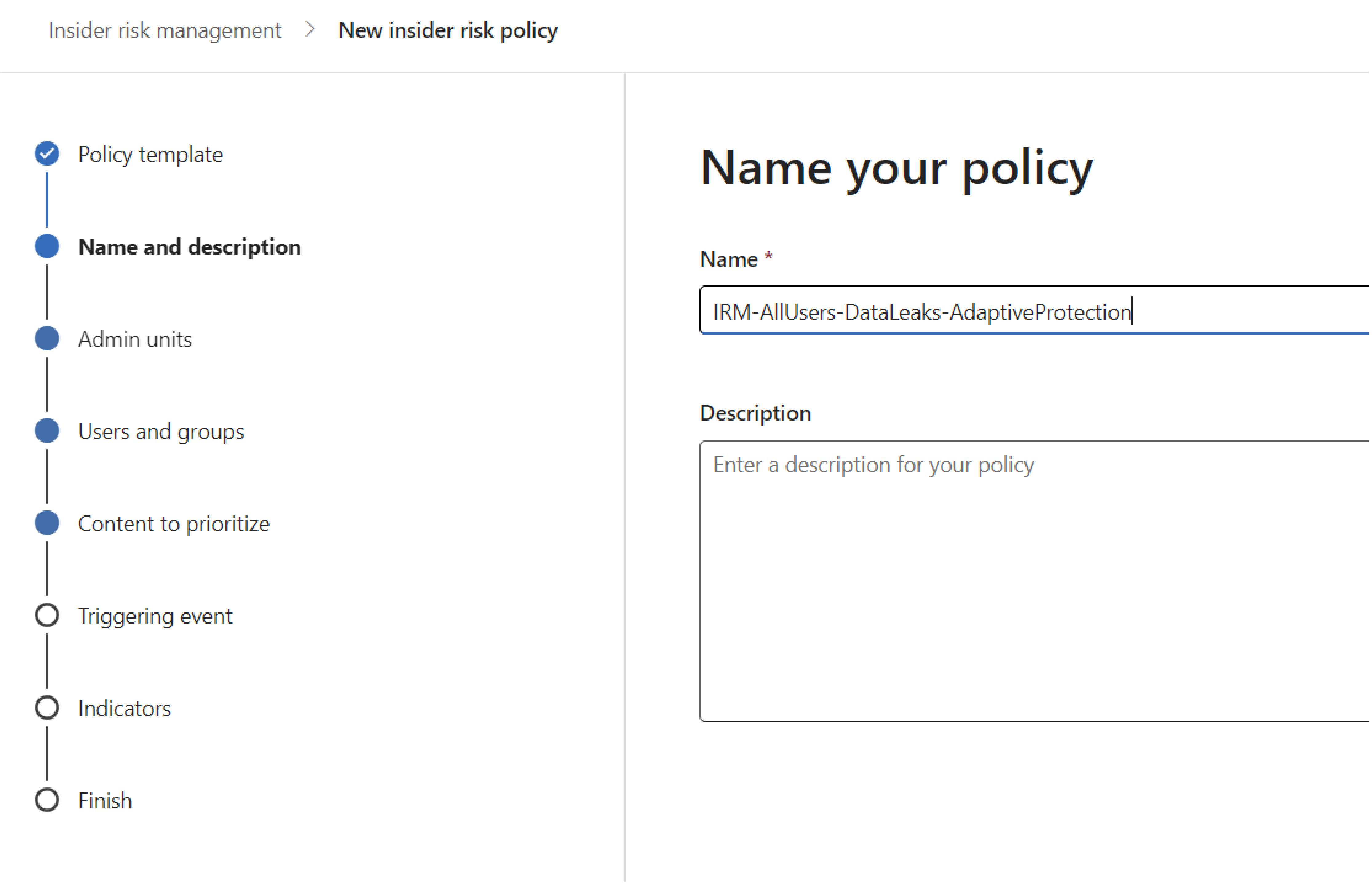
6 Turn on Adaptive Protection



Policies

Policy warnings	Policy recommendations	Healthy policies
1	2	1

		Status	Users in scope	Active alerts	Confirmed alerts
		● 1 warning, 1 recommendation	0	0	0
□	IRM-AllUsers-...	● 1 recommendation	0	0	0



Insider risk management > New insider risk policy

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

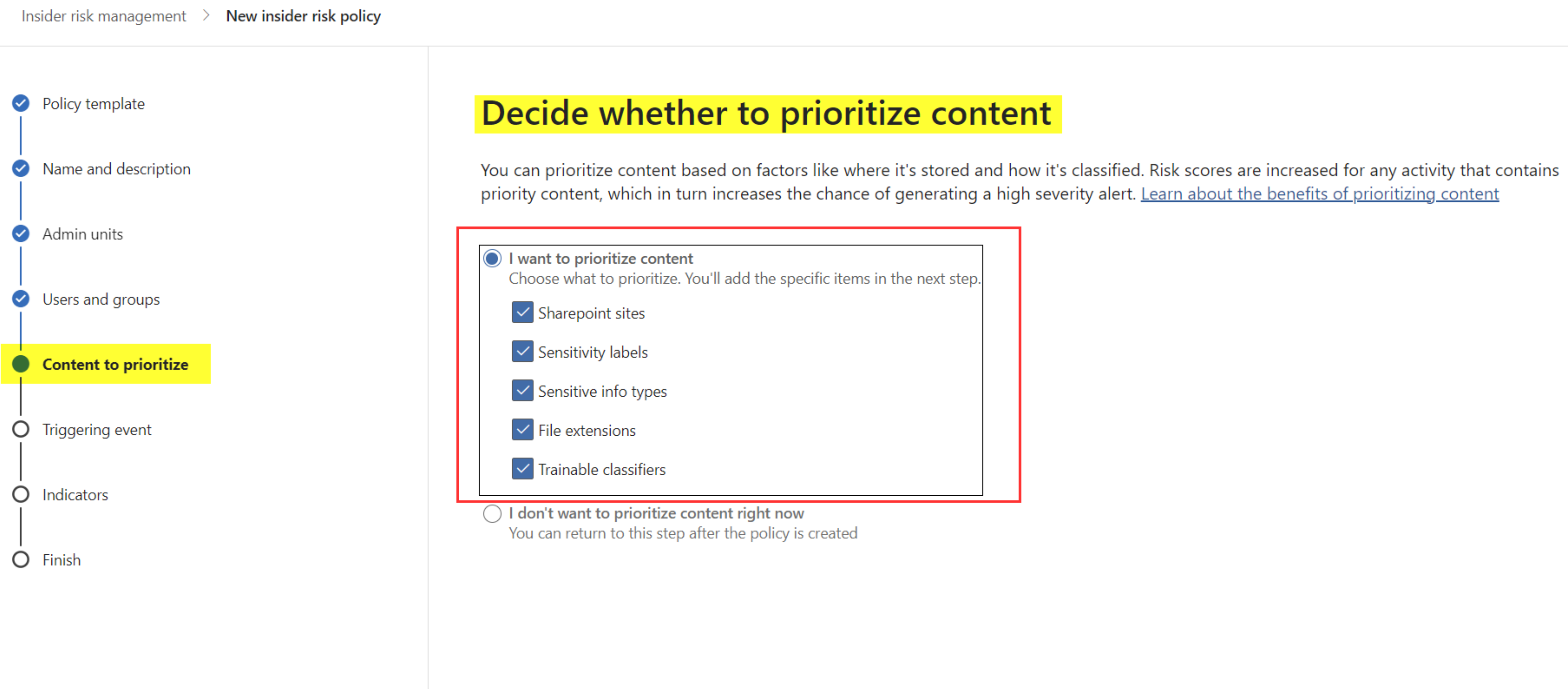
Name your policy

Name *

IRM-AllUsers-DataLeaks-AdaptiveProtection

Description

Enter a description for your policy



Insider risk management > New insider risk policy

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

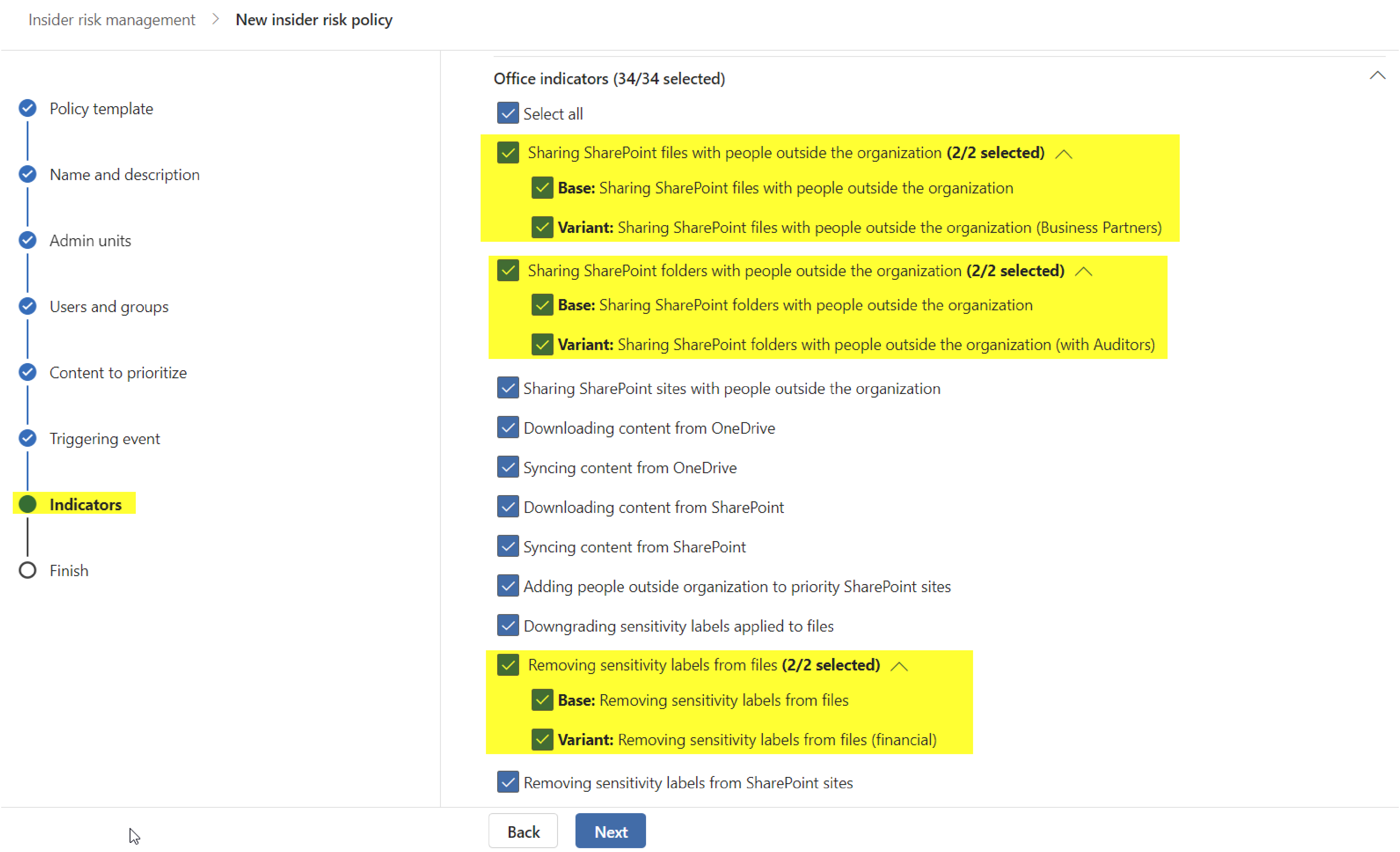
Decide whether to prioritize content

You can prioritize content based on factors like where it's stored and how it's classified. Risk scores are increased for any activity that contains priority content, which in turn increases the chance of generating a high severity alert. Learn about the benefits of prioritizing content

● **I want to prioritize content**
Choose what to prioritize. You'll add the specific items in the next step.

- ☑ Sharepoint sites
- ☑ Sensitivity labels
- ☑ Sensitive info types
- ☑ File extensions
- ☑ Trainable classifiers

○ **I don't want to prioritize content right now**
You can return to this step after the policy is created



Insider risk management > **New insider risk policy**

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

Office indicators (34/34 selected)

☑ Select all

☑ Sharing SharePoint files with people outside the organization **(2/2 selected)**

- ☑ **Base:** Sharing SharePoint files with people outside the organization
- ☑ **Variant:** Sharing SharePoint files with people outside the organization (Business Partners)

☑ Sharing SharePoint folders with people outside the organization **(2/2 selected)**

- ☑ **Base:** Sharing SharePoint folders with people outside the organization
- ☑ **Variant:** Sharing SharePoint folders with people outside the organization (with Auditors)

☑ Sharing SharePoint sites with people outside the organization

☑ Downloading content from OneDrive

☑ Syncing content from OneDrive

☑ Downloading content from SharePoint

☑ Syncing content from SharePoint

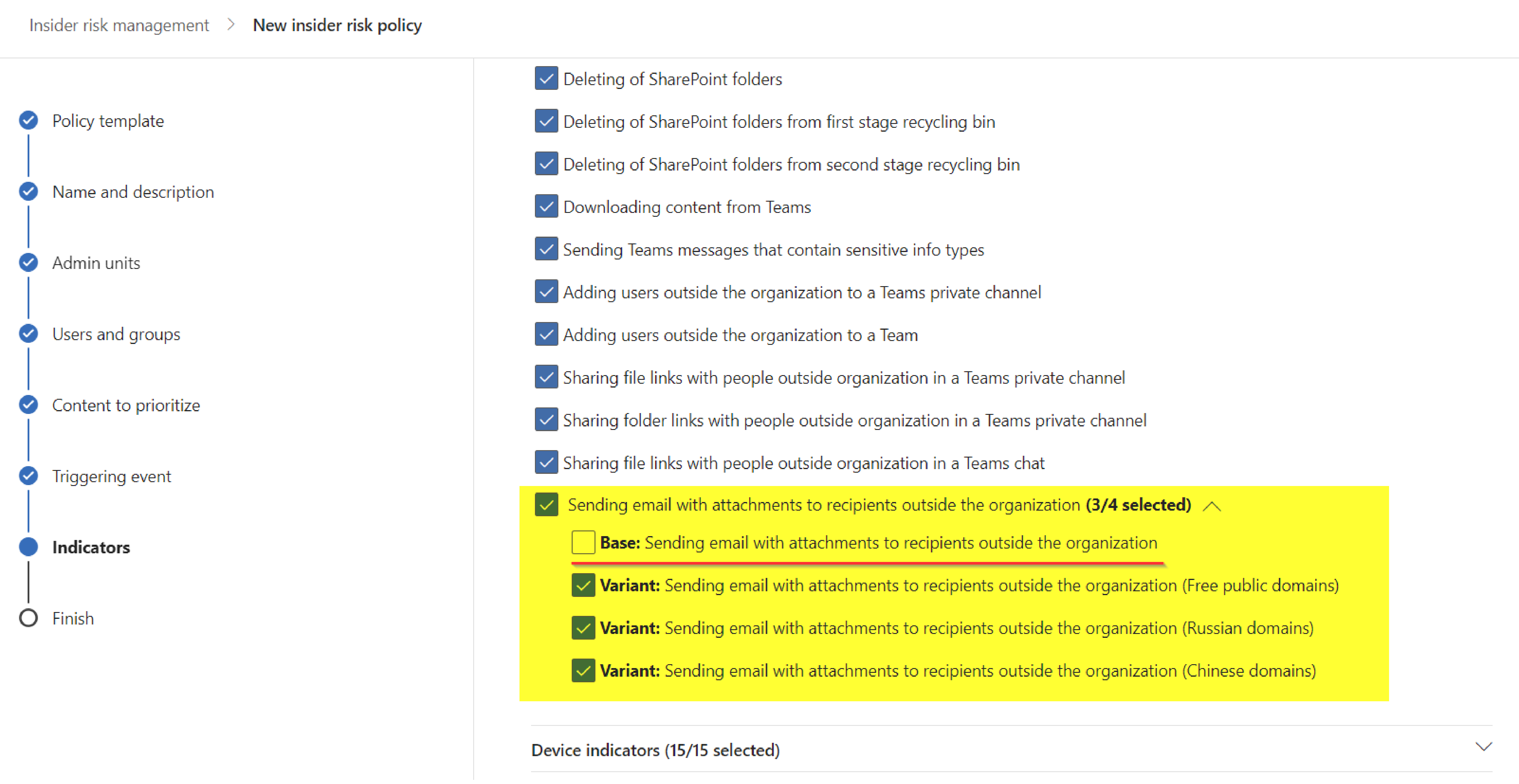
☑ Adding people outside organization to priority SharePoint sites

☑ Downgrading sensitivity labels applied to files

☑ Removing sensitivity labels from files **(2/2 selected)**

- ☑ **Base:** Removing sensitivity labels from files
- ☑ **Variant:** Removing sensitivity labels from files (financial)

☑ Removing sensitivity labels from SharePoint sites



Insider risk management > **New insider risk policy**

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

☑ Deleting of SharePoint folders

☑ Deleting of SharePoint folders from first stage recycling bin

☑ Deleting of SharePoint folders from second stage recycling bin

☑ Downloading content from Teams

☑ Sending Teams messages that contain sensitive info types

☑ Adding users outside the organization to a Teams private channel

☑ Adding users outside the organization to a Team

☑ Sharing file links with people outside organization in a Teams private channel

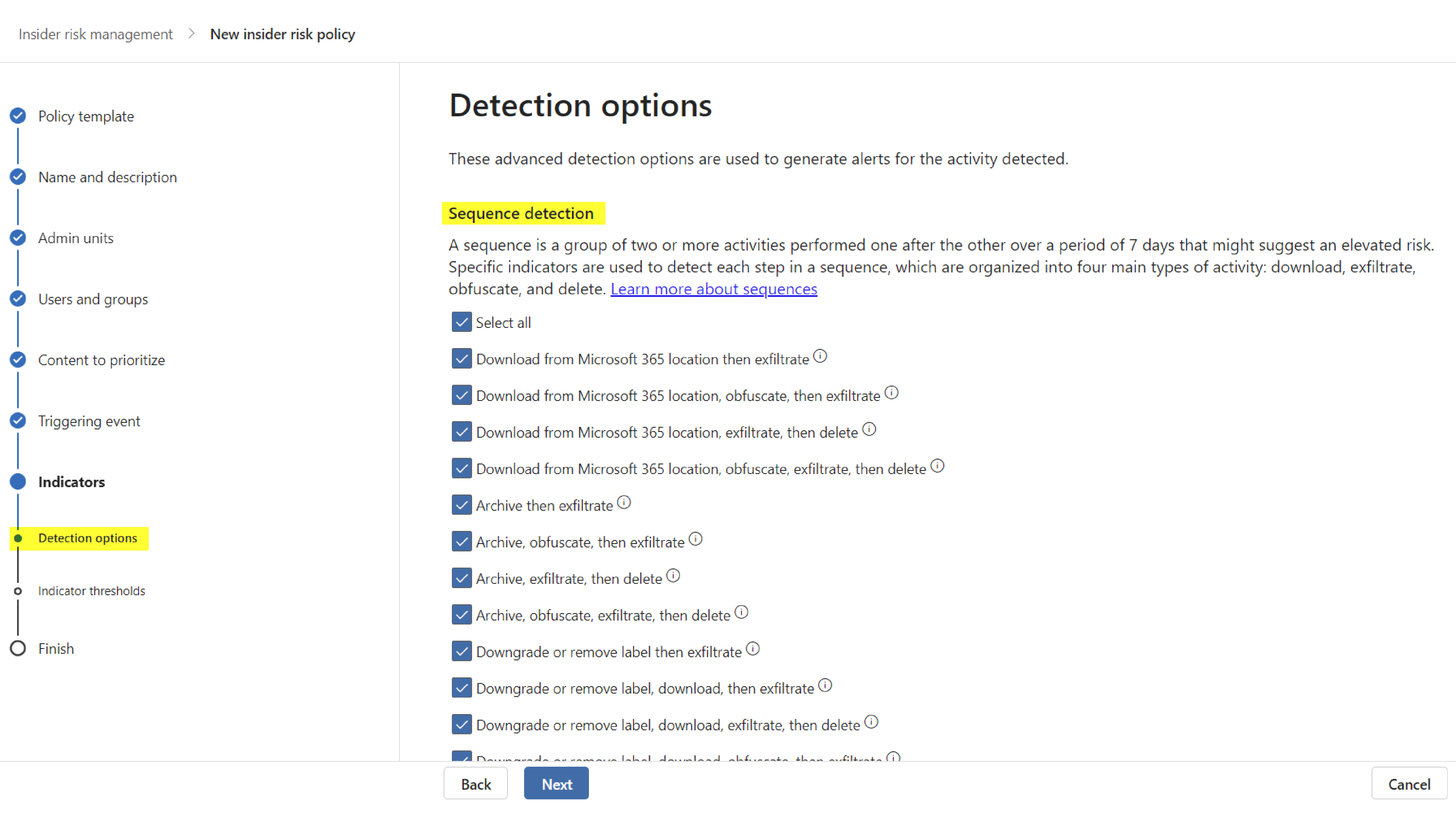
☑ Sharing folder links with people outside organization in a Teams private channel

☑ Sharing file links with people outside organization in a Teams chat

☑ Sending email with attachments to recipients outside the organization **(3/4 selected)**

- □ **Base:** Sending email with attachments to recipients outside the organization
- ☑ **Variant:** Sending email with attachments to recipients outside the organization (Free public domains)
- ☑ **Variant:** Sending email with attachments to recipients outside the organization (Russian domains)
- ☑ **Variant:** Sending email with attachments to recipients outside the organization (Chinese domains)

Device indicators (15/15 selected)



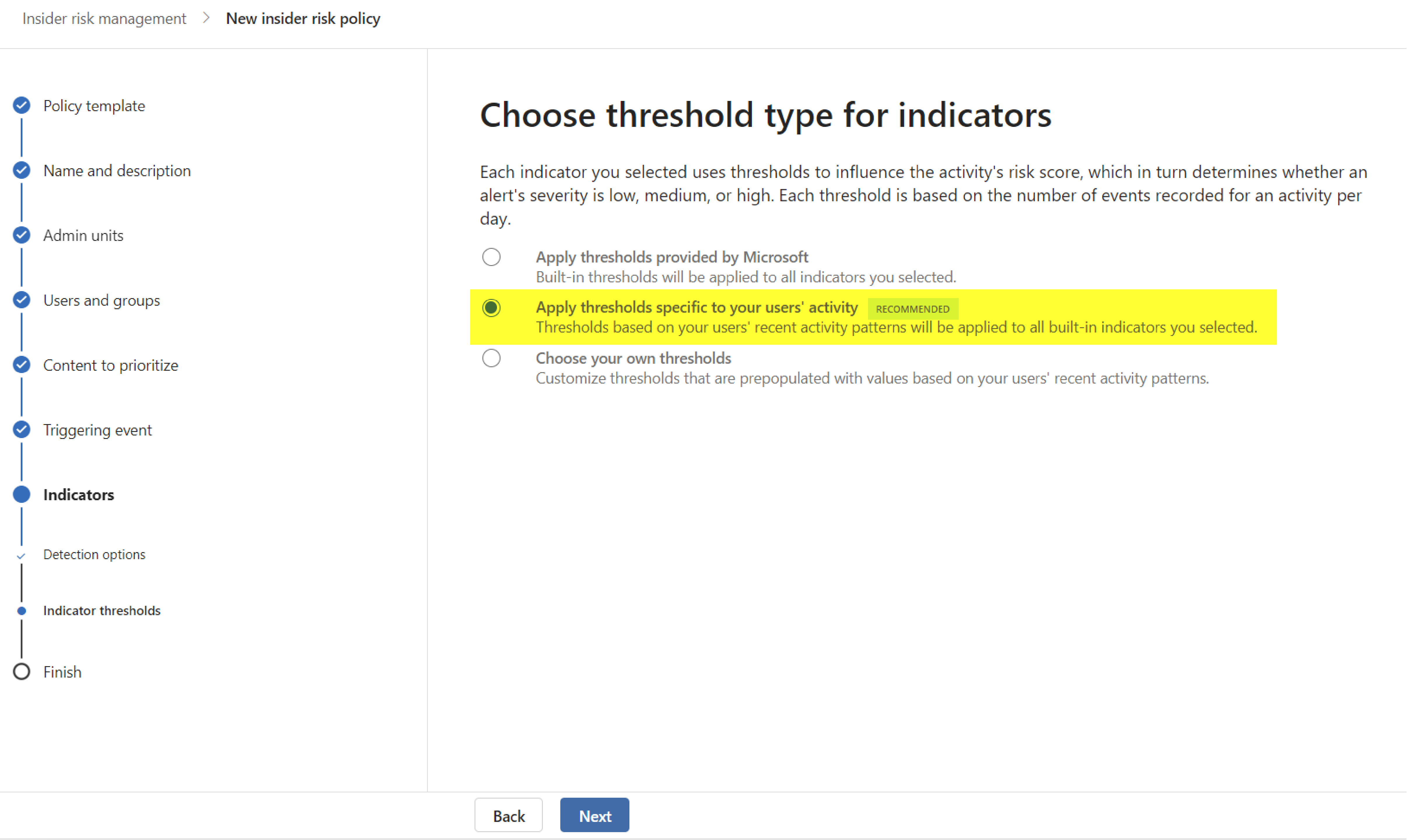
Detection options

These advanced detection options are used to generate alerts for the activity detected.

Sequence detection

A sequence is a group of two or more activities performed one after the other over a period of 7 days that might suggest an elevated risk. Specific indicators are used to detect each step in a sequence, which are organized into four main types of activity: download, exfiltrate, obfuscate, and delete. Learn more about sequences

- ☑ Select all
- ☑ Download from Microsoft 365 location then exfiltrate ⓘ
- ☑ Download from Microsoft 365 location, obfuscate, then exfiltrate ⓘ
- ☑ Download from Microsoft 365 location, exfiltrate, then delete ⓘ
- ☑ Download from Microsoft 365 location, obfuscate, exfiltrate, then delete ⓘ
- ☑ Archive then exfiltrate ⓘ
- ☑ Archive, obfuscate, then exfiltrate ⓘ
- ☑ Archive, exfiltrate, then delete ⓘ
- ☑ Archive, obfuscate, exfiltrate, then delete ⓘ
- ☑ Downgrade or remove label then exfiltrate ⓘ
- ☑ Downgrade or remove label, download, then exfiltrate ⓘ
- ☑ Downgrade or remove label, download, exfiltrate, then delete ⓘ
- ☑ Downgrade or remove label, download, obfuscate, then exfiltrate ⓘ



Insider risk management > **New insider risk policy**

Choose threshold type for indicators

Each indicator you selected uses thresholds to influence the activity's risk score, which in turn determines whether an alert's severity is low, medium, or high. Each threshold is based on the number of events recorded for an activity per day.

○ **Apply thresholds provided by Microsoft**
Built-in thresholds will be applied to all indicators you selected.

● **Apply thresholds specific to your users' activity** RECOMMENDED
Thresholds based on your users' recent activity patterns will be applied to all built-in indicators you selected.

○ **Choose your own thresholds**
Customize thresholds that are prepopulated with values based on your users' recent activity patterns.

Step 3

1

Configure global Insider Risk settings

2

Create/ edit Insider Risk Management policy

3

Configure insider risk level settings

4

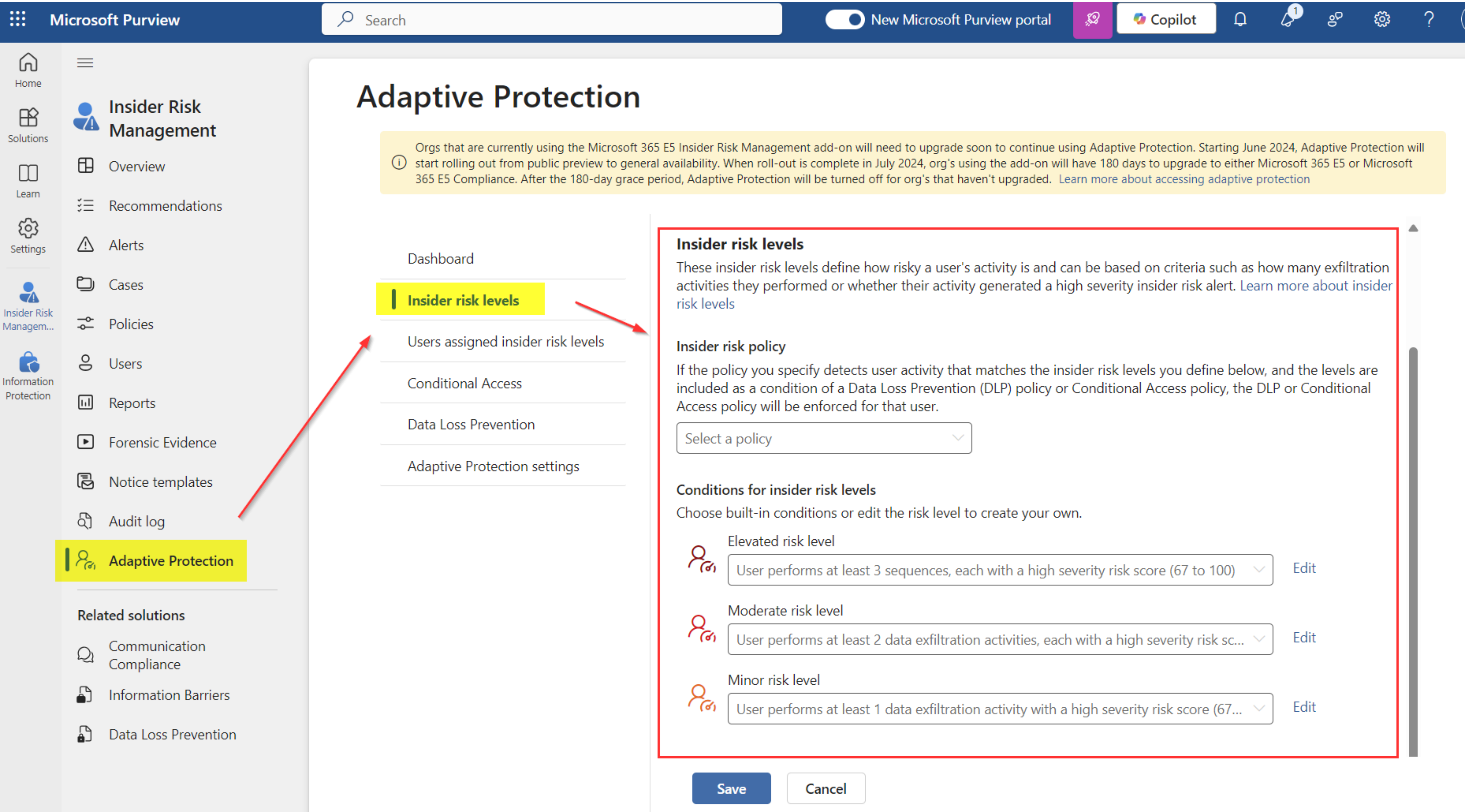
Customise an insider risk level for your policy

5

Create/ edit a Conditional Access policy

6

Turn on Adaptive Protection



Adaptive Protection

Orgs that are currently using the Microsoft 365 E5 Insider Risk Management add-on will need to upgrade soon to continue using Adaptive Protection. Starting June 2024, Adaptive Protection will start rolling out from public preview to general availability. When roll-out is complete in July 2024, org's using the add-on will have 180 days to upgrade to either Microsoft 365 E5 or Microsoft 365 E5 Compliance. After the 180-day grace period, Adaptive Protection will be turned off for org's that haven't upgraded. Learn more about accessing adaptive protection

Insider risk levels

These insider risk levels define how risky a user's activity is and can be based on criteria such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. Learn more about insider risk levels

Insider risk policy

If the policy you specify detects user activity that matches the insider risk levels you define below, and the levels are included as a condition of a Data Loss Prevention (DLP) policy or Conditional Access policy, the DLP or Conditional Access policy will be enforced for that user.

Select a policy

Conditions for insider risk levels

Choose built-in conditions or edit the risk level to create your own.

Elevated risk level
User performs at least 3 sequences, each with a high severity risk score (67 to 100) Edit

Moderate risk level
User performs at least 2 data exfiltration activities, each with a high severity risk sc... Edit

Minor risk level
User performs at least 1 data exfiltration activity with a high severity risk score (67... Edit

Step 4

1 Configure global Insider Risk settings

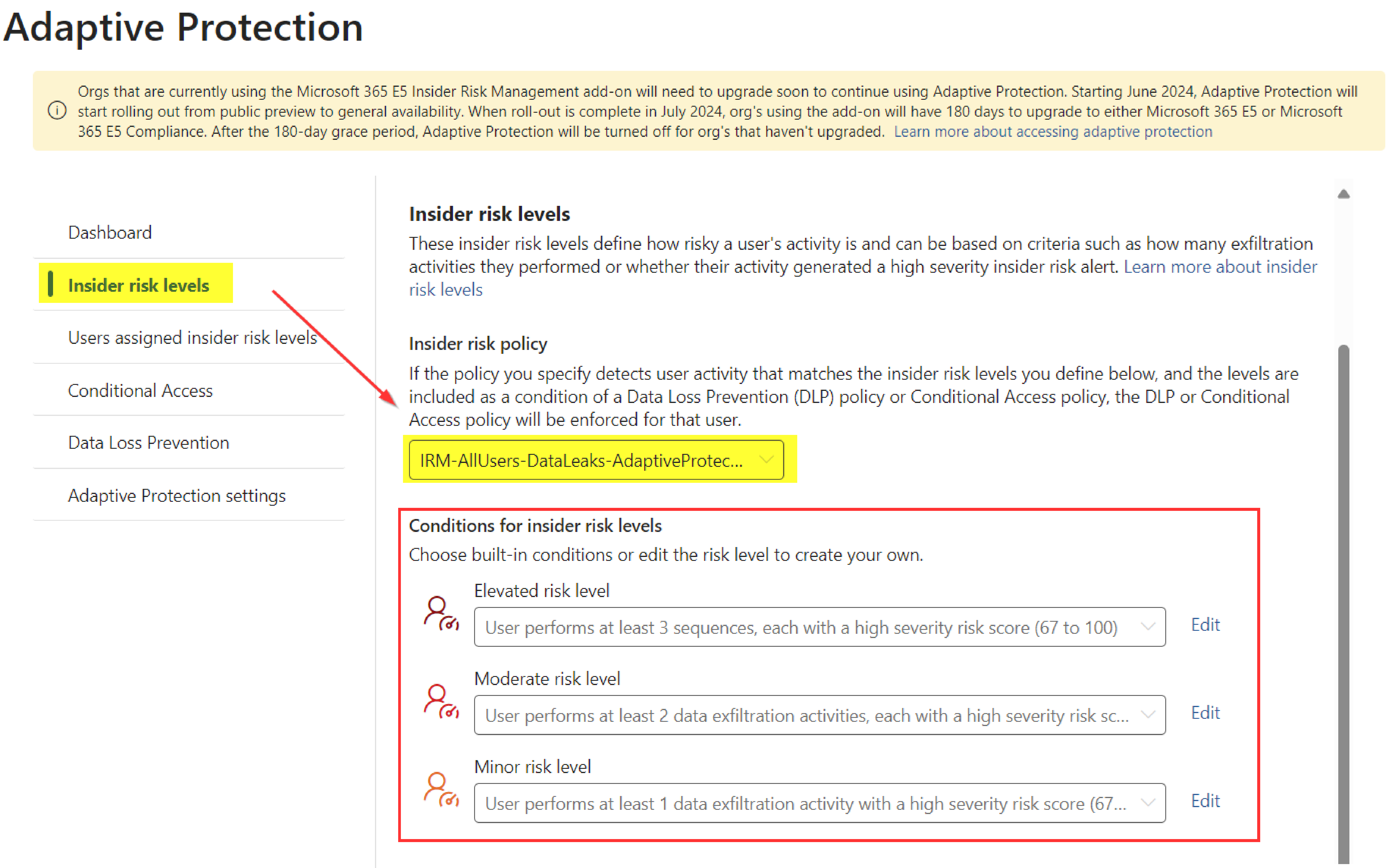
2 Create/ edit Insider Risk Management policy

3 Configure insider risk level settings

4 Customise an insider risk level for your policy

5 Create/ edit a Conditional Access policy

6 Turn on Adaptive Protection



Adaptive Protection

Orgs that are currently using the Microsoft 365 E5 Insider Risk Management add-on will need to upgrade soon to continue using Adaptive Protection. Starting June 2024, Adaptive Protection will start rolling out from public preview to general availability. When roll-out is complete in July 2024, org's using the add-on will have 180 days to upgrade to either Microsoft 365 E5 or Microsoft 365 E5 Compliance. After the 180-day grace period, Adaptive Protection will be turned off for org's that haven't upgraded. Learn more about accessing adaptive protection

Insider risk levels

These insider risk levels define how risky a user's activity is and can be based on criteria such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. Learn more about insider risk levels

Insider risk policy

If the policy you specify detects user activity that matches the insider risk levels you define below, and the levels are included as a condition of a Data Loss Prevention (DLP) policy or Conditional Access policy, the DLP or Conditional Access policy will be enforced for that user.

IRM-AllUsers-DataLeaks-AdaptiveProtec...

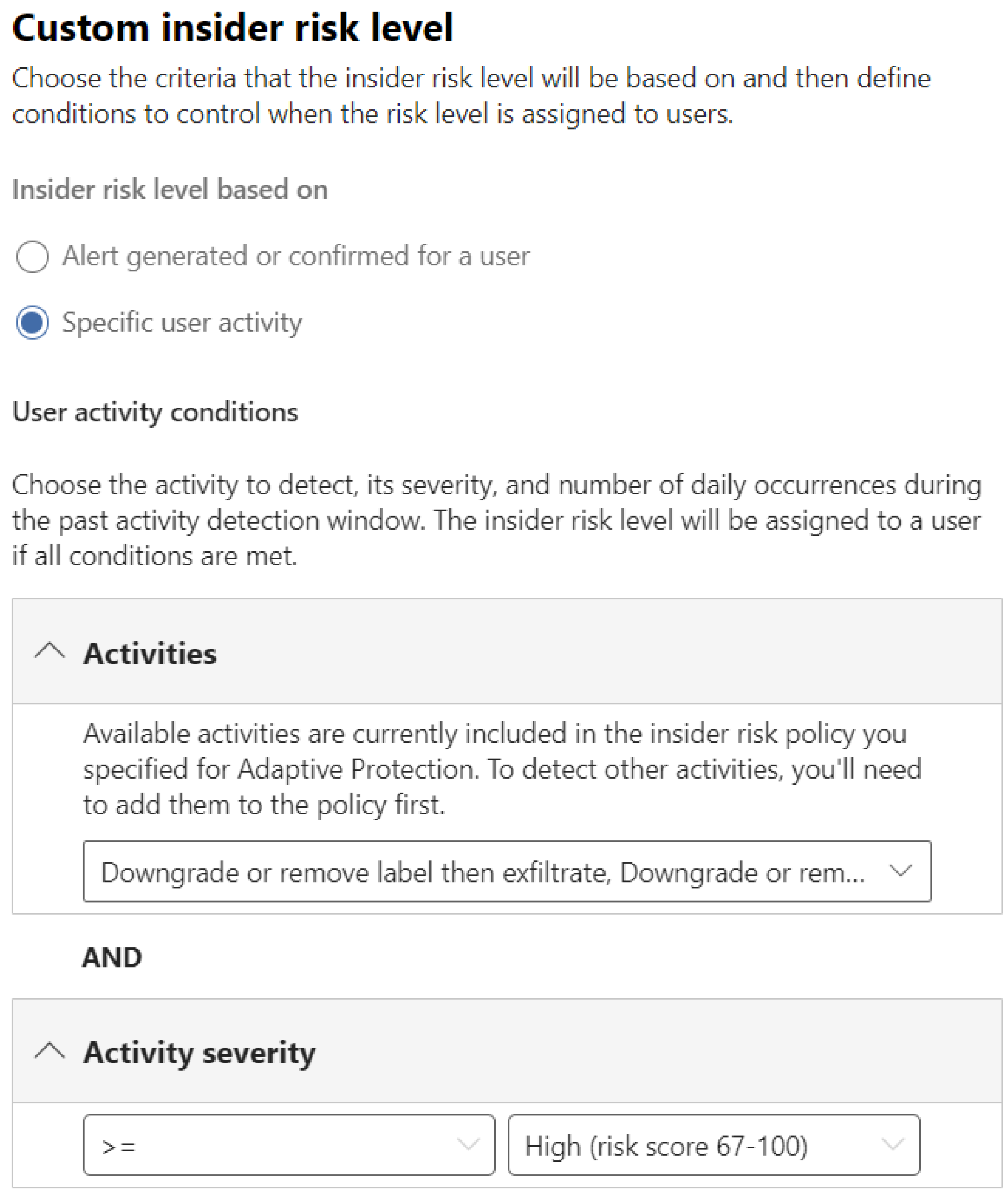
Conditions for insider risk levels

Choose built-in conditions or edit the risk level to create your own.

Elevated risk level: User performs at least 3 sequences, each with a high severity risk score (67 to 100)

Moderate risk level: User performs at least 2 data exfiltration activities, each with a high severity risk sc...

Minor risk level: User performs at least 1 data exfiltration activity with a high severity risk score (67...



Custom insider risk level

Choose the criteria that the insider risk level will be based on and then define conditions to control when the risk level is assigned to users.

Insider risk level based on

○ Alert generated or confirmed for a user

● Specific user activity

User activity conditions

Choose the activity to detect, its severity, and number of daily occurrences during the past activity detection window. The insider risk level will be assigned to a user if all conditions are met.

Activities

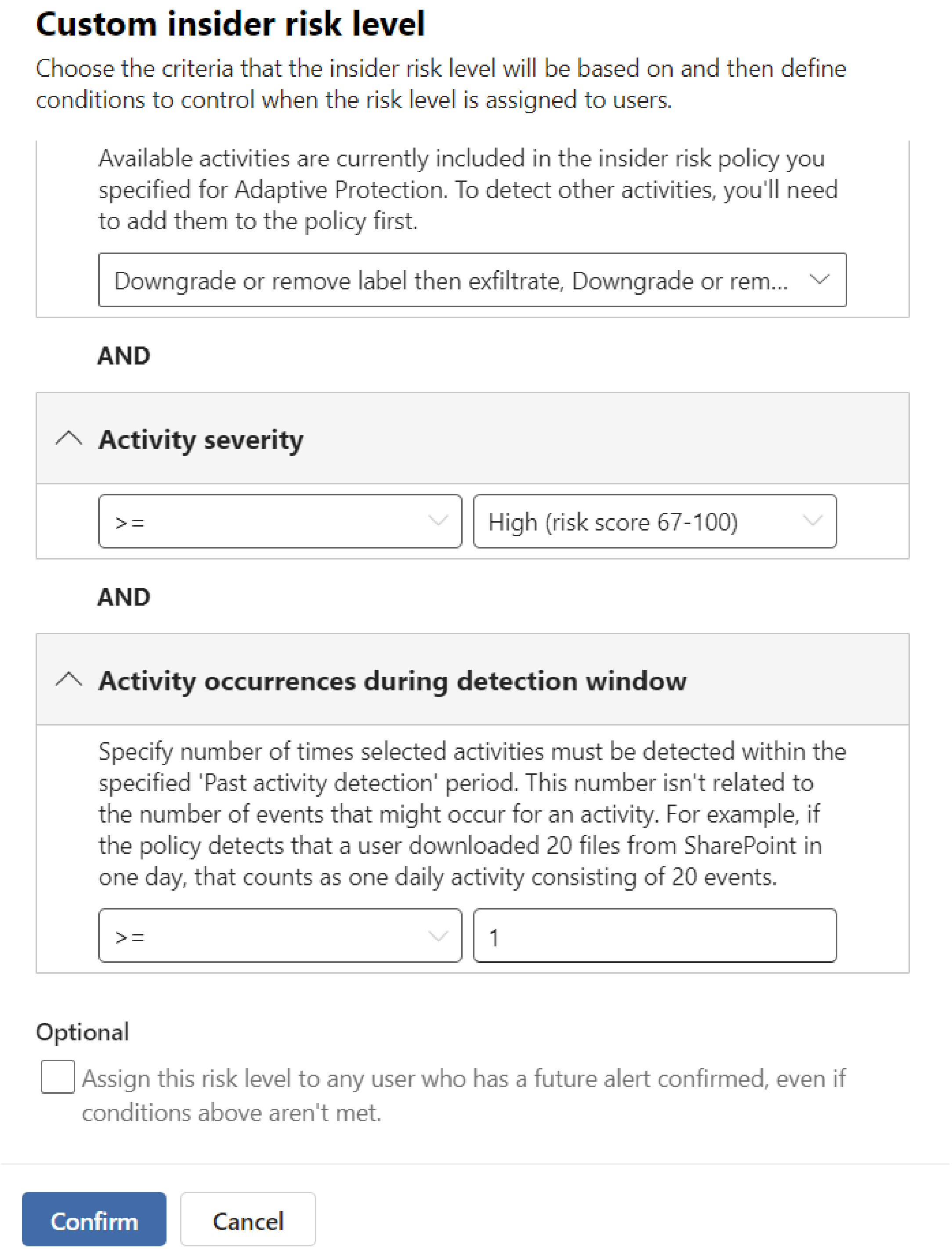
Available activities are currently included in the insider risk policy you specified for Adaptive Protection. To detect other activities, you'll need to add them to the policy first.

Downgrade or remove label then exfiltrate, Downgrade or rem...

AND

Activity severity

>= | High (risk score 67-100)



Custom insider risk level

Choose the criteria that the insider risk level will be based on and then define conditions to control when the risk level is assigned to users.

Available activities are currently included in the insider risk policy you specified for Adaptive Protection. To detect other activities, you'll need to add them to the policy first.

Downgrade or remove label then exfiltrate, Downgrade or rem...

AND

Activity severity

>= | High (risk score 67-100)

AND

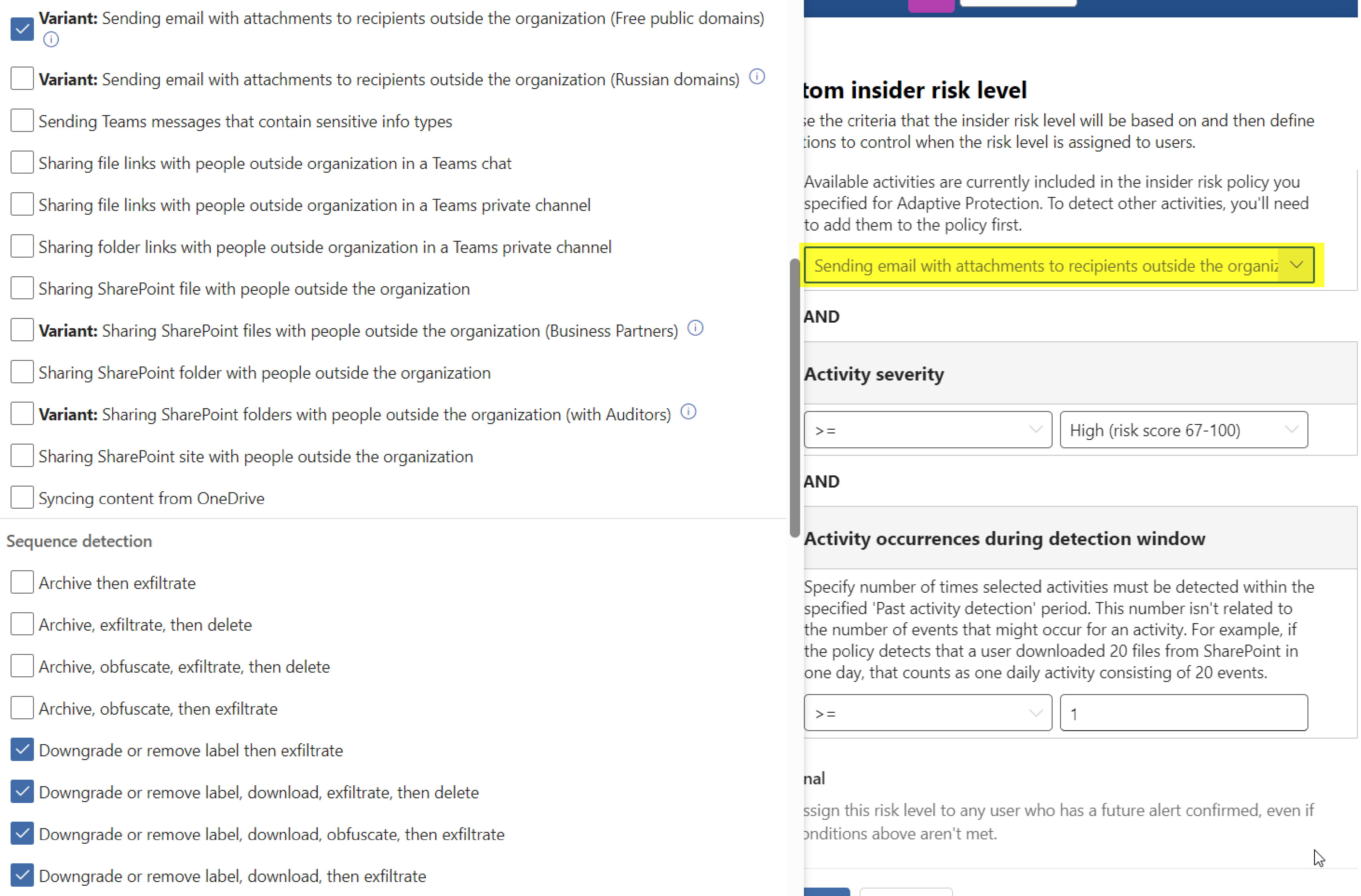
Activity occurrences during detection window

Specify number of times selected activities must be detected within the specified 'Past activity detection' period. This number isn't related to the number of events that might occur for an activity. For example, if the policy detects that a user downloaded 20 files from SharePoint in one day, that counts as one daily activity consisting of 20 events.

>= | 1

Optional

□ Assign this risk level to any user who has a future alert confirmed, even if conditions above aren't met.



☑ **Variant:** Sending email with attachments to recipients outside the organization (Free public domains) ⓘ

□ **Variant:** Sending email with attachments to recipients outside the organization (Russian domains) ⓘ

□ Sending Teams messages that contain sensitive info types

□ Sharing file links with people outside organization in a Teams chat

□ Sharing file links with people outside organization in a Teams private channel

□ Sharing folder links with people outside organization in a Teams private channel

□ Sharing SharePoint file with people outside the organization

□ **Variant:** Sharing SharePoint files with people outside the organization (Business Partners) ⓘ

□ Sharing SharePoint folder with people outside the organization

□ **Variant:** Sharing SharePoint folders with people outside the organization (with Auditors) ⓘ

□ Sharing SharePoint site with people outside the organization

□ Syncing content from OneDrive

Sequence detection

□ Archive then exfiltrate

□ Archive, exfiltrate, then delete

□ Archive, obfuscate, exfiltrate, then delete

□ Archive, obfuscate, then exfiltrate

☑ Downgrade or remove label then exfiltrate

☑ Downgrade or remove label, download, exfiltrate, then delete

☑ Downgrade or remove label, download, obfuscate, then exfiltrate

☑ Downgrade or remove label, download, then exfiltrate

tom insider risk level

e the criteria that the insider risk level will be based on and then define ions to control when the risk level is assigned to users.

Available activities are currently included in the insider risk policy you specified for Adaptive Protection. To detect other activities, you'll need to add them to the policy first.

Sending email with attachments to recipients outside the organiz ⌄

AND

Activity severity

>= ⌄ | High (risk score 67-100) ⌄

AND

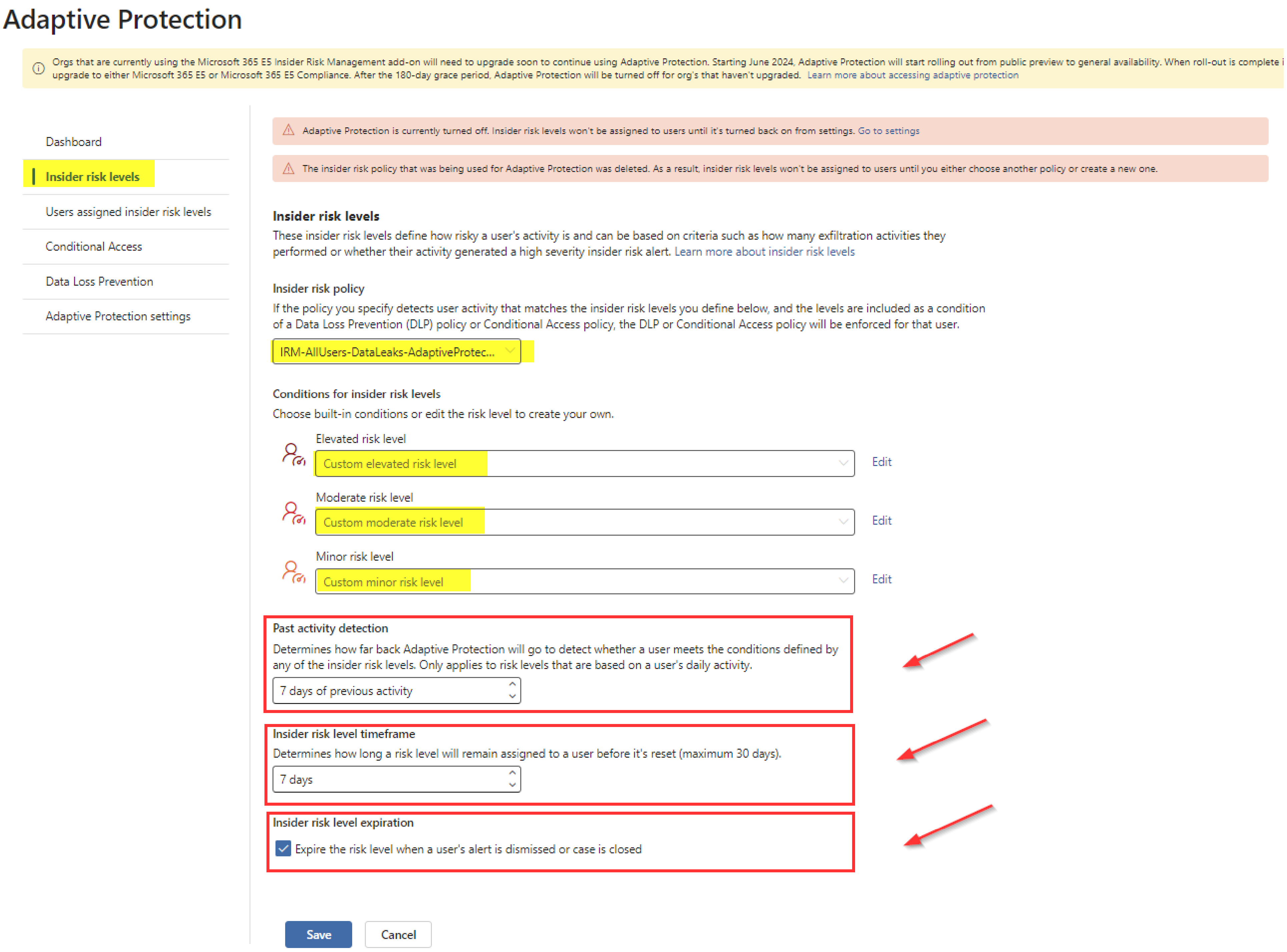
Activity occurrences during detection window

Specify number of times selected activities must be detected within the specified 'Past activity detection' period. This number isn't related to the number of events that might occur for an activity. For example, if the policy detects that a user downloaded 20 files from SharePoint in one day, that counts as one daily activity consisting of 20 events.

>= ⌄ | 1

nal

ssign this risk level to any user who has a future alert confirmed, even if onditions above aren't met.



Adaptive Protection

ⓘ Orgs that are currently using the Microsoft 365 E5 Insider Risk Management add-on will need to upgrade soon to continue using Adaptive Protection. Starting June 2024, Adaptive Protection will start rolling out from public preview to general availability. When roll-out is complete i upgrade to either Microsoft 365 E5 or Microsoft 365 E5 Compliance. After the 180-day grace period, Adaptive Protection will be turned off for org's that haven't upgraded. Learn more about accessing adaptive protection

⚠ Adaptive Protection is currently turned off. Insider risk levels won't be assigned to users until it's turned back on from settings. Go to settings

⚠ The insider risk policy that was being used for Adaptive Protection was deleted. As a result, insider risk levels won't be assigned to users until you either choose another policy or create a new one.

Insider risk levels

These insider risk levels define how risky a user's activity is and can be based on criteria such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. Learn more about insider risk levels

Insider risk policy

If the policy you specify detects user activity that matches the insider risk levels you define below, and the levels are included as a condition of a Data Loss Prevention (DLP) policy or Conditional Access policy, the DLP or Conditional Access policy will be enforced for that user.

IRM-AllUsers-DataLeaks-AdaptiveProtec...

Conditions for insider risk levels

Choose built-in conditions or edit the risk level to create your own.

Elevated risk level: Custom elevated risk level

Moderate risk level: Custom moderate risk level

Minor risk level: Custom minor risk level

Past activity detection

Determines how far back Adaptive Protection will go to detect whether a user meets the conditions defined by any of the insider risk levels. Only applies to risk levels that are based on a user's daily activity.

7 days of previous activity

Insider risk level timeframe

Determines how long a risk level will remain assigned to a user before it's reset (maximum 30 days).

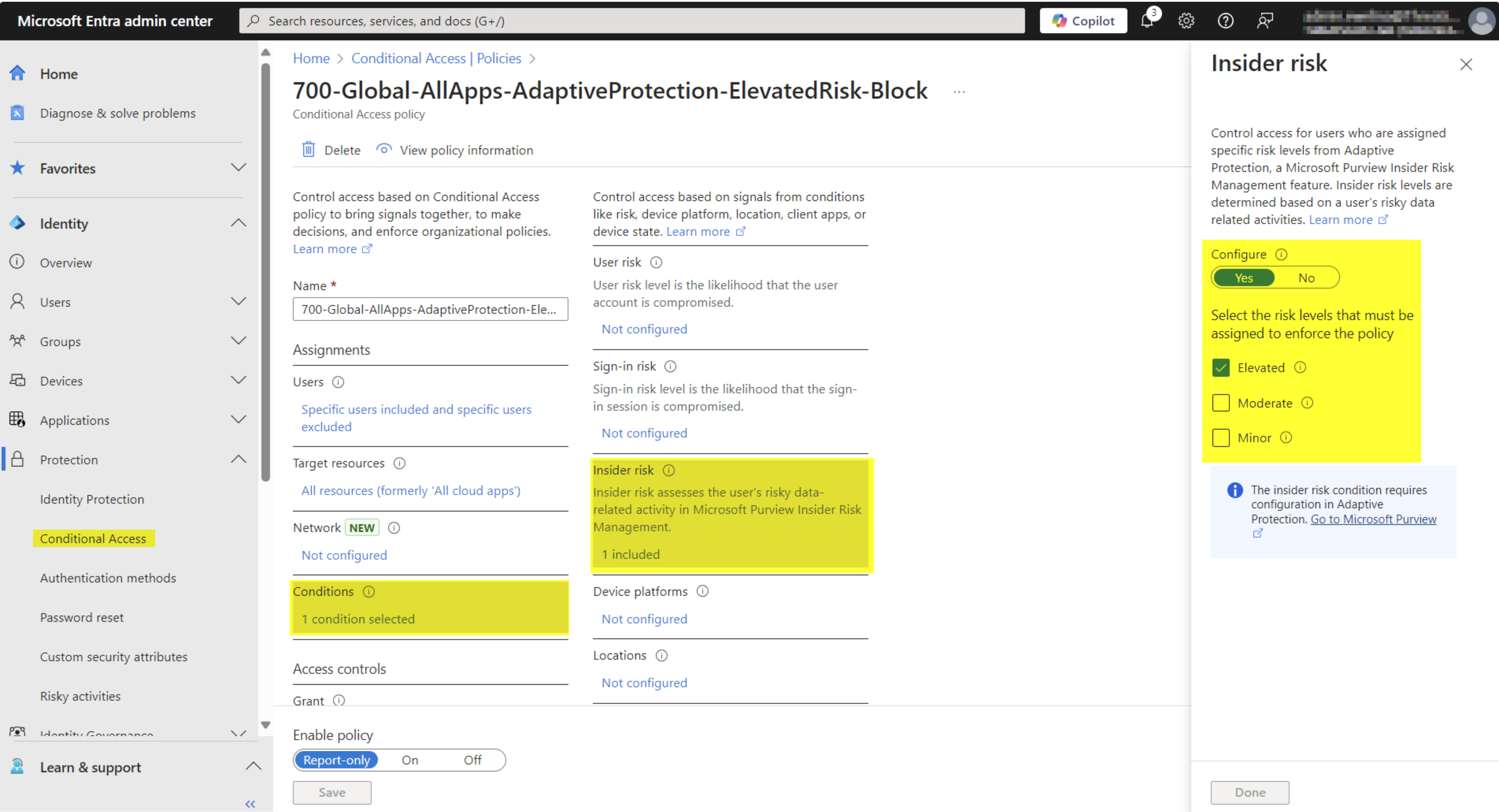
7 days

Insider risk level expiration

☑ Expire the risk level when a user's alert is dismissed or case is closed

Step 5

1. Configure global Insider Risk settings
2. Create/ edit Insider Risk Management policy
3. Configure insider risk level settings
4. Customise an insider risk level for your policy
5. **Create/ edit a Conditional Access policy**
6. Turn on Adaptive Protection



700-Global-AllApps-AdaptiveProtection-ElevatedRisk-Block

Conditional Access policy

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

Name *
700-Global-AllApps-AdaptiveProtection-Ele...

Assignments

Users
Specific users included and specific users excluded

Target resources
All resources (formerly 'All cloud apps')

Network NEW
Not configured

Conditions
1 condition selected

Access controls

Grant

Enable policy
[✓ Report-only] On Off

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk
User risk level is the likelihood that the user account is compromised.
Not configured

Sign-in risk
Sign-in risk level is the likelihood that the sign-in session is compromised.
Not configured

Insider risk
Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.
1 included

Device platforms
Not configured

Locations
Not configured

Insider risk

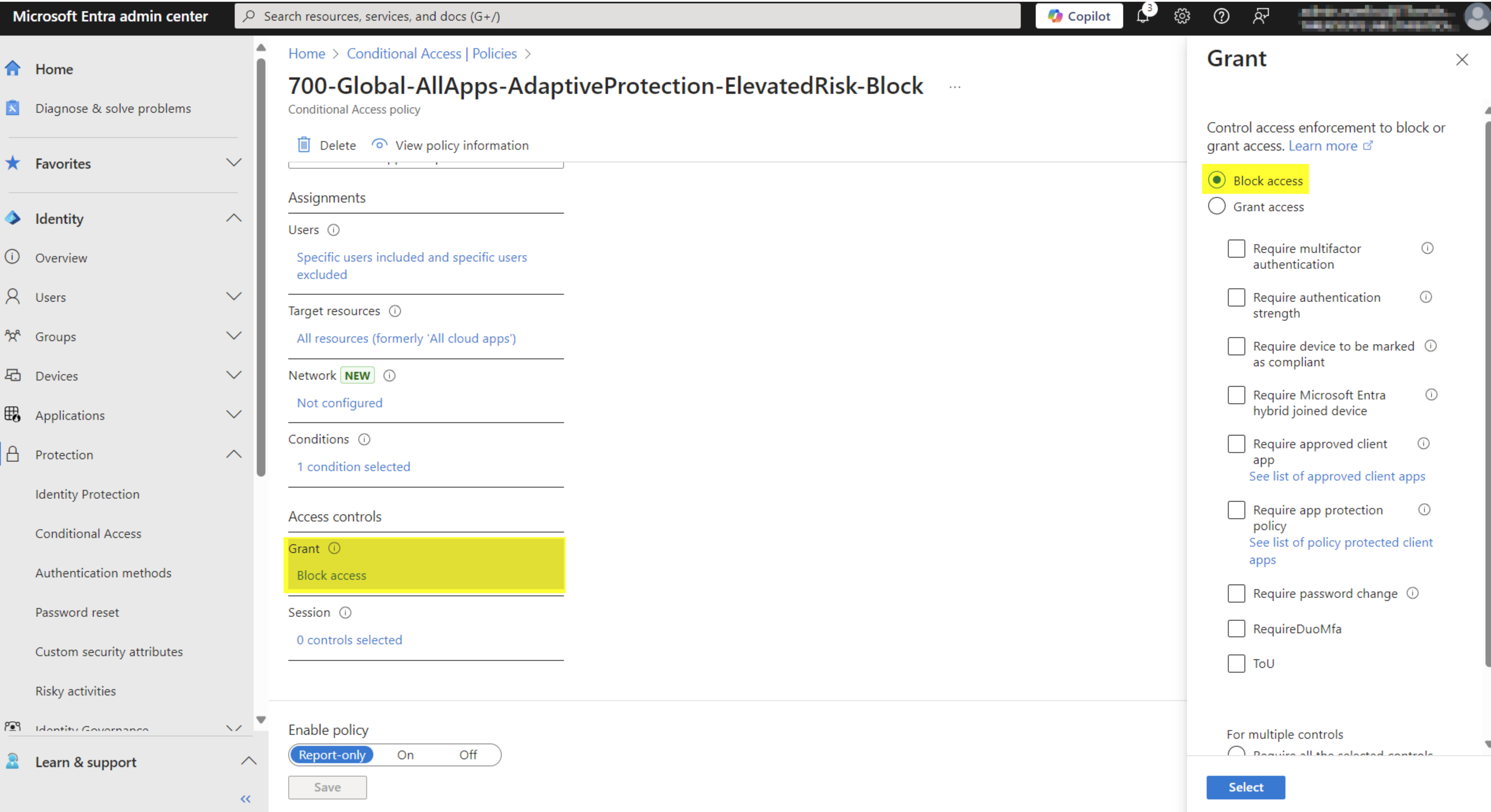
Control access for users who are assigned specific risk levels from Adaptive Protection, a Microsoft Purview Insider Risk Management feature. Insider risk levels are determined based on a user's risky data related activities. Learn more

Configure
[✓ Yes] No

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

☑ Elevated
□ Moderate
□ Minor

The insider risk condition requires configuration in Adaptive Protection. Go to Microsoft Purview



Microsoft Entra admin center

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

Copilot

3

[redacted]

Home

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

Identity Governance

Learn & support

Home > Conditional Access | Policies >

700-Global-AllApps-AdaptiveProtection-ElevatedRisk-Block

Conditional Access policy

Delete   View policy information

Assignments

Users

Specific users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps')

Network NEW

Not configured

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

[✓ Report-only]   On   Off

Save

Grant

Control access enforcement to block or grant access. Learn more

● Block access

○ Grant access

□ Require multifactor authentication

□ Require authentication strength

□ Require device to be marked as compliant

□ Require Microsoft Entra hybrid joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy
See list of policy protected client apps

□ Require password change

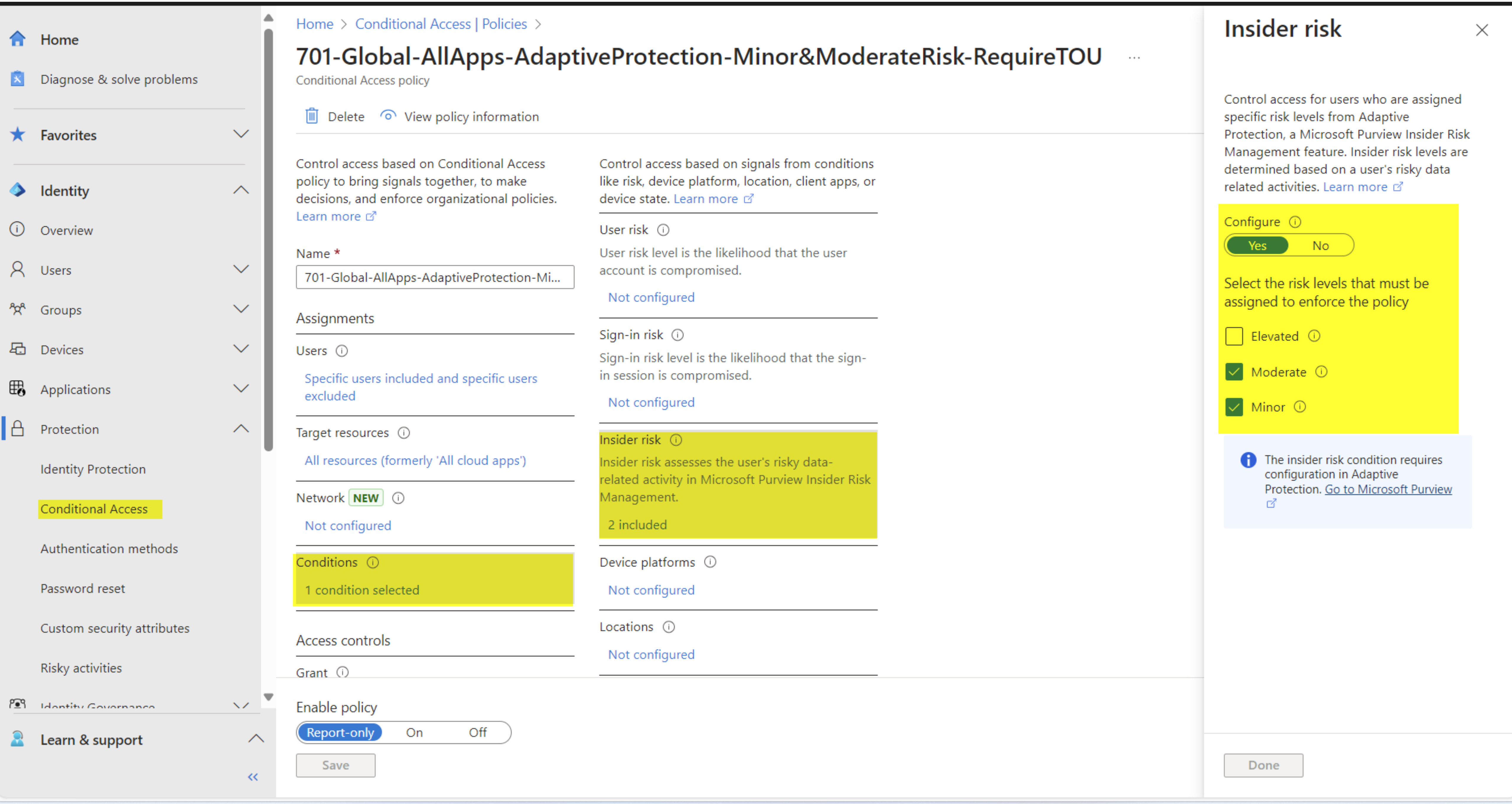
□ RequireDuoMfa

□ ToU

For multiple controls

○ Require all the selected controls

Select



Home > Conditional Access | Policies >

701-Global-AllApps-AdaptiveProtection-Minor&ModerateRisk-RequireTOU ...

Conditional Access policy

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

Name *

701-Global-AllApps-AdaptiveProtection-Mi...

Assignments

Users ⓘ

Specific users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Not configured

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Enable policy

[✓ Report-only] On Off

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk ⓘ

User risk level is the likelihood that the user account is compromised.

Not configured

Sign-in risk ⓘ

Sign-in risk level is the likelihood that the sign-in session is compromised.

Not configured

Insider risk ⓘ

Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.

2 included

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

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

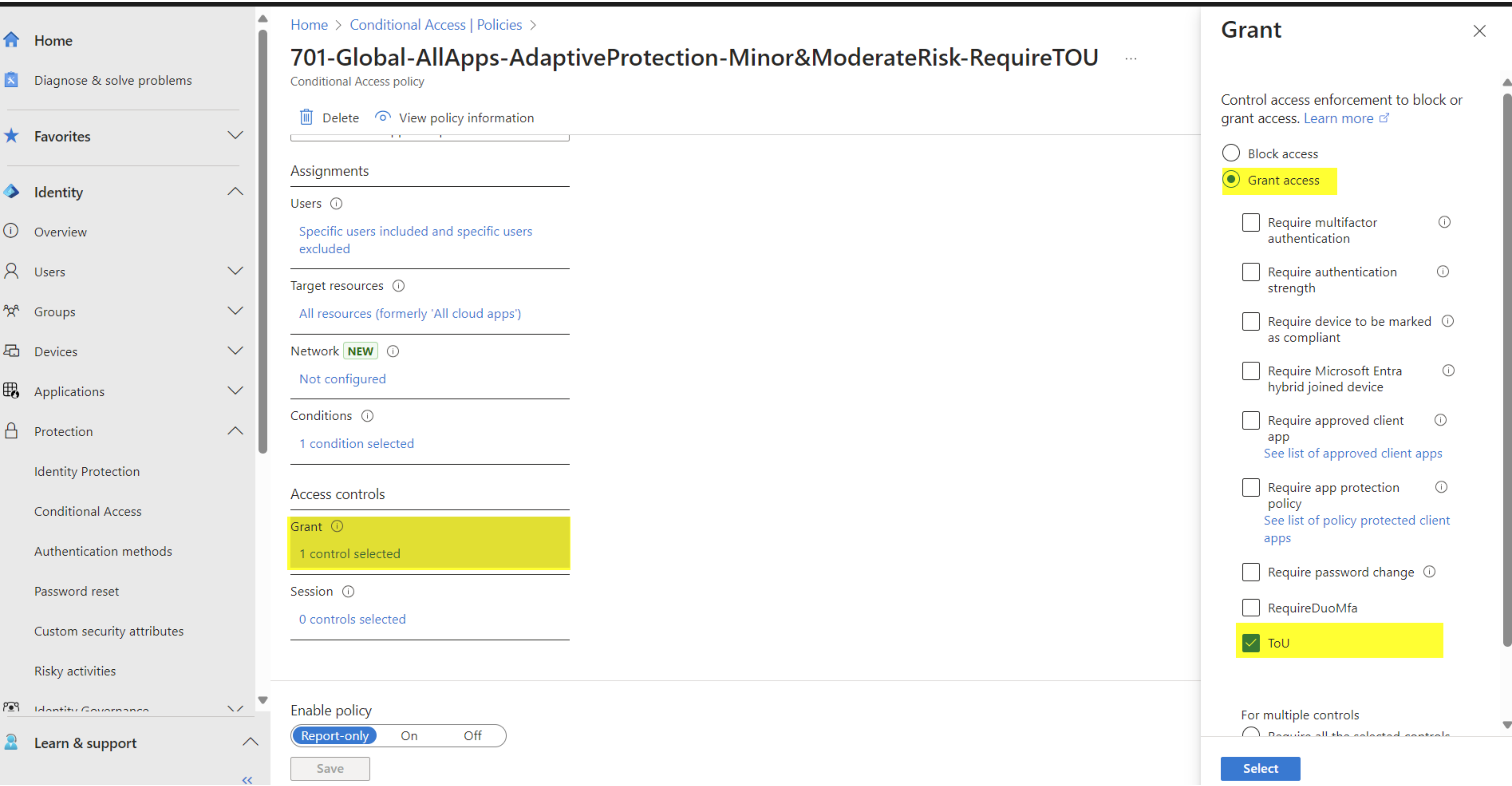
Select the risk levels that must be assigned to enforce the policy

☐ Elevated ⓘ

☑ Moderate ⓘ

☑ Minor ⓘ

The insider risk condition requires configuration in Adaptive Protection. Go to Microsoft Purview



Home
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Identity Governance
Learn & support

Home > Conditional Access | Policies >

701-Global-AllApps-AdaptiveProtection-Minor&ModerateRisk-RequireTOU

Conditional Access policy

Delete   View policy information

Assignments

Users ⓘ
Specific users included and specific users excluded

Target resources ⓘ
All resources (formerly 'All cloud apps')

Network NEW ⓘ
Not configured

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

Enable policy
[✓ Report-only] On Off

Save

Grant

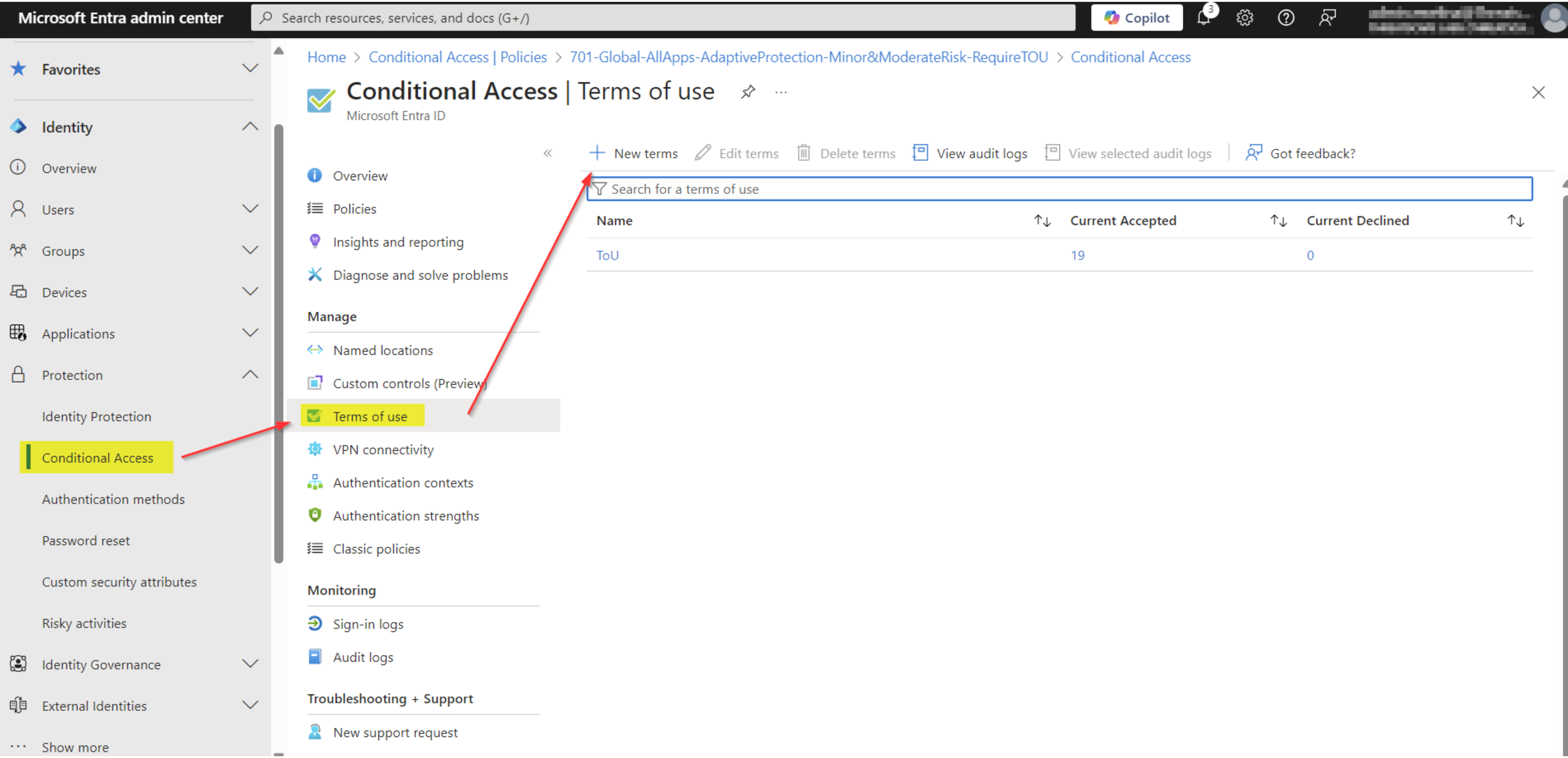
Control access enforcement to block or grant access. Learn more

○ Block access
● Grant access

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

For multiple controls
○ Require all the selected controls

Select

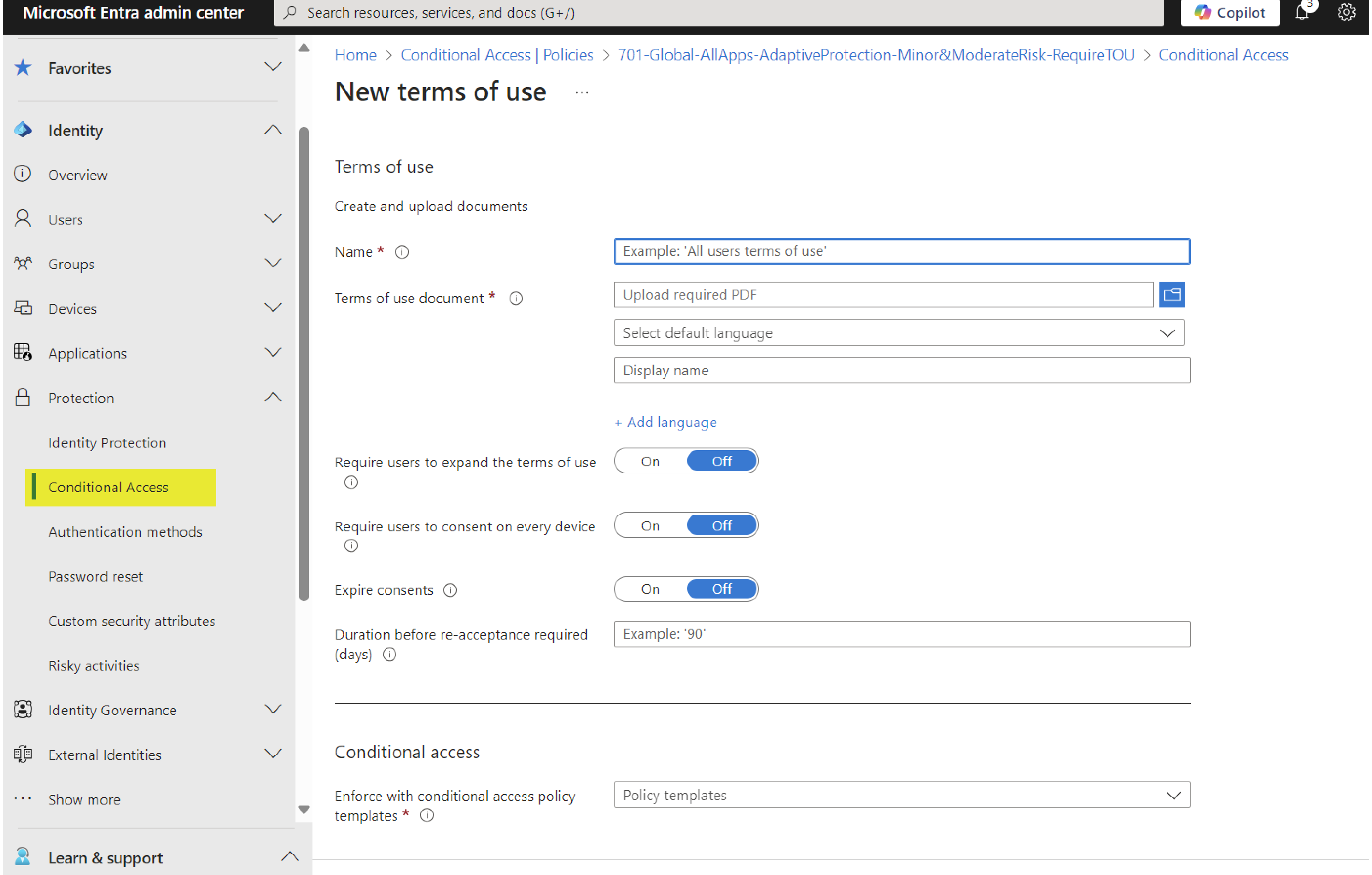


Home > Conditional Access | Policies > 701-Global-AllApps-AdaptiveProtection-Minor&ModerateRisk-RequireTOU > Conditional Access

Conditional Access | Terms of use

Microsoft Entra ID

Name	Current Accepted	Current Declined
ToU	19	0



Home > Conditional Access | Policies > 701-Global-AllApps-AdaptiveProtection-Minor&ModerateRisk-RequireTOU > Conditional Access

New terms of use ...

Terms of use

Create and upload documents

Name * ⓘ Example: 'All users terms of use'

Terms of use document * ⓘ Upload required PDF

Select default language

Display name

+ Add language

Require users to expand the terms of use ⓘ On Off

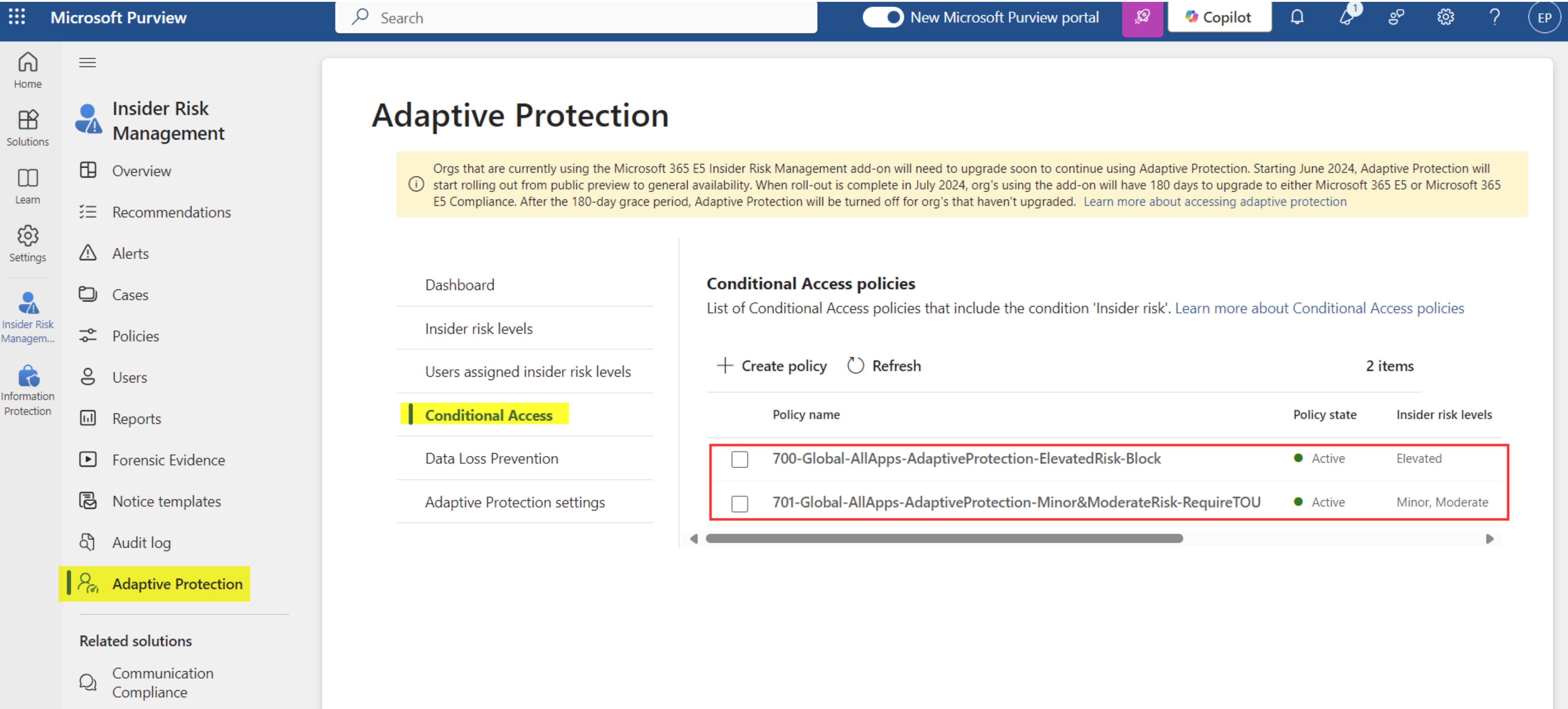
Require users to consent on every device ⓘ On Off

Expire consents ⓘ On Off

Duration before re-acceptance required (days) ⓘ Example: '90'

Conditional access

Enforce with conditional access policy templates * ⓘ Policy templates



Adaptive Protection

Orgs that are currently using the Microsoft 365 E5 Insider Risk Management add-on will need to upgrade soon to continue using Adaptive Protection. Starting June 2024, Adaptive Protection will start rolling out from public preview to general availability. When roll-out is complete in July 2024, org's using the add-on will have 180 days to upgrade to either Microsoft 365 E5 or Microsoft 365 E5 Compliance. After the 180-day grace period, Adaptive Protection will be turned off for org's that haven't upgraded. Learn more about accessing adaptive protection

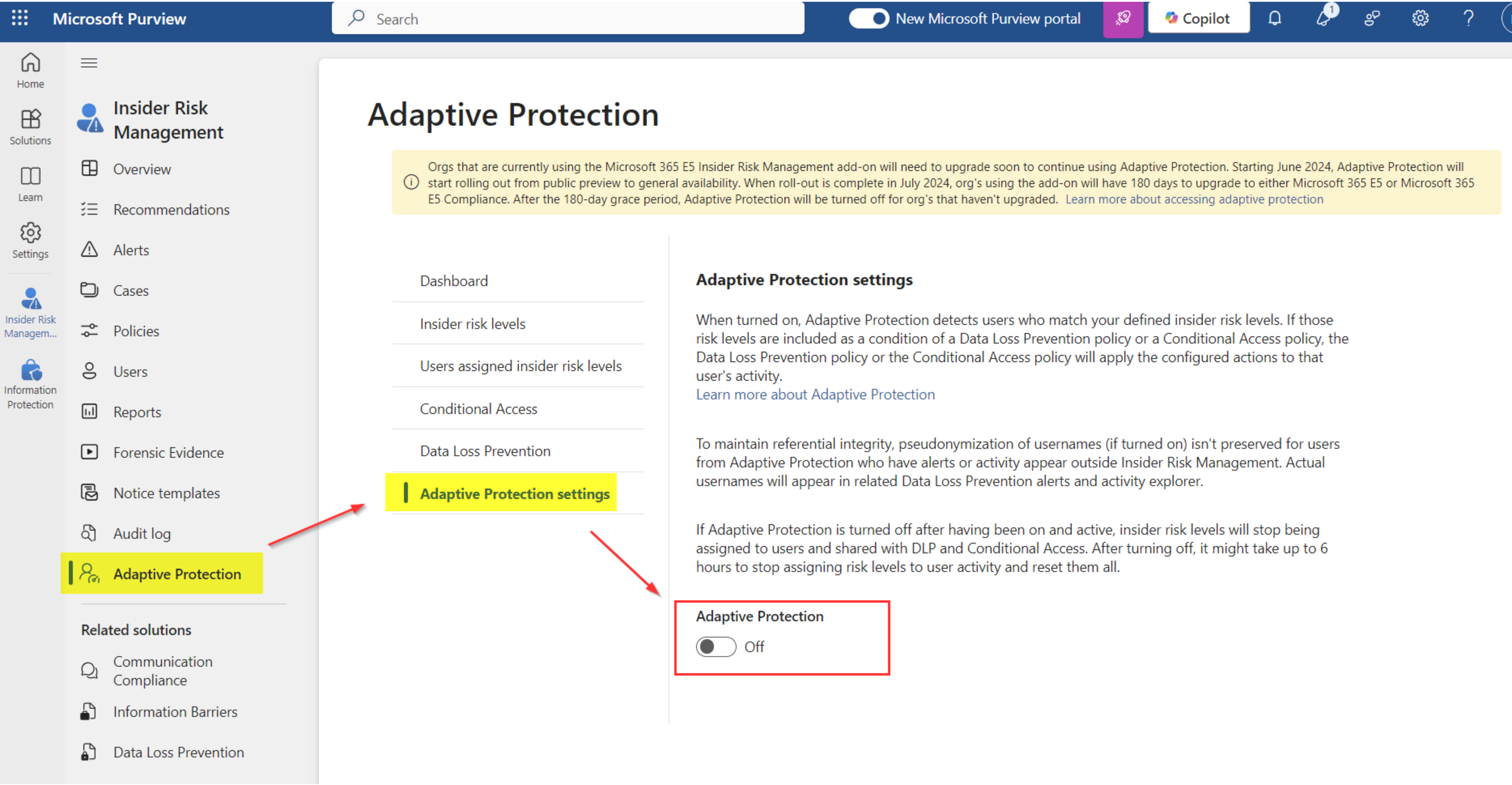
Conditional Access policies

List of Conditional Access policies that include the condition 'Insider risk'. Learn more about Conditional Access policies

	Policy name	Policy state	Insider risk levels
□	700-Global-AllApps-AdaptiveProtection-ElevatedRisk-Block	● Active	Elevated
□	701-Global-AllApps-AdaptiveProtection-Minor&ModerateRisk-RequireTOU	● Active	Minor, Moderate

Step 6

1. Configure global Insider Risk settings
2. Create/ edit Insider Risk Management policy
3. Configure insider risk level settings
4. Customise an insider risk level for your policy
5. Create/ edit a Conditional Access policy
6. Turn on Adaptive Protection



Adaptive Protection

Orgs that are currently using the Microsoft 365 E5 Insider Risk Management add-on will need to upgrade soon to continue using Adaptive Protection. Starting June 2024, Adaptive Protection will start rolling out from public preview to general availability. When roll-out is complete in July 2024, org's using the add-on will have 180 days to upgrade to either Microsoft 365 E5 or Microsoft 365 E5 Compliance. After the 180-day grace period, Adaptive Protection will be turned off for org's that haven't upgraded. Learn more about accessing adaptive protection

Adaptive Protection settings

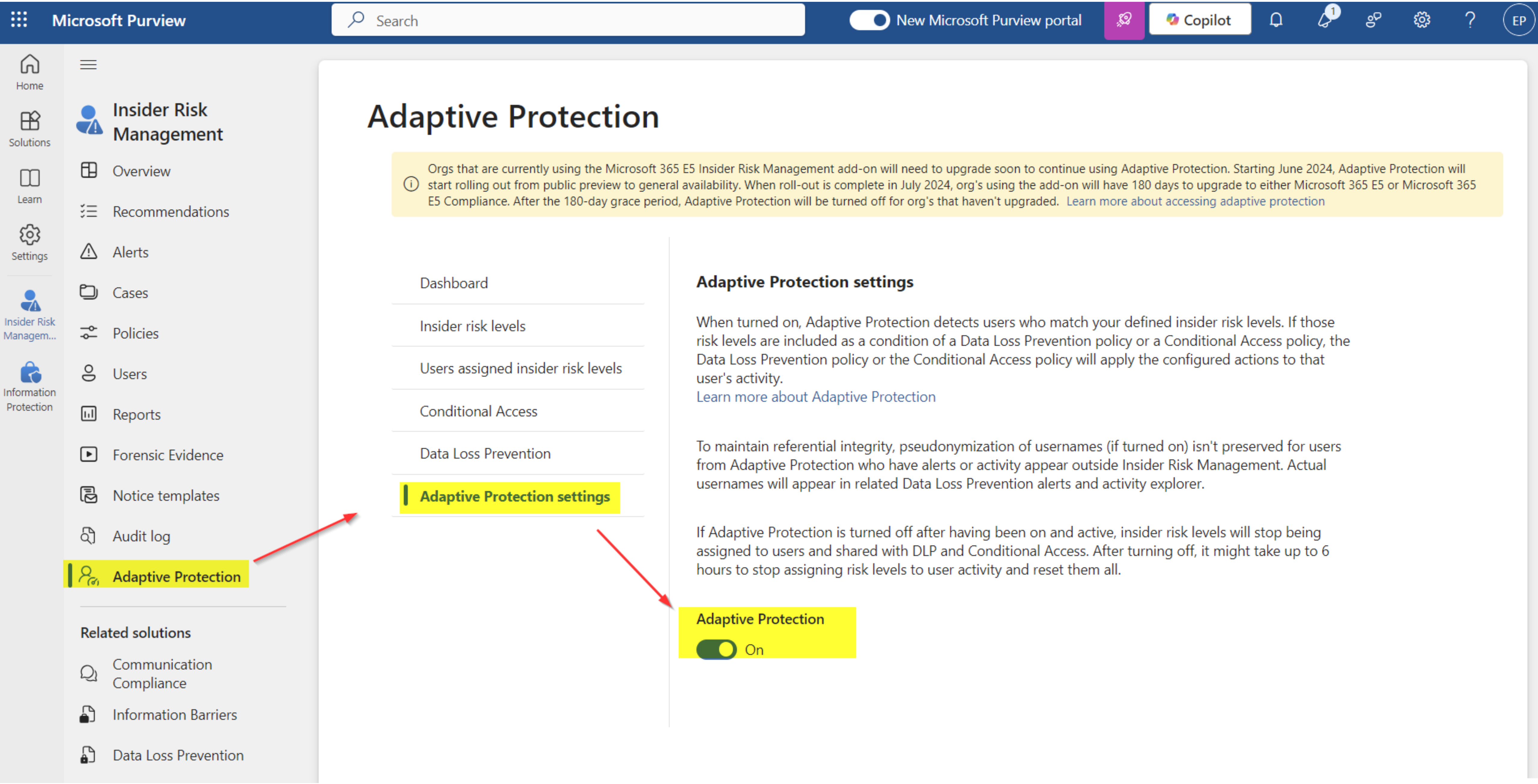
When turned on, Adaptive Protection detects users who match your defined insider risk levels. If those risk levels are included as a condition of a Data Loss Prevention policy or a Conditional Access policy, the Data Loss Prevention policy or the Conditional Access policy will apply the configured actions to that user's activity.
Learn more about Adaptive Protection

To maintain referential integrity, pseudonymization of usernames (if turned on) isn't preserved for users from Adaptive Protection who have alerts or activity appear outside Insider Risk Management. Actual usernames will appear in related Data Loss Prevention alerts and activity explorer.

If Adaptive Protection is turned off after having been on and active, insider risk levels will stop being assigned to users and shared with DLP and Conditional Access. After turning off, it might take up to 6 hours to stop assigning risk levels to user activity and reset them all.

Adaptive Protection

○ Off



Adaptive Protection

Orgs that are currently using the Microsoft 365 E5 Insider Risk Management add-on will need to upgrade soon to continue using Adaptive Protection. Starting June 2024, Adaptive Protection will start rolling out from public preview to general availability. When roll-out is complete in July 2024, org's using the add-on will have 180 days to upgrade to either Microsoft 365 E5 or Microsoft 365 E5 Compliance. After the 180-day grace period, Adaptive Protection will be turned off for org's that haven't upgraded. Learn more about accessing adaptive protection

Adaptive Protection settings

When turned on, Adaptive Protection detects users who match your defined insider risk levels. If those risk levels are included as a condition of a Data Loss Prevention policy or a Conditional Access policy, the Data Loss Prevention policy or the Conditional Access policy will apply the configured actions to that user's activity.
Learn more about Adaptive Protection

To maintain referential integrity, pseudonymization of usernames (if turned on) isn't preserved for users from Adaptive Protection who have alerts or activity appear outside Insider Risk Management. Actual usernames will appear in related Data Loss Prevention alerts and activity explorer.

If Adaptive Protection is turned off after having been on and active, insider risk levels will stop being assigned to users and shared with DLP and Conditional Access. After turning off, it might take up to 6 hours to stop assigning risk levels to user activity and reset them all.

Adaptive Protection

On

Conclusion

- Configure global Insider Risk settings
- Fine-tune your Insider Risk Management (IRM) policies as much as you can
- Customise insider risk levels for your IRM policies
- Start with a report-only mode for your Conditional Access policies
- Refine policies if needed
- Turn on Conditional Access policies only when sure that false positives have been minimised

Q&A

Thank you!