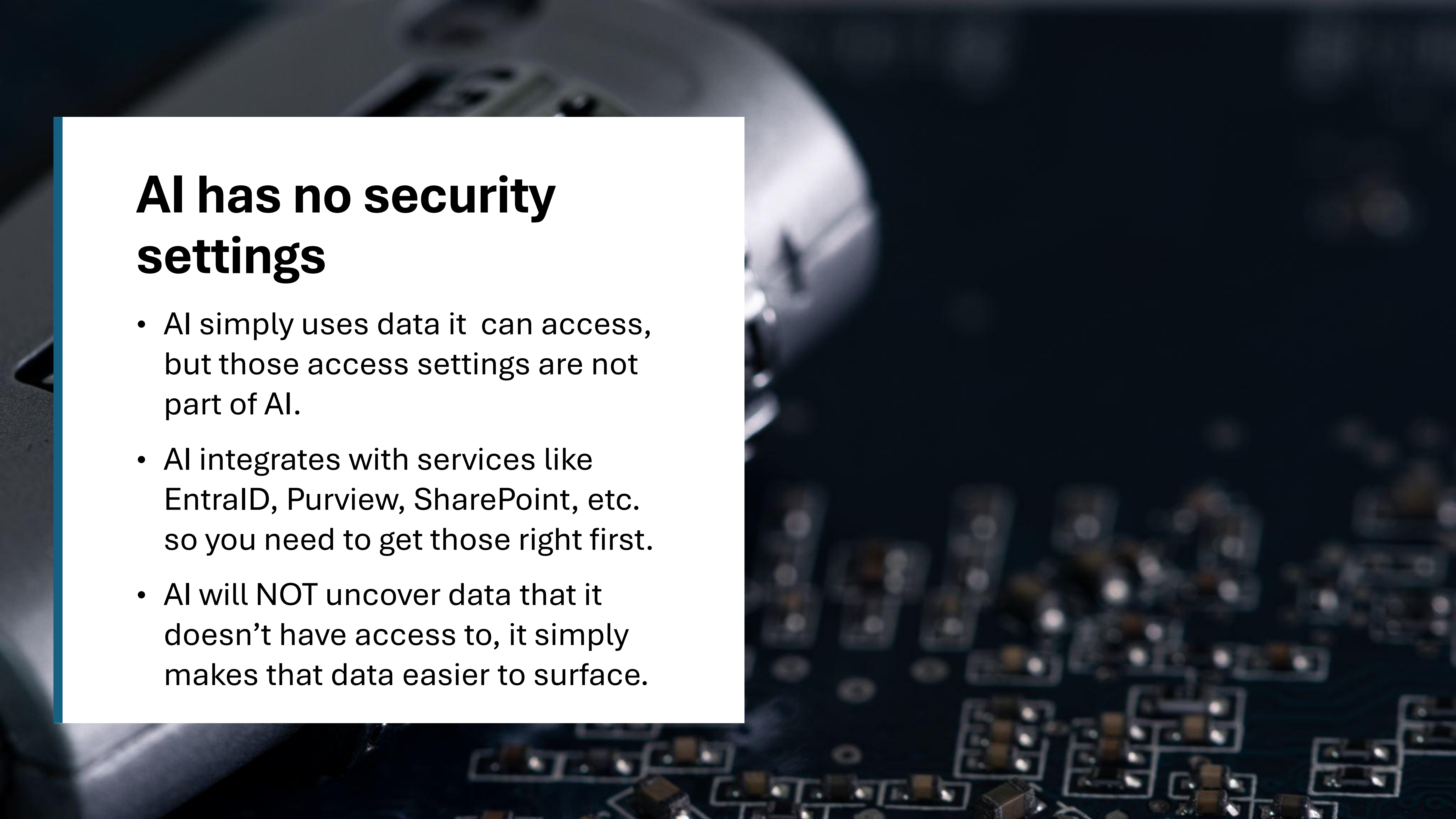
Governing AI with Microsoft 365 March 2025

@directorcia

http://about.me/ciaops

Assumptions

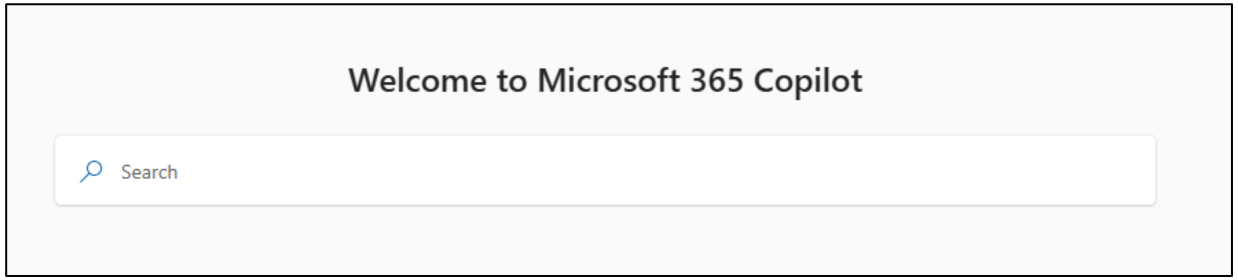
- The license of choice is Business Premium.
- Services like Exchange Online have been configured to best practices.
- The focus for good AI security should be on data item security.
- Data item compliance policies will require consultation with customer.



AI has no security settings

- AI simply uses data it can access, but those access settings are not part of AI.
- AI integrates with services like EntraID, Purview, SharePoint, etc. so you need to get those right first.
- AI will NOT uncover data that it doesn’t have access to, it simply makes that data easier to surface.

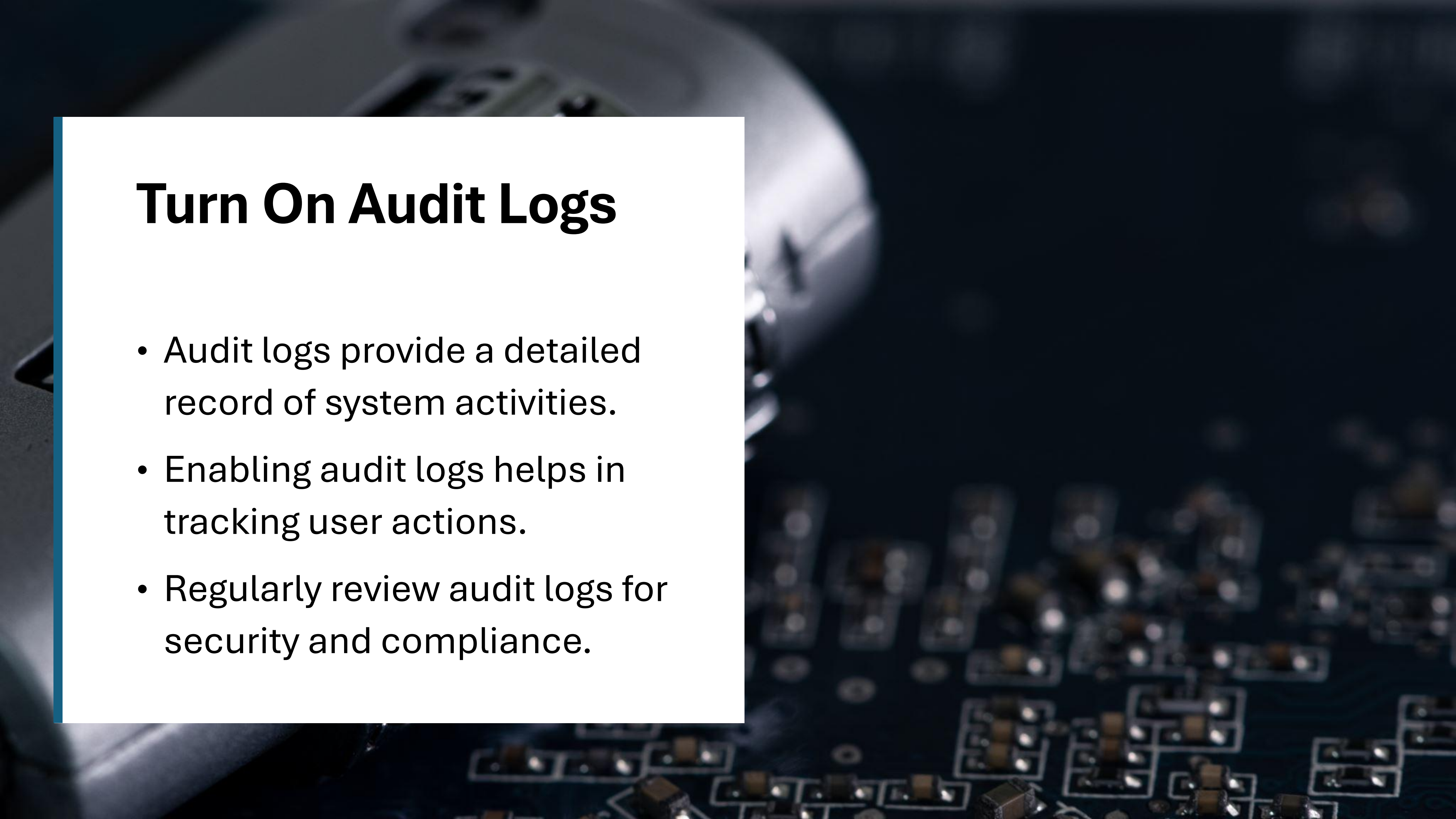
Start with search



Welcome to Microsoft 365 Copilot

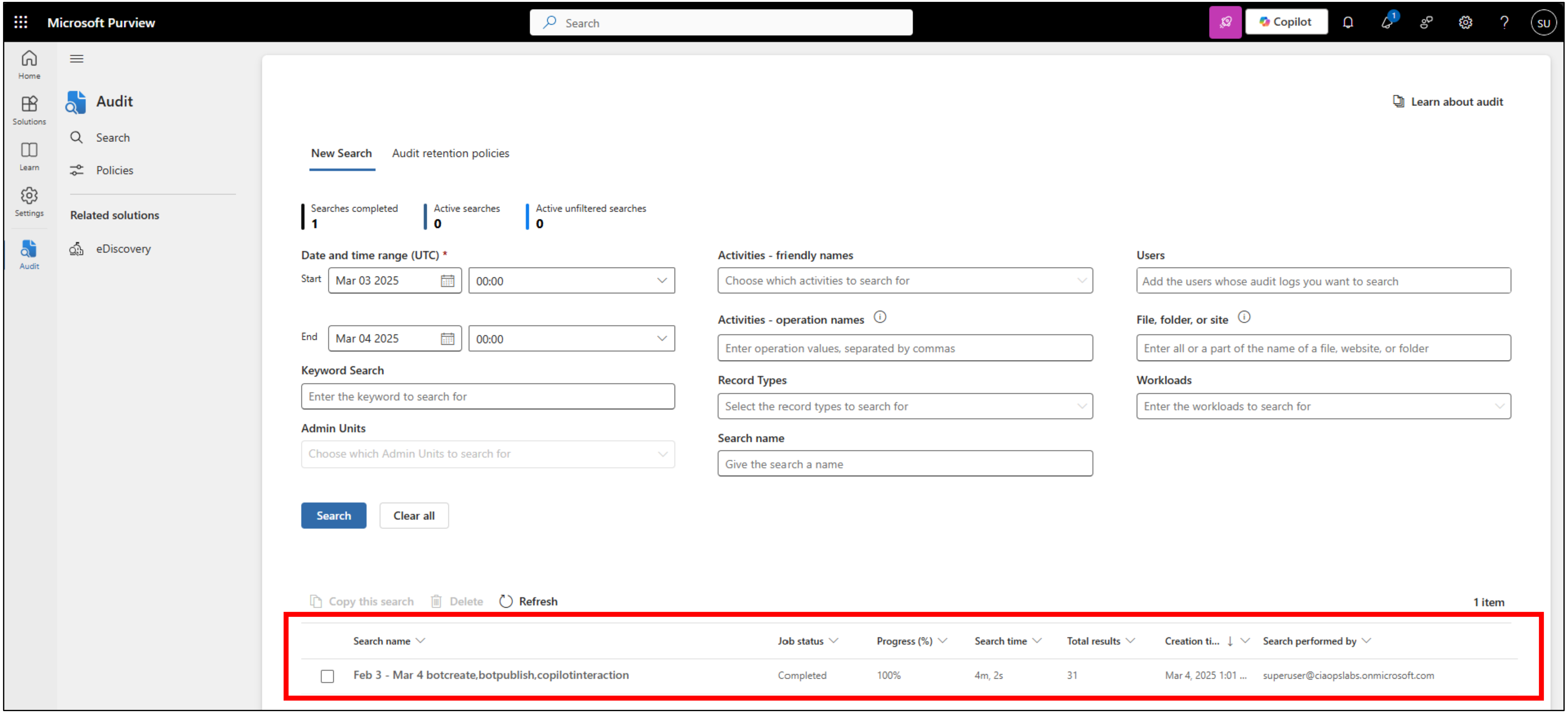
Try these search terms

- Customer address
- Company acquisitions
- Confidential
- Secret
- Payroll



Turn On Audit Logs

- Audit logs provide a detailed record of system activities.
- Enabling audit logs helps in tracking user actions.
- Regularly review audit logs for security and compliance.



Audit

Search

Policies

Related solutions

eDiscovery

Learn about audit

New Search | Audit retention policies

Searches completed 1 | Active searches 0 | Active unfiltered searches 0

Date and time range (UTC) *

Start: Mar 03 2025 | 00:00

End: Mar 04 2025 | 00:00

Keyword Search: Enter the keyword to search for

Admin Units: Choose which Admin Units to search for

Activities - friendly names: Choose which activities to search for

Activities - operation names: Enter operation values, separated by commas

Record Types: Select the record types to search for

Search name: Give the search a name

Users: Add the users whose audit logs you want to search

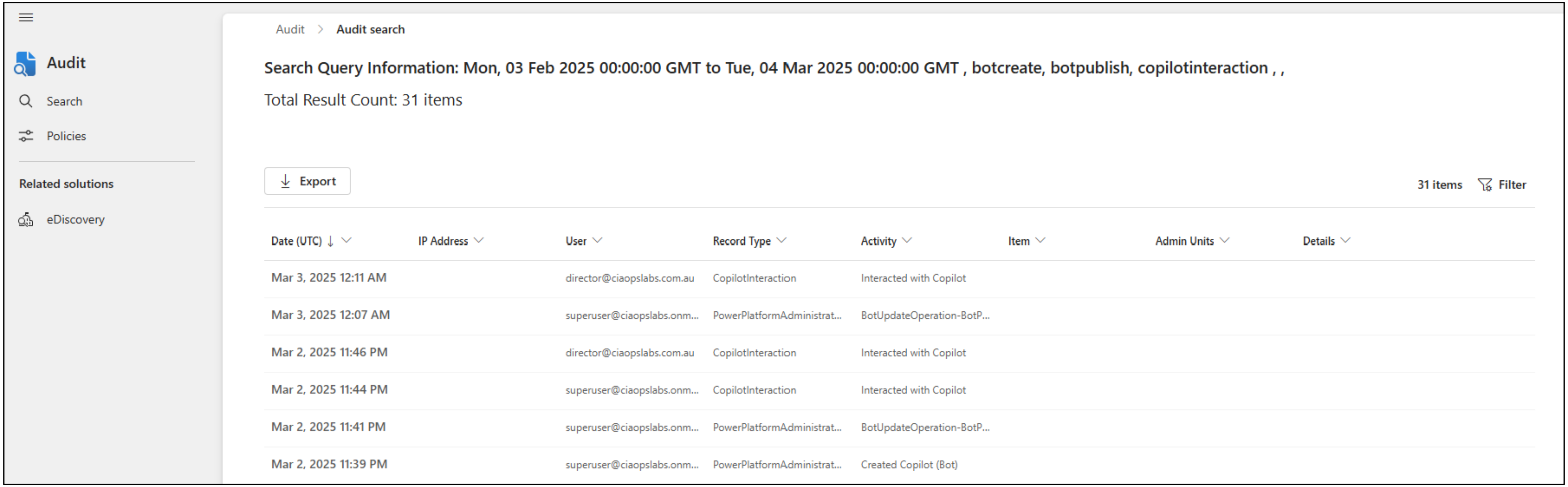
File, folder, or site: Enter all or a part of the name of a file, website, or folder

Workloads: Enter the workloads to search for

Search | Clear all

Copy this search | Delete | Refresh | 1 item

	Search name	Job status	Progress (%)	Search time	Total results	Creation ti... ↓	Search performed by
□	Feb 3 - Mar 4 botcreate,botpublish,copilotinteraction	Completed	100%	4m, 2s	31	Mar 4, 2025 1:01 ...	superuser@ciaopslabs.onmicrosoft.com



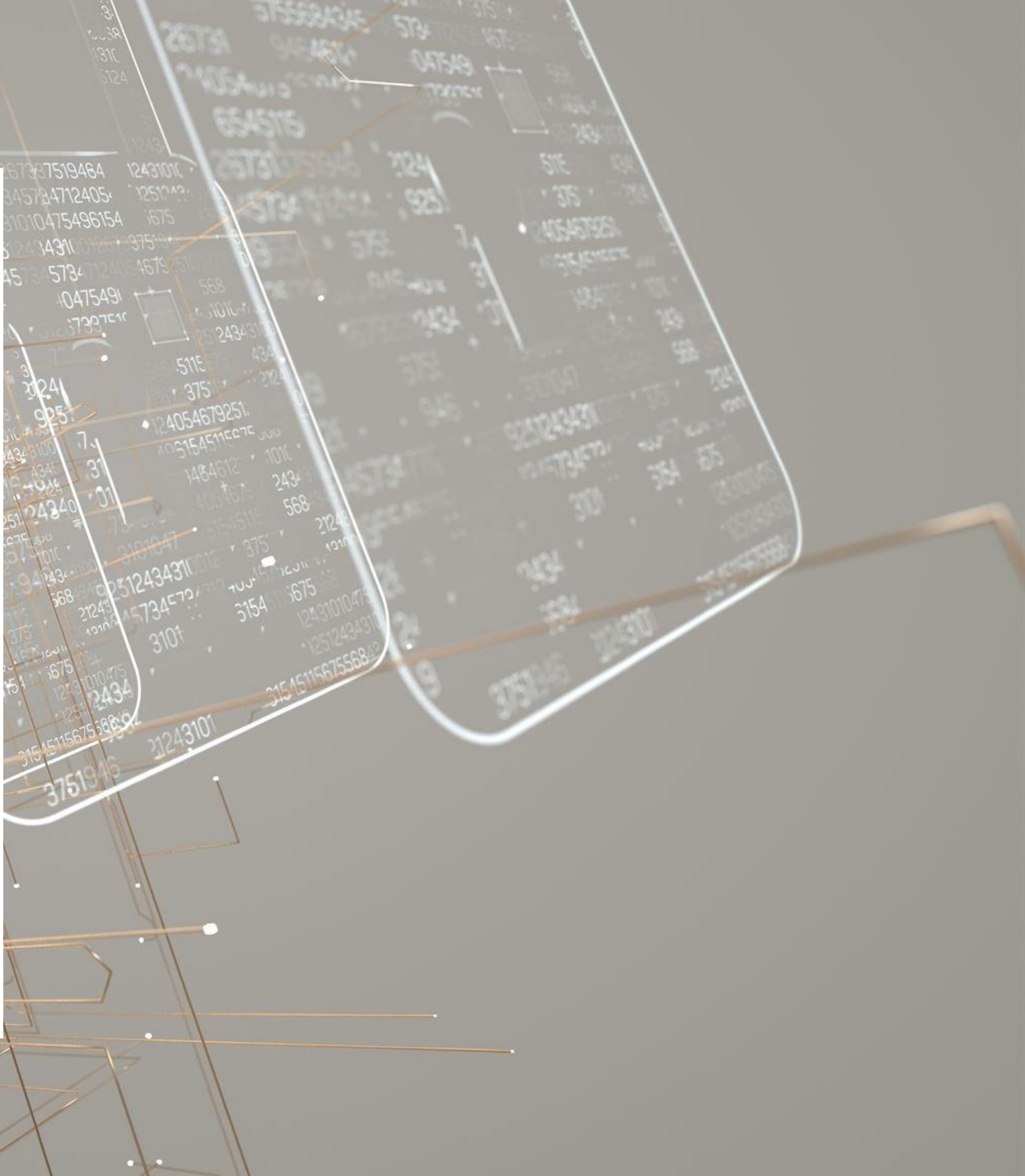
Search Query Information: Mon, 03 Feb 2025 00:00:00 GMT to Tue, 04 Mar 2025 00:00:00 GMT , botcreate, botpublish, copilotinteraction , ,

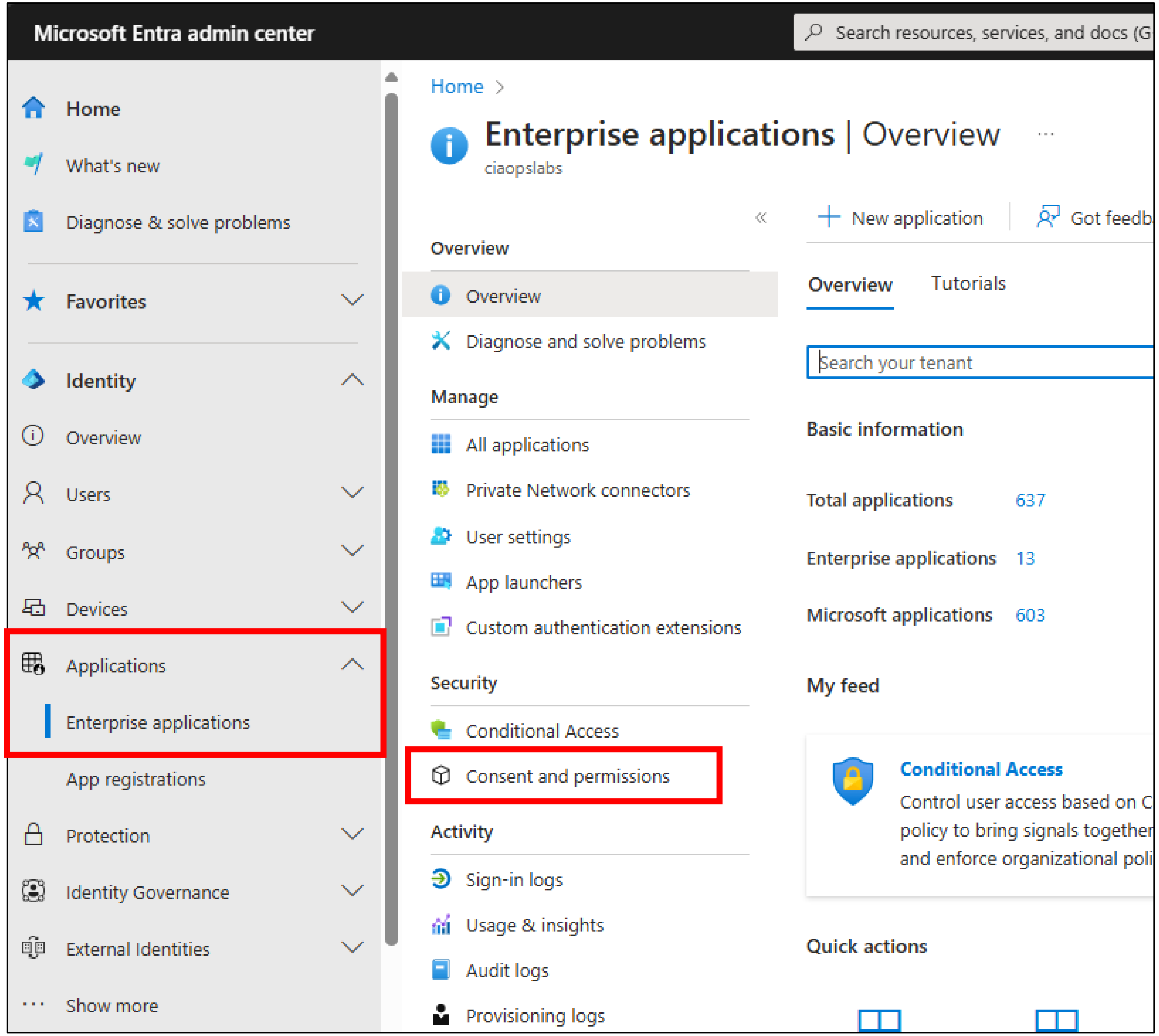
Total Result Count: 31 items

Date (UTC)	IP Address	User	Record Type	Activity	Item	Admin Units	Details
Mar 3, 2025 12:11 AM		director@ciaopslabs.com.au	CopilotInteraction	Interacted with Copilot			
Mar 3, 2025 12:07 AM		superuser@ciaopslabs.onm...	PowerPlatformAdministrat...	BotUpdateOperation-BotP...			
Mar 2, 2025 11:46 PM		director@ciaopslabs.com.au	CopilotInteraction	Interacted with Copilot			
Mar 2, 2025 11:44 PM		superuser@ciaopslabs.onm...	CopilotInteraction	Interacted with Copilot			
Mar 2, 2025 11:41 PM		superuser@ciaopslabs.onm...	PowerPlatformAdministrat...	BotUpdateOperation-BotP...			
Mar 2, 2025 11:39 PM		superuser@ciaopslabs.onm...	PowerPlatformAdministrat...	Created Copilot (Bot)			

Protecting Identities

- Enable two-factor authentication wherever possible.
- Implement Conditional Access control.
- Perform an inventory of users and devices
- Control consent and permissions.





Enterprise applications | Overview

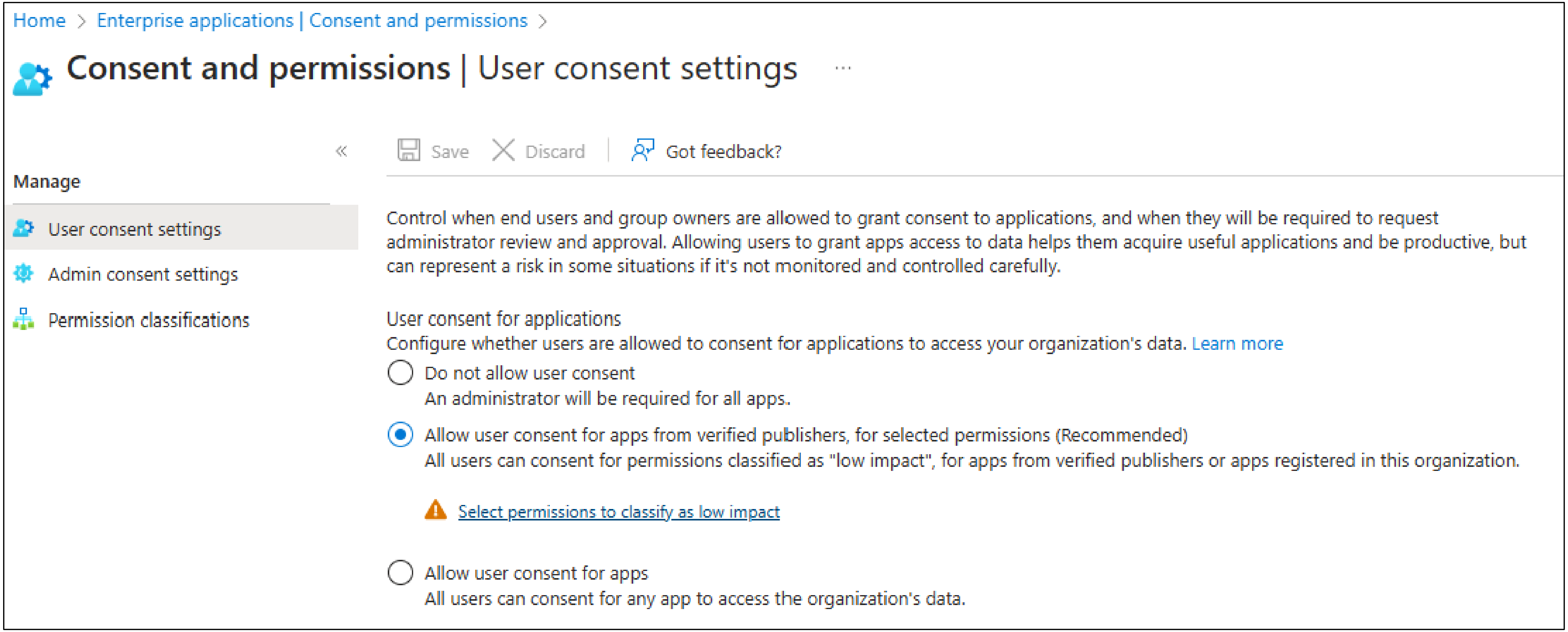
ciaopslabs

Basic information

Total applications	637
Enterprise applications	13
Microsoft applications	603

Conditional Access

Control user access based on C
policy to bring signals together
and enforce organizational poli



Home > Enterprise applications | Consent and permissions >

Consent and permissions | User consent settings ...

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

○ Do not allow user consent
An administrator will be required for all apps.

● Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

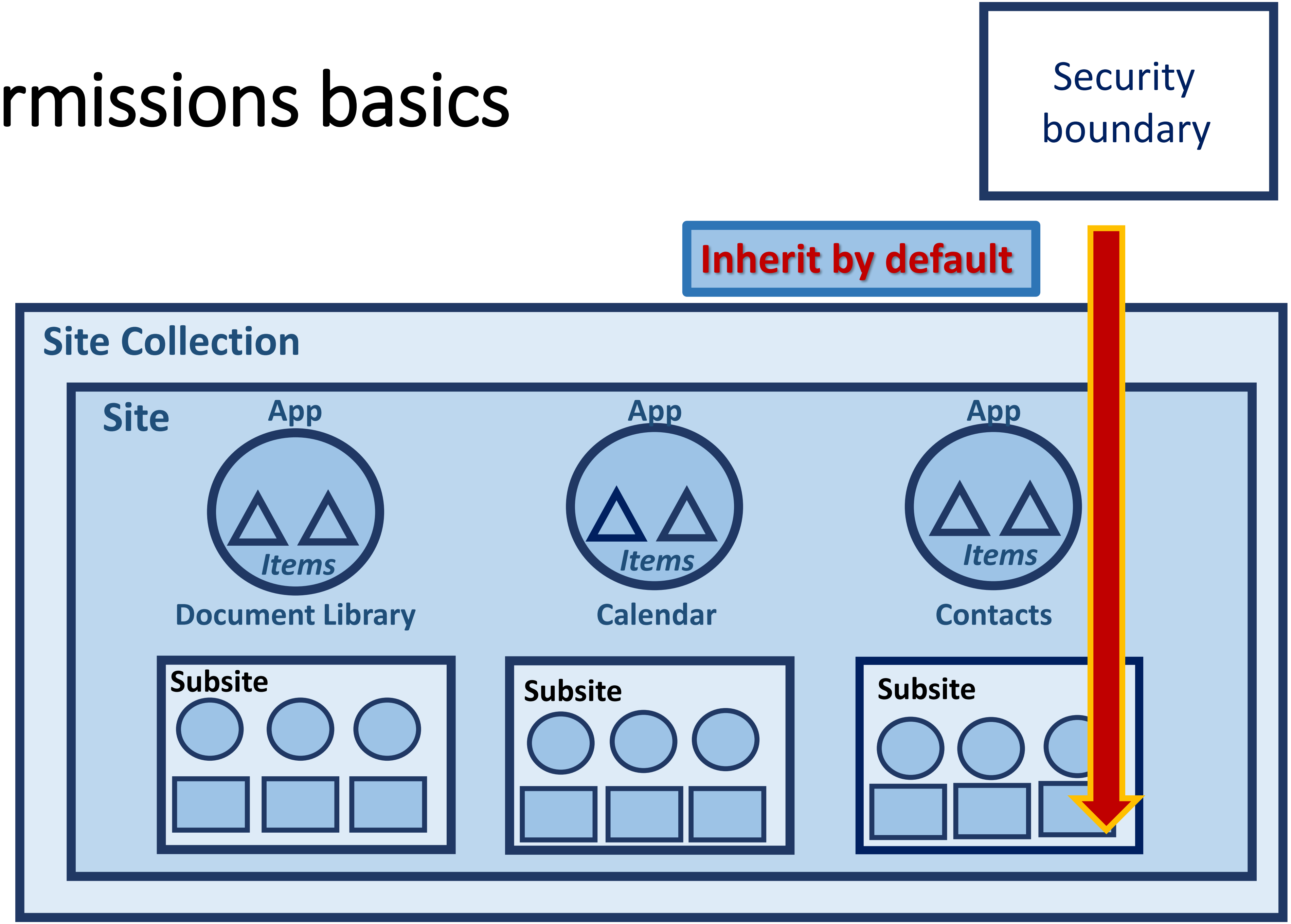
⚠ Select permissions to classify as low impact

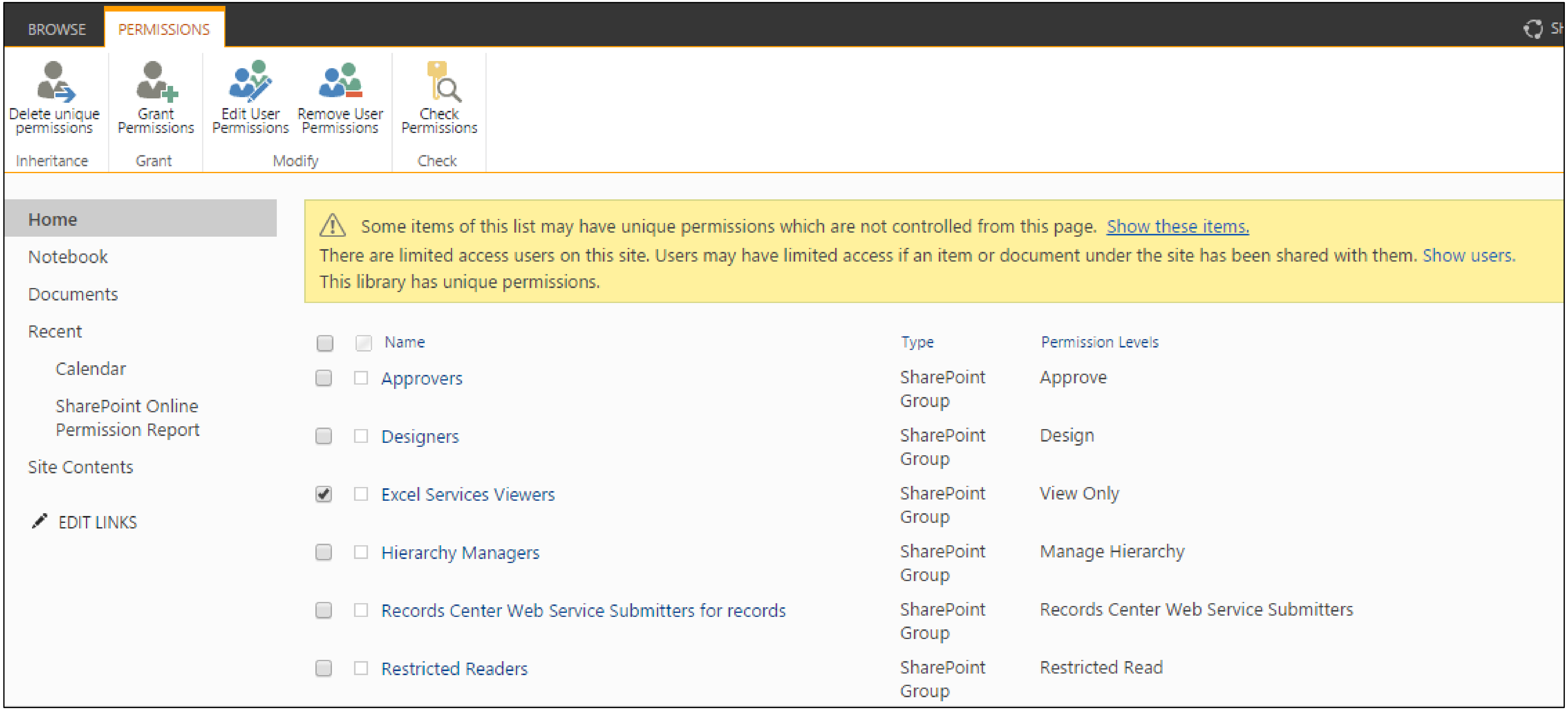
○ Allow user consent for apps
All users can consent for any app to access the organization's data.

Structure Data

- Organize data into structured silos for security.
- Best practice is wide not deep.
- Apply permissions from highest level first.
- Restructure to avoid complex permissions.

Permissions basics





⚠ Some items of this list may have unique permissions which are not controlled from this page. Show these items.
There are limited access users on this site. Users may have limited access if an item or document under the site has been shared with them. Show users.
This library has unique permissions.

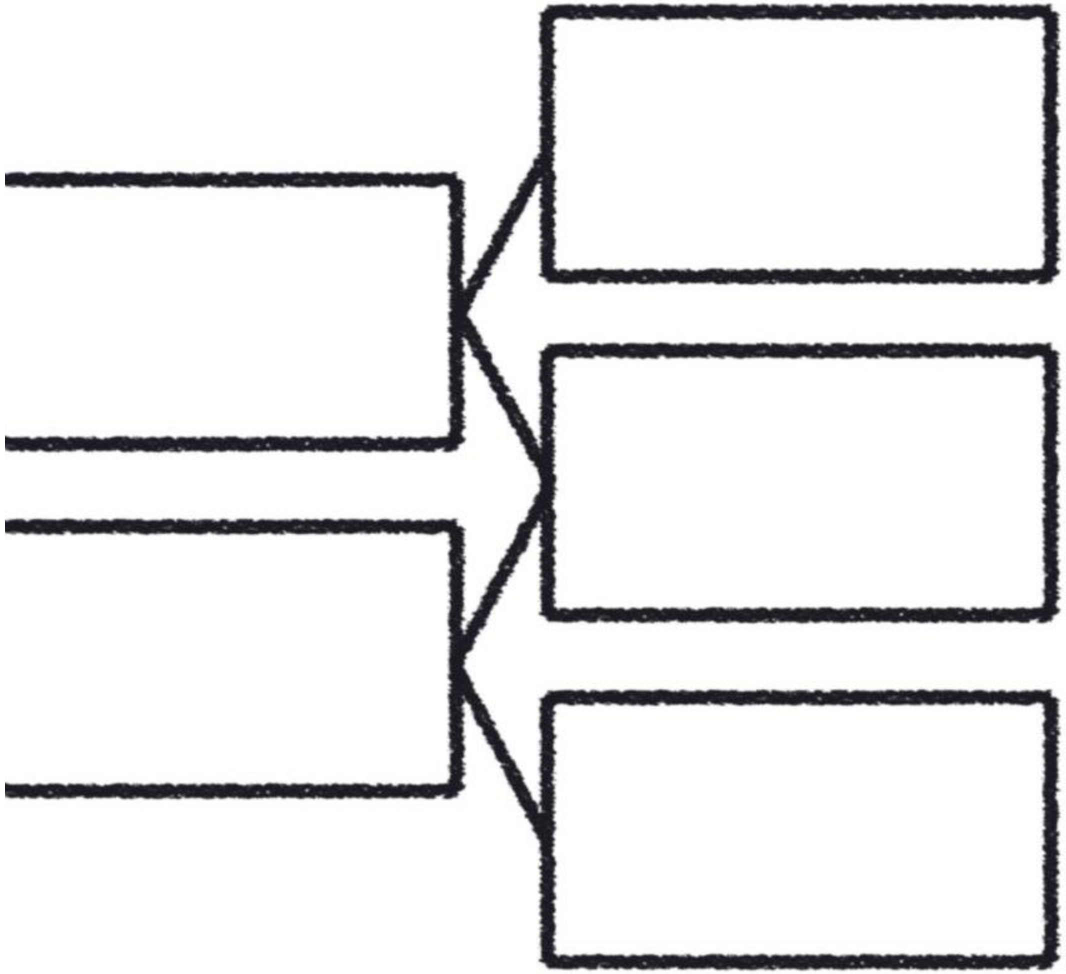
□	□	Name	Type	Permission Levels
□	□	Approvers	SharePoint Group	Approve
□	□	Designers	SharePoint Group	Design
☑	□	Excel Services Viewers	SharePoint Group	View Only
□	□	Hierarchy Managers	SharePoint Group	Manage Hierarchy
□	□	Records Center Web Service Submitters for records	SharePoint Group	Records Center Web Service Submitters
□	□	Restricted Readers	SharePoint Group	Restricted Read

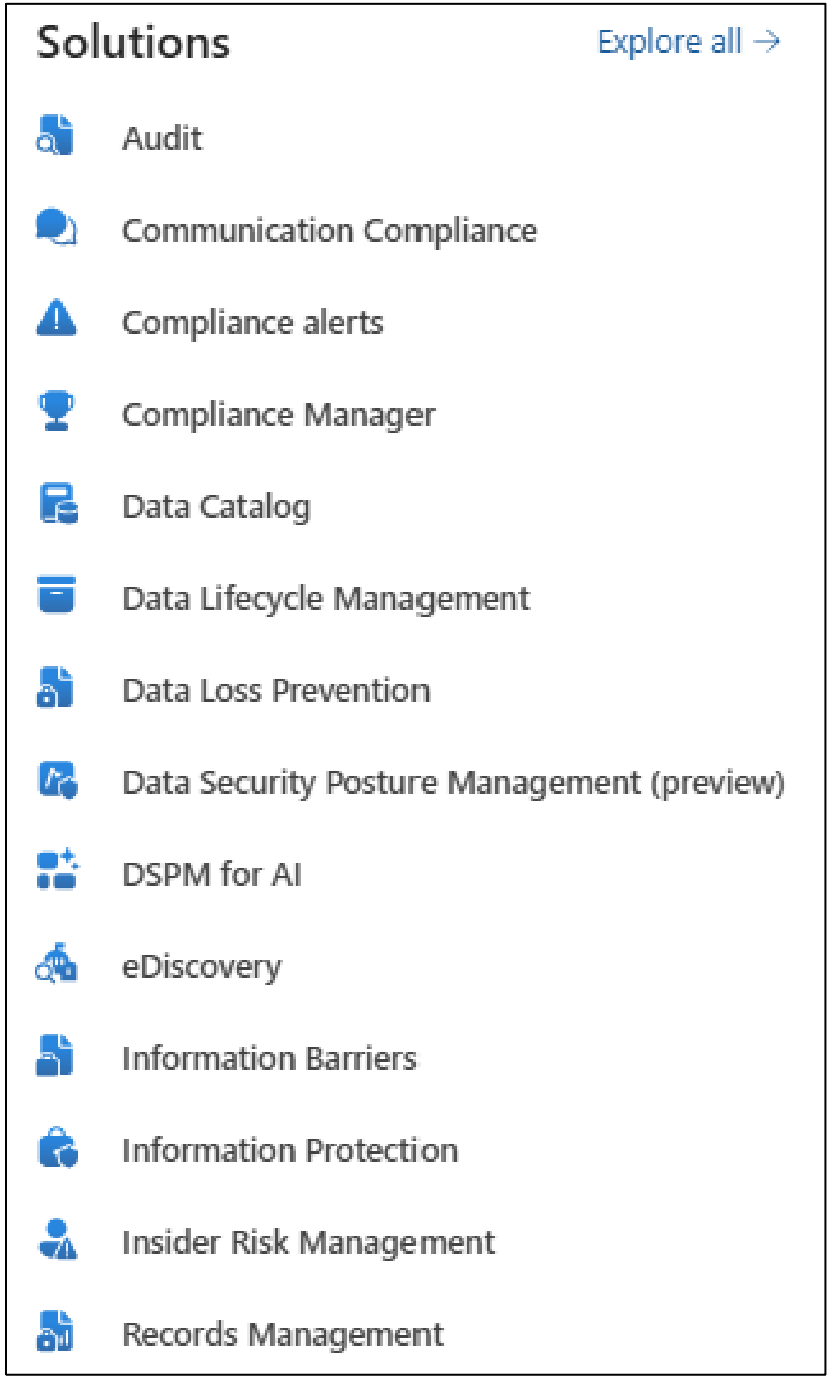
Permission Basics

- Very similar to file based permissions
- Can assign permissions to most things in SharePoint, right down to the item level
- Can assign an individual user rights at a location
- Better practice is to assign rights to SharePoint groups and add users to these groups
- Can share information with anyone with an email
- The default option is to allow sharing

Microsoft Purview helps with data compliance

- Microsoft Purview simplifies data governance and compliance tasks.
- It provides a unified location to manage data protection policies.
- Some features may require a more powerful license, but the basics are there.

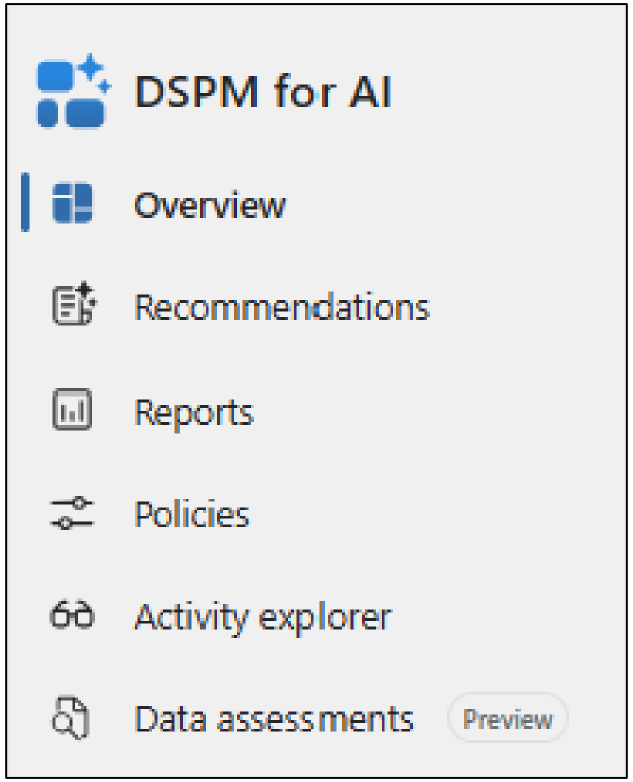




Solutions

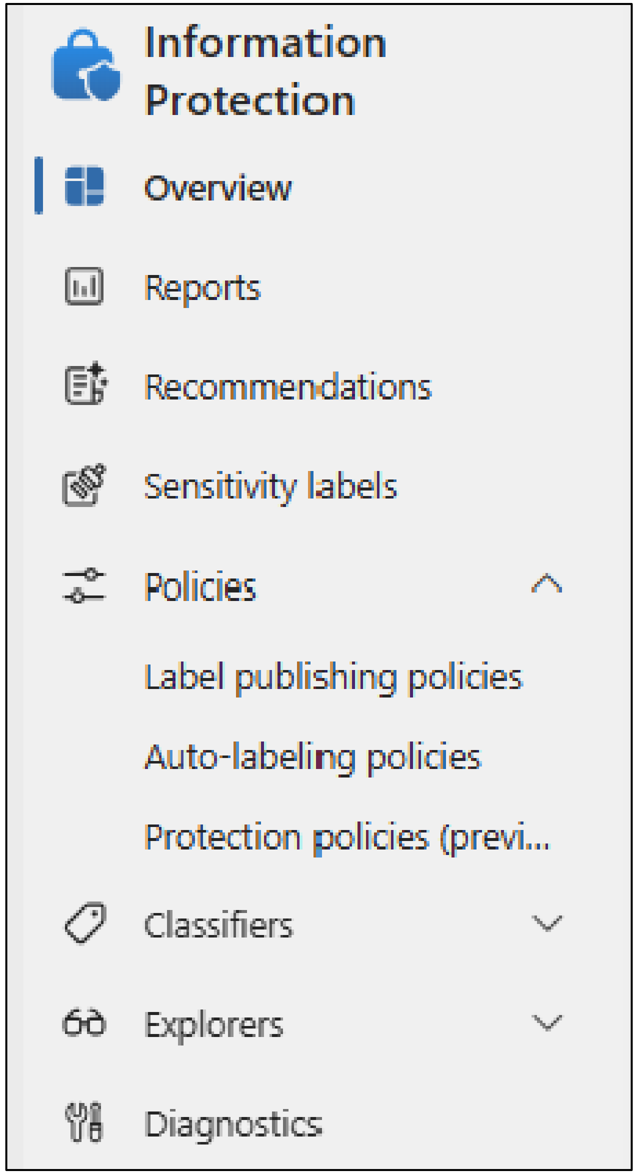
Explore all →

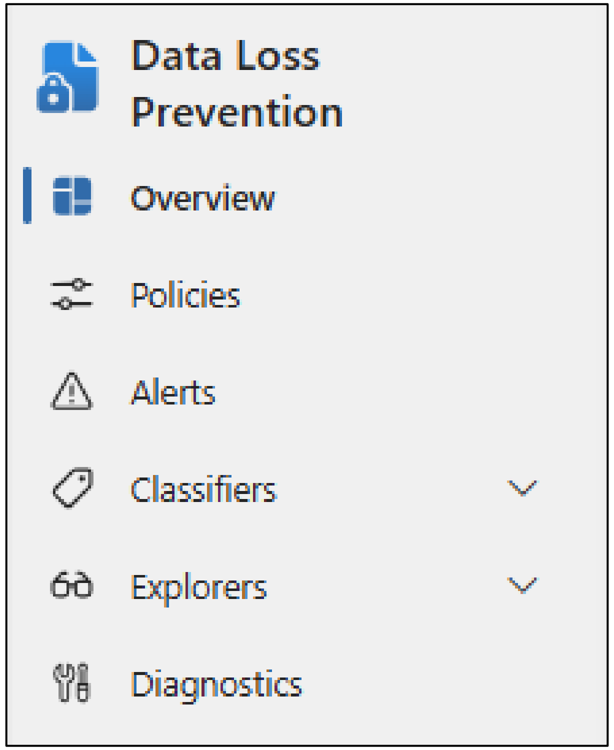
- Audit
- Communication Compliance
- Compliance alerts
- Compliance Manager
- Data Catalog
- Data Lifecycle Management
- Data Loss Prevention
- Data Security Posture Management (preview)
- DSPM for AI
- eDiscovery
- Information Barriers
- Information Protection
- Insider Risk Management
- Records Management

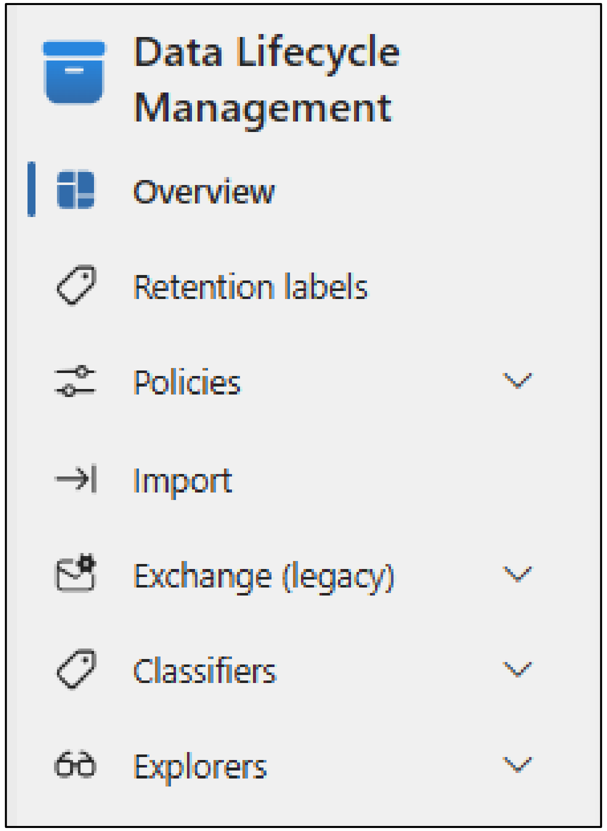


DSPM for AI

- Overview
- Recommendations
- Reports
- Policies
- Activity explorer
- Data assessments Preview

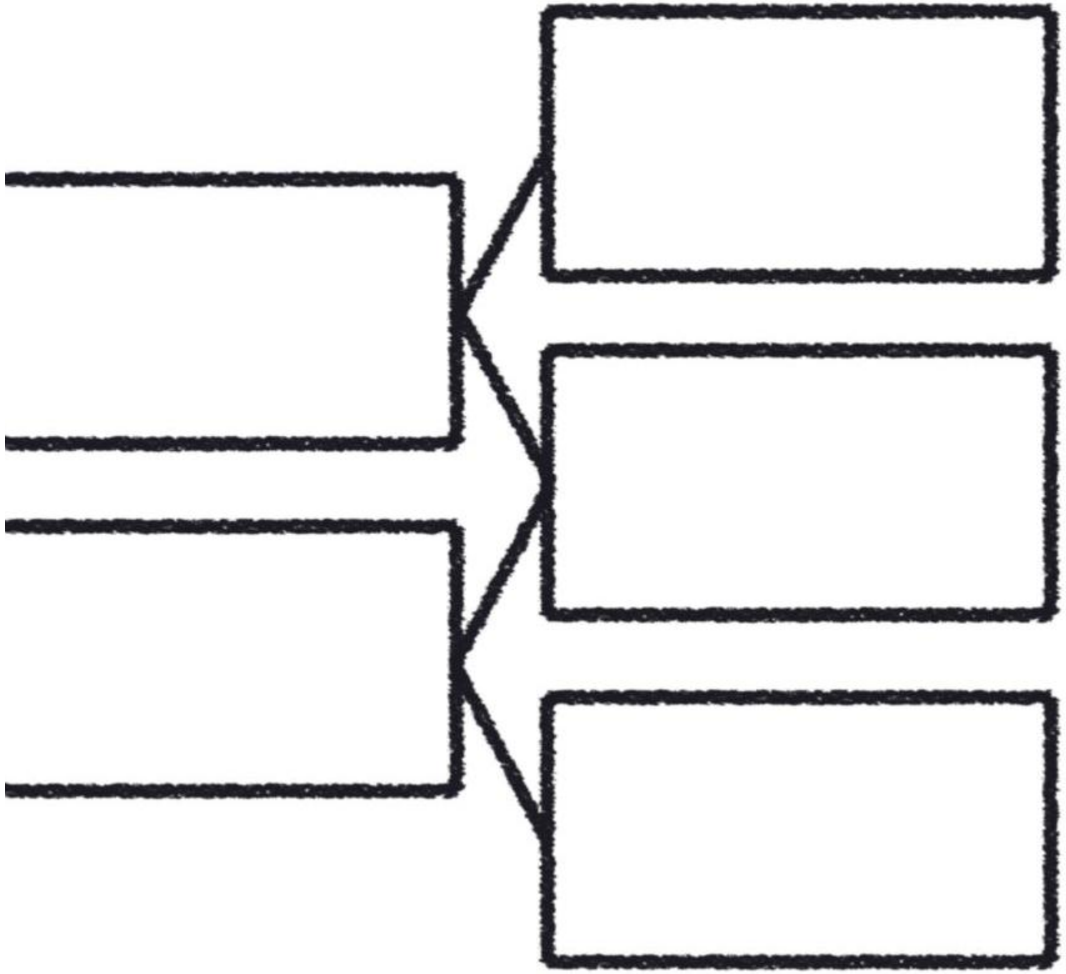

Information Protection
Overview
Reports
Recommendations
Sensitivity labels
Policies
Label publishing policies
Auto-labeling policies
Protection policies (previ...
Classifiers
Explorers
Diagnostics

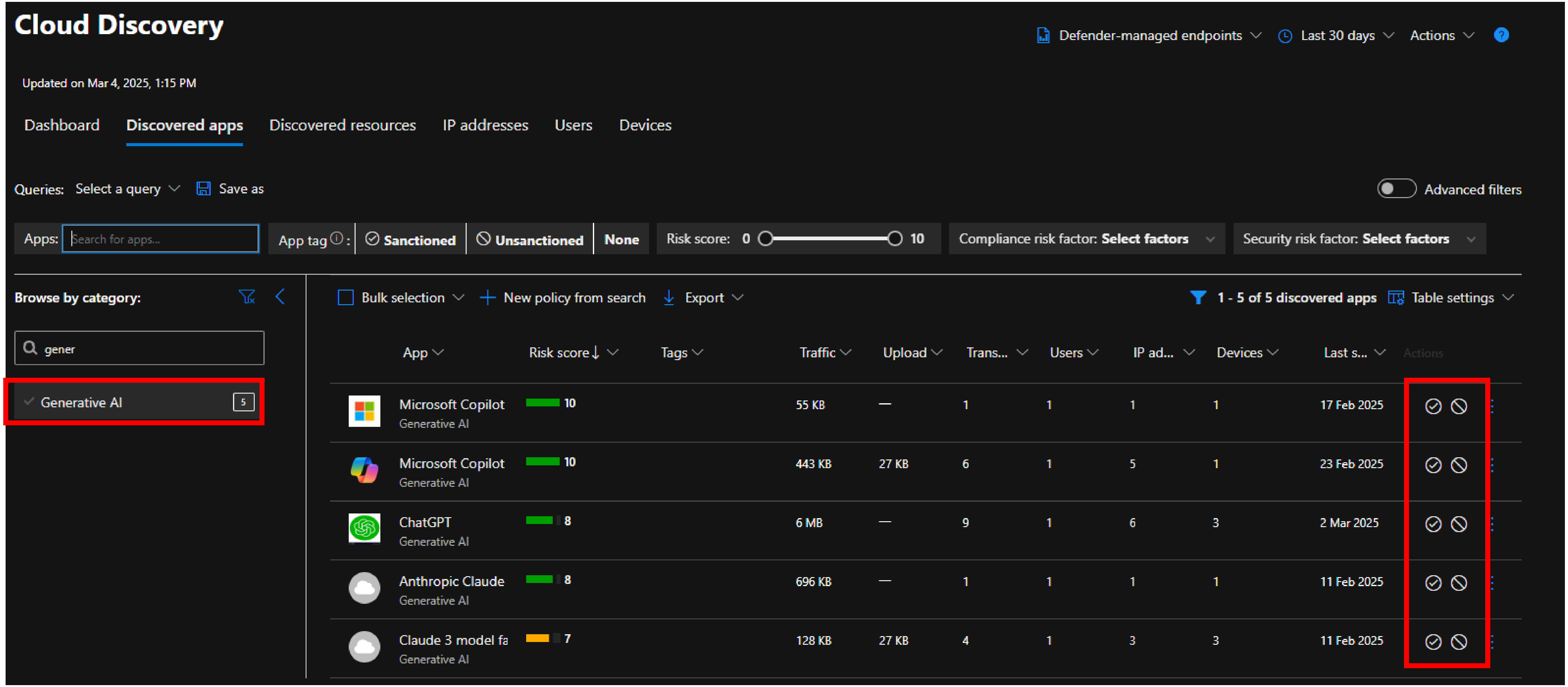

Data Loss Prevention
Overview
Policies
Alerts
Classifiers
Explorers
Diagnostics


Data Lifecycle Management
Overview
Retention labels
Policies
Import
Exchange (legacy)
Classifiers
Explorers

Security portal has a number of handy tools

- Defender for Cloud can monitor and block AI usage.
- Defender for Endpoint can utilize web blocking on URLs.
- Defender for Endpoint can create incidents to be used inside the Microsoft Security stack.





Cloud Discovery

Defender-managed endpoints ⌄ Last 30 days ⌄ Actions ⌄ ?

Updated on Mar 4, 2025, 1:15 PM

Dashboard | **Discovered apps** | Discovered resources | IP addresses | Users | Devices

Queries: Select a query ⌄ Save as

Advanced filters

Apps: Search for apps... | App tag ⓘ: ✓ **Sanctioned** | ⊘ **Unsanctioned** | **None** | Risk score: 0 — 10 | Compliance risk factor: **Select factors** ⌄ | Security risk factor: **Select factors** ⌄

Browse by category:

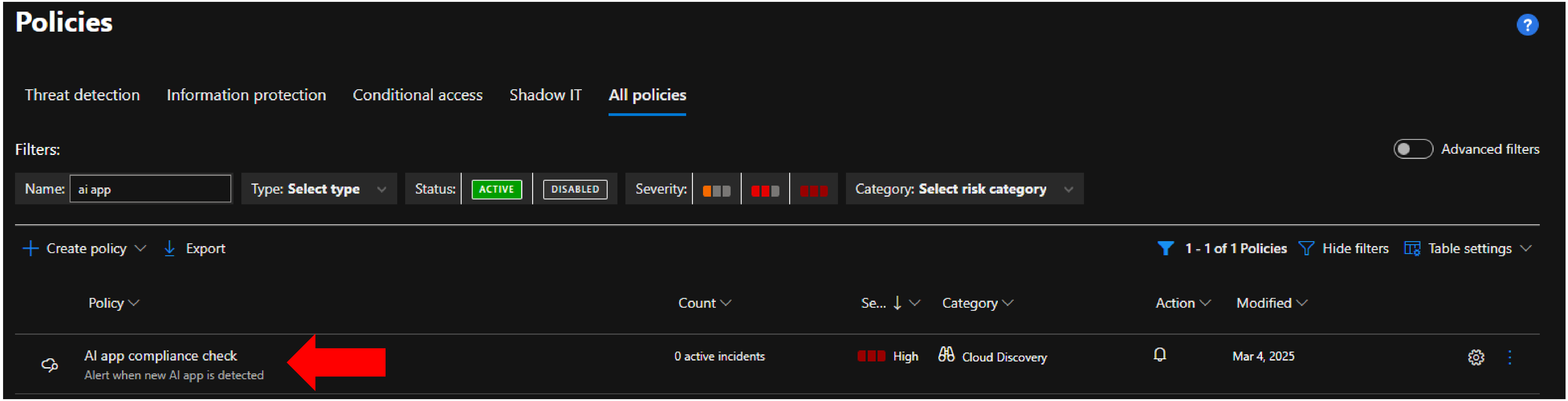
gener

✓ Generative AI 5

□ Bulk selection ⌄ + New policy from search ↓ Export ⌄

1 - 5 of 5 discovered apps Table settings ⌄

App	Risk score ↓	Tags	Traffic	Upload	Trans...	Users	IP ad...	Devices	Last s...	Actions
Microsoft Copilot Generative AI	10		55 KB	—	1	1	1	1	17 Feb 2025	✓ ⊘
Microsoft Copilot Generative AI	10		443 KB	27 KB	6	1	5	1	23 Feb 2025	✓ ⊘
ChatGPT Generative AI	8		6 MB	—	9	1	6	3	2 Mar 2025	✓ ⊘
Anthropic Claude Generative AI	8		696 KB	—	1	1	1	1	11 Feb 2025	✓ ⊘
Claude 3 model fa Generative AI	7		128 KB	27 KB	4	1	3	3	11 Feb 2025	✓ ⊘



Filters:

Name: ai app

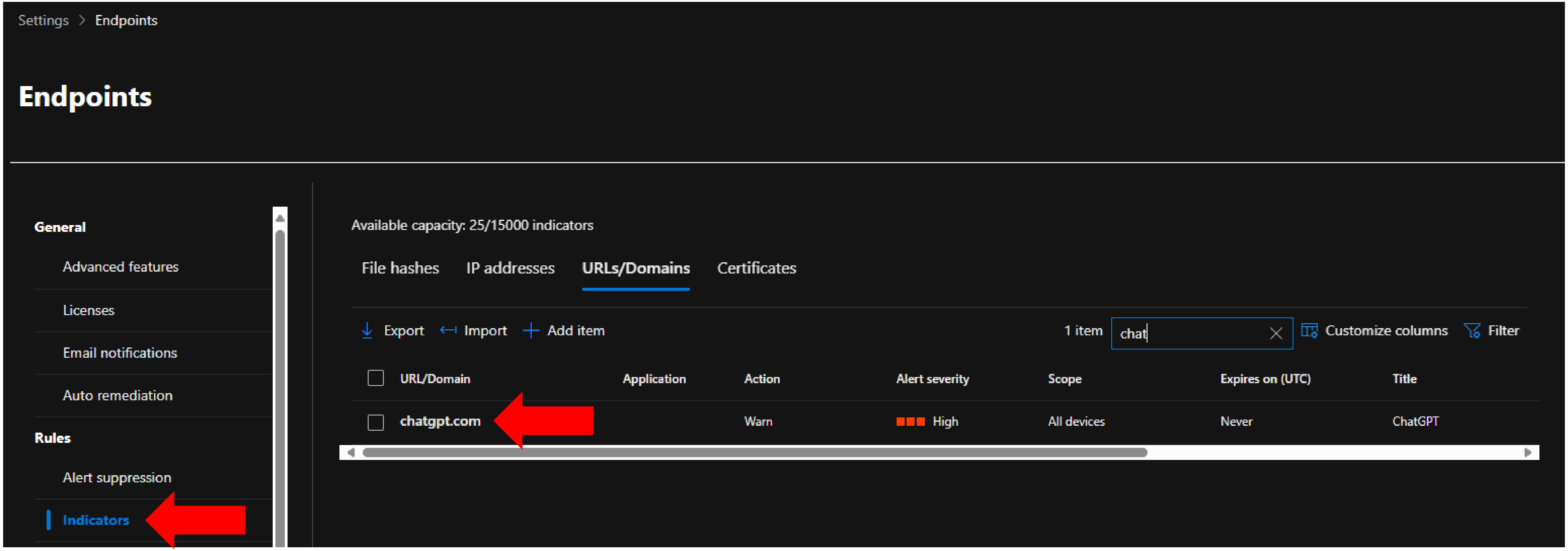
Type: Select type

Status: ACTIVE DISABLED

Severity:

Category: Select risk category

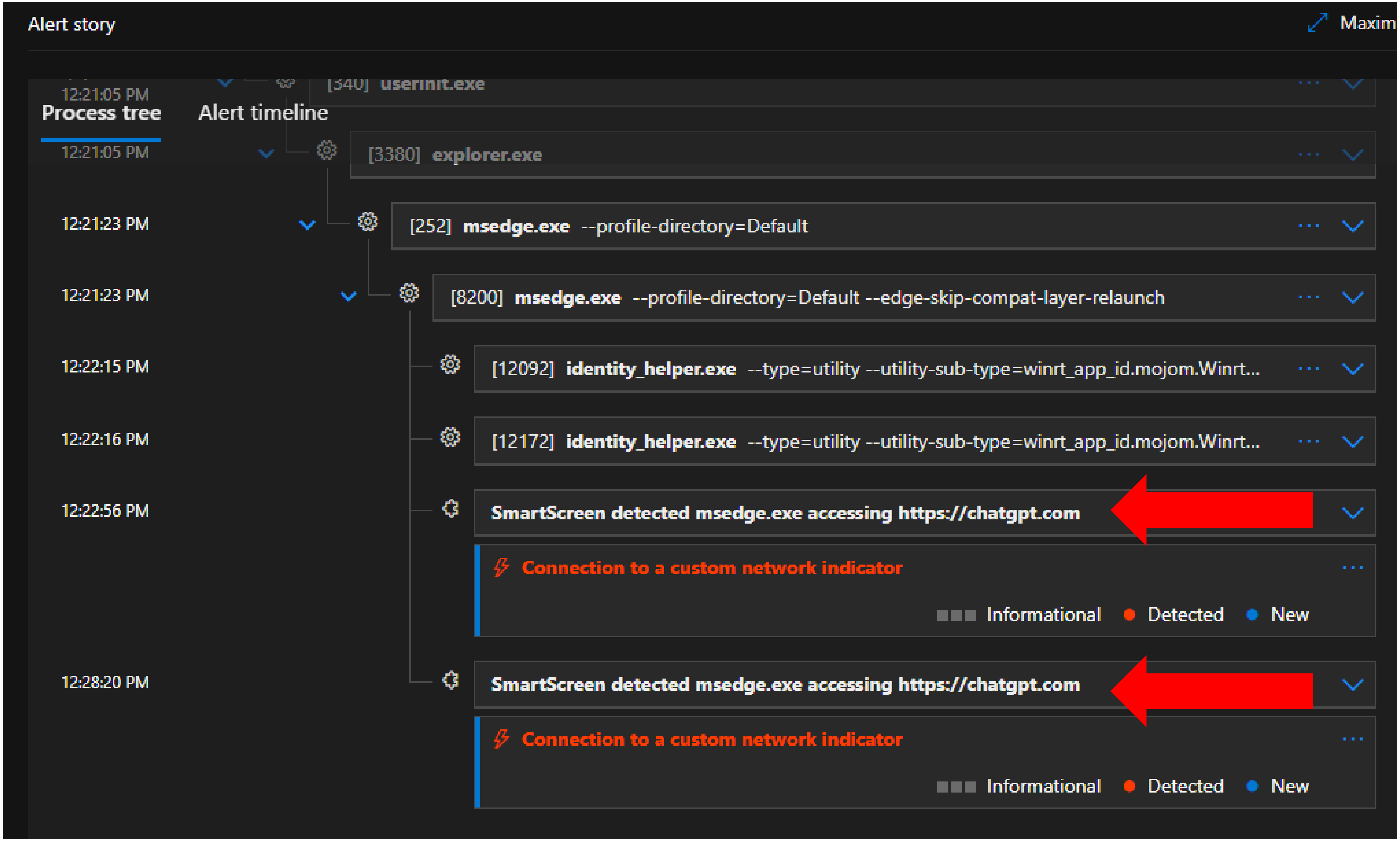
Policy	Count	Se... ↓	Category	Action	Modified
AI app compliance check Alert when new AI app is detected	0 active incidents	High	Cloud Discovery	🔔	Mar 4, 2025



Available capacity: 25/15000 indicators

1 item chat

□	URL/Domain	Application	Action	Alert severity	Scope	Expires on (UTC)	Title
□	chatgpt.com		Warn	■■■ High	All devices	Never	ChatGPT



12:21:05 PM [340] userinit.exe

12:21:05 PM [3380] explorer.exe

12:21:23 PM [252] msedge.exe --profile-directory=Default

12:21:23 PM [8200] msedge.exe --profile-directory=Default --edge-skip-compat-layer-relaunch

12:22:15 PM [12092] identity_helper.exe --type=utility --utility-sub-type=winrt_app_id.mojom.Winrt...

12:22:16 PM [12172] identity_helper.exe --type=utility --utility-sub-type=winrt_app_id.mojom.Winrt...

12:22:56 PM SmartScreen detected msedge.exe accessing https://chatgpt.com

Connection to a custom network indicator

Informational ● Detected ● New

12:28:20 PM SmartScreen detected msedge.exe accessing https://chatgpt.com

Connection to a custom network indicator

Informational ● Detected ● New

Take aways

- To fully govern AI data usage, you need at least Business Premium or better.
- AI has no individual security or configuration settings; it relies on the services underneath.
- A good data structure makes applying permissions easier.
- Data protection policies like DLP require consultation with customer.
- Microsoft Security has a variety of ways to control data flow.

Resources

https://bit.ly/cia20250305

X	Linkedin	Email	Teams
@directorcia	https://www.linkedin.com/in/ciaops	director@ciaops.com	admin@ciaops365.com