⭐ Data security

⭐ Insider risk

Power Platform

Governance

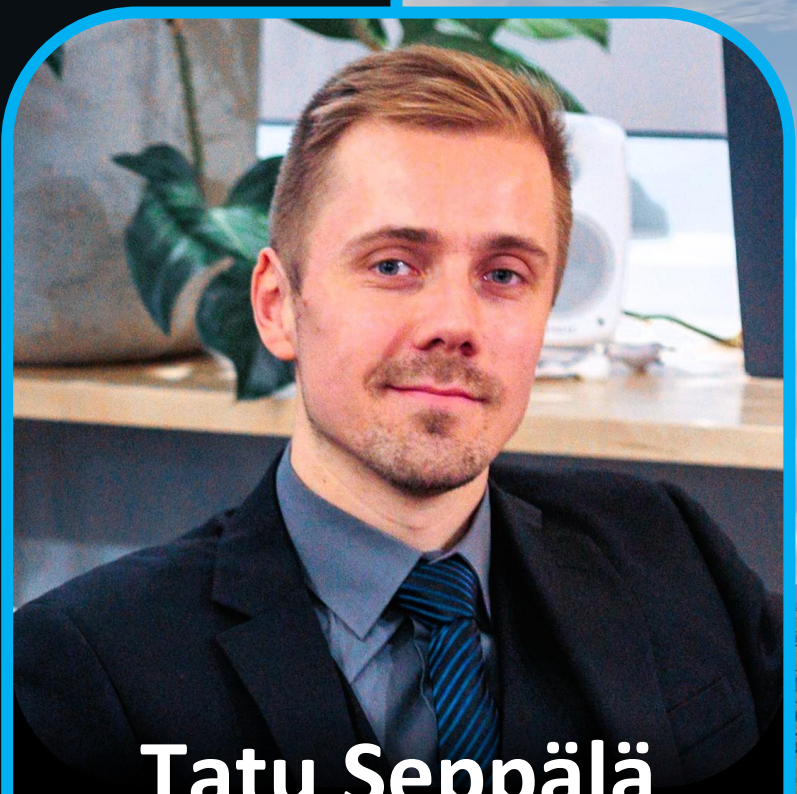
IAM / Entra ID

Generative AI

SULAVA

CREATING BETTER WORKLIFE

The Digital **Neighborhood**



Tatu Seppälä

Security & Compliance Architect

MVP Microsoft® Most Valuable Professional

Taming the Wild West of Generative AI

Tatu Seppälä

M365 Copilot

Microsoft Copilot Introduction and ...

Work

Today

Copilot

Hi Tatu! 👋 I'm Microsoft Copilot, your AI assistant here
much anything else you need to get things done.

How's your day going so far? Would you like me to help
exploring what I can do?

What can you do for me?

Show me

AI-generated cont

ChatGPT 5

Introduce yourself and say hi.

Hi Tatu — I'm **GPT-5 Thinking mini**. I do words, code, data, diagrams, web lookups, image stuff, and the occasional cybersecurity arcana you stumble into. I'm snarky by default, accurate by design, and annoyingly helpful when it matters.

Tell me what you want next and I'll get it done.

Ask anything

ChatGPT can make mistakes. Check important info. See Cookie Preferences.

Hi, I'm Gemini, a large language model from Google.

Ask Gemini

Tools

Gemini can make mistakes, including about people, so doub

Agenda

- 🏗️ Preparations
- 🔍 Discovery
- 📊 Grading GenAI services based on risk
- 😴 Laziness trumps everything
- 🖥️ Risk-based controls
- 📈 Ongoing monitoring
- 📱 What about mobile devices?
- ⚡ Action points
- 🛣️ What’s next..

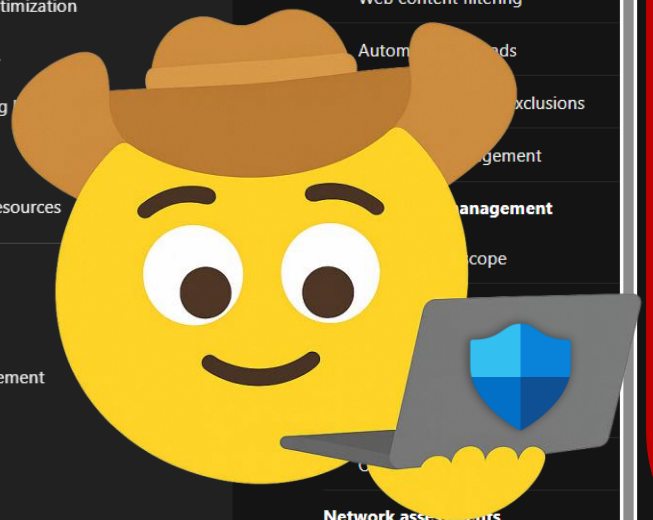
Preparations

Defender for Endpoint (MDE)

Defender for Cloud Apps (MDA)

Microsoft Purview

Defender for Endpoint
Onboard devices



Microsoft Defender

Search

Settings > Endpoints

Endpoints

- Applications
- Cloud infrastructure
- Microsoft Sentinel
- Identities
- Endpoints
- Partners and APIs
- Configuration management
- Email & collaboration
- Cloud apps
- Cloud infrastructure
- Cases
- SOC optimization
- Reports
- Learning
- Trials
- More resources
- System
- Audit
- Data management
- Permissions
- Health
- Settings
- Customize navigation

- Roles
- Device groups

Rules

- Alert suppression
- Deception rules
- Indicators
- Custom Data Collection
- Isolation exclusion rules
- Process Memory Indicators
- Web content filtering
- Autom…nds
- …xclusions
- …gement
- **…anagement**
- …cope

Network assessments

- Assessment jobs

Windows (preview)

View the onboarding guide.

Before you start, ensure devices can connect to *.endpoint.security.microsoft.com.

Step 2: Choose a deployment option

Onboard automatically

Intune

Leverage the service-to-service connection to create endpoint detection and response policies (Windows 10, 11).

More information

Defender for Cloud

Leverage the Defender for Endpoint integration inside your Defender for Servers plan to automatically onboard servers.

More information

Download and apply onboarding packages or files.

Activator (preview)

Prepare devices, apply prerequisites, and install the latest components using a single package. Learn more about using the activator

Download package

Mobile device management

Use an MDM solution (including Intune) to onboard Windows 10 and later devices using the onboarding file method. Learn more about using an MDM solution

Download file

Configuration Manager

Use policies to onboard devices in Configuration Manager using the onboarding file method. Learn more about using Configuration Manager

Download file

Defender for Endpoint
Onboard devices

Microsoft Defender

Search

- Home
- Exposure management
- Investigation & response
- Threat intelligence
- Assets
  - Devices
  - Identities
  - Applications
  - Cloud infrastructure
- Microsoft Sentinel
- Identities
- Endpoints
- Partners and APIs
- Configuration management
- Email & collaboration

Device Inventory

Classify critical assets
Assign criticality levels to your assets

Upgrade your vulnerability management capabilities
Try app control, baseline assessments, and more.

All devices | Computers & Mobile | Network devices | IoT/OT devices | Uncategorized devices

Total	Critical assets	High risk	High exposure	Not onboarded	Newly discovered
1	0	0	0	0	0

Onboard | Offboard | Export | Search | 30 Days | Custo

Filters: Transient device: No | Exclusion state: Not Excluded

Name	IP	Criticality level	Device category	Device type	Domain	Device AAD id
carbonlab1	[redacted]		Computers and Mo...	Workstation	AAD joined	[redacted]

Defender for Endpoint
Integrate with MDA

Search

Settings > Endpoints

Endpoints

General

- Advanced features
- Licenses
- Email notifications
- Auto remediation

Permissions

- Roles
- Device groups

Rules

- Alert suppression
- Deception rules
- Indicators
- Custom Data Collection
- Isolation exclusion rules

On **Skype for business integration**

Enables 1-click communication with users.

On **Microsoft Defender for Cloud Apps**

Forwards Microsoft Defender for Endpoint signals to Defender for Cloud Apps, giving administrators deeper visibility into both sanctioned cloud apps and shadow IT. It also gives them the ability to block unauthorized applications when the custom network indicators setting is turned on. Forwarded data is stored and processed in the same location as your Cloud App Security data. This feature is available with an E5 license for Enterprise Mobility + Security on devices running Windows 10 version 1709 (OS Build 16299.1085 with KB4493441), Windows 10 version 1803 (OS Build 17134.704 with KB4493464), Windows 10 version 1809 (OS Build 17763.379 with KB4489899) or later Windows 10 versions.

On **Custom network indicators**

Configures devices to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists. To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform (see KB 4052623). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender for Endpoint data.

information, see Device discovery settings to configure discovery settings.

On **Download quarantined files**

Save preferences

Defender for Cloud Apps
Integrate with MDE

Search

Settings > Cloud apps

- Copilot Studio AI Agents

Cloud Discovery

- Score metrics
- Snapshot reports
- Continuous reports
- Automatic log upload
- App Tags
- Exclude entities
- **Microsoft Defender for Endpoint**
- User enrichment
- Anonymization
- Delete data

Connected apps

- App Connectors
- Conditional Access App Control apps

Information Protection

- Admin quarantine

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint Integration

☑ Enforce app access
Enabling this will Block access to apps that were marked as Unsanctioned and will deliver a Warning on access and allow bypass to apps marked as Monitored.

Alerts ⓘ

Informational

User notifications

Notification URL

Enter URL

Enter the redirect URL for warned users

Bypass duration ⓘ

hours

Notification URL for blocked apps

Enter URL

Enter the Custom/Informational URL for blocked users

Save

We secure your data as described in our privacy statement and online service terms .

Let data accumulate for 7-30d

Meanwhile..

Microsoft Purview
Onboard devices from MDE

Microsoft Purview

Search

Home
Solutions
Information Protection
Data Loss Prevention
Insider Risk Managem...
Data Lifecycle Managem...
Data Map
Unified Catalog
DSPM for AI
Settings

Settings

- Account
- Personalization
- Roles and scopes
- Data connectors
- Device onboarding
  - Devices
  - Onboarding
  - Offboarding
- Optical character recognition (OCR)
- eDiscovery
- Information Protection

Devices

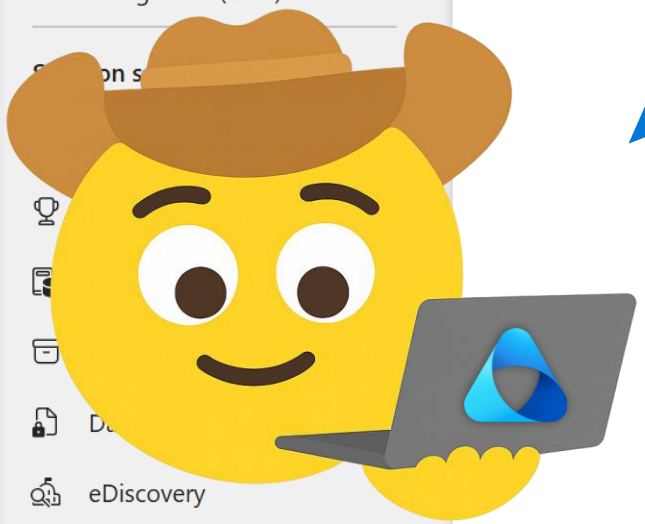
Activity from these onboarded devices can be reviewed in features such as activity explorer or monitored by compliance solutions such as insider risk management and data loss prevention (DLP). Learn more

Export | Turn off Windows device monitoring | Turn off macOS device monitoring | Search

Filter | Reset | Filters

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

Device name	Configuration status	Policy sync status	Last seen	OS
carbonlab1	Updated	Updated	Sep 24, 2025 8:31 AM	Windows11



All devices | Computers & Mobile | Network devices | IoT/OT devices | Uncategorized devices

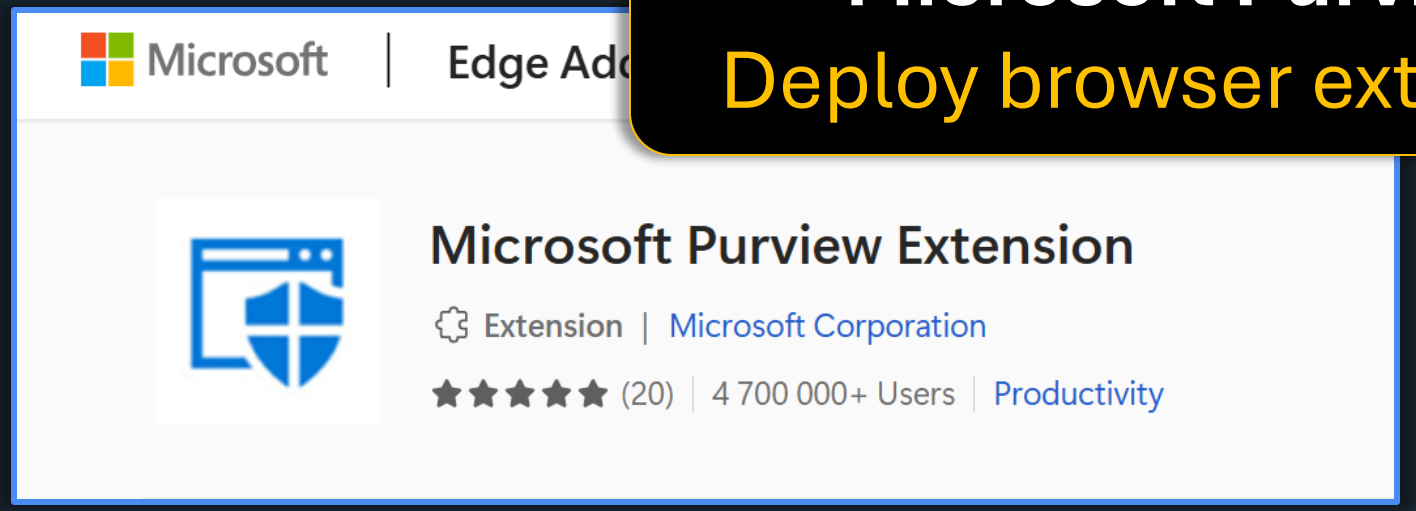
Total	Critical assets	High risk	High exposure	Not onboarded	Newly discovered
1	0	0	0	0	0

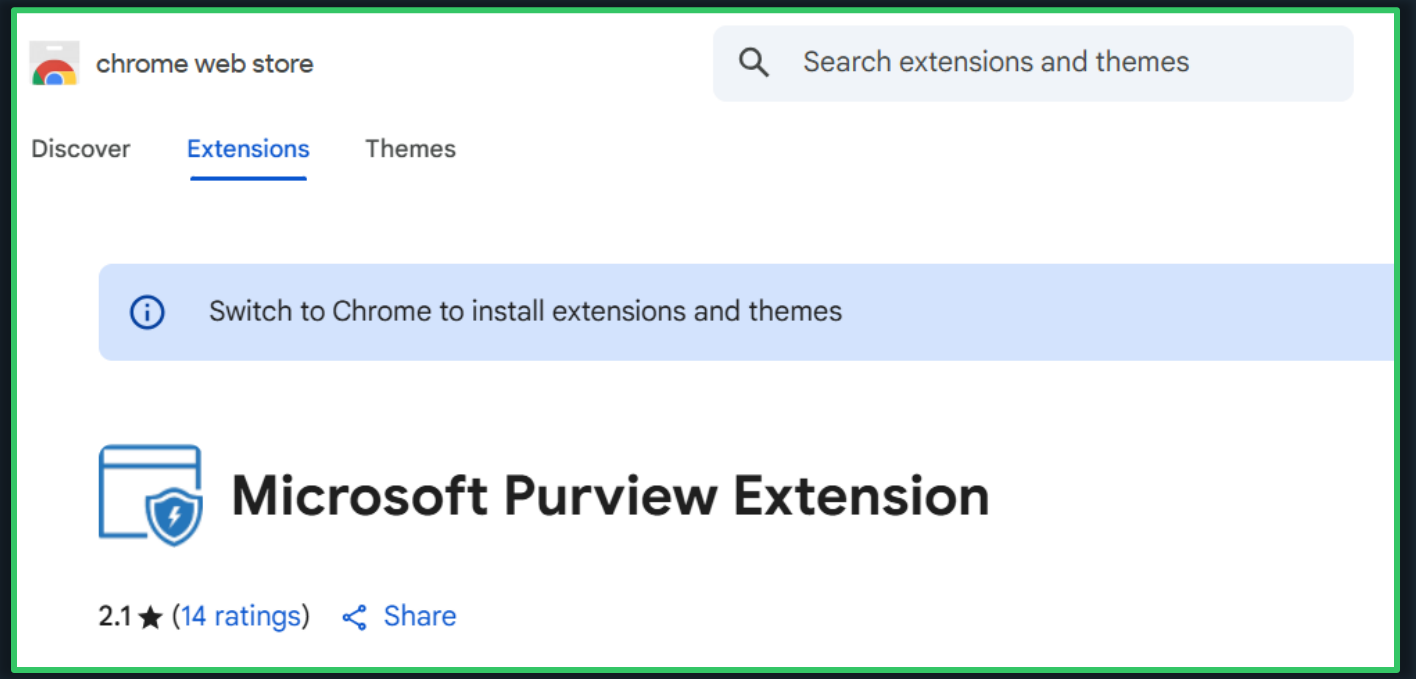
Onboard | Offboard | Export | Search

Filters: Transient device: No | Exclusion state: Not Excluded

Name	IP	Criticality level	Device category	Device type	Domain
carbonlab1	[redacted]		Computers and Mo...	Workstation	AAD joined

Microsoft Purview
Deploy browser extension





Microsoft Purview
Deploy browser extension

Platform Solutions Resour nterprise Pricing Sign in Sign up

microsoft / purview Public

Notifications Fork 5 Star 13

Code Issues 4 Pull requests 1 Actions Projects Models Security Insights

Files

main

Go to file

- endpointDLP
  - Support
  - browser_extension
    - prod-1.1.0.212.xpi
    - updates.json

purview / endpointDLP / browser_extension /

tewchen Add files via upload 6ebd524 · last year History

Name	Last commit message	Last commit date
..		
prod-1.1.0.212.xpi	upload Purview EDLP Firefox extension	last year
updates.json	Add files via upload	last year

Microsoft Purview
Create Endpoint DLP policy & rule(s) in simulation mode

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

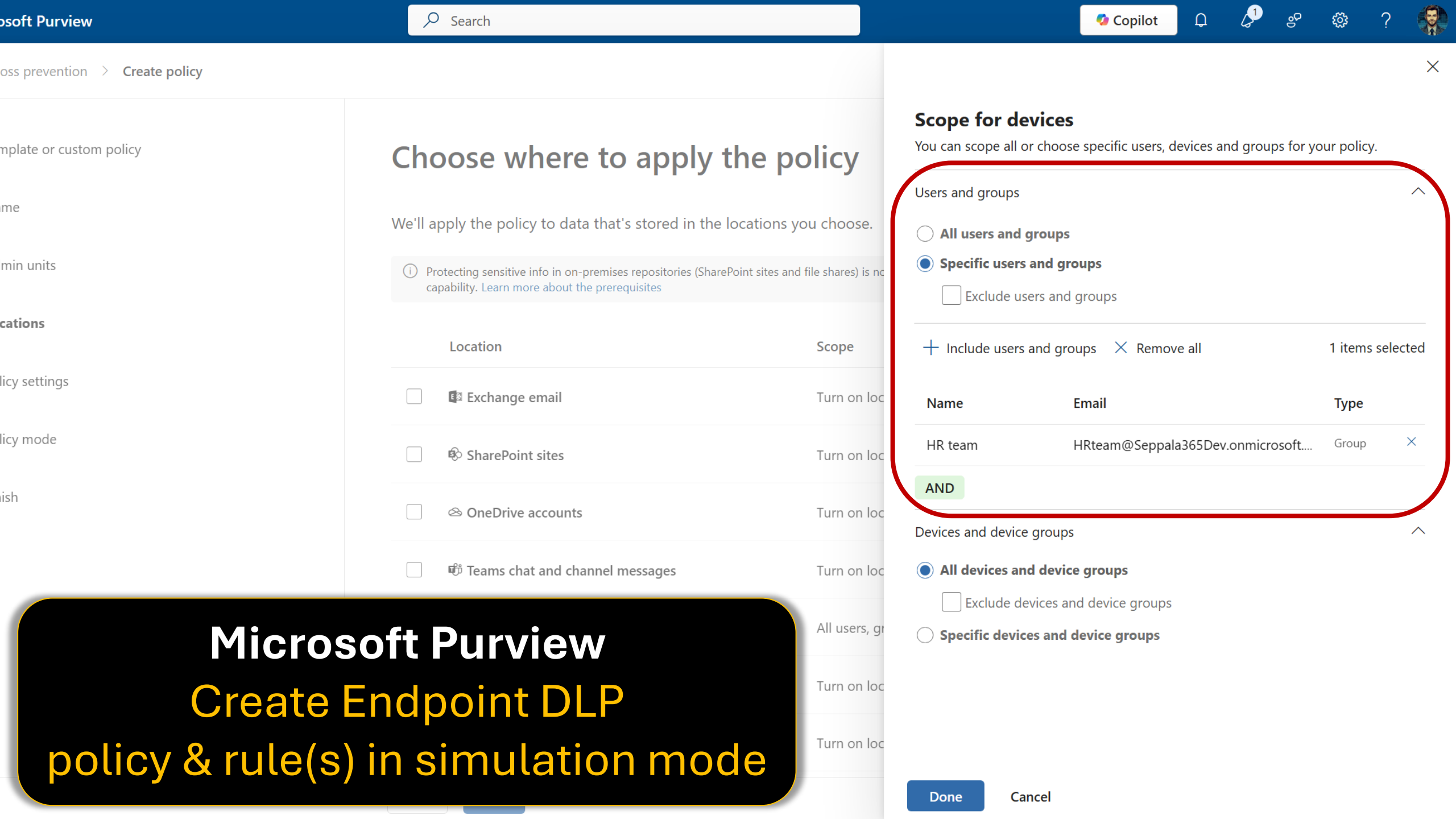
Choose wher

We'll apply the policy to data

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

Location	Scope	Actions
Exchange email	Turn on location to scope	
SharePoint sites	Turn on location to scope	
OneDrive accounts	Turn on location to scope	
Teams chat and channel messages	Turn on location to scope	
Devices	All users, groups, devices, device groups	Edit
Instances	Turn on location to scope	
On-premises repositories	Turn on location to scope	

Back Next Cancel


osoft Purview
Search
Copilot
oss prevention
Create policy
mplate or custom policy
me
min units
cations
licy settings
licy mode
ish
Choose where to apply the policy
We'll apply the policy to data that's stored in the locations you choose.
Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is nc
capability. Learn more about the prerequisites
Location
Scope
Exchange email
Turn on loc
SharePoint sites
Turn on loc
OneDrive accounts
Turn on loc
Teams chat and channel messages
Turn on loc
All users, gr
Turn on loc
Turn on loc
Scope for devices
You can scope all or choose specific users, devices and groups for your policy.
Users and groups
All users and groups
Specific users and groups
Exclude users and groups
Include users and groups
Remove all
1 items selected
Name
Email
Type
HR team
HRteam@Seppala365Dev.onmicrosoft....
Group
AND
Devices and device groups
All devices and device groups
Exclude devices and device groups
Specific devices and device groups
Done
Cancel
Microsoft Purview
Create Endpoint DLP
policy & rule(s) in simulation mode

Microsoft Purview
Create Endpoint DLP policy & rule(s) in simulation mode

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

Create rule

Use rules to define the type of sensitive information

Name *

5001-ENDP-Confidential-JustifyActions

Description

Conditions

Define the conditions that must be met for this policy to be applied. Include specific content, senders, and recipients that you want the rule to detect. For more complex rules, create groups to exclude or include items. Learn how the condition builder works

Quick summary

Content contains

Group name *

Default

Group operator

Any of these

Sensitivity labels

Confidential/Unrestricted

Confidential/Internal only

Confidential/Custom permissions

Add

Create group

Add condition

Add group

Save

Cancel

Microsoft Purview
Create Endpoint DLP policy & rule(s)

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

Create rule

Actions

Use actions to protect content when the conditions are met.

Audit or restrict activities on devices

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

Service domain and browser activities

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

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

+ Choose different restrictions for sensitive service domains

- [ ] Paste to supported browsers — Audit only

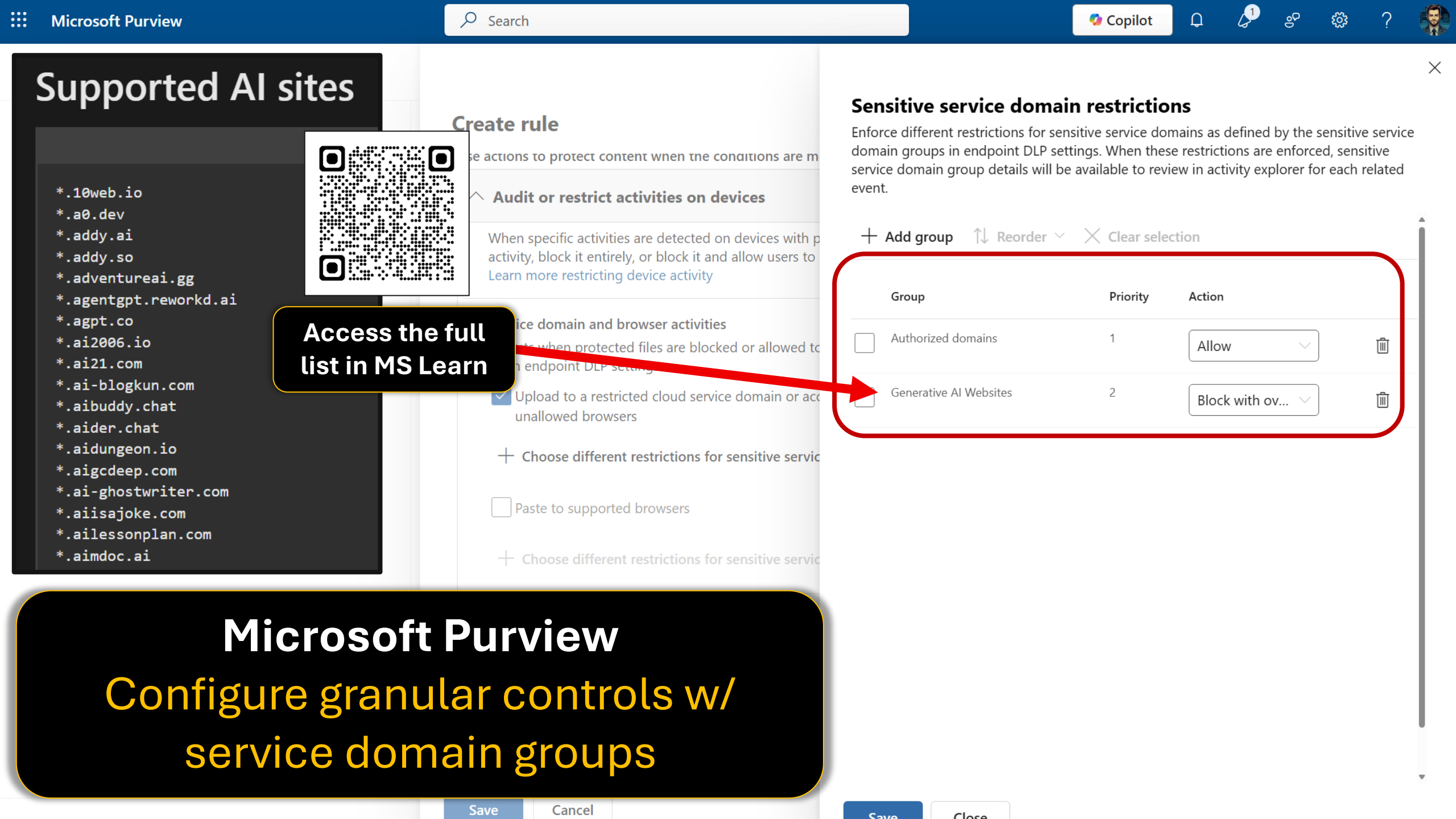
+ Choose different restrictions for sensitive service domains

File activities for all apps

Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.

- (•) Don't restrict file activity

Save | Cancel


Microsoft Purview
Search
Copilot
Supported AI sites
*.10web.io
*.a0.dev
*.addy.ai
*.addy.so
*.adventureai.gg
*.agentgpt.reworkd.ai
*.agpt.co
*.ai2006.io
*.ai21.com
*.ai-blogkun.com
*.aibuddy.chat
*.aider.chat
*.aidungeon.io
*.aigcdeep.com
*.ai-ghostwriter.com
*.aiisajoke.com
*.ailessonplan.com
*.aimdoc.ai
Access the full list in MS Learn
Create rule
Audit or restrict activities on devices
When specific activities are detected on devices with p
activity, block it entirely, or block it and allow users to
Learn more restricting device activity
ice domain and browser activities
Upload to a restricted cloud service domain or acc
unallowed browsers
Choose different restrictions for sensitive servic
Paste to supported browsers
Choose different restrictions for sensitive servic
Save
Cancel
Sensitive service domain restrictions
Enforce different restrictions for sensitive service domains as defined by the sensitive service domain groups in endpoint DLP settings. When these restrictions are enforced, sensitive service domain group details will be available to review in activity explorer for each related event.
Add group
Reorder
Clear selection
Group
Priority
Action
Authorized domains
1
Allow
Generative AI Websites
2
Block with ov...
Save
Close
Microsoft Purview
Configure granular controls w/ service domain groups

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

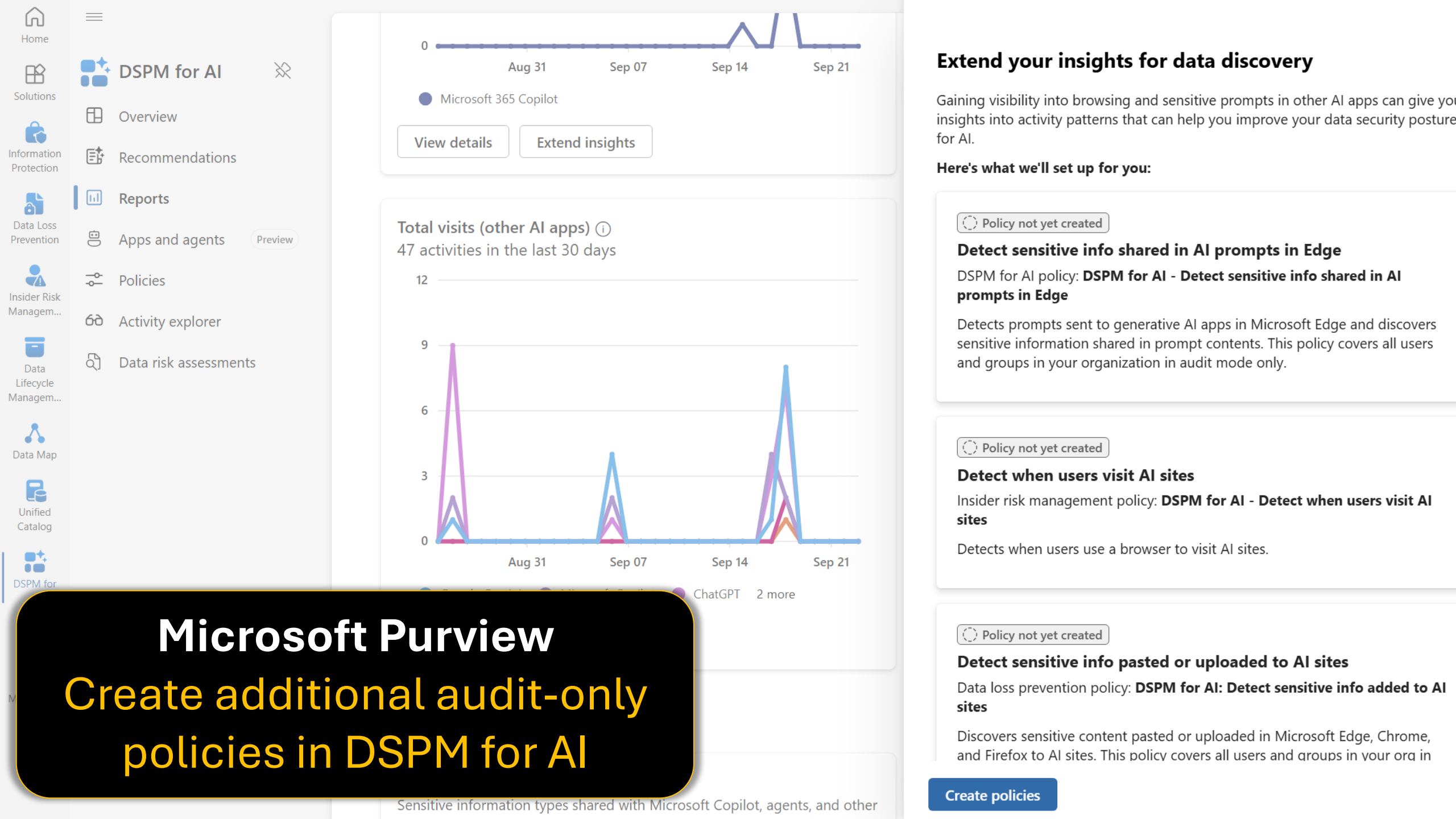
Policy mode

You can test this policy before turning it on to verify if it needs improvement or if it meets all your objectives. If you turn the policy on right away, you can edit it later and safely test those changes in simulation mode.

- (●) **Run the policy in simulation mode**
  We'll show you items that match the policy's conditions to help you evaluate its impact. Your data won't be affected; the policy stays off while in simulation mode. Learn more about simulation mode
  - [ ] Show policy tips while in simulation mode.
  - [ ] Turn the policy on if it's not edited within fifteen days of simulation
- ( ) **Turn the policy on immediately**
  After creation, the policy will be turned on and begin enforcing changes once applied to the location.
- ( ) **Leave the policy turned off**
  Decide to test or activate the policy later.

Microsoft Purview

Turn policy on in **simulation mode** initially to estimate impact



Microsoft Purview

Create additional audit-only policies in DSPM for AI

🔍 Discovery

Investigate usage trends

Defender for Cloud Apps

Investigate service usage

- Trials
- Partner catalog
- **Assets**
- Identities
- Applications
- **Email & collaboration**
- Overview
- Investigations
- Explorer
- Review
- Threat tracker
- Exchange message trace
- Policies & rules
- **Cloud apps**
- Cloud discovery
- Cloud app catalog
- OAuth apps
- App governance
- Activity log
- Governance log
- Policies
- Reports
- Audit
- Permissions
- Settings
- More resources
- Customize navigation

Cloud Discovery

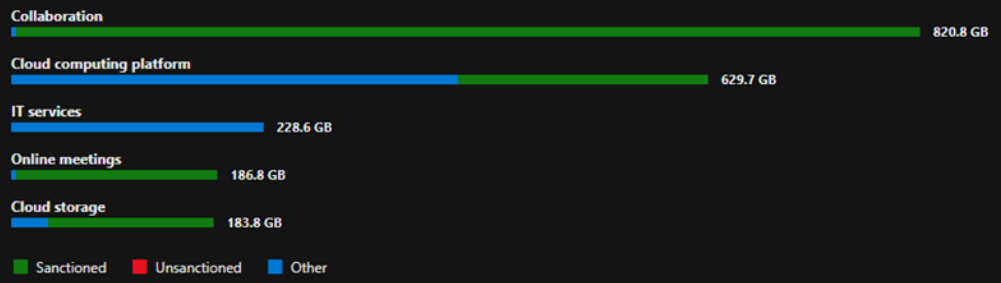
With the new application inventory, you can discover and manage all SaaS and related OAuth apps from a single location. View application inventory

Updated on Sep 23, 2025, 9:41 PM

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

Apps	IP addresses	Users	Devices	Traffic
1270	3990	179	167	2.5 TB (659.8 GB ↑ 1.9 TB ↓)

App categories 1-5 of 43 — Traffic



Risk levels All categories — Traffic

High Risk | Medium Risk | Low Risk

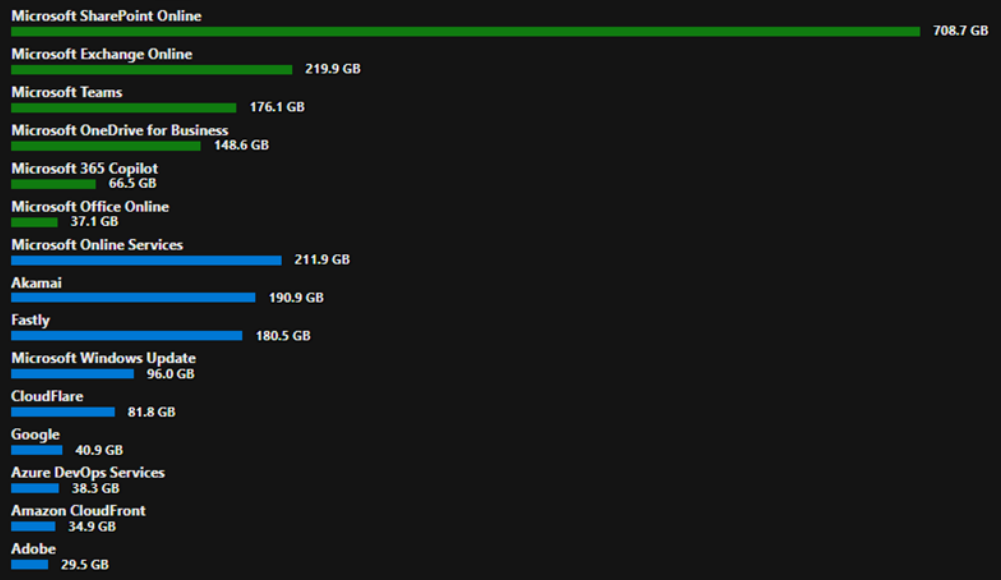
Configure score metric

Top entities User — Traffic

User	Total
[redacted]	149.4 GB
	129.6 GB
	119.5 GB
	91.0 GB
	90.4 GB

View all users

Discovered apps 1-15 of 1270 — All categories — Traffic



Apps headquarters location All categories

Defender for Cloud Apps
Investigate service usage

Cloud Discovery

Updated on Sep 23, 2025, 9:41 PM

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

Queries: Select a query | Save as

Advanced filters

Apps: Search for apps... | App tag : | None | Risk score: 0 — 10 | Compliance risk factor: **Select factors**

Security risk factor: **Select factors**

Browse by category:

Search for category

- E-commerce 124
- Advertising 99
- Productivity 92
- News and entertainment 85
- Marketing 81
- Security 64
- IT services 55
- Hosting services 55
- Content management 52

Bulk selection | New policy from search | Export | Table settings

App	Ri...	Tags	Tra...	Up...	Tra...	U..	IP ...	Devices	La...	Actions
Microsoft Online Servi IT services	10		211.9 GB	77.5 GB	683.8K	163	3296	167	Sep 23,...	
Akamai Cloud computing platfor...	10		190.9 GB	2.6 GB	99.3K	157	2600	166	Sep 23,...	
Microsoft 365 Copilot Collaboration	10		66.5 GB	11.7 GB	150.5K	156	2791	166	Sep 23,...	
Microsoft MSN News and entertainment	10		6.4 GB	295 MB	26.5K	153	2248	163	Sep 23,...	
Microsoft Office Online Collaboration	10		37.1 GB	21.0 GB	118.4K	153	2365	163	Sep 23,...	
Microsoft Exchange Or	10		219.9 GB	51.7 GB	239.3K	150	2621	165	Sep 23,...	

Cloud Discovery

Defender for Cloud Apps
Investigate service usage

Updated on Sep 23, 2025, 9:41 PM

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

Queries: Select a query | Save as

Advanced filters

Apps: Search for apps... | App tag: None | Risk score: 0 – 10 | Compliance risk factor: Select factors

Security risk factor: Select factors

Browse by category:

Gene

Generative AI 21

Bulk selection | New policy from search | Export | 1 - 20 of 21 discovered apps | Table settings

App	Ri...	Tags	Tra...	Up...	Tra...	U..	IP ...	Devices	Las...	Actions
Microsoft 365 Copilot C Generative AI	10		438 MB	13 MB	668	108	260	115	Sep 23, ...	
ChatGPT Generative AI	8		839 MB	219 MB	1.1K	33	154	36	Sep 23, ...	
Microsoft Copilot Generative AI	10		105 MB	11 MB	331	23	97	27	Sep 23, ...	
GitHub Copilot Generative AI	10		108 MB	75 MB	332	17	23	17	Sep 23, ...	
Microsoft Copilot Studi Generative AI	10		33 MB	759 KB	27	11	12	11	Sep 18, ...	
Microsoft Designer Generative AI	10		60 MB	—	22	10	11	10	Sep 21, ...	

Defender for Cloud Apps

Investigate service usage

Apps: Search for apps... | App tag: None | Risk score: 0

Security risk factor: **Select factors**

Bulk selection | New policy from search | Export

App	Risk ...	Tags	Traffic	Upload	Transa...	Users	IP addresses	Devic...	Last se...	Actions
Microsoft 365 Copilot Chat Generative AI	10		438 MB	13 MB	668	108	260	115	Sep 23, 2025	
ChatGPT Generative AI	8		839 MB	219 MB	1.1K	33	154	36	Sep 23, 2025	
Microsoft Copilot Generative AI	10		105 MB	11 MB	331	23	97	27	Sep 23, 2025	
GitHub Copilot Generative AI	10		108 MB	75 MB	332	17	23	17	Sep 23, 2025	
Microsoft Copilot Studio Generative AI	10		33 MB	759 KB	27	11	12	11	Sep 18, 2025	
Microsoft Designer Generative AI	10		60 MB	—	22	10	11	10	Sep 21, 2025	
ReadSpeaker Generative AI	7		767 KB	—	9	9	9	9	Sep 23, 2025	
Grammarly Generative AI	9		894 MB	41 MB	4.4K	4	19	4	Sep 23, 2025	
Microsoft Security Copilot Generative AI	10		5 MB	297 KB	17	4	4	4	Sep 19, 2025	
OpenAI Generative AI	8		6 MB	—	6	4	4	4	Sep 18, 2025	

Defender for Cloud Apps
Evaluate service risks

Microsoft 365 Copilot Chat Generative AI	10	438 MB	13 MB	668
ChatGPT Generative AI	8	839 MB	219 MB	1.1K

ChatGPT is a free and easy-to-use AI assistant that can help you with writing, learning, brainstorming, and more.

Disclaimer

8

GENERAL 7

Category: Generative AI	Headquarters: United States	Data center: United States
Hosting company: Cloudflare	Founded: 2015	Holding: Private
Domain: 16 *.chat.openai.com, *.chatgpt.com, *	Terms of service: openai.com/policies/terms-of-use/...	Domain registration: Nov 30, 2022
Consumer popularity: 10	Privacy policy: openai.com/policies/privacy-policy/	Logon URL: 2 openai.com/api/login, auth0.openai.cc
Vendor: OpenAI	Data types: 2 Documents, Media files	✓ Disaster Recovery Plan

SECURITY 10

Latest breach: Mar 20, 2023	Data-at-rest encryption method: AES	✓ Multi-factor authentication
✓ IP address restriction	✓ User audit trail	✓ Admin audit trail
✓ Data audit trail	✓ User can upload data	⊖ Data classification
✗ Remember password	✓ User-roles support	⊖ File sharing
✓ Valid certificate name	✓ Trusted certificate	Encryption protocol: TLS 1.3
✓ Heartbleed patched	HTTP security headers: Partial	✓ Supports SAML
✓ Protected against DROWN	✓ Penetration Testing	✓ Requires user authentication
Password policy: Partial		

COMPLIANCE 7

⊖ ISO 27001	⊖ ISO 27018	⊖ ISO 27017

Defender for Cloud Apps
Evaluate service risks

- IP address restriction
- Data audit trail
- Remember password
- Valid certificate name
- Heartbleed patched
- Protected against DROWN
- Password policy: **Partial**
- User audit trail
- User can upload data
- User-roles support
- Trusted certificate
- HTTP security headers: **Partial**
- Penetration Testing
- Supports SAML
- Requires user authentication

COMPLIANCE 7

- ISO 27001
- ISO 27002
- GAAP
- ITAR
- SOC 3
- SSAE 18
- GLBA
- Privacy Shield
- COBIT
- HITRUST CSF
- ISO 27018
- FINRA
- HIPAA
- SOC 1
- SOX
- Safe Harbor
- FedRAMP level: Not supported
- FFIEC
- COPPA
- Jericho Forum Commandments
- ISO 27017
- FISMA
- ISAE 3402
- SOC 2
- SP 800-53
- PCI DSS version
- CSA STAR level: Self-assessment
- GAPP
- FERPA

LEGAL 10

- Data ownership
- GDPR readiness statement: openai.com/policie...
- GDPR - Data protection
- DMCA
- GDPR - Right to erasure
- GDPR - User ownership
- Data retention policy: Deleted within more than 3 ...
- GDPR - Report data breaches

Advanced hunting

New query*

Run query | Set in query | Save | Share

Query

```
1  // KQL query written by Sulava (Tatu Seppälä
2  let IdentityInfoLatest = IdentityInfo
3      | where isnotempty(JobTitle)
4      | summarize LatestRecord = arg_max(Timest
5      | project AccountUpn, JobTitle, Departmen
6  CloudAppEvents
7  | where Timestamp >= ago(30d)
8  | where ActionType == "FileUploadedToCloud"
9  | project Timestamp, AccountId, RawEventData.
10 | extend ParentDomain = extract(@"[^.]+\.[^.]
11 | extend UserId = tostring(RawEventData_UserI
12 | join kind=inner (IdentityInfoLatest) on $le
13 | summarize count() by tostring(ParentDomain)
14 | sort by count_ desc
```

TargetDomain	JobTitle	# of files uploaded
drive.google.com	Service Designer	148
icloud.com	Data Analyst	119
salesforce.com	Sales Manager	115
! chatgpt.com	Graphic Designer	114
linkedin.com	Marketing Specialist	102
drive.google.com	Business Controller	94
shopify.com	E-commerce Manager	91
myworkday.com	HR Specialist	87

Getting started | Results | Query history

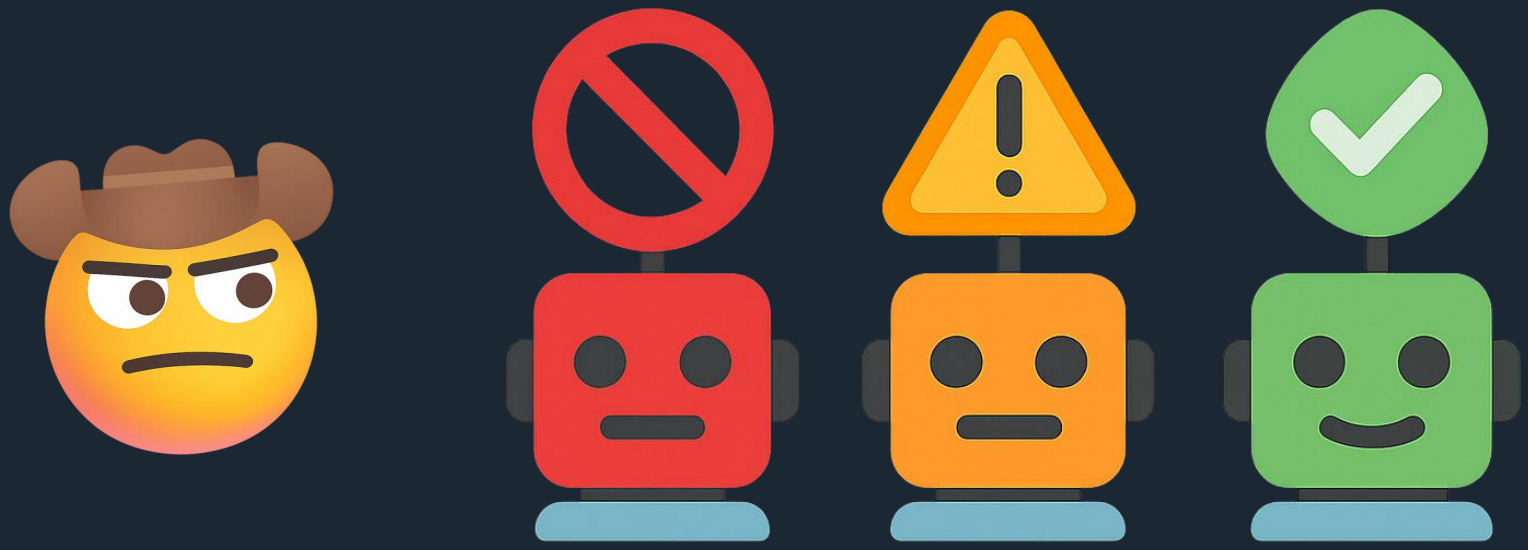
Export | Show empty columns | 299 items | Search | 00:02.548 | Low | Chart type | Full screen

Filters: Add filter

Defender XDR

Gather trends and insights from the Unified Audit Log with Advanced Hunting

📊 Grading services by risk



Cloud Discovery

Defender-managed endpoints | Last 30 days | Actions

Updated on Sep 23, 2025, 9:41 PM

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

Queries: Select a query | Save as

Advanced filters

Apps: Search for apps... | App tag : | Risk score: 0 — 6 | Compliance risk factor: **Select factors**

Security risk factor: **Select factors**

Bulk selection | New policy from search | Export | 1 - 3 of 3 discovered apps | Table settings

App	Risk ...	Tags	Traffic	Upload	Transa...	Users	IP addresses	Devic...	Last se...	Actions
PhotoRoom Generative AI	6		311 KB	—	1	1	1	1	Sep 4, 2025	
Delphi Generative AI	4		2 MB	—	1	1	1	1	Sep 17, 2025	
Gamma App Generative AI	6		31 KB	31 KB	1	1	1	1	Sep 22, 2025	

Cloud Discovery

Defender-managed endpoints | Last 30 days | Actions

Updated on Sep 23, 2025, 9:41 PM

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

Queries: Select a query | Save as

Advanced filters

Apps: Search for apps... | App tag : | None | Risk score: 0 — 6 | Compliance risk factor: **Select factors**

Security risk factor: **Select factors**

- Protected against DROWN
- Remember password
- Requires user authentication
- Supports SAML
- Trusted certificate
- User audit trail
- User can upload data
- User-roles support
- Valid certificate name

search | Export | 1 - 3 of 3 discovered apps | Table settings

Risk ...	Tags	Traffic	Upload	Transa...	Users	IP addresses	Devic...	Last se...	Actions
6		311 KB	—	1	1	1	1	Sep 4, 2025	
4		2 MB	—	1	1	1	1	Sep 17, 2025	
6		31 KB	31 KB	1	1	1	1	Sep 22, 2025	

Cloud Discovery

Defender-managed endpoints | Last 30 days | Actions

Updated on Sep 23, 2025, 9:41 PM

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

Queries: Select a query | Save as

Advanced filters

Apps: Search for apps... | App tag: None | Risk score: 0 — 6 | Compliance risk factor: **Select factors**

Security risk factor: **User can upload data**

Bulk selection | New policy from search | Export

1 - 3 of 3 discovered apps | Table settings

App	Risk ...	Tags	Traffic	Upload	Transa...	Users	IP addresses	Devic...	Last se...	Actions
PhotoRoom Generative AI	6				1	1	1	1	Sep 4, 2025	
Delphi Generative AI	4				1	1	1	1	Sep 17, 2025	
Gamma App Generative AI	6				1	1	1	1	Sep 22, 2025	

Cloud Discovery

Defender-managed endpoints | Last 30 days | Actions

Updated on Sep 23, 2025, 9:41 PM

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

Queries: Select a query | Save as

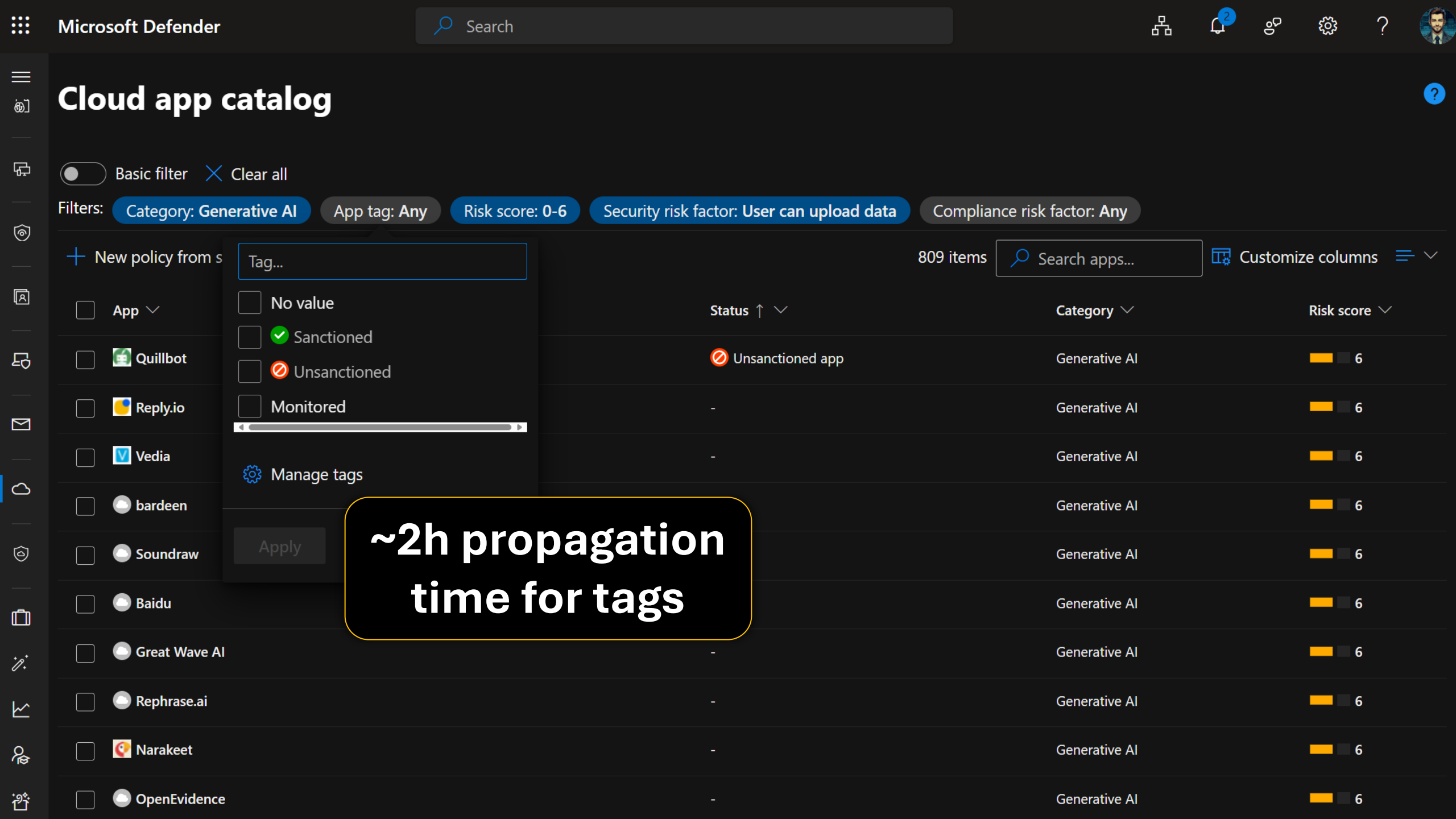
Advanced filters

Apps: Search for apps... | App tag : | None | Risk score: 0 — 10 | Compliance risk factor: **Select factors**

Security risk factor: **User can upload data**

Bulk selection | New policy from search | Export | 1 - 19 of 19 discovered apps | Table settings

App	Risk ...	Tags	Traffic	Upload	Transactions	Users	IP addresses	Devic...	Last se...	Actions
Microsoft 365 Copilot Chat Generative AI	10		[illegible]	13 MB	668	108	260	115	Sep 23, 2025	
ChatGPT Generative AI	8			219 MB	1.1K	33	154	36	Sep 23, 2025	
Microsoft Copilot Generative AI	10			11 MB	331	23	97	27	Sep 23, 2025	
GitHub Copilot Generative AI	10		108 MB	75 MB	332	17	23	17	Sep 23, 2025	
Microsoft Copilot Studio Generative AI	10		33 MB	759 KB	27	11	12	11	Sep 18, 2025	
Microsoft Designer Generative AI	10		60 MB	—	22	10	11	10	Sep 21, 2025	


Microsoft Defender
Search
Cloud app catalog
Basic filter
Clear all
Filters:
Category: Generative AI
App tag: Any
Risk score: 0-6
Security risk factor: User can upload data
Compliance risk factor: Any
New policy from s
Tag...
No value
Sanctioned
Unsanctioned
Monitored
Manage tags
Apply
809 items
Search apps...
Customize columns
App
Status
Category
Risk score
Quillbot
Unsanctioned app
Generative AI
6
Reply.io
Generative AI
6
Vedia
Generative AI
6
bardeen
Generative AI
6
Soundraw
Generative AI
6
Baidu
Generative AI
6
Great Wave AI
Generative AI
6
Rephrase.ai
Generative AI
6
Narakeet
Generative AI
6
OpenEvidence
Generative AI
6
~2h propagation time for tags

Search

Cloud app catalog

Basic filter

Filters: Category: Any | App tag: Any | Risk score: Any | Security risk factor: Any | Cor

Sanction | Unsanction | Tag app | Deploy app | App score | App details

App	Status	Cat
Microsoft 365 Copilot	Protected app	Col
Microsoft Copilot Studio	Protected app	Ge
Microsoft Security Copilot	-	Ge
Microsoft Copilot	Protected app	Ge
Microsoft 365 Copilot Chat	Protected app	Ge
GitHub Copilot Enterprise API	-	AI
GitHub Copilot	Sanctioned app	Ge
Skills Copilot	-	Pro
Education Copilot	-	Ge

GitHub Copilot

Sanction | Unsanction | Tag app | ...

Info

Sanctioned app 10

GitHub Copilot is an AI coding assistant that helps you write code faster and with less effort, allowing you to focus more energy on problem solving and collaboration.

General | Security | Compliance | Legal

Score
8

Category
Generative AI

Headquarters
United States

Data center
Multiple locations

Hosting company
Microsoft Azure

Founded
1975

Holding
Public

Domain
*.github.com/copilot

Terms of service
github.com/site/terms

Cloud app catalog

Basic filter

Filters: Category: Any | App tag: Any | Risk score: Any | Security risk factor: Any | Cor

Tag app | Deploy app | App score | App details

App	Status	Cat
Microsoft 365 Copilot	Protected app	Col
Microsoft Copilot Studio	Protected app	Ge
Microsoft Security Copilot	-	Ge
Microsoft Copilot	Protected app	Ge
Microsoft 365 Copilot Chat	Protected app	Ge
GitHub Copilot Enterprise API	-	AI
GitHub Copilot	Sanctioned app	Ge
Skills Copilot	-	Pro
Education Copilot	-	Ge

Microsoft 365 Copilot

Tag app | Request score update... | ···

Info

1 conditional access app controlled instance — 10

Microsoft 365 Copilot is an AI powered tool that provides real time intelligence to complete tasks more efficiently. The Microsoft 365 Copilot app, formerly Office, lets you create, share, and collaborate all in one place with your favorite apps including Copilot. Users get content relevant to their work tasks, like drafting, summarizing, all in the context of their work within their Microsoft 365 app.

General | Security | Compliance | Legal

Score
10

Category
Collaboration

Headquarters
United States

Data center
Multiple locations

Hosting company
Microsoft Azure

Founded
1975

Holding
Public

Domain

Security only works if the **secure** way also happens to be the **easy** way.

-The 2nd immutable law of security

David S. Platt
Software Legend
UX advocate

That's the key 🔑

Your users will do whatever is easiest,
no matter what.

If you can make the secure thing be easier,
they will do it.

And instead of trying to get them to do
more work *to be safer..*

Hey, how can we make them safer with
even less work?

🖥️ Risk-based controls

Website blocked by your organiz

Blocked content https://www.deepseek.com/en

About deepseek.com

This site is blocked

This site is blocked by your organization. Contact your administrator for more information.

Permissions for this site

Cookies and site data

Tracking prevention for this site (Balanced)

Trackers (0 blocked)

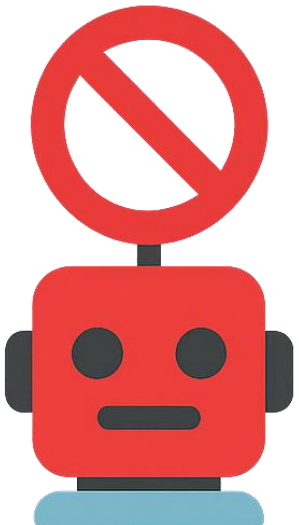
This website is blocked by your organization.

Hosted by www.deepseek.com

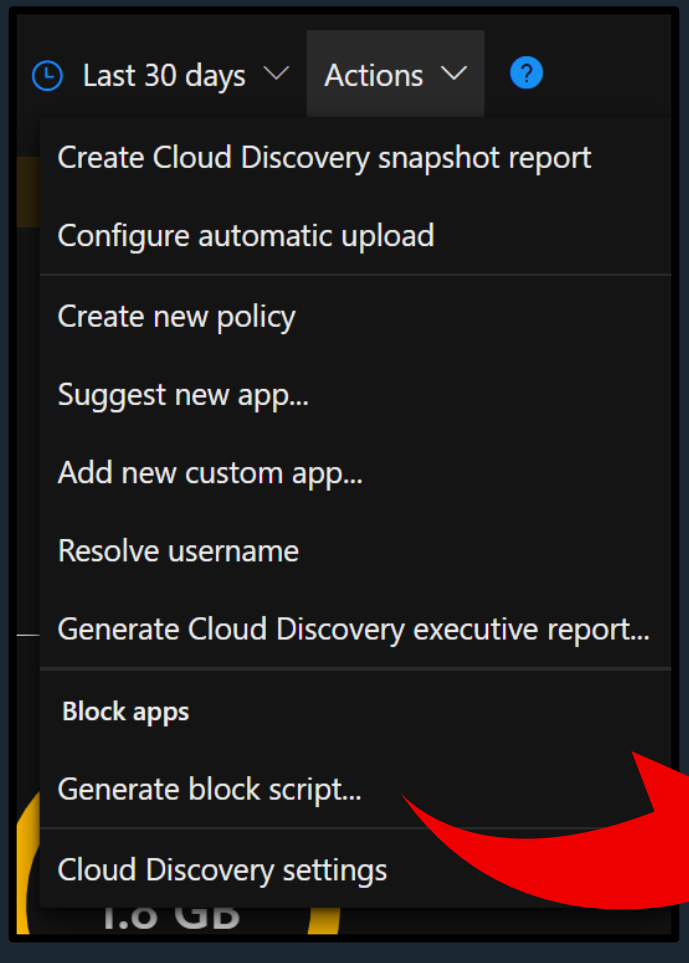
Contact your administrator for more information. Visit the support page.

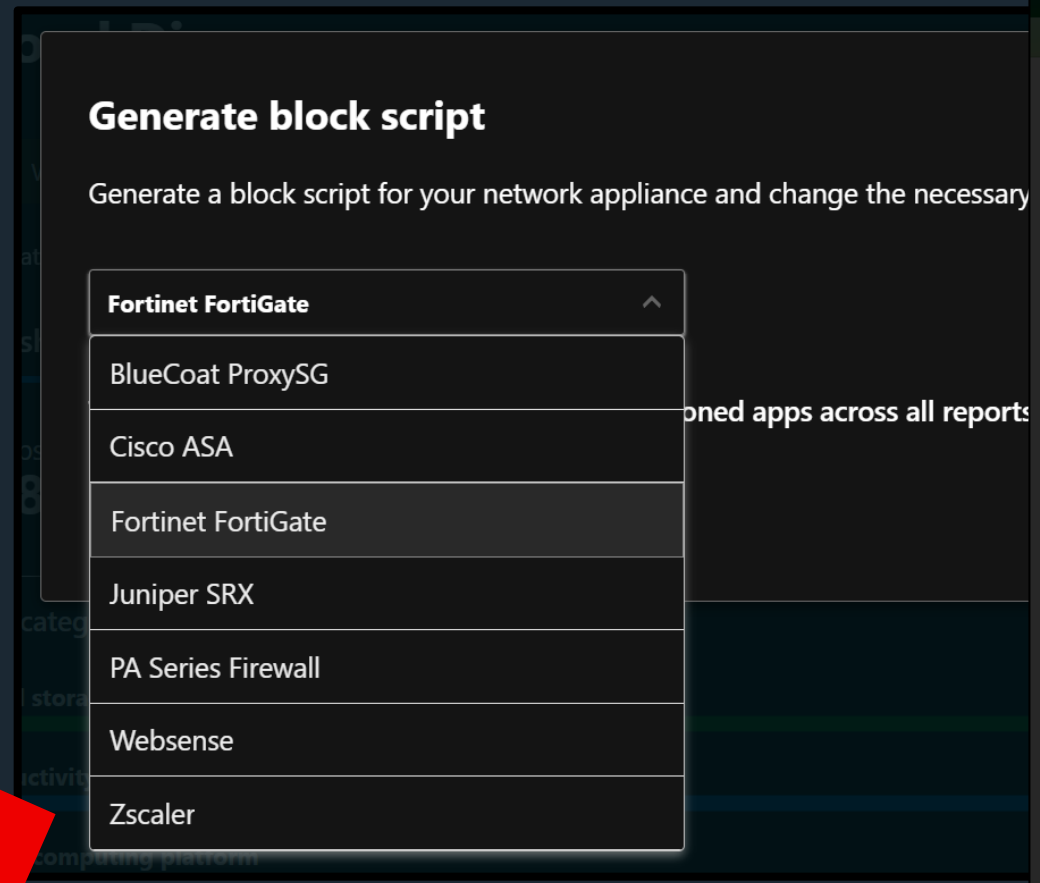
Go back

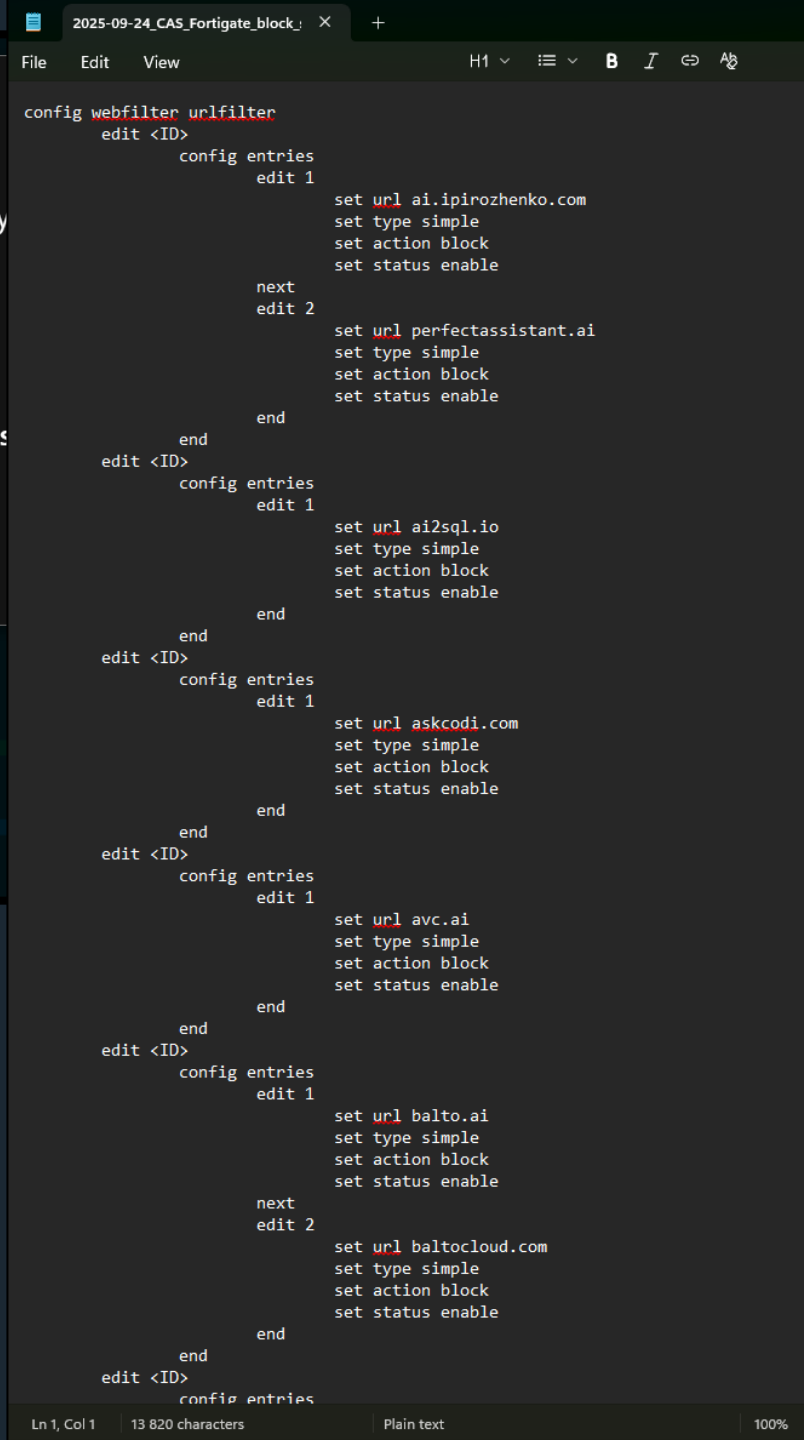
Microsoft Security



High risk → Unsanction in MDA

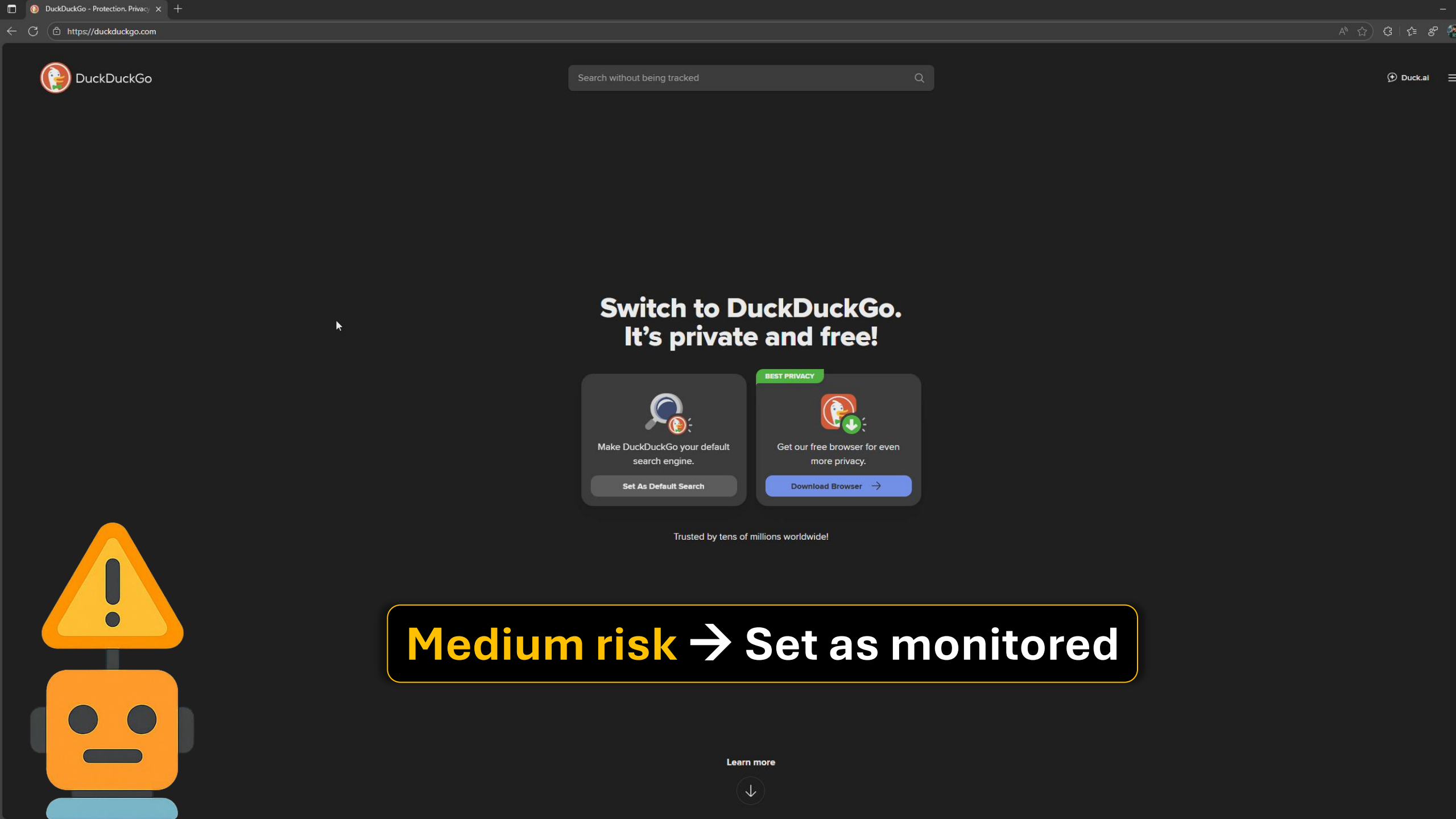






Defender for Cloud Apps

Generate block script for on-prem network appliances


DuckDuckGo - Protection. Privacy
https://duckduckgo.com
DuckDuckGo
Search without being tracked
Duck.ai
Switch to DuckDuckGo.
It's private and free!
BEST PRIVACY
Make DuckDuckGo your default search engine.
Set As Default Search
Get our free browser for even more privacy.
Download Browser
Trusted by tens of millions worldwide!
Learn more
Medium risk → Set as monitored

Cloud apps
Cloud discovery
Cloud app catalog
OAuth apps
App governance
Activity log
Governance log
Policies
Cloud infrastructure
Cases
SOC optimization
Reports
Learning hub
Trials
More resources
System
Audit

My email notifications
AI Agents
Copilot Studio AI Agents
Cloud Discovery
Score metrics
Snapshot reports
Continuous reports
Automatic log upload
App Tags
Exclude entities
Microsoft Defender for Endpoint
User enrichment
Anonymization
Delete data
Connected apps
App Connectors
Conditional Access App Control apps

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint Integration

Enforce app access
Enabling this will Block access to apps that were marked as Unsanctioned and will deliver a Warning on access and allow bypass to apps marked as Monitored.

Alerts

Informational

User notifications

Notification URL

https://seppala365dev.sharepoint.com/sites...

Enter the redirect URL for warned users

Bypass duration

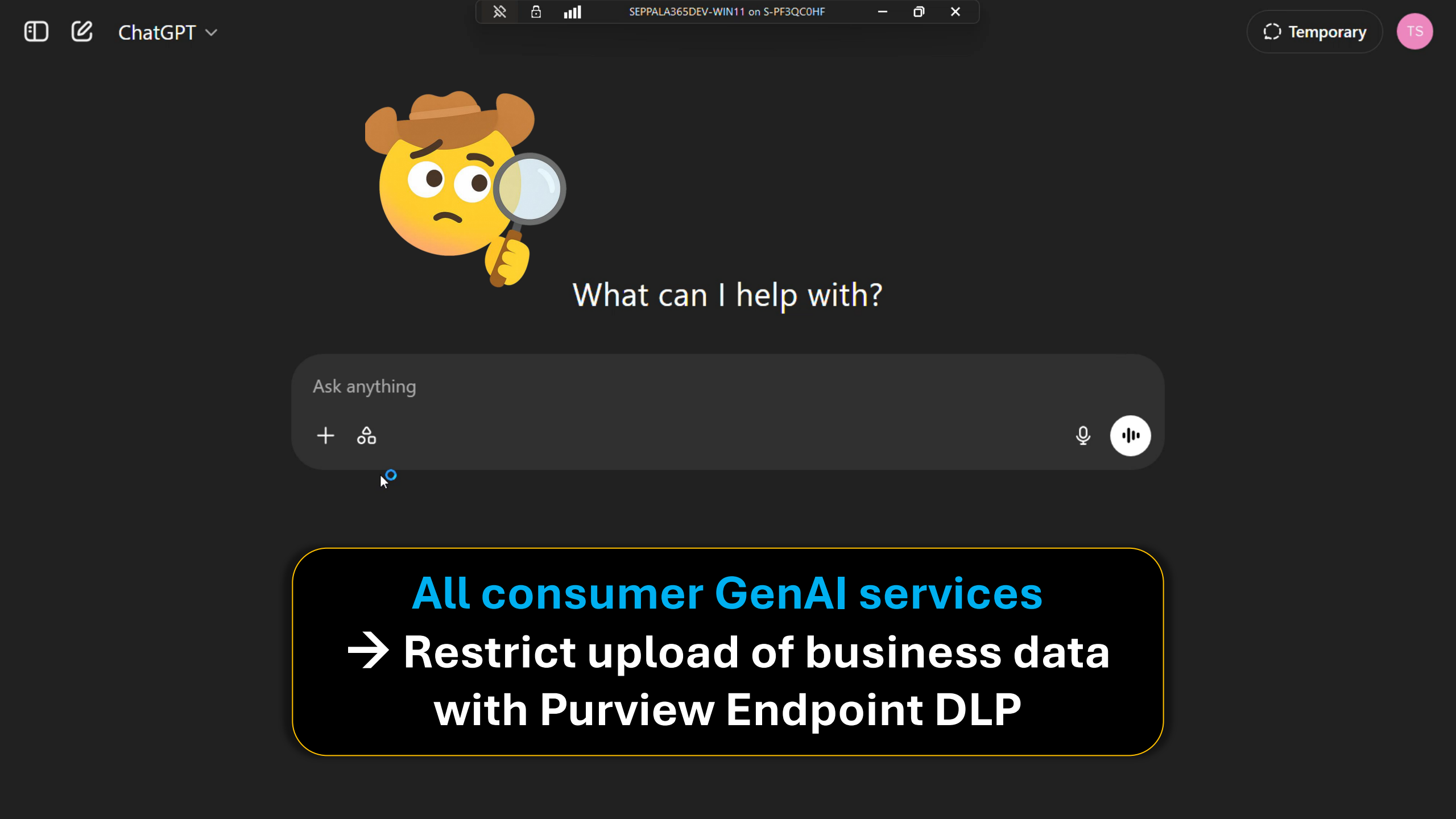
1 hours

Notification URL for blocked apps

https://seppala365dev.sharepoint.com/sites...

Enter the Custom/Informational URL for blocked users

Save


SEPPALA365DEV-WIN11 on S-PF3QC0HF
ChatGPT
Temporary
TS
What can I help with?
Ask anything
All consumer GenAI services
→ Restrict upload of business data with Purview Endpoint DLP

What about mobile devices?

Microsoft Intune

Limit transfer of data from work apps to consumer apps with APP

Microsoft Intune admin center

- Home
- Dashboard
- All services
- Explorer
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Edit policy

MAM-Android

1 Apps 2 Review + save

If you apply assignment filters to this policy, the 'Device Management Type' property will apply in addition to the values specified for 'Target to apps on all device types' and 'Device types' on the 'Apps' page.

To edit device management type targeting, reset 'Target to apps on all device types' = 'Yes'. Then create a MAM assignment filter with the desired values for 'Device Management Type'. Learn more about assigning App Protection Policies

Choose how you want to apply this policy to apps on different devices. Then add at least one app.

Target to apps on all device types: Yes | No

Device types: 0 selected

Target policy to: All Apps

We'll continue to add managed apps to your policy as they become available in Intune. View a list of apps that will be targeted

Review + save Cancel

Basics | Apps | 3 Data protection | 4 Access requirements | 5 Conditional launch | 6 Assignm

This group includes the Data Loss Prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings

Select one of the following options to specify the apps that this app can send data to:

Policy managed apps: Only allow sending org data to other policy managed apps

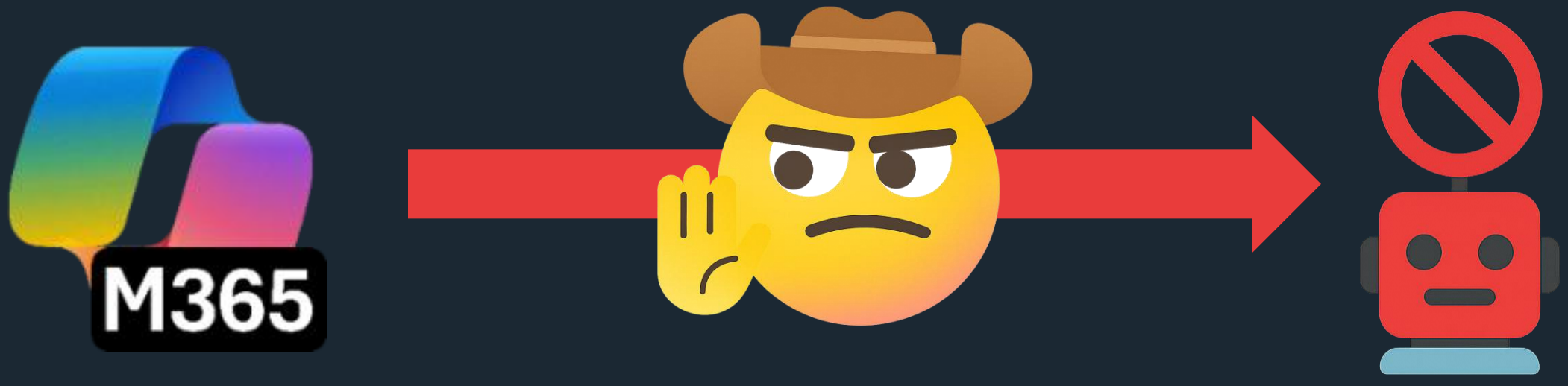
All Apps: Allow sending org data to any app

None: Do not allow sending org data to any app

Block

Send org data to other apps ⓘ

Policy managed apps



Cut, copy, and paste data between your app and other approved apps installed on the device. Choose to block these actions completely between apps, allow these actions for use with any app, or restrict use to apps that your organization manages.

Policy-managed apps with paste in gives you the option to accept incoming content pasted from another app. However, it blocks users from sharing content outwardly, unless sharing with a managed app.

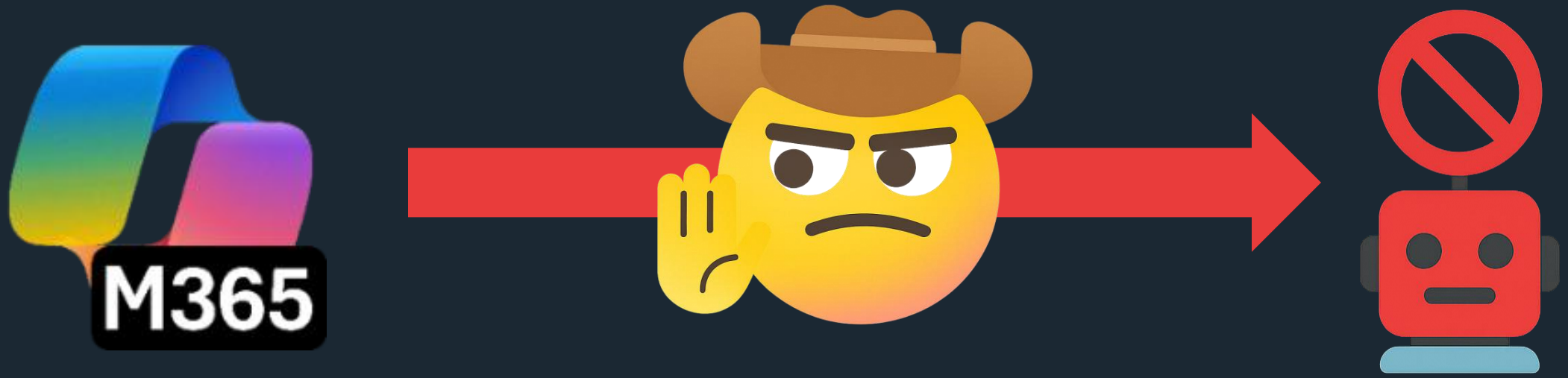
Block

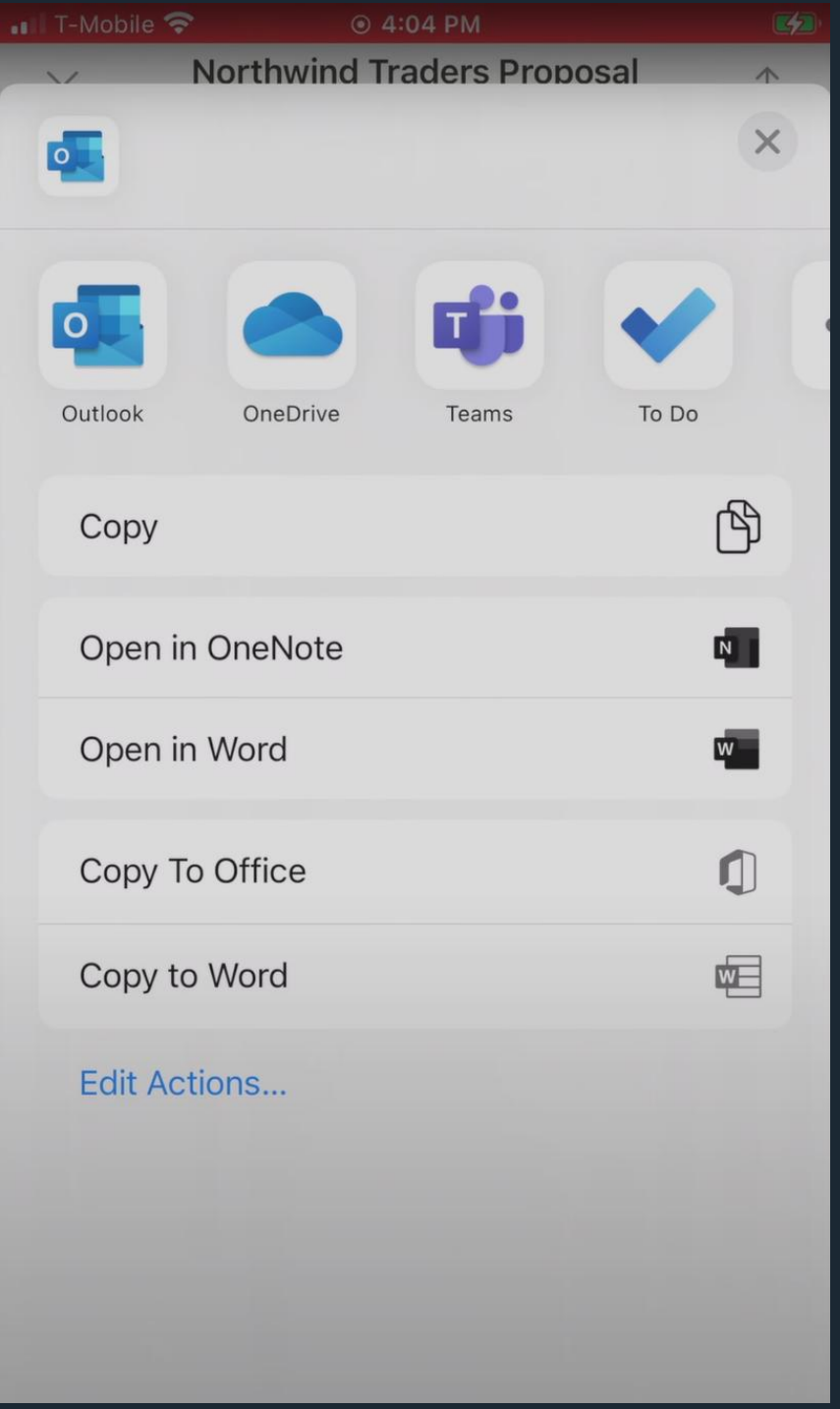
Restrict cut, copy, and paste between other apps

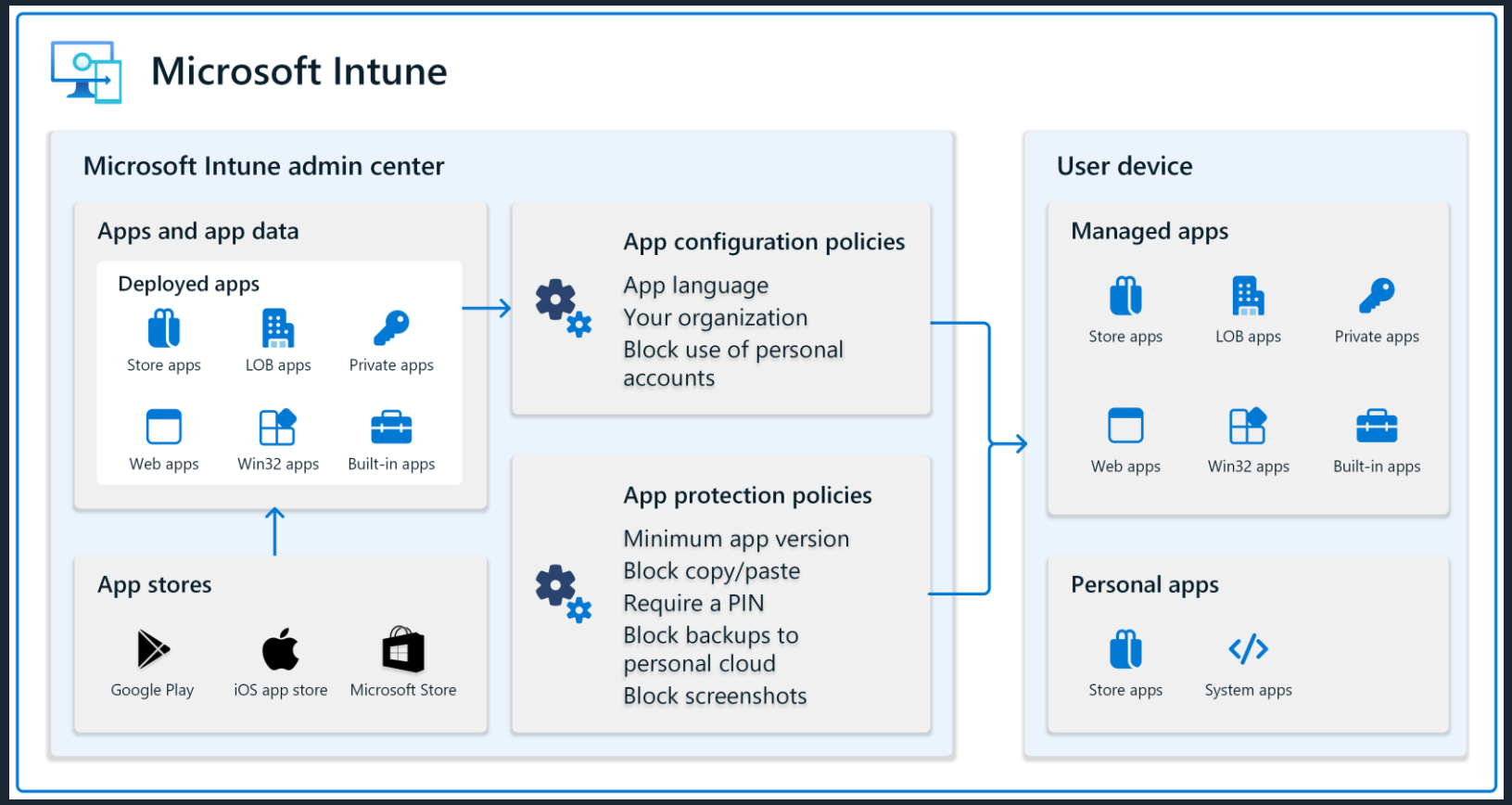
Policy managed apps with paste in

Cut and copy character limit for any app *

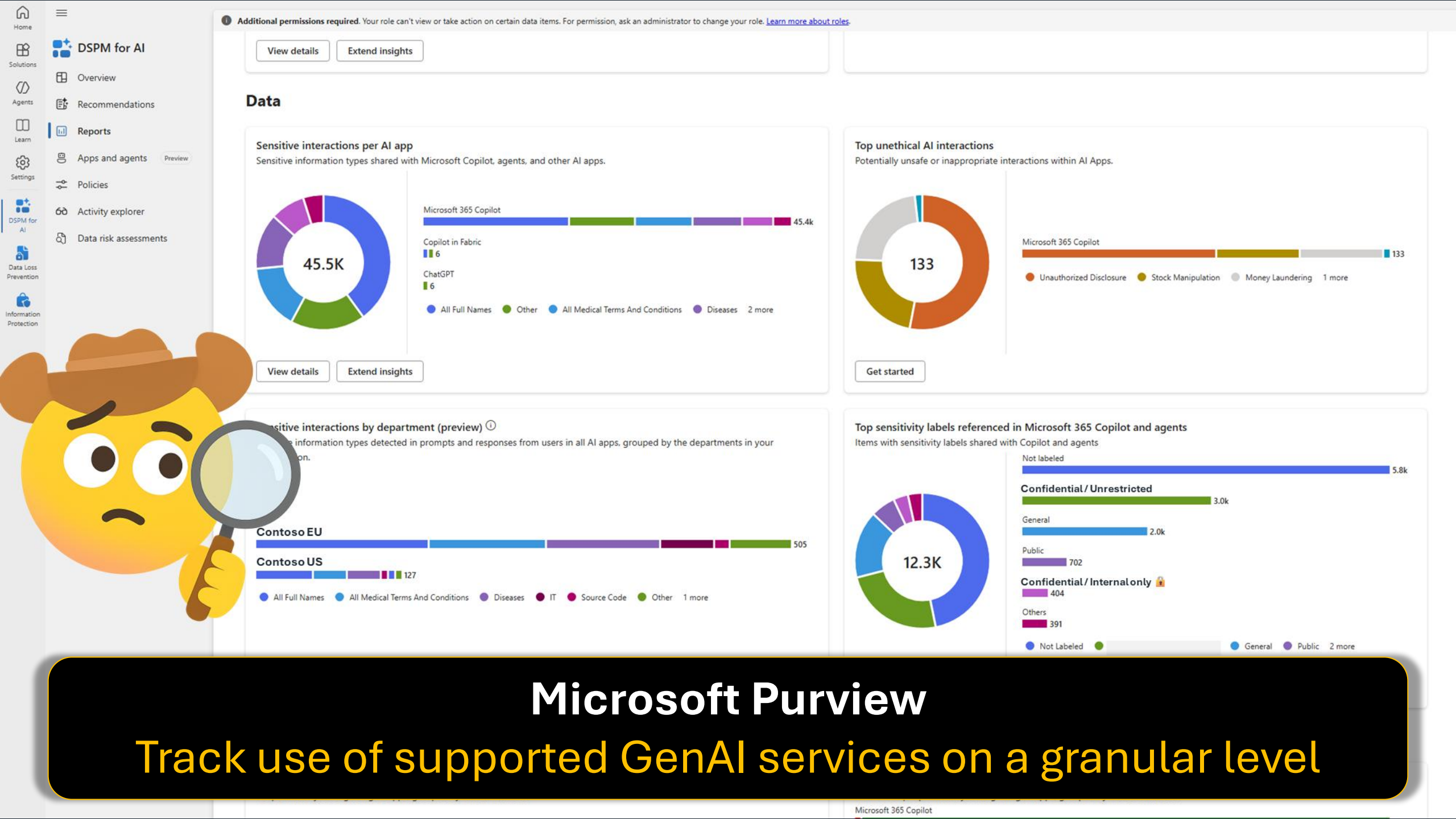
0




T-Mobile
4:04 PM
Northwind Traders Proposal
Outlook
OneDrive
Teams
To Do
Copy
Open in OneNote
Open in Word
Copy To Office
Copy to Word
Edit Actions...


Microsoft Intune
Microsoft Intune admin center
Apps and app data
Deployed apps
Store apps
LOB apps
Private apps
Web apps
Win32 apps
Built-in apps
App stores
Google Play
iOS app store
Microsoft Store
App configuration policies
App language
Your organization
Block use of personal accounts
App protection policies
Minimum app version
Block copy/paste
Require a PIN
Block backups to personal cloud
Block screenshots
User device
Managed apps
Store apps
LOB apps
Private apps
Web apps
Win32 apps
Built-in apps
Personal apps
Store apps
System apps

📈 Ongoing monitoring

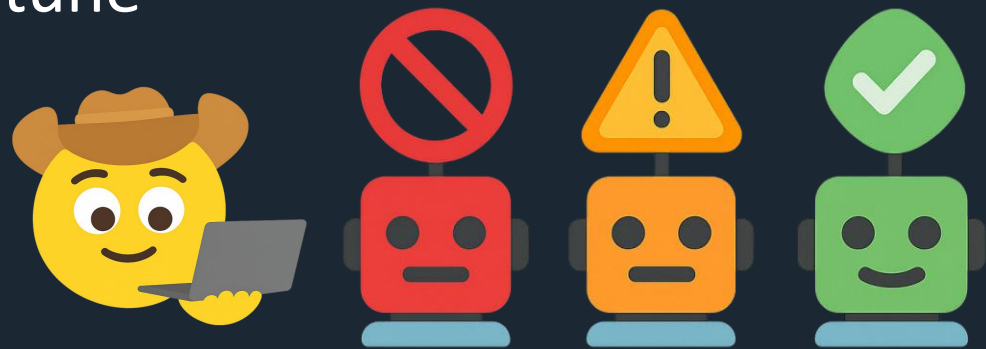


Microsoft Purview

Track use of supported GenAI services on a granular level

⚡ Action points

- **Onboard** devices to Endpoint DLP → Purview
- **Integrate** Defender for Endpoint and Defender for Cloud Apps
- **Create** Endpoint DLP rules in simulation mode → Enable later
- **Discover** GenAI usage trends and grade AI services by risk
- **Block** high risk services, treat less risky services with a soft touch
- **Provide** training and guidance to adopt authorized GenAI
- **Monitor** ongoing trends and fine-tune



What's next..

- **Network Data Loss Prevention**! Catch GenAI add-ons etc.
- **Edge for Business** as a control plane
- **Inline DLP** for prompts to ChatGPT, Gemini and more
- Risky GenAI use as an indicator in **Insider Risk Management**

Comments or questions?

Connect with me!