

skaylink

Cyber Defense

Security starts here.

Skaylink GmbH

Data First: Governance & KI zusammen denken, priorisieren, gestalten

Security & Compliance für Copilot, Agents und
Unternehmensdaten





Data Security Roadmap Microsoft Purview

Insider Risk Management

Identify and act on insider risks with an integrated end-to-end approach

Advanced Data Classification / Advanced Information Protection

Advanced Classifier, Rule based classification

Advanced Data Loss Prevention

Audit Premium

Power your forensic and compliance investigations + (365 days+ more signals captured)

eDiscovery + Premium

RMS decryption Data Review
OCR / Re-indexing

DSPM for AI

Discover and secure all AI activity in Microsoft Copilot, agents, and other AI apps.

MICROSOFT 365 E5

Data Classification

Define and explore relevant content in your Org.

Information Protection

Know, classify, & protect sensitive information

Data Loss Prevention

Prevent sensitive information from leaving your organization

Audit Standard

Power your forensic and compliance investigations (180 days)

eDiscovery Standard

Discover, preserve, collect, process, cull, and analyze your data in place

MICROSOFT 365 E3

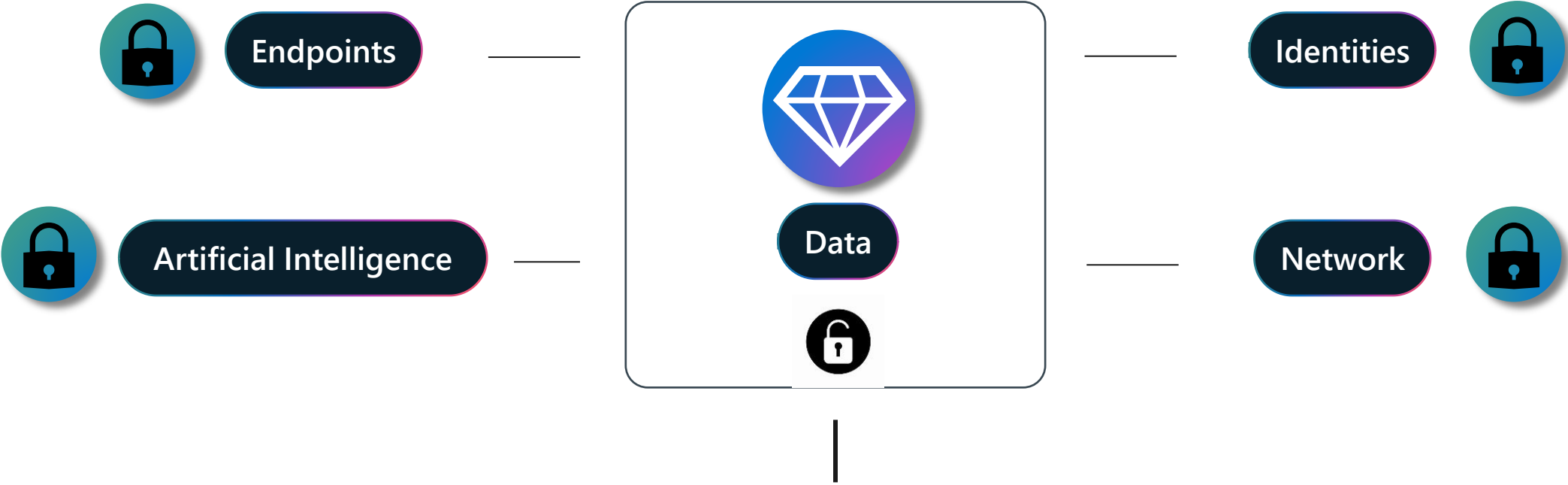
Included in ME3

Included in ME5 Compliance

Pay as you go billing

Zero Trust Framework

Thinking from a data perspective



Have you secured your most valuable treasure: your data?

Classifiers, Labels and Categories



Generative AI



AI Security via Microsoft Purview

Restriction and logging of functionalities in AI



Data Loss Prevention Policies
Data Security Posture Management for AI

Microsoft Defender Solutions into consideration:

- Defender for Cloud Apps
- Defender for Endpoint



Recognition

Recognition of generative AI via Defender for cloud apps

Automated auditing and blocking of shadow AI

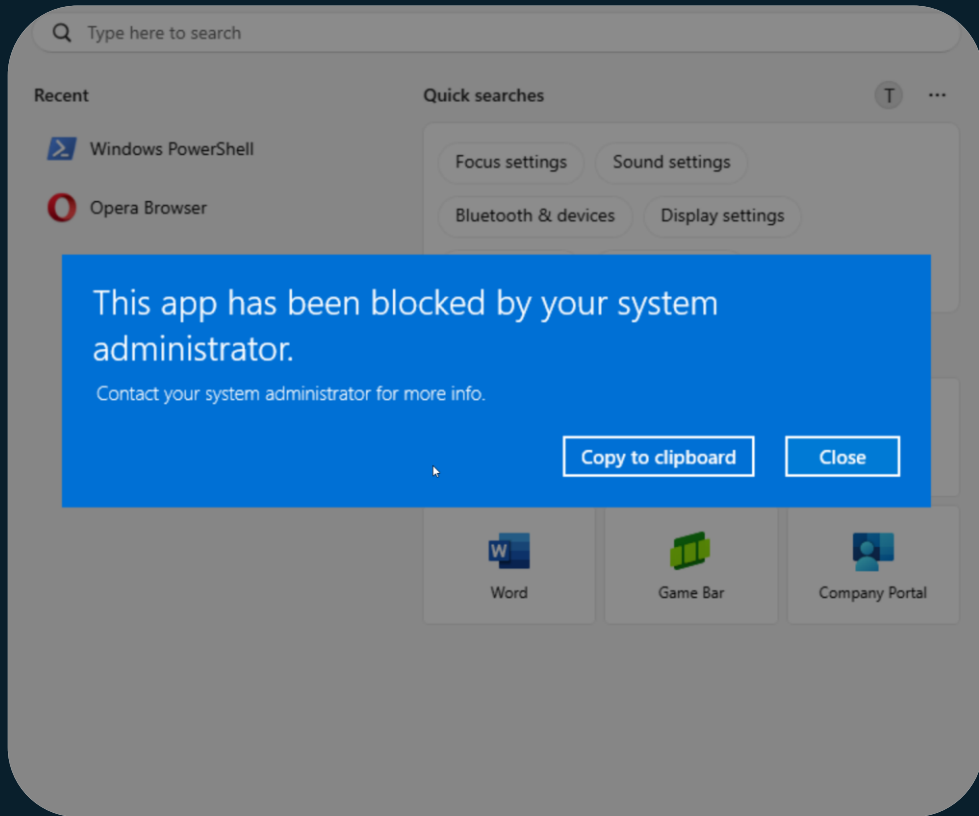


Protection

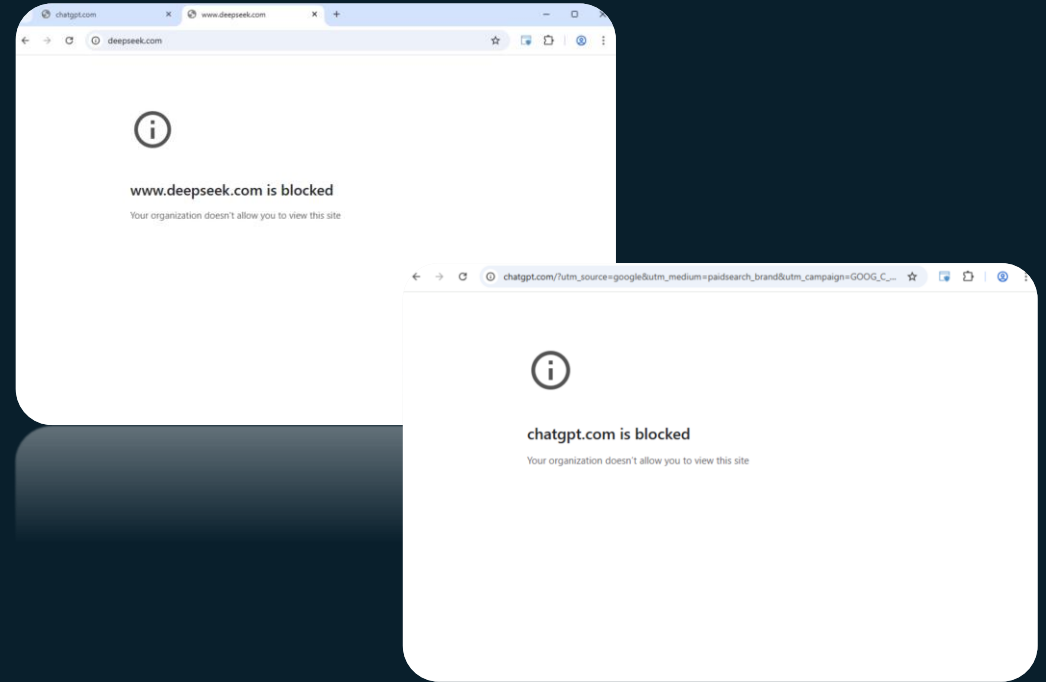
Protection against the loss of sensitive data to AI with Defender for Endpoint

Endpoint AI Protection

Trying to use unallowed Browser

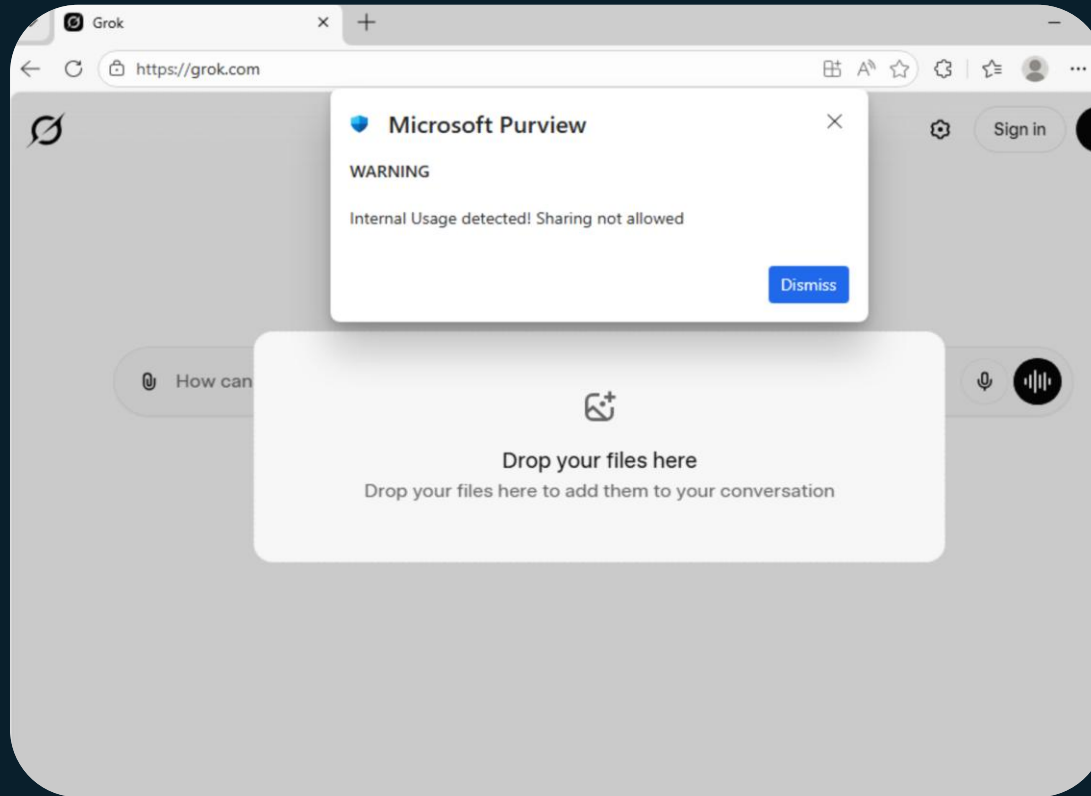


Trying to use unmanaged AI



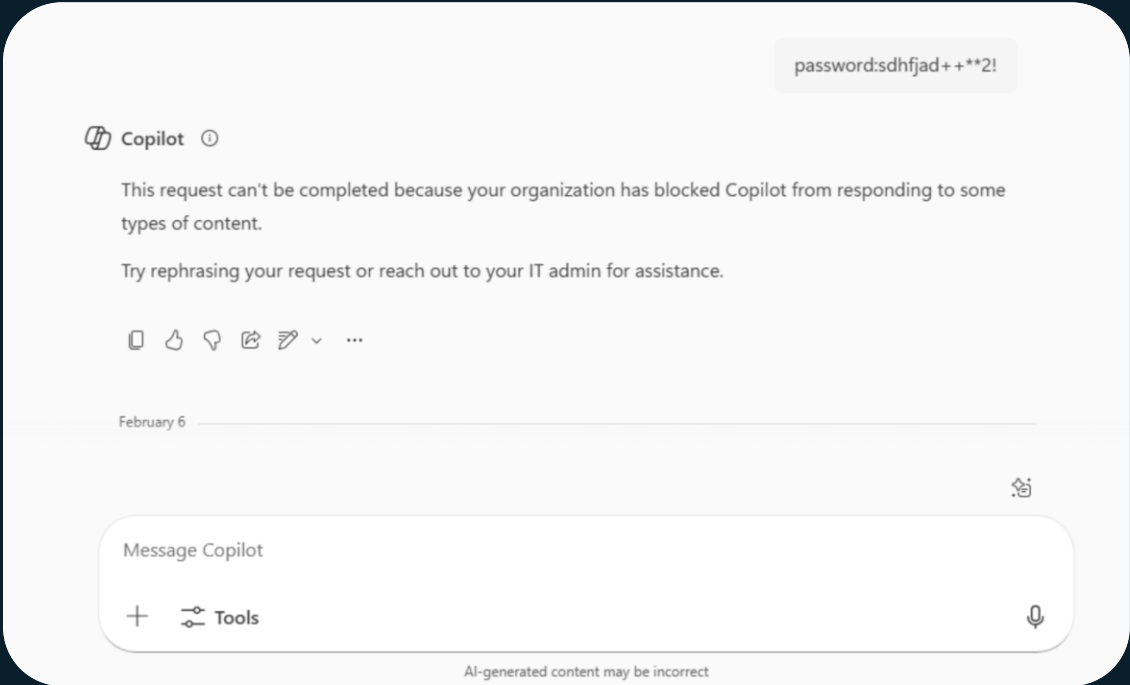
Endpoint DLP

Trying to upload sensitive data to unmanaged AI



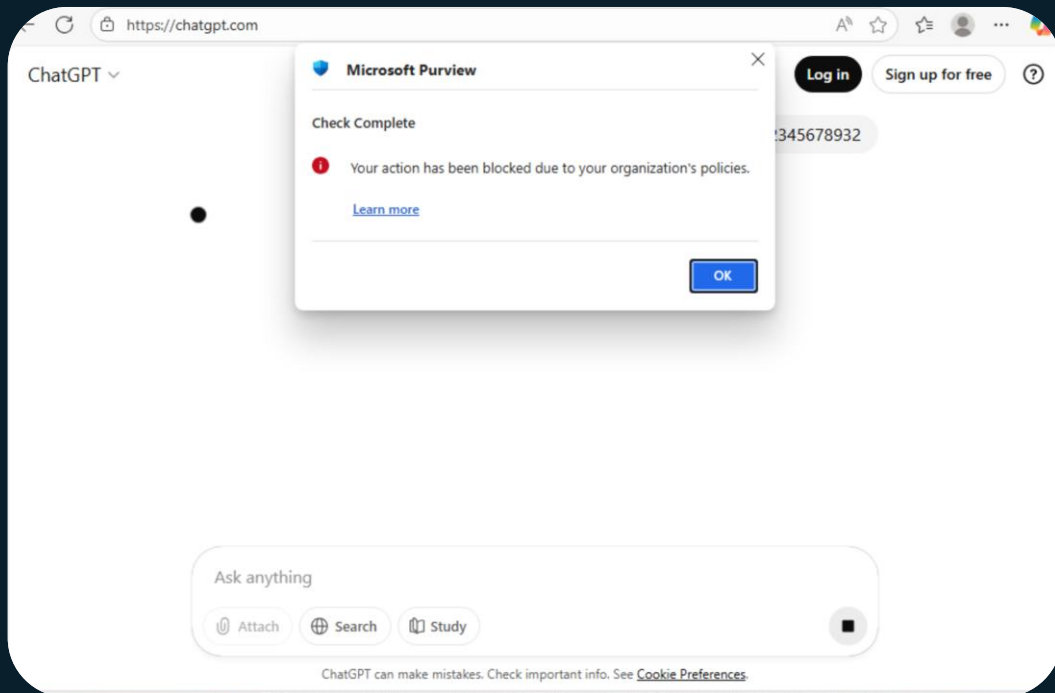
DLP for Microsoft 365 Copilot

Trying to prompt Sensitive Info Type (Password) to Microsoft 365 Copilot Chat

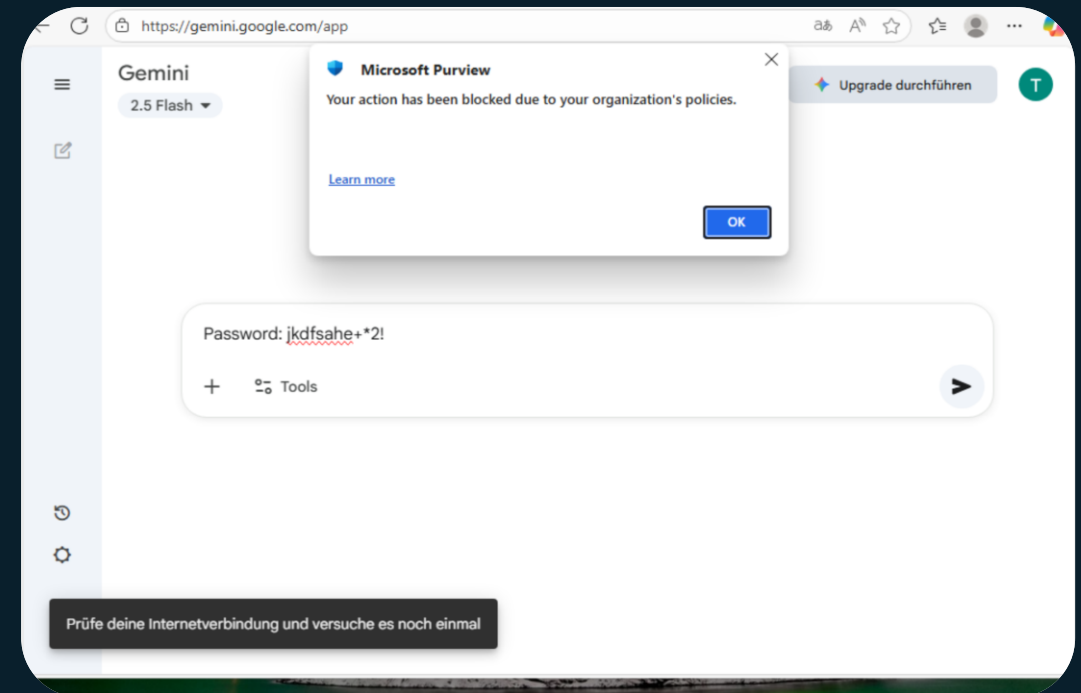


Classifier in AI

Trying to prompt Sensitive Info Type (IBAN) to ChatGPT



Trying to prompt Sensitive Info Type (Password) to Gemini



Data Security Posture Management for AI & Policies



Data Risk Assessment

Identify:

Review assessment results and detect sensitive data access.

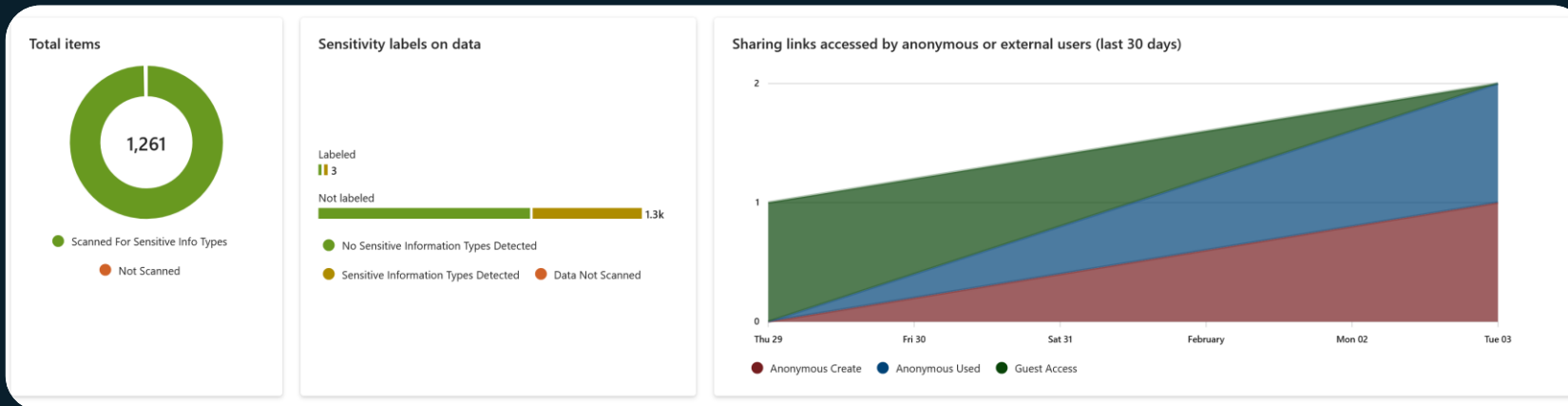
Protect:

Limit Copilot & agent access; apply labels and retention

Monitor:

Continuously review SharePoint sites, permissions, and access.

Data Loss Prevention:
Restrict Microsoft 365 Copilot / unmanaged AI from processing content



DSPM for AI

DSPM for AI

- Overview
- Recommendations
- Reports
- Apps and agents** Preview
- Policies
- Activity explorer
- Data risk assessments

Apps and agents (preview)

Understand the depth and breadth of Microsoft Purview protection for AI applications and agents in the last 30 days.

Apps Agents

Refresh Export 8 items Search Group list Edit columns

AI app	Protection status	User trend	Prompts trend	Response trend	Data protection	Data compliance	Agents
Microsoft Copilot Studio (1) <input type="checkbox"/> Microsoft Copilot Studio	Monitored	No data available	No data available	No data available	0 Policies	0 Policies	0
Copilot experiences & agents (3) <input type="checkbox"/> Microsoft 365 Copilot	Monitored				2 Policies	0 Policies	1
<input type="checkbox"/> Copilot in Fabric	Monitored	No data available	No data available	No data available	0 Policies	0 Policies	0
<input type="checkbox"/> Security Copilot	Monitored	No data available	No data available	No data available	0 Policies	0 Policies	0
Enterprise AI apps (1) <input type="checkbox"/> ChatGPT Enterprise	Monitored	No data available	No data available	No data available	0 Policies	0 Policies	0
Other AI apps (3) <input type="checkbox"/> ChatGPT	Monitored			No data available	5 Policies	0 Policies	1
<input type="checkbox"/> Google Gemini	Monitored			No data available	5 Policies	0 Policies	1
<input type="checkbox"/> Microsoft Copilot	Monitored			No data available	5 Policies	0 Policies	1



Based on:

- Sensitive Info Types
- Labels
- Trainable Classifier
- Collection Policies
- Data Loss Prevention
- Policies
- Defender for Cloud
- Apps

Sample DSPM policy for AI

DSPM for AI

- Overview
- Recommendations
- Reports
- Apps and agents
- Policies
- Activity explorer**
- Data risk assessments

Activity explorer

Review AI activity including AI interactions (prompts and responses), activity with sensitive info types, and more.

Filters: Timestamp: 10/13/2025-10/20/2025 Activity type: Any AI app category: Any App: Any App accessed in: Any Agent name: Any User: Any Sensitive info type: Any

Reset all

Legend: DLP rule match, Sensitive info types, AI Interaction

Export selected item Refresh

Activity type	Timestamp (UTC)	AI app category	App	App accessed in	Agent name	User
<input type="checkbox"/> Sensitive info types	Oct 20, 2025 12:45 PM	Other AI apps	Google Gemini	Browser		tomruebenunter@M365x2...
<input checked="" type="checkbox"/> AI Interaction	Oct 20, 2025 12:45 PM	Other AI apps	Google Gemini	Google Gemini		tomruebenunter@M365x2...
<input type="checkbox"/> DLP rule match	Oct 20, 2025 12:45 PM	Other AI apps	Google Gemini	Google Gemini		tomruebenunter@M365x2...
<input type="checkbox"/> Sensitive info types	Oct 20, 2025 12:45 PM	Other AI apps	ChatGPT	Browser		tomruebenunter@M365x2...
<input type="checkbox"/> DLP rule match	Oct 20, 2025 12:45 PM	Other AI apps	ChatGPT	ChatGPT		tomruebenunter@M365x2...
<input type="checkbox"/> AI Interaction	Oct 20, 2025 12:45 PM	Other AI apps	ChatGPT	ChatGPT		tomruebenunter@M365x2...
<input type="checkbox"/> Sensitive info types	Oct 20, 2025 12:44 PM	Other AI apps	ChatGPT	Browser		tomruebenunter@M365x2...
<input type="checkbox"/> DLP rule match	Oct 20, 2025 12:44 PM	Other AI apps	ChatGPT	ChatGPT		tomruebenunter@M365x2...

AI Interaction

Some data may not be available. Responses and any files referenced are not available for other AI apps.

Activity details

Activity type: AI Interaction
Timestamp: Oct 20, 2025 12:45 PM

Activity: AI App Interaction
Record ID: 8a082b1e-6995-4d6e-a381-19ed959a457e

User details

User: tomruebenunter
User risk: Low

[View more user details in insider risk management](#)

App details

AI app category: Other AI apps
App: Google Gemini
App accessed in: Google Gemini

Interaction details

Prompt: DE99500105171122334455 [Copy](#)

Sensitive info types detected [View related classification activity](#)

DSPM (preview)

- Posture
- Objectives
- AI observability
- Discover**
- Apps and agents
- Activity explorer
- Asset explorer
- Data risk assessments
- Tasks and actions
- Reports

Filters: Timestamp: 3/3/2026-3/4/2026 Activity type: Any AI app category: Any App: Any App accessed in: Any Agents involved: Any User participant: Any Sensitive info type: Any

Add filter Reset all

Legend: AI website visit, DLP rule match, AI Interaction

Export selected item Refresh

Activity type	Timestamp (UTC)	AI app category	App	App accessed in	Agent name	User participant
<input type="checkbox"/> DLP rule match	Mar 4, 2026 12:40 PM	Other AI apps	Grok	Grok		Tim@M365x2737477.onmi...
<input type="checkbox"/> AI website visit	Mar 4, 2026 12:39 PM	Other AI apps	ChatGPT	ChatGPT		Tim@M365x2737477.onmi...
<input checked="" type="checkbox"/> AI website visit	Mar 4, 2026 12:39 PM	Other AI apps	Grok	Grok		Tim@M365x2737477.onmi...
<input type="checkbox"/> DLP rule match	Mar 3, 2026 9:36 AM	Other AI apps	Grok	Grok		Tim@M365x2737477.onmi...
<input type="checkbox"/> AI website visit	Mar 3, 2026 9:35 AM	Other AI apps	Grok	Grok		Tim@M365x2737477.onmi...
<input type="checkbox"/> DLP rule match	Mar 3, 2026 9:35 AM	Other AI apps	Grok	Grok		Tim@M365x2737477.onmi...

AI website visit

Some data may not be available. Prompts, responses, and any files referenced are not available for other AI apps.

Activity details

Activity type: AI website visit
Timestamp: Mar 4, 2026 12:39 PM

Activity: Browse to Url
Record ID: 3f0226dd-d669-404e-99bf-aaf9fac399b8

Client IP: 2.209.230.110

User participant details

User: Tim

[View more user details in insider risk management](#)

App details

AI app category: Other AI apps
App accessed in: Grok