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

Data theft | Risky AI Usage | Data Leaks

MICROSOFT 365 E5

Advanced Data Classification / Advanced Information Protection
Advanced Classifier, Rule based classification

- Exact Data Match
- Trainable Classifiers
- On-demand
- Activity Explorer
- Auto Applied Labels
- Adv. Message Encryption
- Double Key Encryption

Advanced Data Loss Prevention
DLP Policies

- Teams
- M365 Copilot
- OnPrem
- Endpoint
- Edge Activity
- Instances

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.

Policies

- AI interactions
- AI website visit
- DLP rule match
- Sensitive info types

MICROSOFT 365 E3

Data Classification
Define and explore relevant content in your Org.

Sensitive Info Types
- Built-in
- Custom SITs

Information Protection
Know, classify, & protect sensitve information

Sensitivity Labels Manually

- Mail
- Files
- Groups/ Sites

Basic Message Encryption

Data Loss Prevention
Prevent sensitive information from leaving your organization

DLP Policies

- EXO
- ODB
- SPO

Audit Standard
Power your forensic and compliance investigations (180 days)

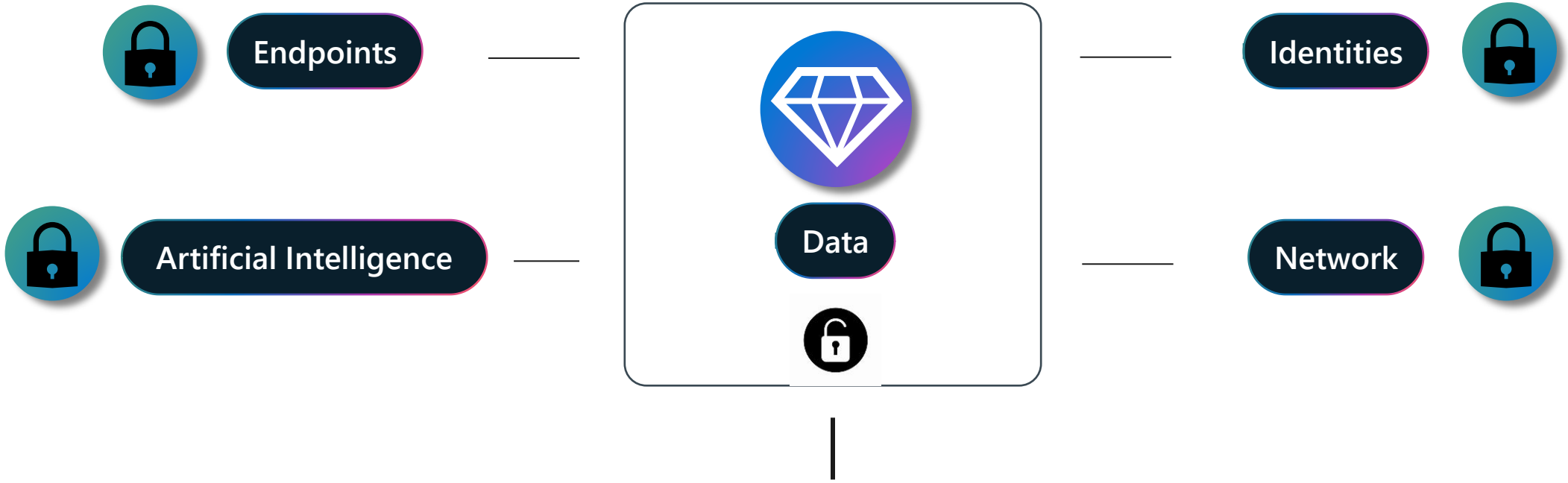
eDiscovery Standard
Discover, preserve, collect, process, cull, and analyze your data in place

- Included in ME3
- Included in ME5 Compliance
- Pay as you go billing

skaylink

Zero Trust Framework

Thinking from a data perspective



Have you secured your most valuable treasure: your data?

skaylink

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

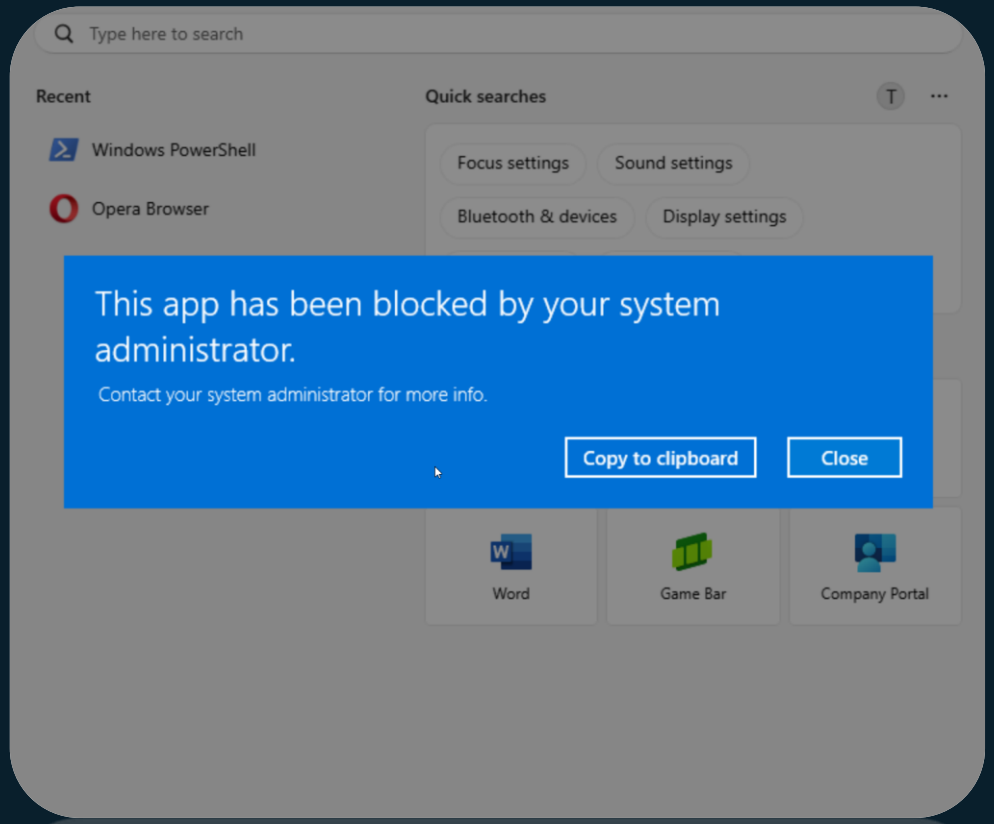
Protection

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

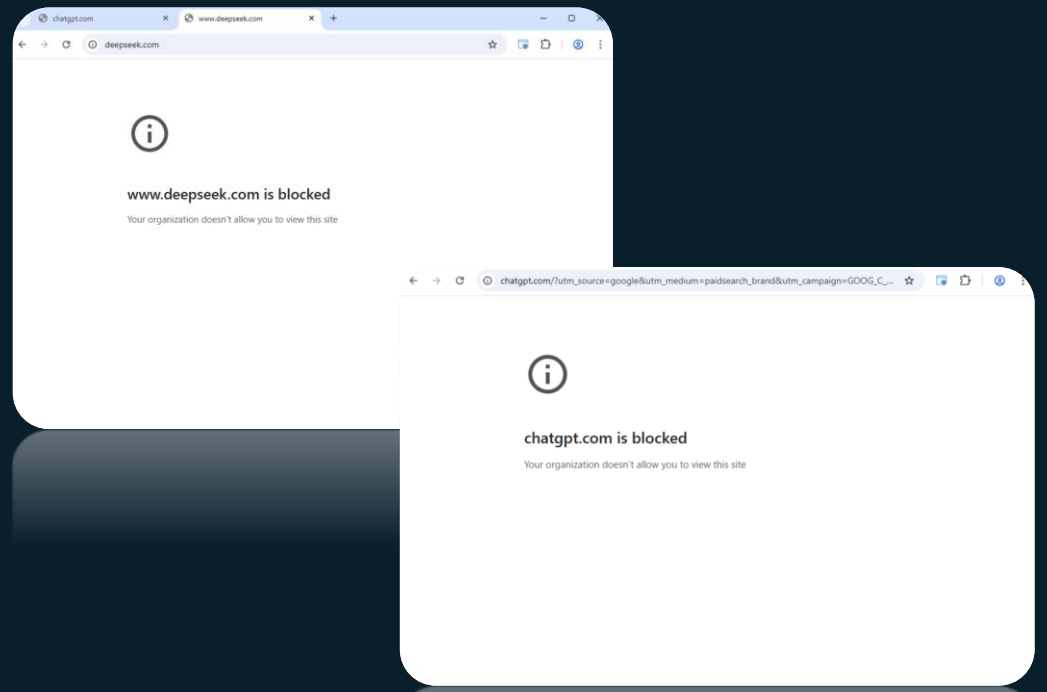
skaylink

Endpoint AI Protection

Trying to use unallowed Browser



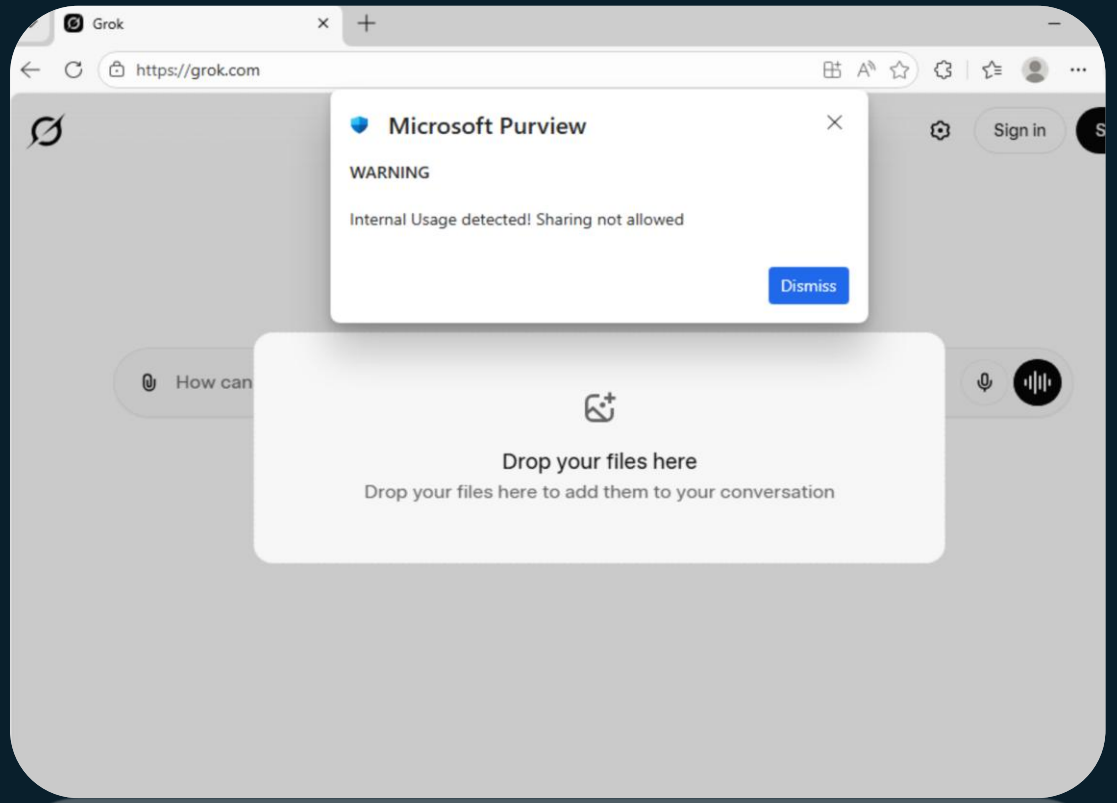
Trying to use unmanaged AI



skaylink

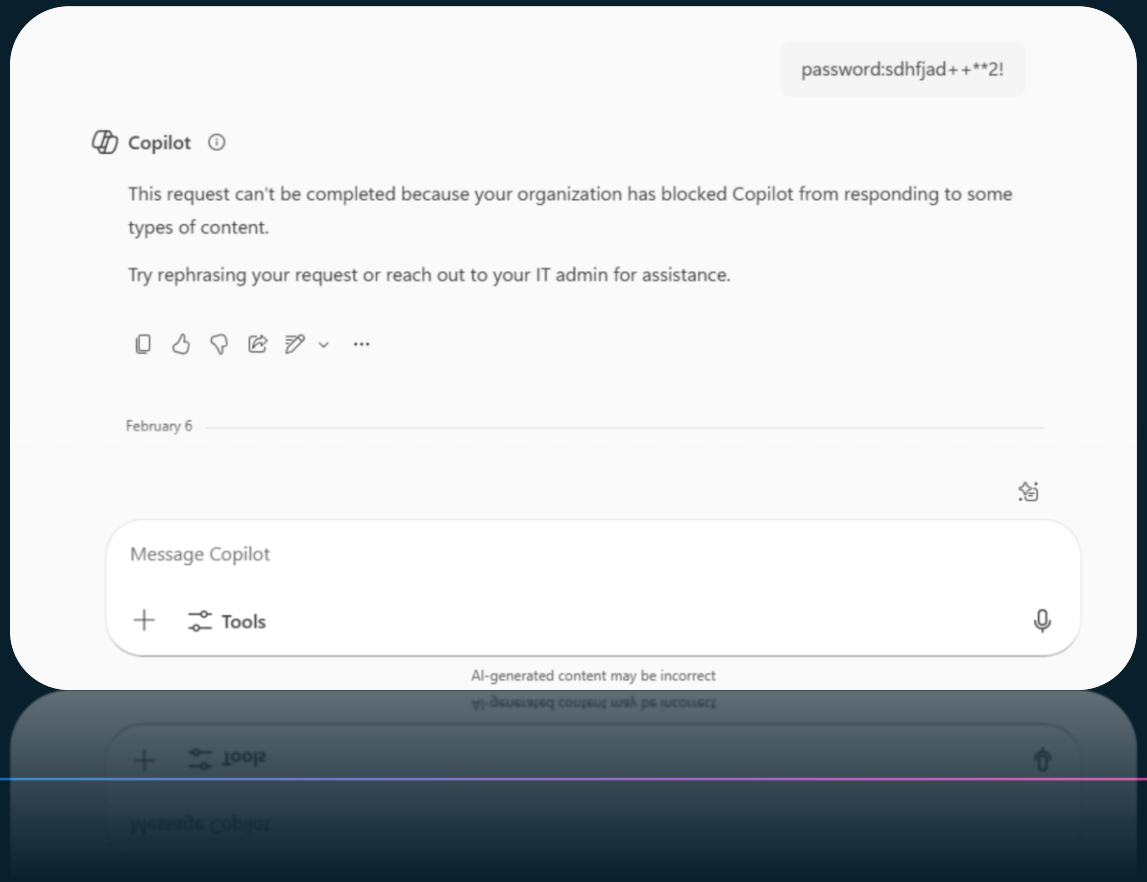
Endpoint DLP

Trying to upload sensitive data to unmanaged AI



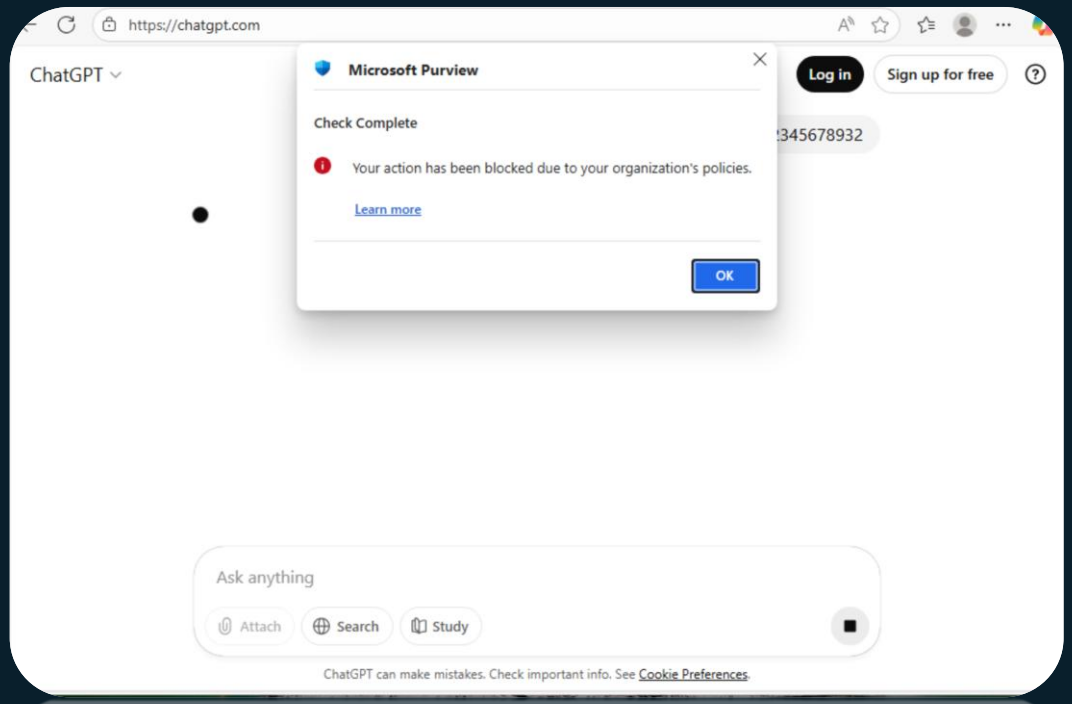
DLP for Microsoft 365 Copilot

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

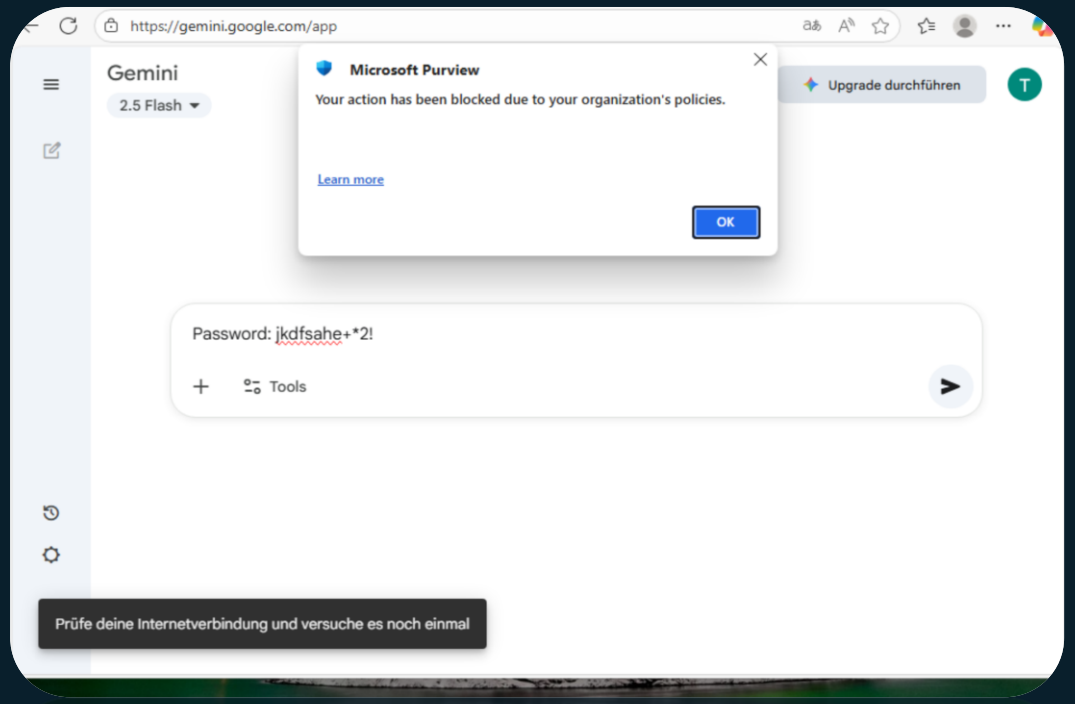


Classifier in AI

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

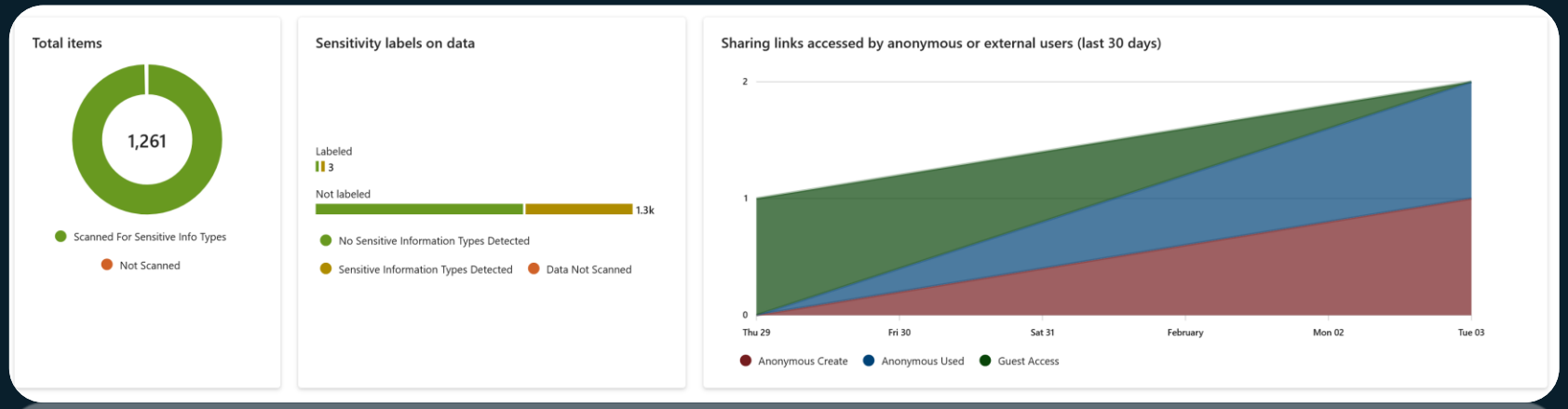
Identify:
Review assessment results and detect sensitive data access.

Protect:
Limit Copilot & agent access; apply labels and retention

Monitor:
Continuously review SharePoint sites, permissions, and access.

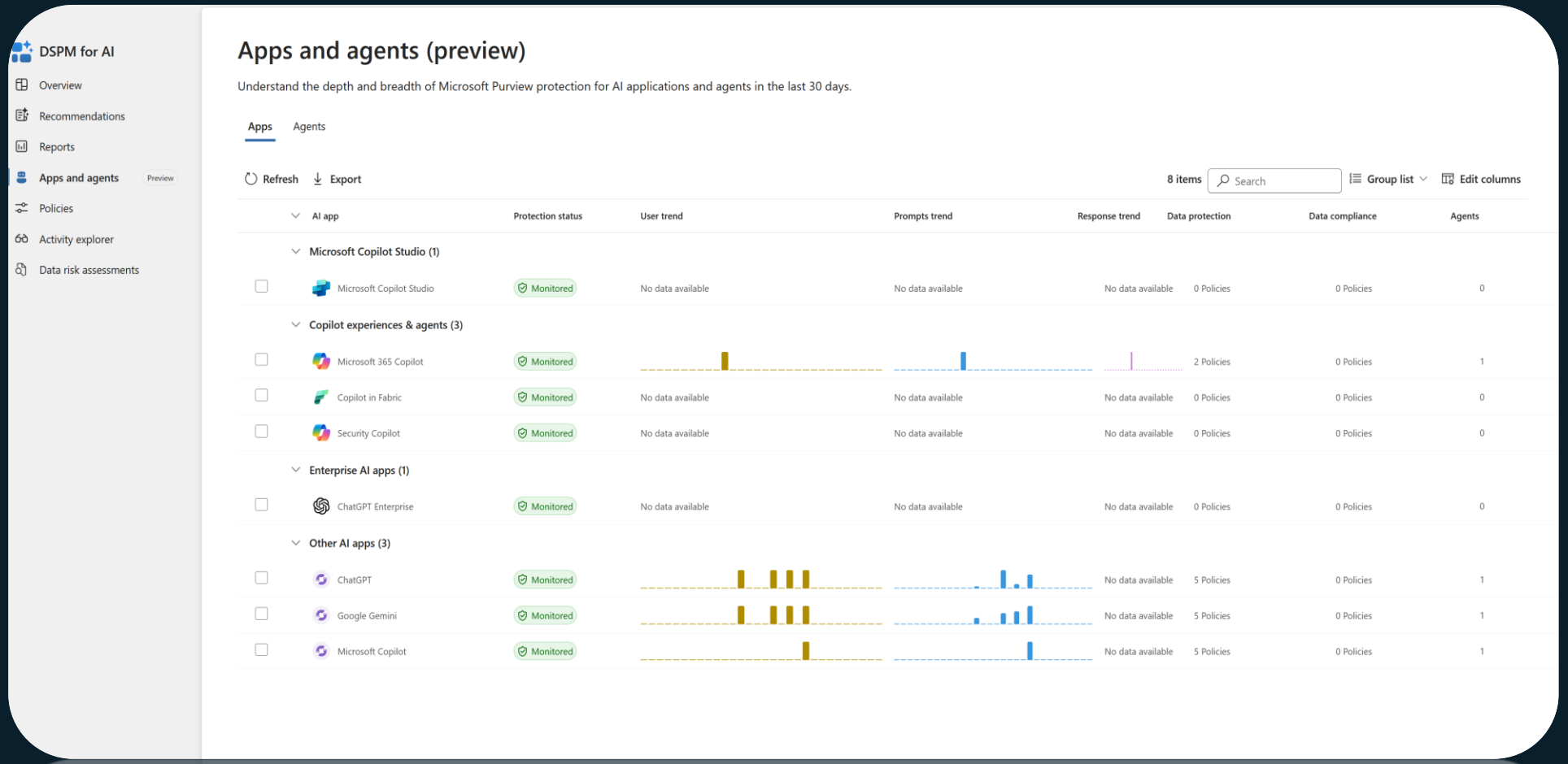
Data Loss Prevention:
Restrict Microsoft 365 Copilot / unmanaged AI from processing content

Copilot



skaylink

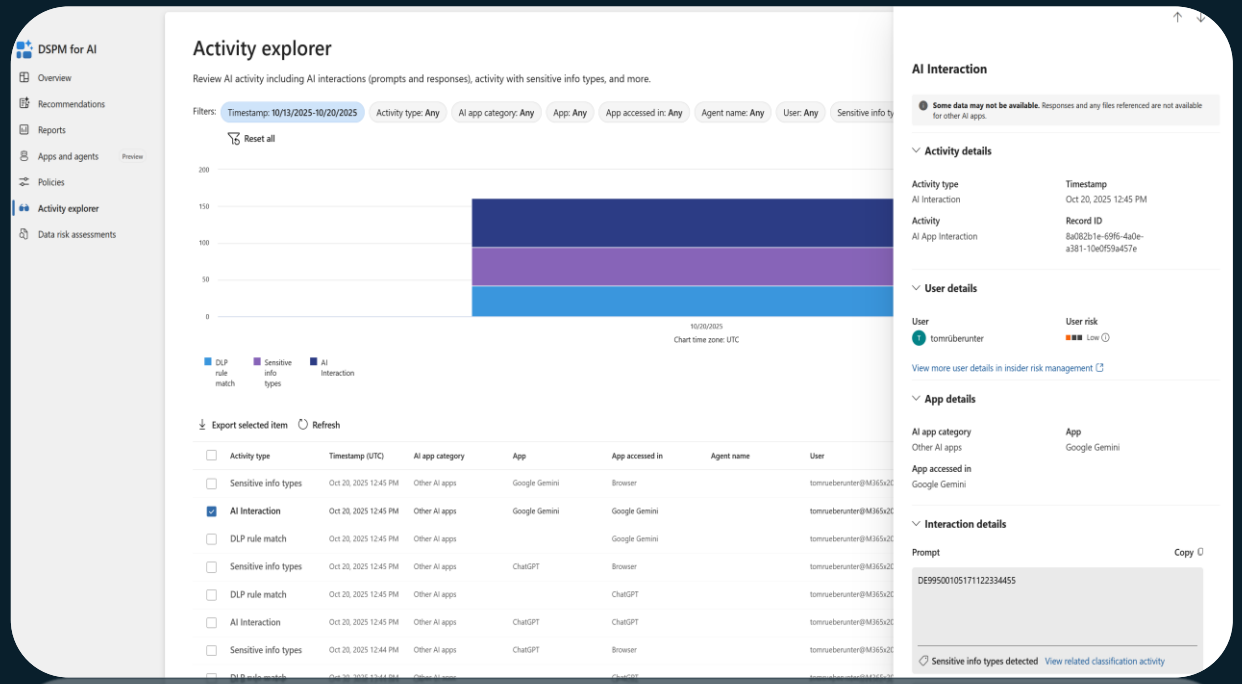
DSPM for AI

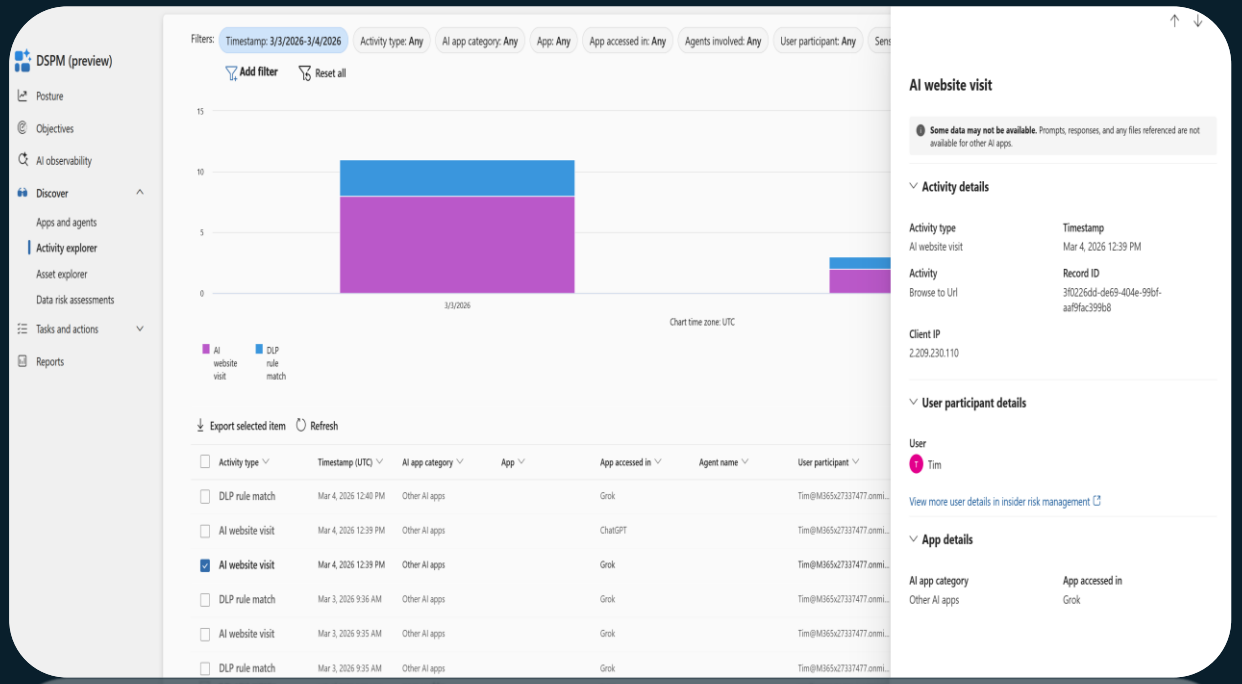


Based on:

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

Sample DSPM policy for AI





skaylink