

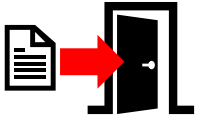
# Microsoft 365 Data Security Masterclass

→ **Mark Warnes**

Architect | Kocho

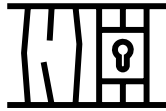


# Neglecting security leads to several risks



## Data Breaches

Unauthorised access can result in exposure, theft, or compromise of sensitive information. This can lead to financial loss and reputational damage.



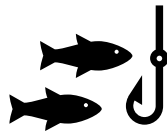
## Misconfiguration

Most security breaches are due to misconfiguration. Incorrect settings can expose data to unauthorised users, making it vulnerable to attacks.



## Compliance Violations

Failure to implement proper security measures can lead to non-compliance with regulatory requirements, resulting in legal penalties and fines.



## Phishing and Malware Attacks

Without robust security, M365 environments are more susceptible to phishing and malware attacks, which can compromise user accounts and data.



## Insider Threats

Inadequate security can make it easier for malicious insiders to access and misuse sensitive information, or for unintentional data sharing to take place.

# Microsoft Purview

Comprehensive solutions to secure and govern your data

## Data governance

Govern data seamlessly to empower your organization

Data Map  
Data Catalog  
Data Estate Insights

## Data Security

Secure data across its lifecycle, wherever it lives

Data Loss Prevention  
Insider Risk Management  
Information Protection  
Adaptive Protection  
DSPM for AI

## Risk & compliance posture

Manage critical risks and regulatory requirements

Compliance Manager  
eDiscovery and Audit  
Communication Compliance  
Data Lifecycle Management  
Records Management

### Shared Platform Capabilities

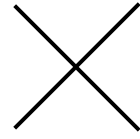
Data Map, Data Classification, Data Labels, Audit, Data Connectors

On-prem and multi-cloud

Unstructured & structured data

Across IaaS and SaaS

Identity  
Security



Data  
Security



Your **data** security is only as strong  
as your **identity** security



BECOME GREATER  
KOCHO.CO.UK





# Securing data

Purview features that help protect sensitive data inside and outside your organisation, and identifies risky data handling behaviour

# Journey to Data Security Success

## Restrict access within SharePoint

Limit who can see the data inside sensitive sites by reviewing permissions and restricting discoverability.

## Apply labels to unstructured content

Raise awareness of document sensitivity and enable further controls and visibility within other M365 tools by adopting a data labelling policy.

## Control inappropriate sharing

Prevent sensitive data loss through unintentional and malicious exfiltration using flexible policies based on content and/or labels.

## Monitor for insider risks

Identify and investigate suspicious activities by users within the environment and invoke dynamic restrictions on risky users.

# Step 1: Restrict access within SharePoint

Govern and control site access using

## SharePoint Advanced Management

Run **Data Access Governance** reports to identify sites with overshared or sensitive content

Run **Site Access Reviews** to require site owner to determine if a site is overshared and requires remediation

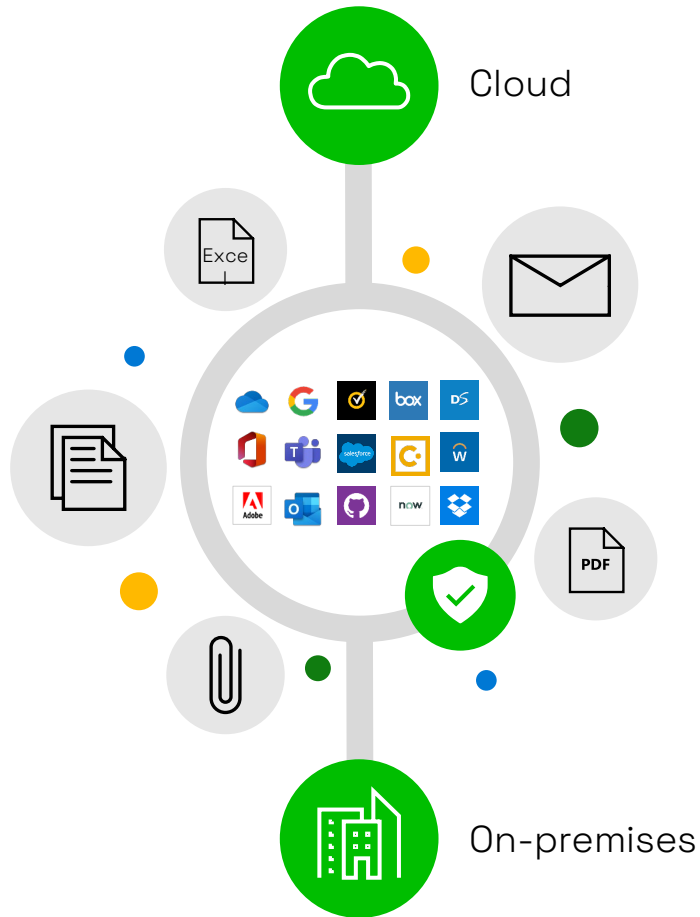
Use **Restricted Access Control** policies to restrict access to SharePoint sites and content to users in a specific group

Use **Restricted Content Discoverability** policies to stop site content being discoverable in organisation-wide search results

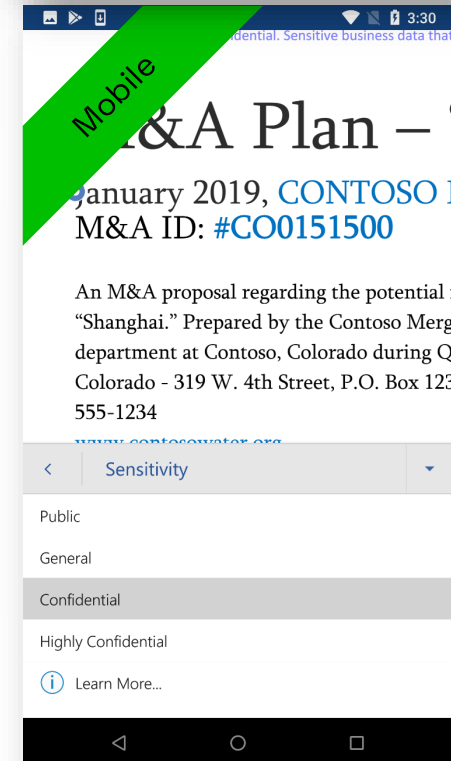
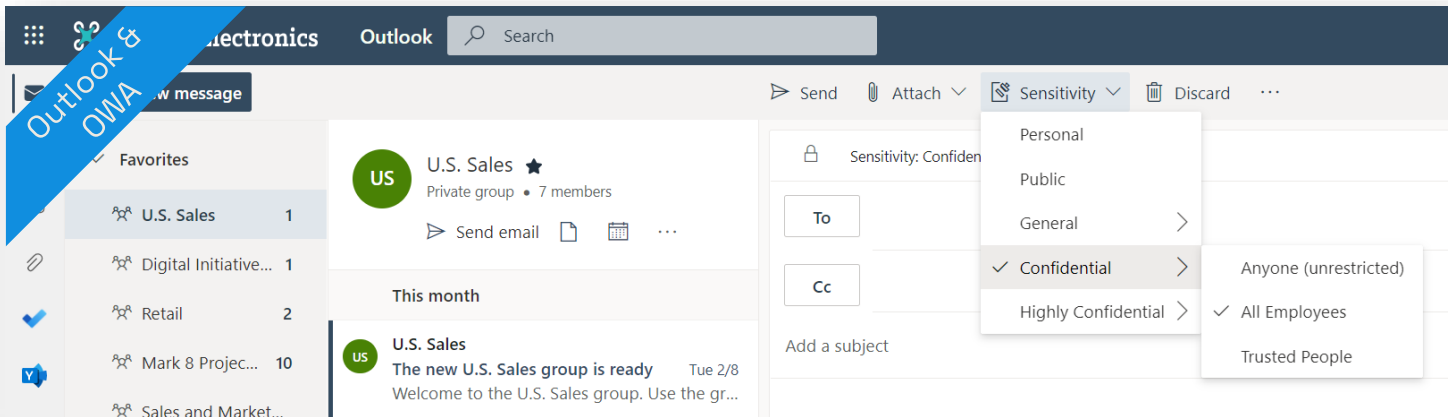
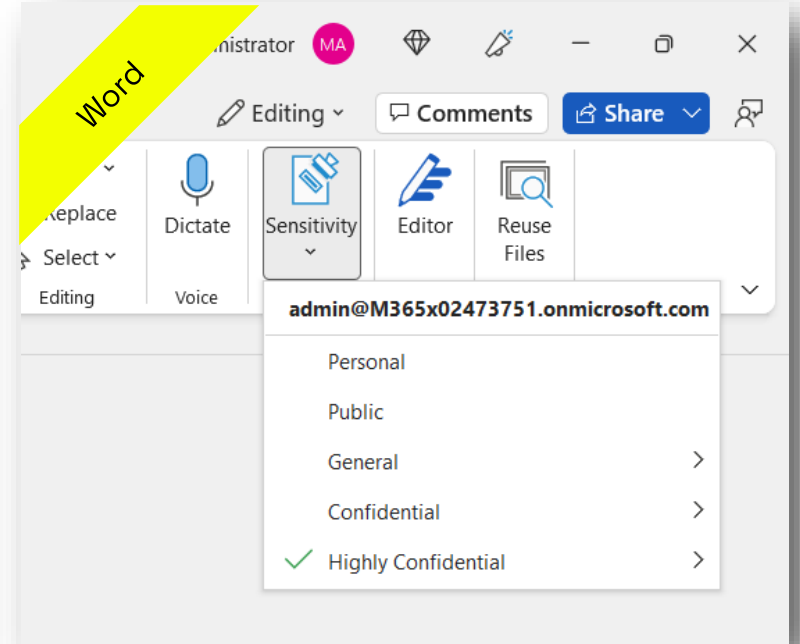
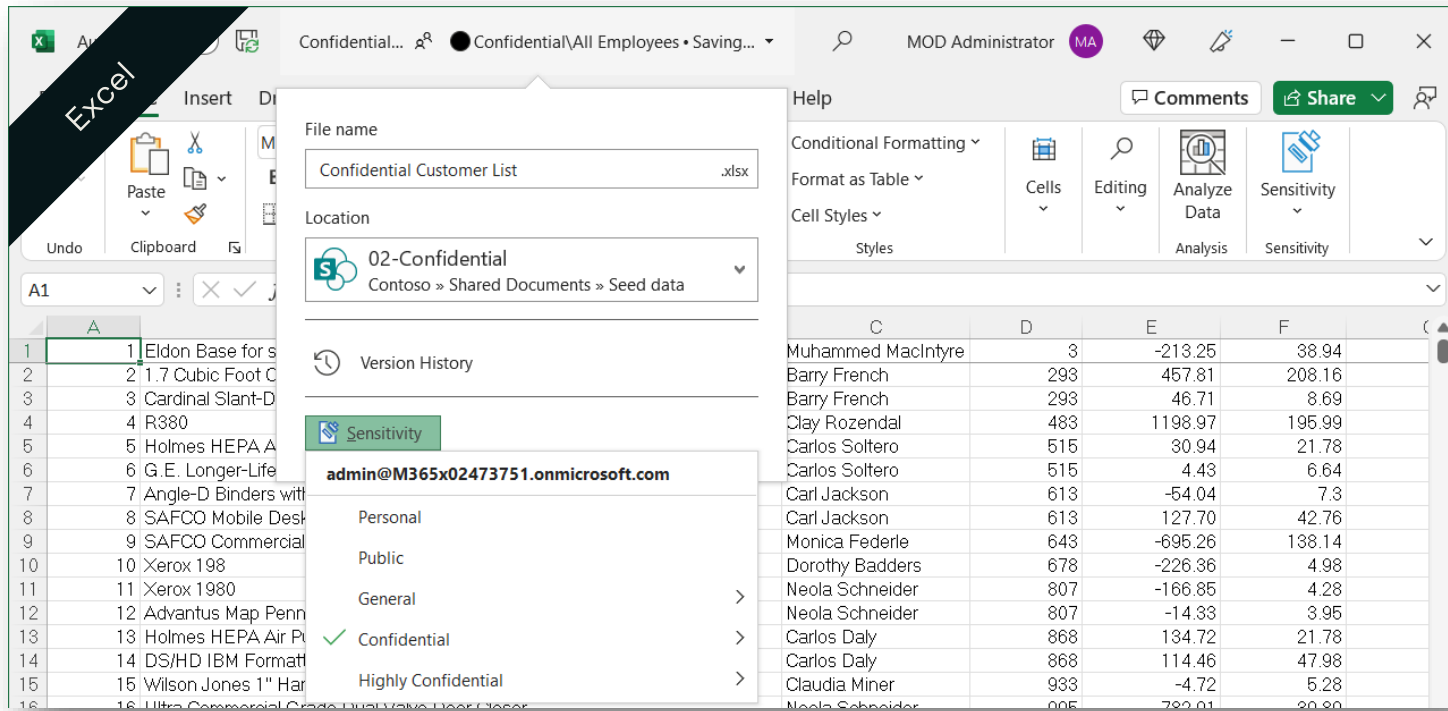
## Step 2: Apply labels to unstructured content

Use [Microsoft Purview Information Protection](#) to understand and protect sensitive data

- Built-in labeling and protection applied simply and quickly within the Office suite across platforms
- Discover and classify data at scale using automation and machine-learning, in M365 and on-premise
- Encrypted files remain protected wherever they reside or travel, accessible only by authorised users







# Protection via sensitivity labels

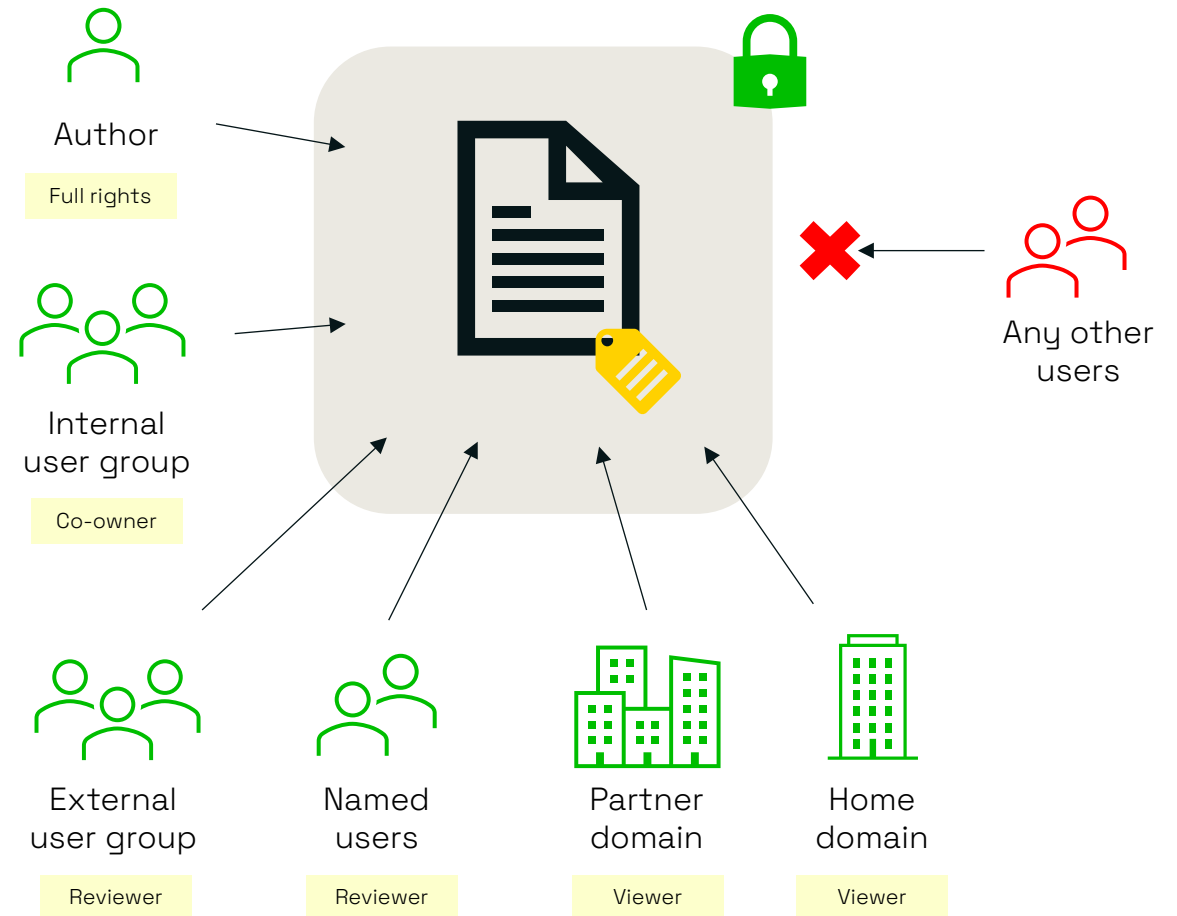
## → Access control

File is encrypted: *only authorised users have access*

## → Usage rights

File use is restricted on actions such as print, copy, save, and change label

## → File protection is portable– **file is protected wherever it resides**



# Microsoft Purview Information Protection licence requirements

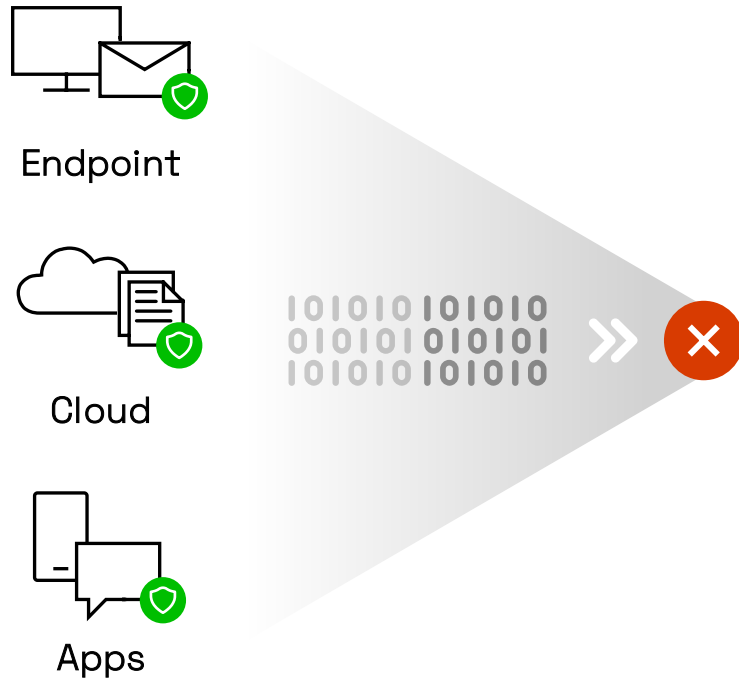
## M365 E3 features

- Manual labelling
- Protection applied via label
- Default labelling and data discovery for on-premise file repositories using MIP scanner
- Basic Office Message Encryption for protecting emails

## Uplift features

- Automated labelling based on classifier conditions, online and on-premises
- Automatic labelling based on content for on-premise file repositories using MIP scanner
- Default library labelling in SharePoint
- Advanced Office Message Encryption for protecting emails (branded templates, portal access enforcement)

## Step 3: Control inappropriate sharing



Use [Microsoft Purview Data Loss Prevention](#) to prevent accidental or unauthorized sharing of your sensitive data

- Automatically enforce compliance with regulations and internal policies across cloud and on-premises
- Take different actions based on the sensitive content detected within your email or file and/or other available properties or attributes
- Extend DLP policy to both Microsoft and non-Microsoft endpoints, on premises file shares, user apps, browsers, and services

# Microsoft Purview Data Loss Prevention



Microsoft 365

Cloud DLP – Service based



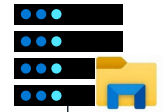
Endpoint

Endpoint – Platform based



Non-Microsoft apps

3rd party API based



On-premises

On-prem service

Data in use

Data in motion

Data at rest

- Unified & flexible policy management
- Integrated with Microsoft Purview Information Protection
- Unified alerting & remediation
- Agentless and integrated within end user experiences



# Microsoft Purview Data Loss Prevention licence requirements

## M365 E3 features

- Detect content sharing within Exchange, SharePoint and OneDrive

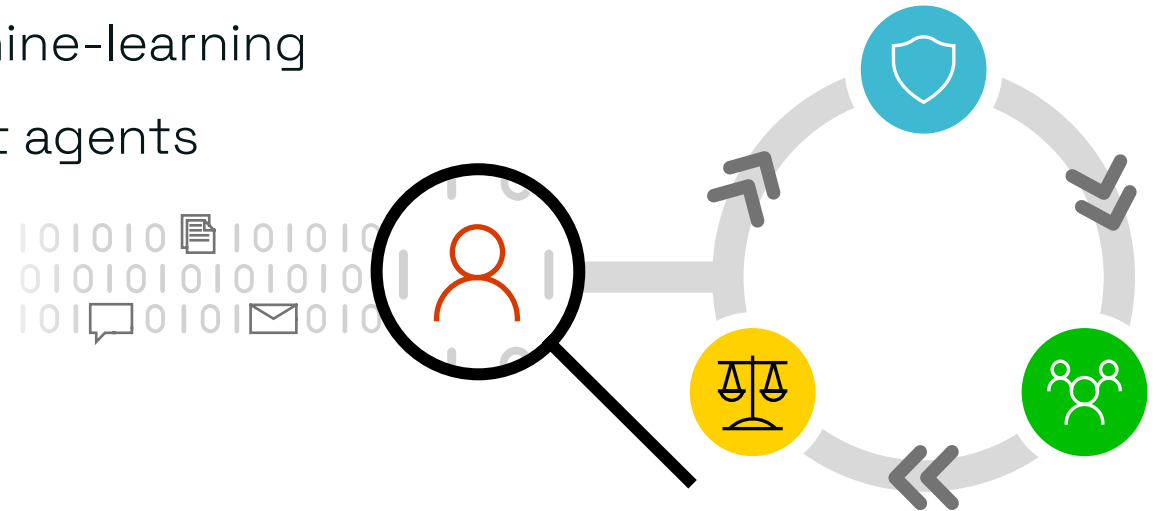
## Uplift features

- Communication DLP for near real-time protection of sensitive content in Teams Chat
- Endpoint DLP for extension of protection to endpoint activities such as printing, copying to USB, and copying to cloud services
- Adaptive Protection integration with Insider Risk Management to enforce DLP controls based on insider risk

## Step 4: Monitor for insider risks

Use [Microsoft Purview Insider Risk Management](#) to identify and act on insider risks

- Identify hidden risks with 100+ built-in machine-learning models and indicators, requiring no endpoint agents
- Maintain user privacy with strong privacy controls and user pseudonymization
- Expedite mitigation with enriched investigations and Adaptive Protection that enforces DLP controls dynamically



Insider risk management - Micro

← → ↺

https://sip.protection.office.com/insiderriskmgmt?viewid=alerts&flight=enablem365compliancecenter,enableinsiderriskmgmt,enableinsiderriskservice&flight=EnableM365ComplianceCenter

☆ ⚙️ 👤 😊 ⋮

Contoso Electronics

Microsoft 365 compliance

🔔 ⚙️ ? MA

☰

Home

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Solutions

Catalog

More resources

Insider risk management

Overview Alerts Cases Policies Users Notices

Alerts needing review

3 alerts need review

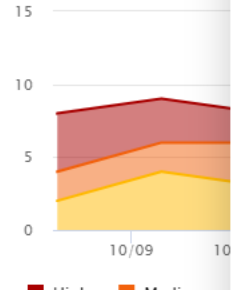
3 alerts need review with no open cases

High

Medium

Low

Open alerts over time



High

Medium

Export

Policy match alert

Status

Severity

▼ Anony85KF-34DF (1)

✓ Alert: Confidentiality obligation during departure

Needs review

High

▼ AnonyO4J5-34PP (1)

Alert: Project Jupiter Confidentiality

Needs review

Medium

2 years ago

No case found

▼ AnonyF3FD-34PK (1)

Alert: Anti-harrasment policy

Needs review

Low

2 years ago

No case found

▼ AnonyIS8-978 (1)

Alert: Confidentiality obligation during departure

Confirmed

High

a month ago

Case 884: (RO) Potential IP theft

Alert: Confidentiality obligation during departure

Overview User activity User profile

History of recent user activity

09/16/2019

HR Event: Resignation Date Set

Resignation date set for: 09/27/2019

09/15/2019

File(s) printed

Risk Score: 65

10 file(s) were printed

4 file(s) have labels including: Top Secret

09/15/2019

File(s) copied to USB device

Risk Score: 92

113 file(s) were copied to USB device(s)

54 file(s) have labels including: Top Secret

09/15/2019

File(s) downloaded from SharePoint Online

Risk Score: 34

113 file(s) were downloaded from 1 SharePoint Online site(s)

54 file(s) have labels including: Top Secret

Confirm and create new case

Dismiss as benign

Type here to search

🔍

📁

📊

📅

📧

📌

🔗

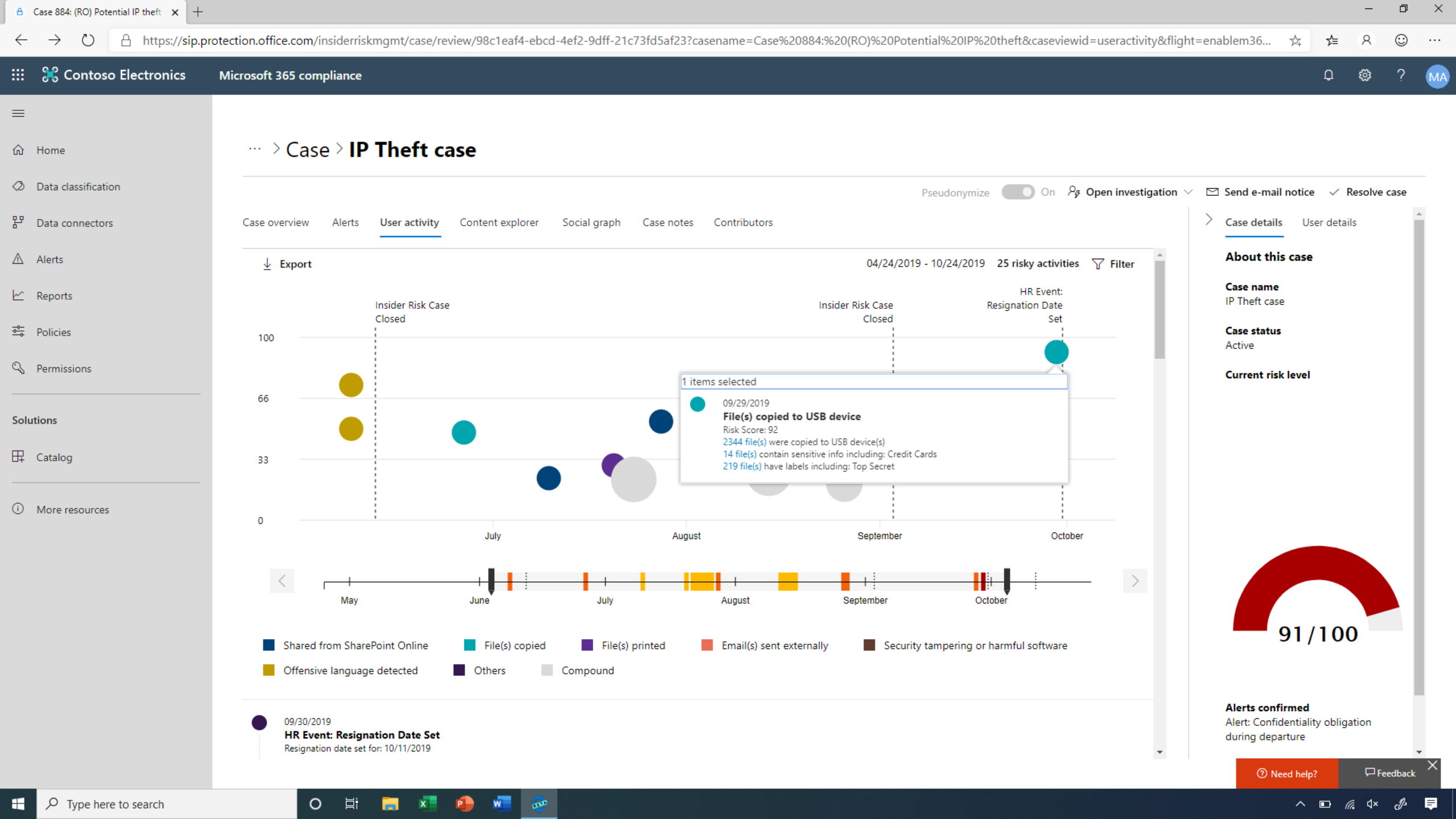
↑

🔊

🔌

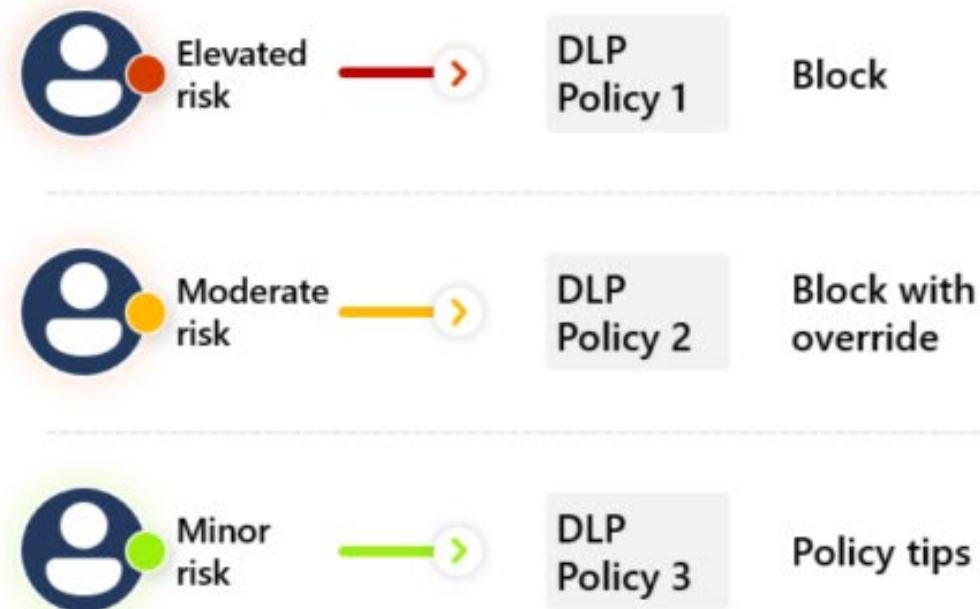
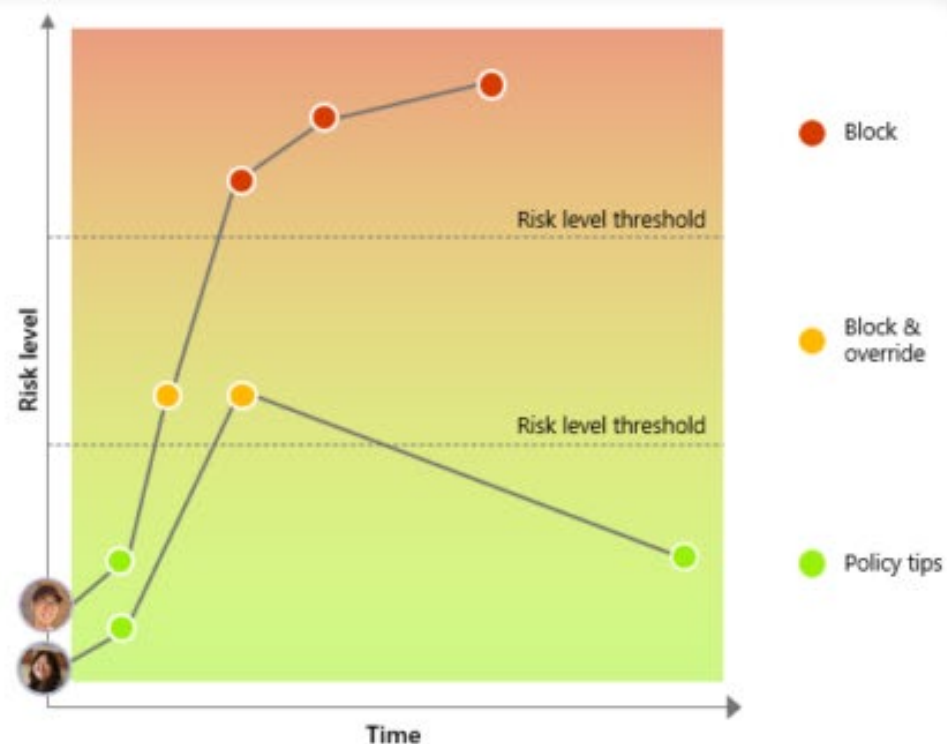
🖨️

🗨️



# Adaptive protection

Dynamic restrictions on users with elevated insider risk levels through integration of Insider Risk Management with Data Loss Prevention





# Microsoft Purview Insider Risk Management licence requirements

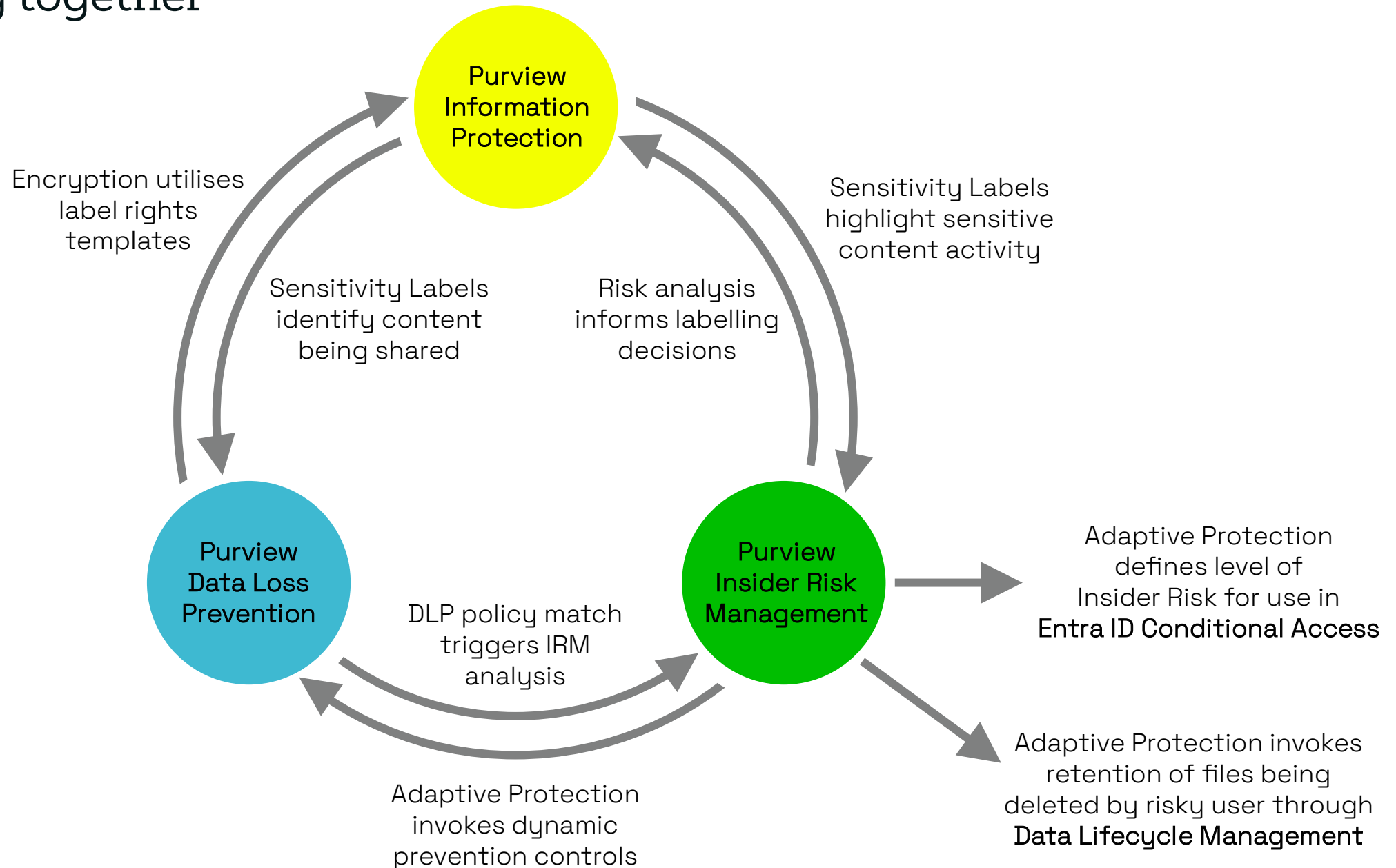
## M365 E3 features

*Not available at E3*

## Uplift features

- Full access to Insider Risk Management features to detect and investigate risky user behaviours
- Adaptive Protection integrations to enforce DLP controls based on insider risk, Conditional Access restrictions, and Data Lifecycle (retention) requirements based on calculated insider risk

# Working together



# Journey to Data Security Success

## Restrict access within SharePoint

- Setup data assessments to identify overly permissive sites and initiate site reviews
- Limit the discoverability of sensitive sites

## Apply labels to unstructured content

- Define and adopt label schema for your organisation
- Use encryption options for the most sensitive content
- Apply widely and swiftly with automation

## Control inappropriate sharing

- Define scenarios and identify sensitive data risks
- Use monitoring or simulation mode to assess impact
- Refine to reduce false positives
- Activate and adopt controls

## Monitor for insider risks

- Define scenarios and implement policies
- Regularly triage alerts and investigate
- Activate adaptive protection to enable dynamic restrictions



# Securing AI

Purview and M365 features to protect your sensitive data from exposure or leakage by AI services

# Top security and governance concerns about generative AI

Data oversharing  
and data leaks

80%

of leaders cited leakage of  
sensitive data as their main  
concern<sup>1</sup>

Identification of  
risky AI use

41%

of security leaders cited that  
the identification of risky users  
based on queries into AI was  
one of the top AI controls they  
want to implement<sup>2</sup>

AI governance and  
risk visibility

84%

of organisations want to  
feel more confident about  
managing and discovering  
data input into AI apps  
and tools<sup>2</sup>

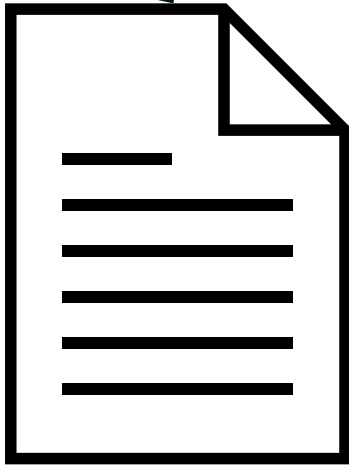
1. First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

2. Microsoft data security index 2024 report (<https://clouddamcdnprodep.azureedge.net/gdc/gdcqTplAT/original?culture=en-us&country=us>)

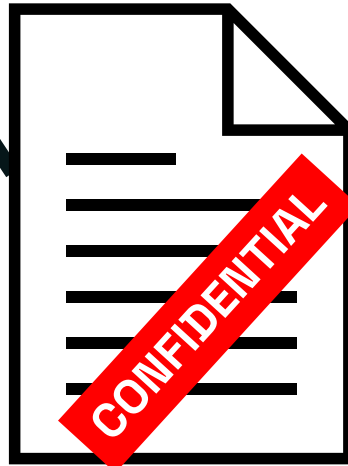




Microsoft 365 Copilot only surfaces organizational data to which individual users have **at least view permissions**



“Ordinary” documents

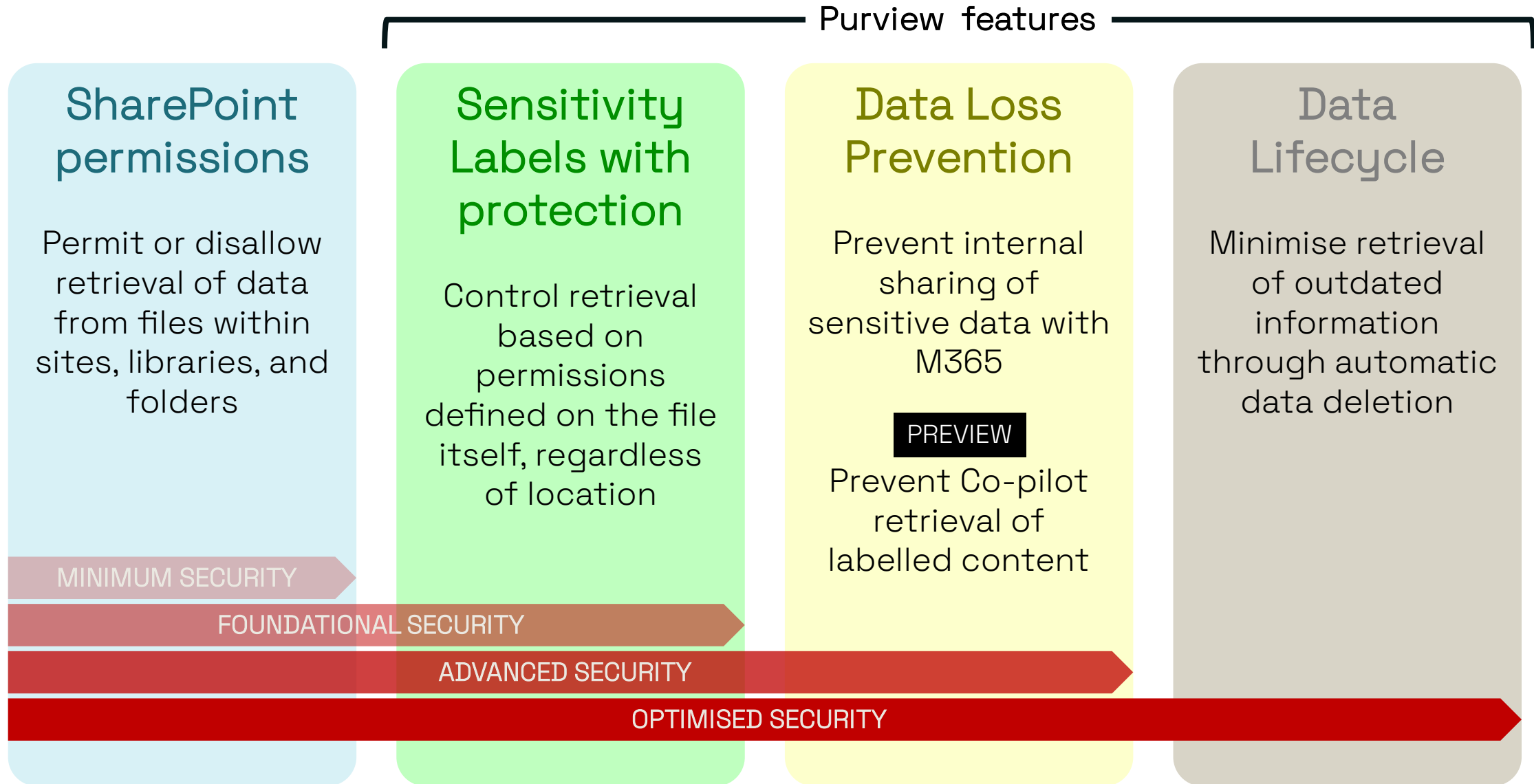


Sensitive documents



Out-of-date documents

# Co-pilot data security with Purview

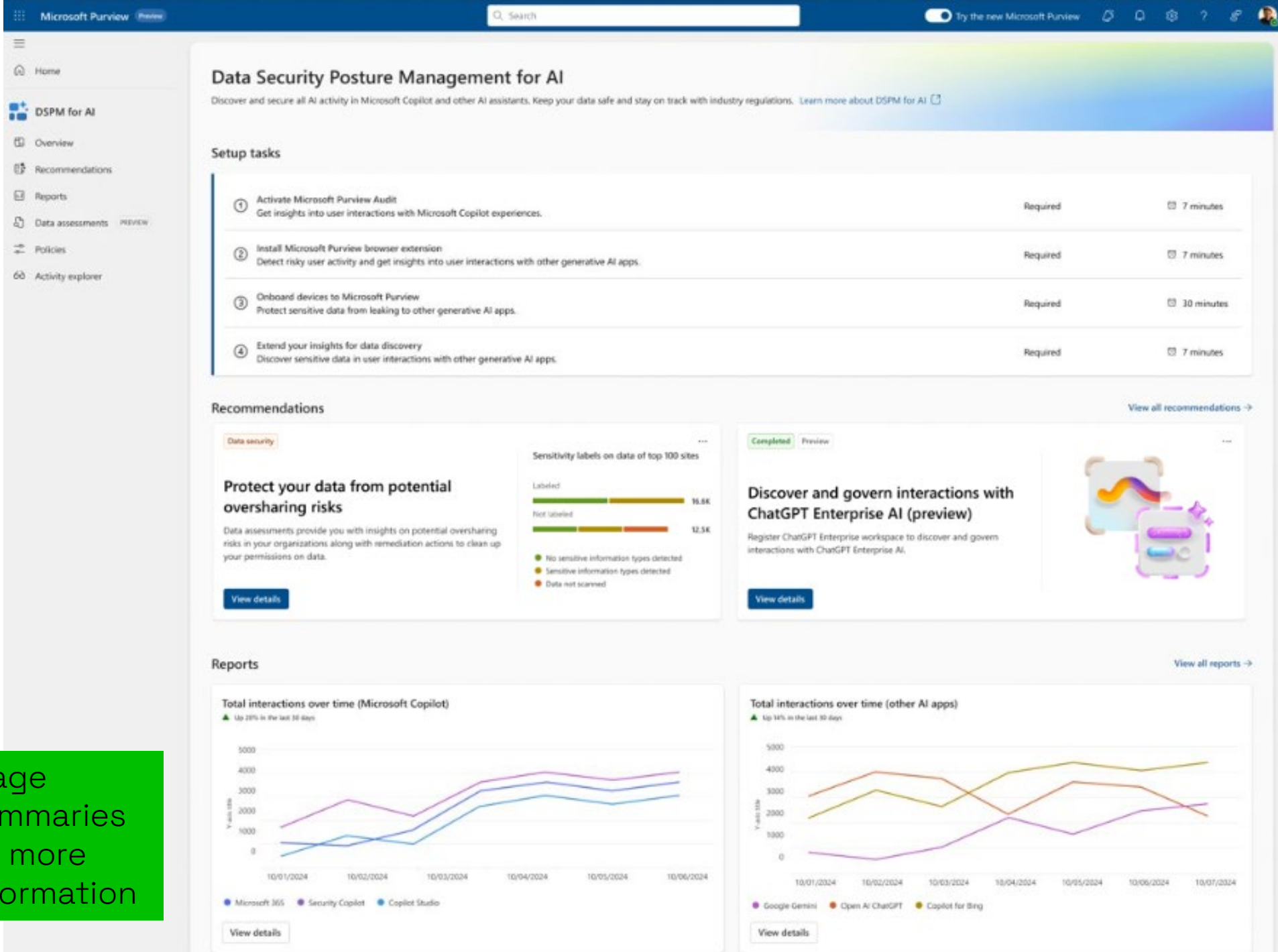


# Monitor and govern AI usage



Use [Data Security Posture Management for AI](#) to track and secure AI interactions in Copilot and beyond

- Identify and secure sensitive AI-related data, ensuring it is protected from unauthorised access and potential breaches
- Assess vulnerabilities and potential security risks within AI workloads to proactively address and mitigate these risks
- Provide visibility into AI interactions and data flows, enabling better oversight and management of AI-driven processes



Overview page showing summaries and links to more detailed information

Home

Solutions

Learn

Settings

Communi... Compliance

Audit

Data Loss Prevention

DSPM for AI

eDiscovery

DSPM for AI

Overview

Recommendations

Reports

Policies

Activity explorer

Data assessments

Preview

# Data Security Posture Management for AI

Discover and secure all AI activity in Microsoft Copilot and other AI apps. Keep your data safe and stay on track with industry regulations. [Learn more about DSPM for AI](#)

## Get started

<input checked="" type="checkbox"/>	<b>Activate Microsoft Purview Audit</b> Get insights into user interactions with Microsoft Copilot experiences.	Required
<input checked="" type="checkbox"/>	<b>Install Microsoft Purview browser extension</b> Detect risky user activity and get insights into user interactions with other AI apps.	Required
<input checked="" type="checkbox"/>	<b>Onboard devices to Microsoft Purview</b> Protect sensitive data from leaking to other AI apps.	Required
<input type="checkbox"/>	<b>Extend your insights for data discovery</b> Discover sensitive data in user interactions with other AI apps.	Required

## Recommendations

Data security

### Fortify your data security

- Keep your sensitive data protected with Adaptive Protection.
- Prevent data leakages in other AI apps.

View details

Data Security Investigations

### Protect sensitive data referenced in Copilot responses

In the last 30 days, 31 unprotected files were referenced in Copilot responses. Start a data investigation or take steps to prevent potential oversharing of sensitive data.

View details

## Reports

## Activate Microsoft Purview Audit

☒ Activated REQUIRED ⌚ 7 minutes to complete

Microsoft Purview Audit is an integrated solution that help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations.

Search the audit log in the Microsoft Purview compliance center to monitor user activity in your organization. You can also trace user activity across emails, documents, sensitivity labels and much more.

Activating Microsoft Purview Audit is essential to get visibility into user interactions with Microsoft Copilot.

[Learn more about Microsoft Purview Audit](#)

### What happens next?

- ⌚ It can take up to 24 hours for activity to be detected.
- 📊 Your analytics report will start getting populated with data observed in your organization's Copilot environment.



Microsoft Purview

Search

Copilot

u412

Home

Solutions

Learn

Settings

Communi... Compliance

Audit

Data Loss Prevention

DSPM for AI

eDiscovery

DSPM for AI

Overview

Recommendations

Reports

Policies

Activity explorer

Data assessments

Preview

# Recommendations

Not Started3

Dismissed0

Completed7

Refresh

Recommendation	Type	Action done by	Action done on
Not Started (3)			
Fortify your data security	Data security		
Protect sensitive data referenced in Copilot responses	Data security		
Discover and govern interactions with ChatGPT Enterprise AI (preview)	Data discovery		
Completed (7)			
Control unethical behavior in AI	Insight into communications		
Guided assistance to AI regulations	AI regulations		
Protect sensitive data referenced in Microsoft 365 Copilot (preview)	Data security	U u411	Jan 25, 2025 1:55 PM
Protect your data from potential oversharing risks	Data security	U u3309	Jan 30, 2025 8:42 PM
Protect your data with sensitivity labels	Data security		
Detect risky interactions in AI apps (preview)	Insider risk management		
Use Copilot to improve your data security posture (preview)	Data security	U u3309	Jan 30, 2025 8:42 PM

Completed

## Detect risky interactions in AI apps (preview)

You now have an active risky AI usage policy in Insider Risk Management. This policy helps calculate user risk by detecting potentially risky prompts and responses in Microsoft Copilot experiences.

Here's what has been set up:

Created

### Detect risky interactions in AI apps

Insider risk management policy: **DSPM for AI - Detect risky AI usage**

Helps calculate user risk by detecting risky prompts and responses in Microsoft Copilot experiences.

View policy

**What to expect**

- Alerts will be generated in Insider Risk Management.

**Useful resources**

[Learn more about Risky AI Usage policy](#)

Investigate alerts

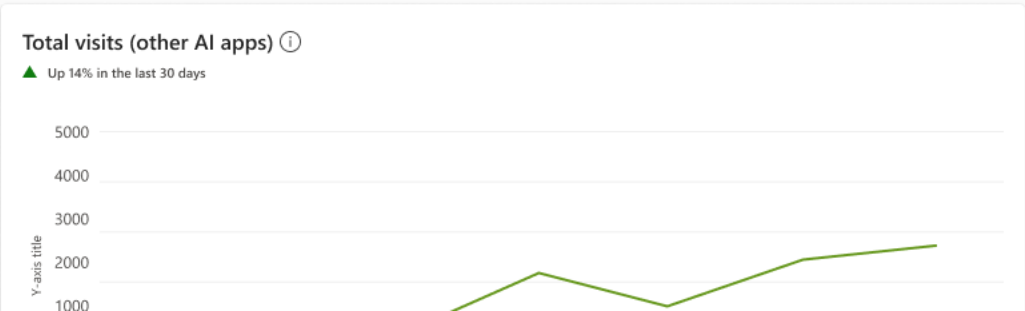
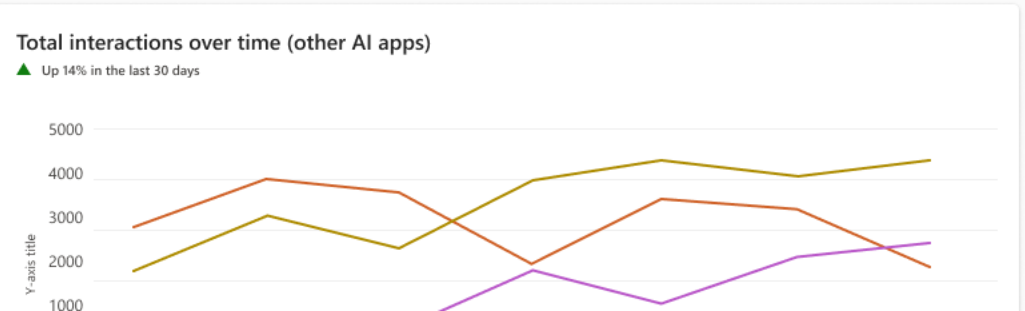
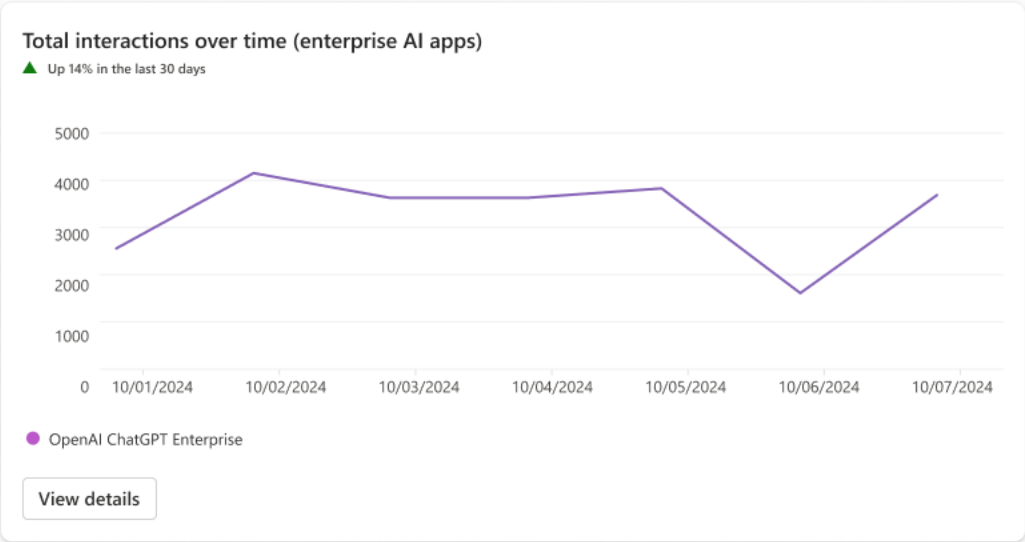
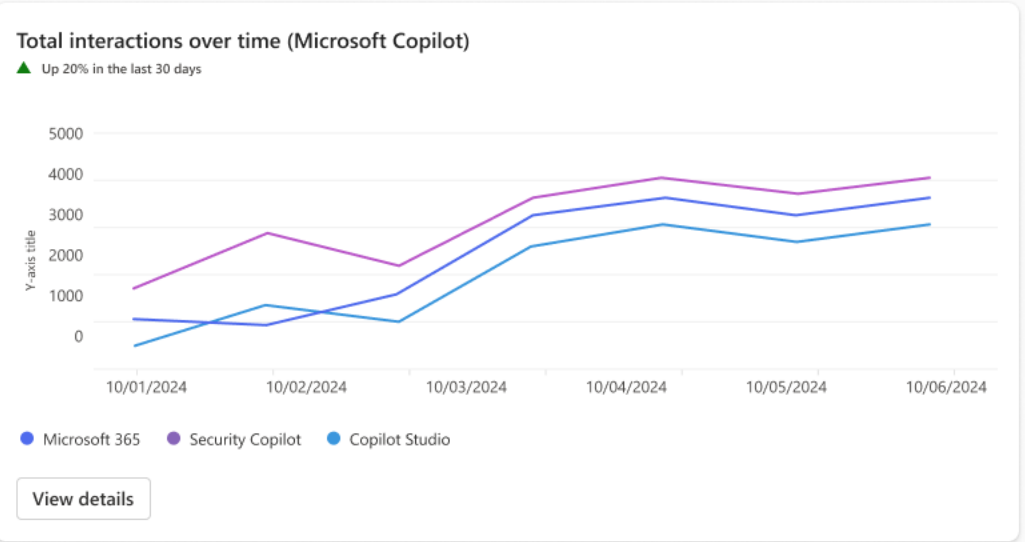


Overview

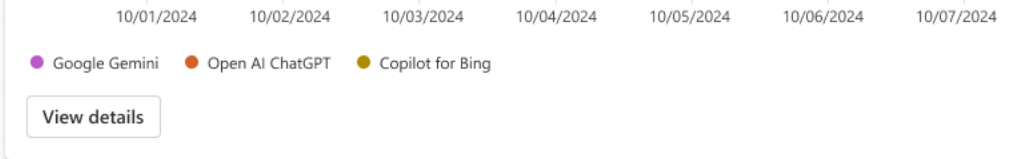
# Reports

- Microsoft Copilot experiences
- Enterprise AI apps
- Other AI apps

## Activity



Reports page showing metrics and trends for past 30 days across monitored AI services



## Data

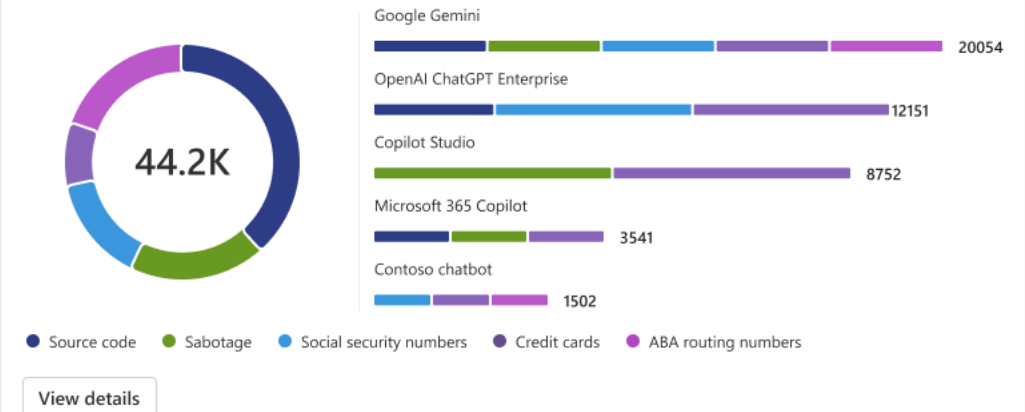
### Top unethical use in AI interactions

Potentially unethical behavior detected in prompts and responses in Microsoft 365 Copilot.



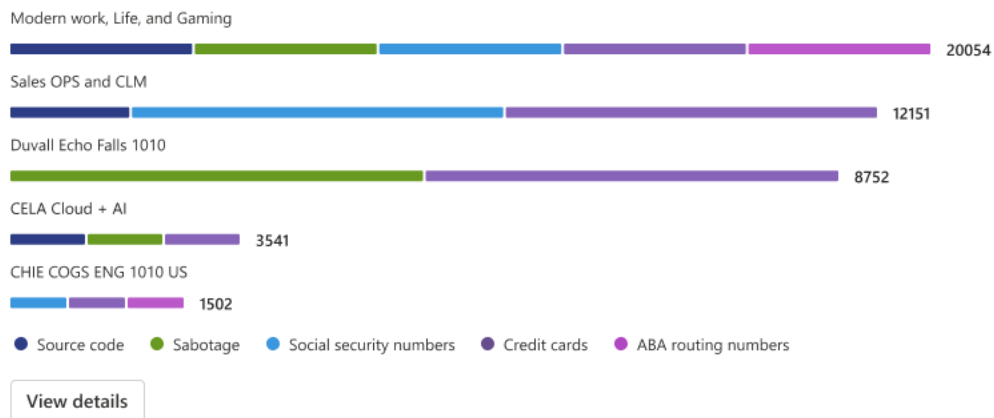
### Sensitive interactions per app

Sensitive information types shared with Copilot and other generative AI apps



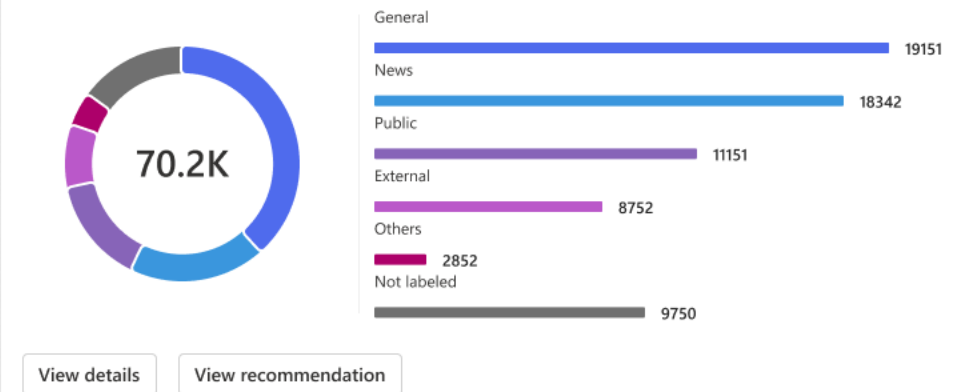
### Sensitive interactions by department

Sensitive information types shared with all AI apps by department



### Top sensitivity labels referenced in Microsoft 365 Copilot

Items with sensitivity labels shared with Copilot



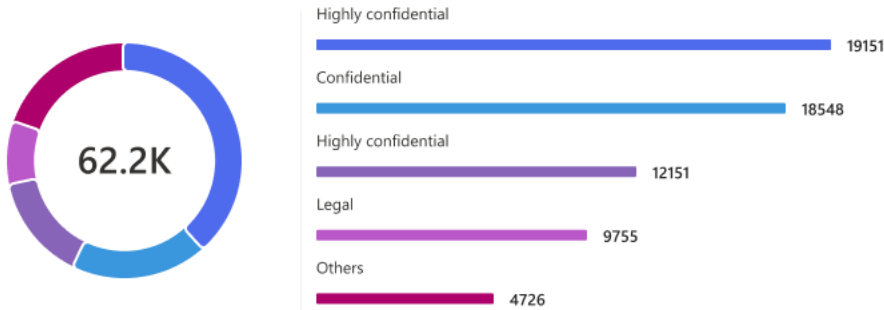
View details

View details

View recommendation

### Top sensitivity labels restricted from Copilot processing

Items with sensitivity labels restricted from Copilot processing



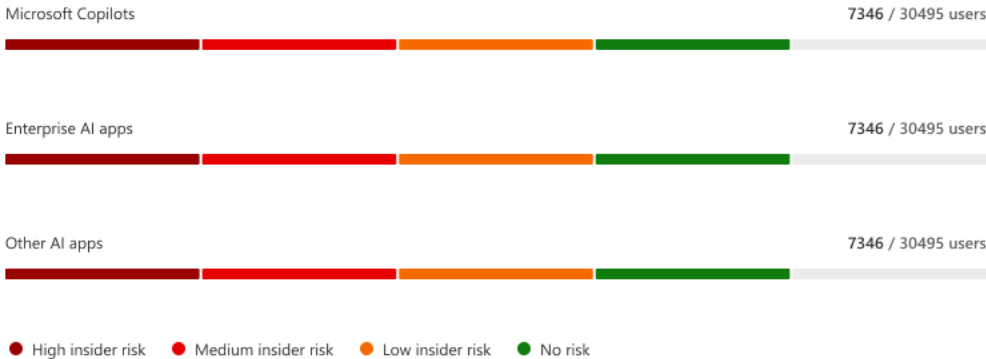
View details

View recommendation

## User

### Insider risk severity

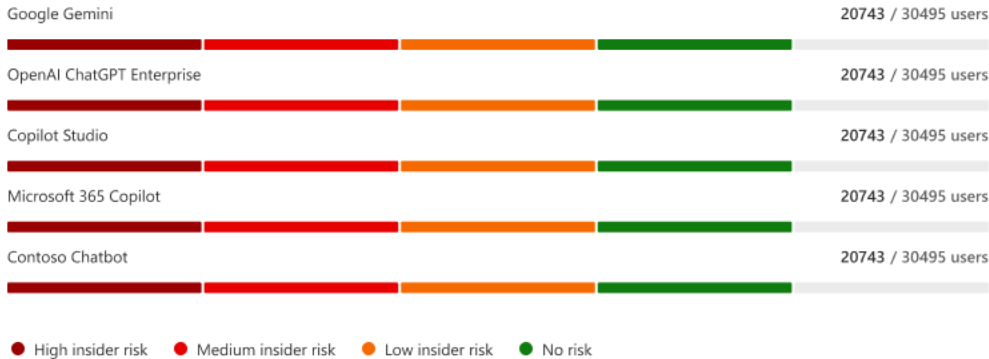
Number of people in your org using AI assistants, grouped by insider risk level



View details

### Insider risk severity per app

People in your org using AI assistants, grouped by insider risk level



View details

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Settings

DSPM for AI

Overview

Recommendations

Reports

Apps and agents

Policies

Activity explorer

Data risk assessments

Preview

Identify oversharing risks

Use data assessments to identify potential oversharing risks in your organization. They also provide fixes to limit access to sensitive data.

Assess and prevent oversharing

1 Identify

Review assessment results for users accessing sensitive items. You can review the weekly results from the default assessment or create custom assessments to review specific data sources and users.

2 Protect

Limit Microsoft Copilot and agents access to sensitive data and apply label and retention policies to SharePoint sites and data.

3 Monitor

Conduct SharePoint site and access reviews to evaluate permissions and user access.

Default assessment

Assess oversharing of sensitive data for the top 100 SharePoint sites based on how many times the sites are accessed.

Results

Total items

431

Sensitive data detected

117

Links sharing data with anyone

0

Last updated

7 Jun 2025

Next update

14 Jun 2025

Frequency

Weekly

View details

Custom assessment status

No data available

Custom assessments (preview)

Custom assessments review specific data sources and users to identify potential oversharing of sensitive data. If the results are expired, you can duplicate the assessment to refresh the results.

+ Create custom assessment

0 items

Custom assessment name	Status	Started on ↓	Completed on	Results expire in
------------------------	--------	--------------	--------------	-------------------

Create a data assessment

To identify potential oversharing risks in your organization, create a data assessment.

Data assessments page showing analysis of oversharing within SharePoint sites



Data risk assessments > Default assessment

## Default assessment

Assesses oversharing of sensitive data weekly for the top 100 SharePoint sites based on how many times the sites are accessed. The top 100 sites may change each week, if different sites are accessed more often.

You can create custom assessments to scan specific data sources and users. [Learn more about custom assessments](#)

Create a custom assessment

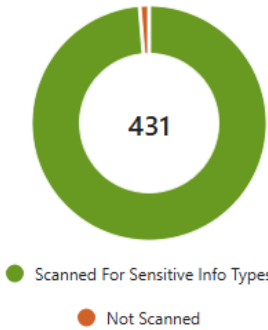
### Assessment details

Last updated  
7 Jun 2025

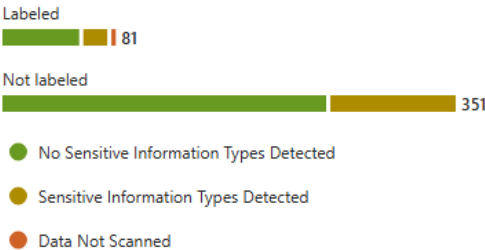
Next updated  
14 Jun 2025

Frequency  
Weekly

### Total items



### Sensitivity labels on data



### Items shared with



### Data risk assessment results

Review results to identify potential oversharing risks in your organization and apply fixes, such as limiting access to sensitive data and evaluating access to SharePoint sites.

Export

37 items Filter Group

<input type="checkbox"/> Data source ID	Source type	Total items	Total items accessed	Times users accessed items	Unique users accessing items	Total sensitive items	Total scan
rawingfiles/	SharePoint	265	1	1	1	93	265
ptest/	SharePoint	14	1	1	1	11	14
emoretenion/	SharePoint	12	1	1	1	2	12

Default assessment runs weekly, showing the top 100 SharePoint sites based on access

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Settings

DSPM for AI

Overview

Recommendations

Reports

Apps and agents

Policies

Activity explorer

Data risk assessments

Data risk assessments > Default assessment

Default assessment

Assesses oversharing of sensitive data weekly for the top 100 SharePoint sites based on how many times the sites are accessed. The top 100 sites m

You can create custom assessments to scan specific data sources and users. [Learn more about custom assessments](#)

Assessment details

Last updated

7 Jun 2025

Next updated

14 Jun 2025

Frequency

Weekly

Total items

431

Scanned For Sensitive Info Types

Not Scanned

Sensitivity labels on data

Labeled

Not labeled

81

No Sensitive Information Types Detected

Sensitive Information Types Detected

Data Not Scanned

Data risk assessment results

Review results to identify potential oversharing risks in your organization and apply fixes, such as limiting access to sensitive data and evaluating ac

Export selected item

<input type="checkbox"/>	Data source ID	Source type	Total items	Total items accessed	Time
<input type="checkbox"/>	/sites/drawingfiles/	SharePoint	265	1	1
<input type="checkbox"/>	/sites/ptest/	SharePoint	14	1	1
<input type="checkbox"/>	/sites/remoretenion/	SharePoint	12	1	1

/sites/drawingfiles/

OverviewIdentifyProtectMonitor

Data source details

Data source type

SharePoint

URL

https://mgmjdev.sharepoint.com/sites/drawingfiles/

Data coverage

Total items in site

265

View site

Labeled

Not labeled

0

265

No Sensitive Information Types Detected

Sensitive Information Types Detected

Data Not Scanned

Default assessment runs weekly, showing the top 100 SharePoint sites based on access

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Settings

DSPM for AI

Overview

Recommendations

Reports

Apps and agents

Preview

Policies

Activity explorer

Data risk assessments

Policies

DSPM for AI policies use Microsoft Purview solutions to discover and safeguard AI activity across your organization. [Learn more about policies](#)

Refresh

3 items

Search

Group

Name	Status	Solution	Last Modified	Last Modified By
Data Loss Prevention (1)				
DSPM for AI: Detect sensitive info added to AI sites	On	Data Loss Prevention	Feb 4, 2025 9:42 AM	Mark Warnes
Insider Risk Management (2)				
DSPM for AI - Detect risky AI usage	On	Insider Risk Management	Mar 26, 2025 4:51 PM	Mark Warnes
DSPM for AI - Detect when users visit AI sites	On	Insider Risk Management	Mar 26, 2025 4:51 PM	Mark Warnes

Policies page showing currently configured AI-related policies across Purview solutions

## Top tips

- Use **Endpoint DLP** to restrict sensitive data being pasted into generative AI services
- Use **Defender for Cloud Apps** to monitor usage of existing and new services
- Block access to unsanctioned AI services with **Defender for Endpoint**



# Data Security

## Access Microsoft funding to kick-start your Purview adoption

See if your organisation qualifies for Microsoft funding.

- Identify your compliance gaps with a risk management assessment and 'dark data' check.
- Understand your compliance challenges and discover tools that can help you improve.
- Immersive Microsoft demos for Information Protection and Data Loss Prevention.
- Findings report with recommended next steps.

Speak to our team today.



# Ensure continuous compliance

## Purview Success Pathway

Meet your regulatory obligations with our bespoke service to assess and continuously improve your compliance posture.

### Discover:

- How well you are meeting regulatory obligations.
- The right systems and controls to ensure ongoing compliance.
- How to adopt new regulations with minimum business disruption



hello@kocho.co.uk



0800 044 5009

