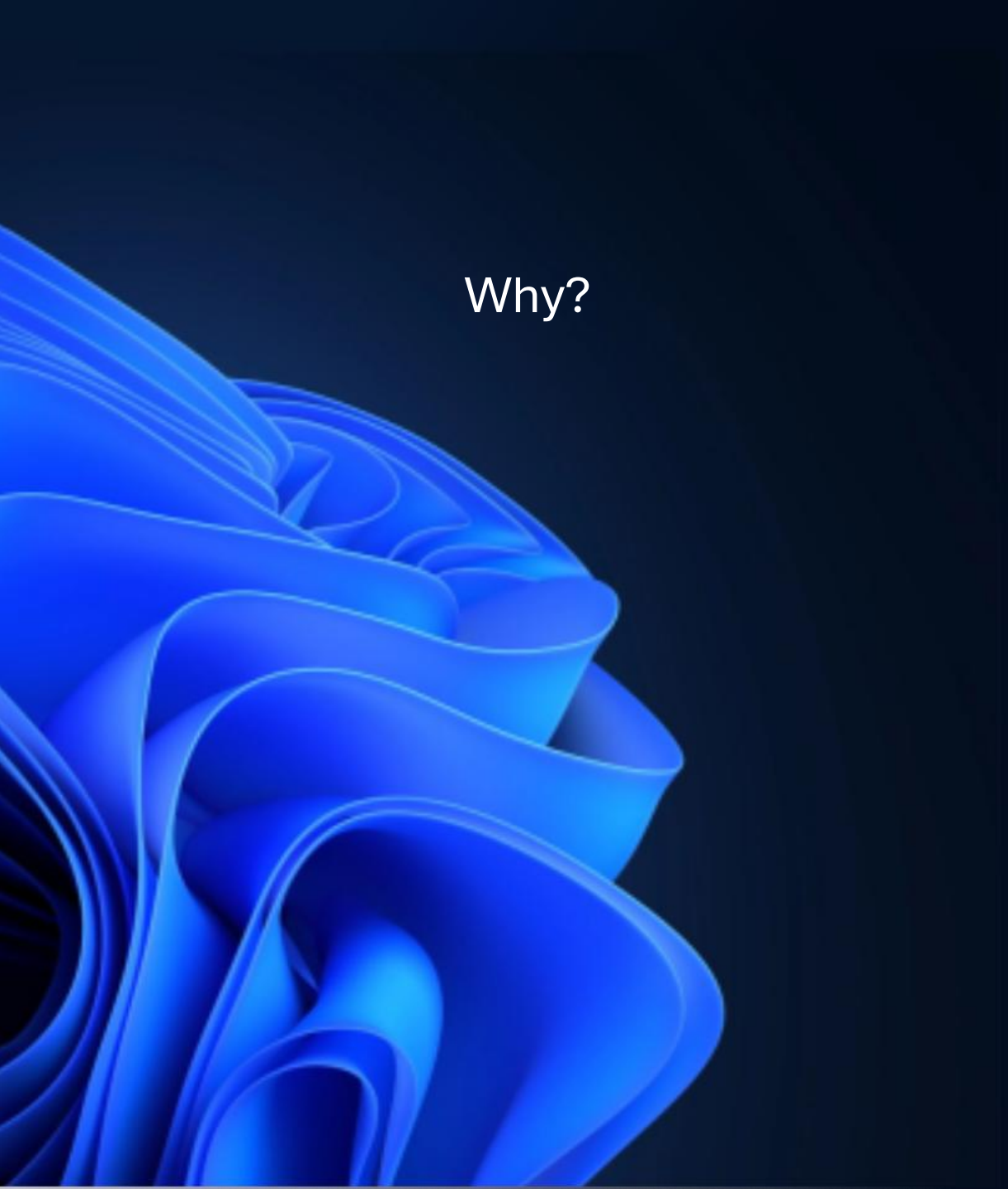
Data Security Considerations for M365 Copilot

Andrew O'Young
Security MVP
Modern Work Specialist
M365 Senpai
Out of Band: AMSP



Why?

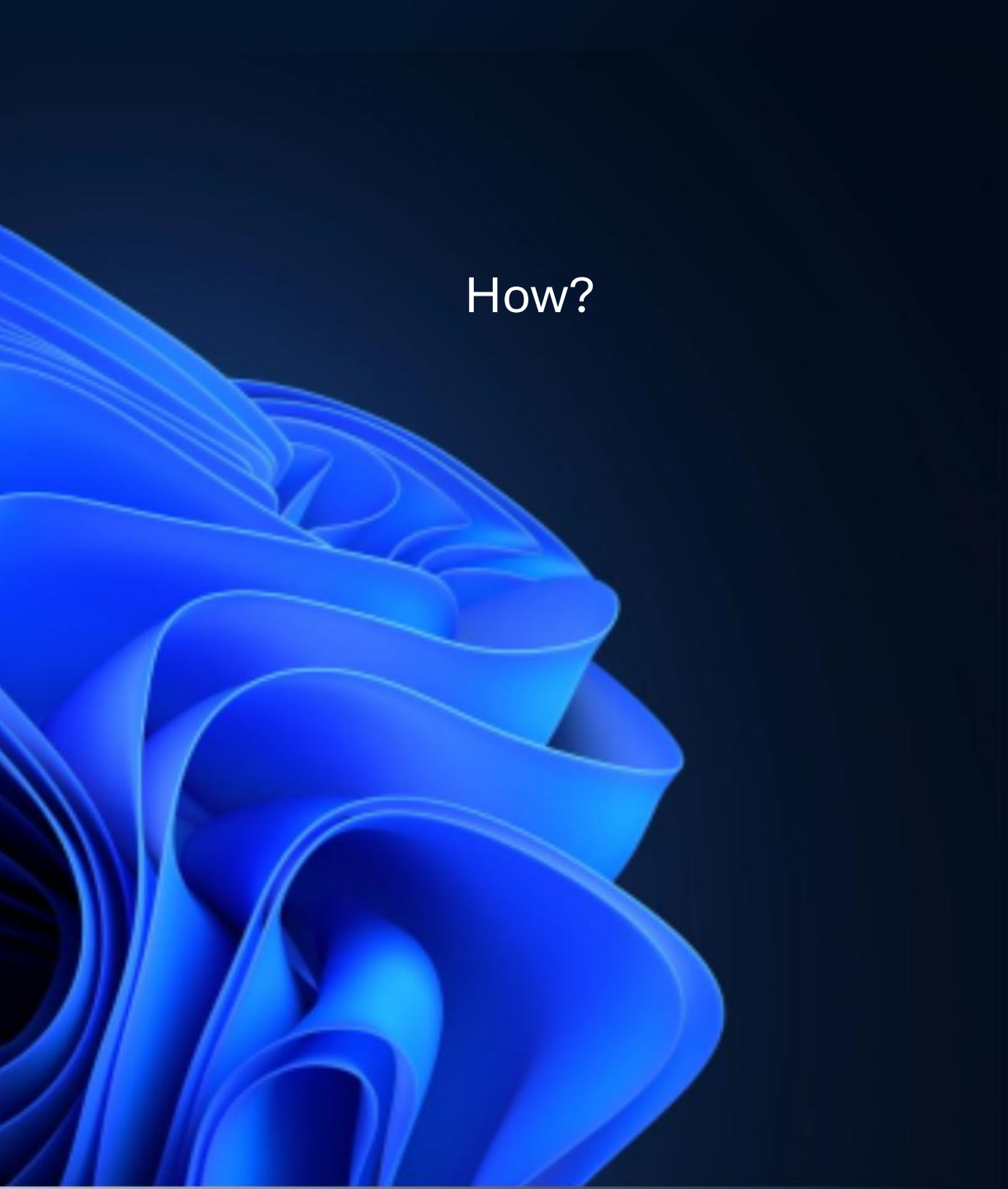
Oversharing

Data Leakage

Auditing

External Threats

Internal Threats



How?

Foundational Security

Copilot Control System

SharePoint Advanced Management

Microsoft Purview

Data Security Posture Management for AI

Foundational Security

Tenant Settings

Permissions

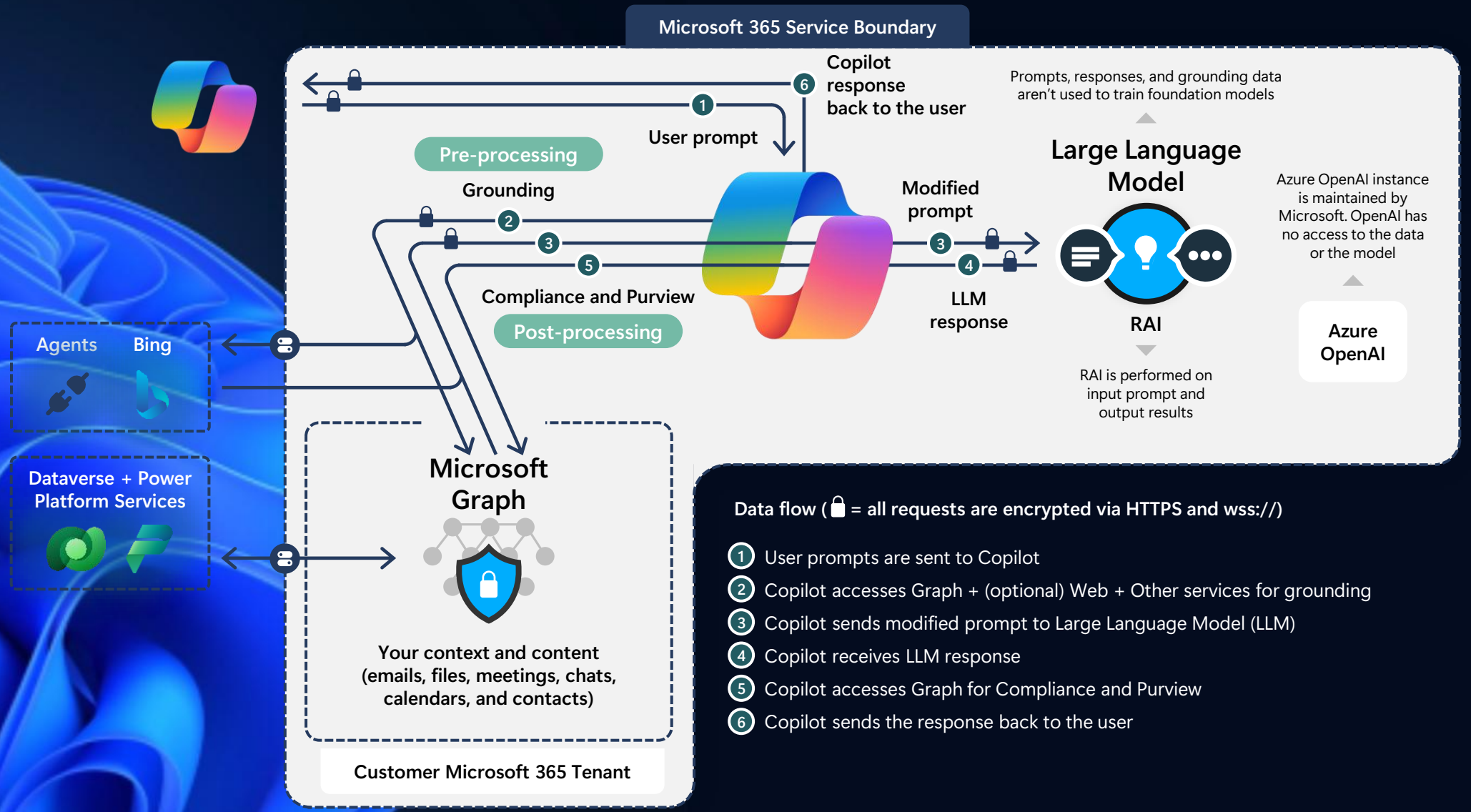
Identity & Access Management

Conditional Access

Defender for X

Introducing: Copilot Control System

Microsoft Copilot for Microsoft 365 architecture and content retrieval



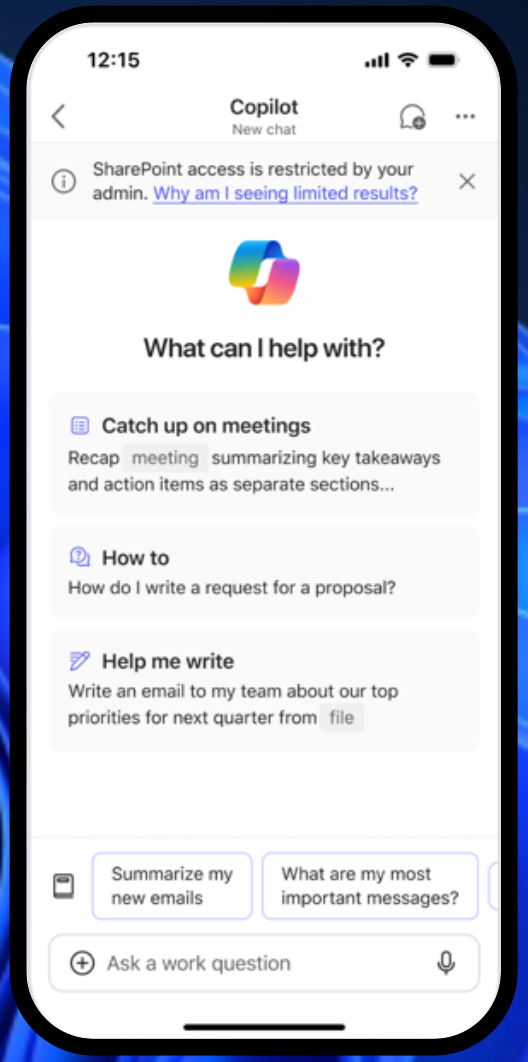
Data flow (= all requests are encrypted via HTTPS and wss://)

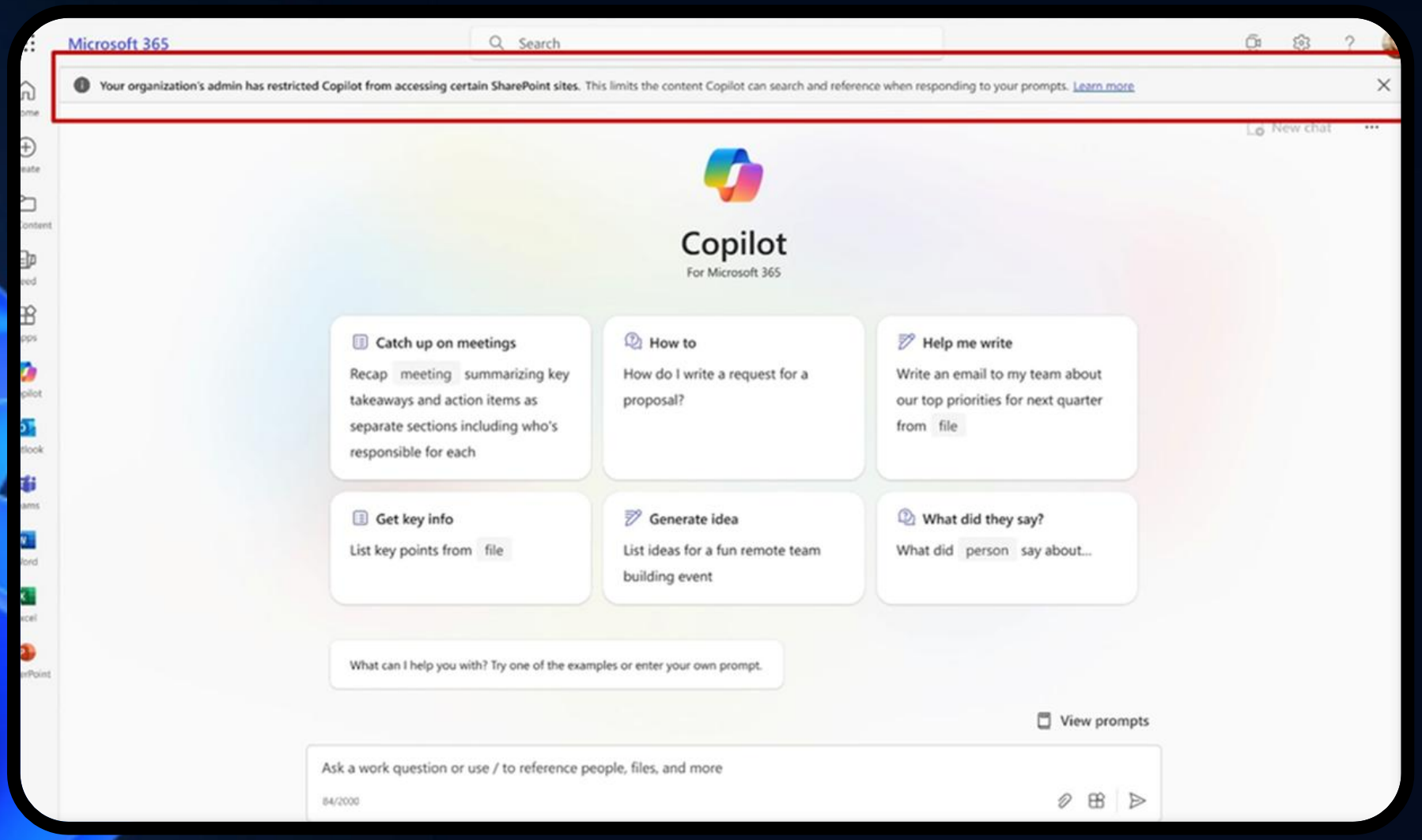
1. User prompts are sent to Copilot
2. Copilot accesses Graph + (optional) Web + Other services for grounding
3. Copilot sends modified prompt to Large Language Model (LLM)
4. Copilot receives LLM response
5. Copilot accesses Graph for Compliance and Purview
6. Copilot sends the response back to the user

Enable SharePoint Restricted Search

Step	Description	Example
1	Get the current mode that is set for Restricted Search	`Get-SPOTenantRestrictedSearchMode`
2	Enable Restricted Search	`Set-SPOTenantRestrictedSearchMode -Mode Enabled`
3a	Add sites using a list	`Add-SPOTenantRestrictedSearchAllowedList -SitesList @("[https://contoso.sharepoint.com/sites/Marketing](https://contoso.sharepoint.com/sites/Marketing)", "[https://contoso.sharepoint.com/sites/Benefits](https://contoso.sharepoint.com/sites/Benefits)")`
3b	Add sites using a CSV file	`Add-SPOTenantRestrictedSearchAllowedList -SitesListFileUrl C:\Users\admin\Downloads\UrlList.csv`

End-User Experience





Restricted SharePoint Search – Key Takeaways

Not a “Copilot” Feature

Should only be considered if your Copilot deployment is blocked due to file oversharing concerns

A temporary solution: Allows full Copilot deployment, and in parallel, implementation of security controls as needed (SAM/Purview) to address oversharing concerns

Does not modify permissions or sharing controls on content

Will impact other org-wide search experiences in Microsoft 365

SharePoint Advanced Management

Manage content sprawl

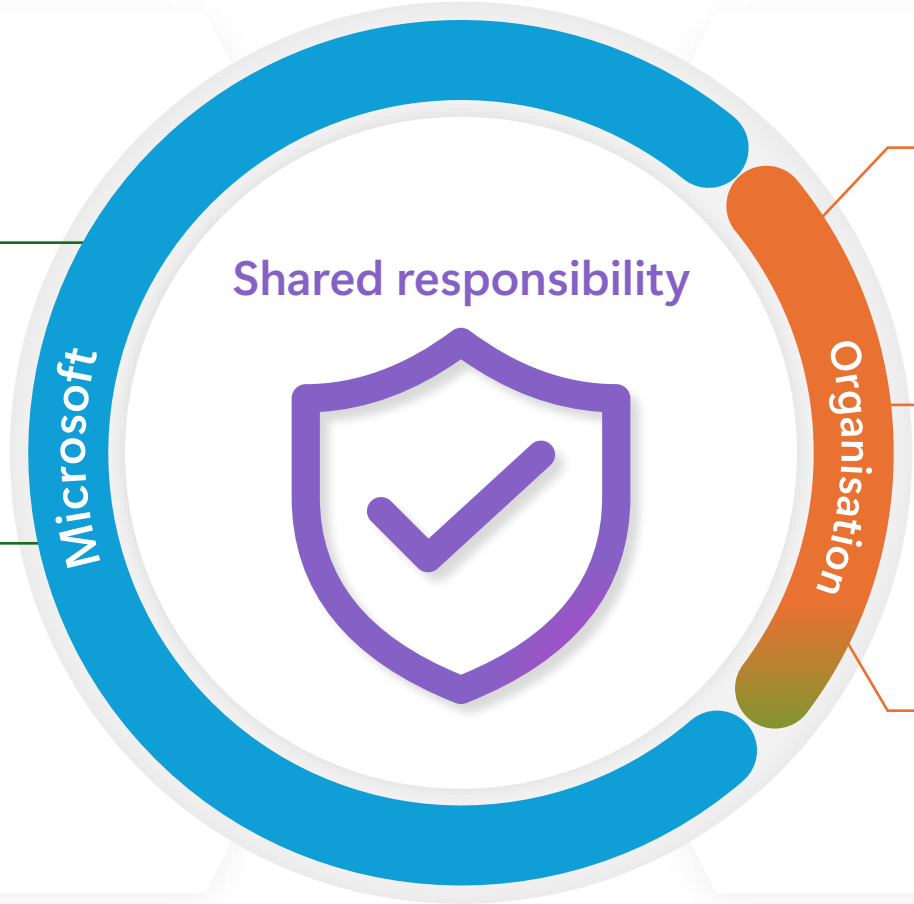
Prevent oversharing

Control Copilot access to content

Manage content lifecycle

Microsoft Purview

Shared responsibilities of security for AI usage for Microsoft 365 Copilot



Access to production environment

Set up access controls that strictly restrict standing access to customer's data or production environment

Protect data

Encrypt data at rest and in transit based on industrial standards (BitLocker, TLS, etc.)

Access to AI apps

Set up access control policy, leveraging identity and access management solutions

Protect data entered and created by AI apps

Apply sensitivity label that associates with encryption and DLP controls to files with sensitive data

User accountability of AI use

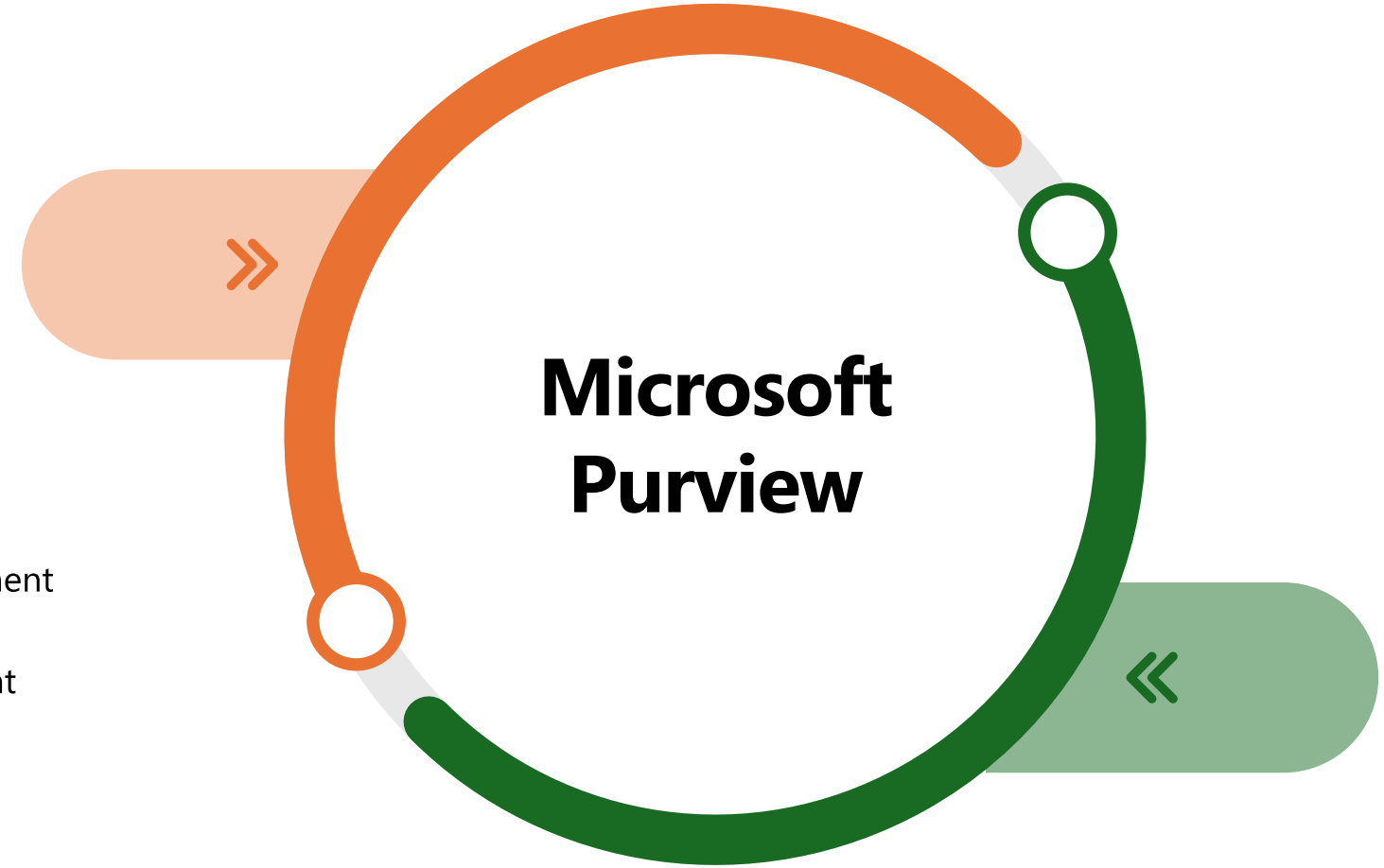
Implement and operate organisation-wide AI security training

Microsoft Purview brings together solutions from our compliance and data governance portfolios

Risk & compliance

For risk, compliance, and legal teams

Information Protection
Data Loss Prevention
Data Lifecycle Management
Data Connectors
Insider Risk Management
eDiscovery
Audit
Records Management
Communication Compliance
Compliance Manager

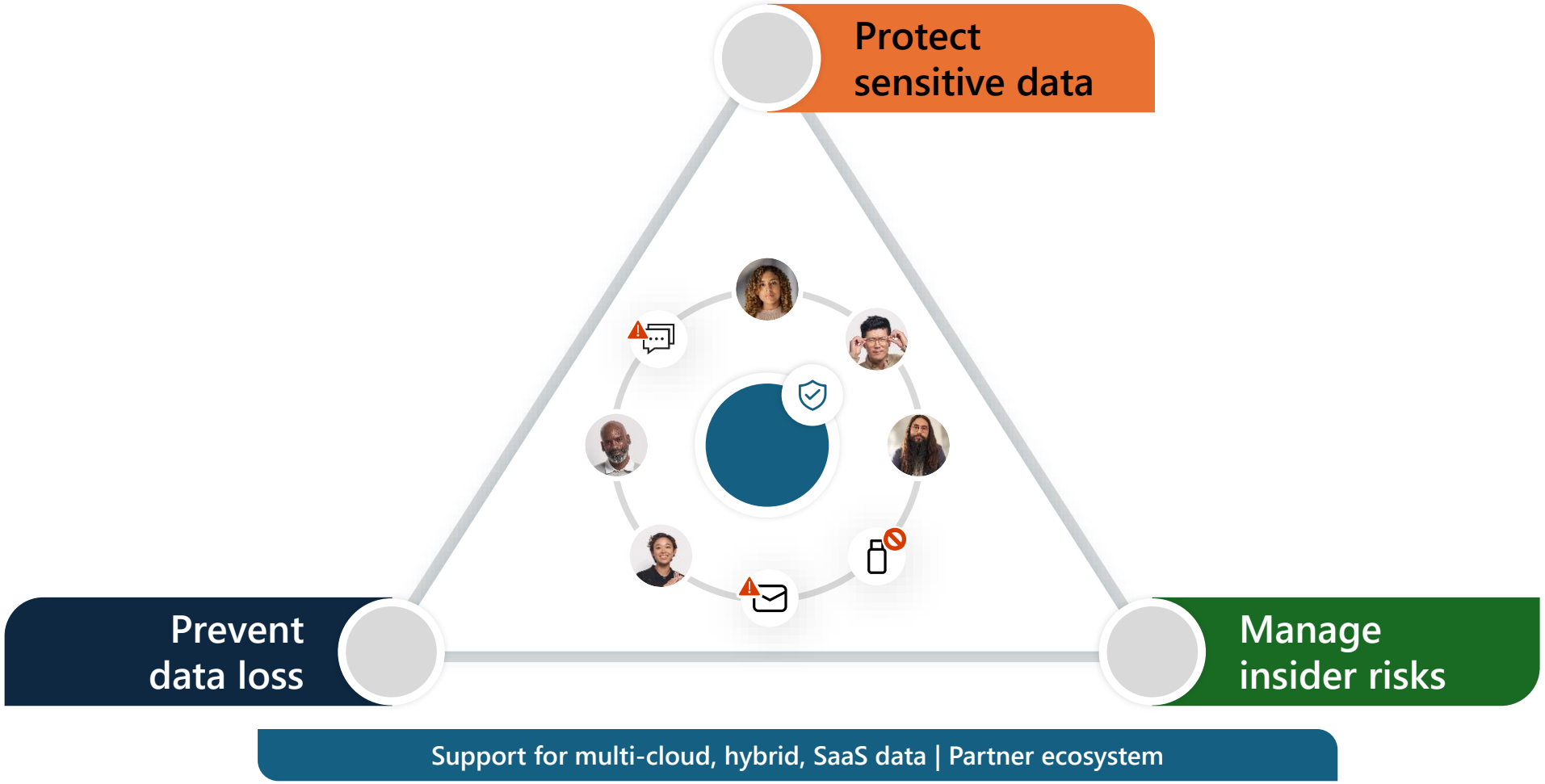


Data Map
Data Catalog
Data Estate Insights

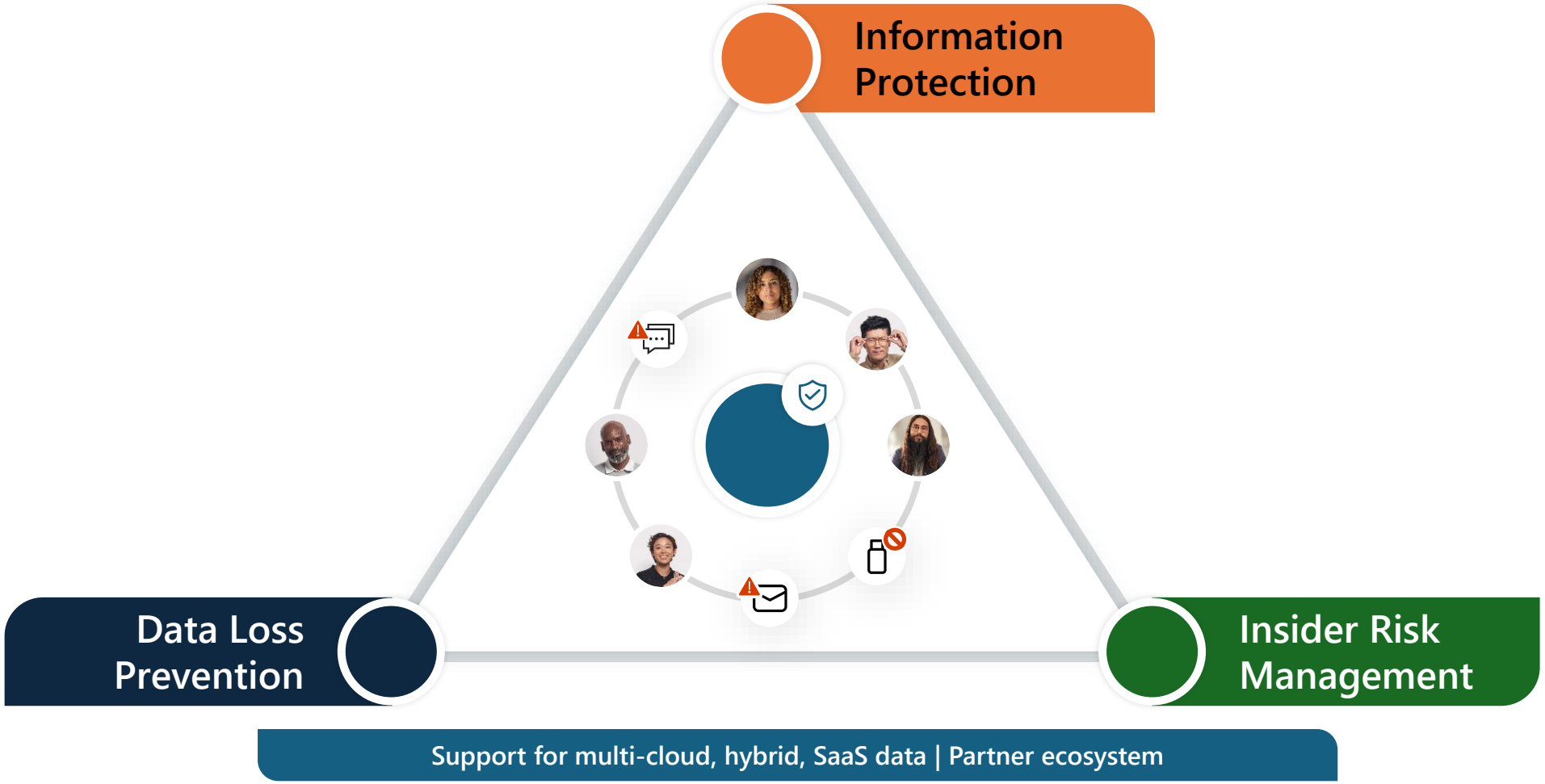
Unified data governance

For data consumers, data engineers, data officers

Microsoft’s approach to data security



Fortify data security with Microsoft Purview



Fortify data security with Microsoft Purview

Information Protection

- **Discover, classify, and protect** data at scale, using automation and ML
- Productivity tools with built-in **user-selectable sensitivity labels** for precise controls
- Data is **protected (encrypted) across environments**, throughout its lifecycle

Insider Risk Management

- Leverage **analytics, machine learning, sequencing** to understand user context and intent
- Investigate potential incidents with **curated, high-quality, and enriched** alerts and evidence
- Ensure user privacy while identifying **highest risk users**

Data Loss Prevention

- **Prevent unauthorized use**, like improperly saving, storing or printing sensitive data
- Create, deploy, and manage DLP policies **across all cloud, apps, and devices from a single location**
- Leverage data classification, labeling, and user **insights to finetune and adapt DLP policies**

Adaptive Protection

Dynamically adjust data security controls based on user risk level

Adaptive Protection in Microsoft Purview

Optimize data security automatically

Context-aware detection

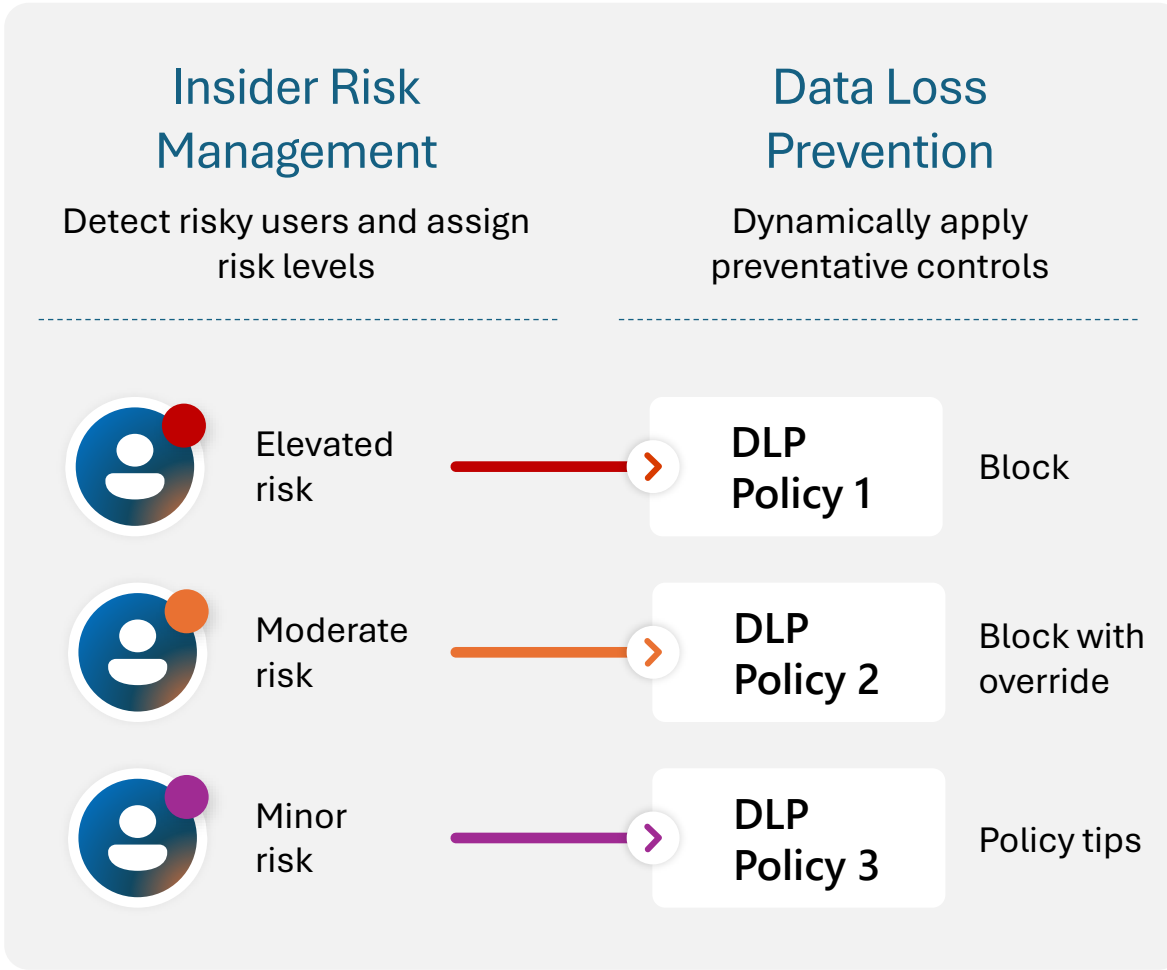
Identify the most critical risks with ML-driven analysis of both content and user activities

Dynamic controls

Enforce effective controls on high-risk users while others maintain productivity

Automated mitigation

Minimize the impact of potential data security incidents and reduce admin overhead

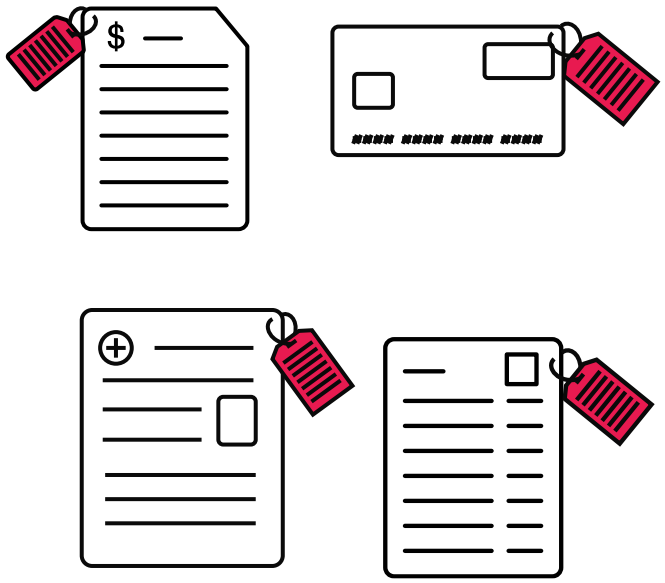


Integrated insights and alerting

Enrich policy and investigation with rich signals

Know the context

Leverage classification and labeling on sensitive data from Information Protection



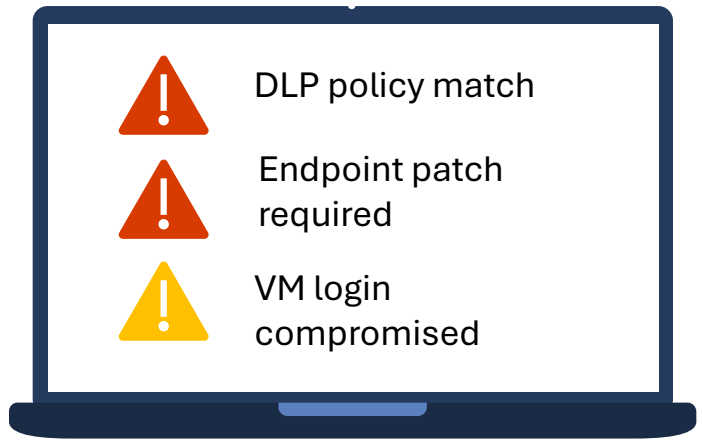
Understand the intent

Automatically apply risk insights from Insider Risk Management to DLP policies

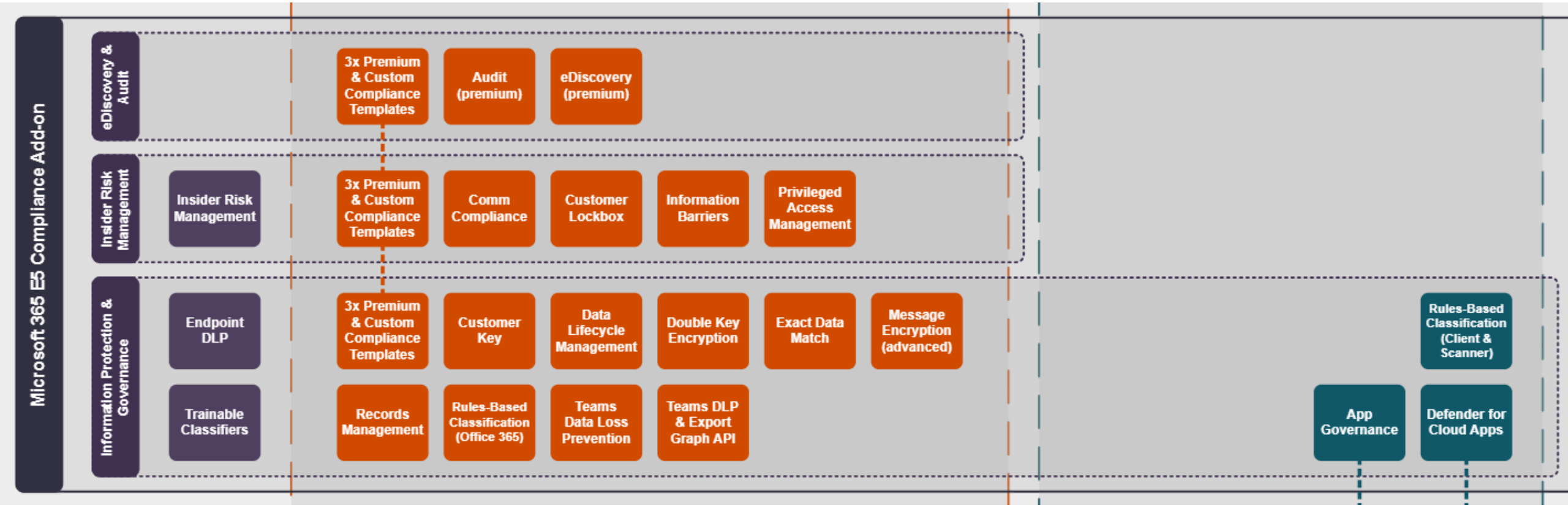
Elevated risk	→	DLP Policy 1	Block
Moderate risk	→	DLP Policy 2	Block with override
Minor risk	→	DLP Policy 3	Policy tips

Integrate alert investigation

Integrate DLP alerts with Microsoft Defender XDR and Sentinel for richer investigation experience



Purview Licensing



Information Protection and Governance ($13pupm)

Adds the additional features below to Microsoft 365 Business Premium:

- *Microsoft Defender for Cloud Apps helps you discover SaaS apps and protect users from accessing risky apps
- Communications DLP (Teams chat) blocks sensitive content when shared with Teams users
- Endpoint DLP prevents data leak of sensitive items physical stored on Windows 10/11 and MacOS devices
- Automatic sensitivity labels (client side) automatically discover, classify, label and protect sensitive data
- Machine Learning-Based sensitivity Labels use trainable classifiers to identify items and apply labels
- Records management helps manages businesses legal obligations
- Advanced Message Encryption helps control sensitive emails shared outside the organisation

Insider Risk Management ($10pupm)

Adds the additional features below to Microsoft 365 Business Premium:

- Insider risk management helps minimize internal risks by responding to malicious activities
- Communication compliance helps detect business code of conduct violations

eDiscovery and Audit ($10pupm)

Adds the additional features below to Microsoft 365 Business Premium:

- eDiscovery (Premium) with end-to-end workflow for managing eDiscovery cases and investigations
- Audit (Premium) with longer record retention and intelligent insights policies

Microsoft Purview Deployment Card

Microsoft's Data Security Platform

Data Security Posture Management for AI & (DSPM) Microsoft 365

Use the Posture Report from the beginning

Information Protection

Build your Label Taxonomy. Example Public, General, Confidential etc.

Consider use of default label and policies, followed by auto-labelling, encryption to restrict access to certain documents

Turn on co-authoring

Turn on labels across M365

Data Loss Prevention

Review where the sensitive info are located.

Leverage Sensitivity Labels to prioritize with policies

Create custom policy or a category that is specific to your org e.g. Health, Finance.

Restrict sensitive data on 3rd party apps

Data Lifecycle Management

Keep what you need and delete what you don't. Create Exceptions

Use file plan to managed retention schedule

Publish retention labels as optional or automatic

Consider Adaptive scopes

Use sensitivity labels to govern what is to retain or delete

Insider Risks Management

Turn on Analytics and understand the data sharing landscape

Understand the policy template requirements from DLP or MDE pre-req to which stake holders do you need involved

Use data classification to prioritize content

Enable Defender XDR Integration

Enable Adaptive Protection including CA, DLP, DLM

Communication Compliance

Ensure you have the correct team to managed alerts

Create policy from our templates. From copilot interactions, conflict of interest, inappropriate images, text, content

Understand the alert volume and fine tune to create clear governance across what is important

DSPM for AI/DSPM

Enable Purview Audit

Install Browser extension

Enabled Recommended Policies

Review the Data Assessment Report

Use the Posture Report from the beginning and on-going

eDiscovery

Enabling the pillars before this makes any content search that much easier

Learn how to preserve, collect, review, analyze and export data so when the time does come, your team knows how to response to a internal or external investigation

Search sensitivity labels for content search and holding of data

Data Governance (Add-on)

Unified Catalog

Security Copilot (Add-On)

Microsoft Sentinel (Add-on)

Enable Audit Log **Products like IRM, eDiscovery, Comm Compliance depend on Audit Log including Copilot Interaction logs**

Microsoft

Not Official Document-
Developed by Ray Reyes
Updated 9th Feb 2025

DSPM for AI

Data Security Posture Management for AI uses Microsoft Purview solutions to discover and safeguard AI activity across your organization

Fundamentals

Enable Purview Audit

Install the Purview Browser Extension

Onboard Devices to Purview

Extend your data discovery by enabling 3 key policies

1. IRM - Detect risky AI usage
2. DLP - Microsoft AI hub - Browsing in AI assistants
3. DLP - Microsoft AI hub - Discover sensitive prompts in AI assistants

Recommendation

Insider Risk - Adaptative Protection - Block elevated risk users from pasting or uploading sensitive info on AI sites

Communication Compliance- Detect unethical behaviour in Microsoft 365 Copilot

Information Protection - Protect your files with Sensitivity Labels

Use Copilot to improve your data security posture (preview)

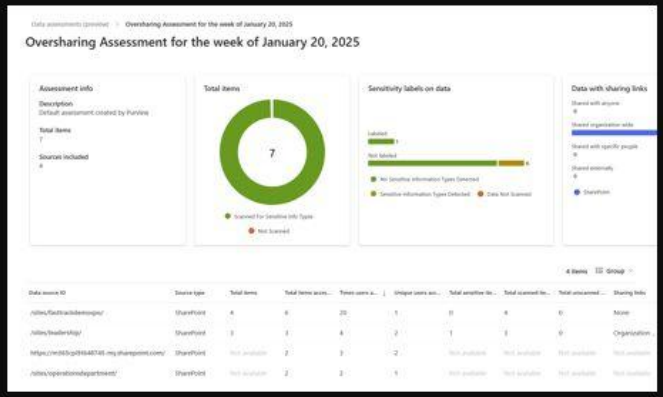
Discover and govern interactions with ChatGPT Enterprise AI (preview))

Data Assessment Report

DLP - Protect sensitive data referenced in Copilot responses

Protect your data from potential oversharing risks

Run a regular assessment, identify gaps and improve your data security posture across your SharePoint Sites



Microsoft

Not Official Document-
Developed by Ray Reyes
Updated 30th Jan 2025

Credentials

Applied Skills

Microsoft Applied Skills: Prepare security and compliance to support Microsoft 365 Copilot

Microsoft Applied Skills: Implement information protection and data loss prevention by using Microsoft Purview

Microsoft Applied Skills: Implement retention, eDiscovery, and Communication Compliance in Microsoft Purview

Certifications

Microsoft Certified: Information Protection and Compliance Administrator Associate

Microsoft Certified: Information Security Administrator Associate (beta)