



Secure & govern agents in Microsoft 365

from grounding data to interactions

A Microsoft Purview deployment blueprint



Microsoft Purview

A unified approach to secure and govern your data in the era of AI

Data security

Dynamically secure data throughout its lifecycle

Data Loss Prevention
Insider Risk Management
Information Protection
Data Security Posture Management
Data Security Investigations

Data governance

Responsibly unlock value creation from data

Data Discovery
Data Quality
Data Curation
Data Estate Health

Data compliance

Manage critical risks and regulatory requirements

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

Unstructured & Structured data

Traditional and AI generated data

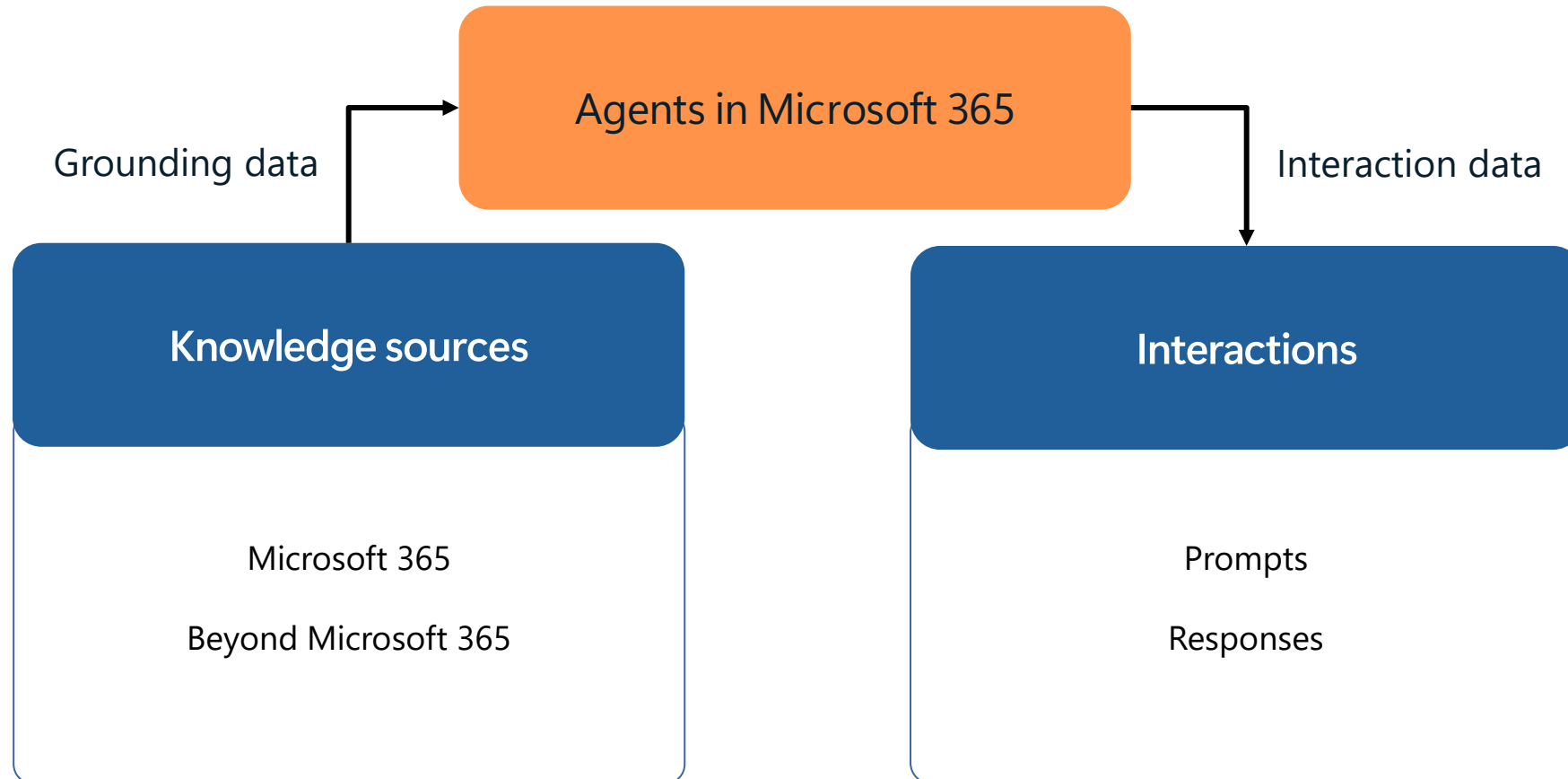
Microsoft 365 and Multi-cloud

Shared Capabilities Value

Data Map • Connectors • Classification • Labels • Audit • Visibility

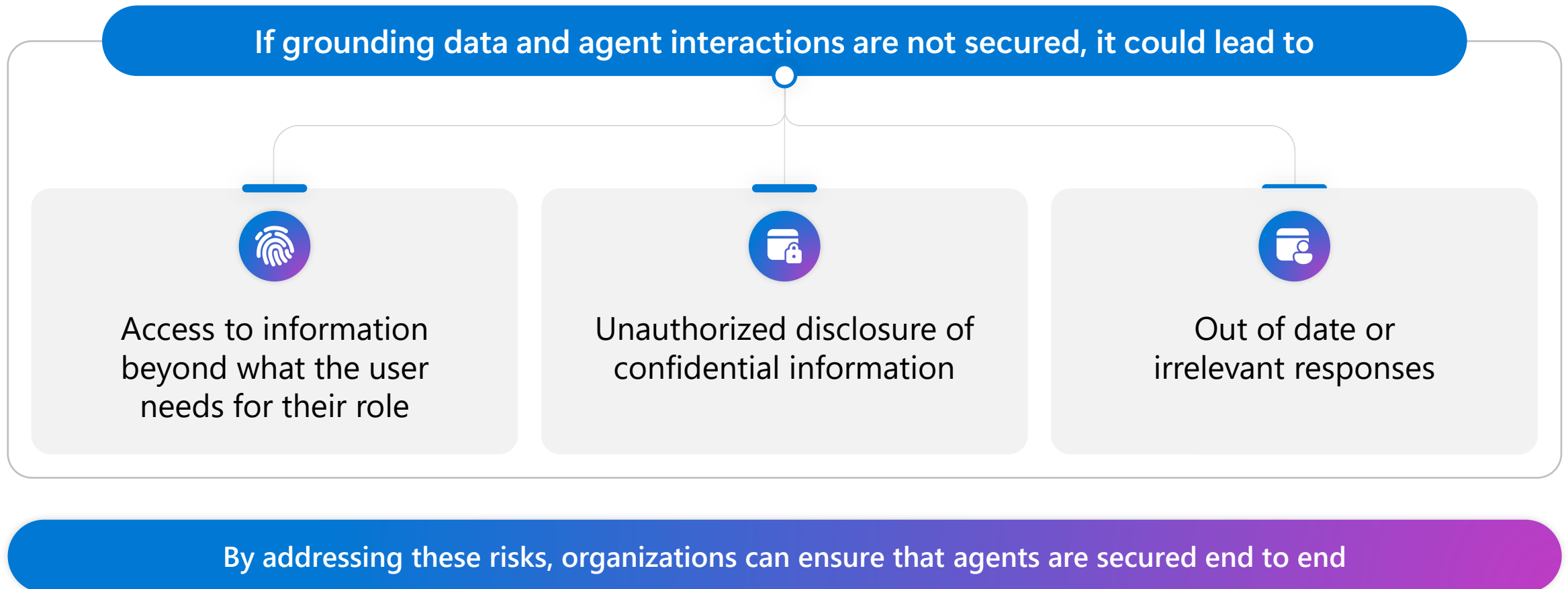
Microsoft Purview

Comprehensive solution to discover, protect, and govern data
Wherever your data flows



Problem summary

Agents in Microsoft 365 Copilot's leveraging information in SharePoint and Dataverse has raised concerns for organizations about oversharing, data loss, and insider risks.



Copilot agent conversation displays the sensitivity label of referenced file and data



A sensitivity label is displayed for the **entire conversation**.

Conversations displays the **most restrictive sensitivity labels** from the references used to formulate a response.

The screenshot shows a Copilot agent conversation interface. At the top, the header reads "Purview for AI Assistant > Summary of Secure Copilot Agents Presentation". A sensitivity label "Confidential/Microsoft Extended" is displayed, stating: "Data is classified and protected. Microsoft Full Time Employees (FTE) and non-employees can edit, reply, forward and print. Recipient can unprotect content with the right justification." Below this, the agent responds to a user request to summarize a document: "Thanks for sharing the file. Here's a summary of the key points from the [Secure Copilot Agents](#) presentation 1:". The summary is titled "Overview: Securing Copilot Agents with Microsoft Purview" and describes a blueprint for deploying secure Copilot agents in Microsoft 365 using Microsoft Purview, focusing on minimizing data loss, insider risks, and oversharing. At the bottom, there are two buttons: "Make this summary customer-ready" and "Create a slide with these key points". A text input field labeled "Message Copilot" is at the bottom, with a plus icon and a microphone icon. A footer note states "AI-generated content may be incorrect".

Honoring access control restrictions on labeled content

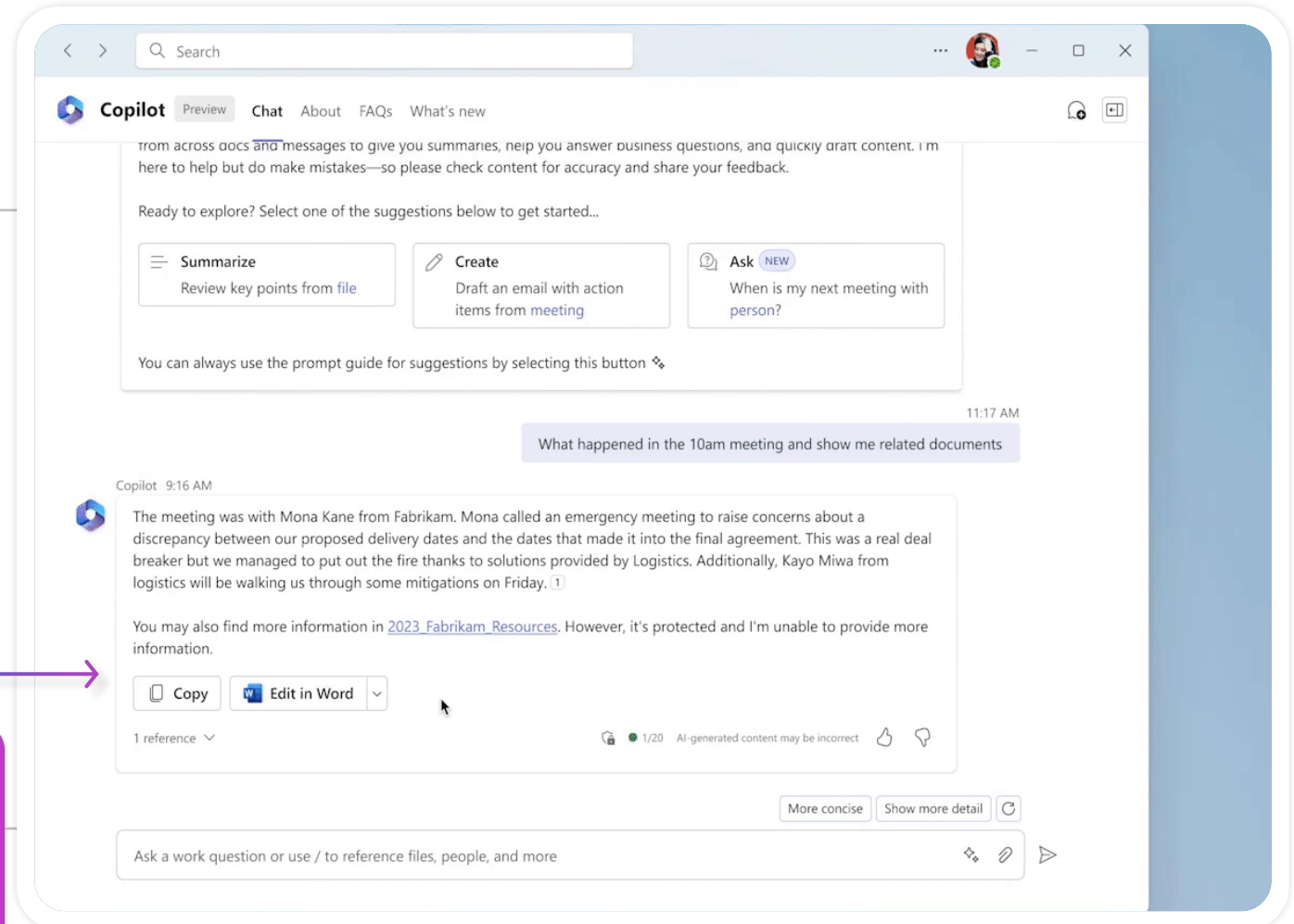


Only content from references where the user has appropriate permission will be included in responses.

If a user lacks the right permissions, Copilot agent will inform the user and provide a link but **will not include the content for generating responses.**



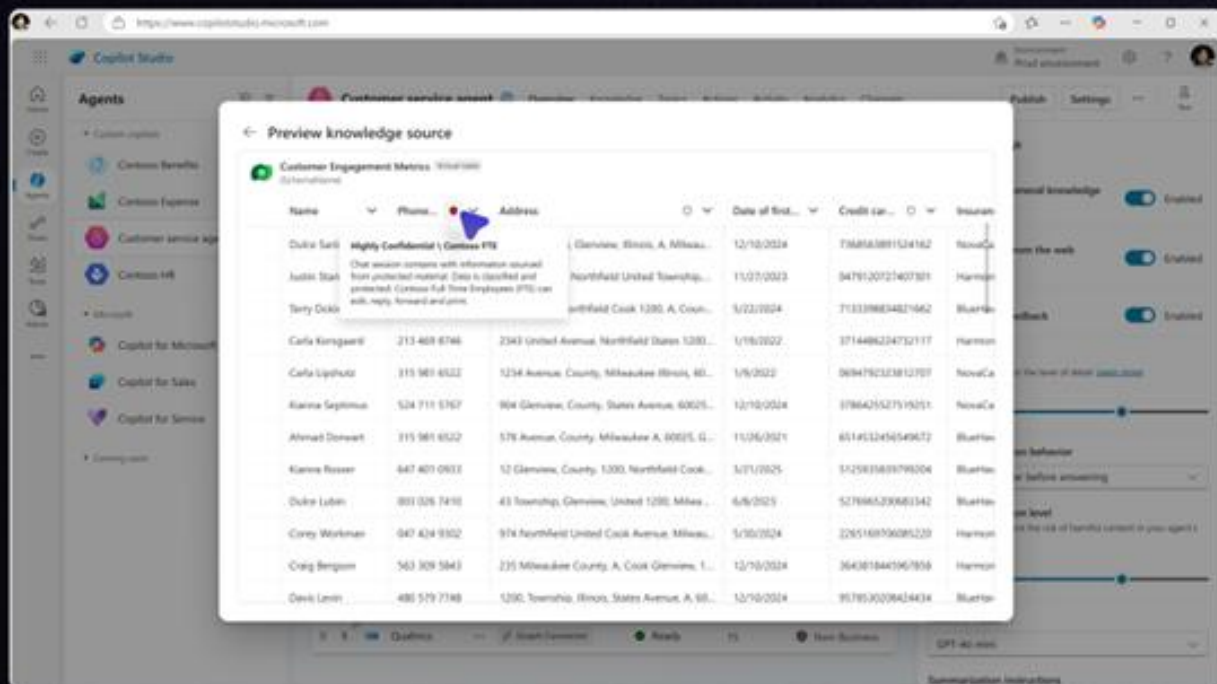
Copilot will not include information from referenced files where the user does not have appropriate access rights.



Introducing

Dataverse ❤️ Purview

Discover and protect sensitive business data and empower its consumers with valuable and trustworthy insights



← Preview knowledge source

Customer Engagement Metrics - (Highly Confidential)

Name	Phone	Address	Date of first...	Credit card...	Insurance
Duke Sato	213 409 8746	2343 United Avenue, Northfield Staten 1280...	12/10/2024	736816381124162	Harmon
Justin Stark	315 981 6522	Northfield United Township...	11/07/2023	9479120721407301	Harmon
Terry Dicks	315 981 6522	Northfield Cook 1280, A. Cook...	1/22/2024	713339834821662	Bluebird
Carla Karsgaard	213 409 8746	2343 United Avenue, Northfield Staten 1280...	1/16/2022	371448623472117	Harmon
Carla Lyschinski	315 981 6522	1234 Avenue, County, Milwaukee Illinois, 60...	1/6/2022	8694792323812707	Harmon
Kiauna Septimus	524 711 5767	864 Glenview, County, States Avenue, 60025...	12/10/2024	3786421527519251	Harmon
Ahmad Donawalt	315 981 6522	578 Avenue, County, Milwaukee A, 60025, G...	11/26/2021	651451245459672	Bluebird
Kiauna Basser	847 401 0932	12 Glenview, County, 1200, Northfield Cook...	3/21/2025	5125835835795204	Bluebird
Duke Labin	801 326 7410	41 Township, Glenview, United 1280, Milwa...	6/6/2025	5276665236621542	Bluebird
Corey Workman	847 424 9302	914 Northfield United Cook Avenue, Milwa...	1/26/2024	22616876085229	Harmon
Craig Bergson	563 309 5843	235 Milwaukee County, A. Cook Glenview, 1...	12/10/2024	3643818443967856	Harmon
David Lemm	480 579 7748	1200, Township, Illinois, States Avenue, A, 60...	12/10/2024	9578530298424434	Bluebird

GA

Enable automated discovery for Dataverse data to enrich your Microsoft Purview data map

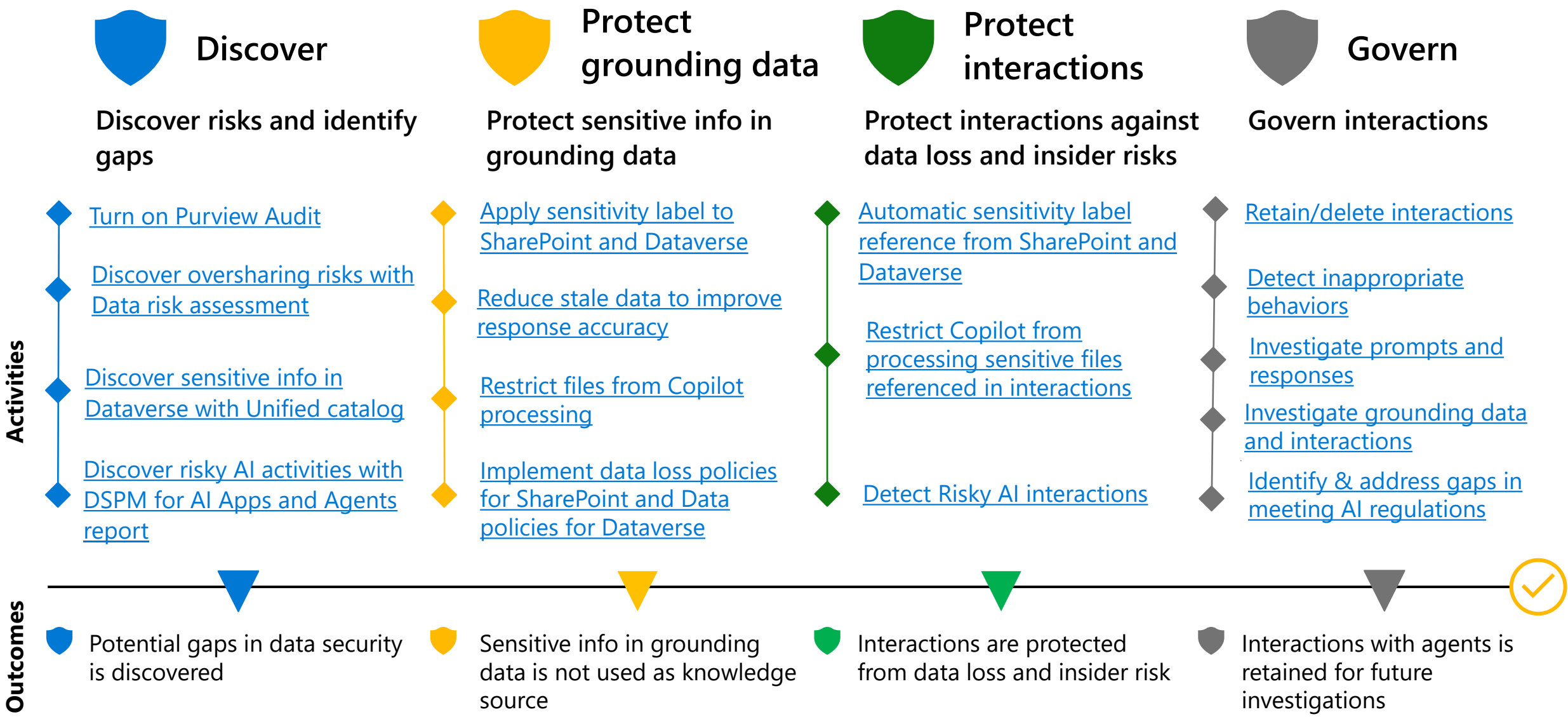
Public Preview

Automatically classify and understand sensitive business data stored in Dataverse

Public Preview

Enhance agent interactions with sensitive data with Purview labels to prevent oversharing of sensitive data

Secure & govern agents in Microsoft 365



Discover

- Turn on Microsoft Purview Audit to log all interactions with grounding data and interactions with AI apps and agents
- Discover potential oversharing in SharePoint/OneDrive with Microsoft Purview data risk assessments
- Discover where sensitive info resides in Dataverse with Microsoft Purview Data Governance's Unified catalog
- Discover risky AI activities with Microsoft Purview Data Security Posture Management (DSPM) for AI's Apps and Agents report

Protect grounding data

- Apply sensitivity label to SharePoint and Dataverse
- Reduce stale data to improve agent response accuracy with Microsoft Purview Data Lifecycle Management
- Restrict sensitive files labeled with specific sensitivity labels from Copilot processing and acting as knowledge source with Microsoft Purview Data loss prevention (DLP) for Copilot
- Implement Data policies for Dataverse to restrict sensitive data from being used as knowledge source for agents
- Implement oversharing DLP policy for SharePoint/OneDrive to detect anyone sharing links for labeled and unlabeled data

Protect interactions

- Sensitivity labels applied to data in SharePoint and Dataverse is automatically displayed and respected by the conversation
- Restrict Copilot from processing sensitive files referenced in interactions with DLP for Copilot, which also ensures the sensitive prompts are not used for web query
- Detect Risky AI interactions with Microsoft Purview Insider risk management's Risky AI policy

Govern interaction data

- Retain interactions for future investigations, and delete interactions based on retention requirements to reduce risk and liability with Microsoft Purview data lifecycle management policies
- Detect inappropriate behaviors with Microsoft Purview Communication Compliance policies with built-in classifiers such as jailbreak, harassment, inappropriate images, etc.
- Investigate legal and internal cases with Microsoft Purview eDiscovery
- Investigate interactions and grounding data leveraging the power of AI with Microsoft Purview Data security investigations (DSI)
- Identify & address gaps in meeting AI regulations with Microsoft Purview Compliance Manager



Additional resources

Data security and protections for AI with Microsoft Purview:
[Microsoft Purview data security and compliance protections for Microsoft 365 Copilot and other generative AI apps | Microsoft Learn](#)

Join the Microsoft customer connection program
aka.ms/JoinCommunity

Deployment guides:
DSPM for AI: aka.ms/DSPMforAI/Deploy
Data Risk assessment: aka.ms/DSPMforAI/Oversharing

Accelerate your Information Protection and Data Loss Prevention deployment:
<https://aka.ms/PurviewDeploymentModels/SecureByDefault>



Purview for Dataverse resources

- [Connect to and manage Microsoft Dataverse in Microsoft Purview | Microsoft Learn](#)
- [View sensitivity labels for SharePoint data sources - Microsoft Copilot Studio | Microsoft Learn](#)
- [Apply sensitivity labels to your data in Microsoft Purview Data Map \(preview\) | Microsoft Learn](#)
- [Security in Microsoft Dataverse - Power Platform | Microsoft Learn](#)

Thank you

Microsoft Deployment models

Read the detailed guide for this model at aka.ms/PurviewDeploymentModels/SecureM365Agents