Microsoft

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

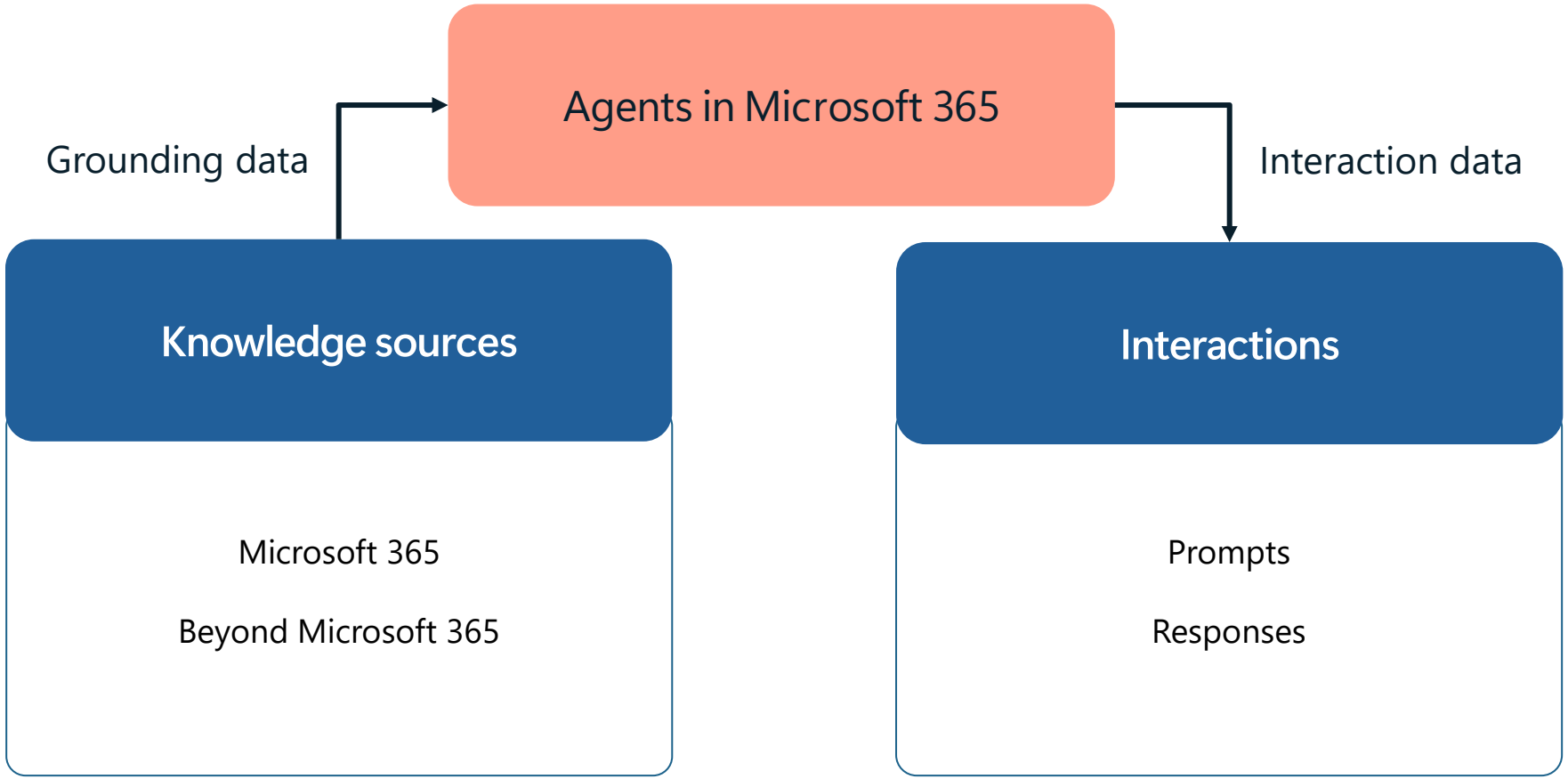
Unstructured & Structured data | **Traditional and AI generated data** | **Microsoft 365 and Multi-cloud**

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.

If grounding data and agent interactions are not secured, it could lead to

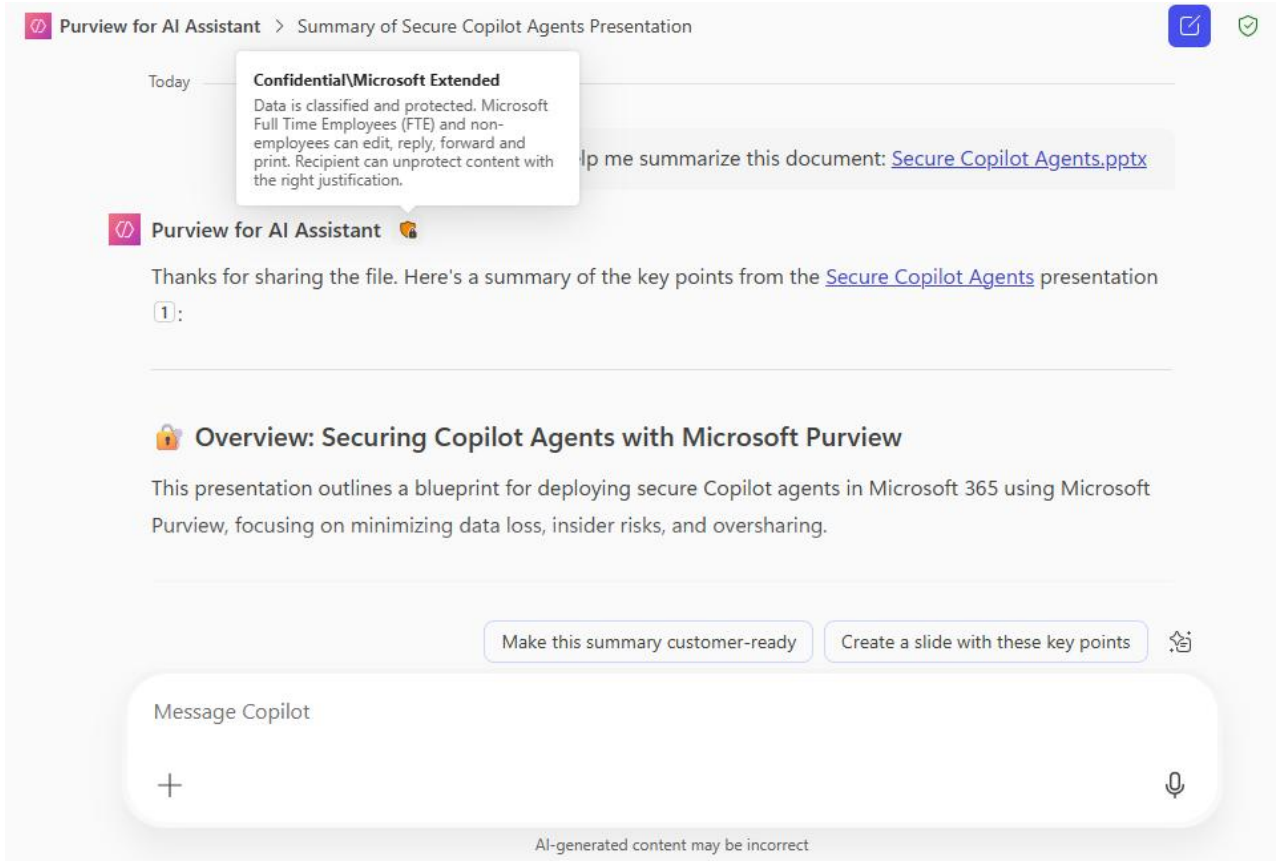
- Access to information beyond what the user needs for their role
- Unauthorized disclosure of confidential information
- Out of date or irrelevant responses

By addressing these risks, organizations can ensure that agents are secured end to end

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

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

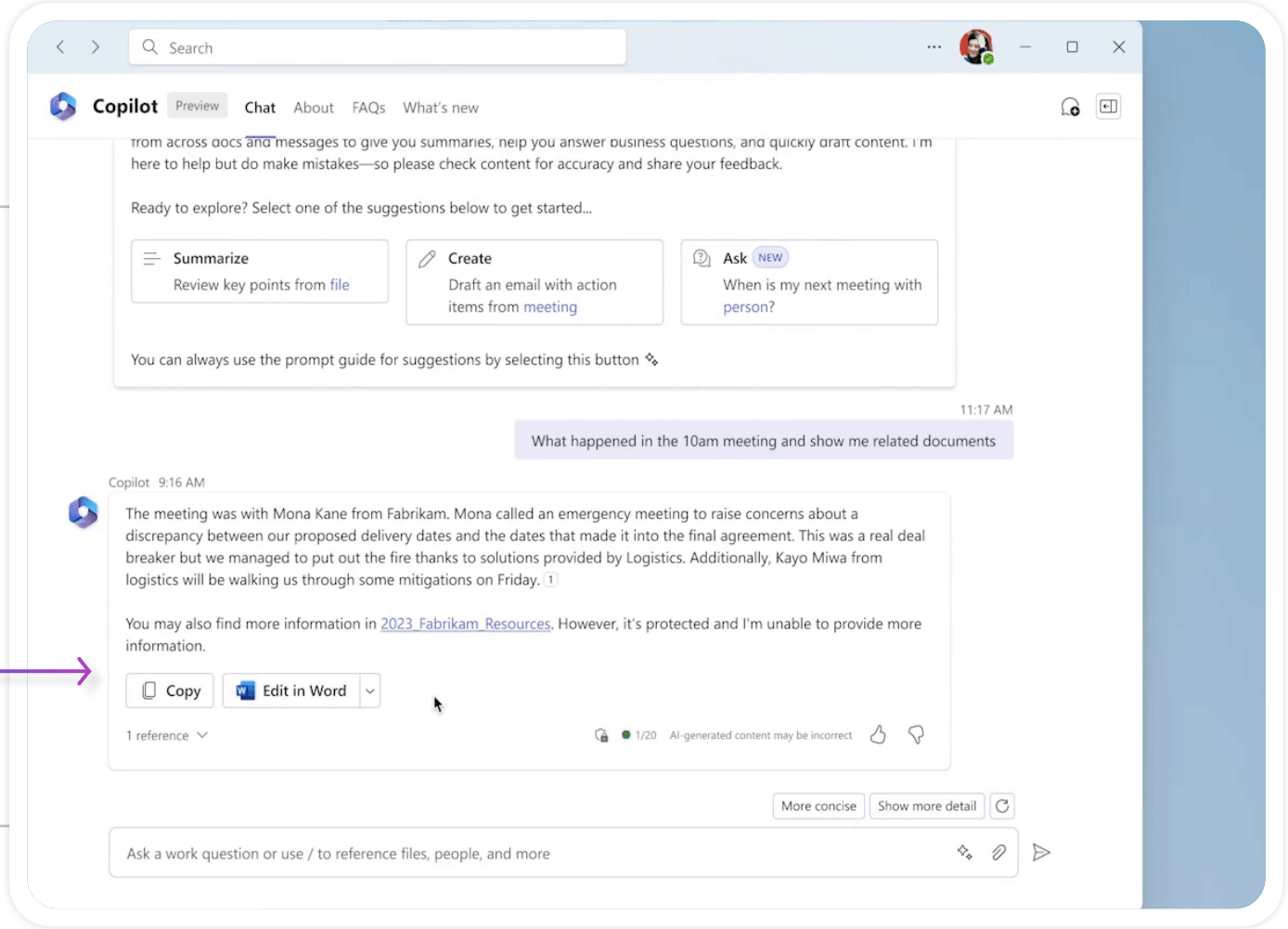
Conversations displays the **most restrictive sensitivity labels** from the references used to formulate a response.



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.**

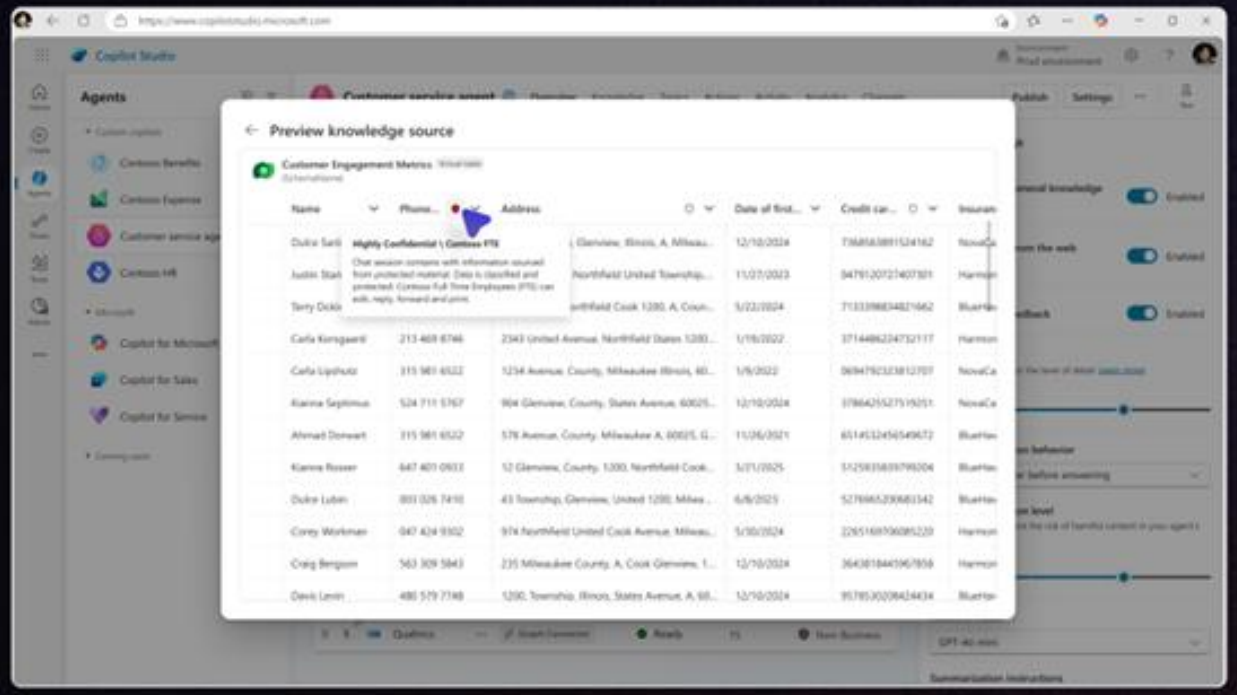


Copilot will not include information from referenced files where the user does not have appropriate access rights.

Introducing

Dataverse ❤ Purview

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



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

Discover risks and identify gaps

Activities

- Turn on Purview Audit
- Discover oversharing risks with Data risk assessment
- Discover sensitive info in Dataverse with Unified catalog
- Discover risky AI activities with DSPM for AI Apps and Agents report

Outcomes

Potential gaps in data security is discovered

Protect grounding data

Protect sensitive info in grounding data

Activities

- Apply sensitivity label to SharePoint and Dataverse
- Reduce stale data to improve response accuracy
- Restrict files from Copilot processing
- Implement data loss policies for SharePoint and Data policies for Dataverse

Outcomes

Sensitive info in grounding data is not used as knowledge source

Protect interactions

Protect interactions against data loss and insider risks

Activities

- Automatic sensitivity label reference from SharePoint and Dataverse
- Restrict Copilot from processing sensitive files referenced in interactions
- Detect Risky AI interactions

Outcomes

Interactions are protected from data loss and insider risk

Govern

Govern interactions

Activities

- Retain/delete interactions
- Detect inappropriate behaviors
- Investigate prompts and responses
- Investigate grounding data and interactions
- Identify & address gaps in meeting AI regulations

Outcomes

Interactions with agents is retained for future investigations

Last updated: September 15, 2025

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

Microsoft

Thank you

Microsoft Deployment models

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