Microsoft

Secure 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

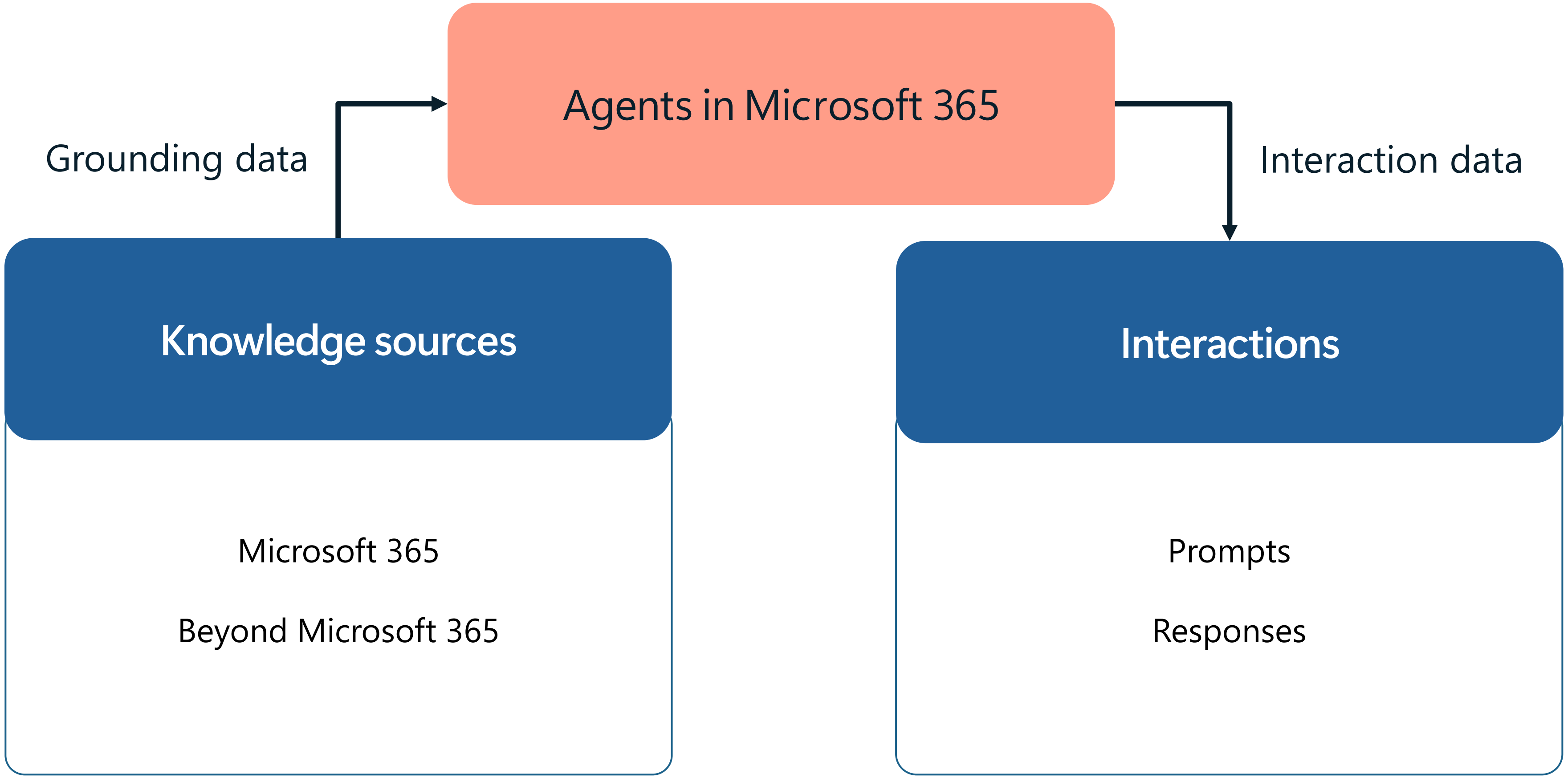
Unstructured & Structured data | **Traditional and AI generated data** | **Microsoft 365 and Multi-cloud**

Shared Capabilities Value

Data Map ● Connectors ● Classification ● Labels ● Audit ● Visibility

Microsoft Purview

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



Agents in Microsoft 365

Grounding data

Interaction data

Knowledge sources

Microsoft 365

Beyond Microsoft 365

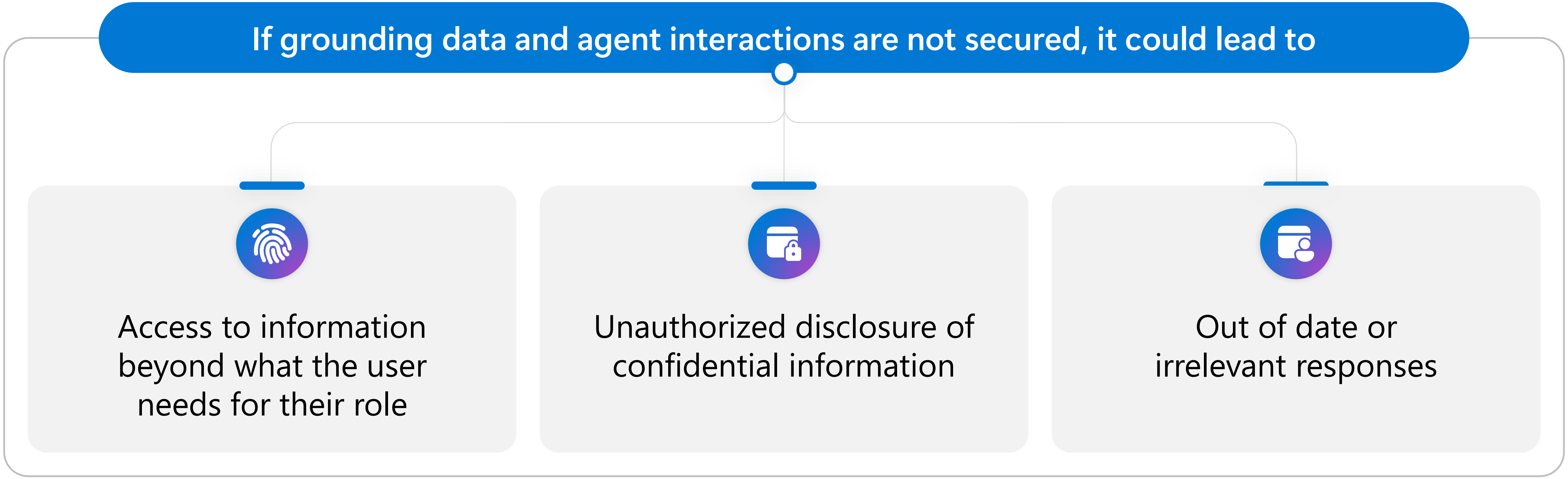
Interactions

Prompts

Responses

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

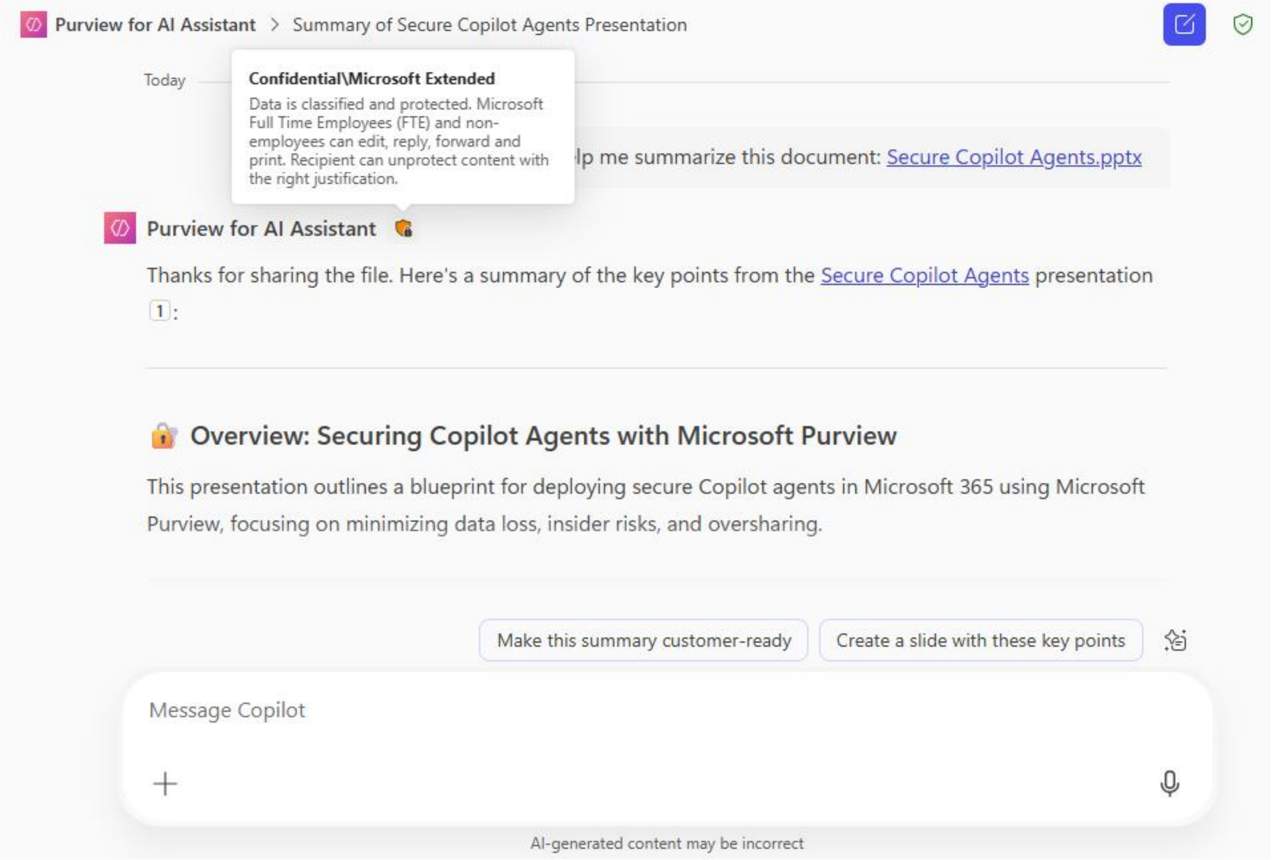
- Access to information beyond what the user needs for their role
- Unauthorized disclosure of confidential information
- Out of date or irrelevant responses

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

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

A sensitivity label applies to the **entire conversation.**

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



Purview for AI Assistant > Summary of Secure Copilot Agents Presentation

Today

Confidential\Microsoft Extended

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.

lp me summarize this document: Secure Copilot Agents.pptx

Purview for AI Assistant

Thanks for sharing the file. Here's a summary of the key points from the Secure Copilot Agents presentation 1:

🔒 **Overview: Securing Copilot Agents with Microsoft Purview**

This presentation outlines a blueprint for deploying secure Copilot agents in Microsoft 365 using Microsoft Purview, focusing on minimizing data loss, insider risks, and oversharing.

Make this summary customer-ready
Create a slide with these key points
Message Copilot
+

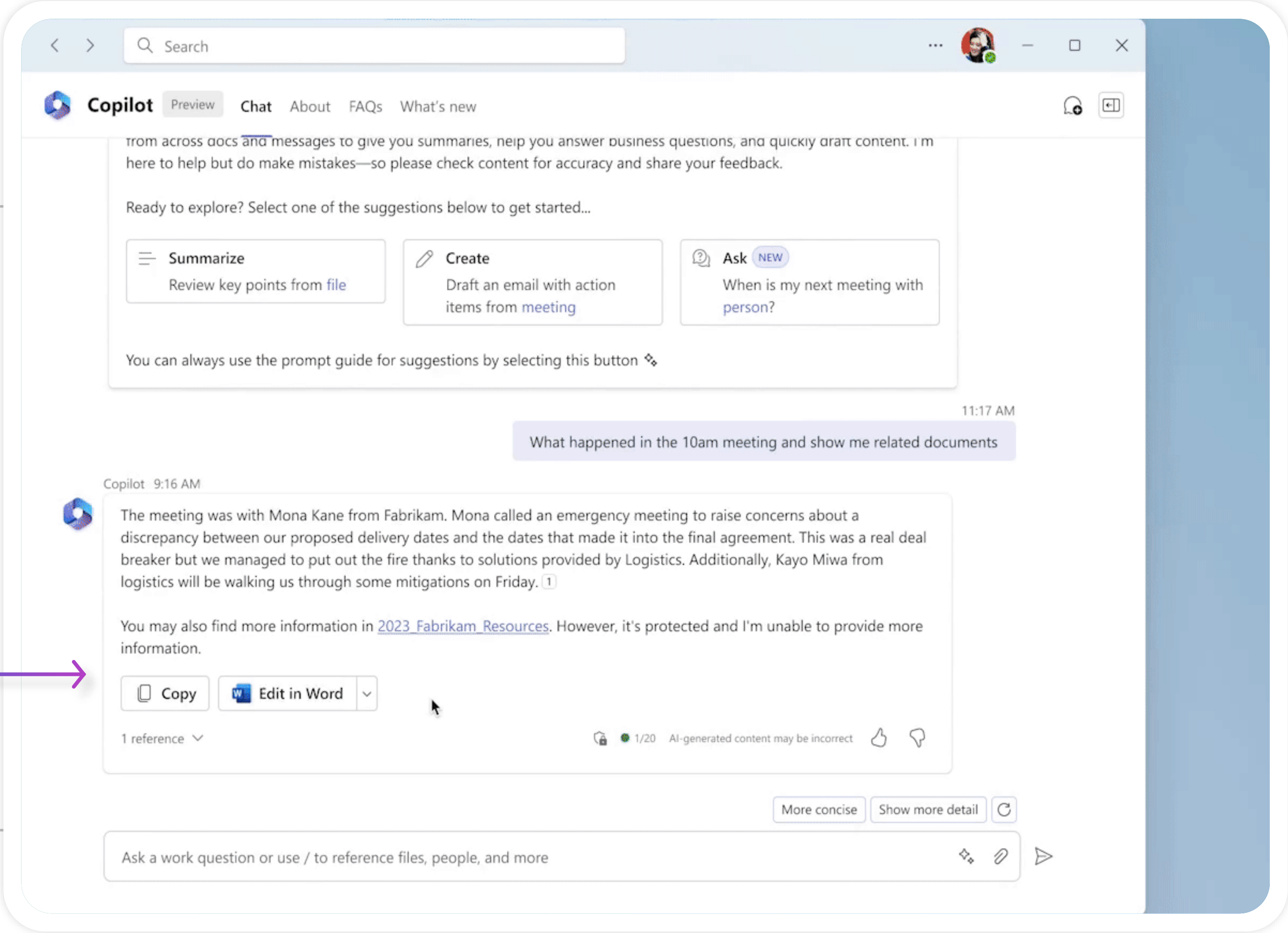
AI-generated content may be incorrect

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.


Search
Copilot
Preview
Chat
About
FAQs
What's new

from across docs and messages to give you summaries, help you answer business questions, and quickly draft content. I'm here to help but do make mistakes—so please check content for accuracy and share your feedback.

Ready to explore? Select one of the suggestions below to get started...

Summarize
Review key points from file
Create
Draft an email with action items from meeting
Ask NEW
When is my next meeting with person?

You can always use the prompt guide for suggestions by selecting this button

11:17 AM

What happened in the 10am meeting and show me related documents

Copilot 9:16 AM

The meeting was with Mona Kane from Fabrikam. Mona called an emergency meeting to raise concerns about a discrepancy between our proposed delivery dates and the dates that made it into the final agreement. This was a real deal breaker but we managed to put out the fire thanks to solutions provided by Logistics. Additionally, Kayo Miwa from logistics will be walking us through some mitigations on Friday. 1

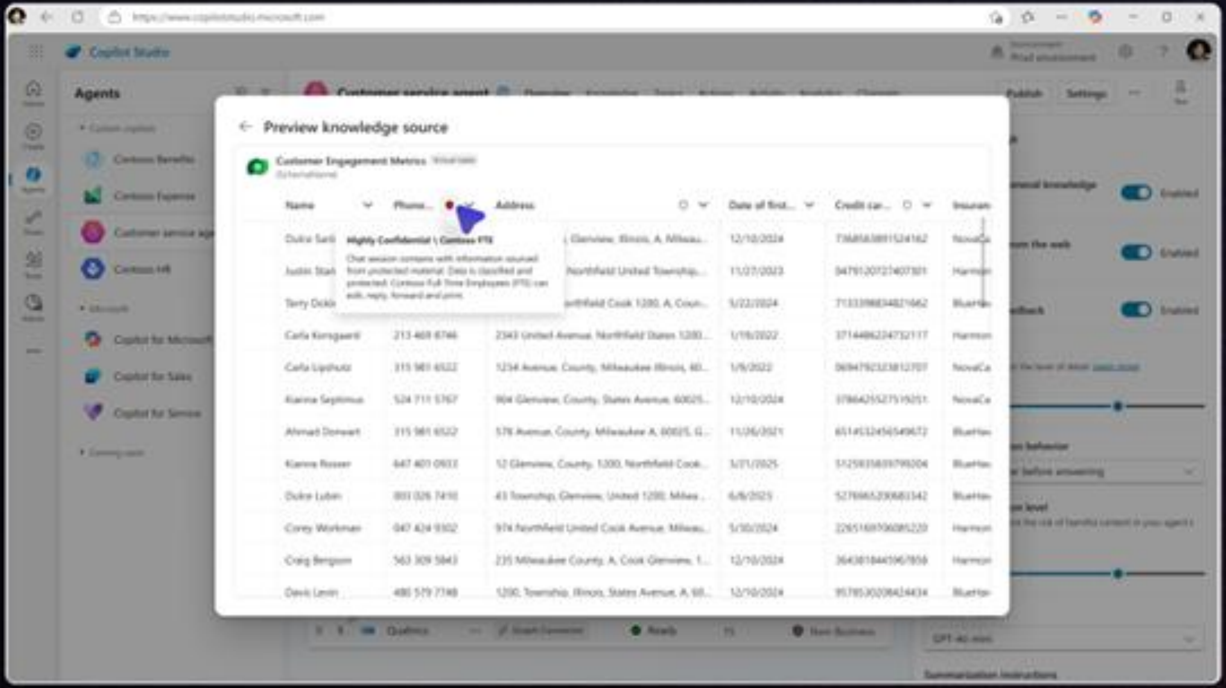
You may also find more information in 2023_Fabrikam_Resources. However, it's protected and I'm unable to provide more information.

Copy
Edit in Word
1 reference
1/20
AI-generated content may be incorrect
More concise
Show more detail
Ask a work question or use / to reference files, people, and more

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 \ Contoso FTE

Chat session contains with information sourced from protected material. Data is classified and protected. Contoso Full Time Employees (FTE) can edit, reply, forward and print.

Name	Phone...	Address	Date of first...	Credit car...	Insuran
Dulce Sari		, Glenview, Illinois, A, Milwau...	12/10/2024	7368563891524162	NovaCa
Justin Stan		Northfield United Township...	11/27/2023	8479120727407301	Harmon
Terry Dickk		orthfield Cook 1200, A, Coun...	5/22/2024	7133398834821662	BlueHa
Carla Korsgaard	213 469 8746	2343 United Avenue, Northfield States 1200...	1/19/2022	3714486224732117	Harmon
Carla Lipshutz	315 981 6522	1234 Avenue, County, Milwaukee Illinois, 60...	1/9/2022	0694792323812707	NovaCa
Kianna Septimus	524 711 5767	904 Glenview, County, States Avenue, 60025...	12/10/2024	3786425527519251	NovaCa
Ahmad Dorwart	315 981 6522	578 Avenue, County, Milwaukee A, 60025, G...	11/26/2021	6514532456549672	BlueHa
Kianna Rosser	647 401 0933	12 Glenview, County, 1200, Northfield Cook...	3/21/2025	5125835839799204	BlueHa
Dulce Lubin	803 026 7410	43 Township, Glenview, United 1200, Milwa...	6/8/2025	5276965230683342	BlueHa
Corey Workman	047 424 9302	974 Northfield United Cook Avenue, Milwau...	5/30/2024	2265169706085220	Harmon
Craig Bergson	563 309 5843	235 Milwaukee County, A, Cook Glenview, 1...	12/10/2024	3643818445967858	Harmon
Davis Levin	480 579 7748	1200, Township, Illinois, States Avenue, A, 60...	12/10/2024	9578530208424434	BlueHa

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 agents in Microsoft 365 with Microsoft Purview

Activities

Discover

Discover risks and identify gaps

- Turn on Purview Audit
- Discover SPO 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

Protect grounding data

Protect sensitive info in grounding data

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

Protect interactions

Protect interactions against data loss and insider risks

- Automatic sensitivity label inheritance from SharePoint and Dataverse
- Restrict Copilot from processing sensitive files referenced in interactions with DLP for Copilot
- Detect Risky AI interactions with IRM Risky AI policy

Govern

Govern interactions

- Retain/delete interactions with DLM policies
- Detect inappropriate behaviors with CC policies
- Investigate cases with eDiscovery
- Investigate grounding data and interactions with DSI
- Identify & address gaps in meeting AI regulations with CM

Outcomes

- Potential gaps in data security is discovered
- Sensitive info in grounding data is not used as knowledge source
- Interactions are protected from data loss and insider risk
- Interactions with agents is retained for future investigations

Last updated: August 26, 2025

Discover

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

Protect grounding data

- Apply sensitivity label to SharePoint and Dataverse
- Reduce stale data to improve agent response accuracy with Purview Data Lifecycle Management (DLM)
- Restrict sensitive files labeled with specific sensitivity labels from Copilot processing and acting as knowledge source with 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 inherited 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 Purview Insider risk management (IRM)’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 Purview DLM policies
- Detect inappropriate behaviors with Purview Communication Compliance (CC) policies with built-in classifiers such as jailbreak, harassment, inappropriate images, etc.
- Investigate legal and internal cases with Purview eDiscovery
- Investigate interactions and grounding data leveraging the power of AI with Purview Data security investigations (DSI)
- Identify & address gaps in meeting AI regulations with Purview Compliance Manager (CM)

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