

Secure and govern Microsoft 365 Copilot

Protect Copilot with
Microsoft Purview



Generative AI introduces new threats

Generative AI is transforming the workplace, but it's also creating an ever-evolving AI threat landscape with critical risk areas such as data leaks, emerging threats and vulnerabilities, and regulatory non-compliance. These threats amplify existing security risks like data loss and insider risks. They also introduce new threats, such as prompt injection attacks and copyright violations.

60%

of companies lack the tools to counter today's AI-enabled threats.¹

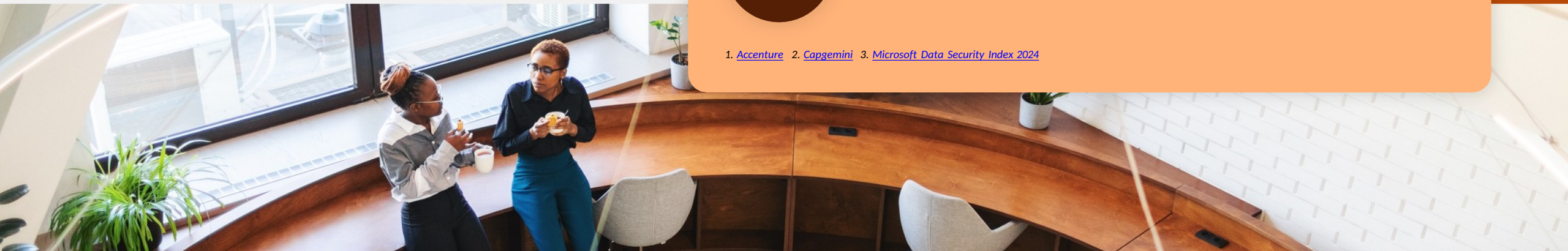
67%

of organizations have encountered breaches related to generative AI use.²

84%

of organizations lack confidence managing data input in AI apps and tools.³

1. [Accenture](#) 2. [Capgemini](#) 3. [Microsoft Data Security Index 2024](#)



[BACK](#)

[NEXT](#)

AI-powered Microsoft 365 Copilot: Secure by design

Customers trust Microsoft 365 Copilot with their sensitive data. Built on a foundation of secure and responsible AI, Microsoft 365 offers industry-leading security and governance capabilities and tools to help organizations manage risks.

Microsoft 365 also provides a time-tested approach to data privacy, grounded in a commitment to give you control over the data.

To ensure you can responsibly manage and protect your Microsoft 365 Copilot data, you need to be able to quickly identify risky AI use, such as when a user suddenly begins interacting with a large volume of sensitive data. Additionally, you need insights into prompts and responses to ensure you remain compliant with your organization's use policies.



Mitigating risks when scaling Microsoft 365 Copilot

Microsoft 365 Copilot helps users generate content based on what they have permission to access.

To mitigate risk means moving beyond reactive oversight and embracing proactive governance. This ensures that the data fueling Microsoft 365 Copilot is consistently managed, appropriately labeled, and securely protected.

To completely secure and govern Microsoft 365 Copilot requires:

Preventing data oversharing and leaks.

Detect potential oversharing risks and get actionable policy recommendations.

Identifying risky AI.

Protect against data loss and insider risks with proactive alerts and adaptive protection.

AI governance and risk visibility.

Help ensure Copilot and AI agent usage complies with regulations, organizational policies, and ethical guidelines.



[BACK](#)

[NEXT](#)





A complete solution to secure and govern Microsoft 365 Copilot

Gain risk visibility, enforce data protection, and apply governance controls with Microsoft Purview.

This comprehensive set of solutions helps your organization govern, protect, and manage Microsoft 365 Copilot data across your entire data estate. A unified view offers a simplified approach to your data protection strategy that addresses the fragmentation of data and ensures compliance.



How Microsoft Purview helps Microsoft 365 Copilot:



Addresses oversharing concerns



Protects against data loss and insider risks



Governs AI use to meet regulations and policies



[BACK](#)

[NEXT](#)

Address oversharing concerns

Detect potential oversharing risks and get actionable policy recommendations.



Microsoft Purview helps you identify potentially overshared sites and files across all of Microsoft 365.

Receive and act on policy suggestions to mitigate your specific oversharing risks. Remove organization-wide site access as needed. Get notifications when new oversharing occurs with options for remediation. Microsoft Purview protects sensitive files wherever they live or travel.



Key features:



Prevention of processing sensitive files



Remediation of excessive permissions



Visibility into overshared content



[BACK](#)

[NEXT](#)

Protect against data loss and insider risks

Analyze interactions with sensitive data, get alerts about risky activity, and adjust policies dynamically based on risk.



Microsoft Purview prevents data leaks by letting you view reports of sensitive data and unprotected files, get alerts to risky use, and detect when files contain sensitive data and auto-apply protections. You can also protect files even if they are moved or downloaded. And with Microsoft Purview Insider Risk Management, you can limit access for high-risk users.

Key features:

Alerts and reports
of risky behavior
and AI use

Protection of
sensitive files and
interactions

Dynamic
application of
security policies
based on risky
actions



[BACK](#)

[NEXT](#)



Govern AI use to meet regulations and policies

Help ensure Microsoft 365 Copilot usage complies with regulations, such as the EU AI Act, organizational policies, and ethical guidelines.



Microsoft Purview helps you audit Microsoft 365 Copilot interactions by accessing detailed log information. You can enforce retention and deletion policies for interactions and meeting recordings and transcripts. Additionally, you receive an alert if a possible compliance or ethical violation occurs, and you can start an investigation.

Key features:



Inspections of interaction content and audit logs



Investigations for compliance and ethical violations



Enforcement of lifecycle policies and legal holds



[BACK](#)

[NEXT](#)

A complete solution to secure and govern Copilot



Microsoft Purview helps organizations confidently adopt and scale Microsoft 365 Copilot and agents by addressing oversharing, preventing data loss, and enforcing governance aligned with evolving AI regulations.



"We use Microsoft Purview to help ensure content generated by Copilot is automatically classified and protected, limiting access to authorized users."

—Manjunatha Sivanna, IT Service Delivery Manager, Cummins



[BACK](#)

[NEXT](#)

Security for AI Assessment| Microsoft 365 Copilot

Are you ready for Microsoft 365 Copilot?

Assess your security and governance readiness and get tailored recommendations that help empower you to prepare your Microsoft 365 environment, detect risks, and protect and govern Microsoft 365 Copilot use.

[Learn more](#)

Resources

1

[Use Microsoft Purview to manage data security & compliance for Microsoft 365 Copilot & Microsoft 365 Copilot Chat](#)

2

[Microsoft Purview protections for Copilot](#)

3

[Oversharing Control at Enterprise Scale | Updates for Microsoft 365 Copilot in Microsoft Purview](#)



[BACK](#)