

Minimize oversharing risks

Ensure trusted access to Microsoft 365 files with visibility into oversharing.

 Microsoft Security



More and more organizations are turning to Microsoft 365 Copilot as their trusted generative AI solution for working with sensitive organizational data. While Microsoft 365 Copilot honors existing user permissions, companies need to prevent oversharing or access to information beyond what is necessary to perform any job.

46%

of US workers upload sensitive data to public AI platforms.¹

24%

of current generative AI projects have a security component.²

60%

of AI-related security incidents lead to compromised data.³

A complete solution to secure and govern Copilot

Detect potential oversharing risks and get actionable policy recommendations. With Microsoft Purview, you proactively surface and remediate oversharing risks before Copilot adoption scales. Enhanced visibility helps deliver actionable policy recommendations, restrict broad access, and remove organization-wide permissions. Access controls ensure that your people have correct file access aligned with their role.



Microsoft Purview helps you:



Gain visibility into overshared content



Remediate identified oversharing permissions.



Prevent from processing certain sensitive files.



We can help you set up a complete solution to secure and govern Microsoft 365 Copilot.

[Learn more](#)

¹. KPMG.
². Cost of a Data Breach Report 2025, IBM, 2025.
³. Securing generative AI, IBM, May 2024.