

Stay ahead of AI risk with Microsoft Copilot auditing

[Tour Copilot](#)

Companies are steadily adopting AI-assisted technology like Microsoft Copilot to support productivity objectives. Yet default data access permissions and system connectivity inadvertently put organizations at risk of data leaks, data privacy violations, and prompt injection attacks.

Cavelo's Copilot Readiness reporting feature scans for overly permissive sharing settings on files with PII, audits Copilot interactions to detect potential risks, and leverages CIS benchmarks for Microsoft O365 to support configuration hardening.

Identify PII at risk of unintended access

Audit Microsoft Copilot interaction with critical or sensitive data.



Track AI access

Monitor files used by Microsoft Copilot and PII data associated with those files



Audit file sharing

Understand which files containing PII have anonymous share links






Understand risk exposure

Compile scan results to understand where Copilot can read sensitive data

CAPABILITIES

What you can expect:

- ✓ **Discovery** — Discover anonymous share links affecting PII in your Microsoft O365 environment.
 - ✓ **Benchmarking** — Evaluate your Microsoft O365 for default file sharing behavior, MFA policies, and more with CIS benchmark scanning; then follow remediation steps to harden your cloud security posture.
 - ✓ **Visibility** — Easily identify files with PII and/or Microsoft sensitivity labels that can be accessed by users with Microsoft Copilot.
 - ✓ **System and file interaction** — Understand and report on files that Microsoft Copilot has interacted with, as well as the entity associated with that interaction.

Anonymously Linked Resources						 Generate a Spreadsheet Report
Source	Type	Resource	Classifications	MSIP Labels	Entity	Permissions
DunderO365	File	/User/OneDrive/employee-travel-info.docx	Passport	Confidential	 Anyone with the generated sharing link	Edit
DunderO365	File	/User/OneDrive/marketing-plan-final.docx			 Anyone with the generated sharing link	Read



“When it comes to understanding our customers’ data access, the Microsoft Copilot Readiness Report helps us identify what data is affected by Microsoft Copilot while providing greater understanding of what our customers’ data posture risk looks like.”

Steven Schoener
Chief Technology Officer



Cavelo empowers businesses to proactively reduce their cyber risk and liability. Its consolidated attack surface management platform combines sensitive data and asset discovery, access management, and risk-based vulnerability management to simplify governance and compliance initiatives and risk remediation. For more information, visit www.cavelo.com.

Schedule a Demo