AI exposure report

Prepared for Northwind Trading by AILeakShield · Checked 11/2/2026, 10:00:00 AM

At a glance

Microsoft 365: 7 AI apps connected, with 1 ranked Critical and 6 ranked High.

Network: In the DNS logs reviewed, 21 of 60 users contacted 5 AI services, making up 8.44% of queries.

7 AI apps are connected to your Microsoft 365. 6 can reach email, files, chats or meetings. 1 holds permissions that work with nobody signed in.

1 Critical risk	**6** High risk
6 AI apps that can reach company data	**1** Work with nobody signed in
26 People who connected AI apps themselves	**4** Publisher not verified by Microsoft

Who can connect new apps
Anyone can connect apps
Staff can give any app access to their company data without an admin.

Microsoft 365 Copilot
12 of 25 seats assigned
Copilot reads what each person can already open, so old file sharing becomes easier to find.

Teams apps your organization published
1 AI of 1 published
Quillmeet AI Notetaker

1 AI Contract Review — Critical — Possibly AI

Can read files across your whole organization, with nobody signed in.

Works with nobody signed in · Approved for the whole organization · Publisher not verified by Microsoft

Its name suggests an AI tool. First seen 10/3/2026.

`Files.Read.All Sites.Read.All`

2 Mailpilot AI Assistant — High — Possibly AI

Can read and change email and calendars and send email for the 2 people who connected it.

Can send email as your people · Publisher not verified by Microsoft

Its name suggests an AI tool. First seen 10/3/2026.

`openid profile Mail.ReadWrite Mail.Send Calendars.ReadWrite`

3 ChatGPT — High — AI app

Can read files for the 22 people who connected it.

Non-US data residency and Zero Data Retention both require OpenAI approval, and regional storage does not by itself guarantee regional processing.

Published by OpenAI, verified by Microsoft. Vendor: OpenAI. Verified publisher: OpenAI. First seen 10/3/2026.

`openid profile Files.Read.All Sites.Read.All`

4 Askfile AI — High — Possibly AI

Can read files for the 4 people who connected it.

Publisher not verified by Microsoft

Its name suggests an AI tool. First seen 10/3/2026.

`openid profile Files.Read.All`

5 Quillmeet AI Notetaker — High — Possibly AI

Can read calendars, meetings and email for the 14 people who connected it.

Its name suggests an AI tool. Verified publisher: Quillmeet Inc. First seen 10/3/2026.

`openid profile Calendars.Read OnlineMeetings.Read Mail.Read`

6 **Transcrivo AI** High Possibly AI

Can read calendars and meetings for the 9 people who connected it.

Its name suggests an AI tool. Verified publisher: Transcrivo Ltd. First seen 10/3/2026.

`openid profile Calendars.Read OnlineMeetingTranscript.Read.All`

7 **Deckwright AI** High Possibly AI

Can read calendars for the 3 people who connected it.

Publisher not verified by Microsoft

Its name suggests an AI tool. First seen 10/3/2026.

`openid profile Calendars.Read User.Read`

What to do next

1. Start with the 7 apps ranked Critical or High. Remove access from anything your organization doesn't need.
2. 26 people connected AI apps on their own. Decide which of those tools you want to approve.
3. Check the 4 apps whose publisher Microsoft hasn't verified. Confirm each is the product it claims to be.
4. Anyone in your organization can connect any app to company data right now. In Microsoft Entra, limit user consent to verified publishers, or require admin approval.

This report shows what each app is allowed to do in Microsoft 365, not what it has done. Vendor details come from public sources and describe the vendor's default plan, so check them against your own contract. Microsoft's own apps are not listed.

AI USAGE & DATA-EXPOSURE ASSESSMENT

Northwind Trading

Prepared by AILeakShield · 11/2/2026

QUERIES ANALYZED	TO AI SERVICES	AI SERVICES SEEN	USERS REACHING AI
147,445	12,445 (8.44%)	5	21 of 60

AI services in use

SERVICE	QUERIES	% OF ALL TRAFFIC	USERS
OpenAI	7,800	5.29%	21
Microsoft (Copilot)	2,300	1.56%	16
Google (Gemini)	1,400	0.95%	11
Anthropic (Claude)	850	0.58%	7
DeepSeek	95	0.06%	2

Findings

HIGH **AI services are in active use, and OpenAI leads**

12,445 of 147,445 queries (8.44%) went to AI providers. OpenAI alone accounts for 7,800 queries (5.29%) from 21 distinct source(s).

MEDIUM **5 different AI services in use**

Traffic reached OpenAI, Microsoft (Copilot), Google (Gemini), Anthropic (Claude), DeepSeek. Multiple tools means no single vendor agreement or admin console covers the exposure.

HIGH **Traffic to AI services with non-US data handling (DeepSeek)**

Anything pasted into these services is processed outside the jurisdictions most customer and vendor agreements assume. This is usually the finding that carries the most weight with legal.

HIGH **AI use is organization-wide, not a few individuals**

21 of 60 source(s) in this log (35.0%) reached an AI service. At that spread, policy and training alone won't contain it. This is normal workflow now.

HIGH **No prompt-level inspection is in place**

DNS logs show which services were reached, never what was sent to them. Nothing in this environment inspects the content of an AI prompt, so there is currently no way to know whether customer records, credentials, or regulated data have been pasted into these tools, or to prove they haven't.

Recommendations

1. Publish an AI usage policy naming which tools are approved and for what data.
2. Brief staff on what must never be pasted into a public AI tool.
3. Decide per AI service whether to allow, restrict, or block it at the firewall, as an interim control while an approval process is agreed.
4. Give staff an approved AI workspace so the useful work continues somewhere governed, instead of moving to personal accounts and personal devices. NEEDS PROMPT-LEVEL DLP
5. Inspect prompts and block sensitive data before it is sent, on whichever AI tool the employee actually uses, not only an approved one. NEEDS PROMPT-LEVEL DLP
6. Keep an auditable record of what was blocked and what was overridden, so AI use can be evidenced to an auditor, insurer, or customer. NEEDS PROMPT-LEVEL DLP

Based on 147,445 log entries from `northwind-dns-october.csv`. DNS and proxy logs show which services were contacted, never what was sent to them, so this assessment establishes exposure, not whether a specific disclosure has occurred. The log was analyzed and discarded; only these aggregate figures were retained.