



YOUR LOGO

managed IT & security

CONFIDENTIAL

Shadow AI Assessment

AI tools observed in network traffic, matched against a register of 18,571 classified AI-tool domains. 13 risk factors evaluated per tool.

PREPARED FOR

Example Client Ltd

SCOPE

Export format: csv

Lines read: 400 | Distinct hostnames: 50

Report date: 2026-09-24 09:09

PREPARED BY

Your Company Ltd

security@yourcompany.example | +1 555 0100

www.yourcompany.example

Introduction

As part of our managed security service, we reviewed which AI tools your network reached over the last 30 days, using the export from your DNS filter. This report lists every AI tool we found, who used it, and whether the vendor trains on the data your staff type into it. Your intro goes here: this text is set on the branding page in your account.

Executive Summary

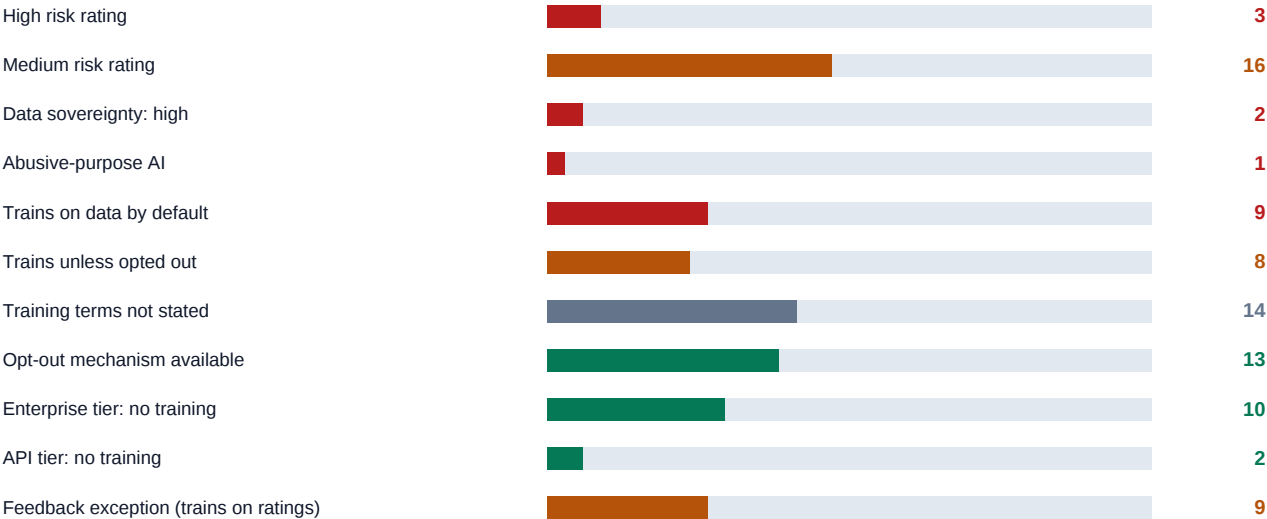


Priority Findings

- F1** 17 tools train on submitted data. 9 train by default on the consumer tier. 8 more train unless the user finds and disables the setting. Enterprise tiers with no-training guarantees exist for 10 of these.
- F2** 3 tools carry a high risk rating, including 1 abusive-purpose destinations (deepfake, nudify, nsfw or uncensored). 2 with data-sovereignty exposure under jurisdictions flagged high.
- F3** 34 of the 34 tools found are not on the organisation's sanctioned list. 0 are sanctioned.
- F4** Most exposed users: desktop-support-03, laptop-marketing-01, laptop-exec-01. The highest reached 23 AI tools with 36 hits.

Risk Factor Profile: 13 Factors

Each AI tool in the register is evaluated against 13 risk factors. Bars show how many of the 34 tools found in this export carry each factor.



Human review of content		9
Subprocessor may train		0
2 offer a zero-retention option.		

Tools by Category

Category	Tools
Text & Language	6
Code & Development	5
Audio, Voice & Music	5
Productivity & Collab	4
Agents & Automation	4
Image & Visual	4
Search, Knowledge & Docs	2
Customer Support	1
Business & Vertical	1
Robotics & Embodied AI	1
Models & Infrastructure	1

AI Tools Observed

Domain	Category	Risk	Sov.	Training	Opt-Out	Ent.Tier	Verdict	Hits	Users
google.com	Productivity & Collab	med	low	Opt-out	Yes	-	Controls	35	9
microsoft.com	Code & Development	med	low	Trains	-	Yes	Controls	31	10
salesforce.com	Customer Support	low	low	Unstated	-	-	Controls	19	9
windows.com	Audio, Voice & Music	med	low	Trains	-	-	Controls	16	9
googleapis.com	Productivity & Collab	low	low	Unstated	-	-	Controls	13	7
grammarly.com	Productivity & Collab	med	low	Trains	Yes	-	Controls	12	8
dropbox.com	Search, Knowledge	low	low	Unstated	-	-	Controls	11	8
openai.com	Code & Development	med	low	Opt-out	Yes	Yes	Controls	10	7
character.ai	Text & Language	med	low	Trains	-	-	Block	10	8
github.io	Agents & Automation	med	low	Opt-out	Yes	-	Block	10	8
replit.com	Text & Language	low	low	Unstated	-	-	Controls	10	9
claude.ai	Business & Vertical	med	low	Opt-out	Yes	Yes	Controls	10	8
slack.com	Text & Language	low	low	Unstated	Yes	No	Controls	10	5
zapier.com	Agents & Automation	med	low	Opt-out	Yes	Yes	Controls	7	5
github.com	Agents & Automation	med	low	Opt-out	Yes	Yes	Controls	7	5
suno.com	Audio, Voice & Music	med	low	Trains	-	-	Block	7	5
canva.com	Image & Visual	low	low	Unstated	Yes	-	Allow	7	7
otter.ai	Audio, Voice & Music	med	low	Trains	-	-	Block	7	6
deepfakemaker.io	Image & Visual	high	low	Unstated	-	-	Block	6	5
cursor.com	Code & Development	low	low	No	Yes	Yes	Controls	6	5

Domain	Category	Risk	Sov.	Training	Opt-Out	Ent.Tier	Verdict	Hits	Users
runwayml.com	Image & Visual	med	low	Trains	-	-	Controls	6	4
midjourney.com	Image & Visual	low	low	Unstated	-	-	Allow	5	4
kimi.com	Code & Development	high	high	Unstated	-	-	Block	5	3
notion.so	Productivity & Collab	low	low	No	-	Yes	Controls	5	5
huggingface.co	Robotics & Embodie	low	low	Unstated	-	No	Allow	5	5
deepseek.com	Code & Development	high	high	Trains	Yes	-	Block	4	3
elevenlabs.io	Audio, Voice & Music	med	low	Opt-out	Yes	-	Block	4	4
fireflies.ai	Audio, Voice & Music	low	low	No	No	Yes	Controls	3	2
deepl.com	Text & Language	med	low	Trains	-	Yes	Controls	2	2
poe.com	Text & Language	low	low	Unstated	-	-	Controls	2	2
perplexity.ai	Search, Knowledge	low	low	Unstated	-	-	Controls	2	2
groq.com	Models & Infrastructu	low	low	Unstated	-	-	Controls	2	2
manus.im	Agents & Automation	low	low	Unstated	-	-	Controls	2	1
lovable.dev	Text & Language	med	low	Opt-out	Yes	Yes	Controls	1	1

Users and Devices Reaching AI Tools

Source	Tools	Hits	Most used
desktop-support-03	23	36	microsoft.com, slack.com, windows.com, suno.com
laptop-marketing-01	18	35	microsoft.com, kimi.com, googleapis.com, grammarly.com
laptop-exec-01	19	32	googleapis.com, google.com, microsoft.com, deepseek.com
laptop-sales-09	15	30	google.com, microsoft.com, github.io, salesforce.com
laptop-finance-02	19	29	google.com, salesforce.com, manus.im, zapier.com
laptop-eng-07	20	28	openai.com, google.com, github.io, claude.ai
laptop-legal-01	19	27	google.com, dropbox.com, windows.com, microsoft.com
laptop-eng-11	17	27	google.com, windows.com, microsoft.com, github.com
laptop-marketing-02	18	24	salesforce.com, replit.com, character.ai, deepfakemaker.io
laptop-hr-01	15	24	microsoft.com, google.com, grammarly.com, github.io

Recommendations

- 1. Block the high-risk tools listed in this report at the DNS filter this week.
 - 2. Move ChatGPT users to an enterprise workspace with no-training terms.
 - 3. Publish an AI acceptable-use policy and share it with all staff.
 - 4. Re-run this assessment next quarter and compare the results.
- (Your recommendations go here. They are also set on the branding page.)

Control Evidence Statement

This report is generated from the organisation's own DNS, proxy or firewall export and a register of 18,571 classified domains. Each matched domain is evaluated against 13 risk factors: risk rating, data-sovereignty exposure, abusive-purpose flag, training on user data, opt-out availability, enterprise and API tier training exclusions, opt-out scope, feedback exceptions, monitoring retention, de-identified data use, human review of content, zero-retention availability and subprocessor training terms, with the date each vendor's terms were last checked.

File this as the AI-usage control inventory for the audit period, together with the enforcement configuration that references the blocklist. The uploaded export was processed in memory and discarded. Only this report is retained, for 90 days, in the account that produced it.