YOUR LOGO

SAMPLE REPORT

CONFIDENTIAL

Shadow AI Assessment

AI tools reached from your network, the risk behind each one, and a plan to bring them under control.

PREPARED FOR

Example Industries Inc.

37	6	9	84
AI TOOLS	HIGH RISK	TO BLOCK	EXPOSURE INDEX

Evidence
5,693 log lines

Prepared by
Your Company Ltd
security@yourcompany.example

Date
27 September 2026

INTRODUCTION

About this assessment

We reviewed the network export your team provided and matched every hostname against a verified register of AI tools.

This assessment shows which AI tools are in use, the risk each one carries and the plan we recommend. Your own introduction goes here in a white-label report.

01 · EXECUTIVE SUMMARY

37 AI tools in use. 9 should be blocked.

We read 5,693 lines of your CSV network export, matched 72 hostnames against 11,890 verified AI tools, and scored each tool on risk, data handling and training terms.

AI EXPOSURE INDEX



84

Severe exposure

0 = no unmanaged AI · 100 = severe

37
AI tools found

6
high-risk tools

27
may train on your data

32
not on your approved list

24
people or devices using AI

29
other services left alone

What we found

01 **32 of 37 AI tools in use are not on your approved list**
5 tools are sanctioned. The rest reached the network without review.

02 **27 tools may train models on what your staff type**
12 train by default and 15 unless someone opts out. 1 vendor does not say.

03 **6 high-risk tools, including deepseek.com, kimi.com, manus.im**
High data-sovereignty exposure, abusive-purpose generators or training by default.

04 **9 tools should be blocked under the General business rules**
28 can stay with controls (business plan, SSO, no-training terms); 0 are fine as they are.

05 **29 other services in your log were left alone**
Only verified AI tools are flagged. Everyday business services are never counted as AI tools.

Recommended policy under the **General business** rules



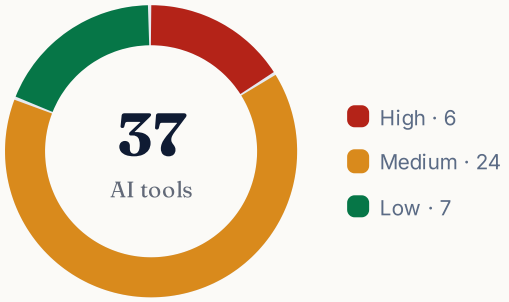
Block · 9 Allow with controls · 28 Allow · 0

02 · RISK LANDSCAPE

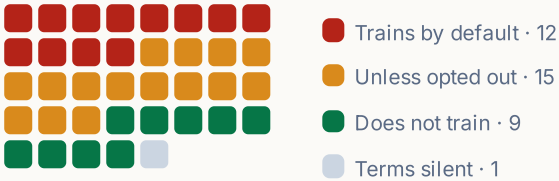
Where the risk sits

Every tool is rated in the register: jurisdiction and data sovereignty, abusive-purpose generators, and what the vendor's own terms say about training on user data.

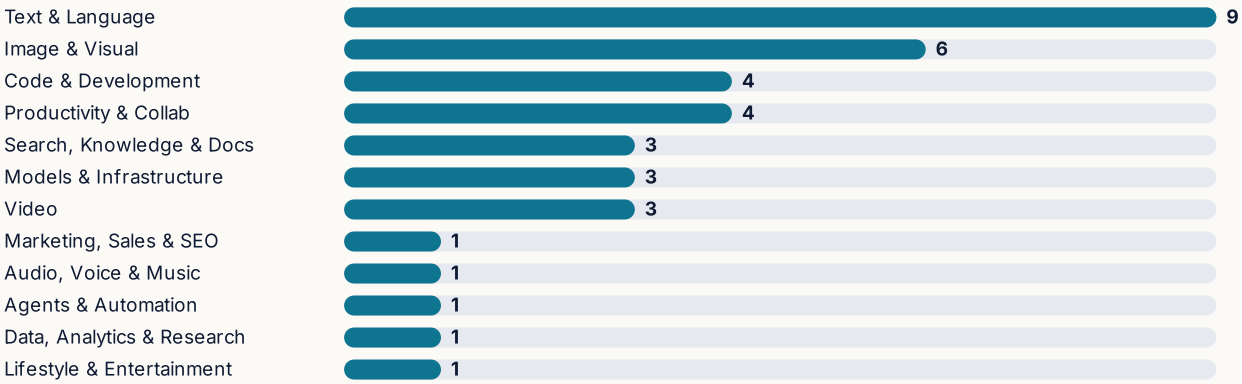
Risk level



Training on user data (one square = one tool)



AI tools by category



6
tools with high data-sovereignty exposure

1
abusive-purpose tools (deepfake, nudify, adult)

34 / 3
AI-native tools / AI features inside other apps

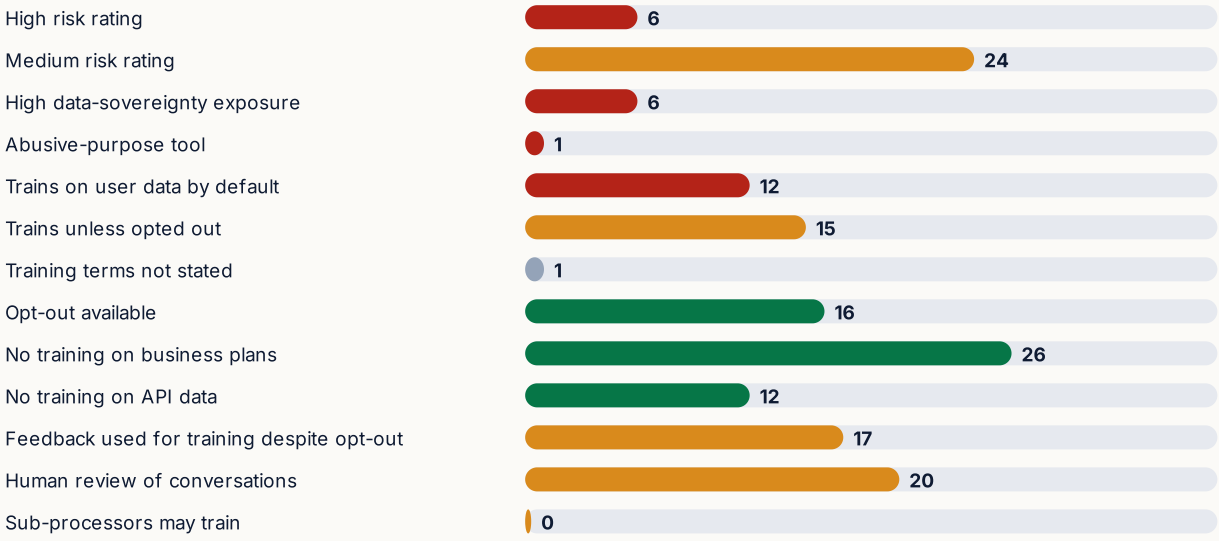
Highest-risk tools and why

TOOL	WHY IT IS RATED HIGH	USERS	VERDICT
deepseek.com	High data-sovereignty exposure: data held under a high-risk jurisdiction	2	Block
kimi.com	High data-sovereignty exposure: data held under a high-risk jurisdiction	1	Block
manus.im	High data-sovereignty exposure: data held under a high-risk jurisdiction	2	Block
seaart.ai	High data-sovereignty exposure: data held under a high-risk jurisdiction	1	Block

03 · RISK FACTOR PROFILE

13 risk factors, tool by tool

Each AI tool in the register is evaluated against 13 factors taken from its jurisdiction, purpose and the vendor's own published terms. The bars show how many of the 37 tools found carry each factor.



How to read this

Red factors raise risk on their own. Amber factors need a decision: a tool that trains unless opted out is acceptable only if someone switches it off for every account. Green factors are protections you can use, such as business plans that exclude training or an opt-out switch.

What "not stated" means

1 of the tools found do not say whether they train on user data. Silence is not proof that they do, but it gives you nothing to rely on. Treat these tools as "may train" until the vendor confirms otherwise in writing.

3 of the tools offer a zero-retention option; 0 may use de-identified data to improve their service.

04 · TEAMS AND PEOPLE

Who uses what

Your export included user names, so the report shows AI use by team. We see which services were reached, never what anyone typed.

Risk by team (tools at each risk level; people in brackets)

	HIGH RISK	MEDIUM	LOW	TOOLS
Other devices (1)	2	1		3
MKT (4)	1	11		12
ENG (5)	1	9	1	11
OPS (2)	1	5	1	7
LEGAL (1)	1	5		6
SALES (3)		7	1	8
HR (2)		7		7
EXEC (2)		6		6
FIN (2)		4	2	6
SUP (2)		3	2	5

Most active users

USER OR DEVICE	AI TOOLS	HIGH-RISK	REQUESTS	MOST USED
ENG\d.szabo	7	—	188	grammarly.com, v0.dev, cursor.com, perplexity.ai
HR\f.laurent	6	—	164	grammarly.com, otter.ai, quillbot.com, claude.ai
SALES\b.moreau	7	—	153	deepl.com, perplexity.ai, grammarly.com, writesonic.com
OPS\h.almeida	7	1	146	chatgpt.com, fireflies.ai, grammarly.com, claude.ai
ENG\n.acar	5	1	144	windsurf.com, deepseek.com, v0.dev, grammarly.com
MKT\s.haddad	6	—	142	remove.bg, suno.com, claude.ai, chatgpt.com
EXEC\o.sato	5	—	136	perplexity.ai, claude.ai, grok.com, grammarly.com
FIN\s.molnar	6	—	135	claude.ai, notebooklm.google, grammarly.com, deepl.com
MKT\m.ferreira	7	1	131	remove.bg, runwayml.com, midjourney.com, suno.com
LEGAL\v.rossi	6	1	121	kimi.com, deepl.com, chatgpt.com, claude.ai
SALES\r.nakamura	4	—	112	deepl.com, claude.ai, gamma.app, perplexity.ai
FIN\g.brunner	6	—	98	claude.ai, grammarly.com, notebooklm.google, chatgpt.com

04 · TEAMS AND PEOPLE (CONTINUED)

USER OR DEVICE	AI TOOLS	HIGH-RISK	REQUESTS	MOST USED
SUP\k.mensah	5	—	95	claude.ai, quillbot.com, deepl.com, poe.com
SALES\c.vandijk	4	—	83	writesonic.com, gamma.app, otter.ai, perplexity.ai
OPS\k.jensen	5	1	79	grammarly.com, deepl.com, perplexity.ai, manus.im
SUP\r.petrov	3	—	76	claude.ai, deepl.com, you.com
ENG\p.okafor	3	1	75	huggingface.co, grammarly.com, deepseek.com
EXEC\m.hartmann	3	—	65	napkin.ai, deepl.com, perplexity.ai
ENG\t.kowalski	4	—	57	windsurf.com, v0.dev, replit.com, deepl.com
MKT\a.okonkwo	3	—	55	grammarly.com, heygen.com, midjourney.com
ENG\j.lindqvist	3	—	44	mistral.ai, chatgpt.com, v0.dev
HR\e.walsh	3	—	43	claude.ai, chatgpt.com, perplexity.ai
MKT\l.duarte	3	—	29	remove.bg, midjourney.com, leonardo.ai
10.24.8.117	3	2	21	character.ai, seaart.ai, deepswap.ai

05 · AI TOOL INVENTORY

Every AI tool we found

Sorted by number of requests. Verdicts follow the General business rules. Sov. = data-sovereignty exposure. Training = what the vendor says about training on your data. Biz plan = whether business or enterprise plans are excluded from training. Controls = allow only with controls.

TOOL	CATEGORY	RISK	SOV.	TRAINING	BIZ PLAN	APPROVED	USERS	VERDICT
claude.ai	Text & Language	Medium	Low	Opt-out	No training	Yes	13	Controls
grammarly.com	Text & Language	Medium	Low	Opt-out	No training	Yes	12	Controls
deepl.com	Text & Language	Medium	Low	Trains	No training	No	14	Controls
perplexity.ai	Search, Knowledge...	Medium	Low	Opt-out	No training	No	11	Controls
chatgpt.com	Text & Language	Medium	Low	Opt-out	No training	Yes	10	Controls
remove.bg	Image & Visual	Medium	Low	Trains	—	No	3	Controls
v0.dev	Code & Development	Medium	Low	Opt-out	No training	No	4	Controls
gamma.app	Productivity & Collab	Medium	Low	Opt-out	No training	No	3	Controls
windsurf.com	Code & Development	Medium	Low	Trains	No training	No	2	Controls
writesonic.com	Marketing, Sales & ...	Low	Low	No training	No training	No	2	Controls
deepseek.com	Models & Infrastruc...	High	High	Opt-out	—	No	2	Block
notebooklm.google	Search, Knowledge...	Low	Low	No training	No training	No	2	Controls
suno.com	Audio, Voice & Music	Medium	Low	Trains	—	No	2	Block
otter.ai	Productivity & Collab	Medium	Low	Trains	No training	No	2	Controls
huggingface.co	Models & Infrastruc...	Low	Low	No training	—	No	2	Controls
quillbot.com	Text & Language	Medium	Low	Opt-out	No training	No	2	Controls
midjourney.com	Image & Visual	Medium	Low	Trains	—	No	4	Controls
heygen.com	Video	Medium	Low	Opt-out	No training	No	2	Controls
napkin.ai	Productivity & Collab	Medium	Low	Opt-out	Trains	No	1	Block
runwayml.com	Video	Medium	Low	Trains	No training	No	1	Controls
cursor.com	Code & Development	Medium	Low	Opt-out	No training	Yes	1	Controls

05 · AI TOOL INVENTORY (CONTINUED)

TOOL	CATEGORY	RISK	SOV.	TRAINING	BIZ PLAN	APPROVED	USERS	VERDICT
grok.com	Text & Language	Medium	Low	Opt-out	No training	No	1	Controls
kimi.com	Text & Language	High	High	Opt-out	No training	No	1	Block
manus.im	Agents & Automation	High	High	No training	No training	No	2	Block
mistral.ai	Models & Infrastruc...	Medium	Low	Opt-out	No training	No	1	Controls
fireflies.ai	Productivity & Collab	Low	Low	No training	No training	Yes	1	Controls
you.com	Search, Knowledge...	Low	Low	No training	No training	No	2	Controls
poe.com	Text & Language	Low	Low	No training	—	No	1	Controls
jasper.ai	Text & Language	Medium	Low	Trains	No training	No	1	Controls
replit.com	Code & Development	Medium	Low	Trains	No training	No	1	Controls
ideogram.ai	Image & Visual	Medium	Low	Trains	No training	No	1	Controls
julius.ai	Data, Analytics & R...	Low	Low	No training	No training	No	2	Controls
character.ai	Lifestyle & Entertai...	Medium	Low	Trains	—	No	1	Block
seaart.ai	Image & Visual	High	High	Not stated	—	No	1	Block
klingai.com	Video	High	High	Opt-out	—	No	1	Block
deepswap.ai	Image & Visual	High	High	No training	—	No	1	Block
leonardo.ai	Image & Visual	Medium	Low	Trains	No training	No	1	Controls

06 · WHAT TO DO NEXT

Your action plan

Three steps, based on the General business rules. Most teams complete all three in a day: the block list loads straight into your firewall or DNS filter.

STEP 1 · BLOCK NOW (9)

- **deepseek.com**
  High risk rating
- **suno.com**
  Audio, Voice & Music default; trains on user data by default
- **napkin.ai**
  Productivity & Collab default; trains unless opted out
- **kimi.com**
  High risk rating
- **manus.im**
  High risk rating
- **character.ai**
  AI companions & character chat
- **seaart.ai**
  High risk rating
- **klingai.com**
  High risk rating
- **deepswap.ai**
  Abusive-purpose AI (deepfake)

STEP 2 · ALLOW WITH CONTROLS (28)

Keep them, on a business plan with single sign-on and no-training terms:

- **claude.ai**
- **grammarly.com**
- **deepl.com**
- **perplexity.ai**
- **chatgpt.com**
- **remove.bg**
- **v0.dev**
- **gamma.app**
- **windsurf.com**
- **writesonic.com**
- **notebooklm.google**
- **otter.ai**
- **huggingface.co**
- **quillbot.com**
- **midjourney.com**
- **heygen.com**

+ 12 more in the inventory

STEP 3 · APPROVE AND TELL STAFF

Publish the approved list, name the approved alternative for each blocked tool, and re-run this audit after the change to confirm it worked.

Ready-made enforcement

The block list is available as ready-to-load files for Cisco Umbrella, Zscaler, Palo Alto, Fortinet, Cloudflare Gateway, Pi-hole and other formats, kept up to date daily.

RECOMMENDATIONS

Our recommendations

1. Block the Week 1 tools at the firewall this week.
2. Move the approved tools onto business plans with single sign-on and no-training terms.
3. Share the approved list with staff and name the alternative for each blocked tool.
4. We re-run this assessment in 30 days to confirm the controls work.

Your own recommendations go here in a white-label report.

07 · HOW THIS REPORT WAS MADE

Method and control evidence

11,890
verified AI tools in the register, each checked one by one

13
risk factors per tool, from each vendor's own published terms

15
industry policy profiles to choose from

What we check for each tool

- Category and whether AI is the product or a feature
- Risk level and the reason for it
- Data sovereignty and jurisdiction
- Abusive-purpose generators (deepfake, nudify, face-swap)
- Training on user data, opt-out and its scope
- Business-plan and API no-training terms
- Human review, retention and sub-processors
- The date the vendor terms were last read

About the exposure index

The index weighs high-risk tools, high data-sovereignty exposure, abusive-purpose generators, tools that train on user data and tools not on your approved list. It rises quickly with a few serious findings. Use it to compare the same organisation over time.

Privacy

Your export was read in memory and deleted. Only this report is kept, for 90 days, in the account that produced it. We see which services were contacted, never the content of anything sent.

Control evidence statement

This report is generated from the organisation's own DNS, proxy or firewall export (5,693 lines, 27 September 2026), matched against a register of 11,890 verified AI-tool domains. Each matched tool carries its category, risk rating, data-sovereignty flag, abusive-purpose flag and the vendor's stated training terms, with the date they were last read. It may be filed as the AI-usage inventory for the audit period, together with the enforcement configuration derived from it.

PRICES

Audit reports and plans

This page appears only in this public example. The reports you give your clients never include it and never mention us.

The same prices as on shadowaitools.com/pricing.php. Not ready to buy? The free preview costs nothing.

One-time audit reports

One network export per report, up to 2,000,000 lines. Credits never expire.

1 AUDIT REPORT

$99

The full report for one network: every tool named, users and teams, PDF and CSV.

3 AUDIT REPORTS

$199

About $66 per report. Run before and after your changes, or for three sites.

5 AUDIT REPORTS · BEST VALUE

$299

About $60 per report. The best value for consultants and multi-site teams.

Plans

Full audits every month; unused credits roll over. Pay by card or PayPal, cancel any time. Every plan comes with a data processing agreement (DPA) on request.

ESSENTIALS

$99 / month

1 full audit a month for a single site or quarterly board evidence.

MSP MULTI-TENANT · FOR MSPS

$249 / month

A block list for each of up to 25 clients, a dashboard for their rules, a monthly summary per client, plus 1 full audit a month.

PROFESSIONAL

$499 / month

5 full audits a month, priority processing, co-branded reports with your logo.

MSP option: client reports, +$149 a month. 25 white-label audits a month, a monthly AI report and a compliance register per client.

Pay with PayPal or credit / debit card. All plans and prices: shadowaitools.com/pricing.php