

Example Corp

AI security findings from a 30-day assessment on 280 endpoints.

Sample report with illustrative data. Prepared by Netra Security.

Company	Example Corp
Assessment window	30 days ending Oct 24, 2026
Endpoints enrolled	280
Active users	262 in 5 departments
Product in scope	AI Security
Policy mode	Observe throughout the assessment

01 Executive Summary

Six numbers describing Example Corp's AI estate, and the findings behind them.

AI APPS DISCOVERED

47

31 unsanctioned

ENDPOINTS WITH AI

198

Of 280 enrolled endpoints

EMPLOYEES ON PERSONAL AI ACCOUNTS

78

Of 194 active AI users

SENSITIVE PROMPTS AND UPLOADS

212

Graded S3 or S4

RISKY AGENT CHAINS

9

2 critical, 4 high

CODING-AGENT USERS

120

5 agents, 10,940 autonomous runs

Top findings

CRITICAL

Two coding-agent chains combine command execution, network access, and labelled files on one device.

J. Brown · Claude Code (9.1) with 12 labelled files on the device; A. Rivera · Codex (8.4) with 25 capabilities.

HIGH

Thirty-one unsanctioned AI apps in use; one chatbot received customer records.

NovaChat has 41 users. Across all apps, 64 prompts contained customer PII.

HIGH

Sales uses more personal AI accounts than corporate ones.

41 of 48 Sales AI users used a personal account; 18 used a corporate one. 78 employees overall used a personal account.

HIGH

Company AI tools used for personal high-frequency trading.

Three Finance users: 338 trading-strategy conversations on the corporate ChatGPT workspace.

HIGH

Three high-risk MCP tools have no control policy.

23 servers and 41 tools across Claude, Cursor, ChatGPT, Codex, and Gemini; six rated High, three Not controlled.

02 Shadow AI

AI apps in use across browser, desktop, terminal, and local runtimes.

SANCTIONED APPS

16

Whitelisted

UNSANCTIONED APPS

31

New discoveries: 9

INSTALLED AI APPS

12

On 118 endpoints

LOCAL MODELS

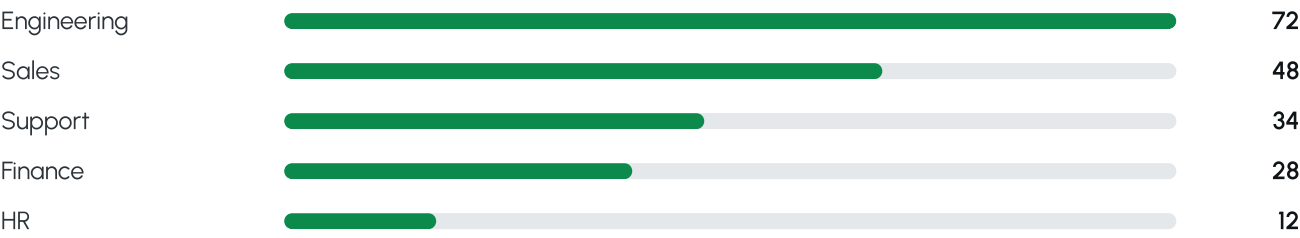
3

Ollama and LM Studio

Top unsanctioned apps

APP	CATEGORY	USERS	HITS
NovaChat	AI Chatbot	41	9,400
TransQuick	AI Tools	22	3,100
SlideGen	AI Tools	18	2,700
NoteMind	AI Tools	9	820
PromptHub	AI Chatbot	3	190

Active AI users by department



194 of 262 users were active in at least one AI tool during the window.

AI outside the browser

INSTALLED APP	TYPE	ENDPOINTS	VULNERABILITY
CodePilot X 3.23.12	AI Coding Assistant	12	CRITICAL 9.8
ChatDesk 2.6.1	AI Chatbot	27	MEDIUM 6.5
LocalLM Runner 0.9.4	AI Model Runtime	5	–

Three local models run on 9 endpoints, through Ollama and LM Studio.

AI BoM: 24 AI components in packages, IDE extensions, autorun entries, and runtimes, including one startup item, ai-sync-agent.

03 Accounts and Usage Topics

Which account each AI session ran on, and what it was used for.

DEPARTMENT	CORPORATE ACCOUNTS	PERSONAL ACCOUNTS
Engineering	62	22
Sales	18	41
Support	34	0
Finance	23	9
HR	8	6

Users on both account types count in both columns: 29 hold both for the same tool. A domain rule cannot tell them apart; an account-type policy can.

Top usage topics

TOPIC	TOOLS	DEPARTMENT	SESSIONS
Code and debugging	Claude Code, Cursor	Engineering	14,600
Customer emails	ChatGPT, Copilot	Sales	4,180
Financial analysis	ChatGPT, Copilot	Finance	1,860
HR documents	Copilot	HR	520
Trading strategy and backtesting	ChatGPT (corporate)	Finance	338

04 Coding Agents and the AI Supply Chain

Agents on endpoints, what they can call, and which combinations are risky.

Coding agents in use

AGENT	USERS	CONVERSATIONS	AUTONOMOUS RUNS	S3-S4 HITS
Claude Code	51	11,800	6,880	38
Cursor	33	5,400	1,720	17
Codex CLI	19	3,300	1,590	11
Gemini CLI	11	1,300	640	4
Kiro	6	480	110	1

MCP tools by risk

TOOL	SERVER	CLIENT	USERS	RISK	CONTROL
exec_command	shell-runner-mcp	Codex	3	HIGH	Not controlled
push_branch	repo-sync-mcp	Cursor	14	HIGH	Audit only
export_contacts	crm-export-mcp	ChatGPT	5	HIGH	Not controlled
read_channel	slack-reader	Claude	22	MEDIUM	Audit only
search_docs	docs-search-mcp	Gemini	31	LOW	Not controlled

23 servers and 41 tools in total. Installed but unused servers are removable attack surface.

Agent Skills flagged for review

SKILL	CLIENT	CAPABILITIES	RISK	SIGNAL
deploy-helper	Claude Code	Command Execution, Network	HIGH	–
csv-cleaner	Codex	Code Execution, Data Processing	MEDIUM	Scripts changed
meeting-notes	Claude Desktop	Filesystem	LOW	Same-name impersonation

14 skills installed across Claude Code, Codex, and Claude Desktop.

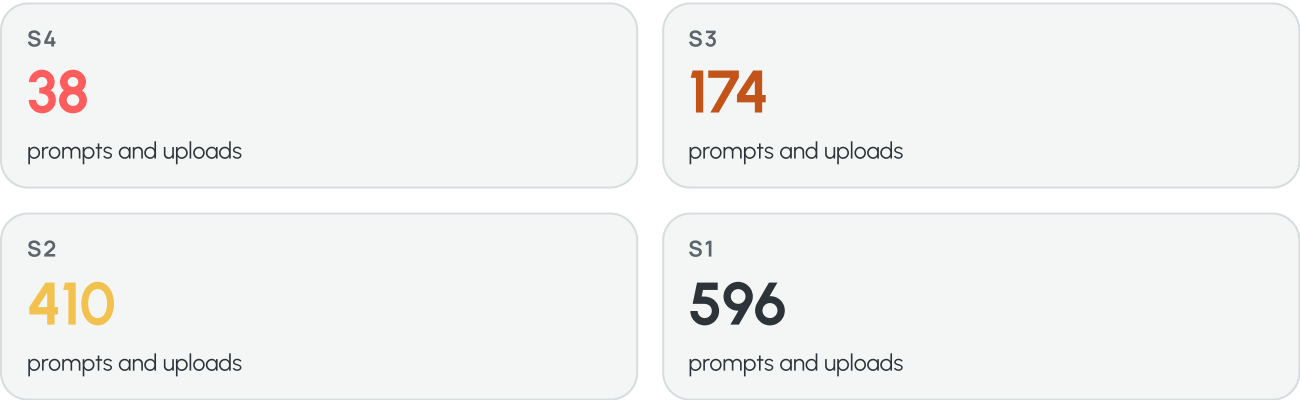
Risky Chains

USER	AGENT	DEVICE	CAPABILITIES	REACH	SCORE	LEVEL
J. Brown	Claude Code	PC-WIN-07	exec, network, filesystem	12 labelled files	9.1	CRITICAL
A. Rivera	Codex	MBP-14	exec, network, filesystem	25 capabilities	8.4	CRITICAL
S. Patel	Codex CLI	PC-WIN-05	exec, filesystem	5 labelled files	6.4	HIGH

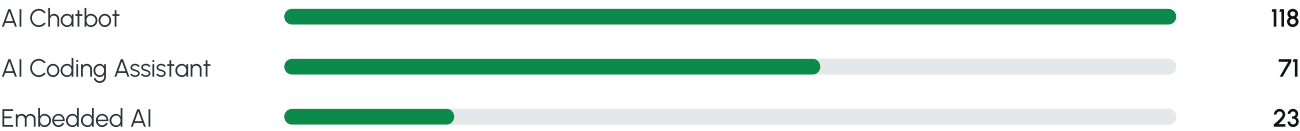
Agent Graph weighs capabilities against labelled data on one device, scoring 0–10. Nine chains: 2 critical, 4 high, 3 medium.

05 Sensitive Data in AI

Prompts, uploads, and tool calls graded S1–S4 by classifiers and MIP labels.



S3–S4 by channel category



Top classifiers matched

Customer PII		64
Proprietary source code		58
Financial data		41
Credentials		27
HR records		22

Example events

USER	CHANNEL	CONTENT	LEVEL	POLICY OUTCOME
A. Rivera	NovaChat	Customer list in prompt	S4	Observed
J. Brown	CodePilot X	Source code in prompt	S4	Observed
S. Patel	PromptHub	API key in prompt	S4	Observed
M. Chen	ChatDesk	q3-board-deck.pptx uploaded	S3	Observed

06 Recommended Next 30 Days

Five policy changes, each in the console view where it is made.

AI SECURITY

Whitelist the 16 sanctioned apps and block execution of CodePilot X until it is patched.

Analytics > Shadow AI · Protection > Access > AI Apps

AI SECURITY

Set policy by account type, starting with Sales: allow the corporate ChatGPT workspace, warn on personal accounts.

Protection > Data

AI SECURITY

Review the Finance trading-strategy conversations, then limit the corporate ChatGPT workspace to working hours for Finance with a SaaS AI access policy.

Incidents > Investigations · Protection > Access > SaaS AI

AI SECURITY

Block `exec_command` and `export_contacts` for all users, keep `push_branch` on Audit only, and revoke `csv-cleaner` pending review.

Assets › MCP › Assets › Skills

AI SECURITY

Move S4 content from Observe to Block for AI chatbots and embedded AI; keep Warn for coding-assistant source code.

Protection › Data

About this report

Example Corp, its people, devices, domains, and figures are invented to show the structure of a Netra assessment. The views are the Netra AI Security console's own: Dashboard, Assets, Activity, Protection, Incidents, and Analytics.

To see these numbers for your environment, [schedule a demo](#) and run a proof of value on your endpoints.