How Much Is the Human in the Loop?

Five AI tools, ranked by how much they check with you. **The less they ask, the more you need to trust them.**

YOU APPROVE EVERY STEP

AI RUNS AUTONOMOUSLY

📁 Claude Cowork

Anthropic · £20/mo

Desktop assistant. Reads & edits files in a folder you choose.

BEST FOR

- Expense reports
- Drafting memos & reports
- Spreadsheet analysis
- Batch file operations

●●●●● HIGH OVERSIGHT

You pick the folder. Sandboxed. You see every change.

🌐 Claude in Chrome

Anthropic · bundled

Browser extension. Clicks, navigates, and extracts web data for you.

BEST FOR

- Multi-site research
- Data extraction
- Automated form filling
- Scheduled browser tasks

●●●●○ GOOD

"Ask before acting" mode. Shares your logged-in sessions.

🔮 Perplexity Comet

Perplexity · free / £20

Full AI browser. Replaces Chrome. Shops & researches for you.

BEST FOR

- Shopping & price comparison
- Email & calendar
- Finance monitoring
- AI-enhanced browsing

●●●○○ MODERATE

Always on. Can access local files. Makes purchases for you.

🖥️ Claude Computer Use

Anthropic · API pricing

Full desktop remote control. Sees screen, moves mouse, types in any app.

BEST FOR

- Legacy software automation
- Cross-app workflows
- Software QA testing
- Complex form filling

●●○○○ LIMITED

Screenshots + acts. Dev tool. Must run in VM.

☁️ Perplexity Computer

Perplexity · £200/mo

Cloud project manager. 19 AI models in parallel, runs for hours.

BEST FOR

- Multi-day research
- Report + deck + app combos
- Building web apps
- Competitive analysis at scale

●○○○○ MINIMAL

Describe the outcome. Delegates across 19 models. Results later.

Real Attacks. Real Consequences.

Every major AI productivity tool has faced serious security incidents in its first months.

Sep 2025 — Claude Computer Use

Chinese state espionage campaign

Attackers jailbroke Claude into hacking ~30 organisations. AI performed 80–90% of the campaign autonomously.

Oct 2025 — Perplexity Comet

Local file system left unprotected

Comet could access local files via file:// protocol. Malicious sites could read your files without consent.

Jan 2026 — Claude Cowork

48-hour file exfiltration exploit

A malicious Word doc could silently upload your confidential files — including financial records — to an attacker's account.

Feb 2026 — Claude Code / Computer Use

CVEs for RCE & API key theft

Opening a malicious repository = full machine takeover. CVE-2025-59536 (CVSS 8.7). Fixed post-disclosure.

Mar 2026 — Perplexity Comet

Phished in 4 min + Amazon injunction

Guardio tricked Comet's AI in under 4 minutes. Amazon won a court order blocking Comet from its marketplace.

~30
Organisations targeted
in AI espionage campaign

48h
Cowork launch to
proven exploit

4 min
Time to phish
Comet's AI agent

1 in 9
Prompt injections
still succeed

Which Tool Fits Your Work?

Start with the question, not the product. Match the tool to the task.

📄 "I need help with documents, reports, and spreadsheets"

→ **Claude Cowork**
Local files, sandboxed. From £20/mo. Keep untrusted downloads in a separate folder.

→ **Perplexity Computer**
For complex multi-format projects. £200/mo. Cloud-based — avoid sensitive data for now.

🔍 "I spend hours researching and extracting data from the web"

→ **Claude in Chrome**
Browser extension for targeted web tasks. Close banking tabs first. Use "Ask before acting".

→ **Perplexity Comet**
Full AI browser for daily use. Free to start. Avoid for sensitive browsing until security matures.

⚙️ "I need to automate tasks across multiple desktop applications"

→ **Claude Computer Use**
Full screen control via API. Developer-oriented. Always run in Docker / VM — never your main machine.

→ **Cowork + Chrome combined**
Less risky alternative: Cowork handles files, Chrome handles web. No full desktop access needed.

🚀 "Big project needing research, code, content, and visuals"

→ **Perplexity Computer**
19 models orchestrated automatically. Runs for hours. £200/mo + credits. Start non-sensitive.

→ **Claude Cowork Max**
Enterprise-ready with department plugins. Data stays local. Better for regulated industries.

⚡ Four Non-Negotiable Safety Rules

01 **Separate sensitive files** from anything downloaded off the internet

02 **Close banking & medical tabs** before AI browses unfamiliar sites

03 **Run desktop-control AI in a sandbox** — never on your real machine

04 **Test with dummy data first.** Build trust before sharing anything real