ottim.ai

Security statement

For the security reviewer at a pilot company · what the app captures, where it keeps it, who can see it, and what leaves the machine · November 2026

> Nothing of substance leaves your Mac: none of your prompts, none of the replies, none of your settings. The one exception is your conversation with otti, which is answered by an outside AI model.

WHAT OTTIM.AI IS

A small application installed on a developer's Mac. It counts every call the developer's AI tools make, what each cost and how long it took, and each morning proposes a few changes to the setup around the prompts (instruction files, tool lists, session length, model choice within the provider already in use). It judges cost and speed only, never the content of anyone's work. There is no server-side processing of your data: the application runs locally, one copy per Mac.

WHAT IS CAPTURED

- Every request to and reply from an AI model made from that Mac by the sources the developer has switched on: Claude Code and Codex (their session records), the Claude desktop app, Cowork through an add-on, claude.ai and ChatGPT in the browser through an extension, and any server usage folder the developer points it at.
- The full text of requests and replies, in order, with the origin of each part (which file, tool, skill, memory or history it came from). Full text is what makes the advice exact: without it the app can count and time calls but cannot say which line to move.
- Each folder is asked for separately, before it is read, and the list of what was looked at is kept in Settings.

WHERE IT IS STORED

- On that Mac only, encrypted, under `~/.ottim`. The folder can be opened and inspected at any time.
- Showing captured text on screen requires Touch ID.
- Nothing is uploaded to ottim.ai or to anyone else. There is no cloud copy.

WHO CAN SEE IT

- The developer whose Mac it is. Nobody else: not their manager, not ottim.ai.
- Task durations and session lengths are shown to nobody but the developer. Time entries per ticket exist only if that person switches them on.

HOW FULL-TEXT CAPTURE IS SWITCHED OFF

- Each source has its own switch, and full-text recording has its own switch, in Settings. With text off the app still counts calls, timings and cost; it loses the advice that depends on reading how a prompt was built (cache order, dead weight).
- **Delete collected data** removes everything ottim.ai keeps on the Mac and names it part by part.

WHAT LEAVES THE MACHINE

- **The conversation with otti**, the in-app assistant. What the developer types to otti goes to Claude through ottim.ai's server, together with the few facts otti needs to answer: which sources are counting, which settings are on, this morning's cards. Never the text of the developer's work with their AI tools. otti can be left unused.
- **Daily totals, only if that switch is on.** One line a day to ottim.ai: the date, the number of calls, the dollars. Never text. The exact lines can be read before and after sending. Off by default.
- ottim.ai's server has one address, so the Mac's own firewall can watch it. No other outbound traffic.

WHAT IT NEVER DOES

- Never changes code, never opens a pull request, never runs an agent, never touches a deployment.
- Never runs a request in the background and never gives a tool permission to write on its own. "Execute with a single click" opens the developer's own tool with the card's request as the first message; the tool's own approval prompt is the last check. Never `--dangerously-skip-permissions`.
- Never routes traffic, never changes provider, never takes money from a provider.

REMOVING IT

Delete collected data, then drag the application to the Bin. Nothing remains on the machine and nothing was ever held elsewhere.