Vigilance

DATASHEET

Sometimes the AI installs code from strangers. We check it first.

Your staff ask AI to fix a spreadsheet or make a tracker. Vigilance checks the code the AI installs.

WORKS WITH

ChatGPT · Claude · Cursor · Codex · Copilot · Gemini CLI · on Mac, Windows and Linux

An expense tracker update turns harmful

× BAD UPDATE

BEFORE

The form helper fills in the expense form.

AFTER THE UPDATE

It can also read saved passwords.

✓ LAST GOOD VERSION

Vigilance tests the version before with your tracker and swaps it in. The job still gets done.

NO GOOD VERSION TO GO BACK TO?

We suggest an established replacement that does the same job. If you say yes, we swap it in. The job still gets done.

Illustrated example. Fictional software.

HOW IT WORKS

Staff ask AI to fix a spreadsheet

The AI downloads free helpers from the internet

Bad update

It can now do something harmful, like read saved passwords

Last good version

Tested with your spreadsheet, then swapped in. The job still gets done.

If the test cannot run, Vigilance asks you to look.

CAUGHT FIRST, IN REAL CASES

No tool, Vigilance included, can promise to catch every attack.

34 seconds

We flagged planted code 34 seconds after it went online.

25 days

We flagged a harmful update on September 17, 2026. A security lab reported it 25 days later.

0 of 63

That day, 0 of 63 virus scanners flagged its Mac program.

PLANS · US$ PER COMPUTER, PER MONTH · FREE FOR 14 DAYS

	SOLO Free	TEAM $49	MANAGED $199
Checks the code the AI installs	✓	✓	✓
Swaps a harmful update for a tested earlier version	–	✓	✓
A security person checks each warning first	–	–	✓
Also checks installed apps	–	–	✓

Solo is for one person on one computer. Managed adds a US$2,500 one-time setup. 60-day refund.

Start the free 14-day trial

The install takes about one minute. Save a card and send your team the join link. We charge nothing until you press Start my plan.

vigihq.com

Book a call: vigihq.com/book

support@vigihq.com

FOR YOUR IT PERSON

What runs on each computer

You install Vigilance once for the whole computer. On Windows and a Mac, an administrator says yes once. It needs no kernel driver, no root certificate and no network proxy. It opens no port to the network.

WHERE VIGILANCE SITS

ASKS
An AI assistant or a person
runs an install command

→

PACKAGE MANAGERS
npm, pnpm, yarn, bun, pip, uv
point at the filter in each person's settings files

→

VIGILANCE ON THE COMPUTER
Local filter on 127.0.0.1
A watchdog checks it every minute

→

FILES COME FROM
npm and PyPI
or your company's own registry

↕

VIGILANCE SERVICE
check.vigihq.com, TCP 443 over HTTPS
Every answer is signed. The servers are in AWS Canada (Central). Most lookups send a 4-character code that dozens of package names share.

WHAT THE PACKAGE MANAGER SEES

TIDY-FORMS · VERSION LIST	
~~4.2.2~~	× BAD UPDATE
4.2.1 · now marked latest	✓ LAST GOOD VERSION
4.2.0	

Vigilance takes the harmful version off the list, so the install gets the last good one. If the test of your project cannot run, Vigilance asks you to look.

HOW VIGILANCE JUDGES A VERSION

TIDY-FORMS 4.2.1 COMPARED WITH 4.2.2, FILE BY FILE	
index.js	NO NEW POWER
validate.js	NO NEW POWER
autofill.js	GAINED: READS SAVED PASSWORDS

Vigilance looks at what a file does, not at the words it contains. If we are unsure of a finding, we hold it and report it. We never clear it on a guess.

COVERED

SYSTEMS	macOS, Windows and Linux, including Chromebooks
AI ASSISTANTS	Claude Code, Cursor, Codex, GitHub Copilot, Devin Desktop and Gemini CLI, and installs typed by hand
DESKTOP APPS	Codex installs in ChatGPT and Claude, and the add-ons that these apps start with npx or uvx
MANAGERS	npm, pnpm, yarn, bun, pip and uv
REGISTRIES	npm and PyPI, and your company's own registry as the source

NOT CHECKED

- Cloud workspaces and cloud agents
- Installs run with sudo, and scripts piped to a shell
- cargo, go, gem, composer, maven, gradle, nuget, Homebrew, conda and Poetry
- Installs inside Cursor's sandbox, Claude Desktop Extensions and Claude Cowork
- The code your team writes. Vigilance checks public packages.

Every report lists these.

WHAT LEAVES THE COMPUTER

- ↑ The computer name and the full name of the user account
- ↑ The public package names and versions that Vigilance checked, and what it did and why. Your Portal shows this for 90 days.

WHAT NEVER LEAVES

- × Your code and files, paths, project and folder names
- × Login names, hardware ids, private package names and lockfiles

IF SOMETHING FAILS

The filter stops
The watchdog puts the old package settings back within about 2 minutes.

Our service is down
Vigilance uses its last saved list for up to 7 days. After that, installs go ahead unchecked.

Vigilance stops on a computer
We email you the same day.