

Approval Summary

From (the person who runs our AI tools) _____

Date _____

What it is

Our staff build apps and tools with AI tools such as Claude Code, Cursor, Codex, Copilot, Devin Desktop and Gemini CLI. Each app pulls in packages, which are free building blocks from the internet. Nobody on our staff reads them. One bad package can read saved passwords and send files out.

Vigilance checks each new package version that our AI tools and our staff install with npm, pnpm, yarn, bun, pip and uv on our computers. It compares the version with the last version that passed, and finds the file that gained a new power, such as reaching the internet or reading passwords. It holds a version that gained a power. One installer on each computer covers every AI tool.

What happens first: a free 14-day watch

- We sign up and save a card. Nothing is charged unless we say yes on day 14.
- For 14 days it only watches. It swaps none of the building blocks our staff install.
- On day one we see how many building blocks are already on each computer.
- On day 14 we get a readout: how many different building blocks came in, on each computer, and which ones needed a look.
- If we say yes, we choose a plan. If not, Vigilance turns off on every computer and removes itself within 30 days. There is nothing to cancel.

After we buy

The free watch checks and counts. Paid service starts only when swapping is ready. Until then, the free watch stays free.

What leaves our computers

- A 4-character code for each package name, and the public package name and version when nobody has checked that version yet.
- A random id and a two-word name for each computer, its counts, and scrambled codes that count different packages.
- Our code, files, file names, paths, folder names and project names stay on our computers. So do staff names, user names, host names, machine names, hardware ids, install ids, lockfiles, private package names and error reports. App names stay too, except the apps that the whole-computer watch flags.
- Vigilance sends no AI tool name outside its fixed list, no program version outside the counts and the join, and no address of a package server that routing puts behind the filter.
- The full field list: vighq.com/security/data

Who checks what is inside

With Vigilance, covered installs use shared checks for public package versions. The scanner compares changed capabilities against its last passed baseline. The readout shows unchecked paths and gaps.

What Vigilance cannot see

Apps built only in a cloud workspace. Computers that did not join. Package managers it does not cover yet. Package versions nobody has checked yet. Who installed what. It cannot tell us which person or app installed a package, because it never gets that data.

What it costs

Per computer, per month. No minimum.

- Done With You: \$49 per computer, per month, or \$490 per computer for a year.
- Done For You: \$199 per computer, per month plus \$2,500 to start, or \$1,990 per computer for a year with no start fee.

Computers (1 or more)	_____
Per month: computers × the plan price	\$ _____
Per year: per month × 12, or the yearly price × computers	\$ _____

On monthly plans, we pay for each computer that runs Vigilance that month. Currency: CA\$ for Canadian companies, US\$ for others. No sales tax is added.

Monthly plans continue until we cancel. Yearly plans renew each year. Ask within 60 days of the first payment and Vigilance refunds the monthly fees, once per company. The \$2,500 start fee comes back only if Vigilance misses full setup and the written review within 14 days. The service stops when the refund is made.

The cost of one bad update (our numbers)

Hours to check the computers and change passwords and keys	_____ h
Hours from our IT provider	_____ h
Hours to rebuild or re-check our apps	_____ h
Total hours × our loaded hourly rate, in dollars	\$ _____
Other costs we know of (for example an insurance deductible)	\$ _____
Cost of one bad update	\$ _____
Vigilance per year (from above)	\$ _____

The risk to us

- Each person runs one installer on their own computer, with a join link. The readout lists each joined computer by its two-word name.
- We send our staff a short notice before they install.
- If Vigilance is down or slow, installs go ahead and Vigilance counts them as unchecked.
- We remove a computer on our owner page. It turns off at once and removes itself within 30 days.
- Our IT provider needs to allow one host and one port. Vigilance gives us a ready email.

Decision

Approve a free 14-day watch for _____ computers:

☐ Yes ☐ No

Signed _____ Date _____