

Your people already use AI every day. SpanDock lets the company see it, keep it safe, and pay less for it.

Developers, analysts and support teams use Claude Code, GitHub Copilot, Cursor, ChatGPT and more. **Most companies can't answer four simple questions about that use.** SpanDock answers all four, from servers the company runs itself.



Who is using AI?

Which tools, which teams, and for which projects.

Is our data safe?

Are customer details or passwords leaving in a prompt?

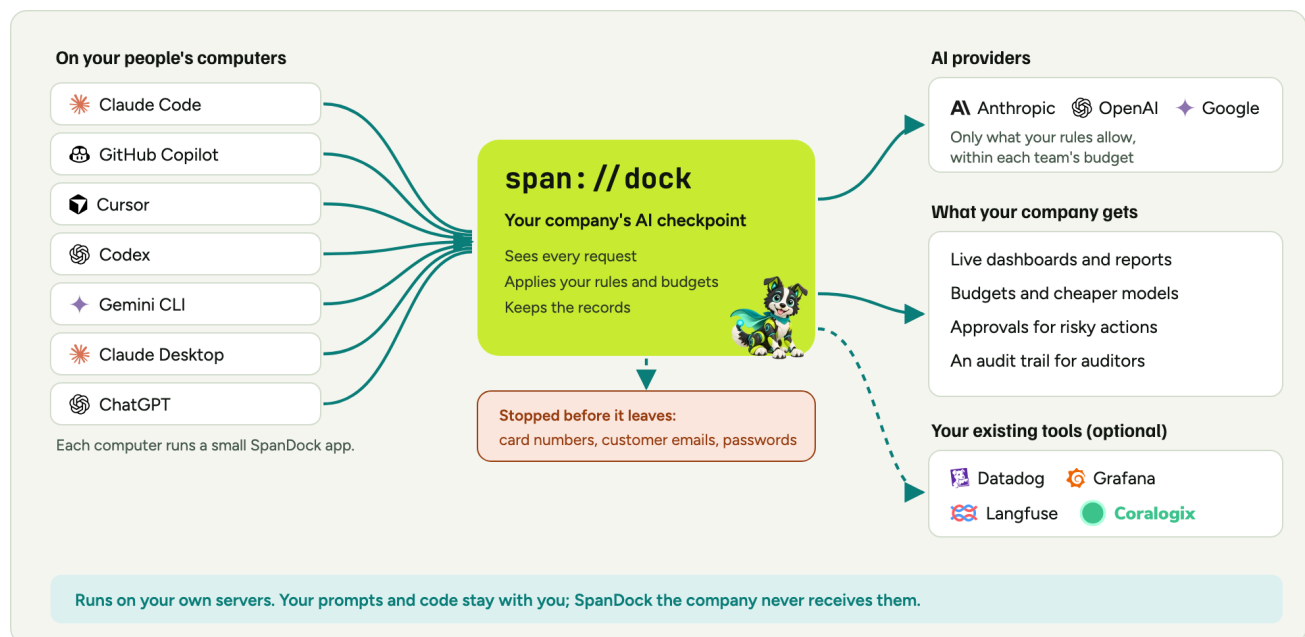
What does it cost?

Per person, per team, per model, this month.

Can we prove it?

To auditors, regulators and the board.

Where SpanDock sits



Every AI request passes the checkpoint on the way out. People keep using the tools they like; the company gets the view and the controls.

WORKS WITH

AI tools

- Claude Code
- Cursor
- ChatGPT
- Claude Desktop
- Codex
- GitHub Copilot
- Gemini CLI

AI providers

- Anthropic
- OpenAI
- Google Gemini

Trademarks and logos belong to their owners; no endorsement implied.

Connected tools

- Jira
- GitHub
- Slack

Monitoring tools

- Datadog
- Grafana
- Langfuse
- Coralogix

See. Protect. Save. Prove.

See

One live picture of AI use across the company: who uses which tool, how much, and on which projects.

- Live activity and dashboards
- AI adoption report by team
- Every computer and server in one view

Protect

Stops sensitive data from leaving in a prompt, and asks a person before an AI tool changes something important.

- Guardrails: block, warn, ask or redact
- Approvals and time-limited access
- Company-approved connections to Jira, GitHub and more

Save

Keeps AI spend predictable and sends simple work to cheaper models automatically.

- Budgets per person and team
- Smart routing between models
- Cost per model, team and month

Prove

Gives auditors and regulators the records they ask for, ready to export.

- Audit log of every setting change
- Change report with who approved what
- A privacy notice people actually see

Why it matters

RISK	WITHOUT SPANDOCK	WITH SPANDOCK
Data leaks	A customer list or a password is pasted into a chatbot, and nobody knows.	It is stopped on the person's computer, with a clear message, and the attempt is recorded.
Shadow AI	Teams use tools nobody approved. IT finds out months later.	Every tool on every computer is visible from day one.
Runaway costs	The AI bill doubles and nobody can say why.	Budgets cap it, and the bill is broken down by team and model.
Audits	Weeks of screenshots and spreadsheets to answer "who changed what".	One export, with approvals and tickets attached.
Adoption	AI gets banned because nobody can control it.	AI is rolled out with confidence, and the company can see what it is worth.

How it fits in

- **Installs in minutes** on a Mac, Linux or Windows server, with a small app on each computer.
- **Nothing changes for people.** They keep their tools; SpanDock sets them up and keeps them updated.
- **Your data stays yours.** It runs on your servers, and connections are encrypted end to end.
- **Grows with you,** from one team to offices around the world.

