

AI tools now see your code, your customers' data and your production systems. SpanDock puts that use under your rules and on the record.



People paste data into prompts. AI agents call tools that change real systems. Teams adopt tools nobody reviewed. Auditors and regulators ask how AI use is governed. **SpanDock is a self-hosted control point for AI use:** it runs on your servers, enforces your rules on every computer, and keeps the evidence.

Sensitive data in prompts

Card numbers, customer details, secrets or code sent to an AI provider.

Unreviewed tools

AI tools and connections in use that nobody approved.

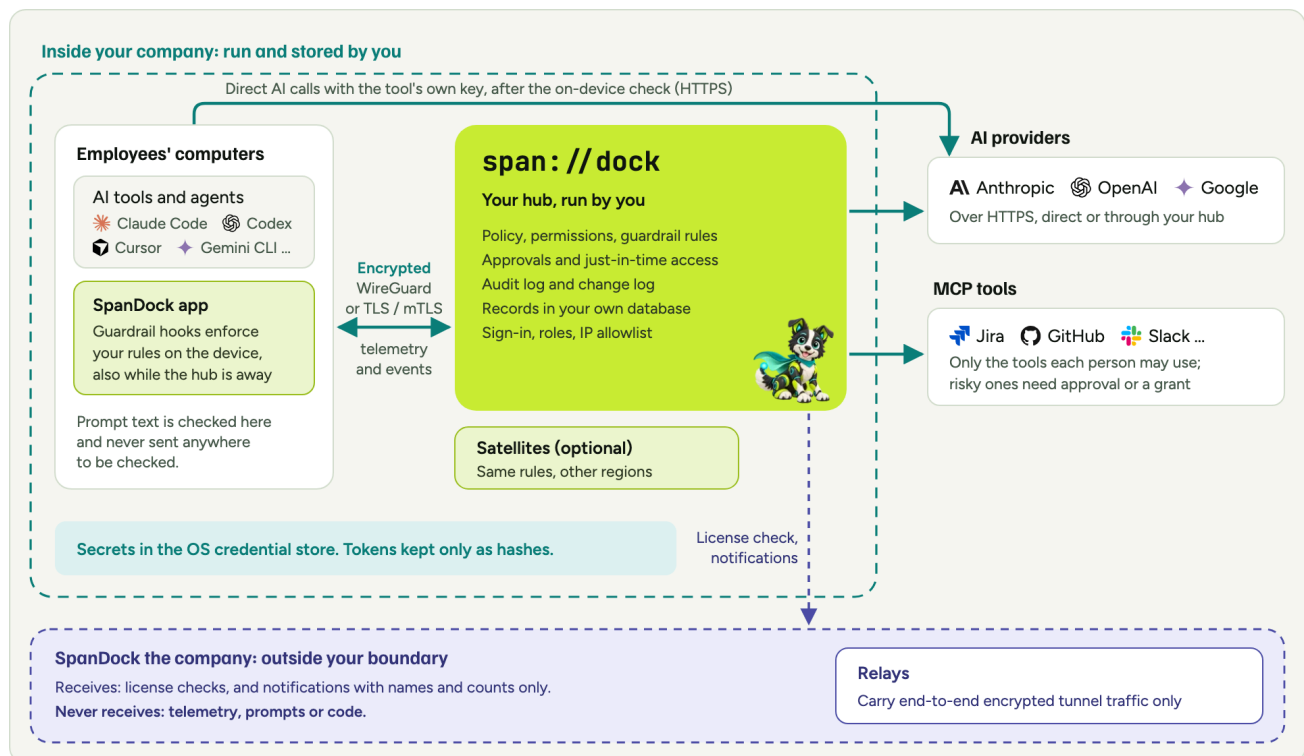
Agents acting on production

An AI agent changes a live system with no approval or ticket.

Proving governance

Auditors, regulators and customers ask for records.

Where data goes, and where it stops



Rules are enforced on each computer and at your hub. SpanDock's records stay on your servers, and reach your own monitoring tools (such as Datadog, Grafana, Langfuse or Coralogix) only if you add them. SpanDock the company sees license checks and notifications with names and counts, nothing more.

Controls

- **Guardrails on computers.** Detect card numbers, IBANs, national ID numbers (US and UK; other countries by pattern), secrets, email addresses, phone numbers, word lists and custom patterns, in prompts, tool arguments and tool results.
- **Four actions per rule:** block, warn, ask the person to confirm, or redact. Each rule also sets what happens when SpanDock can't check: let it through or block.
- **Where they apply:** Claude Code, Codex and Gemini CLI through hooks, and every tool call through SpanDock's MCP gateway. A chat app's typed messages are out of reach; its tool calls are covered.
- **MCP gateway.** Company-approved connections to tools such as Jira and GitHub, with permissions per person, group, tag or user type, read-only mode, block rules and approval before risky tools.
- **Just-in-time access.** Chosen tools work only under a grant of 15 minutes to 8 hours, with a reason and a ticket. Nobody approves their own request; grants expire by themselves and can be revoked.
- **Access to SpanDock.** Sign-in with company SSO (OIDC), spandock.com, passkeys or passwords with one-time codes; viewer, editor, admin and a read-only auditor role; an IP allowlist.

Evidence

- **Audit log** of every change to SpanDock's settings, local or remote: who, when, and which fields. Never the values.
- **Change report:** changes AI tools made to systems you mark as production, with approver, grant and ticket. Flagged first: no approval, no ticket, self-approval, approval with nobody signed in.
- **Exports with a SHA-256 digest**, recorded in the audit log, so a copy can be checked later.
- **Quarterly access reviews** of who may use which tool. Reviewers confirm or remove; nobody reviews their own access.
- **Retention** you set, from 30 days to 10 years (365 days by default).

Privacy and legal

- **Self-hosted.** Records stay in your own infrastructure and region.
- **Prompt capture is off by default.** It is turned on per computer, or left to each person. The first time, an administrator must confirm that people are informed and that there is a lawful basis.
- **Notices people see:** a privacy notice with a suggested text for your country (GDPR-style in the EU, EEA, UK and Switzerland). Notices for prompt capture and guardrails can't be hidden.
- **Prompt text** is taken out of every record before it is stored or forwarded, kept only on the hub (unless you choose to forward it), and deleted once summarised or after the days you set.
- **Access requests:** export a person's data, or delete their records with a preview.
- **Process inventory** never collects command-line arguments or environment variables.

Security of SpanDock

- **Local by default.** The dashboard listens on the server's own machine, refuses foreign host names (DNS rebinding) and needs an anti-forgery header for every change.
- **Remote management needs two tokens,** and destructive or credential-creating actions stay local only.
- **Secrets** live in the operating system's credential store. Tokens and keys are kept only as hashes and shown once.
- **Outbound connections** to destinations use HTTPS; cloud metadata addresses are refused.
- **Updates** come only from SpanDock's release repository, with checksums and automatic rollback.
- **An automated security test suite** checks these properties, with fuzzing of untrusted input.

Questions you will be asked, and the record that answers them

THE QUESTION	IN SPANDOCK	THE EVIDENCE
Who approved this production change?	Change management report	CSV with approver, ticket and grant, and its SHA-256 digest
Can customer data leave in a prompt?	Guardrails on computers	Guardrail events: rule, action and outcome (text samples only masked, and only if you turn them on)
Was access to production temporary?	Just-in-time access	Grants with reason, ticket, approver and expiry, in the change log
Who can use which AI tool, and is that still right?	MCP gateway permissions, access reviews	Access review export with each decision, and its digest
Who changed SpanDock's own settings?	Audit log	Filtered log and CSV export
Do people know what is collected?	Privacy notice, mandatory notices	Acknowledgements per computer and notice revision
What do we hold about this person?	Personal data export	JSON export, recorded in the audit log

These records **help you produce evidence for** SOC 2 (change management, access reviews), ISO/IEC 27001 (access control, logging), the GDPR (transparency, access requests) and the EU AI Act (human oversight, record keeping).*

Plans. Guardrails on computers, change management, just-in-time access and process inventory are Enterprise features. Company SSO, the audit log and offline licenses for air-gapped sites are Enterprise only. The MCP gateway, dashboard sign-in and the IP allowlist are in Premium and Enterprise. The privacy notice and personal data export are on every plan. The 30-day trial includes everything except the Enterprise-only features.

A lapsed license never stops telemetry or switches off protections already in place; it only refuses new configuration and new pairings.

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

* SpanDock helps produce evidence; it does not by itself make an organisation compliant.