What Sentilai does

Your developers are already using AI coding assistants. Sentilai is the control plane that sits between those assistants and the AI providers behind them, so that every request is governed and audited without anyone changing how they work.

The shape of it

There are three parts.

The Gateway is a proxy. Claude Code, Cursor, GitHub Copilot, Gemini CLI and Codex CLI send their requests to it instead of directly to Anthropic or OpenAI. It applies your policy, records what happened, and forwards the request. Your developers see the same tools behaving the same way.

The Endpoint Suite is a small desktop app on each developer machine. It signs the developer in with a passkey, registers the machine, and rewrites each AI tool's configuration so it points at the Gateway. It also governs the MCP servers running locally on that machine — which the Gateway alone cannot see.

The Admin Console is where you set policy, see activity, manage people, and produce evidence. That is this documentation's main subject.

What you get that you didn't have

- **An audit trail.** Every AI request, who made it, which tool, which model, what it cost, and what the policy decided.
- **Enforcement, not just observation.** Blocking a dangerous MCP tool call, stopping a secret before it leaves the building, refusing a request that combines private data access with untrusted content and a way out.
- **Evidence.** A point-in-time record of your policy, your access inventory and your enforcement, for the auditor who asks.

What it is not

Sentilai does not read your source code repositories, does not sit in your CI, and does not replace endpoint security or a code scanner. It governs the traffic between AI assistants and AI providers, plus the MCP servers those assistants call.

It also does not stop a developer who is determined to bypass it — a personal laptop with a personal API key is outside any control plane. What it does is make the governed path the easy path, and make the ungoverned one visible.

Revision #6
Created 2026-08-02 10:19:48 UTC by Sentilai Docs

Updated 2026-08-04 08:39:32 UTC by Sentilai Docs