

What Sentilai does not do

Reading a list of a security product's limits is a better use of five minutes than reading its feature list. Here is ours.

It does not cover ungoverned machines

A personal laptop with a personal API key never touches the Gateway and is invisible to Sentilai. What we give you is a governed path that is easy, drift detection when a governed machine slips out of it, and an egress blocklist so your network can close the direct route. That is control of the managed path, not of every possible path.

It does not read your repositories or your CI

Sentilai governs traffic between AI assistants and AI providers, plus the MCP servers those assistants call. It is not a code scanner, not a secrets scanner for your git history, and not a CI gate.

It does not stop a determined insider

Someone who wants to exfiltrate data has simpler routes than an AI assistant. Sentilai raises the floor and creates a record; it is not an insider-threat programme.

Detection is imperfect

The classifier will miss things and will occasionally flag innocent work. The detectors are tuned to be useful rather than exhaustive, which is why the trifecta detector exists — it constrains the *consequence* of an injection rather than relying on recognizing it.

Some paths are only partly covered

- **Cursor** — chat only; Tab autocomplete is not routed. Requests also still transit Cursor's servers.
- **GitHub Copilot** — chat only through the custom endpoint; inline completions are not routed, and requests still transit GitHub's servers.
- **MCP per-tool rules** — enforced where the Gateway knows a tool name: the local shim and routed remote endpoints. The chat-request side-channel supports server-level policy.

We hold no certifications yet

No SOC 2, no ISO 27001 today. When that changes it will be stated here, with the report available. Ask us for the current status; you will get a straight answer.

Revision #6

Created 2026-08-02 10:20:11 UTC by Sentilai Docs

Updated 2026-08-04 08:39:56 UTC by Sentilai Docs