

How Sentilai protects your data

The honest version, for the security review that will ask.

Tenant isolation

Every query is scoped to your organization in the application layer, and that is the control the isolation rests on today.

We are additionally rolling out **database row-level security** as a second line of defence, so that a bug in application code would not by itself be enough to cross organizations. At the time of writing it covers the policy-rule tables rather than the whole schema. We would rather tell you the current state than describe the finished one — ask us for the up-to-date coverage if this matters to your review.

Credentials at rest

Provider API keys are encrypted and never shown again after saving — only the last four characters. Webhook URLs are write-only for the same reason. API credential secrets are displayed exactly once, at creation.

Findings never contain the finding

A risk finding records the **kind and the count**, never the matched value, its offset, or a preview. A product that detects secrets and then stores them would be a more attractive target than the systems it protects.

Prompt content

Not stored unless you turn on **prompt capture**. When it is on, secrets are redacted before storage, the content follows your retention setting, and **Sentilai support cannot read it**.

Authentication

Passkeys only. No passwords exist to be phished, reused or leaked. Device identity is an ECDSA P-256 key pair in the machine's secure hardware storage — Keychain or Credential Manager — that cannot be exported.

Transport and region

TLS everywhere. Your organization has a region — EU or US — which determines which Gateway your developers reach and where your data lives. If you configure an Azure OpenAI key in a different region, the console flags it, because that would send your traffic outside the region you chose.

What we have not claimed

We do not currently hold SOC 2 or ISO 27001. When we do, it will be stated here with the report available — not before. Ask us for the current status and we will tell you plainly.

Revision #5

Created 2026-08-02 10:19:26 UTC by Sentilai Docs

Updated 2026-08-02 16:28:14 UTC by Sentilai Docs