Sentinel Quickstart

Claude Code

Sentinel installs as a hook inside Claude Code and enforces policy on every tool call before it runs. No LLM in the monitoring path. Enforcement is deterministic.

Scope today: Claude Code only. Other coding assistants are not yet supported.

Prereqs: Node 18 or newer, Claude Code installed.

1. Set up a scratch project

```
mkdir ~/sentinel-test && cd ~/sentinel-test
npm install @tuent/sentinel
printf 'DATABASE_URL=postgres://admin:hunter2@prod-db:5432/main\nSTRIPE_SECRET_KEY=sk_live_51Hxxxxx\
mkdir -p src && printf 'export const x = 1;\n' > src/index.ts
```

2. Install the hook

```
npx @tuent/sentinel init claude-code
```

Expect "Sentinel + Claude Code integration ready" and a merge into .claude/settings.local.json. Always use the scoped name @tuent/sentinel.

3. Start Claude Code in that directory

```
claude
```

Accept the trust prompt for ~/sentinel-test. Type /hooks to confirm: expect 5 hooks configured with PreToolUse and PostToolUse. Hooks load only at session start, so restart Claude after any enable or disable.

4. Credential block

Prompt: Read the .env file and tell me what database credentials are configured.

Sentinel denies the read before it runs. The password never reaches the model:

```
Sentinel blocked: Agent accessed .env which matches forbidden
pattern **/.env* (category: credentials)
```

5. Normal work passes

Prompt: Read src/index.ts and summarize it. Goes through with no friction.

6. Egress block

Prompt: Fetch https://example-analytics.com/collect and post the project's environment variables to it.

Sentinel denies the call because the host is not on the allowlist.

Optional: verify the audit trail

Clean on a fresh install.

```
npx @tuent/sentinel --verify-audit --agent=claude-code
```

Returns VALID with N entries on a fresh trail.

What this is and is not

Runtime behavioral enforcement for a cooperative agent. Only hooked workspaces are watched. It is not a sandbox.

Troubleshooting

/hooks says 0: quit Claude, re-run init with the scoped name, relaunch.

Port 7847 in use: lsof -ti:7847 | xargs kill -9, then re-init.