Vaultless Guard

Your AI sees the problem. Not your secrets.

An on-device AI privacy gateway for Claude Code, Codex and MCP tools. Secrets, customer data and your confidential terms are swapped for keyed tokens **before a request leaves the laptop**, and swapped back locally in the answer. Developers keep their tools; the provider sees tokens.

How it works

1 Stops at the machine. The AI tool points at a gateway on 127.0.0.1. No cloud proxy, no TLS interception, no root.

2 Tokenizes what it detects. `AKIA…` becomes `[VG1:1a2b…]`, encrypted under a key that never leaves the device. No vault server exists to breach.

3 Restores locally. Real values return in the answer and in the agent's next tool call, only on that machine.

Guardrails for agents. With guardrails on, `rm -rf`, `terraform destroy`, `DROP TABLE`, credential reads and persistence are stopped before they run, with a reason the agent sees.

Proof, not promises. `vguard prove` sends fresh test values through every channel and shows what the provider would receive. Hash-chained audit log; auditor evidence packs.

A content-free console. Hosted, self-hosted or air-gapped: fleet coverage, counts by data class, central rules approved by a second person and signed with your key. It never receives prompts or values.

Enterprise identity. SSO (OIDC), SCIM, MFA, roles, scoped API keys, two-person change control, SIEM export (OCSF 1.3). Row-level isolation per organisation.

Pricing

Plan	Price (per seat / month)	For
Community	Free	1-5 people • the complete gateway, local only
Team	$12 billed annually • $15 monthly	5-100 seats • console, central rules, SSO/SCIM/MFA, 90-day analytics
Business	$24 billed annually • $29 monthly	25+ seats • evidence packs, 1-year analytics, 99.5% SLA
Enterprise	from $30 • $36k/year minimum	100+ seats • air-gapped, managed policy, custom terms

Protection is free on every plan and never switches off when a trial or invoice lapses. 30-day Business trial, no card. Not yet: SOC 2 report, third-party pen test, browser/web-chat coverage, Windows GA.

vguard.techmek.io **Request a trial: vguard.techmek.io/contact**