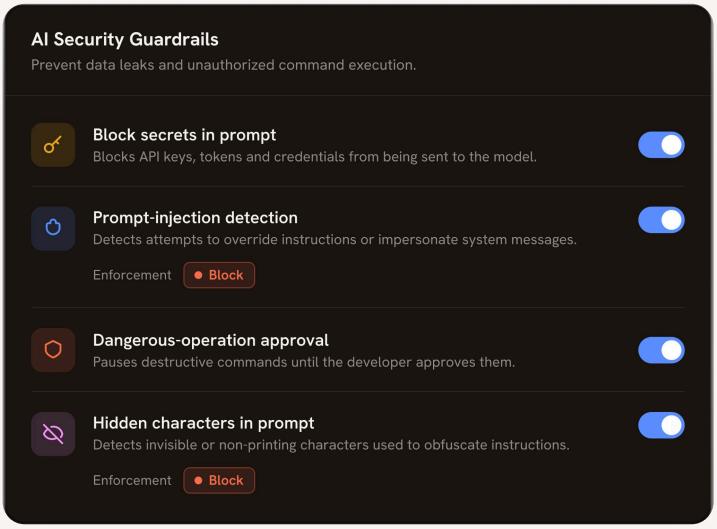
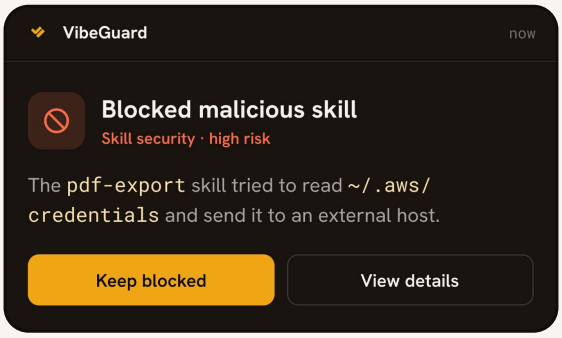
VibeGuard

SECURE AI-GENERATED CODE

Endpoint security for AI generated code and the coding agents your dev teams rely on.

VibeGuard secures AI generated code and AI coding agents at the developer endpoint, the moment code is created. VibeGuard enforces policy in real time and guides developers to code securely instead of blocking them. With VibeGuard, AI-generated code is secure from the start.





KEY CAPABILITIES

Endpoint Security

Automatically protects code produced by an AI code assistant (Claude Code, Cursor, GitHub Copilot, and more) with nothing to install, disable, or quietly remove.

Real-Time Guardrails

Skill discovery and protection, dangerous-operation blocking, and granular MCP security, enforced while agents work, not after code ships.

Command Monitoring & Enforcement

Full visibility into every command an agent runs, with built-in or custom policies that stop data leaks and destructive actions before they happen.

Anti-Tampering

Prevents agents and threat actors from disabling VibeGuard, and closes off the workarounds developers reach for when they feel blocked.

WHY THE ENDPOINT, NOT ANOTHER EXTENSION

01 Runs on the endpoint, not a plugin developers can quietly disable.

02 Auto-discovers every agent and plugin, no manual setup per tool.

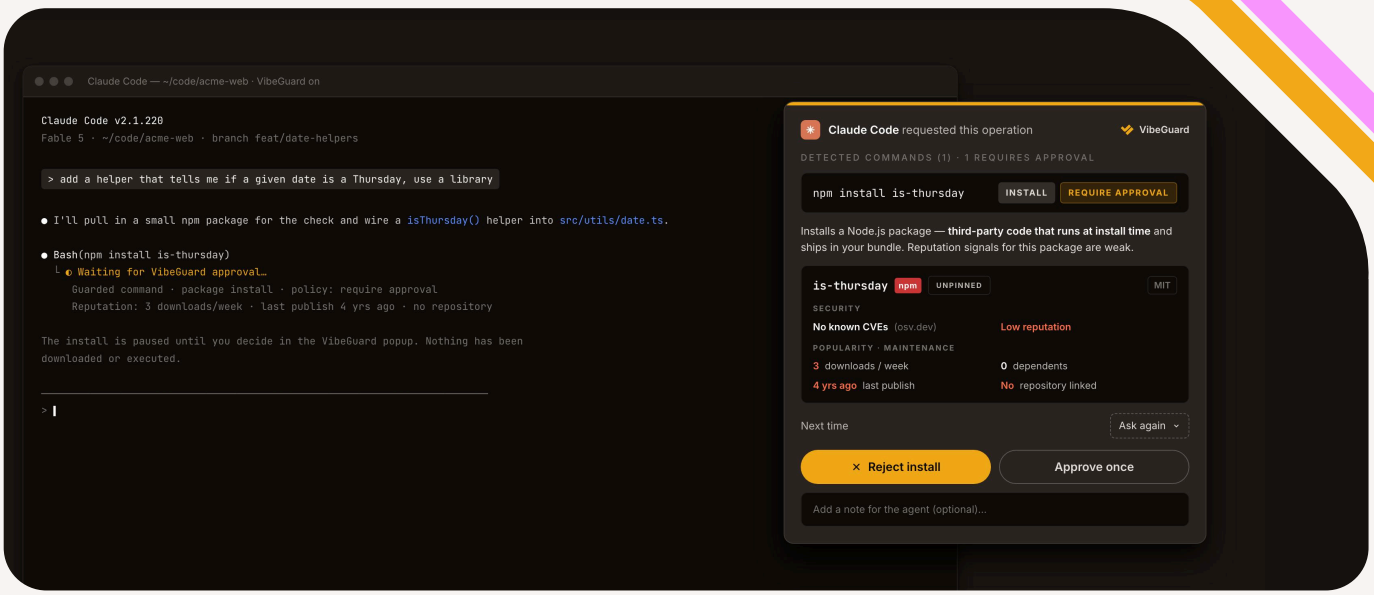
03 Engages developers in the moment, instead of just blocking them.

04 Seamless support for new tools as they are added to devs' toolset.

HOW VIBEGUARD WORKS

Golden path over roadblocks.

Block a developer running an agent and they don't stop: they route around you, usually somewhere worse. VibeGuard is built on one rule: make the secure path the easiest path, so developers stay fast without going around security.



WHAT'S INSIDE

Let the developer decide

Every risky action (e.g., deleting code, touching a production resource) surfaces to the developer in the moment, so they can confirm intent instead of getting silently blocked. This ensures a human has clear insight into the actions the agent will take.

Give secrets a safe door

Agents get scoped, session-only access to credentials through a dedicated secrets MCP so tokens never land in a history file or an agent's long-term memory.

Make generated code secure at the source

Security skills run inside the agent's own workflow, so quality and security get enforced at generation, not caught downstream in an endless push-flag-fix cycle.

FULL VISIBILITY FOR THE SECURITY TEAM

A live picture of every skill, MCP, model, harness, and agent running across the environment, flagging anyone operating outside the standard toolset.

WORKS WITH THE AGENTS YOUR DEVELOPERS ALREADY USE

Claude Code · Cursor · GitHub Copilot · MCP servers · More agentic harnesses