

KONVU VS CLAUDE SECURITY

Claude Security finds bugs. Konvu proves them and ships the fix.

Run Claude Security to find vulnerabilities in your own code, including business logic flaws. Add Konvu when findings from Claude Security, your scanners and your bug bounty program outgrow your team: Konvu runs each exploit against a deployed copy of your app and ships the fix. Claude Security's documented verification reads code, and Anthropic ships no dependency scanner.

Konvu is not a scanner. Claude Security findings come in as reports.

AT A GLANCE

	CLAUDE SECURITY	KONVU
Finds vulnerabilities	Yes, in first-party code, from injection and IDOR to memory safety	No. Konvu decides on findings from scanners, researchers and AI tools
Dependencies	Not documented. The plugin skips vendored and installed packages	Four-precondition exploitability check on scanner findings
Verification	Agents re-read the code. Plugin verifiers never run it	An attacker agent runs the exploit on every report
Runs against	Source code and its history. Severity assumes a default deployment	Konvu's deployed copy of your app, attacked from a separate host
Fixes	Remediation session in Claude Code. Plugin patches run your tests	Draft PRs or a fix prompt for Claude Code, then the exploit re-run against the fix
Write-back	Webhooks for Slack or Jira. CSV or Markdown export	Dismissals to Snyk, Semgrep, Dependabot. Jira on Enterprise
Pricing	Token cost, no platform fee, on Claude Enterprise	Business: \$2,000/month for 400 confident verdicts

Where Claude Security is stronger

- New bugs in your code, including business logic and access control.
- Mythos 5.1 in Claude Enterprise at token cost, no platform fee.
- In session, on demand, on the PR and on a schedule.
- The plugin runs on GitHub, GitLab, Bitbucket and offline, with SARIF.

Where Konvu fits

- One decision record for Claude Security, scanners and bug bounty.
- Findings only a running application can settle.
- Dependency findings, which Anthropic's tools don't cover.
- Fixes shipped, then re-tested against the exploit.

RUNNING BOTH

Claude Security finds. Konvu decides what to fix.

01

Export the findings

Markdown from the hosted product, or the plugin's SARIF file.

02

Konvu reproduces

Each report is triaged, deduplicated and attacked in an isolated lab.

03

The fix goes back

Copy fix prompts Claude Code with the proof. Konvu re-runs the exploit against the fix.

Detection is solved. The decision is not.

Full comparison with every source: konvu.com/compare/konvu-vs-claude-security

Konvu docs: docs.konvu.com

Sources checked October 13, 2026: claude.com/product/claude-security, support.claude.com, code.claude.com/docs (claude-security, security-guidance, code-review), github.com/anthropics, red.anthropic.com/2026/cvd, anthropic.com/news, docs.konvu.com, konvu.com/pricing.