

KONVU VS AIKIDO

Aikido replaces your scanners. Konvu decides on their findings.

Pick Konvu if you keep Snyk, Checkmarx, Wiz or Black Duck: a verdict with evidence per finding, the exploit reproduced, the fix shipped. A small team starting from zero is probably better served by Aikido: a free plan, public prices, code-to-runtime coverage. Aikido's reachability docs list no languages, and every example is JavaScript.

Konvu is not a scanner. Aikido findings come in by upload, or API and MCP on Enterprise.

AT A GLANCE

	AIKIDO	KONVU
Question it answers	What single platform should secure our code, cloud and running apps?	Of the findings your scanners already produced, which can an attacker use, and what is the evidence?
Reachability languages	Not listed. Every example is JavaScript.	Java/Scala/Kotlin, Python, Ruby, JS/TS, C#/NET, Go, PHP, Rust
What it checks	Calls into the vulnerable symbol, dev-only deps, dead code; agent reads package use in code	Installed, environment, reachable, attacker-controllable, each met, not met or inconclusive with evidence
Verdict	Truly exploitable or not, with reasoning per CVE	Exploitable, False Positive, Needs input or Inconclusive
Fixes	AutoFix PRs for deps, SAST, IaC and containers; Libraries backports CVE fixes to the pinned version	Draft PRs that run your tests, or a coding-agent plan; exploit re-run on the fix
Write-back	Agent actions applied inside Aikido	Dismissals go back to Snyk, Semgrep, Dependabot, GitLab and ArmorCode. Jira tickets on Enterprise
Pricing	Free plan; from \$350/month for 10 users (\$35/user), plus credits for AI features	\$2,000/month for 400 confident verdicts; inconclusive runs are free

Where Aikido is stronger

- One vendor for code scanning, CSPM, containers, DAST, AI pentesting, runtime and device protection.
- A free plan for 2 users and 10 repos, and public prices.
- AI pentesting that finds new issues in running apps and APIs.
- FedRAMP Moderate listed on the Enterprise plan.

Where Konvu fits

- Teams that keep Snyk, Checkmarx, Wiz or Black Duck and carry a backlog they cannot work through.
- Backlogs assessed in place, with no migration or rescan.
- One evidence format across findings from several scanners.
- A checklist per CVE with code evidence, and the exploit reproduced against a copy of your app.

CHOOSING ONE, OR RUNNING BOTH

Aikido detects. Konvu proves and fixes.

01

Export from Aikido

Aikido's public API exports all issues as JSON, with CVE ID, package, installed version and file.

02

Bring findings in

Upload CSV, JSON or SARIF, or use API or MCP on Enterprise. Konvu reproduces each.

03

Close the loop

Konvu ships the fix; your team closes it in Aikido. API and CLI need Enterprise.

Detection is solved. The decision is not.

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

Konvu docs: docs.konvu.com

Sources checked October 13, 2026: aikido.dev (home, /code, /pricing, /fedramp-security, Zen, AI pentest, Libraries), help.aikido.dev (CVE Exploitability Analysis, AutoTriage, reachability, CI API, AutoFix, AutoShip), apidocs.aikido.dev, docs.konvu.com, konvu.com/pricing, konvu.com/integrations.