HEELER

heeler.com

AGENTIC DEVELOPMENT SECURITY

Machine-speed security for AI-written code.

Heeler prevents risk, fixes vulnerabilities, and operates the full lifecycle to verified closure — deterministically, from one context engine.

Agents write the code. AI attackers weaponize the flaws.

- **Higher volume, less scrutiny**
- **Every coding agent has a different security posture**
- **Skills & MCP: a new supply chain**
- **Legacy AppSec risk — now at machine speed**

The security operating model for agentic development.

Prevent

Stop risk as code is written.

Heeler enforces one standard at every stage — inside the coding agent, locally, and on every pull request.

COVERAGE

- MCP & Agent Skills
- CLI
- PR Guardrails

Fix

Fix everything, deterministically.

Heeler computes the fix, validates it in your CI, and opens a merge-ready PR — across the whole backlog.

COVERAGE

- SCA Auto-fix
- SAST Auto-fix
- Prioritization

Operate

Replace human-paced AppSec operations.

Native engines verify every commit. Dependency-level ownership routes every finding. Workflows manage SLOs, exceptions, and verified closure.

COVERAGE

- SCA
- SAST
- Secrets
- Agent Skills
- Workflows

TRUSTED BY AI-FORWARD TEAMS

AlphaSense · zappi · Trulioo · lendingtree · SAVVAS LEARNING COMPANY · BigPanda

Context, turned into action.

Connect repos, registries, and cloud — the graph builds itself. Context makes every fix deterministic, every guardrail precise, and every workflow routed to the right owner.

CODE
Every repo, module, and dependency — resolved, with reachability from cross-file taint analysis.

CLOUD & RUNTIME
Live services, exposure, and deployment state — mapped back to the changeset that produced them.

THREAT
CVE feeds, exploit availability, and active-exploitation intelligence, reconciled.

BUSINESS
Applications, tiers, criticality, and compliance scope.

OWNERSHIP
Who owns what — down to the individual dependency.

AGENT
The AI agent supply chain — skills and MCP servers — inventoried and scored.

WHY HEELER

Not a scanner. A platform that *acts.*

Its own engines
Purpose-built SCA and SAST, deep enough to compute a fix — not a dashboard over someone else's scanners.

SAST Auto-fix
The precise code change, computed from the vulnerable data-flow path — deterministic, not an LLM's best guess.

Exploitability, not CVSS
Reachability, exposure, and exploit intel in one signal — fixes go to what attackers can reach first.

SCA Auto-fix
The minimal upgrade that clears the CVEs and breaks nothing — validated in CI, opened as a merge-ready PR.

Sensorless code-to-cloud
Every running artifact matched to the changeset that produced it — no sensors, no build changes (patent-pending).

It secures the agents too
MCP servers and agent skills scored; PR guardrails hold every coding agent to one standard.

Replaces three categories of tools.

TRADITIONAL SCANNERS
Snyk · GitHub Advanced Security · Semgrep · Endor Labs · Mend

REMEDIATION POINT SOLUTIONS
Mobb · Pixee

ASPM & ALL-IN-ONE PLATFORMS
Wiz Code · Apiiro · Ox Security · ArmorCode

See AppSec at machine speed.

In 30 minutes, see Heeler prevent, fix, and operate — across your AI SDLC.

heeler.com/get-a-demo →

SCAN TO DEMO