

LEGIT

Agentic AppSec:

AI-Speed Defense for AI-Speed Attacks

Legit fights AI-speed attacks with
AI-speed defense – starting before
any code hits commit.



Overview

AI-led coding broke the find-it, fix-it model AppSec always relied on. Code ships faster than security teams can manage, and attackers use AI to find and exploit vulnerabilities in minutes, not months.

Legit's Agentic AppSec platform replaces manual triage with a continuous, autonomous cycle: AI-powered remediation fixes what matters most first, and those fixes feed directly back into AI coding agents so fewer vulnerabilities get introduced with every cycle. The result is an AppSec program that gets smarter over time – securing AI-generated code at a speed and scale human-led processes can't match.

How It Works: Context-Driven, Agent-Powered

The core of the Legit platform is context: a real-time understanding of each application's business criticality, sensitive data exposure, reachability, and compliance requirements. Context is what turns AI agents from noise generators into precision tools: it's the difference between a fix that matters and an alert that gets ignored.

With context:

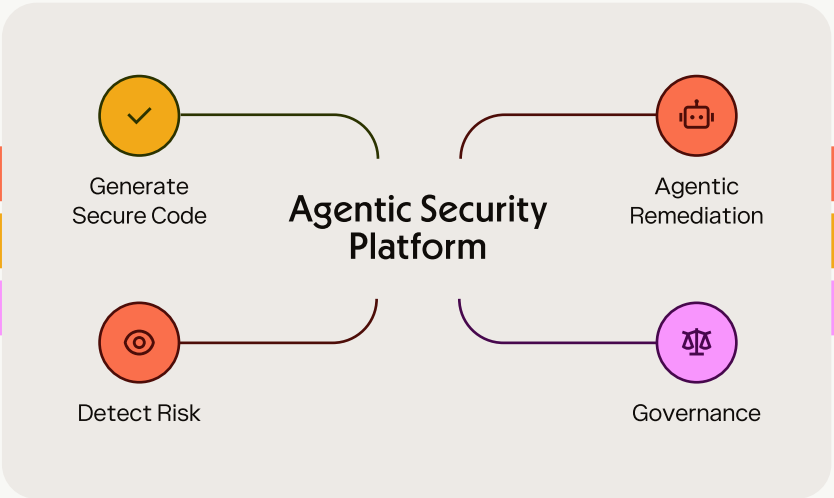
- Security teams know instantly whether a finding is truly exploitable and worth acting on.
- Remediation agents fix the highest-risk issues first – automatically.
- AI coding agents learn from every fix, so the same class of vulnerability shows up less often over time.

This is the virtuous cycle: remediation informs prevention, prevention reduces what needs remediating, and the program compounds in effectiveness with every pass.



Platform Capabilities: From Prompt to Cloud

Legit delivers Agentic AppSec across four integrated pillars, covering the full software lifecycle from code generation through production.



01 Generate Secure Code

- Injects threat models, security skills, and business context directly into AI coding tools
- Scans with Legit SAST and SCA as code is written, resolving issues pre-commit
- Real-time guardrails against prompt injection, malicious MCP servers, secret leakage, and dangerous operations
- Works across Cursor, GitHub Copilot, Claude Code, and more – goal: zero new vulnerabilities

02 Detect Risk

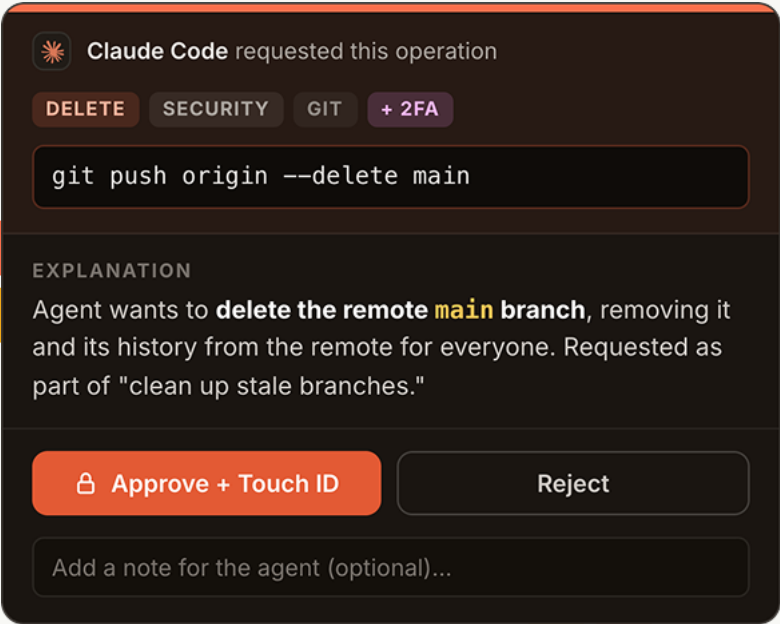
- Always-on secret scanning across code and beyond
- Code security via AST, SCA, and IaC scanners
- CI/CD risk detection, PR checks, pre-receive hooks, gated build steps
- Cuts false positives 95%+ (secret scanning) and total noise 90%+

03 Agentic Remediation

- Aggregates, deduplicates, and prioritizes findings by exposure, reachability, exploitability, EPSS, CISA KEV, and business impact
- Autonomous agents generate fixes and PRs automatically
- Fixes validated against test suites before merge; agents learn from each codebase over time

04 Supply Chain & Governance

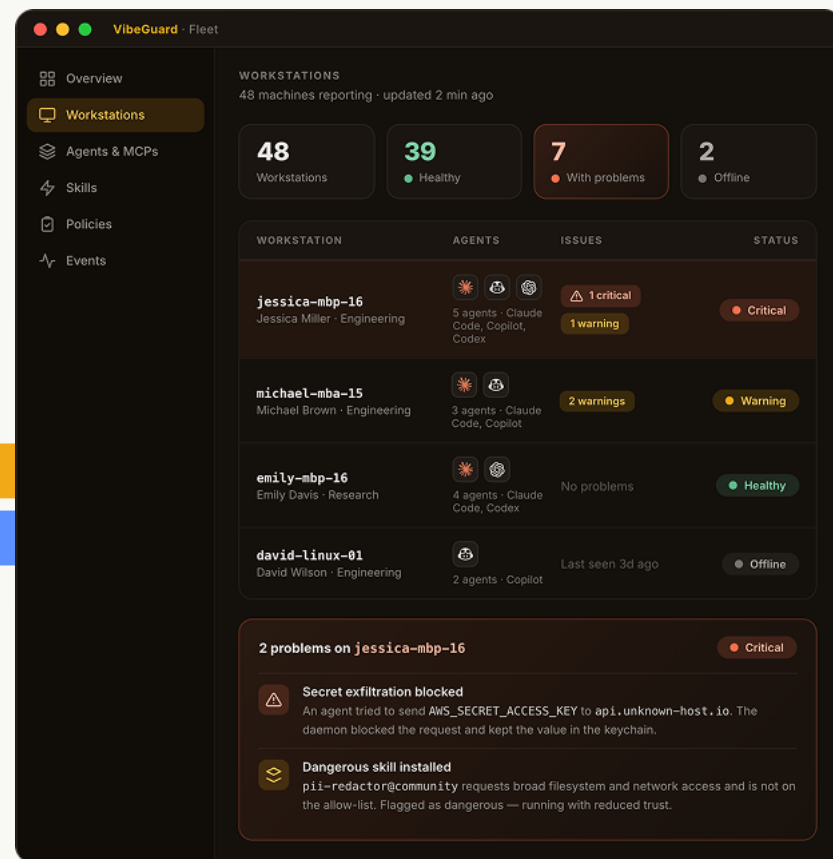
- App Governance: Discovers AI models, APIs, and data flows; flags material changes across code, GenAI models, MCP servers, and CI/CD
- Software Supply Chain Security: CI/CD discovery, Git security, compliance
- AI Advisory: Real-time, policy-based block/allow enforcement for MCP servers, skills, and plugins



Why Legit: Context Is What Matters

Legit is the only platform that leads with secure AI-led coding – stopping vulnerabilities before they’re ever committed. For Legit, find-it, fix-it is a thing of the past.

What makes this a durable advantage is context. Legit correlates code to cloud, so a critical vulnerability in an Internet-facing, PII-handling, revenue-generating application is treated as the priority it is – while a similar issue in a low-risk internal tool isn’t. Most point tools and ASPM platforms can’t tell the difference. Legit can. When Legit says it’s critical, it is.



Two Paths to Value

- 01 **Run on your stack:** Layer Legit VibeGuard, supply chain security, and AI remediation on top of your existing SAST, SCA, and CSPM tools.
- 02 **Consolidate:** Natively replace point tools for SCA, SAST, pipeline, and secrets scanning in one AI-first platform.

Not mutually exclusive – many customers start with the layer and consolidate over time.

Built For Security Teams

Built for the people accountable for risk – CISOs, VPs of Application Security, AppSec engineers – at organizations that are:

- Adopting AI coding tools faster than legacy AppSec can secure
- Resource-constrained relative to their mandate
- Under regulatory or product pressure to fix vulnerabilities early



See how Agentic AppSec keeps pace with AI-generated code.





LegitSecurity.com

Legit Security is the AppSec platform purpose-built to secure AI-powered development. Our AI-native ASPM secures modern software development, including AI-first pipelines, code assistants, agents, and vibe coding. With unmatched visibility across the SDLC and from code to cloud, Legit makes it easy to identify, prioritize, and fix AppSec issues that matter most to the business.

LEGIT