LEGIT

VibeGuard

When AI Writes the Code,
Legit Secures It - From the Start

Challenges of AI-Generated Code

- AI-generated code contains unique vulnerabilities traditional tools don't catch
- AI coding agents are risky and can expose sensitive data and assets
- The speed of AI-generated code delivery far surpasses AppSec's ability to keep up
- Fixing issues after code reaches the SCM is costly, slow, and diverts developers from building great apps fast

SOFTWARE DEVELOPMENT HAS ENTERED

An Entirely New Phase

AI agents now write, test, fix, and deploy code – a 10x acceleration in engineering velocity, but with significant new risks introduced.

"Vibe coding"
where developers use prompts to leverage AI assistants in code generation – and use of AI IDEs have quickly become the norm.

The result
AppSec is falling even further behind as development accelerates exponentially.

Legit VibeGuard

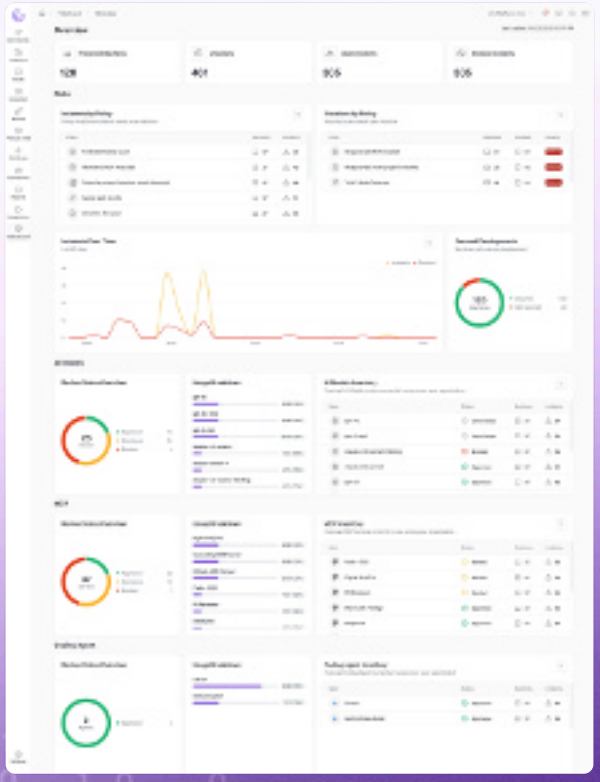
Empower coding agents to deliver secure AI code from the start

Legit VibeGuard is the industry's first AI-native solution purpose-built to enable coding agents to deliver secure AI code from the start – the very moment it's created.

Legit VibeGuard analyzes newly generated code in real-time to detect and fix vulnerabilities as they arise and governs the fleet of AI coding agents, MCPs, and AI models to prevent attacks.

With Legit VibeGuard you can:

- Enable AI assistants to generate secure code by remediating existing and newly generated vulnerabilities
- Train your coding agents to act as secure developers, reducing future risk and rework
- Apply security guardrails to protect sensitive data, prevent prompt injection, and stop model abuse



Key Capabilities of Legit VibeGuard

Complete AppSec for AI-Generated Code, Governance for AI Coding Agents

Legit VibeGuard delivers complete AppSec coverage for AI-generated code and governance for the AI coding agents used by developers.

It integrates directly into your AI IDEs and AI code assistants – such as Cursor, Windsurf, and GitHub Copilot – and others using MCP servers or custom LLM integrations into your main code base to enable continuous protection.

VibeGuard also supports efforts to protect and secure usage of AI coding agents – while governing your entire fleet of AI coders.

Real-Time Code Scanning
Analyze AI code at generation to identify and prevent risk.

Secure Agent Training
Enrich the AI agent with security context, training it to be a secure developer.

Centralized Visibility
Centrally govern the fleet of AI coding agents, MCPs, and AI models across engineering

Gain Full Code Context
Correlate AI-generated code with its application business context.

> We see AI-powered development as a huge opportunity, particularly when it comes to delivering code that is clean and secure from the start. I'm excited to see Legit take this big step forward in delivering capabilities that will help us greatly reduce risk while at the same time ensuring fast code delivery.

Nir Yizhak
CISO and VP at Firebolt

Beyond VibeGuard

Comprehensive Governance for AI-Powered Dev

Legit offers the most comprehensive set of capabilities to secure and gain complete visibility into AI-powered development.

Beyond VibeGuard:

Legit's Governance & Security for AI-Powered Development

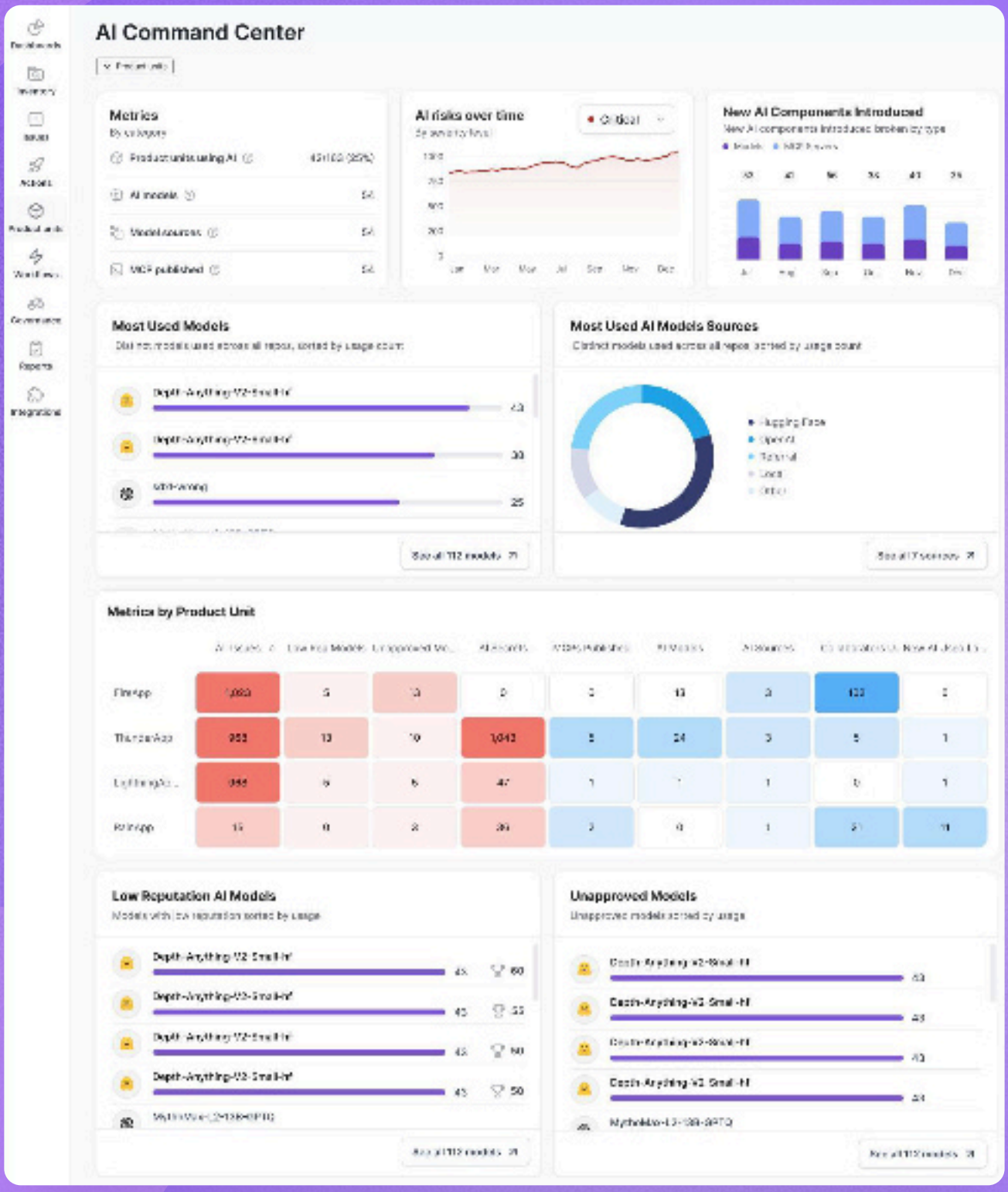
- Secure AI code at generation within AI IDEs and vibe coding platforms
- Govern and train AI coding agents to deliver secure code, prevent attacks
- Gain complete visibility into AI code, models, MCP servers in use across the SDLC
- Test for AI risk and vulnerabilities in code, create AI Bill of Materials

AI Security Command Center

Gain unified visibility into AI-generated code, AI models, and MCP servers across the SDLC.

AI Security Testing

Build your AI Bill-of-Materials (AI-BOM), test code for AI-related risks and vulnerabilities, apply runtime protection for deployed AI apps.


AI Command Center
Metrics
AI risks over time
New AI Components Introduced
Most Used Models
Most Used AI Models Sources
Metrics by Product Unit
Low Reputation AI Models
Unapproved Models