ENDOR LABS

Secure AI-Generated Code at the Source

The AI code revolution has arrived

Developers are moving faster than ever thanks to AI coding assistants like GitHub Copilot and Cursor. Today, over 40% of code is AI-generated. Tomorrow it could be 80%.

But while code velocity increases, security is struggling to keep up.

By the Numbers

77k + organizations are using AI coding assistants

62 % of AI-generated code solutions contain bugs or security vulnerabilities

30 % include known security weaknesses — even from top models

Traditional AppSec tools weren't built for this. SAST and SCA scan for known weaknesses and vulnerabilities. But AI-generated code introduces security design flaws — like changes to authentication methods, new API endpoints, or cryptographic logic — that don't map to CVEs or CWEs.

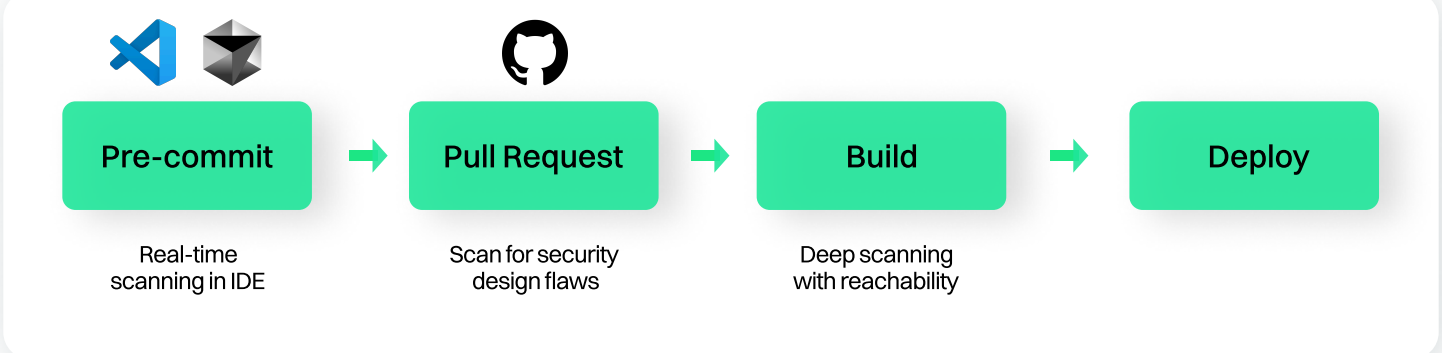
And manual code reviews? They can't scale.

Integrate security into AI-native development

Endor Labs is the AppSec platform built for the era of AI-native software development. With deep insight into the open source code AI is trained on, we help you find and fix the risks that matter — earlier than ever before.

Our platform secures AI-generated code at the source:

- **Before the PR:** Give AI coding tools like GitHub Copilot and Cursor the context they need to detect and fix security issues directly in the IDE, as code is written.
- **At the PR:** Use multiple AI agents to review every pull request for changes to your security posture — including design flaws and architectural changes that traditional tools miss.



Trusted by Security Leaders

"We're looking for better ways to scale how we identify business logic risks and unknown unknowns in our codebase. Traditional static analysis tools haven't really given us the lift we need. Being able to detect risks that we'd otherwise miss manually or through traditional automation would be hugely valuable.

– Mark Breitenbach, Security Engineer at Dropbox

Integrate security into AI-native development

- **Secure code before it's committed.** The Endor Labs MCP Server integrates directly into AI-native tools like GitHub Copilot and Cursor to detect issues as developers code.
- **Fix vulnerabilities with confidence.** Suggests fixes based on deep context about how code behaves — not just blanket upgrades — to avoid breaking changes.
- **Keep developers in flow.** Improve early risk detection in the AI-native tools your developers already use, without adding friction.

Detect design flaws traditional tools can't see

- **Scale security reviews with AI agents.** Agents reason like a developer, architect, and AppSec engineer — catching issues manual review might overlook.
- **Find what traditional tools miss.** AI Security Code Review flags changes to your application's architecture — including new APIs, altered auth flows, and cryptographic logic.
- **Focus on what matters.** Prioritized insights help your team zero in on the PRs that actually impact security.

Get the context you need to act with confidence

- **See what matters, not just what changed.** Endor Labs builds a graph of exactly how your application functions — not just what changed — so we can deliver precise insights, not noise.
- **Built for precision.** Our AI agents use the industry's most extensive dataset about open source code — the same code AI models learn from — with intelligence from 4.5M+ libraries and models.
- **Security, wherever you need it.** Use Endor Labs via MCP, CLI, or API — from IDE to CI — so insights flow seamlessly into your existing workflows

AppSec for the Software Development Revolution

Book a demo today and learn how Endor Labs helps secure AI-generated code from the moment it's written.

endorlabs.com/demo-request