ENDOR LABS

AppSec for The Software Development Revolution

Endor Labs evaluates code early in the SDLC and builds a complete graph of your software estate, so teams can pinpoint and fix critical risks in complex, dependency-rich code, whether it was written by humans or AI.

AppSec Is Only Getting Harder

Too Much Noise

Noisy security scanners put developers and engineers at odds

Too Long To Fix

Remediation advice is often useless or causes more harm than good

AI Everywhere

Copilots, LLMs, and vibe coding mean more code to secure without more resources

Endor Labs is the AppSec platform built to secure modern software - fast, open source-driven, and increasingly AI-generated. Our platform brings together AI-powered security code reviews, code scanning, risk-based prioritization, and efficient remediation in one complete graph of your software estate, giving teams visibility into change and risks across AI and human generated code, and delivering clear, actionable fixes. Everything is driven by flexible policies and APIs that integrate to scale with development.

| The Challenge	The Solution
Endless CVE alerts bury real risk and tax developers	Reachability-based SCA cuts 92% of noise by focusing on fixable, function-reachable vulnerabilities in direct and transitive dependencies
Remediation backlog affects releases and compliance (e.g. FedRAMP)	Upgrade Impact Analysis points developers to safe upgrade paths, and Endor Patches apply small, proven fixes, speeding remediation 6.2X
AI assistants add unvetted code and design drift	AI Security Code Review scans every pull request and flags risky changes, while our MCP server injects security to code generation in the IDE
Disparate security scanners have high maintenance costs and make correlation hard	Endor Labs unifies SCA, SAST, Secret Scanning, and Container scanning into one policy-driven platform
Unapproved AI models and OSS packages create new risk	Endor Labs evaluates and scores OSS packages and AI models on 150+ data points

" In just the first week we saw an 80% reduction in risks we had to remediate, all due to reachability analysis — *and we continue to see that number climb.*"

Raphael Theberge
Head of Security Enablement

Relativity
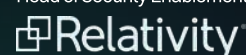
Analyze every line of code, every dependency, on every layer.
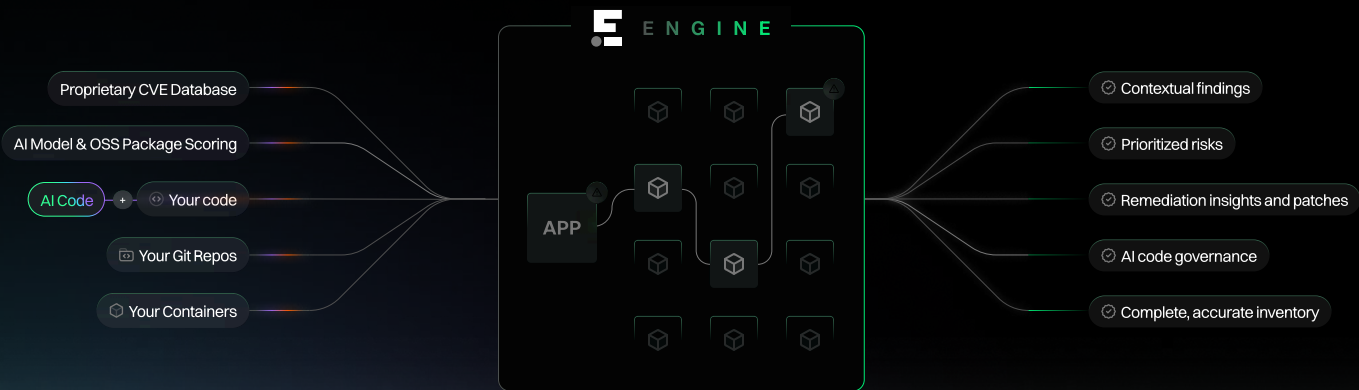
We built an unparalleled knowledge base of open source libraries, vulnerabilities, and code relationships - everything that AI is trained on. As a result, we have data and insights that are completely unique in the market:

1B Risk Factors

Detailed annotations of lines of code with vulnerabilities across open source libraries dating back a decade, and 150+ health and security checks on every open source library and AI models.

Results:

92% reduction in security noise

94% reduction in security related tickets for developers

4.5M Projects

We've Indexed billions of functions across 4.5 million open source projects and libraries in all major programming languages to understand exactly how each function works.
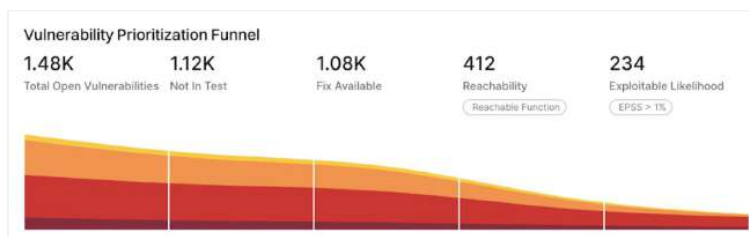
Results:

6.2x faster remediation for application security issues

500M Embeddings

Created over half a billion embeddings to identify the provenance of copied code and detect legal and security risks, even when function names or structures are changed by LLMs or developers.

Results:

Turn AppSec into an enabler for AI-assisted development

Vulnerability Prioritization Funnel

1.48K	1.12K	1.08K	412	234
Total Open Vulnerabilities	Not In Test	Fix Available	Reachability	Exploitable Likelihood
			Reachable Function	EPSS > 1%

Dev Hours Saved
6.21K hours

Cost Saved
434K

AppSec for the Software Development Revolution

Book a demo today and learn how Endor Labs can help secure your code, whether it was written by humans or AI.

endorlabs.com/demo-request