ENDOR LABS

AI Code Governance

Secure AI-generated code — and govern the agents that write it

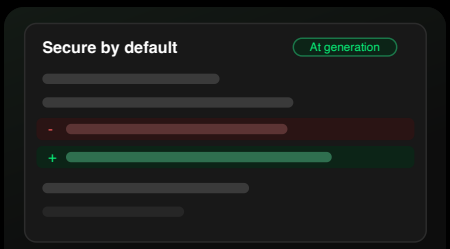
AI coding agents now generate a growing share of the code landing in pull requests — with the security flaws baked into their training data, and often with no central visibility for security. AI Code Governance secures the code at generation, reviews every pull request with security depth, and puts policy and an audit trail on every agent.

10x
fewer security tickets

83%
fewer blocked pull requests

10%
of AI-generated code is both correct and secure (Columbia/Johns Hopkins)

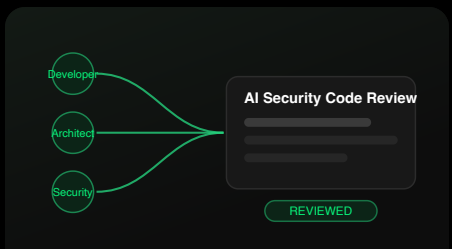
How it works



PREVENT

Secure code at the point of generation

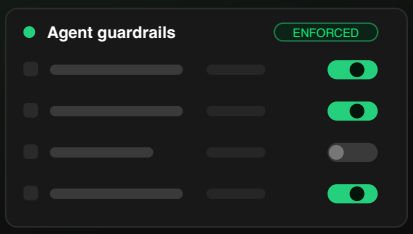
- Embed security context into Cursor, Claude Code, Copilot, and other agents.
- Stop hardcoded secrets, unsafe deserialization, and weak crypto at generation time.
- Codebase-aware guidance so agents stop repeating the same mistakes.



REVIEW

Every pull request, with expert depth

- Catch IDORs, authentication bypasses, and business logic flaws SAST misses.
- Multi-agent triage cuts up to 95% of false positives.
- Every finding ships with data flow, call paths, and evidence.



GOVERN

Policy and audit for every coding agent

- See every agent, model, MCP server, and skill in use.
- Block risky shell commands and sensitive file access in real time.
- Produce the audit trail EU AI Act and ISO 42001 expect.

CUSTOMER STORY

Zebra Technologies cut through the noise

Zebra Technologies adopted Endor Labs to focus its security program on the findings that matter. With fewer alerts and more accuracy, its teams now spend more time building and less time chasing false positives.

"Endor Labs helped us cut through the noise and focus on what matters. With fewer alerts and more accuracy, our teams now spend more time building and less time chasing false positives."

– Michael Hammond, Information Security Engineer @ Zebra Technologies

© 2026 Endor Labs. All rights reserved.

ENDOR LABS

From solution to products

The Endor Labs products that deliver each pillar

AI Code Governance extends AURI, Endor Labs' security harness for agentic software development — each pillar maps to products that share one policy engine and one code context graph.

What delivers each pillar

PREVENT

AURI

The security harness for agentic development — embedded via Hooks, Skills, MCP, and CLI.

PREVENT

Secrets Detection

Detects and validates exposed secrets; stops new leaks at pre-commit.

REVIEW

AI SAST

AI-native detection, triage, and remediation of flaws in source code.

REVIEW

AI Security Code Review

Continuous AI code security reviews for pull requests.

GOVERN

Agent Governance

Sees every AI coding agent, model, MCP server, and skill in use.

GOVERN

Agent Control Plane

Blocks destructive commands and unsafe file access in real time.

ONE PLATFORM

One policy engine, no parallel tools

Agent Governance builds on the same AURI policy engine that already enforces code, SCA, and container policy — so security teams extend what they already use rather than adopting a standalone AI security tool. It plugs into the tools developers already use — Cursor, Claude Code, GitHub, GitLab — with no rip-and-replace.

© 2026 Endor Labs. All rights reserved.