AURI
ENDOR LABS

Security Intelligence
for Agentic Software Development

AI has transformed the software development lifecycle. This is a massive win for developers, but it also means agents are introducing code, dependencies, and container images at a scale humans can't review.

85%
of developers are using AI coding assistants

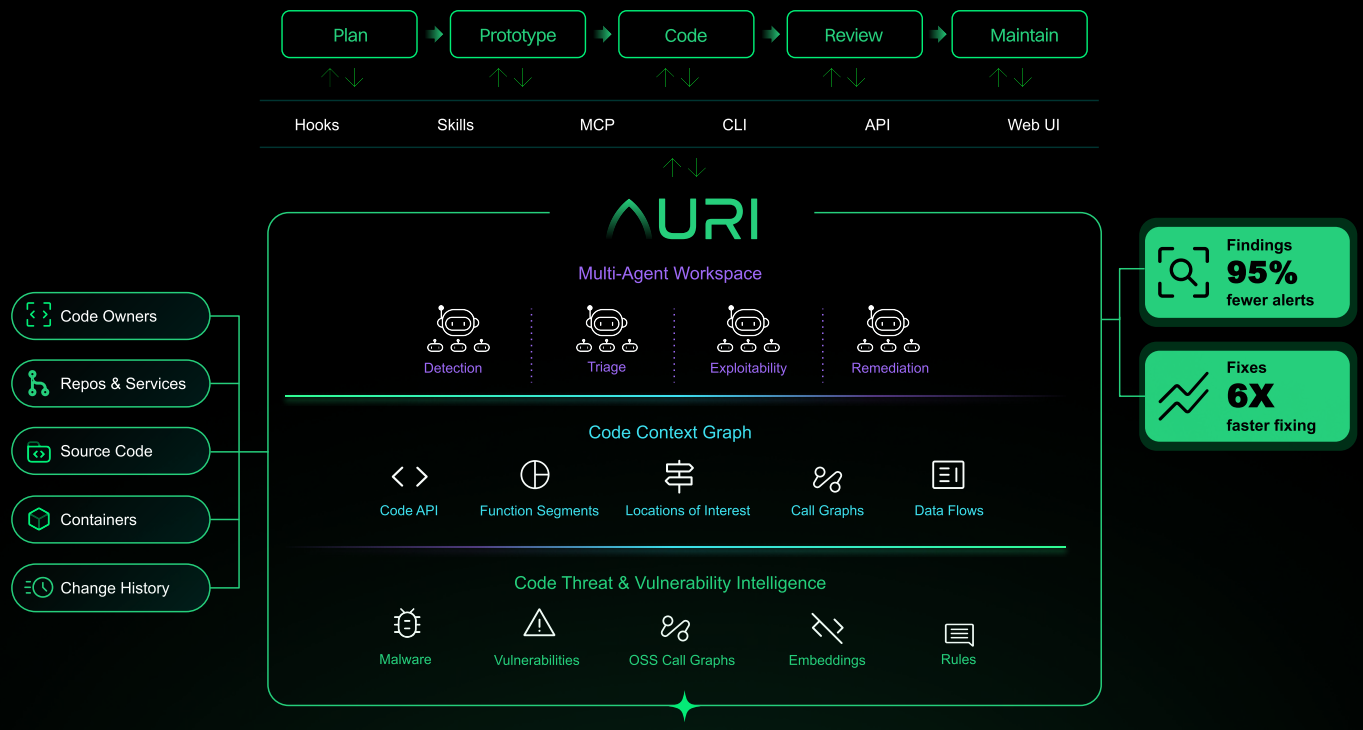
60%
of development teams are using 5+ tools

only **10%**
of AI-generated code is both functionally correct and secure

Security can no longer be a checkpoint after code is written. It needs to be embedded directly into the development lifecycle so agents produce secure code wherever they work.

Security in every line of code

AURI by Endor Labs meets developers where they work — inside tools like Claude Code and Cursor — and powers a team of security agents that work across code generation, review, and remediation.



Trusted by the world's most innovative teams

ATLASSIAN · CURSOR · Dropbox · OpenAI · glean · Robinhood · rubrik

> Over 97% of vulnerabilities flagged by our previous tool weren't reachable in our application. AURI by Endor Labs shows the few impactful vulnerabilities, so we can patch quickly, focusing on what matters."

Travis McPeak
Security at Cursor

Teams build faster and safer with AURI

10x
fewer security tickets

83%
fewer blocked pull requests

6x
faster vulnerability remediation

Deep code intelligence

- **Multi-modal detection:** Combines agentic reasoning with deterministic program analysis to identify both complex logic flaws and well-known vulnerabilities.
- **Code-level understanding:** Uses multi-file and multi-function data flow analysis, source-to-sink taint analysis, and detection of security architecture changes.
- **Code Context Graph:** AURI is powered by the code context graph, a map of your entire stack, from first-party code through open source dependencies to container images.

Full-stack reachability

- **Full-stack reachability analysis:** Trace data flow and call paths across your code, direct and transitive dependencies, and container images to determine real exploitability.
- **Reduce false positives:** Reduce vulnerability noise by up to 95% by identifying which issues are actually reachable and exploitable in your application.
- **Transparent evidence:** Clear data flow and call path evidence helps security and engineering align on real risk while simplifying compliance for frameworks like FedRAMP, PCI DSS, and CRA.

Agentic remediation

- **Don't wait for the pull request:** AURI continuously validates and fixes code as developers and agents work, keeping releases shipping while ensuring code is secure by default.
- **High-impact fixes:** AURI identifies the vulnerabilities with the highest security priority and lowest impact on agents and developers.
- **Meet developers where they work:** AURI Integrates into AI code editors, code review, CI, and autonomous agents, connecting via Hooks, Skills, MCP, or CLI.

Don't choose between speed and security

Book a demo and see how AURI enables teams to code without compromise.

endorlabs.com/demo-request