ENDOR LABS

AI SAST

Static analysis that eliminates up to 95% of false positives

Legacy SAST flags 68–78% false positives on average and misses the OWASP Top 10 categories that cause the most real damage. AI SAST is a new foundation for static analysis: multiple specialized AI agents that read, trace, and reason about code the way a security engineer would — combining rule-based pattern matching, dataflow analysis, and multi-pass LLM reasoning on Endor Labs' semantic Code API.

95%
of false positives eliminated before they ever reach a developer

68–78%
average false positive rate of the legacy SAST it replaces

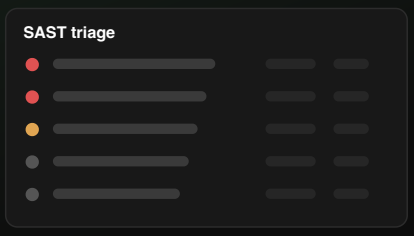
Minutes
to fix a finding with a context-aware remediation — down from 4+ hours

How it works

DETECT

Trace data like a security engineer

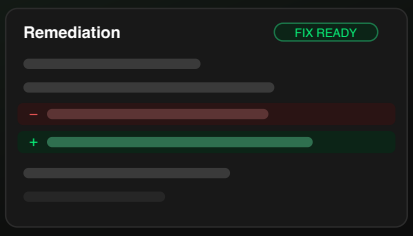
- Trace user-controlled data from source to sink across 3–5 architectural layers and multiple files
- Catch IDOR, broken access control, and insecure design — categories rule-based SAST misses
- Cover the full OWASP 2025 Top 10, including flaws that require semantic understanding



TRIAGE

Every finding classified automatically

- Classify each finding as true positive, false positive, or unknown — with a written explanation
- Recognize legitimate patterns in context instead of flagging everything that matches a rule
- Block pull requests only on high-confidence findings using OPA-based policies



FIX

A fix, not just a finding

- Generate a specific, context-aware fix recommendation alongside every confirmed vulnerability
- Adapt to your architectural patterns and risk priorities through custom prompts and feedback
- Plug into existing CI/CD pipelines and the Endor Labs policy engine — no separate workflow

CUSTOMER STORY

Fewer alerts, more accuracy — and developers who act on findings

When triage costs 15–30 minutes per false positive and enterprises face 1M+ alerts a year, findings stall in backlogs. Accuracy changes developer behavior — that's the shift Endor Labs customers describe.

"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