ENDOR LABS

# Upgrade Impact Analysis

## Know which upgrades are safe before you bump a version

Open source security fixes are easy to find and hard to ship — most live in a newer version of the library, bundled with breaking changes the application team did not ask for. Upgrade Impact Analysis analyzes every viable upgrade path against your actual code and ranks each by remediation risk, so remediation becomes a ranked backlog instead of a research project.

**Every**
viable upgrade path analyzed against your actual application

**Days**
of manual research per vulnerability replaced with ranked evidence

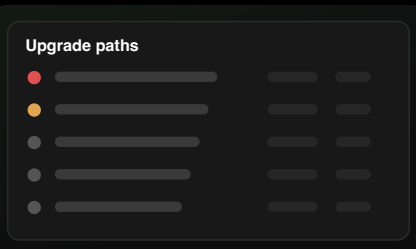
**3 tiers**
of remediation risk — High, Medium & Low — scored per upgrade

## How it works


ANALYZE

### Your code, not a generic diff

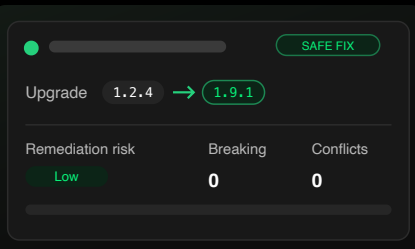
- Surface the exact functions, interfaces, and dependency conflicts likely to break
- Compare paths across direct and transitive upgrades, including overrides and pins
- Build on the same program analysis engine behind function-level reachability




PRIORITIZE

### A ranked backlog, not a debate

- See every vulnerability an upgrade resolves alongside the work it will require
- Give security and engineering one shared evidence base for prioritization
- Pair with reachability so teams fix what's actually exploitable first




SHIP

### Low-risk fixes merge in minutes

- Move easy upgrades into automated remediation PRs developers can merge quickly
- Plan hard upgrades like feature work — by effort and impact, not CVE severity alone
- Hand off to Endor Patches when an upgrade is too disruptive — same platform

WHY NOW

## The upgrade-or-stay-vulnerable dilemma stalls every AppSec program

Developers refuse to merge version bumps they cannot estimate the impact of — reasonably — so CVEs get parked indefinitely while manual upgrade research burns days per vulnerability. Prioritization meetings stall because security and engineering have no shared evidence for what each fix will actually cost. Upgrade Impact Analysis changes the conversation: the easy fixes ship immediately, the hard ones get scoped honestly, and nobody accepts risk by default.