

Secure Everything Your Code Depends On.

Software Supply Chain Security Without the Productivity Tax

June 2024

ENDOR
LABS

What is **software supply chain security**?

If you need it to deliver software (develop, build, deploy, run, or manage),
and you didn't write it, it's in your supply chain.

Code & Dependencies

the applications

Processes & Policies

the people

Systems

the pipelines, tools, infra

Here lie some of the biggest challenges

- Application dependencies
- Code-and-build dependencies
- Operational dependencies

Your organization **is struggling with product security.**

(AND EVERYONE IS MAD AT APPSEC)

You're slowing me down!



Dev

I can't triage this noise!



DevSecOps

Where are your SBOMs?



GRC

AppSec



Don't slow down my pipelines!



Platform Eng

I can't trace these vulns!



SecOps

Secure everything **your code depends on.**

(BE THE SECURITY PARTNER WHO MAKES CODE SHIP FASTER)



Dev

- AI-assisted OSS selection
- Upgrade impact analysis*
- Endor Magic Patches*



DevSecOps

- SCA with reachability
- SAST*
- Container scanning
- Secret detection



Platform Eng

- Artifact signing
- Container scanning
- Repo & pipeline posture mgmt
- GitHub Actions security



SecOps

- OSS Top 10 detection
- Repo to CNAPP traceability

CODE

BUILD

DEPLOY

RUN



AppSec

- SDLC visibility
- Granular policies
- Prioritized dashboards



GRC

- Compliance acceleration (PCI, FedRAMP, etc.)
- SSCS best practices (CIS, SLSA, NIST SSDF, etc.)
- Code provenance & attestation
- SBOM/VEX management

* Releasing in 2024

Endor Labs' secret ingredients.

“Endor Labs is helping us prioritize mission critical third-party library vulnerabilities. I would say their function-level reachability is unparalleled.”

- Principal Product Security Engineer

SCA with Reachability

90%

average noise reduction
by applying prioritization

SDLC Security

5-in-1

best-in-class scanners
consolidated in one tool

Reduced Time-to-Fix

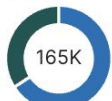
8

hours saved per vulnerability by
automating remediation research

Endor Labs' Customer Example

Scanned By Endor Labs

Dependencies



Direct 56K
Transitive 109K

Vulnerabilities



Reachable 138K
Potentially Reachable 452K
Unreachable 94K

Projects

14.2K

Packages

32K

Scans

26.3K

Notifications

177

Displaying Critical High Medium Low

Vulnerability Prioritization Funnel

781K

Total Open Vulnerabilities

623K

Not In Test

579K

Fix Available

495K

Reachability

Reachable Function

Potentially Reachable Funct...

38.5K

Exploitable Likelihood

EPSS > 5%



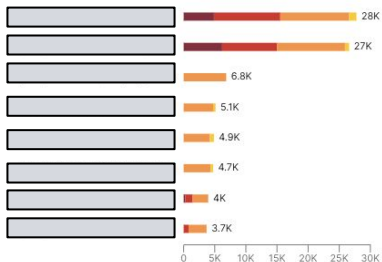
Dev Hours Saved

584K hours

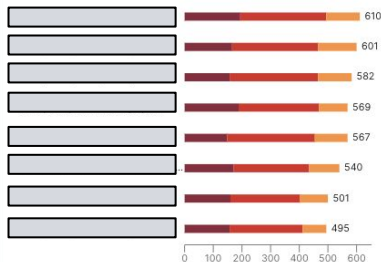
Cost Saved

29.2M

Top Projects By All Findings



Top Packages By Reachable Vulnerabilities



Top Dependencies By Reachable Vulnerabilities

