ENDOR LABS

Software Supply Chain Security

Stop malicious packages, cut the noise, patch what's hard to fix

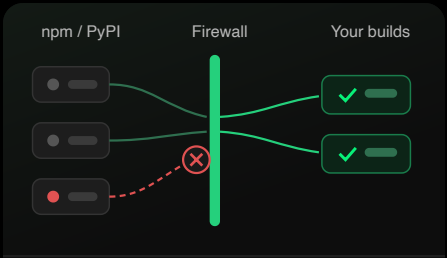
Supply chain attacks have shifted from rare events to a daily reality — malicious packages land in npm and PyPI every day, CVEs get weaponized in days, and CI/CD pipelines are the soft target attackers go after first. Endor Labs covers the full supply chain, from the registry edge to the build pipeline.

92%
average false positive reduction for SCA findings

6x
faster CVE remediation reported by customers

150+
supply chain risk signals on the Package Firewall

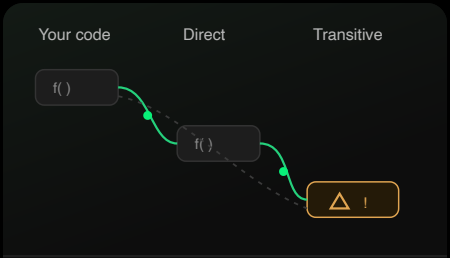
How it works



BLOCK

Real-time enforcement at the registry edge

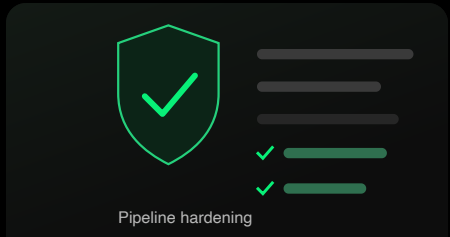
- Block malware, typosquats, and policy-violating packages at install time.
- Detect novel malware on npm, PyPI, Maven, and NuGet within minutes.
- One policy covers human developers and AI coding agents alike.



PRIORITIZE

Fix what attackers can actually reach

- Filter out findings attackers cannot reach from your code paths.
- See exactly what an upgrade will break before opening the PR.
- Backported patches fix CVEs on your current version — no breaking changes.



HARDEN

Secure the pipeline attackers now target

- Inventory every GitHub Actions workflow, its actions, and its secrets.
- Catch exposed secrets in workflows and logs before attackers do.
- Enforce hardening policies across every repo without hand-editing workflows.

CUSTOMER STORY

Cursor patches the vulnerabilities that matter

Cursor compared its existing scanner's backlog against Endor Labs and found that over 97% of previously flagged vulnerabilities were not reachable in its application — so the team now focuses remediation on the few findings that are.

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

– Travis McPeak, Security @ Cursor

ENDOR LABS

From solution to products

The Endor Labs products that deliver each pillar

Software Supply Chain Security is not a bundle name — each pillar maps to specific Endor Labs products, all built on the same dependency intelligence and enforced through one policy engine.

What delivers each pillar

BLOCK

Package Firewall

Blocks malicious, vulnerable, and policy-violating packages at install time.

BLOCK

Malicious Package Detection

Catches malware public feeds miss, within minutes of registry upload.

PRIORITIZE

SCA with Reachability

Shows which vulnerabilities are actually exploitable in your code.

PRIORITIZE

Upgrade Impact Analysis

Predicts breaking changes and ranks every upgrade by risk.

PRIORITIZE

Endor Patches

Backports the upstream security fix to the version you already run.

PRIORITIZE

Container Reachability

Cuts container vulnerability noise by up to 90%.

HARDEN

Secrets Detection

Detects and validates exposed secrets in code, workflows, and logs.

HARDEN

Artifact Signing

Signs every build artifact and verifies it at deployment.

HARDEN

SBOM Hub & VEX

One place to ingest, manage, and continuously monitor every SBOM.

ONE PLATFORM

Built on the same dependency intelligence

Every product draws on the deepest dependency intelligence in the industry — every direct and transitive dependency, with reachability, exploitability, and license context attached — and plugs into the artifact repositories, package managers, and CI/CD systems your teams already use: JFrog, Nexus, GitHub, GitLab. No rip-and-replace.