ENDOR LABS

Container Security & Reachability

Container scanning that cuts vulnerability noise by up to 90%

Container images bundle the application iceberg — app code, language runtimes, shared libraries, and OS packages — and traditional scanners treat every installed package as equally risky. Container Reachability extends Endor Labs' function-level reachability through the runtime and OS layers, classifying every package as Reachable, Potentially Reachable, or Unreachable — application by application.

50–90%
noise reduction on real-world container images

96%
of public container images contain vulnerabilities — most never load

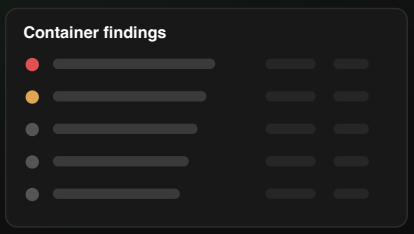
0 agents
no sidecars, daemonsets, or production agents required

How it works

MAP

See the whole application iceberg

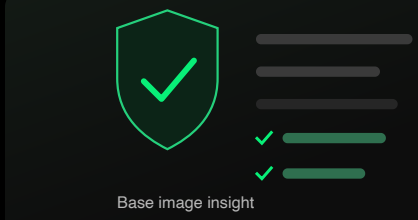
- Know which OS packages and shared libraries the running application loads versus which sit dormant
- Cover Debian, RPM, and Alpine ecosystems in the same graph as your application SCA
- Combine static dependency graph construction with dynamic profiling in a sandbox



PRIORITIZE

Evidence that survives an audit

- Defensibly deprioritize unreachable vulnerabilities under FedRAMP's 30-day windows
- Deduplicate SCA and container findings so each vulnerability is one ticket and one fix
- Block builds on reachable findings and let unreachable ones through — by policy



MAINTAIN

Safer base images without lock-in

- See which OS packages downstream applications actually use before pruning a shared base image
- Aggregate reachability across application images to design cleaner golden images
- Skip the forced migration to vendor-locked hardened or distroless images

CUSTOMER STORY

Focus on the few vulnerabilities that matter

Reachability changes the remediation math: when most findings are provably unreachable, the backlog shrinks to the small set worth engineering time.

"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