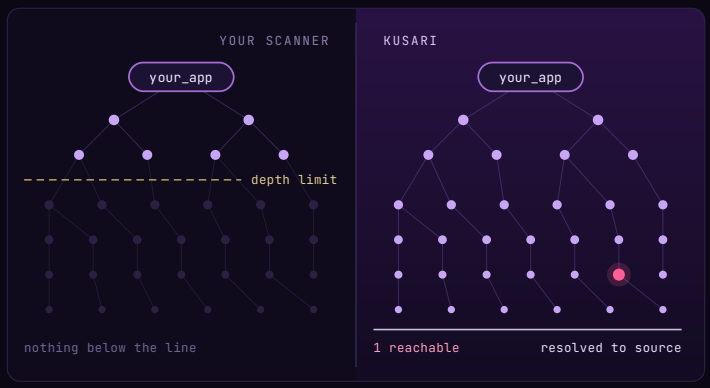
kusari

FOR CISOS AND SECURITY LEADERS

Find the gaps your scanner can't see.

Security leaders choose Kusari to prioritize software supply chain risk, verified at source.



Built by the team behind GUAC and SLSA

COMMERCIAL AND OPEN SOURCE PARTNERS

Google Microsoft intel. Red Hat vmware yahoo! DTCC
GUIDEWIRE Roche ClearAlpha PURDUE

95% of software vulnerabilities sit at least two layers below the dependency your developer actually changed.

THE THREE QUESTIONS YOU HAVE TO ANSWER

01
Do we have this dependency, and in which artifacts and services?

02
Where did it come from, and does the build match the source?

03
What's exploitable right now, and what's the proven fix?

See past your direct dependencies

Most exposure sits below the dependency your team actually chose. Kusari traces it down through every layer, verified at source.

`Transitive depth` `Traceability` `Blast radius`

Prioritize on a foundation you can trust

Reachability and exploitability analysis put only genuinely exploitable findings in your team's queue.

`Kusari Score` `Reachability` `Open methodology`

Ship fixes you can defend

AutoFix generates and validates environment-aware fix PRs, so the fix is vetted before it reaches your repo.

`Kusari Agent` `AutoFix` `Inspector`

<2%
false positives, verified against source, not estimated
ACCURACY

90%
of vulnerability noise removed from a backlog tens of thousands deep
NATIONAL HEALTH INSURER

82%
faster mean time to remediate, with proof behind every closed fix
KUSARI PLATFORM

> "We invest heavily in application security, but we had a real gap in transitive and indirect dependencies. The last thing we want is another Shai-Hulud without Kusari in place."
>
> Director of Security Architecture · 6,000-seat health insurer

The next zero-day is coming. Have the answer ready.

Request a demo →