ENDOR LABS

SBOM Hub & VEX

One system of record for every SBOM — yours and your vendors'

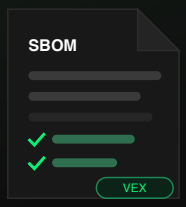
Software transparency has moved from a nice-to-have to a regulatory and commercial requirement: Executive Order 14028, the EU Cyber Resilience Act, FDA rules, and enterprise procurement teams all expect an SBOM and a VEX document on demand. SBOM Hub ingests, generates, and continuously monitors every first-party and third-party SBOM across the enterprise.

Seconds
to find every affected application — yours and your vendors' — when the next Log4j hits

2 standards
supported end to end: CycloneDX and SPDX, in the format stakeholders ask for

Continuous
monitoring of every stored SBOM against the Endor Labs vulnerability database

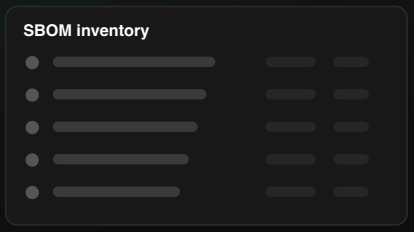
How it works



GENERATE

SBOM and VEX in any format

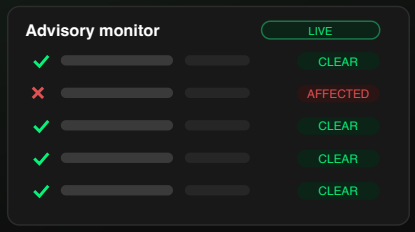
- Generate CycloneDX or SPDX SBOMs automatically in CI for every supported language
- Produce a VEX with reachability-based justification for which vulnerabilities actually apply
- Meet evidence requirements for EO 14028, CRA, FedRAMP, PCI DSS, and FDA without manual exports



CENTRALIZE

First- and third-party in one place

- Store your SBOMs and your vendors' in one inventory instead of scattered folders
- Ingest vendor SBOMs directly from their pipeline so updates land the moment they ship
- Apply the same Endor Labs scoring to imported components as to your own code



MONITOR

Risk that stays current

- Get alerted when a new vulnerability affects a component in any stored SBOM — no re-scan
- Pivot from a CVE to every affected application, across your code and your vendors'
- Keep risk profiles current automatically as new advisories are published

WHY NOW

A shared folder is not a system of record

Most organizations store SBOMs in SharePoint, Google Drive, or team intranets — with no canonical version per release, no consistent format across vendors, and no way to answer portfolio-wide questions. A static SBOM reflects risk at the moment it was created, not today: when a new CVE drops, teams without continuous monitoring spend days or weeks working out which applications and which vendors are affected. Meanwhile customers now request SBOMs as part of enterprise deals — and "we'll get back to you" slows the sale.