

Endor Labs for Connected Products

AppSec built for firmware, devices, and embedded software

From industrial HVAC and EV charging to smart meters and consumer wearables, connected products ship software at their core — and AppSec tools built for cloud SaaS cannot inventory their firmware, separate real exploits from noise, or remediate without risking a recall. Endor Labs is the AppSec platform built for the product side.

40+

languages covered by function-level reachability — including C/C++

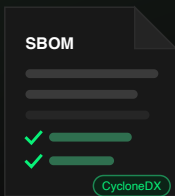
92%

average false positive reduction for SCA

6x

faster CVE remediation with safe upgrade paths

How it works

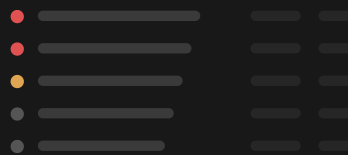


INVENTORY

Accurate SBOMs for every product

- Inventory firmware built in C, C++, Rust, and mixed languages
- Export CycloneDX or SPDX for CRA, FDA, and customer reviews
- Answer “what’s in this device” the day a critical CVE drops

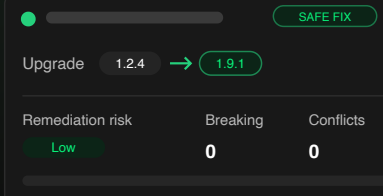
Findings



PRIORITIZE

Cut CVE noise to what's exploitable

- Function-level reachability shows which vulnerable functions the device actually calls
- Defensibly deprioritize unreachable CVEs to regulators and customers
- Stop burning firmware engineering hours on findings that aren't real



FIX

Remediate without bricking the device

- Upgrade Impact Analysis shows what breaks before certification and rollout
- Endor Patches backport fixes when an upgrade doesn't fit the release
- Close transitive CVEs on long-supported devices without clean upgrade paths

CUSTOMER STORY

Zebra Technologies cuts the noise, ships the next release

Daikin, Whoop, Peloton, Zebra, ChargePoint, Itron, and other connected product companies trust Endor Labs to keep AppSec ahead of CRA and customer requirements — without slowing the product engineering teams shipping the next firmware release.

“Endor Labs helped us cut through the noise and focus on what matters. With fewer alerts and more accuracy, our teams now spend more time building and less time chasing false positives.”

– Michael Hammond, Information Security Engineer @ Zebra Technologies