ENDOR LABS

Reduce FedRAMP Compliance Costs

Complex and time consuming

Open source vulnerability management is a challenging requirement for FedRAMP compliance. You must scan all code and containers in your organization to identify vulnerabilities — and fix them within defined timeframes. This is an expensive requirement, and many organizations struggle to meet FedRAMP SLAs for fixing vulnerabilities. Legacy tools generate a lot of noise, and leave application security teams to correlate findings, prioritize vulnerabilities, and to remediate problems on their own. It's time your SCA tool helped you get those costs under control.

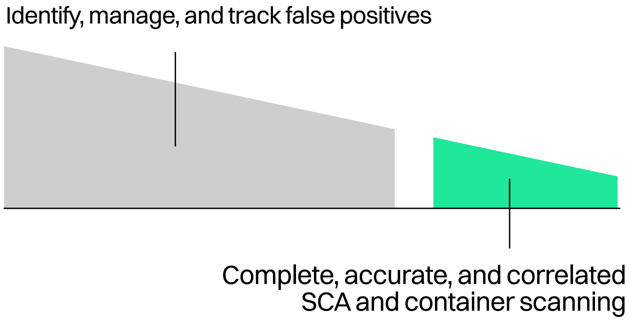
By the Numbers

742%	average yearly increase in software supply chain attacks[1]
187	average days to remediate CVEs in open source libraries[2]
61%	of businesses impacted by a software supply chain attacks in the past 12 month[3]

Higher confidence, lower costs

Endor Labs reduces false positives and prioritizes real vulnerabilities, helping your team meet FedRAMP requirements with less stress and lower costs. On average, Endor Labs customers experience a **70-80% reduction in their remediation workload** and remediate vulnerabilities **6.2 times faster.**

Remediate vulnerabilities 6.2x faster



Without Endor Labs: **187 days to fix.**

Jan Feb Mar Apr May Jun

Jan

With Endor Labs: **30 days or less.**

[1] The Evolution of Software Supply Chain Attacks (Sonatype)
[2] Endor Labs survey
[3] 2023 Software Supply Chain Survey (Capterra)

Trusted by Security Leaders

“Without the tedium and minutia of tracking down individual items that might not matter, we can focus on the remaining vulnerabilities that would impact customers and our FedRAMP compliance.”

– Raphael Theberge, Head of Security Enablement at Relativity

Complete, accurate, and correlated SCA and container scanning

- **Identify all dependencies.** Go beyond manifest files to pinpoint all direct and transitive dependencies, including phantom dependencies not included in manifest files.
- **Scan before deployment.** Prevent container vulnerabilities from entering production by scanning the base image and application dependencies.
- **Correlate results.** Natively correlate container and SCA results to simplify your POA&M tracking, reducing noise from duplicated results.

Identify, manage, and track false positives

- **Identify vulnerabilities at the function level.** Understand which dependencies are reachable in your code, down to which functions are being called.
- **Prioritize risk.** Separate vulnerabilities that are likely to be exploited and need urgent attention from findings FedRAMP assessors will accept as false positives.
- **Reassess and monitor changes.** Get prompt updates should code changes in your application result in a vulnerability becoming reachable.

Save time and money on patching vulnerabilities

- **Get the work where you need it.** Intelligent, policy-driven routing of findings to the places where your software engineering teams are already working.
- **Find the best upgrade paths.** Upgrade Impact Analysis helps you select the best upgrades options and plan work effectively.
- **Avoid the riskiest updates.** Use Endor Patches to remove the risk of breaking changes when an upgrade will take longer than the allowed SLA for FedRAMP.

Secure everything
your code depends on.

Book a demo today and learn how Endor Labs can reduce the costs and work of managing FedRAMP compliance requirements.

endorlabs.com/demo-request