Mend SCA

The Gold Standard for Open Source Risk Reduction

The Challenge

Open source components help developers create better applications faster, but they also introduce multiple sources of risk for organizations. Open source vulnerabilities can leave applications open to attack, licensing complexities can create legal hazards, and malicious packages can allow threat actors to wreak havoc on your applications and systems.

With potential threats taking many forms across the software development life cycle, security leaders need a way to protect every developer and every application from multiple forms of risk.

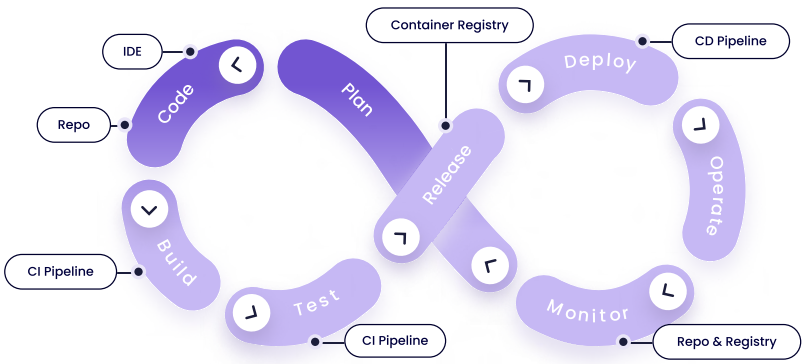
The Solution

At Mend.io, we approach the problem of open source risk and SCA (software composition analysis) differently. Mend SCA gives organizations full visibility and control over open source usage and security—and makes it easy for developers to remediate open source risk directly from the tools they already use.

Running silently in the background, Mend SCA detects open source components (including direct and transitive dependencies) every time a developer commits code or builds the application. When Mend SCA detects vulnerabilities, malicious packages, or licensing policy violations, it can issue real-time alerts with automatic remediation capabilities, or even block malicious packages and licensing violations before they become part of your code base.

Remediate Open Source Risk at Every Step

Mend SCA supports teams in every phase of the software development life cycle. It integrates with IDEs, repositories, registries, and CI/CD pipelines to provide automated risk remediation and policy enforcement that works while you code, build, deploy, and improve your applications.



Why Mend SCA?

Reduce MTTR

Accelerate remediation with automated pull requests to fix open source vulnerabilities fast.

Stop Malicious Packages

Detect and eliminate malicious packages in your existing code base and block them from entering new applications with Mend.io's 360° malicious package protection.

Eliminate False Positives

Ensure your developers are focused on real risks. Mend SCA detects whether vulnerabilities are actually reachable, indicating non-exploitable vulnerabilities that can safely be ignored.

Automate Dependency Updates

Proactively reduce up to 70% of vulnerabilities from your code base by automatically identifying outdated dependencies and generating pull requests enriched with crowdsourced update insights.

Deploy Fast at Scale

Implement Mend SCA for thousands of developers in less than an hour, across all your applications in development.

Ensure Full Adoption

Ensure 100% adoption of Mend SCA and enhance overall risk reduction by opting to require scans after every code commit.

What You Get From Mend SCA: Features & Capabilities

Trusted by tech leaders like Microsoft, IBM, Google, and more to provide proactive application security. Security teams choose Mend SCA for its unique capabilities, including:

Broad language support - With over 200 supported languages, Mend SCA can detect vulnerabilities and licensing issues for a wide range of applications.

SBOM creation - Create and export software bills of material (SBOM) in standard formats to comply with regulatory requirements and customer requests.

Rapid critical vulnerability remediation - With immediate detection and automatic remediation of newly disclosed vulnerabilities, finish the fire drill faster so your teams can keep doing what they do best.

Reporting and dashboards - Get a holistic view of your entire open source risk picture, from licensing and compliance to your security posture and remediation backlogs.

Low developer burden - Mend SCA is a security product your developers will actually use, with fast and automated workflows that don't require switching tools.

Advanced reachability analysis - Patented reachability path analysis that shows you which vulnerabilities pose the biggest threat.

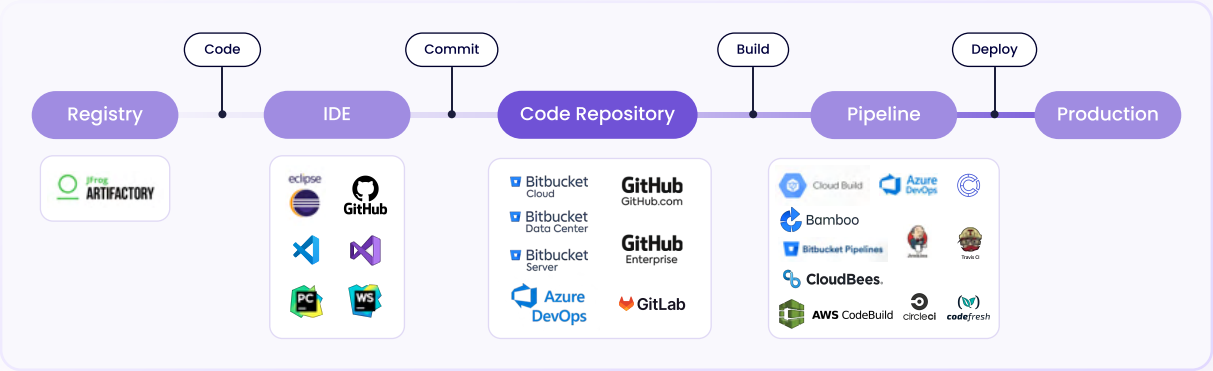
Risk-based prioritization - Gain deeper insights into vulnerability risks with CVSS 4.0 severity ratings and EPSS exploitability data.

Automated remediation - Automatic pull requests enable developers to fix security and licensing issues with a single click.

Merge confidence data - Provides developers with crowd-sourced statistics that indicate the likelihood that a dependency update will break their project.

Open source license compliance - Gives legal teams visibility and control over open source license usage.

Container image scanning - Find vulnerabilities in container image layers before they reach production.



About Mend.io

Trusted by the world's leading companies, including IBM, Google, and Capital One, Mend.io's enterprise suite of application security tools is designed to help you build and manage a mature, proactive AppSec program.

Mend understands the different AppSec requirements of developers and security teams. Unlike other AppSec solutions that force everyone to use a single tool, Mend helps them work in harmony by giving each team different, but complementary, tools—enabling them to stop chasing vulnerabilities and start proactively managing application risk.

Learn more at