Checkmarx

Selecting the right SCA solution:
a Checkmarx buyer's guide

Open source code can take you anywhere. Travel safely.

Be free to explore the opportunities that open source code creates – while doing it securely. The right software composition analysis (SCA) solution will identify vulnerabilities, potential license conflicts, and outdated libraries, giving you and your teams the actionable insight you need to avoid or remediate potential risk. And that's while your developers are coding – not afterwards.

This checklist will help you choose the right solution for your organization.

1. Focus on solutions with higher accuracy and fewer false positives. Comprehensive results can be good, but only if you have the time to review and verify them all. It's also worth noting that risk metrics aren't standardized across vendors, and can vary in severity or priority.

2. Highly consider vendors whose solution is supported by a dedicated security research team. Make sure the vendor is proactively finding zero day or non-public vulnerabilities, and enhancing their existing security records.

3. Look for vendors that provide a comprehensive list of any publicly reported vulnerabilities in open source components, together with appropriate remediation guidance.

4. Ensure the solution will fully support the requirements of your security, legal, and engineering teams. It should enable them to configure and enforce policies against the analysis results.

5. Prioritize solutions that are part of a complete application security testing (AST) portfolio, or that complement what you're currently using.

6. Certify available integrations with your package managers, build tools, code repositories, issue management solutions, and so on. Give priority to solutions which enable cross-product synergy, which will help to prioritize your remediation efforts and enhance the accuracy and actionability of the analysis.

7. Verify that the solution integrates with the tools you're already using in your SDLC or CI/CD pipelines. It must enable you to automatically trigger scans, share results, and reduce time-to-remediation.

8. Validate that the solution supports unified user management, project creation, and scan initiation capabilities for multiple testing technologies. Solutions that do this will yield the greatest efficiencies and reduce your total cost of ownership.

In summary, you need an SCA solution that complements the AST solutions you already have, integrates with the tools your developers use, and matches the way your organization develops software. This will enable you to prioritize, focus, and speed remediation efforts where they will be most effective and least costly. An SCA solution that is supported by a dedicated security research team will ensure your risk evaluation, insight, and reduction will always be based on the most up-to-date information available.

Checkmarx is named a Leader in the 2020 Gartner Magic Quadrant for Application Security Testing

Read the report

Discover next generation open source security

Checkmarx CxSCA

About Checkmarx

Checkmarx is the global leader in software security solutions for modern enterprise software development. Checkmarx delivers the industry's most comprehensive Software Security Platform that unifies with DevOps and provides static and interactive application security testing, software composition analysis, and developer AppSec awareness and training programs to reduce and remediate risk from software vulnerabilities. Checkmarx is trusted by more than 40 of the Fortune 100 companies and half of the Fortune 50, including leading organizations such as SAP, Samsung, and Salesforce.com. Learn more at www.checkmarx.com.

Checkmarx