Checkmarx Open Source Analysis (OSA)

datasheet

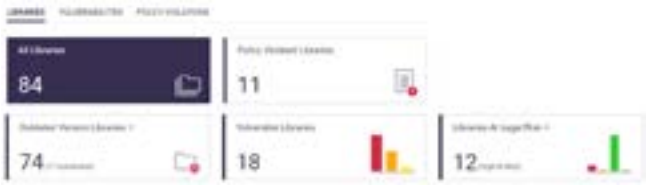
Take Control of Your Open Source

Open source software has facilitated the rapid evolution of application development and shortened development cycles. As with any new advancement in technology, there can be risks associated with open source components which organizations must identify, prioritize, and address. Security vulnerabilities can leave sensitive data exposed to a breach, complex license requirements can jeopardize your intellectual property, and outdated open source libraries can place unnecessary support and maintenance burdens on your development teams.

Checkmarx Open Source Analysis (OSA) is a software composition analysis solution that detects and identifies the open source components within your applications, and provides detailed risk metrics regarding open source vulnerabilities, potential license conflicts, and outdated libraries. Integrated as part of your secure CI/CD pipeline, Checkmarx OSA enables development and security teams to prioritize and focus remediation efforts where they will be most effective and least costly.

Reduce the Noise, Focus Security Efforts

Checkmarx OSA provides deep insight into open source security vulnerabilities affecting your applications, with risk severity metrics, detailed vulnerability descriptions, and remediation guidance to mitigate the risk of exploitation.



Only Checkmarx supports direct correlation of open source risk metrics with static analysis results from Checkmarx SAST, enabling automatic prioritization of security risks and verifying whether an open source vulnerability can be exploited within the application. Streamline application security testing efforts by scanning proprietary code and analyzing open source with one tool, and aggregate both static and software composition analysis for a complete, unified security risk profile.

Encourage Secure Open Source Consumption

Checkmarx OSA sits atop the Checkmarx Software Security Platform, providing a centralized management and orchestration layer, a single dashboard for security metrics, unified policies across all testing methods, and automated prioritization. Establish standards for security and license compliance for both custom code and open source components, trigger policy violation alerts, and leverage a full suite of integrations to automatically enforce policies throughout your CI/CD pipeline.

Automate Open Source Security: Don't wait until security testing to identify and address open source vulnerabilities. Initiate Checkmarx OSA from a standard web browser or directly inside your build environment. Results are aggregated, presented in the web UI, or delivered directly to the build manager interface in a unified project view.

Research-Backed Security Insight: Improve and maintain your software security posture with detailed insight into thousands of public open source vulnerabilities, security advisories, and bugs. Elevate your security awareness with Checkmarx-exclusive vulnerabilities and remediation guidance provided by Checkmarx's security research team.

Simplify Complex Licensing: Open source licenses can be complex, and failure to comply license requirements can result in litigation and lost intellectual property. Checkmarx OSA clearly defines potential license risks and provides metrics to help ensure that developers don't use components with licenses which conflict with your projects' technological or business structures.

Multiple Tests, One Solution: Checkmarx OSA and Checkmarx SAST are natively integrated, and their results can be directly correlated for improved and automated prioritization of vulnerabilities. Manage weaknesses in custom code and open source vulnerabilities within one console, initiate static and software composition analysis at the same time, and determine if an open source vulnerability is actually exploitable within the application.

Enforce Open Source Policies: Create and automatically enforce policies for secure, compliance open source consumption. Define acceptance and rejection criteria, and establish internal approval processes based on an array of component metadata and project details. When a developer attempts to add an open source component that violates policies, you'll get an alert, and an automated policy workflow will begin (e.g. break a build).

Optimize Open Source Selection: Open source selection is easy with the Checkmarx OSA browser plugin. Developers can browse for open source components online and verify if they are appropriate for use, examining various risk metrics for security, quality, and license compliance – even before they incorporate it into their projects.

Enhance Coverage and Accuracy: Checkmarx OSA supports all popular open source programming and scripting languages. Its proprietary open source identification algorithm focuses on minimizing false positives for faster, more-effective remediation.

Languages/Frameworks

Java | JavaScript | .NET | Node.js | Typescript | Python | Angular | React | WCF | WPF | Groovy | Kotlin | Scala | C#

CI & Build System Integrations

Bamboo | Jenkins | TeamCity | Azure DevOps

Package Managers

Maven | Gradle | NPM | Nuget | Yarn | Bower | pip

Software = Security

About Checkmarx

Checkmarx makes software security essential infrastructure, setting a new standard that's powerful enough to address today's and tomorrow's cyber risks. Checkmarx delivers the industry's only comprehensive, unified software security platform that tightly integrates SAST, SCA, IAST and AppSec Awareness to embed security into every stage of the CI/CD pipeline and minimize software exposure. Over 1,400 organizations around the globe trust Checkmarx to accelerate secure software delivery, including more than 40 percent of the Fortune 100 and large government agencies. Learn more at Checkmarx.com

Checkmarx, All rights reserved 2019 ©