Checkmarx Software Composition Analysis (CxSCA)

datasheet

Take Control of Your Open Source

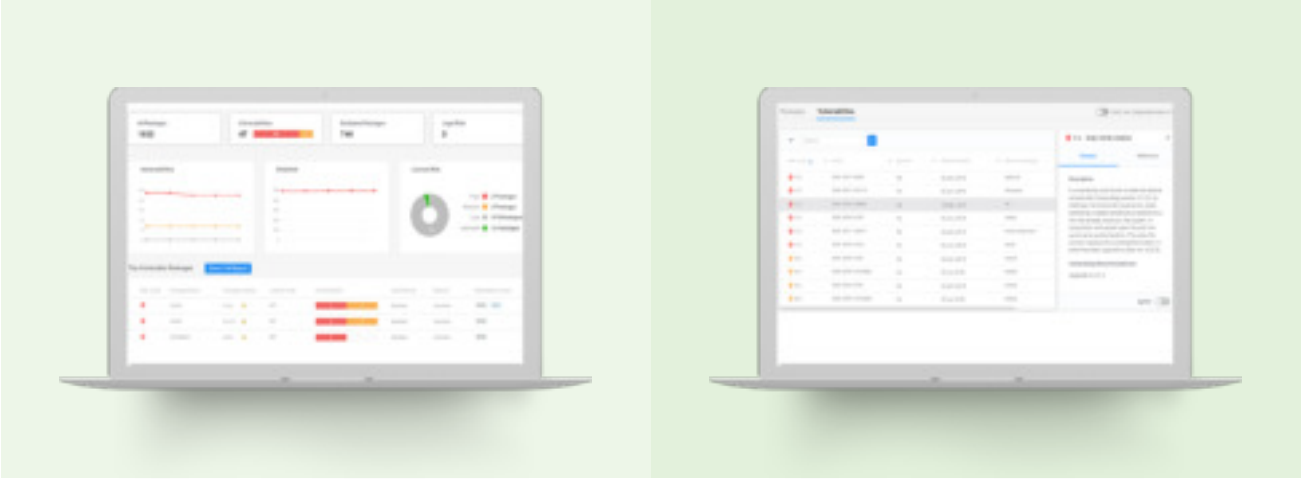
As with custom code and commercial software, open source libraries can introduce risks which organizations must identify, prioritize, and address. Security vulnerabilities can leave sensitive data exposed to a breach, license requirements can jeopardize your intellectual property, and outdated open source libraries can place unnecessary support and maintenance burdens on your development teams. In today's complex landscape of agile DevOps and CI/CD, development teams can't afford to have security testing slow them down and security teams can't afford to have vulnerable software in production.

CxSCA addresses these issues for modern DevOps, keenly focused on providing highly accurate, relevant, and actionable open source risk insight, backed by a dedicated open source security research team and seamlessly integrated throughout the SDLC.

Accurate Results Prioritized for Maximum Impact

CxSCA tracks the open source components that are actually in your applications, rather than handing you a lengthy list of fuzzy matches and potential false positives that waste your time by parsing through them to find the true issues. Our proprietary scanning engine detects and identifies specific component versions within the scanned project and any declared or transitive dependencies resolved during a build. This provides the greatest coverage with the highest accuracy possible, accelerating time-to-remediation.

Checkmarx elevates the standard for software composition analysis (SCA) by leveraging source-level insight from our industry-leading SAST technologies, empowering security teams to easily identify vulnerabilities within open source software that present the greatest risk and enabling developers to focus and prioritize remediation efforts accordingly. This dramatically reduces time spent from the point of vulnerability detection to remediation and increases developers' overall productivity.



Flexible, Automated Open Source Security for DevSecOps

Secure DevOps depends on providing direct access to security risk information for the people who create, secure, and deploy software, without impeding their ability to ship code on tight schedules. CxSCA was purpose-built to automatically analyze projects and to provide rapid feedback in the manner most relevant to each stakeholder, including dashboards, exportable reports, triggered email notifications, and summary data within the tools developers use daily (e.g. build manager interfaces, code repositories). CxSCA features a variety of out-of-the-box integrations with CI tools and build systems to automate activities for secure DevOps.

FIND THREATS TO SECURITY, IP, AND YOUR TIME: Identify open source vulnerabilities and get useful severity metrics, detailed descriptions, and actionable remediation guidance. Identify potential license conflicts and risks of non-compliance. Determine which outdated libraries may place increased support and maintenance burden on your development teams. Generate detailed risk reports or extract data via API.

FLEXIBLE, SECURE DELIVERY OPTIONS: Don't let complex infrastructure and configuration challenges become a barrier to secure software development. CxSCA is delivered in a scalable, enterprise-class cloud, with integrations, REST APIs, and secure data communications for your cloud-based or on-premises SDLC and CI/CD pipelines

AUTOMATIC, INSTANT ALERTS TO NEW THREATS: Trust CxSCA to watch for new vulnerabilities impacting previously analyzed projects long after they have gone into production. Get instant email notifications, or leverage APIs for data extraction, providing alerts to new vulnerabilities that affect your projects without the need to scan them again.

OPTIMIZE EFFORTS, ACCELERATE REMEDIATION: CxSCA leverages Checkmarx's industry-leading source analysis technologies to improve your triage capabilities and enable you to focus efforts on the immediate risks. Prioritize remediation efforts by verifying if vulnerable components are in the execution path of the application, leveraging our industry-leading source analysis technologies. Decode complex dependency paths to pinpoint the exact origin of an inherited vulnerability.

GLOBALLY RECOGNIZED SECURITY RESEARCH: Checkmarx's security experts have a strong history of recognition for their research. Our dedicated open source security research team is focused on providing detailed descriptions and remediation guidance for known CVEs, as well as additional coverage beyond what's available from public resources like the NVD with Checkmarx-exclusive vulnerabilities with no corresponding CVEs at the time of discovery.

SIMPLIFY APPSEC, STREAMLINE OPERATIONS: As part of the Checkmarx application security testing (AST) portfolio, CxSCA benefits from centralized, unified user management, access control, project creation, and scan initiation with CxSAST. This greatly simplifies user administration and access control configuration, so you spend less time managing software and more time managing software security.

Languages/Frameworks

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

Package Managers

Maven | Gradle | NPM | NuGet | Yarn | Bower | Pip | Composer | SBT

CI & Build System Integrations

Jenkins | CLI

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