Application Security Testing Developers Actually Use

CHECKMARX

WHAT WE DO

Checkmarx CxSAST is a highly accurate and flexible Source Code Analysis product that allows organizations to automatically scan un-compiled / un-built code and identify hundreds of **security vulnerabilities** in the most prevalent coding languages.

CxSAST is available as a standalone product and can be effectively integrated into the Software Development Lifecycle (SDLC) to streamline detection and remediation. CxSAST can be deployed on-premise in a private data center or hosted via a public cloud.

ABOUT CHECKMARX

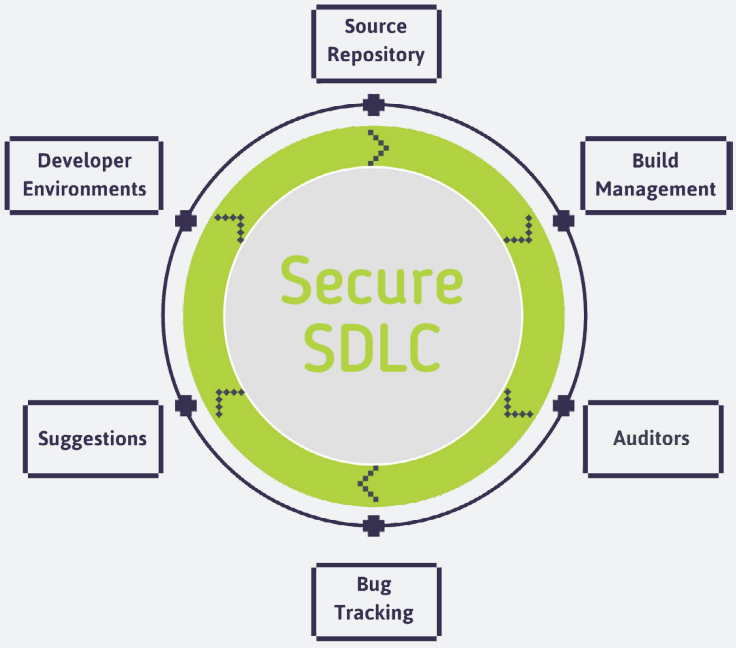
Checkmarx is a leader in Application Security testing solutions. Customers include 4 of the world's top 10 software vendors and hundreds of Fortune 500 and SMB organizations from all industries.

WHY CxSAST

For enterprise companies who want to minimize application security risk, CxSAST provides the ability to eliminate vulnerabilities early in the SDLC. Unlike other SAST solutions, CxSAST is widely adopted by development teams because it seamlessly fits in with their existing software development lifecycle.

Gartner

The only vendor to score a perfect 5.0 for "Static Analysis Product," AST Critical Capabilities Report 2014.



SUPPORTED CODING LANGUAGES

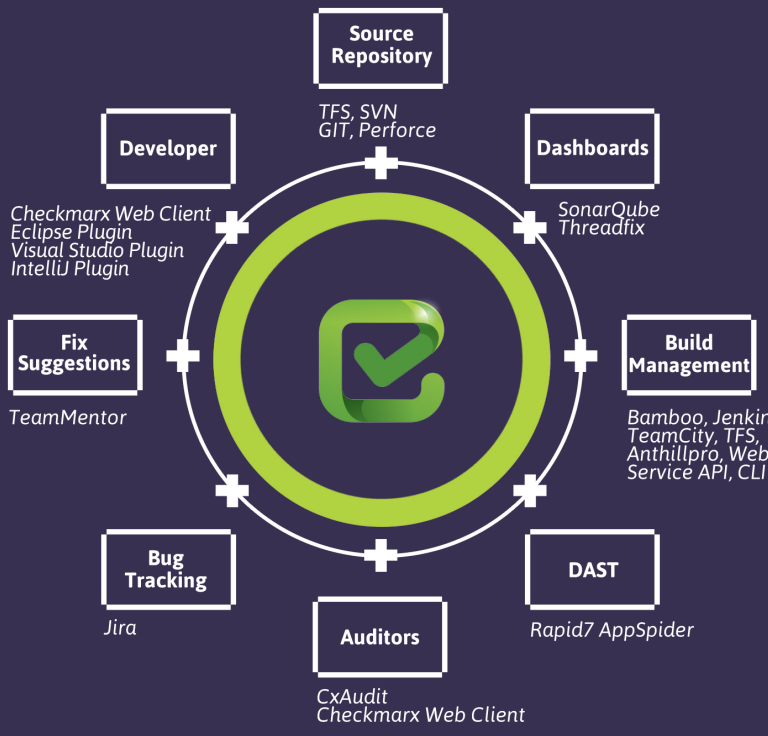
Java, JS, php, python, Groovy, Swift, Apex, Android, Apple, Perl, Microsoft .net, HTML, Windows Mobile, C++, Scala, Ruby, Microsoft ASP.net, VB.NET, Visual Basic 6.0, PL/SQL

contact@checkmarx.com | www.checkmarx.com

SECURE SDLC

Checkmarx enables organizations to integrate Static Application Security Testing into their SDLC.
We integrate with the most popular source repositories, build management servers, bug tracking tools and have plugins for the major IDEs. If we don't support an integration with one of your SDLC components out-of-the-box, this can be easily done via our comprehensive API. The benefits of a fully integrated SAST model are:

- Security team focuses on setting the policy, using Checkmarx to enforce it automatically.
- Security testing of the recent code fragments means any findings are quickly remediated by developers. This significantly reduces costs and eliminates the problem of having to deal with many security vulnerabilities close to release.



SUPPORTED VULNERABILITIES

CxSAST scans for hundreds of vulnerabilities out-of-the-box, including the most common ones:

- SQL Injection
- Cross-Site Scripting
- Code Injection
- Buffer Overflow
- Parameter Tampering
- Cross-Site Request Forgery
- HTTP Splitting
- Log Forgery
- Denial of Service
- Session Fixation
- Session Poisoning
- Unhandled Exceptions
- Unreleased Resources
- Unvalidated Input
- Dangerous Files Upload
- Hardcoded Password
- And more ...

SUPPORTED STANDARDS

OWASP Top 10 2013 | OWASP Mobile Top 10 | SANS 25 | HIPAA | Mitre CWE | FISMA | PCI DSS | MISRA | BSIMM

FAQ

What types of reports can Checkmarx provide?
Checkmarx offers project progress reports and configurable dashboards in PDF, RTF, CSV or XML.

Do you support scanning of mobile applications?
Yes, Checkmarx fully supports Android, iOS, Windows and hybrid mobile applications.

How do you do your magic?
Checkmarx parses raw source code (no need to compile), stores it in a database and queries it with hundreds of rules to find vulnerabilities.

Does Checkmarx provide a product or a service?
Checkmarx provides both on-premise solutions and private or public hosted solutions, including managed services.

Can I use Checkmarx to understand how changes in the code resulted in vulnerabilities?
Yes, Checkmarx provides a side-by-side comparison of scans and points out the differences.

What Makes Us Unique?

WE SCAN UNCOMPILED CODE

Our ability to scan raw source code means that you are able to scan your code starting from the earliest stages of the development lifecycle, when it is most effective to identify security bugs. It also means that you never have to worry about achieving a compiled build, allowing you to scan code fragments at any time.

WE ARE TRANSPARENT AND EASY TO CUSTOMIZE

Checkmarx's product was designed using an open query language that means it is easy to see what Checkmarx scans for and how it does that. It can be quickly modified to your specific environment and taught about any sanitation methods that aren't part of the framework, thus reducing the false positive and false negative rates to a negligible number. Advanced customers tend to add their own queries and use Checkmarx to enforce best coding practices, compliance to specific regulations, and more.

WE OPTIMIZE YOUR REMEDIATION EFFORTS

Checkmarx goes beyond identifying all the security vulnerabilities in your code. We optimize your remediation efforts, taking a bird's eye view of the data flow in the application and identifying the critical junctions that eliminate multiple vulnerabilities through a single fix.

WE DON'T RE-SCAN CODE THAT HASN'T CHANGED

Using Checkmarx's unique incremental scan capabilities, we eliminate the need to re-scan the entire code base if only several lines of code were changed. We analyze the code that changed since the last scan and its dependent files and only scan them. This enables fast results and is especially useful in fast-paced agile environments.

WE INTEGRATE INTO YOUR BUILD PROCESS

Checkmarx is flexible enough to integrate into your existing SDLC so that you decide on your desired security policy, and Checkmarx automatically enforces it for you. We support the most common source repositories, build servers, bug tracking tools, IDEs, and reporting systems to enable you to streamline your security testing and ensure it is as effective as possible.

WE COVER THE MOST COMMON CODING LANGUAGES

We currently support 20 coding and scripting languages and their most popular frameworks and add 2 to 3 new languages every year.

OUR AWARDS

2nd Fastest Growing Security Company in EMEA

Top 20 Security Products

Red Herring EMEA Top 100 Winners

Best Application Security Product in 2014 by Cyber Defense Magazine

FAQ

Can I integrate with a build management system?
Yes. We currently have plugins for Jenkins, Bamboo, TeamCity, TFS, Anthill Pro and others.

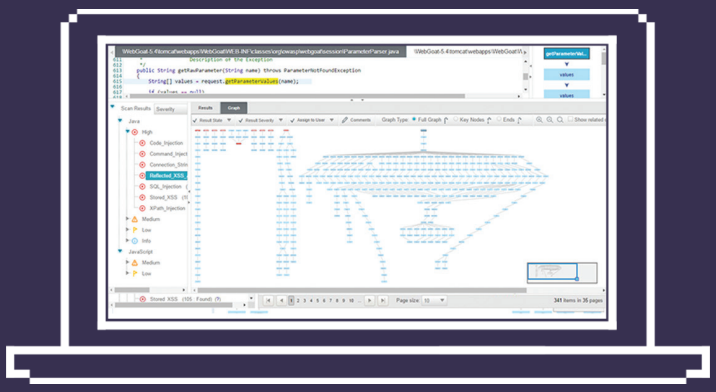
How often do you release product updates?
A new version is released every year. A service pack is released every quarter. Hotfixes are released as needed.

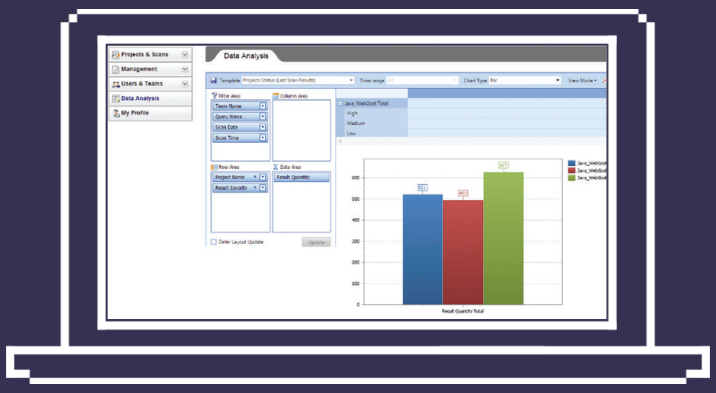
What is your false positives ratio?
Checkmarx has a low rate of false positives (less than 5%). We achieve that by marking a result as a false positive in the UI and adapting the rules to your environment. Our professional services team can do this for you.

Do I have to rescan my entire code base every time?
No. The incremental scan option will automatically scan only the updated files and their dependencies.

CxSAST VIEWER

The CxSAST Viewer provides an optimal user experience for security professionals and developers, enabling them to investigate the identified vulnerabilities and decide on the best remediation action. The Viewer presents the attack vector and the flow of data from input to sink.
Clicking on a node presents the relevant line of code and remediation method.



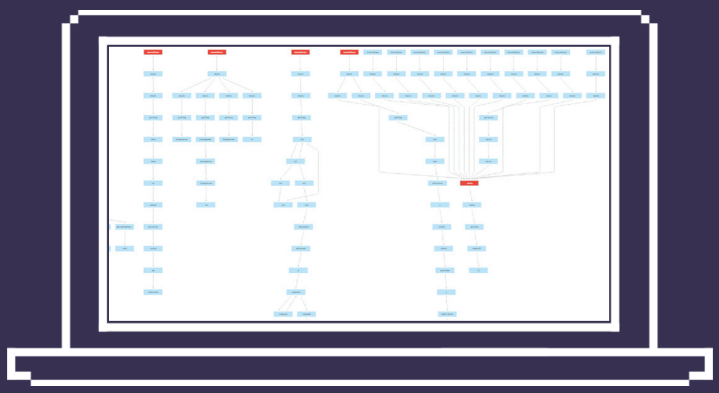


DASHBOARD & REPORTS

Analyzing data and generating reports with Checkmarx is simple. You can use the predefined data analysis reports, or modify and create your own via an intuitive drag and drop mechanism specifying the parameters you wish to analyze, how you wish to alter the data and by specifying the graph type. Modifications take effect in real time. Analysis can then be exported to PDF or Excel.

OPTIMIZING REMEDIATION EFFORTS

Checkmarx goes a step beyond identifying vulnerabilities. In addition to listing the findings, we utilize graph theory algorithms to consolidate attack vectors and point out the critical junctions multiple attack vectors flow through which serve as the best locations to fix the code. Graph View optimizes developer remediation efforts by ensuring they fix the minimum amount of places in the code to achieve full coverage.



Atlassian

"Using Checkmarx is easier than other tools. Important - you do not need to integrate it into your build process, just throw source code at it. The team was extremely happy with the levels of support they received. It was both professional and timely despite the time zone differences."
Vitaly Osipov, Information Security Expert, Atlassian

playtech SOURCE OF SUCCESS

"Checkmarx is loved by both our InfoSec team and our developers. It is easy to use and provides highly accurate results combined with the flexibility we need to enforce our application security policy."
Kobi Lechner, Information Security Manager, Playtech

LIVEPERSON

"Checkmarx's technology is highly accurate and easy to use. It offers great performance and the ability to scan incomplete code samples. Checkmarx was agile enough to support special requests we had for our secure SDLC and was the most sensible decision commercially."
Security Specialist, LivePerson

salesforce

Salesforce.com selected Checkmarx's Static Code Analysis tool as the official Force.com Security Code Scanner. With over 2.5 billion LoC scanned to date and 2 million vulnerabilities detected, Checkmarx ensures all AppExchange applications are secured to the highest standards.

contact@checkmarx.com | www.checkmarx.com