Checkmarx CxSuite 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. 

CxSuite is available as either a standalone product but can also be effectively integrated into the SDLC process and streamline the detection and remediation process. It is available OnPremise, or OnDemand via as a private/public cloud.

CxSuite is trusted by hundreds of the world's largest software vendors, financial and government organizations and top consultancy firms.

Supported Coding Languages:
**FAQ**

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

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

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

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.

How do you do your magic?
Checkmarx parse raw source code (no need to compile) stores it in a DB and queries it with hundreds of rules to find vulnerabilities. Rules can be easily modified & added.

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 FP in the UI and by adapting the rules to your specific environment. Our professional services team can do this for you.

Does Checkmarx provide a product or a service?
Checkmarx's product is available either On-premise, on a private cloud or on our secure CxCloud service.

How 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.

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.

Can you please describe your product architecture?
Checkmarx is installed on a central server with web clients and thin IDE plugins connecting via http.

**SUPPORTED VULNERABILITIES:**

CxSuite 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
- DoS
- Session Fixation
- Session poisoning
- Unhandled exceptions
- Unreleased resources
- Unvalidated input
- URL redirection attack
- Dangerous Files Upload
- Hardcoded password
- And more...

**SUPPORTED STANDARDS**

- OWASP Top10 2013
- OWASP MobileTop 10
- SANS 25
- PCI DSS
- HIPAA
- Mitre CWE
- FISMA
- BSIMM
- MISRA
- CYSC
- CWSF
- AFS
- SANS
- MISRA

**REFERENCES**

salesforce.com selected Checkmarx's static code analysis tool as the official Force.com Security Source Code Scanner. With over 1.3 Billion LoC scanned to date, Checkmarx ensures all AppExchange applications are secured to the highest standards.

“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
**WHAT MAKES US UNIQUE?**

**We scan uncompiled code |** Our ability to scan raw source code means that you are able to scan your code at the earliest stages of the development lifecycle, when it is most effective to identify and fix security bugs. It also means that you do not have to worry about achieving a compiled build and can literally throw code fragments at the product and the scan will start.

**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 also means it can be quickly modified to suit your specific environment and taught about any sanitation methods that aren't part of the framework, thus reducing the false positive / false negative rate to a negligible amount. Advanced customers tend to add their own queries and use Checkmarx to enforce best coding practices, compliance to specific regulations and more. Checkmarx goes beyond identifying all the security vulnerabilities in your code. We optimize your remediation efforts, by taking a bird's eye view of the data flow in the application and identifying the critical junctions that if your code will be fixed there, multiple vulnerabilities will be eliminated with a single fix.

**We Optimize Your Remediation Efforts |** Checkmarx goes beyond identifying all the security vulnerabilities in your code. We optimize your remediation efforts, by taking a bird's eye view of the data flow in the application and identifying the critical junctions that if your code will be fixed there, multiple vulnerabilities will be eliminated with a single fix.

**We Optimize Your Remediation Efforts |** 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 re-scan them. This enables fast results and is especially useful in high pace agile environments.

**We integrate into your build process |** Checkmarx is flexible enough to integrate into your existing Software Development Lifecycle (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 done as effectively as possible.

**We cover the most common coding languages |** Checkmarx was designed so that it is fairly easy for us to add support for new coding languages and frameworks. We currently support 16 coding & scripting languages and their most popular frameworks, and add 2-3 new languages every year.

**CX SUITE VIEWER**

The CxSuite viewer provides an optimal user experience for security professionals and developers that have 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. Every click on a node presents the relevant method and line of code.
**DASHBOARD & REPORTS**

Analyzing data and generating reports with Checkmarx is simple. You can use the pre-defined 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 filter 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 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 developers' remediation efforts by ensuring they fix the minimum amount of places in the code to achieve a full coverage.

**BEST PLACE TO FIX**

Graph View pinpoints the best place in the application to fix the vulnerability. Provides automatic recommendations of the best x locations but also has a manual mode. A "What If" remediation can be applied and analyzed dynamically.