CHECKMARX

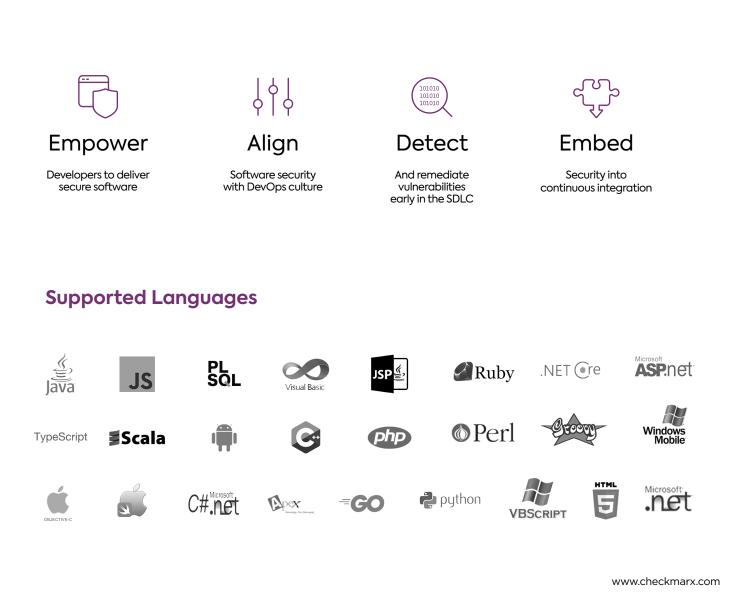# Manage Software Exposure at the Speed of DevOps

The software security platform that helps organizations deliver secure software faster.

Breaking Down Barriers with DevSecOps

Reducing development "time-to-market" is the new standard. If an organization can provide new features faster than its competition, it will gain market share. This has led to widespread adoption of DevOps teams using Agile development methodologies to deliver new features faster. This also brings new challenges to security teams trying to adjust to this new environment. Checkmarx delivers a platform for all aspects of DevOps including development and CI/CD environments by redefining security's role in the SDLC, all while operating at the speed of DevOps. The fast feedback loop makes security testing of new or edited code fragments quick, allowing speedy remediation by developers. This significantly reduces costs and eliminates the problem of having to deal with many security vulnerabilities close to release.

Empower
Developers to deliver
secure software

Align
Software security
with DevOps culture

Detect
And remediate
vulnerabilities
early in the SDLC

Embed
Security into
continuous integration

Supported Languages

Java JS PL SQL Visual Basic JSP Ruby .NET Core Microsoft ASP.net

TypeScript Scala (Android) C++ php Perl Groovy Windows Mobile

OBJECTIVE-C (Swift) C#.net Microsoft Apex Develop On-Demand GO python VBSCRIPT HTML 5 Microsoft .net

Software Exposure

Software Exposure is an emerging discipline for managing and measuring the *software everywhere* attack surface to accurately understand and reduce business risk.

Software security involves more than just testing code for vulnerabilities. Simply finding vulnerabilities doesn't protect the applications from attacks. Organizations must ensure that they address all risks within the code and risks within the organization that could be exploited by an adversary. These risks - software exposure - present themselves in a variety of ways. They can be in the code organizations write, the code they use from 3rd parties, weaknesses in organizational knowledge, the way in which they address bugs and vulnerabilities in software, and weaknesses in internal processes.

The Checkmarx Software Exposure Platform

The Checkmarx Software Exposure aligns Software Security with DevOps culture, detecting, intelligently prioritizing, and remediating exposure across the SDLC from the coding stage through to the runtime application testing stage. Checkmarx empowers developers to deliver secure software faster with one holistic solution.
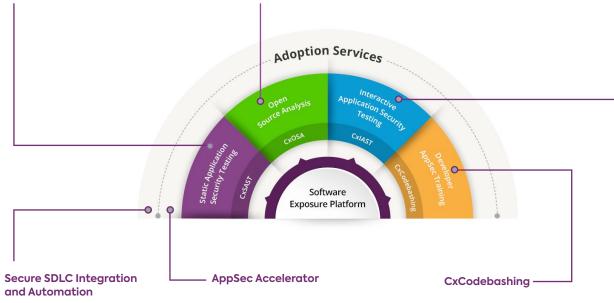
CxSAST

A highly accurate and flexible Source Code Analysis product that allows organizations to automatically scan uncompiled/unbuilt code and identify hundreds of security vulnerabilities in the most prevalent coding languages.

CxOSA

CxOSA enforces open source analysis as part of the SDLC and manages open source components while ensuring that vulnerable components are removed or replaced before they become a problem.

CxIAST

A solution that detects vulnerabilities in running applications under test. Built for DevOps, it seamlessly integrates into your CI/CD pipeline. CxIAST provides advanced vulnerability detection with zero impact on testing cycle times.

Secure SDLC Integration and Automation

Checkmarx enables organizations to integrate Software Security into their SDLC and DevOps workflows. We integrate with the most popular source code repositories, build management servers, bug tracking tools, and have plugins for major IDEs.

AppSec Accelerator

A Software Security managed service that helps development organizations transition into a secure SDLC. With AppSec Accelerator, a team of qualified experts helps you ramp-up, streamline, and automate your Software Security.

CxCodebashing

An interactive Software Security training platform that sharpens the skills developers need to avoid security issues, fix vulnerabilities, and write secure code in the first place.

What Makes Checkmarx Unique?

Only Checkmarx provides a full platform to identify, analyze, intelligently prioritize, and remediate issues with software exposure in a DevOps environment. Checkmarx supports a combination of integrations for the automation required in a fast-paced development environment along with a variety of technologies to empower development and security to improve the overall security posture of an organization.

Integrate with Your DevOps / Continuous Integration Environment

The ability to scan raw source code means that you are able to **scan your code starting from the earliest stages** of the development lifecycle. And by using Checkmarx's unique **incremental scan** capabilities, the need to re-scan an entire code base if lines of code are added or changed is eliminated, thus enabling fast results for fast-paced agile environments.

Optimize Your Remediation Efforts

Checkmarx optimizes remediation efforts with the **Best Fix Location**, which takes a bird's eye view of an application's data flow and identifies critical junctions that eliminate multiple vulnerabilities through a single fix, **reducing remediation times by up to 80%**.

Developer Friendly

Checkmarx easily **integrates with existing work environments**, allowing developers to stay in their comfort zone while addressing secure coding practices as part of their daily routine. We currently support over 25 coding and scripting languages and top frameworks.

Secure Use of Open Source

CxOSA quickly identifies the open source components you use to avoid known vulnerabilities and restrictive licenses. It also continues to monitor the threat space and provide alerts on new vulnerabilities.

Custom Queries for Your Code

Checkmarx's software security platform can be modified to your unique environment. Customers can choose from a list of existing query presets or create your own **custom queries to enforce secure coding practices**, regulation compliance, and more.

Completely Protect your Software from Security Threats

The powerful combination of CxSAST, CxOSA, and CxIAST is key for DevSecOps success. This ensures the software's security posture is addressed as early as possible in the SDLC and is validated after the application is fully built.