CHECKMARX
Application Security Made Easy

CxSAST for Mobile

Mobile applications have become an integral part of daily personal and business activities. Users (employees or customers) rely on their mobile applications to store their data and manage their daily tasks. It's the application vendor's responsibility to keep the end user's information safe and avoid data leakage. A mobile application breach can be devastating not only to the end user but to the entire organization as well.

Checkmarx's CxSAST for Mobile delivers unique and dedicated analysis for iOS, Android and Windows applications. Checkmarx ensures security is an integral part of the application development process and reduces the time to market by eliminating code vulnerabilities during the coding process rather than detecting them at a later stage. Mobile Developers are constantly introduced with new and complex security challenges. Application permissions, data input vectors, sensitive data storage, supporting multiple operating systems and providing frequent version releases, cross application communication and cross platform functionality increase the risk of introducing vulnerabilities during development.

Checkmarx's CxSAST for Mobile was designed with these challenges in mind and takes mobile static analysis to the next level.

Identify & fix mobile security vulnerabilities as they are created

Checkmarx CxSAST for mobile is a powerful Source Code Analysis (SCA) solution designed for identifying, tracking and fixing technical and logical security flaws from the root: the source code. With the proliferation of mobile applications and the ever-changing mobile operating systems this task requires a unique approach specifically designed to address the mobile landscape.

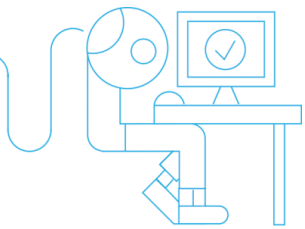
Checkmarx's out of the box mobile security analysis ruleset includes standards such as OWASP Top 10 for Mobile, PCI DSS, HIPPA and others.

Supports all mobile languages, frameworks and Operating Systems

Checkmarx's CxSAST for Mobile offers a unique solution adapted to the ever growing landscape of mobile applications. Both native and hybrid application development bare their own risks. Implementing code security during development and across multiple frameworks is critical to ensure vulnerability free applications. CxSAST for mobile supports analysis on all major coding languages for Android, iOS and Windows including Adobe's popular Phonegap framework.

New Operating Systems released by the different mobile vendors are supported immediately due to Checkmarx's unique ability to scan un-compiled code.

Checkmarx provides complete iOS Security guidelines coverage updated per iOS version release.



Unique Behavioral Mobile Application Security Analysis

XSS, SQLi and other known vulnerabilities are important and have to be addressed when analyzing application code. Mobile devices introduce new risks which are not clearly defined as vulnerabilities, while posing significant risks to mobile applications and their users. These include wrong usage of permissions, wrong dictionary usage, 3rd party keyboard risks and other mobile related functionality. CxSAST for mobile was designed to detect those types of mobile related risks using specially crafted heuristics which can easily be expanded or modified as needed.

Full SDLC Integration

Checkmarx CxSAST for mobile enables organizations to integrate Static Application Security Testing into their SDLC and automate the process. We integrate with the most common source repositories, build management servers, bug tracking tools and IDEs and fit in with how your development and security processes are managed.

Key Functionality

- Secure applications early in the development cycle to reduce time to market
- Support multiple development platforms, coding languages and operating systems including Native, Hybrid, iOS, Android and Windows applications.
-
- Integrate at every stage of the development lifecycle to streamline the secure code analysis process.
- Full automation
- Superb productivity through algorithmic remediation advice – eliminate multiple vulnerabilities with a single fix.