Tab 1

NowSecure Mobile App Security Testing: Complete Guide

Mobile applications are extremely relevant in our life in the modern digital world. Mobile apps deal with sensitive customer information on a daily basis in the banking and healthcare sectors, as well as in shopping and entertainment. Due to this reason, the mobile apps are frequently targeted by cybercriminals to steal or use security flaws.

That is why mobile app security testing is not an option anymore. Several firms have to test their applications on a regular basis to guarantee the safety of data and confidence of users. NowSecure mobile app security testing is one of the famous solutions in this field. This paper defines what NowSecure is, how it functions, and how it is comparable to other well-known mobile security testing software.

What is NowSecure Mobile App Testing?

NowSecure is a mobile testing based security solution which specifically targets Android and iOS applications. Compared to generic application security devices, NowSecure is limited to identifying the dangers associated with mobile apps, so it is very efficient to uncover vulnerabilities which are specific to mobile apps.

NowSecure assists companies to detect security concerns during an early stage of development. It assists automated testing, actual device testing, and industry standardized security reporting. This ensures that it is a powerful alternative to businesses, DevSecOps, and security professionals.

Key Features of NowSecure

Automated Mobile App Security Testing

NowSecure offers a scanning process that is automated which is able to scan and analyze the mobile applications and identify known security risks. This saves manpower and time during the testing.

Static and Dynamic Analysis

NowSecure applies the dynamic and the static testing techniques. The static analysis process checks the code of the application or the binary and does not run the application whereas the dynamic analysis process tests the application at runtime to identify the vulnerabilities.

Real-Device Testing

Real-device testing is one of the most powerful characteristics of NowSecure. The platform provides better results since it does not use emulators but the actual mobile devices to test the apps, thereby giving better results that are more reliable.

OWASP MASVS Compliance

NowSecure adheres to OWASP Mobile Application Security Verification Standard (MASVS). This assists organizations to achieve compliance and security needs with ease.

CI/CD Integration

NowSecure is integrated with CI/CD pipelines. This enables teams to conduct continuous security tests at the stages of development and deployment.

Reasons why Businesses prefer NowSecure.

A lot of organizations would choose nowsecure since it is specifically designed to do mobile security. It provides enterprise-grade security and advanced reporting which assists the teams to know and remedy vulnerabilities in a timely fashion.

Businesses prefer NowSecure due to the fact that it:

Focuses only on mobile apps

Helps to uphold standards of compliance and regulation.

Buddy fits into DevSecOps processes.

Gives precise findings with actual equipment.

Competitor Landscape Google Search.

Whenever a user types NowSecure mobile app security testing on Google, he/she tends to know how NowSecure works or how it is compared to other tools. This keyword will appeal to decision-makers, including CTOs, developers, and security teams who are considering mobile security solutions.

Due to this fact, competitor analysis is significant in this case to determine the position of NowSecure in the market.

The leading competitors of NowSecure

Appknox

Appknox is a mobile app testing environment that is made popular and provides automated and manual testing. It is associated with quick installation and simple reports.

Appknox is appropriate when there are teams that desire rapid delivery and mobile-first strategy.

Veracode

Veracode is a general application security platform which supports mobile, web applications as well as cloud applications. Large enterprises have been known to use it.

Veracode is however not entirely mobile-focused as NowSecure, which can minimize its usefulness in mobile-specific risks.

HCL AppScan

HCL AppScan offers automated and compliance reporting on mobile and web applications. It is appropriate in large companies that have complicated security requirements.

Data Theorem

The Data Theorem provides automated testing of mobile apps security and API security. It lays emphasis on constant supervision and adherence.

This is a tool mostly used where businesses require mobile and backend coverage.

Pradeo Security

Pradeo is an AI-technology that is used to detect mobile threats. It pays attention to behavioral analysis and recognition of malware.

It is also innovative but has a limited market share as compared to NowSecure.

MobSF (Open-Source Tool)

MobSF is an open-source mobile security system that is commonly used by developers and researchers. It offers both the dynamic and static analysis of Android and iOS applications.

MobSF is free, but it does not have enterprise-level automation and support.

The selection of the appropriate Mobile App Security Tool

The appropriate mobile application testing tool is based on the size of business and the security needs.

Startups and small teams can find it preferable to use open-source and friendly tools. The firms tend to require high-level compliance, automation, and reporting capabilities. The tools used by DevSecOps teams can be integrated into CI/CD pipelines without much effort.

NowSecure would be most appropriate to organizations that are in need of in-depth testing of mobile security and compliance.

Strengths and Weaknesses of NowSecure.

Advantages

NowSecure provides powerful mobile-first security testing, real-device testing, and reporting suitable to satisfy compliance. It is credible and is reliable among enterprises.

Limitations

NowSecure can be expensive with small teams and can be more than necessary to fulfill simple security needs.

The reason the Mobile App Security Testing is important in 2026

Attackers are also becoming more organized and intense as the use of mobile intensifies across the world. The contemporary mobile apps are not mere stand alone products anymore. They exchange APIs, cloud services, payment gateways, third-party SDKs and external databases. Every integration makes the application more vulnerable to attacks.

Mobile applications will be used to store even more personal information in 2026, in this case, biometric data, financial credentials, and personal health records. The exposure of thousands or even millions of users can be done through a single vulnerability. It is based on the fact that mobile app security testing is a necessity, as opposed to an option.

Conducting frequent testing of the mobile app security assists organizations in the following:

Avert information breach, malware injections and reverse engineering attacks.

Secure user authentication, tokens, and business logic.

Sustain brand equity and trust.

Eschew criminal fines and compliance cost.

Identify vulnerabilities in time before they are disclosed to the public or submitted to the storage system.

Current testing is facilitated on platforms such as NowSecure that enable security teams to be ahead of the new threats due to the in-depth risk visibility and actionable insights.

Common Mobile App Security Risks NowSecure Helps Detect

Mobile applications face a wide range of security risks. Many of these issues are unique to mobile environments and are often missed by general application security tools.

NowSecure helps identify common mobile app vulnerabilities such as insecure data storage, weak encryption practices, improper certificate validation, insecure communication channels, and exposed APIs. It also detects issues related to hardcoded credentials, excessive permissions, and unsafe third-party libraries.

By identifying these risks early, organizations can reduce the likelihood of exploitation and improve overall application security.

How NowSecure Fits Into Modern DevSecOps Workflows

Modern software development relies heavily on DevSecOps practices, where security is integrated directly into the development lifecycle. Instead of testing security at the end, teams aim to test continuously during development.

NowSecure integrates smoothly into DevSecOps workflows by supporting CI/CD pipelines. This allows security tests to run automatically whenever a new build is created. Developers receive early feedback, enabling faster remediation and reducing delays during release cycles.

This approach not only improves security but also reduces development costs and improves collaboration between development and security teams.

FAQs

Is NowSecure suitable for startups?

NowSecure is mainly designed for enterprises, but security-focused startups can also use it if budget allows.

Does NowSecure support OWASP standards?

Yes, NowSecure aligns with OWASP MASVS guidelines.

Are there alternatives to NowSecure?

Yes, Appknox, Veracode, HCL AppScan, Data Theorem, and MobSF are common alternatives.

Final Verdict

NowSecure mobile app security testing is a powerful solution for organizations that want serious protection for their mobile applications. Its focus on mobile security, real-device testing, and industry-standard compliance makes it a strong choice for enterprises and security-focused teams.

NowSecure is especially useful for businesses that operate in highly regulated industries such as finance, healthcare, and e-commerce, where mobile app security is critical. The platform helps reduce risks, improve security posture, and maintain user trust over the long term.

While other tools also offer mobile security testing, NowSecure stands out for its depth, accuracy, enterprise readiness, and mobile-first approach. Choosing the right security testing solution ultimately depends on budget, compliance needs, and development workflow, but NowSecure remains one of the most reliable options in the market.

Tab 2

Checkmarx Mobile App Security Testing: Complete Guide for 2026

Mobile apps have become an integral part of our daily lives. From banking and shopping to education and entertainment, mobile apps manage sensitive data every day. This makes **mobile app security** a critical concern for businesses, developers, and users alike.

Cyberattacks targeting mobile apps are increasing, with hackers exploiting vulnerabilities such as weak authentication, insecure APIs, and data leakage. To prevent this, companies are adopting **mobile app security testing tools**. One of the leading platforms in this space is **Checkmarx**.

In this article, we will explore **Checkmarx Mobile App Security Testing**, its features, benefits, comparisons with other tools, and why it is essential for modern mobile apps.

What is Checkmarx?

Checkmarx is a well-known **Application Security Testing (AST)** platform that helps businesses identify and fix vulnerabilities in their software. It is widely used by developers, security teams, and enterprises to secure applications during the development process.

Checkmarx supports multiple types of security testing, including:

- **SAST (Static Application Security Testing):** Scans source code for vulnerabilities without running the app.
- **SCA (Software Composition Analysis):** Detects risks in third-party libraries and open-source components.
- **DevSecOps Integration:** Works with CI/CD pipelines to catch vulnerabilities early in development.

While Checkmarx can secure web applications, its **mobile app security capabilities** make it a top choice for Android and iOS app developers.

Understanding Mobile App Security Testing

Mobile app security testing involves identifying and fixing vulnerabilities before hackers can exploit them. Mobile apps face unique challenges compared to web applications, such as:

- Sensitive data stored on devices
- Insecure network communication
- Weak authentication or session management
- Risks of reverse engineering and code tampering

The two main types of testing are:

1. **Static Analysis (SAST):** Examines the app's source code for vulnerabilities without running the app. It identifies issues like hard-coded credentials, insecure API calls, and weak encryption.
2. **Dynamic Analysis (DAST):** Tests the app while it is running to identify runtime vulnerabilities like data leakage, input validation issues, and improper session handling.

Checkmarx emphasizes **SAST**, which allows developers to secure their code early in the development process, reducing the chances of costly post-release fixes.

Checkmarx Mobile App Security Testing Features

Checkmarx offers a comprehensive set of **mobile-specific security features**:

1. APK & IPA Scanning

Checkmarx can scan **Android APK files** and **iOS IPA files** for potential vulnerabilities. It detects hard-coded secrets, insecure storage, and risky API usage.

2. OWASP Mobile Top 10 Coverage

The platform checks for all **OWASP Mobile Top 10 vulnerabilities**, including improper platform usage, insecure data storage, weak server-side controls, and insufficient cryptography.

3. CI/CD Pipeline Integration

Checkmarx integrates with tools like **Jenkins, GitLab, Azure DevOps**, and others, allowing teams to detect security issues early in the development cycle, also known as **Shift Left Security**.

4. Third-Party Library Analysis

It identifies vulnerabilities in open-source libraries and SDKs, preventing supply chain attacks and reducing compliance risks.

5. Comprehensive Reporting

Checkmarx generates clear and prioritized reports for developers and security managers, highlighting severity levels and offering remediation guidance.

Benefits of Using Checkmarx

Checkmarx provides multiple benefits for **developers** and **enterprises**:

For Developers

- Early detection of vulnerabilities in the code
- Reduced risk of security breaches
- Integration with familiar development tools
- Clear guidance on fixing security issues

For Enterprises

- Enhanced app security and customer trust
- Compliance with standards like **GDPR, HIPAA, SOX**
- Lower cost of fixing vulnerabilities after release
- Centralized management of multiple projects and teams

By using Checkmarx, businesses can ensure their mobile apps are secure, reliable, and market-ready.

Comparing Checkmarx with Other Mobile Security Tools

Checkmarx is a leading platform for mobile app security, but several other tools also help developers identify vulnerabilities. **Appknox**, for example, is a mobile-first security platform designed specifically for Android and iOS. It excels in real-device testing and API security, making it ideal for teams focused mainly on mobile apps. **Veracode**, on the other hand, provides a broad enterprise-level solution with SAST, DAST, and open-source library scanning. While Veracode covers both mobile and web applications, it may not offer the same depth of mobile-specific testing as Checkmarx or Appknox.

Other tools like **SonarQube** and **Snyk** are developer-focused, emphasizing code quality and open-source vulnerability management rather than full mobile app security. **OWASP ZAP** is free and open-source, primarily for web application testing, and offers limited mobile scanning capabilities. Overall, Checkmarx stands out by combining **static analysis, mobile-focused rules, library checks, and CI/CD integration**, providing a balanced solution for both developers and enterprises.

Use Cases & Industry Applications

Checkmarx is widely used across industries to ensure mobile app security:

- **Banking & Finance:** Protects sensitive financial data and ensures regulatory compliance.

- **Healthcare:** Secures patient information and meets HIPAA standards.

- **E-commerce:** Prevents data breaches and protects payment information.

- **Startups:** Helps small teams detect security issues early in development to save cost and time.

Many organizations integrate Checkmarx into their **DevSecOps workflows** to automatically detect vulnerabilities during the development process, reducing the chances of security breaches and improving user trust.

Conclusion

Mobile apps handle sensitive user data and are frequent targets of cyberattacks. Security cannot be an afterthought. Platforms like **Checkmarx Mobile App Security Testing** help developers and enterprises identify vulnerabilities early, fix them efficiently, and comply with industry standards.

Compared to other tools, Checkmarx provides a balanced approach for both mobile-first testing and enterprise-wide security management. By adopting Checkmarx, businesses can ensure safer mobile apps, protect users, and strengthen customer trust.

FAQs

What types of mobile apps can Checkmarx scan?

Checkmarx supports both **Android and iOS apps**, including native, hybrid, and cross-platform applications.

Does Checkmarx support both Android and iOS?

Yes. Checkmarx scans **APK files for Android** and **IPA files for iOS** using mobile-specific security rules.

How does Checkmarx differ from Appknox or Veracode?

Checkmarx focuses on **static code scanning and DevSecOps integration**, while Appknox prioritizes **mobile-first real device testing**, and Veracode is an **enterprise-wide solution** with broad AppSec coverage.

Can developers integrate Checkmarx into CI/CD pipelines?

Yes. Checkmarx integrates with **Jenkins, GitLab, Azure DevOps**, and other CI/CD tools to detect vulnerabilities early in the development lifecycle.

Is Checkmarx suitable for startups or only large enterprises?

Checkmarx is suitable for both startups and large enterprises, though small teams may need additional guidance for mobile-specific testing.

Tab 3