

Mobile Application Security

Find the flaws in your Android and iOS apps before attackers do

Mobile apps carry some of the most sensitive data a business holds: payment details, health records, identity documents and session tokens that open the door to backend systems. Once installed, your app runs on a device you do not control, in the hands of anyone who downloads it.

Attackers can decompile it, tamper with it, intercept its traffic and replay its API calls. One weakness in local storage, certificate validation or authentication can expose every user at once.

SentryArk's mobile assessments test the app, the data it leaves on the device and the APIs behind it, combining automated analysis with manual testing that follows the OWASP Mobile Application Security Verification Standard (MASVS).

TESTING BEYOND THE SCANNER

Automated scanners catch hard-coded keys and outdated libraries, but they cannot judge whether your authentication flow or business logic can be abused. Our consultants reverse engineer the app, instrument it at runtime and attack it the way a motivated adversary would, on rooted and non-rooted devices.

- Static and binary analysis
- Runtime instrumentation
- Insecure data storage
- Certificate pinning and TLS
- Authentication and sessions
- Backend API testing

ANDROID, IOS AND THE APIS BEHIND THEM

We test native, hybrid and cross-platform apps, including those built with React Native and Flutter. Every finding is checked by hand, rated for real business impact and reported with proof and clear remediation steps your developers can act on.

Testing can run on production builds, pre-release builds or both, and a retest confirms that fixes work before release.

ASSESSMENT DETAILS AND METHODOLOGY

Our mobile methodology maps to OWASP MASVS and the Mobile Application Security Testing Guide (MASTG). Each engagement combines automated tooling with manual analysis, so results are precise and repeatable.

Planning and information gathering	01	We agree scope, builds, platforms and test accounts, then map the app's features, data flows and backend endpoints.
Static analysis	02	We decompile and review the binary for hard-coded secrets, weak cryptography, insecure configuration and vulnerable third-party libraries.
Dynamic analysis	03	We run the app on instrumented devices, intercept its traffic, bypass client-side controls such as root detection and pinning, and inspect what it stores.
Backend and logic testing	04	We attack the APIs the app relies on for broken authorisation, data exposure and business logic flaws that affect every user.
Reporting and retest	05	A clear report with risk ratings, proof and remediation steps, followed by a retest to confirm the fixes.

The assessment includes

- Executive summary
- Risk ratings with proof of concept
- Android and iOS coverage
- Findings mapped to OWASP MASVS
- Detailed remediation steps
- Retest of fixed issues

ABOUT SENTRYARK

SentryArk is a team of security engineers and offensive security specialists. Our consultants hold OSCE, CRYPTO and CEH certifications. We have secured 20+ organisations, assessed 8K+ devices and 30+ applications, and reported 250+ vulnerabilities. Our focus is offensive security that shows the real-world risk to your business.