ZIMPERIUM®

Mobile Application Security Testing

Most companies do not fully integrate automated binary security scanning into their mobile app development workflows. Scanning the mobile binary can identify vulnerabilities such as insecure data storage, missing tamper protection, insufficient encryption, lack of runtime protection, and supply chain risks. Mobile app binaries are often not scanned or only scanned at the end of the release cycle, which does not help manage vulnerabilities effectively. Despite penetration testing's popularity, it is time-consuming and costly, making it unscalable. The development of mobile apps should include robust security measures, such as binary security scanning, to protect sensitive data, comply with regulations, and protect brand reputation.

Why Zimperium zSCAN

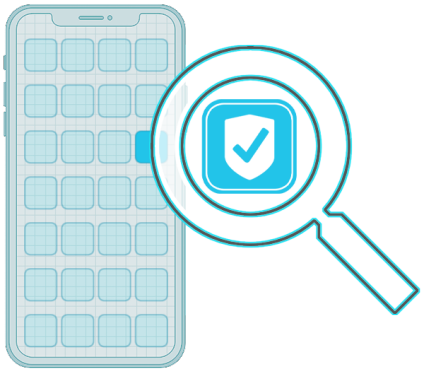
Zimperium zScan is a mobile app scanning solution that analyzes the binary of a mobile app to detect known or unknown vulnerabilities, including third-party libraries and frameworks not developed in-house. It can detect unique vulnerabilities not detectable through source code scanning, particularly when dealing with third-party libraries, obfuscated code, exploits, and tampering. All the findings from the scan are detailed, prioritized, and aggregated on a console to help application teams quickly locate and mitigate critical risks during development and pre-release testing. Dashboards and reports facilitate cross-functional collaboration and help ensure that apps become safer over time. In minutes, zScan provides actionable insights into your mobile apps' security, privacy, and compliance risks.

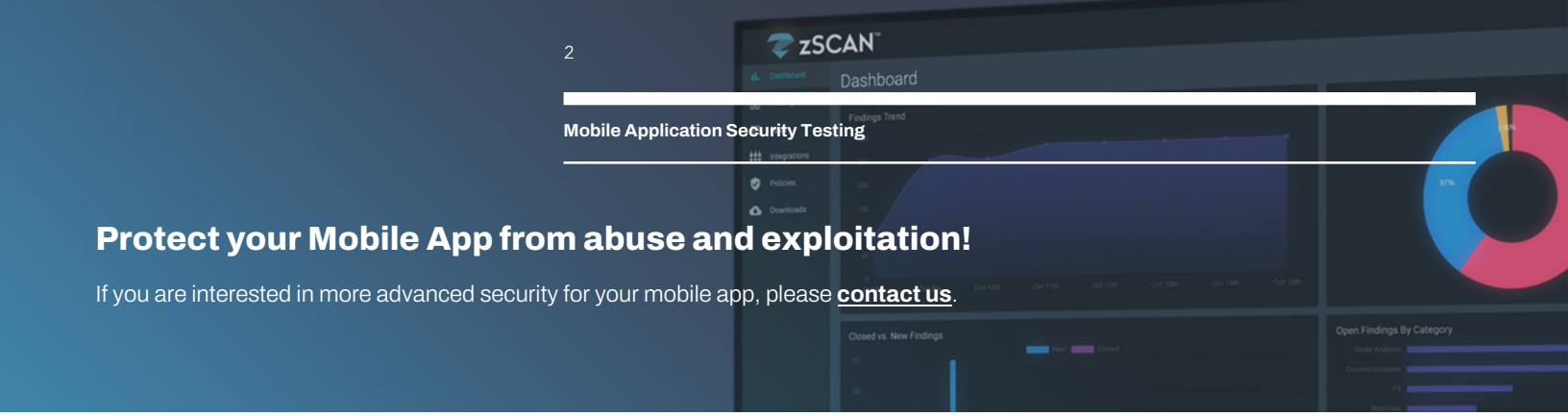
Core Benefits

- **Quick Time-To-Value -** SaaS-based solution needs no customer setup with Scans completing in 10-20 mins.
- **Comprehensive Scans -** Static and dynamic assessments of the entire app, including first-party and third-party components.
- **Ensure Compliance -** Coverage for OWASP Mobile Top 10, MASVS, NIAP, PCI, GDPR, etc.
- **SBOM Assessment -** Upload your SBOM and identify vulnerable and outdated components.
- **Focus On What's Important -** CVE, CVSS, CWE and impact information is provided to allow the security team to focus on fixing critical findings.
- **CI/CD Integrations -** Plugins, APIs, and actions in GitHub can be used to automate scans and action on findings via security orchestration tools within the ecosystem.
- **File Formats Supported -** IPA for iOS, APK & AAB for Android.

Why A Mobile-Focused Scan Is Critical

- **Mobile apps are subject to different compliance requirements -** Apps in highly regulated industries must comply with rules such as those from the FDA, GDPR, PCI, NIAP, OWASP for Mobile, MASVS, and HIPAA. Security guidelines for mobile apps differ significantly from those for web and desktop applications.. zScan provides an understanding of what your apps are doing and shows you risks you could be unaware of.
- **Mobile apps are attacked differently -** Mobile apps do not run inside the enterprise perimeter. Public app stores make it easy for attackers to download and analyze mobile apps. Therefore, each brand is targeted by cloned apps, malware, and phishing attacks. As mobile devices have high levels of hardware fragmentation, you should determine whether your code, data, and cryptographic key protections are adequate for all cases.
- **Mobile apps work best when they access device features -** Accessing device features that are typically not available to traditional applications, such as location, microphone, camera, contacts, and personal information, is one of the benefits of mobile applications. If you don't understand which permissions are dangerous, they can be abused. zScan provides an understanding of what your apps are doing and shows you risks you could be unaware of.





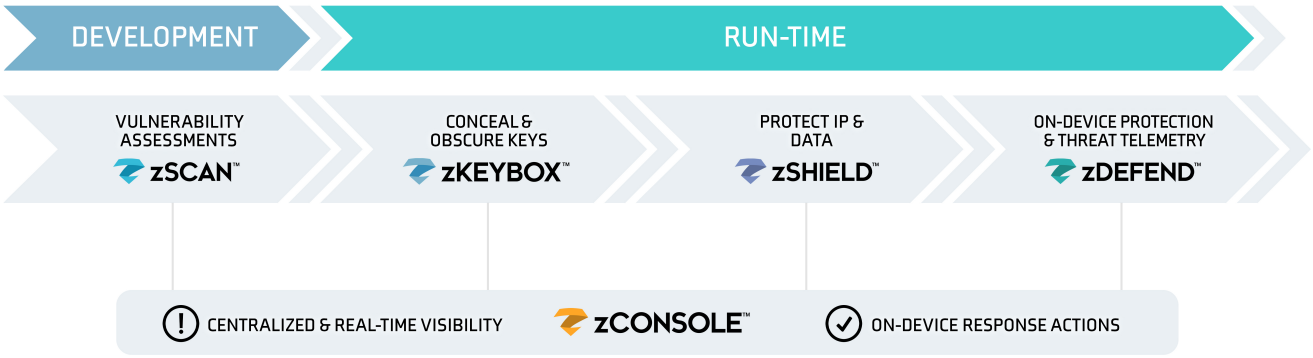
Protect your Mobile App from abuse and exploitation!

If you are interested in more advanced security for your mobile app, please **contact us**.

Why Zimperium

Zimperium's Mobile Application Protection Suite (MAPS) helps enterprises and developers build safe and secure mobile apps resistant to attack. It is the only unified solution that combines comprehensive app protection with centralized threat visibility.

MAPS comprises of four capabilities, each of which address a specific enterprise need as shown below.



Solution	Value Proposition
zSCAN™	Helps organizations continuously discover and fix compliance, privacy, and security issues prior to being published.
zKEYBOX™	Protect your cryptographic keys so they cannot be discovered, extracted, or manipulated.
zSHIELD™	Protects and hardens your source code, intellectual property (IP), and data from potential attacks like reverse engineering and code tampering.
zDEFEND™	Provides threat visibility, attestation, and on-device ML-based run-time protection against device, network, phishing, and malware attacks.
zCONSOLE™	Centralized dashboard to view risks and threats and create and deploy response policies.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244