ZIMPERIUM®
ADVANCED MOBILE SECURITY

zSCAN™

Solution Brief

Building safe and secure apps

Today, mobile applications are an effective digital channel for worker productivity and business growth, but they also introduce unprecedented risk. Organizations developing and using mobile apps are keenly aware of security risks as mobile apps are multifunctional and process more sensitive information than ever before.

The biggest hurdle for enterprises today is having to work with a highly fragmented set of point products that provide limited-to-no visibility into real-world risks, threats, and attacks.

Zimperium's Mobile Application Protection Suite (MAPS) is the only unified solution that combines comprehensive app protection with centralized threat visibility.

zScan: Continuous & automated security

While organizations have become proficient at developing mobile apps, many lack the ***ongoing and automated*** ability to discover privacy, security, and compliance issues in those mobile apps. When attackers discover and exploit these issues in the wild, the lack of visibility and actionable information can lead to breaches, stolen data, brand impact, and lost revenue.

For example, a recent analysis of the top shopping apps showed 100% of iOS-based apps and 90% of Android-based apps failed to receive a passing privacy grade, and 83% of iOS-based apps and 97% of Android-based apps failed to receive a passing security grade.

FOCUS ON MOBILE APP SECURITY ISSUES

7 out of 10
Number of mobile apps in which insecure data storage constituted a vulnerability

1 Day or Less
Amount of time in which DISA wants to be able to vet mobile applications for security gaps

71%
Percentage of mobile apps that leave information exposed to unauthorized access

180
Number of "critical" security problems found in a recent examination of 30 mobile apps in the financial services sector

74%
Percentage of flaws in iOS apps related to shortcomings of protection mechanisms that arise during the design phase

Why Mobile Apps are different

Compared to assessing and securing traditional applications, mobile apps have additional risks needing consideration:

1. **No control on device:** Mobile apps are often running on employees' or consumers' personal devices over which the app developer has little or no control
2. **Access to PII**: Mobile apps may have access to sensitive private information not typical for traditional applications such as location, microphone, camera, contacts and personal files on the device
3. **Third Party Code**: Mobile apps often utilize freely available libraries or SDKs that developers don't have the time or ability to fully inspect before embedding them; and
4. **Easy Access to Code**: Many mobile apps can easily be downloaded from public app stores and analyzed by attackers for vulnerabilities.

Why Pen testing is Not Sufficient

Enterprises cannot simply rely on pen testing inline without injecting delay in the development process. It's also not cost-effective. These two characteristics make pen testing unscalable as developers release changes more frequently.

Traditional code scanners do not identify some key risks (a few listed below) that make it easier to exploit mobile apps.

- Using SDKs that can violate privacy;
- Code that is easily reversed;
- Not securing communications;
- Sending sensitive data off the device;
- Contacting servers that are unsafe;
- Using compiler settings that are unsafe; and
- Having easily accessible API Keys.

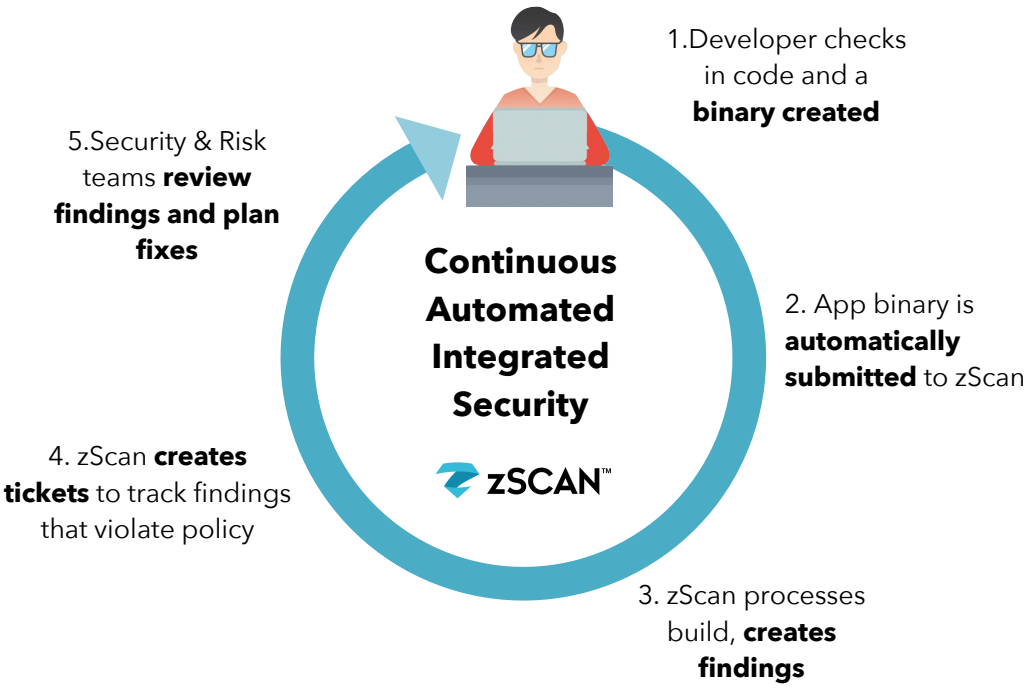
All of these realities call for a new approach to mobile app security. Organizations need an automated means to discover privacy, security, and compliance risks within the mobile app development process.

How zScan can help

Zimperium zScan helps mobile app developers avoid reputation and financial risks by automatically identifying privacy, security and compliance risks in the development process before apps are released to the public. While traditional code analysis tools help assess the quality of a developer's code overall, zScan's binary analysis capabilities help identify Security, Privacy and Compliance gaps and vulnerabilities that can be exploited by Cybercriminals.

As shown in Figure 1, zScan is designed to fit directly into the development process without requiring developers to do anything unusual.

Figure 1: zScan in the SDLC workflow



Benefits

- **Focus on Privacy:** Provides immediate visibility into Security and Privacy risks. Most scanning point solutions are focused solely on security.
- **Compliance Visibility**: Helps uncover compliance violations tied to NIAP, PCI, GDPR and the OWASP Top 10.
- **Prioritize Findings**: Allows security team to prioritize findings by providing CVE, CVSS and CWE information.
- **Compare Builds:** Quickly allows you to compare two builds to determine delta between the findings.
- **Customize What to Look For:** In zScan's administrative console, zConsole, compliance and security teams can define and customize policies to ensure only the findings being sought after are opened.

Easy Implementation

- **Easy App Upload:** Apps can be added directly from the build pipeline or manually uploaded as desired.
- **DevSecOps Integration**: Integration via plugins and APIs allow better integration, automaton, and collaboration across the DevSecOps lifecycle.
- **No Hardware Needed**: A SaaS solution that does not require investment in additional hardware.

Get a free risk assessment today

To learn more about Zimperium zScan or receive a demonstration, contact us today.

Why Zimperium MAPS

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

MAPS is comprised 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™	Protects your keys so they cannot be discovered, extracted, or manipulated
zSHIELD™	Protects the source code, intellectual property (IP), and data from potential attacks like reverse engineering and code tampering
zDEFEND™	Provides threat visibility and on-device ML-based run-time protection against device, network, phishing, and malware attacks

ZIMPERIUM®