






# Solution Brief

## STEP ONE IN MOBILE APP SECURITY: BUILDING COMPLIANT APPS

Organizations that develop mobile apps are keenly aware of the need to secure mobile apps, but their efforts have been stymied by a highly fragmented set of solutions and no visibility into threats on end user devices. To solve both problems, Zimperium's Mobile Application Protection Suite (MAPS) identifies security and privacy risks during app development and protects/monitors apps from attacks while in use.

MAPS is comprised of three solutions, each of which address a specific enterprise need:

Enterprise Need	MAPS Solution	Value
<b>Build Compliant</b> <i>What issues should be fixed before releasing our app?</i>	 <b>zSCAN™</b>	zScan helps organizations discover and fix compliance, privacy, and security issues within mobile apps before they are released as part of the development process.
<b>Build Secure</b> <i>How can we harden our app against reverse engineering or code tampering?</i>	 <b>zSHIELD™</b>	zShield app obfuscation and anti-tampering functionality protects the app from potential attacks like reverse engineering and code tampering.
<b>Run Secure</b> <i>How can we protect our app from advanced attacks on end user devices?</i>	 <b>zDEFEND™</b>	zDefend SDK is embedded in apps to help detect and defend against device, network and malicious app attacks.



This solution brief explains how Zimperium zScan helps organizations build compliant apps by identifying issues that should be fixed before releasing their app.

# DISCOVERING PRIVACY, SECURITY & COMPLIANCE ISSUES

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.<sup>[i]</sup>

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

1. Mobile apps are often running on employees' or consumers' personal devices over which the app developer has little or no control;
2. 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. 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

## FOCUS ON MOBILE APP SECURITY ISSUES

### 7 out of 10

Number of mobile apps in which insecure data storage constituted a vulnerability<sup>[ii]</sup>

### 1 Day or Less

Amount of time in which DISA wants to be able to vet mobile applications for security gaps<sup>[iii]</sup>

### 71%

Percentage of mobile apps that leave information exposed to unauthorized access<sup>[iv]</sup>


### 180

Number of "critical" security problems found in a recent examination of 30 mobile apps in the financial services sector<sup>[v]</sup>

### 74%

Percentage of flaws in iOS apps related to shortcomings of protection mechanisms that arise during the design phase<sup>[vi]</sup>



- 
4. Many mobile apps can easily be downloaded from public app stores and analyzed by attackers for vulnerabilities.

Mobile app risk mitigation is more than just obfuscation and anti-tampering. Manual pentesting cannot be done inline without injecting delay in the development process, and traditional code scanners do not identify risks (a few of which are listed below) that make it easier to exploit mobile apps.

- Using SDKs that can violate privacy;
- Including 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 *before they are available to users*.

## DISCOVERING MOBILE APP THREATS IN DEVELOPMENT WITH ZIMPERIUM zSCAN

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 identify risks that an attacker could uncover to exploit the completed app.

zScan documents risks within mobile apps including hardware specific usage, insecure API calls, and sensitive data handling. Apps can be added directly from the build pipeline or manually uploaded as desired. 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.



As shown in Figure 1, zScan is designed to fit directly into the development process without requiring developers to do anything unusual, implement any new code, or have to log into zConsole. Once findings are discovered, zScan can open tickets in ticketing systems to provide developers with detailed information and work packages necessary to address the risk. Once developers fix and mark findings closed (as they would any bug or feature request), the information is synced back to zScan so security and compliance teams can verify the fix.

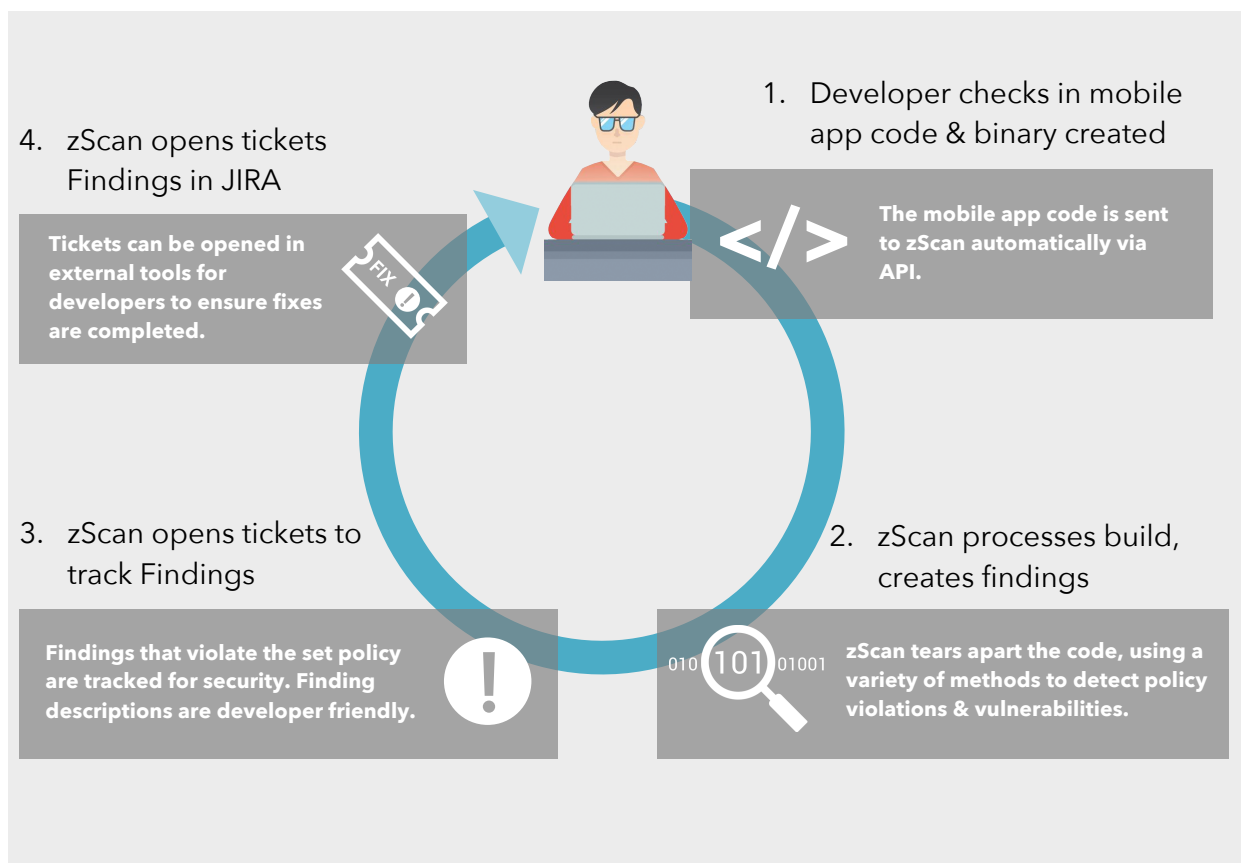


Figure 1: zScan in the SDLC workflow

Additionally, zScan's "Build Compare" capability quickly shows whether risks are trending up or down in each version over time. The version comparisons enable organizations to measure progress toward compliance and to deliver increasingly less vulnerable mobile apps.





## OVERCOME CHALLENGES WITH ZIMPERIUM zSCAN

Zimperium zScan helps organizations overcome challenges and consistently produce mobile apps with fewer privacy, security and compliance risks. Here are a few examples of the value brought by zScan:

Challenge	How zScan Helps
<b>The organization lacks visibility into mobile app risks that could damage its reputation or profitability.</b>	zScan gives you immediate visibility into app risks you would not see with other scanners across privacy and security.
<b>The organization has no automated way to ensure its mobile apps are compliant.</b>	zScan uncovers findings that may cause compliance issues for NIAP, GDPR and the OWASP Top 10.
<b>The development and security teams have little communication, leading to unidentified/unmitigated privacy and security risks.</b>	zScan connects security teams directly to developers by connecting the build pipeline, analyzing the data, and pushing tickets to the SCRUM tool making it simple to collaborate.

## REDUCE YOUR MOBILE APP RISKS WITH ZIMPERIUM zSCAN TODAY

To learn more about Zimperium zScan or receive a demonstration, [contact](#) us today.

[i] "Issues Found in Popular Shopping Apps", November 2019, Zimperium

[ii] Computer Weekly. Most mobile apps vulnerable to malware.

<https://www.computerweekly.com/news/252465425/Most-mobile-apps-vulnerable-to-malware>

[iii] NextGov. The agency is asking experts to submit ideas for an app development platform that would automatically check apps against the Pentagon's numerous security standards.

<https://www.nextgov.com/emerging-tech/2019/08/disa-wants-vet-mobile-app-security-day-or-less/158948/>

[iv] Dark Reading. Cyber-Risks Hiding Inside Mobile App Stores.

<https://www.darkreading.com/mobile/cyber-risks-hiding-inside-mobile-app-stores/d/d-id/1335031>

[v] Forbes. Financial Services Cybersecurity Still Porous: Report.

<https://www.forbes.com/sites/taylorarmerding/2019/08/01/financial-services-cybersecurity-still-porous-report/#3b327bd25379>

[vi] Dark Reading. Cyber-Risks Hiding Inside Mobile App Stores.

<https://www.darkreading.com/mobile/cyber-risks-hiding-inside-mobile-app-stores/d/d-id/1335031>