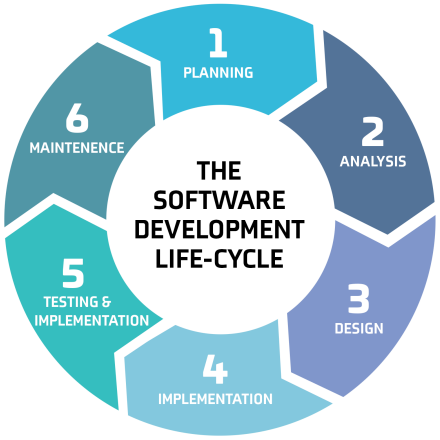
ZIMPERIUM®
MOBILE THREAT DEFENSE

Mobile Application Protection Suite (MAPS) Solution Brief

BARRIERS TO SECURING MOBILE APPS

Organizations that develop mobile apps are keenly aware of the need to secure those apps. Mobile apps are increasingly more sophisticated and are processing more sensitive personal and corporate information than ever before. Organizations are also well aware of the huge reputation and financial risks--whether direct via fraud or indirect via fines, etc.--that can result from mobile breaches.

Development and security teams need visibility throughout the entire software development life cycle (SDLC), but their efforts have been stymied by a highly fragmented set of solutions and no visibility into threats on end user devices. Mobile apps can drive significant business value, but only if the barriers to app security can be overcome, e.g.,



Barrier	Need
Fragmented Risk Assessment Solutions	Organizations need a consolidated view of all risks during development and continuously after application release.
No Visibility into Threats on User Devices	Organizations need clear and ongoing visibility into threats on user devices that can lead to data exfiltration and other risks.

ZIMPERIUM'S MOBILE APPLICATION SUITE (MAPS)

To solve both problems for our customers, Zimperium offers the only complete Mobile Application Protection Suite (MAPS). Zimperium MAPS identifies security/privacy/compliance risks during app development and protects/monitors apps from attacks while in use. MAPS is the only mobile app security solution that provides risk identification and protection across the entire SDLC.

MAPS is comprised of three solutions, each of which address specific enterprise needs and SDLC stages. With MAPS, the whole truly is greater than the sum of the parts. The solutions all utilize the same backend and administrative console, zConsole, to provide comprehensive and seamless visibility and management of risks and threats. By having an integrated suite across the SDLC, MAPS provides valuable insights that not only detect current risks, but also helps developers identify issues that can be solved in future releases.

The MAPS solutions include:

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

DISCOVERING MOBILE APP RISKS 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 provides immediate visibility into privacy and security app risks that are not detected with other scanners, and also uncovers findings that may cause compliance issues for NIAP, GDPR and the OWASP Top 10. In zScan's administrative console, zConsole, compliance and security teams define and customize policies so that only the non-compliant issues are delivered to developers to fix.

PREVENTING APP TAMPERING ATTEMPTS WITH ZIMPERIUM zSHIELD

Once a mobile app is released publicly, potential attackers can inspect it for any coding errors and vulnerabilities that can be exploited. Zimperium zShield's obfuscation and anti-tampering functionality hardens and protects the app from attacks such as reverse engineering, piracy, removing ads, extracting assets, extracting API keys and inserting malware. Unlike obfuscation solutions that rely upon manual pen testing to demonstrate effectiveness and have no active reporting, zShield provides on-going and immediate visibility into app tampering attempts on end user devices by reporting the events into Zimperium's administration and reporting dashboard, zConsole.

PROTECTING APPS FROM MOBILE ATTACKS WITH ZIMPERIUM zDEFEND

Zimperium's zDefend software development kit (SDK) enables developers to quickly and painlessly embed Zimperium's leading machine learning-based detection engine, z9, directly inside any mobile app. With the zDefend SDK embedded, mobile apps can immediately determine if a user's device is compromised, any network attacks are occurring and even if malicious apps are installed. zDefend is completely configurable by app developers, who can select whatever remedial action should apply when a given threat is detected. When a device is under attack, zDefend informs the app and initiates those predetermined risk mitigation actions.

SEE MAPS IN ACTION

Zimperium MAPS identifies security/privacy/compliance risks during app development and protects/monitors apps from attacks while in use. MAPS solves both barriers to mobile app security by being the only solution to provide:

- A consolidated view of all risks during development and continuously after application release.
- Clear and ongoing visibility into threats on user devices that can lead to data exfiltration and other risks.

If your business could benefit from immediate, effortless and robust mobile app security, Zimperium's MAPS is right for you.

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