ZIMPERIUM®
MOBILE THREAT DEFENSE

ZIMPERIUM zDEFEND™

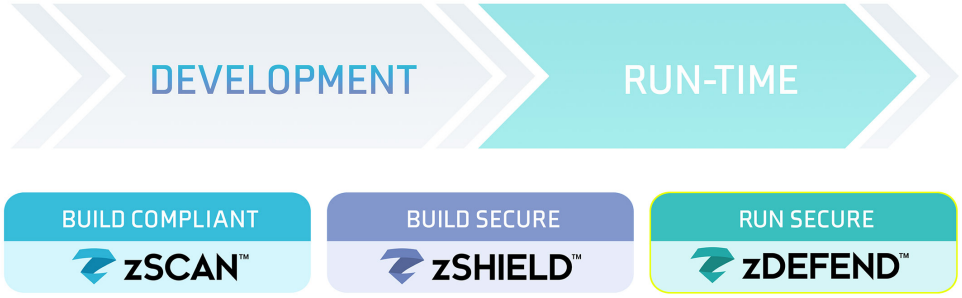
World-class threat protection for your mobile app, in seconds.

STEP THREE IN MOBILE APP SECURITY: RUNNING SECURELY ON DEVICES

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
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.



This solution brief explains how Zimperium zDefend protects apps from advanced attacks on end user devices.

NEW THREATS TARGETED AT MOBILE APPS

Mobile apps are now extremely attractive targets for malicious activity. Attackers have repeatedly shown the ability to exploit vulnerabilities, fake Wi-Fi networks and malicious apps in order to compromise mobile devices. And when device owners open the door to their device, even accidentally, mobile app providers inherit the risk.

"Mobile malware will amount to one-third of total malware reported in standard tests."

Gartner

Malware has become pervasive throughout app stores, especially third-party stores outside of Apple's App Store and Google Play. Mobile applications that elevate privileges and device exploits can collect and disclose sensitive data. They are leveraged as attack vectors to infiltrate the network and gain access to resources and data. These attacks bypass existing security and exploit prevention controls, using advanced techniques to gain control of devices or customer accounts through social engineering[v].

Mobile devices now constitute the majority of web traffic globally, and consumers are embracing mobile apps in record numbers, e.g,.

- Of the 7.6 billion people in the world, there are 5.1billion unique mobile device users[i].
- In the first quarter of 2017, 50.03% of global web traffic was from mobile devices[ii].
- The average mobile user spends over 100 hours per day online, more than 3x the average desktop usage[iii].

In the fourth quarter of 2017 alone, there were 26 billion app downloads from Google Play and the Apple App Store (19 billion and 7 billion, respectively)[iv].

THE BUSINESS CASE FOR IN-APP MOBILE THREAT DEFENSE

Mobile attacks are rampant and increasingly sophisticated today. They cause huge damage to profitability, reputation and brand value.

Data leakage, in particular, exposes organizations to the following risks:

- **Brand image deterioration**
- **Customer trust erosion**
- **User experience damage**
- **Unauthorized access and fraud**
- **Confidential data theft**
- **Revenue loss from piracy**
- **Intellectual property theft**

Mobile app protection presents unique challenges. Mobile app developers are under pressure to deliver apps quickly and often prioritize functionality over security. Vulnerability assessments are often limited to basic Jailbreak or root checks gathered from public code examples. Protecting mobile apps and their users requires solutions that are built from the ground up for mobile environments. These solutions should also adapt to new threats without requiring the app developer to update or rewrite the application.

zDEFEND: POWERING IN-APP PROTECTION

Mobile attacks are rampant and increasingly sophisticated today. They cause huge damage to profitability, reputation and brand value.

Zimperium solutions allow customers to detect and prevent more mobile threats, with the least amount of organizational friction, than any alternative.

> ***"Zimperium's on-device mobile threat protection technology is well-suited to providing In-App Protection from both known and, hugely importantly, unknown threats."***
>
> Chris Marsh
> Research Director for Enterprise Mobility at 451 Research

As a part of MAPS, Zimperium provides a powerful tool with which developers can rapidly and easily enhance mobile app security. 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.

zDEFEND™

zCONSOLE™

zDefend is supported by zConsole, Zimperium's management and reporting console, including threat forensics, policy administration and industry-leading integrations with SIEM solutions.

zDEFEND: DETECTION & REMEDIATION

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. zDefend remediations include, but are not limited to:

- **Clear app cache**
- **Logging the user out**
- **Invalidating the session**
- **Deleting any app security keys**
- **Marking the transaction & flipping a fraud alert flag**
- **Aborting any active transactions**
- **Alerting the user**
- **Making app read-only** (e.g. search for an ATM allowed, but no cash transfer)
- **Triggering another authentication in a multi-factor authentication chain**
- **Reducing transfer limits**

> ***"Combating fraud is a major focus for our bank. We selected Zimperium to protect millions of online customers, and billions of transactions, against malicious apps like BankBot, device exploits and rogue WiFi networks."***
>
> ———
>
> -CSO,
> Global 100 Financial Institution

Here are some examples to make this real. If the embedded zDefend detects:

- A man-in-the-middle (MITM) attack is occurring, the app can automatically establish a VPN to create a secure tunnel.
- A device has malware like BankBot installed, the app can trigger immediate steps to freeze access until the user deletes the BankBot-carrying app and resets their password online.
- A device has been Jailbroken by the user, the app can allow the session to continue, but raise the user's fraud score to account for the additional risk.
- A device has been compromised by an external actor, the app can display a dialog box asking the user to complete their transaction offline [vi].

SEE zDEFEND IN ACTION

zDefend enables developers to spend more time developing and less time worrying about security. zDefend quickly and dramatically improves the security of any mobile app and its sessions. With security safely embedded in mobile apps, organizations can focus on innovations that will delight customers, increase customer loyalty and unleash the full potential of the mobile era.

If your business could benefit from immediate, effortless and robust mobile app security, Zimperium's zDefend™ in-app protection is right for you.

Feel free to give us a call at 844.601.6760 or visit us at http://www.zimperium.com to learn more.

ZIMPERIUM®

[i] The World Going Digital, Statista, 2018
[ii] Percentage of mobile device website traffic worldwide from 1st quarter 2015 to 3rd quarter 2017. Statista, 2017
[iii] "Mobile Advertising Forecast, 2016", Zenith, 2016
[iv] "Record Levels of App Downloads & App Store Consumer Spend in Q4 2017", App Annie, 2018
[v] "Market Guide for Mobile Threat Defense Solutions", ID: G00314969, Gartner.2017
[vi] 451 Research, "2016 Trends in Enterprise Mobility", 2016