



Zimperium zShield

Shield your code. Don't just obfuscate it.

Enterprises today rely on mobile applications to drive business and productivity across employees, partners, and customers. These apps deliver value by bringing together sensitive data, confidential keys, APIs, and proprietary business logic within the application's code. But most of these applications are published to the official app stores with little to no code protections. This allows malicious actors and competitors to download, inspect, exploit and abuse the application without setting off any enterprise alarms.

A malicious actor can very easily download the targeted app from an app store and reverse-engineer it within their local environment using a suite of advanced inspection tools. Once inspection is successful, they can then tamper with the code, repackaging it with malware and redistribute it to customers via third-party stores and phishing campaigns to steal account credentials and commit fraud.

So using rudimentary obfuscation alone is not sufficient. You need additional protections against code tampering.

Below are some key elements that are exposed when you don't protect your code:

- Hardcoded Sensitive Data
- Embedded Keys
- Critical Business logic
- Cloud Access Keys
- Vulnerable Third-party components
- Permissions
- API URLs, Token and key

The Commission on the Theft of American Intellectual Property estimates that annual costs from IP losses range from \$225 billion to \$600 billion. This number should not be a surprise considering that mobile application revenue alone is projected to hit \$953 Billion by 2023.

How Zimperium Can Help Secure Code

Zimperium's zShield is a comprehensive application shielding solution. It protects the app with advanced obfuscation and anti-tampering functionality to protect the source code, intellectual property (IP), APIs and data within the application. Protecting the application from the inside allows enterprises to protect the business, brand, and customer trust proactively.

Anti-Reverse Engineering

Advanced Obfuscation

Anti-Debugging

Binary Packing

Diversification



Anti-Tampering

Integrity Checking

Anti-Method Swizzling

Function Caller Verification

Jailbreak / Rooting Detection

Shared Library Cross-Checking

Mach-O Binary Signature Verification

Google Play Licensing Protection

Customizable Defense Actions

Customer Case Study | Protect Payments on Point of Sale Devices

Our customer offers a cloud-based software-only point of sale (SoftPoS) mobile application for merchants. It turns any Android off-the shelf (COTS) mobile phone/tablet into a mobile POS terminal. Once the app is installed on the merchant's device, they can tap the customer's card or mobile device onto the back of the mobile device to process the payment via NFC. zShield helps accelerate the process of achieving and remaining PCI compliant. The advanced code protection secures the business-critical code handling payments from being reverse-engineered and abused via malware on the device.

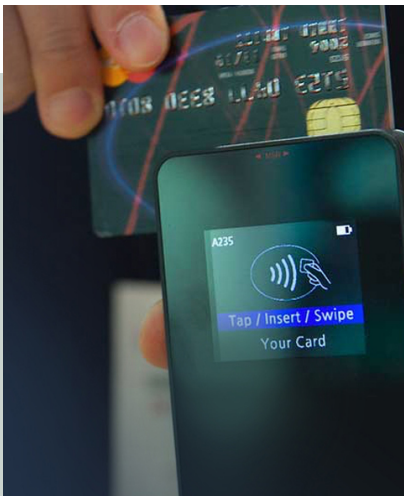
According to Research and Markets, the mPOS terminals market is set to grow by **USD 6.01 billion during 2021-2025**. The mPOS also uses a device (phone or tablet) but it must be paired with an external card reader that acts as an electronic POS terminal. On the other hand, the SoftPOS doesn't need an external card reader to work as a POS terminal.

Customer Case Study | Securing Connected Health Devices

Our customer builds and offers mobile and desktop applications that control and collect information directly from diabetes management systems, such as insulin pumps and glucose monitoring devices. The data is shared with end-users and doctors via mobile and web apps to help align on diagnosis and treatment. The apps contain patented software that reads real-time readings and automatically adjusts dosage every few minutes. The mobile application connects directly with the pump, allowing the end-user to view sugar trends and insulin delivery on the go.

zShield protects proprietary algorithms within the code that calculates and dispenses the right amount of insulin. This advanced code protection helps customers preserve their competitive differentiation in the market and, more importantly, prevent tampered fake apps from being used, resulting in compromised patient health.

According to Verified Market Research, the Global Connected Medical Devices Market size was valued at **USD 27.39 Billion** in 2020 and is projected to reach **USD 136.76 Billion** by 2028, growing at a CAGR of 22.26% from 2021 to 2028.



Why Zimperium's zShield

Anti-Reverse Engineering

Advanced protection from reverse engineering with techniques such as advanced obfuscation, anti-debugging, diversification and binary packing.

Advanced Anti-Tamper defense

Embed robust tamper detection mechanisms such as Integrity Checking, Anti-Method Swizzling, Function Caller Verification, Jailbreak / Rooting Detection, etc, and automated defense response to prevent any attempts at altering or inserting malware into your code. This prevents applications from being repackaged and distributed with malicious campaigns.

Runtime Visibility

Immediate and ongoing reporting on tampering attempts once the application is published.

Easy implementation that accelerates time-to-market

Bring highly secure, standards-compliant applications to market faster. Fully automated protection easily slots into your existing build cycle.

Performance Tuning

Tune the level of code protection embedded to ensure optimal application performance, application size and a positive end-user experience.

Widest Platform Support

- Platforms: Android, iOS, tvOS, macOS, iPadOS, watchOS, Windows, Linux, QNX, and others.
- Languages: Java, C, C++, Objective-C, Swift, Kotlin.

Regulatory-grade

Meet and exceed data privacy and application security requirements while minimizing approval and testing timelines for regulation such as PCI CPoC, SPoC, EMVCo, etc.

Protect Your Code Today

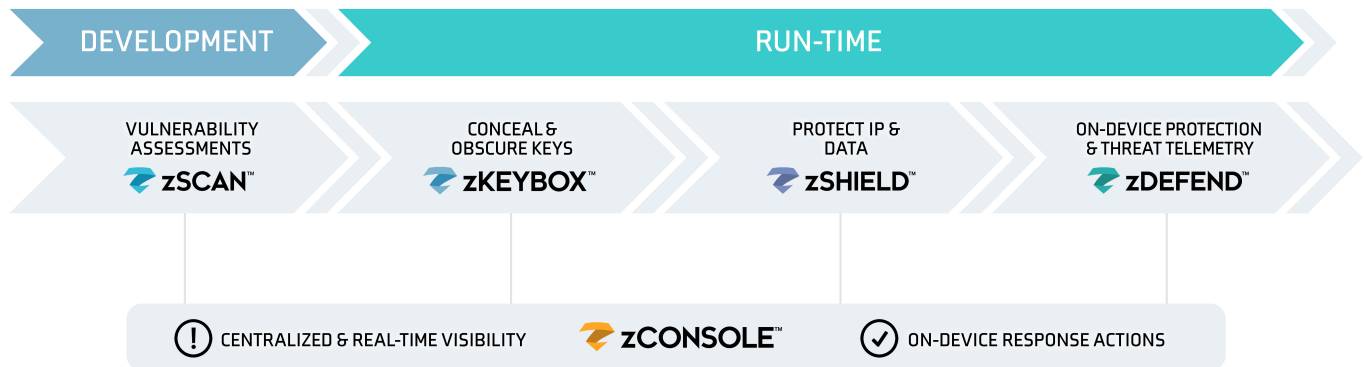
If you are interested in more advanced security for your application's source code, please [contact us](#).



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 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 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.
zCONSOLE™	Centralized dashboard to view threats and create response policies.