Why You Need To Shield Your Apps

zSHIELD™

ZIMPERIUM®

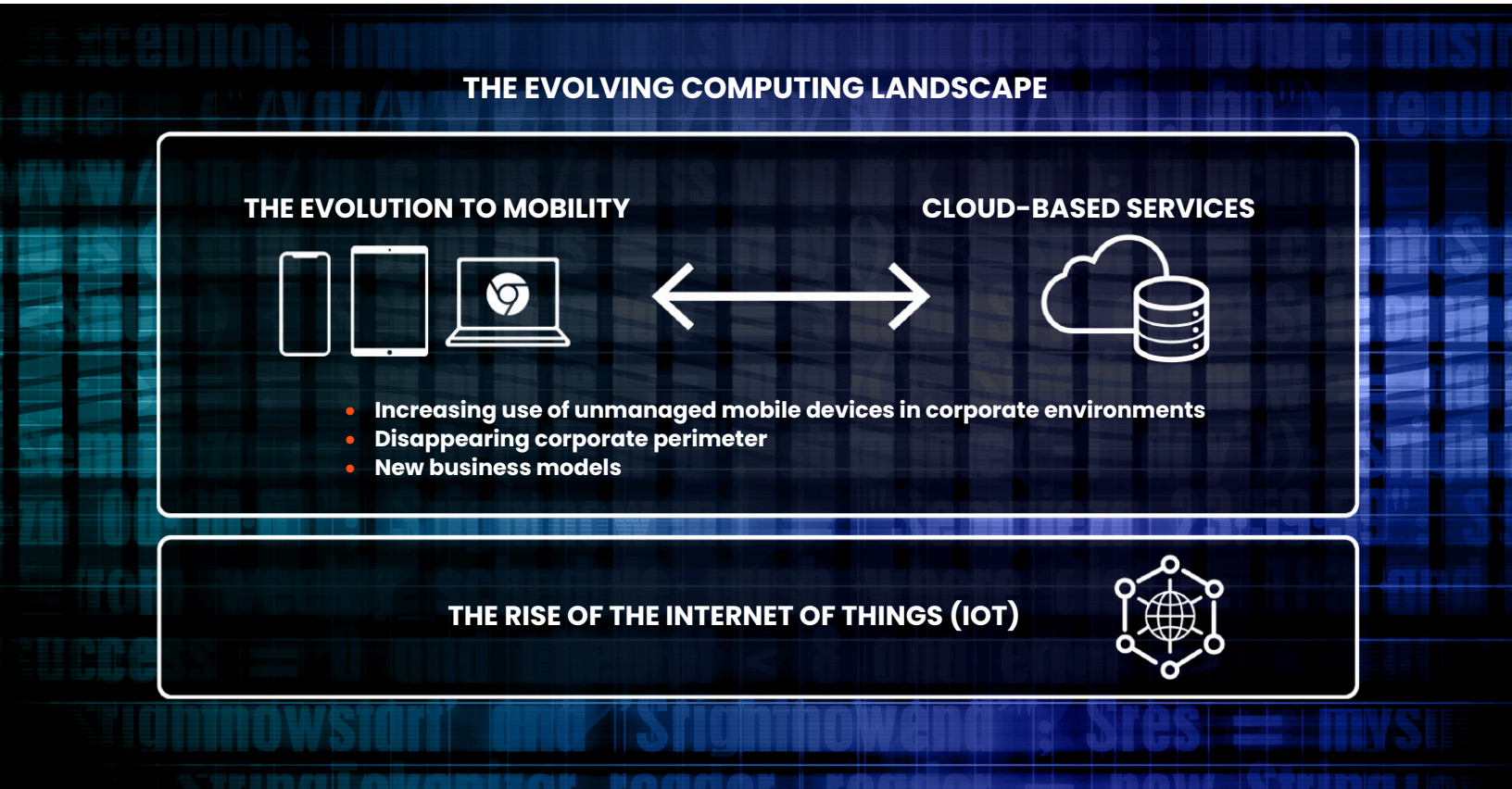
Executive Summary

The world of computing has changed. Security is not just about physically secure data centers and corporate controlled computing assets. Instead, end users have gone mobile, connecting to cloud enabled services, often with their own personal devices. And with the rise of the Internet of Things, there will be billions of connected computing devices on the planet in the next several years. These changes significantly impact the way organizations are providing services to their customers, enabling new business models and new ways to do business.

But these changes also create new opportunities for hackers who have unprecedented physical access to these devices. Hackers have a wide variety of goals including bypassing business logic, stealing intellectual property or sensitive data, obtaining cryptographic keys to steal content, masquerade as users, snoop on secure communications, or hack a device as a stepping stone to launch attacks against other devices. If they are successful, then the consequences can include financial loss, impact on brand reputation, and exposure to liability.

The way hackers go about achieving their goals starts with reverse engineering software to find vulnerabilities they can exploit, data they can extract, or ways to modify the software to do something it was never intended to do. As hackers get increasing access to mobile and IoT devices, this threat also increases. As a consequence, it is becoming increasingly important for organizations to deploy **application shielding** technology that makes it difficult for hackers to reverse engineer and tamper with software.

This white paper describes these threats in detail, and describes Zimperium's market leading application shielding product, **zShield**. zShield provides application developers with a comprehensive suite of anti-reverse engineering and runtime application security protections to help protect your applications. zShield is easy to use and requires no significant changes to the code itself or the existing build chain. Since zShield secures source code before it is compiled, protected builds can easily be delivered to an app store, end point, mobile device, connected car, and other types of IoT devices.



Zimperium's zShield is a powerful application shielding solution designed to prevent malicious actors from reverse engineering and tampering with your mobile applications and SDKs. By combining obfuscation, integrity checking, anti-debug, anti-tampering, and other techniques, the solution protects source code and binary codes from a variety of sophisticated inspection techniques and dynamic attacks. Apps protected by zShield can detect threats and defend themselves on the device by taking predefined on-device actions. In addition to identifying performance-sensitive code, the solution's analysis features can help app teams determine how well the app has been protected after protection.

zShield can be integrated without modifying the original source code or current build processes with minimal configuration. All protections applied to the app are optimized so that they have the least impact on the app's size, performance, and debugging.

zShield aims to make it infeasible for bad actors to perform unauthorized static or dynamic inspection of your mobile applications.

Key Benefits

Prevent Code Theft

Protect intellectual property, such as proprietary algorithms or innovative features, from being stolen.

Stop Unauthorized Modifications

Restrict malicious actors from reverse engineering apps in an attempt to alter their behavior, insert malware, or introduce malicious features.

Prevent Adversarial Analysis

Make it infeasible to inspect the app to understand its inner workings and find exploitable vulnerabilities.

Piracy and Copyright Infringement

Prevent unauthorized distribution and bypassing licensing mechanisms.

Protect Credentials & Sensitive Data

Protect sensitive data from malware, phishing, and compromised devices.

Real-time Visibility

Get real-time alerts when a malicious actor attempts to tamper with an application.

Fit for Purpose: Choose the Option that's Right for You

zShield offers two options —**Low Code** and **No Code** —designed to provide robust security measures tailored to your specific requirements. Whether you prefer a no-code approach or seek advanced precision and control we have the right solution for you.

You can choose from the two options below:

	Low Code Granular Control	**No Code** Upload & Protect
Decisive Factor	Select the code to protect and the level of protection to apply	Upload the app binary and choose from predefined protection options
Protection Method	Source Code and Binary Code	Binary Code
Level of Detail		
Precision	Choose files or functions to protect	Choose the binary to protect
Granular Control	Choose specific protection techniques	Choose broad protection types
Profiling	Protecting Tuning	
Protection Preview	Post Protection Results	
Protections		
Code Obfuscation	Advanced	Basic
Anti- Reverse Engineering	Advanced	Basic
Anti-Tampering	Advanced	Basic
Integrity Protection	Advanced	Basic
Debugging/Hooking Protection	Advanced	Basic
Rooting/Jailbreak Detection	Advanced	Basic
Platform Threat Detection	Yes	Yes
Network Threat Protection	Add-On	Add-On
Malware Protection	Add-On	Add-On
Custom Response Actions	Advanced	Basic

	Low Code Granular Control	No Code Upload & Protect
Threat Telemetry		
Centralized Console	Yes	Yes
Threat Forensics	Yes	Yes
Over-The-Air Updates		
Response Actions	Yes	Yes
Dynamic Detections	Yes	Yes
Support		
Platforms Supported	Mobile & Non-Mobile	Mobile Apps
Deployment Model	On-Premise	SaaS

Why Zimperium zShield

Flexibility
- Enables you to select Low-Code or No-Code options according to your security and development needs.

Regulatory-grade Protection
- Meet and exceed data privacy and application security requirements while minimizing approval and testing timelines for regulations such as PCI CPoC, SPoC, EMVCo etc.

CI/CD Integration
- The process of applying protections to an app can be fully integrated and automated via APIs.

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

Support for Application Types
- Supports native and hybrid applications.

*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**.*

Case Studies

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 Medical 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.

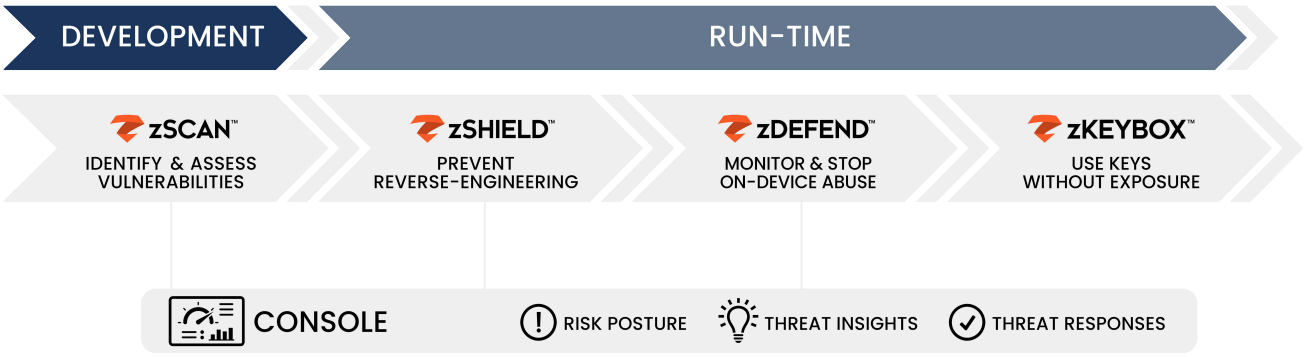
Protect Your Application Today

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 four capabilities, each of which address a specific enterprise need as shown below.



Solutions	Value Proposition
zSCAN™	Helps organizations continuously discover and fix compliance, privacy, and security issues prior to being published.
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.
zKEYBOX™	Protect your keys so they cannot be discovered, extracted, or manipulated.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244