Advanced Application Shielding

zSHIELD™

ZIMPERIUM®

Application Shielding is a core part of Zimperium's Mobile Application Protection Suite (MAPS), built to protect mobile apps and SDKs from reverse engineering and tampering.

It combines code obfuscation, integrity checks, anti-debugging, and runtime protections to defend both source code and binaries from static and dynamic attacks. Protected apps can detect threats and respond instantly with on-device actions, updated over-the-air (OTA) to keep pace with evolving threats.

Apps can also be **assessed** for remaining security, privacy, and compliance gaps, giving teams clear visibility and confidence in their protection.

Integration is easy. Apply advanced protections in the CI/CD pipeline, or quickly secure apps by uploading the binary, no code changes required. Protections are lightweight and optimized for performance and usability.

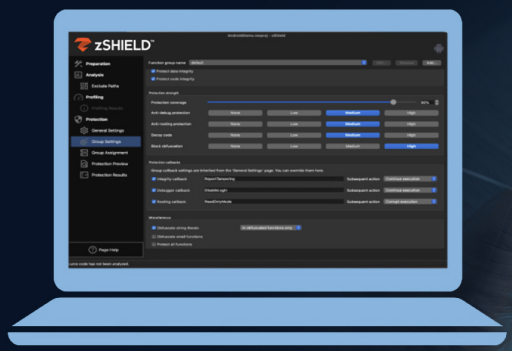
Unlike point solutions, zShield is part of a complete mobile app security platform—integrated with runtime protection, threat telemetry, OTA updates, and centralized policy management—offering more than just shielding.

Update Security Over-The-Air.

Fewer Security Patches.

During App Development

Granular Control



Specify Code to Protect

Select Protection Types

Choose Protection Levels

Once the App is Published

Centralized Threat Visibility

Key Benefits

Prevent Code Theft

Protect proprietary algorithms, business logic, and innovative features from reverse engineering and theft.

Stop App Repackaging

Prevent attackers from modifying, repackaging, and redistributing your app with injected malware or unauthorized changes.

Detect Jailbreaks, Roots & Emulators

Identify and respond to high-risk environments like rooted/jailbroken devices or emulators to stop exploitation.

Harden APIs Against Abuse

Obfuscate API structures and encrypt interactions to prevent spoofing, tampering, and abuse of backend services.

Protect Credentials & Sensitive Data

Safeguard embedded secrets, tokens, and personal data on compromised devices.

Real-time Threat Visibility

Get instant alerts and telemetry when apps are tampered with enabling faster response and better risk scoring.

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

The solution 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
Protection		
Protection Level	Source Code	App Binary
Implementation Options	Select the code to protect and the level of protection to apply	Upload the app binary and choose from predefined protection options

	Low Code Granular Control	**No Code** Upload & Protect
Level of Control		
Code Selection	Choose files or functions to protect	Choose the app to protect
Protection Features	Choose protections to apply	Choose broad protection types
Performance Profiling	Yes	No
Protection Validation	Yes	Yes
Protections		
Code Obfuscation	Advanced	Essential
Anti- Reverse Engineering	Advanced	Essential
Anti-Tampering	Advanced	Essential
Integrity Protection	Advanced	Essential
Repackaging Protection	Advanced	Essential
Device Attestation	Advanced	Essential
Debugging/Hooking Protection	Advanced	Essential
Rooting/Jailbreak Protection	Advanced	Essential
Java String Encryption	Yes	Yes
Resource Protection	Yes	Yes
Network Threat Protection	Yes	Yes
Outdated OS Protection	Add-On	Add-On
Malware Protection	Add-On	Add-On
Response Actions	Shut Down App Redirect URL Call Custom Function	Shut Down Ap Redirect URL

	Low Code Granular Control	**No Code** Upload & Protect
Threat Telemetry		
Centralized Console (No Additional Cost)	Yes	Yes
Threat Reporting	Yes	Yes
Threat Forensics	Yes	Yes
Over-The-Air Updates (Without Republish the App)		
Response Actions	Yes	Yes
Detections	Yes	Yes
Support		
Compatible with R8 Optimization	Yes	Yes
Compatible with Crashlytics	Yes	Yes
Platforms Supported	Mobile & Non-Mobile	Mobile Apps
Deployment Model	On-Premise	SaaS

Why Zimperium Application Shielding

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 MPoC, 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, Windows, Linux 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.

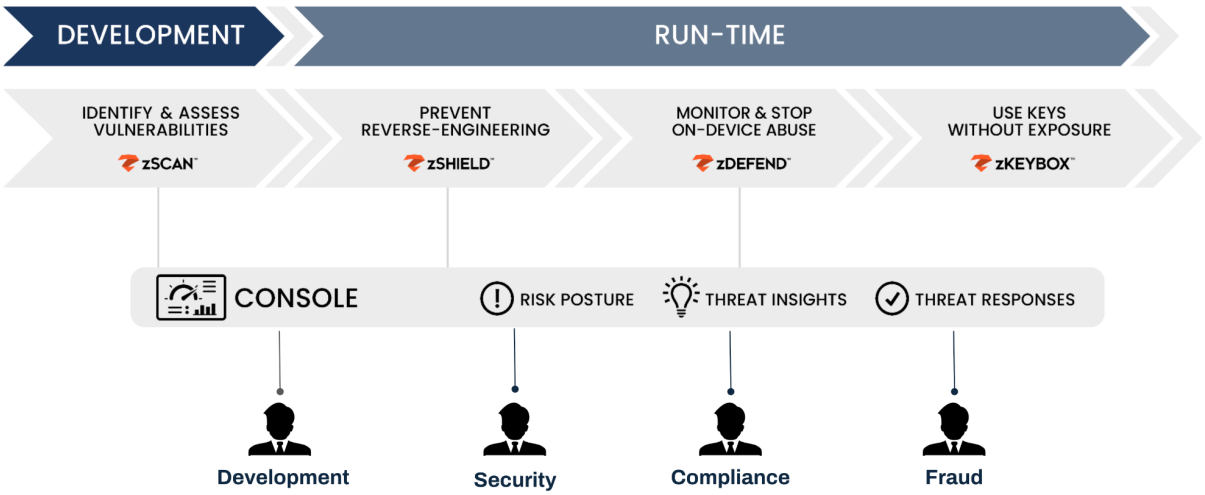
Protect Your Application Today

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.



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

About Zimperium

Zimperium is the world leader in mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244