ZIMPERIUM®
ADVANCED MOBILE SECURITY

zSHIELD™

Solution Brief

Building safe and secure apps

Today, mobile applications are an effective digital channel for worker productivity and business growth, but they also introduce unprecedented risk. Organizations developing and using mobile apps are keenly aware of security risks as mobile apps are multifunctional and process more sensitive information than ever before.

The biggest hurdle for enterprises today is having to work with a highly fragmented set of point products that provide limited-to-no visibility into real-world risks, threats, and attacks.

Zimperium's Mobile Application Protection Suite (MAPS) is the only unified solution that combines comprehensive app protection with centralized threat visibility.

zSHIELD: Hardening your apps

Once a mobile app is publicly released, attackers can inspect it for exploitable coding errors and vulnerabilities. Zimperium zShield hardens and protects the application source code, intellectual property, and data. Its advanced multi-layered obfuscation and anti-tampering functionality limits attacks such as reverse engineering, piracy, removing ads, extracting assets, and repackaging with malware.

zShield hardens and protects your apps in three primary ways:

- Obfuscation to Prevent Reverse Engineering
- App Tampering Visibility in the Wild
- Seamless Development & Security Integrations

Benefits

- **Visibility:** Immediate and on-going reporting on tampering attempts.
- **Benefits Powerful code obfuscation:** Patented source code level obfuscation gives you unsurpassed protection while maintaining performance.

- **Advanced anti-tamper defense**: Embed robust tamper detection mechanisms and automated defense response to prevent any attempts at altering or inserting malware into your code.
- **Accelerate time to market:** Bring highly secure, standards compliant applications to market faster. Fully automated protection easily slots into your existing build cycle.
- **Widest platform support:** Protect native, hybrid, and embedded apps on mobile devices, desktops, servers, and IoT devices.
- **Comply with regulations:** Meet and exceed data privacy and application security requirements while minimizing approval and testing timelines.

Easy implementation that accelerates time-to-market

- **Fully automated** Minimal or no changes required to the original source code. Fits right into your existing SDLC.
- **Code profiling:** Ensures maximum performance and minimum footprint for protected applications with no manual configuration required.
- **Security expertise:** Deep expertise is built in and continuously improved to stay ahead of changing conditions and customer needs.
- **Full control:** Select the modules to protect to optimize safety, footprint and performance. GUI or CLI: Use the intuitive GUI or the CLI to integrate into existing CI/CD workflows.

Wide platform support

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

Seamless development & security integrations

zShield transparently integrates into your build process and requires no changes to your source code. It provides plugins for all common build tools and development environments like Gradle, Android Studio, Ant, Eclipse, Maven, and custom builds.

After your app is optimized and obfuscated with zShield, it will report hacking and reversing attempts directly into your security information and event management (SIEM) system for further analysis and action. zShield's standard integrations enable your security teams to view mobile threats in the same console they currently use for managing threats from traditional endpoints and networks. Depending on the

attack, the security team can quickly provide details to development to fix the issues and prevent future exposures from the threat.

Make your apps tamper resistant today

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

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 is comprised 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™	Protects 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