

Mobile Application Protection Suite (MAPS)



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 access and process more sensitive information than ever before.

Mobile application risks start in development and persist throughout the app's entire lifecycle, including when running on an end user's device. Uncovering these during development saves time, money, and resources associated when compared to reacting to them in production. Once an app is published, it remains exposed to the untrusted environments in which it runs. These risks include compromised devices running the app, the vulnerable networks the device connects to, and bad actors attempting to tamper the app for their benefit.

When left unchecked these risks can lead to the following:

- **Data breaches or fraud** due to attacks or through reverse engineering;
- **Damages to your company's reputation** and bottom line, resulting from private information being leaked; and
- **Regulatory fines** resulting from not being compliant or because of a breach.

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

A Single Integrated Platform – Development Through Runtime

Zimperium's Mobile Application Protection Suite (MAPS) helps enterprises build safe and secure mobile apps resistant to attacks. It is the only unified platform that **combines comprehensive in-app protection with centralized threat visibility**. The platform provides app shielding, key protection, app scanning, and runtime protection capabilities. In addition, a threat management dashboard provides real-time threat visibility and the ability to respond to emerging threats instantly without an app update.

90%

of mobile time is spent in apps

83%

of the apps insecurely stored data

High-risk vulnerabilities were found in

38% of iOS and in **43%** of Android applications

89%

of all vulnerabilities discovered could be exploited using malware

Here are some key benefits:



Identify Security & Privacy Vulnerabilities



Protect Cryptographic Keys & Secrets



Gain Runtime Threat Visibility



Ensure Internal & External Compliance



Protect Source Code, IP, and Sensitive Data

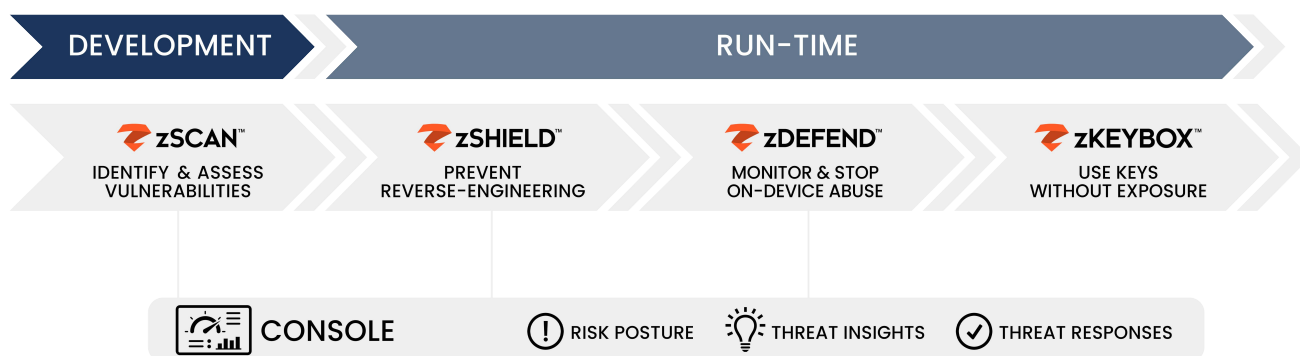


Respond to Data Theft & Fraud Attempts

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.



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.