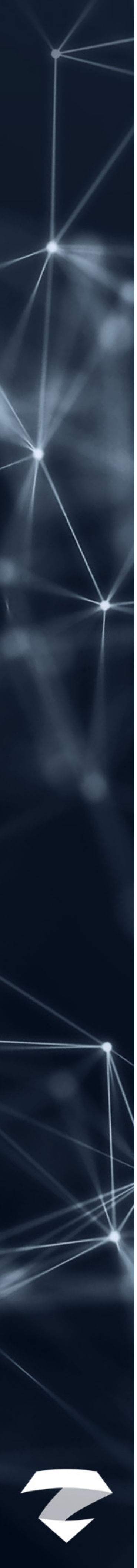
ZIMPERIUM®
ADVANCED MOBILE SECURITY

zDEFEND™

Solution Brief

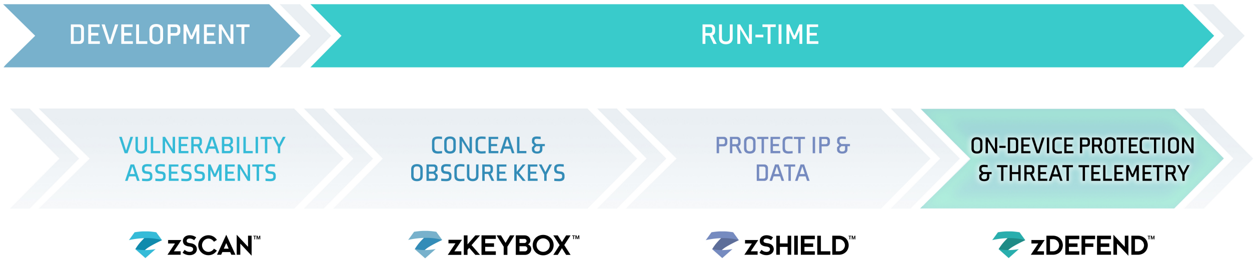


Building safe and secure apps

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.



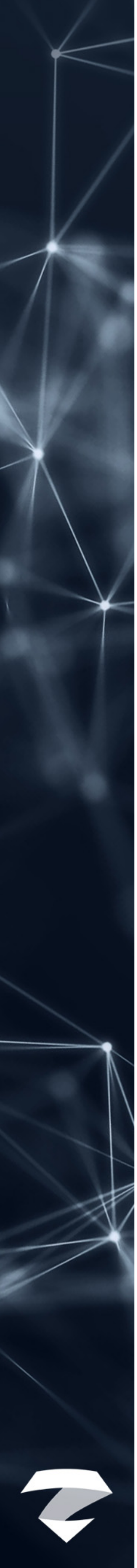
zDEFEND: Preventing on-device exploitation

Mobile apps are highly targeted for on-device exploitation as they process vast amounts of sensitive data and run compromised devices outside the developer's control. To make matters worse, the targeted app binaries and the tools necessary to reverse engineer them freely available, allowing attackers to targeted techniques. Attackers have repeatedly shown the ability to exploit mobile apps on the device via vulnerabilities, fake Wi-Fi networks, phishing, and malicious apps. Poor cyber hygiene and an ever-increasing attack sophistication put data and overall brand value at risk.

Traditional application security solutions focus on an inside-out approach to harden and provide runtime check of root/jailbreak devices. These approaches are generally signature-based and do not keep up with the fast-moving threat landscape on mobile.

Zimperium offers an outside-in approach to address these challenges with behavioral/machine learning techniques as part of the DevSecOps process to embed security, monitor, and close the feedback loop.

Zimperium's zDefend helps enterprises gain runtime threat visibility and enables mobile apps to defend themselves against mobile attacks during runtime. zDefend leverages z9™, Zimperium's patented machine-learning-based Mobile Threat Defense engine. The solution is easily embedded into any iOS or Android application as a software development kit (SDK).



Benefits

- **Comprehensive On Device Protection**: On-device, machine learning-based mobile security for device, network, phishing, and malicious app attacks
- **Threat Visibility:** Provide real-time device threat telemetry across install base for Security, Risk, and Compliance teams
- **Dynamic Threat Response**: On device response can be updated dynamically without needing a new app version
- **Security Ecosystem Integrations**: Dashboard integrates with SIEM/SOAR and other Incident Response systems
- **Easy To Implement:** Quickly and invisibly embeds as an SDK inside apps resulting in 100% security adoption
- **Negligible Overhead**: Has negligible overhead and minimal permission requirements
- **Flexible Deployment Models**: Solution can be deployed as a SaaS and On-Premises
- **Native and Hybrid App Support**: Supports apps built using via Native and Hybrids frameworks

Data leakage, in particular, exposes organizations to the following risks:

- Brand image deterioration
- Customer trust erosion
- User experience damage
- Unauthorized access and fraud
- Confidential data theft
- Revenue loss from piracy
- Intellectual property theft

> *"Zimperium's on-device mobile threat protection technology is well-suited to providing In-App Protection from both known and, hugely importantly, unknown threats."*
>
> Chris Marsh
> Research Director for Enterprise Mobility at 451 Research

Example of actions your app can take with zDEFEND embedded

Threat / Attack Detected	Potential Action
A man-in-the-middle (MITM) attack occurs	The app can automatically establish a VPN to create a secure tunnel
A device has malware like BankBot installed	The app can trigger immediate steps to freeze access until the user deletes the BankBot-carrying app and resets their password online
A device has been Jailbroken by the user	The app can end the session or flag certain transactions to additional verification
A device has been compromised by an external actor	The app can display a dialog box asking the user to complete their transaction from a different device
A money transfer attempt was made on an unsafe WiFi network	Ask user to connect to safer network, reducing transfer limits or request additional verification
A 2FA token is sent to a compromised device	Request additional authorization on a different device

See zDEFEND in action today

zDefend enables developers to spend more time developing and less time worrying about security. zDefend quickly and dramatically improves the security of any mobile app and the helps enterprises better understand their risk posture. With security safely embedded in mobile apps, organizations can focus on innovations that will delight customers, increase customer loyalty and unleash the full potential of the mobile era.

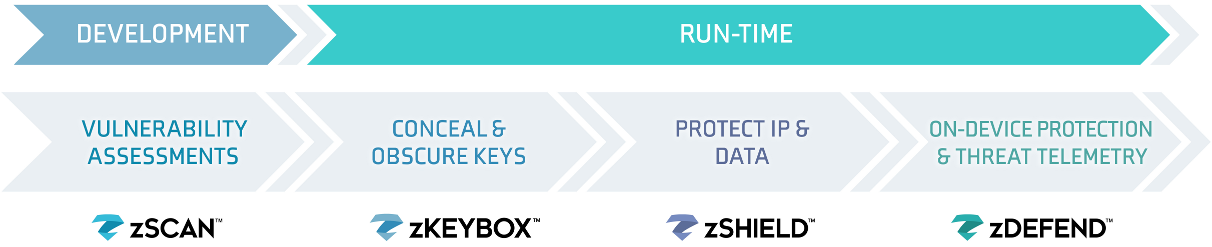
If your business could benefit from immediate, effortless and robust mobile app security, Zimperium's zDefend's in-app protection is right for you.

Contact us to see a demo and learn more.

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

ZIMPERIUM®