Zimperium Runtime Protection

zDEFEND™

ZIMPERIUM®

Comprehensive Runtime Visibility & Protection

ZDefend is part of Zimperium's MAPS platform, providing in-app runtime protection that enables mobile apps to detect and defend against threats directly on end-user devices. It includes an embedded SDK and a centralized console (zConsole) that work together to detect, alert, and respond in real time.

The SDK utilizes AI-driven behavioral and deterministic techniques to identify risks, threats, and attacks. When a threat is detected, it informs the app and sends detailed forensic information to zConsole. Threat policies reside within the app itself, enabling immediate on-device responses—such as blocking actions or logging out users—without waiting for server-side response.

Security Operations(SOC) teams can monitor threats in real-time through zConsole's dashboard, while app teams can model threats and refine defenses using real-world threat data. Threat policies can be updated instantly **without republishing ~~the app,~~** ~~ensuring fast and scalable protection~~ across large user bases. **With zDefend, mobile apps stay resilient against untrusted environments and emerging zero-day threats.**

Key Benefits

Anti-Fraud Protection	Stops overlay attacks, session hijacking, and other UI manipulation techniques used in fraud.
Anti-Malware Protection	Identifies and blocks malicious apps from stealing credentials, data, and hijacking OTPs.
Bot Protection	Detects and blocks emulators, automation tools, and device farms attempting to abuse the app.
Device Attestation	Verifies device trustworthiness by assessing OS integrity, rooting/jailbreak status, and environment risks.
App Attestation	Ensures that only authentic messages from legitimate protected applications reach the servers.
Threat Telemetry & Alerts	Provides real-time threat intelligence to enable SOC teams to respond faster.

Why zDefend Stands Apart from Other Runtime Solutions

1 **AI-Driven Protection**
On-device, AI-based mobile security for device, network, phishing, and malware threats.

2 **On-device Threat Mitigation**
The app's ability to respond instantly to threats on the device ensures immediate protection, significantly reducing the risk and impact of potential cyberattacks.

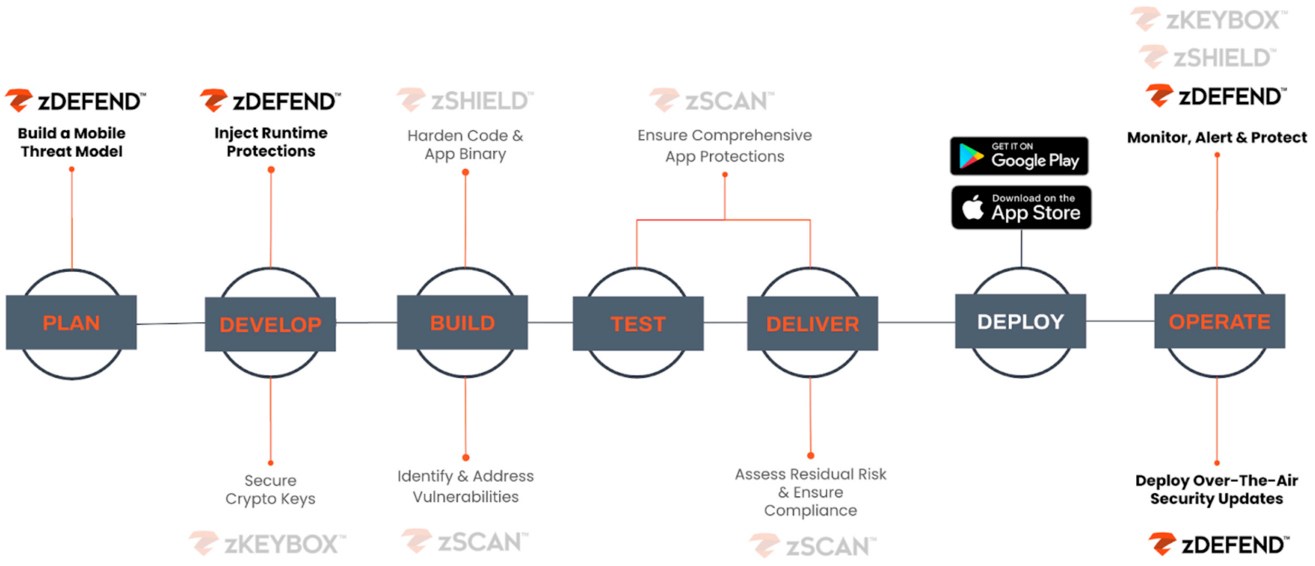
3 **Tamper-Proof API Communication**
Ensure API calls originate from legitimate, protected apps and remain unaltered before reaching the server.

4 **Over-the-Air Updates**
New detections and response actions can be updated in real-time via the centralized console without requiring a new version to be published.

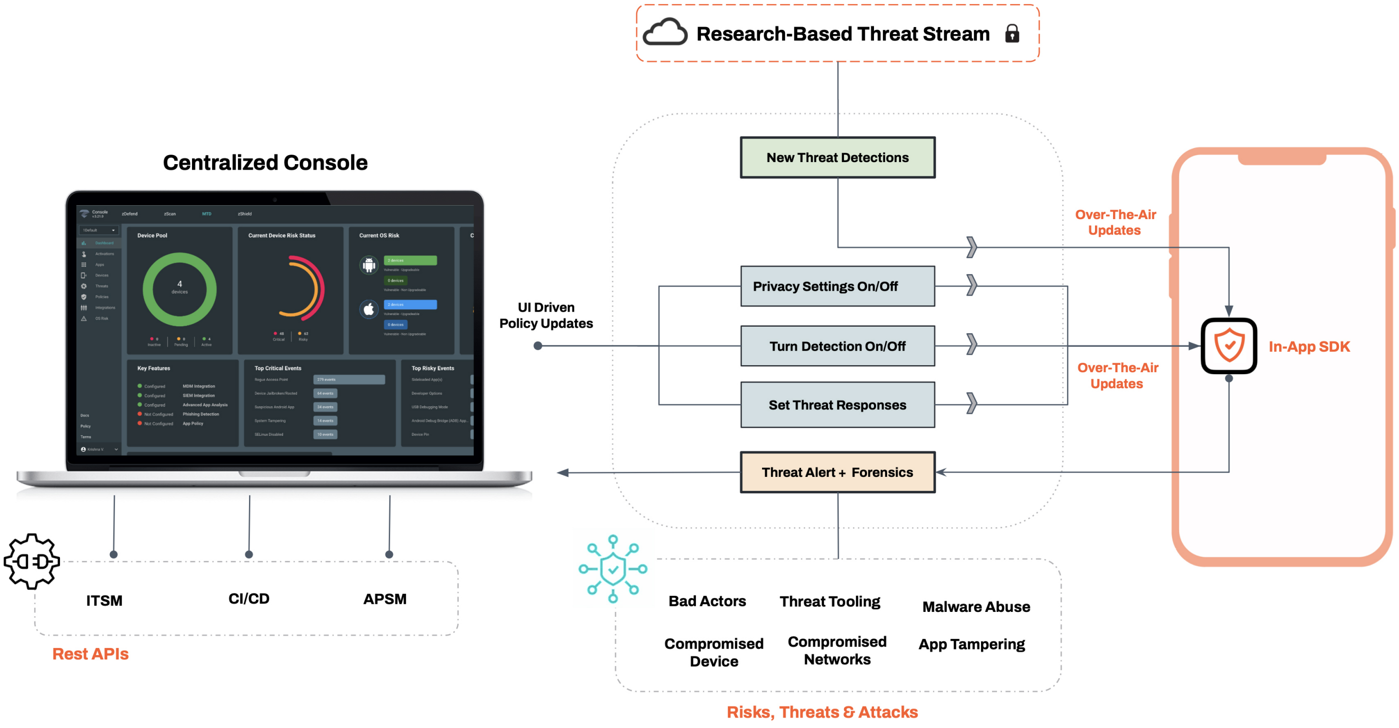
5 **Modular and Lightweight SDK**
Designed for flexibility, the SDK's modular architecture allows you to integrate only the components you need, keeping the footprint minimal and preserving app performance.

6 **Compatibility**
Support for native and hybrid mobile applications, enhancing security across various platforms.

Integrates Runtime Protection Seamlessly into your SDLC


zDEFEND
Build a Mobile Threat Model
zDEFEND
Inject Runtime Protections
zSHIELD
Harden Code & App Binary
zSCAN
Ensure Comprehensive App Protections
GET IT ON Google Play
Download on the App Store
zKEYBOX
zSHIELD
zDEFEND
Monitor, Alert & Protect
PLAN
DEVELOP
BUILD
TEST
DELIVER
DEPLOY
OPERATE
Secure Crypto Keys
zKEYBOX
Identify & Address Vulnerabilities
zSCAN
Assess Residual Risk & Ensure Compliance
zSCAN
Deploy Over-The-Air Security Updates
zDEFEND

Operational Architecture Diagram



> “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 Mars
> Research Director for Enterprise Mobility at 451 Research

Protect Your App From Malware and Phishing

If you are interested in more advanced security for your mobile app, please contact us.

Customers Case Study

Anti-Malware to Prevent Account Takeover Fraud

One of the world's largest global banks was concerned about mobile fraud. The bank operates in over 50 countries and maintains over 50 internal and external mobile applications. Their primary focus was their consumer-facing app that ran on more than 40 million consumer mobile devices. Existing traditional fraud platforms provided little threat visibility and protection from attempts to compromise the mobile app on end user devices. They wanted run-time malware protection to prevent credential theft and fraud. Within the first six months of embedding zDefend in their digital banking apps, they realized their apps were running on 18,000 devices with malware, 120,000 compromised machines, and 2 million risky devices. They are leveraging zDefend's on-device actions to prevent users from accessing and conducting high-risk transactions on untrusted devices to proactively prevent fraud.

Logins from a new device and trusted account were accountable for over 75% of fraud value for online banking logins at Q2 2022 which indicates that account takeover is still the most common fraud attack at login.

Source: Outsider First Half of 2022 Outseer Fraud & Payments Report

Prevent Mobile Banking Fraud With Compliance Grade Security

A large national bank in Europe was concerned that the security posture of their current mobile applications was insufficient. They were concerned that transactions originating within the mobile apps were at risk and the current protections in place would be insufficient to meet upcoming banking regulations. The enterprise embedded zDefend into their seven Android and iOS applications that serve over 5 million customers. The primary focus was to prevent on-device exploitation from malware (Ex:Bankbot). Once complete, they fed the threat telemetry to their Fraud Engine to enable better decision making downstream.

70%

of fraudulent online banking originated within the mobile channel.

Source:Outsider First Half of 2022 Outseer Fraud & Payments Report

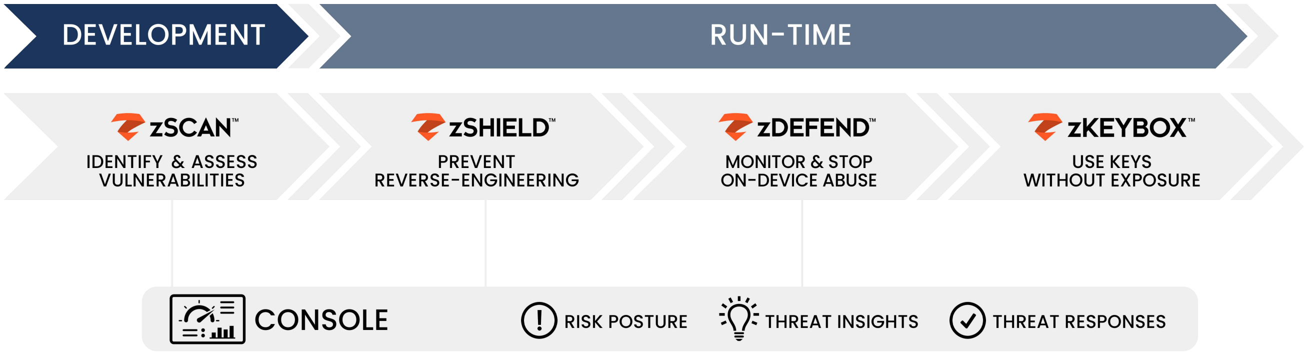
Protect your application today on every mobile device

If you are interested in building self-defending mobile apps that proactively prevent fraud and theft, 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.


DEVELOPMENT
RUN-TIME
zSCAN™
IDENTIFY & ASSESS VULNERABILITIES
zSHIELD™
PREVENT REVERSE-ENGINEERING
zDEFEND™
MONITOR & STOP ON-DEVICE ABUSE
zKEYBOX™
USE KEYS WITHOUT EXPOSURE
CONSOLE
RISK POSTURE
THREAT INSIGHTS
THREAT RESPONSES

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