Zimperium zDefend

Runtime Application Self Protection (RASP) for Mobile Applications

ZIMPERIUM®

Comprehensive Runtime Visibility & Protection

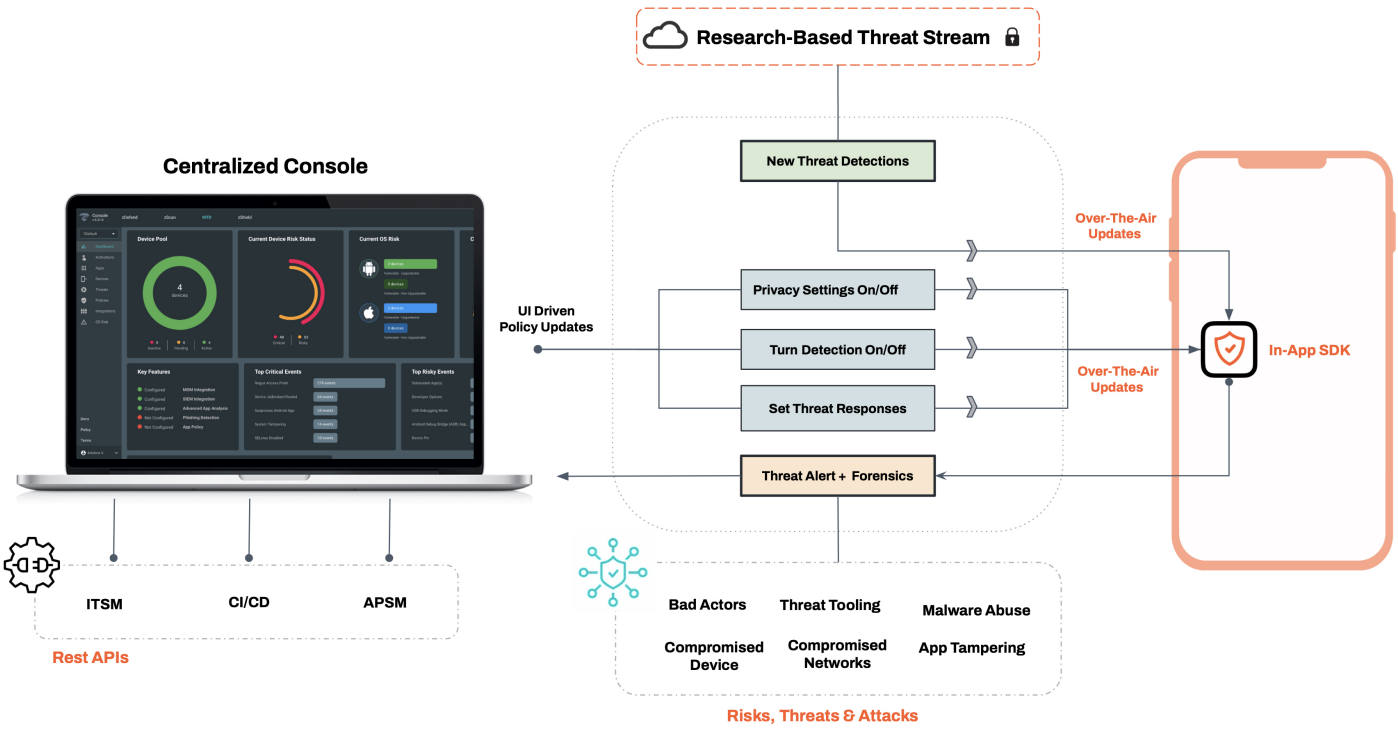
Zimperium zDefend is a runtime protection solution that enables mobile applications to detect and proactively protect themselves on end-user devices. zDefend includes both an **in-app SDK** and a **centralized console** called zConsole. The SDK automatically connects to the zConsole when embedded in the host application.

The in-app SDK detects and protects apps from dynamic threats such as runtime attacks, data interception, and exploitation of user interactions using machine learning, behavioral, and deterministic methods. ZConsole displays threats from zdefend protected application instances and manages threat responses through a policy. Once set in a policy, a threat response triggers an on-device action.

When at threat is detected, the SDK informs the host app and sends an alert with in-depth, actionable forensics to zConsole. As a result, the host app can take action in real-time to prevent the threat from progressing. Using the threat dashboard on the zConsole, security teams can monitor threats and take action when necessary. Additionally, mobile app development and security teams can model threats and enhance protection measures based on this data.

App teams can select from preconfigured threat responses or customize callbacks. These threat policies can be updated in real-time without needing to publish a new app version, making it practical and scalable for large install bases.

With zDefend, mobile apps are protected from untrusted devices and zero-day threats, which are continuously evolving.



Here are some key detection capabilities that the solution has to prevent on-device abuse a:

Assess Device Risk Posture	Detect Risk, Threats & Attacks
Emulators	Phishing
Hooking Frameworks	Malware
Compromised Devices	Tampering
Jailbroken/Rooted Devices	Screen Overlay
Rooting Detection Evasion	Screen Sharing
Insecure Device Settings	Privilege Escalation
Actively Exploited Android	Accessibility
Versions Actively Exploited iOS	Permissions Network
Versions	Traffic Interception

Key Benefits

- **Real-time Threat Awareness** - Continuous runtime threat visibility and monitoring via a centralized console allows teams to make informed security decisions in real-time.
- **Mitigate Fraud** - Safeguard against mobile malware from hijacking accounts to prevent unapproved financial transactions.
- **Mitigate Account Takeover Risks** - Prevent phishing attacks on end-user devices to steal account credentials, session cookies, and one-time passwords from the app.
- **Malware Protection** - Prevent malware from stealing sensitive PII, PHI, and payment data when it's being processed and viewed within the app.
- **Keep Security Current** - Visibility into real-world threats impacting apps allows app teams to stay updated with the latest security trends and emerging threats, ensuring the app remains secure over time.

zDEFEND™

Why Zimperium's zDefend

- **Patented Machine-Learning** - On-device, machine learning-based mobile security for device, network, phishing, and malware threats. On-device Threat Mitigation - The ability of the app to respond instantly to threats on the device ensures immediate protection, significantly reducing the risk and impact of potential cyber-attacks.
- **Over-The-Air-Updates** - New detections and response actions can be updated in real-time via the centralized console without publishing a new version.
- **Small and Performant SDK** - With a minimal footprint of just 2MB, the SDK ensures streamlined integration without compromising the app's performance.
- **Flexible Deployment Models** - The solution can be deployed as a SaaS and On-Premises
- **Compatibility** - Support for native and hybrid mobile applications, enhancing security across various platforms.

> “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

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

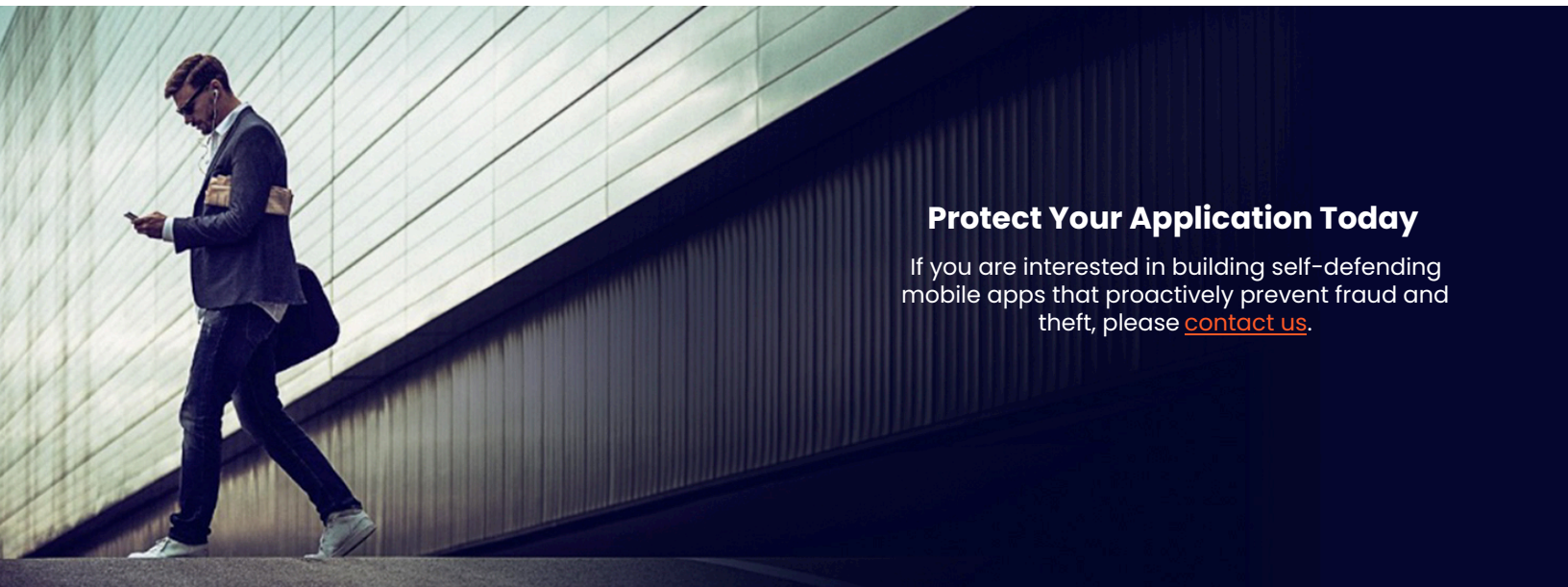
Prevent Mobile Banking Fraud With Compliance Grade Security

A large national bank in Europe was concerned that their current mobile applications security posture was insufficient. They were concerned that transactions originating within the mobile apps were at risk and the current protections in place would be sufficient to meeting upcoming banking regulations. The enterprise began by embedding 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



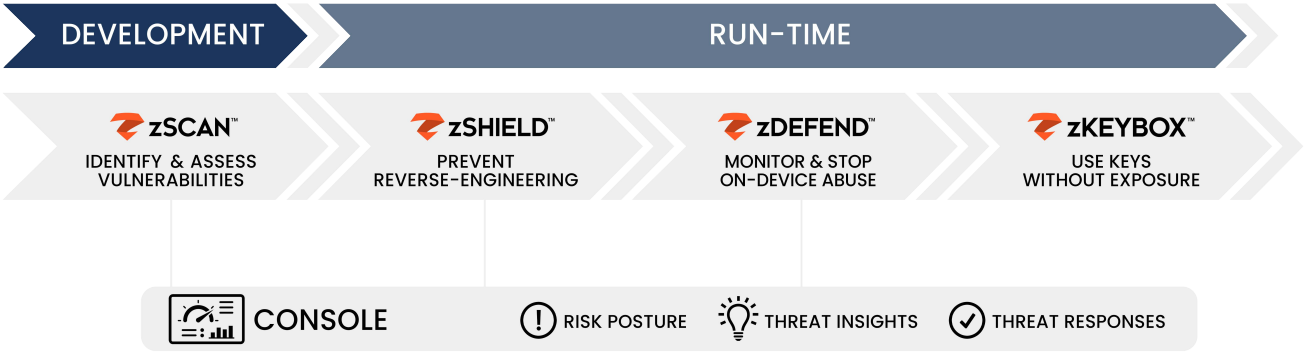
Protect Your Application Today

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.



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.