

Global Bank Adopts AI-Empowered Malware Defense to Cut Mobile Fraud and Ensure Compliance

Quick Answer

A Tier 1 global bank replaced its legacy, signature-based mobile app security tool with Zimperium's AI-Empowered Mobile App Security Platform, MAPS — spanning App Security Testing, App Hardening, Runtime Protection, Key Protection, and Real-time Threat Visibility. The switch gave the bank AI-driven, real-time threat visibility, zero-day malware detection, and the ability to push new security controls over the air without an app release. The result: lower fraud exposure, faster compliance response, and a mobile app defense built to keep pace with new threats instead of reacting to them.



The Challenge:

Staying Ahead of a Fast-Moving AI-Driven Threat Landscape

A Tier 1 global financial institution serving millions of mobile banking customers across multiple international markets faced a growing regulatory mandate tied directly to mobile malware-driven fraud. Their security stack checked devices for known risk factors and flagged malware by matching it against a database of previously identified threats — a widely used approach, but one that depends on constant updates to keep pace with threats that haven't been seen before. As attackers increasingly use AI to generate new malware variants and improve fraud tactics faster than any signature list could track, the bank recognized an opportunity to get ahead of the curve rather than stay in a reactive posture. They set out to find a solution that wouldn't just close the gap, but leapfrog it entirely.

What the bank wanted to add

- **Real-time telemetry and visibility**
Live data on device and app risk, so the security team could make real-time decisions when it mattered most.
- **Lower Release Overhead**
The ability to update security requirements without tying every change to a new app release.
- **Freedom from Signature Maintenance**
No more continuously updating and maintaining malware signature lists manually just to keep detection current.
- **Resilience against tampering**
Protection that could keep pace with attackers probing the app binary for ways to bypass controls — without a lag between a new technique appearing and a fix going live.

The Solution Selection Process: How the Bank Evaluated Mobile Runtime Protection Vendors

The bank ran a formal evaluation, including an RFI and RFP process, to find a next-generation Mobile Runtime Protection solution. This meant rigorous technical reviews and Proof of Concept deployments of multiple leading Runtime Protection vendors.

The POC tested each vendor against a set of RASP success criteria. The bank's internal pen test team reviewed and validated the results directly. From there, the team ran performance testing. App loading time, app size, and memory usage were all benchmarked against the bank's current baseline and had to stay within an acceptable range.

Following comprehensive testing across a geographically diverse range of devices, operating systems, and simulated attack scenarios, the institution selected Zimperium's AI-Empowered Mobile App Security Platform (MAPS) as its in-app Advanced Runtime Protection solution.

Why the Bank Selected MAPS

The decision was based on operational impact and proven performance.

1. Real-Time Visibility

MAPS delivered live runtime threat intelligence through a centralized console, giving fraud and security teams the data to respond to the threat.

2. Broader Malware Coverage, Including Zero Day

Zimperium is part of the Google App Defense Alliance and scans apps before they are approved on Google Play, catching malware before it ever reaches the store. Zimperium also covers devices and regions outside Google's own scanning reach, closing a gap the bank's prior vendor left open. Signature based tools cannot catch what has not been seen before. Zimperium's zero day malware detection gave the bank protection its old approach could never reach.

3. Instant Response Through Over the Air Updates

MAPS pushed new malware controls and policy updates the moment a threat emerged, without waiting on an app release. This kept the bank ahead of a threat landscape that never stops changing, and lowered AppDev operational cost by cutting the need for frequent releases.

4. Accurate Runtime Protection

MAPS delivered broad coverage, strong configurability, and low false positives across real world attack scenarios, validated in testing.

5. Proven Scale and Reliability

MAPS held consistent performance across a wide range of devices and operating system versions, validated through the proof of concept.

6. Strategic Partnership

Zimperium showed up as the most responsive and technically capable partner, earning a request for long term collaboration on mobile fraud prevention.

Industry Recognition

Zimperium is recognized as a Leader in the 2025 Forrester Wave™ for Mobile Threat Defense Solutions, a Leader in the QKS 2026 SPARK Matrix™ for In-App Protection, and named Visionary Leader and Strongest Performer in the Frost & Sullivan 2026 Frost Radar™ for Mobile Threat Defense.

Learn More

See how Zimperium's AI-Empowered Mobile App Security Platform can help your organization build secure, compliant, and fraud-resistant mobile apps.

www.zimperium.com

About Zimperium

Zimperium is the world leader in AI-empowered mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging the power of AI to deliver autonomous security that counters evolving threats including phishing, malware, and zero-day attacks.



Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244

© 2026 Zimperium, Inc. All rights reserved.