



# Mobile Protect

In-app runtime protection, dynamic obfuscation, and on-device anti-fraud for iOS and Android.

## 01 OVERVIEW

Mobile Protect is Data Theorem's in-app runtime protection layer for deployed mobile apps. It pairs dynamic obfuscation, anti-tampering, jailbreak and root detection, and runtime telemetry with on-device fraud scoring to prevent account takeover, payment fraud, and reverse engineering. A single SDK for iOS and Android, integrated with Mobile Secure findings to close the loop between pre-production testing and production defense.

### Runtime defense and on-device anti-fraud for mobile apps.

Dynamic obfuscation, anti-tampering, jailbreak and root detection, and runtime telemetry combined with on-device fraud scoring across bot, emulator, device, and behavior signals.

## 02 CAPABILITIES

### Platform capabilities



#### Dynamic obfuscation

Mutates code, strings, and control flow at runtime. Defeats static obfuscation tooling and open-source de-obfuscators.



#### Anti-tampering and anti-debugging

Detects code modification, repackaged binaries, and attached debuggers. Protects proprietary algorithms and trade secrets.



#### Jailbreak and root detection

Surfaces jailbroken iOS, rooted Android, emulators, and tampered runtimes before they reach your backend or transaction APIs.



#### On-device anti-fraud

Scores transactions, sessions, and devices for bot, emulator, and fraud signals. Catches account takeover, payment fraud, and identity theft.



#### Runtime telemetry

Real-time observability of hostile traffic, suspicious SDK activity, and attacker behavior across deployed iOS and Android fleets.



#### Lightweight SDK

500 KB SDK with no startup tax on Android, no compile tax on iOS, and roughly 10 KiB per second of telemetry per session.

**SUPPORTS APPS  
BUILT ON**

iOS · Android | React Native · Flutter · Xamarin · Cordova · Unity

**THREATS BLOCKED**

Account Takeover · Payment Fraud · Reverse Engineering · App Tampering · Bot &amp; Emulator · Jailbroken &amp; Rooted Devices · Fraud Farms

**03 OUTCOMES****Key benefits****Stop fraud before financial loss**

On-device fraud scoring catches account takeover, payment fraud, and identity theft before transactions complete or losses post.

**Defend on untrusted devices**

Detect jailbroken, rooted, and emulated devices, GPS and time spoofing, and fraud farm clusters before they touch your backend.

**Defeat reverse-engineering toolkits**

Dynamic obfuscation mutates code at runtime, blocking the open-source de-obfuscators that defeat static-only protections.

**Ship without performance tax**

The 500 KB SDK adds no measurable startup time on Android and no compile time on iOS, even at production scale.

**04 PERFORMANCE****Engineered to disappear****FOOTPRINT****500 KB**

SDK on Android. 500 KB to 1 MB on iOS. No measurable disk overhead at runtime.

**STARTUP****0 ms**

On Android. 100 ms on iOS, only on apps over 200 MB. No compile-time impact on iOS.

**TELEMETRY****~10 KiB/s**

Steady-state network. Each event is roughly 400 bytes. Buffered to disk if connectivity drops.

**05 AI DEFENSE****Built for AI-augmented threats****AI 01****Attack path mapping**

Detects AI-orchestrated attack chains inside the deployed app, then routes each step back to your security team in real time.

**AI 02****Memory scraping defense**

Blocks LLM-targeted memory scraping and credential theft against the live app process. Surfaces exfiltration attempts as they happen.

**AI 03****Overlay and bot defense**

Detects AI-orchestrated overlay malware, scraping bots, password spraying, and login automation against deployed iOS and Android apps.

**PAIRS WITH**

**Mobile Secure** · Continuous mobile application security testing. SAST, DAST, behavioral analysis, and SDK risk on every release for iOS and Android.

**ABOUT DATA THEOREM**

Data Theorem delivers continuous, automated AppSec across mobile, API, code, and cloud, with AI/LLM woven through. Hacker-style discovery and dynamic runtime analysis route fixes to the teams that own them. We secure 2.8 billion users and 7 of the top 10 banks.

Copyright © 2026 Data Theorem, Inc. All rights reserved.

**GET STARTED**

[www.datatheorem.com](http://www.datatheorem.com)  
[info@datatheorem.com](mailto:info@datatheorem.com)

[Schedule a Demo →](#)