PRODUCT OVERVIEW

datatheorem

Mobile Protect for Gaming

Protect IAP and IAA revenue, detect fake users, prevent fraud and secure UA spend

Stop Revenue Leaks Before They Impact Your Bottom Line

Every bypassed IAP, every fake install, and every modded APK costs real money. Mobile Protect delivers enterprise-grade runtime protection purpose-built for mobile gaming revenue streams.

What Is Mobile Protect?

Mobile Protect is a lightweight SDK that delivers continuous runtime protection for mobile games. It combines anti-tampering, anti-cheat, and anti-fraud telemetry with industry-first dynamic obfuscation to stop paywall bypass, block modded APKs, and protect acquisition spend from fake users and bots.

Unlike traditional security tools, Mobile Protect requires no changes to game logic, integrates in hours, and starts blocking revenue-impacting threats immediately.

The Revenue Problem

IAP and IAA Bypass

Cracked APKs, Lucky Patcher, and modded builds let users access premium content without paying. A 1–2% hit on IAP revenue = $100K+ monthly loss for scaled titles.

UA Fraud and Fake Installs

Device farms, GPS spoofers, and bot networks poison attribution data, inflate CPIs, and destroy ROAS calculations—wasting millions in ad spend.

Games lose real money when attackers bypass in-app purchases, abuse ad inventory, or use device farms to inflate metrics. Even a 1 to 2 percent hit on IAPs or ad quality can translate to six figures in lost revenue every month for scaled titles.

Threats That Directly Erode Revenue

- Paywall bypass and patched binaries
- Modded apps and cracked APKs
- Cheat engines and instrumentation tools
- Fraud farms, fake installs, and bots
- GPS spoofing and location manipulation
- Emulator-based fraud networks
- Memory editors and speed hacks



PRODUCT OVERVIEW

Core Capabilities

Three-layered protection designed for revenue defense

Active Anti-Tampering and Anti-Cheat

Continuous runtime monitoring detects and blocks the most common exploit tools and modified binaries that enable paywall bypass and cheating.

DETECTION CAPABILITIES

- GameGuardian, Lucky Patcher, XModGames
- Cracked and repackaged APKs
- Jailbreak and root detection
- Memory editing tools
- Debugger and instrumentation detection

PROTECTION MECHANISMS

- Runtime integrity validation
- Binary signature verification
- Code injection prevention
- Prevents exploits before spread
- Real-time threat response

Anti-Fraud for UA and Ad Quality

Real-time device-level fraud scoring protects user acquisition budgets and ensures clean attribution data for accurate LTV and ROAS calculations.

FRAUD DETECTION

- Device farm identification
- Fake install detection
- GPS spoofing and location fraud
- Bot and fake user gesture detection
- Emulator and simulator detection

BUSINESS IMPACT

- Protects ROAS and LTV projections
- Improves campaign optimization
- Reduces wasted ad spend
- Clean data for attribution partners
- Real-time fraud scoring API

INDUSTRY FIRST

Dynamic Obfuscation

Unlike static obfuscation that can be reverse-engineered once and shared, Mobile Protect's dynamic obfuscation re-scrambles runtime code every session, making it impossible to create reusable cheats or patches.

HOW IT WORKS

- Runtime code re-scrambling every session
- Polymorphic protection layers
- Unique binary fingerprint per install
- Continuous code transformation

THREAT MITIGATION

- Defeats break-once-run-everywhere attacks
- Prevents cheat sharing and distribution
- Stops automated patching tools
- Makes reverse engineering impractical

PRODUCT OVERVIEW

Built for Performance and Scale

Enterprise-grade protection with minimal overhead

~500KB
SDK size on iOS and Android

<1%
CPU overhead during gameplay

Minimal
Battery and network impact

Performance Characteristics

- Low friction integration with minimal overhead
- No required changes to game logic
- Designed for high-MAU titles (10M+ MAU)
- Asynchronous threat detection
- Minimal network traffic for telemetry
- Optimized for mobile battery life
- Zero impact on frame rates
- Production-tested at scale

Quick Integration

Step 1: Add SDK

Add Mobile Protect via your preferred package manager.

```
pod 'DataTheoremMobileProtect'
```

Step 2: Initialize

Initialize with your API key in your app launch sequence. Protection starts immediately.

```
MobileProtect.initialize(apiKey)
```

Total integration time: 2–4 hours · Production deployment in days, not weeks

Platform Support

iOS Native
CocoaPods, SPM

Android
Maven

Unity
All versions

React Native
0.60+

Flutter
2.0+

PRODUCT OVERVIEW

Revenue Impact and ROI

Measurable protection, predictable pricing

How Mobile Protect Protects Revenue

Prevent IAP Bypass

Runtime checks validate purchase flows and block tampered binaries, fake receipts, and instrumentation tools. Every blocked bypass is a recovered transaction—typically hundreds to thousands per month for mid-scale titles.

Stop Ad Fraud and Protect UA Spend

Block device farms and spoofers that inflate installs and poison bidding signals. Anti-fraud telemetry feeds into attribution and UA optimization, preventing wasted spend and improving targeting accuracy.

Recover Lost Value and Improve Retention

Fraud and cheating rates are typically 1 to 2 percent, often higher in hyper-casual and fast-scaling games. Even partial blocking recovers meaningful revenue, improves retention, and preserves fair player economies.

Pricing Snapshot

$350

Per app to get started

< 15,000 MAUs

price per MAU after 15,000 MAUs

2 week free trial available to measure impact

Volume discounts for multi-app publishers

All features included

Interested in Seeing the Platform in Action?

Schedule a demo to see how Mobile Protect blocks cheats, detects fraud, and protects IAP and IAA revenue in real time.

https://www.datatheorem.com/demo

datatheorem.com/solutions/mobile-gaming

Learn More