SOLUTION BRIEF

datatheorem

Catching mobile fraud on the device in real time

How Mobile Protect detects and flags fraud at runtime

Account takeover, payment fraud, and fraud farms exploit rooted devices, emulators, and GPS spoofing faster than backend rules can correlate.

Mobile fraud has moved to the device layer

Fraud farms run thousands of spoofed devices in parallel. Server-side rules cannot see what the app sees. Detection has to happen inside the running app, on the actual hardware.

Why traditional approaches fall short

By the time signals reach the backend, the session has authenticated and the transaction has submitted. Detection has to live where the attack runs.

WHAT SERVER-SIDE RULES SEE

- API call metadata
- User token and session state
- IP address (often rotated or spoofed)
- Coarse device fingerprint

WHAT MOBILE PROTECT SEES

- Root, jailbreak, hooking frameworks
- Real vs. spoofed GPS and clock
- Emulators, hardware integrity, IMEI
- User input cadence and bot patterns

Continuous fraud defense inside the running app

Mobile Protect runs inside every iOS and Android app, scoring correlated signals in real time and flagging risky sessions to your fraud team as they happen.

FRAUD INDICATORS DETECTED AT RUNTIME

Root / Jailbreak | Hooking frameworks | GPS spoofing | Hardware spoofing | Emulator detection | App integrity | IMEI validation | SIM / phone change | IP integrity | Fraud farm clustering | Bot detection | Input cadence

SOLUTION BRIEF

datatheorem

How we solve it

Four capability groups feeding one scoring engine, inside the app.

Device integrity signals

Catches rooted and jailbroken devices, hardware spoofing, GPS manipulation, OS discrepancies, IMEI rewrites, and emulator use on every session.

Identity and account defense

Catches account takeover via SIM and phone number changes, application integrity violations, and stolen device validations against IMEI registries.

Fraud farm and network detection

Identifies device clustering across fraud farms, IP and network inconsistencies, and install patterns that signal coordinated abuse.

Behavioral and bot detection

Surfaces emulator activity, bot-driven input, suspicious SDK behavior, and input cadence that distinguishes humans from automation.

What it looks like in production

CONFIGURABLE SCORING

Tune fraud weights per indicator

AVG 2.0

Bot Detection	0	0.5	1	1.5	**2**
GPS Spoofers	0	0.5	1	**1.5**	2
Device Clustering	0	0.5	**1**	1.5	2
App Cloners	0	0.5	1	1.5	**2**

ANTI-FRAUD CONSOLE

Fleet-wide signal visibility

467	10	457
TOTAL DEVICES	FRAUDULENT	FRAUD SIGNALS

210 Application Integrity · **117** Rooted · **50** Bot Detection · **30** Emulator · **20** Hardware Spoofers · **3** GPS Spoofers

datatheorem

Data Theorem provides full-stack application security across mobile, API, code, and cloud. Mobile Protect delivers in-app runtime protection on every iOS and Android release: anti-fraud, RASP, jailbreak and root detection, and anti-tampering, shipped as one runtime layer with a single SDK and one telemetry feed.

Schedule a Demo →

www.datatheorem.com
info@datatheorem.com

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