SHIELD

SHIELD for iGaming Platforms

SHIELD's Device-First Fraud Intelligence platform consists of device identification and intelligence. We identify the root of fraud with the **SHIELD Device ID** and actionable **Fraud Intelligence**, helping iGaming platforms stop fraud, build trust, and drive growth.

Trusted by

MPL · Pipa · Bingo Plus · Lottogo.com · Leon · Big Cash · PokerBaazi · A23 · inbet · neo group · Goal123 · digiplus · Arena Plus · Game Zone · Casino Plus · Comtrade Gaming · ... and more

"Partnering with SHIELD marks an important milestone in Pipa Studios' mission to create a fun and secure experience for our players. By leveraging SHIELD's Device-First Fraud Intelligence platform, we can safeguard our players from fraud and uphold the integrity of our games. This collaboration empowers us to deliver a fairer, more enjoyable experience for our community."

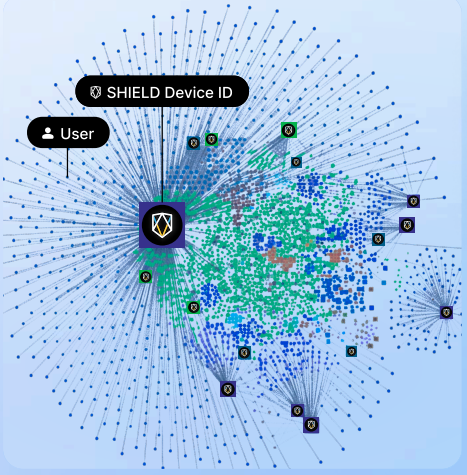
Pedro Moraes
CEO, Pipa Studios Brazil

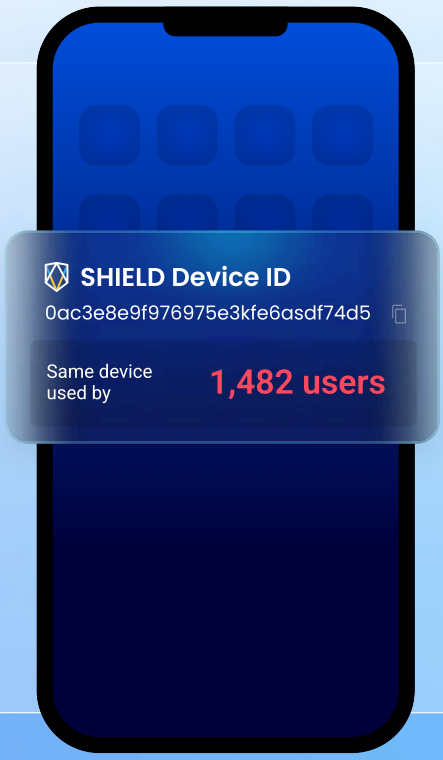
Our Solution

Plug-and-Play · No Additional Codes · No PII Required

SHIELD Device ID

persistently identifies the root of fraud & fake accounts >99.9% accuracy





SHIELD Fraud Intelligence

real-time actionable insights into fraudulent activity

20+ Configurable Risk Signals

- App Cloner — Low / High
- Auto-Clicker — Low / High
- GPS Spoofer — Low / High
- Emulator — Low / High
- Device Masking — Low / High

... and more

Expose Every Fraud Risk in the Player Journey

From signup to payout, SHIELD delivers comprehensive fraud protection across the entire player journey. Our device-first intelligence exposes every hidden threat, ensuring only trusted users and genuine devices interact with your platform.

Use Cases

Wallet Activity (Deposits & Withdrawals)

Payment Fraud
Chargebacks
...

Gameplay & Tournaments

Bot Traffic
Automated Abuse
GPS Spoofing
...

Login

Account Takeovers
GPS Spoofing
Fake Accounts
...

Authentication

E-KYC Bypass
Deepfakes
Hooking
...

Account Creation

Multi-Accounting
Collusion
Bot Traffic
Promo Abuse
...

App Launch

Device Intelligence Activates

Fraud Intelligence

`emulator_running` `auto_clicker_running`
`is_bot` `gps_spoofer_running`

Use Cases

Eliminate Deepfakes & E-KYC Bypass

How Does E-KYC Bypass Happen?

Fraudsters bypass identity verification by injecting AI-generated deepfakes with hooking techniques, faking faces, documents, and liveness checks. These attacks are often carried out from the same device, enhanced by app cloners and emulators. At scale, fraudsters automate attacks to mimic thousands of real users.

Curb Deepfakes & AI Fraud

Prevent fraudsters from using AI-generated deepfake videos and images to bypass biometric verification and trick liveliness detection.

Stop Hooking & App Tampering

Detect and block attackers who manipulate and tamper apps to disable app security measures and inject fake identity data.

Prevent Device Spoofing

Stop fraudsters from spoofing multiple device profiles and masking their real device identity with emulators, app cloners, and more.

SHIELD Fraud Intelligence

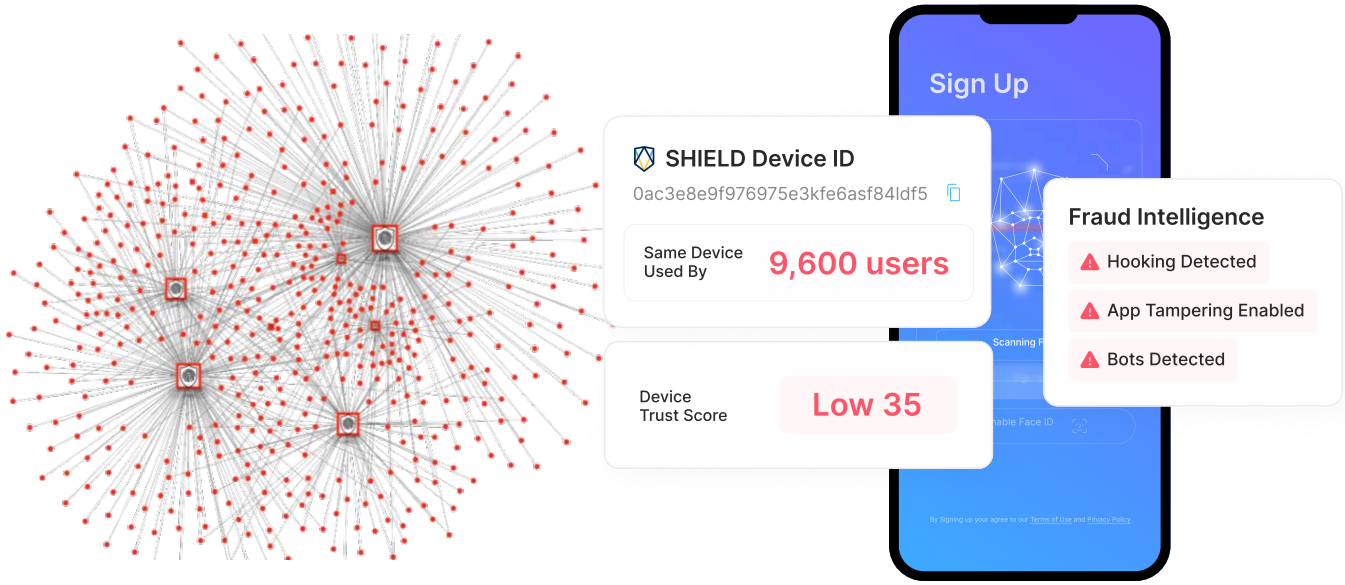
App cloners running
Emulators running
Suspicious factory reset
Hooking
Jailbroken devices
App tampering

How it Works

Fraudsters use app cloners and emulators to spoof device profiles and control multiple accounts at once. They manipulate IDV processes with hooking tools and tampered apps, injecting AI-generated deepfakes to bypass identity verification.

SHIELD's Device ID unmasks spoofed devices and **traces them back to their true origin**, exposing connections between multiple accounts. Beyond that, SHIELD is also able to flag malicious tools and behavior in real-time, protecting industries like **iGaming** from collusion fraud.

By stopping deepfakes and device spoofing, SHIELD helps iGaming platforms maintain trust, security, and compliance. In one case, we exposed a large scale fraud syndicate - **a cluster of 9600 users linked to a single device**.



Use Cases

Prevent Multi-Accounting & Collusion

What is Multi-Accounting & Collusion?

Fraudsters **create multiple fake accounts at scale** with malicious tools, using these accounts to manipulate game outcomes. Multi-accounting is also the gateway to other types of fraud, including **collusion and bonus abuse**.

Block Fake Players

Fake players cause unfairness, draining resources, inflating user numbers, and making it difficult to accurately analyze growth and engagement.

Stop Collusion

Fraudsters use multiple accounts to enter tournaments and creating an unfair advantage against genuine players.

Eliminate Bonus Abuse

Fraudsters create multiple accounts at scale, abusing sign up bonuses for new users, referral codes, and limited time discounts.

SHIELD Fraud Intelligence

App cloners running
Emulators running
VPN running
Suspicious factory reset
Screen-sharing
Jailbroken devices
App tampering

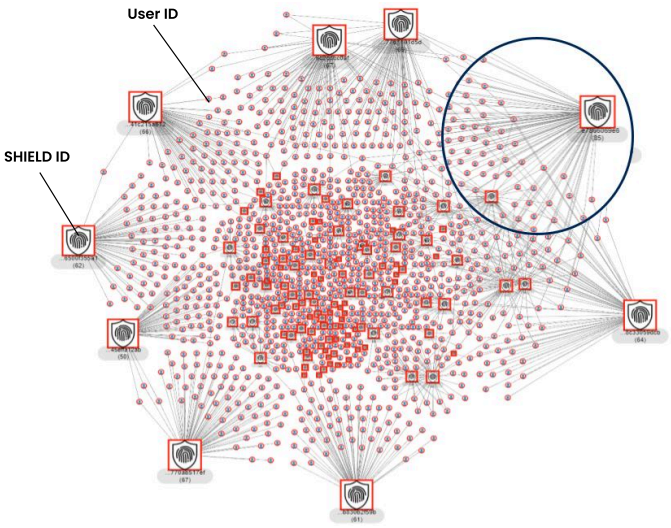
Example Fraud Case

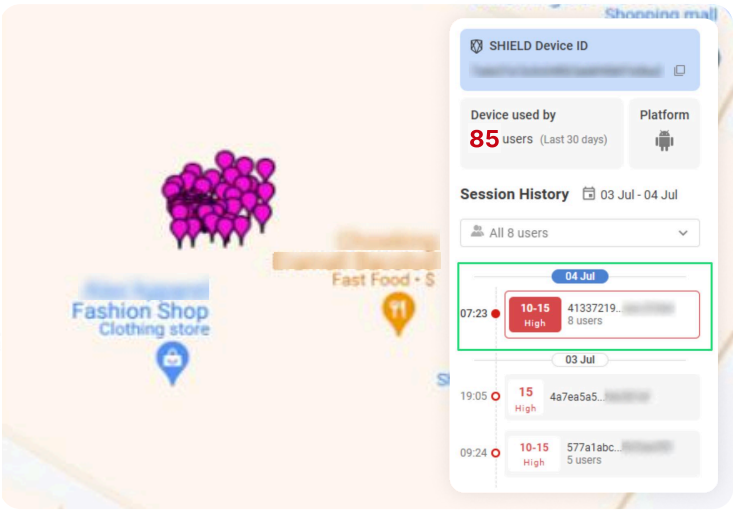
Fraudsters use app cloners and emulators to create multiple accounts. In this case, SHIELD identified a syndicate where the device to player ratio averaged at **1 : 10**.

Zooming in, we see a cluster of **85 users linked to a single device**, within a vicinity of 2.74 metres. Amongst these, **8 users share the same device session**. Screen-sharing is being used to coordinate moves across devices and maximize winnings.

This is typical of fraudsters that enter tournaments with multiple profiles, giving them an advantage for games like poker.

Fraudsters also use VPNs in tandem to bypass restrictions and enter geo-locked tournaments, giving them a further edge over genuine players.





Use Cases

Safeguard Against Payment Fraud & Chargeback

What is Payment Fraud and Chargeback?

Fraudsters attempt to fund accounts or withdraw winnings with stolen card details and identities, which could result in **high chargeback rates and heavy financial losses**.

Minimize Risk & Maintain Card Network Compliance

High chargeback rates can result in higher processing rates and heavy penalties by vendors like Visa & Mastercard.

Reduce Chargebacks & Boost Acceptance Rates

Protect your annual GMV. Instantly detect risky activities, and proactively identify trustworthy transactions.

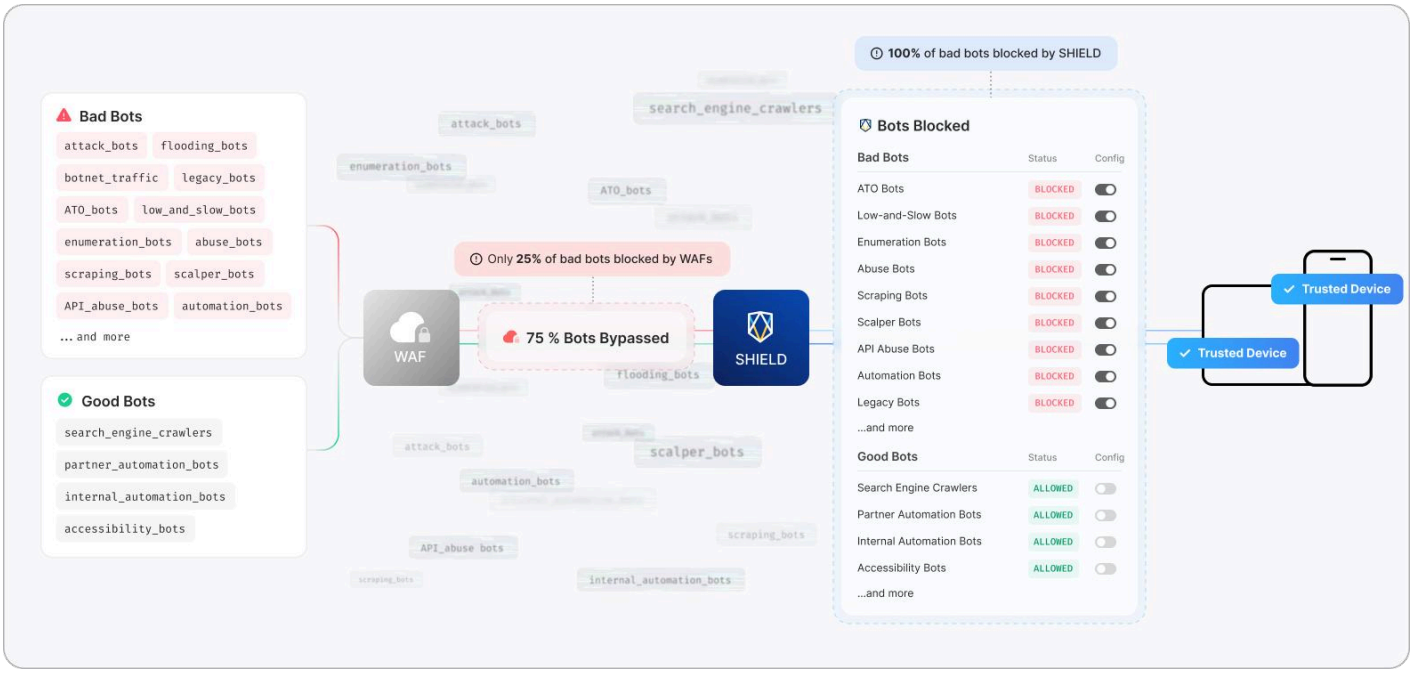
Automate Reviews & Unlock Business Growth

Streamline payment decisions, reduce manual reviews, and investigate complex trends in real time.

Mitigate Bot Traffic

WAFs focus only on **network-level signals** and typically detect just **~25% of bot and DDoS activity**, leaving significant blind spots.

To address these gaps, SHIELD operates at the **application layer**, analyzing the device fingerprint behind each request to accurately distinguish genuine users from automated environments with **99.99% accuracy**.



Use Cases

Detect Location Spoofing
Compliance & Geofencing

What is Location Spoofing?

Fraudsters spoof their locations to enter geo-locked tournaments or access platforms from sanctioned regions, creating unfair play and compliance risk.

SHIELD detects GPS spoofers, VPNs, proxies, and other non-genuine environments, giving operators **high-fidelity location integrity** so only legitimate players can participate.

SHIELD Fraud Intelligence

GPS spoofer running
App tampering
Emulator running
VPN running

Apart from detecting multi-accounting and collusion, SHIELD also identifies when GPS spoofers and VPNs are used, pinpointing players' **trusted location.**

This ensures users aren't playing from restricted locations. In addition, operators can use location data to ensure compliance with local regulations and prevent underage gambling.

Defend Against Account Takeovers (ATOs)

What is Account Takeover?

Fraudsters use stolen credentials, credential stuffing, and brute-force attacks to break into player accounts, leading to payment fraud, bonus exploitation, and data theft.

SHIELD's trusted device intelligence enables platforms to **verify genuine users without unnecessary friction**, and apply additional checks on suspicious users and devices.

SHIELD Fraud Intelligence

App cloners running
Emulator running
Suspicious factory reset
Jailbroken devices
App tampering
Hooking

SHIELD helps stop account takeovers by detecting compromised devices commonly used in credential-stuffing and brute-force attacks.

By identifying emulators, app cloners, rooted or jailbroken devices, and tampered environments, operators gain a trusted view of who is accessing each account, preventing unauthorised logins and protecting player funds and data.