SHIELD

# SHIELD para Plataformas de iGaming

A plataforma de Inteligência de Fraude focada na identificação de dispositivos da SHIELD identifica a raiz da fraude por meio do **SHIELD Device ID** e **Fraud Intelligence**, ajudando plataformas de iGaming platforms a eliminar fraude, fortalecer confiança e impulsionar crescimento.

Quem Confia em Nós

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

"A parceria com a SHIELD representa um passo importante na missão da Pipa Studios de oferecer uma experiência divertida e segura para os jogadores. Com a tecnologia da SHIELD, conseguimos proteger nossa base de clientes contra fraudes e garantir a integridade dos jogos. Essa colaboração nos permite proporcionar uma jornada mais justa e divertida para nossa comunidade, reforçando nosso compromisso em oferecer o melhor dos jogos de bingo."

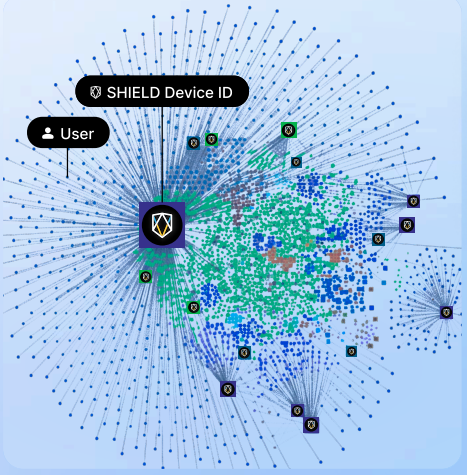
**Pedro Moraes**
CEO, Pipa Studios Brazil

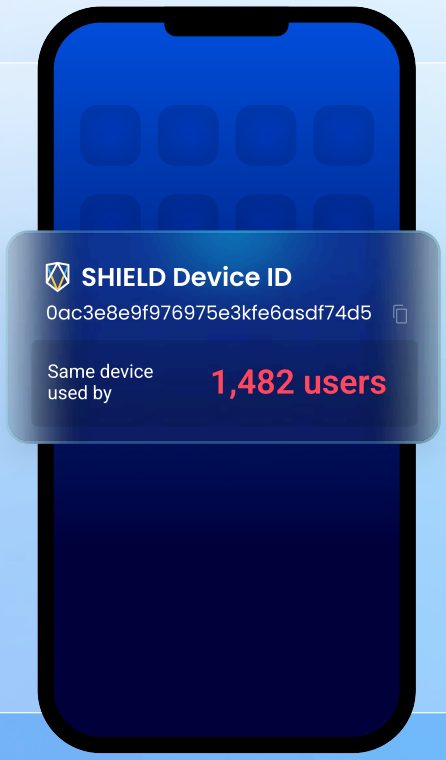
## Nossa Solução

Plug-and-Play · Sem códigos adicionais · Não requer PII

### SHIELD Device ID

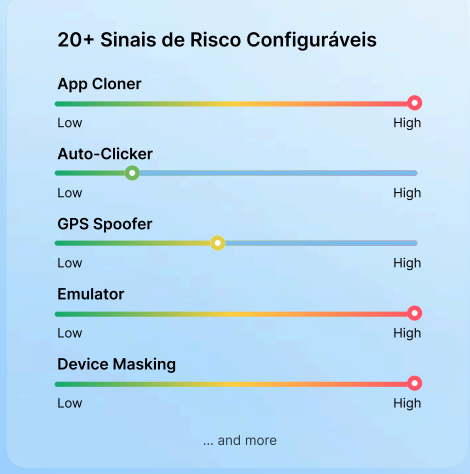
identifica de forma persistente a raiz da fraude & contas falsas >99.9% de precisão




### SHIELD Fraud Intelligence

insights acionáveis em tempo real sobre atividades fraudulentas



# Expõe Todo Risco de Fraude ao longo da Jornada do Jogador

Da criação da conta ao saque, a SHIELD oferece proteção completa contra fraudes em toda a jornada do jogador. Nossa inteligência de fraude focada na identificação de dispositivos revela ameaças ocultas e garante que apenas usuários confiáveis e dispositivos legítimos interajam com a sua plataforma.

## Casos de Uso

### Transações da Carteira (Depósitos & Saques)

Fraude de Pagamento
Chargebacks
...

### Jogos & Torneios

Tráfego de Bot
Abuso Automatizado
Falsificação de GPS
...

### Login

Account Takeovers
Falsificação de GPS
Contas Falsas
...

### Autenticação

Bypass de E-KYC
Deepfakes
Hooking
...

### Criação de Conta

Multi-Accounting
Conluio
Tráfego de Bot
Abuso de Promoção
...

### Lançamento de App

Ativação do Device Intelligence


**Fraud Intelligence**

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

Casos de Uso

# Elimine Deepfakes & Bypass de E-KYC

## Como os fraudadores burlam processos de E-KYC?

Fraudadores burlam a verificação de identidade ao usar deepfakes gerados por IA combinados com técnicas de hooking, falsificando rostos, documentos e testes de liveness. Esses ataques geralmente são realizados a partir do mesmo dispositivo e podem ser potencializados por emuladores e apps clonados. Em grande escala, os fraudadores automatizam os ataques para imitar milhares de usuários reais.

### Combata Deepfakes e Fraudes com IA

Evite que fraudadores usem vídeos e imagens deepfake gerados por IA para burlar a verificação biométrica e enganar os testes de liveness.

### Elimine Hooking e Adulteração de Apps

Detecte e bloqueie fraudadores que manipulam aplicativos para desativar medidas de segurança e injetar dados falsos de identidade.

### Previna Falsificação de Dispositivos

Impeça que fraudadores criem múltiplos perfis de dispositivos e mascarem a identidade com emuladores e outras técnicas.

### SHIELD Fraud Intelligence

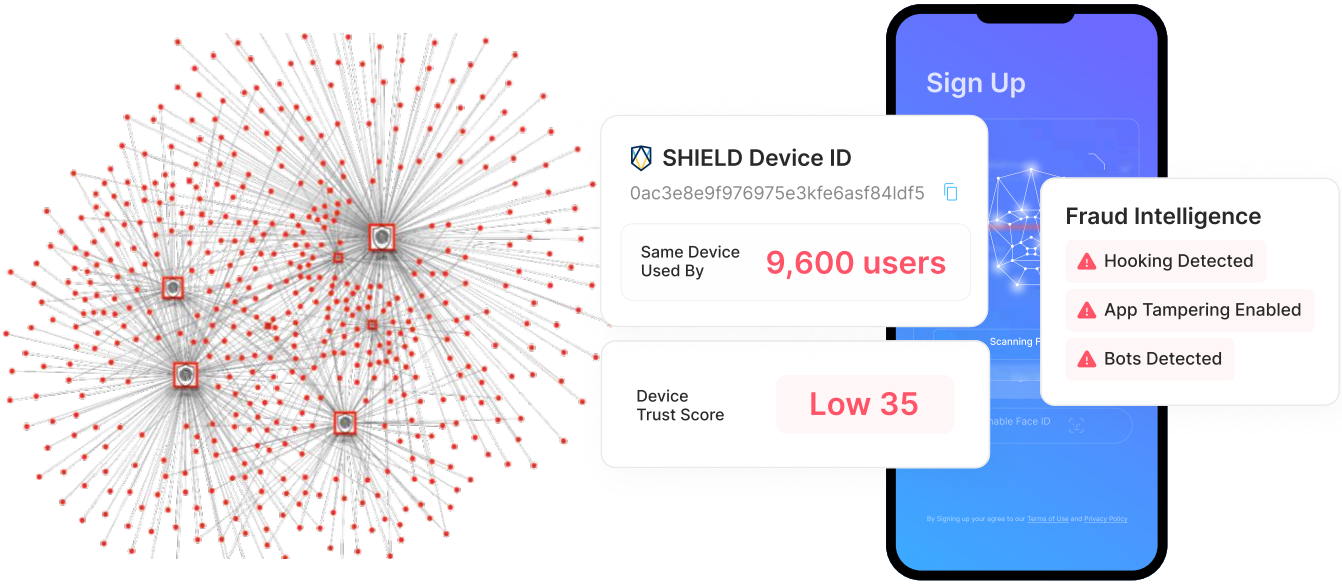
Uso de App cloners
Uso de Emuladores
Reset de Fábrica
Hooking
Jailbroken devices
Adulteração de App

### Como funciona

Fraudadores usam emuladores e apps clonados para criar perfis falsos de dispositivos e controlar várias contas ao mesmo tempo. Eles manipulam processos de verificação de identidade (IDV) com ferramentas de hooking.

O Device ID da SHIELD identifica dispositivos falsificados e rastreia sua origem real, revelando conexões entre múltiplas contas. Além disso, a plataforma sinaliza em tempo real ferramentas maliciosas, protegendo setores como o iGaming de fraudes por conluio.

Ao bloquear deepfakes e spoofing de dispositivos, a SHIELD ajuda plataformas de iGaming a manter confiança, segurança e conformidade. Em um caso, identificamos um esquema de fraude em larga escala: **um cluster de 9.600 usuários ligados a um único dispositivo**.



Casos de Uso

# Previna Contas Múltiplas & Conluio

## O que são Contas Múltiplas & Conluio?

Fraudadores criam múltiplas contas falsas em grande escala usando ferramentas maliciosas, utilizando essas contas para manipular resultados de jogos. O multi-accounting também é a porta de entrada para outros tipos de fraude, como **conluio e abuso de bônus**.

### Bloqueie Jogadores Falsos

Jogadores falsos comprometem a integridade da plataforma, inflacionam o número de usuários e dificultam a análise precisa de crescimento e engajamento.

### Elimine Conluio

Fraudadores usam múltiplas contas para participar de torneios, criando vantagem injusta sobre jogadores legítimos.

### Elimine o Abuso de Bônus

Fraudadores criam várias contas em escala para explorar bônus de cadastro, códigos de indicação e descontos por tempo limitado.

### SHIELD Fraud Intelligence

Uso de App cloners
Uso de Emuladores
Uso de VPN
Reset de Fábrica
Screen-sharing
Jailbroken devices
Adulteração de App

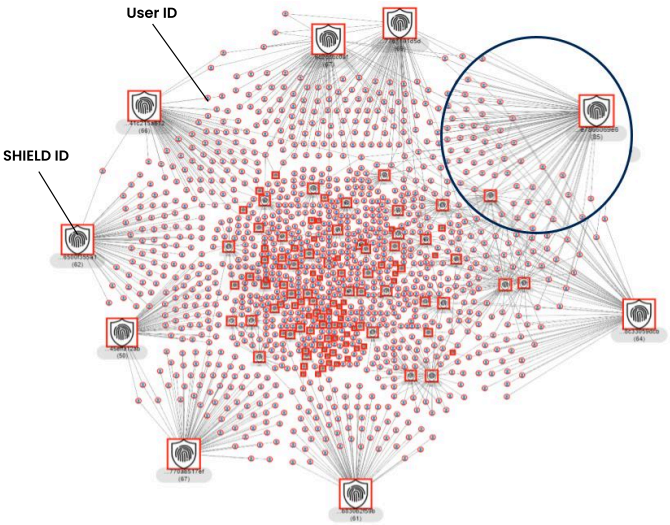
### Exemplo de Caso de Fraude

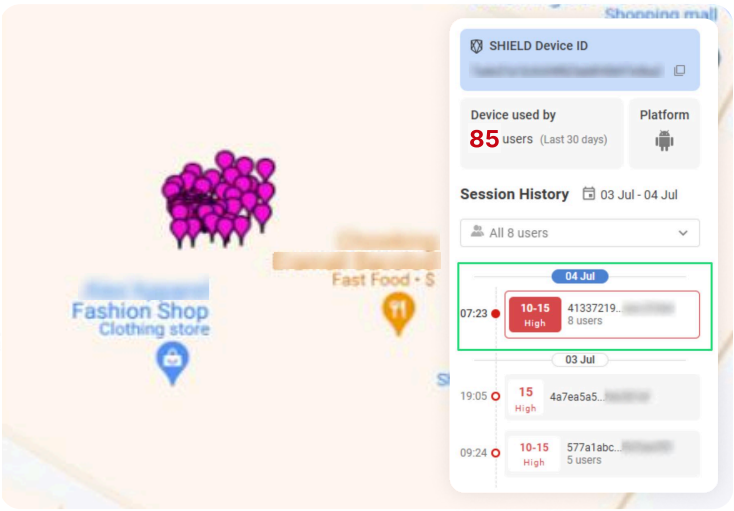
Fraudadores utilizam apps clonados e emuladores para gerar múltiplas contas. Neste caso, a SHIELD identificou um esquema de fraude com uma média de **1 dispositivo para 10 jogadores**.

Analisando mais de perto, encontramos um cluster de **85 usuários ligados a um único dispositivo**, dentro de uma proximidade de **2,74 metros**. Entre eles, 8 usuários compartilharam a mesma sessão do dispositivo. O screen-sharing estava sendo usado para coordenar movimentos entre dispositivos e maximizar ganhos.

Esse é um padrão típico de fraudadores em torneios, especialmente em jogos de poker, onde múltiplos perfis ganham vantagem sobre jogadores legítimos.

Além disso, fraudadores utilizam VPNs para contornar restrições e acessar torneios com bloqueio geográfico.



Casos de Uso

# Proteja-se contra Fraudes de Pagamento e Chargebacks

## O que são Fraudes de Pagamento e Chargebacks?

Fraudadores tentam financiar contas ou sacar ganhos usando dados de cartões e identidades roubadas, o que pode gerar altas taxas de chargeback e prejuízos financeiros significativos.

### Mantenha a Conformidade com Redes de Cartão

Altas taxas de chargeback podem resultar em altas tarifas de processamento e penalidades por parte de bandeiras como Visa e Mastercard.

### Reduza Chargebacks & Aumente Taxas de Aceitação

Proteja seu GMV anual. Detecte imediatamente atividades de risco e identifique proativamente transações confiáveis.

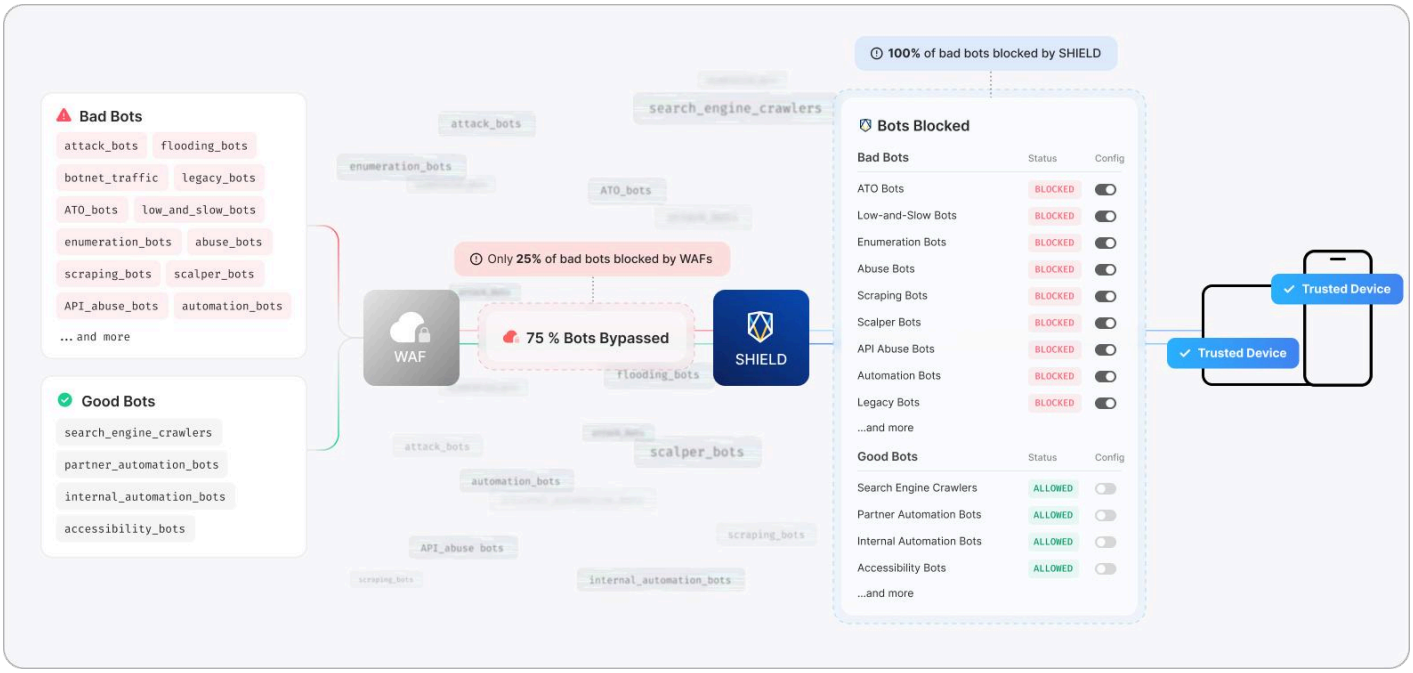
### Automatize Revisões e Impulsione o Crescimento

Otimize decisões de pagamento, reduza análises manuais e investigue tendências complexas em tempo real.

# Mitigue Tráfego de Bots

WAFs focam apenas em sinais de rede e normalmente detectam apenas ~25% do tráfego de bots e ataques DDoS, deixando lacunas significativas.

Para preencher essas brechas, a SHIELD atua na camada de aplicação, analisando o fingerprint do dispositivo por trás de cada requisição para distinguir com precisão usuários legítimos de ambientes automatizados, com 99,99% de acurácia.



Casos de Uso

# Detecte Falsificação de Localização

## Compliance & Geofencing

### O que é Falsificação de Localização?

Fraudadores alteram sua localização para acessar torneios com bloqueio geográfico ou entrar em plataformas de regiões sancionadas, criando jogadas injustas e riscos de conformidade.

A SHIELD detecta GPS spoofers, VPNs, proxies, oferecendo aos operadores integridade de localização, garantindo que apenas jogadores legítimos possam participar.

### SHIELD Fraud Intelligence

- Uso de Falsificação de GPS
- App tampering
- Uso de Emulador
- Uso de VPN

Além de detectar multi-contas e conluio, a SHIELD identifica quando GPS spoofers e VPNs são usados, permitindo rastrear a localização confiável do jogador.

Isso garante que usuários não estejam jogando de locais restritos. Além disso, os operadores podem usar esses dados de localização para cumprir regulamentos locais e evitar apostas de menores de idade.

# Proteja contra Account Takeovers (ATOs)

### O que é Account Takeover?

Fraudadores usam credenciais roubadas e ataques de força bruta para invadir contas de jogadores, gerando fraude em pagamentos, exploração de bônus e roubo de dados.

A inteligência de dispositivos da SHIELD permite que as plataformas verifiquem usuários legítimos sem criar fricções desnecessárias, aplicando verificações adicionais apenas em usuários e dispositivos suspeitos.

### SHIELD Fraud Intelligence

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

A SHIELD ajuda a prevenir account takeovers identificando dispositivos comprometidos usados em ataques de força bruta ou credential stuffing.

Ao identificar emuladores, apps clonados, jailbroken devices e dispositivos adulterados, os operadores obtêm uma visão confiável de quem está acessando cada conta, evitando logins não autorizados e protegendo fundos e dados dos jogadores.