SHIELD

SHIELD for SaaS Platforms

Protecting digital onboarding solutions, PSPs,
all-in-one trading platforms, digital commerce and beyond.

SHIELD's Device-First Fraud Intelligence platform stops fraud at the root with the **SHIELD Device ID** and actionable **Fraud Intelligence**, serving as the trusted technology enablement partner for SaaS platforms and adding an essential layer of defense to solutions across industries.

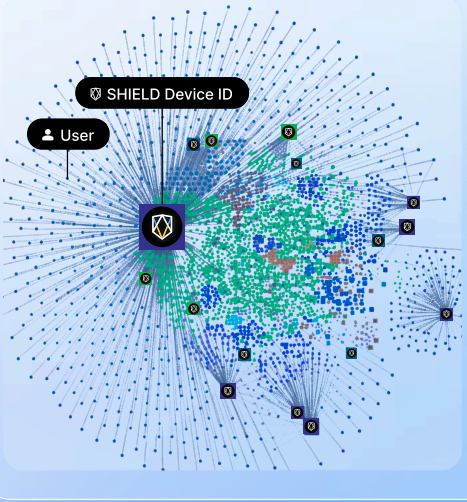
Trusted by

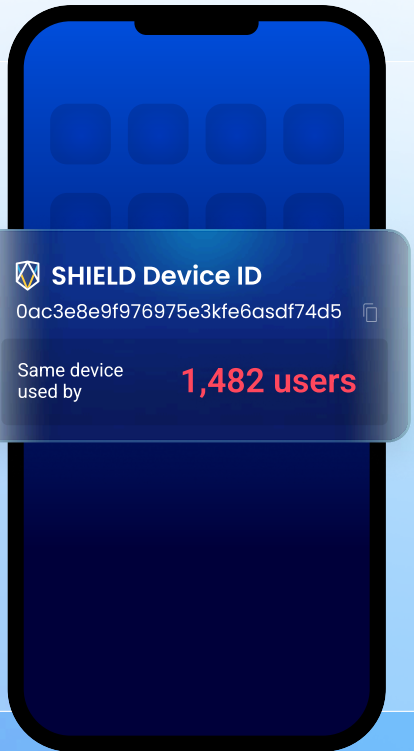
truemoney maya KIRVANO OTA tazapay surepass IDWise ondato UNICO BTSE ... and more

Our Solution

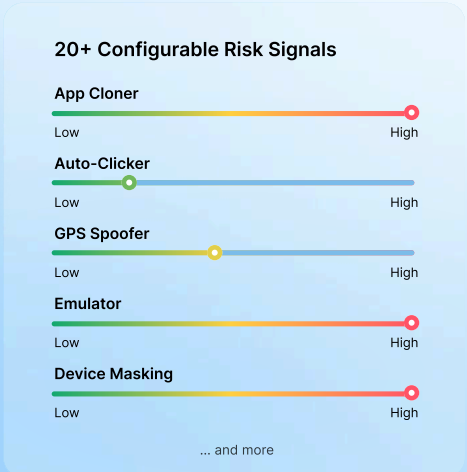
Plug-and-Play | No Additional Codes | No PII Required

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





SHIELD Fraud Intelligence
real-time actionable insights into fraudulent activity



Built to Stop All Fraud In Every Industry

From mobility and fintech, to trading, and beyond, SaaS platforms power the industries that keep the digital economy moving. SHIELD's Device-First Fraud Intelligence platform ensures those industries stay secure by stopping fraud at the source, enabling your clients to grow with confidence.

Fintech | Crypto / Trading | Digital & Neo Banks | E-Commerce & Marketplace | iGaming | Mobility | Online Delivery | Social Media & Networking | Media & Streaming | ...and more

Use Cases

Transactions

Market Manipulation
Mule Accounts
Money Laundering
In-Game Collusion
...

Card Payments

Payment Fraud
Promo Abuse
Money Laundering
Account Takeovers
...

Login

Account Takeovers
GPS Spoofing
...

Authentication

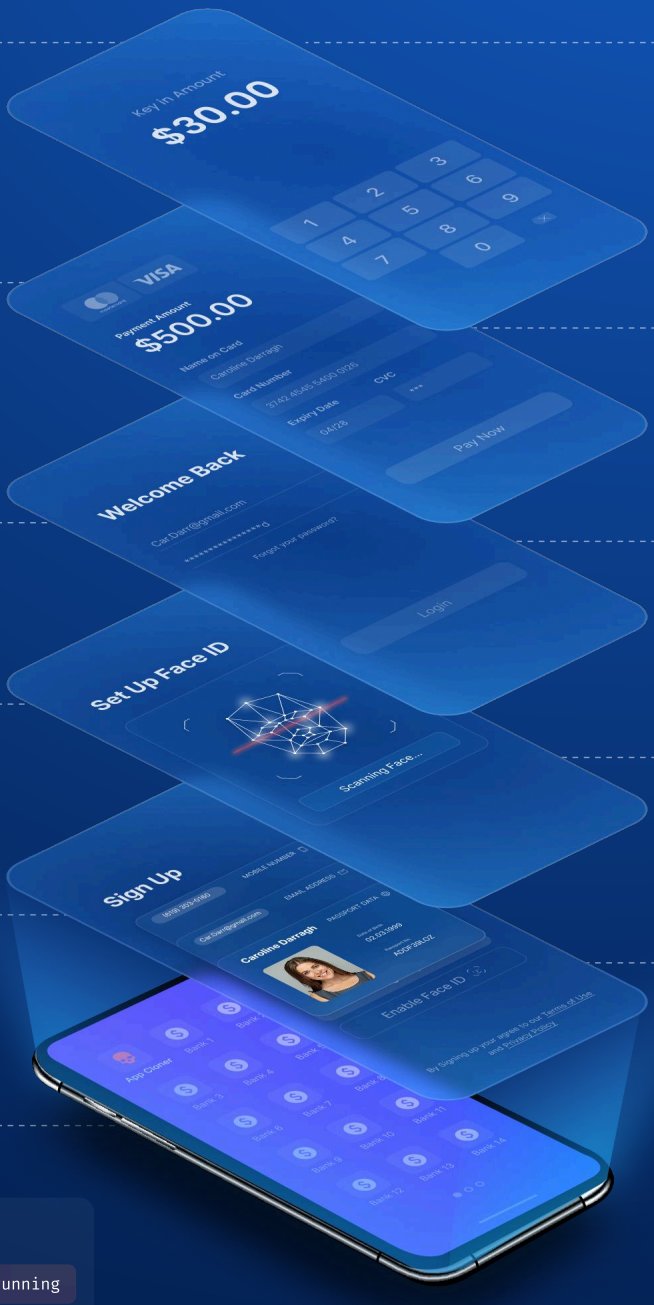
Deepfakes
Hooking Attacks
Account Takeovers
...

Registration

Fake Accounts
Multi-Accounting
Promo Abuse
...

App Launch

Device Intelligence Activates



Fraud Intelligence

`emulator_running` `auto_clicker_running` `gps_spoofer_running`

Industries

Mobility, Online Delivery, Fintech, E-Commerce, Digital Banks, iGaming, Trading, and more...

Fintech, E-Commerce, Digital Banks, Trading, and more..

Mobility, Social Media, Media Streaming, Online Delivery, Fintech, E-Commerce, Digital Banks, iGaming, Trading, and more...

E-KYC, Enterprise Solutions, and more...

Mobility, Social Media, Media Streaming, Online Delivery, Fintech, E-Commerce, Digital Banks, iGaming, Trading, and more...

Use Cases

Prevent 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 liveliness 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 conduct account takeovers (ATOs).

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.

Secure Transaction & Market Integrity

How Does Fraud Undermine Transactions & Market Integrity?

Fraudsters **exploit payments**, **promotions**, and **trading systems** to gain unfair advantages or cause financial losses. Using stolen cards, fake accounts, and coordinated networks, they **distort market activity** and exploit incentives. These attacks erode trust, damage reputation, and drain revenue.

Combat Payment Fraud

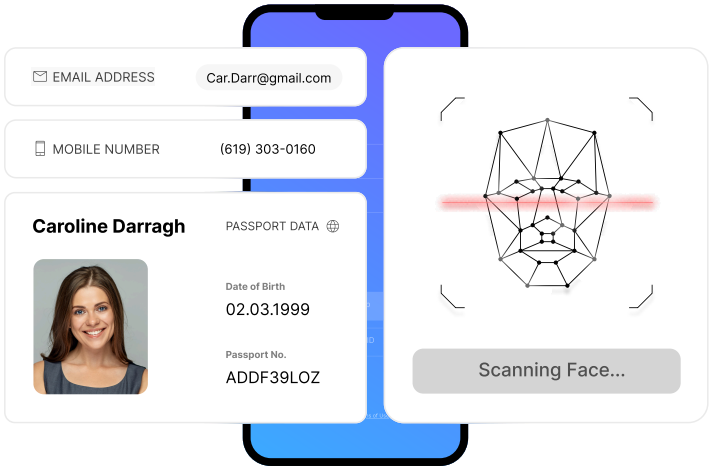
Stop fraudsters from using stolen cards or bank details to make unauthorized transactions and withdraw illicit earnings.

Prevent Market Manipulation

Detect and block coordinated activity that distorts market prices, rankings, or outcomes for unfair financial or competitive gain.

Catch Promo Abuse

Prevent fraudsters from creating multiple accounts to exploit limited-time offers, ensuring fair rewards and protecting campaign ROI.



Use Cases

Powering Secure & Seamless Authentication

Why Seamless Authentication Matters

SaaS platforms often need to verify user legitimacy at multiple points in the customer journey, but excessive re-verification can create unnecessary friction for genuine users. SHIELD's advanced device intelligence accurately **recognizes when users return on the same trusted device**, reducing re-verification needs, and enabling a more seamless authentication experience.

Stay Compliant with Regulations

SHIELD helps enforce regulations like age restrictions by detecting signs of account manipulation, shared credentials, or attempts to bypass restrictions using emulators and spoofed devices.

Monetize Beyond Onboarding

SHIELD helps SaaS platforms unlock new revenue streams by extending fraud protection beyond the sign-up flow. By activating SHIELD across the full user journey, you can offer added-value protection and upsell full real-time fraud coverage to clients.

SHIELD Fraud Intelligence

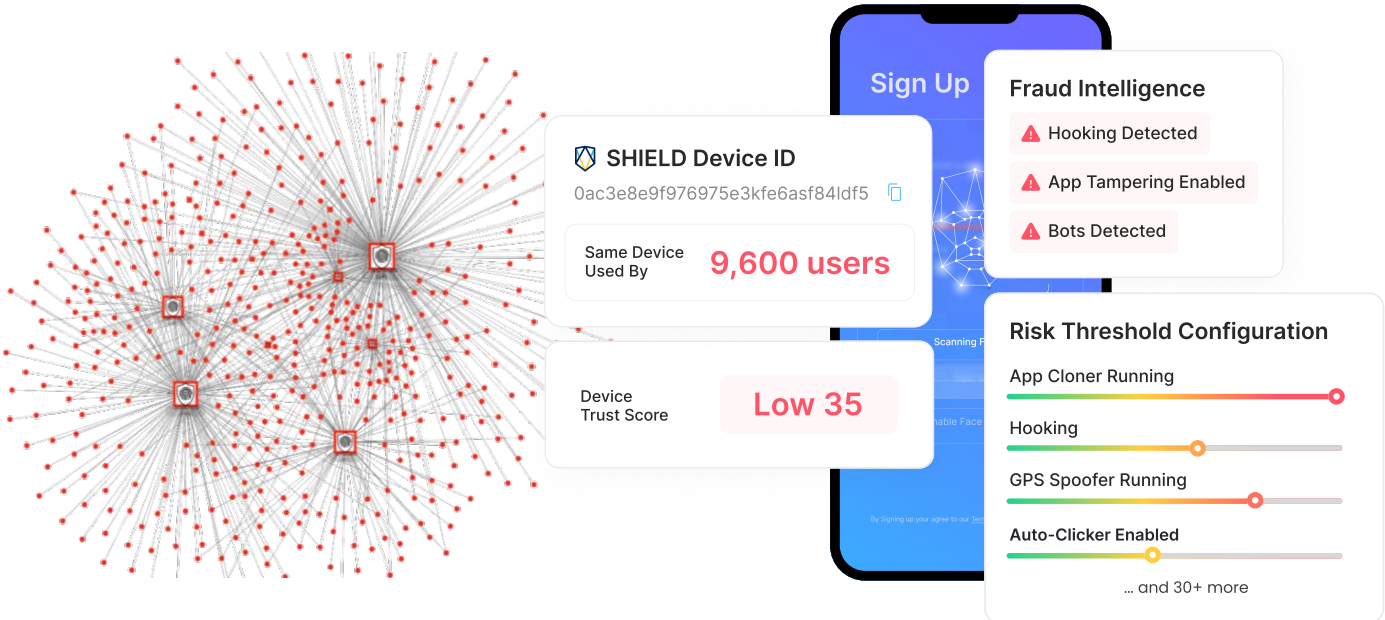
App Cloners Running
Emulator Running
Suspicious Factory Reset
Hooking
Jailbroken Devices
Tampered apps

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 **mobility**, **trading**, **e-commerce**, and **iGaming** from collusion fraud.

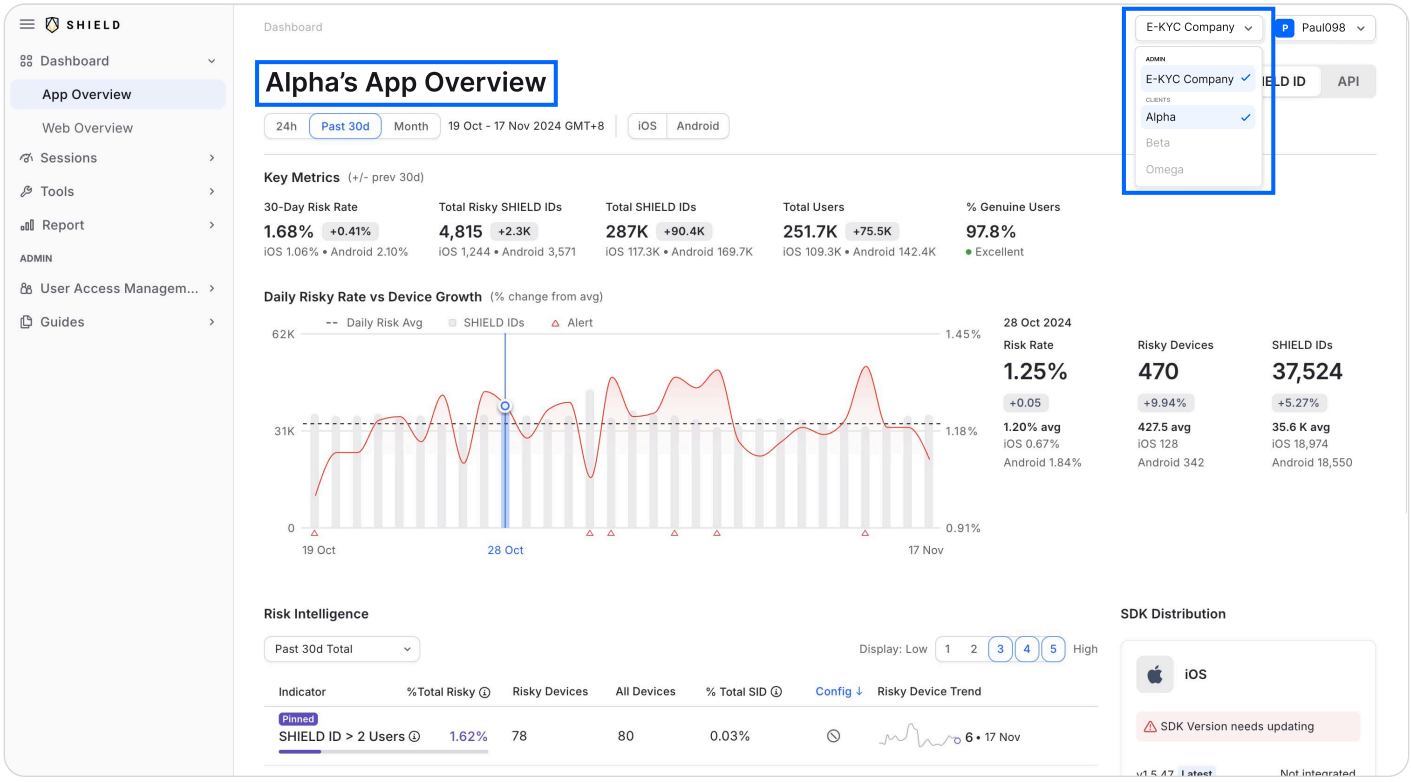
By stopping deepfakes and device spoofing, SHIELD helps B2B platforms and their clients maintain trust, security, and compliance. In one case, we exposed a large scale fraud syndicate - **a cluster of 9600 users linked to a single device**.



Use Cases

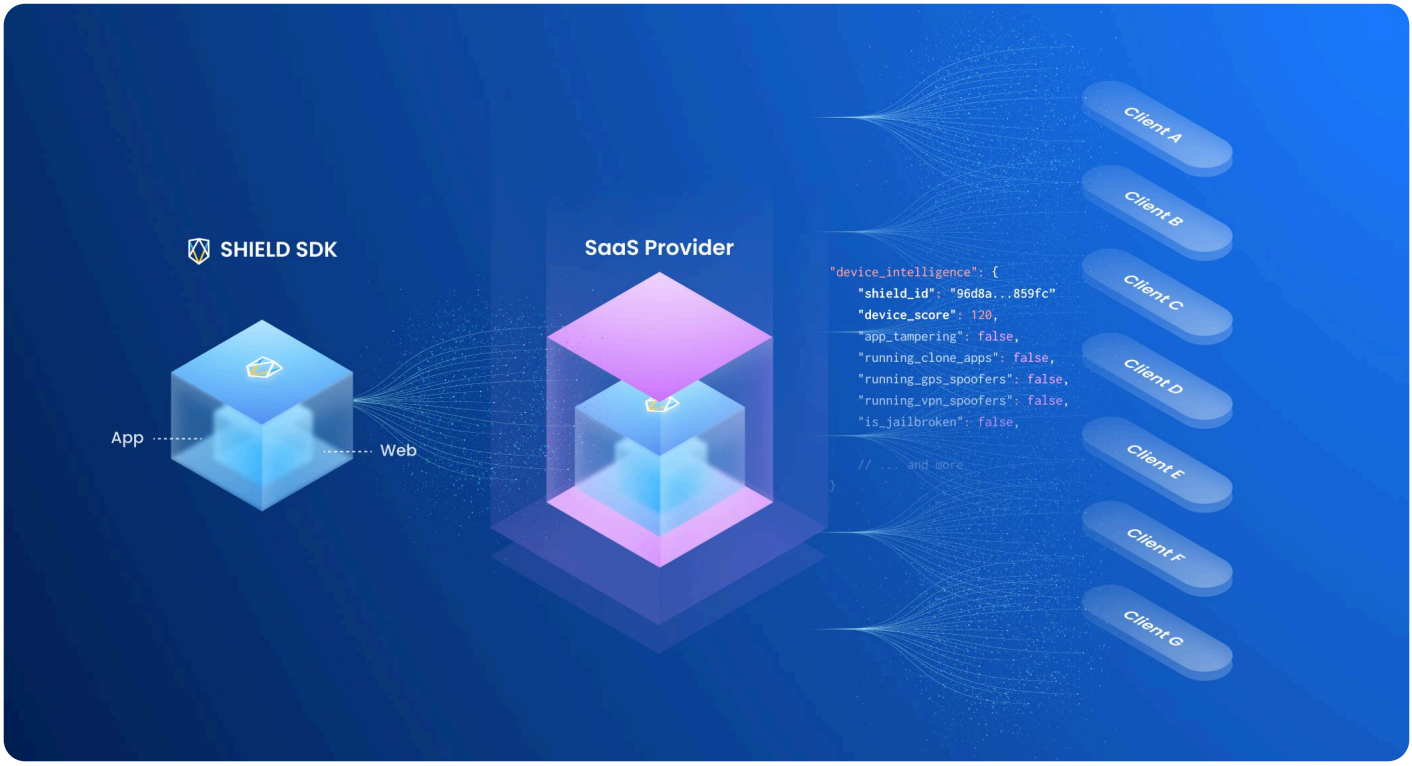
Complete Visibility Across Your Client Base

SHIELD makes it easy to view and manage the risk levels of every client you serve. From eKYC companies to platforms with multiple partners, switch effortlessly between tenants to see where action is needed.



Frictionless Integration For Every Client

Our SDK flow makes it simple to embed SHIELD into your solution, enabling fast deployment and instant protection for every client you serve, no matter the industry.



The SHIELD Advantage

Persistent Cross-App Device Identifier

Built to see what others can't

Traditional device identifiers like UUIDs, IDFAs, and GAIDs are inconsistent and easily changed.

SHIELD is the **only solution** that persistently and accurately identifies devices **across multiple apps** — even after reinstalls, factory resets, or OS-level changes.

This unmatched identification capability is the foundation of SHIELD's **Global Intelligence Network**, ensuring that every malicious device detected in one app can be instantly recognized and neutralized across others, anywhere in the world.

Global Scale & Unbeatable Coverage

Global Intelligence Network

Powered by our Persistent Cross-App Device Identifier, the SHIELD Global Intelligence Network combines device recognition with real-time fraud signals from over 231 countries.

This creates an ever-growing repository of every fraud pattern, malicious tool, and attack technique we've encountered — synced across industries and geographies in real-time.

For example, if a malicious device has been profiled on App A, SHIELD will flag it instantly when it resurfaces on App B—even if it's been reset, reinstalled, or masked.

1.5B+
devices screened yearly

231+
countries covered

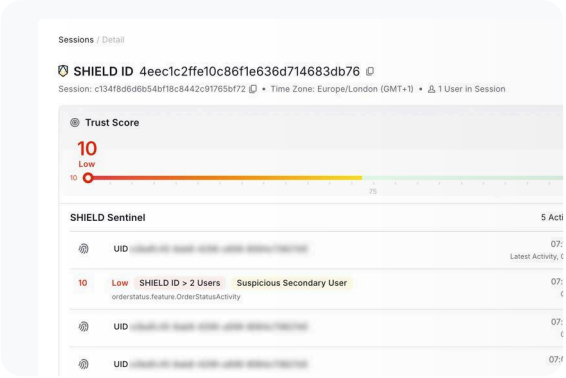
5B+
activities screened yearly

Enterprise-Grade Performance

Built to scale, backed to win

SHIELD is trusted by enterprise-grade businesses with complex infrastructure and high user volume , including global unicorns like like Unico, InDrive, TrueMoney, and more.

We deliver 99.9% accuracy, fast support, and a battle-tested platform that performs at scale no matter where in the world you are.



No PII, No Problem

Skip compliance headaches. We run with existing user permissions, are GDPR compliant & SOC 2, PCI DSS accredited.

Plug & Play SDKs or JS

Integrate with minimal engineering effort. Get up and running in mins with a simple setup and dev friendly docs.

See Results Instantly

No training period. No delays. See real ROI from the moment you go live. We flex with you at every stage of growth.