VIDA

Spot deepfakes, emulators and device farms in every session.

Stop fraud before it starts. **ID FraudShield silently checks 400+ data points** during every session, separating real customers from bad actors, all without slowing down the user journey.

400+
Device, behavior and network signals read per session

<200ms
Fraud attempts blocked by our Liveness SDK

5M+
Devices registered across South East Asia

PAD Level 3
Liveness Detection certified

A face check alone is no longer proof.

Deepfakes and injected videos

Fraudsters bypass the camera altogether, injecting a fake face directly into your app.

Device farms at scale

One device can register hundreds of fake accounts using emulators and automation.

Takeovers and coached scams

Stolen credentials and remote access tools let fraudsters impersonate real customers.

ID FraudShield reads device and session signals in real time, surfacing risk before it escalates.

VIDA ID FraudShield

What We Detect

Real time signals. Earlier intervention.

By 2027, 40% of enterprises will no longer consider face biometrics reliable in isolation because of AI-generated deepfakes. (Gartner, June 2025)

Powered by sardine

Environment & Integrity

- Fingerprint devices across hardware, software, sensors, and environmental attributes
- Detect emulators, malware access, jailbroken or rooted devices, and tampered operating systems
- Persistent device IDs across resets, reinstalls, and incognito sessions

Connections & Network

- Mobile intelligence including phone type and connectivity type, SIM type, device motion, and mobile carrier
- Identify suspicious network connections and high-risk VPN usage
- SIM-to-IP country matching and carrier-level analysis

Bot, AI & Automation Detection

- Flag suspicious devices, bots, and repeated device usage during registration
- Behavioral biometrics: keystroke dynamics, copy paste, clipboard events
- Detect remote access tools and screen-sharing software

Deepfake & Account Takeover

- Monitor every touchpoint for device tampering and injection attacks
- Detect active phone calls during high-risk sessions
- Detect remote-access software during high-risk transactions

Our intelligence. Your decision.

ID FraudShield sends risk signals to your backend and never blocks your users. It runs alongside RASP. VIDA manages custom rules server-side with no code change.

Low Risk **Very Fast Session**
Session total time < 1s

High Risk **Phone Call During Sessions**
Session.isCallActive == true

Critical Risk **SIM and IP Country Mismatch**
SimCountry =! IP.Country

VIDA

Protection at Every Stage

Fraud detection at every stage

From onboarding to transaction, every touchpoint is monitored for device tampering, injection attacks, and behavioral anomalies stopping fraud before it completes.

01 · Onboarding

New Account Fraud Prevention

Combine liveness detection and face verification with device signals to flag suspicious devices, bots, and repeated device usage during registration.

- Liveness + device risk scored together
- Bot and emulator detection

02 · Identity Verification

Identity Fraud Prevention

Add device and session-risk context to identity checks. Identify emulators, modified devices, and automated sessions alongside injection attacks and deepfakes.

- Complements existing KYC
- Injection attack detection

03 · Account Access

Account Takeover Defense

Monitor device integrity and behavioral anomalies across the customer journey to trigger step-up authentication.

- Cross-session device linking
- Behavioral anomaly flags

04 · Transactions

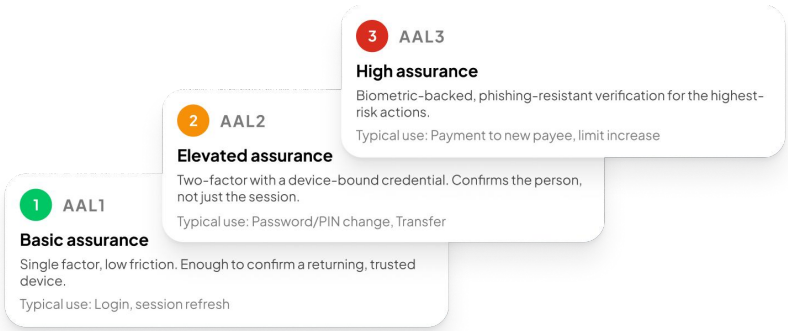
Scam & Payment Protection

Detect risk signals during payments—active calls, VPN use, SIM-IP mismatches—to trigger step-up when needed.

- Active call detection
- SIM-IP country mismatch

Let risk pick the challenge

Low risk passes silently. High risk asks for a live face. Critical risk is rejected outright. Your fraud engine or ID Fraud Shield sets the level.



CERTIFICATIONS & LICENSES

- Certified
- Certified
- PAD Level 3 Certified
- Service Provider
- Certified
- Associate Member
- Certified

ID Graph
Every entity connected to every entity it was seen with

The identity graph links users, Device IDs, IPs, Hash ID Numbers, and Hash face (biometrics) across every session. Spot fraud rings, detect device farms, and surface hidden connections all in real time.



Stay ahead of identity fraud.

Strengthen your fraud prevention with device intelligence, behavioural signals, and connected identity insights. Start with a proof of concept tailored to your use case.

mail.marketing@vida.id
www.vida.id