VERTICAL EDITION 10 · CONSUMER, D2C & EARLY-STAGE APPS

Stop the leak that never reached your server.

An early-stage company carries the same statutory duty as a bank on a fraction of the headcount: DPDP obligations from the first user, a six-hour CERT-In reporting clock, and a security questionnaire from every enterprise buyer and investor. Most of the exposure sits on the handset, before a single request reaches your backend. NonaShield answers a deterministic question at exactly that point — was this exact request produced by the physical device holding the non-exportable key, and has it been altered since? Attestation, RASP, fingerprinting, network defence, risk decisioning and forensic evidence run as one signed pipeline, on one integration.

400+	40+	9	1
Distinct threat vectors monitored across device, network and server	Behavioural vectors profiled per user session, continuously	Architectural layers delivered as one cryptographically signed pipeline	Vendor, contract, integration and console — not four or five

IN THIS DOCUMENT

EX 1 The fraud that actually costs a young company — eight vectors, and the layer that stops each

EX 2 One platform, nine layers — and only three permitted to make a binary decision

EX 3 Commercial & deployment model — one vendor instead of five, diligence-ready evidence

HARDWARE ATTESTATION · RASP · FINGERPRINTING · BEHAVIOURAL BIOMETRICS · GRAPH INTELLIGENCE · NETWORK DEFENCE · API GATEWAY · RISK DECISION ENGINE · EVIDENCE & COMPLIANCE

EXHIBIT 1 — EIGHT VECTORS, ONE ARCHITECTURE

The vocabulary is growth. The question underneath is possession.

Every vector below reduces to the same test: was this request produced by the physical device it claims to come from, by the person entitled to hold it, in an environment that has not been tampered with? The architecture does not change per sector — what changes is the policy set in Layer 7 and the entity model in Layer 5.

VECTOR	HOW IT ARRIVES ON A CONSUMER APP	LAYER
Personal data lifted from the device	Hooking frameworks and instrumentation reading personal data out of app memory and local storage before it is ever transmitted.	**1–2**
Cloned & repackaged builds	Your app republished with trackers, ads or exfiltration inserted — and your brand carrying the breach.	**1–3**
API abuse & scraping	Mobile endpoints called by headless clients; catalogue, pricing and user data enumerated at scale.	**2, 3**
Credential stuffing & account takeover	Breached password lists replayed against login, with saved addresses and payment instruments as the prize.	**1–3, 7**
Promotion, referral & first-order abuse	Emulators and device farms harvesting launch discounts, referral credit and free-tier limits.	**1, 3, 7**
Return, refund & COD abuse	Serial non-delivery and refund claims staged from clusters sharing device, address and payment markers.	**5, 7**
Payment & card testing	Scripted checkout attempts probing stolen card ranges, with gateway penalties landing on you.	**2, 3, 7**
Incidents you cannot reconstruct	A reportable event with no device-side record to reconstruct it from, against a six-hour clock.	**8–9**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a real user on their own device is persuaded to hand over an OTP or complete a payment, every cryptographic check passes correctly — because every check is correct. That case belongs to behavioural baselining and intent analysis (Layers 4–6), which you can switch on as the entity model matures, rather than a second purchase later.

APPS COVERED ON ONE INTEGRATION

Consumer and D2C apps, marketplace and subscription journeys, internal ops and field apps — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–3 and 7–9** from day one, with Layers 4–6 available on the same integration as the entity and behaviour model matures.

EXHIBIT 2 — ONE PLATFORM, NINE LAYERS

Six procurements, one signed pipeline — and only three layers may say no.

Device trust, app logic, network gateways, identity, backend controls and forensic chain-of-custody are conventionally six disjointed purchases correlated after the fact. NonaShield delivers them as a single pipeline in which every signal is bound to the same cryptographic assertion at the moment of capture.

BAND A · LAYERS 1–3

Deterministic device & payload truth

1 Mobile SDK — runtime signal capture, RASP, on-device enforcement

2 API Gateway & Network — edge enforcement, signed-payload validation

3 Trust Verification — server-side hardware key attestation

WHAT IT ESTABLISHES

Binary authority. These layers may allow or block outright because their error rate justifies it.

BAND B · LAYERS 4–6

Probabilistic risk enrichment

4 Fraud Intelligence — risk modelling and scoring across entities

5 Graph Intelligence — entity linkage, mule and coordinated-network detection

6 Behavioural Intelligence — continuous interaction and intent analysis

WHAT IT ESTABLISHES

Graded risk only. These layers modulate friction; they never make a binary access decision alone.

BAND C · LAYERS 7–9

Verdict & accountability

7 Decision Engine — real-time rule and model enforcement: allow / step-up / block

8 Evidence Engine — hash-chained, tamper-evident immutable record

9 Compliance — regulatory controls, WORM retention, regulator-mapped export

WHAT IT ESTABLISHES

One graded, signed verdict — and non-repudiable accountability as a by-product of the transaction path.

DETECT ——▶ ENFORCE ——▶ DECIDE ——▶ HARDENED RULES PUSHED BACK TO THE SDK

THE SEPARATION MATTERS MORE THAN THE COUNT

Most platforms fail not because they lack signals but because they let weak signals make strong decisions. Segregating binary authority (Bands A and C) from probabilistic enrichment (Band B) keeps false positives out of the journey that earns — a blocked genuine first order is a customer you paid to acquire and then turned away — while still allowing behavioural evidence to add friction the instant a session deviates from its own baseline.

EXHIBIT 3 — POINT SOLUTIONS VERSUS ONE UNIFIED PLATFORM

The stack you would otherwise assemble has four seams.

	FOUR TO FIVE POINT SOLUTIONS	NONASHIELD (UNIFIED)
Vendors to contract & manage	4–5 separate vendors	**1**
Integrations to build & maintain	One per vendor, each with its own SDK and API	**Single SDK + gateway + backend**
Signal correlation across layers	Manual or none — each tool sees only its own slice	**Fused into one explainable risk score**
Threat vectors covered	Varies per tool; gaps at the seams	**400+, continuously correlated**
Compliance & audit evidence	Assembled after the fact from disparate logs	**Native hash-chained evidence, regulator-mapped**
Time to deploy	Sequential vendor onboarding	**A single integration cycle**

DEPLOYMENT

01 Threat-surface review — map your current stack, seams and highest-loss journeys. Two weeks.

02 Pilot — one app, one journey, production traffic, measured against your existing controls.

03 Production rollout — full journey coverage, policy tuning, evidence chain live for audit.

04 Continuous hardening — detect, enforce, decide — with hardened rules pushed back to the SDK.

COMPLIANCE & ASSURANCE

Digital Personal Data Protection Act and DPDP Rules, 2025

CERT-In Directions, 2022 — six-hour incident reporting and log retention

OWASP MASVS v2 and ISO 27001 alignment for enterprise and investor diligence

PCI DSS v4.0.1 where cardholder data is in scope

An evidence chain that answers a diligence questionnaire without a reporting project

Five-year WORM retention under compliance lock; regulator-mapped export

WHY DIMEAI

25 years of banking-technology and e-governance security experience behind the architecture

Patent published in India, grant awaited — tamper-evident evidence chain

Explainable ML risk scoring — decisions you can defend to a regulator

Android & iOS from one Kotlin Multiplatform SDK

Cloud, on-premises or hybrid — matched to your infrastructure posture

One commercial relationship, one console, one support line

NONASHIELD · STARTUPS & D2C

Stop the fraudster. Before the fraud.

contactus@diimeai.com
+91 85917 55427
DIIMEAI.COM