VERTICAL EDITION 12 · CUSTOMER, RIDER & DARK-STORE APPS

Stop the delivery that never happened.

Quick commerce runs on a ten-minute promise and a single-digit margin, and the fraud sits on both sides of it: a rider marking an order delivered from a spoofed location, and a customer claiming it never arrived. Every extra check costs the promise. NonaShield answers a deterministic question before the request leaves the handset — was this exact request produced by the physical device holding the non-exportable key, and has it been altered since? Attestation, RASP, fingerprinting, behavioural intelligence, network defence, risk decisioning and forensic evidence run as one signed pipeline across your customer, rider and dark-store apps.

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

IN THIS DOCUMENT

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 delivery. 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 DELIVERY APP	LAYER
GPS spoofing & false delivery marking	Mock-location and app-tamper tooling on rider handsets marking orders delivered from outside the delivery radius.	**1, 2, 5**
Rider account sharing & ghost riders	One onboarded identity worked by several people or sold on — the handset changes, the account does not.	**1, 3, 5**
Incentive, surge & streak farming	Device estates cycling orders and login windows to harvest surge pay, streak bonuses and joining incentives.	**1, 3, 5**
Collusive & self-placed orders	Orders placed and accepted by linked customer and rider accounts sharing device, address and payout markers.	**5, 7**
COD collection & payout diversion	Cash marked collected but never remitted; rider bank details changed from a compromised or unenrolled handset.	**3, 7, 8**
Refund, missing-item & RTO abuse	Serial missing-item and non-delivery claims staged by clusters sharing device, address and payment markers.	**5, 7**
Promotion, referral & first-order abuse	Emulators and re-flashed handsets creating accounts in bulk to harvest launch discounts and referral credit.	**1, 3, 5**
Checkout card testing & takeover	Stolen card ranges probed at a checkout built for speed; saved cards and wallet balances taken over at login.	**1–3, 7**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a genuine customer on their own device abuses a policy — serial missing-item claims, staged non-delivery — every cryptographic check passes correctly. That case belongs to graph, behavioural and intent analysis (Layers 4–6), which surface repeat-abuse clusters across customer and rider accounts and apply friction only to the affected journey, never to a ten-minute checkout.

APPS COVERED ON ONE INTEGRATION

Customer ordering apps, rider and delivery-partner apps, dark-store picker and store-ops apps, checkout and wallet journeys — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–3 and 5–7**, with Layers 8–9 engaged where chargeback, payout and gig-payment evidence is required.

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 order is a customer lost in the ten seconds they were willing to wait — 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

Consumer Protection (E-Commerce) Rules, 2020

PCI DSS v4.0.1 for cardholder data and card-network dispute evidence

DPDP Act and Rules 2025 — customer and rider data handled on device

CERT-In Directions 2022 — incident reporting and log retention

FSSAI traceability obligations where food and grocery are handled

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 · QUICK COMMERCE & DELIVERY

Stop the fraudster. Before the fraud.

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