VERTICAL EDITION 08 · TRADING, WEALTH & DEALER APPS

Stop the order the client never placed.

In broking the loss is booked the moment the order is matched: there is no reversal window, and the burden of showing what actually happened sits with the broker. NonaShield answers a deterministic question before the order leaves the handset — was this exact instruction 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 trading, wealth and dealer apps.

400+	40+	9	1
Distinct threat vectors monitored across device, network and server	Behavioural vectors profiled per trading 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 markets. 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 TRADING APP	LAYER
Unauthorised order placement	A hijacked or persisted session used to place, modify or square off orders the client never authorised.	**1–3, 7**
Session hijack & token replay	Session tokens lifted from a compromised handset and replayed from another client entirely.	**2, 3, 8**
Account takeover after SIM swap	Credentials plus a swapped SIM reproduce the trading account on a device that was never enrolled.	**1, 3, 7**
Scripted & unauthorised algo access	Headless clients driving the mobile API at machine speed, outside any approved algo arrangement.	**2, 3, 6**
Pump-and-dump via taken-over accounts	Clusters of compromised accounts trading the same illiquid scrip inside a narrow window.	**5, 7**
Order-parameter tampering	Price, quantity or instrument altered between the handset and the order-management system.	**2, 3, 8**
Mule accounts & layered pay-outs	Pay-out bank details changed from compromised handsets; proceeds layered across linked accounts.	**5, 7, 8**
Dealer & RM-app misuse	Relationship-manager and dealer apps used to act on client accounts without a recorded instruction.	**1, 6, 8**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a client places an order on their own enrolled device under someone else's persuasion, every cryptographic check passes correctly — because every check is correct. That case belongs to behavioural baselining, graph and intent analysis (Layers 4–6), which surface coordinated and out-of-character trading and apply friction there, never to the order path as a whole.

APPS COVERED ON ONE INTEGRATION

Trading and investing apps, wealth and advisory journeys, dealer and relationship-manager apps, onboarding flows — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–3 and 6–9**, with Layers 8–9 producing the retained, tamper-evident record a cyber-resilience audit asks for.

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 missed market and an investor complaint — 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

SEBI Cyber Security and Cyber Resilience Framework (CSCRF) for regulated entities

SEBI technical-glitch and audit-trail expectations for trading applications

ISO 27001 and OWASP MASVS v2 alignment for the mobile application

DPDP Act and Rules 2025 — client data handled on device

Dual-ECDSA-signed order evidence for dispute and exchange review

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 · TRADING & BROKING

Stop the fraudster. Before the fraud.

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