VERTICAL EDITION 02 · EXCHANGE, WALLET & VDA APPS

The withdrawal is irreversible. The proof comes first.

In digital assets there is no chargeback and no reversal window: once a withdrawal is broadcast, the control either worked or it did not. NonaShield answers a deterministic question before the request leaves the handset — was this exact transaction produced by the physical device holding the non-exportable key, and has it been altered since? Hardware attestation, RASP, device fingerprinting, behavioural intelligence, network defence, risk decisioning and forensic evidence run as one signed pipeline across your exchange app, custodial and non-custodial wallets and onboarding journeys.

400+	40+	9	1
Distinct threat vectors monitored across device, network and server	Behavioural vectors profiled per wallet 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 custody. 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 WALLET OR EXCHANGE APP	LAYER
Key & seed-phrase extraction	Malware, hooking frameworks or a rooted handset reading key material, clipboard or recovery phrases out of the wallet process.	**1, 2**
Device cloning & app repackaging	A repackaged or cloned wallet build distributed outside official stores, or an install copied to a second handset or emulator.	**1–3**
Automated withdrawal scripting	Credentials driven by a script or headless client against withdrawal and transfer endpoints at machine speed.	**2, 3, 6**
Deepfake & liveness defeat at onboarding	Synthetic face and document submission from an emulator or injected camera feed during VDA KYC.	**1, 3, 4**
Rapid multi-account creation	Device farms opening accounts in bulk for airdrop farming, limit evasion and layering across the exchange.	**3, 4, 5**
Address-swap overlay & clipboard attacks	An overlay or clipboard hijack rewrites the destination address after the user has verified it on screen.	**1, 2, 7**
Remote access & social-engineering payouts	A support-impersonation scam driving the genuine device to approve a withdrawal to an attacker address.	**4, 6, 7**
API-key abuse on trading endpoints	Leaked or over-scoped API keys replayed from unattested clients against order and transfer APIs.	**2, 3, 7–8**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When the user physically holds the device and is talked into approving the withdrawal, every cryptographic check passes correctly. That case belongs to behavioural baselining, graph and intent analysis (Layers 4–6), which apply surgical friction the moment a session deviates from its own pattern — destination address novelty, amount, hour, approval rhythm.

APPS COVERED ON ONE INTEGRATION

Exchange and wallet apps, custodial approval and treasury apps, VDA onboarding and liveness journeys — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–4 and 6–8**, with Layers 5 and 9 engaged where mule-network and supervisory reporting demand it.

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 on withdrawal and address-book endpoints **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 across wallets and accounts **6 Behavioural Intelligence** — continuous interaction and withdrawal-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 per withdrawal and approval **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 legitimate withdrawal flow — a blocked genuine payout is a support ticket and a churned user — 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 withdrawal flow, measured against 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

Aligned to PMLA / FIU-IND obligations for VDA service providers, including travel-rule reporting

ISO 27001, SOC 2 and DPDP alignment; AML and sanctions-screening handoff

Five-year WORM retention under compliance lock

Court-admissible, dual-ECDSA-signed transaction evidence

Fail-closed queuing; zero backend exposure on blocked traffic

Post-quantum-ready cryptographic design

WHY DIMEAI

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

Patent-backed, 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 · CRYPTO, WALLETS & DIGITAL ASSETS

Stop the fraudster. Before the fraud.

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