VERTICAL EDITION 04 · POLICY, CLAIMS & AGENT APPS

Stop the claim that was staged, not suffered.

Insurance fraud is decided by evidence: who submitted the proposal, from which device, and whether the claim material was produced where it claims to have been. NonaShield answers a deterministic question before the submission 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, agent and claims-surveyor apps.

400+	40+	9	1
Distinct threat vectors monitored across device, network and server	Behavioural vectors profiled per submission 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 claims. 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 POLICY OR CLAIMS APP	LAYER
Fabricated identity at proposal	Synthetic or stolen identity and forged documents submitted from emulated or cloned devices during onboarding.	**1, 3, 7**
Cloned & repackaged insurer apps	Fake policy or claims apps circulating outside official stores, harvesting customer data and premium payments.	**1–3**
Agent-channel collusion	Agent or POSP apps used outside mandate — misselling, ghost policies, premium misappropriation from shared handsets.	**1, 5, 8–9**
Claim fraud from tampered devices	Claim intimation, geo-tag and evidence upload from rooted, hooked or GPS-spoofed handsets.	**1, 2, 7**
Duplicate & networked claim rings	The same claim staged across policies and insurers by a cluster sharing device, network and beneficiary markers.	**5, 7**
Deepfake & liveness defeat	Synthetic video KYC or survivor-verification submissions from injected camera feeds.	**1, 3, 7**
Payout & bank-mandate diversion	Beneficiary bank details altered ahead of settlement, paired with contact-detail and SIM changes.	**2, 3, 7**
Bot floods on quote & claim APIs	Scripted clients and device farms scraping quotes, testing policy numbers and stuffing credentials.	**2, 3, 6**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When the policyholder physically holds the device and submits a genuine-looking but fabricated claim, every cryptographic check passes correctly. That case belongs to graph, behavioural and intent analysis (Layers 4–6), which surface duplicate-claim networks, repeat beneficiaries and submission patterns that deviate from the portfolio baseline.

APPS COVERED ON ONE INTEGRATION

Customer policy and claims app, agent, POSP and bancassurance apps, surveyor and investigator apps, video-KYC and onboarding journeys — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–3, 5 and 7–9**, with Layers 4 and 6 engaged where claim volume warrants 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 claim-submission and settlement 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, duplicate-claim and coordinated-ring detection across policies and beneficiaries **6 Behavioural Intelligence** — continuous interaction and submission-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 claim and settlement **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 genuine claims — a wrongly held settlement is a regulatory and reputational cost — 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 claim 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 IRDAI information- and cyber-security guidelines for insurers and intermediaries

ISO 27001, DPDP and AML/CFT guideline alignment for insurers

Five-year WORM retention under compliance lock

Court-admissible, dual-ECDSA-signed claim and settlement 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 · INSURANCE, CLAIMS & AGENT CHANNEL

Stop the fraudster. Before the fraud.

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