VERTICAL EDITION 09 · STREAMING, SUBSCRIPTION & LIVE APPS

# Stop the stream that was never a subscriber.

Leakage in streaming is not a security line item — it is the licence. Credential sharing dilutes ARPU quietly, and a single rooted handset capturing a live sports feed puts the content deal itself at risk. NonaShield answers a deterministic question before playback is authorised — 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 streaming, subscription and live-event apps.

| 400+ | 40+ | 9 | 1 |
|---|---|---|---|
| Distinct threat vectors monitored across device, network and server | Behavioural vectors profiled per viewing 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 platform — 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, licensor-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 content. 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 STREAMING APP | LAYER |
|---|---|---|
| **Credential sharing beyond the household** | One subscription concurrently active across device estates sharing no location, network or usage rhythm. | **3, 5, 6** |
| **Rooted-device capture & stream ripping** | Playback on rooted or hooked handsets where output protection can be bypassed and the decoded frame captured. | **1–2** |
| **Cloned & modded streaming apps** | Patched builds with entitlement checks removed, distributed through third-party stores and links. | **1–3** |
| **Token & entitlement replay** | Playback tokens lifted from one session and replayed by unauthorised clients and re-streaming services. | **2, 3, 8** |
| **Account takeover & resale** | Breached credentials replayed at scale, then sold as discounted 'accounts' on resale channels. | **1, 3, 7** |
| **Free-trial & promotion farming** | Emulators and device farms cycling trials, referral credit and regional pricing offers in bulk. | **1, 3, 5** |
| **Screen-capture & overlay attacks** | Capture, mirroring and overlay tooling active during protected playback and during payment entry. | **1–2** |
| **Subscription & card-testing fraud** | Stolen card ranges probed against subscription checkout; chargebacks landing after the content is consumed. | **2, 4, 7** |

### WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a subscriber hands their own credentials to someone they know, every check passes correctly — the device is genuine and the session is authentic. That case belongs to graph, concurrency and behavioural analysis (Layers 4–6), which surface household boundaries and apply friction only to the sessions that break them, never to playback as a whole.

### APPS COVERED ON ONE INTEGRATION

Subscriber and viewing apps, live-event and sports journeys, partner and distributor apps, subscription checkout — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–3 and 5–9**, with Layers 8–9 producing the evidence licensor reporting and takedown processes require.

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 viewer churns in the first ten seconds of a live match — 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

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Licensor content-protection and forensic-traceability obligations

PCI DSS v4.0.1 for subscription checkout and cardholder data

CERT-In Directions 2022 — incident reporting and log retention

DPDP Act and Rules 2025 — subscriber data handled on device

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 · MEDIA & OTT

## Stop the fraudster. Before the fraud.

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