PRODUCT BRIEF · IV OF IV

Plaza.

The super-app layer that turns your banking or lifestyle app into a destination — social commerce, community, loyalty, and content inside the trusted shell your customers already opened.

YOUR APP, THEIR GATHERING PLACE.

CONTENTS

Table of Contents

A technical-reference document for digital, product, and transformation leaders evaluating the Plaza layer within their own application estate.

Section 01

Executive *Summary*

A one-page orientation for board-level and C-suite readers. The rest of this document expands every claim made here.

Nexilis Plaza is the fourth horizontal product in the Nexilis portfolio, joining Sentinel (security), Enclave (secure communications), and Reach (customer engagement). Plaza's category is the *super-app layer* — the in-app destination that converts utility into daily presence.

The banking and lifestyle apps of most Indonesian institutions today are transaction terminals. Customers open them with a task in mind, complete it, and close them. Opening frequency averages one to three times per month; session duration averages under two minutes. By every meaningful metric of consumer attention, the institutional app has ceded the destination role to Gojek, Grab, TikTok, Tokopedia, and Shopee — platforms that were built to be ***places***, not tools.

Plaza is the answer. It is a composable, institution-owned super-app layer that adds four capability pillars to the host application — social commerce, community, loyalty, and lifestyle content — while inheriting the identity, policy, telemetry, and encryption primitives already delivered by Sentinel, Enclave, and Reach. The institution retains control of brand, data, merchant relationships, and regulatory posture; the customer gains a reason to open the app outside the transaction moment.

> THE PLAZA THESIS
>
> The destination layer belongs inside the trusted app, not outside it. Every hour of customer attention spent inside a super-app your institution does not own is an hour of adjacent-product opportunity — credit, wealth, insurance, merchant commission — redirected to a platform that will eventually compete with you directly.

WHAT THIS DOCUMENT CONTAINS

- A formal definition of the Plaza category and product boundary (Sections 02–03)
- The seven-layer platform architecture and capability pillars (Sections 04–05)
- The composition model with Sentinel, Enclave, and Reach (Section 06)
- Regulatory mapping against OJK, BI, PDP Law, and Kominfo (Section 07)
- Deployment, integration, competitive frame, and commercial tiers (Sections 08–10)
- Three reference scenarios drawn from BFSI, public-sector, and lifestyle use (Section 11)

WHO SHOULD READ IT

Chief Digital Officers, Heads of Digital Product, Heads of Retail Distribution, Heads of Merchant Partnership, and the architects and procurement officers who support them. Security buyers should read Sentinel's brief first; customer-service buyers should read Reach's. Plaza sits one layer up from both and depends on them.

Section 02

The Category *Problem*

Why the banking app, the government service app, and the lifestyle-brand app all stop short of becoming destinations — and what that costs.

2.1 The last sovereign surface

Every digital surface an institution once controlled has been disintermediated. Search belongs to Google. Social belongs to Meta, ByteDance, and X. Commerce belongs to Amazon, Tokopedia, Shopee, and Lazada. Messaging belongs to WhatsApp and LINE. Even the web browser — arguably the last neutral ground — is increasingly mediated by Chrome and Safari.

The mobile application is the single remaining surface where the institution sets the rules. It is the only channel where the bank, the ministry, or the brand controls identity, authentication, content, placement, ordering, merchandising, and telemetry end-to-end. And yet, for most institutions, this sovereign surface is used in the narrowest possible way — as a transaction terminal.

2.2 The utilitarian app and its ceiling

A utilitarian app has a hard ceiling. Customers open it when they need to do something specific, complete the task, and leave. Opening frequency is bounded by the frequency of the underlying job — paying bills, checking balance, transferring funds, confirming an alert. For a typical Indonesian retail banking app, that yields 1.2 to 3.5 sessions per month at 60 to 110 seconds each.

This is not a failure of design. It is the logical end-state of a product whose sole purpose is transaction. What it leaves unclaimed is every minute of attention ***between*** transactions — the morning commute, the lunch scroll, the evening browse — all of which now flow to apps that were built from the beginning to be places.

> *"A utility app is opened when the customer must.*
> *A destination app is opened when the customer wants to."*

2.3 Why bolt-ons have failed

Most institutions have, at some point, tried to add engagement capability to their app. The standard approach is to license three or four separate SDKs — one for rewards, one for merchant

commerce, one for social feed, one for content — and integrate them in parallel. The result is familiar and predictable:

SYMPTOM	MECHANISM
Identity fragmentation	Each SDK requires its own account or profile, forcing customers to log in separately or accept inconsistent personalization.
Policy drift	Different vendors enforce different content moderation, refund, and dispute rules — and the institution inherits the lowest common denominator.
Telemetry blind spots	Engagement data sits in three or four vendor dashboards that do not reconcile; the institution cannot answer basic questions about customer behaviour.
Audit fragmentation	Regulatory inquiries cross vendor boundaries. Responses become brittle and delayed.
Brand erosion	Each SDK imposes its own UI conventions; the app becomes visually schizophrenic and trust degrades.
Commercial leakage	Vendor take-rates stack; by the time a merchant transaction settles, 8–15% has been paid across three intermediaries.

The compounding effect is severe. A bolt-on strategy does not merely ***underperform*** a composed strategy — it actively undermines the trust posture that made the institution's app worth opening in the first place.

2.4 The category that does not yet have a name

Industry analysts call this space “super-app functionality,” “commerce-as-a-layer,” “embedded commerce,” or “loyalty-and-engagement platform.” None of these terms captures the full proposition. Plaza defines the category as the ***institutional super-app layer***: a single, trust-native surface that composes social commerce, community, loyalty, and lifestyle content under one identity, one policy, one telemetry fabric, and one brand.

> **DEFINITION — INSTITUTIONAL SUPER-APP LAYER**
>
> A coherent, identity-bound, policy-governed, telemetry-unified surface inside a regulated-institution application that delivers social-commerce, community, loyalty, and lifestyle capability without requiring the customer to leave the host app and without fragmenting the institution's control of brand, data, or regulatory posture.

The Plaza *Proposition*

What Plaza is, what it is not, and the five claims that distinguish it from adjacent categories.

3.1 Working definition

Nexilis Plaza is an institution-owned super-app layer that composes four engagement pillars — *social commerce, community, loyalty, and lifestyle content* — inside an existing banking, public-service, or lifestyle application, under the host institution's identity, policy, and telemetry control.

3.2 The five distinguishing claims

CLAIM 01 — COMPOSABILITY

One layer, four pillars, one contract

Plaza delivers social commerce, community, loyalty, and lifestyle content as a single integrated surface — not four SDKs stapled together. Institutions buy one product under one contract, receive one invoice, and operate one admin console.

CLAIM 02 — TRUST INHERITANCE

Built to compose, not to compete

Every transaction, post, point, and redemption in Plaza inherits the hardened identity, device posture, encryption, and audit fabric already delivered by Sentinel, Enclave, and Reach. Plaza does not reinvent the trust stack — it consumes it.

CLAIM 03 — SOVEREIGNTY

Institution-owned, domestically deployable

Plaza runs on the institution's own cloud or on-premise footprint. Merchant data, community content, and loyalty ledgers remain under the institution's legal and regulatory custody. No mandatory data export to a third-party platform.

CLAIM 04 — POLICY UNITY

One moderation, refund, and dispute regime

Content moderation rules, merchant onboarding standards, refund mechanics, and dispute escalation all flow from the institution's existing policy lifecycle — not from a vendor's default behaviour. Regulators see one continuous audit trail.

CLAIM 05 — REGULATORY FIT

Mapped to Indonesian financial and content law

Plaza is built against OJK, Bank Indonesia, PDP Law, and Kominfo requirements from the first release — not retrofitted. Merchant onboarding, content moderation, payment rails, and data residency are pre-mapped to applicable regulation.

THE COMBINED EFFECT

A destination the institution owns

The combined claims yield an outcome no single-purpose SDK can reproduce: a destination layer that increases opening frequency and session depth without compromising the trust, sovereignty, and regulatory continuity that justify the institution's app in the first place.

3.3 What Plaza is not

A disciplined product boundary matters. Plaza is not, and does not attempt to be, any of the following:

PLAZA IS NOT…	BECAUSE…
A contact center	Inbound service moments and outbound campaigns belong to Nexilis Reach. Plaza's loyalty campaign engine hands off to Reach for delivery through the trusted messaging fabric.
A secure messaging fabric	Encrypted peer-to-peer, relationship-manager-to-customer, or workforce conversations belong to Nexilis Enclave. Plaza's community layer uses Enclave for any conversation beyond public post-and-comment.
A security or integrity runtime	Device posture, attestation, ZTA enforcement, session hardening, and anti-tamper belong to Nexilis Sentinel. Plaza inherits these primitives; it does not re-implement them.
A payments rail	Plaza integrates with the institution's existing payment infrastructure — QRIS, card scheme, e-wallet, account transfer. It does not issue its own payment credentials.
A standalone marketplace app	Plaza is always a layer inside an existing host application. Greenfield consumer apps are sold as a bundle with Sentinel and Enclave at minimum.
A content production studio	Plaza delivers the surfaces and workflows. Editorial and merchant content remain the responsibility of the institution and its partners.

PRODUCT BOUNDARY DISCIPLINE

Plaza's usefulness compounds precisely because it refuses to absorb adjacent categories. A super-app layer that tries to be its own secure messenger, its own contact center, and its own payments rail reproduces the fragmentation it was meant to solve — only now inside one vendor contract instead of four. The Nexilis portfolio is built to avoid that trap.

Platform *Architecture*

A seven-layer composition that sits above the Nexilis Platform Substrate (identity, policy, telemetry, security) and below the host-app UI.

4.1 The seven layers of Plaza

L7	**Experience Surfaces** Feed, marketplace, storefront, loyalty centre, events, partner offers — all rendered inside the host application	host-native UI / Flutter / native bridge
L6	**Journey & Orchestration** Personalization, segmentation, cross-pillar journeys, experimentation, referral mechanics	journey engine / A·B framework
L5	**Capability Services** Social Commerce · Community · Loyalty · Lifestyle Content — four pillar services with shared primitives	microservice mesh · gRPC / REST
L4	**Engagement Graph** Unified profile, interest graph, merchant graph, content graph, reward ledger — the data spine of Plaza	graph store · event bus · CDP
L3	**Governance & Moderation** Content policy engine, merchant lifecycle, KYB/KYC-M, dispute & refund workflows, regulator reporting hooks	policy lifecycle · case mgmt
L2	**Integration Fabric** Connectors to core banking, payment rails, CRM, ERP, content supply, partner catalogues, regulatory reporting	ISO 20022 · REST · webhooks
L1	**Plaza Runtime** Container, isolation boundaries, configuration, observability, supply-chain integrity	Kubernetes · SBOM · OCI
L0	***Nexilis Platform Substrate*** *Identity, policy, telemetry, and security primitives inherited from Sentinel, Enclave, and Reach — not re-implemented*	*shared across all Nexilis products*

4.2 Architectural principles

COMPOSABILITY BEFORE COMPLETENESS

Every Plaza service exposes a stable gRPC/REST contract. Institutions can disable a pillar, replace a service with an internal equivalent, or extend the platform with bespoke services without modifying the core — a precondition for long-term regulatory defensibility.

IDENTITY IS INHERITED, NEVER RE-ISSUED

Plaza never creates a separate user identity. The host institution's customer identifier, enriched by Sentinel's device binding, is the only identity that flows through the engagement graph. Merchant identity follows the same principle via the institution's KYB process.

POLICY IS EXPRESSED, NOT HARD-CODED

Moderation thresholds, merchant tier rules, refund windows, content category restrictions, and loyalty redemption limits are all expressed as policy artifacts in the institution's existing policy lifecycle — versioned, approvable, auditable, and reversible.

TELEMETRY IS UNIFIED, NEVER SILOED

Every user action, merchant action, content event, and policy decision is emitted to the institution's unified telemetry bus in the same schema used by Sentinel, Enclave, and Reach. Engagement data is a first-class input to risk, fraud, credit, and customer-service decisions.

SOVEREIGNTY IS A DEFAULT, NOT A PREMIUM

Plaza runs in-tenant by default. Institutional data does not leave the institution's regulatory boundary. Multi-tenant SaaS is available only for non-regulated lifestyle deployments.

Capability *Pillars*

The four pillars that constitute Plaza, each with its own capability set but sharing the engagement graph, governance layer, and trust substrate.

5.1 Pillar I — Social Commerce

Social commerce is Plaza's commercial engine. The institution becomes the host of a curated marketplace in which verified merchants — local craft producers, regional food brands, lifestyle partners, financial-adjacent services — operate storefronts inside the institution's app. Transactions settle through the institution's existing payment rails; merchant commissions and take-rates are set by the institution, not by Plaza.

CORE CAPABILITIES

- **Verified merchant storefronts** with institution-controlled KYB/KYC-M, tiered onboarding (individual seller, MSME, enterprise), and regulator-aligned documentation
- **Product catalogue & category governance** with institution-defined taxonomies, prohibited-category lists, and automated compliance screens
- **Integrated checkout** against the institution's native payment stack (QRIS, card, account transfer, e-wallet, installment, BNPL where licensed)
- **Live commerce & video storefront** with native inline streaming, product pinning, interactive pricing, and dispute-grade session recording
- **Promotion engine** supporting merchant-funded, institution-funded, and co-funded campaigns with financial reconciliation built in
- **Fulfilment integration** against institution-approved logistics partners with SLA telemetry feeding the engagement graph
- **Dispute & refund workflow** unified with the institution's existing case management, not a separate vendor system

5.2 Pillar II — Community

Community is the social fabric that turns the app from a tool into a place. It supports customer-generated content, merchant-generated content, and institutional editorial under one moderation regime — with the trust controls that regulated institutions require.

CORE CAPABILITIES

- **Social feed** with institution-controlled ranking policy (chronological, engagement-weighted, or risk-aware hybrid) — never an opaque vendor algorithm

- **User-generated content** with progressive moderation (automated, escalated, human review) and institution-owned appeal workflow
- **Reactions, comments, follows, and saved lists** with privacy controls derived from the institution's PDP obligations
- **Verified-only publishing mode** for regulated institutions that require publishers to be KYB/KYC'd before posting
- **Topic and interest graphs** that inform loyalty campaigns, merchant recommendations, and lifestyle content surfacing
- **Content moderation integration** with the institution's existing trust-and-safety workflow, not an opaque third-party system
- **Crisis-mode controls** that allow the institution to suspend publishing, freeze trending, or redirect traffic during regulatory or reputational events

CONTENT-MODERATION PIPELINE

Automated moderation in Plaza is a named component of the Community pillar, not an opaque black box. The pipeline is structured as three stages operating under institution-controlled policy:

1. **Fast classification** — a lightweight classifier evaluates every post, comment, and media item against the institution's prohibited-category policy (sub-50ms P95 latency). Handles the majority of clearly-in-policy and clearly-out-of-policy content deterministically.
2. **Nuanced evaluation** — ambiguous cases escalate to a language-model-based classifier that evaluates context, intent, and policy edge cases (sub-2-second P95 latency). Confidence scores are recorded for every decision.
3. **Human review** — content below a configurable confidence threshold, or content flagged by user reports, escalates to the institution's trust-and-safety team through the moderator console. Review decisions feed back into classifier retraining with documented provenance.

All moderation models run in-tenant by default, on CPU for the fast classifier and on co-located GPU for the language-model stage. Models are delivered through signed updates via the Plaza release channel; model cards, training-data provenance, evaluation metrics, and known failure modes are published per release. Institutions may substitute their own models at either stage through a documented service boundary. For deployments subject to PP 17/2025 (PP TUNAS), a dedicated child-safety classifier runs in parallel to the fast-classification stage, with hard-block semantics and mandatory escalation paths.

5.3 Pillar III — Loyalty & Rewards

The loyalty pillar converts engagement into commercial return. It is built on a unified reward ledger bound to the institution's primary customer identity — not a parallel account, not a vendor's proprietary identity system.

CORE CAPABILITIES

- **Unified reward ledger** with point accrual, tier progression, redemption, and expiry — fully auditable, double-entry, and reconciliation-ready
- **Tier engine** supporting rule-based, spend-based, frequency-based, and hybrid tier progression with transparent advancement rules
- **Partner redemption network** integrating merchant catalogues, airline/hotel partners, third-party voucher networks, and bill-payment destinations
- **Referral & advocacy mechanics** with fraud-resistant referral codes, cohort tracking, and double-sided reward fulfillment
- **Gamification primitives** (streaks, quests, milestones, limited-time events) expressed through the same policy engine as the rest of the platform
- **Earn-and-burn analytics** showing cost-of-point, breakage rate, redemption velocity, and tier-lift economics in real time
- **Fraud detection** wired into Sentinel's device signals and the institution's existing risk models — loyalty abuse is treated as fraud, not a marketing problem

5.4 Pillar IV — Lifestyle Content

Lifestyle content is the "reason to open the app when there is no transaction." It is the editorial and partnership layer that gives the institution a continuous voice in the customer's daily life — without surrendering that voice to a social platform owned by someone else.

CORE CAPABILITIES

- **Editorial publishing workflow** for institution-authored content (financial literacy, regional travel, cultural events, partner stories)
- **Local events directory** with geo-fenced relevance, RSVP mechanics, and optional ticketing integration
- **Partner offers** supporting co-branded deals, geo-exclusive promotions, and tier-gated access
- **Content recommendation** driven by the engagement graph (interests, merchant affinity, prior reading) — with institution-adjustable ranking
- **Series, collections, and editorial shelves** for curated content journeys ("East Java in Seven Days," "Your Financial Year in Review," etc.)
- **Sponsored content controls** with mandatory disclosure, paid-placement labelling, and regulator-ready separation from organic editorial
- **Accessibility** — WCAG 2.2 AA conformance for Plaza-provided surfaces and components; institution-implemented surfaces inherit the primitives but remain responsible for application-level conformance. Multi-language support (Bahasa Indonesia primary, English secondary), regional dialect awareness.

5.5 Generative-AI posture

Generative-AI capability is integrated across the four pillars rather than offered as a separate product. The posture is consistent: institution-controlled, in-tenant by default, with model provenance documented and audit-trail parity with non-AI actions.

PER-PILLAR CAPABILITIES

- **Social Commerce** — AI-assisted merchant listing generation (title, description, category, translation), visual-search over the merchant catalogue, agentic shopping assistant scoped to the institution's marketplace, automatic compliance screening of merchant content against prohibited-category policy.
- **Community** — the moderation pipeline described in §5.2 is the primary GenAI application; additional capabilities include auto-summarisation of long threads, auto-translation across regional languages, and transparent ranking explanations for user-facing "why am I seeing this" disclosures.
- **Loyalty & Rewards** — personalisation of offer surfaces; anomaly detection on redemption patterns for fraud scoring; natural-language querying of the institution's earn-and-burn analytics by authorised operators.
- **Lifestyle Content** — editorial drafting assistance for the institution's content team (humans retain final authorship); recommendation ranking informed by interest-graph signals; auto-generation of series and collection metadata.

OPERATING POSTURE

- **Deployment** — AI workloads run in-tenant by default, co-located with the Plaza runtime. Managed-cloud model APIs (OpenAI, Anthropic, domestic providers) are available as opt-in substitutes where the institution's policy permits cross-tenant model calls.
- **Model provenance** — every AI model in the trust-critical path is documented with a model card (training data, evaluation metrics, known limitations, update cadence). Model versions are pinned per deployment; model updates follow the signed-release mechanism used for the rest of Plaza.
- **Auditability** — every AI-assisted action emits to the same telemetry bus as non-AI actions, including prompt (redacted for PII), model version, confidence score, and downstream action taken. Regulator-facing audit queries surface AI participation without additional plumbing.
- **Institution control** — per-pillar AI-feature toggles; institution-defined policy on training data use (opt-in by default, never sent to third-party training sets); per-model risk classification under ISO/IEC 42001.
- **Regulatory alignment** — compliance with emerging Indonesian AI-governance guidance (including KBLI 2025 classifications for AI-based activities), OJK sector-specific AI expectations, and the ISO/IEC 42001 AI-management-system framework.

ON RESPONSIBILITY

Plaza delivers AI capabilities as primitives the institution can adopt, configure, or disable pillar-by-pillar. The institution remains the controller of data, the owner of policy, and the accountable party to regulators and customers. Nexilis is the processor and the provider of the substrate; it is not an autonomous actor in the institution's engagement decisions.

Trust Inheritance & Portfolio *Composition*

How Plaza composes with Sentinel, Enclave, and Reach — and why that composition is the single most important technical decision an evaluator will make.

6.1 Composition, not integration

Plaza does not integrate with Sentinel, Enclave, and Reach as external systems. It *composes* with them — inheriting primitives directly from the shared Nexilis Platform Substrate rather than calling them as remote services. The difference matters.

An integrated super-app layer consumes security, messaging, and engagement services through APIs, translating between its own data model and the host institution's. It is functional but fragile: each integration point is a potential failure surface, and every schema upgrade to an underlying product triggers regression testing in the layer above.

A composed super-app layer consumes the same primitives as part of its native runtime. Sentinel's device binding is the same device binding Plaza checks before allowing a high-value merchant transaction. Enclave's key hierarchy is the same key hierarchy Plaza uses to encrypt a merchant's off-book correspondence. Reach's policy engine is the same policy engine that governs a Plaza loyalty campaign. There is no translation, no mismatch, and no shadow data model.

6.2 What Plaza inherits from each sibling product

SOURCE	INHERITED PRIMITIVE	HOW PLAZA USES IT
Sentinel	Device attestation, ZTA session context, integrity signals, anti-tamper runtime	High-value merchant checkouts, loyalty redemption, community moderation actions are gated by the same device posture that gates financial transactions.
Sentinel	Bound identity (customer ↔ device ↔ session)	The engagement graph uses the institution's bound identity directly — no shadow account, no third-party login broker, no fragmentation.
Enclave	End-to-end encryption primitives & key hierarchy	Merchant-to-customer correspondence, high-trust community DMs, and sensitive loyalty notifications are delivered via Enclave — not a public messaging channel.
Enclave	Secure voice/video for transaction escalation	A Plaza merchant dispute that escalates to a video consultation uses the same encrypted fabric as a bank's named-RM conversation.
Reach	Journey engine & campaign orchestration	Plaza loyalty and lifestyle campaigns are authored once and delivered through Reach — not through a parallel campaign runtime. One contact policy, one suppression list, one unsubscribe state.
Reach	Contact centre for merchant and customer support	Merchant onboarding disputes, customer refund escalations, and content-moderation appeals are handled through Reach agents — not a separate Plaza support product.
Platform Substrate	Unified telemetry, policy lifecycle, audit trail	Every Plaza action emits to the same telemetry bus, is governed by the same policy artefacts, and is logged to the same regulator-facing audit trail as Sentinel, Enclave, and Reach.

6.3 Three vertical bundles

BUNDLE 01

Trusted Channel (BFSI)

Sentinel + Enclave + Reach + **Plaza**

The complete BFSI bundle. Plaza converts the banking app into a weekly destination while the rest of the stack ensures regulatory, security, and service continuity.

BUNDLE 02

TrustLink (Gov / Defense)

Sentinel + Enclave

Plaza is explicitly ***outside*** the default TrustLink bundle. Sovereignty-first agencies rarely need a social-commerce surface. Plaza is available as an optional add-on for public-service apps with consumer reach.

BUNDLE 03

Relationship Banking Stack

Sentinel + Enclave

For wealth, private, and priority banking, where the named RM thread is the franchise asset. Plaza is optional; social commerce may complement but is not the core motion.

PORTFOLIO COMPOSITION DISCIPLINE

Plaza is designed to compose with Sentinel at minimum. It is technically installable as a standalone layer on a host app with its own security runtime, but this configuration is not recommended for regulated institutions. The trust inheritance is the primary differentiator; removing it reduces Plaza to a commodity super-app SDK.

6.4 Composition at the code level

"Composition, not integration" is the single claim on which Plaza's architecture rests, and it deserves specificity. The difference from integration is observable at four layers:

LAYER	WHAT "COMPOSITION" MEANS CONCRETELY
Client SDK	Plaza, Sentinel, Enclave, and Reach are delivered as a federated mobile SDK bundle. They share the host- seconds, not through an HTTPS call to a Sentinel service.
Shared libraries	Plaza services import Sentinel's ZTA-evaluation middleware, Enclave's encryption-primitive library, and Re
Service mesh	Server-side, Plaza services and the substrate services run inside the same Kubernetes namespace under
Shared data plane	The policy-decision point, the telemetry bus, and the audit store are single instances across Plaza, Sentine

The practical consequence: a security regression introduced anywhere in the substrate is detected by Plaza's own test suite because Plaza runs against the substrate as a co-located

dependency. A schema change in the engagement graph is visible to Sentinel's session-risk engine on the next deployment, not on the next integration sprint.

> **WHAT COMPOSITION DOES NOT MEAN**
>
> Composition is not elimination of product boundaries. Plaza, Sentinel, Enclave, and Reach remain separately licensable, separately deployable, and separately versioned. An institution can run Sentinel and Enclave without Plaza; an institution can replace Reach's journey engine with an internal equivalent through the service-mesh boundary. Composition constrains how the products interoperate when deployed together — it does not collapse them into a monolith.

6.5 Trust boundaries and threat-model surface

Plaza's production threat model (maintained as a living STRIDE-aligned document, shared under NDA) identifies six trust boundaries, six primary threat-actor classes, and the controls that mitigate them.

TRUST BOUNDARIES

BOUNDARY	WHAT IT SEPARATES	PRIMARY CONTROL
Customer device ↔ host app	User input from application state	Sentinel device attestation; session binding; anti-tamper runtime
Host app ↔ Plaza runtime	Mobile surface from server-side pillar services	mTLS; bound session token; ZTA policy evaluation per request
Plaza runtime ↔ Platform Substrate	Pillar services from identity, policy, telemetry	Intra-cluster mTLS; identity-aware service mesh; policy decision point co-located
Plaza runtime ↔ Merchant surface	Institution data from merchant-operated content and catalogue	KYB gate at onboarding; per-merchant policy envelope; read-only merchant access to institution data
Plaza runtime ↔ Moderator console	Platform operations from privileged admin actions	FIDO2 authentication; PAM integration; just-in-time elevation; session recording; four-eyes on high-impact actions
Plaza runtime ↔ Payment rail / core banking	Engagement surface from money movement	Institution-operated PJP; payment credentials never held by Plaza; settlement reconciliation via institution's ledger of record

THREAT ACTORS AND PRIMARY MITIGATIONS

- **Compromised customer device** — mitigated by Sentinel attestation, device binding, step-up authentication for high-value actions, fraud scoring wired to loyalty ledger.

- **Rogue or compromised merchant** (bust-out, fake catalogue, refund fraud) — mitigated by tiered KYB with ongoing monitoring, sanctions/PEP/adverse-media screening, transaction-velocity anomaly detection, institution-held settlement holdback, merchant-reputation ledger.
- **Malicious UGC author** (harmful content, abuse, minor-targeted content) — mitigated by the content-moderation pipeline described in §5.2, PP TUNAS-aligned age gating, crisis-mode controls, evidence preservation for UU ITE enforcement.
- **Insider at the institution** (operator abuse, policy override) — mitigated by PAM, four-eyes on high-impact admin actions, immutable audit log with cryptographic chaining, session recording of moderator consoles.
- **Supply-chain compromise** (upstream dependency, third-party model, CDN) — mitigated by SBOM generation, signed build artefacts (SLSA Level 3 target), dependency pinning policy, reproducible builds for the trust-critical path, AI-model provenance attestation.
- **Nexilis itself as third-party risk** — mitigated by SOC 2 Type II attestation on Nexilis operations, ISO/IEC 27001 certification, annual third-party penetration test, quarterly vulnerability scan disclosure, contractual incident-disclosure commitment, background-check regime on Nexilis personnel with production access.

AUDIT-TRAIL INTEGRITY

Plaza's regulator-facing audit trail uses append-only storage with cryptographic hash chaining across records, third-party timestamping on daily chain-roots, and WORM-compatible archival. The institution cannot retroactively tamper with its own audit record without detection; Nexilis cannot tamper with the institution's audit record at all.

REWARD-LEDGER INTEGRITY

The unified reward ledger (§5.3) is implemented as a double-entry append-only ledger with per-entry signing, daily reconciliation against the institution's GL, four-eyes approval on manual adjustments, and geo-replicated backup with fifteen-minute RPO on the Growth and Enterprise tiers. Breakage, expiry, and high-value redemption events are logged with identical semantics to settlement events in Sentinel's financial-transaction audit trail.

Regulatory & Compliance *Mapping*

A pre-mapped compliance posture against Indonesian financial, content, data protection, and payment regulation — plus the international frameworks relevant to cross-border and export-ready deployments.

7.1 Indonesian regulatory surface

REGULATOR / INSTRUMENT	SCOPE	PLAZA COMPLIANCE POSTURE
OJK — POJK 11/ POJK.03/2022 Implementation of IT by Commercial Banks	IT governance, risk management, and third-party IT risk for commercial banks. Mandates that primary and disaster-recovery data centres be located within Indonesian territory.	Risk assessments, change management, incident response, and third-party risk artefacts embedded in Plaza deployment. In-tenant and on-premise postures both satisfy the domestic-data-centre obligation; Nexilis-Cloud posture is unavailable to BFSI deployments by design.
OJK — SEOJK 24/ SEOJK.03/2023 Digital Maturity Assessment for Commercial Banks	Digital maturity assessment framework implementing POJK 11/2022.	Plaza deployment artefacts mapped to the five-pillar maturity framework; supports institution self-assessment against the maturity scoring rubric.
OJK — SEOJK 29/ SEOJK.03/2022 Cyber-Resilience and Cybersecurity for Commercial Banks	Cyber-resilience and cybersecurity operating standard implementing POJK 11/2022.	Plaza security operations and SIEM integration conform to the SEOJK 29 control set; inherited from Sentinel's security primitives.
OJK — POJK 22/2023 Consumer and Public Protection in the Financial Services Sector	Consumer and public protection, market-conduct supervision, complaint handling, data/information security obligations. Replaces POJK 6/POJK. 07/2022.	Plaza complaint and dispute workflows are built to POJK 22 standards with regulator-ready reporting templates; merchant and product-information disclosure mechanics satisfy the market-conduct obligations.
OJK — POJK 44/2024 Banking Confidentiality	Confidentiality obligations for depositor and investor customer information; documentation and authorisation mechanics for disclosure.	Plaza surfaces that handle transaction-adjacent data (loyalty accrual tied to spend, merchant payment flows) enforce confidentiality controls; documented disclosure pathways for lawful requests.
OJK — POJK 3/2024 Financial Technology Innovation and Aggregation Services	DFI regime, sandbox mechanics, data-localization obligations for fintech and payment-system aggregation services.	Applicable where the institution operating Plaza is a fintech or payment-aggregation provider; Plaza data-localization posture satisfies the DFI residency obligations.
Bank Indonesia — PBI 23/6/PBI/2021 Payment System Operators	Payment service operation and supervision.	Plaza does not operate its own payment rail; it integrates with the institution's licensed PJP. No PSO obligations triggered at the Plaza layer.
Bank Indonesia — SNAP v1.0	National Open API standard for payment services.	Plaza merchant-payment integration is SNAP v1.0-aligned. Forward compatibility maintained

REGULATOR / INSTRUMENT	SCOPE	PLAZA COMPLIANCE POSTURE
Standar Nasional Open API Pembayaran		across SNAP revisions through the Integration Fabric layer.
UU 27/2022 (UU PDP) Personal Data Protection Law	Consent, data-subject rights, cross-border transfer, breach notification. Extraterritorial effect.	Granular consent capture; in-product rights fulfilment (access, rectification, erasure, portability); data residency by default; breach notification to the Indonesian PDP Authority and affected data subjects within 3×24 hours; cross-border transfer supported via adequacy assessment, appropriate safeguards (standard contractual clauses, binding corporate rules), or explicit consent as the lawful basis.
PP 71/2019 Operation of Electronic Systems and Transactions	Foundational implementing regulation for Electronic System Operators (PSE); data classification, residency, and operational standards.	Plaza deployment aligns with private-scope PSE obligations for the host institution; public-scope PSE obligations supported for government and state-linked deployments.
Kominfo — PM 5/2020 Private-Scope Electronic System Operators	Registration, content moderation, prohibited content, takedown response times.	PSE registration artefacts; content-moderation workflows with takedown response times aligned to the four-hour and twenty-four-hour categories; prohibited-category enforcement.
PP 17/2025 (PP TUNAS) Governance of Electronic Systems for Child Protection	Child-safety obligations on electronic-system operators: age-appropriate design, moderation of minor-directed content, consent mechanics for minors.	Community and Lifestyle Content pillars enforce age-verification gates, age-appropriate ranking and recommendation policy, minor-specific moderation escalation, and parental-consent workflows where applicable. Relevant especially to consumer-platform and lifestyle deployments.
UU 11/2008 (UU ITE) Electronic Information and Transactions, as last amended by UU 1/2024	Electronic information, transactions, content liability, defamation, and harmful content. Most recently amended by Law No 1 of 2024.	Content-liability framework; publisher identification; evidence preservation for regulator and law-enforcement requests; moderator-action auditability.
BSSN — Peraturan BSSN 4/2021 & SNI ISO/IEC 27001	Cyber-security management framework and information-security certification applicable to state-linked deployments.	Plaza runtime and operating procedures mapped to ISO/IEC 27001 controls; SNI ISO/IEC 27001 certification path supported; BSSN cyber-security management framework satisfied for state-linked and sovereign deployments.
DSN-MUI No 86/ DSN-MUI/XII/2012 Hadiah in Raising and	Sharia-compliance framework for incentives, gifts (hadiah), and loyalty	Loyalty pillar supports DSN-MUI 86-aligned hadiah mechanics; merchant category governance supports syariah-only marketplace

REGULATOR / INSTRUMENT	SCOPE	PLAZA COMPLIANCE POSTURE
Distributing Funds by Sharia Financial Institutions	mechanics in Islamic-finance product design.	configurations; sharia-supervisory-board review workflow integrated.

7.2 International framework alignment

For institutions with cross-border operations or export-ready posture:

- **GDPR & UK-GDPR** — data-subject rights and lawful-basis controls interoperate with Indonesian PDP mechanics; Plaza's cross-border-transfer controls satisfy both regimes.
- **PCI DSS v4** — Plaza does not touch primary account numbers; PCI scope is minimised by architecture, not retrofitted.
- **SOC 2 Type II** — Plaza control objectives are pre-aligned for SOC 2 attestation at the platform level.
- **NIST SP 800-207 (Zero Trust)** — every Plaza action evaluates identity, device posture, and contextual risk before permitting the action. Inherited from Sentinel.
- **ISO/IEC 42001 (AI Management)** — Plaza's generative-AI capabilities (see §5.5) are governed by an ISO/IEC 42001-aligned AI management system covering model provenance, risk classification, and lifecycle controls.

7.3 Audit artefacts

Plaza ships with a documented set of regulator-ready artefacts that mirror those used in Sentinel, Enclave, and Reach:

- Policy catalogue (moderation, merchant tier, refund, loyalty redemption, content category, child-safety)
- Change log with formal approval gates
- Data-flow diagrams for every pillar, annotated with lawful basis, data classification, and residency
- Breach-response runbook with regulator-notification templates for the Indonesian PDP Authority, OJK, Bank Indonesia, and BSSN
- Third-party risk register for merchant, content, integration, and AI-model partners
- Quarterly audit evidence bundle (telemetry extracts, policy diffs, access reviews, AI-system inventory)
- Threat model and trust-boundary documentation (see §6.5)

Deployment Models & *Integration*

Three deployment postures, matched to the regulatory, sovereignty, and operational realities of different buyer types.

8.1 Deployment postures

POSTURE 01

In-tenant (Institution Cloud)

Default for BFSI. Plaza runs inside the institution's own cloud tenant (AWS, Azure, GCP, or domestic equivalent). Data, keys, and telemetry remain under the institution's cloud contracts. Nexilis operates under a managed-service agreement.

POSTURE 02

On-premise (Sovereign)

Default for public-sector and state-linked. Plaza runs on the institution's physical data centre with no outbound dependency beyond software update channels. Supports air-gapped variants for defence-adjacent consumer apps.

POSTURE 03

Managed (Nexilis Cloud)

For non-regulated lifestyle deployments. Plaza runs in Nexilis-operated multi-tenant infrastructure with domestic residency guarantees. Available only where the buyer is not subject to financial or public-sector data-localization requirements.

8.2 Integration surface

INTEGRATION POINT	PROTOCOL / STANDARD	TRIGGER
Host application (native)	Native SDK (iOS / Android), Flutter module, web embed	Mandatory
Identity provider	OIDC, SAML 2.0, SCIM 2.0	Mandatory (inherited from Sentinel)
Payment rail	ISO 20022, SNAP, proprietary PJP APIs	Mandatory for Social Commerce pillar
Core banking	REST / gRPC, ISO 20022 messages, institution-specific connectors	Optional (for loyalty tier-linked account products)
CRM / CDP	REST, Kafka event streams, SCIM	Recommended
Merchant management	REST, webhook callbacks	Mandatory for Social Commerce
Logistics partners	REST, partner-specific adapters	Mandatory for physical-goods Social Commerce
Regulatory reporting	Structured export (JSON, XML, CSV); PDF for hard-copy filings	Mandatory
SIEM / Security operations	Syslog, CEF/LEEF, STIX/TAXII	Mandatory
Content supply partners	RSS, REST, proprietary feeds	Optional (Lifestyle Content)

8.3 Implementation cadence

Plaza is designed for phased rollout. A typical BFSI implementation proceeds across four waves over 6 to 9 months:

1. **Wave 1 — Foundation (Weeks 1–10).** Platform install, identity binding, substrate integration, institution admin console, first pillar (typically Loyalty).
2. **Wave 2 — Social Commerce (Weeks 8–18).** Merchant onboarding pipeline, payment rail connection, first merchant cohort live, dispute workflow operational.
3. **Wave 3 — Community & Lifestyle (Weeks 16–26).** Feed launch with institution-authored seed content, editorial pipeline, partner offers integration.
4. **Wave 4 — Optimisation (Weeks 24–36+).** Experimentation framework active, engagement graph tuned, loyalty economics validated, growth-scaling posture in place.

Competitive *Landscape*

Plaza does not compete head-on with any single incumbent, because no incumbent delivers the same composed proposition. It competes, instead, against the decision to bolt together four separate SDKs.

9.1 The adjacent categories

CATEGORY	REPRESENTATIVE INCUMBENTS	WHERE PLAZA DIFFERS
Super-app SDKs	Gojek Platform SDK, Grab Embed, Sea Money Embed	Those SDKs embed the vendor's ecosystem into your app. Plaza embeds ***your*** ecosystem into your app; no vendor brand capture, no upstream data flow.
Marketplace orchestration	Mirakl, Marketplacer, Izberg	Marketplace orchestration platforms deliver social commerce only. Plaza delivers social commerce as one of four pillars, composed with community, loyalty, and content.
Embedded commerce	Salesforce Commerce Cloud mobile, Commercetools, Shopify Hydrogen embed	Embedded commerce platforms assume a retail buyer, not a regulated institution. They lack native KYB, regulator reporting, and policy-lifecycle integration.
Loyalty platforms	Antavo, LoyaltyLion, Comarch, Capillary	Dedicated loyalty platforms deliver one pillar very well. They do not unify with community, commerce, and content under one identity, telemetry, and policy layer.
Community platforms	Discourse, Circle, Bevy, InSided	Community platforms are typically web-first, weak on mobile-native in-app embedding, and built for prosumer brands — not regulated institutions with KYC, AML, and moderation obligations.
In-moment commerce	Rokt, Fast Simon, Bolt	In-moment commerce adds a transaction surface inside the flow of another action. Plaza builds a destination, not a detour.
Consumer-built super-app	Build-your-own using CMS + commerce + loyalty + SDK integration	The default alternative. Plaza's pitch is against this option, not against the named vendors above. The composition, not the pieces, is the product.

9.2 Where Plaza wins

Plaza wins against the "four SDKs stitched together" default in six situations:

1. The institution is a regulated financial, public-sector, or trust-heavy consumer brand that cannot tolerate fragmented identity, policy, and audit trail.
2. The institution is already a Sentinel, Enclave, or Reach customer, and the trust inheritance economics compound the Plaza decision.
3. Domestic data residency and sovereignty are hard requirements (not preferences).
4. The institution values merchant ecosystem ownership — the merchant relationship is a balance-sheet asset, not a SaaS vendor's asset.
5. The institution's competitive threat is losing customer attention to Gojek/Grab/TikTok — not losing a specific product feature.
6. The institution has been burned by a previous engagement/loyalty vendor integration that fragmented the app and is seeking a reset under one platform.

Plaza is not the right fit where the buyer is a retail-first consumer brand seeking a best-of-breed single pillar — loyalty only, marketplace only, or community only. In those cases a dedicated single-pillar vendor will serve the buyer better. The fit for Plaza is platform-level, not feature-level.

> **HOW TO EVALUATE PLAZA**
>
> Plaza is a young category entrant. The single-pillar incumbents have 10+ years of product maturity in their specific pillar. A buyer evaluating Plaza only on loyalty-feature depth against Antavo, or only on marketplace-feature depth against Mirakl, will find Plaza narrower. The correct evaluation is on composition, not depth.

Commercial *Structure*

Three tiers, each matched to an institutional scale and engagement ambition. Pricing is indicative; final commercial terms respect the institution's procurement framework and any Nexilis portfolio composition discount.

TIER 01 — FOUNDATION

Plaza Foundation

For institutions establishing their first destination layer — typically single-pillar launch plus one adjacent.

- Two pillars active (typical: Loyalty + Lifestyle Content)
- Up to 500,000 engaged monthly users
- Up to 500 active merchants (if Social Commerce active)
- In-tenant or on-premise deployment
- Standard moderation policy pack
- Unified admin console
- Single production + single staging environment
- 8×5 support, 4-hour P1 response
- Quarterly policy review

IDR 3.2B – 4.8B / year
Professional services: from IDR 1.8B

TIER 02 — GROWTH

Plaza Growth

For institutions running three or four pillars at scale, with a live merchant ecosystem and growing editorial presence.

- All four pillars active
- Up to 5 million engaged monthly users
- Up to 10,000 active merchants
- Advanced journey & experimentation framework
- Live commerce and video storefront enabled
- Multi-region deployment option
- Custom policy authoring & approval workflows
- 24×7 support, 1-hour P1 response
- Monthly policy review & engagement analytics
- Dedicated solutions architect

IDR 7.5B – 14B / year
Professional services: from IDR 4.5B

TIER 03 — ENTERPRISE

Plaza Enterprise

For national-scale institutions operating destination layers with complex merchant ecosystems and high regulatory load.

- Unlimited engaged monthly users
- Unlimited active merchants
- Dedicated deployment isolation
- Custom pillar extensions
- Sovereign or air-gapped option
- Custom regulator reporting pipelines
- On-site Nexilis embedded team
- 24×7 support, 15-minute P1 response
- Executive quarterly business reviews
- Dedicated reliability engineering

From IDR 18B / year
Professional services: custom scope

10.1 Commercial notes

- **Portfolio composition discount.** Institutions acquiring Plaza alongside Sentinel, Enclave, and Reach receive a compounding discount — typically 15–25% off list at the Growth tier and above — reflecting the lower integration and support cost of a composed stack.
- **Merchant take-rate sharing.** For Social Commerce deployments, Nexilis does not take a cut of merchant transaction value by default. A revenue-share alternative is available on request, typically priced 50–70% below the entry list subscription.
- **Payment rail neutrality.** Plaza commercial terms are payment-rail neutral. The institution's PJP relationships and take-rates pass through unchanged.
- **Regulatory-grade support.** Enterprise tier includes regulator-facing support (BI, OJK, Kominfo) with formal documentation, direct engineering engagement on regulator queries, and joint remediation planning.
- **Indonesian procurement alignment.** Pricing, contract structure, and deliverable definitions align with standard BUMN, BPD, and state-linked procurement frameworks. Kontrak payung and multi-year structures are supported.

Reference *Scenarios*

Three composed scenarios showing how Plaza is deployed against distinct institutional realities. Each scenario represents a composite institutional profile grounded in real Indonesian market conditions; none refers to a specific customer.

11.1 Scenario I — Tier-1 National BFSI

Institution profile. A Tier-1 Indonesian bank with 15–20 million retail mobile-banking customers, average two to three sessions per customer per month, average session duration under two minutes. Active in retail, SME, and priority banking. Runs an existing in-house loyalty program that has become commercially inert.

Engagement ambition. Transform the mobile banking app into a weekly destination layer, with a curated merchant marketplace drawn from the bank's existing SME portfolio. Target outcomes: 4× opening frequency, 5× session duration, 2× cross-product conversion.

Plaza configuration. Plaza Growth tier. All four pillars. Social Commerce opened to 2,400 merchants drawn from the bank's SME book. Community enabled with institution-verified publishers. Loyalty migrated from the legacy engine with tier-mapping. Lifestyle Content editorially produced by the bank's marketing team with two content partners.

Portfolio composition. Sentinel + Enclave + Reach + Plaza. Trusted Channel bundle pricing with portfolio composition discount applied.

11.2 Scenario II — Regional Development Bank (BPD)

Institution profile. A BPD serving a provincial economy with tens of millions of residents, a few million mobile banking customers, strong regional brand identity, and a mandate to serve local MSMEs and cultural commerce.

Engagement ambition. Build a differentiating regional destination layer that national competitors cannot replicate — local events, regional merchant promotions, provincial cultural content, a merchant marketplace drawn from the provincial craft and food ecosystem.

Plaza configuration. Plaza Foundation tier with Growth upgrade path. Social Commerce and Lifestyle Content active at launch; Community and Loyalty added in Wave 2 once merchant ecosystem achieves critical mass. Integration with the province's tourism directory and partner events calendar.

Portfolio composition. Sentinel + Reach + Plaza, with Enclave as a future cross-sell for the bank's priority-banking segment.

11.3 Scenario III — Public-Service Consumer Platform

Institution profile. A national public-service consumer platform with tens of millions of registered users, predominantly utilitarian traffic, limited merchant or commerce activity, strong institutional brand, high regulatory scrutiny.

Engagement ambition. Deepen consumer engagement beyond the core service interaction without compromising the platform's institutional credibility or regulatory posture. Enable partner-service integration (health-adjacent wellness content, financial literacy, public-benefit awareness) and a controlled merchant layer for qualified public and private partners.

Plaza configuration. Plaza Growth tier. Lifestyle Content and Community active as primary pillars. Loyalty in a public-benefit form (incentive mechanics for public-policy goals, not commercial points). Social Commerce restricted to qualified institutional partners.

Portfolio composition. Sentinel + Enclave + Plaza. Reach optional for the consumer-service layer.

“Your app, their gathering place.”

About · Trademarks · Contact

Administrative close.

12.1 About Nexilis

Nexilis is a product portfolio of PT Easysoft Indonesia — a Jakarta-headquartered technology company specializing in trust-native communications and engagement platforms for regulated institutions. The portfolio currently comprises four horizontal products — Sentinel, Enclave, Reach, and Plaza — composed into three vertical bundles: Trusted Channel (BFSI), TrustLink (government and defense), and the Relationship Banking Stack. The trust-critical application layer is built in-house, with no third-party product dependencies on the client-side attestation, encryption, or policy-decision paths. Platform-layer components (operating system, runtime, TLS libraries, orchestration) follow an SBOM-pinned, signed-build discipline with documented vulnerability-response SLAs. This architecture gives Nexilis a clean supply chain, full codebase control at the trust boundary, and natural alignment with Indonesian data sovereignty obligations.

12.2 Document metadata

Document	Nexilis Plaza — Product Brief
Version	1.2
Issued	April 2026
Classification	Confidential — for evaluation use only
Owner	PT Easysoft Indonesia · Product & Strategy
Review cadence	Quarterly

12.3 Trademarks & notices

Mention of regulatory instruments is for orientation; this document is not legal advice. Institutions evaluating Plaza against their specific regulatory posture should engage qualified counsel.

12.4 Contact

Commercial enquiries	plaza@nexilis.io
Partner enquiries	partners@nexilis.io
Security disclosures	security@nexilis.io
Website	nexilis.io
Entity	PT Easysoft Indonesia · Jakarta, Indonesia