THE NEXILIS PLATFORM

NEXILIS

Nexilis *Reach*

CUSTOMER ENGAGEMENT, EMBEDDED

The mobile-native customer engagement platform that unifies contact centre, outbound journeys, surveys, and video service inside the one channel the institution already owns — its own application.

PT EASYSOFT INDONESIA

PRODUCT BRIEF
EDITION 2026.1

01 Overview — *a platform, not a product*

Reach brings the contact centre, the campaign orchestrator, the survey tool, the video KYC booth, and the AI copilot into a single capability — one that lives inside the same application the customer has already authenticated, already trusted, and already opened.

Nexilis Reach is a customer engagement platform built for regulated institutions whose mobile application is their most important channel. It is not a contact-centre product with a mobile add-on, nor an engagement platform that ships notifications to the device. It is an engagement fabric that operates *inside* the institution's own application, inheriting the identity, device posture, and audit guarantees that application has already put in place.

Reach consolidates five categories that most institutions currently buy from five different vendors: inbound contact centre, outbound engagement and campaigns, customer surveys and in-moment feedback, video service and video KYC, and AI-assisted agent tooling. Each of these has a mature global category leader. Reach does not try to beat each leader on their strongest feature. It tries to beat the fragmentation that buying five different leaders inevitably produces.

WHAT REACH IS, IN ONE PARAGRAPH

An embedded engagement platform that replaces the institution's patchwork of CPaaS, CCaaS, CEP, survey, and video providers with a single fabric — designed to run inside the mobile application the institution already ships, under the institution's own identity, telemetry, and consent model. Every customer conversation, whether initiated by the institution or by the customer, ends up in one evidence-grade record.

WHO REACH IS FOR

- **Retail and digital banks** whose customers have already installed the mobile application and whose regulators now require auditable communications for critical journeys.
- **Insurance, multifinance, and wealth managers** where the relationship manager–client conversation is itself a franchise asset and currently runs on WhatsApp.

- **Public service institutions** (social security, tax, public utilities) whose constituent conversations must remain on sovereign-hosted infrastructure.
- **Regulated enterprises** where off-channel communications have already drawn supervisory attention and where a single audit story is worth the migration cost.

THE REACH THESIS

The customer conversation that matters most belongs *inside the application the institution already owns* — not on SMS, not on WhatsApp, not on a contact-centre desktop the customer never sees, and not on an impersonator's spoofed number. Every category Reach occupies has come to run, for one reason or another, outside the institution's trust perimeter — some because they drifted there, some because they were born there.

5 → 1	100%	1 log
VENDOR CATEGORIES CONSOLIDATED INTO ONE FABRIC	IN-APP — NO EXTERNAL NUMBER, NO EXTERNAL URL	ONE EVIDENCE-GRADE RECORD PER CUSTOMER CONVERSATION

WHAT REACH IS NOT

Reach is not a customer relationship management system, a core banking platform, a fraud detection engine, a payment gateway, a loan origination platform, or a mobile application development framework. It integrates with each of these and derives value from being adjacent to them. It does not replace them.

THE SOVEREIGNTY POSTURE

Reach is built by an Indonesian company, under Indonesian law, hosted in Indonesia, engineered in Indonesia. Customer data does not leave the country unless the institution explicitly configures an exception. For institutions subject to PADG 24/2022, POJK digital-banking obligations, and UU 27/2022, this is not a feature; it is a structural fit that no foreign-headquartered incumbent in the competitive landscape can match without material architectural rework. For BUMN and government-owned institutions, the domestic-content (TKDN) posture is explicit and documented.

ON CONCENTRATION RISK

What consolidation to one fabric does — and does not — imply

Reach replaces five vendor relationships with one. The obvious concern is concentration: one vendor, one failure domain, one lock-in. Reach's architecture is designed to keep this

> concern answerable. Every event, consent record, conversation transcript, and journey definition is streamed in real time to the institution's own data lake in standard formats. Reach can be migrated off the same way it is migrated on — progressively, journey by journey. The institution owns its data at all times, and the coexistence integration model means Reach never takes a dependency the institution cannot unwind.

02
The problem Reach addresses

The customer conversation has dispersed. Reach is a response to what that dispersal costs.

The critical conversations between a bank and its customer — fraud rescue, consent capture, dispute resolution, complaint handling, advisory guidance, marketing promises — no longer travel on any single channel the bank fully controls. They run across WhatsApp groups hosted by relationship managers, SMS short codes rented from aggregators, outbound voice campaigns dialled from untraceable GSM lines, Instagram direct messages that impersonate the institution with alarming fidelity, and a contact-centre desktop whose view of the customer begins only when the call connects. No single party sees the complete conversation.

FIVE COSTS OF FRAGMENTATION

Regulatory exposure

Since 2021, off-channel communications enforcement in the United States has produced the largest sustained wave of record-keeping penalties in decades, affecting most of the world's largest financial institutions — investment banks, broker-dealers, and swap dealers. In the United Kingdom, the Financial Conduct Authority has issued supervisory correspondence on off-channel communications and signalled that enforcement is a forward priority; major firms are already restructuring their archival posture in anticipation. Indonesia's POJK 22/2023 on consumer protection and the Personal Data Protection Law (UU 27/2022) set the direction locally — consent must be captured, communications retained, complaints auditable. A WhatsApp thread on a relationship manager's personal phone is none of these.

Fraud and impersonation

When the institution's real contact centre calls from an ordinary GSM number, so do the fraudsters. When the bank markets promotions on Instagram, so do the scam accounts. The customer has no principled basis to distinguish authentic channels from counterfeit ones. The institution has handed this verification burden to the customer — and the customer, understandably, fails it.

Evidence fragmentation

A typical complaint touches the mobile app, the contact centre desktop, an SMS, a call log, and at least one internal email thread. No system stitches these together. When the regulator asks the institution to produce the full communication trail for a single dispute, the answer is typically several days of manual reconstruction — and often an incomplete record.

Learning loss

Every external conversation the institution cannot observe is a lesson the institution cannot learn. The contact centre sees call outcomes but not the app journey that preceded them. The CEP sees campaign clicks but not the service complaint that followed. The institution accumulates the activity but loses the insight.

Vendor sprawl

Five categories, five vendors, five contracts, five integrations, five support teams, five renewal cycles, five security reviews. The institution ends up paying a premium for the privilege of maintaining the seams between systems that were never designed to work together.

> *A conversation that lives outside the application is a conversation the institution cannot audit, protect, learn from, or prove.*

REGULATORY CONTEXT

Why fragmentation is becoming a compliance problem, not just an operational one

In the United States, off-channel communications enforcement has moved from firm-level settlements to individual accountability — supervisors and relationship managers at major broker-dealers have been personally fined. The same pattern has historically preceded equivalent enforcement in other jurisdictions. POJK 22/2023, POJK 6/2022, POJK 11/2022, and the PDP Law give Indonesian supervisors the tools to act when a similar enforcement priority emerges locally.

03 Architecture — *seven layers, one fabric*

Reach is structured as a stack of capabilities, not a collection of products. Each layer operates under the same identity, policy, and telemetry model.

Reach's architecture is deliberately layered. A layered architecture is slower to build than a federated one, but it produces something a federated architecture cannot: a single customer conversation that is coherent across every capability the institution deploys. The seven layers below can be adopted progressively — Foundation tier begins with layers 1 through 3; Enterprise tier runs all seven.

L1

Orchestration Fabric

The substrate beneath every other layer — unified identity (FIDO2/passkey, biometric keys bound to iOS Secure Enclave and Android StrongBox, device attestation via Sentinel), unified policy engine (consent, frequency caps, DLP), a CloudEvents-based unified telemetry schema, and a journey event bus. The canonical customer-conversation model is aligned with BIAN service domains where applicable, with a documented custom extension for engagement-specific events. Every customer action, agent action, and system action becomes a correlated event in one timeline. This is the shared trust substrate that sits beneath every Nexilis product and lets the institution compose capabilities without losing coherence.

L2

Inbound Service — Contact Centre

In-app queue, intelligent routing (skill, language, tier, device posture), agent desktop with live customer journey context, supervisor live monitoring, IVR-to-chat escalation, omnichannel presence (voice, video, chat, in-app), and a full conversation record written back to the orchestration fabric. Voice targets a mean opinion score of 4.0+ on well-connected mobile networks, with Opus as the default codec and packet-loss concealment tuned for Indonesian mobile conditions. The desktop is a web application; the customer experience is entirely in-app.

L3

Outbound Engagement — Campaigns and Journeys

Self-service campaign builder for marketing operations, journey orchestration (triggered, scheduled, behavioural), in-app messaging, push, SMS fallback (when the customer is offline), A/B testing, consent-aware suppression, frequency capping, and partner ecosystem integration. Every outbound touch is logged as a distinct event in the customer's unified timeline.

L4

AI Copilot — Assistant and Agent Assist

Conversational AI (intent, NLU including Bahasa Indonesia), automated resolution for routine queries, agent copilot (draft responses, next-best-action, knowledge retrieval), chatbot-to-human handoff with full context, and an agentic workflow layer for multi-step resolutions. Built on a retrieval-augmented architecture so institutions control their own knowledge base. Inference runs in one of three models depending on deployment: Indonesia-hosted self-managed foundation models for sovereign deployments; the institution's own enterprise LLM contracts where they exist; or a Nexilis-managed inference layer with no cross-border data flow. The institution selects the model; no customer utterance flows to a foreign-hosted API without explicit contractual consent.

L5

Surveys and In-Moment Feedback

NPS, CSAT, CES, post-resolution surveys, journey-triggered feedback, and long-form voice of customer research. Feedback is bound to the specific conversation that produced it — so a low score is always traceable to the agent, the channel, the time of day, and the customer segment that generated it.

L6

Video Service — KYC, Teller, Expert

Embedded video for KYC enrolment (with liveness detection and presentation-attack detection), video teller for tellerless branches, video expert consultation for wealth and insurance, live document review, screen share, and full session recording with hash-chained chain-of-custody metadata. The session opens inside the authenticated app, with no customer-facing URL or dial-in. Signalling and media-relay infrastructure is deployed in the institution's own sovereign environment or in Nexilis-managed Indonesian-hosted infrastructure, depending on the selected hosting model.

L7

Analytics and Evidence

Operational dashboards (queue, agent, journey, campaign), regulatory evidence exports (complaint case, off-channel attestation, consent history), customer journey analytics, and archival retention governed by the policy engine. The audit log is hash-chained and WORM-backed; third-party time-stamping is available as an optional assurance layer. Produces a single audit record per customer, per conversation, per supervisory request.

ARCHITECTURE NOTE

Why layered, not federated

A federated architecture — separate best-of-breed products for each capability — is faster to deploy and often cheaper at year one. It produces, as a byproduct, the fragmentation Reach exists to solve. The layered architecture trades initial simplicity for long-term coherence: the same identity, the same policy, the same telemetry across every capability. By year three, the federated institution is paying its vendors to maintain the seams. The layered institution has no seams to maintain.

RESILIENCE, TENANCY, AND REVOCATION

A platform embedded in a regulated mobile application must answer, before evaluation begins, three operational questions that evaluators routinely press on. Reach's answers are as follows.

Failure posture. Reach is designed to fail to a safe local mode. If the Reach control plane is unreachable, the host app does not block the customer journey; it degrades to a cached-policy path with a signed timestamp, re-syncs when connectivity returns, and preserves a complete record of the offline interval. For journeys where fail-closed is preferred (high-value authorisation, consent capture), the institution configures this explicitly per journey.

Tenancy and isolation. In Nexilis-managed SaaS deployments, tenants are logically isolated at database and schema level, with per-tenant encryption keys; bring-your-own-key (BYOK) is supported via institution-controlled KMS. In private single-tenant and on-premises deployments, isolation is absolute. Tenant-boundary audit evidence is produced on demand.

Revocation and kill-switch. A compromised agent session, tenant connection, or app installation can be revoked from the administrator console; revocation propagates to all sessions within seconds and is logged as a first-class event. The institution retains the revocation authority.

Disaster recovery. Indonesia-hosted deployments include a secondary regional availability zone within-country, with documented RPO and RTO commitments appropriate to each tier. Cross-region failover preserves the audit log without gap.

04
Capability matrix

A reference map of the features Reach delivers, organised by layer and by buyer persona.

LAYER	CAPABILITY	PRIMARY BUYER
L1 Orchestration	Unified identity binding to host app (FIDO2, device attestation via Sentinel)	CISO, Enterprise Architect
L1 Orchestration	Consent lifecycle and preference centre (PDP Law, POJK 22/2023)	Data Protection Officer, Compliance
L1 Orchestration	Unified event bus and telemetry schema	Enterprise Architect, Data Platform
L2 Inbound	In-app contact centre (voice, video, chat) with agent desktop	Head of Contact Centre, CX
L2 Inbound	Intelligent routing (skill, tier, language, device risk)	Contact Centre Ops
L2 Inbound	Supervisor monitoring, QA, workforce management	Contact Centre Ops
L3 Outbound	Self-service campaign builder and journey designer	Head of Marketing, CMO
L3 Outbound	Push, in-app message, SMS fallback, rich notification	CX Ops, Marketing Ops
L3 Outbound	A/B testing, frequency capping, suppression, consent gating	Marketing Ops, Compliance
L3 Outbound	Partner ecosystem promotions with attribution	CMO, Partnership Lead
L4 AI Copilot	Conversational AI with Bahasa Indonesia NLU	CX, Product
L4 AI Copilot	Agent assist (draft, next-best-action, retrieval)	Contact Centre Ops
L4 AI Copilot	Retrieval-augmented generation over institution's own knowledge base	Data Platform, CX
L5 Surveys	NPS / CSAT / CES triggered by journey event	CX, Insights
L5 Surveys	In-moment feedback bound to conversation ID	CX, QA

LAYER	CAPABILITY	PRIMARY BUYER
L6 Video	Embedded video KYC with liveness and document capture	Onboarding, Risk
L6 Video	Video teller and expert consultation with recording	Retail Banking, Wealth
L7 Analytics	Operational dashboards and agent performance analytics	Contact Centre Ops, CX
L7 Analytics	Regulatory evidence exports (complaint, consent, communication trail)	Compliance, Audit

05 Competitive frame

Reach does not compete on per-feature depth against any single category leader. It competes on a different axis entirely — coherence under one identity, inside the institution's own application.

The incumbent engagement landscape is organised by category. An institution that wants what Reach offers must currently buy a CCaaS product, a CEP product, a CPaaS product, a survey product, and a video KYC product — and integrate them. Reach's competitive position is not the best contact centre; it is the only contact centre whose customer conversation continues, uninterrupted, into a campaign, into a survey, into a video expert call, and into a regulatory audit, all under the institution's own identity.

INCUMBENT	CATEGORY	STRUCTURAL LIMITATION	REACH'S ANSWER
Genesys Cloud CX	CCaaS	Desktop-first, heavy to mobile-embed; no device posture; routes to agents but not to device context.	Mobile-native from L2 down; device posture inherited from Sentinel.
NICE CXone	CCaaS	Enterprise but generic; no in-app trust layer; no regulatory-specific conversation evidence.	Evidence-grade log purpose-built for BFSI supervisory questions.
Amazon Connect	CCaaS	Toolkit-oriented; requires custom build; no banking-specific templates; heavy engineering cost.	Pre-built for BFSI journeys; self-service where possible.
Twilio Flex + Engage	CCaaS + CEP	Strong APIs, no consolidated identity across inbound and outbound; no regulatory evidence export.	One identity, one audit, one consent model across both directions.
Braze	CEP	Outbound-only; no contact centre, no voice, no video; no evidence model for supervisory use.	Outbound is one layer of a fabric, not a standalone product.
CleverTap	CEP	Same shape as Braze with stronger APAC presence; mobile-native but engagement-only.	Same coverage plus contact centre, surveys, video KYC, AI copilot.
MoEngage	CEP	Strong in Indonesia but engagement-only; no consolidated service layer.	Engagement is a feature, not a product.
Qualtrics / Medallia	VoC / Surveys	Separate system of record for feedback; not bound to the conversation that produced it.	Feedback is inseparable from the conversation — same event bus.
Jumio / Onfido	Video KYC	Hosted outside the institution's app; recordings live in vendor cloud.	Video inside the app, recording in the institution's storage.
Salesforce Service Cloud	Customer 360 + CCaaS	CRM-first; heavy desktop footprint; mobile-embed is a	Mobile-native; inherits the institution's identity

INCUMBENT	CATEGORY	STRUCTURAL LIMITATION	REACH'S ANSWER
		secondary capability; no in-app trust layer.	rather than imposing its own.
Infobip	CPaaS + CEP	Strong APAC presence; channel-focused; no consolidated contact centre, no video service, no evidence model.	Single fabric across channels with regulator-ready evidence from day one.

The table covers the most-encountered incumbents in Indonesian BFSI engagement procurement. A longer comparative analysis, including Avaya Experience Platform, Sinch, and on-premises Genesys PureConnect, is available under NDA as part of the technical evaluation package.

> *The incumbents are not wrong. They are partial. Reach's claim is that partiality, not product quality, is the limiting constraint of the current architecture.*

A NOTE ON FEATURE DEPTH

Where point solutions may still be the right answer

Reach is built for coherence across the customer conversation, not for maximum feature depth in any single category. Institutions whose strategic constraint is a specific best-of-breed capability — global-scale SMS pricing, longitudinal voice-of-customer research, the deepest workforce management feature set — should evaluate point solutions alongside Reach. For institutions whose strategic constraint is the fragmentation of the conversation itself, Reach is the more defensible architecture.

BUILD, BUY, OR PARTNER

An institution with strong internal engineering can plausibly build its own orchestration layer and keep best-of-breed vendors underneath; an institution with a deep systems-integrator relationship can plausibly ask its SI to assemble the fabric. These are legitimate paths. Reach is the faster path where the institution's strategic constraint is time-to-coherence rather than engineering capacity, and where the regulatory evidence burden is large enough that the cost of assembling the platform from parts exceeds the cost of buying the platform pre-assembled. Where either path is the better answer, Reach will say so during the executive briefing.

ON THE DIRECT-AI ALTERNATIVE

A 2026 evaluator will reasonably ask: why Reach's AI layer rather than a direct integration of OpenAI or another foundation-model provider into the institution's own stack? The honest answer is that the foundation model is the easy part. What Reach contributes above the model is conversation context, coherence with the identity and audit fabric, the retrieval layer over the institution's own knowledge base, the sovereign deployment option, the safety architecture around customer-facing generation, and the evidence retention the regulator will eventually ask about. Institutions whose constraint is raw model capability will still buy foundation-model access directly; institutions whose constraint is regulator-ready agentic service will find Reach's position defensible.

06
Integration model — *coexistence, then consolidation*

Reach is designed to sit beside the institution's existing systems for the duration of the migration, and to absorb them only when the institution chooses.

No BFSI institution with a working contact centre, a working CEP, and a live customer base is going to replace its engagement stack in a single programme. Reach's integration model is built for a two-to-three-year migration in which the institution runs Reach alongside the incumbents, moves journeys one at a time, and retires legacy systems at its own pace.

INTEGRATION SURFACE

SYSTEM	INTEGRATION PATTERN	YEAR-ONE BEHAVIOUR
Core banking	SNAP adapter (BI), REST/SOAP gateway, message queue	Reach reads customer and transaction context; writes nothing to the core.
Existing CCaaS	Coexistence via SIP trunking and agent federation	CCaaS continues for external-initiated calls; Reach owns in-app initiated contact.
Existing CEP	Event bridge on the campaign event bus	CEP continues for email and SMS-broadcast campaigns; Reach owns in-app journeys.
CPaaS (Twilio, Sinch, Vonage)	Fallback delivery channel via provider API	Reach sends via CPaaS only when the customer is offline; usage declines as app engagement rises.
Identity provider (IdP)	OIDC with FIDO2 second factor; device attestation via Sentinel	Reach inherits the institution's existing IdP; no parallel identity.
Complaint / case management	Bidirectional event exchange; case-ID federation	Reach produces the communication trail; case system retains the case-of-record.
Analytics / data lake	Streaming export via Kafka / Kinesis / Pulsar	Every Reach event replicated to the institution's lake; no vendor data lock-in.

DATA RESIDENCY AND SOVEREIGNTY

Reach supports three hosting models: Nexilis-managed SaaS in Indonesia (Kominfo PSTE-compliant, PADG 24/2022-aligned), private single-tenant in the institution's cloud (AWS Jakarta, GCP Jakarta, Azure Indonesia Central), and fully on-premises for institutions with classified data obligations. All three run from a single codebase with model-specific deployment profiles; release cadences, support models, and operational runbooks differ by model and are documented per engagement.

EVENT PLATFORM

Reach runs its internal event bus on Apache Pulsar with CloudEvents-formatted payloads. Events are produced onto the Reach bus and exported, via streaming connector, to the insti-

tution's own event platform (Kafka, Kinesis, Pulsar, or equivalent). The institution owns every event that passes through Reach; exportable, portable, no vendor data lock-in.

07 Operational tooling

What administrators, supervisors, compliance officers, and marketing operators actually see and use.

ADMINISTRATOR CONSOLE

The administrator console is a web application for platform operators: tenant configuration, user and role management, policy authoring, consent template design, retention rules, data subject request handling, and integration management. All actions are themselves audited; the administrator console produces evidence the same way the customer-facing layers do.

AGENT DESKTOP

The agent desktop is purpose-built for in-app conversations. When a customer initiates a service moment, the agent receives the customer's identity, recent journey, device posture, open products, and outstanding issues before the conversation opens. The agent writes a resolution record; the record is the audit trail. There is no separate wrap-up dictation, no separate call-notes field, and no separate system of record to reconcile.

Insider risk is addressed as a first-class concern. Agent sessions are bound to a specific device and a specific shift; sensitive fields (full card number, full identity number, contact details) are masked by default and require just-in-time step-up authentication to reveal; a tamper-evident screen recording of every sensitive action is captured and retained under the same policy as the customer conversation; agent-side DLP prevents copy-out of sensitive content.

CAMPAIGN STUDIO

The campaign studio is a self-service environment for marketing operations. Journeys are designed visually; segments are built against the unified telemetry; consent gates and frequency caps are enforced at design time, not at run time; A/B tests are scoped automatically. Marketing operations can ship a journey without engineering involvement — which, in most institutions, is the single largest blocker today.

SUPERVISOR AND WORKFORCE TOOLS

Supervisors see live queues, agent states, real-time conversation quality indicators, and the standard operational KPIs of a modern contact centre: AHT, FCR, service level, ASA, occu-

pancy, adherence, and shrinkage. Workforce management produces schedules against forecasted volume, honouring agent skills and compliance constraints. For institutions with existing enterprise WFM investments (NICE WFM, Verint, Calabrio), Reach publishes the events those systems need and coexists with them rather than replacing them. Quality review samples conversations across channels uniformly; the sample frame is the unified conversation record, not the channel-specific one. AI-assisted quality review is available in the Enterprise tier.

COMPLIANCE COCKPIT

The compliance cockpit is the interface for Data Protection Officers, complaint handlers, and audit teams. It produces three specific outputs on demand: the complete communication trail for a single customer, the consent history for a specific marketing touch, and the off-channel attestation report that supervisors now expect to receive within days rather than weeks.

OPERATIONAL DISCIPLINE

What the operator does *not* have to do

Reach is designed to remove, not add, operational work. The operator does not reconcile conversation records across systems, does not build consent templates per channel, does not manually export compliance evidence, does not maintain per-channel identity, does not run separate A/B tests for in-app versus push, and does not maintain a separate knowledge base for the chatbot and the agent. Each of these, in a federated architecture, is a standing operational tax.

08 Regulatory alignment

Reach was designed to satisfy the customer-communications and consent obligations of Indonesian financial services regulation and the data protection law, with direct mappings to specific provisions.

REGULATION	RELEVANT REQUIREMENT	REACH CAPABILITY
OJK POJK 11/2022 *Digital Banking Resilience*	Mobile channel integrity, tamper detection, incident response, customer authentication	App-integrity inheritance from Sentinel, single-session audit log across all Reach-owned channels, incident evidence export
OJK POJK 22/2023 *Consumer Protection in Financial Sector*	Consent capture, complaint handling, record retention, responsible marketing	Unified consent lifecycle, evidence-grade complaint trail, retention under policy engine
OJK POJK 6/2022 *Consumer Conduct*	Clear communication, accurate disclosure, complaint resolution timelines	In-app disclosure templates, SLA enforcement on resolution windows
UU 27/2022 (PDP Law)	Lawful basis, consent, data subject rights (to know, access, correct, erase), retention, data residency	Consent lifecycle, subject-request console, retention policy, Indonesia hosting — posture adjusted as Kominfo implementing regulations mature
SEOJK on Digital Banking Risk Management *current instrument*	Audit trail and evidentiary retention for digital channel communications	Single audit log across inbound, outbound, survey, video, and AI interactions
Bank Indonesia SNAP *open banking payment standard*	Secure consumption of SNAP APIs from the mobile channel	SNAP-compatible client adapter with attestation-bound authentication via Sentinel
Bank Indonesia PADG 24/2022 *under PBI 23/6/2021*	Data localization for payment system providers	Indonesia-hosted deployment; data plane, control plane, and archival storage in-country
Kominfo PP 71/2019 (PSTE) *and current implementing instruments*	Data sovereignty for strategic electronic systems	Indonesia-hosted SaaS; institution-hosted deployment supported
US SEC Rule 17a-4 / FINRA 3110 *reference precedent*	Record retention for broker-dealer communications; off-channel enforcement precedent	Evidence-grade archive of every conversation across every channel Reach owns
GDPR (reference)	Lawful basis, consent, right to be forgotten, breach notification	Same consent architecture applies; GDPR posture available for multinational deployment

AVAILABLE UNDER NDA

Detailed control mapping

A detailed control-mapping document, showing each regulatory provision and the specific Reach layer or capability that satisfies it, is available under mutual non-disclosure as part of the technical evaluation package. Institutions with active procurement cycles receive this package promptly on NDA execution.

09 Commercial structure — *three tiers, one platform*

Reach is packaged in three tiers. Each tier is a proper subset of the next — investments made at a lower tier are preserved on upgrade.

Foundation

ESSENTIAL SERVICE · SINGLE JOURNEY

From IDR 2.4 B / year

- L1 Orchestration (identity, consent, telemetry)
- L2 Inbound — in-app contact centre (voice, chat)
- L3 Outbound — push and in-app messaging
- Basic A/B testing and frequency capping
- Regulatory evidence export (complaint, consent)
- Indonesia-hosted SaaS deployment
- Up to 50 agent seats; up to 500k MAU

Growth

FULL ENGAGEMENT · SERVICE AND OUTREACH

From IDR 4.8 B / year

- Everything in Foundation
- L2 Inbound — video, intelligent routing, WFM
- L3 Outbound — journey orchestration, partner ecosystem
- L4 AI Copilot — chatbot, agent assist, Bahasa NLU
- L5 Surveys — NPS, CSAT, in-moment feedback
- SMS fallback via CPaaS provider
- Private single-tenant deployment option
- Up to 200 agent seats; up to 2M MAU

Enterprise

COMPLETE FABRIC · EVERY LAYER

Tailored — typically IDR 8–15 B / year

- Everything in Growth
- L6 Video — embedded KYC, video teller, expert consult
- L7 Analytics — full operational and compliance analytics
- Retrieval-augmented AI over institution's knowledge base
- Agentic workflow automation
- Dedicated compliance cockpit
- On-premises or sovereign cloud deployment
- Unlimited seats; unlimited MAU; priority support

SERVICE LEVELS, SUPPORT, AND IMPLEMENTATION

Foundation includes a 99.9% control-plane availability SLA with business-hours support. Growth includes 99.95% availability with 24×7 support and a dedicated customer success manager. Enterprise includes 99.99% availability on customer-facing integration with priority engineering access and named incident management. Production go-live from contract signature typically lands between three and nine months depending on integration scope; professional services are scoped per engagement and, as an indicative guide, run between twenty and sixty per cent of first-year licence for a typical deployment.

SCALE, CHANNEL, AND MULTINATIONAL DEPLOYMENT

Tier seat and MAU figures are licensing envelopes, not technical ceilings; the platform scales well beyond Enterprise tier ranges and every engagement produces a formally agreed capacity plan. Reach is available directly from Nexilis and through established Indonesian systems integrators; L1 support sits with the integrator where one is engaged, with L2 and L3 at Nexilis. For multinational deployments, pricing is quoted in USD and taxation follows the customer's jurisdiction.

ON PRICING BY ENVELOPE RATHER THAN VOLUME

Reach does not price by message volume; campaign volume scales within the tier envelope rather than producing a usage surprise at month-end. Telecommunications pass-through costs — SMS aggregation, voice termination, video bandwidth — are billed at cost plus a declared margin, on the principle that the institution should not pay the vendor a premium on what the vendor itself pays a carrier. Institutions that prefer usage-based pricing — particularly those running very heavy outbound volumes where vendor cost alignment is the primary concern — can request a usage-linked alternative; the tiered envelope is the default because, for most institutions, it produces more predictable annual planning.

ON ESCAPE VELOCITY AND DATA OWNERSHIP

Every conversation record, event, consent history, and journey definition held in Reach is streamed in real time to the institution's own data lake in standard formats, and is exportable at any time. The institution owns its operational data; there is no vendor data lock-in; Reach can be migrated off the same way it is migrated on — progressively, journey by journey, in the same coexistence mode that allowed migration in.

ON VENDOR VIABILITY

PT Easysoft Indonesia is a focused Indonesian technology company with a single platform codebase and a product family built entirely in-house. Source-code escrow is available for Enterprise deployments; continuity provisions are written into the master agreement on re-

quest. The sovereign-vendor posture is a deliberate strategic choice, not an accident of size: a smaller Indonesian-headquartered engineering organisation, operating close to its regulators and its customers, is able to move on Indonesian BFSI requirements faster than any of the global incumbents in the competitive landscape.

ON REFERENCE CUSTOMERS

Reach is a newly consolidated product assembled from components of the Nexilis platform that have been deployed in production with Indonesian financial services and government institutions since 2023. Anonymised reference narratives covering specific component deployments are provided under NDA during technical evaluation. As named references accrue, they will be shared directly with the relevant evaluation team.

ON SMS FALLBACK AND THE TRUST BOUNDARY

The Reach thesis is that the customer conversation belongs inside the institution's own application. SMS fallback, where included, is not a substitute channel — it is a delivery-of-last-resort for moments when the customer is genuinely offline or has not yet opened the app. Every SMS-delivered touch is accompanied by a signed in-app counterpart that supersedes it the moment the customer reconnects. The fallback exists because no platform can assume 100% of customers are always-on; it is the exception the institution manages actively, not the default architecture.

10 Next steps

How an institution evaluates Reach, from first conversation to production engagement.

STEP 01

Executive briefing

A focused session for CEO, CX leadership, and digital operations, structured around the institution's current engagement architecture and the two or three specific costs of fragmentation most visible to it. No product demonstration; this is a strategic conversation.

Technical evaluation

STEP 02

Architecture review with the institution's engineering, security, and compliance teams. Full layer-by-layer walkthrough, integration mapping against current systems, and regulatory control-mapping under NDA. Typically three to four sessions over two weeks.

STEP 03

Proof of concept

A scoped integration into the institution's mobile application on a single journey — most commonly fraud rescue or complaint handling — for six to ten weeks. Success criteria are agreed in writing before the PoC begins. Findings are addressed before any production engagement.

In Indonesian formal procurement, where the institution issues a Request for Information and a Request for Proposal, the executive briefing, technical evaluation, and proof of concept described here fit naturally into those procurement gates. Nexilis responds to structured procurement on the institution's own timetable.

PT Easysoft Indonesia

Jakarta, Indonesia · nexilis.io

reach@nexilis.io

This document and the product architecture it summarises are the confidential property of PT Easysoft Indonesia. Distribution to parties outside the receiving institution requires written authorisation. Specific architectural details, third-party security assessment summaries, and

regulatory control mappings are provided to qualified institutional evaluators under mutual non-disclosure as part of the technical evaluation package.