

KNOW YOUR CUSTOMER (KYC)

Financial Crimes Compliance

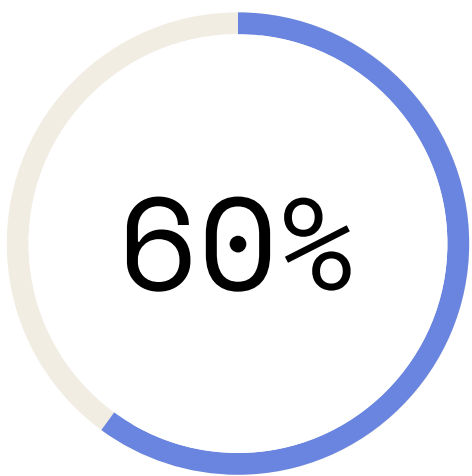
Contents

Navigation – click the Liminal logo to return to this page.

Introduction	2	Market Overview	18	Liminal Index	23	Vendor Overview	35	Appendix	39
Market Overview	3	Market Demands	19	KYC Vendor Product Evaluation	24	Shufti	36	Market Presence Survey Demographics	40
Vendor Landscape	5	Market Challenges	20	Additional factors for consideration	26			Liminal Index Methodology Exceptional, Excellent, Strong Scoring Buckets Definitions	41
Use Case Overview	7	Key Purchasing Criteria for KYC Solutions	21	KYC Vendor Strategy Evaluation	27			Product Capability Definitions	42
Use Case Overview: KYC	8	Future Outlook	22	KYC Vendor Market Presence Evaluation	28			Liminal Index Methodology: Product	48
Liminal’s Use Case Methodology: Key Product Requirements	9			Universe of Vendors	29			Liminal Index Methodology: Strategy	49
KYC Buyer Personas	11			Leadership Thresholds for KYC: Minimum product execution threshold	30			Liminal Index Methodology: Market Presence	50
Chief Operating Officer	12			Leadership Thresholds for KYC: Minimum strategy threshold	31				
Chief Information Officer	13			KYC Leading Vendors	32				
Chief Technology Officer	14			22 Leaders, 82 Evaluated Vendors	33				
Head of Finance	15			Liminal Index Leading Vendors for Know Your Customer in 2026	34				
Head of Risk Management	16								
End-to-End Solutions	17								
								About Liminal	51

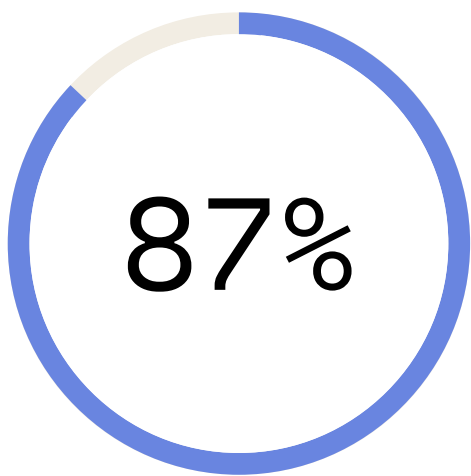
Market Overview

Key Takeaways



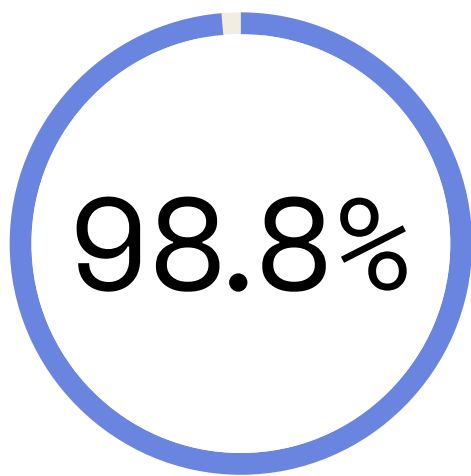
Manual-Review Triggers

Customer-data-vs-document mismatches are the most common manual-review trigger



Platform Consolidation

87% of banks now prefer a one-stop or broad financial crime compliance platform for KYC



Perpetual KYC

98.8% of banks have already deployed, are deploying, or plan to deploy perpetual KYC within the next 12 months

01

Synthetic Identities and Deepfake-Driven Fraud Are Reshaping Identity Risk¹

Identity verification is being tested by AI-generated documents, deepfake media, and synthetic profiles that defeat legacy onboarding controls. Industry fraud indexes have flagged a multi-fold rise in deepfake-related identity attacks over the past two years, and only a minority of banks today operate detection models calibrated to that threat surface. Customer-data-vs-document mismatches (60%) and failed biometric or liveness checks (48%) are the most common manual-review triggers - pointing to exactly the gaps that synthetic-identity actors exploit. As the EU’s Anti-Money Laundering Regulation (AMLR) takes effect and U.S. and UK regulators push for stronger digital-identity standards, institutions must shift from periodic, document-led KYC toward continuous, signal-rich identity assurance.

03

Buyers Are Consolidating Around Platforms, Not Point Solutions¹

Despite years of best-in-class procurement, 87% of banks now prefer a one-stop or broad financial crime compliance platform for KYC, while only 12% favor specialized point providers. The drivers are operational: KYC, BEV, and AML signals must increasingly be reconciled in a unified case-management view to satisfy regulators, reduce false positives, and cut onboarding friction. This mirrors the broader compliance-tech shift visible across the EU’s AMLA framework and the U.S. push toward integrated AML/CFT programs.

02

Perpetual KYC Has Moved From Aspiration to Operating Standard¹

What was an experimental capability two years ago is now the default trajectory: 98.8% of banks have already deployed, are deploying, or plan to deploy perpetual KYC within the next 12 months, and most complete rollout in under six months once started. The shift is driven by event-based triggers, dynamic risk scoring, and the falling cost of orchestrated identity data - and is reinforced by regulators in the UK, EU, and Singapore who increasingly expect ongoing customer due diligence rather than periodic refresh cycles.

¹ Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Market Overview

Current Challenges¹

Manual review remains the operational bottleneck

47% of banks manually review more than a quarter of all KYC verifications, and 62% report each review takes 30 minutes or longer - a structural drag on onboarding capacity.

Synthetic-identity & deepfake defenses lag threats

Document mismatches and failed biometric/liveness checks dominate manual-review triggers, exposing the gap between fraud sophistication and detection maturity.

Multi-framework regulatory pressure

Banks are simultaneously navigating EU AMLDs, FATF guidance, the Bank Secrecy Act, FinCEN CDD rules, and the USA PATRIOT Act - a multi-jurisdictional reality that strains region-specific KYC stacks.

Future Demands¹

Intelligence beats infrastructure

Over the next two years, banks move Analytical Capabilities and Automation furthest up their priority lists - each rising nearly a full rank ahead of where buyers place them today. Compliance Alignment follows. Buyers are paying a premium for what sits on top of the data layer, not the layer itself.

Hygiene is now table stakes

Data Quality and Ease of Implementation drop the most sharply as forward-looking differentiators - not because they matter less, but because any serious vendor in 2026 is assumed to deliver them.

Perpetual KYC replaces the annual review

EU AMLR (effective July 2027) and the UK ECCTA's failure-to-prevent-fraud regime push event-driven re-verification from "nice to have" to baseline expectation.

AI-native risk decisioning becomes the standout capability

Buyers expect identity, device, behavioural, and network signals fused into explainable risk scores defensible to a regulator.

Orchestration over single-vendor lock-in

Banks increasingly favour platforms that let compliance teams swap underlying providers without re-platforming.

Agentic AI targets the manual-review bottleneck directly

58.4% of buyers view agentic identity as one of the technologies that will have the greatest impact on identity and fraud solutions over the next two years - a direct response to the manual-review drag noted above, where nearly half of banks spend 30+ minutes per case. Early implementations aim to support, not replace, the analysts acting on risk scores, with human sign-off remaining the control point for any compliance-relevant decision.

Leading Key Purchasing Criteria (KPC) for KYC Solutions¹

Data Quality

Rated important or very important by 94% of buyers. Assesses the completeness and accuracy of identity, documentation, and risk scoring data. High-quality data supports effective customer classification and regulatory reporting.

Compliance Alignment

Rated important or very important by 94% of buyers. Evaluates compliance with AML, FATF, and jurisdiction-specific identity verification requirements. Built-in controls support consistent adherence and reduce regulatory risk.

Scalability

Rated important or very important by 93% of buyers. Captures the ability to support growing customer bases and evolving regulatory standards. Scalable solutions accommodate high verification volumes and diverse risk tiers across geographies.

¹ Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Vendor Landscape

Liminal's Know Your Customer (KYC) vendor landscape analysis identifies the top [22 leading vendors](#) addressing the complexity of verifying real-world identities in digital environments

Challenges arise from evolving fraud tactics - including synthetic identities, deepfakes, and AI-generated documents - diverse global regulations, and the growing need for accurate, scalable verification across the customer lifecycle.

Vendors within this landscape offer specialized approaches, categorized into three primary groups: **Identity Orchestration & Decisioning Platforms**, **End-to-End KYC & Compliance Platforms**, and **Document Verification & Biometrics Specialists**.

Landscape Analysis

Identity Orchestration & Decisioning Platforms

These vendors operate as meta-layers that orchestrate IDV, fraud, AML, and onboarding decisions across multiple data sources and downstream vendors. Rather than providing every component natively, they unify identity decisioning, case management, and workflow logic into a single configurable layer. Their strength lies in flexibility and breadth - letting compliance teams compose, route, and adapt KYC workflows across geographies, customer segments, and risk policies without rebuilding the underlying stack.

Document Verification & Biometrics Specialists

These vendors specialize in verifying individuals through document capture and biometric analysis. Focused on speed and accuracy, their platforms match IDs with selfies or live scans using anti-spoofing, liveness detection, and deepfake defenses. Their core strength lies in real-time identity verification, often powering high-volume onboarding flows in banking, fintech, gaming, and regulated digital services.

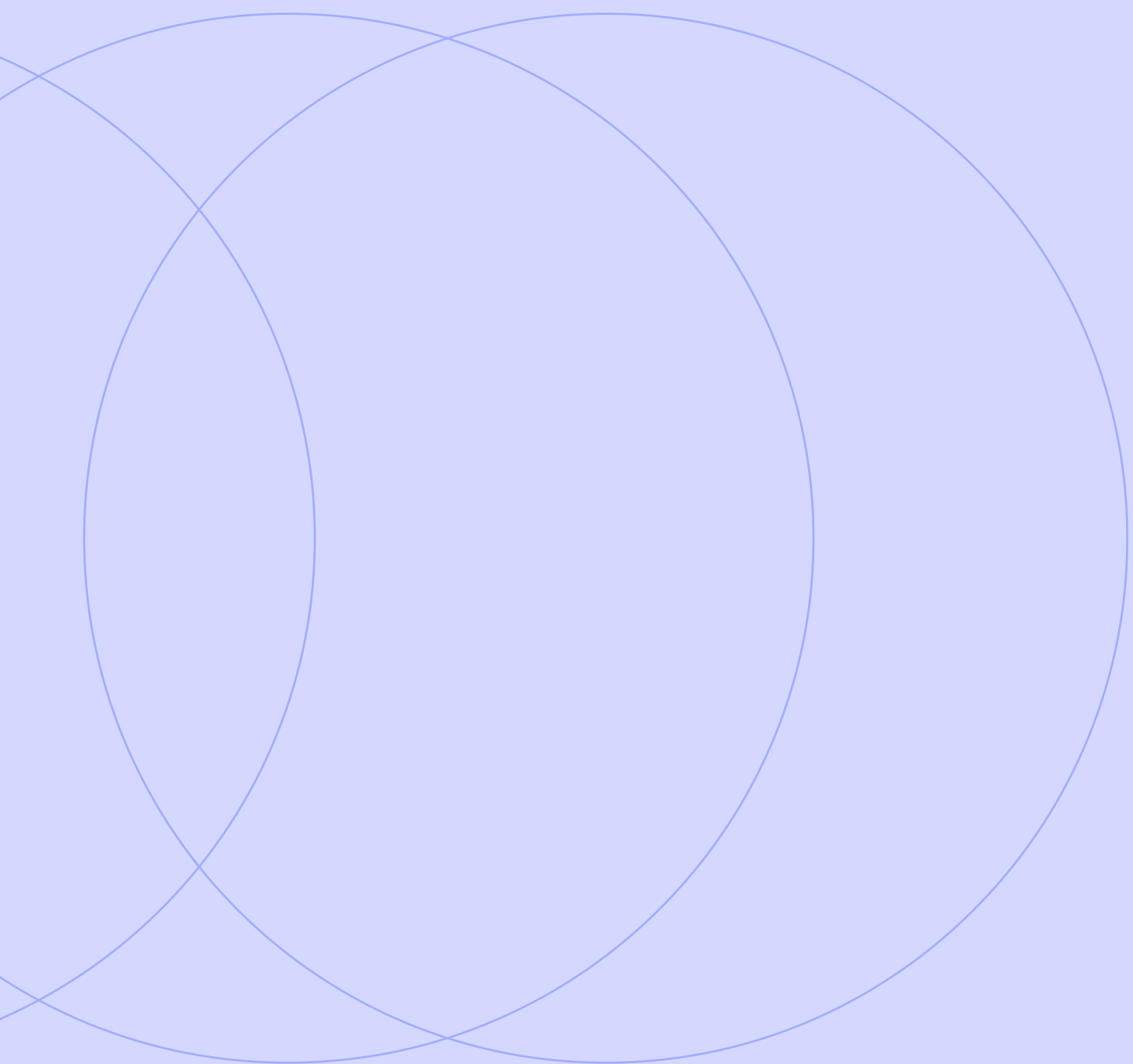
End-to-End KYC & Compliance Platforms

These platforms deliver a full-stack KYC suite - document verification, biometric checks, watchlist screening, risk scoring, and continuous monitoring - built for onboarding and ongoing identity lifecycle management. Geared toward global compliance, they support multiple regulatory frameworks with modular APIs, robust orchestration, and strong automation. Many embed broader fraud and AML capabilities, making them well-suited for scalable, multi-jurisdictional KYC programs.

Vendor Landscape

22 Leading Vendors for KYC





01

Use Case Overview



Use Case Overview: KYC

Know Your Customer Strengthens Financial Crimes Compliance, Mitigates Onboarding Risk, and Powers Trust Across the Customer Lifecycle

Know Your Customer (KYC) is the process by which financial institutions verify the identity of individuals or entities at onboarding and throughout the customer lifecycle to ensure regulatory compliance, assess risk, and prevent fraud or illicit financial activity. It typically combines document verification of government-issued IDs, biometric matching with liveness detection, database screening against sanctions, PEP, and adverse media lists, and behavioral or device intelligence to confirm that an applicant is who they claim to be. Effective KYC programs span the full customer journey - from first-time onboarding through periodic refresh and event-driven re-verification - serving as a foundation for downstream AML monitoring, fraud prevention, and customer due diligence obligations across retail banking, wealth management, lending, and digital financial services.

Regulatory expectations around KYC continue to expand globally, with frameworks such as the EU Anti-Money Laundering Directives, FATF Recommendations, the Bank Secrecy Act, and FinCEN CDD Rules holding financial institutions directly accountable for the integrity of customer identification, beneficial

ownership identification, and ongoing risk assessment. Failures can result in multi-million dollar enforcement actions, consent orders, restrictions on growth, and significant reputational damage. Banks must simultaneously contend with synthetic identity fraud, deepfakes, and AI-generated documents, while delivering low-friction digital onboarding experiences across jurisdictions with diverging documentation standards, data privacy regimes, and risk thresholds.

From a supply perspective, vendors are advancing AI-driven identity verification platforms that combine document authentication, facial biometrics with passive liveness, and real-time database checks to detect increasingly sophisticated identity-based attacks. Perpetual KYC architectures, with continuous monitoring of customer attributes, transaction behavior, and external risk signals, are replacing static periodic reviews. Buyers are also shifting toward orchestrated, platform-based approaches that unify KYC, fraud, sanctions, and case management workflows, reducing vendor fragmentation, accelerating decisioning, and giving compliance teams a single source of truth for customer risk.

KYC is essential for financial crimes compliance, helping financial institutions combat fraud, balance security, and adapt to evolving threats through AI-driven risk detection, biometrics, and automation

Why it matters now

Across 84 banking KYC decision-makers surveyed, 9 in 10 rate improving financial crimes compliance capabilities as critical or important within the next 12-24 months, and roughly half intend to consolidate their compliance tech stack around KYC. Three structural forces - AI-generated fraud techniques, the shift to perpetual KYC, and platform consolidation - are reshaping the buyer roadmap simultaneously, raising the cost of standing still.

A parallel, still-emerging development is the application of agentic AI to support the analysts operating these programs day to day. Rather than replacing manual review, early implementations are aimed at reducing its burden - drawing together identity, transaction, and adverse-media information into a single case view, highlighting likely anomalies, and preparing a recommended disposition for an analyst to confirm.

Regulatory Landscape

Banks operate under a layered regime: EU Anti-Money Laundering Directives (cited by 49% of KYC buyers), FATF Recommendations (47%), the US Bank Secrecy Act (46%), and FinCEN CDD Rules (45%) carry the most weight, with GDPR and the UK Money Laundering Regulations each influencing roughly 30% of respondents. The EU AMLR (effective July 2027), the UK's failure-to-prevent-fraud regime (in force September 2025), and continued FATF guidance on synthetic identity and beneficial ownership will progressively tighten KYC requirements toward continuous verification and AI-defensible decisioning.

Liminal’s Use Case Methodology: Key Product Requirements

To support KYC, vendors must meet [nine core requirements](#), each with varied capabilities to match evolving compliance and customer demands

Nine key requirements outline the product capabilities and technical features needed to solve KYC. According to our survey, the most sought-after capabilities for solving KYC are listed below. For a comprehensive mapping of these capabilities to corresponding technical features, please refer to [Liminal Command](#). The following scale was used to prioritize capabilities:

- **High:** Capabilities essential for solving the use case
- **Medium:** Helpful capabilities
- **Low:** Capabilities that practitioners do not prioritize

● High ◉ Medium ○ Low

1 Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Requirements to Satisfy the Use Case

Perform Identity Verification

Buyer Demand for Product Capability¹

	Active Liveness Detection	●
	Email Verification	●
	Mobile Device Identity Binding	●
	Portable KYC	●
	Video KYC	●
	Identity Verification Orchestration	◉
	Passive Liveness Detection	◉
	Physical Biometrics	◉
	Address Verification	○
	Date of Birth (DOB) Verification	○
	Document Verification	○
	Government Identification Number Verification	○
	Name Verification	○
	Phone Number Verification	○
Perform Customer Due Diligence (CDD)	Active Liveness Detection	●
	Negative News / Adverse Media Monitoring	●
	Sanctions Screening	●
	Consumer Financial Transaction Data Integration	◉
	Government Identification Number Verification	◉
	Passive Liveness Detection	◉
	Politically Exposed Persons (PEP) Screening	◉
	Address Verification	○
	Date of Birth (DOB) Verification	○
	Document Verification	○
	Name Verification	○
Perform Customer Enhanced Due Diligence (EDD)	Negative News / Adverse Media Monitoring	●
	Physically-present Identity Proofing	●
	Sanctions Screening	●
	Consumer Financial Transaction Data Integration	◉
	Government Identification Number Verification	◉
	Document Verification	○
	Name Verification	○
	Politically Exposed Persons (PEP) Screening	○

Liminal’s Use Case Methodology: Key Product Requirements

To support KYC, vendors must meet [nine core requirements](#), each with varied capabilities to match evolving compliance and customer demands

Nine key requirements outline the product capabilities and technical features needed to solve KYC. According to our survey, the most sought-after capabilities for solving KYC are listed below. For a comprehensive mapping of these capabilities to corresponding technical features, please refer to [Liminal Command](#). The following scale was used to prioritize capabilities:

- **High:** Capabilities essential for solving the use case
- **Medium:** Helpful capabilities
- **Low:** Capabilities that practitioners do not prioritize

● High ◉ Medium ○ Low

1 Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Requirements to Satisfy the Use Case

Trigger Step-Up Verification Based on User Risk

Buyer Demand for Product Capability¹

Adaptive Authentication	●
Video KYC	●
Continuous/Perpetual KYC	◉
Document Verification	○
Location Intelligence	●
Behavioral Analytics	○
Behavioral Biometrics	○
Bot Detection	○
Continuous/Perpetual KYC	○
Synthetic Identity Risk Scoring	○
Customer Risk Profiling	●
Unified Customer View Creation	●
Location Intelligence	◉
Mobile Carrier API Access	◉
Behavioral Biometrics	○
Behavioral Analytics	○
Device Intelligence	○
Customer Risk Profiling	●
Location Intelligence	●
Negative News / Adverse Media Monitoring	●
Behavioral Analytics	◉
Behavioral Biometrics	◉
Device Intelligence	◉
AML Risk Scoring	○
Fraud Monitoring	○
Politically Exposed Persons (PEP) Screening	○
Document Retention & Storage	●
AML Audit Trail Management	○
Fraud Alert and Case Management	●
AML Alert and Case Management	○

KYC Buyer Personas

KYC solution buyers span operations, technology, finance, and risk leadership. COOs, CTOs, and CROs are the most represented decision-makers

01

COO – Chief Operating Officer

COOs own the operational performance of KYC programs end-to-end, from onboarding throughput to escalation management. They prioritise automation, accuracy, and operational throughput, and look to remove manual review bottlenecks that slow the bank’s customer journey. Their highest concerns are vendor pricing predictability and the quality of vendor support - they want partners who can scale with the bank without surprising them on cost.

02

CIO – Chief Information Officer

CIOs are the architects of the bank’s data and technology stack. In KYC, they drive decisions on system interoperability, data infrastructure, and enterprise-wide identity strategy. Their priorities centre on integration with core banking platforms, data security, and consolidating vendor sprawl. They are particularly attuned to regulatory data requirements and the organisation’s broader cloud and AI roadmap.

03

CTO – Chief Technology Officer

CTOs evaluate technical fit and engineering depth - API quality, biometrics performance, AI-driven verification, and real-time processing. They are most engaged with detection-side capabilities such as synthetic identity and deepfake controls, and prioritise faster verification times and accuracy improvements. Their frustrations centre on legacy detection gaps as fraud techniques evolve.

04

Head of Finance

Finance leaders own KYC budget allocation and represent one of the largest functional segments among KYC buyers. They balance vendor pricing, total cost of ownership, and ROI against compliance and reputational risk exposure. Their highest sensitivities are data-breach risk and regulatory penalties - both have direct financial consequences. They support consolidation when it can demonstrably lower cost without weakening compliance posture.

05

Head of Risk Management

Risk leaders own the bank’s risk appetite and ensure KYC controls match it. Their top concern is regulatory compliance gaps - by far the strongest switch trigger among Risk respondents in the survey. They prioritise risk scoring accuracy, dynamic AML risk assessment, and continuous monitoring, and they typically champion the move from periodic to perpetual KYC.

01 02 03 04 05

Chief Operating Officer

A Chief Operating Officer streamlining KYC operations improves onboarding throughput, reduces manual review bottlenecks, and enables scalable compliance across geographies

The COO oversees day-to-day operations, ensuring KYC onboarding and compliance workflows run efficiently at scale. As the largest C-suite buyer segment for KYC, COOs prioritise automation, accuracy, and operational throughput, balancing vendor pricing and support quality against the cost of manual review.

Goals

- Automate KYC Onboarding Workflows
- Ensure Compliance Alignment Across Jurisdictions
- Reduce Manual Review Bottlenecks
- Scale Compliance Operations Without Adding Headcount
- Improve Identity Verification Accuracy

Needs

- Easy-to-Deploy Solutions
- Scalable Infrastructure for Peak Volumes
- High-Quality Data Coverage
- Cost-Effective Vendor Options With Predictable Pricing

Frustrations

- High Manual Review Rates
- Vendor Pricing Volatility
- PEP Screening False Positives
- Complex Ownership Structures Slowing Onboarding

Decision Drivers

- Lower Total Cost of Ownership
- Quality of Vendor Support
- Vendor Consolidation Opportunity
- Advanced Technology / AI Capabilities

KPCs

- Pricing / Cost Efficiency
- Ease of Implementation
- Scalability
- Compliance Alignment
- Data Quality & Coverage

01 02 03 04 05

Chief Information Officer

A Chief Information Officer aligning KYC technology with enterprise architecture improves system interoperability, accelerates deployment, and ensures data infrastructure supports compliance at scale

The CIO drives IT strategy, including the selection and integration of compliance technology platforms. CIOs are critical decision-makers for KYC technology architecture, system interoperability, and the bank's broader data infrastructure and AI roadmap

Goals

- Drive Vendor Consolidation Around Fewer, Broader Platforms
- Ensure System Interoperability with Core Banking Infrastructure
- Strengthen Data Quality & Coverage at Enterprise Scale
- Maintain Compliance Alignment with Data Privacy and AI Regulations
- Automate KYC Processes Through Modern Architecture

Needs

- Compliance-Aligned, Architecturally-Sound Solutions
- Scalable Technology Architecture That Reduces Vendor Sprawl
- Strong Data Security and Privacy Controls
- Cost-Effective Vendor Options

Frustrations

- Vendor Sprawl and Integration Drag
- Data Privacy and Localisation Complexity
- Legacy System Limitations
- Inconsistent Vendor Roadmaps

Decision Drivers

- Integration with Existing Infrastructure
- Vendor Consolidation Opportunity
- Compliance with Regulatory Requirements
- Advanced Technology / AI Capabilities

KPCs

- Compliance Alignment
- Ease of Implementation
- Data Quality & Coverage
- Scalability
- Accuracy of Identity Verification

01 02 03 04 05

Chief Technology Officer

A Chief Technology Officer integrating scalable fraud and identity services improves system operability, supports secure customer journeys, and simplifies integration with existing infrastructure

The CTO leads technology engineering and innovation strategy, ensuring KYC solutions are secure, scalable, and future-ready. CTOs evaluate solutions for technical fit, API integration, and alignment with the bank's broader technology roadmap - particularly around AI-driven verification, biometrics, and detection of synthetic identities and deepfakes.

Goals

- Improve Identity Verification Accuracy
- Strengthen Detection of Synthetic Identities and Deepfakes
- Accelerate Verification Speed
- Maintain Compliance Alignment Through Strong Engineering

Needs

- Scalable, Secure Infrastructure
- Robust API Integration Capabilities
- Modern Biometric and AI Detection Tooling
- Strong Internal User Experience

Frustrations

- Detection Gaps for Emerging Fraud Vectors
- Slow Verification Times
- Integration Complexity Across Legacy Systems
- Inconsistent Match Rates

Decision Drivers

- Better Accuracy / Match Rates
- Better Fraud Detection Capabilities
- Faster Verification Times
- Technology / AI Capabilities

KPCs

- Accuracy of Identity Verification
- Analytical Capabilities
- Scalability
- Compliance Alignment
- Internal User Experience

01 02 03 04 05

Head of Finance

A Head of Finance evaluating KYC vendor economics ensures cost-effective compliance, aligns technology spending with risk reduction, and supports defensible budget allocation

The Head of Finance oversees budgeting, cost management, and financial risk for compliance technology investments. As one of the largest functional segments among KYC buyers, this persona controls vendor pricing negotiations, ROI evaluation, and budget allocation - with particular sensitivity to data-breach exposure and regulatory penalty risk.

Goals

- Lower Total Cost of Ownership for KYC Technology
- Strengthen Defences Against Data-Breach Exposure
- Ensure Compliance Alignment to Limit Regulatory Penalties
- Improve Identity Verification Accuracy and ROI

Needs

- Strong Data Quality & Coverage
- Comprehensive Compliance Coverage
- Predictable Vendor Pricing
- Better Integration to Reduce Operational Cost

Frustrations

- Data-Breach Exposure and Reputational Risk
- Regulatory Compliance Gaps Driving Penalty Risk
- Vendor Pricing Volatility
- Manual Processes Inflating Operational Cost

Decision Drivers

- ROI and Total Cost of Ownership
- Better Accuracy / Match Rates
- Compliance with Regulatory Requirements
- Integration with Existing Infrastructure

KPCs

- Pricing / Cost Efficiency
- Compliance Alignment
- Data Quality & Coverage
- Accuracy of Identity Verification
- Ease of Implementation

01 02 03 04 05

Head of Risk Management

A Head of Risk Management integrating fraud and identity analytics reduces operational losses, improves risk visibility, and supports defensible governance decisions

The Head of Risk identifies, evaluates, and mitigates enterprise risk across regulatory, operational, and financial domains. For KYC, this persona is the strongest internal advocate for vendor switching when regulatory exposure surfaces - prioritising risk scoring accuracy, dynamic AML risk assessment, and continuous monitoring.

Goals

- Close Regulatory Compliance Gaps
- Improve Identity Verification Accuracy
- Strengthen Continuous Monitoring & Perpetual KYC
- Strengthen Data Quality & Coverage

Needs

- Advanced Analytical Capabilities
- Automated, Event-Driven KYC Processes
- Strong Compliance Alignment with Evolving Regulations
- Better Integration with FCC and Risk Systems

Frustrations

- Regulatory Compliance Gaps in Vendor Coverage
- Adverse Media Alert Volume
- Complex Ownership Structures
- Cross-Border Compliance Complications

Decision Drivers

- Compliance with Regulatory Requirements
- Effectiveness in Reducing False Positives
- Automation of Core Workflows
- Integration with Existing Infrastructure

KPCs

- Compliance Alignment
- Analytical Capabilities
- Automation of KYC Processes
- Internal User Experience
- Scalability

1 User Initiates Account Creation

The KYC process starts when a user signs up on a financial institution's platform. The system collects personal and device data - including behavioral signals and IP address - to build an initial user profile before verification begins.

2 Risk Assessment

The platform analyzes location, IP history, device info, and behavior to assess risk based on data collected during registration. This early-stage scoring helps determine the level of scrutiny applied in subsequent verification steps.

3 Identity Verification

Users upload government-issued ID documents. The system uses OCR and third-party databases to extract, validate, and confirm the document's authenticity, checking for signs of tampering or forgery.

4 Biometric Verification

Users take a live selfie, which is compared against the submitted ID photo using facial recognition. Liveness detection is applied to confirm the capture is genuine and not a spoofing attempt.

5 Sanctions Screening and Proof of Address

Users provide proof of address, which the platform verifies through document analysis. The system simultaneously screens the user against sanctions lists to identify any compliance red flags.

6 Ongoing Monitoring

After verification, the system continuously tracks user activity, flagging suspicious behavior through real-time anomaly detection. Transaction patterns, login behavior, and device changes are all monitored.

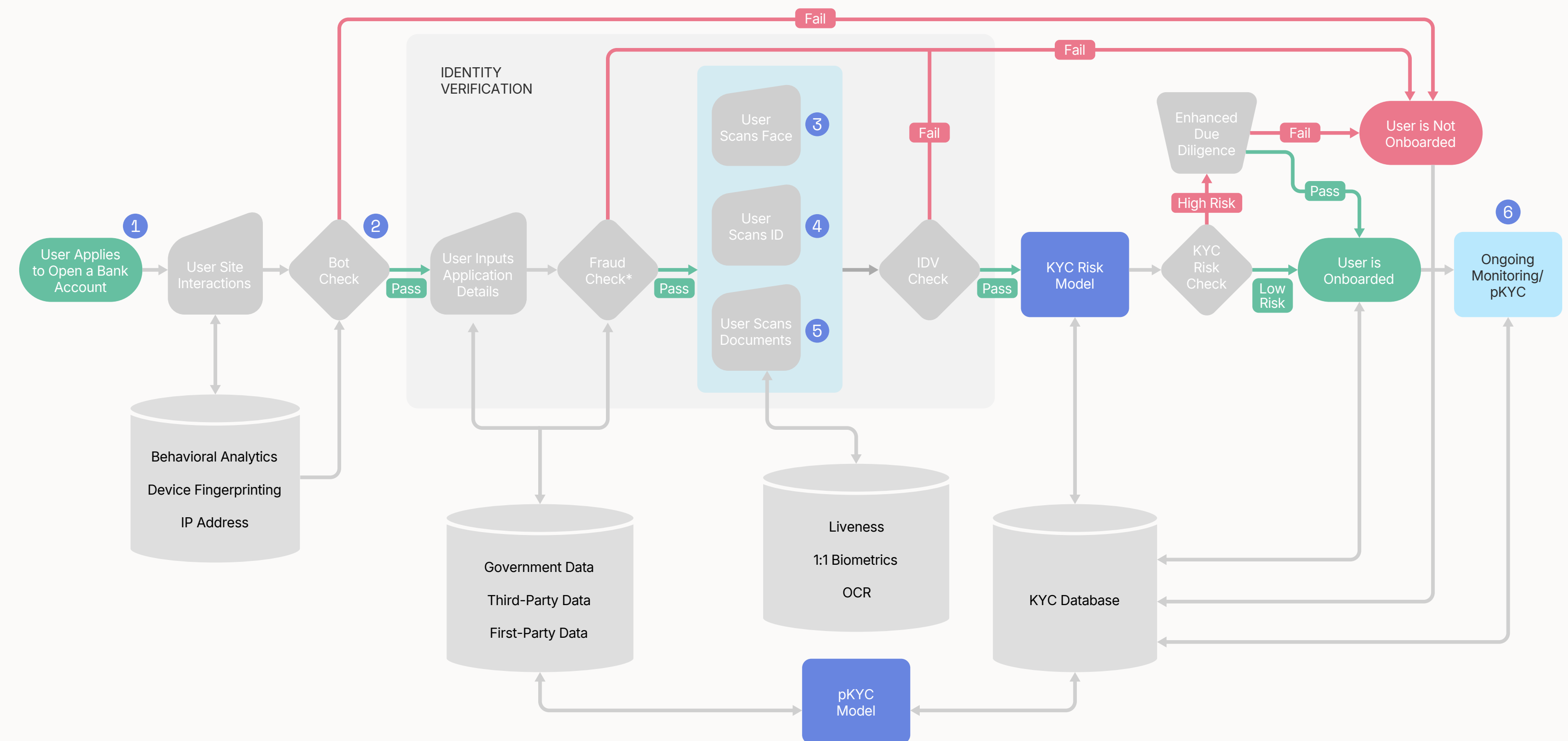
7 Periodic Re-verification

Users are periodically asked to resubmit ID and biometrics to ensure their information remains accurate and current. This supports ongoing regulatory compliance throughout the customer lifecycle.

8 Reporting and Compliance

The platform logs all KYC steps and anomalies in structured reports that support regulatory audits and compliance checks, providing a clear audit trail for examiners.

KYC solutions guarantee compliance, mitigate fraud, and deliver a seamless user experience throughout the customer journey



* Fraud checks are commonly incorporated into KYC workflows, but are not required in many geographies.

02

Market Overview

Market Demands

KYC Market Shifts Toward Accuracy, Perpetual Monitoring, and Integrated Platforms

Buyers are prioritising better identity verification accuracy and continuous monitoring, while consolidating onto end-to-end platforms equipped to handle synthetic identity and deepfake threats.

01

Accuracy is the #1 capability buyers want next

Better identity verification accuracy and reduced false positives ranks as the top single improvement banks would prioritise - well ahead of any other criterion. As AI-generated identity threats proliferate, accuracy has shifted from a hygiene factor to a defensive necessity.

02

Perpetual KYC has crossed from concept to plan

Nearly all surveyed banks (around 99%) have deployed, are deploying, or plan to deploy pKYC within the next 12 months, and high or medium demand for continuous KYC sits near three-quarters of buyers. The EU AMLR (effective July 2027) and the UK's failure-to-prevent-fraud regime (in force September 2025) reinforce the move from static annual reviews to event-driven verification.

03

Buyers want platforms, not point tools

A clear majority of banks now prefer a one-stop or near-one-stop FCC platform over best-of-breed point products. Consolidation intent is real: roughly half of buyers say they intend to reduce vendor count.

04

Behavioural and synthetic-identity signals are now table stakes

Around two-thirds of buyers cite synthetic-identity detection as a requirement, and an even higher share require behavioural anomaly detection - a direct response to the rise of AI-generated fraud techniques flagged in recent FATF and FinCEN advisories.

05

Agentic identity is already on buyers' radar

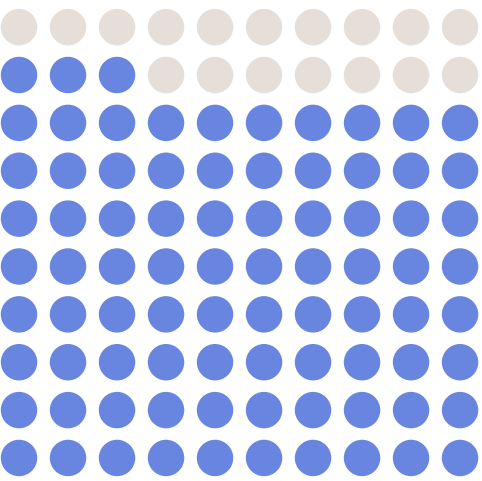
58.4% of buyers already view agentic identity as one of the technologies expected to have the greatest impact on identity and fraud solutions over the next two years - a figure that puts agentic capability on a similar footing to synthetic-identity detection as a forward-looking priority. As with pKYC in its early days, buyer expectation here is currently running ahead of widespread production deployment.

1 Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Market Challenges

Manual Review, Vendor Fragmentation, and AI-Driven Fraud Slow KYC Automation

Manual workloads remain heavy, vendor stacks are expanding, and AI-generated fraud is outpacing legacy detection - creating the central bottlenecks to KYC effectiveness.



83%

of banks review more than 10% of KYC cases manually, with most teams spending 30+ minutes per case

Manual review remains the bottleneck

More than 8 in 10 banks (83%) review more than 10% of KYC cases manually, with most teams spending 30+ minutes per case. Data-document mismatches drive the majority of escalations, with high-risk profiles and failed biometrics rounding out the top three triggers. Agentic AI is emerging as a concrete way to ease this bottleneck, assisting - not replacing - analysts by assembling case data and flagging anomalies for review, provided human oversight, audit trails, and governance keep pace.

Vendor sprawl is creeping back

The share of banks running four or more KYC vendors has roughly doubled year-over-year. Capability gaps and geographic coverage are the most-cited reasons, with redundancy a clear secondary irritant.

AI-generated fraud is outpacing legacy controls

Two-thirds of buyers now treat synthetic-identity detection as a hard requirement, but most banks rate their existing detection stack as only partially equipped to handle synthetic identities and deepfakes. This capability gap will define the 2026-2027 vendor selection cycle.

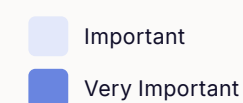
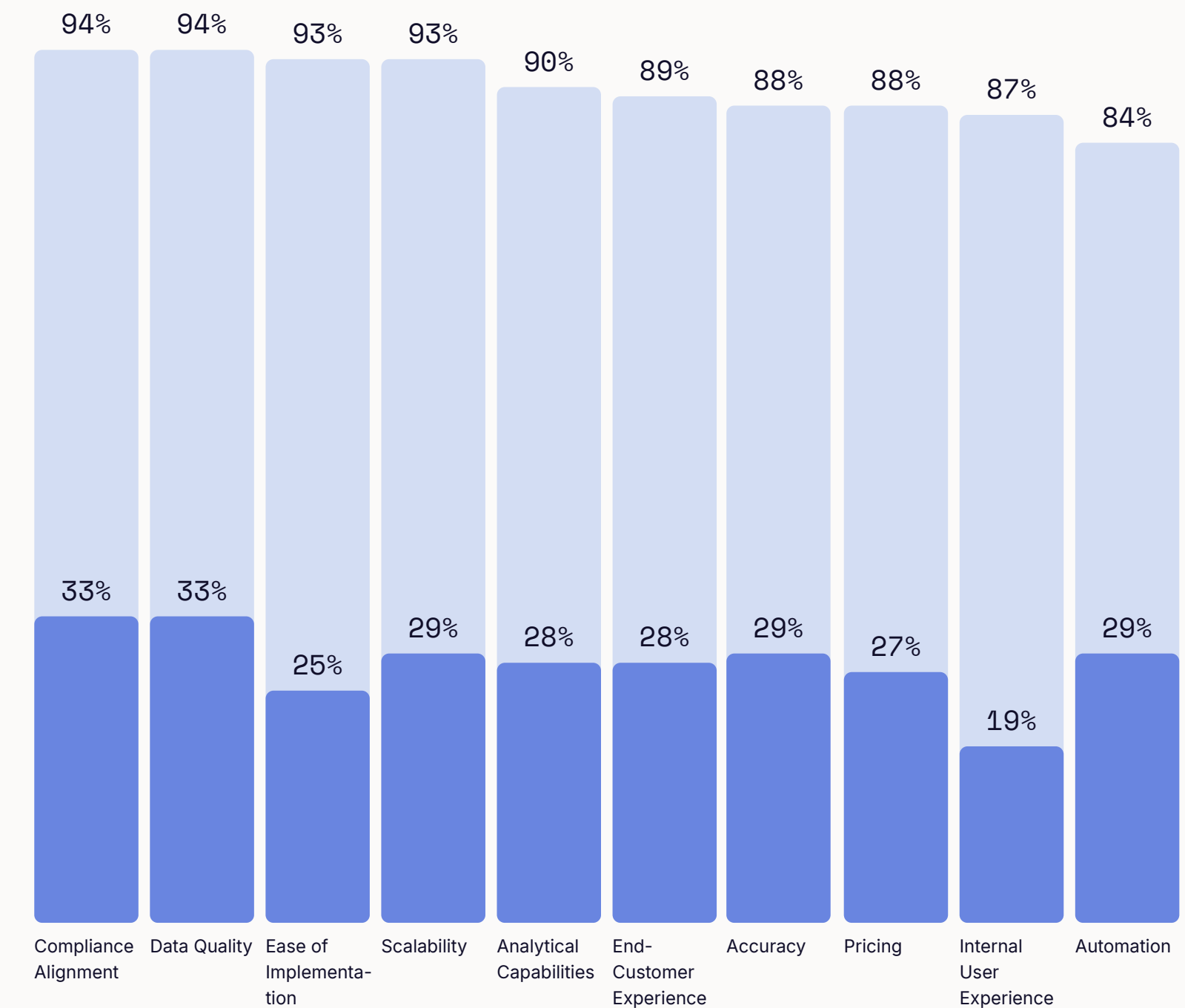
1. Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Key Purchasing Criteria for KYC Solutions¹

KYC practitioners rank compliance alignment and data quality as the top purchasing criteria, followed by scalability and ease of implementation, with analytical capabilities emerging as a rising future priority

¹ Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Buyer Perception of Key Purchasing Criteria

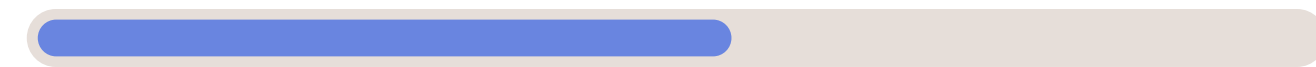


Future Outlook

KYC Moves Toward Perpetual Monitoring, Analytical Differentiation, and Platform Consolidation

Analytics and automation will define the next purchasing cycle, perpetual KYC becomes the default operating model, and cost pressure accelerates the shift to fewer, broader providers.

55%



Vendor Switching

55% of banks rate KYC vendor switching as likely in the next 12 months, and a similar share plan to consolidate

Analytics and automation overtake hygiene as the differentiators

Asked to rank purchasing criteria for the next two years, banks elevate analytical capabilities and automation the most, while data quality and ease-of-implementation recede - not because they matter less, but because they're now assumed of any credible vendor.

Platform consolidation accelerates under cost pressure

KYC budgets are growing at a faster rate than vendor pricing (+5.5% vs +4.8%), but sustained vendor price increases of 4–5% annually are sustaining consolidation pressure as compliance programs seek efficiency gains. More than half of banks (55%) rate KYC vendor switching as likely in the next 12 months, and a similar share plan to consolidate.

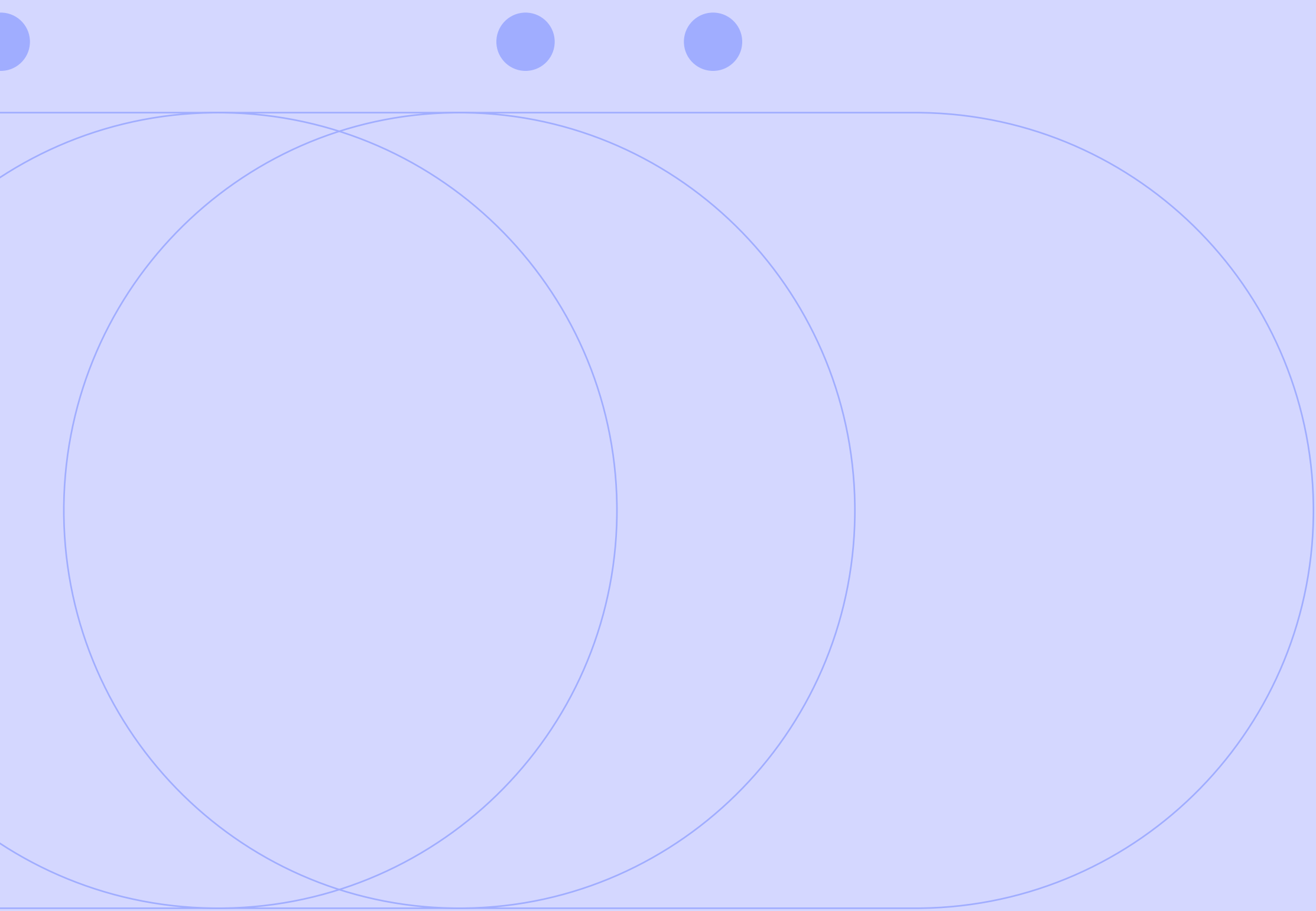
pKYC becomes the default operating model

With nearly all surveyed banks (~99%) committed to pKYC within 12 months and the EU AMLR taking effect in mid-2027, perpetual KYC will move from differentiator to baseline expectation by the end of next year.

Orchestration replaces single-vendor lock-in

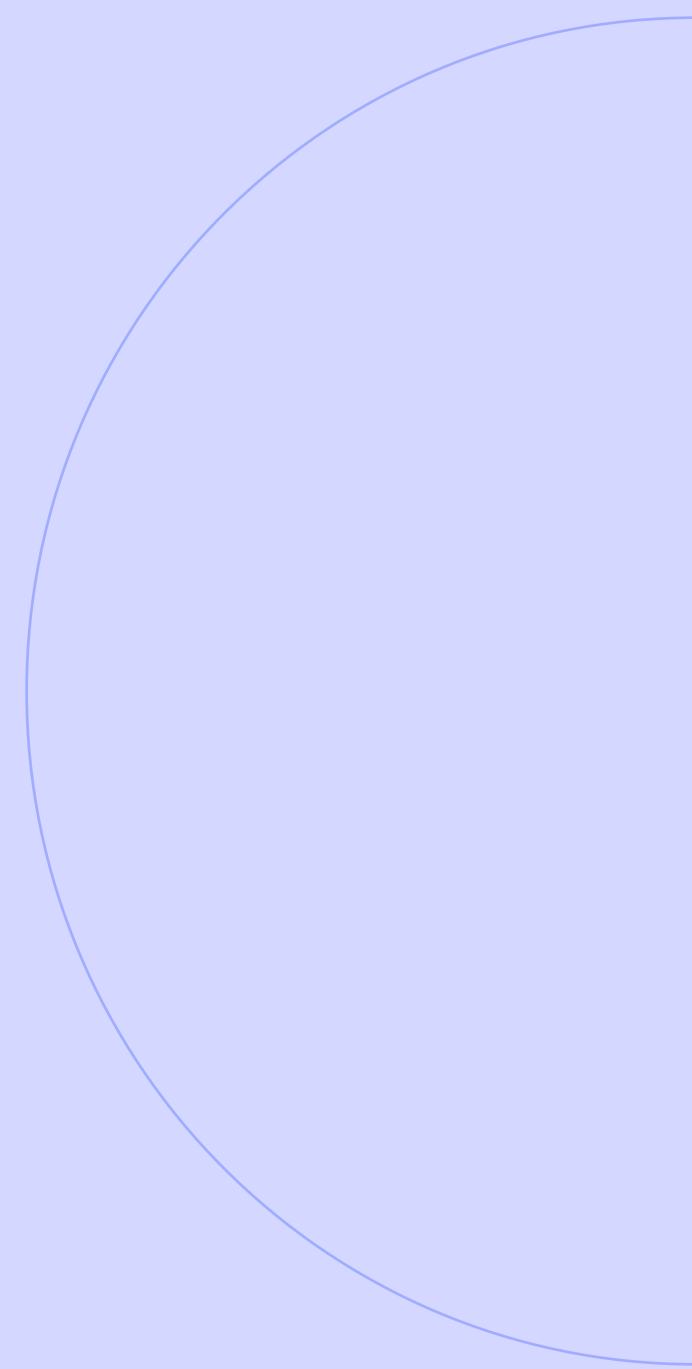
Buyers increasingly favour platforms that allow underlying providers to be swapped without re-platforming - a structural response to the vendor concentration risk and capability churn visible in the survey.

1. Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)



03

Liminal Index



KYC Vendor Product Evaluation

Vendor products were evaluated based on their coverage of product capabilities and performance against top solution purchasing criteria

● High ● Medium ○ Low

1 Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Requirements to Satisfy the Use Case

Perform Identity Verification

Buyer Demand for Product Capability¹

	Active Liveness Detection	●
	Email Verification	●
	Mobile Device Identity Binding	●
	Portable KYC	●
	Video KYC	●
	Identity Verification Orchestration	●
	Passive Liveness Detection	●
	Physical Biometrics	●
	Address Verification	○
	Date of Birth (DOB) Verification	○
	Document Verification	○
	Government Identification Number Verification	○
	Name Verification	○
	Phone Number Verification	○
Perform Customer Due Diligence (CDD)	Active Liveness Detection	●
	Negative News / Adverse Media Monitoring	●
	Sanctions Screening	●
	Consumer Financial Transaction Data Integration	●
	Government Identification Number Verification	●
	Passive Liveness Detection	●
	Politically Exposed Persons (PEP) Screening	●
	Address Verification	○
	Date of Birth (DOB) Verification	○
	Document Verification	○
	Name Verification	○
Perform Customer Enhanced Due Diligence (EDD)	Negative News / Adverse Media Monitoring	●
	Physically-present Identity Proofing	●
	Sanctions Screening	●
	Consumer Financial Transaction Data Integration	●
	Government Identification Number Verification	●
	Document Verification	○
	Name Verification	○
	Politically Exposed Persons (PEP) Screening	○

KYC Vendor Product Evaluation

Vendor products were evaluated based on their coverage of product capabilities and performance against top solution purchasing criteria

● High ● Medium ○ Low

1 Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Requirements to Satisfy the Use Case

Trigger Step-Up Verification Based on User Risk

Detect Synthetic or Manipulated Identities

Detect Anomalous Behavioral Activity for Fraud Threats

Generate a Dynamic User AML Risk Score

Document an Audit Trail

Manage Investigations and Case Workflows

Buyer Demand for Product Capability¹

Adaptive Authentication

Video KYC

Continuous/Perpetual KYC

Document Verification

Location Intelligence

Behavioral Analytics

Behavioral Biometrics

Bot Detection

Continuous/Perpetual KYC

Synthetic Identity Risk Scoring

Customer Risk Profiling

Unified Customer View Creation

Location Intelligence

Mobile Carrier API Access

Behavioral Biometrics

Behavioral Analytics

Device Intelligence

Customer Risk Profiling

Location Intelligence

Negative News / Adverse Media Monitoring

Behavioral Analytics

Behavioral Biometrics

Device Intelligence

AML Risk Scoring

Fraud Monitoring

Politically Exposed Persons (PEP) Screening

Document Retention & Storage

AML Audit Trail Management

Fraud Alert and Case Management

AML Alert and Case Management

KYC Vendor Product Evaluation

Additional factors for consideration

Additional Factors for Consideration

Identity Verification Accuracy	Ability to accurately verify customer identities through document authentication, biometric matching, and data cross-referencing while minimizing false positives and false negatives - the foundational requirement for KYC compliance.
Synthetic Identity & Deepfake Detection	Ability to detect AI-generated fraudulent identities including deepfakes, synthetic identities, and presentation attacks - an emerging critical capability as AI-driven fraud increases in sophistication and volume.
Data Quality & Coverage	Breadth and depth of identity data sources, document coverage, and global registry access for comprehensive verification - ensuring high match rates across diverse populations and geographies. Includes passive behavioral biometric signals and device intelligence as emerging data layers that strengthen fraud detection during onboarding without adding friction.
Screening & Watchlist Capabilities	Depth of sanctions, PEP, adverse media, and watchlist screening with configurable matching rules, fuzzy matching, and real-time updates - enabling precise risk assessment during onboarding and ongoing monitoring.
Risk Scoring & Decisioning	Integrated risk assessment and automated decisioning capabilities that contextualize identity signals, behavioral data, and compliance requirements into actionable risk scores. Model explainability and governance are now regulatory expectations for AI-based scoring. Includes agentic AI capabilities for autonomous case remediation and exception handling in complex or escalated KYC reviews.
Ease of Implementation & Deployment	How quickly and simply KYC verification can be deployed, integrated into customer onboarding flows, and producing results. Includes verification processing time and coverage expansion metrics as operational benchmarks.
Compliance Alignment & Audit Controls	Built-in regulatory compliance frameworks, automated audit trails, and jurisdiction-specific controls. Must align with evolving EU AMLR/AMLA standards, FATF requirements, and outcome-based supervision trends emphasizing board-level accountability.
Buyer Satisfaction	The extent of buyer satisfaction with the vendor’s KYC solution as measured by independent review platforms, analyst recognition, and customer advocacy metrics.

KYC Vendor Strategy Evaluation

KYC vendor strategies were assessed based on the [top buyer purchasing priorities](#) for the coming years

01 Automation & Orchestration

Capability for KYC operations to run without human intervention - automated identity verification, risk decisioning, document processing, and workflow orchestration. Includes straight-through processing rates and manual review reduction as key operational efficiency metrics.

02 Continuous Monitoring & Perpetual KYC

Ongoing, event-driven re-verification of customer identity and risk - moving beyond periodic reviews to real-time detection of changes in PII, risk signals, adverse media, and sanctions status. pKYC is becoming the reference model requiring upgraded data pipelines, triggers, and governance.

03 Global Coverage Strategy

Ability to verify identities across jurisdictions with multi-country document support, local data source access, and region-specific regulatory alignment - critical for organizations with cross-border customer bases.

04 Product Integration & Ecosystem

Ability to integrate natively with core banking, CRM, case management, and third-party data providers. Emphasis on interoperable APIs, common data schemas, and integration hooks - not just all-in-one suites. Cross-functional integration with fraud and credit systems is increasingly expected.

05 Internal User Experience

How intuitive and effective tools are for compliance analysts, operations teams, and developers to adopt, use, and derive value in daily KYC workflows - enabling faster onboarding, case review, and risk triage.

06 Pricing & Commercial Model

Transparent, scalable pricing that delivers ROI through efficient licensing, reduced manual review costs, and flexible deployment - budget alignment with value delivered across verification volumes.

07 Platform vs. Point Solution Positioning

Strategic approach to market positioning - whether the vendor offers a consolidated platform spanning multiple FCC use cases or specializes deeply in KYC with clean integration to other systems. Buyers increasingly favor platform consolidation.

08 FCC-Fraud Convergence Strategy

Strategic approach to converging financial crime compliance with fraud prevention and cyber risk - reflecting the market shift toward integrated intelligence and case-management functions across historically siloed compliance and fraud teams.

09 Agentic AI in Production

The extent to which the vendor has moved beyond AI-assisted decisioning into deployed agentic workflows for KYC operations - autonomous agents that conduct CDD/EDD reviews, periodic refresh, and escalation handling end-to-end at named regulated customers, with transparent

human-in-the-loop controls. As of 2026, this is the clearest forward-looking discriminator at the top of the KYC market: most vendors market "AI" but only a handful operate agents in production with quantified analyst-time savings and documented governance.

KYC Vendor Market Presence Evaluation

The market presence of KYC vendors was evaluated based on company size and growth, market leadership perception, funding history, digital footprint and media coverage



Company Size

This metric reflects a vendor’s total workforce, indicating operational capacity and resources. Larger vendors offer greater infrastructure, regulatory expertise, and customer support. In KYC, this ensures stability, scalability, and strong compliance while making them well-equipped to meet evolving security and verification demands.



Employee Growth (YoY)

Employee growth tracks a vendor’s workforce expansion, signaling investment in innovation, compliance, and customer support. Consistent growth suggests increasing demand and ongoing improvements in identity verification solutions. Buyers benefit from vendors scaling their teams, ensuring adaptability, enhanced features, and reliable long-term service.



Market Leadership Perception

This metric reflects how buyers perceive a vendor’s leadership in KYC, measuring its innovation, reliability, and influence. A strong perception boosts trust, signaling advanced solutions and compliance. Market leaders drive best practices, making buyers more likely to choose their offerings over competitors.



Funding History

This criterion assesses the vendor’s financial backing, including the volume, frequency, and sources of external investment. A strong funding record demonstrates market confidence, provides resources for innovation and expansion, and supports long-term stability within the identity verification ecosystem.



Digital Footprint

This criterion evaluates the extent and quality of a vendor’s digital presence, including its website performance, social engagement, and online visibility. A strong digital footprint indicates active market communication, accessibility to buyers, and transparency about product capabilities and compliance posture.



Media Coverage

This criterion measures the volume and sentiment of media mentions related to the vendor across industry and mainstream sources. Consistent, positive coverage reflects market relevance, public trust, and influence, while high visibility across credible outlets can signal leadership and authority in the identity verification space.

Universe of Vendors

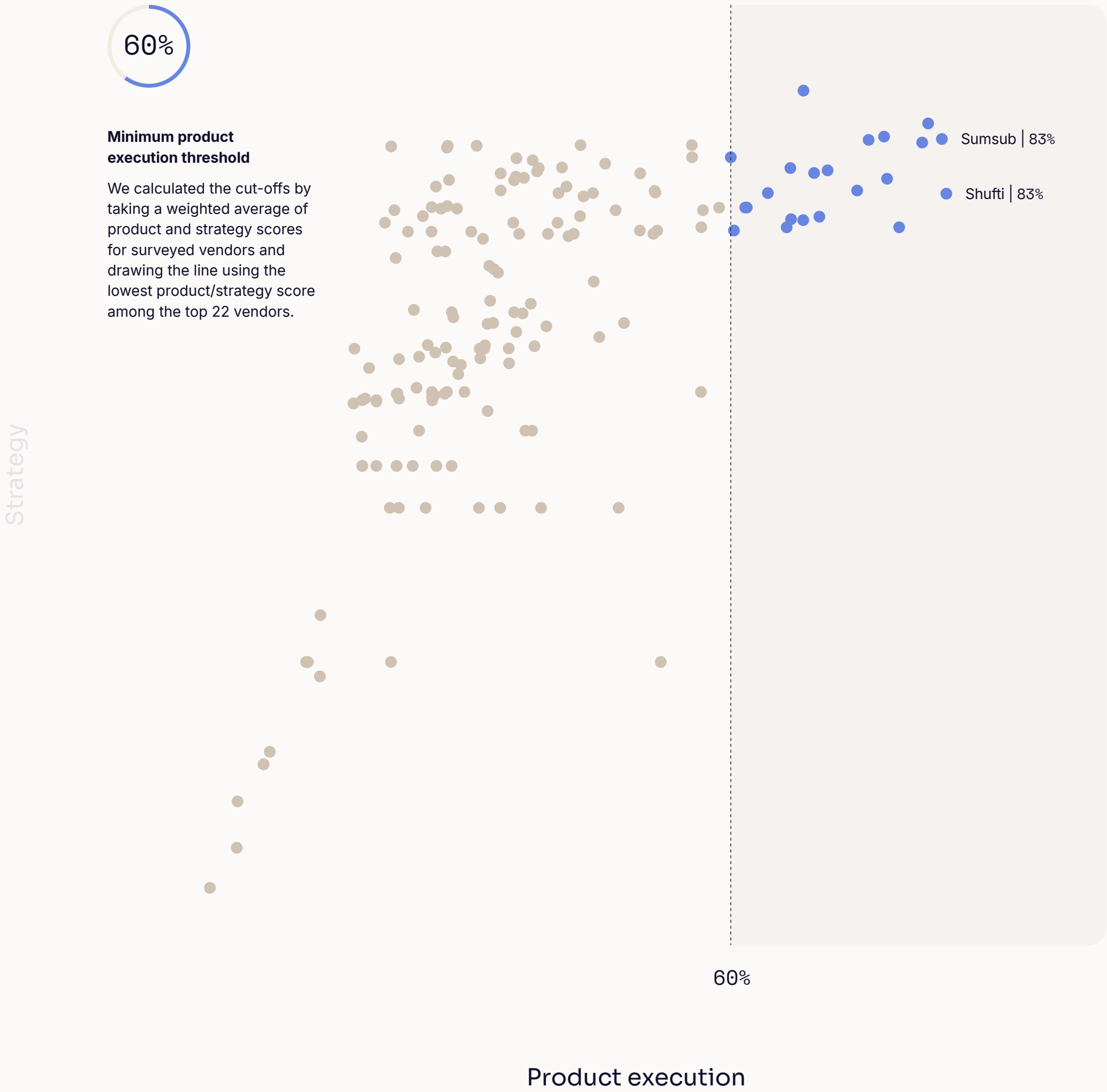
Liminal evaluated 82 vendors that solve the KYC use case. Minimum product execution and strategy thresholds were established to identify the leading vendors



Leadership Thresholds for KYC

Minimum product execution threshold

To establish a minimum product execution threshold for KYC, we evaluated buyer demand and practitioner feedback across regulated sectors (banks, fintechs, payment providers, capital markets, crypto, and regulated gaming). The highest-value product capabilities identified include identity verification accuracy (low false accepts and rejects), synthetic identity and deepfake detection, comprehensive identity data quality and coverage, sanctions/PEP/adverse media screening, integrated risk scoring and decisioning, and ease of implementation across onboarding flows. These capabilities collectively determine a vendor’s ability to verify identities accurately at scale while maintaining low onboarding friction and sustaining audit-ready compliance. Based on aggregated buyer demand and solution performance benchmarks, vendors must achieve a minimum product execution score of **60%** to sufficiently meet the requirements of a leading KYC solution.

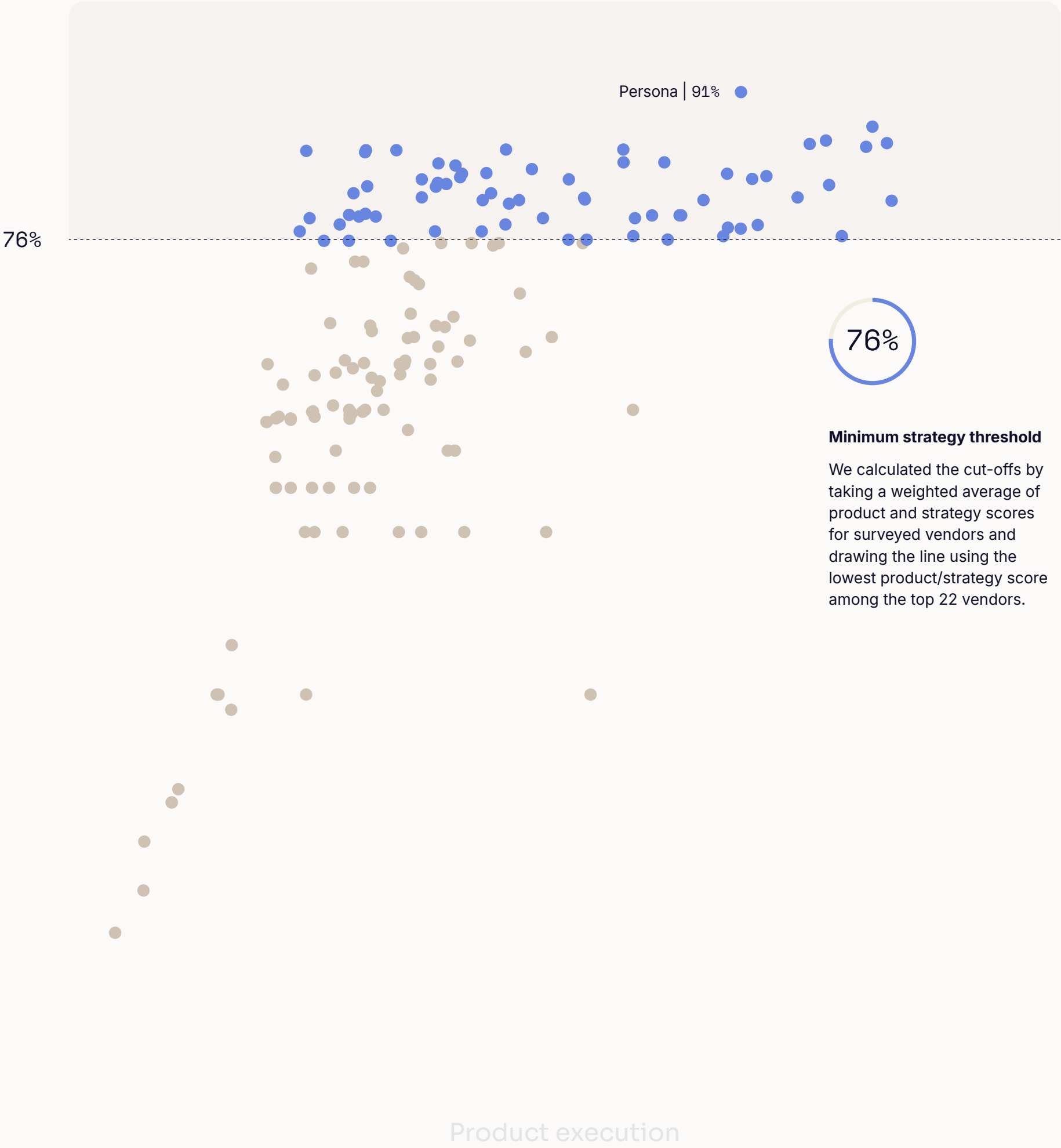


Leadership Thresholds for KYC

Minimum strategy threshold

The strategy threshold for KYC reflects the market’s shift from periodic onboarding checks to perpetual KYC, automated decisioning, and platform consolidation across the customer lifecycle. Key elements driving strategic differentiation include automation and orchestration of CDD/EDD workflows, continuous monitoring and event-driven risk refresh, global jurisdictional coverage, ecosystem integration with core banking and case management, intuitive operations experience for compliance and onboarding teams, transparent commercial models, and platform versus point-solution positioning across KYC+BEV+AML. Vendors must also demonstrate forward-looking investment in FCC-fraud convergence and agentic AI for autonomous decisioning. To qualify as a strategic leader in KYC, a vendor must achieve a minimum strategy score of **76%** signaling alignment with evolving buyer expectations for unified compliance platforms, perpetual monitoring, and AI-driven operational efficiency.

Strategy



KYC Leading Vendors

Among the 82 vendors Liminal evaluated that solve the KYC use case, **22 leading vendors** met the minimum product and strategy threshold

Adjacent Vendors

Strong overall solutions but do not have the required capabilities for this use case

Specialized Vendors

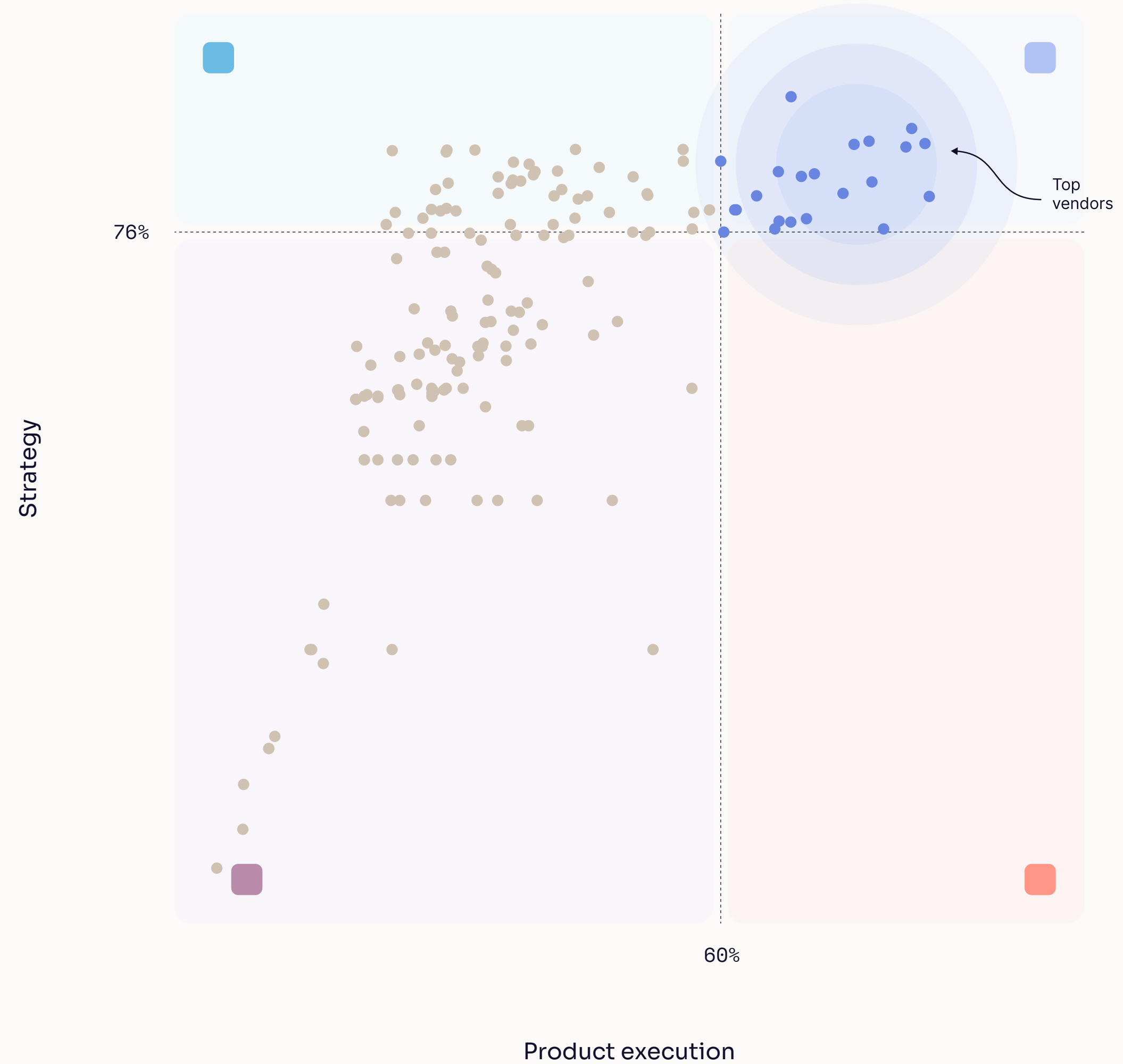
Solutions that can solve for a part of the use case but do not have all must have capabilities

Leading Vendors

Strong overall solutions that possess the must have product and strategy capabilities for this use case

Product-Focused Vendors

Solutions with strong product capabilities but do not meet the strategy score threshold



22 Leaders, 82 Evaluated Vendors

Liminal evaluated 82 vendors that solve the KYC use case across the product and strategy criteria, and determined [22 leading vendors](#)

Leaders

Alloy	FrankieOne	Persona	Sumsub
AU10TIX	Identomat	Plaid	Trulioo
Checkin.com	Incode	Sardine	TrustCloud
Entrust	Jumio	SEON	Veriff
Experian	LexisNexis Risk Solutions	Shufti	
Footprint	Mitek	Socure	

Other Evaluated Vendors

Airside	Eastnets	Hawk	Ondato
Alessa	Elliptic	Hummingbird	Oracle
Baselayer	Encompass	iDenfy	Prove
Bureau	Equifax	IDnow	Quantexa
Castellum.AI	Featurespace, a Visa Solution	Know Your Customer	RapidRatings
Chainalysis	Feedzai	Kyckr	REG-1
Coface	Fenergo	London Stock Exchange Group (LSEG)	Salv
Cognito	FICO	Lucinity	Sanctions.io
ComplyAdvantage	Fiserv	Markaaz	SAS
ComplyCube	Flagright	Microblink	Sigma360
Creditsafe	Focaldata	Middesk	SymphonyAI
Data Zoo	Fourthline	Moody's	ThetaRay
Discai	GBG	Napier AI	Tookitaki
Dow Jones	Global Data Consortium (GDC)	Nasdaq Verafin	Unit21
Dun & Bradstreet	greenID	NICE Actimize	Vespia

Liminal Index Leading Vendors for Know Your Customer in 2026

This view includes the product and strategy score cut-off, showcasing the [22 Leading Vendors](#) for this year’s Know Your Customer Index

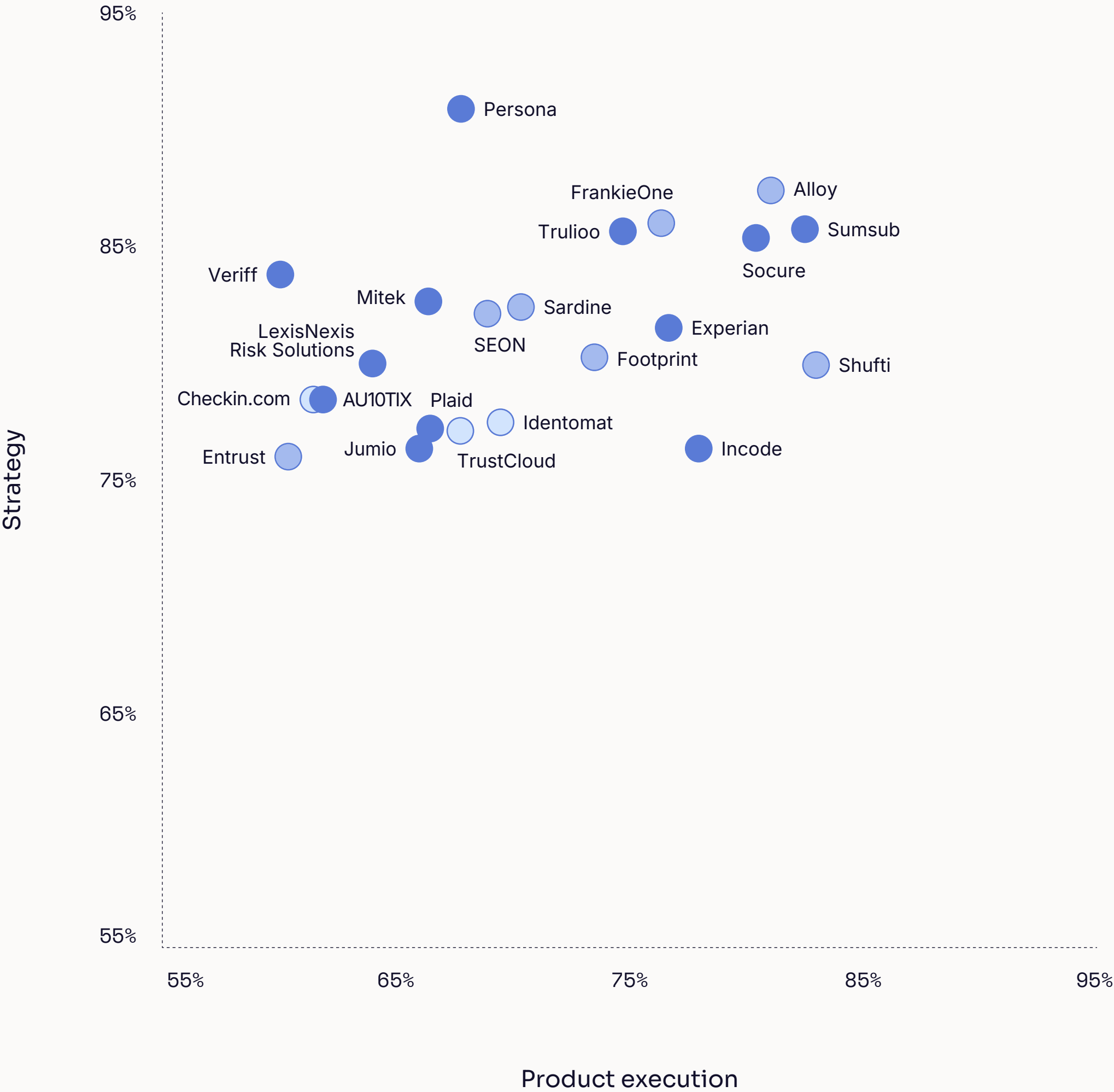
Market Presence

- Exceptional
- Excellent
- Strong

Inclusion Cutoff

Product Score 60%
Strategy Score 76%

We calculated the cut-offs by taking a weighted average of product and strategy scores for surveyed vendors and drawing the line using the lowest product/strategy score among the top 22 vendors.



04

Vendor Overview

Shufti

About Shufti

Shufti develops identity verification, compliance, and fraud prevention solutions for digital onboarding and customer lifecycle management. Its platform combines document verification, biometric authentication, liveness detection, AML screening, and risk assessment capabilities to help organizations verify identities, meet regulatory requirements, and mitigate fraud. The platform includes workflow automation, case management, and orchestration tools that enable businesses to build and manage verification processes across multiple channels and geographies. Shufti positions its offering as a unified trust platform, bringing identity, compliance, and fraud controls together within a single integration framework.

Company Information (as of April 2026)

Headquarters	London, United Kingdom
No. of Employees	201–500
Last Raised	\$20M, Series A in March 2022
Market Cap	Privately held
Industry Focus	Fintech, Crypto, iGaming, E-commerce, Banking, Healthcare, Insurance, Trading, Telecommunications, Payment Service Providers (PSPs), Social Networks
Geographic Focus	Asia Pacific, Europe, LATAM & Caribbean, Middle East/Africa, North America
Focus Region	Europe (UK)

Notable Customers   

 Exceptional  Excellent  Strong

¹ The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of only the leading vendor for KYC. Vendors outside the scoring buckets are not considered leading vendors for KYC.

Performance on KYC Liminal Index Benchmarking Criteria

Avg.	Criteria	Performance ¹
 Strategy	Automation & Orchestration	
	Continuous Monitoring & Perpetual KYC	
	Global Coverage Strategy	
	Product Integration & Ecosystem	
	Internal User Experience	
	Pricing & Commercial Model	
	Platform vs. Point Solution Positioning	
	FCC-Fraud Convergence Strategy	
	Agentic AI in Production	
	Identity Verification Accuracy	
 Product	Synthetic Identity & Deepfake Detection	
	Data Quality & Coverage	
	Screening & Watchlist Capabilities	
	Risk Scoring & Decisioning	
	Ease of Implementation & Deployment	
	Compliance Alignment & Audit Controls	
	Buyer Satisfaction	
	Company Size	
	Employee Growth (YoY)	
	Market Leadership Perception	
 Market Presence	Funding History	
	Digital Footprint	
	Media Coverage	

Shufti

KYC Analyst Note

Shufti’s KYC offering is delivered through its Global Trust Platform, a configurable identity verification solution that combines document verification, biometric authentication, AML screening, and fraud prevention capabilities within a unified orchestration layer. The platform supports verification of over 10,000 document types across 240+ jurisdictions and 150+ languages, leveraging AI-driven document analysis, OCR, and facial biometrics with 3D liveness detection to validate user identity and mitigate spoofing, presentation attacks, and deepfake threats. Identity verification accuracy is reinforced through a hybrid AI + human review model, with configurable decisioning modes that balance speed and assurance, while fraud controls extend beyond onboarding via post-verification modules such as deepfake detection, device intelligence, and behavioral anomaly analysis. Data quality and coverage are supported through extensive global data connectivity and multilingual verification capabilities, with operational coverage across diverse document ecosystems in regions including MENA, LATAM, and Southeast Asia. Screening and watchlist capabilities include real-time checks against 1,800+ sanctions, PEP, and adverse media sources, combined with continuous monitoring to support lifecycle compliance. Risk scoring and decisioning are driven by dynamic user risk assessment models incorporating profile, behavioral, and transaction signals, while case management and audit trails ensure traceability and compliance oversight. The platform also supports emerging digital identity initiatives through NFC-enabled verification, reusable identity credentials, and readiness for European Digital Identity (EUDI) Wallet ecosystems. Ease of implementation is supported through a single API, SDKs, and a no-code Journey Builder, while compliance alignment is reinforced through GDPR, SOC 2, and ISO certifications. Buyer feedback highlights strong onboarding speed and ease of integration, with customer sentiment generally reflecting positive experiences around implementation and operational efficiency.

Shufti’s strategy emphasizes platform unification and accessibility, positioning KYC as part of a broader trust and compliance infrastructure spanning KYB, AML screening, transaction monitoring, authentication, and fraud prevention. Its roadmap focuses on automation and orchestration through no-code workflow configuration, enabling organizations to design adaptive verification journeys that adjust dynamically based on risk signals and geography. Continuous monitoring and perpetual KYC are embedded through automated re-screening, adverse media tracking, and event-driven risk updates, aligning with industry demand for lifecycle-based compliance. The company’s global coverage strategy is a central differentiator, with emphasis on broad jurisdictional reach, multilingual support, and operational coverage of locally relevant identity documents across both mature and emerging markets. Shufti also positions itself to address increasing convergence between identity verification,

● High ● Medium ○ Low

1 Greyed out capabilities are not offered with the vendor solution.
2 Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

KYC Capabilities¹

Requirements to Satisfy the Use Case

Perform Identity Verification

Buyer Demand for Product Capability²

Active Liveness Detection	●
Email Verification	●
Mobile Device Identity Binding	●
Portable KYC	●
Video KYC	●
Identity Verification Orchestration	●
Passive Liveness Detection	●
Physical Biometrics	●
Address Verification	○
Date of Birth (DOB) Verification	○
Document Verification	○
Government Identification Number Verification	○
Name Verification	○
Phone Number Verification	○

Active Liveness Detection	●
Negative News / Adverse Media Monitoring	●
Sanctions Screening	●
Consumer Financial Transaction Data Integration	●
Government Identification Number Verification	●
Passive Liveness Detection	●
Politically Exposed Persons (PEP) Screening	●
Address Verification	○
Date of Birth (DOB) Verification	○
Document Verification	○
Name Verification	○

Negative News / Adverse Media Monitoring	●
Physically-present Identity Proofing	●
Sanctions Screening	●
Consumer Financial Transaction Data Integration	●
Government Identification Number Verification	●
Document Verification	○
Name Verification	○
Politically Exposed Persons (PEP) Screening	○

Perform Customer Due Diligence (CDD)

Perform Customer Enhanced Due Diligence (EDD)

Shufti

KYC Analyst Note

fraud prevention, and digital trust services through investments in reusable digital identity, advanced liveness detection, behavioral analytics, and deepfake detection. Its ownership of the core technology stack provides greater control over document support, deployment flexibility, and regulatory responsiveness. The company positions itself as a platform rather than a point solution, with strong FCC–fraud convergence through integration of identity, behavioral, and transaction signals into unified risk scoring. Its hybrid AI + human approach supports both automation and regulatory explainability, while ongoing investment in fraud and identity intelligence capabilities reflects broader market demand for adaptive, AI-enabled verification.

Shufti has established a broad global presence, with reported deployments across more than 2,000 businesses and coverage spanning over 240 countries and territories, supporting industries such as fintech, crypto, marketplaces, gaming, telecommunications, and payment services. The platform processes millions of verifications daily, with vendor-reported metrics highlighting sub-10-second verification times, high first-time pass rates, and significant reductions in manual review through automation. Customer feedback across platforms such as G2 and Trustpilot emphasizes ease of use, fast onboarding, and strong customer experience, while noting occasional challenges with OCR accuracy and repeated verification attempts. Strategic partnerships in sectors such as iGaming and embedded finance further extend its ecosystem reach. Market momentum is driven by increasing demand for globally scalable, low-friction KYC solutions that can balance compliance requirements with user experience. Within this context, Shufti is positioned as a flexible, full-stack KYC provider with strong global coverage and a focus on automation, accessibility, and end-to-end identity lifecycle management. Its differentiation increasingly stems from the combination of active global document processing, digital identity readiness, fraud prevention capabilities, and the integration of identity, compliance, and risk management functions within a unified platform architecture.

● High ● Medium ○ Low

1 Greyed out capabilities are not offered with the vendor solution.
2 Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

KYC Capabilities¹

Requirements to Satisfy the Use Case

Trigger Step-Up Verification Based on User Risk

Buyer Demand for Product Capability²

- Adaptive Authentication ●
- Video KYC ●
- Continuous/Perpetual KYC ●
- Document Verification ○

Detect Synthetic or Manipulated Identities

- Location Intelligence ●
- Behavioral Analytics ○
- Behavioral Biometrics ○
- Bot Detection ○
- Continuous/Perpetual KYC ○
- Synthetic Identity Risk Scoring ○

Detect Anomalous Behavioral Activity for Fraud Threats

- Customer Risk Profiling ●
- Unified Customer View Creation ●
- Location Intelligence ●
- Mobile Carrier API Access ●
- Behavioral Biometrics ○
- Behavioral Analytics ○
- Device Intelligence ○

Generate a Dynamic User AML Risk Score

- Customer Risk Profiling ●
- Location Intelligence ●
- Negative News / Adverse Media Monitoring ●
- Behavioral Analytics ●
- Behavioral Biometrics ●
- Device Intelligence ●
- AML Risk Scoring ○
- Fraud Monitoring ○
- Politically Exposed Persons (PEP) Screening ○

Document an Audit Trail

- Document Retention & Storage ●
- AML Audit Trail Management ○

Manage Investigations and Case Workflows

- Fraud Alert and Case Management ●
- AML Alert and Case Management ○

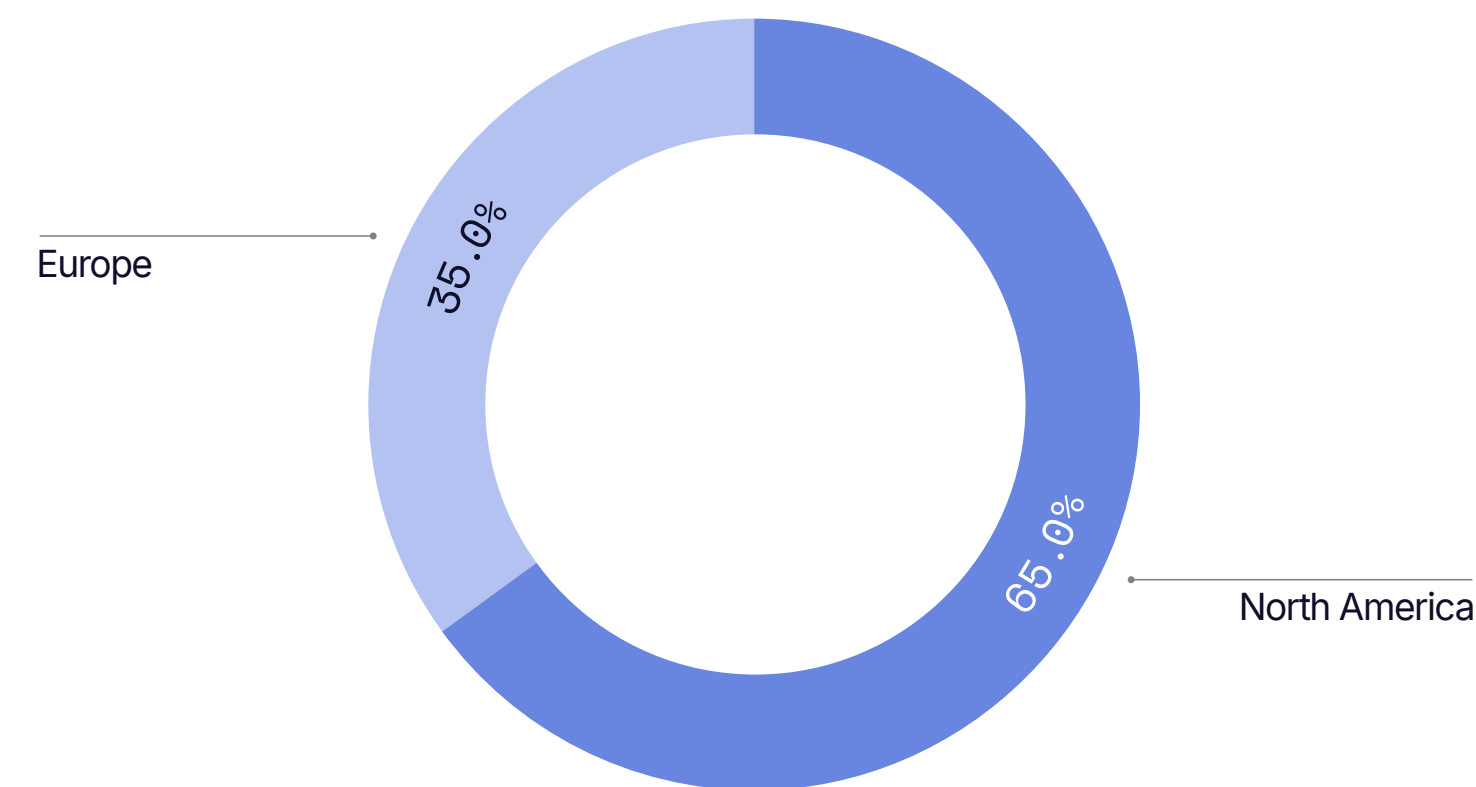
05 Appendix

Market Presence Survey Demographics

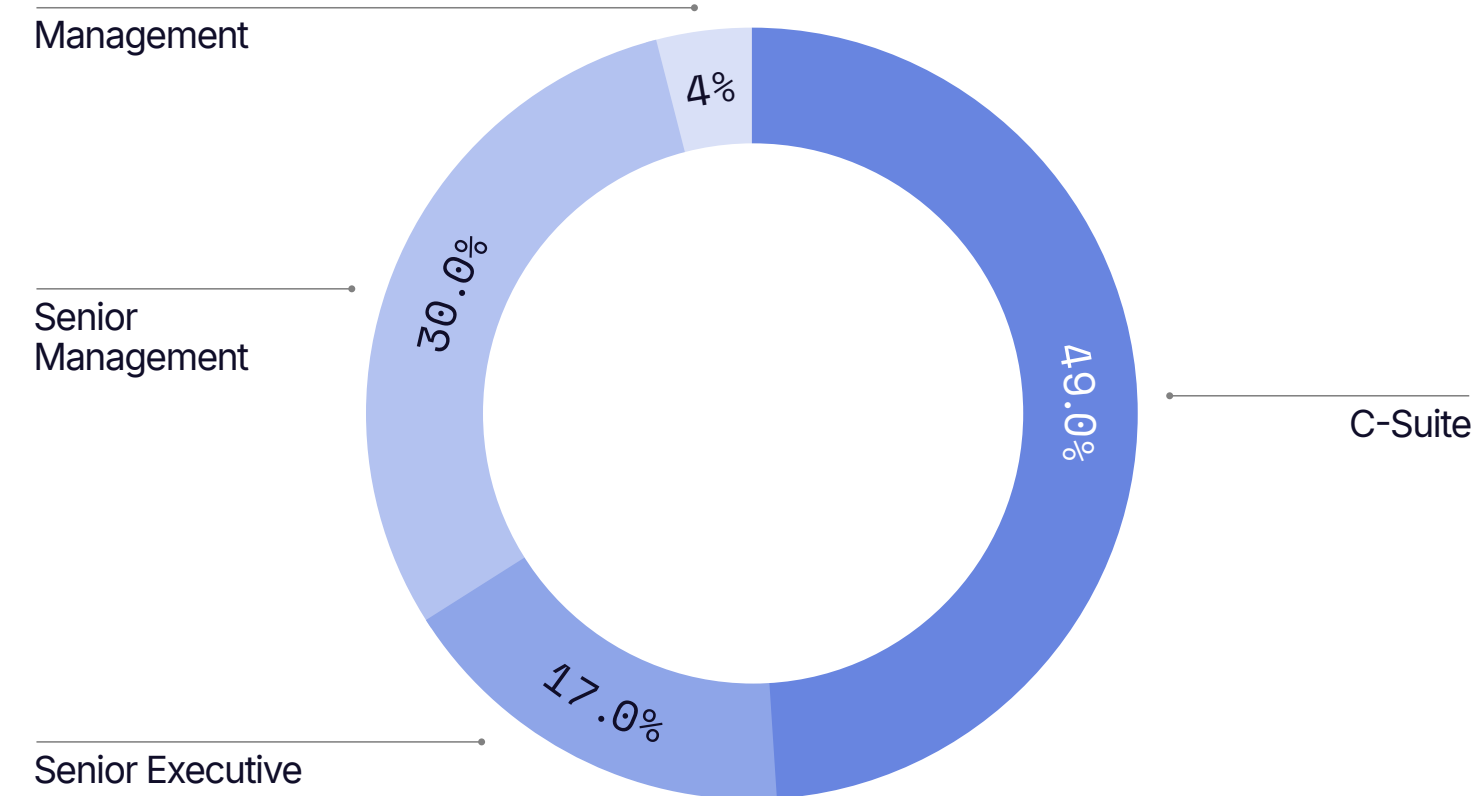
Survey Respondent Demongraphics (N=100)¹

Geography

By Region, highest priority based on revenue

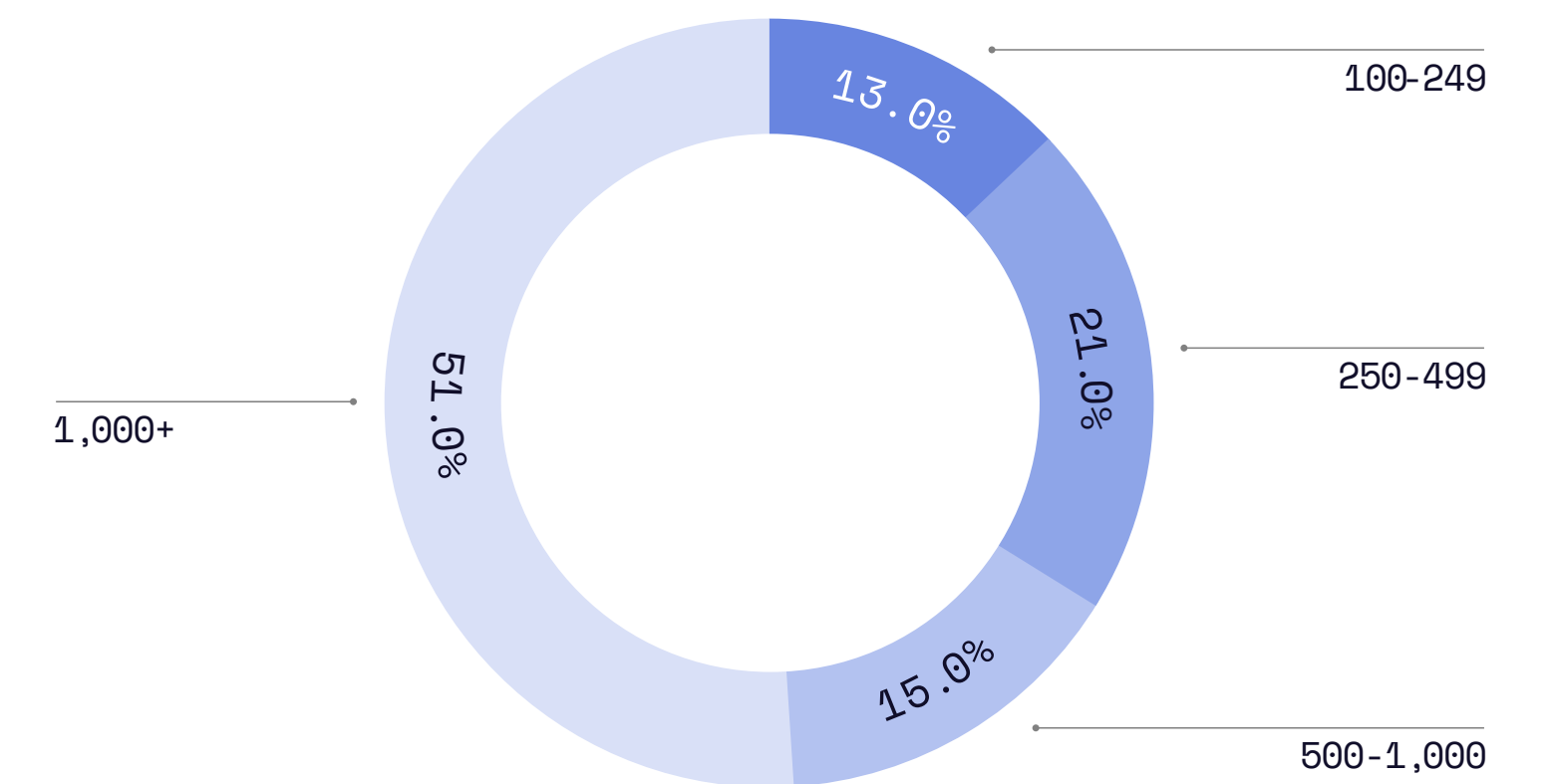


Job Level



Company Size

By Customers



¹ Financial Crimes Compliance Buyer Demand Survey, March 2026 (N=100)

Liminal Index Methodology

Exceptional, Excellent, Strong Scoring Buckets Definitions

Scoring Buckets

 **Exceptional**

Definition

Vendors in this category represent the highest level of performance in the KYC and identity verification market, ranking above the third quartile among leading providers. They exceed regulatory and industry standards, offering advanced AI-driven identity verification, deepfake and synthetic-identity detection, real-time risk scoring, perpetual KYC capabilities, and seamless integration across onboarding and ongoing-due-diligence workflows. Their solutions empower financial institutions to onboard customers with precision, detect identity fraud at scale, and meet evolving global KYC regulations including the EU AMLR and UK ECCTA failure-to-prevent-fraud regime.

 **Excellent**

Vendors in this category provide highly effective KYC and identity verification solutions, ranking between the first and third quartile among leading providers. They offer strong identity verification accuracy, reliable PEP/sanctions and adverse-media screening, biometric and document authentication, and scalable automation, though they may not reach the same level of capability breadth as Exceptional vendors. These providers improve onboarding conversion, reduce manual review burden, and streamline regulatory reporting, making them strong choices for organisations seeking robust yet cost-effective KYC solutions.

 **Strong**

Vendors in this category meet core KYC and identity verification requirements, ranking below the first quartile among top providers while outperforming those not making the final list. They offer dependable solutions covering essential identity verification, screening, and customer due-diligence needs. While they may lack advanced perpetual-monitoring capabilities, deepfake detection, or deep orchestration, their solutions remain suitable for organisations with fundamental KYC compliance and identity verification requirements.

Product Capability Definitions

Capability	Definition
Active Liveness Detection	Active liveness detection is a security measure used in identity verification that requires users to perform specific actions or responses to verify their presence and authenticity. This capability ensures that the biometric data being captured is from a live person.
Adaptive Authentication	Dynamically adjusts the level of authentication required based on user behavior, context, and risk signals. It enables frictionless access for low-risk interactions while adding verification steps when anomalies or high-risk attributes are detected.
Address Verification	Confirms that a physical or mailing address provided by a user or entity is valid, accurate, and associated with the correct individual or organization. It reduces fraud risks involving false identities, synthetic identities, or stolen address data.
AML Alert and Case Management	Provides a comprehensive system for managing alerts and cases related to Anti-Money Laundering (AML) activities. This capability ensures efficient tracking, investigation, and resolution of potential money laundering incidents, aiding compliance with regulatory requirements.
AML Audit Trail Management	AML (Anti-Money Laundering) Audit Trail Management refers to the process of systematically recording, storing, and retrieving all activities related to AML compliance. This includes user actions, data access, rule changes, alerts generated, investigations conducted, and decisions made throughout the AML lifecycle. The goal is to provide a transparent and tamper-proof record that enables regulators, auditors, and internal stakeholders to verify compliance and assess the effectiveness of AML controls.
AML Risk Scoring	AML risk scoring is a methodology used by financial institutions to assess the risk level of their clients in relation to money laundering and terrorist financing. This scoring system assigns a numerical value or category to each client based on various risk factors, such as geographic location, transaction behavior, occupation, and associations with PEPs (Politically Exposed Persons).

Product Capability Definitions

Capability	Definition
Behavioral Analytics	Behavioral analytics is a data analysis process that focuses on understanding how users interact with systems and applications to detect unusual behaviors that may indicate security threats or unauthorized activities. It tracks and analyzes a wide range of user activities - from account creation and form submissions to purchasing behavior - to glean insights into user preferences, habits, and intentions.
Behavioral Biometrics	Authenticates users based on unique patterns in how they interact with devices (e.g., keystroke dynamics, mouse movements, touch pressure, swipe patterns, and device handling). Unlike static biometrics (fingerprint, face), these signals are captured continuously and passively during sessions.
Bot Detection	Distinguishes automated traffic from legitimate human users by analyzing request patterns, device fingerprints, behavioral signals, and environmental attributes. It identifies both unsophisticated scrapers and advanced bots that mimic human interaction.
Consumer Financial Transaction Data Integration	Integrates detailed personal financial information collected from various financial institutions, including transaction history, balance details, and fee information related to credit cards, loans, mortgages, and securities. It encompasses purchases, payments, debits, credits, interest payments, and other consumer transactions. It supports behavioral baselining and typology detection at the individual level.
Continuous/ Perpetual KYC	Extends traditional point-in-time identity verification into an ongoing process that monitors customers throughout the relationship for changes in risk profile, sanctions status, adverse media, and identifying information. It replaces periodic manual reviews with automated, event-driven reassessment that detects relevant changes closer to when they occur.
Customer Risk Profiling	Customer risk profiling is the process of evaluating and categorizing customers based on their likelihood of exhibiting high-risk behavior, such as fraud, credit default, policy abuse, or non-compliance. This involves analyzing data points such as identity attributes, transaction history, behavioral patterns, device and location signals, and external risk indicators to assign a risk score or classification.

Product Capability Definitions

Capability	Definition
Date of Birth (DOB) Verification	Confirms that the birthdate provided by an individual is accurate by cross-referencing against authoritative data sources rather than accepting self-declared information at face value. It serves as a foundational identity attribute for age verification, identity proofing, and fraud detection by validating a data point that is both stable over time and consistently recorded across official records.
Device Intelligence	Device Intelligence is a fraud prevention capability that identifies, analyzes, and assesses the risk of the device a user. It plays a critical role in multi-layered fraud defense by adding an invisible layer of authentication and risk scoring without impacting user experience.
Document Retention & Storage	Provides secure, compliant preservation of documents and records collected during identity verification, due diligence, and compliance processes. It ensures that documentation remains accessible for regulatory inquiries, audit examinations, and litigation while meeting data protection requirements for sensitive information.
Document Verification	Document verification establishes an individual is who they say they are through the validation and verification of a government-issued identity document.
Email Verification	Confirms that an email address provided during registration, transaction, or account update is valid, deliverable, and controlled by the claimed user. It serves as both a data quality measure and a security control, preventing typos, fake addresses, and account creation using others' email identities.
Fraud Alert and Case Management	Fraud alert and case management detects suspicious activity in real-time, generating alerts, and managing investigation workflows to determine whether fraud has occurred. It enables organizations to triage, escalate, and resolve alerts efficiently while maintaining detailed audit trails and cross-functional collaboration.

Product Capability Definitions

Capability	Definition
Fraud Monitoring	Fraud monitoring is the surveillance and analysis of networks, accounts, and transactions to identify potentially fraudulent activity for automated fraud decisioning.
Government Identification Number Verification	Validates that identity numbers provided by users—Social Security Numbers, national ID numbers, tax identification numbers, passport numbers—are legitimate, properly formatted, and consistent with the claimed identity. It detects synthetic identities, data entry errors, and fraudulent use of stolen or fabricated credentials during onboarding and high-risk transactions.
Identity Verification Orchestration	The process of coordinating and automating the flow of identity verification tasks across multiple systems and workflows. It ensures that all necessary steps in the identity verification process are executed efficiently and consistently, from data collection to decision-making.
Location Intelligence	Uses geographical, network, and environmental context to evaluate risk or authenticity. It is used across fraud detection, AML, cybersecurity, and identity verification to detect high-risk geographies, impossible travel patterns, mismatched locations, or cross-border anomalies. This capability enhances decision-making by incorporating contextual location-based risk.
Mobile Carrier API Access	Mobile Carrier API Access refers to the ability to integrate and utilize APIs provided by mobile network operators (MNOs) to access mobile subscriber data and services, such as authentication, identity verification, and SIM swap detection.
Mobile Device Identity Binding	Cryptographically associates a user's identity or account with a specific mobile device, ensuring that authentication and sensitive operations can only occur from that registered device. It prevents credential theft from enabling unauthorized access on attacker-controlled devices.

Product Capability Definitions

Capability	Definition
Name Verification	Confirms that a name provided by an individual is accurate, consistently formatted, and matches authoritative records across identity data sources. It validates a foundational identity attribute that appears across virtually all identity documents, financial records, and official registrations, detecting errors, inconsistencies, and potential fraud.
Negative News / Adverse Media Monitoring	Screens individuals and entities for news indicating financial crime risk, corruption, sanctions evasion, fraud, or legal actions. It provides early warning signals before official records or sanctions lists are updated. This supports enhanced due diligence and ongoing monitoring obligations.
Passive Liveness Detection	Passive liveness detection is a security measure used in identity verification to ensure that the biometric data being captured originates from a live user rather than a spoof or synthetic source, without requiring explicit user actions. This capability unobtrusively analyzes and validates the authenticity of a user's presence during the verification process.
Phone Number Verification	Confirms that a user controls the phone number they provide by delivering a one-time code via SMS or voice call that must be correctly entered to proceed. It validates both number authenticity and current possession, serving as an identity signal during registration, transaction authorization, and account recovery flows.
Physical Biometrics	Physical biometrics is the use of unique physical characteristics, such as fingerprints, facial features, or iris patterns, to verify the identity of individuals. This technology enhances security and user convenience by providing a reliable and non-intrusive method for authentication.
Physically-present Identity Proofing	Physically-present identity proofing is a method of verifying an individual's identity where the person is required to be physically present with their identification documents. This process typically involves the individual presenting government-issued ID documents, such as a driver's license or passport, to a trusted authority who can validate the authenticity of the documents and confirm the identity of the person.

Product Capability Definitions

Capability	Definition
Politically Exposed Persons (PEP) Screening	PEP Screening identifies Politically Exposed Persons (PEPs) and their close associates or family members. These individuals require enhanced monitoring due to potential exposure to corruption or political influence. This capability supports global EDD requirements and ensures higher-risk customers receive appropriate scrutiny.
Portable KYC	Allows individuals to reuse their verified identity information across multiple service providers without needing to go through the Know Your Customer (KYC) process repeatedly. It provides a standardized, shareable digital identity that can be accessed and verified by various organizations, streamlining the onboarding process.
Sanctions Screening	Checks customers, counterparties, businesses, and transaction details against global sanctions lists (OFAC, UN, EU, UK, etc.). It ensures compliance with regulatory requirements to block and report prohibited transactions. This reduces exposure to financial crime, terrorism financing, and state-sponsored illicit activity.
Synthetic Identity Risk Scoring	Evaluates the likelihood that an identity presented during onboarding or transactions is fabricated from a combination of real and fictitious information rather than representing an actual person. It addresses a fraud type that evades traditional identity verification by using valid but misassembled identity elements—real SSNs paired with fake names, manufactured credit histories, or blended attributes from multiple individuals.
Unified Customer View Creation	Unified customer view creation is the process of consolidating data from multiple sources to create a single, comprehensive profile for each customer. It enables organizations to gain a holistic understanding of their customers, enhancing personalization and improving decision-making.
Video KYC	Conducts identity verification through live or recorded video sessions where customers present identity documents and undergo biometric verification remotely. It provides higher assurance than fully automated document verification by incorporating human review, liveness confirmation, and interactive questioning while maintaining remote accessibility.

Liminal Index Methodology

Product

Product Criteria	Weighting	Definition	Why It Matters
KYC Capabilities	60%	The breadth of capabilities a vendor offers to address the requirements of this use case.	Strong capabilities enable financial institutions to verify customer identities accurately at scale, reduce fraud exposure, and meet evolving regulatory standards across the customer lifecycle.
Identity Verification Accuracy	8%	Ability to accurately verify customer identities through document authentication, biometric matching, and data cross-referencing while minimizing false positives and false negatives - the foundational requirement for KYC compliance.	Accurate identity verification is the cornerstone of effective KYC compliance, reducing false positives that burden operations teams while minimizing false negatives that expose the organization to regulatory and fraud risk.
Synthetic Identity & Deepfake Detection	5%	Ability to detect AI-generated fraudulent identities including deepfakes, synthetic identities, and presentation attacks - an emerging critical capability as AI-driven fraud increases in sophistication and volume.	Robust detection of synthetic identities and deepfakes is essential as AI-driven fraud increases in sophistication, helping institutions prevent account-level exposure and preserve trust in their onboarding processes.
Data Quality & Coverage	6%	Breadth and depth of identity data sources, document coverage, and global registry access for comprehensive verification - ensuring high match rates across diverse populations and geographies. Includes passive behavioral biometric signals and device intelligence as emerging data layers that strengthen fraud detection during onboarding without adding friction.	Comprehensive, high-quality identity data ensures strong match rates across diverse populations and geographies, improving onboarding conversion while strengthening fraud detection without adding user friction.
Screening & Watchlist Capabilities	4%	Depth of sanctions, PEP, adverse media, and watchlist screening with configurable matching rules, fuzzy matching, and real-time updates - enabling precise risk assessment during onboarding and ongoing monitoring.	Effective sanctions, PEP, and adverse media screening is a regulatory imperative, with precise matching rules and real-time updates ensuring organizations respond to emerging risks before exposure materializes.
Risk Scoring & Decisioning	5%	Integrated risk assessment and automated decisioning capabilities that contextualize identity signals, behavioral data, and compliance requirements into actionable risk scores. Model explainability and governance are now regulatory expectations for AI-based scoring. Includes agentic AI capabilities for autonomous case remediation and exception handling in complex or escalated KYC reviews.	Integrated risk scoring translates complex identity and behavioral signals into consistent, defensible decisions, while explainable models support regulatory expectations and audit readiness.
Ease of Implementation & Deployment	4%	How quickly and simply KYC verification can be deployed, integrated into customer onboarding flows, and producing results. Includes verification processing time and coverage expansion metrics as operational benchmarks.	Fast, simple deployment accelerates time-to-value and reduces engineering burden, enabling organizations to scale verification capacity as customer volumes grow.
Compliance Alignment & Audit Controls	6%	Built-in regulatory compliance frameworks, automated audit trails, and jurisdiction-specific controls. Must align with evolving EU AMLR/AMLA standards, FATF requirements, and outcome-based supervision trends emphasizing board-level accountability.	Built-in regulatory frameworks and automated audit trails reduce the manual effort required to demonstrate compliance and help organizations adapt to evolving requirements across markets.
Buyer Satisfaction	2%	The extent of buyer satisfaction with the vendor's KYC solution as measured by independent review platforms, analyst recognition, and customer advocacy metrics.	High buyer satisfaction indicates the solution delivers real-world value, meets operational expectations, and supports efficient KYC workflows, encouraging long-term adoption and advocacy.

Liminal Index

Methodology

Strategy

Strategy Criteria	Weighting	Definition	Why It Matters
Automation & Orchestration	11%	Capability for KYC operations to run without human intervention - automated identity verification, risk decisioning, document processing, and workflow orchestration. Includes straight-through processing rates and manual review reduction as key operational efficiency metrics.	Automation reduces manual review burden, accelerates onboarding throughput, and lowers operational costs, freeing compliance teams to focus on complex cases and improving overall decision quality.
Continuous Monitoring & Perpetual KYC	14%	Ongoing, event-driven re-verification of customer identity and risk - moving beyond periodic reviews to real-time detection of changes in PII, risk signals, adverse media, and sanctions status. pKYC is becoming the reference model requiring upgraded data pipelines, triggers, and governance.	Moving from periodic reviews to event-driven monitoring enables institutions to detect changes in customer risk in real time, reducing exposure windows and aligning with the regulatory shift toward perpetual KYC as the reference compliance model.
Global Coverage Strategy	8%	Ability to verify identities across jurisdictions with multi-country document support, local data source access, and region-specific regulatory alignment - critical for organizations with cross-border customer bases.	Cross-border customer bases require verification capabilities that span jurisdictions, document types, and local data sources, reducing onboarding friction while ensuring region-specific regulatory alignment.
Product Integration & Ecosystem	8%	Ability to integrate natively with core banking, CRM, case management, and third-party data providers. Emphasis on interoperable APIs, common data schemas, and integration hooks - not just all-in-one suites. Cross-functional integration with fraud and credit systems is increasingly expected.	Seamless integration with core banking, CRM, and case management systems reduces data silos, enabling unified compliance workflows and faster response to cross-functional risk signals.
Internal User Experience	9%	How intuitive and effective tools are for compliance analysts, operations teams, and developers to adopt, use, and derive value in daily KYC workflows - enabling faster onboarding, case review, and risk triage.	Intuitive tools for compliance analysts and operations teams improve productivity, case resolution speed, and risk triage quality, reducing training time and minimizing errors across daily KYC workflows.
Pricing & Commercial Model	10%	Transparent, scalable pricing that delivers ROI through efficient licensing, reduced manual review costs, and flexible deployment - budget alignment with value delivered across verification volumes.	Transparent, scalable pricing aligns KYC spend with verification volumes and operational value, lowering total cost of ownership and supporting sustainable scaling as customer bases grow.
Platform vs. Point Solution Positioning	15%	Strategic approach to market positioning - whether the vendor offers a consolidated platform spanning multiple FCC use cases or specializes deeply in KYC with clean integration to other systems. Buyers increasingly favor platform consolidation.	As buyers increasingly favor platform consolidation, vendors offering unified solutions across multiple FCC use cases reduce integration complexity, lower total cost of ownership, and provide a more cohesive view of customer risk.
FCC-Fraud Convergence Strategy	18%	Strategic approach to converging financial crime compliance with fraud prevention and cyber risk - reflecting the market shift toward integrated intelligence and case-management functions across historically siloed compliance and fraud teams.	Convergence of financial crime compliance and fraud prevention reflects a market shift toward integrated intelligence across historically siloed teams, helping institutions reduce redundant tooling, share risk signals, and respond to threats more holistically.
Agentic AI in Production	7%	The extent to which the vendor has moved beyond AI-assisted decisioning into deployed agentic workflows for KYC operations - autonomous agents that conduct CDD/EDD reviews, periodic refresh, and escalation handling end-to-end at named regulated customers, with transparent human-in-the-loop controls. As of 2026, this is the clearest forward-looking discriminator at the top of the KYC market: most vendors market "AI" but only a handful operate agents in production with quantified analyst-time savings and documented governance.	Agentic AI capabilities for autonomous CDD/EDD reviews and case remediation are emerging as a forward-looking discriminator at the top of the KYC market, signaling strategic leadership and the potential for step-change improvements in analyst productivity.

Liminal Index Methodology

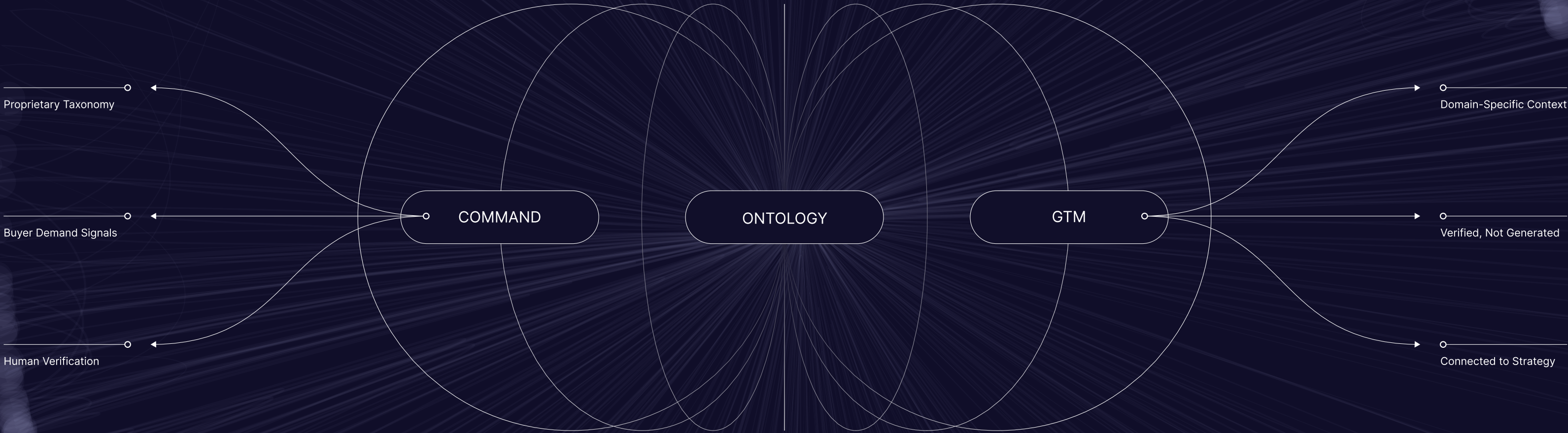
Market Presence

Market Criteria	Weighting	Definition	Why It Matters
Company Size	20%	The total employee headcount of a company.	Larger company size demonstrates operational stability, resource availability, and the ability to handle complex or large-scale customer requirements. It signals reliability and strong organizational infrastructure.
Employee Growth (YoY)	20%	How fast a company's employee count is growing.	Workforce growth reflects the vendor's ability to scale operations, invest in talent, and meet increasing market demands. It indicates organizational health, innovation capacity, and long-term growth potential.
Market Leadership Perception	20%	The number of buyers who believe this vendor is a market leader.	Perceived market leadership signals the vendor's ability to set trends, deliver innovative solutions, and meet evolving customer needs. It highlights credibility, industry influence, and a competitive advantage.
Funding History	30%	Total funding a company has incurred.	Total funding reflects investor confidence and the vendor's capacity to invest in product development, talent acquisition, and market expansion, supporting long-term viability and innovation.
Digital Footprint	5%	The company's total social media footprint.	A strong digital footprint increases brand visibility, supports thought leadership, and reflects active market engagement, making it easier for buyers to discover and evaluate the vendor.
Media Coverage	5%	Vendor mentions/quotes in authoritative outlets reflect market presence.	Vendor mentions in authoritative outlets reflect market presence, credibility, and industry recognition, reinforcing buyer confidence and competitive positioning.



The Actionable Intelligence Company

The same depth and rigor you’ve just read, now powering the verified intelligence behind your next strategic decision



Three interfaces, one verified foundation:

Command

validate roadmaps against verified buyer demand, monitor competitive moves, and detect market shifts before they go public

GTM

target the right accounts, arm reps with live battlecards and AI-coached outreach, and close with context no competitor can access

Expert Desk

every signal verified by human domain experts recruited from Identity, Fraud, and Cybersecurity

Ontology

All three run on a continuously verified ontology of 2.5M+ real relationships across vendors, buyers, regulations, capabilities, and threat vectors.

Proven
across our portfolio

Liminal maps the real relationships in Identity, Fraud, and Cybersecurity into a continuously verified, queryable ontology. Purpose-built interfaces sit on top: Command for strategy and product teams, GTM for revenue teams, and the Expert Desk for human verification.

9x

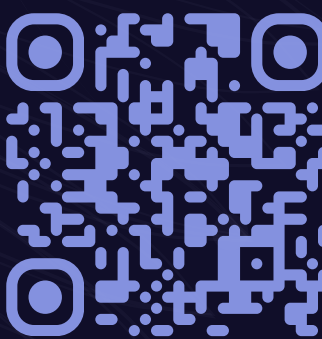
FASTER STRATEGIC
DECISIONS

30%

HIGHER COMPETITIVE
WIN RATES

70%

LESS MANUAL
RESEARCH TIME



From strategy to execution, verified. See how one intelligence system powers both the decisions you make and the deals you win.

GET ACCESS



Liminal Strategy, Inc.
200 Park Avenue South, Suite 1514, New York, New York 10003

www.liminal.co | info@liminal.co

