



Link Index

# Know Your Customer (KYC)

June 2025 | This Report is Licensed for Reprint Distribution by Socure

<b>Introduction</b>		<b>Use Case Overview</b>	<b>5</b>	<b>Market Overview</b>	<b>13</b>	<b>Link Index</b>	<b>18</b>	<b>Vendor Overview</b>	<b>29</b>
Market Overview	3	KYC is essential for AML compliance, helping financial institutions combat fraud, balance security, and adapt to evolving threats through AI-driven risk detection, biometrics, and automation	6	Firms struggle to integrate automation amid rising due diligence demands from sanctions, synthetic IDs, and deepfake-related fraud threats	14	Vendor products were evaluated based on their coverage of product capabilities and performance against top solution purchasing criteria	19	Socure	30
Vendor Landscape	4	To support KYC, vendors must meet five core requirements, each with varied capabilities to match evolving compliance and customer demands	7	KYC automation speeds onboarding as buyers prioritize accuracy, compliance, and vendor consolidation for a unified AML strategy	15	KYC vendor strategies were assessed based on the top buyer purchasing priorities for the coming years	20	<b>Appendix</b>	<b>32</b>
		KYC solution buyers include compliance professionals such as AML Officers, Chief Compliance Officers, and Compliance Program Managers	8	KYC practitioners prioritize accuracy, data quality, regulatory compliance, and scalability as the most important criteria in their purchasing process	16	The market presence of KYC vendors was evaluated based on leadership perception, brand awareness, company size, and company growth	21	Market Presence Survey Demographics	33
		An AML Officer overseeing KYC ensures compliance through customer ID, due diligence, risk assessment, and automation to boost efficiency	9	The market is moving toward pKYC and mDLs, while priorities are shifting toward partnerships, analytics, and integration	17	Minimum product execution and strategy thresholds were established to identify the leading vendors for KYC	22	Link Index Methodology: Exceptional, Excellent, Strong Scoring Buckets Definitions	34
		A Chief Compliance Officer ensures KYC compliance by leading customer verification, risk assessments, and due diligence to reduce financial crime risk	10			Among the 191 vendors Liminal evaluated that solve the KYC use case, 27 leading vendors met the minimum product and strategy threshold	23	Product Capability Definitions	35
		A KYC Program Manager ensures compliance by managing ID, onboarding, and risk checks using automation, data integration, and analytics tools	11			Liminal evaluated 191 vendors that solve the KYC use case across the product and strategy criteria, and determined 27 leading vendors	24	Link Index Methodology: Product	38
		KYC solutions guarantee compliance, mitigate fraud, and deliver a seamless user experience throughout the customer journey	12			Link Index Leading Vendor for Know-Your-Customer in 2025	25	Link Index Methodology: Strategy	39
						KYC vendors take distinct approaches based on use case complexity, risk tolerance, and regulatory needs	26	Link Index Methodology: Market Presence	40
						Leading vendors are shaping the future of KYC through real-time verification, global coverage, and fraud detection capabilities	27	<b>About Liminal</b>	<b>41</b>
						Several leading vendors piecemeal capabilities and features through partnerships with leading end-point solutions to build platforms	28		



# Market Overview

## Key Takeaways

- 1. Synthetic Identities and Deepfakes Challenge Identity Verification Standards:** Financial institutions struggle to combat AI-generated fraud, with 87% of organizations unequipped to handle deepfakes and 79% unprepared for challenges with synthetic identities. The primary challenges include a lack of advanced AI/ML models to detect synthetic content and dependence on outdated legacy systems lacking agility, integration capabilities, and real-time adaptability. Institutions must enhance their detection capabilities as fraud techniques evolve to prevent traditional KYC measures from becoming ineffective.<sup>1</sup>
- 2. Perpetual KYC (pKYC) Gains Momentum as Static Compliance Checks Become Obsolete:** pKYC adoption is accelerating as institutions seek automated real-time risk monitoring over periodic, manual reviews. Among large financial institutions, 34% have already adopted pKYC, and 61% plan to implement it, while mid-sized organizations face resource constraints limiting adoption.<sup>1</sup> 76% of pKYC adopters report improved compliance accuracy and faster risk detection, emphasizing the shift toward continuous compliance models that reduce reliance on outdated, static KYC workflows.<sup>1</sup>
- 3. Mobile Driver's Licenses (mDLs) Show Limited Adoption as Existing AML Solutions Remain Sufficient:** mDLs are often cited as a potential digital identity solution for AML. However, few institutions currently use them; overall adoption has yet to materialize. While larger organizations show some interest (45% exploring mDLs), adoption is stalled by a lack of regulatory alignment, interoperability challenges, and the absence of a compelling compliance advantage over existing solutions.<sup>1</sup> Without clear regulatory backing or a demonstrable efficiency gain, mDLs remain an unproven tool in AML workflows.

## Current Challenges<sup>1</sup>

- **Integration Complexity Remains a Barrier for Organizations:** The complexity of integrating automated solutions with existing systems is a major barrier, with 66% citing it as a challenge in KYC automation.
- **Synthetic Identities and Deepfakes are Emerging as the Most Pressing Threats in Identity Verification:** A majority of organizations feel unprepared for synthetic identities (79%) and deepfakes (87%), highlighting challenges posed by gen-AI in onboarding.
- **Geopolitical Developments and Sanctions Drive Stricter Compliance Requirements:** Geopolitical developments and sanctions have increased enhanced due diligence requirements for 40% of organizations and verification challenges for 32%.

## Future Demands

- **pKYC Is Becoming the New Standard:** The market is moving toward pKYC, with 72% planning adoption within two years, shifting from static onboarding to continuous risk assessment.<sup>1</sup>
- **mDLs Are Gaining Traction:** As digital ID ecosystems mature and regulatory frameworks catch up, mDL consideration is accelerating in adoption, with 69% of practitioners now considering them for identity verification.<sup>1</sup>
- **Increase in Importance in Partnerships and Analytical Capabilities:** While accuracy and compliance remain core to KYC, partnerships and analytics are gaining ground, up 17% and 12%, respectively. This reflects a need for broader geographic coverage and smarter tools to detect increasingly complex fraud.<sup>1</sup>

## Leading Key Purchasing Criteria (KPC) for KYC Solutions<sup>2</sup>

- **Accuracy:** 91% of KYC Practitioners consider accuracy important when selecting a solution.
- **Data Quality:** 89% of KYC Practitioners consider data quality important when selecting a solution.
- **Regulatory Compliance:** 89% of KYC Practitioners consider regulatory compliance important when selecting a KYC solution.
- **Scalability:** 79% of KYC Practitioners consider scalability important when selecting a KYC solution.

(1) Anti-Money Laundering Buyer Demand Survey, January 2025 (N=53)

(2) The Key Purchasing Criteria percentages shown here are based on a weighted average calculation.

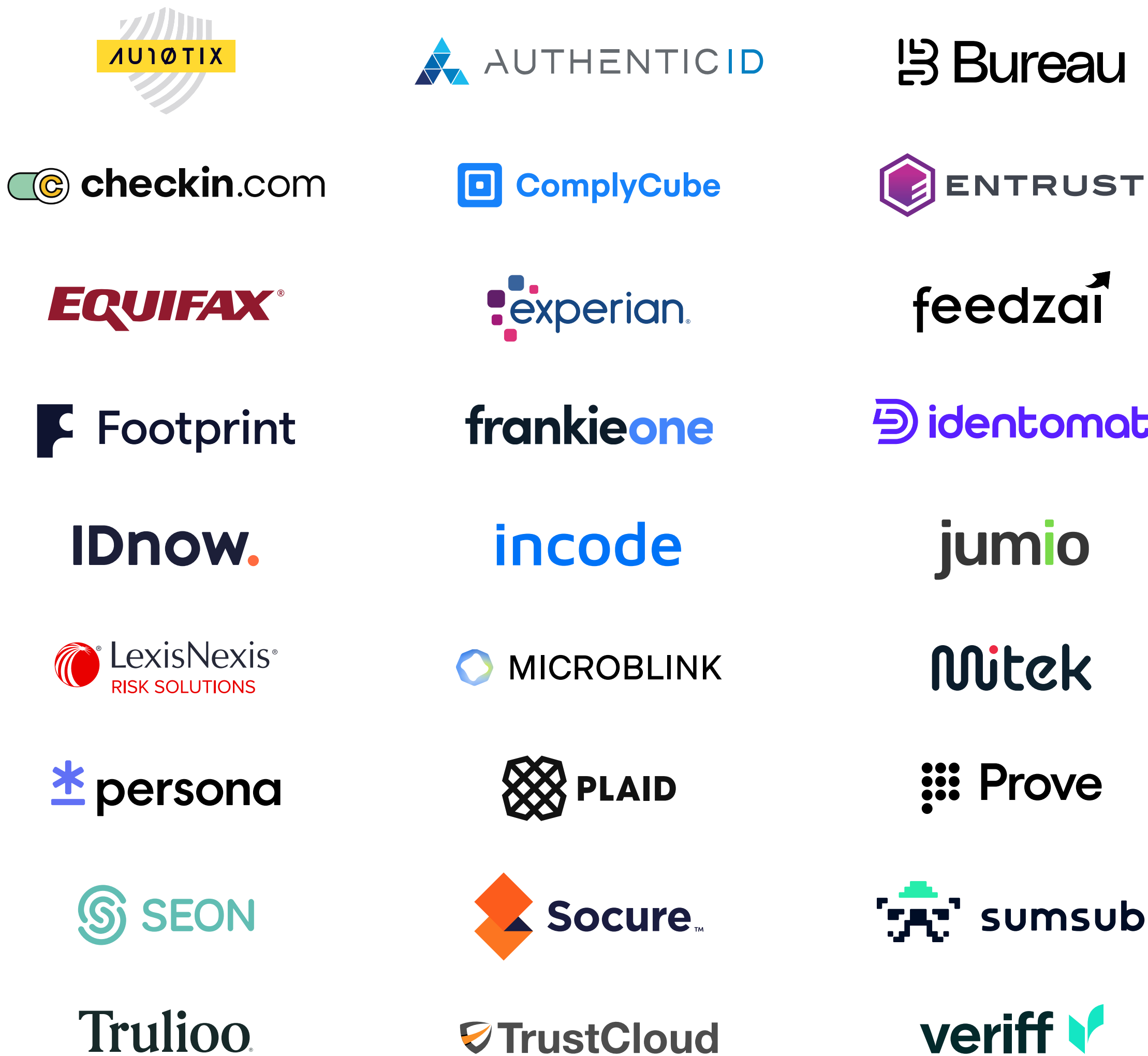
# Vendor Landscape

Liminal’s Know Your Customer (KYC) vendor landscape analysis identifies the top 27 vendors addressing the complexity of verifying real-world identities in digital environments. Challenges arise from evolving fraud tactics, diverse global regulations, and the growing need for accurate, scalable verification. Vendors within this landscape offer specialized approaches, categorized into three primary groups: End-to-end AML Platform Players, KYC-Focused Platforms, and Document Verification and Biometrics Specialists.

## Landscape Analysis (Market Analysis)

- **End-to-end AML Platform Players:** These vendors focus on KYC by offering advanced tools for transaction monitoring, identity risk scoring, behavioral analytics, and AML compliance. They typically integrate with banking and fintech platforms to flag suspicious activities and assess user risk in real time. Many also provide fraud detection and identity verification features to support broader financial compliance needs.
- **KYC-Focused Platforms:** These platforms offer a complete KYC stack; document verification, biometric checks, watchlist screening, and continuous monitoring built for onboarding and ongoing identity lifecycle management. Geared toward global compliance, they support multiple regulatory frameworks with modular APIs and strong automation, making them ideal for scalable KYC operations.
- **Document Verification and 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 and liveness detection. Core strength lies in real-time IDV, often powering onboarding flows in fintech, gaming, and mobility.

## Leading Vendors for KYC







LINK INDEX

# Use Case Overview

©2025 Liminal Strategy, Inc. All rights reserved. Liminal and the Liminal marks used herein are trademarks or registered trademarks of Liminal Strategy, Inc. Other product and company names mentioned herein are the trademarks of their respective owners. No part of this copyrighted work may be reproduced, modified, or distributed in any form or manner without the prior written permission of Liminal.

Liminal Confidential



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

AML is the overarching domain governing multiple interconnected use cases, including KYC, Business and Entity Verification (BEV), and transaction monitoring. Within this framework, KYC plays a critical role in verifying identities, assessing risk, and preventing fraud. KYC is essential for AML compliance since it helps financial institutions verify identities, assess risk, and prevent illicit activity. As digital banking, fintech, cryptocurrency, and cross-border payments expand, KYC is critical for combating money laundering, terrorism financing, and synthetic identity fraud. However, compliance is increasingly complex due to evolving fraud tactics and regulations fragmented by specific regions and verticals, such as the USA PATRIOT Act, and the EU's 6 Anti-Money Laundering Directive (6AMLD).

A core challenge is balancing security with seamless onboarding. Excessive verification steps cause high abandonment rates, while weak controls invite fraud and regulatory non-compliance penalties. Neobanks and fintechs optimize for speed, using AI-driven identity verification to reduce friction. In contrast, crypto exchanges and cross-border payment providers require enhanced due diligence, including biometric authentication and AI-powered anomaly detection, to counteract higher fraud risks.

As fraudsters increasingly use deepfakes and synthetic identities, financial institutions must strengthen defenses with the following tools.

- AI-powered risk assessments: real-time anomaly detection reduces manual reviews.
- Automated compliance frameworks: continuous monitoring not only supports adherence to 6AMLD but also helps detect AI-powered fraud that may have bypassed controls during onboarding.

Liminal's proprietary market sizing model, constructed using a bottoms-up approach, is grounded in a comprehensive assessment of the potential demand for solutions. This increasing market demand highlights the need for effective KYC frameworks across financial services.

KYC has always been a core regulatory requirement for financial integrity and compliance. However, leading platforms are now evolving beyond baseline compliance by leveraging KYC data and technologies to unlock additional value—such as detecting fraudulently opened accounts, improving risk scoring, and enhancing customer insights. In today's environment, modernizing KYC is not just about meeting regulations; it's about strengthening trust, reducing fraud, and improving the overall customer experience.

# To support KYC, vendors must meet five core requirements, each with varied capabilities to match evolving compliance and customer demands

Five 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 [Link™](#). 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

Requirement	Capability¹	Buyer Demand²
<b>Detect Anomalous User Activity:</b> Detecting anomalous user activity involves using behavioral analytics and machine learning to identify deviations from normal patterns, helping to prevent security threats, unauthorized access, and fraud while ensuring system integrity.	Customer Risk Profiling	High
	Behavioral Analytics	Medium
	Behavioral Biometrics	Medium
	Bot Detection	Medium
	Synthetic Identity Fraud Risk Scoring	Medium
<b>Generate a Dynamic User Risk Score:</b> User risk scoring assesses users' risk levels based on behaviors, transaction history, and other factors, enabling organizations to adjust security measures and responses dynamically in real time.	Customer Risk Profiling	High
	AML Risk Scoring	Medium
	Behavioral Analytics	Medium
	Behavioral Biometrics	Medium
	Bot Detection	Medium
	Negative News / Adverse Media Monitoring	Medium

(1) [Liminal Link](#)  
(2) AML Buyer Demand Survey, January 2025 (N=53)

Requirement	Capability¹	Buyer Demand²
<b>Generate a Dynamic User Risk Score:</b> User risk scoring assesses users' risk levels based on behaviors, transaction history, and other factors, enabling organizations to adjust security measures and responses dynamically in real time.	Synthetic Identity Fraud Risk Scoring	Medium
	Verification of Employment (VOE)	Low
	Verification of Income (VOI)	Low
<b>Perform Customer Due Diligence:</b> CDD involves verifying customer identity, assessing risk profiles, and monitoring transactions to ensure regulatory compliance and detect potential money laundering or terrorist financing.	Address Verification	High
	Document Verification	High
	Government Identification Number Verification	High
	Name Verification	High
	Active Liveness Detection	Medium
	Negative News / Adverse Media Monitoring	Medium
	PEP (Politically Exposed Persons) Screening	Medium
	Passive Liveness Detection	Low
	Verification of Employment (VOE)	Low
	Verification of Income (VOI)	Low
<b>Document an Audit Trail:</b> Audit trails systematically record all actions and changes within a system, enabling accountability, compliance, and security by providing a detailed log of transactions, user activities, and system modifications.	CDD/EDD Audit Trail Management	Medium
	Electronic AML Regulatory Report Filing	Low
<b>Prepare and Submit Regulatory Reports:</b> Regulatory reporting ensures timely, accurate submission of compliance reports by collecting and formatting data to meet industry regulations and minimize non-compliance risks.		

# KYC solution buyers include compliance professionals such as AML Officers, Chief Compliance Officers, and Compliance Program Managers



## AML Officer

The AML Officer in a bank is responsible for overseeing the institution’s anti-money laundering efforts. This includes implementing and managing AML policies, monitoring transactions for suspicious activity, and ensuring compliance with regulatory requirements. The AML Officer works closely with compliance teams and other stakeholders to identify and mitigate money laundering risks while adhering to legal standards.



## Chief Compliance Officer (CCO)

The Chief Compliance Officer (CCO) is a C-Suite executive responsible for confirming that the institution meets all regulatory and legal requirements. This role involves developing and implementing compliance programs, monitoring regulatory changes, and managing risk related to financial crimes, consumer protection, and corporate governance. As a senior leader, the CCO works closely with other executives to maintain the integrity and ethical standards of the bank.



## KYC Program Manager

The KYC Program Manager is in a mid-level management role and oversees the development, implementation, and execution of the bank’s KYC processes. This role involves managing compliance with regulatory requirements, coordinating cross-departmental efforts, and confirming the effective onboarding and ongoing monitoring of customers. The KYC Program Manager typically leads teams, collaborates with senior leadership, and drives program success.



# An AML Officer overseeing KYC ensures compliance through customer ID, due diligence, risk assessment, and automation to boost efficiency



## AML Officer

An AML Officer focused on KYC in banking is responsible for implementing and overseeing customer identification and verification processes to ensure compliance with regulatory requirements. They monitor KYC practices to detect potential money laundering risks, conduct customer due diligence, and ensure accurate documentation and risk assessments. The AML Officer also ensures that the institution adheres to evolving KYC standards while working to prevent financial crime and maintain regulatory compliance.



### Goals

- Ensure Regulatory Compliance
- Optimize Monitoring Systems
- Ensure Accurate Customer Identification
- Improve Customer Onboarding Efficiency
- Conduct Ongoing Customer Monitoring



### Needs

- Comprehensive Risk Assessment Tools
- Integrated Third-party Data Sources
- Automation of Manual Tasks



### Frustrations

- Inconsistent Data Quality
- Regulatory Uncertainty
- Reliance on Manual Processes
- High False Positive Rates
- Overwhelming Alert Volume



### Decision Drivers

- Compliance with Regulatory Requirements
- Reliable Data Across Systems
- Scalability with Transaction Volume
- User-friendly Interface
- Automation of Core Workflows



### KPCs

- Compliance and Regulatory Alignment
- Automation
- Data Quality
- Scalability
- Internal User Experience

# A Chief Compliance Officer ensures KYC compliance by leading customer verification, risk assessments, and due diligence to reduce financial crime risk



## Chief Compliance Officer (CCO)

A CCO focused on KYC in banking is responsible for ensuring that the institution properly identifies and verifies customer identities in compliance with regulatory standards. They oversee the development and execution of KYC policies, ensuring accurate risk assessments and customer due diligence processes. The CCO manages KYC procedures to detect and prevent financial crimes such as money laundering and fraud while maintaining regulatory compliance and protecting the bank's integrity.



### Goals

- Ensure Regulatory Compliance
- Minimize Financial Crimes Risk
- Improve Customer Onboarding Efficiency
- Enhance Customer Risk Profiling
- Strengthen GRC Program



### Needs

- Integrated Third-Party Data Sources
- Automation of Manual Tasks
- Regular Compliance Reports
- Comprehensive Risk Assessment Tools



### Frustrations

- Regulatory Uncertainty
- Customer Friction and Abandonment
- Resource Constraints
- Inconsistent Data Quality
- Reliance on Manual Processes



### Decision Drivers

- Compliance with Regulatory Requirements
- Automation of Core Workflows
- Reliable Data Across Systems
- Scalability with Transaction Volume



### KPCs

- Compliance and Regulatory Alignment
- Automation Capabilities
- Data Quality
- Customer Experience
- Scalability

# A KYC Program Manager ensures compliance by managing ID, onboarding, and risk checks using automation, data integration, and analytics tools



## KYC Program Manager

A KYC Program Manager focused on banking oversees the development, implementation, and management of the bank's KYC program. They ensure customer identification and verification processes align with regulatory requirements and best practices. The KYC Program Manager works to enhance onboarding efficiency, customer due diligence, and risk assessment procedures while maintaining strong compliance with AML regulations.



### Goals

- Ensure Regulatory Compliance
- Minimize Financial Crimes Risk
- Improve Customer Onboarding Efficiency
- Drive Operational Efficiency and Effectiveness
- Ensure Accurate Customer Identification



### Needs

- Unified Customer View
- Automation of Manual Tasks
- Integrated Third-Party Data Sources
- Integrated Data Analytics
- Data Security and Privacy Protections



### Frustrations

- Fragmented or Siloed Data
- Reliance on Manual Processes
- Regulatory Uncertainty
- High False Positive Rates
- Complex Systems Integration



### Decision Drivers

- Compliance with Regulatory Requirements
- Reliable Data Across Systems
- Automation of Core Workflows
- Scalability with Transaction Volume

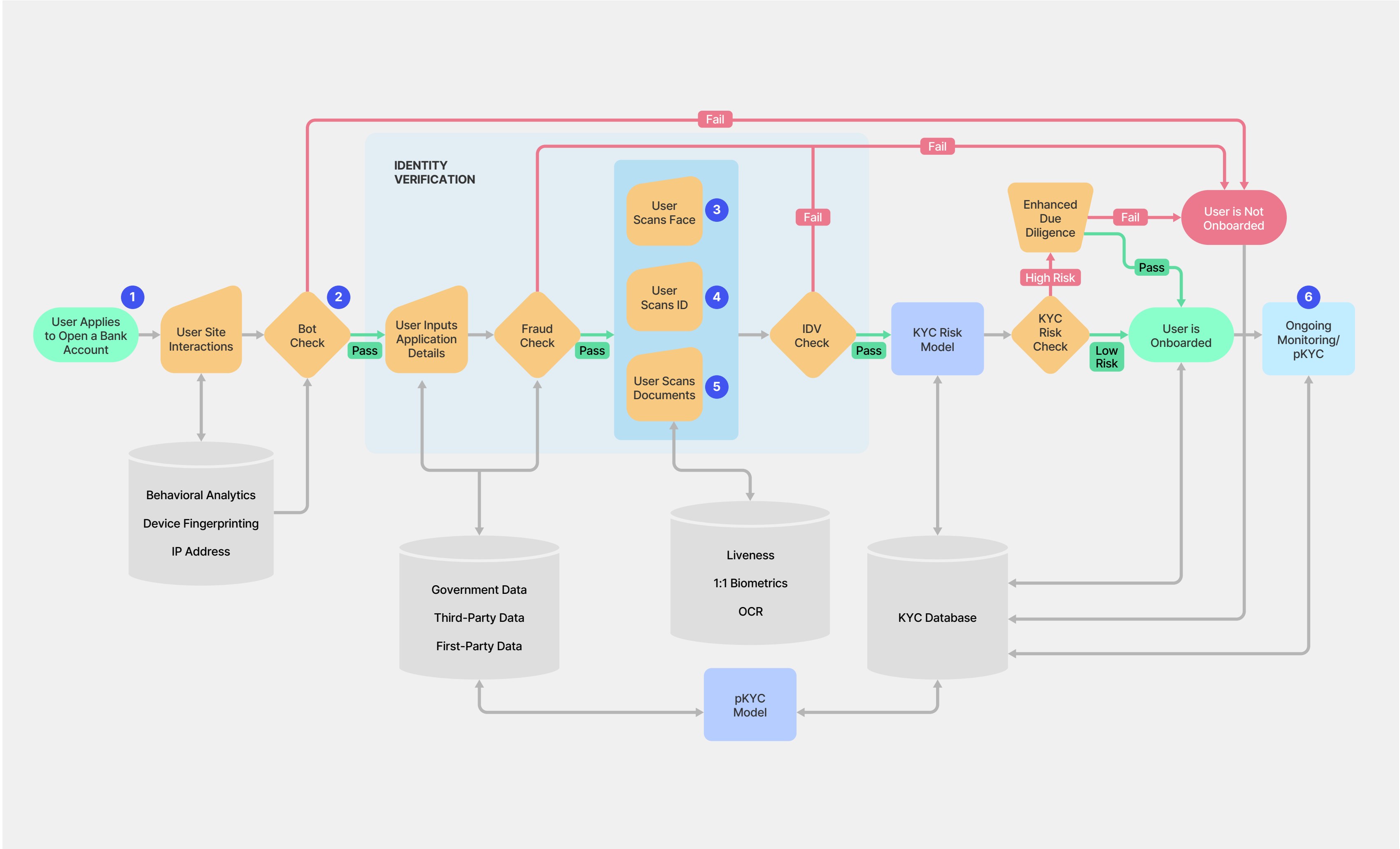


### KPCs

- Pricing
- Compliance and Regulatory Alignment
- Data Quality
- Automation Capabilities
- Global Coverage



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



**1 User Initiates Account Creation.** The KYC process starts when a user signs up. The system collects personal and device data to build an initial user profile..

**2 Risk Assessment.** The platform analyzes location, IP history, device info, and behavior to assess risk based on the data collected during registration.

**3 Identity Verification.** Users upload ID documents. The system uses OCR and databases to extract, validate, and check the document's authenticity.

**4 Biometric Verification.** Users take a live selfie. Facial recognition and liveness checks confirm their identity against the submitted ID photo.

**5 Sanctions Screening and Proof of Address.** Users provide proof of address. The platform verifies documents and screens against sanctions lists.

**6 Ongoing Monitoring.** After verification, the system tracks user activity, flagging suspicious behavior through real-time anomaly detection.

**7 Periodic Re-verification.** Users are asked to periodically resubmit ID and biometrics to ensure their information is accurate and up to date.

**8 Reporting and Compliance.** The platform logs all KYC steps and anomalies in reports that support regulatory audits and compliance checks.





LINK INDEX

# Market Overview

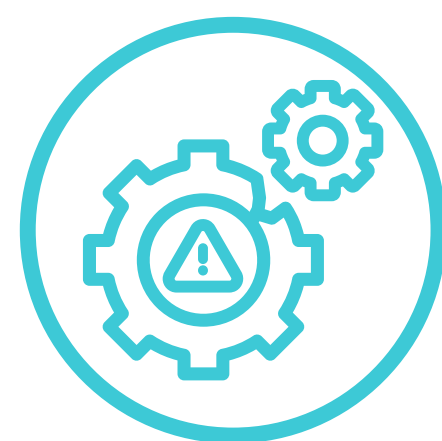
©2025 Liminal Strategy, Inc. All rights reserved. Liminal and the Liminal marks used herein are trademarks or registered trademarks of Liminal Strategy, Inc. Other product and company names mentioned herein are the trademarks of their respective owners. No part of this copyrighted work may be reproduced, modified, or distributed in any form or manner without the prior written permission of Liminal.

Liminal Confidential





# Firms struggle to integrate automation amid rising due diligence demands from sanctions, synthetic IDs, and deepfake-related fraud threats



## Integrating new automation with legacy systems is a key barrier to optimizing KYC processes

With most practitioners looking to automate tasks in their KYC processes, 66% of survey respondents cite that the complexity of integration with existing systems is a challenge their organizations face when automating KYC processes. The high complexity of integration is a barrier to automation adoption in KYC processes.<sup>1</sup>



## A majority of organizations feel unprepared to handle synthetic identities and deepfakes

Most respondents (79%) feel that their organization is not equipped to deal with synthetic identities. In comparison, 87% feel that they are not equipped to deal with deepfakes, highlighting the challenges that gen-AI has caused in onboarding new customers.<sup>1</sup>



## Geopolitical developments and sanctions have led to additional challenges for KYC processes

Due to recent geopolitical events and sanctions, 40% of respondents have increased enhanced due diligence requirements. Additionally, 32% report challenges verifying individuals—especially in high-risk regions—linked to these developments.<sup>1</sup>

(1) AML Buyer Demand Survey, January 2025 (N=53)

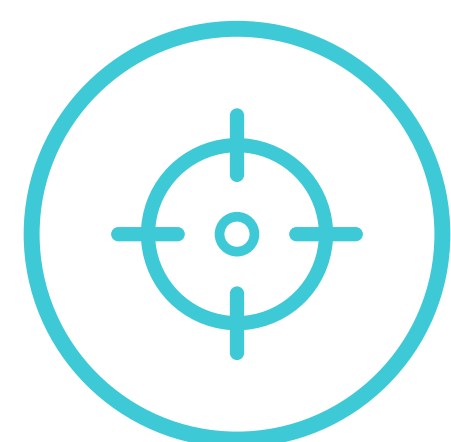


# KYC automation speeds onboarding as buyers prioritize accuracy, compliance, and vendor consolidation for a unified AML strategy



## Most practitioners automate KYC tasks to speed up reviews, decisions, and onboarding

Today, 98% of practitioners automate some tasks for KYC, with 30% automating most. Automation practitioners see faster reviews and decision-making, accelerating KYC processes and leading to quicker customer onboarding.<sup>1</sup> In contrast, organizations with limited automation struggle with bottlenecks, higher operational costs, and greater exposure to regulatory scrutiny.



## Accuracy tops KYC buying criteria, followed by data quality, compliance, and scalability

91% of respondents cite accuracy as the top purchasing criterion for KYC solutions.<sup>1</sup> Data quality and regulatory compliance also rank highly, followed by scalability. As transaction volumes grow and threats evolve, organizations need solutions that ensure high data quality, meet compliance standards, and scale efficiently.



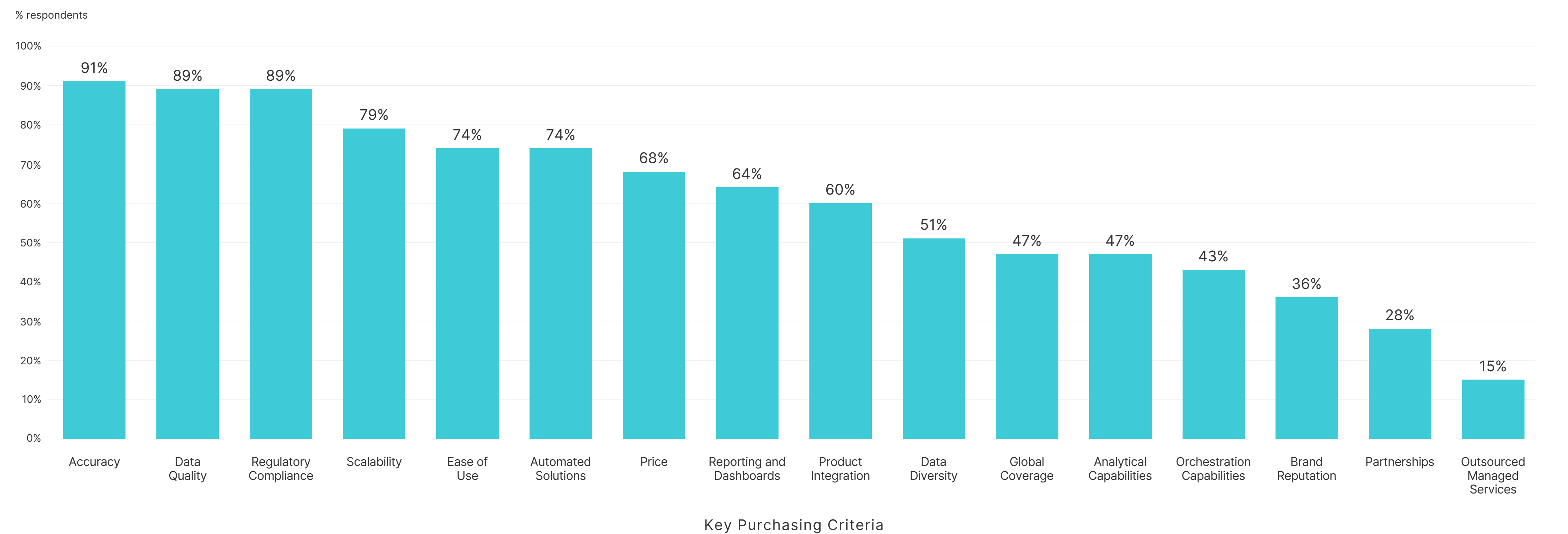
## Practitioners seek to consolidate vendors for a unified AML approach, driving demand for integrated solutions

Just over half of practitioners (55%) want to consolidate their vendor list, opting for a more unified approach to AML.<sup>1</sup> This shift indicates a demand for integrated solutions that streamline compliance, reduce complexity, and improve operational efficiency. Vendors offering end-to-end AML capabilities will have a competitive edge in this market.

(1) AML Buyer Demand Survey, January 2025 (N=53)

# KYC practitioners prioritize accuracy, data quality, regulatory compliance, and scalability as the most important criteria in their purchasing process

Key Purchasing Criteria for KYC Solutions<sup>1</sup>



Citation: (1) AML Buyer Demand Survey, January 2025 (N=53)

# The market is moving toward pKYC and mDLs, while priorities are shifting toward partnerships, analytics, and integration



## The market is moving toward pKYC, with the majority of organizations planning adoption within two years

The market is shifting toward pKYC, or continuous monitoring, moving beyond traditional onboarding checks to ongoing risk assessment. While KYC verifies customers at account creation, pKYC continuously monitors users post-onboarding to detect suspicious activities in real time. Within the next two years, 72% of survey respondents plan to adopt pKYC, highlighting the growing demand for proactive compliance and risk management.<sup>1</sup>



## KYC automation boosts onboarding as firms prioritize accuracy, compliance, and consolidation

With 69% of practitioners considering mDLs and other eIDs for customer identification, adoption is set to rise. While consumer adoption remains limited, expanding use cases position this technology as a crucial component of future identity verification. As regulatory frameworks evolve and digital identity ecosystems mature, mDLs and eIDs will be central in streamlining authentication and verification.<sup>1</sup>



## Accuracy, data, and compliance lead KYC picks, but analytics and partnerships are rising

While accuracy, data quality, and regulatory compliance remain fundamental in KYC solution selection, the biggest shift is the importance of partnerships and analytical capabilities, which are expected to rise by 17% over two years. Integration has also gained traction, which will increase by 12%, while the significance of dashboards and data diversity is declining.<sup>1</sup>

(1) AML Buyer Demand Survey, January 2025 (N=53)





# Link Index

©2025 Liminal Strategy, Inc. All rights reserved. Liminal and the Liminal marks used herein are trademarks or registered trademarks of Liminal Strategy, Inc. Other product and company names mentioned herein are the trademarks of their respective owners. No part of this copyrighted work may be reproduced, modified, or distributed in any form or manner without the prior written permission of Liminal.

Liminal Confidential





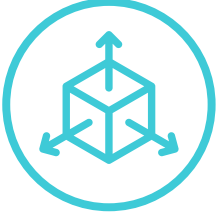




# Vendor products were evaluated based on their coverage of product capabilities and performance against top solution purchasing criteria

Requirement	Capability <sup>1</sup>	Buyer Demand <sup>2</sup>
<b>Detect Anomalous User Activity:</b> Detecting anomalous user activity involves using behavioral analytics and machine learning to identify deviations from normal patterns, helping to prevent security threats, unauthorized access, and fraud while ensuring system integrity.	Behavioral Biometrics	High
	Behavioral Analytics	Medium
	Bot Detection	Medium
	Synthetic Identity Fraud Risk Scoring	Medium
	Synthetic Identity Fraud Risk Scoring	Low
<b>Generate a Dynamic User Risk Score:</b> User risk scoring assesses users' risk levels based on behaviors, transaction history, and other factors, enabling organizations to adjust security measures and responses dynamically in real time.	Verification of Employment (VOE)	High
	Verification of Income (VOI)	High
	Behavioral Analytics	Medium
	Behavioral Biometrics	Medium
	Bot Detection	Medium
	Negative News / Adverse Media Monitoring	Medium
	Synthetic Identity Fraud Risk Scoring	Medium
	AML Risk Scoring	Low
	Customer Risk Profiling	Low
	Negative News / Adverse Media Monitoring	High
<b>Perform Customer Due Diligence:</b> CDD involves verifying customer identity, assessing risk profiles, and monitoring transactions to ensure regulatory compliance and detect potential money laundering or terrorist financing.	Passive Liveness Detection	High
	Verification of Income (VOI)	High
	Active Liveness Detection	Medium
	Government Identification Number Verification	Medium
	PEP (Politically Exposed Persons) Screening	Medium
	Verification of Employment (VOE)	Medium
	Address Verification	Low
	Document Verification	Low
	Name Verification	Low
	CDD/EDD Audit Trail Management	High
<b>Document an Audit Trail:</b> Audit trails systematically record all actions and changes within a system, enabling accountability, compliance, and security by providing a detailed log of transactions, user activities, and system modifications.		
<b>Prepare and Submit Regulatory Reports:</b> Regulatory reporting ensures timely, accurate submission of compliance reports by collecting and formatting data to meet industry regulations and minimize non-compliance risks.	Electronic AML Regulatory Report Filing	High

(1) [Liminal Link](#)  
(2) AML Buyer Demand Survey, January 2025 (N=53)

Additional Factors for Consideration		
Accuracy		The precision of results, minimizing false positives and false negatives when validating user identities.
Buyer Satisfaction		The extent of buyer satisfaction with a vendor's solution for KYC.
Orchestration		The ability to configure and manage multiple identity verification workflows dynamically, integrating various data sources and risk signals for streamlined processes.
Data Quality		The completeness, accuracy, and timeliness of user identity data.
Scalability		The ability of the KYC solution to efficiently handle growing volumes of customer verifications across different geographies and regulatory environments.

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



## Ease of Use

A user-friendly KYC solution streamlines onboarding, case management, and workflow maintenance, reducing operational friction and ensuring compliance teams can work efficiently.



## Automation

Automating verification reduces manual effort, accelerates decision-making, and minimizes errors, helping organizations meet compliance requirements faster and at scale.



## Integration

Seamless connectivity with compliance, fraud detection, and customer onboarding systems ensures a holistic approach to risk management and reduces data silos.



## Price

Cost-effectiveness is critical, as high per-verification fees and additional charges can make scaling KYC operations expensive, impacting long-term sustainability.



## Global Coverage

Organizations operating across multiple jurisdictions need broad identity verification capabilities to comply with varying regulatory requirements and access diverse data sources.



## Account Opening (AO) Fraud Capabilities

Detecting synthetic identities and stolen credentials at account opening is essential to preventing fraud before bad actors gain access to financial services.



## pKYC Capabilities

Continuous monitoring of customer risk profiles enhances compliance by proactively detecting emerging risks, reducing reliance on periodic reviews, and adapting to evolving regulations.

# The market presence of KYC vendors was evaluated based on leadership perception, brand awareness, company size, and company growth



## Market Leadership Perception / Brand Reputation

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.



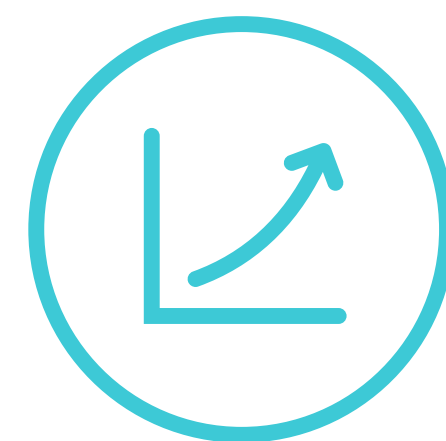
## Brand Awareness

This metric measures how familiar buyers are with a vendor in identity verification. Strong brand awareness fosters trust, reduces perceived risk, and reassures buyers of solution quality and compliance. Recognizable vendors are more likely to be chosen, as familiarity signals reliability and confidence in their verification technology.



## 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 identity verification, this ensures stability, scalability, and strong compliance while making them well-equipped to meet evolving security and verification demands.



## Employee Growth (Year-over-Year)

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.



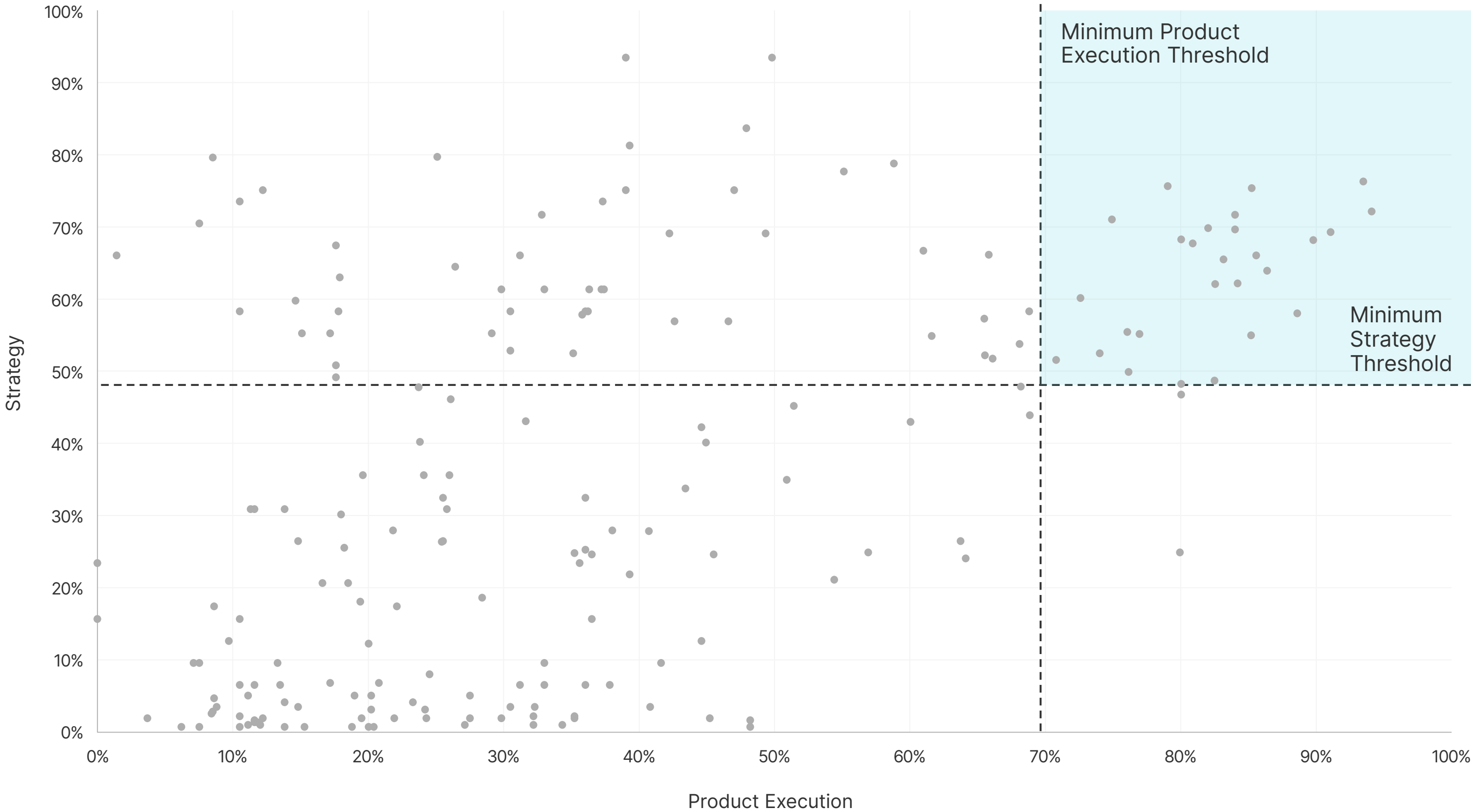
# Minimum product execution and strategy thresholds were established to identify the leading vendors for KYC

## Minimum Product Execution Threshold

To establish a minimum product execution threshold for KYC, we surveyed buyers across key industries to identify the most highly valued capabilities. These include satisfaction, accuracy, orchestration, data quality, and scalability. By prioritizing these capabilities based on buyer demand, we determined that a vendor must achieve a minimum product execution score of 69% to sufficiently meet a leading KYC solution’s functional and compliance requirements.

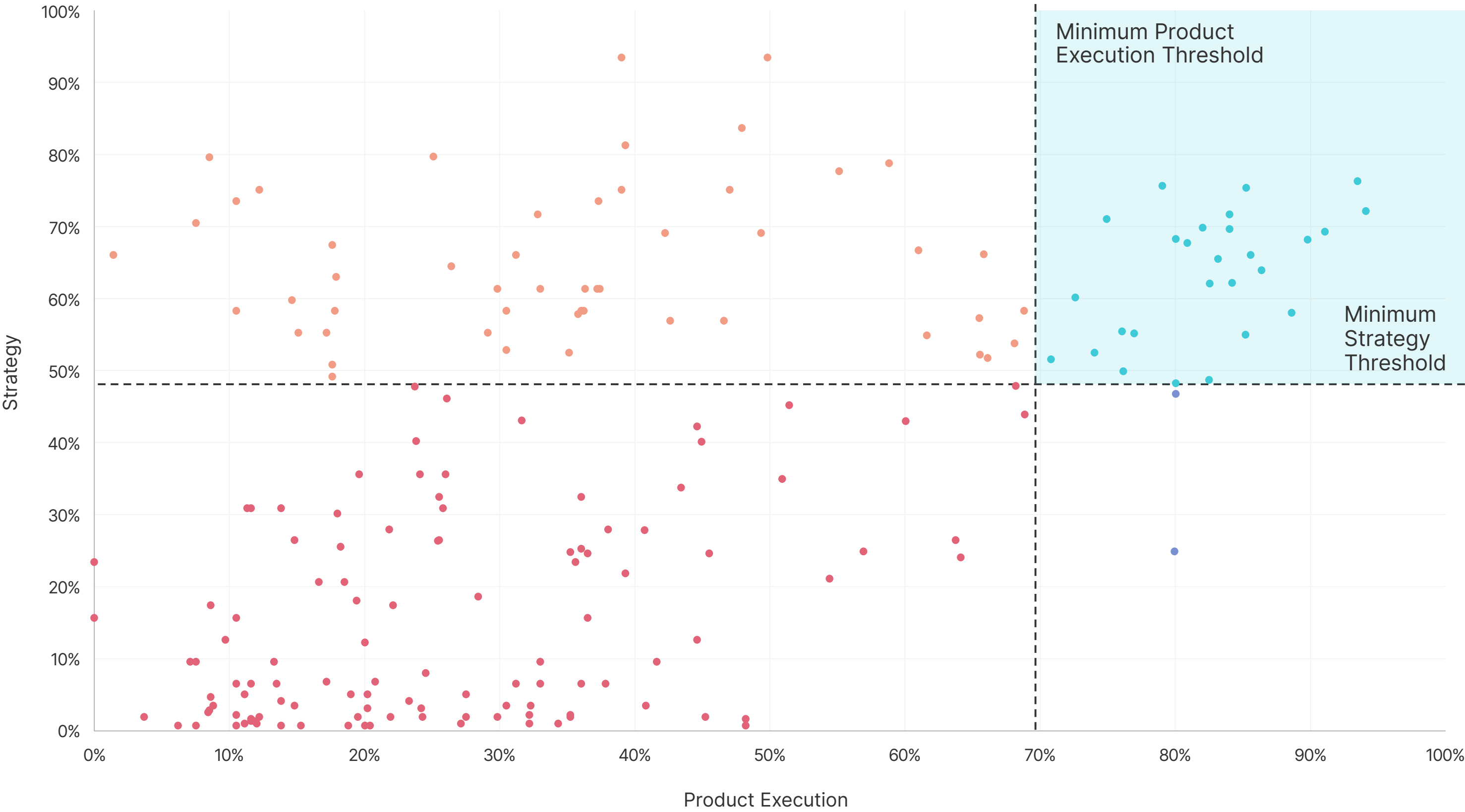
## Minimum Strategy Threshold

We analyzed a leadership strategy threshold for KYC by analyzing critical future demand elements. These elements include an easy-to-use solution, automation, integration capabilities, vast global coverage, continuous monitoring, and fraud capabilities. Leading vendors must achieve a minimum strategy score of 49% to demonstrate a forward-thinking approach that aligns with the market’s evolving needs.



# Among the 191 vendors Liminal evaluated that solve the KYC use case, 27 leading vendors met the minimum product and strategy threshold

- **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
- **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





# Liminal evaluated 191 vendors that solve the KYC use case across the product and strategy criteria, and determined 27 leading vendors





# Link Index Leading Vendor for Know-Your-Customer in 2025

This view includes the product and strategy score cut-off, showcasing the 27 Leading Vendors for this year’s KYC Index



# KYC vendors take distinct approaches based on use case complexity, risk tolerance, and regulatory needs



## End-to-end AML Platform Players

These vendors focus on KYC by offering advanced tools for transaction monitoring, identity risk scoring, behavioral analytics, and AML compliance. They typically integrate with banking and fintech platforms to flag suspicious activities and assess user risk in real time. Many also provide fraud detection and identity verification features to support broader financial compliance needs.



## KYC and Compliance Platforms

These platforms offer a complete KYC stack: document verification, biometric checks, watchlist screening, and continuous monitoring built for onboarding and ongoing identity lifecycle management. Geared toward global compliance, they support multiple regulatory frameworks with modular APIs and strong automation, making them ideal for scalable KYC operations.



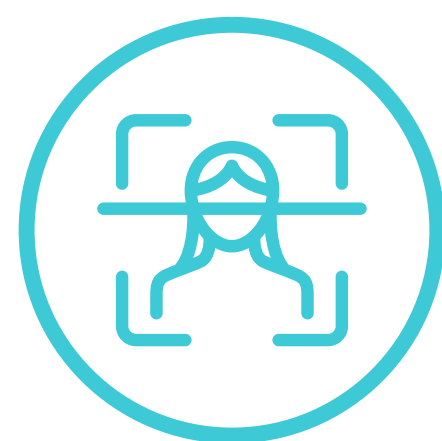
## Document and Biometric Verification

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 and liveness detection. Core strength lies in real-time IDV, often powering onboarding flows in fintech, gaming, and mobility.

(1) Liminal Anti-Money Laundering Buyer Demand Survey, January 2025 (N=40)



# Leading vendors are shaping the future of KYC through real-time verification, global coverage, and fraud detection capabilities



## Real-time, Frictionless Verification

Leading KYC vendors are streamlining user onboarding through instant identity verification powered by document scanning, facial biometrics, and automated decision-making. These solutions reduce friction without compromising accuracy and enable platforms to scale quickly while improving conversion rates. By minimizing manual reviews and error-prone inputs, they support fast-growing fintechs, crypto platforms, and digital banks that prioritize speed and compliance.



## Global, Multi-Jurisdictional Coverage




















Top vendors are building verification infrastructure that spans countries, languages, and regulatory regimes. They support various government-issued IDs and local KYC requirements to help global platforms onboard users compliantly across markets. Whether aligning with the General Data Protection Regulation (GDPR) in Europe, Financial Action Task Force (FATF) recommendations, or specific eKYC frameworks, these vendors make it easier to expand internationally while remaining audit-ready and regulation-compliant.



## Advanced Fraud and Risk Detection

These vendors go beyond basic KYC by integrating real-time fraud detection during onboarding. They help detect synthetic identities, bot attacks, social engineering, and deepfake attempts. By embedding proactive fraud detection into identity verification workflows, they're turning compliance checkpoints into active security controls, which are especially valuable in high-risk industries.

# Several leading vendors piecemeal capabilities and features through partnerships with leading end-point solutions to build platforms

Capability	Capability Definitions and Vendor Offerings	Exemplary Leaders
Account Opening Fraud	Vendors in this space leverage tools like behavioral analytics, behavioral biometrics, device fingerprinting, identity graphing, and risk scoring to help detect and prevent account opening fraud.	 
AML Screening	Vendors in this space conduct advanced screening of individuals and entities using adverse media feeds and global watchlists to more accurately detect PEPs, sanctioned entities, and high-risk affiliations.	 
Deterministic Data	Vendors in this space provide verified and authoritative personal data that can be confidently matched to an individual, often through partnerships with credit bureaus, government registries, and telecommunications providers.	  
Document Verification	Vendors in this space use Optical Character Recognition (OCR), image forensics, and template validation to verify ID documents, checking for authenticity, tampering, and compliance with expected formats.	 
eCBSV/ Social Security Verification	eCBSV (Electronic Consent Based Social Security Number Verification) is a service that allows approved entities to verify if a person's name, date of birth, and SSN match SSA records in real time, with the individual's consent.	  
Fuzzy Matching	Vendors in this space apply algorithms to identify and reconcile non-exact matches across identity records, helping unify fragmented data entries.	
Liveness/Biometric	Vendors in this space offer facial recognition and liveness detection techniques to ensure that users are physically present and match the submitted identity documents.	  
Probabilistic Data	Vendors in this space use alternative data sources such as social signals, behavioral patterns, and device metadata to infer or corroborate identity attributes, particularly when authoritative PII is limited or unavailable.	  





LINK INDEX

# Vendor Overview

©2025 Liminal Strategy, Inc. All rights reserved. Liminal and the Liminal marks used herein are trademarks or registered trademarks of Liminal Strategy, Inc. Other product and company names mentioned herein are the trademarks of their respective owners. No part of this copyrighted work may be reproduced, modified, or distributed in any form or manner without the prior written permission of Liminal.

Liminal Confidential





# Socure

Link™ Profile [↗](#)

## Company Description

Socure’s KYC solution leverages AI-driven identity verification, fraud detection, and risk assessment to streamline customer onboarding and compliance. Its Risk OS platform integrates document verification, biometric authentication, and real-time decisioning, detecting synthetic identities and fraudulent activity. With continuous monitoring, sanctions screening, and seamless API integration, Socure helps financial institutions and enterprises enhance security while reducing manual reviews.

## Company Information<sup>1</sup> (as of March 24, 2025)

Headquarters	Incline Village, Nevada
No. of Employees	550
Last Raised	\$450MM, Series E, November 2021
Market Cap	N/A
Industry Focus	Financial Services, Fintech, Gaming, Healthcare
Geographic Focus	North America, Europe

Notable Customers

 **Betterment**  

(1) [Socure Link Profile](#)  
(2) 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.

## Socure RiskOS Platform Performance on KYC Link Index Benchmarking Criteria

Criteria Bucket	Avg. Score	Criteria	Performance <sup>2</sup>
Strategy	Exceptional	<b>Automation:</b> The solution’s ability to streamline tasks and reduce effort.	Exceptional
		<b>Account Opening Fraud Capabilities:</b> The ability to detect and prevent fraud at account opening.	Excellent
		<b>Ease of Use:</b> Simplicity of deploying & configuring the solution.	Exceptional
		<b>Global Coverage:</b> Ability to handle verifications across multiple countries and jurisdictions.	Excellent
		<b>pKYC:</b> Continuously monitor customer risk profiles in real time.	Excellent
		<b>Price:</b> The cost-effectiveness of the solution.	Excellent
		<b>Product Integration:</b> The ability to integrate with other systems.	Excellent
Product	Exceptional	<b>Accuracy:</b> The solution’s precision in performing its intended function.	Exceptional
		<b>Buyer Satisfaction:</b> The solution’s satisfaction rating among practitioners.	Excellent
		<b>Data Quality:</b> The completeness, accuracy, and timeliness of data.	Exceptional
		<b>Orchestration:</b> Ability to configure workflows dynamically.	Exceptional
		<b>Product Capability:</b> The solution’s range of features and functionalities.	Exceptional
		<b>Scalability:</b> The solution’s ability to maintain performance at high volumes.	Exceptional
Market Presence	Exceptional	<b>Brand Awareness:</b> Solution’s recognition among practitioners.	Exceptional
		<b>Market Leadership:</b> The solution’s perceived leadership in the market.	Excellent
		<b>Company Size:</b> Total employee headcount.	Excellent
		<b>Employee Growth:</b> Year over year employee growth.	Exceptional



## Analyst Notes

Socure provides a comprehensive KYC solution through its Risk OS platform, integrating identity verification, fraud prevention, and business verification within a single API. The platform supports 20+ pre-built products with workflow orchestration, achieving a 96% auto-decision rate and a 98% true accept rate for document verification. Socure ensures high data quality by employing authoritative and alternative sources, including educational and property records. It delivers 99% verification coverage for mainstream populations, with a 30% higher verification rate for 18-year-olds than competitors, while passive liveness detection reaches 98% accuracy. Risk OS offers pre-built workflows, intelligent data waterfalling, and no-code customization, enabling businesses to streamline verification and fraud prevention. The platform is designed for scalability and provides real-time decision-making with AI-powered fraud detection. It integrates 50+ data services and processes high transaction volumes, which makes it ideal for enterprises needing high-speed, high-accuracy identity verification.

Socure’s business strategy prioritizes automation, ease of use, and global compliance. The platform’s no-code interface features drag-and-drop workflow customization, enabling businesses to modify decision-making logic without API changes. AI-powered automation—including embedded AI agents, pre-configured templates, and real-time model updates—reduces manual intervention while improving fraud detection efficiency. Socure integrates multiple global data sources, such as SSN metadata and authoritative records, to support identity verification across regions. While pricing details were not disclosed, the platform consolidates multiple verification services, potentially lowering operational costs. Risk OS integrates via API with providers like Middesk, Kyckr, and Base Layer to facilitate business verification and compliance automation. It enhances fraud detection for account openings with device intelligence, passive liveness detection, and network analytics, achieving 74% synthetic fraud detection within the top 3% risk band. The platform supports perpetual KYC (pKYC) and monitoring of Politically Exposed Persons (PEPs), adverse media, and sanctions with automated updates and risk-based adjustments. Looking ahead, Socure plans to expand into financial risk assessment with a credit underwriting solution set for Q4 2025.

Socure has established itself as a leader in AI-driven identity verification and fraud prevention, with a strong presence in financial services and government sectors. The company has expanded its market visibility through acquiring Effectiv and continuous enhancements to its Risk OS platform. Serving over 2,800 customers across 40+ industries, Socure utilizes a consortium of more than 4 billion known outcomes to strengthen identity verification and fraud detection. While employee numbers were not disclosed, its growing customer base and industry reach indicate a substantial presence in the identity verification market. Ongoing acquisitions and product expansions suggest continued operational scaling, supporting its growth in AI-driven compliance solutions.

(1) [Liminal Link](#)  
(2) AML Buyer Demand Survey, January 2025 (N=54)

## Socure RiskOS Platform KYC Capabilities

Requirements to Satisfy the Use Case	Product Capability <sup>1</sup>	Buyer Demand <sup>2</sup>
<b>Detect Anomalous User Activity:</b> Detecting anomalous user activity involves using behavioral analytics and machine learning to identify deviations from normal patterns, helping to prevent security threats, unauthorized access, and fraud while ensuring system integrity.	Customer Risk Profiling	High
	Behavioral Analytics	Medium
	Behavioral Biometrics	Medium
	Bot Detection	Medium
	Synthetic Identity Fraud Risk Scoring	Medium
<b>Generate a Dynamic User Risk Score:</b> User risk scoring assesses users’ risk levels based on behaviors, transaction history, and other factors, enabling organizations to adjust security measures and responses dynamically in real time.	Customer Risk Profiling	High
	AML Risk Scoring	Medium
	Behavioral Analytics	Medium
	Behavioral Biometrics	Medium
	Bot Detection	Medium
	Negative News / Adverse Media Monitoring	Medium
	Synthetic Identity Fraud Risk Scoring	Medium
	Verification of Employment (VOE)	Low
<b>Perform Customer Due Diligence:</b> CDD involves verifying customer identity, assessing risk profiles, and monitoring transactions to ensure regulatory compliance and detect potential money laundering or terrorist financing.	Verification of Income (VOI)	Low
	Address Verification	High
	Document Verification	High
	Government Identification Number Verification	High
	Name Verification	High
	Active Liveness Detection	Medium
	Negative News / Adverse Media Monitoring	Medium
	PEP (Politically Exposed Persons) Screening	Medium
	Passive Liveness Detection	Low
	Verification of Employment (VOE)	Low
<b>Document an Audit Trail:</b> Audit trails systematically record all actions and changes within a system, enabling accountability, compliance, and security by providing a detailed log of transactions, user activities, and system modifications.	Verification of Income (VOI)	Low
	CDD/EDD Audit Trail Management	Medium
<b>Prepare and Submit Regulatory Reports:</b> Regulatory reporting ensures timely, accurate submission of compliance reports by collecting and formatting data to meet industry regulations and minimize non-compliance risks.	Electronic AML Regulatory Report Filing	Low



LINK INDEX

# Appendix

©2025 Liminal Strategy, Inc. All rights reserved. Liminal and the Liminal marks used herein are trademarks or registered trademarks of Liminal Strategy, Inc. Other product and company names mentioned herein are the trademarks of their respective owners. No part of this copyrighted work may be reproduced, modified, or distributed in any form or manner without the prior written permission of Liminal.

Liminal Confidential

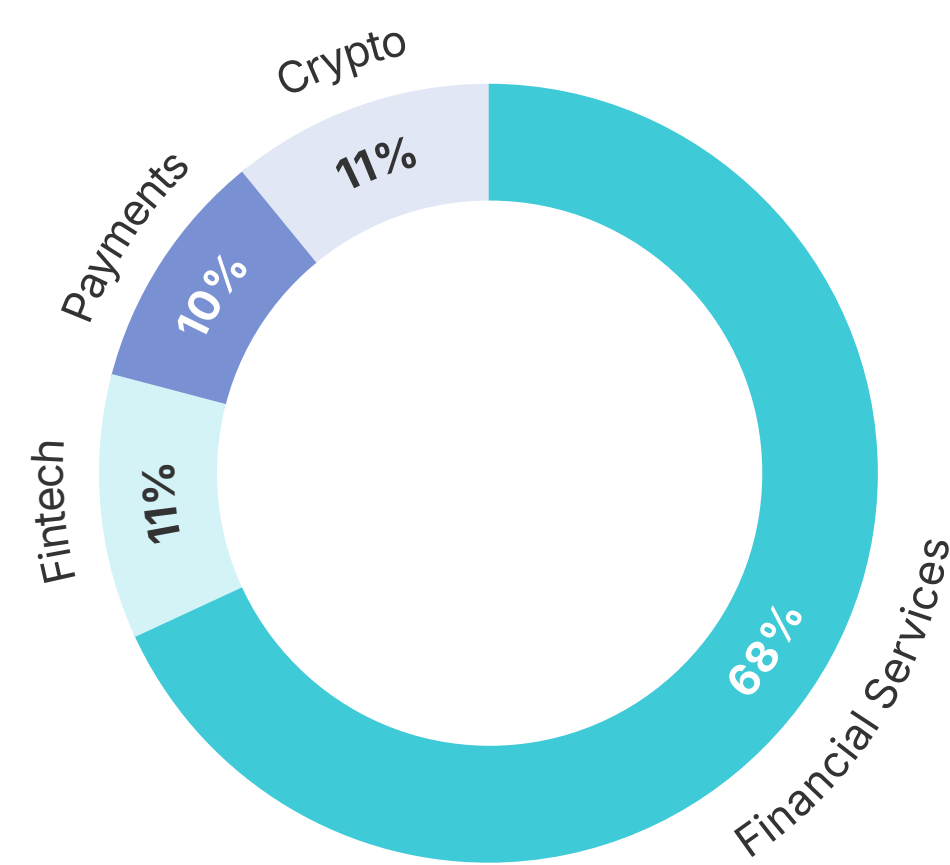




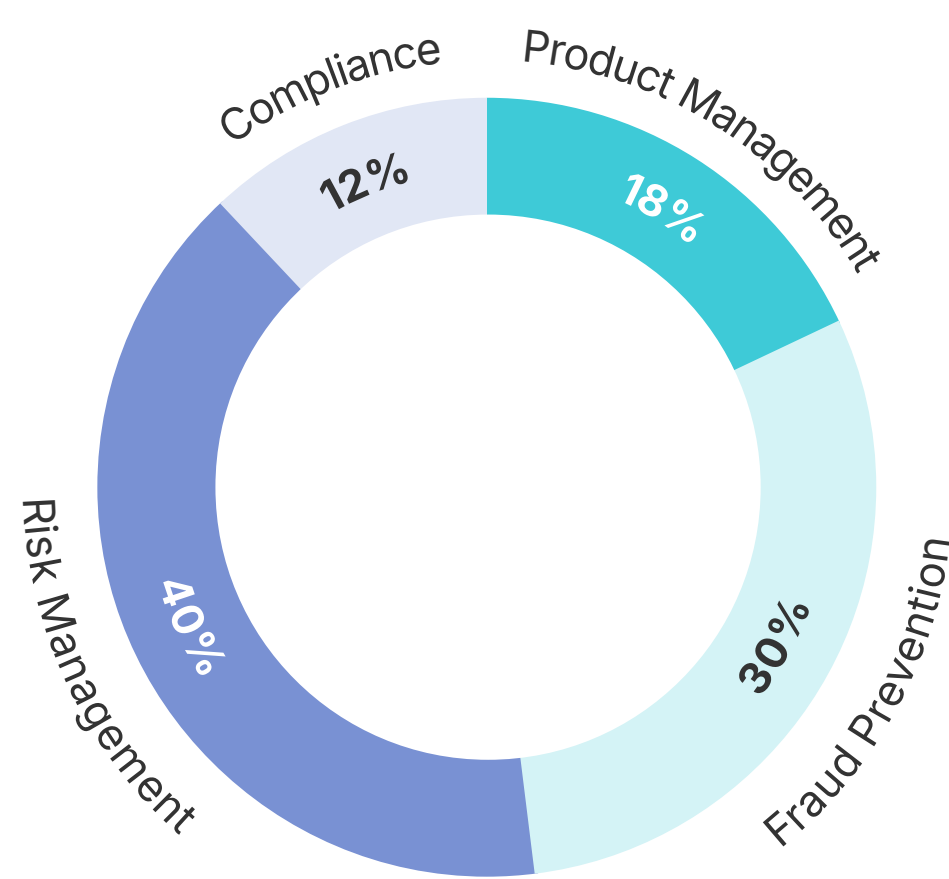
# Market Presence Survey Demographics

Survey Respondent Demographics (N=225)<sup>1</sup>

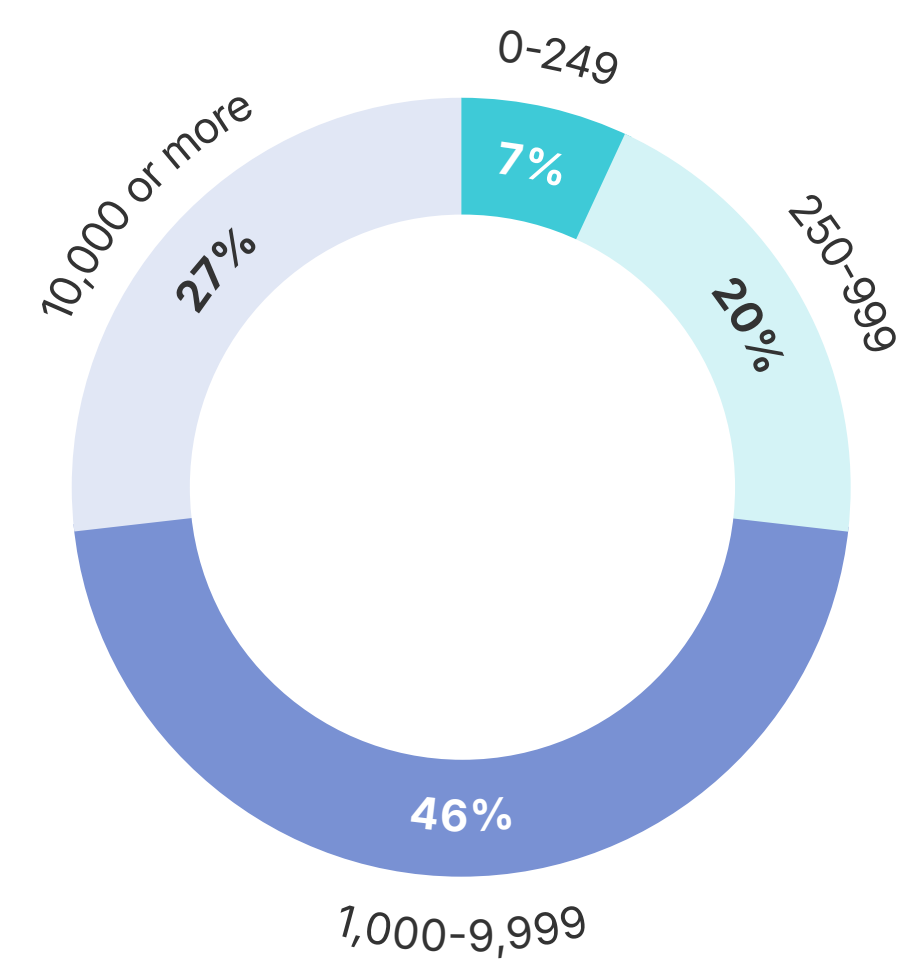
Respondent Breakdown  
by Company Segment



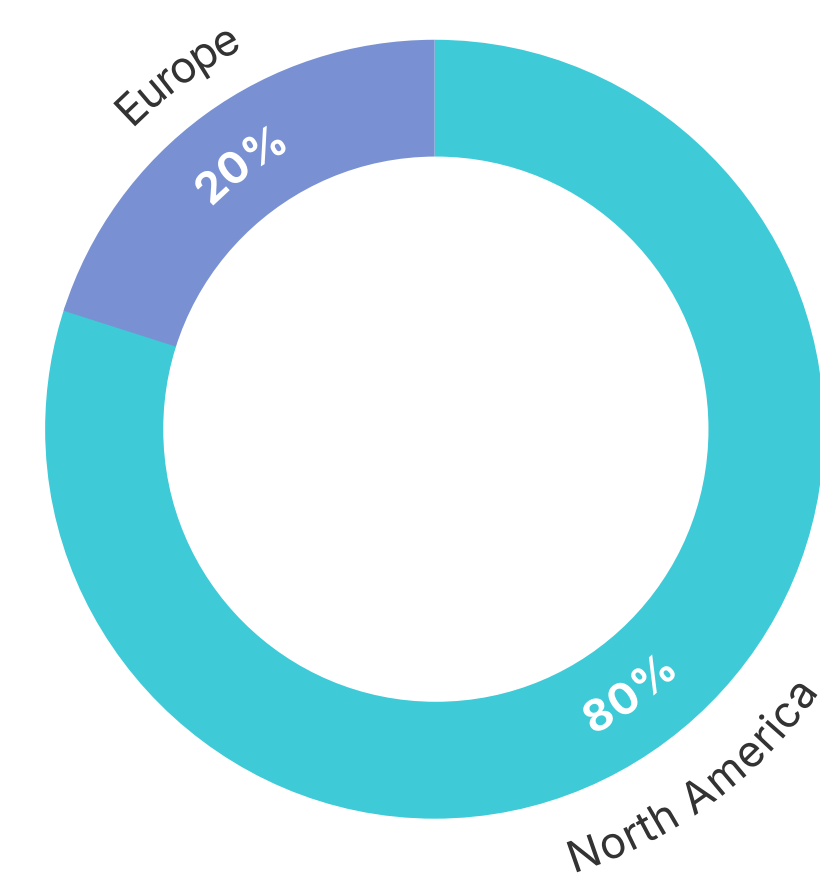
Respondent Breakdown  
by Business Unit



Respondent Breakdown  
by Employee Count



Respondent Breakdown  
by Company Headquarters



(1) Liminal Anti-Money Laundering Market Presence Survey, January 2025 (N=225)

# Link Index Methodology: Exceptional, Excellent, Strong Scoring Buckets Definitions

Scoring Buckets	Definition
Exceptional	Vendors in this category represent the highest level of performance in the transaction monitoring market, ranking above the third quartile among leading providers. These vendors not only meet but exceed regulatory and industry standards, offering advanced AI-driven fraud detection, real-time risk scoring, seamless system integrations, and comprehensive compliance reporting. Their solutions empower financial institutions to detect suspicious activities with precision, minimize false positives, and ensure compliance with evolving AML regulations.
Excellent	Vendors in this category provide highly effective transaction monitoring solutions, ranking between the first and third quartile among leading providers. They offer strong detection capabilities, reliable compliance support, and scalable automation, though they may not reach the same level as Exceptional vendors. These providers enhance fraud detection accuracy, improve operational efficiency, and streamline regulatory reporting, making them strong choices for organizations seeking robust yet cost-effective monitoring solutions.
Strong	Vendors in this category meet core transaction monitoring requirements, ranking below the first quartile among top providers while outperforming those not making the final list. They offer dependable monitoring solutions that cover essential fraud detection, compliance, and risk assessment needs. While they may lack advanced automation, deep integrations, or AI-driven analytics, their solutions remain suitable for organizations with fundamental AML compliance and fraud detection requirements.



# Product Capability Definitions

Term	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 is captured from a live person.
Address Verification	Address verification is a critical component of the KYC process, which financial institutions and other regulated entities use to confirm the physical address of their clients.
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.
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	Behavioral biometrics identifies individuals based on their unique patterns of behavior, particularly in the context of human-computer interaction. Unlike physical biometrics, which rely on innate physical characteristics like fingerprints or iris patterns, behavioral biometrics focuses on patterns that emerge from a person's natural interactions and activities, such as typing rhythm, mouse movements, gait, and voice dynamics.
Bot Detection	Bot detection involves identifying entities or individuals that mimic user behavior, such as bots, malware, or rogue applications. These may attempt to evade traditional security tools by blending in with normal user activities like browsing the web or sending emails. Bot detection also refers to analyzing traffic to a website, mobile application, or API to detect and block malicious bots.
CDD/EDD Audit Trail Management	Records detailed logs of all Customer Due Diligence and Enhanced Due Diligence activities performed during the onboarding and monitoring of customers. This includes tracking all actions, reviews, decisions, and changes made in relation to the due diligence process
Customer Risk Profiling	Customer risk profiling is the process of evaluating and categorizing customers’ risk levels based on their likelihood of engaging in illicit activities, such as money laundering or terrorist financing.

# Product Capability Definitions

Term	Definition
DOB Verification	Date of Birth verification is a critical component of the KYC process, primarily used by financial institutions, online platforms, and other regulated entities to confirm the age and identity of their clients.
Document Verification	Document verification establishes that an individual is who they say they are by validating and verifying a government-issued identity document.
Electronic AML Regulatory Report Filing	Electronic AML Regulatory Report Filing is the capability of electronically submitting required financial reports to regulatory bodies, such as Suspicious Transaction Reports and Currency Transaction Reports. This ensures compliance with AML regulations by automating the filing process, reducing errors, and improving the efficiency of reporting suspicious activities.
Name Verification	Name verification is the process of validating an individual's full name against a trusted data source during the onboarding process to ensure its authenticity and accuracy.
Negative News / Adverse Media Monitoring	Negative news search, also known as adverse media monitoring, is the process of identifying and analyzing unfavorable information about individuals, organizations, or entities across a wide variety of news sources. This information can include reports on financial crimes, corruption, legal issues, and other illicit activities that could pose significant risks to businesses and financial institutions.
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.
PEP (Politically Exposed Persons) Screening	PEP Screening refers to the process of identifying and assessing individuals who hold or have held prominent public positions to determine the associated risks of engaging in financial transactions with them.
PEP Alert and Case Management	Manages alerts and cases related to PEPs, ensuring that potential risks are promptly identified and addressed. This capability helps organizations comply with anti-corruption and anti-money laundering regulations.



# Product Capability Definitions

Term	Definition
Supplier Diversity Verification	Supplier Diversity Verification certifies that a business is owned, managed, and controlled by individuals from certain groups that are typically underrepresented in the business community. These groups can include women, minorities, veterans, LGBTQ+ individuals, and people with disabilities.
Synthetic Identity Fraud Risk Scoring	Employs advanced algorithms to assess the risk of synthetic identity fraud by analyzing various data points and patterns. This capability helps financial institutions detect and prevent fraudulent activities involving fabricated identities.
Verification of Employment (VOE)	Employers, lenders, or other interested parties use employment verification to confirm a job candidate’s or employee’s current or past employment status, job title, salary, and other job-related information.
Verification of Income (VOI)	Verification of Income involves validating the income information provided by an individual through official documentation, such as pay stubs, tax returns, or direct verification with employers.

# Link Index Methodology: Product

Product Criteria	Weighting	Definition	Why It Matters
Capability Score	55.00%	A measure of how well a KYC solution meets key capabilities and technical features based on the capabilities demanded by buyers.	Measures a vendor’s overall ability to deliver effective KYC solutions, ensuring compliance, fraud prevention, and seamless identity verification.
Buyer Satisfaction	15.00%	The extent of buyer satisfaction with a vendor's solution for KYC	Reflects user experience, reliability, and vendor responsiveness, helping organizations choose solutions that meet their operational and compliance needs.
Accuracy	9.00%	The precision of results, minimizing false positives and false negatives when validating user identities.	Ensures precise identity verification, reducing false positives and negatives, which is critical for compliance, fraud prevention, and smooth customer onboarding.
Orchestration	4.31%	The ability to configure and manage multiple identity verification workflows dynamically, integrating various data sources and risk signals for streamlined processes.	Enables seamless integration and automation across multiple verification and compliance systems, reducing manual effort and improving efficiency.
Data Quality	8.81%	The completeness, accuracy, and timeliness of user identity data.	Ensures reliable and up-to-date customer information, minimizing errors in identity verification and strengthening regulatory compliance.
Scalability	7.88%	The ability of the KYC solution to efficiently handle growing volumes of customer verifications across different geographies and regulatory environments.	Supports high transaction volumes and business growth, ensuring KYC processes remain efficient and effective as demands increase.



# Link Index Methodology: Strategy

Strategy Criteria	Weighting	Definition	Why It Matters
Ease of Use	16.08%	The simplicity of onboarding, managing, and maintaining KYC workflows, including user-friendly interfaces and case management capabilities.	Simplifies onboarding and compliance workflows, reducing operational friction and ensuring a smooth experience for both users and compliance teams.
Automation	24.27%	The extent and how well the verification process is automated, reduces manual reviews, and increases the speed of decision-making.	Speeds up identity verification, reduces manual reviews, and improves accuracy to make KYC processes more efficient and scalable.
Integration	15.79%	The ability of the KYC solution to seamlessly connect with other compliance, fraud detection, and customer onboarding systems.	Enables seamless connectivity with fraud detection, compliance, and customer onboarding systems for a unified risk management approach.
Price	19.88%	The overall cost-effectiveness of the KYC solution, including licensing, per-verification fees, and additional charges for advanced features.	Impacts the total cost of ownership, influencing affordability, scalability, and long-term sustainability of KYC operations.
Global Coverage	9.94%	The solution's ability to verify identities across multiple countries, supporting various regulatory frameworks and official data sources.	Ensures the ability to verify identities across multiple jurisdictions to support compliance with diverse regulatory frameworks.
AO Fraud Capabilities	11.40%	The ability to detect and prevent fraud, including synthetic identities and stolen credentials at account opening.	Detects synthetic identities and stolen credentials at account opening to prevent fraud before bad actors gain access.
pKYC	2.63%	The capability to continuously monitor customer risk profiles in real time, rather than relying on periodic reviews to ensure compliance with evolving regulations.	Enables continuous risk monitoring beyond onboarding for real-time compliance and proactive fraud detection.

# Link Index Methodology: Market Presence

Market Criteria	Weighting	Definition	Why It Matters
Market Leadership Perception / Brand Reputation	35.00%	The number of buyers who believe this vendor is a market leader.	A vendor perceived as a leader helps shape industry standards and regulatory approaches, influencing buyer confidence and market direction. Strong market leadership differentiates vendors, making them more attractive to enterprises seeking reliable, future-proof identity verification solutions.
Brand Awareness	35.00%	The number of buyers who are aware of a vendor.	High brand awareness increases visibility and credibility. When organizations look for identity verification solutions, the vendor is a top consideration. Strong awareness drives inbound interest, accelerates market adoption, and establishes trust with large-scale clients.
Company Size	15.00%	The total employee headcount of a company.	A larger company typically has greater financial stability, established infrastructure, and resources to maintain and upgrade identity verification solutions. This provides buyers with confidence in long-term vendor viability and sustained product innovation.
Employee Growth (YoY)	15.00%	How fast a company’s employee count is growing.	A growing workforce indicates investment in R&D, customer support, and market expansion. Rapid employee growth suggests the vendor is scaling operations, improving technology capabilities, and staying ahead of evolving regulatory requirements in identity verification.





---

# Actionable Market Intelligence

---

## Link

Through our proprietary database, Link, we monitor thousands of companies and products across the digital landscape. Our insights allow us to predict and understand trends before they happen.

Paid and free access options available.

- Specialized Data on Companies, Products, Regulations, and more
- Market and Buyer's Guides
- Benchmarking Reports
- Outside-in Research
- Market Sizing
- Competitive Battlecards

## Membership

Liminal is your trusted partner. As a member, you have unparalleled access to our team and extended network of industry experts. Our deep domain experience provides us with the ability to remain on-call and to provide you with market intelligence when opportunity strikes.

- Analyst Access
- Executive Summits
- Private Events
- Expert Network
- Virtual Workshops
- Ad hoc Support

## Advisory

We advise the world's most innovative leaders on building, buying, and investing in the next generation of integrated digital identity technologies.

- Market Intelligence
- Business and Corporate Strategy
- M&A and Commercial Due Diligence

[www.liminal.co](http://www.liminal.co)

| [www.liminal.co/linkplatform](http://www.liminal.co/linkplatform)





Liminal Strategy, Inc.  
825 Third Avenue, Suite 1700, New York, NY 10022

[www.liminal.co](http://www.liminal.co) | [info@liminal.co](mailto:info@liminal.co)



©2025 Liminal Strategy, Inc. All rights reserved. Liminal and the Liminal marks used herein are trademarks or registered trademarks of Liminal Strategy, Inc. Other product and company names mentioned herein are the trademarks of their respective owners. No part of this copyrighted work may be reproduced, modified, or distributed in any form or manner without the prior written permission of Liminal.

Liminal Confidential