



Link Index

Account Takeover Prevention in Banking

July 2024 | Strictly Confidential

Contents

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

Introduction	Market Overview	Link Index	Vendor Overviews	Survey Results
Executive Summary: Market Overview 3	The continued prevalence of phishing attacks, diminished prioritization of account recovery, and mobile ATO attacks pose challenges for banks 7	Banks consider biometric authentication, continuous authentication, and social engineering and scam detection key capabilities for ATO prevention 16	Accertify 26-30	Market Demand Survey Results Overview 147
Executive Summary: Vendor Landscape 4	Banks look for highly accurate ATO prevention solutions from third party-vendors that leverage biometric signals and address scam attack threats 8	Future buyers will demand cost-effective behavioral signals and passwordless authentication solutions with strong user experience 17	Arkose Labs 31-35	Survey Demographics: Buyer Profile 148
The adoption of passwordless authentication and the widespread availability of generative AI are fundamentally reshaping the ATO threat landscape. 5	Customers want solutions that can provide frictionless experiences, behavioral signals, passwordless authentication, and regional customization 9	Brand awareness, leadership, market penetration, company size, and employee growth are the key market presence criteria for ATO prevention vendors 18	BioCatch 36-40	Top KPCs include accuracy, user experience, product integration, and customization for ATO prevention in banking 149
	AI/ML tools, FIDO2 standards, and the ubiquity of biometric authentication from Big Tech aid banks in the fight against account takeover fraud 10	To identify the leading vendors in ATO Prevention in Banking, we set benchmarks for minimum product execution and strategy 19	Bureau 41-45	Phishing and social engineering are the top ATO threat vectors 150
	Vendors struggle to address social engineering, lack a strategy for handling Big Tech data restrictions, and struggle to cover the complete customer lifecycle 11	Of the 56 companies analyzed, 27 met minimum product execution requirements, with 24 classified as Leading Vendors 20	Caf 46-50	ATO attacks predominantly occur via mobile app and mobile web rather than on desktop platforms 151
	Banks most highly prioritize accuracy, user experience, product integration, and customization when purchasing ATO prevention solutions 12	Vendor positioning on the Link Index for ATO Prevention in Banking 21	Callsign 51-55	There is a large and growing total addressable market (TAM) for ATO prevention solutions 152
	Top vendors can achieve significant reductions in successful ATO attacks, average fraud losses, and customer abandonment 13	Leading vendors have three distinct focuses: authentication, fraud prevention, and identity 22	DataVisor 56-60	Appendix 153
	Banks can reduce fraud losses by nearly \$500 million while also seeing significant operational cost and customer retention savings 14	Link Index for Account Takeover Prevention in Banking: Leading Vendors 23	Entersekt 61-65	Product Capabilities Definitions: High Demand 154
		Link Index for Account Takeover Prevention in Banking: Leading Vendors and Adjacent Leaders 24	Entrust 66-70	Product Capabilities Definitions: Medium Demand 155
			Experian 71-75	Product Capabilities Definitions: Low Demand 156
			Feedzai 76-80	Passwordless Feature Definitions 157
			HUMAN 81-85	Exceptional, Excellent, Strong Scoring Buckets Definitions 158
			Kount 86-90	Link Index Methodology: Product 159
			LexisNexis Risk Solutions 91-95	Link Index Methodology: Strategy 160
			Mastercard 96-100	Link Index Methodology: Market Presence 161
			NeuroID 101-105	ROI Calculations 162
			Outseer 106-110	About Liminal 163
			Ping Identity 111-115	
			Prove 116-120	
			Socure 121-125	
			SpyCloud 126-130	
			Telesign 131-135	
			Transmit Security 136-140	
			TransUnion 141-145	

Executive Summary: Market Overview

Key Takeaways

- **ATO prevention defends against a wide range of threats.**
Account takeover (ATO) is a type of third-party fraud where a malicious actor gains unauthorized access to a user's account, enabling them to steal funds, sensitive data, or initiate fraudulent transactions. Unauthorized access is typically achieved through phishing or by exploiting user credentials obtained via data breaches or malware. ATO threats come in various forms, including credential stuffing, phishing, social engineering, malware, SIM swapping, and man-in-the-middle attacks.
- **ATO can lead to severe financial consequences, especially for banks.**
The consequences of ATO can be severe, often resulting in significant financial losses for the user or the institution where the account is maintained. Average losses can range from about \$6,000 to \$13,000 USD per ATO incident in the banking industry.¹ The full scope of the ATO costs banks incur remains difficult to quantify, as banks are reluctant to publicly divulge the frequency and value of successful ATO attacks.
- **Fraudsters are becoming more effective, and vendors are counteracting with sophisticated solutions.**
As ATO prevention methods have become more effective at thwarting simplistic attacks like credential stuffing, fraudsters have shifted their focus to deceiving individuals through phishing and social engineering tactics. Specifically, banks have seen a sharp rise of 66.8% in social engineering attacks over the last two years.¹ In response, solution providers have developed sophisticated detection methods utilizing multi-factor authentication, biometrics, and passive behavioral signals to identify anomalous behavior. Banks are adopting these advanced techniques to reduce fraud losses, as their user accounts hold significant value.

Current Challenges

- **Large-scale phishing attacks.** Phishing is the most common ATO attack, responsible for 26.7% of all ATO incidents among the eight primary attack methods.¹
- **Account recovery vulnerability due to login defense prioritization.** 94% of banks recognize account recovery as a threat yet are more likely to prioritize login defense.¹
- **Inadequate protection of mobile channels.** Banks report that most ATO attacks originate from mobile apps, yet only 44% utilize mobile device signals for protection.¹

Future Demands

- **Social engineering and scam detection.** 84% of bank ATO solution seekers highly demand social engineering and scam detection, the second most buyer-requested capability.¹
- **Behavioral signals.** Banks increasingly demand passive capabilities like behavioral biometrics, with 81.8% of those not currently using them planning to adopt them within the next two years.¹
- **Passwordless authentication.** Over 40% of consumers consider traditional password-based authentication insecure, adding pressure for banks to transition towards passwordless solutions.²

Key Purchasing Criteria (KPC)

- **Accuracy:** 90% of ATO solution buyers at banks prioritize accuracy.¹
- **User Experience:** 86% of ATO solution buyers at banks prioritize user experience.¹
- **Product Integration:** 84 of ATO solution buyers at banks prioritize product integration.¹
- **Customization:** 82% of ATO solution buyers at banks prioritize customization¹

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

(2) ATO Prevention Consumer Survey, April 2024 (N=511)

Executive Summary: Vendor Landscape

Liminal's ATO Prevention in Banking landscape analysis identifies the top vendors that address the fraud threats facing financial institutions today. With criminal actors deploying a wide range of attack vectors that include phishing, social engineering, and credential stuffing, a fragmented solutions landscape has emerged with vendors taking specialized approaches to address ATO attacks that can be grouped into three primary categories: Authentication-focused vendors, Fraud-focused vendors, and Identity-focused vendors. Fraud-focused vendors use probabilistic data, including behavioral signals, to protect against fraud, mainly at the transaction level, while authentication-focused vendors use comprehensive authentication capabilities to prevent unauthorized access during login. Identity-focused vendors combine select capabilities of both authentication and fraud prevention methods, using identity as the bedrock.

The analysis highlights 24 leading companies, selected based on an evaluation of their product offerings, strategies, and market presence.

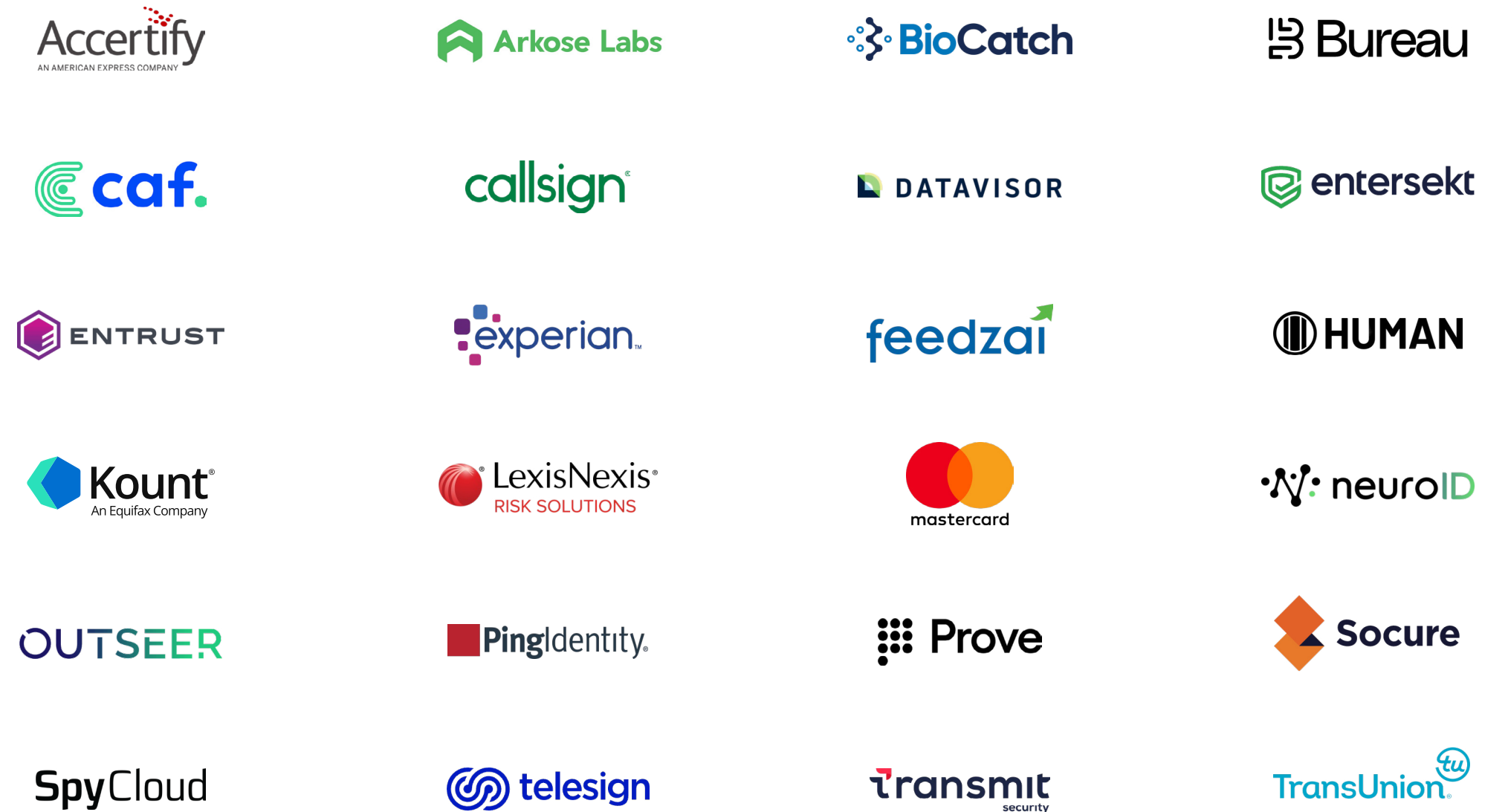
Landscape Analysis

- **The market is split into fraud, authentication, and identity vendors.** Solution providers in the ATO landscape employ diverse strategies, with some exhibiting limited capability overlap.
- **Banks leverage multiple vendors in their tech stack.** Vendors with unique capabilities collaborate to offer comprehensive coverage.
- **Credit bureaus and card issuers hold strong market presence.** Experian, TransUnion and Mastercard are all ranked within the top 5 for market presence.
- **Overall satisfaction is most strongly correlated with scalability.** Despite being ranked fifth among KPCs, buyer satisfaction showed the highest correlation with satisfaction in scalability.

Key Benefits of Leading Account Takeover Solutions

- **Reduction in successful ATO attacks:** Highly accurate solutions limit the amount of ATO attacks that lead to financial loss by 64%.¹
- **Reduction in average fraud loss:** Leading solutions effectively minimize average fraud losses, reducing them by 52%.¹
- **Reduction in customer abandonment:** By providing a seamless user experience, leading solutions reduce customer abandonment by 24%.¹

Top 24 Vendors for Account Takeover Prevention in Banking



(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

The adoption of passwordless authentication and the widespread availability of generative AI are fundamentally reshaping the ATO threat landscape.

Digital banking fraud is big business in 2024, with the bulk of ATO attacks perpetrated not by sole actors but by well-coordinated and financed criminal groups working at scale from jurisdictions across the globe. In this increasingly institutionalized attack environment, bank accounts have emerged as prized ATO targets due to the high profitability of a successful attack.

This ATO threat landscape is being shaped by two wider trends: continued adoption of more secure passwordless authentication technologies by banks, and the widespread availability of powerful generative AI tools to fraudsters. Passwordless authentication is raising the cost and technical capabilities required for illicit actors to compromise an account via phishing and other forms of credential theft. Technologies like FIDO2 Passkeys make phishing effectively impossible. In parallel, generative AI is making the deployment of current fraud techniques more scalable, cost effective, and executable by criminals who lack requisite technical or language skills.

These trends account for the continued rise of social engineering or “scam” attacks as an overall percentage of successful ATO attempts as fraudsters adapt to the increasing challenge of defeating the more rigorous authentication methods adopted by financial institutions. The current vendor landscape for ATO Prevention reflects this shifting risk environment, with platforms taking one of several general approaches toward addressing increasingly sophisticated threats.

Authentication-focused vendors seek to address threat vectors that fundamentally compromise a user’s login credentials via phishing or data breaches. This approach can be likened to upgrading the physical security of a home’s front door to make it resistant to lock picking or the physical breach.

In contrast, fraud-focused vendors seek to quantify the risk of a user’s session and the resulting transactions after the session has already been authenticated. Or, in home security terms, deploying security cameras inside a house to observe when criminals are walking around inside

and notify the police. As each of these approaches are suited to detect specific types of attacks, banks today typically deploy multiple vendors within their tech stack to build layered defenses.

The newest entrants into the ATO prevention space, identity-focused vendors take an approach that follows the evolution of IT Security defenses used to protect banks and other institutions against cybersecurity threats at the fundamental platform level. They transition away from solutions that focus on securing the network perimeter or endpoint devices themselves and instead take an identity-centric approach. Current identity-focused ATO vendors combine features from authentication- and fraud-focused approaches, built on top of a clear understanding of the underlying identity of the account holder themselves.



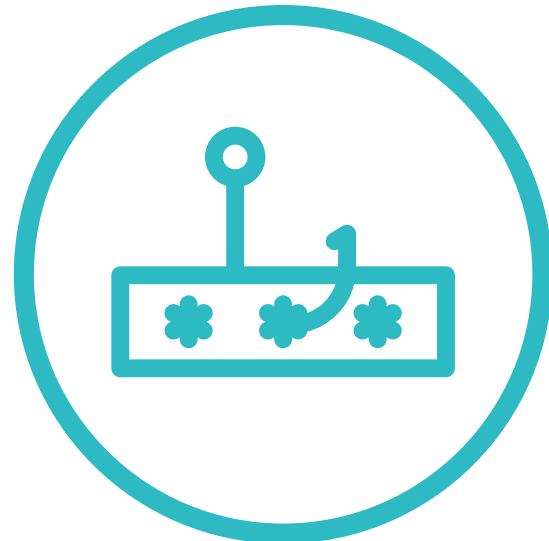
LINK INDEX

Market Overview

©2024 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

The continued prevalence of phishing attacks, diminished prioritization of account recovery, and mobile ATO attacks pose challenges for banks



Phishing continues to be the most significant ATO threat vector

Among the eight primary attack methods, phishing accounts for 26.7% of all account takeovers, making it the most common threat.¹

Banks face significant challenges in protecting their customers from phishing attacks, particularly as fraudsters embrace new technologies like generative AI.



Account recovery continues to be a weak point as banks prioritize login defense

Over three times as many banking respondents view login as a major concern; however, 94.0% acknowledge that account recovery is also a significant threat.¹

Weak account recovery protocols can significantly increase account takeovers and financial losses.



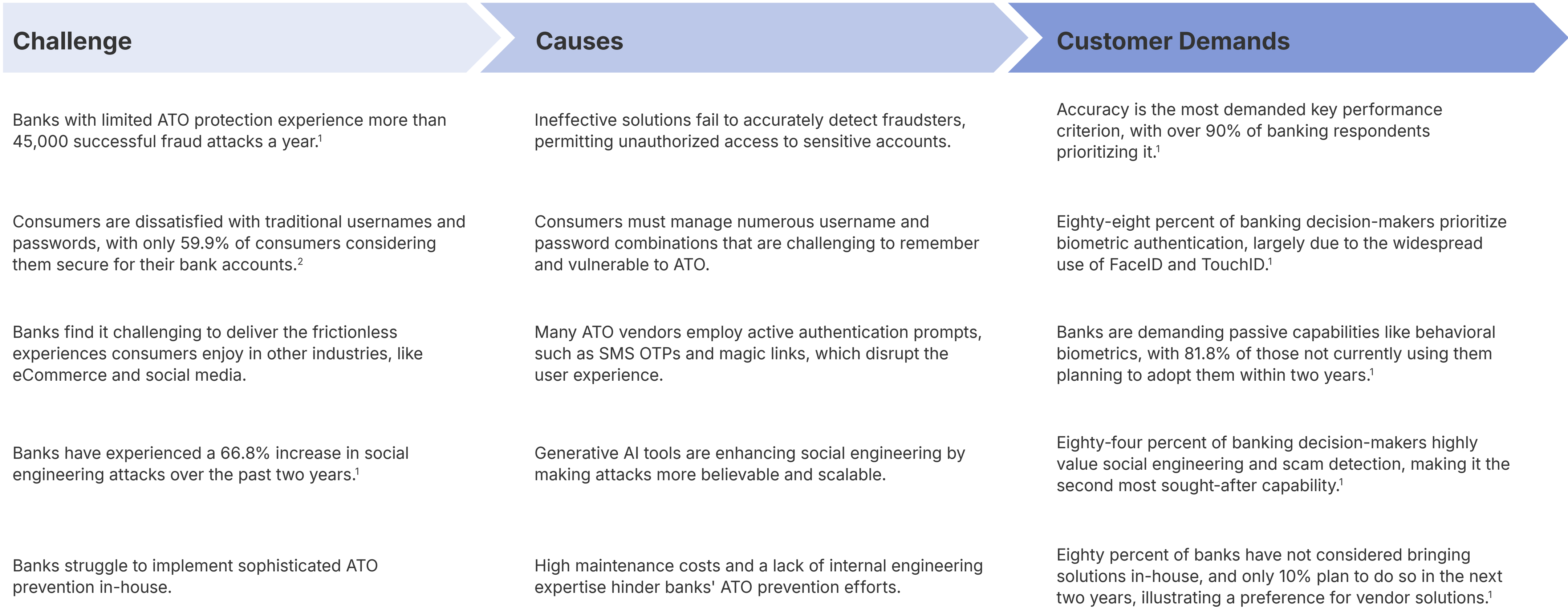
Banks are failing to adequately protect mobile channels

Banks report that the majority of ATO attacks originate from mobile apps rather than mobile web or desktop, yet only 44.0% utilize mobile device signals for protection.¹

Neglecting mobile device signals presents a significant risk to the banking industry, particularly as mobile channels continue to grow in prevalence.

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Banks look for highly accurate ATO prevention solutions from third party-vendors that leverage biometric signals and address scam attack threats



(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

(2) ATO Prevention Consumer Survey, April 2024 (N=511)

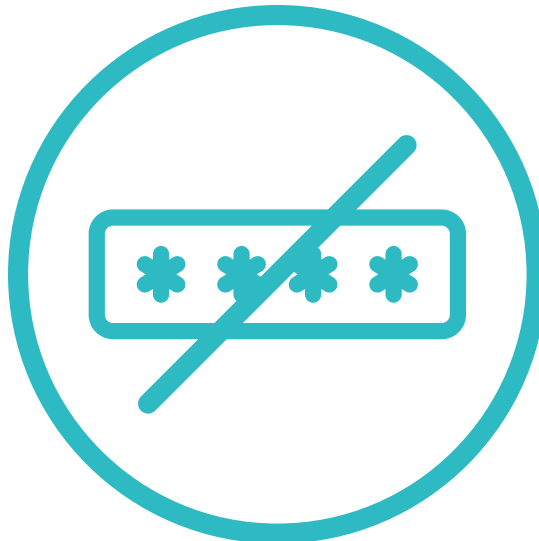
Customers want solutions that can provide frictionless experiences, behavioral signals, passwordless authentication, and regional customization



Frictionless Experience



Behavioral Signals



Passwordless Authentication



Regional Customization

Description

Ensuring robust account security while minimizing user friction.

Using the patterns and characteristics of user behavior, such as typing speed and mouse movements, to prevent ATO attempts.

Authenticating a user without the use of traditional passwords, instead relying on biometrics, security keys, or other methods.

Deploying ATO solutions that remain compliant with evolving national and state-level privacy and data protection regulations.

Blockers

Friction-Filled Authentication Methods
Security Concerns

High Cost
Extensive Implementation Process

Password Stickiness
Legacy System Integrations

Fragmented Privacy Landscape
Regional Vendor Focus

AI/ML tools, FIDO2 standards, and the ubiquity of biometric authentication from Big Tech aid banks in the fight against account takeover fraud



Vendors provide sophisticated AI / ML fraud detection methods

Solution providers are increasingly leveraging sophisticated machine learning and artificial intelligence to detect advanced fraud techniques, such as social engineering and man-in-the-middle attacks. These tools analyze a wide range of signals to identify anomalies, preventing fraudulent actors from stealing funds.



FIDO2 paves the way for more secure authentication

FIDO2 authentication is an open standard that uses public key cryptography to enable secure, passwordless logins across devices and platforms.¹ It is important in protecting against account takeovers because it eliminates the risks associated with traditional passwords, such as phishing and credential theft, by relying on strong cryptographic keys stored on users' devices.



Big Tech has made biometric authentication ubiquitous

Device manufacturers like Apple have seamlessly integrated biometric authentication into consumers' everyday lives with products like FaceID and TouchID. Device-native biometric authenticators can be easily integrated into banks' onboarding and login processes, enhancing user experience without compromising security.

(1) FIDO Alliance

Vendors struggle to address social engineering, lack a strategy for handling Big Tech data restrictions, and struggle to cover the complete customer lifecycle



Only a portion of vendors can address the growing social engineering threat

Eighty-four percent of banks highly demand social engineering and scam detection, making it the second highest demanded product capability. However, only about 3 in 5 of the top vendors offer this capability. Many banks may continue to struggle with social engineering, which has resulted in a reported increase of 66.8% in financial losses over the past two years.¹



Solution providers are unsure how to deal with Big Tech data restrictions

Ninety-six percent of banking professionals believe restricting access to device signals could compromise their ATO solutions - additionally, 90% share similar concerns over losing other data signals, such as third-party cookies. ATO prevention solutions may face significant challenges from Big Tech data restrictions, particularly when attempting to fingerprint devices.¹



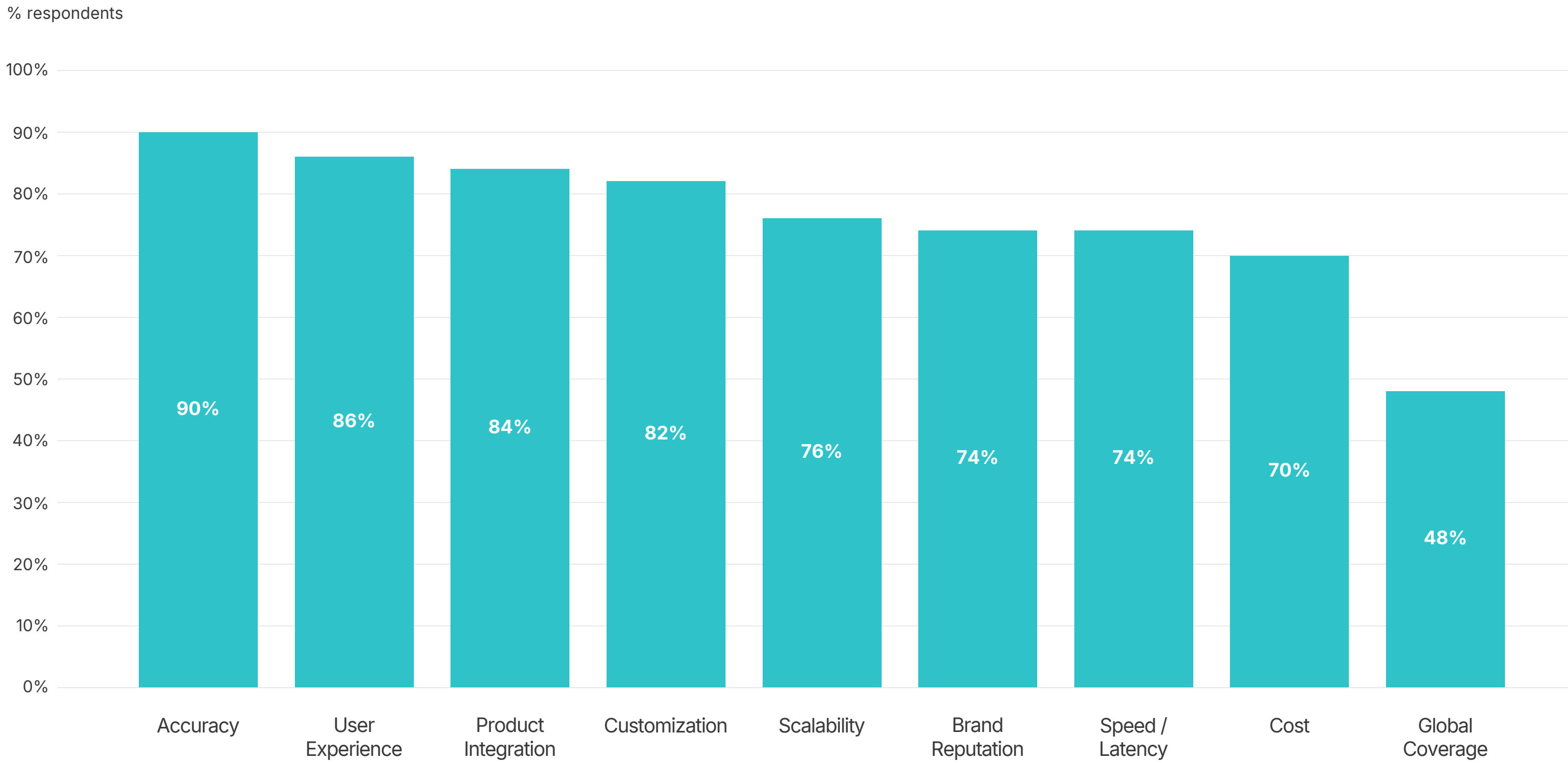
Few vendors offer unified platform solutions

The ATO prevention market is fragmented into fraud, authentication, and identity vendors. While many banks utilize multiple vendors in their tech stack, few vendors offer platform solutions that cover the entire user lifecycle.

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Banks most highly prioritize accuracy, user experience, product integration, and customization when purchasing ATO prevention solutions

Key Purchasing Criteria for ATO Prevention Solutions in Banking¹



(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Top vendors can achieve significant reductions in successful ATO attacks, average fraud losses, and customer abandonment



Reduction in Successful ATO Attacks¹

Banks employing leading vendors experience an average of around 16,000 successful ATO incidents annually, nearly three times fewer than banks using lagging solutions.¹



Reduction in Average Fraud Loss¹

Leading solution providers reduce the average fraud losses by more than half, from \$13,400 to \$6,430 USD.¹






Reduction in Customer Abandonment¹

By limiting friction during onboarding, login, transaction, and account recovery processes, customers of leading ATO vendors may experience a decrease in abandonment rates from 19.8% to 15.1%.¹

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Banks can reduce fraud losses by nearly \$500 million while also seeing significant operational cost and customer retention savings¹

 Reduction in Fraud Losses²	Lagging Solution	134,000 Successful fraud incidents	×	34% Share of losses related to ATO	×	\$13,430 Average ATO loss	÷	37 M Average customer base	=	~\$16 fraud loss per customer	~\$12 in fraud loss savings per customer
	Leading Solution	77,000 Successful fraud incidents	×	21% Share of losses related to ATO	×	\$6,400 Average ATO loss	÷	26 M Average customer base	=	~\$4 fraud loss per customer	
 Operational Cost Savings²	Lagging Solution	3 Employees required to handle ATO incident	×	\$21 Employee hourly wage	×	6.1 Average hours spent per employee			=	~\$390 total cost	~\$26 in savings per ATO incident
	Leading Solution	3 Employees required to handle ATO incident	×	21% Employee hourly wage	×	5.7 Average hours spent per employee			=	~\$364 total cost	
 Customer Retention Savings^{2,3}	Lagging Solution	15% Customer retention rate	×	\$4,500 Average customer LTV					=	~\$675 customer value captured	~\$215 in customer retention savings
	Leading Solution	20% Customer retention rate	×	\$4,500 Average customer LTV					=	~\$900 customer value captured	

(1) The average bank size of respondents was about 28 M customers. Further calculations and sources can be found in the appendix.

(2) ROI data captured from Liminal Market Demand Survey, March 2024, N=50.

(3) Customer retention rates can be influenced from several factors, and may not be fully attributed to ATO solutions.



Link Index

©2024 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

Banks consider biometric authentication, continuous authentication, and social engineering and scam detection key capabilities for ATO prevention

Demand ¹	Product Capabilities
H	App-based Authentication
H	Biometric Authentication
H	Continuous Authentication
H	Data Breach Monitoring
H	Email-based One-Time Passcode
M	SMS / Phone One-Time Passcode (SMS OTP)
M	Social Engineering and Scam Detection
M	Behavioral Biometrics
M	Device Risk Scoring
M	Location Intelligence
M	Proxy And VPN Detection
M	SIM Swap Detection
M	Time-based One-Time Passcode (TOTP)
M	Behavior Analytics
L	Bot Detection
L	FIDO2 Authentication
L	Knowledge-Based Authentication
L	Magic Links
L	Signal Sharing Network
L	User Risk Scoring

H High Demand M Medium Demand L Low Demand

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Other Factors For Consideration

Accuracy		Accurate solutions effectively decrease the amount of fraud losses without false positives, ensuring a secure and safe solution.
Buyer Satisfaction		Solution providers with robust customer support and responsiveness to customer needs deliver high satisfaction for banks.
Customization		Customizable solutions allow for the adjusting risk-scoring models, configuring rules, and setting up alerts/notifications.
Product Integration		Solutions with strong product integration require minimal time and resources to implement ATO prevention measures effectively.
Scalability		Scalable solutions maintain their effectiveness, regardless of the volume of logins, transactions, and account recovery attempts.

Future buyers will demand cost-effective behavioral signals and passwordless authentication solutions with strong user experience (UX)

Behavioral Capabilities

- Behavioral Analytics
- Behavioral Biometrics
- Bot Detection

Passwordless Capabilities

- Device-based / Cloud-based Passkeys
- QR Code Authentication
- WebAuthn

Additional Factors for Consideration

Cost



Customer perception of the cost-effectiveness of their ATO prevention solution can be influenced by pricing models, supplemental services, and additional capabilities that surpass those of competitors.

User Experience



Vendors offering strong UX provide strong fraud detection alongside minimal friction, limiting customer abandonment rates.

(1) See Appendix for Definitions of Product Capabilities

Brand awareness, leadership, market penetration, company size, and employee growth are the key market presence criteria for ATO prevention vendors



Brand Awareness

A well-known vendor will be able to capture more customers. We gauged the awareness of each vendor for their ATO prevention solution among buyers in banking.



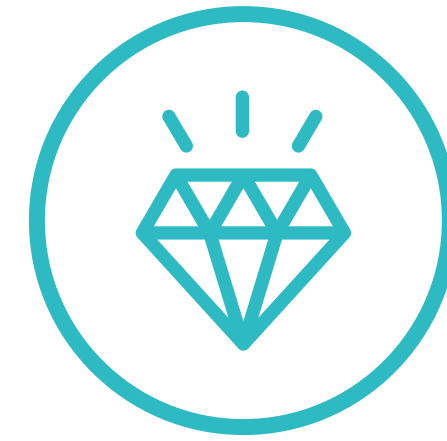
Company Size

Large vendors possess the stability and the capacity to accommodate bigger clients, thus driving larger revenues. We compiled employee headcount data and compared top companies.



Employee Growth

Vendors experiencing headcount growth indicate strong prospects for revenue growth and position it as a more formidable player in the market. We calculated year-over-year growth and compared vendors to each other.



Market Leadership Perception

Vendors perceived as market-leading are better positioned to capture market share. We surveyed ATO prevention customers in banking to analyze the levels of customer satisfaction across vendors.



Market Penetration

Having more customers increases your presence in the market. We surveyed banks to analyze the most frequently used vendors.

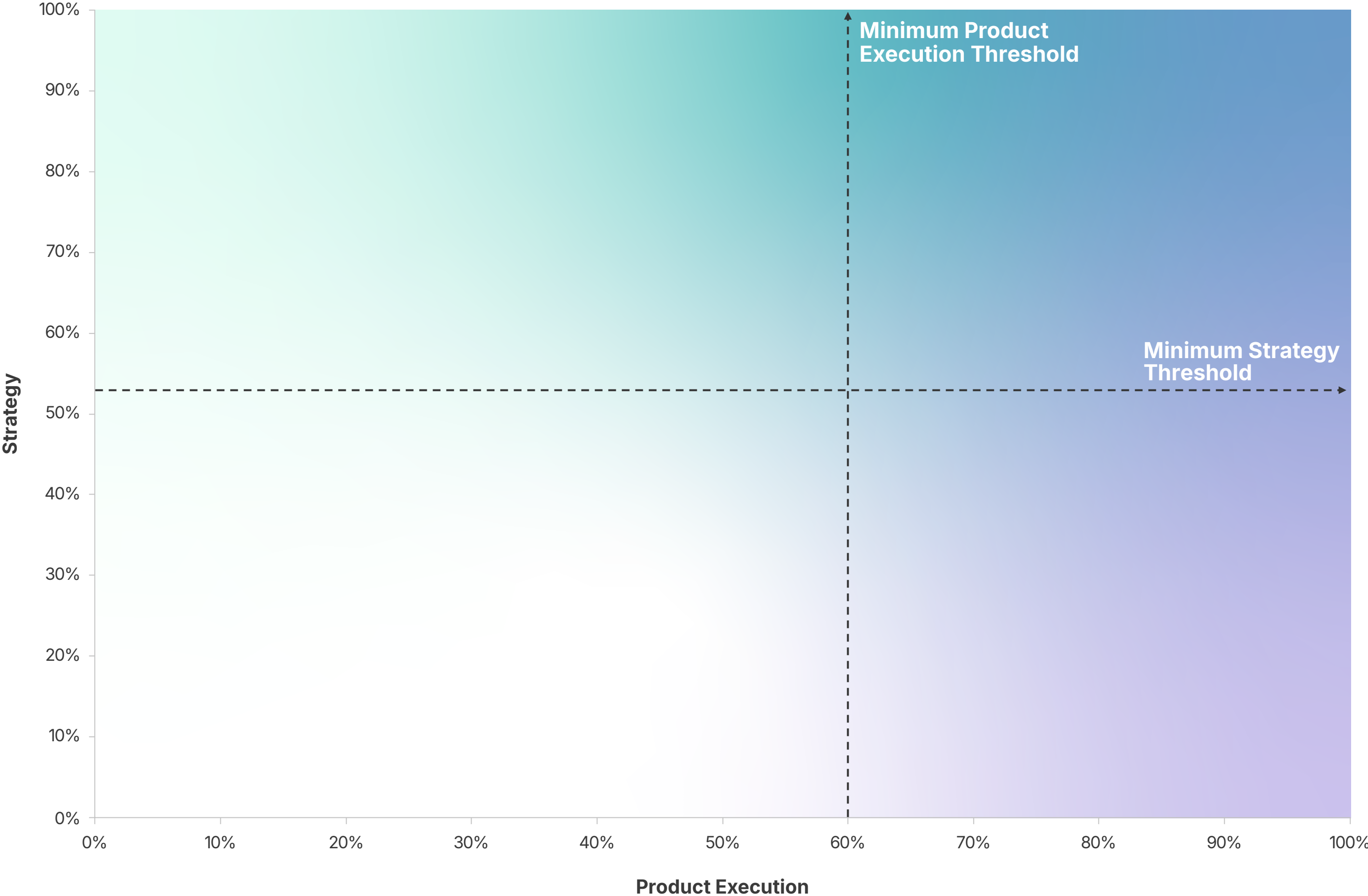
To identify the leading vendors in ATO Prevention in Banking, we set benchmarks for minimum product execution and strategy

Minimum Product Execution Threshold

To establish a minimum product execution threshold, we surveyed financial services buyers to identify the most highly valued capabilities for ATO prevention capabilities. By prioritizing capabilities according to demand, we determined that a company needs a minimum product execution score of 60% to sufficiently meet product capability demand.

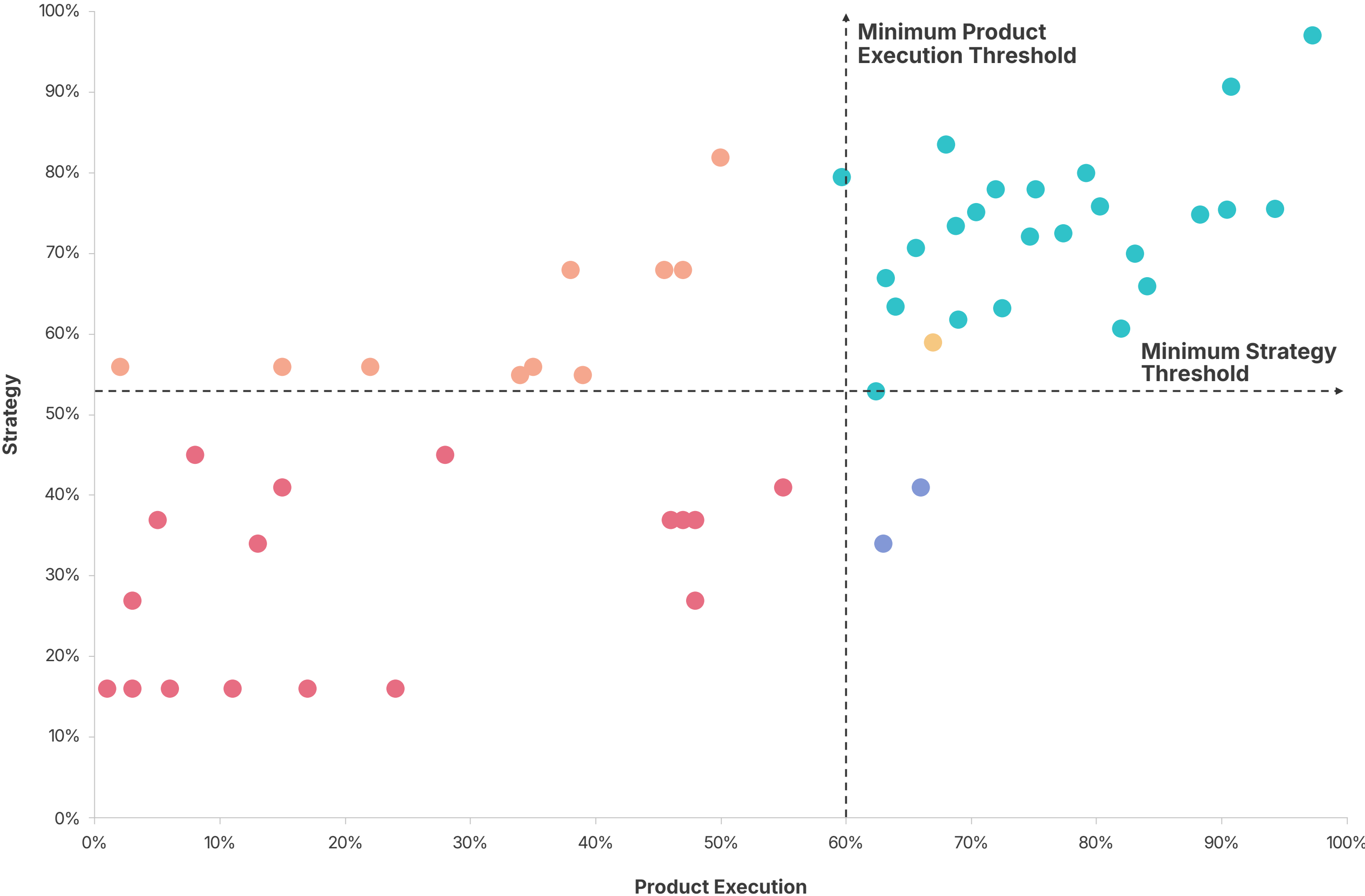
Minimum Strategy Threshold

We established a leadership strategy threshold by analyzing critical future demand elements, behavioral signals, and passwordless authentication capabilities. Leading vendors attain a minimum strategy score of 53%.

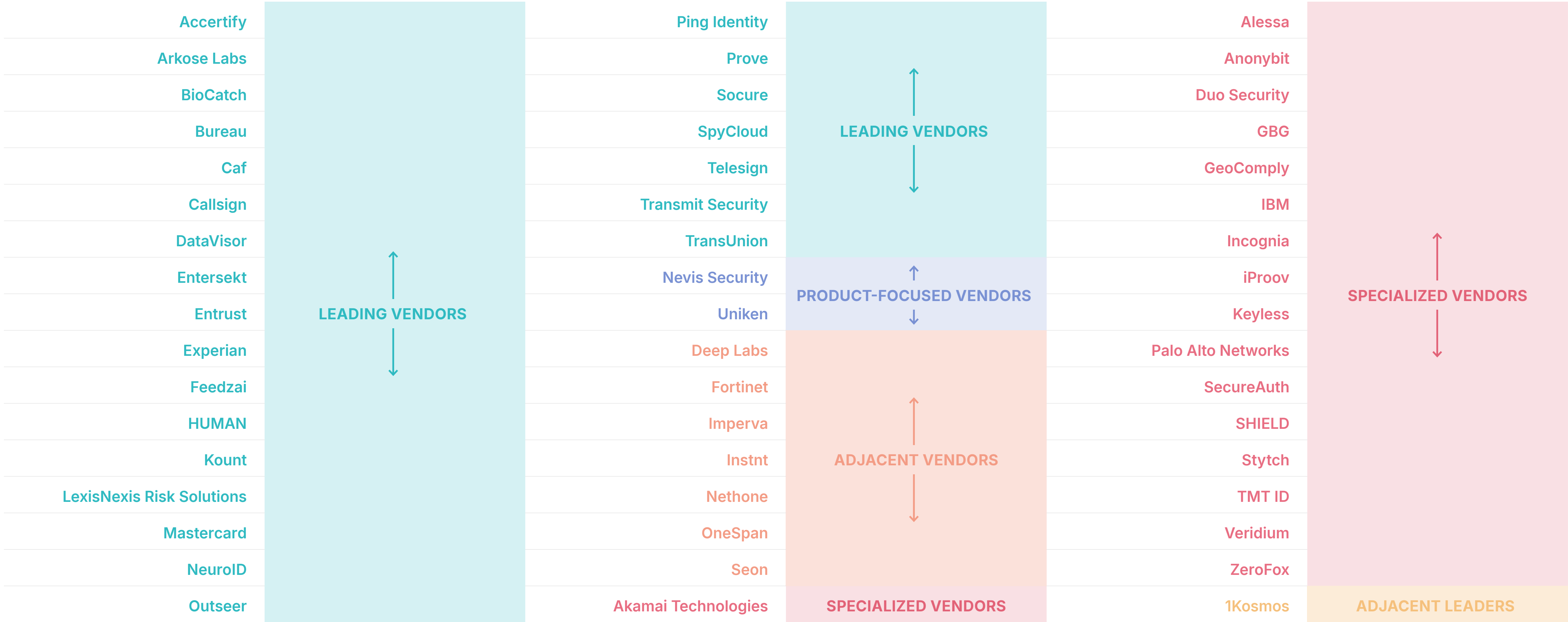


Of the 56 companies analyzed, 27 met minimum product execution requirements, with 24 classified as Leading Vendors

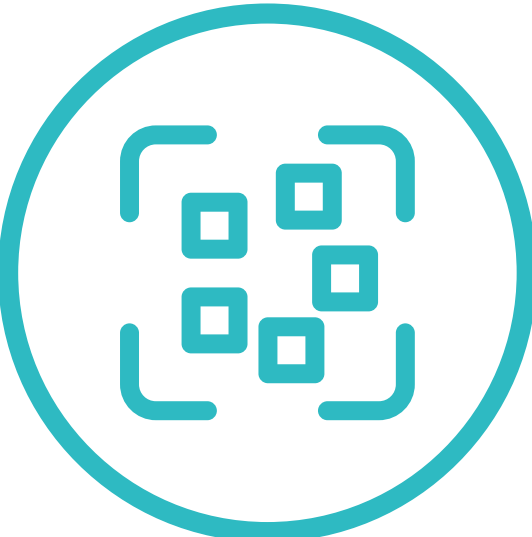
- **Leading Vendors**
 Strong overall solutions that possess the must have product and strategic capabilities for this use case
- **Product-Focused Vendors**
 Solutions with strong product capabilities but do not meet the strategy score threshold
- **Adjacent Vendors**
 Strong overall solutions but do not have the required capabilities for this market use case
- **Specialized Vendors**
 Solutions that can solve for a part of the use case but do not have all must have capabilities
- **Adjacent Leaders**
 Solutions with capabilities that compete with leading vendors but are not primarily focused on serving this use case



Vendor positioning on the Link Index for ATO Prevention in Banking



Leading vendors have three distinct focuses: authentication, fraud prevention, and identity



Vendors have distinct focuses when combatting ATO

Most vendors focus on authentication, fraud prevention, or identity approaches.



Solution providers in the ATO landscape have differentiated strategies and some have limited capability overlap.



Banks leverage multiple vendors in their tech stack

Vendors with differentiated capabilities work alongside each other to provide comprehensive coverage.



Fraud, authentication, and identity capabilities complement each other to cover the entire customer lifecycle.

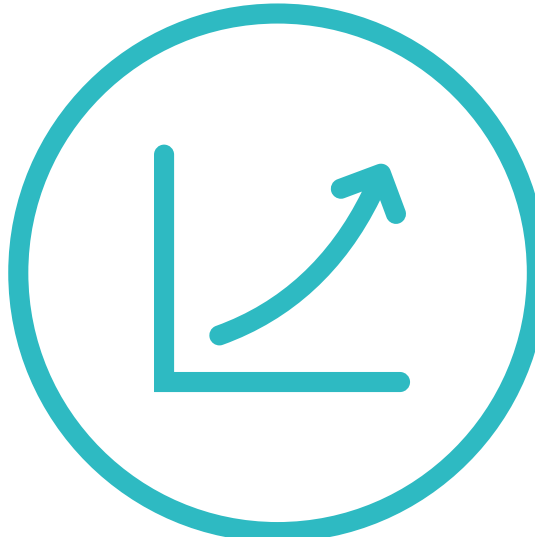


Credit bureaus and card issuers have strong market presence

Experian, TransUnion, and Mastercard all rank within the top 5 for market presence.



These companies can leverage their extensive data assets to fine-tune models and accurately detect ATO.



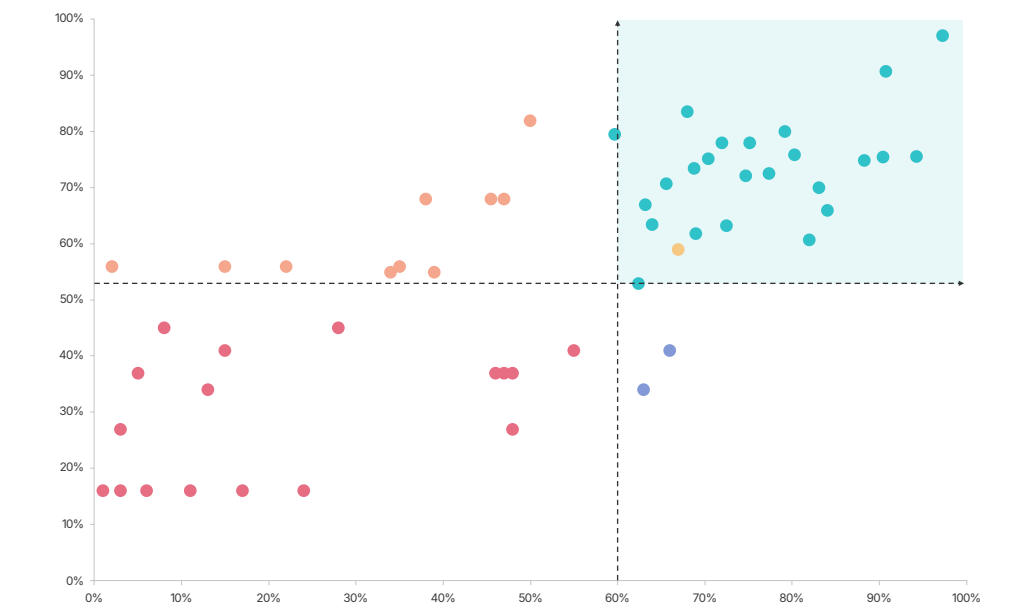
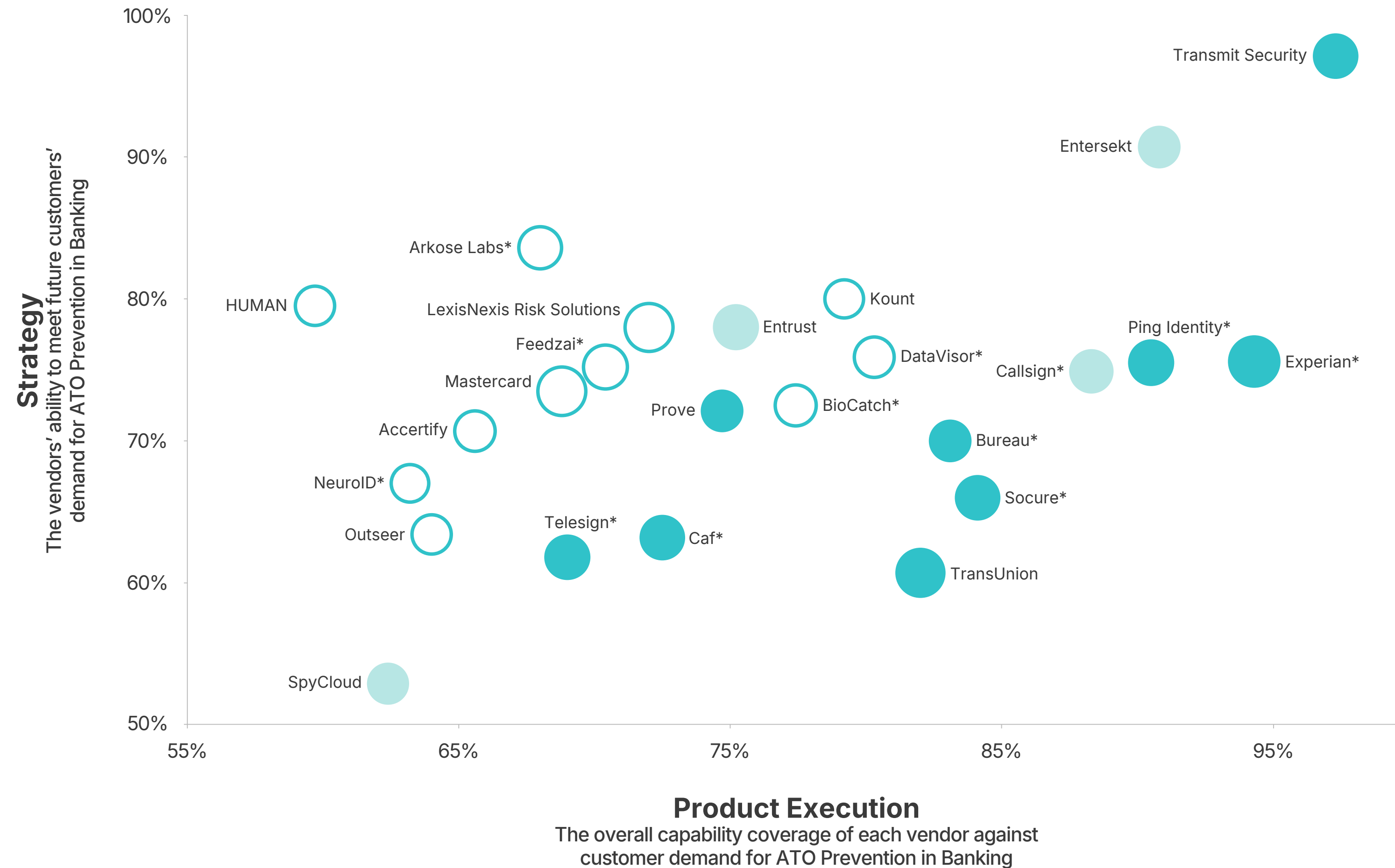
Overall satisfaction has highest correlation with scalability

Despite being the 5 ranked KPC, buyer satisfaction saw the highest correlation with scalability satisfaction.



Scalability is vital for banks to handle increasing volumes and evolving fraud tactics efficiently.

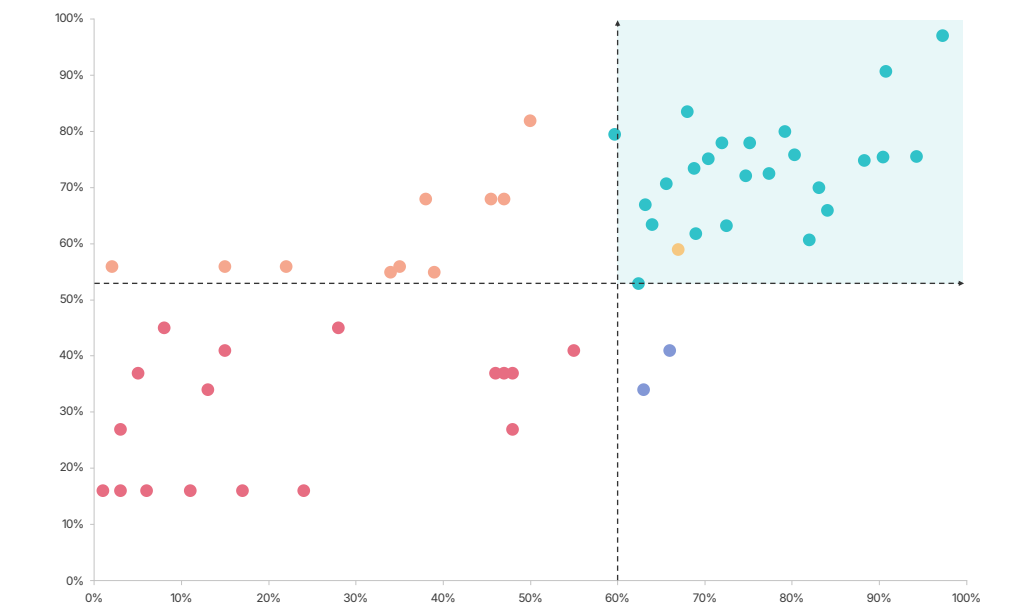
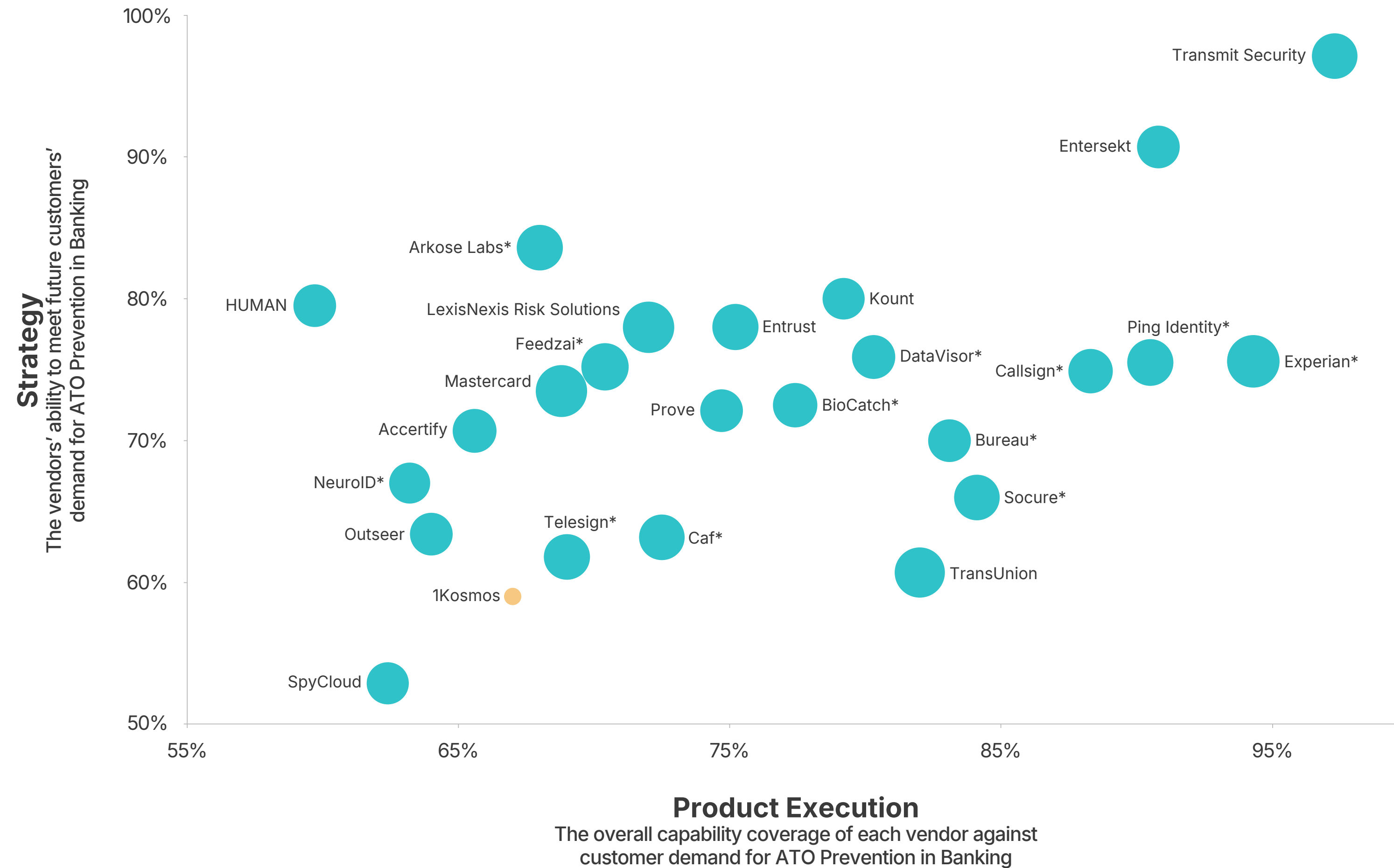
Link Index for Account Takeover Prevention in Banking: Leading Vendors



- Fraud-Focused Vendors**
 These solutions use probabilistic data, including behavioral signals, to protect against fraud mainly at the transaction level
- Authentication-Focused Vendors**
 These solutions use comprehensive authentication capabilities to prevent unauthorized access to accounts during login
- Identity-Focused Vendors**
 These solutions take a hybrid approach, combining authentication and fraud prevention methods, with identity acting as the bridge between the two

Note: Companies with an asterisk (*) participated in an Analyst Briefing with Liminal for this report. Bubble Size on the Link Index displays size of Market Presence.

Link Index for Account Takeover Prevention in Banking: Leading Vendors and Adjacent Leaders



- **Leading Vendors**
 Strong overall solutions that possess the must have product and strategic capabilities for this use case
- **Adjacent Leaders**
 Solutions with capabilities that compete with leading vendors but are not primarily focused on serving this use case

Note: Companies with an asterisk (*) participated in an Analyst Briefing with Liminal for this report. Bubble Size on the Link Index displays size of Market Presence.



LINK INDEX

Vendor Overviews

©2024 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

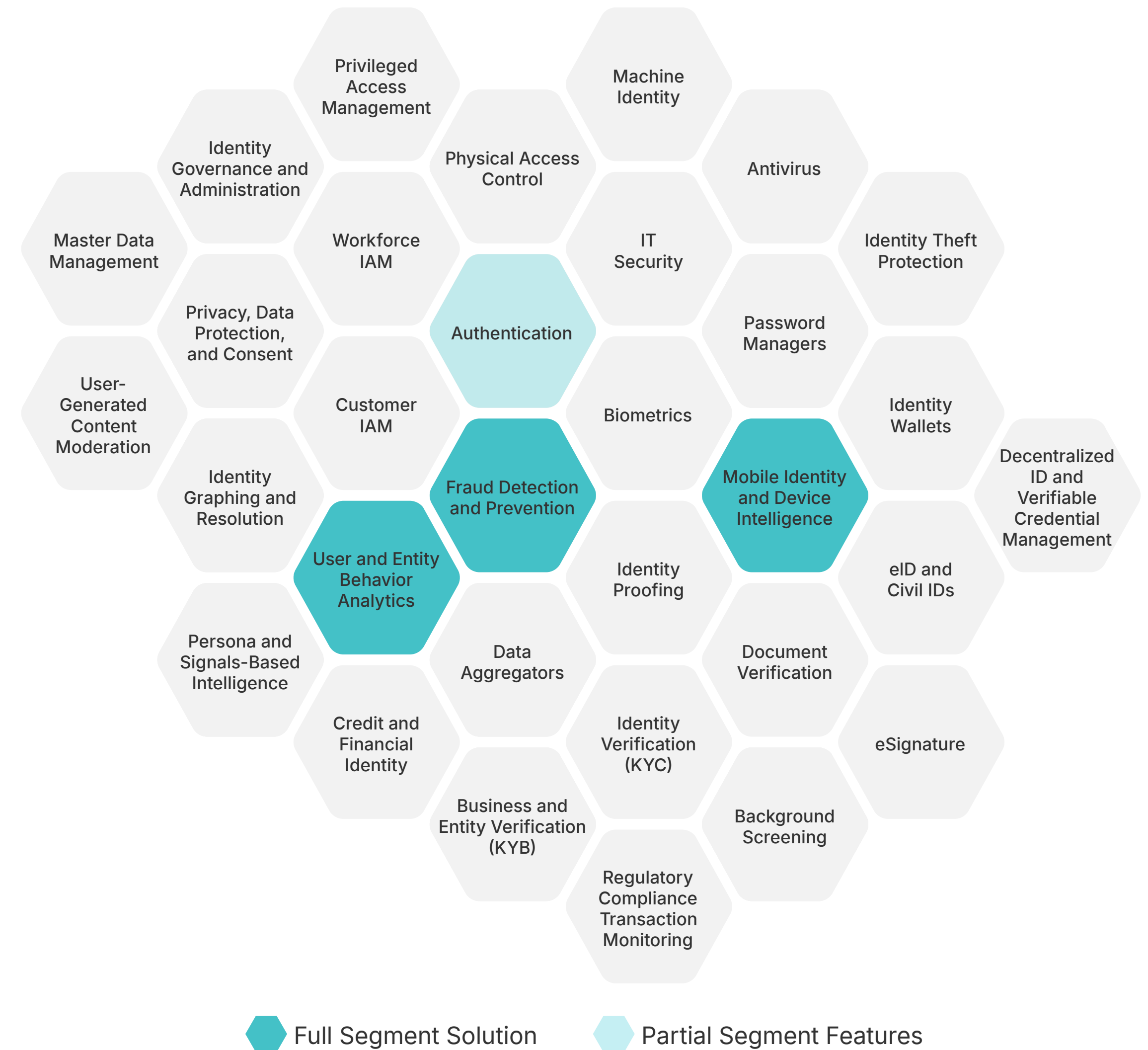


Accertify

Accertify helps its customers by addressing fraud-related use cases across the customer lifecycle. Its solutions focus on fraud prevention, chargeback management, and digital identity verification. The company prevents fraud across various verticals, including e-commerce, financial services, and travel. Accertify focuses on providing tools for risk assessment, customer authentication, fraud transaction monitoring, payment facilitation, and dispute management that balance the need to operate a secure business with the imperative to reduce friction for digital customers.

Company Information ¹	
Headquarters	Itasca, Illinois
No. of Employees	563 as of May 2024
Last Raised	Buyout/LBO, May 2024
Primary Segment	Fraud Detection and Prevention, User and Entity Behavior Analytics, Authentication, Mobile Identity and Device Intelligence
Vertical Focus	Financial Services, Gaming, eCommerce, Travel
Geographic Focus	North America, Europe, Asia-Pacific
Notable Customers	Accertify does not publicly disclose banking customers

(1) Link



Accertify's Strategy

Strategy	Excellent	Accertify is in a strong strategic position on the back-end of ATO detection suites; these capabilities power an exceptional UX that delivers frictionless digital experiences for banking customers.
Behavioral Capabilities	Excellent	Accertify provides behavioral analytics and bot detection to effectively identify and prevent fraudulent behavior, leading to fraudulent transactions and financial losses. However, it does not offer behavioral biometrics like some other ATO prevention vendors.
Passwordless Authentication	Strong	As a back-end analytics and fraud management tool, Accertify does not focus on passwordless authentication methods such as passkeys, QR code authentication, or WebAuthn. Instead, it emphasizes leveraging behavioral signals for fraud prevention.
Cost	Excellent	Accertify's pricing model is non-public, however the company appears to concentrate on enterprise sales as a primary channel. Customers found that cost efficiency generally provided high value for spend. Accertify predominantly serves enterprise clientele with hundreds of thousands to millions of customers, enterprise deployments are likely to maximize spend efficiency.
User Experience	Exceptional	According to banking customers, Accertify offers one of the best customer experiences among all ATO prevention vendors. With experience in both eCommerce and financial services, the company is adept at providing friction-free solutions, which are highly demanded by the eCommerce sector.

Analyst Notes on Strategy

Accertify's Account Protection solution employs a multi-layered approach to combat account takeover and fraudulent account creation attempts. First, it leverages behavioral analytics to analyze user behaviors, device interactions, and transaction patterns, enabling the identification of anomalies that may indicate fraudulent activities.

Apart from its excellent ability to address emerging behavioral requirements, Accertify is noted for empowering buyers to deliver stellar customer experiences. Major e-commerce and travel merchants accept that an optimal amount of fraud is non-zero; Accertify specializes in its solution that enables clients to monitor buyer activity to position fraud within risk appetites while minimizing friction.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Accertify's Market Presence

Market Presence	Excellent	Accertify is primarily recognized for its chargeback management solutions. While it benefited from strong brand recognition as a former subsidiary of American Express, Accertify is most known for its impressive customer portfolio across financial services and e-commerce.
Brand Awareness	Excellent	Accertify was a subsidiary of American Express till January 2024 when it was acquired by Accel-KKR. However, they benefited from strong brand recognition as part of the American Express parent company with 76% of financial service familiar with their brand and solutions.
Market Leadership	Excellent	Of those practitioners who were familiar with the brand, 22% recognized them as market leaders. The company's recent acquisition positions it for accelerated growth and innovation, further solidifying its leadership in the global fraud protection technology market.
Market Penetration	Excellent	Accertify has achieved strong market penetration in financial services by providing fraud prevention and chargeback management solutions to major banks and financial institutions globally. Leveraging advanced machine learning and behavioral analytics, Accertify's platform helps these institutions mitigate fraud risks, enhance transaction security, and improve operational efficiency.
Company Size	Excellent	Accertify, headquartered in Itasca, Illinois, employs approximately 550 people and operates globally with regional offices in London, Madrid, Sydney, Amsterdam, Mexico City, and Gurgaon.
Employee Growth	Strong	The company has experienced an 8% year-over-year employee growth. This growth reflects the company's ongoing expansion and commitment to enhancing its fraud prevention and digital identity solutions.

Analyst Notes on Market Presence

Accertify is a leading provider of fraud prevention, chargeback management, account protection, and payment gateway solutions. Accertify's advanced technologies help enterprises globally to address ATO challenges. Accertify's customer base is predominantly in the United States, though it also has a significant presence in the United Kingdom and India.

In May 2024, Accel-KKR, a technology-focused private equity firm, completed the acquisition of Accertify from American Express—this strategic move positions Accertify for accelerated growth and innovation in the global fraud protection technology market. The acquisition allows Accertify to operate as an independent company, focusing on expanding its market presence and enhancing its product offerings. While Accertify has natively offered payment fraud capabilities capable of interfacing with all of the major card networks, the company may enjoy cozier relationships with financial institutions as they attain their independence from the card giant.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Accertify Account Protection

Accertify Account Protection is designed to safeguard against fraudulent account openings and account takeovers. It provides insights by analyzing device information, connection methods, location, and user behavior. The platform aims to distinguish between legitimate and fraudulent activities, enhancing both security and user experience. The solution suits various industries, including online retail, financial services, travel, and iGaming.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

Product Visuals

Accertify does not provide publicly available product visuals for Account Protection.

Accertify Account Protection

Product	Strong	Accertify achieves exceptional buyer satisfaction by offering accurate and scalable ATO solutions for banks, protecting against ATO using several fraud detection features.
Product Capability	Strong	While Accertify does not primarily focus on authentication and therefore has a more limited capability set in that area, the company excels at fraud prevention. It offers robust capabilities such as social engineering detection, device risk scoring, and location intelligence to effectively prevent ATO-related fraudulent transactions.
Scalability	Excellent	Accertify has large customers across a wide range of different verticals, reflecting very strong scalability satisfaction ratings according to customer feedback. Additionally, by offering coverage for use cases such as returns abuse and chargeback management, the company can assist banks looking to expand their fraud prevention strategies.
Customization	Excellent	By offering a comprehensive range of security measures, including device profiling, connection analysis, behavioral analytics, and reputational information, Accertify enables customers to customize end-to-end user journeys to meet their organization's specific needs.
Accuracy	Excellent	By combining various signals such as behavioral analytics, device risk scoring, bot detection, and location intelligence, Accertify effectively detects ATO threats and minimizes financial loss with high accuracy.
Product Integration	Strong	Accertify offers an Account Protection API that enables customers to monitor user actions to guard against ATO and new account openings. Additionally, the company provides separate APIs for chargebacks, retail fraud, and other specific products, allowing for targeted and comprehensive fraud prevention.
Buyer Satisfaction	Exceptional	Accertify achieved one of the highest buyer satisfaction ratings among all the vendors we profiled. By offering comprehensive coverage across the customer lifecycle, the company provides robust risk detection to effectively combat ATO.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Accertify Account Protection

Accertify's Account Protection solution is a comprehensive fraud prevention offering designed to safeguard businesses against account-related fraud, including account takeovers, and account creation fraud. It employs advanced techniques such as device fingerprinting, IP intelligence, geolocation analysis, and user behavior analytics to verify the true identity behind digital transactions and account logins. This helps detect unauthorized access attempts using stolen credentials and prevent fraudsters from creating fraudulent accounts using stolen personal information from data breaches.

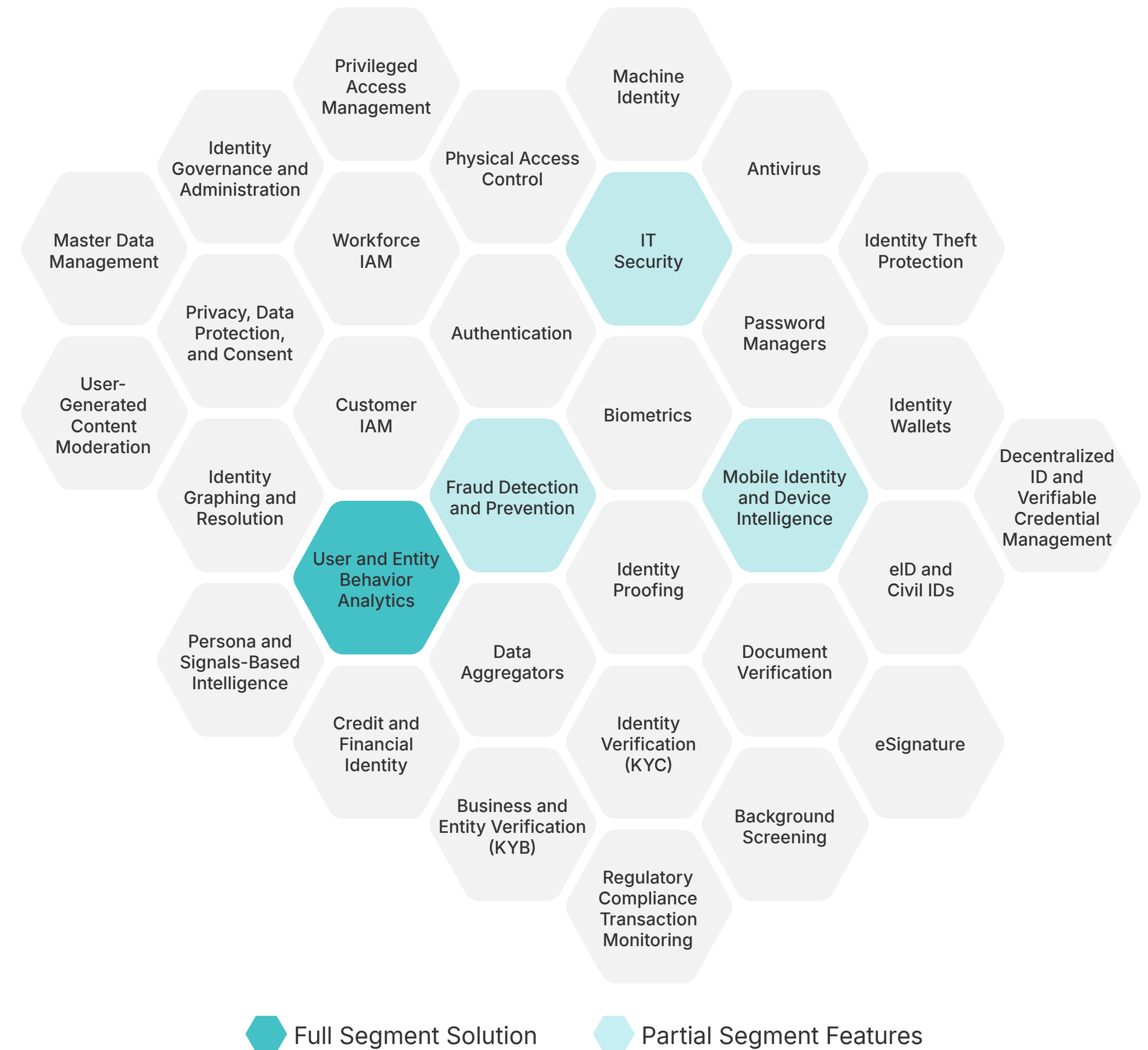
The solution leverages machine learning models to differentiate between genuine and synthetic identities during account creation, mitigating the risk of account creation fraud and bust-out fraud schemes. Additionally, it identifies patterns indicative of multiple account abuse, such as a single device being used to open multiple accounts to exploit promotions, leave fake reviews, or circumvent bans across various industries like gaming, retail, and more.

With customizable rules, risk scoring, reporting capabilities, and seamless integration with Accertify's other fraud prevention offerings like chargeback management and payment gateways, the Account Protection solution enables businesses to effectively combat account-related fraud risks while delivering a seamless customer experience.

Arkose Labs

Arkose Labs offers advanced fraud prevention and bot management solutions to protect businesses from automated attacks and online fraud. The company detects and mitigates threats across various digital channels. It provides tools for securing account onboarding and login and aims to reduce fraud losses and operational costs, supporting finance, retail, and gaming industries.

Company Information ¹	
Headquarters	San Mateo, California
No. of Employees	216 as of May 2024
Last Raised	\$70M, Series C Round in May 2021
Primary Segment	User and Entity Behavior Analytics
Vertical Focus	Financial Services, Travel, Media and Entertainment, Gaming, Gig Economy, Technology, Travel and Hospitality
Geographic Focus	Nrth America, Europe, Latin America, Asia-Pacific
Notable Customers	Arkose Labs does not publicly disclose banking customers



(1) Link

Arkose Labs' Strategy

Strategy	Exceptional	Arkose Labs is a leading provider of behavioral signal solutions, offering an exceptional user experience by leveraging passive signals.
Behavioral Capabilities	Exceptional	Arkose Labs effectively leverages a comprehensive set of behavioral signals to detect fraudulent behavior across a wide range of ATO threat vectors. The company offers behavioral biometrics, behavioral analytics, and bot detection to effectively prevent ATO.
Passwordless Authentication	Excellent	Passwordless authentication is not a focus for Arkose Labs. Instead, the company relies heavily on behavioral signals to prevent fraudulent logins and transactions, rather than completely rely on passwordless methods like QR code authentication and WebAuthn
Cost	Excellent	Arkose Labs received favorable rankings for value among ATO prevention solutions in banking. As a point solution focusing on behavioral signals, the company is often integrated alongside other vendors in tech stacks.
User Experience	Exceptional	By operating in the background and leveraging contextual data such as PII, device profiles, reputation, and network assessments, Arkose Labs provides threat detection without relying on cumbersome authentication methods like passwords that users find inconvenient.

Analyst Notes on Strategy

Arkose Labs heavily relies on behavioral analytics to detect and mitigate fraud across various attack vectors. Their solutions analyze user behaviors, device interactions, and transaction patterns to accurately assess risk in real-time. The platform correlates real-time, historic, customer-specific, and global data to provide transparent risk scoring and enhance decision-making confidence. Moreover, bot detection is a core capability of Arkose Labs' solutions, mainly their flagship product, Arkose Bot Manager. The platform utilizes multi-layered detection techniques, including machine learning, global telemetry, and adaptive step-up challenges, to identify and differentiate malicious bot traffic from legitimate user traffic. Arkose Labs provides over 70 raw risk insights and 125+ signals to enhance bot detection accuracy.

Arkose Labs offers a unique \$1 million warranty against credential stuffing attacks, underscoring its confidence in its bot detection and mitigation capabilities. This warranty and its guaranteed mitigation SLA for 100% remediation of automated attacks set it apart in the market and provide customers with added assurance.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Arkose Labs' Market Presence

Market Presence	Excellent	Arkose Labs offers a market-leading bot detection and mitigation solution that is well-recognized by financial institutions for its efficacy.
Brand Awareness	Exceptional	The company's innovative \$1 million warranties for credential stuffing, SMS toll fraud, and card testing, along with its commitment to digital accessibility, have supported strong brand awareness – 70% of surveyed financial institutions were familiar with their brand and solution for ATO prevention.
Market Leadership	Exceptional	Arkose Labs is a leader in bot detection and mitigation and is widely recognized for their solutions - of those financial institutions that were familiar with their brand, 40% recognized them as market leaders.
Market Penetration	Excellent	Arkose Labs has achieved significant penetration in the financial services sector, protecting some of the world's largest banks, payment providers, and fintech companies from sophisticated fraud and bot attacks.
Company Size	Excellent	Arkose Labs, headquartered in San Mateo, California, employs approximately 200 people and operates across multiple global offices, including locations in Australia, the United Kingdom, and Costa Rica. The company has raised a total of \$106.5 million in funding, reflecting its significant presence and influence in the cybersecurity
Employee Growth	Excellent	The company has experience strong employee growth metrics – roughly 20% increase YoY. The company experienced growth in APAC and EMEA while also expanding its North American foothold.

Analyst Notes on Market Presence

Arkose Labs has established itself as a prominent player in fraud prevention and bot management, serving some of the world's largest enterprises and Fortune 500 companies across various industries. They boast two of the top three global banks and one of the top three neobanks in North America as customers.

The company's flagship product, Arkose Bot Manager, leverages advanced AI and machine learning capabilities to detect and mitigate sophisticated automated attacks, including account takeover attempts, credential stuffing, and SMS toll fraud. The company's market reach spans finance and fintech, retail and e-commerce, online gaming and telecommunications, technology platforms, social media and streaming, travel, and the sharing economy. Arkose Labs boasts an impressive client base, with 20% of its customers being Fortune 500 companies, further solidifying its position as a trusted partner for large enterprises.

Arkose Labs' growth trajectory has been significant, with the company ranking No. 76 on Inc. Magazine's prestigious list of the fastest-growing private companies in the Pacific region in 2024. The company's growth rate of 162.77% between 2020 and 2022 surpassed the average growth rate of companies on the list, reflecting the increasing demand for its solutions and the efficacy of its technology.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Arkose Labs Bot Manager

Arkose Labs Bot Manager is a security solution designed to prevent fraud and bot attacks. It uses a combination of multi-layered detection techniques, including device, network, and behavioral analysis, to identify and mitigate threats in real-time. The platform aims to target suspicious activity and provide extensive risk insights while minimizing disruption for legitimate users.

ATO Prevention Product Capability Coverage¹

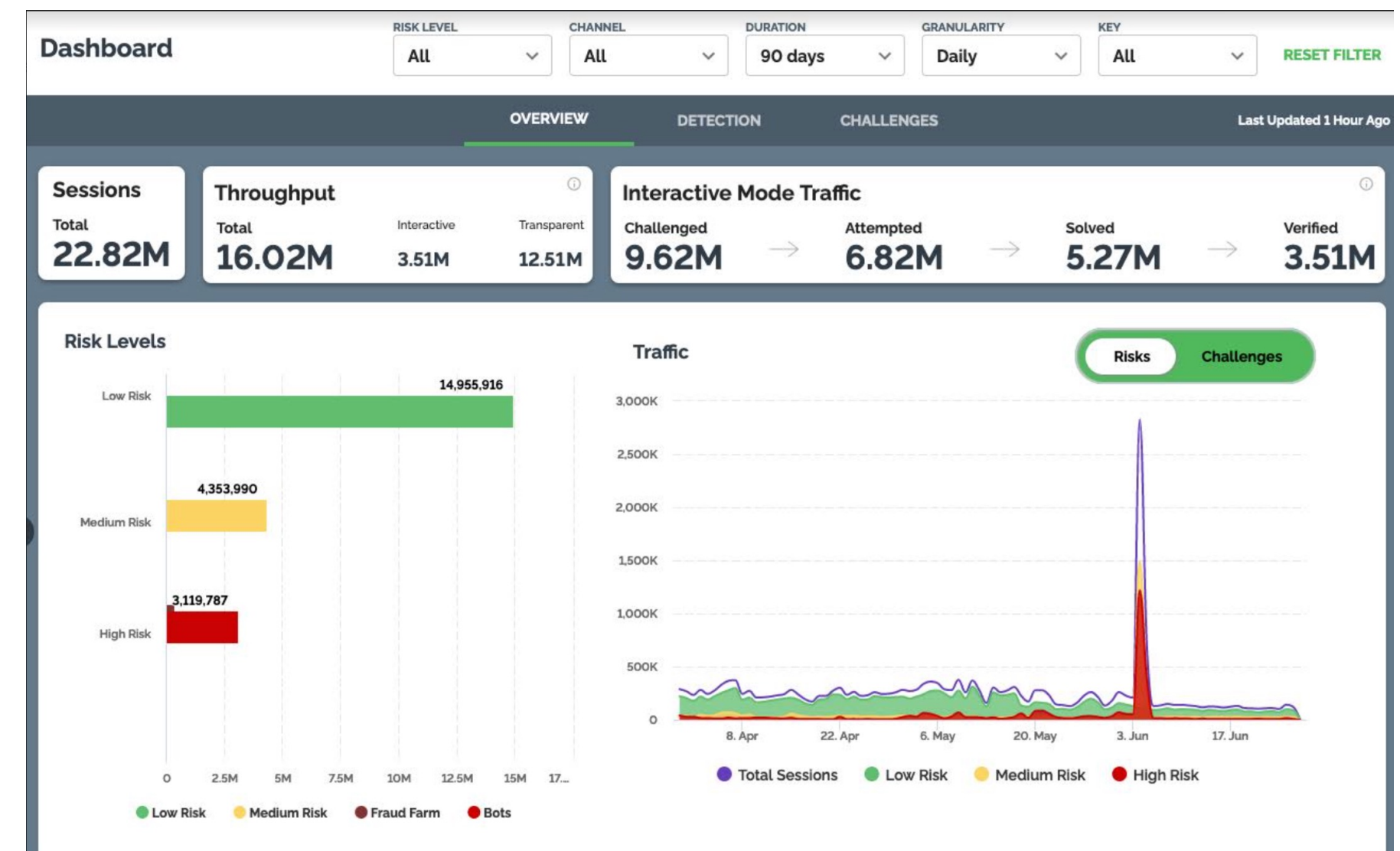
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from company.

Product Visuals²



Arkose Labs Bot Manager

Product	Strong	Specialized bot management capabilities enable Arkose Labs to robustly detect and prevent challenging ATO threat vectors such as credential stuffing and phishing.
Product Capability	Strong	While Arkose Labs has a less extensive product suite in terms of overall capabilities, its Bot Manager excels in providing highly accurate bot detection. This ensures that non-human sessions are identified and terminated before financial loss can occur.
Scalability	Excellent	One of Arkose's key differentiators is its continuous learning models that leverage a wide range of data. This allows the solution to become increasingly effective as the number of users and transactions rises.
Customization	Exceptional	Arkose Labs leverages a wide range of signals, including device profiling and reputation, network assessment, customer data exchange, and PII intelligence. It also provides a visualization portal for further customization, enhancing its ability to detect and prevent fraudulent activities.
Accuracy	Exceptional	Arkose Labs achieved one of the highest accuracy scores among the vendors we profiled, according to banking customers. By combining behavioral biometrics and behavioral analytics, the company provides highly precise bot detection.
Product Integration	Excellent	Arkose Labs offers API integration with its Bot Manager platform, providing several configuration options tailored to the specific use cases and needs of its banking customers.
Buyer Satisfaction	Exceptional	Arkose Labs provides highly effective bot detection and management, as evidenced by positive customer feedback. The company's confidence in their product is further demonstrated by their \$1 million credential stuffing warranty. Additionally, Arkose Labs offers 24/7 support from SOC specialists to ensure comprehensive customer assistance.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.




Analyst Notes on Arkose Labs Bot Manager

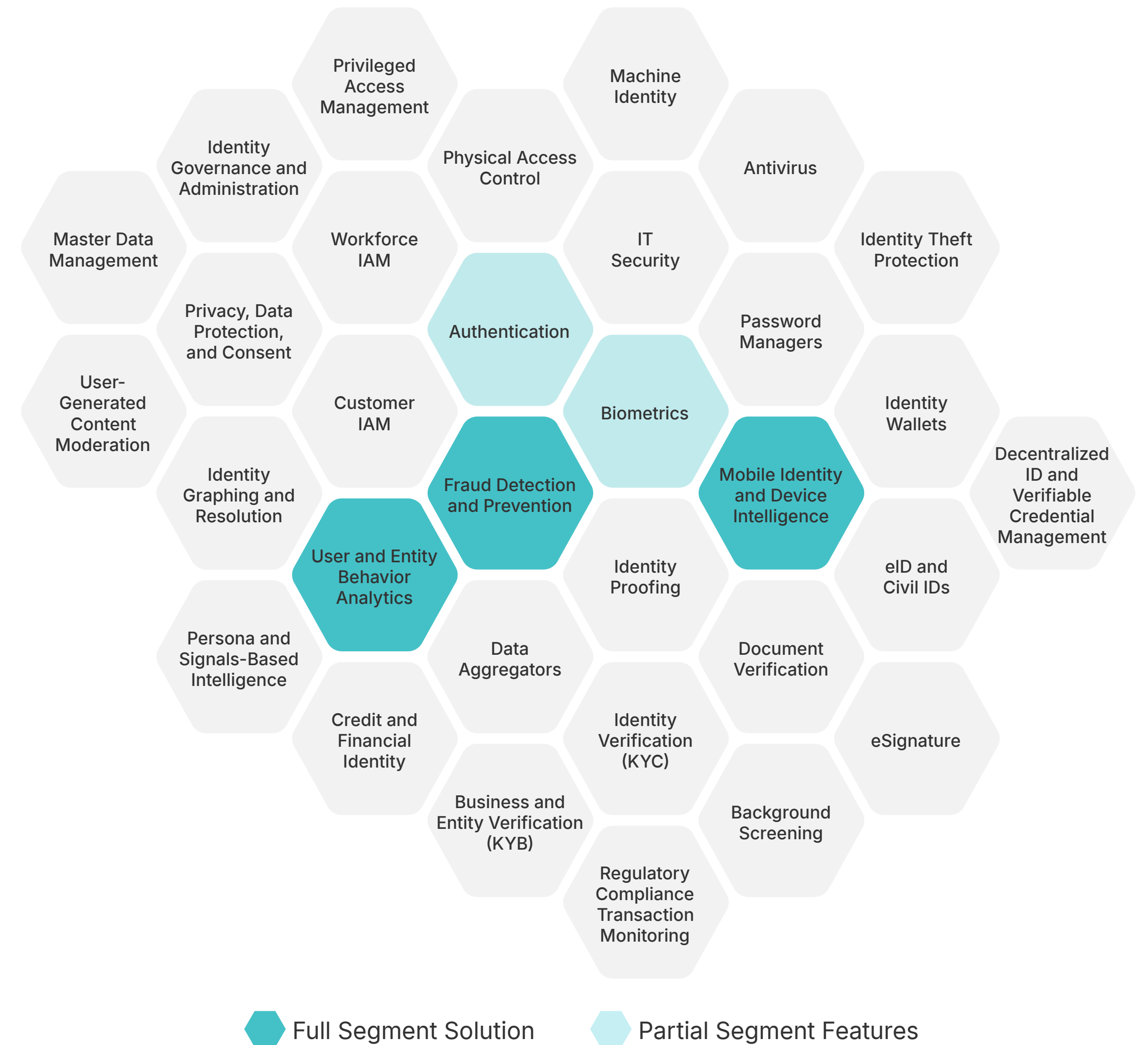
Arkose Labs Bot Manager offers a comprehensive solution for defending against automated bot attacks across a variety of online platforms. The product leverages advanced machine learning and behavioral analysis for various solutions including account protection and transaction protection. This ensures Arkose's clients a robust defense against bots without disrupting genuine users. Their platform provides real-time risk classification and dynamic response mechanisms, allowing organizations to identify and mitigate threats as they occur.

The platform's defenses-in-depth strategy encompasses various detection and response layers. Its real-time risk classification differentiates between good users and malicious actors, using detailed analysis of user behavior, device attributes, and network signals. Specifically, the company analyzes 70 risk attributes in their model to ensure high accuracy. With dynamic attack response capabilities, Arkose Labs can adapt to emerging threats and ensure that legitimate users are not affected. Additionally, their decisioning and data-sharing frameworks enhance collaboration and threat intelligence across industries.

BioCatch

BioCatch specializes in behavioral biometrics, providing solutions to detect and prevent fraud by analyzing user behavior. Their platform leverages machine learning to create unique user profiles based on interactions such as typing patterns and mouse movements. This technology enables real-time risk assessments to identify and mitigate fraudulent activities, enhancing security for online transactions and account management.

Company Information ¹	
Headquarters	Tel Aviv-Yafo, Tel Aviv
No. of Employees	320 as of May 2024
Last Raised	\$44.4M Series C, July 2020
Primary Segment	User and Entity Behavior Analytics, Fraud Detection and Prevention, Mobile Identity and Device Intelligence
Vertical Focus	Financial Services
Geographic Focus	NA, Europe, APAC, MEA
Notable Customers	  



(1) Link

BioCatch's Strategy

Strategy	Excellent	As a leading behavioral biometrics provider, BioCatch leverages highly sophisticated signals to detect and prevent fraud.
Behavioral Capabilities	Exceptional	As a pioneer in behavioral biometrics, BioCatch boasts one of the strongest behavioral capabilities among ATO prevention vendors in the market. The company can track users across sessions, analyzing details such as keystroke rhythm, mouse movements, and touchscreen behavior to detect risk.
Passwordless Authentication	Strong	BioCatch, with its primary focus on behavioral biometrics, offers limited passwordless authentication options. As a result, passwordless authentication methods are not a central focus of their solutions.
Cost	Strong	Behavioral biometrics solutions typically require lengthy and costly implementations before reaching full effectiveness, making them an expensive option. As a result, BioCatch predominantly collaborates with very large financial institutions that are willing to accept higher costs for highly sophisticated fraud detection solutions.
User Experience	Strong	BioCatch effectively leverages behavioral biometrics to conduct passive analysis of user sessions, thereby minimizing friction. However, its user experience scores were slightly lower compared to some of the other vendors we profiled.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Strategy

BioCatch Connect, its ATO Prevention solution, delivers profound visibility into fraud risk by continuously monitoring user behavior from login to logout. It leverages BioCatch's proprietary Behavioral Biometrics technology to analyze a user's physical and cognitive digital behavior throughout a session, enabling the detection of even the most sophisticated account takeover attacks. The solution tackles various account takeover threats, including bots and aggregators, malware, social engineering, voice scams, remote access tools, mobile emulators, and instances of account takeover using stolen account credentials.

To combat bots and aggregators, BioCatch detects automated patterns by analyzing behavioral indicators such as navigation preferences, hand-eye coordination, and press size against the user's historical profile. For malware detection, the platform compares a user's cognitive behavior, including shortcuts, long-term memory, and navigation patterns, against population-level profiles to identify anomalies. Additionally, the solution determines user intent and emotional state by surfacing behaviors that align with complex fraud threats, such as hesitation, dictation, and coercion, which can indicate social engineering or voice scams.

Connect incorporates behavioral biometrics to identify digital traits like device type and operating system, allowing for a seamless experience across desktop and mobile. Connect also provides gesture analysis for consistent formatting by analyzing mouse movements, gestures, and other digital traits when using websites or mobile apps.

BioCatch's Market Presence

Market Presence	Excellent	BioCatch is a strong fraud detection player with particular leadership in behavioral biometrics. They are well-recognized and adopted among financial institutions.
Brand Awareness	Excellent	BioCatch is highly recognized within the financial industry for its solutions in preventing account takeover (ATO), with 57% of surveyed financial institutions familiar with their brand. This high level of recognition positions BioCatch among the top brands in the space, strengthening their ability to attract new business.
Market Leadership	Excellent	Among those familiar with BioCatch, 91% view them as market leaders, underscoring the effectiveness of their solutions, which primarily utilize behavioral biometrics.
Market Penetration	Excellent	BioCatch has achieved substantial market penetration in financial institutions, with over 30 of the world's largest 100 banks and more than 180 financial institutions relying on its behavioral biometric intelligence to combat fraud and facilitate digital transformation.
Company Size	Excellent	BioCatch, headquartered in Tel Aviv, employs over 300 people across eight global locations, including the United States, Israel, Australia, Brazil, India, and Mexico. The company has raised over \$300 million in funding, reflecting its significant growth and market presence in the fraud prevention industry.
Employee Growth	Excellent	They have experienced roughly 14% YoY employee growth driven by the company's market expansion and increasing demand for its behavioral biometric solutions across several customers.

Analyst Notes on Market Presence

BioCatch has solidified its position as a global leader in digital fraud detection and response, powered by its pioneering behavioral biometric intelligence technology. The company's rapid growth and adoption are evident from its impressive customer base, which includes 29 of the world's top 100 banks and 176 of the largest 500 companies across various industries. As of June 2023, BioCatch was processing over seven billion user sessions per month, a testament to its technology's scalability and ability to meet the increasing demand for advanced fraud prevention solutions. The company's flagship product, BioCatch Connect, has gained significant traction, particularly in the Latin American region, where organizations are investing heavily in digital transformation initiatives.

BioCatch's market reach extends beyond the financial sector. The company recently onboarded one of the top three global telecommunications providers as a customer. Additionally, eight of the top ten banks in Australia now rely on BioCatch's solutions for advanced fraud detection powered by behavioral biometric intelligence.

The company's growth trajectory has been remarkable, with BioCatch achieving a 45% increase in annual recurring revenue (ARR) in Q2 2023 compared to the same period in 2022. Furthermore, in November 2023, BioCatch surpassed the \$100 million ARR milestone, solidifying its status as a "Centaur" company and cementing its position as a market leader in the behavioral-powered digital fraud prevention space.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

BioCatch Connect

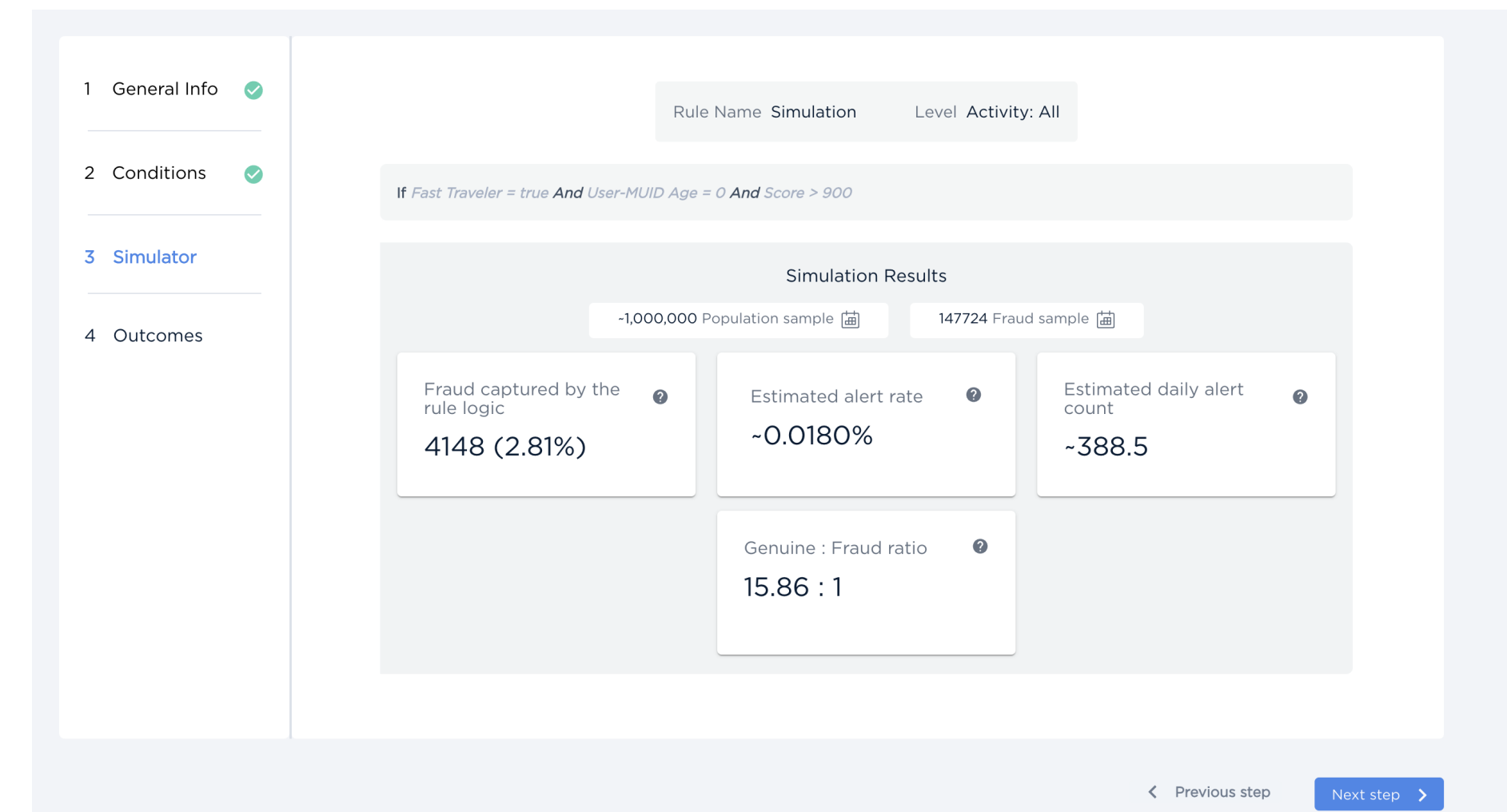
BioCatch Connect is a fraud detection platform that leverages machine learning to analyze a wide range of behavioral, device, network, and transactional data. It provides real-time risk assessments and insights into user behavior to identify and mitigate fraudulent activities. The platform uses behavioral biometrics to detect anomalies, aiding fraud and AML teams in visualizing and investigating suspicious activities.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from company website (link: <https://www.biocatch.com/biocatch-connect/predictive-intelligence>).

Product Visuals²



BioCatch Connect

Product	Excellent	BioCatch is one of the leading behavioral biometrics solutions, offering highly accurate ATO prevention by looking at signals such as keystroke behavior and mouse movements.
Product Capability	Excellent	BioCatch's capability set is driven by its impressive behavioral biometrics, which analyze mouse movements, keystroke patterns, and touchscreen behavior to assess risk and identify malicious actors.
Scalability	Excellent	BioCatch has focused on targeting large financial institutions with its behavioral biometrics solution. The company has a strong track record of scaling alongside major banks without compromising on accuracy.
Customization	Strong	BioCatch offers Continuous Behavioral Sequencing™, which allows for the analysis of data collected by fraud models. The company also provides intelligence briefings with experts to help banks customize their techniques and procedures according to their organizational needs.
Accuracy	Excellent	Behavioral biometrics enable tracking users across multiple sessions and detecting anomalies, terminating sessions if risk levels significantly rise. Additionally, because BioCatch collaborates with large-scale financial institutions, they have access to extensive data sets to inform and refine their models.
Product Integration	Excellent	Due to the nature of behavioral biometrics solutions, which require multiple user sessions to become effective, product integration times may be longer than other solutions. BioCatch primarily collaborates with large banks that possess significant engineering resources to manage these integrations.
Buyer Satisfaction	Excellent	With behavioral biometrics, social engineering detection, and money mule detection all integrated into the single BioCatch Connect platform, the company offers a comprehensive range of protections that are easily accessible to customers.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on BioCatch Connect




BioCatch Connect is an integrated fraud product designed to proactively detect and accelerate the interdiction of fraudulent activities. Rather than treating behavior as a secondary signal, behavior is leveraged as a source of biometric intelligence at the center of the solution's artificial intelligence and machine learning models. At BioCatch Connect's core is its Fraud Telemetry Collection capability. It uses lightweight mobile and web SDKs to continuously collect thousands of signals from five distinct data sources – applications, user behaviors, devices, networks, and transactions – across billions of monthly user sessions. This real-time streaming collection ensures no gaps in user activity awareness and enables correlated telemetry analysis without compromising user privacy.

BioCatch's proprietary Continuous Behavioral Sequencing™ (CBS) technology leverages advanced cognitive human behavioral science, data modeling, and machine learning algorithms to parse, match, analyze, merge, and score every collected data element. This process delivers fully integrated, actionable fraud intelligence by evaluating the authenticity of each unique user and calculating highly accurate, dynamic risk scores.

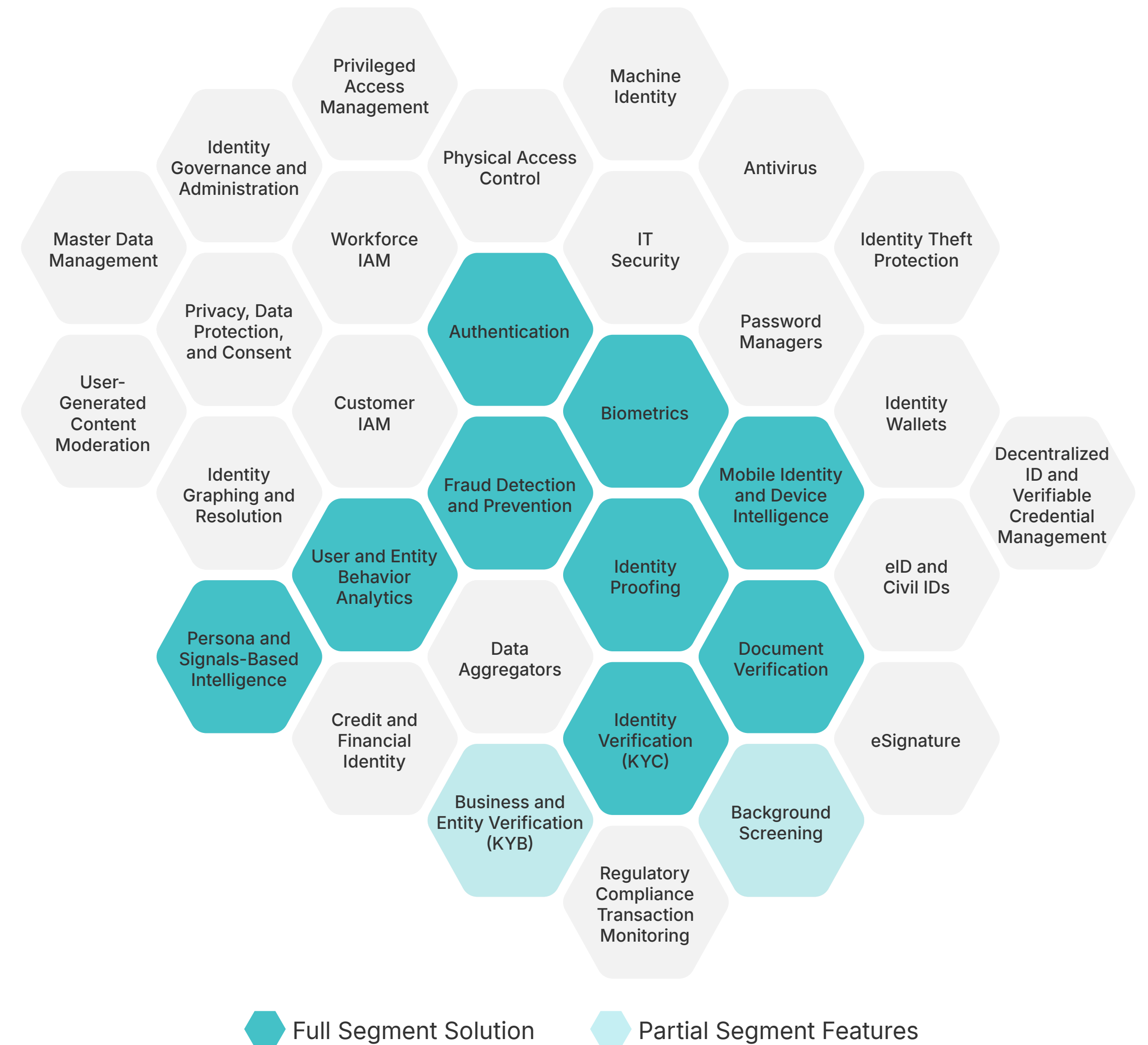
The Predictive Intelligence module of BioCatch Connect sits atop CBS technology, structuring and visualizing these dynamic user risk scores as actionable intelligence. This enables fraud teams to monitor, investigate, and prevent potential fraudulent user activities and sessions in real-time.

Bureau

Bureau provides an identity decisioning platform that enables fraud management and identity verification solutions. Their platform aggregates data and analyzes signals across the customer journey, to support bot protection, onboarding, transaction verification, and account management. Their solutions leverage machine learning, device intelligence, behavioral biometrics, and entity graphs to mitigate identity risk. Bureau empowers businesses to establish robust fraud management and compliance workflows that can protect their customers.

Company Information ¹	
Headquarters	San Francisco, California
No. of Employees	100 as of May 2024
Last Raised	\$16.5M, Series A Round in July 2023
Primary Segment	Fraud Detection and Prevention, Identity Verification (KYC)
Vertical Focus	Financial Services, Fintech, eCommerce, Gig Economy
Geographic Focus	North America, Europe, Middle East, Latin America, Asia Pacific
Notable Customers	  

(1) Link



Bureau's Strategy

Strategy	Excellent	Bureau possesses a robust set of behavioral capabilities that offer sophisticated threat detection to prevent ATO.
Behavioral Capabilities	Exceptional	Bureau specializes in providing behavioral biometrics to detect risk in a sophisticated manner. By analyzing signals such as mouse movements and typing patterns, the Bureau can identify anomalies and potential fraudsters.
Passwordless Authentication	Strong	Bureau focuses on providing behavioral signals for fraud detection and does not offer passwordless authentication options such as passkeys, QR codes, or WebAuthn.
Cost	Strong	Compared to other ATO prevention solutions, Bureau is considered to be expensive. However, by combining behavioral biometrics and device risk scoring, the company offers sophisticated threat detection for its customers.
User Experience	Strong	The end-customer experience facilitated by Bureau was not appraised as strongly as other vendors for banking customers. Liminal analysis found that its overall user experience still performed more strongly than many other solutions in the vendor universe. Bureau's solution does feature passwordless authentication which has a positive impact on user friction.

Analyst Notes on Strategy

Bureau offers a no-code identity and risk orchestration solution designed to streamline decisions from onboarding to KYC and fraud. Their platform leverages behavioral analytics and behavioral biometrics to enhance security and user verification processes. By analyzing user behaviors, device interactions, and transaction patterns, Bureau's platform can identify anomalies and potential fraud attempts, providing a robust defense against sophisticated threats. The platform also incorporates bot detection capabilities, utilizing machine learning algorithms to identify and mitigate automated attacks, ensuring that only legitimate users can access services.

Regarding the cost and commercial model, Bureau's platform is offered as a Software-as-a-service solution, which typically follows a subscription-based pricing model. The exact cost of the solution is determined through direct discussions with Bureau's sales team, considering factors such as the organization's size, required capabilities, and desired level of support and professional services. This flexible pricing approach allows organizations to tailor the solution to their specific needs while ensuring they receive the necessary support to effectively manage identity verification, compliance, and fraud prevention.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Bureau's Market Presence

Market Presence	Strong	Bureau has demonstrated strong penetration across the APAC region, boasting notable clients in India. The company can leverage their recent Series A funding to drive growth in new markets.
Brand Awareness	Strong	Bureau is primarily a device intelligence and fraud prevention provider – 44% of surveyed financial institution practitioners were familiar with their brand and solutions for ATO prevention.
Market Leadership	Excellent	Of those familiar with the Bureau brand and their solutions, roughly 22% recognized them as market leaders, indicating strong brand recognition among financial institutions. Bureau can capitalize on this market leadership to capture new business and upsell current customers.
Market Penetration	Excellent	Bureau has made significant strides in the financial services by providing many financial institutions with advanced identity verification and fraud prevention solutions, primarily in the APAC region.
Company Size	Strong	Bureau, founded in 2020, employs roughly 100 people and operates across multiple locations, including India, San Francisco, and Southeast Asia. The company has raised \$16.5 million in Series A funding that could be used to fuel additional growth.
Employee Growth	Excellent	Bureau has experienced substantial employee growth, increasing its workforce by roughly 30% in the past year, reflecting its rapid expansion and market demand for its services. This growth aligns with the company's strategy to enhance its global presence.

Analyst Notes on Market Presence

Founded in 2020, Bureau is an identity decisioning platform for fraud prevention and compliance management. Businesses use the Bureau Risk Orchestration Platform to manage compliance and prevent fraud in their customer journey. Today, the company serves customers across banking, fintech, insurance, the gig economy, and real money gaming. Bureau's revenues have grown 6x in the last 12 months, with over 300M identities verified through its platform. Bureau raised a \$4.5 million extension to its Series A in July 2023, as it looks to expand its current data coverage from 20 to more than 100 markets globally.

Bureau was set up in 2020 by Ranjan Reddy, who earlier founded payments startup Qubecell in Asia. It was acquired by Boku, and Ranjan served as the Chief Business Officer at Boku Identity, which Twilio later acquired. Bureau is the culmination of Ranjan's two decades of experience innovating customer journeys and starting a source of truth for a verified identity network. Bureau is backed by tier-one investors Okta, XYZ Capital, Quona Capital, Blume Ventures, Commerce Ventures, and Village Global. The company is headquartered in San Francisco, with offices in Bangalore, Singapore, and Dubai.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Bureau Device Intelligence

Bureau Device Intelligence combines device attributes, explicit user behavior like keystrokes and mouse movements, implicit user behavior like gestures and movement, and location data to provide modern, predictive signals to detect and prevent fraud. It analyzes hundreds of parameters beyond traditional device risk scoring for comprehensive ATO assurance. The solution provides real-time risk assessments to identify trustworthy identities and unique devices and detect bots, fraud rings, and bad actors. It integrates with iOS, Android, and web platforms to enhance security across digital interactions.

ATO Prevention Product Capability Coverage¹

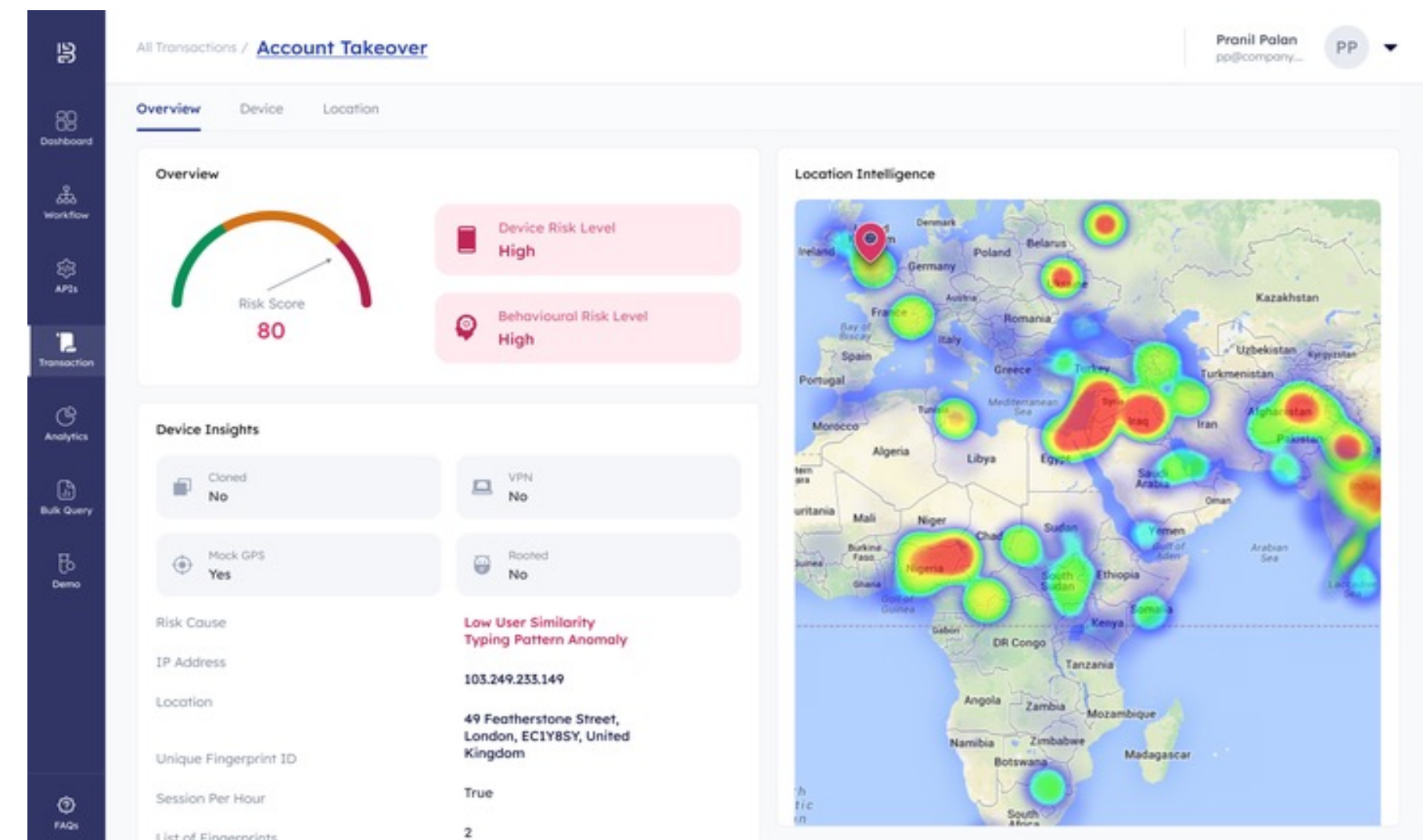
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from the company.

Product Visuals²



Bureau Device Intelligence

Product	Excellent	Bureau offers customizable solutions that protect against key ATO threat vectors such as social engineering, credential stuffing, and phishing.
Product Capability	Exceptional	Bureau offers a robust capability suite, including highly demanded features such as social engineering and scam detection, as well as behavioral biometrics, which is increasingly sought after by banking buyers.
Scalability	Strong	According to buyers, Bureau ranks lower than some competitors in terms of scalability. However, it offers identity verification and transaction abuse capabilities, which can be beneficial for banks looking to expand into new use cases.
Customization	Excellent	Bureau's primary differentiator is its orchestration platform, which supports various use cases and allows customers to customize the solution to their specific needs. It collects data throughout the customer journey, enabling a tailored and comprehensive approach to security and risk management.
Accuracy	Strong	Bureau's Device Intelligence feature binds the device ID to the account. If new devices are detected during a session, it can assess increased risk levels, driving accurate ATO threat detection
Product Integration	Excellent	Bureau offers a no-code platform that simplifies the integration process, enabling customers of all sizes to implement the solution without requiring significant engineering expertise. This approach allows for a quicker and easier start to using the product.
Buyer Satisfaction	Strong	By leveraging behavioral biometrics, behavioral analytics, and other key capabilities, Bureau can address a wide range of use cases. As customers increasingly seek comprehensive platform solutions, Bureau is well-positioned to continue satisfying clients with its versatile and robust offerings.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Bureau Device Intelligence


Bureau's Device Intelligence solution combines advanced algorithms, machine learning, and behavioral biometrics to provide comprehensive fraud detection and prevention capabilities. Bureau delivers a comprehensive identity and access fraud mitigation solution capable of addressing a diverse array of ATO threats.

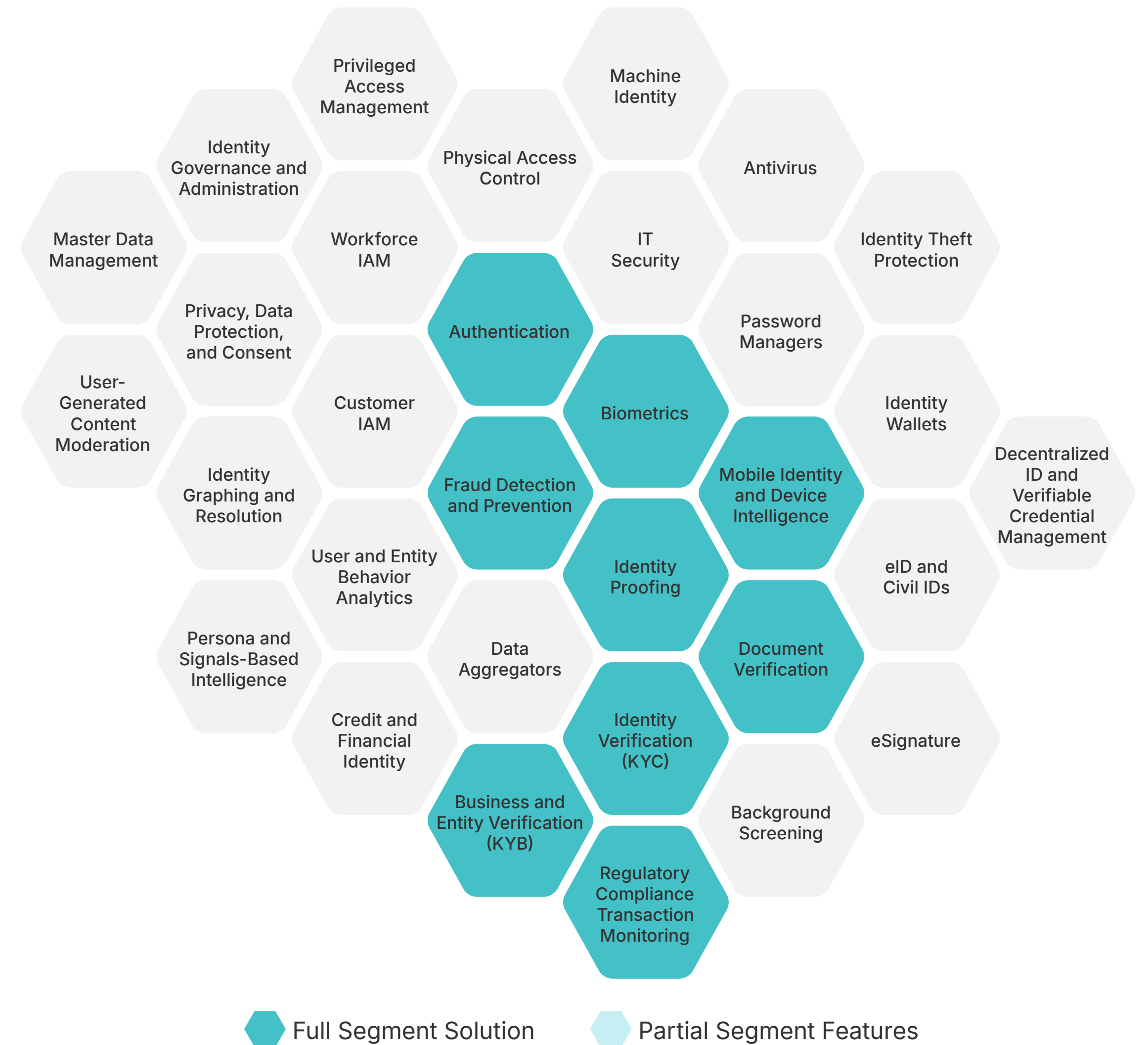
The platform analyzes over 200 device attributes, including device type, geolocation, IP and network information, device motion signals, and user-device interactions, to create a unique device fingerprint and risk score for each user. This extensive analysis helps identify and mitigate various types of fraud, such as account takeovers, promo abuse, and device hijacking, without compromising user experience. Bureau's solution is designed to be entirely passive, ensuring that legitimate users can seamlessly access services while preventing fraudsters from slipping through. The platform's capabilities include detecting emulators, active remote software apps, rooting, proxy usage, and application anomalies, providing a robust defense against sophisticated cyber threats.

Integrated with Bureau's broader platform and workflows, the Device Intelligence solution can be combined with identity verification (IDV) and alternative data sources to enhance overall security and fraud prevention efforts.

Caf

Caf is a provider of comprehensive identity verification, proofing, fraud detection, and authentication solutions in Brazil. The company serves customers in financial services, fintech, e-commerce, technology platforms, and sports betting. Caf's Know Your Everything (KYE) platform combines advanced computer vision ML models, an AI-powered decision engine, and identity orchestration with a vast repository of biometrics and identity databases.

Company Information ¹	
Headquarters	Sao Paulo, Brazil
No. of Employees	275 as of May 2024
Last Raised	\$15M, Angel in July 2022
Primary Segment	Identity Proofing, Identity Verification (KYC), Document Verification, Business and Entity Verification (KYB), Mobile Identity and Device Intelligence
Vertical Focus	Financial Services, Fintech, Gambling, Marketplaces
Geographic Focus	North America, Europe, Latin America
Notable Customers	



(1) Link

Caf's Strategy

Strategy	Strong	Caf offers a strong integrated identity platform that provides capabilities for identity verification, authentication, and fraud detection. Its solutions deliver a customizable and cost-effective experience for end-users.
Behavioral Capabilities	Excellent	Caf offers recurring user analysis, which can help detect account takeovers and other fraudulent activities that might result from successful phishing attacks. Caf specializes in facial identification and recognition technology, which can help prevent identity fraud and impersonation attempts often used in social engineering attacks.
Passwordless Authentication	Strong	Their solutions leverage advanced facial recognition and AI-powered verification to authenticate users without traditional passwords. Caf ensures a seamless and secure authentication process by combining multiple technologies such as biometrics, document verification, and data point validation. This approach not only reduces the risk of phishing and social engineering attacks but also simplifies the sign-in experience for users.
Cost	Excellent	Caf platform lives up to its 'Know Your Everything' moniker by bringing together an array of modules for identity verification, document verification, fraud prevention, and know your business, which can be leveraged to support a reduction of overlapping vendors in customers' tech stack. 46% of surveyed customers indicated high satisfaction with Caf's solutions' cost.
User Experience	Strong	Caf combines multiple technologies for identity validation, including biometrics, document verification, and data point validation, enhancing security without compromising user convenience.

Analyst Notes on Strategy

Caf's authentication capabilities are robust and multifaceted, designed to enhance security and streamline the user experience. Caf offers passwordless authentication via biometric methods, such as fingerprint and facial recognition, along with hardware tokens and mobile device-based authentication. This approach eliminates vulnerabilities associated with passwords, such as reuse, brute-force attacks, and phishing, and provides a more user-friendly login process.

Moreover, their full customer lifecycle platform leverages data insights from onboarding to ongoing monitoring to help detect anomalies including credential stuffing, phishing, and SIM Swap attacks. This involves analyzing traffic patterns, IP addresses, and other contextual data points. Additionally, Caf uses behavioral biometrics to create unique digital profiles for users based on their inherent behavioral traits, such as how users type, move their mouse, and interact with their devices. Caf uses adaptive authentication to enable step-up authentication measures only when behaviors indicative of fraud merit further intervention in user journeys.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Caf's Market Presence

Market Presence	Excellent	Caf is one of the largest regional identity vendors in Brazil, and recently rolled up their solution into a single platform offering that supports several use cases including ATO prevention.
Brand Awareness	Excellent	Caf has recently launched a Know Your Everything Platform solution that integrates all their solutions into a single platform offering. Nonetheless, roughly 55% of surveyed financial institutions were familiar with their brand and solutions for ATO prevention.
Market Leadership	Strong	Despite having a leading presence in the Brazilian market, of practitioners who were familiar with the Caf brand and its solutions, 21% recognized it as a market leader. This indicates their ability to demonstrate strong market leadership in Latin America, and highlights Caf's opportunity to scale into a global market leader.
Market Penetration	Excellent	The vendor is well adopted among financial institutions in Brazil, and is one the largest and most recognized identity vendors in the region. By rolling up their solutions into a single platform, they can expect to capture new business from financial institutions looking to consolidate vendors in their tech stack.
Company Size	Excellent	Caf has over 200 employees across Brazil, the United States, and the United Kingdom. This competition positions them to continue to innovate and capture new business as one of the largest regional identity vendors in Brazil.
Employee Growth	Exceptional	Caf has had strong employee growth year-on-year, which comes at the tailwind of strong revenue growth over the last few years – Caf reported a 250% increase in revenue in 2022.

Analyst Notes on Market Presence

Caf, a Brazil-headquartered firm, has rapidly established a significant market presence since its founding in 2019. The company, formerly known as Combate à Fraude, is the only company in Brazil to have earned a security certificate for its proof-of-life technology from iBeta Quality Assurance, demonstrating its commitment to high-security standards. Caf's innovative identity verification and digital onboarding solutions have been adopted across various sectors.

In 2022, Caf experienced transformative growth, achieving a 250% increase in revenue despite global economic challenges. This impressive performance was driven by the company's aggressive expansion into international markets, including the USA, UK, and Canada, and opening new offices in major technology hubs. Caf's strategic focus on product innovation and expanding its customer base has positioned it as a key player in the global digital identity market. Looking ahead, Caf plans to expand its presence in Brazil and boost growth in major international markets, focusing on the sports betting industry, poised for significant growth due to favorable regulatory developments. The company's commitment to enhancing digital identity security and its strategic global expansion efforts underscore its strong market presence and potential for continued growth in the rapidly evolving digital identity landscape.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Caf Know Your Everything Platform

Caf's Know Your Everything (KYE) Platform is a unified solution for customer onboarding, document verification, user onboarding, KYC, KYB, and employee onboarding. The KYE platform integrates computer vision ML models, an AI-powered decision engine, and identity orchestration with a comprehensive collection of biometrics and identity databases. It also includes a no-code workflow designer, enabling automated processes for customer onboarding, KYC, fraud prevention, authentication, document verification, and background checks.

ATO Prevention Product Capability Coverage¹

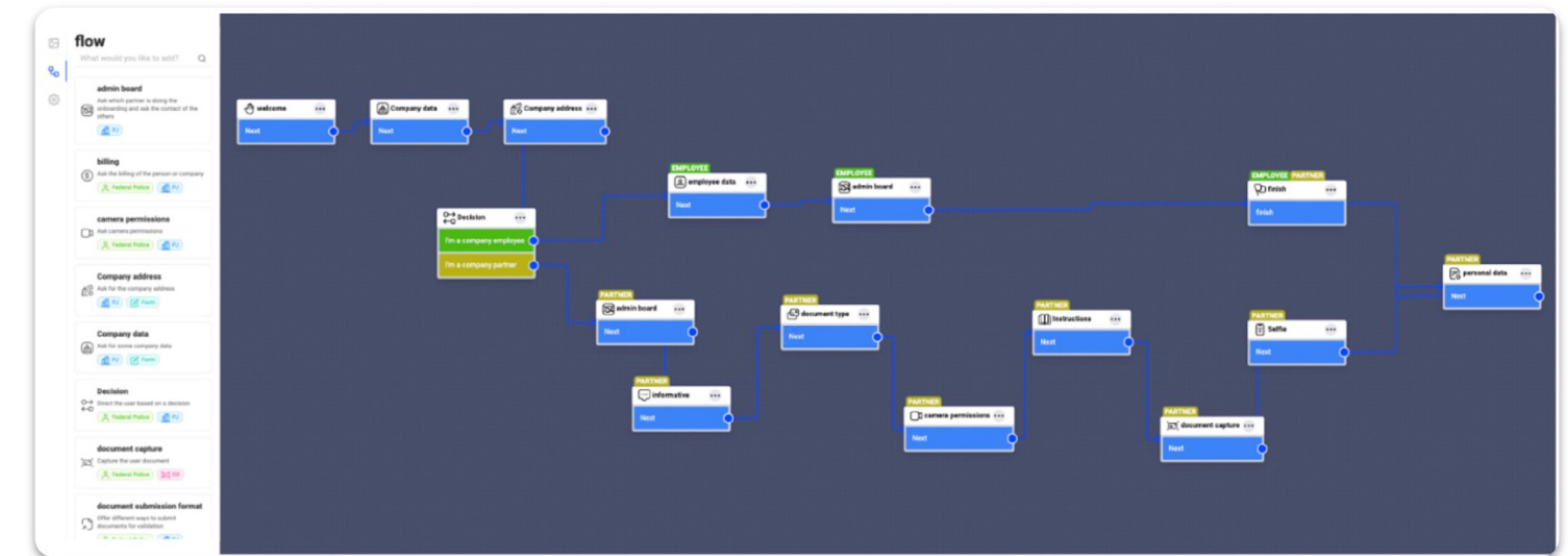
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from the company.

Product Visuals²



Caf Know Your Everything Platform

Product	Excellent	Caf offers a wide range of highly demanded capabilities on its KYE Platform, covering a broad spectrum of use cases.
Product Capability	Excellent	With biometric and continuous authentication capabilities, along with device risk scoring, location intelligence, and proxy/VPN detection, Caf effectively integrates both authentication and fraud prevention features into a comprehensive suite. This combination ensures robust security and accurate threat detection.
Scalability	Strong	Caf's all-in-one platform is suitable for businesses looking to deploy an end-to-end solution out of the gate. Buyers can scale up or down their adoption of Caf's modules per their preference.
Customization	Strong	Caf allows customers to define rules that best suit their organization without locking them into predefined application scenarios for ATO prevention. The company offers a high level of customization regarding rules creation, ensuring tailored and flexible solutions.
Accuracy	Strong	The KYE platform leverages a wide range of signals from identity, fraud, and authentication perspectives. This enables the company to provide a comprehensive risk profile of customers and prevent financial losses.
Product Integration	Strong	While Caf offers no-code/low-code integration, customers access their ATO services through the company's initiation portal to launch their SDK. From there, customers can choose additional API integrations based on their specific needs, allowing for a tailored and scalable solution.
Buyer Satisfaction	Strong	The KYE platform effectively services a wide range of use cases, including customer onboarding, document verification, KYB, and KYC. This comprehensive use case coverage is particularly appealing to customers seeking all-encompassing solutions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.




Analyst Notes on Caf Know Your Everything Platform

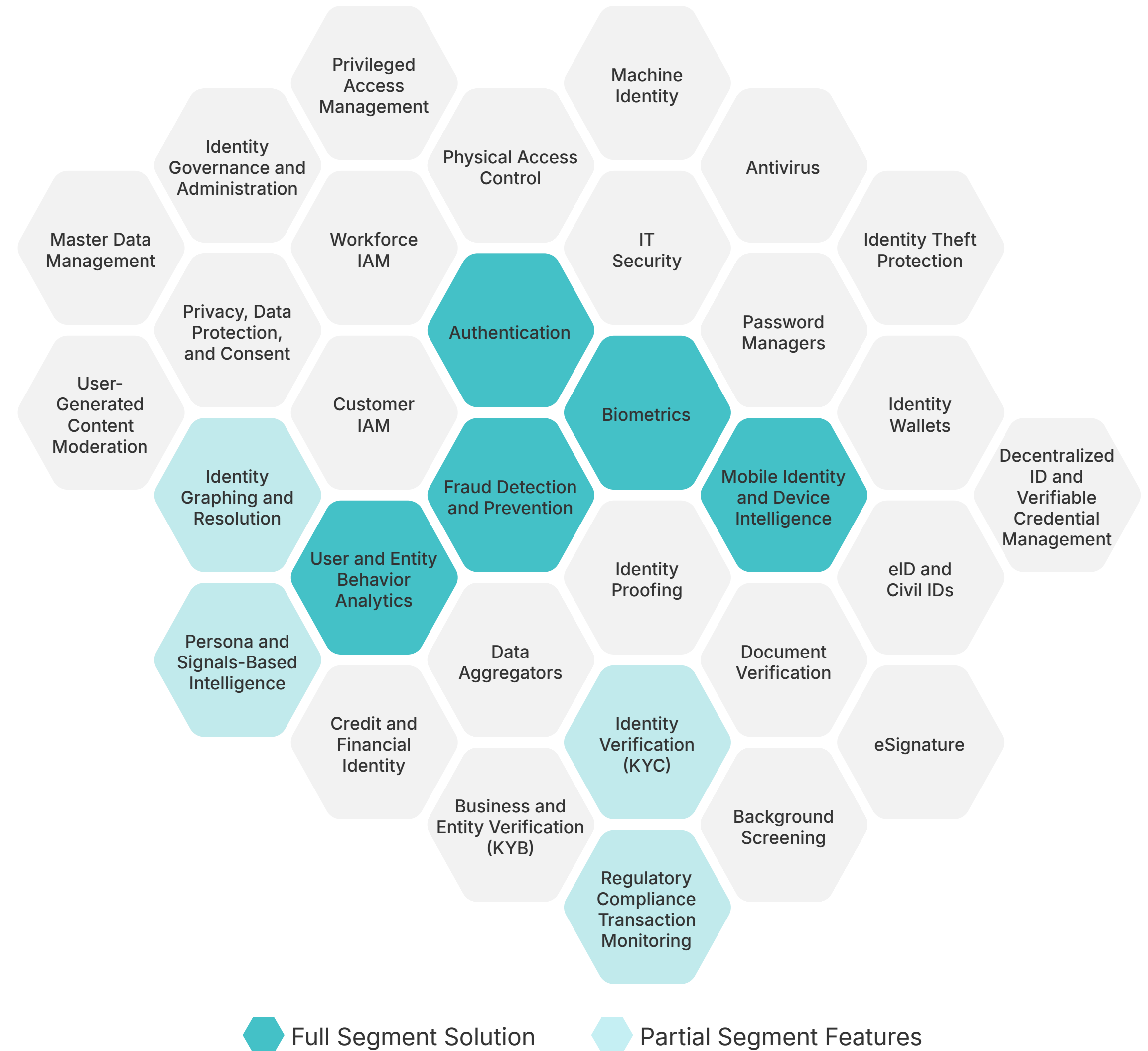
Caf's Know Your Everything (KYE) platform is an advanced, comprehensive solution designed to enhance digital identity verification and onboarding processes for businesses worldwide. Launched in early 2023, the KYE platform aims to provide a seamless and secure user experience while protecting against sophisticated fraud. It integrates various technologies, including advanced computer vision, machine learning models, and an AI-powered decision engine, to deliver robust identity verification, Know Your Customer (KYC), Know Your Business (KYB), and fraud prevention solutions.

The KYE platform consolidates Caf's existing solutions, including user onboarding, document verification, identity validation, and account takeover prevention. It also enhances biometrics detection and ensures the liveness of every user. The platform includes a drag-and-drop, no-code workflow builder and a flexible orchestration engine, allowing businesses to customize their verification processes easily. Rules and workflows alike can be customized to the requirements of the business. These features simplify the integration and management of identity verification workflows, making the Caf solution accessible for non-technical administrators.

Callsign

Callsign provides an authentication platform for secure and adaptive authentication services. Their products analyze events, threats, and user behavior with multi-factor authentication (MFA) to ensure secure access while maintaining a seamless user experience. Callsign's solutions address account login, online payments, account creation, and registration, effectively preventing account takeover, social engineering, malware, and synthetic identity fraud.

Company Information ¹	
Headquarters	London, England
No. of Employees	229 as of May 2024
Last Raised	Venture – Series Unknown in November 2020 (Amount Undisclosed)
Primary Segment	Authentication, Mobile Identity and Device Intelligence, Fraud Detection and Prevention
Vertical Focus	Financial Services, Telecommunications, Retail, Government
Geographic Focus	Europe, Asia-Pacific, Middle East
Notable Customers	  



(1) Link

Callsign's Strategy

Strategy	Excellent	With a robust suite of behavioral capabilities, Callsign provides strong security and a user experience that customers highly value.
Behavioral Capabilities	Exceptional	Callsign boasts one of the most robust behavioral suites among the vendors we analyzed. By offering behavioral biometrics, behavioral analytics, and bot detection, the company effectively detects various ATO threats, including social engineering and phishing.
Passwordless Authentication	Strong	Callsign relies on behavioral signals to detect fraud and prevent ATO, rather than focusing on passwordless authentication mechanisms like passkeys, QR code authentication, or WebAuthn.
Cost	Excellent	Banking buyers reported being satisfied with Callsign's cost-effectiveness. With one of the most comprehensive product capability suites among the vendors we analyzed, buyers can achieve robust ATO protection through a single solution, potentially allowing them to eliminate other vendors from their tech stack.
User Experience	Excellent	By leveraging robust behavioral signals, device-level data, and location data to detect fraud, along with offering silent authentication, Callsign provides ATO protection in the background. This approach results in lower false positives and minimal user friction.

Analyst Notes on Strategy

Callsign's Intelligence Engine is built on advanced artificial intelligence (AI) and machine learning techniques that analyze user patterns, behaviors, and interactions in real time. It incorporates behavioral analytics capabilities to understand user behaviors, device interactions, and transaction patterns, enabling Callsign to deliver seamless and secure authentication experiences. The platform also leverages behavioral biometrics, which involves analyzing unique user characteristics such as typing patterns, swipe gestures, device movements, and other behavioral traits. By combining behavioral analytics and behavioral biometrics, Callsign can create comprehensive user profiles, detect anomalies, and adapt authentication requirements based on the assessed risk level.

Moreover, CallSign offers robust passwordless authentication capabilities, including fingerprint, facial, and voice recognition, allowing users to leverage their unique biometric traits for secure and convenient authentication. Callsign also offers a range of mobile authenticators that facilitate passwordless authentication on mobile devices. Users can authenticate by performing simple swipe gestures or tracing specific patterns on their device's screen, leveraging Callsign's behavioral biometrics capabilities. Additionally, the platform supports device binding, which enables passwordless authentication based on the unique fingerprint of the user's device.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Callsign's Market Presence

Market Presence	Excellent	Callsign offers robust authentication capabilities through their platform solution – financial institutions highly regard their brand.
Brand Awareness	Excellent	Callsign offers a robust authentication platform that is well recognized amongst financial institutions as being able to solve for ATO prevention – 71% of surveyed solution seekers at financial institutions were familiar with the Callsign brand and their solutions.
Market Leadership	Excellent	Amongst those that were familiar with the Callsign brand and their solution for ATO prevention, 28% recognized them as market leaders for ATO prevention – this indicates their market leadership in fraud by developing an effective authentication solution.
Market Penetration	Excellent	Callsign has competitive market penetration across financial institutions through its robust authentication platform and attractive orchestration capabilities – their solutions are well-regarded among financial institution practitioners.
Company Size	Excellent	With over 200 employees, Callsign is well positioned for future growth. Moreover, with over 30% of their employee headcount in engineering roles, Callsign can continuously innovate and develop additional capabilities as demands of buyers continue to shift.
Employee Growth	Strong	Despite negative employee headcount growth, Callsign's brand awareness and market leadership will enable them to capture new business in the market.

Analyst Notes on Market Presence

Callsign has established itself as a prominent player in the intelligent authentication and fraud detection market, serving organizations across various industries, including banking, fintech, retail, and healthcare. Founded in 2011 and headquartered in London, United Kingdom, the company has recently raised \$38 million in funding.

While Callsign primarily focuses on authentication, it also provides comprehensive fraud signals to complement their product stack. This approach has made them popular, particularly among banks seeking full-stack solutions. The company has achieved high brand awareness and market leadership scores, indicating a strong presence among banking buyers looking for full-stack ATO solutions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Callsign Intelligence Engine

The Callsign Intelligence Engine passively analyzes data points from devices, locations, behaviors, and third-party systems to authenticate users. It utilizes artificial intelligence and machine learning to detect genuine users while identifying potential threats from malware, bots, and scams. This platform aims to provide secure, frictionless access for legitimate users and ensure compliance with security regulations.

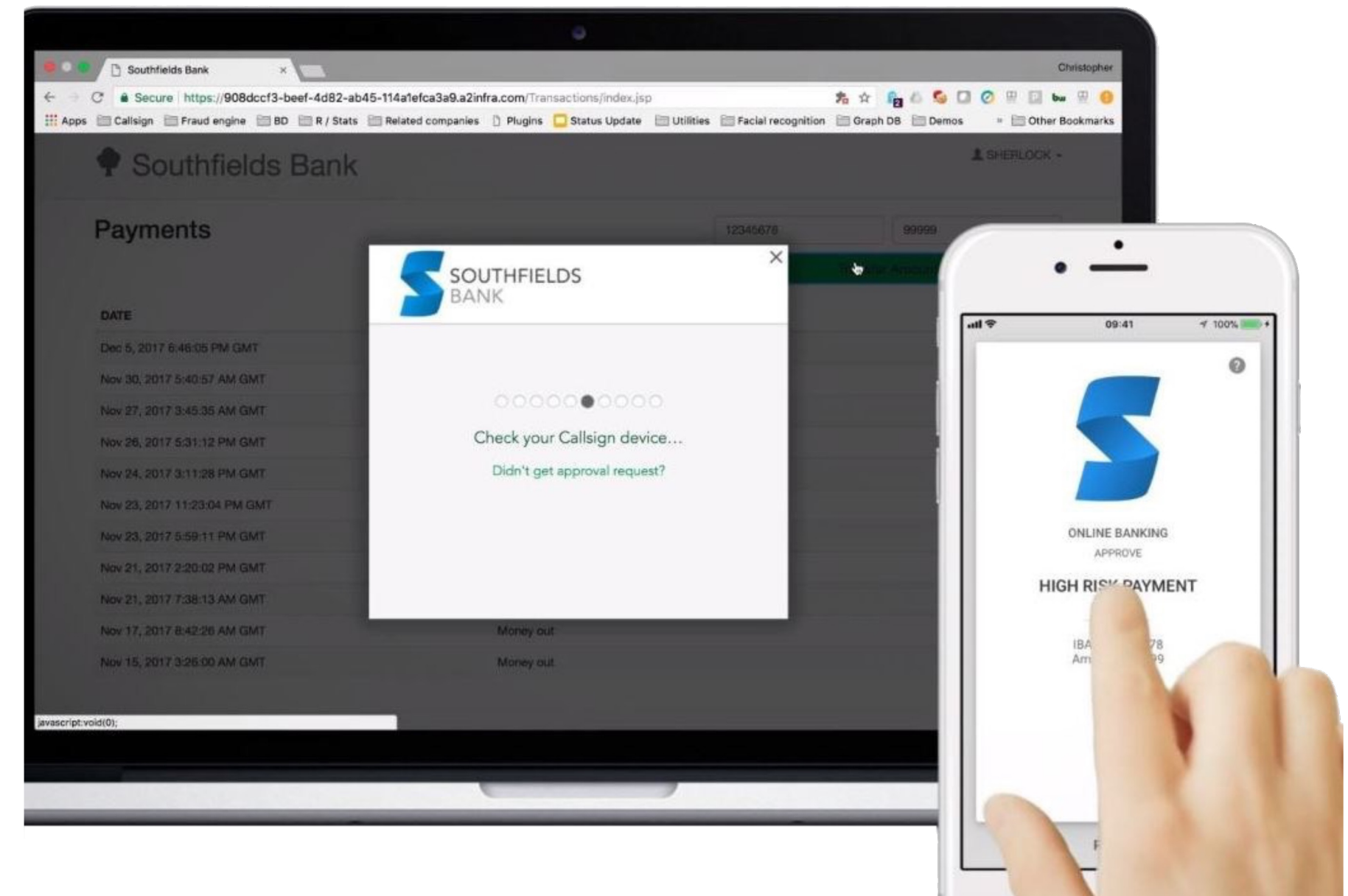
ATO Prevention Product Capability Coverage¹

H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from public sources (link: <https://appsource.microsoft.com/en-us/product/web-apps/callsign.callsign?tab=overview>).

Product Visuals²



Callsign Intelligence Engine

Product	Exceptional	Callsign has an exceptionally robust product capability suite, enabling the company to provide highly accurate solutions for preventing ATO.
Product Capability	Exceptional	Callsign has the most extensive product capability set of all the vendors we analyzed for ATO prevention in banking. The company offers a complete authentication stack combined with comprehensive fraud detection signals, creating a robust ATO prevention defense.
Scalability	Strong	Callsign serves notable clients such as Capital One and HSBC. Though, Callsign buyers noted room for improvement in their sentiments around Callsign's scalability when compared to other leading vendors. Still, Callsign's client base demonstrates their ability to handle clients with large user bases and significant transaction volumes.
Customization	Strong	The company's orchestration layer allows for policy management, including testing and simulation capabilities. This enables customers to design tailored user flows and set risk levels specific to their bank's needs.
Accuracy	Excellent	Callsign uses behavioral biometrics to monitor users across sessions, ensuring their identities remain consistent. Additionally, they employ other continuous authentication capabilities to provide extra security layers.
Product Integration	Excellent	Callsign's orchestration layer offers no-code integration designed to seamlessly integrate with other systems and vendors.
Buyer Satisfaction	Excellent	Callsign aims to provide passive authentication that maintains a strong customer experience without compromising accurate ATO threat detection. This approach has resulted in very high satisfaction ratings from banking customers.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.




Analyst Notes on Callsign Intelligence Engine

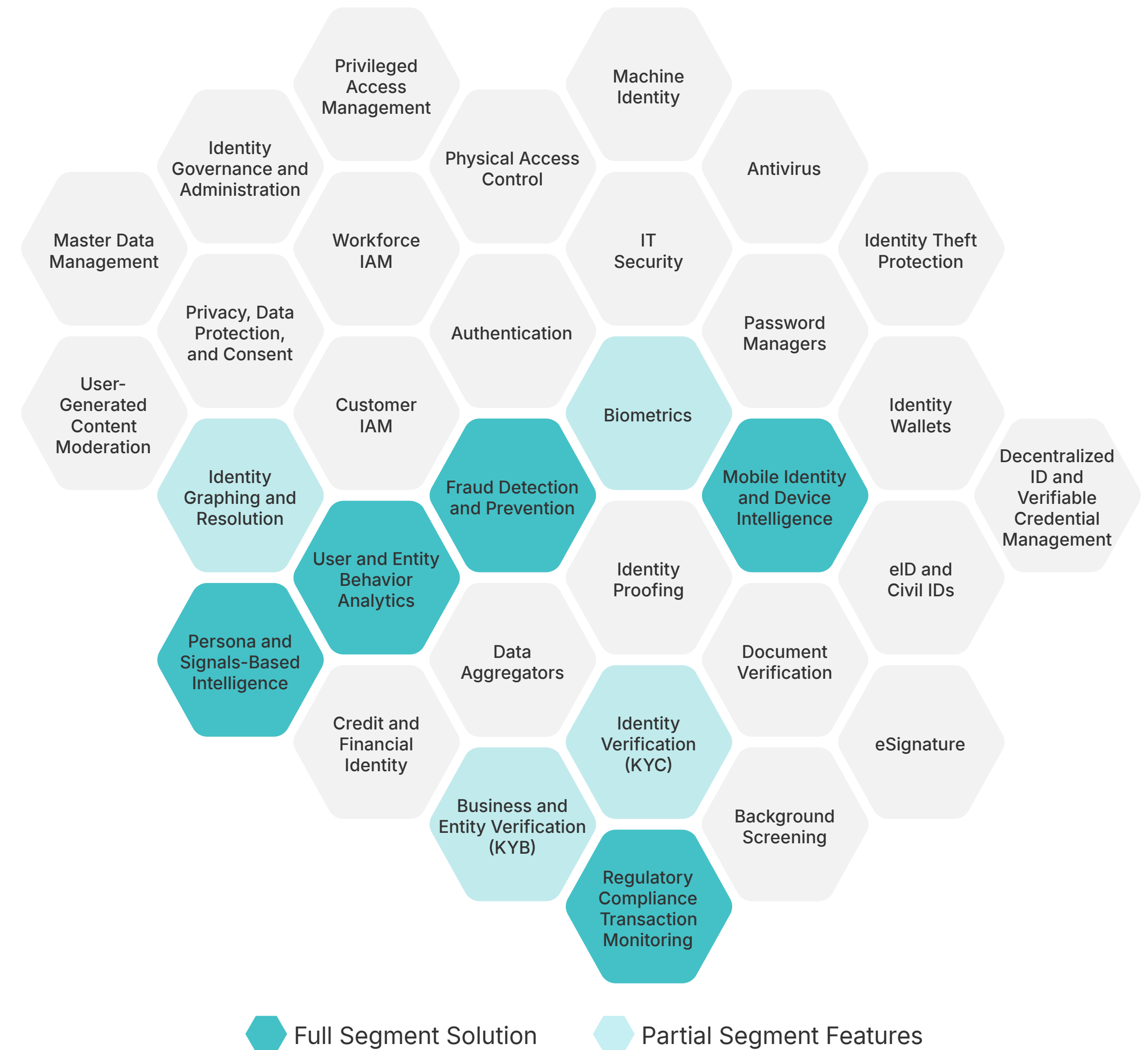
Callsign offers a comprehensive platform designed to deliver secure authentication and fraud prevention experiences through the power of artificial intelligence (AI) and behavioral analytics. At the core of Callsign's platform is the Intelligence Engine, which leverages advanced AI and machine learning techniques to analyze and understand user patterns, behaviors, and interactions in real time.

The Intelligence Engine intelligently orchestrates authentication journeys by analyzing over 1,000 data points and applying AI algorithms to dynamically adjust authentication requirements based on the assessed risk level and transaction context. This adaptive approach ensures that the most appropriate authentication action is requested for every situation, striking the perfect balance between robust security and a frictionless user experience. The platform's Orchestration Layer seamlessly integrates with existing systems and technologies, allowing organizations to manage their users' end-to-end journey in one place via a user-friendly drag-and-drop GUI. This layer enables organizations to manage and deploy new processes and controls quickly, providing control over the authentication journey, zero-risk testing capabilities, and the ability to view, review, and audit authentication processes.

DataVisor

DataVisor provides fraud and risk management solutions that detect and prevent fraudulent activities across various industries. Their platform uses offers unsupervised machine learning algorithms within a proprietary analytics engine to identify patterns and anomalies indicative of fraud. DataVisor’s solutions include account protection, transaction monitoring, and anti-money laundering tools through a single platform. DataVisor powers anti-financial crime functions looking to center machine learning and data science approaches within their technology stack.

Company Information ¹	
Headquarters	Mountain View, California
No. of Employees	141 as of May 2024
Last Raised	Venture – Series Unknown (Amount Undisclosed) in May 2023
Primary Segment	Fraud Detection and Prevention
Vertical Focus	Financial Services, Fintech
Geographic Focus	North America, Europe, Middle East, Asia-Pacific
Notable Customers	  



(1) Link

DataVisor's Strategy

Strategy	Excellent	DataVisor provides extensive behavioral capabilities while offering solutions at a highly competitive price.
Behavioral Capabilities	Exceptional	DataVisor boasts a robust suite of behavioral capabilities that effectively defend against ATO. The company provides advanced solutions, including behavioral biometrics, behavioral analytics, and bot detection, all integrated into its comprehensive Fraud and Risk Platform. These sophisticated tools enable DataVisor to offer thorough and reliable protection against a wide range of fraud threats.
Passwordless Authentication	Strong	DataVisor does not prioritize passwordless authentication methods. Instead, it analyzes various behavioral, network, and device signals to detect risks and prevent various ATO threat vectors.
Cost	Exceptional	DataVisor is considered by buyers to be one of the most cost-effective solutions among all the ATO vendors Liminal profiled. They offers a robust suite of capabilities that provide comprehensive coverage across the customer lifecycle, from account opening to login to transactions. This allows DataVisor to deliver substantial use case coverage through a single platform solution.
User Experience	Strong	DataVisor utilizes passive signals to differentiate bad users from legitimate ones, effectively protecting against fraud. However, in terms of user experience, it did not score as highly as some other vendors. This indicates that while DataVisor excels in fraud detection and prevention, there may be room for improvement in creating a more seamless and user-friendly interface for its customers.

Analyst Notes on Strategy

DataVisor's Fraud Platform leverages advanced behavioral analytics and behavioral biometrics capabilities. The platform captures various behavioral intelligence signals, such as copy-and-paste actions, typing speed, and more, providing a comprehensive understanding of user behavior and potential fraud risks. This behavioral data is analyzed using DataVisor's patented machine-learning technology to identify anomalies and suspicious patterns indicative of fraudulent activities.

Fraud Platform also leverages native device intelligence to identify emulators, botnets, and rooted and hooked devices, effectively detecting and mitigating bot-driven fraud attempts. DataVisor's solution can accurately distinguish between legitimate user interactions and automated bot activities by combining behavioral analytics, behavioral biometrics, and device intelligence. However, their solution notably lacks passwordless authentication capabilities. The solution leverages a subscription-based pricing model.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

DataVisor's Market Presence

Market Presence	Excellent	DataVisor offers a well-recognized AI-powered fraud and compliance platform solution that has established itself as a trusted partner to several financial institutions.
Brand Awareness	Excellent	Roughly 61% of surveyed financial institution practitioners recognized DataVisor's fraud and risk platform. This recognition underscores its growing influence and effectiveness within the industry.
Market Leadership	Excellent	Of those who were familiar with the DataVisor brand and their platform solution, roughly 29% suggested they were market leaders for solving ATO prevention, highlighting competitive recognition in financial services.
Market Penetration	Excellent	DataVisor has achieved significant market penetration in the financial services sector, supporting several major financial institutions, including banks, credit unions, and fintech companies, through their fraud and compliance solutions.
Company Size	Excellent	DataVisor, headquartered in Mountain View, California, employs approximately 140 people in the United States. The company has raised a total of \$95 million in funding, which it can use to make strategic hires and engage in product development.
Employee Growth	Strong	They have had moderate employee growth, reflecting the company's ongoing expansion and commitment to enhancing its AI-powered fraud detection and risk management solutions.

Analyst Notes on Market Presence

DataVisor has established itself as a prominent fraud and risk management player, offering a comprehensive AI-powered platform to protect organizations from online fraud, digital risks, and sophisticated attacks. DataVisor's adoption by many Fortune 500 companies across the globe is indicative of a significant market presence. DataVisor's market reach extends beyond the financial sector, with large consumer-facing enterprises leveraging their solutions across multiple industries. Diversifying its customer base underscores the platform's versatility and applicability in addressing fraud and risk management challenges across various domains.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

DataVisor Fraud & Risk Platform

The DataVisor Fraud & Risk Platform leverages AI and machine learning to detect and prevent real-time fraudulent activities. The platform offers capabilities such as unsupervised machine learning, automated decisioning, and an AI Copilot to enhance detection accuracy and operational efficiency. The platform protects against a wide range of threats, including ATO, check fraud, wire fraud, card fraud, and money laundering.

ATO Prevention Product Capability Coverage¹

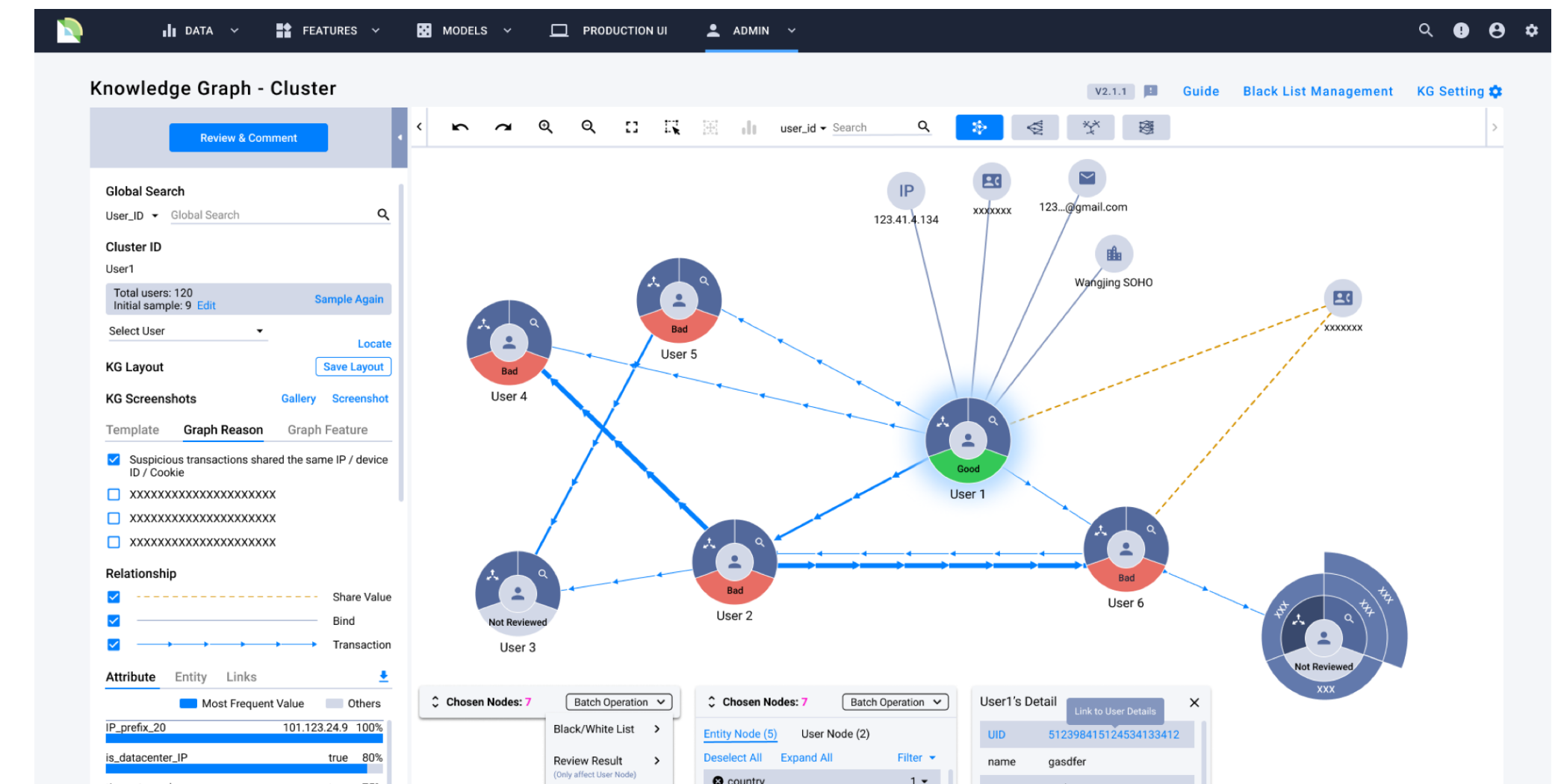
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from company website (link: <https://www.datavisor.com/fraud-platform/>)

Product Visuals²



DataVisor Fraud & Risk Platform

Product	Excellent	DataVisor offers a robust capability set, leveraging unsupervised learning machines to accurately detect fraud.
Product Capability	Excellent	DataVisor offers a robust set of fraud prevention capabilities on its Fraud & Risk platform, including social engineering and scam detection, location intelligence, and behavioral biometrics. These features work together to effectively prevent various ATO threats.
Scalability	Strong	While DataVisor did not rank as highly in terms of scalability according to buyers compared to other top solutions, the company has experience working with large customers such as SoFi.
Customization	Strong	The Fraud and Risk platform offers no-code rule building and instant rule backtesting, along with automated rule tuning suggestions through its AI Copilot. This enables banking customers to easily customize solutions to their desired preferences.
Accuracy	Excellent	The DataVisor Fraud and Risk platform uses unsupervised machine learning to uncover deep contextual insights and detect anomalous behavior by comparing it to normal user activity. This approach effectively captures ATO threats.
Product Integration	Excellent	With its unsupervised learning capabilities, DataVisor aims to significantly reduce the time required to implement a new solution. The company highlights this as a key differentiator, as rapidly evolving fraud patterns can render models outdated during lengthy implementation processes.
Buyer Satisfaction	Excellent	By offering a platform with a comprehensive range of solutions covering account opening, login, and transactions, paired with a powerful unsupervised learning model, DataVisor is able to deliver efficient solutions that satisfy customers.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on DataVisor Fraud & Risk Platform

DataVisor offers a comprehensive AI-powered fraud detection and risk management platform to protect organizations from online fraud, digital risks, and sophisticated attacks. At the core of DataVisor's Fraud Platform is its ability to detect and respond to fast-evolving fraud attacks in real-time. It leverages unsupervised machine learning models to quickly identify emerging fraud patterns without relying on historical data or labels. This approach enables the platform to detect new and unknown fraud types, ensuring organizations stay ahead of evolving threats.




The Fraud Platform integrates with existing systems and supports real-time and batch processing, allowing for flexible integration and deployment. It provides accurate detection results, reducing financial losses and manual review costs. Additionally, the platform offers powerful case management capabilities, including contextual linkage visualization, group investigations, and bulk actioning, enhancing review efficiency and enabling accelerated investigations.

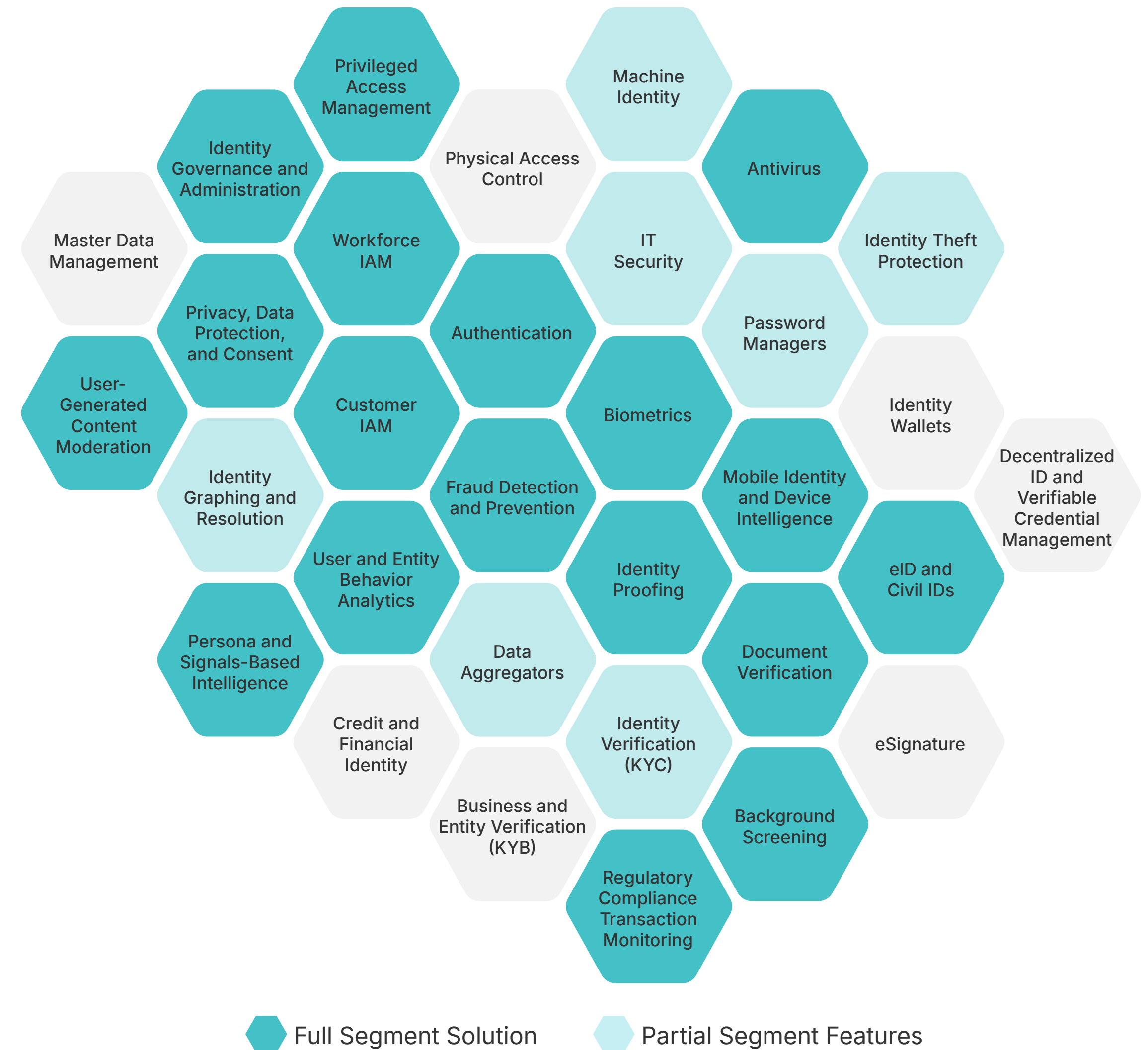
DataVisor's platform incorporates advanced device intelligence capabilities, enabling the identification of sophisticated attack techniques such as emulators, botnets, and rooted and hooked devices. It captures various behavioral intelligence signals, including copy-and-paste actions, typing speed, and more, providing a comprehensive understanding of user behavior and potential fraud risks.

The platform's decision engine tailors fraud management strategies by applying diverse fraud strategies tailored to specific customer segments and use cases. It offers purpose-built rulesets for effectively detecting different types of fraud and the ability to streamline fraud strategies through flexible decision workflows and automated rule refinement powered by generative AI.

Entersekt

Entersekt provides secure authentication and payment solutions, focusing on protecting digital transactions. It offers multi-factor authentication, biometric authentication, and mobile app security to safeguard user identities and financial activities. The platform integrates with existing systems to provide seamless, real-time security across various channels, including online banking, mobile apps, and E-commerce.

Company Information ¹	
Headquarters	Atlanta, Georgia
No. of Employees	358 as of May 2024
Last Raised	Venture – Series Unknown in June 2022 (Amount Undisclosed)
Primary Segment	Authentication, Fraud Detection and Prevention
Vertical Focus	Financial Services
Geographic Focus	North America, Europe, Middle East, Latin America
Notable Customers	  



(1) Link

Entersekt's Strategy

Strategy	Exceptional	Entersekt is primarily an authentication player through a robust platform solution – their solution can be leveraged by financial services to leverage risk-based authentication for ATO prevention.
Behavioral Capabilities	Exceptional	Entersekt offers protection against ATO attacks through its robust behavioral capabilities which include behavioral biometrics, behavioral analytics, as well as bot detection to inform its analysis and prevention of fraud.
Passwordless Authentication	Exceptional	The company's platform-agnostic approach supports various passwordless methods, including biometrics like fingerprints and facial scans, FIDO2-aligned authentication and passkeys, providing financial institutions with a highly secure alternative to traditional password-based systems.
Cost	Exceptional	Entersekt's pricing model is primarily subscription-based, tailored to the specific needs and deployment options of each client. The company offers customizable solutions across various channels and devices
User Experience	Exceptional	The company supports a strong user experience by offering a single-unified authentication platform that leverages its proprietary Context Aware™ Authentication to create personalized, frictionless experiences while maintaining high-security standards. This ultimately reduces frustration and cart abandonment for financial institutions and their customers.

Analyst Notes on Strategy

Entersekt's platform solution takes a comprehensive approach to authentication, leveraging various advanced capabilities to provide secure and frictionless experiences across multiple channels. The platform incorporates behavioral analytics to analyze user behaviors, device interactions, and transaction patterns, enabling the identification of anomalies that may indicate fraudulent activities. Additionally, Entersekt's solutions leverage behavioral biometrics, which involves analyzing unique user characteristics such as typing patterns, swipe gestures, and device movements to create comprehensive user profiles and detect deviations from expected behavior.

Entersekt's platform supports various passwordless authentication methods, including biometrics (facial recognition, fingerprint, and voice recognition), mobile authenticators, and industry standards like FIDO Authentication. These passwordless capabilities enable financial institutions to reduce reliance on traditional passwords, enhance security, and provide seamless user experiences across multiple channels, such as mobile banking apps, online banking, and digital payments.

Entersekt's focus on providing a secure SaaS platform suggests a subscription-based pricing model. Additionally, the emphasis on delivering measurable ROI, such as higher transaction success rates, reduced fraud losses, and cost savings through streamlined authentication processes, indicates that the commercial model may be tailored to individual customer needs and aligned with the platform's ability to drive tangible business benefits.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Entersekt's Market Presence

Market Presence	Excellent	Entersekt demonstrates a strong vertical focus in financial services with its authentication and payment security capabilities. They are well positioned to secure additional customers.
Brand Awareness	Excellent	As a prominent player in authentication, about 61% of surveyed financial institutions recognize Entersekt and their solutions for consumer account takeover prevention. Entersekt's solutions exclusively focus on supporting financial institutions mitigate fraud risk.
Market Leadership	Excellent	Entersekt's financial authentication solution was recognized by 24% of banking respondents as being market-leading. Entersekt should consider leveraging additional fraud detection and prevention capabilities to boost its market leadership score for account takeover prevention.
Market Penetration	Excellent	By pursuing channel partner strategies with Mastercard and Q2, Entersekt has facilitated user growth, with over 200 million users leveraging its software. The company also has a specific vertical focus in financial services and is, therefore, well-penetrated.
Company Size	Excellent	As of May 2024, Entersekt has 300+ employees in offices in 23 countries worldwide, with a concentration in South Africa, the US, central Europe, and northern Europe. Its size positions the company between emerging players and industry incumbents.
Employee Growth	Strong	Following the acquisition of Modirum in December 2023, Entersekt retained much of Modrium team and, subsequently, experienced a period of employee growth of around 14% YoY.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Market Presence

Entersekt has solidified its position as a global leader in transaction authentication solutions for financial fraud prevention. The company has experienced significant revenue and customer acquisition growth, fueled by its continued expansion in the United States market and strategic partnerships. Since receiving an investment from Accel-KKR, a prominent Silicon Valley-based private equity firm, in fiscal 2022, Entersekt has witnessed a rapid acceleration of its business outside of South Africa. In fiscal 2023 alone, the company's contracted annual recurring revenue increased by an impressive 191%, while its US-based customer base grew by nearly 220%.

Entersekt's market presence extends across the United States, Europe, and Africa, where it has established a strong track record of working with leading financial services institutions over the past decade. The company's patented security innovations, including its Context-Aware Authentication technology, have positioned Entersekt as a global industry leader in authentication.

In 2023, Entersekt acquired Modirum 3-D Secure Payment Solutions. Entersekt added Modirum's 3DS solutions to its Entersekt Secure Platform for transaction authentication, and the Modirum 3DS team joined the company. The acquisition accelerates product development, expands Entersekt's existing product offering, and bolsters the company's ability to scale and support global customers. Modirum also brings an impressive list of customers that increases Entersekt's market share of financial institutions offering 3-D Secure.

Entersekt Authentication

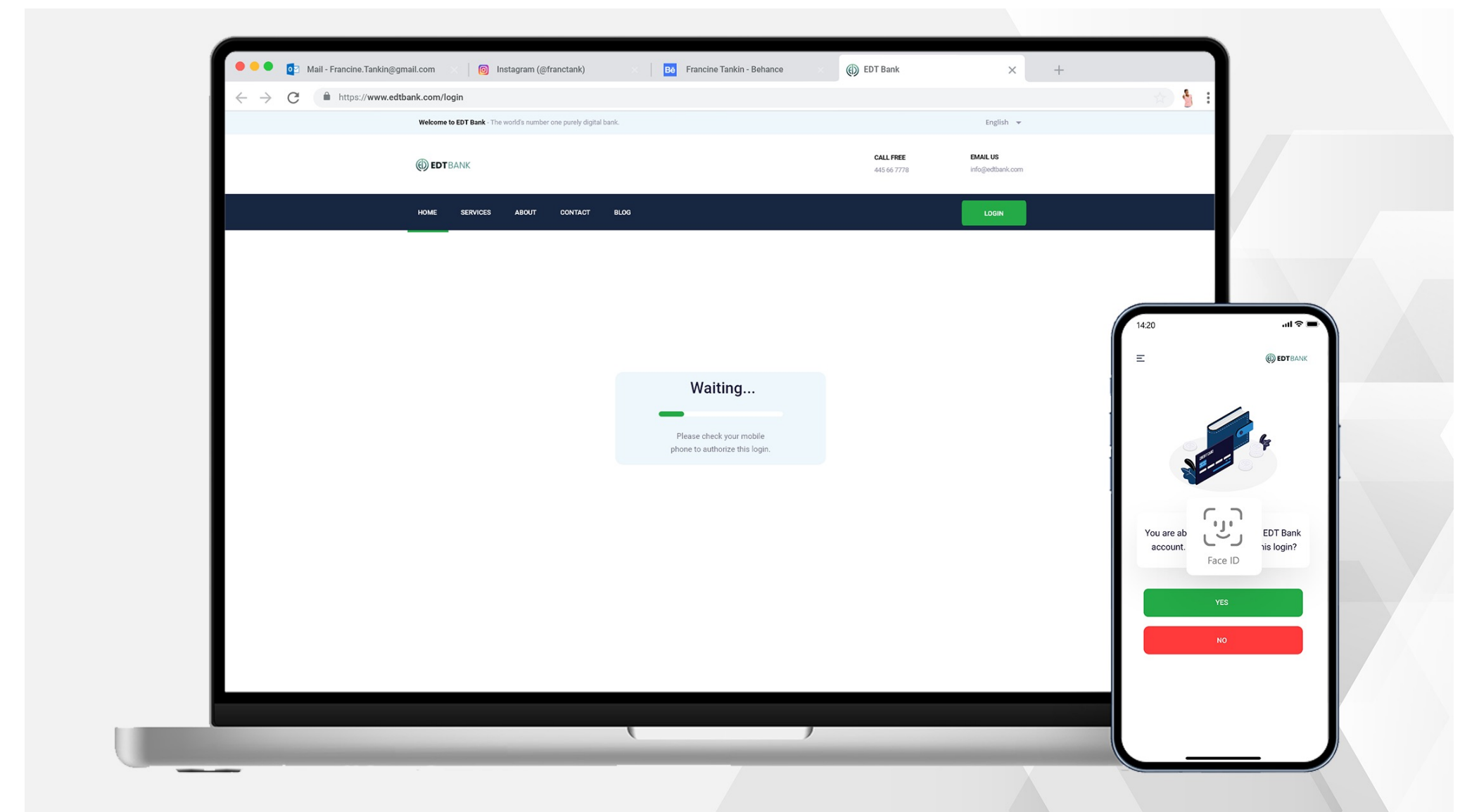
Entersekt Authentication offers a unified authentication platform for all company channels, such as mobile network operators (MNOs), browser, and mobile device. The product features multi-factor authentication (MFA), biometric authentication, and incorporates risk scoring models using multiple device signals, creating a comprehensive solution for protecting against account takeover (ATO).

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from the company.

Product Visuals²



Entersekt Banking Authentication

Product	Exceptional	Entersekt offers a complete set of tools for ATO prevention, featuring customizable options for both fraud detection and authentication.
Product Capability	Exceptional	Entersekt's product capability suite integrates both authentication and fraud signals, including biometric authentication and social engineering scam detection. This comprehensive approach makes it one of the most complete solutions among all benchmarked vendors.
Scalability	Excellent	Focusing exclusively on financial services, Entersekt has demonstrated its ability to support organizations as they scale, securing more than 2.5B transactions in the last year.
Customization	Excellent	Entersekt customers can create seamless experiences with step-up authentication that assesses risk levels based on user actions and contextual data, aligning with the preferences of financial institutions.
Accuracy	Strong	Entersekt's authentication accuracy rates are lower compared to other vendors we've benchmarked. However, its extensive product suite ensures robust coverage across the entire customer lifecycle, providing strong protection for various stages of user interaction.
Product Integration	Excellent	As an all-in-one platform, Entersekt allows customers to access all its services through a single integration, providing a wide range of highly demanded capabilities.
Buyer Satisfaction	Excellent	Entersekt employs a variety of signals and silent authenticators for comprehensive threat detection. By offering a wide range of MFA methods, the company meets buyers' specific needs, ensuring tailored security solutions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.




Analyst Notes on Entersekt Banking Authentication

Entersekt provides financial institutions with a secure, cross-channel authentication platform that addresses financial fraud prevention, account takeover schemes, and seamless user experiences. At its core is the patented Context Aware™ Authentication technology, which considers factors like transaction context, risk signals, and customer preferences to determine the best authentication method in real time. This technology enables a unified authentication strategy across online banking, in-branch services, call centers, digital payments, and open banking channels.

The platform includes mobile, MNO, and browser authentication to protect customers from digital fraud and identity theft. It also offers 3D Secure solutions for low-friction payment authentication and secure cashless payment experiences. Entersekt enhances fraud prevention, customer experiences, transaction success rates, and compliance with regulations by migrating its customers to a SaaS model and focusing on API-based capabilities. The company is developing deployment packages to streamline specific use cases such as login, account recovery, and identity verification.

Entrust

Entrust provides solutions that secure payments, digital identities, and sensitive data. Entrust’s digital security and credential issuance solutions address use cases including zero trust and digital onboarding. Their identity product suite features identity verification, identity and access management (IAM), and e-signature solutions. Additionally, Entrust offers data protection solutions such as hardware security modules, key management, and encryption.

Company Information ¹	
Headquarters	Shakopee, Minnesota
No. of Employees	3255 as of May 2024
Last Raised	\$270M, Debt Financing in March 2024
Primary Segment	Authentication, eIDs and Civil IDs, Customer IAM, eSignatures, Identity Governance and Administration, Biometrics, Regulatory Compliance Transaction Monitoring, Document Verification, Fraud Detection and Prevention, Identity Proofing
Vertical Focus	Financial Services, Transportation, Government, Energy
Geographic Focus	North America, Europe, Middle East, Asia-Pacific
Notable Customers	  



(1) Link

Entrust's Strategy

Strategy	Exceptional	Entrust offers one of the most robust passwordless authentication suites among ATO prevention vendors, effectively securing accounts in the process.
Behavioral Capabilities	Excellent	Entrust utilizes behavioral biometrics and behavioral analytics for ATO prevention, effectively analyzing mouse patterns, keystroke movements, and other signals to identify potential fraudsters.
Passwordless Authentication	Exceptional	Entrust offers both passkeys and QR code authentication to verify users without traditional passwords. This approach enables the company to provide highly secure authentication that is very effective at thwarting ATO.
Cost	Excellent	According to banking buyers, Entrust receives excellent cost-effectiveness scores compared to other ATO prevention solutions. According to public sources, Entrust's pricing sits between \$2 and \$3.50 per monthly user depending on plan selected. The company offers a comprehensive package at an attractive price point to buyers.
User Experience	Strong	While Entrust does offer behavioral signals that operate in the background, customer ratings were less favorable compared to other ATO vendors regarding user experience. This suggests that the current client base may find their passwordless authentication options less user-friendly.

Analyst Notes on Strategy

Entrust primarily focuses on multi-factor authentication (MFA) methods, such as one-time passwords, push notifications and hardware tokens. The solution complies with FIDO (Fast Identity Online) standards, enabling passwordless authentication using biometrics or possession-based factors like security keys. Entrust's Premium Workforce Bundle package offers easily deployed mobile digital identities, enabling passwordless access to resources through proximity-based login and cross-platform biometrics. Entrust IDaaS also supports virtual smart cards, which can be used for passwordless authentication and secure access to applications and resources.

Entrust IDaaS follows a subscription-based pricing model with different bundles available in cost and commercial models. Moreover, Entrust IDaaS integrates with various third-party applications and services using standards like SAML, OIDC, and Radius. This ensures that organizations can easily incorporate Entrust IDaaS into their existing IT ecosystems, which helps to support a strong customer experience.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Entrust's Market Presence

Market Presence	Excellent	Entrust is a large identity provider with a breadth of solutions spanning identity access management, authentication, and eSignatures – they are well positioned to grow in this market.
Brand Awareness	Exceptional	Entrust is primarily recognized as an identity and access management provider but offers a strong cloud-based identity solution with authentication capabilities to support strong brand awareness for ATO prevention – roughly 77% of financial institutions were familiar with their brand.
Market Leadership	Excellent	26% of surveyed financial institutions regard Entrust as offering market-leading solutions for ATO prevention. Despite being primarily known as an identity and access management vendor, their solutions are well-regarded in the market.
Market Penetration	Exceptional	Entrust has established a significant presence in the financial services sector by issuing over 4.7 billion financial and government credentials annually and protecting over 100 million identities.
Company Size	Exceptional	Entrust Corporation, headquartered in Shakopee, Minnesota, employs over 3000 people globally and operates across 29 locations in North America, South America, Europe, Middle East, and Asia-Pacific.
Employee Growth	Strong	Despite moderate employee growth over the last year, Entrust has recently secured debt financing and can use the injection of capital to continue to innovate new solutions and capture additional business in the market.

Analyst Notes on Market Presence

Entrust has established itself as a leading provider of trusted identity, payment, and data protection solutions, with a significant market presence in the global Transport Layer Security (TLS) certificate market. With over 10,000 enterprise customers using Entrust solutions, including renowned organizations like Visa, Mastercard, and VMware, the company has demonstrated its reliability and trustworthiness in providing secure digital infrastructure solutions. Entrust's extensive customer base spans various industries, including financial services, healthcare, retail, manufacturing, information technology, and the public sector, underscoring its broad market reach.

Earlier this year, Entrust acquired Onfido, a global identity verification player. Entrust will service various business requirements by leveraging Onfido's cutting-edge identity verification solutions across the Entrust portfolio, including its biometrics, AI/machine learning, and no-code orchestration capabilities. Capabilities include automated security defenses, with a layered, enhanced approach to fraud detection, using AI developed in-house to verify genuine identities.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Entrust Identity as a Service

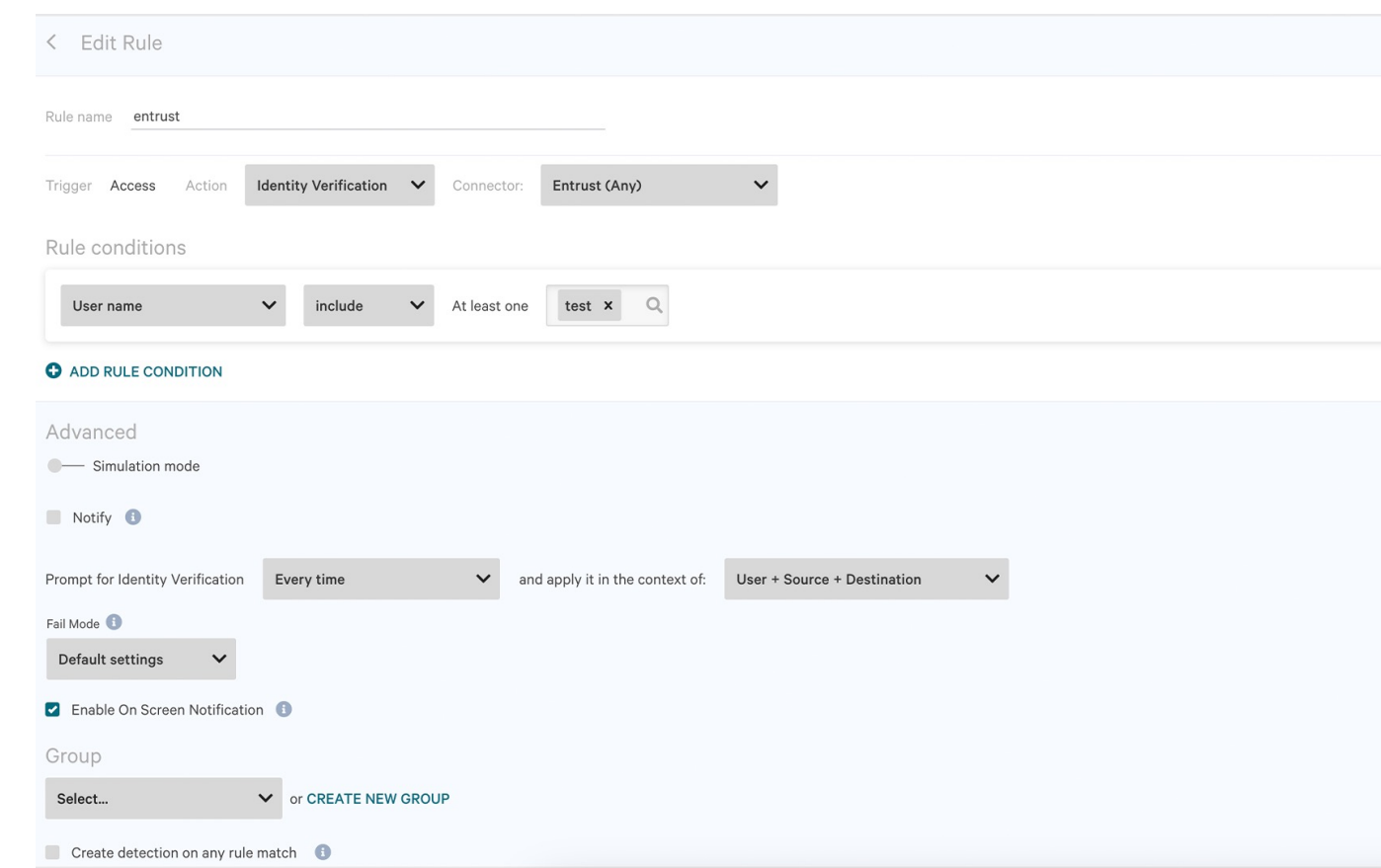
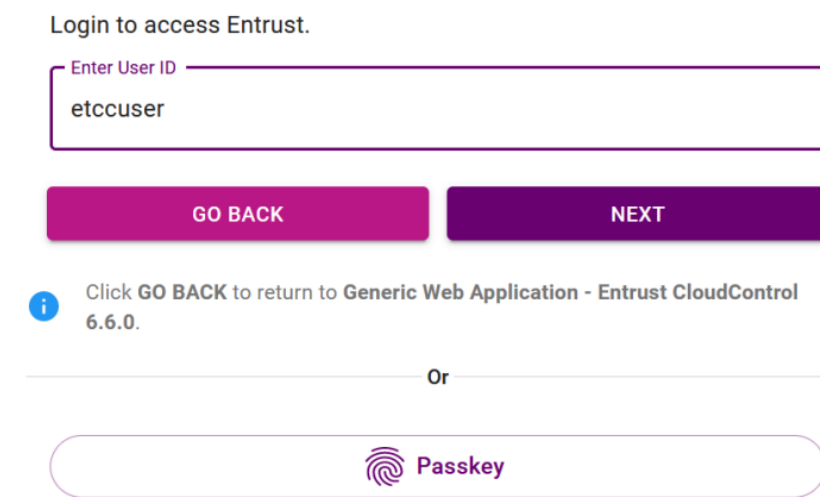
Entrust Identity as a Service (IDaaS) is a cloud-based identity and access management solution. It provides multi-factor authentication, credential-based passwordless access, and single sign-on (SSO). The application supports various authentication methods and integrates with systems such as Microsoft Active Directory and Azure Active Directory. It offers adaptive risk-based authentication to enhance security and user experience while preventing ATO.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from public sources (link: <https://marketplace.crowdstrike.com/listings/entrust-identity-as-a-service-idaas>).

Product Visuals²



Entrust Identity as a Service

Product	Excellent	With a comprehensive capability set, Entrust effectively defends against ATO using both authentication and fraud prevention capabilities.
Product Capability	Excellent	Entrust offers one of the most comprehensive authentication suites we analyzed, including app-based authentication, biometric authentication, SMS OTP, and email OTP. Combined with behavioral biometrics, Entrust provides a formidable set of capabilities to combat ATO effectively.
Scalability	Excellent	Entrust focuses on financial services and enterprises, having collaborated with many large companies to provide ATO prevention. This indicates their ability to effectively scale with clients, regardless of the institution's size.
Customization	Strong	By offering both authentication and fraud-specific capabilities, Entrust can tailor their solutions to meet a diverse range of customer needs in combating various ATO threats. This flexibility allows for comprehensive protection, addressing multiple aspects of security with precision.
Accuracy	Excellent	By focusing on providing certificate-based authentication combined with behavioral signals across the customer lifecycle, Entrust can accurately detect and prevent ATO threats with a high degree of precision. This comprehensive approach ensures robust security throughout user interactions.
Product Integration	Excellent	Entrust offers an open API architecture for customers seeking IAM and ATO prevention services. Additionally, the company provides comprehensive SDKs that can be directly embedded into existing applications, providing customers with flexibility and ease of integration.
Buyer Satisfaction	Strong	While Entrust's customer satisfaction is not as high as some other vendors we covered, we believe that their strategy of combining multiple authentication features with behavioral biometrics will continue to meet customer needs. As demand for behavioral biometrics increases, this approach is likely to enhance customer satisfaction over time.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.


Analyst Notes on Entrust Identity as a Service

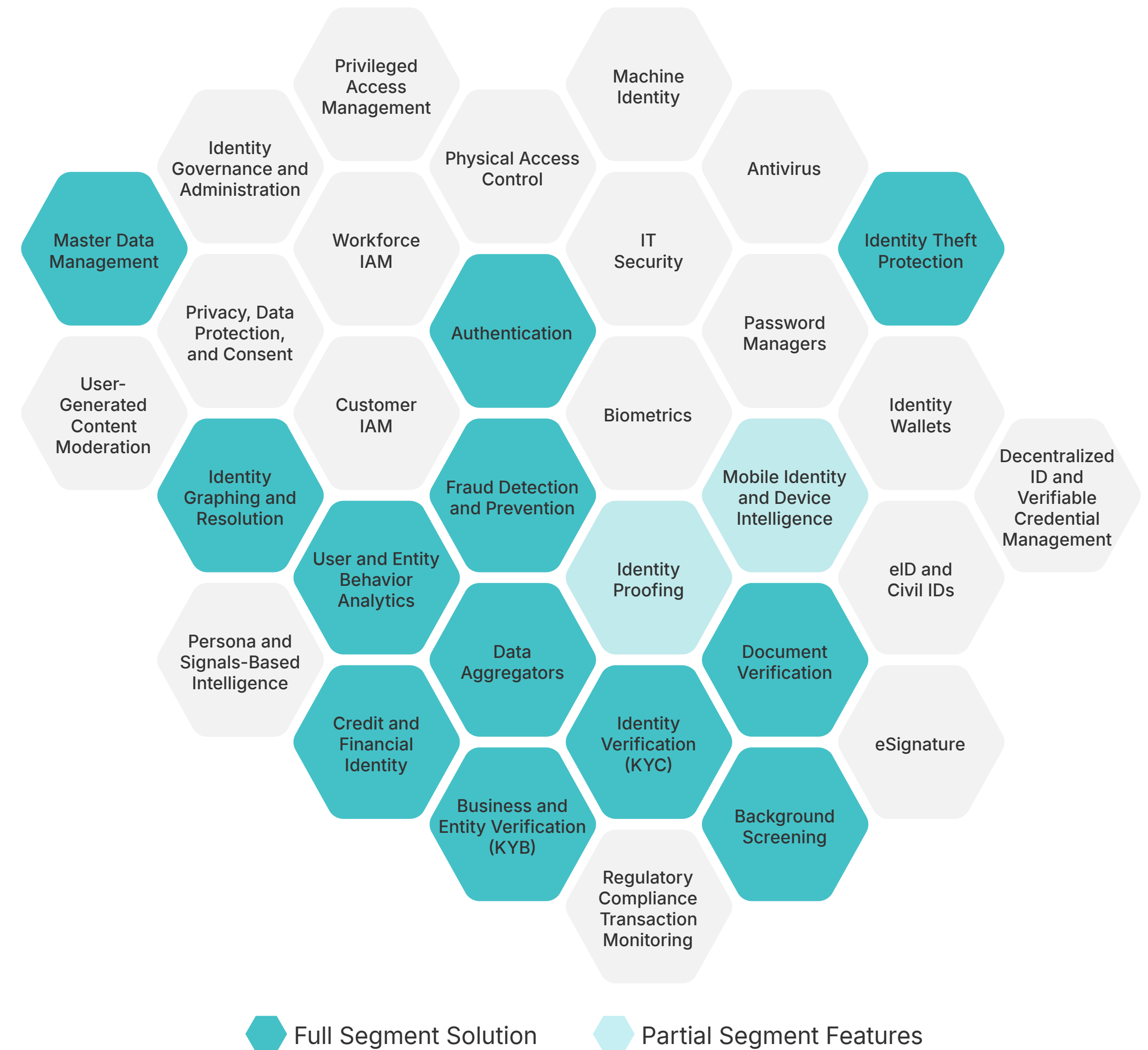
Entrust Identity as a Service is a cloud-based identity and access management (IAM) solution that provides comprehensive digital security solutions for organizations across various industries, including banking, government, and healthcare. At its core, Entrust IDaaS enables trusted identities for workforces and consumers, allowing them to engage securely and seamlessly with an organization. Key features of Entrust Identity as a Service include best-in-class multi-factor authentication (MFA) with support for numerous authenticators and use cases, high-assurance credential-based access using digital certificates, single sign-on (SSO) for secure access to cloud and on-premises applications, and passwordless authentication options compliant with FIDO standards. The solution also offers identity orchestration capabilities, allowing organizations to unify user registration and authentication across multiple identity providers, including social logins. Additionally, it provides robust authorization and access management through role-based access control (RBAC), URL/API protection with OAuth 2.0/2.1 and OpenID Connect (OIDC), and support for embedded device app authentication and authorization.

Entrust IDaaS incorporates adaptive risk-based access and authentication, enabling organizations to apply contextual authentication and step-up user challenges based on risk factors. It also supports email and file encryption, document signing, identity proofing for secure remote onboarding, fraud detection and prevention, and secure access to consumer and partner portals. The platform offers off-the-shelf integrations, APIs, and developer toolkits, including SAML and OIDC for identity federation, RESTful APIs, and a comprehensive list of available integrations. Organizations can also opt to deploy IDaaS as a managed service through Entrust's certified Managed Service Provider (MSP) partners.

Experian

Experian is a global credit bureau and information services company providing data and analytical tools. It offers services in credit reporting, fraud detection, decision analytics, and consumer credit education. Experian helps businesses manage credit risk, prevent fraud, and automate decision-making processes while enabling consumers to manage their financial health.

Company Information ¹	
Headquarters	Dublin, Ireland
No. of Employees	22,829
Last Raised	Public Company
Primary Segment	Credit and Financial Identity, eIDs and Civil IDs, Identity Theft Protection, Fraud Detection and Prevention, Master Data Management, User and Entity Behavior Analytics, Identity Graphing and Resolution, Identity Graphing and Resolution, Data Aggregators, Background Screening
Vertical Focus	Financial Services
Geographic Focus	North America, Europe, Latin America, Asia-Pacific, Middle East
Notable Customers	



(1) Link

Experian's Strategy

Strategy	Excellent	Experian leverages passive signals to provide robust protection against phishing and social engineering, all while delivering a strong user experience at a competitive price.
Behavioral Capabilities	Exceptional	By offering behavioral biometrics, behavioral analytics, and bot detection capabilities, Experian's CrossCore product provides robust protection against social engineering and scams. Additionally, their Ascend platform leverages Experian's extensive data network to detect fraud.
Passwordless Authentication	Strong	Experian does not offer passwordless options like passkeys, opting instead for a signal-based approach to ATO prevention. However, the company does provide biometric authentication to guard against ATO threats like credential stuffing.
Cost	Excellent	According to banking buyers focused on ATO prevention, Experian offers excellent cost-effectiveness. The Experian CrossCore platform provides a wide range of product capabilities and use case coverage, allowing customers to meet their needs without using multiple products.
User Experience	Excellent	Banking buyers noted high satisfaction with Experian's customer experience. This may be because Experian leverages its extensive datasets, including both deterministic and probabilistic data, to detect anomalies using passive signals such as behavioral biometrics and behavioral analytics; using passive signals helps to minimize customer friction.

Analyst Notes on Strategy

Experian has integrated NeuroID's behavioral analytics capabilities into its CrossCore fraud prevention platform. NeuroID's solution analyzes users' real-time behaviors, such as keystrokes, mouse movements, and typing speed, to detect genuine or fraudulent intentions during online interactions. This behavioral analytics approach enables Experian to capture the underlying behavioral patterns exhibited by fraud rings, bots, and other malicious actors, helping to identify warning signs before they can successfully carry out attacks. NeuroID's technology can proactively identify and thwart fraudulent entities by interpreting these subtle nuances in user behavior while ensuring a seamless experience for legitimate customers.

In addition to NeuroID's behavioral analytics, CrossCore also leverages artificial intelligence and behavioral biometrics to recognize how users interact with their devices during account opening, login, transactions, and account management processes. These behavioral biometric signals provide additional insight into user intent and risk assessment. CrossCore's integration of behavioral analytics and biometrics complements its suite of diverse fraud detection capabilities, including identity verification, risk-based authentication, and advanced analytics. This layered defense approach orchestrates multiple fraud signals and data sources into a unified risk assessment, enabling Experian to make real-time, informed decisions throughout the customer lifecycle.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Experian's Market Presence

Market Presence	Exceptional	Experian is a large credit reporting agency that benefits from leading brand awareness and leadership. Its fraud solutions are widely recognized and utilized in financial services.
Brand Awareness	Exceptional	The company's comprehensive fraud detection and identity management solutions, including the CrossCore platform, are trusted by businesses worldwide to protect against a wide range of fraud types – 97% of surveyed financial service practitioners were familiar with the Experian brand the second highest awareness of profiled vendors.
Market Leadership	Exceptional	Experian has established itself as a market leader in fraud prevention being consistently recognized by industry analysts for its advanced fraud detection capabilities. Of practitioners familiar with their brand, 63% recognize them as market leaders, which leads among all profiled vendors.
Market Penetration	Exceptional	The company's flagship platform, CrossCore, integrates multiple data sources and cutting-edge technologies like AI and machine learning to provide real-time risk analytics and decision-making, protecting a wide range of financial institutions from diverse fraud threats.
Company Size	Exceptional	Experian, headquartered in Dublin, Ireland, employs approximately 23,000 people and operates in 32 countries, with major offices in locations such as Costa Mesa (California), London, Nottingham, and São Paulo. The company reported an annual revenue of \$7.10 billion for the fiscal year ending March 31, 2024, reflecting its substantial global presence.
Employee Growth	Excellent	Experian has experienced strong employee growth metrics, roughly a 20% increase over the last year, despite strategic layoffs, including a reduction of 150 employees in its Information Solutions unit and 200 employees across North America. Despite these layoffs, Experian has also focused on strategic hires and expansion, such as launching a new India Development Centre in Hyderabad, aiming to create 2,500 jobs by 2024.

Analyst Notes on Market Presence

Experian is a major global player in the data analytics and credit bureau industries. Their customer base spans 4,286 companies worldwide, with a strong presence across the insurance, wealth management, and financial services sectors. Most of Experian's data analytics customers are mid-sized to large enterprises, with companies ranging from 1,000 to over 10,000 employees. Geographically, Experian operates in 32 countries and has around 23,000 employees globally. Its largest concentration of customers comes from the United States and the United Kingdom.

Experian's strong foothold in the credit bureau sector, along with its global reach and diverse customer base across industries and company sizes, underscores its significant market presence. The company's financial strength and continued investments in data analytics and fraud prevention solutions further reinforce its position as a formidable force in these domains.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Experian CrossCore

Experian CrossCore is a modular platform designed to integrate various fraud and identity solutions into a single system, providing a comprehensive approach to managing risk. It enables businesses to enhance their fraud detection capabilities by combining multiple tools and data sources, thereby improving accuracy and efficiency in identifying potential threats. CrossCore's flexible architecture allows for easy addition and management of new solutions as fraud patterns evolve, ensuring businesses can adapt quickly to new challenges.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from public sources (link: <https://brianjleach.com/eds>).

Product Visuals²

The screenshot displays the Experian CrossCore interface for a case titled 'Case: KVWYKLS3 Investigating'. The user is logged in as 'Brian'. The interface is divided into several sections:

- Case Information:** Summary, Comparisons, Calendar, Data Spider, SketchMatch.
- Contact Information:** Email (m.smith@gmail.com), Home Address (12345 Anystreet, Anytown, CA, 98765), Mailing Address (PO Box 1234, Anytown, CA, 98765), Mobile Phone (+1 123-456-7890), and Phone (+1 098-765-4321).
- Personal Information:** Date of Birth (01-Jul-1980, Age 39), Driver's License Number (60-627-0825, Issued: 24-Jul-2008), Customer ID (USCZXR5AAF), Internal ID (SXKZSDQ1), Other App ID (CEPJMEBXPX), and External Code (AUCJMIWVOYO).
- Case Administration:** Assigned to: Brian (Lastname, Firstname).
- Summary:** Features a large risk score of 776 and a profile picture of Melinda Smith. Recommended actions include 'Accept', 'Hold', 'Decline', and 'Export'.
- ANALYSIS:**
 - Machine Learning Score (755):** 2 of 8 matches. Includes K6: NAP+Dana+FP (129) and K7: NAS+FP+Risks (170).
 - Fraud Risk Management (820):** Audit trail showing PNNIP - Negative IP Address (100) and PNNCP - Negative C Block (150).
 - Identity Authentication (800):** Metrics include PreciseID (10), Validation (30), Verification (10), PFD (25), and PreciseMatch (25).
 - Email Risk Assessment (903):** Low Risk. Metrics include Email Fraud Risk (25), IP Risk Level (40), and Domain Risk Level (35).
 - Document Verification (98%):** Authenticated. Metrics include Document Data Comparison (Authentic, probability: 1000) and Rounded Corner Presence (Authentic, probability: 1000).
 - Identity Fraud Score (440):** Metrics include CVI (10 [250]), K1: InstantID + FP (50), NAS (10), and Watchlist Warning (100).
- NOTES:** A list of notes including 'Auto-approved by strategy' (29-Dec-2019, 2:37PM), 'Dispositioning case' (29-Dec-2019, 10:15AM), and 'Case added to Queue ABC' (28-Dec-2019, 7:30PM).

Experian CrossCore

Product	Exceptional	CrossCore provides a fully-featured toolkit that leverages a wide range of capabilities for highly accurate and scalable ATO prevention.
Product Capability	Exceptional	CrossCore provides one of the most comprehensive product capability suites among the vendors we profiled. It offers several highly demanded features, including email and SMS OTP, social engineering and scam detection, behavioral biometrics, and location intelligence.
Scalability	Exceptional	As a multinational corporation, Experian has extensive experience working with the world's largest banks. They provide robust ATO prevention solutions that scale effectively as banks expand their user base and transaction volumes.
Customization	Excellent	The Ascend sandbox offers customers access to vast amounts of data and allows them to customize models. It also provides other customizable tools, enabling a tailored approach to data analysis and model development.
Accuracy	Exceptional	Experian achieved one of the highest accuracy scores among the vendors we analyzed, according to banking customers. CrossCore leverages extensive behavioral signals and device intelligence to effectively identify fraudsters. Its unsupervised machine learning models enable highly sophisticated threat detection.
Product Integration	Exceptional	CrossCore provides a comprehensive range of services for banking customers focused on ATO prevention. Their flexible API solution allows for customized implementations to meet the specific needs of each bank.
Buyer Satisfaction	Excellent	Starting as a data aggregator, Experian possesses one of the most comprehensive datasets among the companies profiled. Leveraging extensive fraud datasets, the company ensures thorough detection for their customers while maintaining a seamless user experience.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.




Analyst Notes on Experian CrossCore

Experian CrossCore is an integrated digital identity and fraud risk platform that consolidates risk-based authentication, identity proofing, and fraud detection into a single cloud-based system. This platform allows businesses to integrate and orchestrate decisions across various fraud and identity solutions from Experian, third-party providers, and their internal systems via a common, flexible API. It features advanced analytics, machine learning models, and leading industry tools for detecting fraud signals throughout the customer lifecycle, including during account opening, login, transactions, and account management. Additionally, CrossCore offers robust identity-proofing capabilities using Experian's extensive identity data assets, analytics, and scoring to verify customer identities confidently. It also assesses risks associated with digital identifiers like internet-enabled devices and email addresses to bolster fraud defenses.

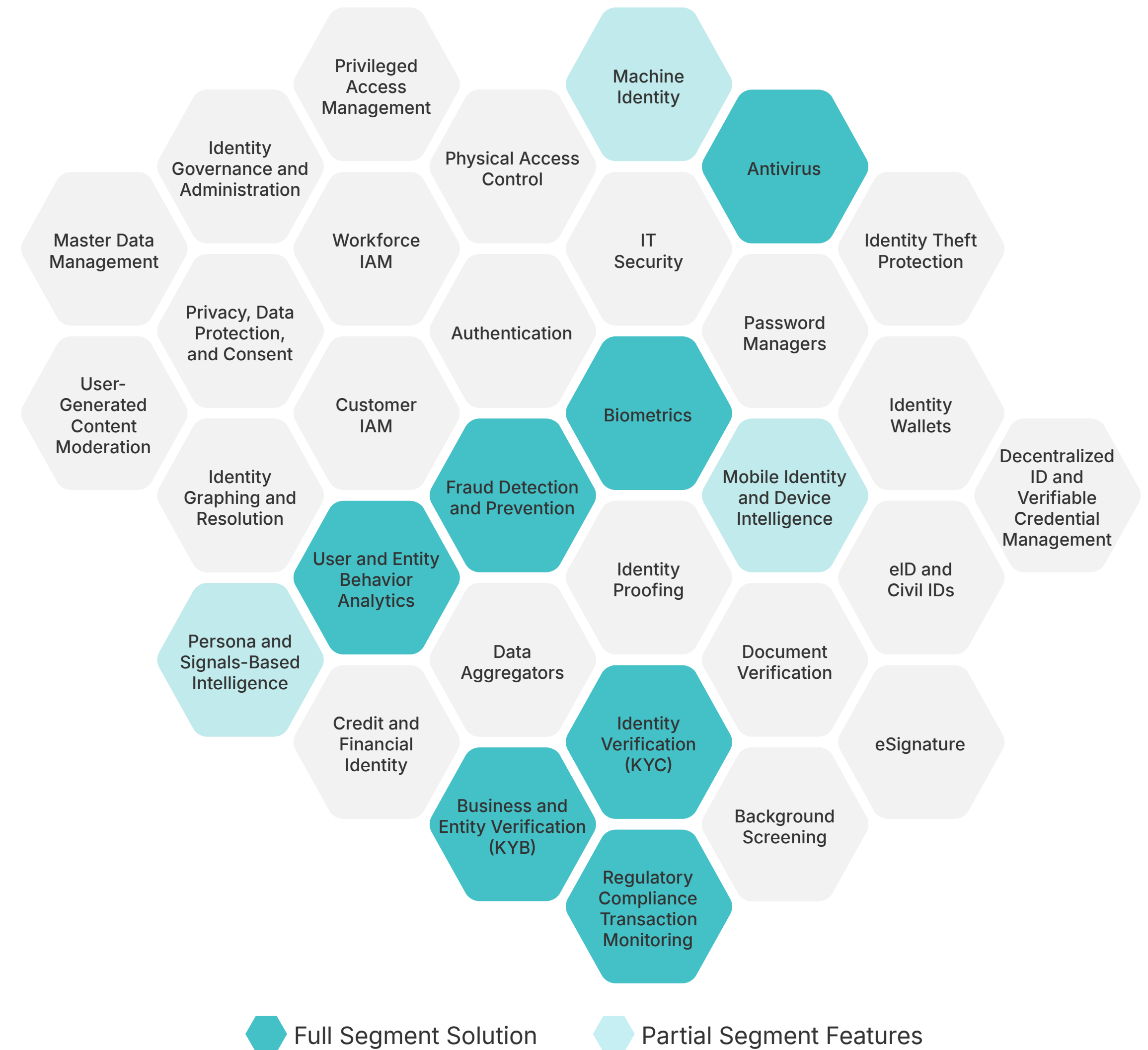
Customers of CrossCore also get access to Experian's Ascend Platform, which includes the Ascend Analytical Sandbox and Ascend Ops. The Ascend Sandbox enables access to years of credit data on 245 million consumers, commercial data, property data, and other alternative data sources. In addition to thousands of scores and attributes, it offers industry-standard analytics and data visualization tools, such as SAS, RStudio, Python, Hue, and Tableau, for insights that speed decisions about consumers and businesses. Ascend Ops provides constant monitoring of usage and health statistics to track and improve the drift and performance of the models being leveraged. Moreover, it supports customers' model governance process by tracking lifecycle lineage and storing model artifacts all in one place to meet compliance and audit process needs, including development code, documentation, test data, results, and approvals.

Feedzai

Feedzai provides an analytics-enabled platform to detect and prevent financial crimes, including fraud and money laundering. Their solutions encompass transaction monitoring, account opening verification, fraud prevention, and KYC/CDD compliance, leveraging machine learning to analyze behavioral and transactional data. The platform integrates with various systems to provide comprehensive protection and risk management across different financial services, and aims to enable Financial Crime functions to more holistically embed analytics within their operations and workflows.

Company Information ¹	
Headquarters	San Mateo, California
No. of Employees	636 as of May 2024
Last Raised	Venture – Series Unknown (Amount Undisclosed) in August 2021
Primary Segment	Fraud Detection and Prevention
Vertical Focus	Financial Services
Geographic Focus	North America, Europe, Asia-Pacific, Latin America
Notable Customers	  

(1) Link



Feedzai's Strategy

Strategy	Excellent	Feedzai provides comprehensive behavioral signals at reasonable cost and levels of friction, ensuring a positive user experience and effective ATO prevention for banking customers.
Behavioral Capabilities	Exceptional	Feedzai boasts a robust suite of product capabilities for detecting fraud, utilizing behavioral signals, transaction data analysis, behavioral analytics, and bot detection. This comprehensive approach provides accurate solutions to prevent various ATO threats.
Passwordless Authentication	Strong	Feedzai emphasizes fraud prevention signals rather than passwordless solutions, opting not to offer passkeys or QR code authentication for ATO prevention. By focusing on advanced behavioral analytics and transaction data, Feedzai provides robust protection against fraudulent activities without relying on traditional passwordless authentication methods.
Cost	Excellent	Feedzai prioritizes proactive ATO defenses that minimize financial losses and deliver strong ROI. Additionally, the company's cost effectiveness is regarded as very strong compared to other ATO prevention solution providers in the banking sector.
User Experience	Excellent	In addition to providing behavioral signals that reduce user friction, Feedzai Active Defense proactively prevents malware and phishing attacks from stealing user credentials. This ensures that users do not have to deal with stolen credentials and account recovery processes.

Analyst Notes on Strategy

Feedzai's RiskOps platform heavily relies on behavioral analytics and behavioral biometrics to detect and prevent fraud. In 2021, Feedzai acquired Revelock, an advanced behavioral biometrics platform, to integrate its technology natively into the RiskOps platform. This acquisition allows Feedzai to provide customers with comprehensive models, rules, labels, and reports that leverage behavioral biometric intelligence from day one through a single platform solution. This addition to the Feedzai platform makes it a competitive end-to-end risk management platform for prevention, detection, remediation, and compliance that will improve the user experience while minimizing the burden on fraud teams.

While Feedzai has not adopted passwordless authentication modalities, behavioral analytics and biometrics power its step-up authentication capabilities. The platform also generates real-time risk scores based on behavioral signals, device intelligence, and other contextual factors. This enables organizations to distinguish between legitimate users and potential fraudsters during authentication flows. Feedzai enables organizations to implement step-up authentication measures, such as adaptive or risk-based authentication, based on the assessed risk level and transaction context.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Feedzai's Market Presence

Market Presence	Exceptional	Feedzai's RiskOps platform can solve a range of fraud and compliance use cases, positioning them well to penetrate financial services and compete with incumbent vendors.
Brand Awareness	Excellent	Feedzai has established strong brand awareness in the financial services sector, being trusted by 80% of the world's Fortune 500 companies – of surveyed practitioners in financial services, 65% were familiar with the brand and the RiskOps platform.
Market Leadership	Exceptional	Of those who were familiar with the Feedzai brand and RiskOps platform, 41% recognized them as market leaders. This is indicative of Feedzai's ability to effectively solve fraud use cases for financial institutions through their platform solution
Market Penetration	Exceptional	Feedzai has achieved significant market penetration in the financial services, serving some of the world's largest banks, payment providers, and merchants. The company's technology protects 900 million people across 190 countries, safeguarding trillions of dollars in transactions.
Company Size	Exceptional	The company employs over 600 people and operates 10 global offices, supporting customers in 190 countries. It has also raised more than \$200 million in funding, reflecting its significant presence and development in the fraud detection market.
Employee Growth	Strong	Feedzai experienced negative employee growth in the last year – roughly a 3% decrease YoY. This reduction is part of the company's restructuring efforts amid challenging economic conditions despite its strong financial performance and market presence.

Analyst Notes on Market Presence

Feedzai has experienced significant growth and now provides services to major financial institutions, safeguarding over 900 million consumers across 190 countries via its RiskOps platform. Moreover, their solution processes roughly 45% of all U.S. debit and credit card transactions. Its over \$1.5 billion valuation as a Series D company further underscores its significant market presence and growth potential.

Their platform is recognized for its robust fraud detection and management capabilities, tailored to the complex needs of large-scale financial environments. Feedzai has established a considerable international presence with ten global offices and customer bases across North America, Latin America, Europe, the Middle East, and Asia. This ensures a responsive and localized service offering. Feedzai's market influence is further enhanced through strategic channel partnerships with prominent financial services companies such as Ernst and Young, Thomson Reuters, Fiserv, and MasterCard. These collaborations extend Feedzai's reach and enrich its capabilities with advanced insights and technologies, reinforcing its position as a leader in financial security.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Feedzai RiskOps Platform

The Feedzai RiskOps platform integrates fraud detection, AML, and risk management into a unified system. It analyzes data across the customer lifecycle to provide real-time risk assessments and prevent financial crimes. The platform offers visual link analysis, white box explanations, and omnichannel case management tools to streamline workflows and enhance decision-making. The platform covers several use cases, such as account opening, ATO, KYC/AML, transaction fraud, scam and mule detection, digital identity data management, and watchlist screening.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from public sources (link: <https://www.softwareadvice.com/risk-management/feedzai-profile/>).

Product Visuals²

Feedzai RiskOps Platform

Product	Excellent	Feedzai offers robust fraud prevention capabilities on its RiskOps platform to fight against ATO.
Product Capability	Excellent	Feedzai focuses on fraud-related ATO capabilities, such as social engineering and scam detection and behavioral analytics. The RiskOps platform uses these capabilities to prevent bad actors from making fraudulent transactions.
Scalability	Excellent	Feedzai provides robust automation that allows the solution to handle large transaction volumes and scale with their clientele.
Customization	Strong	Feedzai allows customers to import third-party models through standard APIs into their OpenML Engine, a comprehensive tool for engineering teams that enables seamless customization of multiple solutions and data sources.
Accuracy	Excellent	The RiskOps platform delivers accurate solutions by leveraging sophisticated behavioral data to detect fraudulent activity. By analyzing a wide range of transactions, the company can fine-tune its fraud models to effectively identify fraud.
Product Integration	Excellent	The RiskOps platform offers automated solutions designed to reduce tedious engineering workflows. It provides extensive model selection to simplify product integration and implementation.
Buyer Satisfaction	Excellent	The automated RiskOps platform offers extensive use case coverage and robust capabilities for ATO prevention in banking. We anticipate that the company will continue to excel as customers increasingly seek behavioral biometrics and behavioral analytics solutions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Feedzai Risk Ops Platform

Feedzai's RiskOps platform is a comprehensive, cloud-based solution designed to tackle various forms of financial risk, including fraud prevention and detection. At its core, the platform leverages advanced artificial intelligence (AI) and machine learning technologies to analyze vast amounts of data. The solution can identify patterns indicative of fraudulent activities across multiple payment channels, devices, networks, and user behaviors.

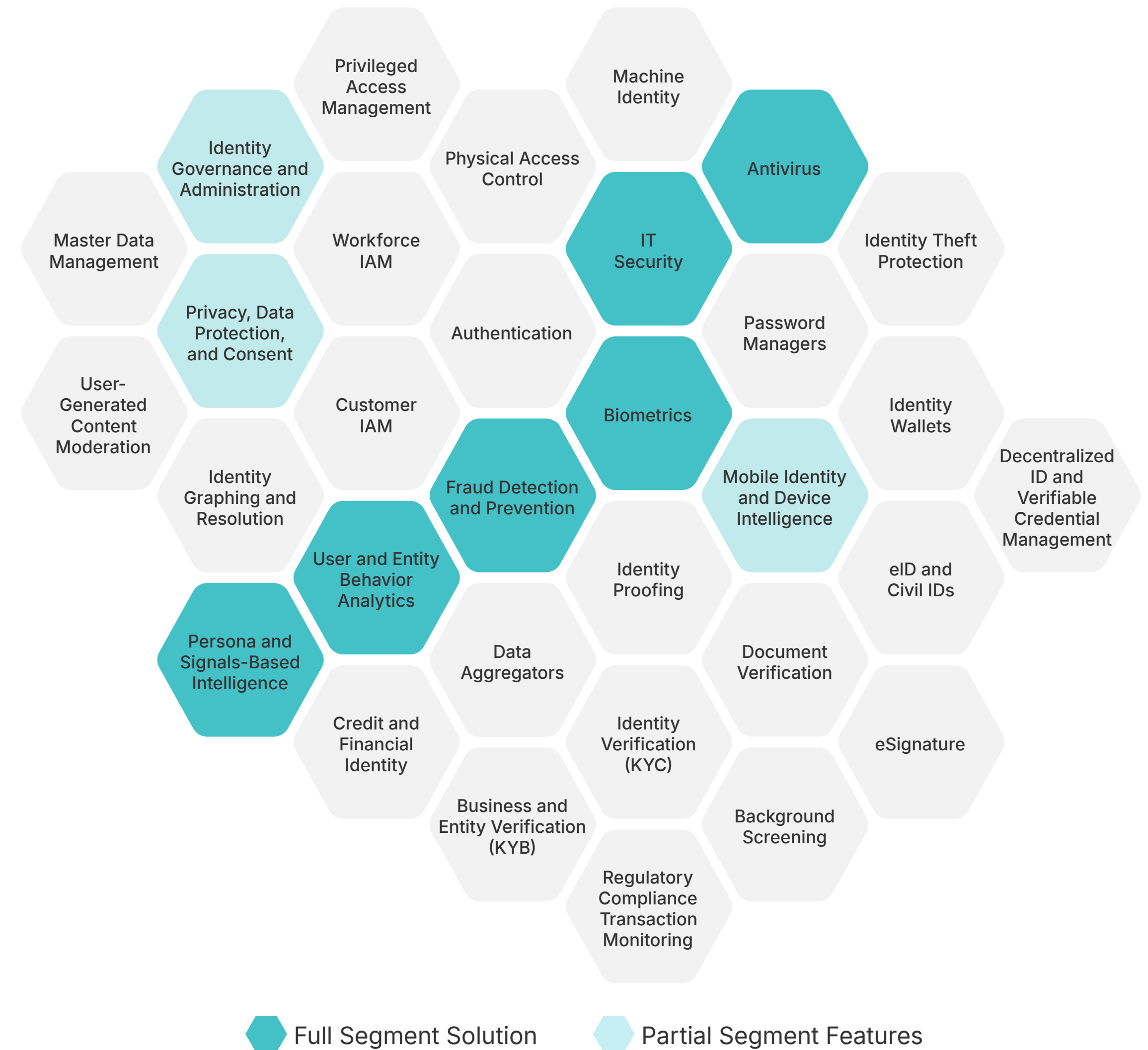
The RiskOps platform's fraud capabilities are powered by Feedzai's Pulse Risk Engine, which enables organizations to connect data from various payment channels, payment types, devices, networks, user behaviors, accounts, geolocations, and more. This engine accurately assesses risk in real-time, allowing companies to detect and prevent fraud before it occurs. Additionally, the platform's Human-Centered AI approach ensures that risk assessments are individualized and not based on cohort-based models, reducing the risk of bias and false positives and providing a frictionless customer experience.

The platform's Case Manager component automatically contextualizes information, speeding up alert disposition and enabling analysts to transform data points into actionable insights for preventing and detecting future attacks. Additionally, the Genome feature utilizes Visual Link Analysis to sequence the DNA of risk and financial crime patterns, helping organizations better understand the relationships between criminal networks that may otherwise go undetected. Feedzai's RiskOps platform also integrates with the company's Financial Intelligence Network (FIN), a vast database containing over 1 trillion data points, sessions, and profiles of both good and bad actors. This network further enhances the platform's fraud detection capabilities by leveraging anonymized data from various sources to identify and mitigate emerging threats.

HUMAN

HUMAN Security specializes in protecting digital interactions from sophisticated bots and fraud. HUMAN provides comprehensive solutions for ad fraud defense, account protection, transaction abuse prevention, and application security, ensuring robust protection while maintaining a seamless user experience to safeguard businesses against evolving cyber threats. The company provides a unified cybersecurity and fraud solution that covers a wide range of use cases.

Company Information ¹	
Headquarters	New York, New York
No. of Employees	444 as of May 2024
Last Raised	\$8.5M, Venture – Series Unknown in May 2024
Primary Segment	User and Entity Behavior Analytics
Vertical Focus	Financial Services, Fintech, Healthcare, Gig Economy, eCommerce, Government, Media & Entertainment
Geographic Focus	North America
Notable Customers	HUMAN does not publicly disclose banking customers



(1) Link

HUMAN's Strategy

Strategy	Exceptional	As a leading player in bot management, HUMAN leverages behavioral signals to provide high levels of security while ensuring a strong user experience.
Behavioral Capabilities	Exceptional	As one of the leading bot detection vendors, HUMAN offers effective bot detection management capabilities. Additionally, the company provides behavioral biometrics and behavioral analytics to detect and prevent ATO threats such as phishing.
Passwordless Authentication	Strong	HUMAN does not offer passwordless authentication options like device-based or cloud-based passkeys. Instead, it leverages behavioral signals to detect fraud by analyzing contextual indicators such as device movement and keystroke dynamics.
Cost	Exceptional	While point solutions like HUMAN typically operate alongside other vendors in tech stacks, customers of HUMAN were very satisfied with the company's cost-effectiveness. In fact, HUMAN received the third-highest value-for-money ranking among all the vendors we profiled, according to current customers.
User Experience	Exceptional	HUMAN employs a robust suite of behavioral capabilities to prevent account takeovers. By analyzing a wide range of signals, HUMAN's solution operates in the background during user sessions, avoiding high-friction authentication mechanisms that can lead to user drop-off.

Analyst Notes on Strategy

At the core of HUMAN's solution is their decision engine that examines over 2,500 signals per interaction. These signals are parsed through more than 400 algorithms and adaptive machine-learning models to detect anomalies and threats with high precision. It offers real-time visibility into threats by generating telemetry data at every touchpoint along the customer journey. This helps in identifying and countering emerging threats and fraud in real-time.

Moreover, their HUMAN's Bot Defender which comes as part of their broader Defense Platform is a behavior-based bot management solution designed to protect websites, mobile applications, and APIs from automated attacks. Bot Defender offers a range of enforcement actions to mitigate the impact of unwanted bots, including blocking, rate-limiting, or redirecting them to decoy sites. It features the Human Challenge, a user-friendly verification feature that protects against CAPTCHA-solving bots while maintaining a positive user experience. Bot Defender provides rich analytics through the Bot Defender Portal, including pre-built and customizable dashboards, as well as a Business Insights Dashboard for executive-level insights and industry benchmarking.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

HUMAN's Market Presence

Market Presence	Strong	HUMAN is a well-recognized fraud and cybersecurity vendor primarily known for its superior bot detection capabilities; the vendor supports a wide range of customers.
Brand Awareness	Excellent	HUMAN brand awareness is primarily driven by their solutions to identity and mitigate sophisticated bot attacks. Of surveyed practitioners in financial services, 50% were familiar with the brand and solution to solve for ATO prevention.
Market Leadership	Strong	HUMAN has established itself as a market leader by leveraging its advanced Defense Platform to protect over 500 brands from bot attacks. Of practitioners we surveyed familiar with the HUMAN brand 19% recognize them as market leaders.
Market Penetration	Excellent	The company leverages a unique multilayered defense platform, which includes machine learning, threat intelligence, and technical evidence, to safeguard over 20 trillion interactions weekly and over 3 billion unique devices monthly.
Company Size	Excellent	HUMAN, headquartered in New York City, employs about 450 employees with other offices in Miami, Dallas, Washington D.C., London, and San Mateo. The company has raised a total of \$131 million in funding, underscoring its significant market influence and capacity for research and development to protect against sophisticated bot attacks and digital fraud.
Employee Growth	Strong	They experienced a notable employee growth of 7% over the last year.. This growth was bolstered by strategic hires, including the appointment of a new Chief Revenue Officer and a new Chief Marketing Officer, to drive the company's market expansion and enhance its go-to-market strategy.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Market Presence

HUMAN has established a significant market presence with its ATO solution, particularly in the realm of bot management and human presence detection systems. HUMAN was originally founded in 2012 as White Ops before changing the company name in early 2021.

The company advocates for a collective form of protection with companies working together to prevent attacks by botnets, such as the sophisticated PARETO botnet it helped foil with the help of Roku, Google, and its Human Collective. HUMAN says it verifies more than 15 trillion interactions a week from its client companies.

In 2022, HUMAN announced a merger with PerimeterX, a company focused on safeguarding web apps from account takeover and automated fraud. PerimeterX had protected mostly e-commerce companies, while Human was well-penetrated across AdTech. Together their solution addresses the bot attack problem through using machine learning to understand authentic "human" behavior, which helps to detect anomalous actions driven by bots.

HUMAN Defense Platform

The HUMAN Defense Platform offers comprehensive threat detection and protection across digital interactions, leveraging machine learning and extensive data analysis. The platform supports various applications, including ad fraud prevention, account protection, and web security. It integrates with existing security systems to enhance decision-making against sophisticated cyber threats.

ATO Prevention Product Capability Coverage¹

H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from public sources (link: <https://time.com/collection/best-inventions-2023/6323152/human-defense-platform/>).

Product Visuals²



HUMAN Defense Platform

Product	Strong	HUMAN specializes in bot management solutions, which customers report to be highly scalable and customizable.
Product Capability	Strong	HUMAN aims to prevent financial losses caused by bots. Its product capabilities include bot detection, behavioral analysis, and device risk scoring, among others. However, the company has limited authentication capabilities.
Scalability	Strong	Given the increasing volume of sophisticated bots in recent years, HUMAN has developed scalable solutions to ensure effectiveness as login attempts rise due to non-human attacks.
Customization	Excellent	The HUMAN Dashboard provides customers with deep insights into bot activity and security measures. Additionally, customers can create and customize views within the dashboard to effectively manage their ATO solutions.
Accuracy	Strong	While HUMAN is considered by those surveyed to be less accurate than some of the other top solutions analyzed, it effectively deals with bot detection. It successfully identifies headless sessions involved in credential stuffing, DDOS, and other ATO attacks.
Product Integration	Excellent	HUMAN provides its MediaGuard API and Reporting API, enabling customers to access FraudSensor data to effectively counteract ATO threats and minimize financial losses.
Buyer Satisfaction	Strong	For banks seeking point solutions for bot management, HUMAN is a strong option, offering accurate detection of non-human actors. This is particularly crucial as bot activity continues to rise across all sectors.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.



Analyst Notes on HUMAN Defense Platform

HUMAN's Defense Platform is a comprehensive solution designed to protect organizations against various digital threats, including ad fraud, online fraud, data contamination, and account takeovers. At the core of the Defender Platform is HUMAN's ability to verify the humanity of over 20 trillion digital interactions per week, observing more than 3 billion unique devices monthly. This massive observability provides unparalleled visibility into online traffic patterns, enabling the platform to accurately distinguish between human and non-human (bot) activities.

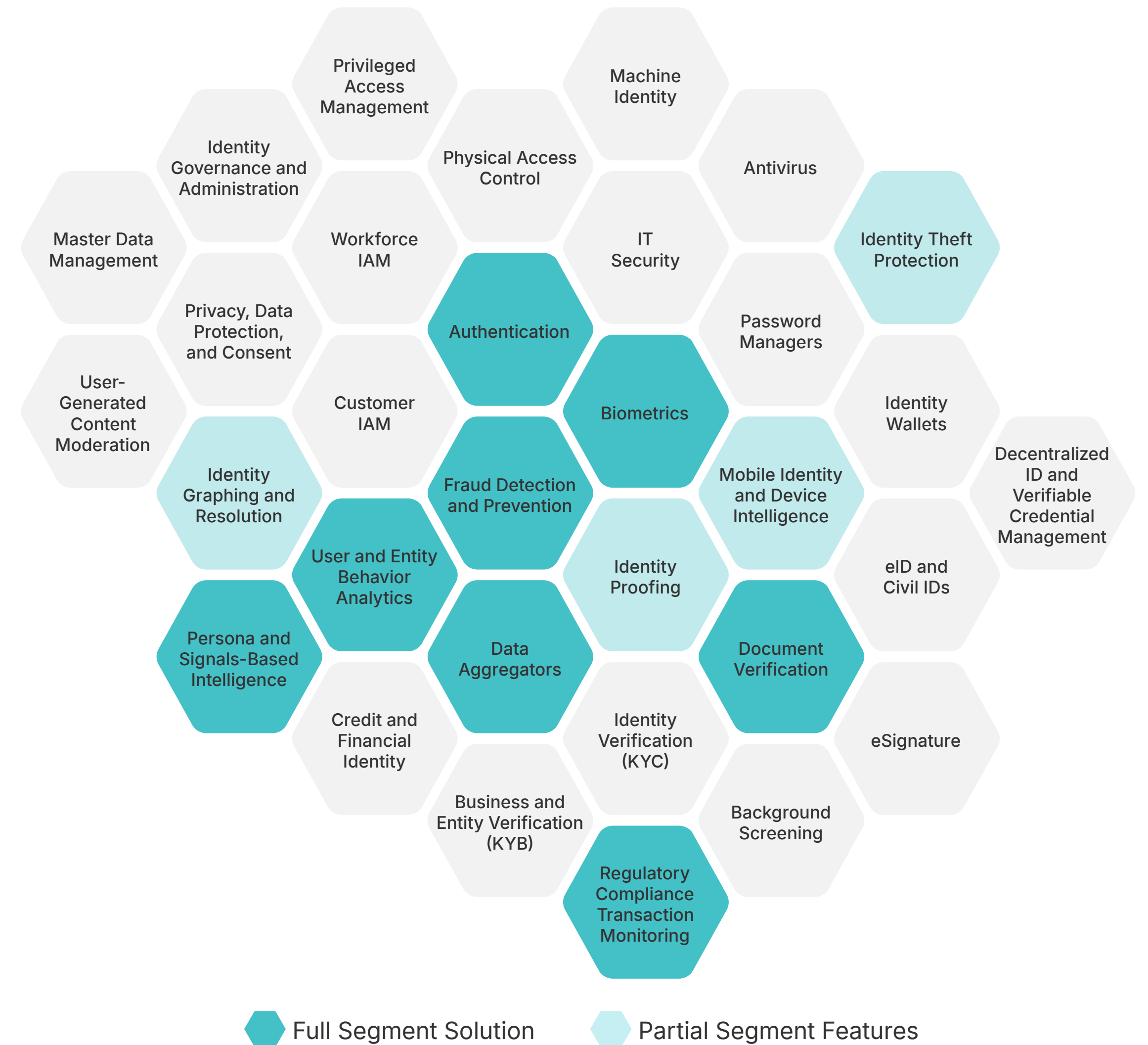
The Defense Platform comprises several modular solutions that can be tailored to address specific cybersecurity challenges. HUMAN Bot Defender, a behavior-based bot management solution, protects websites, mobile applications, and APIs from automated attacks, safeguarding online revenue, reducing the risk of data breaches, and improving operational efficiency. HUMAN Code Defender, on the other hand, is a client-side web application security solution that continuously protects websites from digital skimming, form jacking, and Magecart attacks, stopping data breaches and reducing the risk of non-compliance with various industry data protection standards. HUMAN Account Defender provides post-login account security, detecting compromised and fake accounts on apps and websites using behavioral analysis to identify suspicious patterns that define fraudulent activity. HUMAN Credential Intelligence is a cloud-native web app security solution that stops the use of compromised credentials in real-time, leveraging an expansive and up-to-date collection of signals gathered from HUMAN's position protecting some of the most popular and highly-trafficked sites on the web.

Kount

Kount, a subsidiary of Equifax, provides fraud detection and prevention solutions. The platform offers tools for managing payment fraud, chargebacks, and account takeover, helping businesses protect their operations across various digital channels. Kount’s technology creates detailed customer profiles to distinguish legitimate users from fraudsters, ensuring a secure and seamless user experience.

Company Information ¹	
Headquarters	Boise, Idaho
No. of Employees	550 as of May 2024
Last Raised	\$640M, Acquisition by Equifax in February 2021
Primary Segment	Fraud Detection and Prevention, Data Aggregators
Vertical Focus	Financial Services, eCommerce, Gaming, Healthcare, Media & Entertainment
Geographic Focus	North America
Notable Customers	 

(1) Link



Kount's Strategy

Strategy	Exceptional	Kount provides strong behavioral capabilities on a platform designed to handle various use cases, all at a competitive price. This makes it a versatile and cost-effective solution for fraud prevention.
Behavioral Capabilities	Exceptional	Kount offers an extensive suite of behavioral capabilities, including behavioral biometrics, behavioral analytics, and bot detection. This allows banks to gain sophisticated insights into risky behavior and enhance their fraud prevention efforts.
Passwordless Authentication	Strong	While Kount does offer passwordless authentication in the form of biometrics, it primarily focuses on leveraging behavioral signals for fraud prevention, rather than providing UX-oriented passwordless authentication options like QR codes or passkeys.
Cost	Exceptional	Kount achieved one of the best value-for-money scores among all the vendors we profiled, according to current customers. Kount consolidates a variety of solutions in identity, payments and compliance into a single solution, Kount 360, its pricing starts at \$0.07 per transaction for pay-as-you-go or starts at \$1,000 per month for their "Advanced" SaaS offering.
User Experience	Exceptional	Kount also boasts one of the highest user experience scores among all the vendors we profiled. With a robust set of passive behavioral capabilities, device risk scoring, location intelligence, and proxy and VPN detection, the company provides strong fraud detection without unnecessary friction.

Analyst Notes on Strategy

Behavioral analytics in Kount 360 helps understand user interactions and detect anomalies indicating fraudulent activities. Behavioral biometrics further enhance security by analyzing unique user behaviors, such as typing patterns and mouse movements, to verify identities without relying on traditional credentials. The platform's bot detection capabilities are designed to identify and block automated attacks, ensuring that only legitimate users can access services. Additionally, Kount 360 offers components of passwordless authentication, allowing users to log in using more secure methods like biometrics or trusted devices, thereby virtually eliminating account creation fraud and takeover schemes.

Regarding the cost structure, Kount 360 employs a flexible, a la carte pricing model, allowing businesses to pay only for the services they need. The pricing is influenced by several factors, including the specific solutions chosen, the volume of transactions processed, and the level of customization required. Kount buyers can select between packaging options including pay-as-you-go on a per transaction basis, a subscription offering that bundles together multiple features, or custom plan for larger enterprises needing advanced support and other white-glove services. This transparent and flexible pricing approach ensures businesses can tailor their trust and safety strategies to their unique requirements while optimizing costs.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Kount's Market Presence

Market Presence	Strong	As a subsidiary of Equifax, Kount benefits from extensive resources and strong brand recognition; however, it is best known as a chargeback management vendor.
Brand Awareness	Strong	Kount's integration with parent company Equifax and its advanced AI/ML technology has positioned it as a trusted partner for financial services businesses. They are well-recognized with 62% of surveyed practitioners recognizing their brand and solutions.
Market Leadership	Strong	The company's innovative technology and strategic partnerships with major financial institutions and payment providers have earned it recognition from other research firms. Of those practitioners familiar with the Kount brand, 11% recognize them as market leaders.
Market Penetration	Strong	Kount has achieved market penetration in the financial services sector, providing its AI-driven fraud detection and chargeback management solutions to over 9,000 global brands, including major banks and payment processors. The company's technology touches billions of transactions annually and is recognized for its effectiveness in preventing fraud across 180 countries.
Company Size	Excellent	Kount, an Equifax company since February 2021, has grown to employ more than 200 employees.
Employee Growth	Strong	Kount experienced modest employee growth of 2% over the last year, which positions them competitively, even during a period of unfavorable macroeconomic conditions.

Analyst Notes on Market Presence

Kount, an Equifax company, has established a significant market presence in the financial fraud detection and trust and safety technology sectors. Their platform is adopted by a diverse range of industries, with retail (26%), manufacturing (11%), internet (6%), and apparel and fashion (5%) being the most significant segments.

Kount's solutions are particularly popular among companies in the United States, which accounts for 64% of its customer base, followed by Canada (7%) and Australia (4%). Its platform is employed by various businesses, from small enterprises to large corporations, including notable names like PayPal, IBM, and Juul Labs. Kount's global reach is expanding, with operations growing in the United Kingdom and new markets in Latin America and Australia. This reflects its commitment to meeting the increasing demand for worldwide digital identity trust and fraud prevention solutions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Kount 360

Kount 360 is a comprehensive risk and compliance platform protecting businesses across the customer journey. It integrates identity verification, fraud prevention, and compliance solutions into a single system, using machine learning and a robust consortium data network to enhance decision accuracy. The platform provides a single API integration, customizable policies, and reusable identities to improve operational efficiency and reduce fraud.

ATO Prevention Product Capability Coverage¹

H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from company website (link:<https://www.equifax.com/newsroom/all-news/-/story/introducing-kount-360-a-comprehensive-identity-and-payments-platform/>).

Product Visuals²



Kount 360

Product	Excellent	Kount 360 covers a wide range of use cases and is perceived as highly accurate at ATO protection.
Product Capability	Excellent	Kount offers multiple authentication mechanisms for fortifying applications and implementing MFA. It excels at social engineering and scam detection, one of the most highly demanded features in ATO prevention among banking buyers. The company also provides behavioral biometrics and device risk scoring, among other capabilities, to enhance its fraud prevention solutions.
Scalability	Excellent	With Equifax as its parent company, Kount has the resources and experience to service large clients with substantial user bases and transaction volumes, enabling them to effectively scale as they grow.
Customization	Exceptional	Kount offers flexible automation by pairing businesses with fraud and risk experts to customize solutions according to each bank's specifications. This includes adjusting acceptable risk levels and other rules. Businesses can determine the level of automation and control they desire in their solution, ensuring it meets their specific needs.
Accuracy	Exceptional	Kount is rated as one of the most accurate solutions among the vendors we analyzed, according to buyers. The company employs multiple types of machine learning to uncover contextual signals of fraudulent behavior; the additional intelligence helps clients to enhance their ATO protection.
Product Integration	Exceptional	Kount offers its product through a single API, allowing convenient integration with banks' internal systems. Customers have specifically rated Kount highly for its product integration capabilities relative to peer firms.
Buyer Satisfaction	Excellent	By offering highly accurate solutions and expert customer service to streamline implementations, Kount provides a product that buyers rate as highly satisfactory.



Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

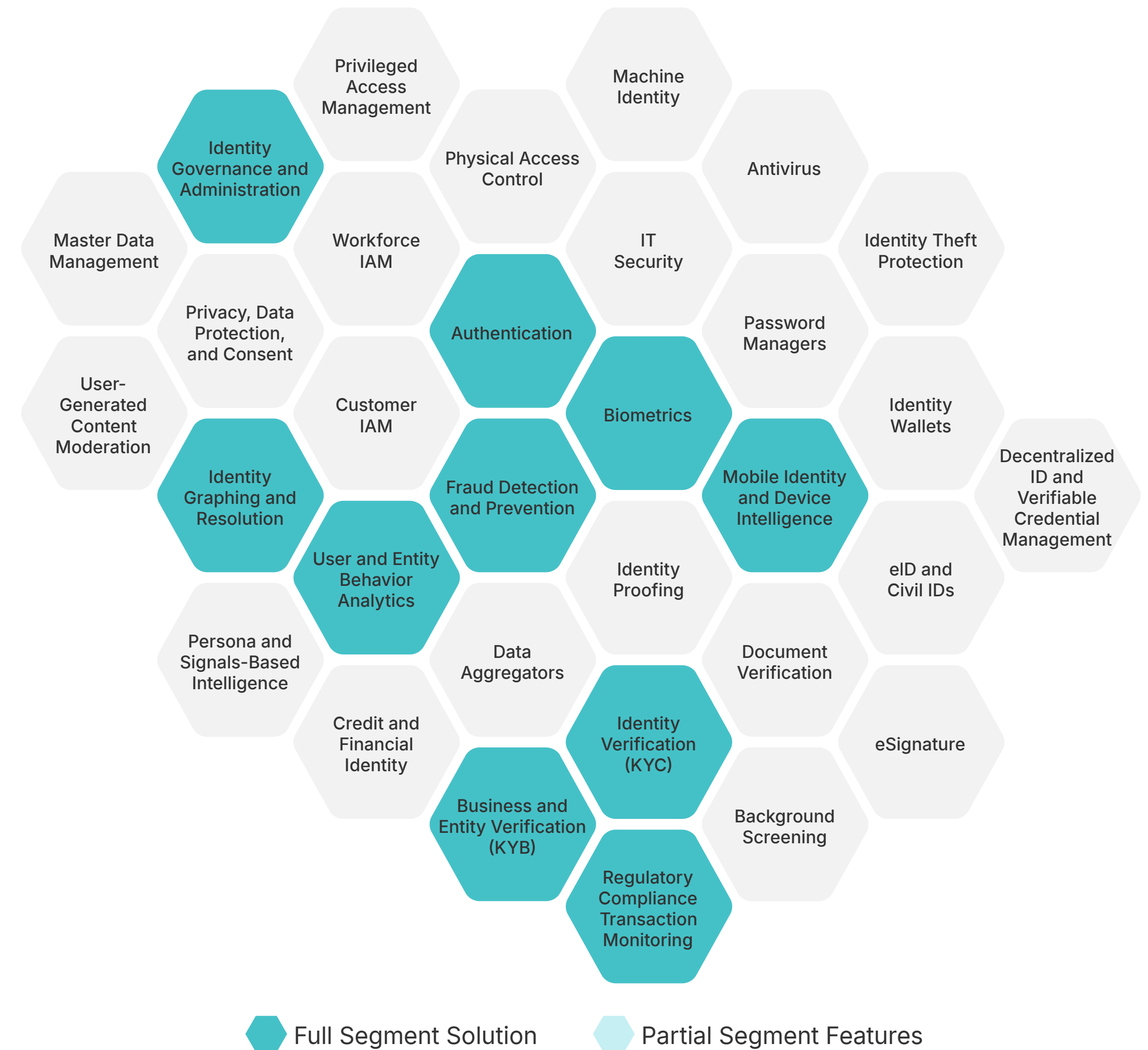
Analyst Notes on Kount 360

Kount 360 is a cloud-based platform that provides a complete suite of risk and compliance solutions. Kount 360 consolidates Kount's fraud prevention, identity verification, compliance, and payment solutions into one unified platform with a single user interface and API integration. This eliminates the need for businesses to manage multiple-point solutions, enabling operational efficiency. The platform offers end-to-end protection of the digital consumer journey by providing access to first-party data sources like device information, email insights, payment history, and more. Kount 360 leverages advanced artificial intelligence (AI) and machine learning (ML) models for data contextualization, scoring, and decision-making. This includes supervised and unsupervised learning models that promote stability, longevity, and relevance, reducing manual processes while enabling accurate and automated decisioning. Moreover, the platform has features allowing users and analysts to quickly develop rules and tailor fraud prevention strategies to their business needs. With a single API integration, Kount 360 can be easily integrated into existing systems, enabling businesses to protect their operations across the entire customer journey from a centralized platform.

LexisNexis Risk Solutions

LexisNexis Risk Solutions provides analytics and data solutions to help organizations detect and prevent fraud, ensure compliance, and make informed decisions. Utilizing vast data resources and sophisticated analytics, the company supports risk management across various sectors, including finance, healthcare, insurance, and government. LexisNexis Risk Solutions helps clients to reduce operational risks, navigate complex regulatory environments, and protect against evolving threats.

Company Information ¹	
Headquarters	Alpharetta, Georgia
No. of Employees	8800 as of May 2024
Last Raised	Funding Data Unknown
Primary Segment	Fraud Detection and Prevention, Background Screening, Regulatory Compliance and Transaction Monitoring, Authentication, Biometrics, Identity Verification (KYC), Business and Entity Verification (KYB), Identity Proofing, Master Data Management, Data Aggregators, Credit and Financial Identity, User And Entity Behavior Analytics
Vertical Focus	Financial Services, Government, Healthcare
Geographic Focus	North America, Europe, Middle East, Asia-Pacific
Notable Customers	 



(1) Link

LexisNexis Risk Solutions' Strategy

Strategy	Excellent	According to buyers, LexisNexis Risk Solutions offers end-customers one of the most frictionless user experiences among ATO solutions; this rests on highly effective behavioral signals.
Behavioral Capabilities	Exceptional	With its BehavioSec product, LexisNexis Risk Solutions offers one of the leading behavioral biometrics solutions on the market. This enables the company to effectively recognize when users are being coached or exhibiting unusual behavior.
Passwordless Authentication	Strong	LexisNexis primarily relies on behavioral signals to prevent fraud, forgoing passwordless authentication mechanisms like QR codes or passkeys. Instead, it utilizes advanced behavioral biometrics and behavioral analytics for ATO prevention.
Cost	Excellent	According to buyers, LexisNexis Risk Solutions offers exceptional cost effectiveness. This is particularly noteworthy given that behavioral biometric solutions are typically more expensive than other ATO solutions, indicating that the company delivers substantial value and ROI for its customers.
User Experience	Exceptional	According to the banking buyers we surveyed, LexisNexis Risk Solutions offers one of the best user experiences among all ATO prevention solutions. The company achieves this by using passive signals that operate in the background, avoiding friction-filled authentication methods.

Analyst Notes on Strategy

LexisNexis Risk Solutions has leveraged an acquisition strategy to continue adding new and emerging technologies to its product suite. In 2018, LexisNexis Risk Solutions acquired ThreatMetrix for about \$817 million. More recently, in 2022, LexisNexis Risk Solutions acquired BehavioSec, a highly predictive behavioral biometrics solution that uses behavior analysis for continuous authentication to establish identity trust and help prevent fraud. The acquisition of BehavioSec brought the ability to convert complex mobile signals from touchscreen and sensors into rules and advanced mobile behavioral biometric-based authentication capabilities, complementing the browser-based solutions within ThreatMetrix. By integrating offerings from BehavioSec into ThreatMetrix, customers will benefit from continuous authentication, advanced machine learning capabilities, and additional behavioral data for enhanced authentication processes.

LexisNexis Risk Solutions' focus on behavioral biometrics and frictionless authentication aligns with the benefits of passwordless flows. Integrating BehavioSec and ThreatMetrix provides a multi-layered approach to authentication, enabling organizations to distinguish between legitimate and potentially malicious users based on their behavioral patterns and digital identities while minimizing friction for genuine customers. However, they have not indicated plans to support integrating device-based or cloud passkeys as part of their authentication solutions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

LexisNexis Risk Solutions' Market Presence

Market Presence	Exceptional	LexisNexis is a large identity provider with a breadth of capabilities. The company has leveraged acquisitions to bolster their product offerings and grow their team continuously.
Brand Awareness	Exceptional	LexisNexis Risk Solutions is a well-established provider offering a variety of tools for financial service actions. It is highly recognized within the industry; 93% of financial service professionals surveyed are familiar with LexisNexis as a leading brand in preventing ATO fraud.
Market Leadership	Exceptional	Of the financial services practitioners familiar with LexisNexis, 71% regarded them as market leaders, the highest rate among all other leading vendors. This underscores their solution's efficacy in supporting financial institutions in mitigating ATO risk.
Market Penetration	Exceptional	LexisNexis has demonstrated market-leading penetration across global financial institutions as an incumbent solution provider. Leveraging advanced analytics, big data technology, and expansive identity intelligence, LexisNexis supports over 90% of the top 50 U.S. banks.
Company Size	Exceptional	LexisNexis, headquartered in New York City, employs over 8,000 people globally and operates in more than 150 countries. The company is a division of publicly traded RELX Group and continues to leverage acquisition strategies to grow its offerings and employee workforce.
Employee Growth	Strong	Over the last year, LexisNexis has acquired Henschman, a Belgium-based contract drafting legal technology company, and Human API, a provider of a consumer-driven data platform contributing to strong employee growth over the last year.

Analyst Notes on Market Presence

LexisNexis Risk Solutions is a global provider of information-based analytics and decision tools, operating as part of the Risk segment within RELX Group. With a workforce of 11,100 employees, LexisNexis Risk Solutions serves customers in more than 180 countries worldwide. In the fiscal year 2023, the company reported revenues of £3,133 million, representing a significant increase from £2,909 million in 2022 and £2,474 million in 2021. LexisNexis Risk Solutions derives most of its revenue from North America, accounting for 79%. In comparison, Europe contributes 14%, and the remaining 7% comes from the rest of the world.

LexisNexis Risk Solutions has a strong presence in the global market, serving 92% of the Fortune 100 companies, 84% of the Fortune 500 companies, nine of the world's top ten banks, and 21 of the world's top 25 insurers. The company's LexisNexis Digital Identity Network analyzes over 300 million transactions daily and over 100 billion transactions annually, showcasing its extensive reach and capabilities in fraud prevention and identity verification.

The company's revenue model is diversified, with subscription revenue representing 40% of the total and transactional revenues, including long-term contracts with volumetric elements, accounting for the remaining 60%. LexisNexis Risk Solutions operates across various market-facing industry verticals, including Business Services (around 45% of revenue), Insurance, Specialized Industry Data Services, and Government Solutions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

LexisNexis BehaviorSec

LexisNexis BehaviorSec provides behavioral biometrics solutions to enhance security and prevent fraud. It analyzes user interactions, such as typing patterns and mouse movements, to create unique user profiles and detect anomalies that indicate potential threats. The platform operates continuously in the background, ensuring minimal disruption to the user experience while maintaining high security. It integrates with existing systems to offer real-time risk assessments to prevent fraud.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

Product Visuals

LexisNexis Risk Solutions does not provide publicly available product visuals for BehaviorSec.

LexisNexis BehavioSec

Product	Excellent	BehavioSec is a leading provider of behavioral biometrics solutions, offering highly accurate detection of bad actors attempting ATO.
Product Capability	Strong	LexisNexis Risk Solutions, through BehavioSec offers including highly demanded features like social engineering and scam detection. It also provides advanced behavioral biometrics for enhanced security and user experience.
Scalability	Exceptional	LexisNexis Risk Solutions is a leading identity provider in the market, with extensive experience working with banking customers of all sizes. The company has demonstrated its capability to service a diverse range of clients as they expand, offering robust solutions to support their growth.
Customization	Exceptional	The company's behavioral biometrics solution analyzes the typical behavior of a bank's specific user base, ensuring that threat detection and ATO prevention are tailored specifically to the needs of banks.
Accuracy	Exceptional	BehavioSec offers one of the most sophisticated behavioral biometrics solutions on the market. It can distinguish between regular and abnormal behavior using various signals such as mouse patterns and keystroke dynamics, ensuring accurate and reliable user identification.
Product Integration	Exceptional	Despite behavioral biometric solutions generally requiring longer implementation times, buyers were highly satisfied with LexisNexis' integration process. They noted the ability to deploy solutions much faster than its competitors. Its API integration is also combined with ThreatMetrix.
Buyer Satisfaction	Exceptional	LexisNexis Risk Solutions achieves one of the highest buyer satisfaction rates among vendors due to its sophisticated behavioral biometrics solution. As banks increasingly integrate behavioral biometrics into their tech stacks, we expect this trend of high satisfaction to continue.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.



Analyst Notes on LexisNexis BehavioSec

LexisNexis Risk Solutions' BehavioSec is a behavioral biometrics solution that analyzes how users interact with their devices during online sessions. It creates unique user profiles by examining activity patterns such as typing speed, mouse movements, keystroke behavior, and phone tilt angles. The solution transparently evaluates risk throughout the user journey by analyzing subtle behavioral nuances exhibited during digital interactions, using machine learning to detect anomalies that may indicate fraudulent behavior. BehavioSec generates a near real-time "authenticity score" for each session by assessing environmental risk factors and behavioral intelligence signals. This score helps organizations distinguish between legitimate and potentially malicious users. The solution is designed to complement and integrate with LexisNexis' existing digital identity intelligence solutions like ThreatMetrix, providing a multi-layered defense that combines behavioral biometrics with device intelligence, email risk, phone risk, and other fraud signals for enhanced risk assessment.

By recognizing good, returning customers based on their behavioral patterns, BehavioSec enables a seamless authentication experience without added friction for legitimate users. At the same time, it helps organizations identify fraudsters, distinguish between human and bot activity, detect session anomalies, and reliably profile high-risk users based on their behavioral footprints. BehavioSec does not capture passwords or personally identifiable information, ensuring data protection and privacy compliance from the initial stage. BehavioSec is fully integrated into LexisNexis' ThreatMetrix platform, an enterprise solution for global digital identity intelligence and authentication. It adds a layer of defense by analyzing user interactions, enabling more reliable fraud decisions across account openings, logins, payments, and other high-risk touchpoints.

Mastercard

Mastercard is a global technology company in the payments industry that provides a wide range of financial services. Primarily known for its payments card network, Mastercard offers solutions for credit, debit, and prepaid cards, digital payment platforms, and cybersecurity. Mastercard focuses on enabling secure, convenient, and efficient transactions for consumers, businesses, and governments worldwide. The company also offers fraud detection and ATO prevention solutions.

Company Information ¹	
Headquarters	Purchase, New York
No. of Employees	36686 as of May 2024
Last Raised	Public company
Primary Segment	Fraud Detection and Prevention, Regulatory Compliance Transaction Monitoring, Mobile Identity and Device Intelligence, Credit and Financial Identity, Identity Wallets, Identity Theft Protection
Vertical Focus	Financial Services, Fintech
Geographic Focus	North America, Europe, Middle East, Asia-Pacific
Notable Customers	 



(1) Link

Mastercard's Strategy

Strategy	Excellent	Mastercard provides protection throughout the customer lifecycle, offering both behavioral signals and passwordless authentication solutions.
Behavioral Capabilities	Excellent	Mastercard leverages behavioral signals to protect banking customers from ATO attacks. These signals are provided throughout the customer lifecycle, offering robust coverage across various threat vectors.
Passwordless Authentication	Excellent	Mastercard offers passkeys for passwordless authentication and specifically provides FIDO2 authentication for customers looking to transition away from high-friction, low-security passwords.
Cost	Strong	Mastercard is considered expensive compared to other ATO solutions on the market. However, the company offers highly scalable solutions, indicating that its cost structures are favorable for large user counts and transaction volumes, though it may be more costly for smaller banking customers.
User Experience	Excellent	Mastercard aims to provide comprehensive coverage across the customer lifecycle, from onboarding to login to transactions. By offering passive signals throughout this entire process, the product ensures an excellent user experience that satisfies customers.

Analyst Notes on Strategy

Mastercard's Account Protection solution employs advanced behavioral analytics and machine learning capabilities to safeguard customer accounts from identity theft and unauthorized access.

At its core is NuDetect, a fraud detection tool that utilizes behavioral analytics to identify and mitigate sophisticated automated attacks, including those targeting mobile devices. NuDetect analyzes behavioral patterns and signals to detect anomalies indicating fraudulent activities, such as account takeover attempts. It can identify bots mimicking human behavior by using different IP addresses multiple times daily, a tactic commonly employed in automated attacks.

In addition to behavioral analytics, Mastercard's Account Protection solution leverages other security measures like end-to-end encryption, tokenization, and authentication protocols. This multi-layered approach secures the entire payments ecosystem, spotting unusual activity patterns and identifying fraud before it reaches businesses.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Mastercard's Market Presence

Market Presence	Exceptional	Mastercard is among the top two most recognized brands and market leaders compared to other leading vendors – they have a significant market presence and strong growth metrics.
Brand Awareness	Exceptional	As a large consumer-facing card network, Mastercard benefits from leading brand awareness with 99% of surveyed financial services practitioners familiar with their brand and solutions for fraud. Their Zero Liability policy and partnerships with major financial institutions, make it a trusted leader in safeguarding digital transactions globally.
Market Leadership	Exceptional	Mastercard has established itself as a market leader in fraud prevention by leveraging advanced AI technologies and launching innovative solutions. Of those practitioners that were familiar with their brand 70% recognize them as market leaders – the second highest recognition of any other leading vendor.
Market Penetration	Exceptional	Mastercard has achieved extensive market penetration in the financial services sector, providing secure and efficient payment solutions to over 210 countries and territories worldwide. Moreover, Mastercard's participation in the Global Anti-Scam Alliance (GASA) underscores its commitment to combating global scams and protecting consumers from financial fraud.
Company Size	Exceptional	Mastercard, headquartered in Purchase, New York, employs over 30,000 people globally, reflecting its significant market. The company reported an annual revenue of \$25.1 billion in 2023, underscoring its substantial operational scale.
Employee Growth	Excellent	The company experienced significant layoffs in February 2024, affecting various departments. Nonetheless, they've experienced significant YoY employee growth – roughly 25%.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Market Presence

Mastercard has established itself as a leading provider of fraud prevention and cybersecurity solutions in the global payments industry. With its extensive network and insights derived from processing billions of transactions annually, Mastercard leverages advanced technologies like artificial intelligence (AI) and machine learning to combat various types of fraud across multiple channels. Mastercard provides a comprehensive suite of fraud monitoring and management tools, including web security protocols, verification tools, and remediation plans to help merchants develop effective risk management strategies and maintain compliance with fraud thresholds set by card networks.

Mastercard subsidiary NuData Security is a leading provider of behavioral biometrics and behavioral analytics solutions for fraud prevention and user verification. NuData Security's solutions are used by companies across various industries, with a notable presence in the financial services sector, which accounts for 14% of their customer base. The company has a strong foothold in the United States, where 54% of its customers are located, followed by the United Kingdom (10%) and Australia (7%). NuData Security caters to a diverse range of clients, with 49% of their customers being small businesses (fewer than 50 employees), 18% medium-sized, and 21% large enterprises (over 1,000 employees). Additionally, most (61%) of NuData Security's customers have revenues below \$50 million, while 24% are large companies with revenues exceeding \$1 billion.

With a strong focus on innovation and leveraging cutting-edge technologies like AI and machine learning, Mastercard has solidified its position as a trusted partner for businesses worldwide looking to address payments, fraud, and related use cases.

Mastercard Account Protection

Mastercard Account Protection offers comprehensive solutions to prevent account takeover and safeguard digital identities. The platform helps businesses protect user accounts from attacks by integrating sophisticated detection tools and ensuring compliance with global security standards. The solution offers coverage across customer lifecycle events including account onboarding and account login.

ATO Prevention Product Capability Coverage¹

H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

Product Visuals

Mastercard does not provide publicly available product visuals for Account Protection.

Mastercard Account Protection

Product	Excellent	Mastercard provides highly scalable solutions that large enterprises can utilize to prevent various ATO threats.
Product Capability	Excellent	Mastercard provides biometric authentication, which is the most highly demanded feature according to banking buyers. It also includes device risk scoring, location intelligence, and other distinguishing capabilities to complete its ATO prevention suite.
Scalability	Exceptional	Mastercard is one of the largest payment processors globally, partnering with major banking customers. As it continues to build out its identity solutions, its extensive experience enables it to provide highly scalable solutions to meet the needs of its clients.
Customization	Excellent	By offering solutions that span the entire customer lifecycle, Mastercard allows clients to select specific capabilities for particular stages, catering to unique organizational needs.
Accuracy	Excellent	Account Protection utilizes capabilities such as bot detection, proxy and VPN detection, and location intelligence. By applying behavioral analytics to identify anomalies, it assesses the likelihood of customers committing fraud.
Product Integration	Excellent	Buyers noted that Mastercard offers excellent product integration, allowing customers to implement their ATO prevention solutions without significant engineering disruptions or long wait times.
Buyer Satisfaction	Excellent	Mastercard offers comprehensive coverage beyond transaction-level, encompassing everything from account opening to authentication. Their extensive protection and strong brand reputation contribute to a high buyer satisfaction score.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Mastercard Account Protection

Mastercard's Account Protection solution aims to safeguard customer accounts from identity theft and unauthorized access, providing comprehensive security measures from account opening to login. This solution leverages Mastercard's digital identity solutions and insights to protect against sophisticated account takeover attacks and fraudulent activities. At the core of Account Protection is NuData NuDetect, an advanced fraud detection tool that utilizes machine learning and behavioral analytics to identify and mitigate automated attacks, including those targeting mobile devices.

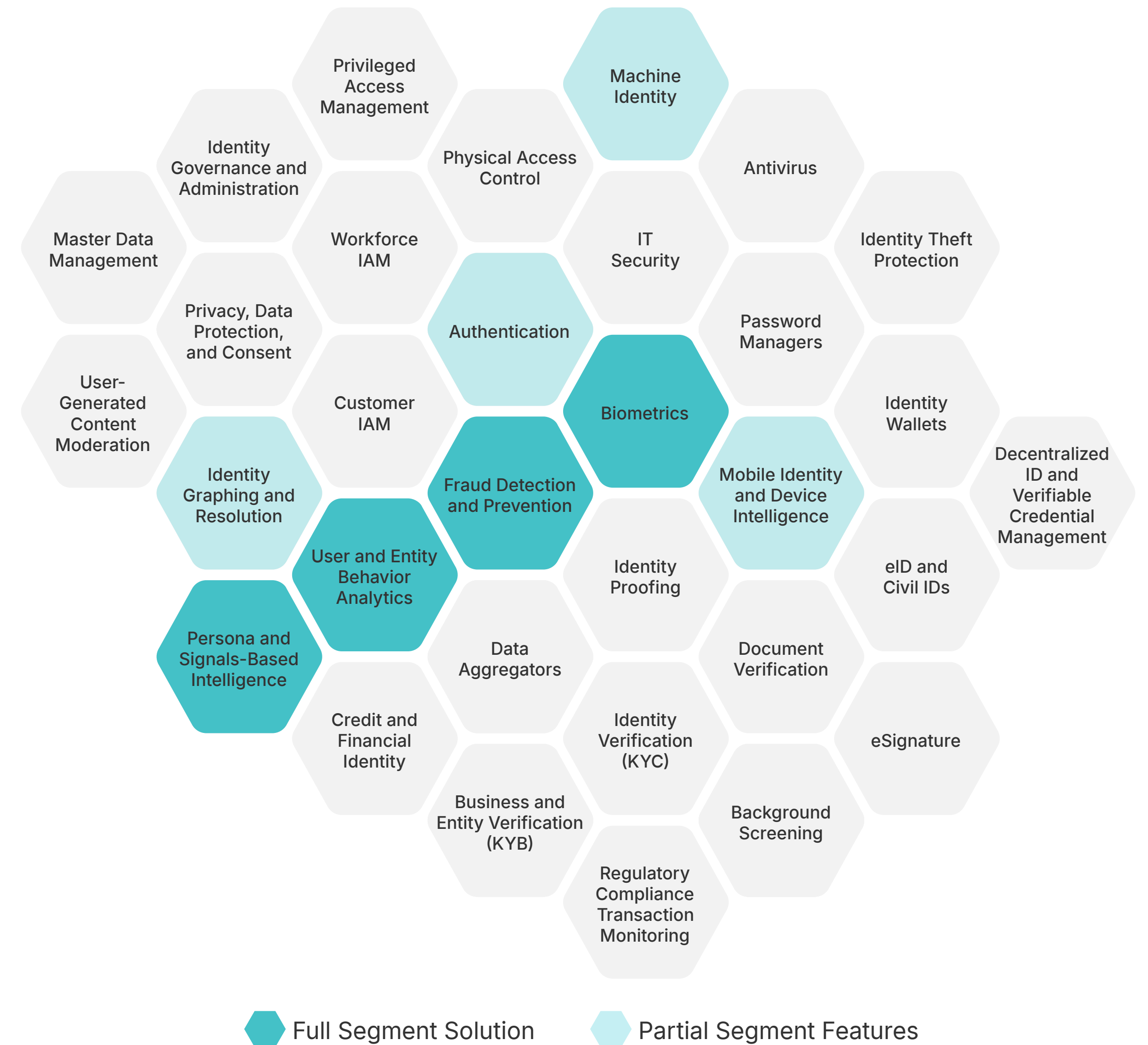
Mastercard's Account Protection solution combines NuDetect's fraud detection capabilities with other security measures, such as end-to-end encryption, tokenization, and authentication protocols. This multi-layered approach ensures the entire payments ecosystem is secured, spotting unusual activity patterns and identifying fraud before it reaches businesses. With Account Protection, Mastercard provides financial institutions and merchants with a comprehensive suite of tools to protect customer accounts from sign-up to sign-in, mitigating the risks of identity theft and unauthorized access while maintaining a seamless user experience.

NeuroID

NeuroID specializes in behavioral analytics, which detects and prevents fraud by analyzing user interactions and patterns in real-time. Their platform identifies anomalies in user behavior during account onboarding, login, and transactions to mitigate risks from bots, fraud rings, and other malicious activities. By leveraging advanced data analysis, NeuroID provides businesses with actionable insights to enhance security and reduce fraud without compromising the user experience.

Company Information ¹	
Headquarters	Whitefish, Montana
No. of Employees	60 as of May 2024
Last Raised	\$35M, Series B Round in November 2021
Primary Segment	User and Entity Behavior Analytics
Vertical Focus	Financial Services, Fintech, eCommerce, Gaming
Geographic Focus	North America, Europe, Latin America
Notable Customers	NeuroID does not publicly disclose banking customers

(1) Link



NeuroID's Strategy

Strategy	Excellent	NeuroID is a specialized vendor offering robust behavioral capabilities to detect and prevent account takeovers.
Behavioral Capabilities	Exceptional	NeuroID is a vendor specializing in leveraging behavioral signals for advanced fraud prevention and detection. It offers one of the most robust behavioral capability suites in the ATO prevention market, effectively guarding against social engineering, phishing, and other account takeover threats.
Passwordless Authentication	Strong	NeuroID does not offer passwordless authentication capabilities such as passkeys. Instead, the company focuses on leveraging behavioral signals to provide sophisticated threat detection. By analyzing these signals, NeuroID can effectively prevent account takeovers and offer advanced protection against various threats.
Cost	Strong	As a point solution, NeuroID is often integrated into tech stacks alongside several other vendors. Current customers have indicated that they find it less cost-effective than other solutions on the market that offer more expansive product capability sets.
User Experience	Strong	NeuroID uses passive signals for threat detection, operating in the background of user sessions to identify risks. However, current customers have noted lower levels of satisfaction with the company's user experience compared to other ATO prevention vendors.

Analyst Notes on Strategy

NeuroID does not offer authentication capabilities like passwords, biometrics (fingerprints, facial recognition, etc.), or multi-factor authentication. Instead, its solution focuses on behavioral analytics and behavioral biometrics to assess user intent and identify potential fraud threats. NeuroID analyzes real-time user interactions like keystrokes, mouse movements, typing patterns, hesitation, and navigation behavior to establish behavioral profiles and detect anomalies that may indicate fraudulent activity. NeuroID analyzes real-time user interactions like keystrokes, mouse movements, typing patterns, hesitation, and navigation behavior to establish behavioral profiles and detect anomalies that may indicate fraudulent activity. These capabilities also help to identify potential bots through their focus on detecting "inhuman" behaviors.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

NeuroID's Market Presence

Market Presence	Strong	NeuroID is a leader in the behavioral analytics market with strong partnerships across financial institutions, powering Experian's CrossCore solution with their behavioral analytics.
Brand Awareness	Strong	NeuroID is a leader in the fraud prevention and behavioral analytics market, however their solutions are primarily leveraged at account opening. Nonetheless, 52% of surveyed practitioners in financial services were familiar with the brand and solution for ATO prevention.
Market Leadership	Strong	Of those practitioners who were familiar with the NeuroID brand and their ATO prevention solution, 18% recognized them as market leaders, signifying that the market understands and highly values their behavioral analytics.
Market Penetration	Excellent	NeuroID has made significant inroads in the financial services sector by providing real-time behavioral analytics solutions that enhance fraud detection and customer onboarding. The company's innovative technology, which captures and interprets digital behaviors, has been adopted by major financial institutions.
Company Size	Strong	NeuroID, headquartered in Whitefish, Montana, employs 60 people and operates across three locations in the United States. The company has raised \$42 million in funding and can leverage this capital to make strategic hires and capture new business.
Employee Growth	Strong	NeuroID's workforce decreased by about 20% over the past year, a trend seen across many companies in the industry due to tough economic conditions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Market Presence

NeuroID is a leading company in the behavioral analytics space, providing solutions to detect fraud and understand customer intent and behavior during digital interactions. The company has experienced rapid growth in recent years. NeuroID secured \$35 million in Series B funding led by Canapi Ventures in November 2021, building on a \$7 million Series A round in December 2020. This significant funding indicates investor confidence in NeuroID's market potential. As of early 2022, NeuroID reported triple-digit year-over-year revenue growth, boasting a competitive customer list including Intuit, Square, Affirm, and OppFi.

At the end of 2023, NeuroID announced a partnership with Experian to integrate its behavioral analytics capabilities into Experian's CrossCore and PreciseID solutions. Similarly, NeuroID has partnered with TransUnion since 2020. NeuroID's partnership strategy has allowed it to showcase its expertise in behavioral analytics and support enterprise clients in managing their customers' risk within an end-to-end solution flow.

NeuroID Account Defense

NeuroID Account Defense uses behavioral analytics and device intelligence to detect and prevent fraud across login, account management, and transactions. Analyzing user behavior and device signals identifies anomalies that indicate potential fraud, even when valid credentials are used. This platform helps distinguish between legitimate users and fraudsters, ensuring secure access while minimizing user friction. It is designed to protect against various threats, including scripting attacks, account takeovers, money mules, and scams.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from public sources (link: <https://www.alloy.com/partners/neuroid>).

Product Visuals²



NeuroID Account Defense

Product	Strong	NeuroID offers sophisticated behavioral analysis for ATO prevention, which customers find highly customizable.
Product Capability	Excellent	NeuroID provides advanced behavioral analysis through behavioral biometrics, location intelligence, and device risk scoring. Additionally, it offers social engineering and scam detection, one of the most highly demanded capabilities.
Scalability	Strong	While NeuroID was considered less scalable in the eyes of banking customers when compared to others, this may be misleading because of their use of channel partners. Specifically, NeuroID works with Experian, one of the largest credit bureaus in the world, and provides highly scalable solutions.
Customization	Excellent	NeuroID offers a wide range of capabilities that can be tailored to address specific ATO threats. The company plans to begin customizing risk scores based on industry segment in the near future.
Accuracy	Strong	NeuroID utilizes behavioral biometrics to deliver advanced threat detection. This is particularly beneficial for banks, as behavioral biometrics systems improve over time by creating unique user profiles across multiple sessions, which is common in banking.
Product Integration	Strong	NeuroID offers API integration for its services, allowing multiple calls during a user session. The company collaborates with both channel partners and large financial institutions that have substantial engineering resources.
Buyer Satisfaction	Strong	NeuroID's passive signals detect bots and other malicious behavior that could lead to financial losses, operating in the background to enhance the customer experience. This vendor is a strong option for banks seeking to supplement their current vendor stack with sophisticated behavioral and device signals.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on NeuroID Account Defense




NeuroID's Account Defense Solution is a behavioral analytics platform that protects customers across login, account management, and transactions by detecting suspicious user behavior and potential fraud threats. It analyzes user behavior during the login process, looking for anomalies in patterns such as typing cadence, mouse movements, and hesitation to differentiate legitimate users from fraudsters using stolen credentials or bots attempting brute-force attacks.

Even if a fraudster gets past the login stage, NeuroID monitors user behavior within the account, detecting unusual activities like atypical profile changes, navigation patterns, or mismatches between stated user details and observed behavior to identify account takeover attempts. The solution extends its behavioral monitoring to transaction processes like payments, transfers, and purchases, analyzing user interactions to flag potential fraud, such as uncharacteristic transaction amounts, deviations from typical patterns, or signs of automation.

A key advantage of NeuroID's solution is its invisible fraud detection layer that operates in the background, collecting behavioral data without any user friction or additional authentication steps. This allows for a seamless customer experience while enhancing fraud detection capabilities. NeuroID's Account Defense Solution complements existing fraud prevention tools by providing an additional layer of behavioral intelligence, helping organizations reduce fraud losses, minimize manual review costs, and streamline processes by accurately identifying genuine users and malicious actors across the entire customer journey.

Outseer

Outseer specializes in fraud prevention and risk management solutions, focusing on protecting digital transactions from login to payment. Outseer offers products like Outseer 3-D Secure, Outseer Fraud Manager, and Outseer FraudAction, designed to detect and mitigate fraud while maintaining a seamless user experience.

Company Information ¹	
Headquarters	Palo Alto, California
No. of Employees	224 as of May 2024
Last Raised	Spun off from RSA Security in 2021
Primary Segment	Fraud Detection and Prevention
Vertical Focus	Financial Services, eCommerce
Geographic Focus	North America
Notable Customers	  



(1) Link

Outseer's Strategy

Strategy	Strong	Strong passwordless authentication mechanisms enable Outseer to provide robust security against account takeover threats.
Behavioral Capabilities	Strong	Outseer predominantly leverages authentication mechanisms to ensure protection against account takeover threats. The company does not offer behavioral biometrics, behavioral analytics, or bot detection, focusing instead on robust authentication solutions to secure user accounts.
Passwordless Authentication	Exceptional	Outseer leverages WebAuthn and QR code authentication to provide passwordless options for its banking customers. These solutions help institutions move away from cumbersome passwords, which users often find difficult to remember and inconvenient.
Cost	Excellent	The company received strong satisfaction scores from its current customers regarding its solutions' cost-effectiveness. By offering protection throughout the user lifecycle, from login to transaction, the platform supports a wide range of use cases in addition to ATO prevention.
User Experience	Excellent	Outseer received strong user experience ratings from current banking customers. The company highlights that only a very small portion of their overall cases require intervention, leading to limited friction and minimal user drop-off.

Analyst Notes on Strategy

Outseer leverages advanced authentication techniques to prevent against ATO and provide continuous authentication capabilities. Banking buyers note strong user experience, indicating their background analysis limits friction.

Outseer also provides robust passwordless authentication capabilities - they have integrated support for FIDO passwordless authentication standards like FIDO2 and WebAuthn to enhance security during registration and authentication flows. Moreover, as part of their Fraud Manger solutions they offer risk-based authentication that can trigger step-up authentication based on risk policies.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Outseer's Market Presence

Market Presence	Excellent	Outseer was spun off of RSA Security to be a standalone company focused on fraud detection for financial services; as such, they've garner strong brand awareness and market leadership.
Brand Awareness	Excellent	Outseer has significantly increased its brand awareness in the cybersecurity and fraud prevention market through a strategic PR campaign that resulted in 85 media placements within the first year, including top-tier outlets like ZDNet, TechRadar, and Forbes. As a result, about 63% of surveyed financial services practitioners were familiar with their brand and fraud solutions.
Market Leadership	Strong	The company's solutions, such as Fraud Manager, 3-D Secure, and FraudAction, have cemented its leadership in the fraud market—of those participants who were familiar with its brand and solutions, about 22% recognized it as market leader.
Market Penetration	Excellent	Outseer's advanced fraud detection capabilities, including active call detection and enriched instant payment details, have made it a trusted partner for major banks and payment providers in combating sophisticated fraud schemes.
Company Size	Excellent	Outseer was spun off from RSA Security in June 2021, becoming a standalone company focused on fraud and risk intelligence to better serve its financial and digital payments client, as such they company has grown to employ over 200 people across its headquarters in Bedford, Massachusetts, and additional offices in key regions such as London, Melbourne, Mumbai, and Toronto.
Employee Growth	Strong	Outseer experienced modest employee growth, increasing its workforce by 1% over the last year, bringing the total number of employees to 224. This growth reflects the company's steady expansion and commitment to enhancing its fraud prevention and risk management solutions.

Analyst Notes on Market Presence

Outseer was founded as a spin-out from RSA Security's Fraud & Risk Intelligence business unit - it was launched in June 2021 when RSA Security transitioned its Fraud & Risk Intelligence business into a new standalone company. This move followed RSA Security's acquisition by Symphony Technology Group in 2020, which valued RSA at \$2.1 billion. Outseer originated from RSA's decades-long heritage and innovations in anti-fraud and payment authentication solutions. Today, Outsider protects over 450 million cards and bank accounts annually, and safeguards over \$5 trillion in annual payment transaction value. The company has garnered high market visibility relative to its age, and has achieved medium size for the companies featured in this report.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Outseer Fraud Manager

Outseer Fraud Manager is a risk management platform that uses, assesses, and mitigates fraud during digital interactions; Outseer concentrates on the customer journey between login and transaction. It integrates first-party and third-party data to enhance risk scoring and provides policy and case management features for effective fraud prevention. The platform supports cloud and on-premise deployment options, ensuring flexible integration with existing systems to protect against evolving fraud threats.

ATO Prevention Product Capability Coverage¹

H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from company website (link: <https://www.outseer.com/products/outseer-fraud-action/>).

Product Visuals²



Outseer Fraud Manager

Product	Strong	Outseer provides scalable and accurate authentication solutions to prevent ATO.
Product Capability	Strong	Outseer offers a more limited range of product capabilities compared to other vendors we profiled. However, its continuous authentication capabilities are among the most sought-after, with particularly high adoption rates among large banks.
Scalability	Excellent	Outseer has demonstrated its ability to work with regional, national, and multinational banks, offering scalable solutions for all three. Buyers highly regard its scalability compared to other vendors we profiled.
Customization	Excellent	Outseer provides a KPI dashboard that highlights key fraud metrics such as detection rates and transaction volumes. This feature allows banking customers to track operational costs and return on investment effectively.
Accuracy	Excellent	The company utilizes a diverse array of data signals for precise detection, including its global data network as well as third-party and first-party signals, to protect against a wide range of ATO threats.
Product Integration	Strong	Customers can use Outseer's configuration management to modify and adjust parameters that influence the experience of internal banking risk teams, with the goal of reducing operational costs.
Buyer Satisfaction	Excellent	Outseer Fraud Manager offers comprehensive coverage from login to payment, addressing a significant portion of the customer lifecycle. It is particularly appealing to banks seeking extensive use case coverage.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.




Analyst Notes on Outseer Fraud Manager

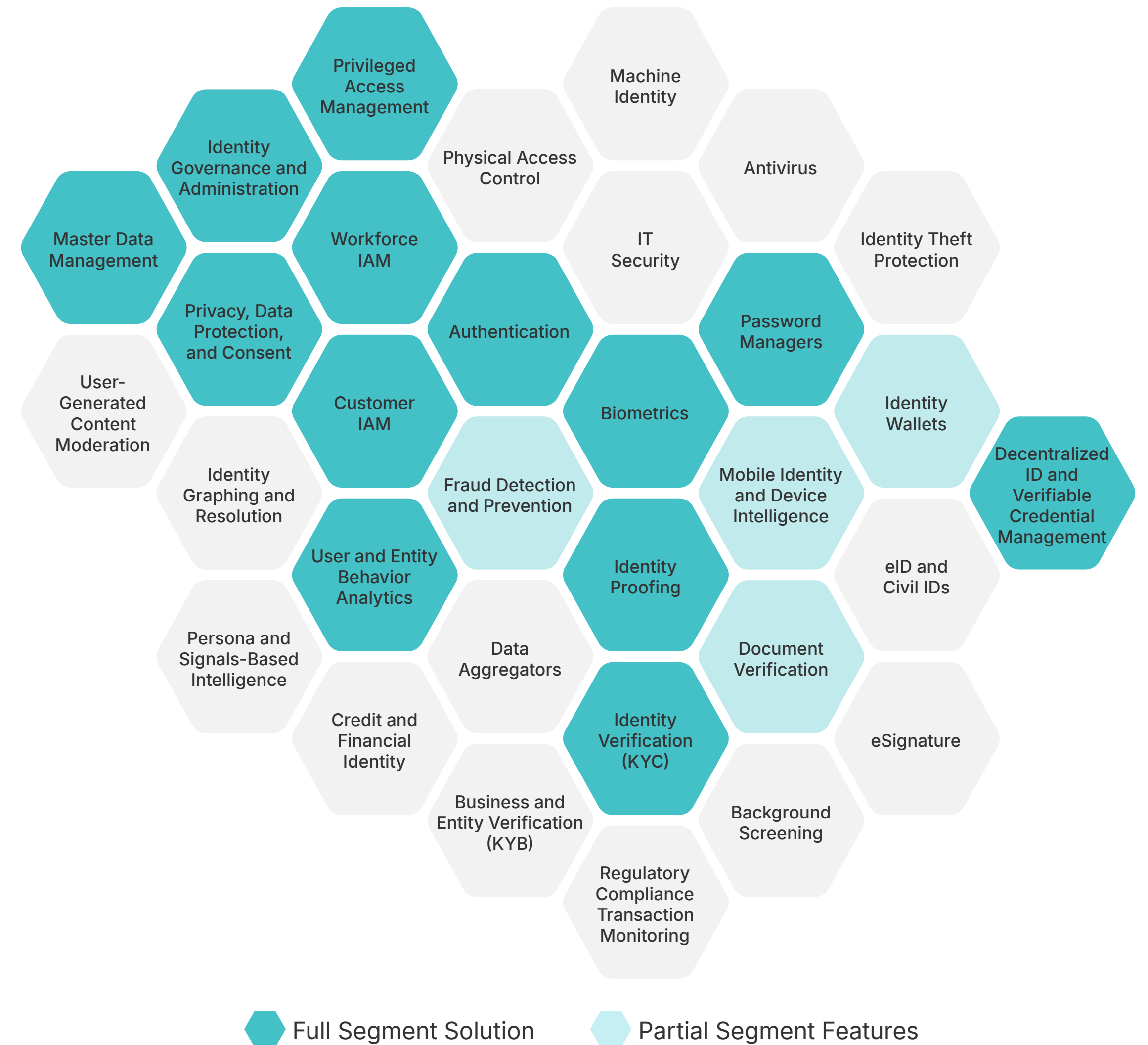
Outseer Fraud Manager is a transactional risk management platform designed to protect digital interactions from login to payment completion. Utilizing advanced machine learning and a robust policy management system, the platform safeguards over \$5 trillion in transaction value annually and processes more than 120 billion transactions and digital interactions each year.

Outseer Fraud Manager uses data science approaches on top of its consortium data to defend against evolving fraud trends, employing risk models trained on billions of transactions from the world's largest financial institutions. It integrates risk scoring by ingesting first- and third-party data signals, enabling consistent risk controls across all customer touchpoints. The solution also offers flexible deployment options, including cloud and on-premises, and features such as step-up authentication for high-risk transactions, policy management for setting granular rules, and case management for tracking and confirming fraudulent activities. This holistic approach ensures optimized customer experience and operational efficiency, making Outseer Fraud Manager a trusted solution for fraud prevention in high-threat environments.

Ping Identity

Ping Identity provides enterprise identity security solutions, offering secure access and authentication across digital platforms. Their services include single sign-on (SSO), multi-factor authentication (MFA), and identity governance to protect user identities and ensure compliance. Ping Identity focuses on enabling organizations to manage identities, prevent fraud, and implement zero-trust security models.

Company Information ¹	
Headquarters	Denver, Colorado
No. of Employees	1932 as of May 2024
Last Raised	\$35M, Series F Round in September 2014
Primary Segment	Workforce IAM, Customer IAM, User and Entity Behavior Analytics, Authentication, Identity Governance and Administration, Decentralized Identity and Verifiable Credential Management
Vertical Focus	Financial Services, Automotive, Retail, Government, Healthcare
Geographic Focus	North America, Europe, Middle East, Africa, Asia-Pacific
Notable Customers	  



(1) Link

Ping Identity's Strategy

Strategy	Excellent	Ping offers both behavioral capabilities and passwordless authentication options, providing a strong user experience with various pricing tiers.
Behavioral Capabilities	Excellent	Ping offers behavioral biometrics to track users across sessions, effectively preventing fraud by detecting anomalies against baseline behavior. Additionally, it efficiently detects and prevents bots from breaching accounts and causing financial losses.
Passwordless Authentication	Excellent	Ping Identity offers QR code authentication, providing customers with a highly secure, passwordless authentication solution. This capability protects against various ATO threats and reduces financial risk.
Cost	Excellent	Ping Identity offers three pricing tiers: Essential (starting at \$20,000 per year), Plus (starting at \$40,000 per year), and Premium (custom pricing for enterprises). Banking customers regard the company as providing exceptional cost-effectiveness compared to other solutions.
User Experience	Excellent	By offering behavioral biometrics alongside traditional authentication mechanisms, Ping effectively provides passive signals that operate in the background without causing unnecessary user friction during the login or transaction processes throughout the customer lifecycle.

Analyst Notes on Strategy

The Ping Identity Platform can easily integrate with other Ping Identity modules to deliver comprehensive capability coverage across fraud detection and authentication.

The PingOne Protect module evaluates multiple risk signals, including user and entity behavior analytics, to calculate an overall risk score for each end-user. PingOne Protect incorporates behavioral biometrics as a risk signal for risk scoring and fraud detection. The solution can identify fraudulent activity anomalies by analyzing behavioral biometrics, such as typing patterns, mouse movements, and device interactions.

The PingMFA module offers robust passwordless authentication capabilities across its identity and access management solutions. The company supports passwordless multi-factor authentication (MFA), enabling organizations to leverage more than one advanced authentication mechanism, such as biometrics, device trust, and risk policies, to verify users without relying on traditional passwords. Biometrics, including facial recognition and fingerprint scans, can be configured as the primary authentication factor, reducing the reliance on passwords altogether.

Ping Identity's solutions comply with the FIDO open standard, which helps prevent phishing attacks by leveraging trusted devices for authentication. The company aims to remove passwords from account creation processes, advancing registration, verification, and continuous authentication processes to enable passwordless experiences from the outset.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Ping Identity's Market Presence

Market Presence	Exceptional	Ping Identity has grown to become a large identity provider following its acquisition by Thoma Bravo and merger with ForgeRock.
Brand Awareness	Excellent	Ping Identity's platform solution is highly recognized among practitioners, with 64% of surveyed financial services practitioners aware of the brand. This widespread recognition has been amplified by the company's nearly \$3 billion acquisition by Thoma Bravo in 2022.
Market Leadership	Excellent	Ping is frequently mentioned in analyst briefings as a leading competitor in the IAM space, known for the comprehensiveness of its solution suite. This is further amplified with its recent merger with ForgeRock, which has broadened Ping's market leadership, capturing 27% of practitioner sentiment.
Market Penetration	Excellent	Ping Identity has made significant inroads among global enterprises, servicing 59% of the Fortune 100 and facilitating hundreds of millions of authentications daily for its major banking clients. Ping has proven its ability to address the needs of businesses of all sizes, with particular strength in meeting larger enterprises' scalability and complex integration requirements.
Company Size	Exceptional	Following its merger with ForgeRock, Ping now has 1,932 employees and twice the number of developers, with offices in the United States, Canada, India, Israel, Singapore, and the United Kingdom.
Employee Growth	Strong	Ping has experienced a substantial 21% increase in its workforce over the last year, primarily fueled by a 56% growth in its sales team.

Analyst Notes on Market Presence

Ping Identity was established in Denver, Colorado, in 2002 as an enterprise-focused IAM vendor. Over the next decade, the company secured multiple funding rounds, notably receiving \$35 million from KKR to cultivate its market presence in the emerging IAM space. In 2016, Vista Equity Partners acquired a majority stake in Ping Identity through a leveraged buyout, providing the company with enhanced financial backing and strategic support to expand its market presence. This partnership proved fruitful, as Ping Identity went public successfully in 2019 under Vista's guidance.

Thoma Bravo acquired Ping Identity in 2022 for \$2.8 billion in an all-cash transaction and later announced the integration of ForgeRock into Ping Identity following its acquisition of ForgeRock. Moreover, Ping Identity serves as a trusted partner to some of the world's largest organizations, including nine of the top nine U.S. retail banks, seven of the nine CMA9 U.K. retail banks, eight of the 10 top global healthcare companies, six of the 10 top North American retailers, and all of the top 10 information and manufacturing companies.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Ping Identity Platform

The Ping Identity Platform is a comprehensive, AI-driven digital solution that empowers organizations to manage the full lifecycle, provide secure access, and govern any identity, enabling them to orchestrate personalized user experiences while safeguarding users and resources. The Ping Identity Platform delivers strong user experiences for any identity type across the workforce, customers, partners, and B2B users.

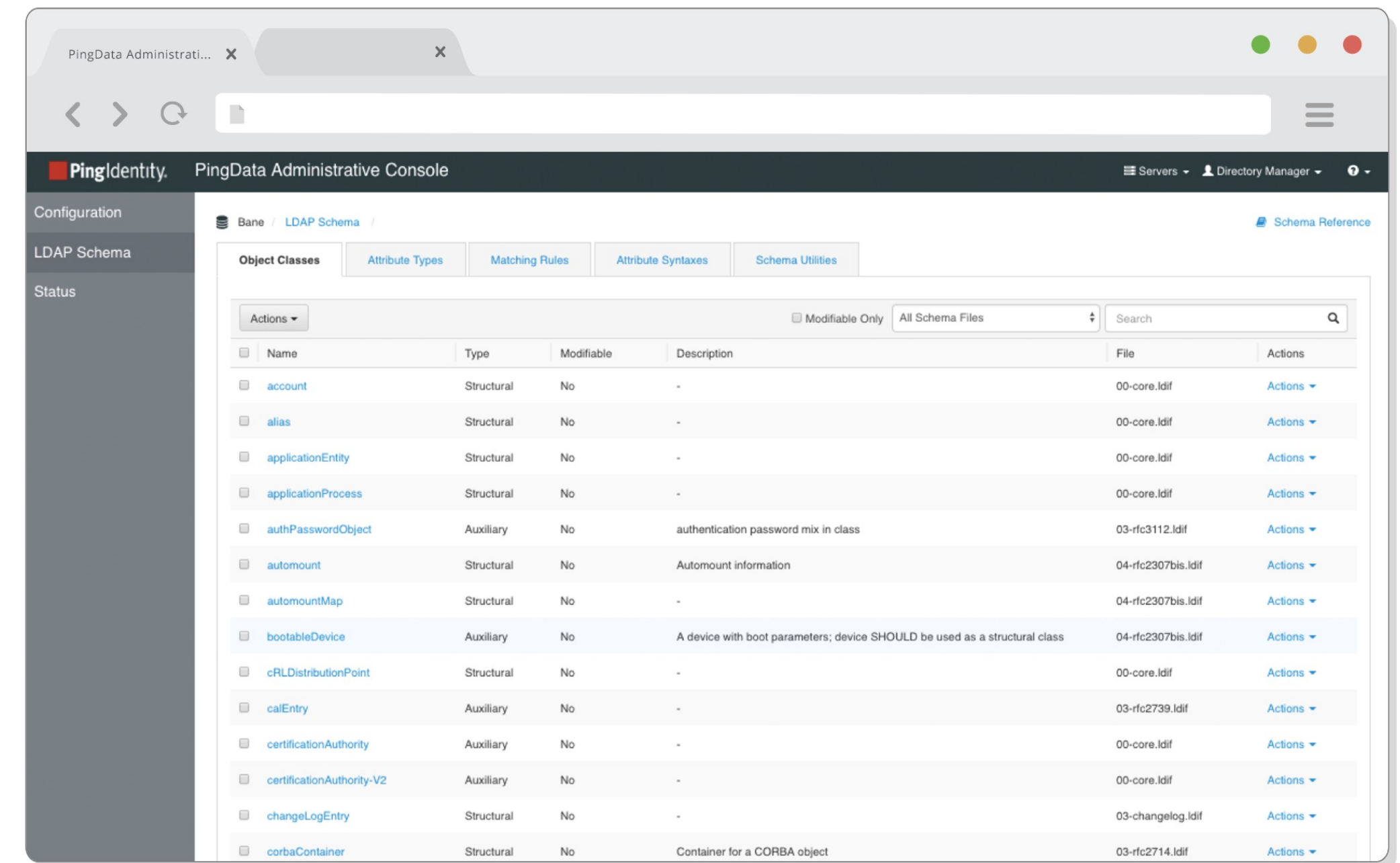
ATO Prevention Product Capability Coverage¹

H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from public sources (link: <https://www.softwareadvice.com/authentication/pingidentity-profile/>).

Product Visuals²



Ping Identity Platform

Product	Exceptional	Ping Identity offers one of the most comprehensive capability sets, providing highly scalable and accurate solutions for banks.
Product Capability	Exceptional	The Ping platform offers one of the most comprehensive authentication product suites we analyzed. It includes app-based authentication, biometric authentication, continuous authentication, SMS OTP, and email OTP, ensuring robust security across multiple authentication methods.
Scalability	Exceptional	According to buyers, Ping is the most scalable vendor among those we analyzed. The Ping platform utilizes AI to manage large user volumes effectively while maintaining high accuracy in fraud prevention.
Customization	Exceptional	The Ping platform offers extensive customization options due to its flexible and comprehensive identity management features. It incorporates no-code and low-code orchestration capabilities, allowing organizations to tailor authentication, user management, and multi-factor authentication services to meet their specific needs.
Accuracy	Exceptional	According to banking buyers, Ping achieved the highest accuracy metrics among all the vendors we analyzed. By leveraging a robust product suite that includes both fraud detection and authentication capabilities, Ping effectively identifies fraudulent activities and minimizes financial losses.
Product Integration	Exceptional	Ping's API integration achieves one of the highest product integration satisfaction scores among top ATO prevention solution providers. This seamless integration reduces implementation times and allows customers to easily integrate with existing systems.
Buyer Satisfaction	Excellent	By offering one of the most extensive product suites among ATO prevention vendors, Ping achieves very high buyer satisfaction rates, a trend expected to continue in the future.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.




Analyst Notes on Ping Identity Platform

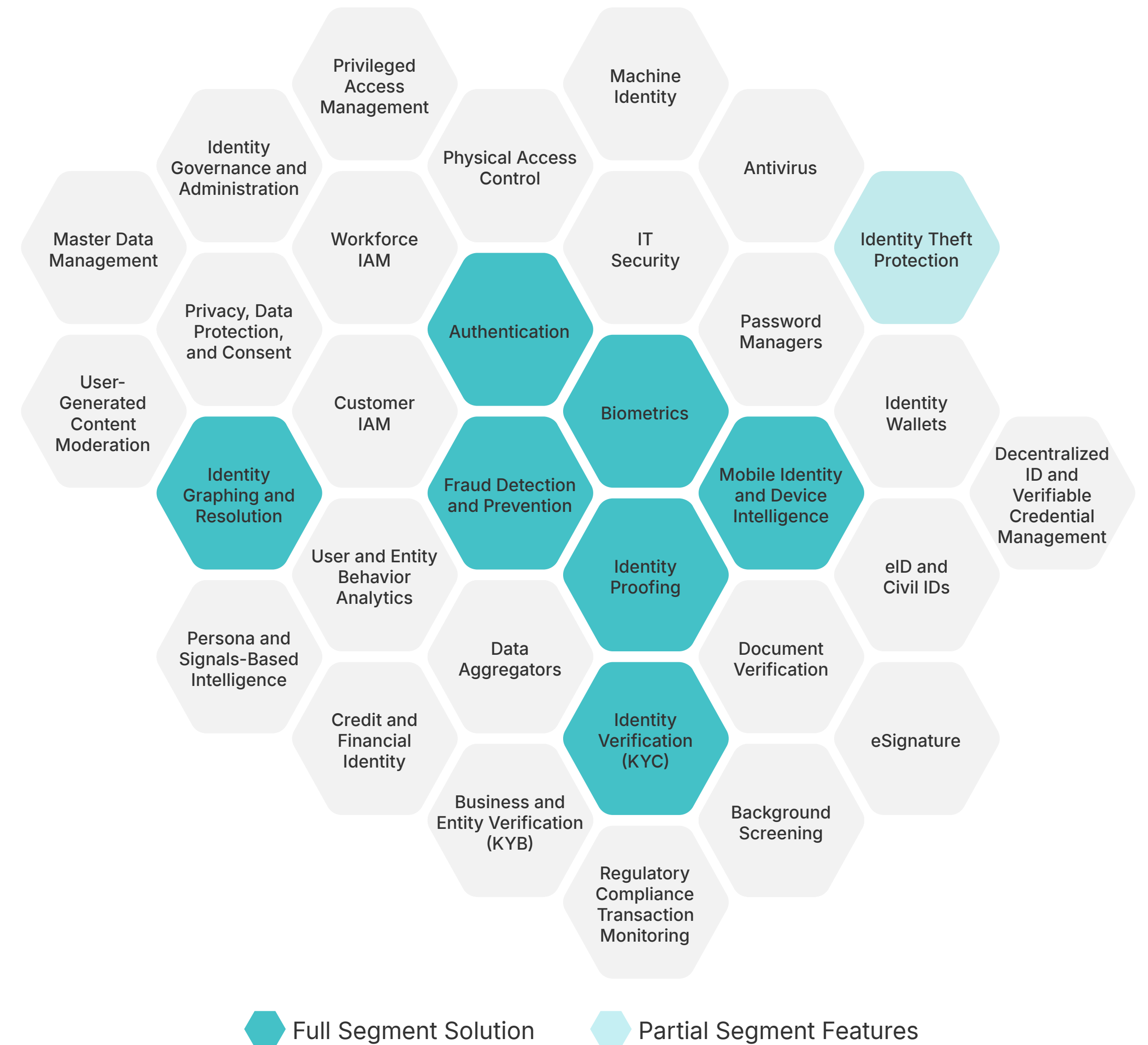
The Ping Identity Platform is a comprehensive identity and access management solution designed for enterprise-level companies, particularly those in industries requiring high levels of security, such as financial services, healthcare, and government. The platform provides cloud-based IAM services, including single sign-on (SSO), multi-factor authentication (MFA), risk management, fraud detection, and identity verification. Key features include adaptive and passwordless authentication options, risk assessment integrated into authentication flows, and robust user management capabilities such as directory services, provisioning, and de-provisioning. As a cloud-based solution, the Ping Identity Platform is easy to deploy and integrate with existing systems and is designed to work seamlessly in a hybrid IT environment. Administrators can customize sign-on forms and user interfaces to align with company branding.

Customers of the platform also get access to their PingOne Protect module. PingOne Protect dynamically evaluates multiple risk signals, even before login, to calculate an overall risk score for the end user. These signals include user and entity behavior analytics, behavioral biometrics, IP and network reputation telemetry, and device intelligence. The calculated risk score then drives identification, authentication, and authorization policies, enabling organizations to deliver a tailored approach to preventing fraudulent activity based on the individual's level of risk. The solution leverages machine learning and configurable, intelligent security policies to analyze user identity and detect potential threats. It evaluates risk levels based on various data points, such as network information, location, device hardware and settings, behavioral biometrics, and other relevant factors.

Prove

Prove offers identity verification and authentication solutions focused. Their platform leverages phone numbers to verify identities, streamline customer onboarding through pre-fill capabilities, and enhance security for various digital interactions. Prove's solutions include mobile authentication, identity verification, and fraud prevention, aiming to improve user experience while mitigating risks.

Company Information ¹	
Headquarters	New York, New York
No. of Employees	416 as of May 2024
Last Raised	\$40M, Venture – Series Unknown in October 2023
Primary Segment	Identity Verification (KYC) , Authentication, Mobile Identity and Device Intelligence, Identity Graphing and Resolution
Vertical Focus	Financial Services, Fintech, Healthcare, eCommerce, Gambling, Crypto
Geographic Focus	North America, Europe, Asia-Pacific, Latin America
Notable Customers	  



(1) Link

Prove's Strategy

Strategy	Excellent	Prove delivers strong fraud prevention and authentication capabilities to help financial institutions deliver personalized and secure customer experiences that protect against ATO attack vectors.
Behavioral Capabilities	Excellent	Prove's social engineering and phishing prevention capabilities are designed to protect organizations by leveraging advanced behavioral biometrics. These features help detect and prevent fraudulent activities by analyzing user behavior patterns and ensuring that interactions are legitimate.
Passwordless Authentication	Exceptional	Prove's passwordless authentication capabilities leverage advanced device intelligence and biometric verification to provide a seamless and secure user experience. By utilizing mobile signals and FIDO2 web-based authentication, Prove Auth enables frictionless, omni-channel authentication that significantly reduces the risk of account takeovers and enhances organizations' overall security posture.
Cost	Strong	Prove does not offer a free plan or a free trial for their services. Additionally, Prove Auth features an unlimited-use pricing model, which can help reduce costs and facilitate deployment across various use cases. 30% of surveyed customers indicated high satisfaction with Prove's cost.
User Experience	Excellent	Prove focuses on creating a frictionless and secure authentication experience for users across various channels, including mobile apps, web-based platforms, and omni-channel experiences. Their Prove Auth solution enables passwordless authentication, which can significantly improve the user experience by eliminating the need for traditional passwords or one-time passcodes.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Strategy

Prove Auth utilizes behavioral biometrics, such as location data and usage patterns, to create comprehensive user profiles and detect anomalies that may indicate fraudulent activities. The solution can distinguish between legitimate users and potential threats by analyzing behavioral biometric signals, enabling more reliable authentication decisions.

While the solution does not include bot detection capabilities, Prove's focus on analyzing user behaviors, device interactions, and transaction patterns aligns with the potential integration of mechanisms to identify and mitigate automated attacks or fraudulent activities from bots. By leveraging behavioral analytics and biometrics, the solution can likely differentiate between human and bot-driven activities.

Passwordless authentication is a core capability of Prove Auth. By combining support for FIDO2 standards, biometric authentication, mobile device binding, cryptographic keys, push notifications, continuous risk assessment, and omnichannel support, Prove Auth aims to provide a comprehensive passwordless authentication solution that enhances security while delivering a frictionless user experience. A key aspect of Prove Auth's passwordless authentication approach is using the user's smartphone as the primary authentication device. Prove Auth leverages cryptographic keys stored on the user's device for authentication through push notifications, providing a secure, passwordless authentication experience by leveraging the user's device as a possession factor. Prove Auth supports passwordless authentication across multiple channels, enabling organizations to provide a consistent and frictionless authentication experience across various touchpoints.

Prove's Market Presence

Market Presence	Strong	Prove is a well-recognized identity vendor that has recently gone to market with an Auth product – they have a strong presence amongst large financial institutions and are well-positioned for growth.
Brand Awareness	Strong	Prove is a strong identity vendor focusing on onboarding solutions; however, in late 2022, they released an authentication product. As such, 39% of surveyed financial institutions recognized their brand and solutions for ATO prevention.
Market Leadership	Excellent	Despite their solution being in the market for less than three years, about 37% of surveyed financial institutions recognize Prove as a market leader, indicating strong brand value among ATO prevention solutions seekers at global banks.
Market Penetration	Excellent	Prove has established itself as a trusted partner to many large global financial institutions, including Visa, Bilt, Synchrony, and TD Ameritrade. Therefore, demonstrating competitive market penetration across financial institutions.
Company Size	Excellent	With over 400 employees, Prove has a competitive workforce that prioritizes further product development. Moreover, roughly 15% of their workforce includes sales professionals, highlighting their strong ability to capture new customers across North America, Europe, and Asia.
Employee Growth	Strong	Prove has experienced moderate employee growth of 5% YoY. However, they've increased headcount for business development roles by 10% YoY, indicating a priority towards continued investment in growth and service.

Analyst Notes on Market Presence

Prove has established a significant market presence as a leading identity verification and authentication solutions provider. The company's innovative platform and proprietary Phone Identity Network™ (PIN) have garnered widespread adoption across various industries, including financial services, e-commerce, insurance, and telecommunications.

Prove's solutions are trusted by some of the largest companies in the world, with nine of the 10 top U.S. banks relying on Prove's platform to enhance cybersecurity, mitigate fraud, and eliminate the costs associated with legacy identity verification solutions. Over 1,000 businesses leverage Prove's technology to enable trusted digital transactions throughout the customer journey.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Prove Auth

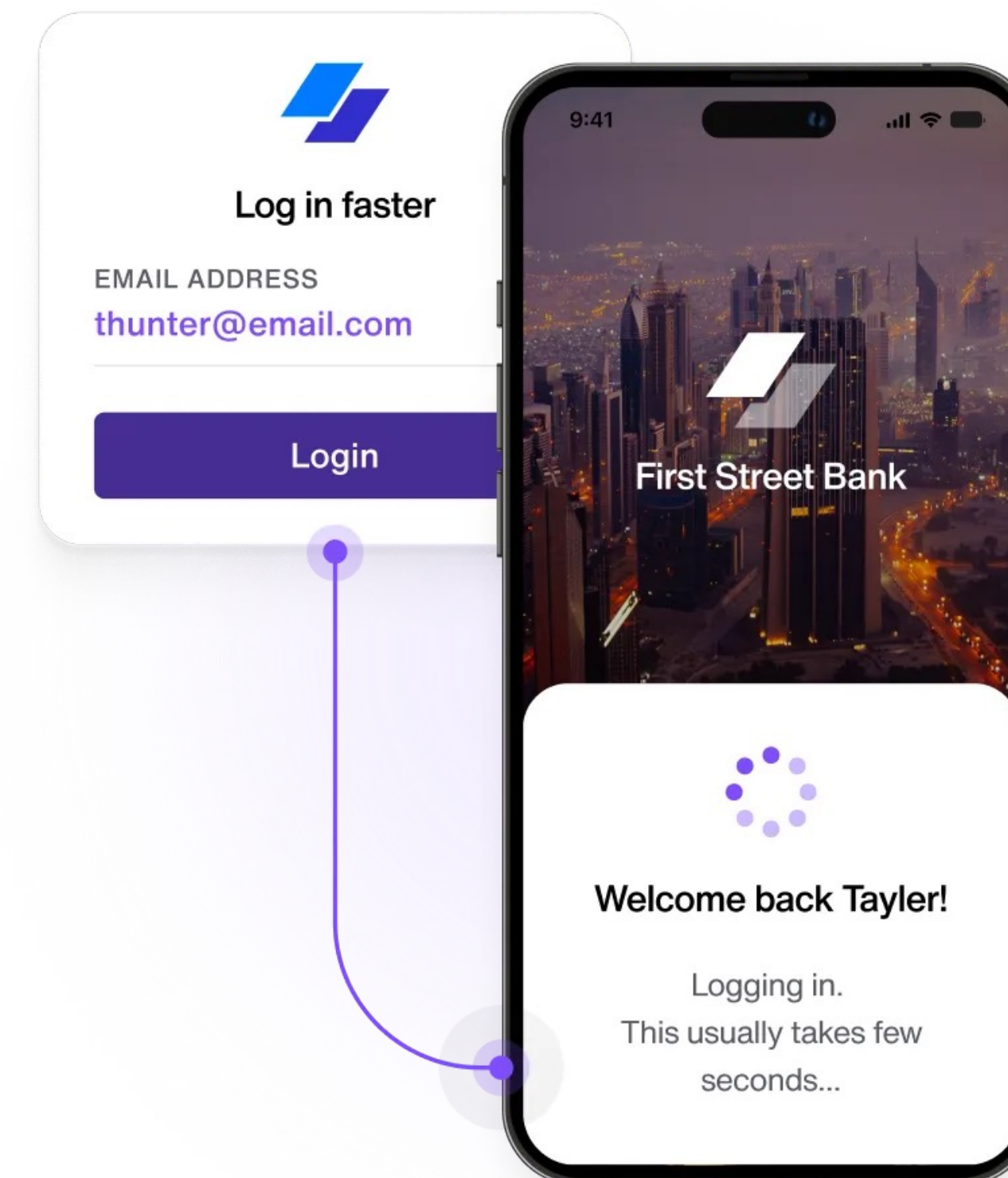
Prove Auth is an authentication solution designed to enhance security and user experience. It leverages MFA technology, reducing reliance on traditional methods like passwords and SMS one-time passwords. Prove Auth uses a combination of phone number verification, behavioral analysis, and other device signals to ensure secure and seamless authentication across various customer interactions, including account logins, transactions, and onboarding processes.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from company website (link: <https://www.prove.com/solutions/auth>).

Product Visuals²



Prove Auth

Product	Excellent	Prove offers highly scalable ATO solutions with a robust authentication suite featuring several in-demand capabilities.
Product Capability	Excellent	Prove offers biometric authentication, the most highly demanded capability for ATO prevention in banking. Additionally, the company provides device risk scoring and location intelligence, creating a strong set of capabilities to defend against ATO effectively.
Scalability	Exceptional	Prove is a leading player in the identity market, serving major clients such as Bank of America, Wells Fargo, and Citibank. Covering three of the top four largest banks demonstrates their ability to seamlessly scale with large organizations and provide robust ATO prevention.
Customization	Exceptional	Prove received one of the highest customization scores among all the vendors we analyzed. By offering both biometric authentication and behavioral signals, Prove enables customers to tailor their threat detection strategies effectively.
Accuracy	Exceptional	By integrating biometric authentication with behavioral signals, Prove gains a precise understanding of each user's identity. This approach makes it extremely challenging for fraudsters to take over accounts and cause financial loss.
Product Integration	Exceptional	Prove offers their solutions split up as 8 API services where users can purchase individual data signals or verifications. Clients can also buy these as bundled solutions, including possession APIs, reputation APIs, and ownership APIs. Their Trust Score API encompasses their ATO prevention solution, providing comprehensive protection against account takeovers.
Buyer Satisfaction	Exceptional	Prove Auth aims to provide passwordless authentication that is passive, ensuring a seamless user experience. The product's high buyer satisfaction scores indicate its success in achieving this goal.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Prove Auth




Prove Auth is a comprehensive authentication solution designed to enable passwordless and OTP-less authentication for mobile apps, web-based, and omnichannel experiences. Prove Auth leverages a strong identity bind to authenticate users across various channels, including push notifications, cryptographic keys, and biometrics. At the core of Prove Auth is the company's proprietary Phone Identity Network™ (PIN), a registry of over 1 billion privacy-enhancing phone identity tokens under continuous management. This network allows Prove to establish a trusted relationship between a user's physical device and phone number, enabling accurate identity verification and authentication.

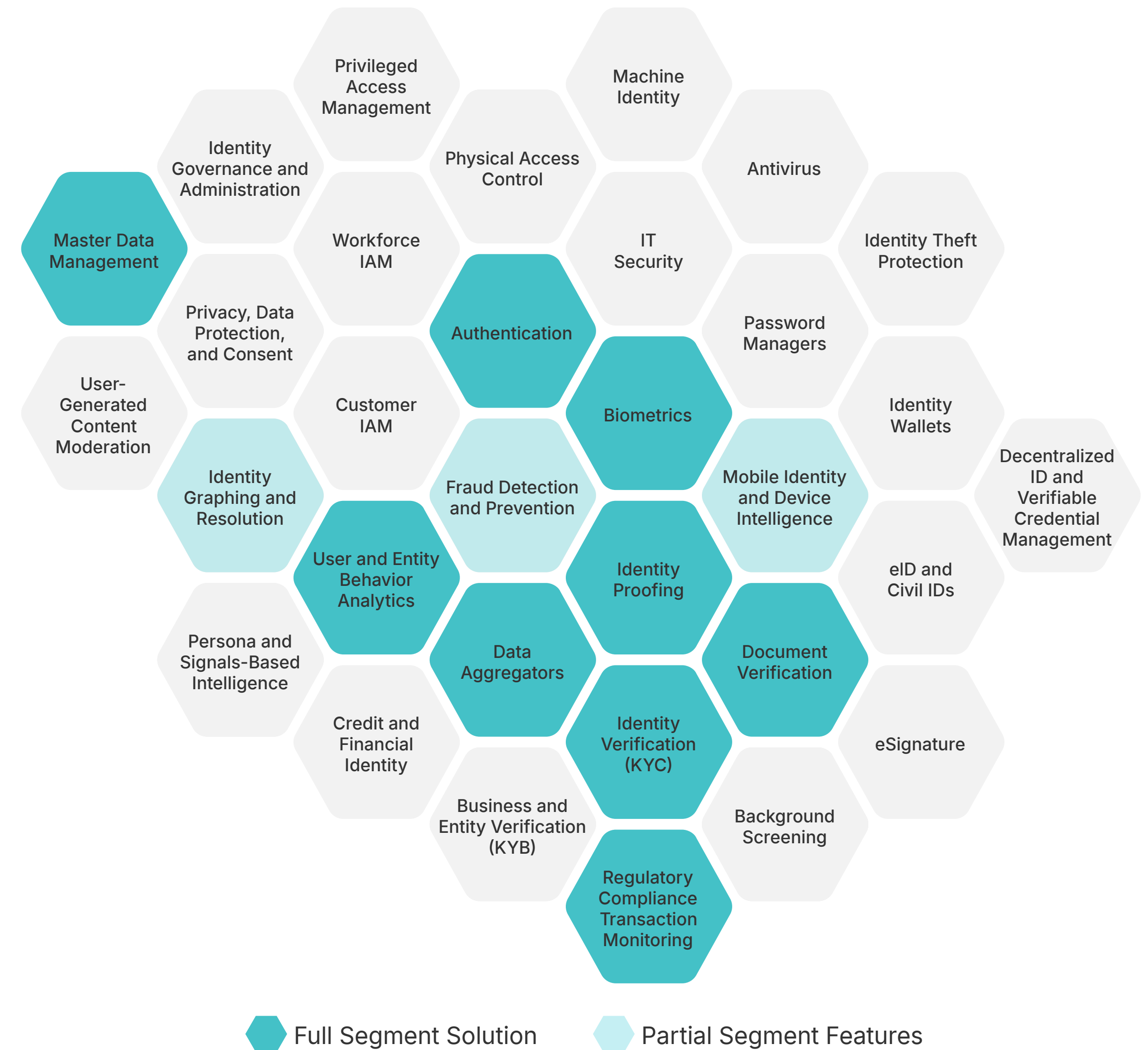
Prove Auth utilizes the user's smartphone as the authentication device, maximizing convenience without compromising security. It verifies ownership of the phone number by analyzing its behavior over an extended period, typically ten years, and ensuring that it is genuinely owned and operated by the user attempting to log in. Once ownership is established, cryptographic keys on the physical device are used to passively verify the user's identity through push notifications and behavioral biometrics, such as location and usage patterns, continuously assessing the risk associated with the device.

Prove Auth supports FIDO2 standards for web-based authentication, enabling passwordless authentication through biometrics or possession-based factors like security keys. Users can authenticate directly with Prove or utilize on-device biometrics for step-up measures, increasing the rate of successful authentications for legitimate users.

Socure

Socure offers an identity risk platform that provides coverage across several use cases. Specifically, Socure's solutions include identity verification, KYC compliance, and fraud detection, which aim to improve the efficiency and security of digital onboarding and transaction processes. The company focuses on helping businesses prevent identity fraud while ensuring a seamless user experience, covering solutions through its ID+ platform.

Company Information ¹	
Headquarters	Incline Village, Nevada
No. of Employees	450 as of June 2024
Last Raised	\$450M, Series E Round in November 2021
Primary Segment	Identity Verification (KYC), Data Aggregators, Regulatory Compliance and Transaction Monitoring, Document Verification, Mobile Identity & Device Intelligence
Vertical Focus	Financial Services, eCommerce, Gig Economy, Government, Gaming, Crypto
Geographic Focus	North America, Europe, Middle East, Asia-Pacific
Notable Customers	  



(1) Link

Socure's Strategy

Strategy	Strong	Socure offers an excellent user experience and extensive use case coverage, effectively preventing ATO threats through its advanced digital identity fraud prevention tools.
Behavioral Capabilities	Excellent	The Socure platform utilizes advanced behavioral analytics to detect anomalies in user behavior, which may indicate potential fraud. By identifying these irregularities, the platform provides robust protection for banks against ATO threats. This comprehensive approach ensures that fraudulent activities are detected early, protecting banks and customers from would-be ATO attackers.
Passwordless Authentication	Strong	Socure's platform prevents financial losses through its fraud prevention and identity verification technologies. However, it does not extensively integrate passwordless authentication solutions such as passkeys which offer more secure device authentication options.
Cost	Strong	According to current customers, Socure is considered more expensive than some other vendors we profiled. However, the Socure platform offers extensive use case coverage, making it a strong solution for banking customers. Despite the higher cost, its comprehensive capabilities provide significant value for financial institutions seeking robust security solutions.
User Experience	Excellent	Socure is highly regarded for its strong customer experience according to banking customers. By leveraging graph technology that analyzes networks for anomalies and fraudulent behavior, Socure provides robust ATO prevention without imposing significant friction on users.

Analyst Notes on Strategy

Socure takes an identity-centric approach, offering identity signals for comprehensive fraud compliance and ID verification. The company effectively prevents ATO by developing a deep understanding of identity.

Socure's platform uses bot detection and behavioral signals, employing sophisticated algorithms to identify and mitigate automated attacks and other malicious activities. The platform can distinguish between legitimate user interactions and fraudulent activities by analyzing device and network characteristics, ensuring only genuine users can access services. By offering a platform solution with Socure's ID+, the company attracts banks seeking comprehensive solutions across the customer lifecycle, addressing multiple use cases and reducing the need for extensive tech stacks involving many vendors.

Despite not offering OTP capabilities, Socure has a roadmap to develop these features in-house rather than relying on third-party authentication vendor integrations. These additions to the Socure platform will help support increased ATO prevention by coupling advanced fraud detection and comprehensive authentication services.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Socure's Market Presence

Market Presence	Excellent	Socure is a scaling identity vendor that has raised over \$700 million in funding. Socure are well-recognized amongst financial institutions and are well-positioned to attain market share.
Brand Awareness	Excellent	Socure has established strong brand awareness through a robust customer portfolio – boasting more than 2000 customers. Of surveyed practitioners at financial institutions, roughly 52% were familiar with their brand and solution for ATO prevention.
Market Leadership	Excellent	Among those practitioners who were familiar with Socure, 18% recognized them as market leaders for fraud prevention. While the solution is primarily focused on identity verification, this underscores its ability to effectively solve fraud use cases in financial services.
Market Penetration	Strong	Socure has established a dominant presence in financial services, supporting over 400 fintechs. The company's platform is trusted by four of the top five banks and 13 of the top 15 card issuers, making it a critical partner for major financial institutions worldwide.
Company Size	Excellent	Socure, headquartered in Incline Village, Nevada, employs 450 people and operates across multiple global locations. The company has raised a total of \$755.8 million in funding, reflecting its substantial market presence and growth in the digital identity verification sector.
Employee Growth	Exceptional	The company has experienced significant YoY employee growth – roughly 52%. They also maintain roughly 40% of their team focused on engineering or information security, which positions them well to continuously innovate solutions based on changes in buyers' demands.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Market Presence

Socure has rapidly emerged as a market leader in the identity verification industry. The company's customer base has grown exponentially, tripling in 2021 to serve over 1,800 customers across various sectors like financial services, fintech, cryptocurrency, online gaming, telecommunications, e-commerce, insurance, and healthcare. Socure's solutions have become a gold standard for identity verification use cases, and are trusted by four of the five largest banks, seven of the 10 largest credit card issuers, top Buy Now, Pay Later (BNPL) providers, top cryptocurrency exchanges, and the largest online gaming operators.

The company has seen tremendous growth, tripling its valuation to \$4.5 billion in 2021, making it the highest-valued private company in the identity verification industry. Socure has attracted investments from top venture firms like Accel, T. Rowe Price, Bain Capital Ventures, Tiger Global, and several customer-turned-investors, including Citi Ventures, Wells Fargo Strategic Capital, and Capital One Ventures.

Socure ID+ Platform

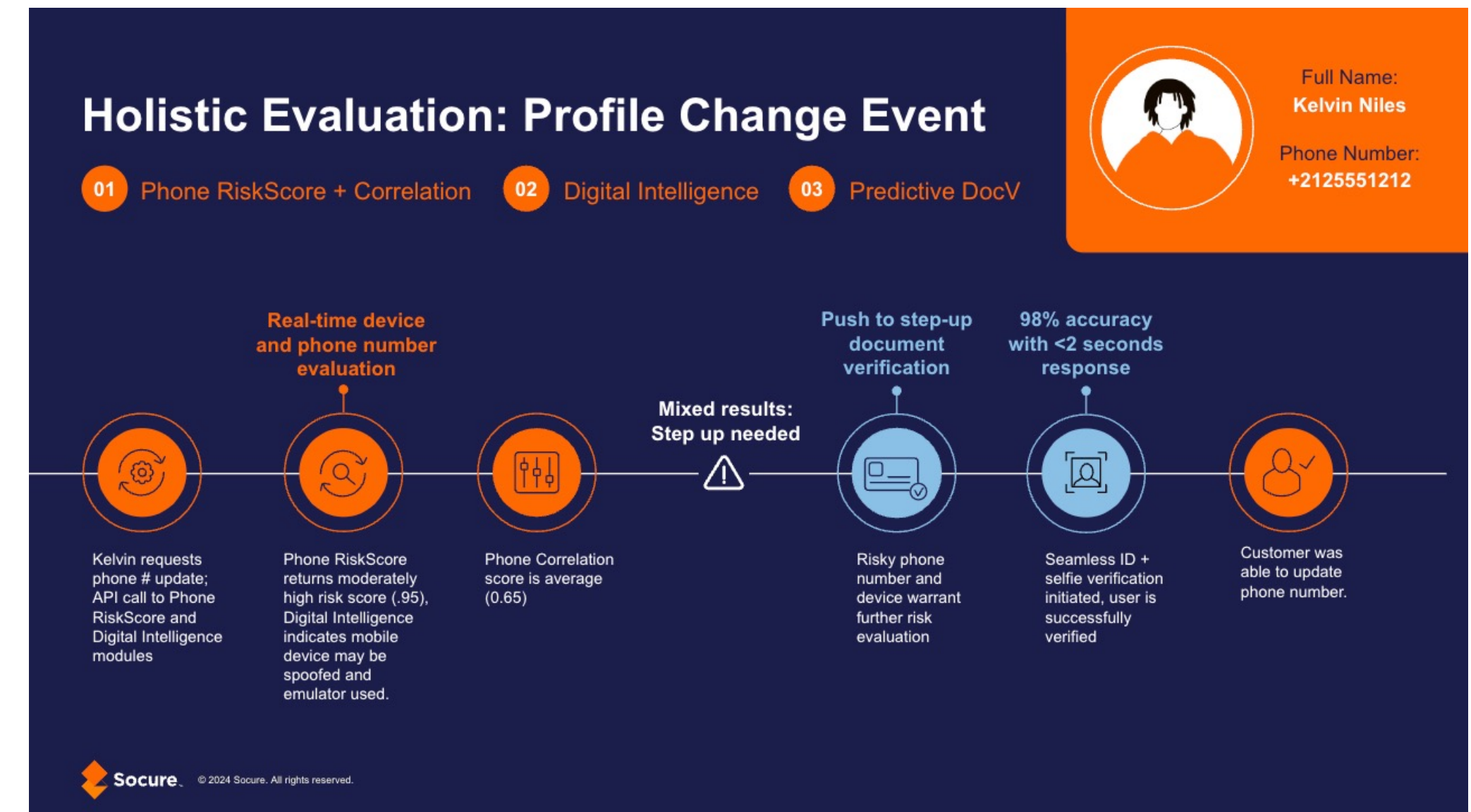
The Socure ID+ platform provides digital identity verification and fraud prevention using real-time predictive analytics. It leverages risk scoring and AI/ML to analyze a broad range of data sources for accurate identity verification and fraud prevention. The platform features a single API that integrates various identity elements to prevent against ATO.

ATO Prevention Product Capability Coverage ¹	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from the company.

Product Visuals²



Socure ID+ Platform

Product	Exceptional	Socure's ID+ platform offers a wide range of use cases, delivering high levels of customer satisfaction in ATO prevention.
Product Capability	Excellent	Socure uses fraud signals such as device, location, and proxy and VPN detection, along with other behavioral analytics on its Socure ID+ platform, to provide robust defense against a wide range of ATO threats.
Scalability	Excellent	Socure is a leading player in identity and fraud prevention, with extensive experience working with large institutions that have substantial user bases and high transaction volumes. Buyers also report strong scalability ratings for the company, indicating its ability to effectively support growing organizations.
Customization	Excellent	Socure provides a unified platform where customers can orchestrate various capabilities to best suit their needs in combating account takeovers. This integration allows for a streamlined and effective approach to identity verification and fraud prevention.
Accuracy	Strong	While the company utilizes several fraud signals, it lacks key capabilities such as behavioral biometrics and social engineering scam detection. As a result, buyers rank their accuracy relatively lower compared to some of the other vendors we analyzed.
Product Integration	Excellent	The Socure ID+ platform offers identity verification and fraud prevention solutions through a single API integration, simplifying the integration process for banks. Their solution can also be integrated with other solution providers to support more robust capability coverage.
Buyer Satisfaction	Exceptional	Buyers rate Socure highly in terms of satisfaction, making it one of the top vendors we profiled. The Socure ID+ platform offers broad use case coverage, providing comprehensive fraud prevention solutions for banking customers.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Socure ID+ Platform

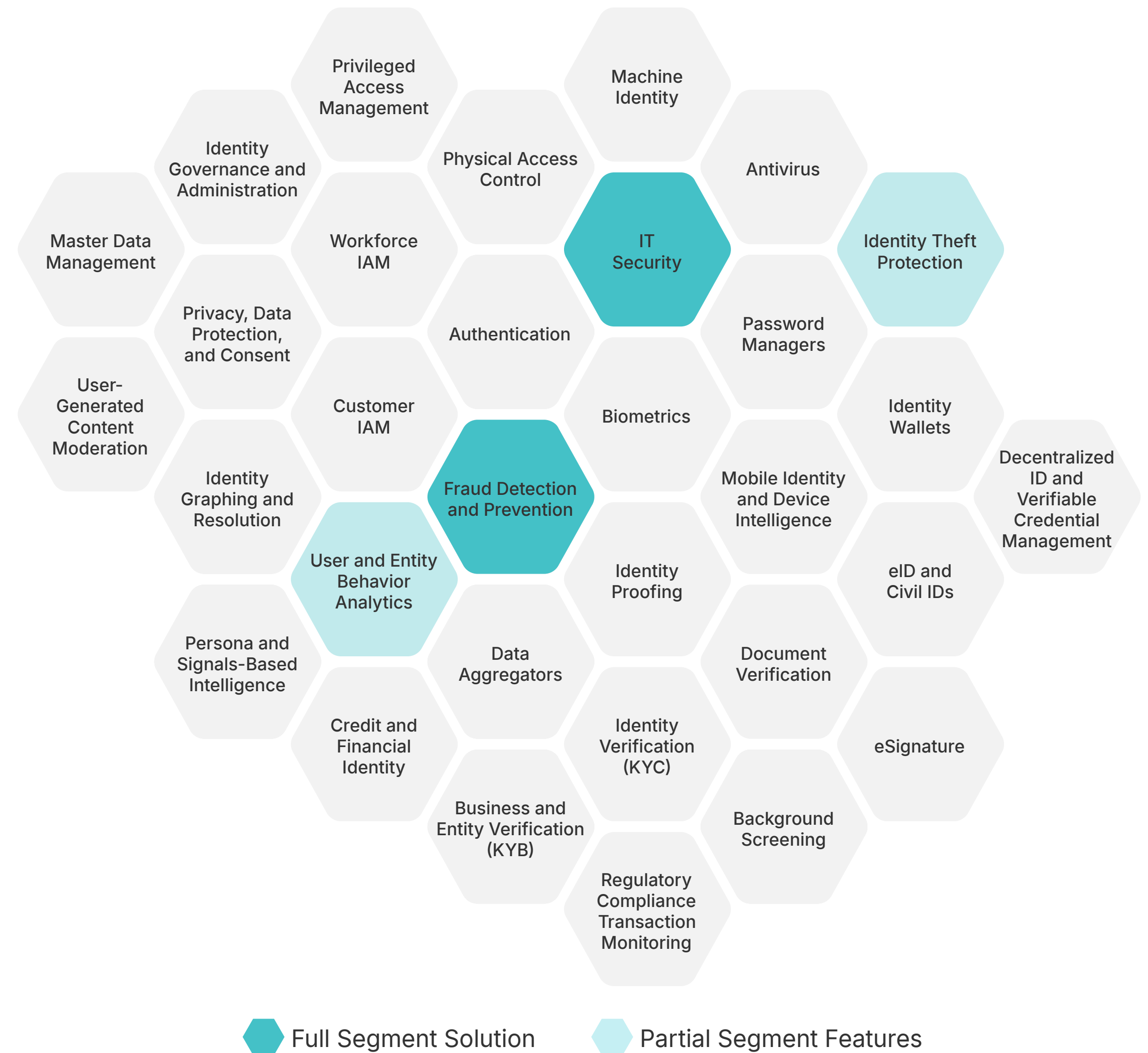
Socure's ID+ platform is a digital identity verification and fraud prevention solution that leverages advanced artificial intelligence and machine learning to provide real-time, predictive analytics for accurate and comprehensive identity verification. The platform integrates a vast array of data sources, including physical government-issued documents, email, phone, address, IP, device, velocity, date of birth, and Social Security Number (SSN), to create a complete view of an individual's digital identity. By analyzing and correlating every facet of an individual's identity, Socure's ID+ platform aims to maximize accuracy, reduce false positives, and eliminate the need for disparate products. The platform's graph-defined network continuously learns from billions of predictions and outcomes from over 2,400 top financial institutions, government agencies, and enterprises, ensuring accuracy and coverage.

SpyCloud

SpyCloud provides cybersecurity solutions focused on preventing account takeovers and online fraud. The platform identifies and remediates compromised credentials by monitoring the dark web for stolen data. SpyCloud’s services include automated password resets, fraud detection, and breach recovery to help businesses protect their users and maintain trust. By leveraging extensive breach data and machine learning, SpyCloud enhances security measures and reduces the risk of account-related threats.

Company Information ¹	
Headquarters	Austin, Texas
No. of Employees	174 as of May 2024
Last Raised	\$110M, Series D Round in August 2023
Primary Segment	Fraud Detection and Prevention
Vertical Focus	Financial Services, Government, Crypto
Geographic Focus	North America
Notable Customers	SpyCloud does not publicly disclose banking customers

(1) Link



SpyCloud's Strategy

Strategy	Strong	SpyCloud is a heavily specialized vendor focused on dark web monitoring, providing protection against stolen credentials.
Behavioral Capabilities	Strong	SpyCloud specializes in dark web and data breach monitoring, prioritizing these areas over leveraging behavioral signals. While this focus allows SpyCloud to excel in identifying compromised credentials and sensitive data on the dark web, it does not provide the same level of behavioral analysis for fraud detection and ATO prevention that some other vendors offer.
Passwordless Authentication	Strong	The company does not offer passwordless authentication features such as passkeys or QR codes, nor does it leverage WebAuthn like some of the other vendors we profiled. Instead its focus remains on other areas of ATO security, requiring customers who are looking for these advanced passwordless authentication options to adopt additional vendors.
Cost	Excellent	According to current customers, SpyCloud offers strong cost-effectiveness compared to other top vendors. As a point solution focused on scanning the dark web for compromised credentials, SpyCloud is typically integrated into larger tech stacks and does not provide comprehensive ATO coverage on its own.
User Experience	Excellent	SpyCloud received excellent customer feedback regarding user experience. The product searches for compromised credentials and operates without directly interacting with user flows, thus avoiding unnecessary friction that could lead to customer drop-off.

Analyst Notes on Strategy

SpyCloud's solution currently does not include bot detection, behavioral analytics, behavioral biometrics, or passwordless authentication features. Instead, its approach to preventing account takeover primarily involves identifying compromised credentials and session cookies from devices infected with malware, and shielding against synthetic identity fraud. After a fundraising event in 2023, SpyCloud plans to expedite the development of new technologies within its Enterprise Protection, Consumer Risk Protection, and Investigations services. Part of their future strategy is to introduce solutions that prevent authentication bypass, aiming to secure both businesses and consumers against the risks of compromised passkeys. Additionally, SpyCloud is working to enhance its analytical tools to better connect exposures of both personal and corporate identity and authentication data, fostering an identity-focused security perspective that extends beyond mere device-centric approaches.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

SpyCloud's Market Presence

Market Presence	Strong	SpyCloud is a competitive cybercrime analytics company with a strong identity around its data breach monitoring capabilities.
Brand Awareness	Strong	SpyCloud has leading brand awareness positioning itself as a thought leader through strategic media engagements and a robust PR campaign, resulting in frequent coverage in top-tier publications like Forbes, POLITICO, and SC Media. Of surveyed practitioners in financial services 45% were familiar with the brand.
Market Leadership	Strong	SpyCloud has established itself as a market leader in cybercrime analytics, specifically for its solutions that leverage recaptured data from the criminal underground to protect businesses from account takeovers, ransomware, and other cyber threats – of those practitioners that were familiar with their brand 19% recognized them as market leaders.
Market Penetration	Strong	Leveraging its extensive breach data and human intelligence-driven approach, SpyCloud enables financial institutions to proactively identify and remediate compromised credentials, safeguarding millions of customer accounts and ensuring compliance with stringent regulatory requirements.
Company Size	Excellent	SpyCloud, headquartered in Austin, Texas, employs approximately 170 people with roughly 20% of their workforce dedicated to sales. They have also raised a total of \$168.5 million in funding, with the most recent funding coming in August 2023.
Employee Growth	Strong	Spycloud has experienced moderate employee growth – roughly 8% YoY. This is primarily driven by a 19% increase in sales professionals and a 65% increase in information technology employees over the last year.

Analyst Notes on Market Presence

SpyCloud has over 500 customers globally, including half of the Fortune 10 companies. The majority of SpyCloud's customers are large enterprises, mid-size companies, and government agencies. Most of their customer base is concentrated in the United States. SpyCloud utilizes data reclaimed from the darknet to enhance cybersecurity for businesses. By employing Cybercrime Analytics (C2A), it generates actionable insights that help companies proactively shield against ransomware, account takeovers, and consumer fraud. This approach not only aids businesses in preventing financial losses but also supports investigations into cybercrime. SpyCloud's extensive dataset includes information sourced from breached data, malware-compromised devices, and other clandestine online activities. This dataset also supports various dark web monitoring and identity theft protection services.

Following a \$30 million Series C funding round in 2020, SpyCloud tripled its revenue and created cutting-edge solutions to mitigate new and prevalent cyberattacks for large and mid-sized enterprises including top financial institutions, retailers, and software and technology companies. Its partnerships include popular identity monitoring services and MSSPs who leverage SpyCloud's analytics to deliver ongoing value to consumers and businesses of all sizes. In 2023, they raised a \$110 million growth round commitment of primary and secondary capital led by Riverwood Capital.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

SpyCloud Consumer Risk Prevention

SpyCloud Consumer Risk Prevention helps protect customer accounts from takeover by monitoring for compromised credentials across the dark web. It alerts organizations when customer data is exposed in data breaches, enabling prompt action to secure accounts. The platform utilizes extensive breach and malware data to automate responses such as password resets or step-up authentication, enhancing security and user experience.

ATO Prevention Product Capability Coverage¹

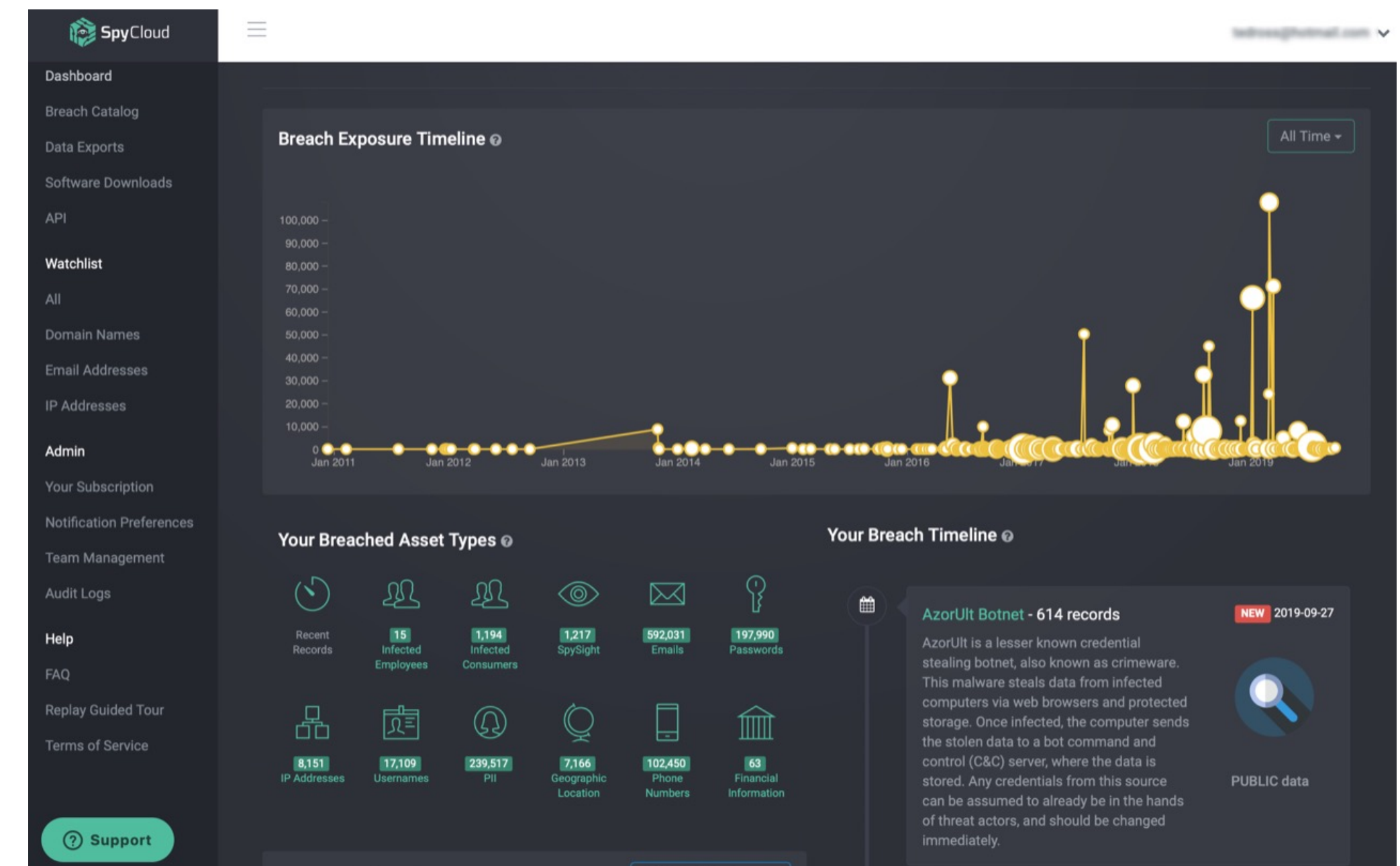
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from public sources (link: <https://cybersecurity-excellence-awards.com/candidates/spycloud-provides-the-most-current-relevant-and-actionable-data-for-ato-and-online-fraud-prevention/>).

Product Visuals²



SpyCloud Consumer Risk Prevention

Product	Strong	SpyCloud, with its focused capability set on monitoring the dark web for stolen credentials, receives high ratings from customers for scalability, accuracy, and customization.
Product Capability	Strong	SpyCloud is highly focused among ATO vendors, concentrating specifically on monitoring the dark web for compromised credentials. As a result, it has more limited capabilities in other areas of ATO prevention.
Scalability	Excellent	The company is highly focused among ATO vendors, concentrating specifically on monitoring the dark web for compromised credentials. As a result, it has more limited capabilities in other areas of ATO prevention.
Customization	Exceptional	Consumer Risk Prevention offers an investigation service that provides companies with a comprehensive range of identity and fraud information. This enables businesses to gather accurate insights to inform their investigations effectively.
Accuracy	Excellent	SpyCloud improves penetration testing accuracy by leveraging recaptured data from third-party breaches and malware-infected devices, allowing testers to replicate authentic attacker behaviors. This method swiftly identifies security gaps and validates exposed credentials, providing detailed insights into vulnerabilities.
Product Integration	Excellent	The SpyCloud API integrates breach and malware data into existing workflows, offering fast, high-volume access. It enables organizations to proactively protect accounts from takeover, expedite fraud investigations, and seamlessly integrate with SOARs, SIEMs, and other detection tools for enhanced visibility.
Buyer Satisfaction	Excellent	SpyCloud is a strong solution for enterprises looking to enhance their ATO tech stack with data breach and dark web monitoring capabilities. Buyers have rated their ATO protection highly in terms of satisfaction.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

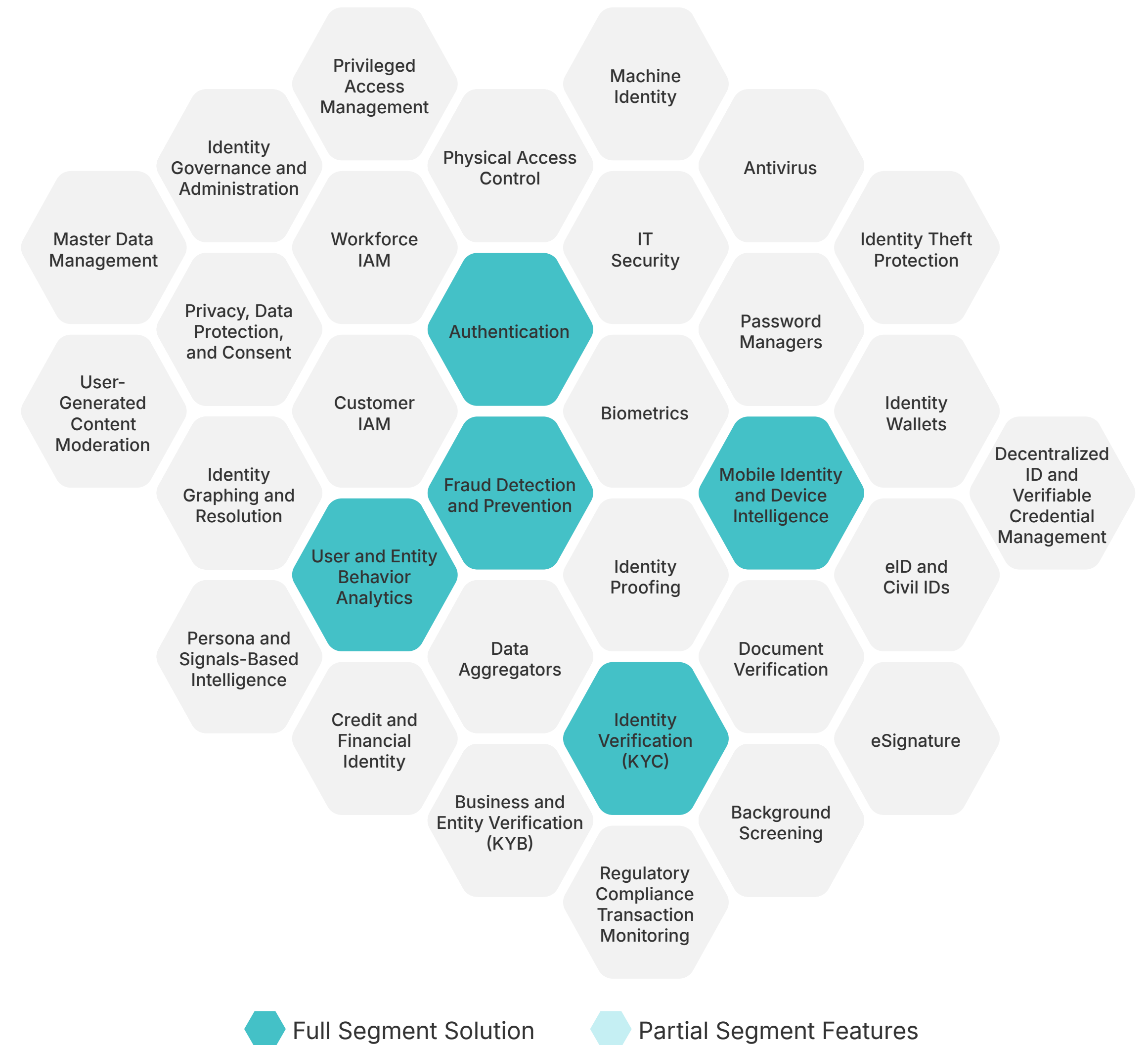
Analyst Notes on SpyCloud Consumer Risk Prevention

SpyCloud's Consumer Account Takeover leverages SpyCloud's extensive repository of recaptured data from the criminal underground, including breached credentials, malware-exfiltrated authentication data, and exposed personally identifiable information (PII). By integrating this data into security workflows, SpyCloud enables businesses to detect and mitigate risks associated with compromised consumer accounts proactively. The solution automates the detection and invalidation of stolen session cookies, preventing criminals from bypassing multi-factor authentication (MFA) and other security measures. SpyCloud's Consumer Risk Prevention Solution also provides actionable insights that allow security teams to enforce strong password policies, reset compromised credentials, and monitor suspicious activity. This proactive approach reduces the risk of financial losses and brand damage and enhances operational efficiency by automating remediation processes and reducing the need for manual intervention. Trusted by numerous global enterprises, SpyCloud's solution helps businesses stay ahead of cybercriminals, ensuring the security and integrity of consumer accounts.

Telesign

Telesign provides solutions to enhance security primarily using SMS OTP. It offers services like phone number verification, two-factor authentication, and fraud prevention to help businesses protect user accounts and reduce fraud. The company protects against synthetic identity fraud and bot attacks while facilitating onboarding and customer engagement.

Company Information ¹	
Headquarters	Los Angeles, California
No. of Employees	783 as of May 2024
Last Raised	\$40M, Series B Round in July 2024
Primary Segment	Mobile Identity and Device Intelligence, Authentication
Vertical Focus	Financial Services, eCommerce, Gaming
Geographic Focus	North America, Europe
Notable Customers	Telesign does not publicly disclose banking customers



(1) Link

Telesign's Strategy

Strategy	Strong	As the premier SMS OTP vendor, Telesign effectively defends against fraud while offering a solution with high cost-effectiveness according to customer sentiment.
Behavioral Capabilities	Excellent	Telesign offers bot detection capabilities to prevent non-human users from breaching security systems and causing financial loss. However, the company does not provide behavioral biometrics, unlike some other vendors in the space.
Passwordless Authentication	Strong	Focusing on SMS OTP, the company does not provide extensive passwordless authentication options. While it excels in delivering secure one-time passwords via SMS, it lacks more other passwordless solutions like device-based or cloud-based passkeys and QR codes for authentication.
Cost	Exceptional	Banking customers of Telesign find their solution to be very cost-effective. As the premier SMS OTP vendor in the space, Telesign provides highly demanded SMS OTP protection at a low price while ensuring strong security.
User Experience	Excellent	According to current banking customers in our survey, Telesign provides an excellent user experience. Telesign also operates in eCommerce, retail, and gaming, where their expertise in low-friction solutions is validated by strong user experience ratings.

Analyst Notes on Strategy

Telesign has historically been a leader in providing SMS OTP solutions for authentication and risk reduction. Recently, the company has expanded its capabilities to offer more robust ATO protection by integrating identity attributes with authentication and fraud detection signals, providing comprehensive use case coverage.

Telesign boasts one of the highest satisfaction scores for cost-effectiveness among top ATO vendors. Its Intelligence solution uses a flexible, pay-as-you-go pricing model, allowing businesses to scale usage based on demand. The cost is influenced by transaction volume and specific services utilized, with volume-based discounts available, making it a cost-effective option for businesses of all sizes.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Telesign's Market Presence

Market Presence	Excellent	Telesign is recognized for its mobile and device intelligence services that can be leveraged for low-friction fraud analysis to prevent ATO attacks.
Brand Awareness	Excellent	Telesign offers a comprehensive suite of services, including phone verification APIs, user verification, and omnichannel communications – their solutions and brand were familiar with about 72% of surveyed practitioners in financial services.
Market Leadership	Excellent	The company is regarded as a leading provider of mobile intelligence services for fraud detection and prevention, garnering market leadership perception from 18% of surveyed financial institutions.
Market Penetration	Excellent	Telesign supports 20 of the 25 largest global brands, enhancing security and customer engagement through real-time communications and robust identity intelligence. However, they are particularly penetrated among global e-commerce companies boasting clients like Alibaba.
Company Size	Exceptional	Telesign maintains a significant global presence with four strategically located offices. Its headquarters are based in California, US, complemented by additional offices in Columbia, Serbia, Singapore, the United Kingdom. This international footprint supports a diverse and extensive workforce, with a total employee count of more than 700 across all locations.
Employee Growth	Excellent	Telesign has experienced a significant employee count over the past year, showing an increase of more than 30%, driven primarily by a 3% increase in its information technology department, and 5% increase in their marketing department.

Analyst Notes on Market Presence

Telesign, a Proximus company, has established a significant market presence in the mobile identity and fraud detection and prevention sectors. As one of the largest players in the mobile identity industry, Telesign provides a comprehensive suite of APIs and SDKs that enable real-time communications, user verification, and security for some of the world's largest brands. The company's solutions are trusted by 20 of the 25 largest global brands, reflecting its strong reputation and reliability in the market.

The company's customer base is diverse, spanning various industries and geographies, with a significant presence in the United States, United Kingdom, and France. Telesign's clients range from small businesses to large enterprises, including notable names such as TD Bank and Jenius Bank. The company continues to expand its global footprint, with offices in key regions such as Beijing and Singapore and a workforce distributed across multiple countries.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Telesign Intelligence

Telesign Intelligence provides data-driven insights to enhance security and reduce fraud. Their services utilize machine learning and real-time data analysis to assess the risk associated with phone numbers and user accounts. By offering solutions such as phone number intelligence, they aim to help businesses identify potential fraud before it occurs, improving overall safety and customer trust.

ATO Prevention Product Capability Coverage¹

H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from <https://youtu.be/kBaDvhd3znM?t=301>

Product Visuals²

#	Risk Band	Total volume	%	True positive rate	Fraud
1	Very-low	30	0.87		
2	Low	3000	86.96		
3	Medium-low	0	0		
4	Medium	150	4.35		
5	High	180	5.22	50	90
6	Very-high	90	2.61	90	81
Total		3450	100%		171

Solution details

Solution: Demo Project 1 Job date: 09/04/2023

Customer: ABC Corp Period multiplier: 30

Telesign Intelligence

Product	Excellent	Telesign is a leading provider of SMS OTP and has proven to have accurate and scalable solutions for ATO prevention in banking.
Product Capability	Excellent	Telesign is best known for its SMS OTP capabilities, which it provides for many other vendors in the space. Additionally, it offers social engineering and scam detection, device risk scoring, and SIM swap detection, among other capabilities.
Scalability	Excellent	The company provides scalable services with a range of offerings from basic to advanced, allowing customers to adapt their solution mix as they grow. The company's cloud-based solutions allow businesses to scale up or down quickly without the need for expensive hardware or software upgrades.
Customization	Excellent	Telesign highlights its diverse verification channels as a key strength in customization, enabling customers to select the methods that best suit their needs. This flexibility is particularly appreciated by banking customers, who rate Telesign highly for its customizable options.
Accuracy	Excellent	Leveraging various fraud prevention capabilities such as social engineering and scam detection powered by AI and ML models, Telesign provides accurate solutions to defend against growing threats. This technology ensures effective protection against evolving fraud risks.
Product Integration	Strong	Offering multiple APIs and SDKs, Telesign allows customers to pick and choose the solutions they need to prevent ATO. This flexibility enables users to customize their security measures by integrating only the necessary components for their specific requirements.
Buyer Satisfaction	Strong	Telesign's buyer satisfaction scores are currently lower than some other top vendors. However, the company is expected to improve its position as it continues to expand its product suite to include various authentication and fraud prevention solutions. This growth will likely enhance its overall appeal and customer satisfaction.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Telesign Intelligence




Telesign's Intelligence product enhances user verification and fraud prevention by leveraging advanced phone number intelligence. It provides real-time risk assessments, comprehensive reason codes, and intelligent recommendations to help businesses make informed decisions about user risk.

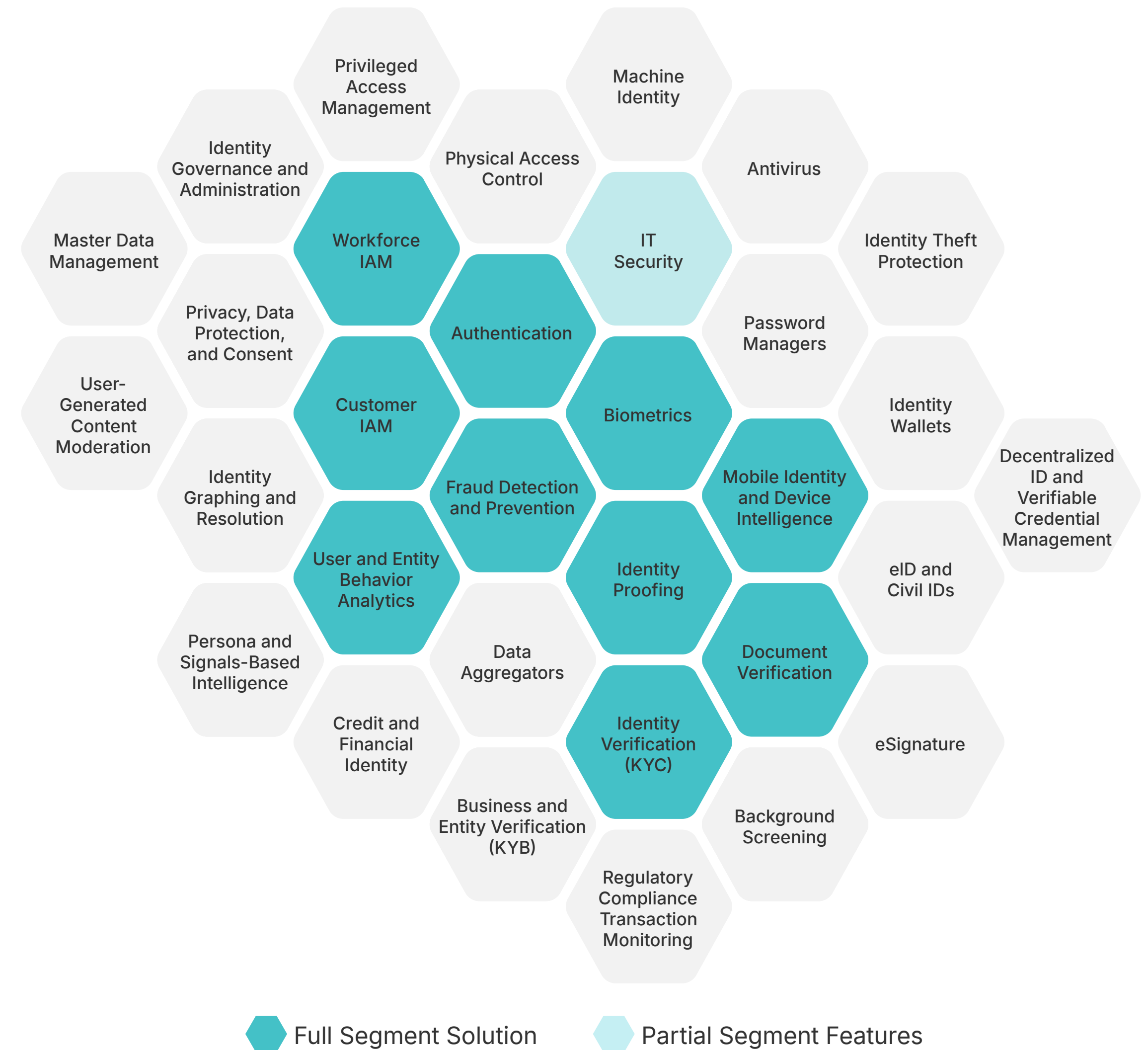
The solution dynamically evaluates fraud risk throughout the customer journey, using tailored scoring models and a proprietary global data consortium to analyze billions of consumer data points, identity signals, and traffic patterns. This enables businesses to identify and block potential fraud before it happens, ensuring a secure and seamless user experience.

Telesign's Intelligence product integrates seamlessly into existing security workflows, offering customizable machine learning models that deliver accurate and actionable insights. It also supports global reach with over 120 optimized points of presence and 700+ direct-to-carrier routes, allowing businesses to scale efficiently. The flexible, pay-as-you-go pricing model and volume-based discounts make it accessible for companies of all sizes. Additionally, Telesign offers a free trial for developers and technical product managers to test the product's capabilities. Overall, Telesign's Intelligence product empowers businesses to protect their brand reputation, reduce fake accounts, and mitigate fraud with high accuracy and minimal friction for legitimate users.

Transmit Security

Transmit Security, founded in 2014, is a customer identity and access management (CIAM) solution provider based in Tel Aviv and Boston. The company has developed a comprehensive cross-identity-lifecycle platform that includes capabilities in identity verification, customer authentication, orchestration, identity management, fraud detection and response, and data validation.

Company Information ¹	
Headquarters	Boston, Massachusetts
No. of Employees	332 as of May 2024
Last Raised	\$543M, Series A Round in June 2021
Primary Segment	Customer IAM, Workforce IAM, Fraud Detection and Prevention
Vertical Focus	Financial Services, Telecommunications, E-commerce, Transportation
Geographic Focus	North America, Europe, Middle East, Asia-Pacific
Notable Customers	  



(1) Link

Transmit Security's Strategy

Strategy	Exceptional	Transmit Security offers robust authentication capabilities and has delivered innovative passwordless authentication capabilities – their solution is well regarded in terms of cost.
Behavioral Capabilities	Exceptional	The Transmit Security platform employs AI-driven detection and response mechanisms that continuously monitor and analyze hundreds of risk signals, such as device configurations and user behavior, to identify and mitigate suspicious activities in real time.
Passwordless Authentication	Exceptional	Transmit Security offers advanced passwordless authentication capabilities, including WebAuthn, QR code authentication, and device-bound passkeys. By integrating Transmit Security's passwordless authentication with third-party platforms, businesses minimize security risks while reducing customer friction across various channels and devices.
Cost	Exceptional	Transmit Security primarily prices its platform based on the number of Monthly Active Users. Moreover, the company offers discounts for multi-year commitments, which can be attractive for organizations looking to secure favorable pricing over an extended period – 80% of surveyed customers indicated satisfaction with their cost.
User Experience	Excellent	Integrating Transmit Security's passwordless authentication with Microsoft Azure Active Directory B2C Excellent enhances security by meeting the PSD2's Strong Customer Authentication requirements and supports biometric and phishing-resistant authentication. Transmit improves UX with one-step passwordless MFA, and enables convenient omnichannel authentication.

Analyst Notes on Strategy

Transmit Security offers an advanced attack simulator that enables users to understand and experiment with emerging threats, demonstrating their commitment to cover a wide range of fraud use cases. Through the "Simulate" tab of the user interface, users can select from various attack types—such as bots, emulators, spoofed devices, and virtual machines—and customize simulations by adjusting parameters like the number of requests or unique devices involved. This tool provides insights into how attacks differ from regular traffic by comparing traffic characteristics against known legitimate traffic.

By integrating multiple detection methods, the Transmit Security platform enhances its ability to tackle the sophisticated challenges of cyber fraud. The attack simulator is an educational tool and a practical resource for training teams on handling and mitigating potential threats. Scheduled for public release, the simulator is available in preview upon request, providing a comprehensive platform for hypothetical testing and real-world attack response within the Transmit Security ecosystem.

Transmit Security provides orchestration capabilities that allow customers to customize and optimize their user journeys. Customers can conduct A/B testing, make adjustments, and deploy changes to production through their enterprise-grade interfaces. The system includes built-in monitoring and instant rollback capabilities for seamless performance management. The solution can integrate with other identity and data sources through a simple user interface.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Transmit Security's Market Presence

Market Presence	Excellent	Transmit Security is well recognized among ATO prevention solutions seekers in financial institutions. They boast an impressive client list and a strong global presence.
Brand Awareness	Strong	Transmit Security is primarily a customer identity and access management provider. However, solutions seekers recognize their platform solution as being able to solve account takeover prevention - 44% of surveyed buyers were familiar with their brand.
Market Leadership	Excellent	Transmit Security is widely recognized among its competitors, specifically for its contributions to the adoption of passwordless authentication in the customer context and is perceived to be a market leader by 25% of surveyed solution seekers.
Market Penetration	Excellent	The capital infusion from its Series A funding has enabled Transmit to focus on global expansion, extending its reach across North America, Latin America, Europe, and Asia. Major brands like Citibank, UBS, and Santander utilize the company's technology, indicating a strong market penetration among global financial institutions.
Company Size	Excellent	Transmit Security, with 332 employees, is positioned between larger, more vendors in the market. The company's headquarters is in Boston, with an additional presence in Canada, Israel, Japan, and the United Kingdom.
Employee Growth	Exceptional	Transmit has experienced an 11% decrease in employees over the past year. However, its IT department has grown by 11%, suggesting a recent strategic emphasis on strengthening the company's internal network security, especially as the company continues to expand its global customer base.

Analyst Notes on Market Presence

Since June 2021, following the announcement of a record-setting Series A funding round for cybersecurity, Transmit Security has increased its first-half revenues by 40% year over year, expanded its workforce by 41%, and grown its customer base by 51%, surpassing \$100 million in annual recurring revenue. The company has added notable clients such as Goldman Sachs, BRED Banque Populaire, and America's Car-Mart to its roster, which already included major firms like Citigroup, Lowe's, UBS, Santander, and HSBC. In March, Fast Company recognized Transmit Security as one of "The 10 Most Innovative Security Companies" for 2022. Additionally, the company has rebranded and reorganized its product suite—BindID, RiskID, FlexID, VerifyID, and UserID—under the Transmit Security CIAM Platform, streamlining the process for enterprises to obtain identity services that balance security with customer experience.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Transmit Security Platform

The Transmit Security platform offers a variety of solutions, including customer identity management, identity verification, and fraud prevention. Their solution spans the entire customer lifecycle, from onboarding to login to transactions. Specifically, the security platform prevents account takeover (ATO) through multiple authentication mechanisms such as multi-factor authentication (MFA), passkeys, and identity verification.

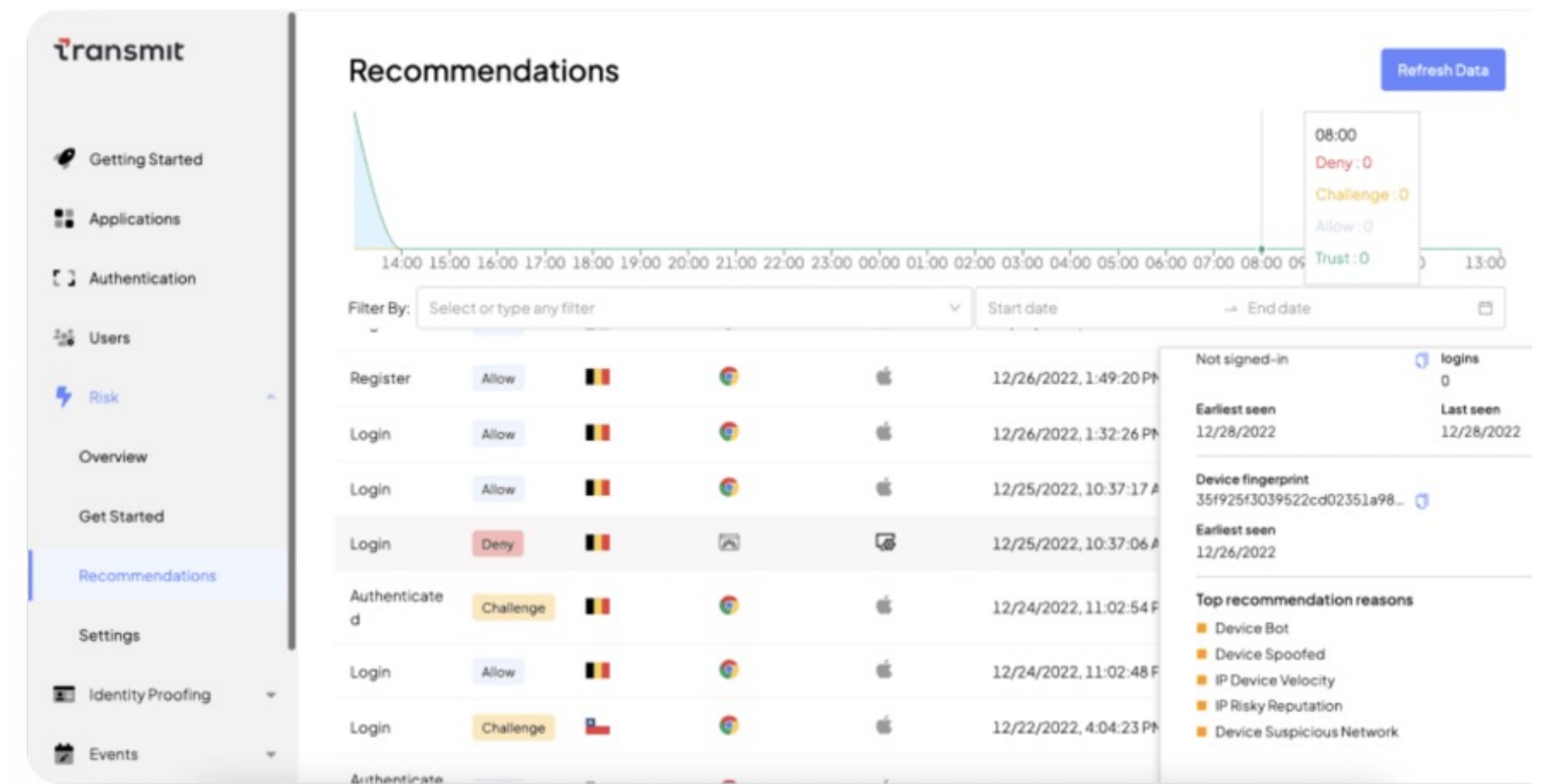
ATO Prevention Product Capability Coverage¹

H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
 (2) Product visuals sourced from company website (link: <https://transmitsecurity.com/platform/full-stack-authentication>).

Product Visuals²



Transmit Security Platform

Product	Exceptional	Transmit offers a robust product suite that layers in both authentication and fraud capability coverage to provide one of the most comprehensive ATO product offerings.
Product Capability	Exceptional	Transmit Security boasts one of the most comprehensive product suites for ATO prevention. The company offers extensive fraud prevention and authentication capabilities, ensuring full protection throughout the customer lifecycle.
Scalability	Excellent	Working with large banks like UBS, Transmit has demonstrated its ability to effectively scale alongside major financial services organizations. This capability ensures they can handle substantial user bases as they grow and face increased volumes of transactions and authentication attempts.
Customization	Excellent	With its modular platform, Transmit Security allows customers to selectively choose the ATO prevention measures that best fit their organization. This flexibility provides strong customization, enabling banks to offer tailored solutions that meet their specific needs.
Accuracy	Excellent	By utilizing a layered approach to ATO prevention, Transmit Security incorporates various behavioral signals and authentication methods, such as biometric authentication and behavioral analytics. This helps maximize the ability of anti-fraud teams to differentiate between legitimate and phony users.
Product Integration	Exceptional	Transmit Security's platform enables customers to effortlessly add new capabilities and use cases without requiring lengthy implementations, decreasing the need for extensive engineering capabilities from banks.
Buyer Satisfaction	Excellent	Transmit Security's platform, known for its robust fraud and authentication suites, satisfies customers by offering a comprehensive range of capabilities within a single solution. This approach reduces the need to rely on multiple vendors for ATO prevention.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Transmit Security Platform

The Transmit Security Platform integrates a wide range of sensor-driven telemetry and digital data feeds from various detection frameworks, such as device fingerprinting, behavioral biometrics, and bot detection. This data is enhanced by integrating global threat intelligence and analyzed against a customer's usual behavior to provide a comprehensive, real-time view of ATO risk.

The platform's unified service consolidates data to prevent the creation of silos and uses machine learning to make informed, context-aware security decisions. It uses machine learning and artificial intelligence to detect new threats as they emerge and adapt continuously by updating its detection mechanisms and algorithms. This ongoing evolution in security measures helps maintain robust protection against the latest threats.

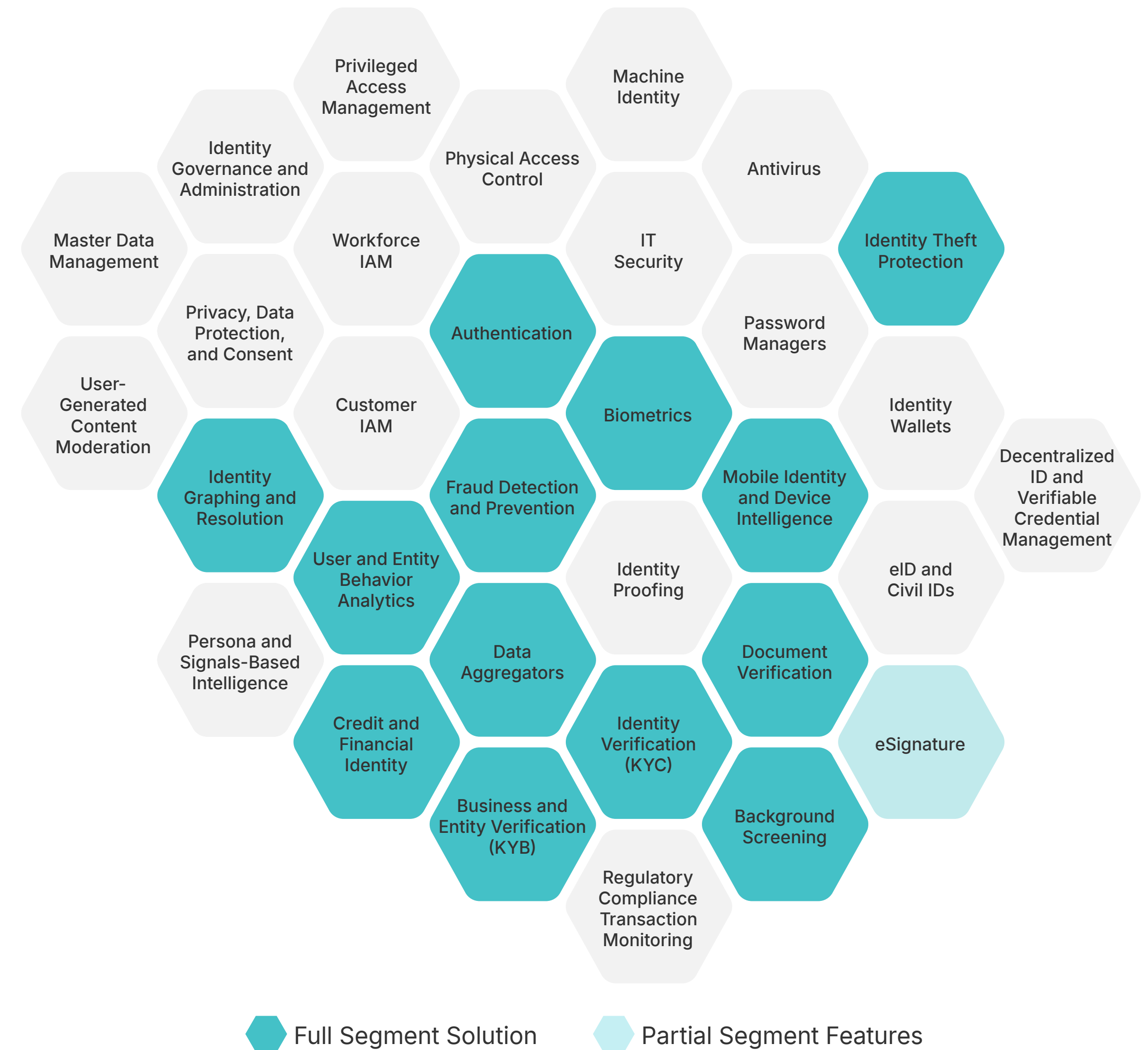
Furthermore, the platform offers unified, orchestrated customer identity and access management (CIAM) services that secure and simplify the entire identity lifecycle, reducing IT efforts and costs. It supports integration with other services like Identity Verification and Authentication, enhancing its ability to manage risks efficiently. Continuous trust profiling and device fingerprinting allow for the reduction of unnecessary security steps for verified users, improving the user experience without sacrificing security.

TransUnion

TransUnion is a leading credit bureau in the United States, supplying consumers and businesses with information essential to granting and receiving consumer credit. The company also offers a breadth of services across customer engagement and financing lifecycle, including identity resolution, fraud prevention, financial risk management, customer contact, and enhanced due diligence (EDD) investigations. Transunion’s anti-fraud capabilities include identity verification, device intelligence, authentication, and fraud analytics. Transunion’s offerings are backed by extensive data aggregation efforts and enhanced by the recent acquisitions of Neustar and Verisk Financial.

Company Information ¹	
Headquarters	Chicago, Illinois
No. of Employees	15069 as of May 2024
Last Raised	\$1.4B, Post-IPO Debt in April 2018
Primary Segment	Credit and Financial Identity, User-Generated Content Moderation, Identity Theft Protection, Fraud Detection and Prevention, Data Aggregators
Vertical Focus	Financial Services, Retail, Energy, Gaming, Healthcare, Government, Media and Entertainment
Geographic Focus	North America, Europe, Middle East, Asia-Pacific, Latin America
Notable Customers	TransUnion does not publicly disclose banking customers

(1) Link



TransUnion's Strategy

Strategy	Strong	TransUnion leverages a wide range of data signals for passive threat detection, ensuring a strong user experience with multiple pricing options.
Behavioral Capabilities	Excellent	TransUnion offers behavioral analytics but does not provide behavioral biometrics, which is highly demanded by customers, especially with anticipated increased adoption over the next two years. However, TransUnion leverages its expansive datasets for behavioral analytics to effectively detect anomalies and ATO.
Passwordless Authentication	Strong	TransUnion does not offer passwordless authentication solutions such as passkeys for ATO prevention. Instead, the company leverages fraud prevention signals to detect anomalies and prevent bad actors from causing financial losses.
Cost	Excellent	TransUnion's pricing varies by region but is generally usage-based, with additional bundle options available for specific clients. Customers have reported high satisfaction with the company's cost-effectiveness.
User Experience	Excellent	According to banking customers, TransUnion offers an excellent user experience. The company analyzes numerous data points, including location, device-level data, and a data consortium, to detect anomalies without introducing friction through authentication prompts.

Analyst Notes on Strategy

TruValidate's Digital Insights capability utilizes behavioral analytics and machine learning to analyze device recognition, context, and online behaviors. This enables organizations to improve customer conversions and better determine the riskiness of anonymous users in real-time. This component helps identify and mitigate potential fraud risks associated with digital interactions.

While the solution does not offer passwordless authentication capabilities, it boasts robust authentication capabilities through its Omnichannel Authentication and Step-Up Authentication components. The Omnichannel Authentication feature leverages phone and device data to separate legitimate consumer interactions from potentially risky ones, effectively mitigating account takeover fraud across call center and digital channels. It seamlessly integrates with existing workflows to recognize consumer devices, creating a hassle-free second layer of authentication. For scenarios requiring more robust authentication measures, TruValidate provides advanced Step-Up Authentication solutions. These include Phone Number Verification, which leverages unique global phone datasets corroborated with authoritative ownership linkages to verify associations between users and phone numbers before issuing one-time passcodes (OTPs), guarding against fraud vectors like SIM swapping. Additionally, the Adaptive Authentication feature allows organizations to customize out-of-wallet exam questions derived from diverse data sources according to transaction risk and organizational needs, providing an adaptable authentication approach.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

TransUnion's Market Presence

Market Presence	Exceptional	Transunion is a large credit reporting agency with strong buyer awareness and market leadership among financial institutions—they have strong financial backing and are well-positioned in the market.
Brand Awareness	Exceptional	As a large credit reporting agency, Transunion benefits from competitive brand awareness among financial institutions – roughly 77% of surveyed practitioners were familiar with their brand and solutions for ATO prevention.
Market Leadership	Exceptional	Of surveyed financial institution practitioners familiar with Transunion, 52% considered their solutions market-leading. This demonstrated the market's receptiveness to Transunion's fraud prevention solutions.
Market Penetration	Exceptional	TransUnion has achieved significant market penetration in the financial services sector. Its U.S. Financial Services revenue reached \$352 million in the first quarter of 2024, marking a 13% year-over-year increase.
Company Size	Exceptional	TransUnion, headquartered in Chicago, Illinois, employs over 15,00 people globally and operates in over 30 countries across five continents. The company reported a total revenue of \$3.7 billion for the full year 2023, reflecting its substantial market presence and growth.
Employee Growth	Excellent	Transunion has had significant employee growth – around 20% YoY. This growth is part of the company's broader strategy to optimize its operating model and advance its technology, despite plans to cut 1,300 jobs as part of a multiyear transformation plan.

Analyst Notes on Market Presence

TransUnion is a global information and insights company providing consumer risk data, analytics, and technology solutions to various industries. TransUnion is one of the three major credit reporting agencies and has a significant presence in the consumer credit and risk management markets. The company serves 92% of the Fortune 100 companies, 84% of the Fortune 500 companies, nine of the world's top ten banks, and 21 of the world's top 25 insurers. Moreover, their Truvalidate product has protected over 63 billion transactions.

In 2021, Transunion signed a definitive agreement to acquire Neustar, a premier identity resolution company with leading Marketing, Fraud, and Communications solutions, from a private investment group led by Golden Gate Capital and with minority participation by GIC. The acquisition expanded TransUnion's powerful digital identity capabilities by adding Neustar's distinctive data and analytics, such as a comprehensive consortium data set, enabling consumers and businesses to transact online more confidently.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

TransUnion TruValidate

TransUnion TruValidate is a fraud prevention solution that uses consumer identity data, device identifiers, and behavior patterns to verify identities and detect fraud. It integrates with existing systems to provide real-time risk assessments, aiding businesses in user authentication and fraud prevention. TruValidate enhances security and user experience through advanced data analytics and machine learning techniques.

ATO Prevention Product Capability Coverage¹

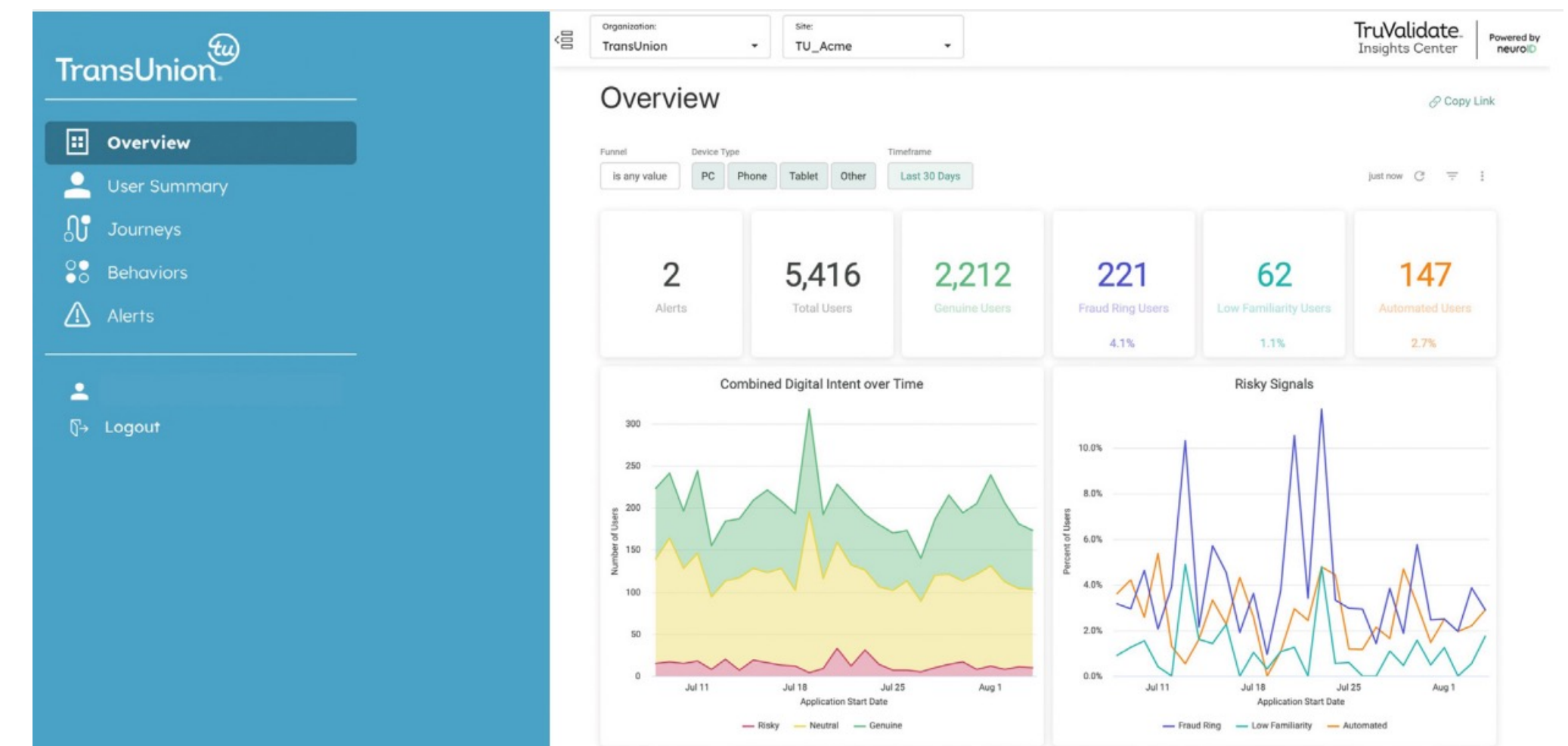
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand **M** Medium Demand **L** Low Demand

(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology

(2) Product visuals sourced from public sources (link: <https://www.helpnetsecurity.com/2022/09/28/transunion-truvalidate-device-risk-with-behavioral-analytics/>).

Product Visuals²



TransUnion TruValidate

Product	Excellent	TransUnion offers a wide range of product capabilities and very strong scalability to protect against ATO.
Product Capability	Excellent	TruValidate boasts a robust capability set, including highly demanded features such as biometric authentication, SMS OTP, and social engineering and scam detection. Additionally, it offers coverage of other critical signals like location intelligence and proxy/VPN detection.
Scalability	Exceptional	TransUnion has demonstrated its capability to service substantial-sized customers, being one of the largest credit bureaus globally. This enables it to scale effectively with banking customers as they continue to grow.
Customization	Excellent	By offering both authentication and fraud capabilities along with identity information, TransUnion provides multiple methods to prevent ATO. This allows for solutions that can be customized to meet the specific needs of different organizations.
Accuracy	Excellent	TruValidate utilizes advanced device intelligence to uncover fraud rings and detect patterns of anomalous behavior. The company further enhances accuracy by leveraging its robust identity information to provide precise solutions.
Product Integration	Excellent	TruValidate offers a single API integration, allowing banking customers to easily implement the solution into their tech stack. This enables them to select the specific capabilities they need, simplifying the integration process and enhancing flexibility.
Buyer Satisfaction	Exceptional	TransUnion boasts one of the highest buyer satisfaction ratings among the vendors we profiled. This is driven by a robust set of capabilities and highly scalable solutions that effectively serve a diverse range of customers.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes TransUnion TruValidate

TransUnion's TruValidate is a comprehensive fraud prevention and verification solution that orchestrates identity, device, and behavioral insights to help organizations securely interact with legitimate consumers while mitigating fraud risks. It delivers an accurate and comprehensive view of each consumer by linking proprietary data, personal data, device identifiers, and online behaviors. TruValidate leverages TransUnion's vast identity data, including over 1 billion worldwide customer records, 50+ petabytes of data, and over 4 billion monthly data updates from 200+ trusted identity data sources across 200+ countries. This data is continuously corroborated and evaluated using advanced data science and machine learning to ensure the most accurate offline, offline-to-online, and online-to-online linkages.

The solution provides several key capabilities, including Identity Insights, which helps verify consumer identities against robust credit, non-credit, and digital data sources worldwide, improving experiences and exposing fraud risks. Digital Insights improves customer conversions and determines the riskiness of anonymous users in real time with insights into device recognition, context, and behaviors. TruValidate also offers Omnichannel Authentication, leveraging phone and device data to separate legitimate consumer interactions from potentially risky ones, mitigating account takeover fraud across call center and digital channels. Additionally, its Fraud Analytics component streamlines transactions, detects hidden connections and proactively monitors threats with custom and purpose-built models, embedding sophisticated data and analytic expertise into the solution.



LINK INDEX

Survey Results

©2024 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 Demand Survey Results Overview

We conducted outreach to banking customers who leverage ATO prevention solutions.

Our survey¹ reached 50 leading professionals in the identity and fraud space as respondents. We received significant participation from representatives of large enterprises with extensive global customer reach and gathered responses from various functional roles within each organization.

According to our survey findings, we've collected valuable insights to grasp the market's demand for ATO prevention solutions.



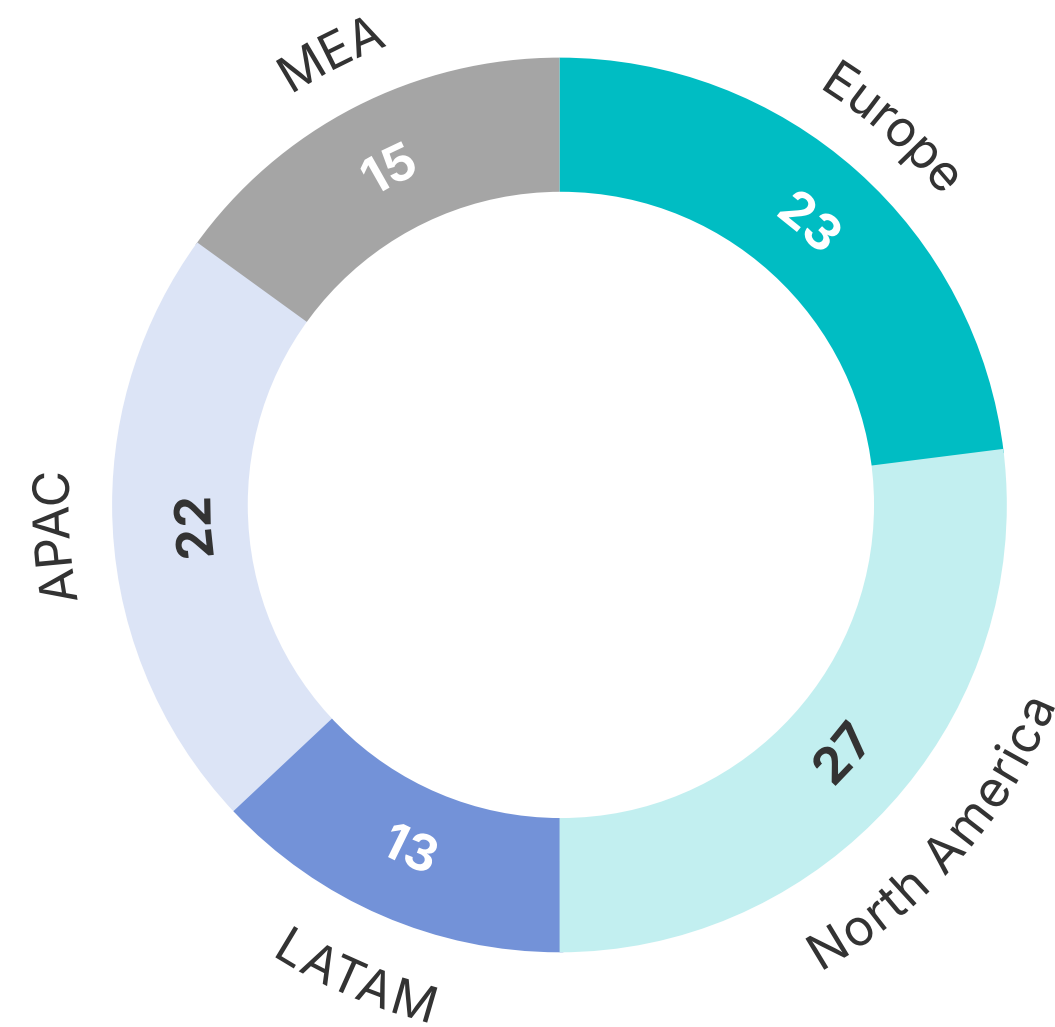
(1) All results referred to below are sourced from ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Survey Demographics: Buyer Profile

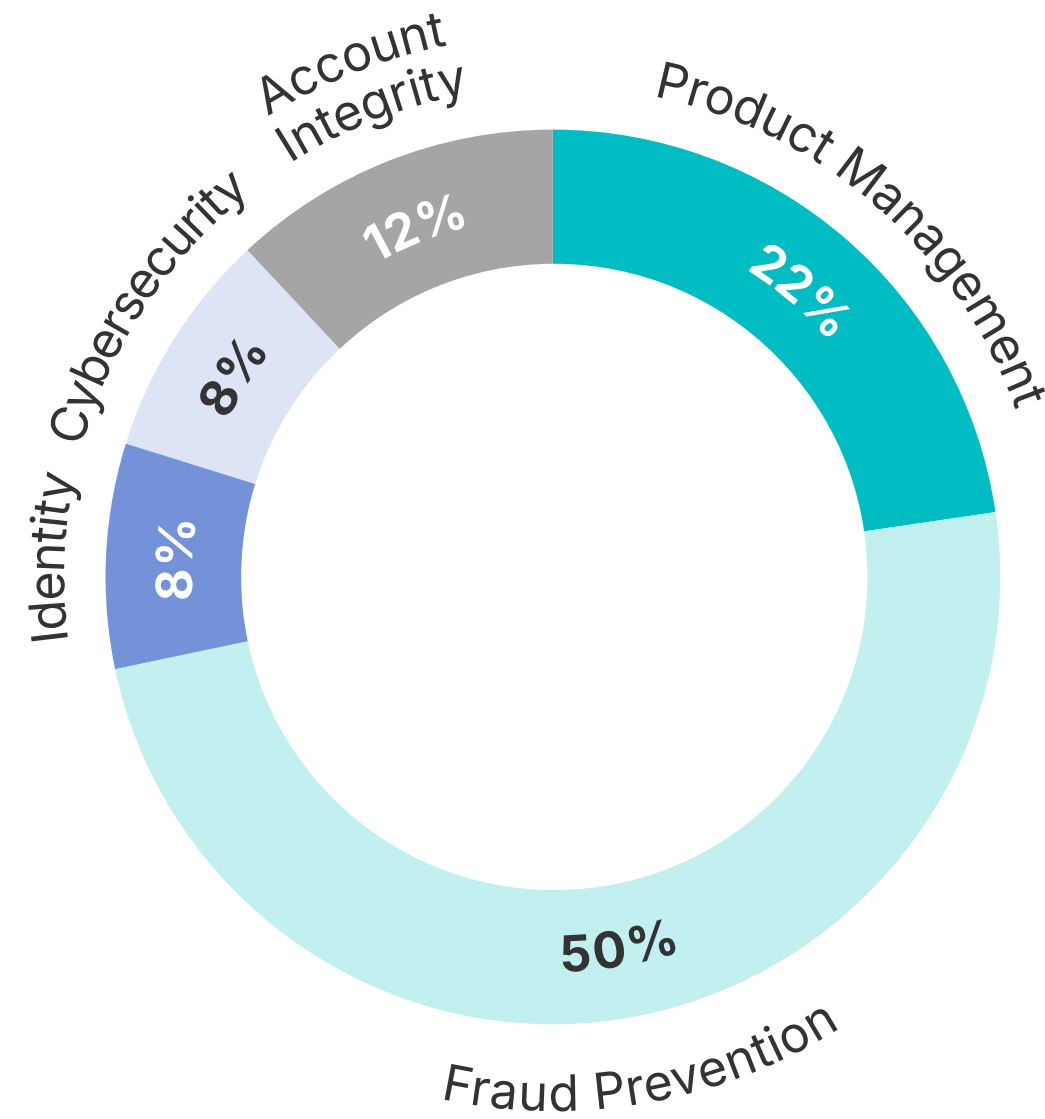
Our survey had a global set of respondents from several geographies, functional areas, and company sizes who are current solution seekers of ATO prevention solutions.

Survey Respondent Demographics (N = 50)

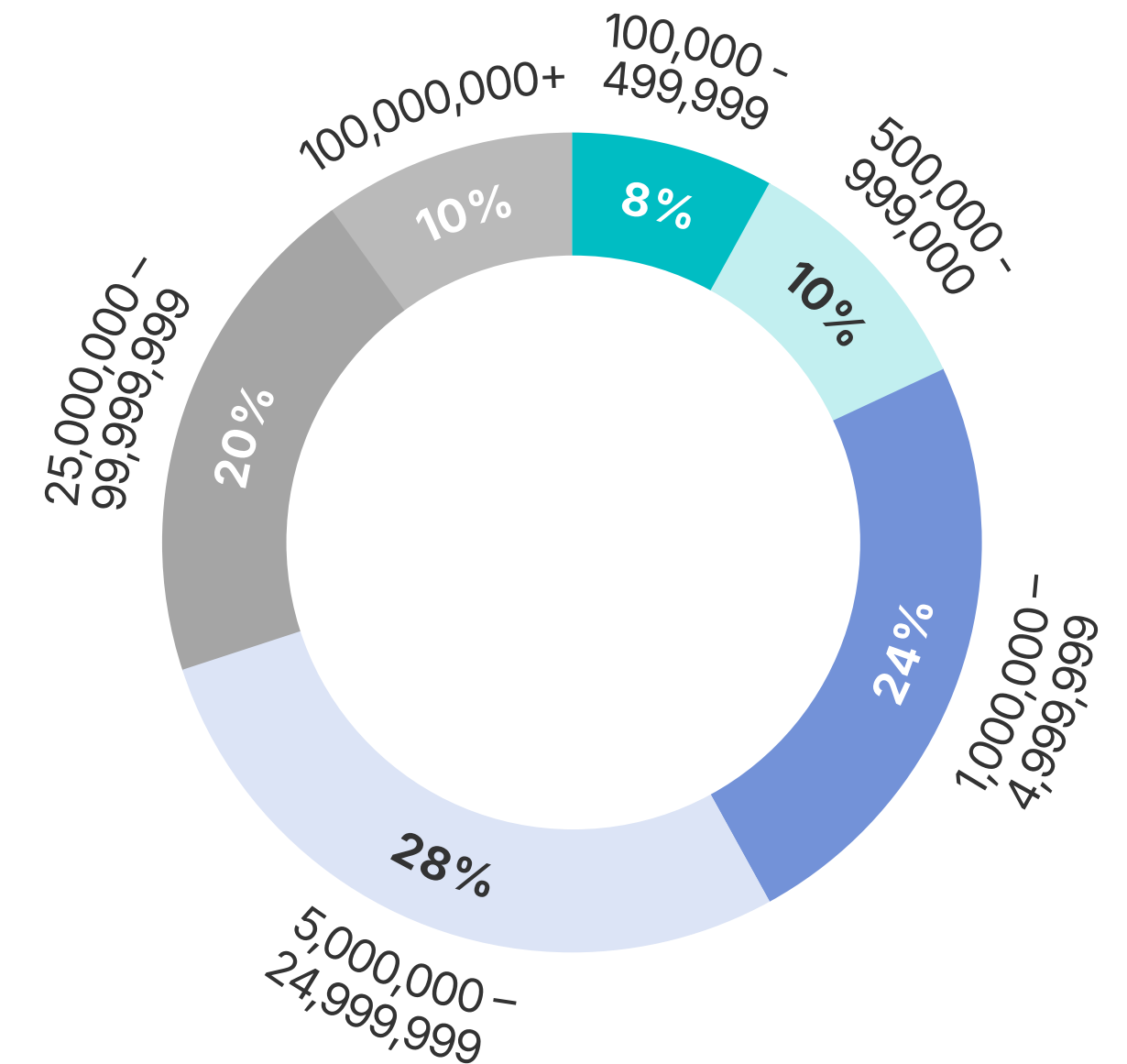
Geography (By Region¹)



Functional Area (By Department)



User Count

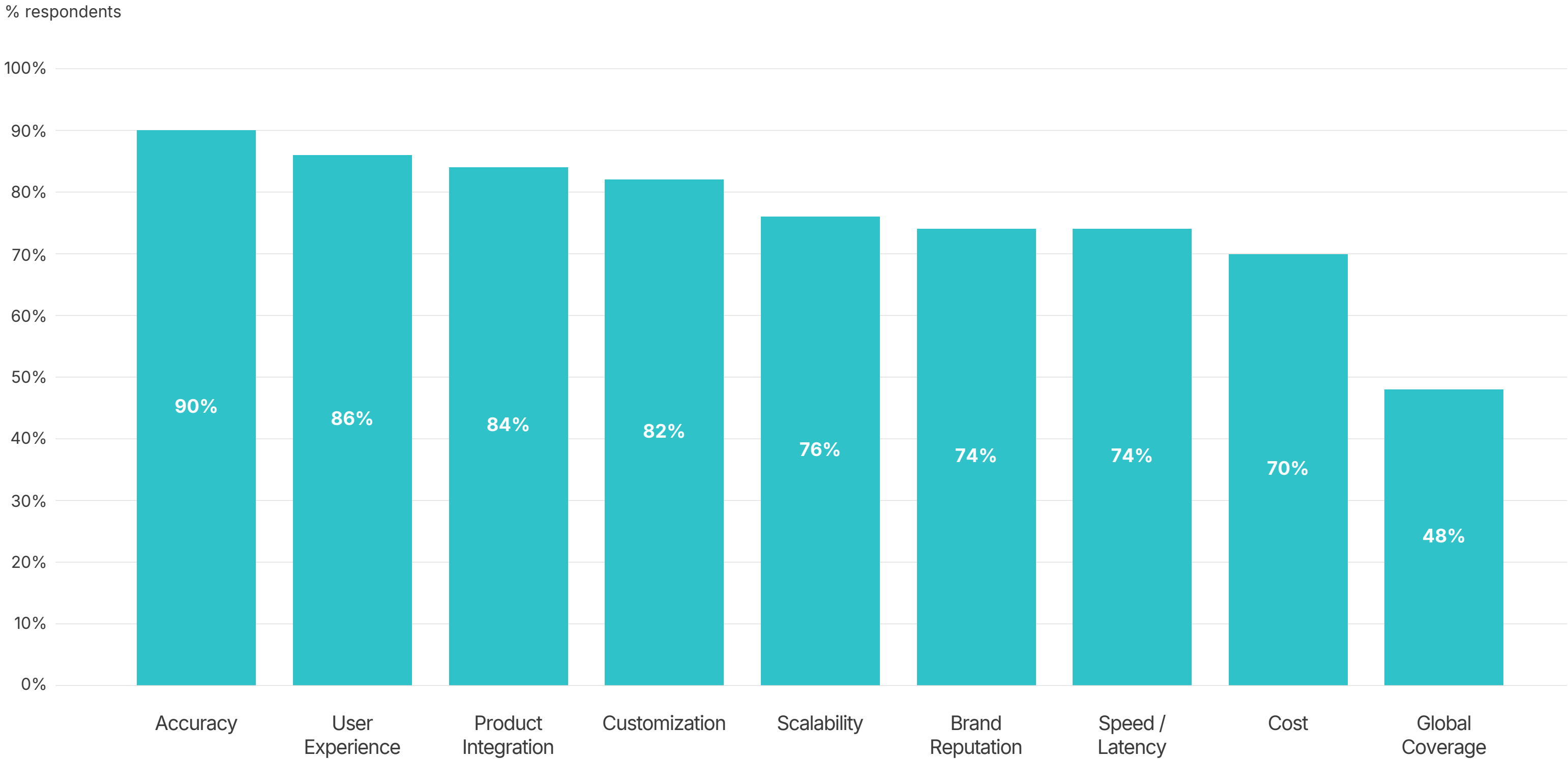


(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Top KPCs include accuracy, user experience, product integration, and customization for ATO prevention in banking

Key Purchasing Criteria for ATO Prevention Solutions in Banking

How would you prioritize the key purchasing criteria for ATO solutions?



Accuracy (90%), user experience (86%), product integration (84%), customization (82%) are the most important key purchasing criteria for ATO prevention in banking.

Banks prioritize accurate, user-friendly, and easily implementable customizable solutions.

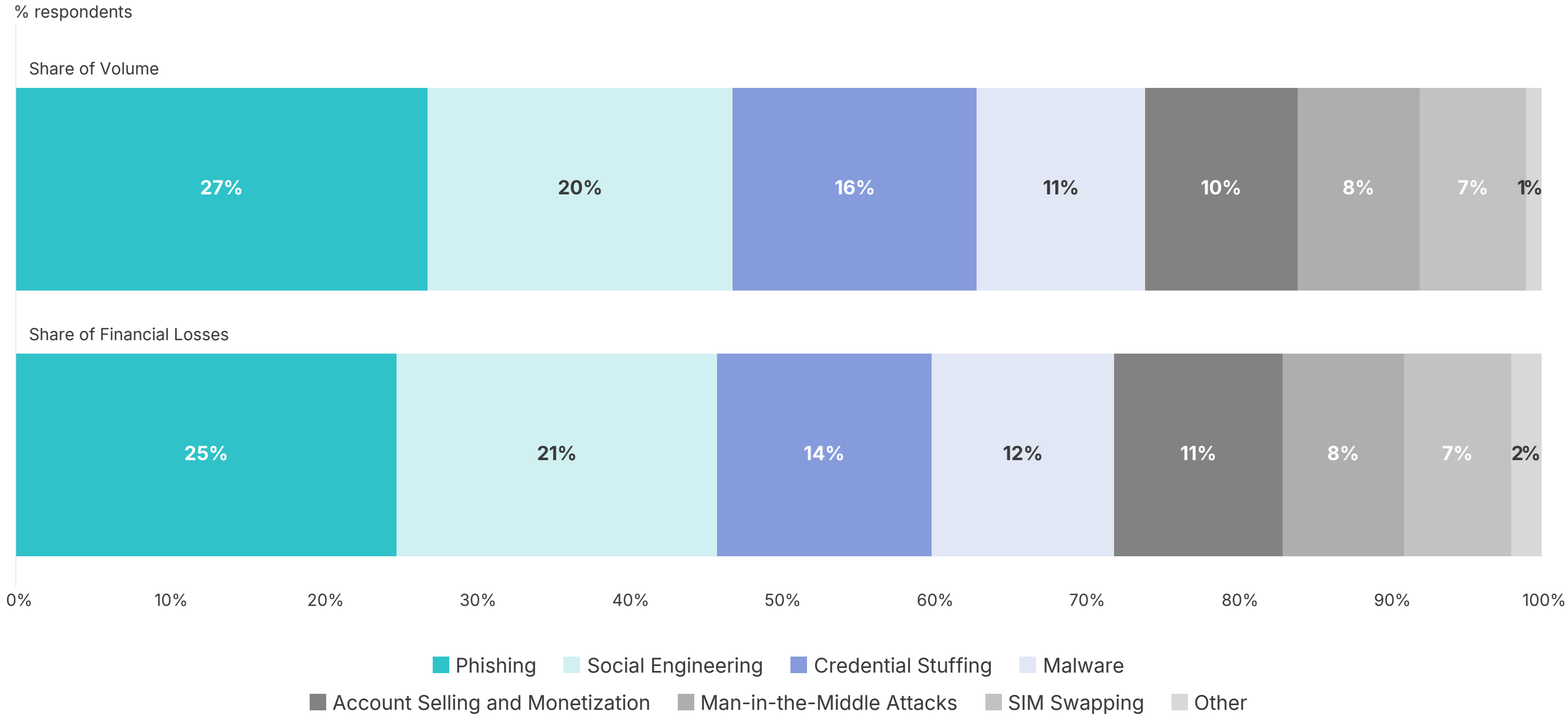
Interestingly, global coverage, cost, and speed performed the weakest among our proposed key purchasing criteria. This suggests our buyers face highly localized and expensive problems, that are not addressed though maximizing efficiency but rather by optimizing for effectiveness.

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Phishing and social engineering are the top ATO threat vectors

ATO Attack Vectors by Share of Financial Losses and Share of Total Volume¹

What percentage of total ATO attack volumes are made up of the following threat vectors?
 What percentage of financial losses from ATO attacks are made up of the following threat vectors?



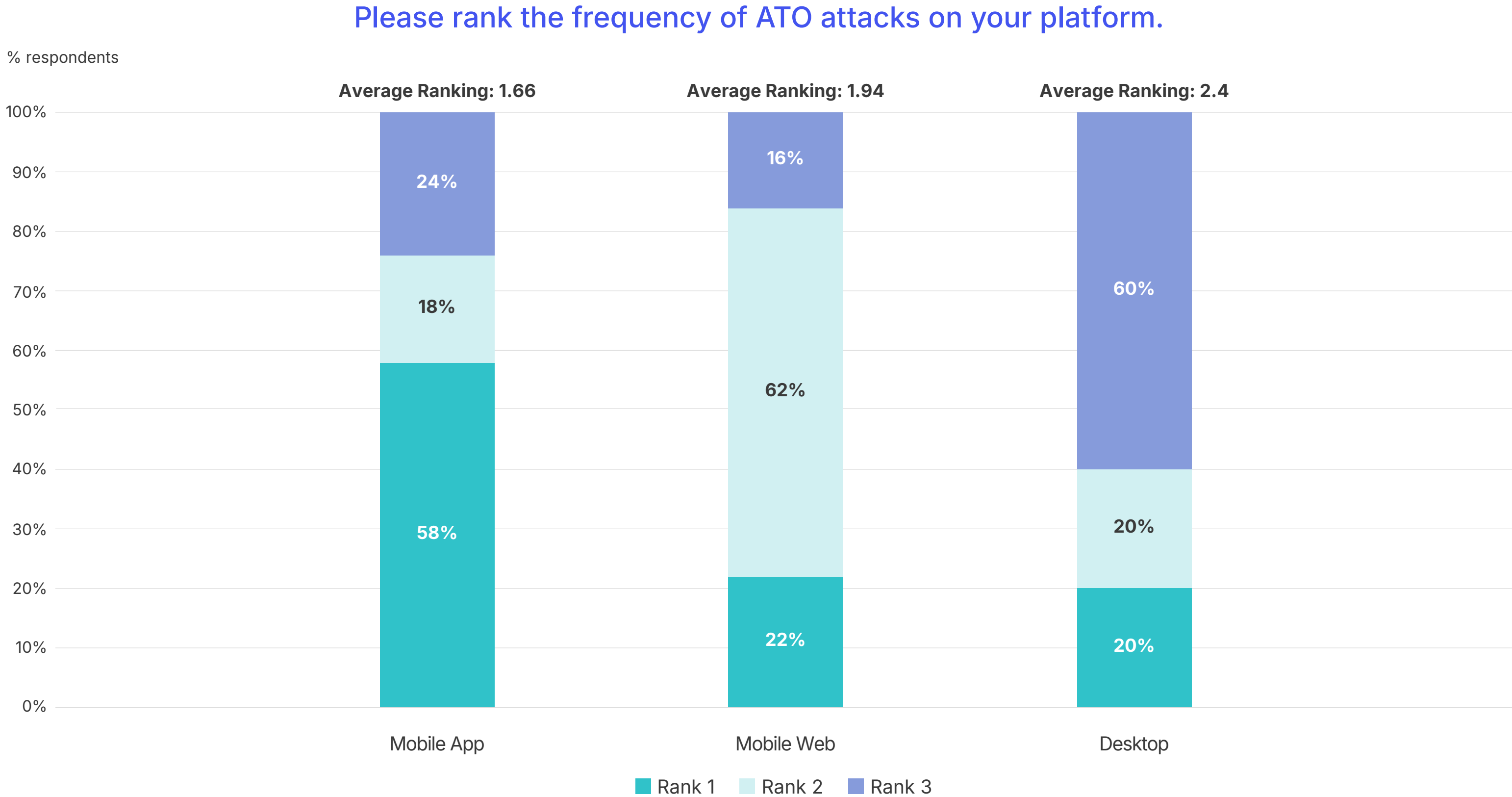
Phishing and social engineering are the biggest ATO threat vectors in terms of financial losses and total volume, with credential stuffing, account selling and monetization, and man-in-the-middle attacks following behind.

Phishing and social engineering are becoming more sophisticated as generative AI tools aid fraudsters to increase the scale and sophistication of attacks.

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

ATO attacks predominantly occur via mobile app and mobile web rather than on desktop platforms

Frequency of ATO Attacks by Mobile App, Mobile Web, and Desktop¹



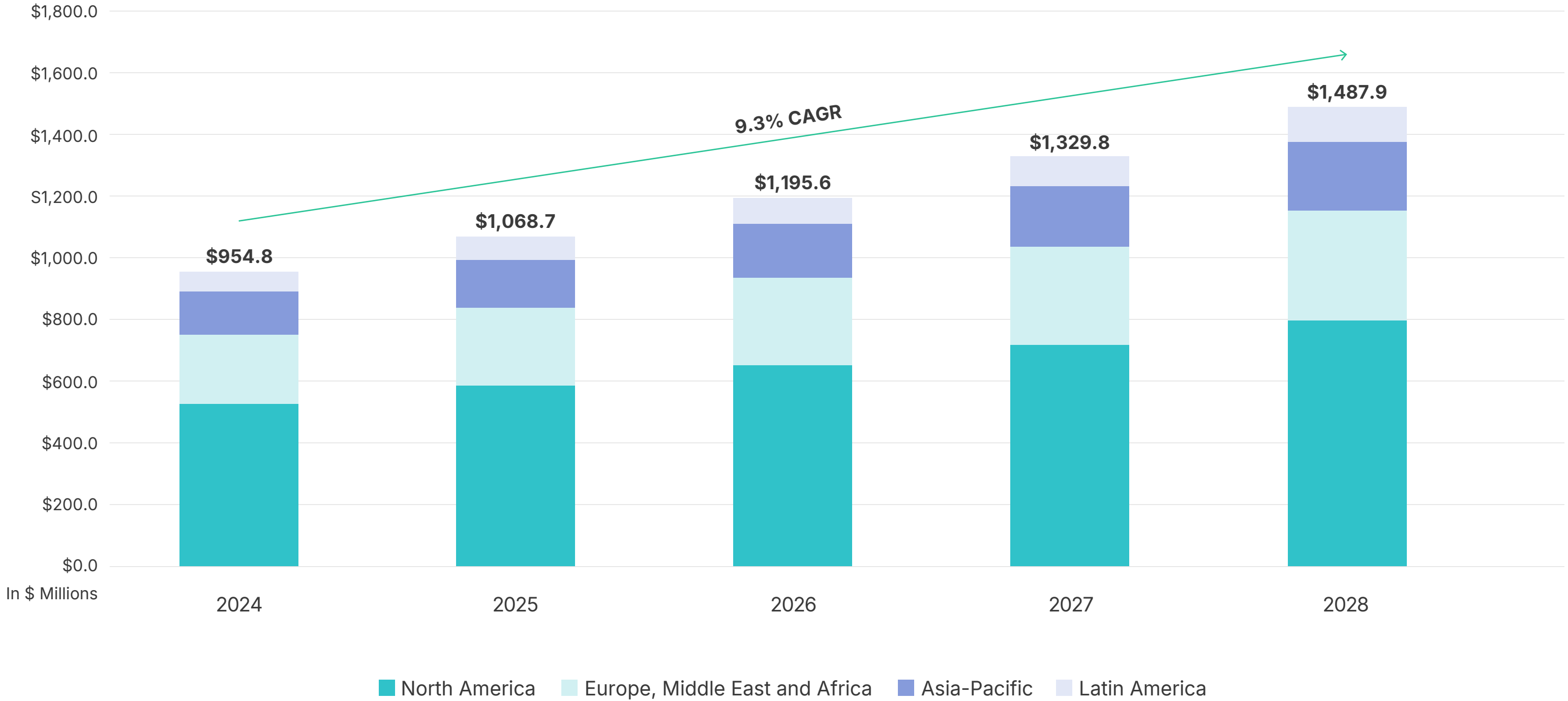
Mobile applications and mobile websites see more ATO attacks than desktop web channels, suggesting that fraudsters are prioritizing mobile channels.

Despite the outsized prevalence of mobile ATO attacks, only 44% of respondents report using mobile device signals as part of their ATO defense strategies, indicating a gap in prevention controls.

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

There is a large and growing total addressable market (TAM) for ATO prevention solutions

Market Size for ATO Prevention Solutions in Banking¹



The global TAM for ATO prevention in banking is projected to grow from about \$954.8 million in 2024 to \$1.5 billion by 2028, with a compound annual growth rate (CAGR) of 9.3%.¹

We expect that demand for solutions will persist as banks aim to combat increasing levels of ATO fraud across various regions.

(1) Liminal's proprietary market sizing model, bottom-up approach building off of datasets on individual banks along with growth trends by geography, sector and other factors.



LINK INDEX

Appendix

©2024 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



Product Capabilities Definitions: High Demand

Demand	Product Capabilities	Definition
H	App-based Authentication	Biometric authentication is a process that verifies a user's identity using unique biological traits such as fingerprints, voices, retinas, and facial features.
H	Biometric Authentication	Biometric authentication is a process that verifies a user's identity using unique biological traits such as fingerprints, voices, retinas, and facial features.
H	Continuous Authentication	Continuous authentication is a security approach that verifies a user's identity throughout a session rather than just at the login point.
H	Data Breach Monitoring	Data breach monitoring is a threat detection capability that alerts users when one of their accounts and associated data has been leaked in a data breach. It involves tracking compromised personal information on the dark web and other illicit platforms to prevent identity theft.
H	Email-based One-Time Passcode	An email-based one-time passcode (OTP) is a form of authentication where a unique, temporary code is sent to a user's email address, which they must enter to gain access to a system or service. This code is valid for only one transaction or login session, making it more secure than a static password that could be reused or compromised.
H	SMS / Phone One-Time Passcode (SMS OTP)	SMS OTP (Short Message Service One-Time Password) is a form of two-factor authentication (2FA) that enhances security by sending a unique, automatically generated numeric or alphanumeric string of characters to a user's mobile device via text message.
H	Social Engineering and Scam Detection	Social engineering and scam detection involves rules-based or machine-learning models configured to identify customer behavior indicative of social engineering. Social engineering involves manipulating individuals to divulge sensitive information or perform actions that aid fraudsters in gaining unauthorized access to data or systems. Scam detection refers to identifying and preventing fraudulent schemes to deceive individuals into providing personal information or financial assets.

H High Demand

Product Capabilities Definitions: Medium Demand

Demand	Product Capabilities	Definition
M	Behavioral Biometrics	Behavioral biometrics identifies individuals based on their unique behavior patterns, particularly in 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.
M	Device Risk Scoring	Device risk scoring is a subcategory of risk scoring that assesses the trustworthiness of a device. By analyzing various factors related to the device, such as IP address, device fingerprint, and location, businesses can assign risk scores to transactions or users, enabling them to make informed decisions on whether to approve, review, or reject transactions based on the likelihood of fraud.
M	Location Intelligence	Location intelligence leverages geolocation data to understand user behavior, deliver personalized services, and enhance marketing strategies based on real-time location information.
M	Proxy And VPN Detection	Proxy and VPN Detection refers to the methods and technologies used to identify whether a user connects to a service or network through a proxy server or a Virtual Private Network (VPN).
M	SIM Swap Detection	SIM Swap Detection is a security process used to identify and prevent SIM swap fraud, a type of identity theft where a fraudster manages to transfer a victim's phone number to a new SIM card they control.
M	Time-based One-Time Passcode (TOTP)	A time-based one-time passcode (TOTP) is an algorithmically generated temporary passcode, most commonly used as a secondary factor for multi-factor authentication. TOTP can be generated by dedicated hardware tokens, websites, or mobile applications.

M Medium Demand

Product Capabilities Definitions: Low Demand

Demand	Product Capabilities	Definition
L	Behavior Analytics	Behavioral analytics is a data analysis process focusing 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.
L	Bot Detection	Bot detection involves identifying entities or individuals that mimic user behavior, such as bots, malware, or rogue applications. These may evade traditional security tools by blending with regular user activities like browsing the web or sending emails. It also refers to analyzing traffic to a website, mobile application, or API to detect and block malicious bots.
L	FIDO2 Authentication	FIDO2 is an open authentication standard developed by the FIDO Alliance, an industry standards association dedicated to addressing the limitations of traditional password-based authentication. FIDO2 authentication utilizes device-stored credentials that are immune from phishing and brute-force attacks.
L	Knowledge-Based Authentication	Knowledge-based authentication (KBA) is used for identity verification by asking personal questions about the account owner. (e.g., "What was the name of your first pet?")
L	Magic Links	Magic links are a one-time use link sent to the customer during the authentication process, enabling passwordless authentication.
L	Signal Sharing Network	Signal-sharing networks (or consortiums) are collaborative platforms where businesses share real-time fraud risk signals and intelligence to enhance fraud prevention strategies. These networks enable communication between organizations to share information regarding trusted users and bad actors.
L	User Risk Scoring	User risk scoring in fraud detection is a critical tool that evaluates the likelihood of a user's behavior indicative of fraudulent activity. This process involves analyzing various data points and behaviors, such as transaction history, login patterns, and device usage, to assign a risk score to each user.

L Low Demand

Passwordless Feature Definitions

Product Capabilities	Definition
Device Based / Cloud Based Passkeys	Device-Based Passkeys are stored locally on a user's device and use biometric or PIN-based authentication, eliminating the need for passwords. Cloud-Based Passkeys are stored in the cloud, enabling synchronization and access across multiple devices with protection through multi-factor authentication.
QR Code Authentication	QR Code Authentication is a method where users scan a QR code with their mobile device to authenticate and gain access to an account or service, typically leveraging the camera and secure apps for verification.
WebAuthn	WebAuthn is a web standard that enables secure, passwordless authentication using public key cryptography, allowing users to log in to online services security keys or other authenticators.

Exceptional, Excellent, Strong Scoring Buckets Definitions

Scoring Buckets	Definition
Exceptional	Vendors in this category represent the pinnacle of performance in the market and are in the top quartile among leading vendors for specific criteria. They not only meet all industry standards but also significantly exceed them. Exceptional vendors demonstrate advanced technological capabilities, comprehensive coverage, innovative solutions, and extraordinary customer service.
Excellent	Vendors rated as excellent provide very strong services that go beyond the basic fulfillment of criteria and are in the second quartile among leading profiles for specific criteria. They showcase high levels of proficiency and reliability in their solutions and customer support. These vendors are recognized for their robust feature sets, comprehensive integrations, and effective detection and reporting capabilities. While they may not reach the pinnacle of the Exceptional category, their performance significantly enhances customer authentication processes.
Strong	Vendors classified as strong adequately meet the established criteria necessary for effective customer authentication and are in the fourth quartile among top vendors (though perform better than vendors who did not make our final list). They provide solid, dependable technology and support. These vendors offer functional and effective solutions that satisfy basic requirements for authentication and risk detection. While they may lack the cutting-edge features of higher-ranked vendors, their services are competent and reliable for organizations looking to authenticate their customers.

Link Index Methodology: Product

Product Criteria	Weighting	Definition	Why It Matters
Product Capability	40.0%	The completeness of a vendor's product capabilities at solving ATO prevention in banking based on buyer demand.	Companies with more in-demand product capabilities are better at solving ATO prevention.
Buyer Satisfaction	15.0%	How satisfied customers report being when using a specific vendor.	A vendor who satisfies its customers is more likely to retain and increase their customer base.
Accuracy	17.5%	The ability to identify bad actors with high effectiveness.	Accurate solutions effectively decrease the amount of fraud losses without false positives.
Product Integration	10.0%	How easy a solution is to deploy / integrate for buyers.	Solutions that are easy to implement can be more easily adopted and will be able to capture more of the market.
Customization	10.0%	The degree of customization available in a solution, such as adjusting risk-scoring models, configuring rules, and setting up alerts/notifications.	Banks want to be able to fine tune ATO solutions to most effectively cater to their risk posture and customer flows to effectively provide security while limiting friction.
Scalability	7.5%	The ability to defend against high volumes of ATO attempts while maintaining effectiveness.	Vendors with scalable solutions will be able to capture bigger customers and, therefore, service more of the market.

Link Index Methodology: Strategy

Product Criteria	Weighting	Definition	Why It Matters
User Experience	30.0%	The ability of a vendor to provide ATO protection while also ensuring a seamless user experience for consumers.	Banking users want to feel like their account is adequately protected while avoiding considerable friction.
Cost	25.0%	The ability to offer cost-effective solutions for ATO prevention in banking.	Banks want to find highly effective solutions but also want to stay within budget.
Behavioral Capabilities	25.0%	Behavioral signals refer to patterns and characteristics of user behavior that are monitored and analyzed to detect fraudulent activities. Vendors with strong behavioral capabilities offer capabilities such as behavioral biometrics, behavioral analytics, and bot detection.	Behavioral signals provide highly sophisticated fraud detection leveraging passive signals, ensuring strong user experience paired security.
Passwordless Authentication	20.0%	Passwordless Authentication is a method of verifying a user without requiring a traditional password, instead relying on alternative methods. Vendors with passwordless authentication offer WebAuthn, QR code authentication, and device-based / code-based passkeys for ATO prevention.	Passwordless Authentication is a method of verifying a user without requiring a traditional password, instead relying on alternative methods.

Link Index Methodology: Market Presence

Market Criteria	Weighting	Definition	Why It Matters
Brand Awareness	25.0%	The amount of buyers that are aware of a vendor.	Well-known vendors are better suited to capture more market share.
Market Leadership	30.0%	The number of buyers who believe this vendor is a market leader.	Vendors known as market leaders are better suited to capture more market share.
Market Penetration	25.0%	The share of the market that uses a particular vendor.	Vendors that process large numbers of transactions for large clients will yield higher market penetration
Company Size	10.0%	The total employee headcount of a company.	A large company has the stability and bandwidth to take on bigger clients and drive larger revenues.
Employee Growth	10.0%	How fast a company's employee count is growing (YoY).	A growing company means it has strong prospects for revenue growth and will be a more formidable player in the market.

ROI Calculations

Reduction in Fraud Losses

Metric	Value	Source
Number of successful fraud incidents using poor solution	133,633.33	Buyer Demand Survey
% of successful fraud incidents related to ATO	33.50%	Buyer Demand Survey - weighted average
Number of ATO incidents using poor solution	44,767	Calculation
Average loss per ATO incident using poor solution	\$13,400.00	Buyer Demand Survey
Poor solution fraud losses	\$599,880,033.33	Calculation
Average customer base of those using a poor solution	36,700,000	Buyer Demand Survey
Average fraud loss per customer	\$16.35	Calculation
Number of successful fraud incidents using strong solution	76,913.65	Buyer Demand Survey
% of successful fraud incidents related to ATO	20.94%	Buyer Demand Survey - weighted average
Number of ATO incidents using strong solution	16,109	Calculation
Average loss per ATO incident using strong solution	\$6,430.50	Buyer Demand Survey
Strong solution fraud losses	\$103,589,797.00	Buyer Demand Survey
Average customer base of those using a poor solution	26,498,889	Buyer Demand Survey
Average fraud loss per customer	\$3.91	Calculation
Reduction in Fraud Losses per Customer	\$12.44	Calculation

Reduction of Operation Costs

Metric	Value	Source
Total number of employees required per ATO with poor solution	3	Assumption
Employee time (hours) spent per ATO with poor solution	6.10	Buyer Demand Survey
Cost of employee per hour	\$21.29	Indeed
Total cost of team using a poor solution	\$389.61	Calculation
Total number of employees required per ATO with strong solution	3	Assumption
Employee time (hours) spent per ATO with strong solution	5.69	Buyer Demand Survey
Cost of employee per hour	\$21.29	Indeed
Total cost of team using a strong solution	\$363.65	Calculation
Reduction of Operational Costs with a Strong Solution	\$25.96	Calculation

Customer Retention Savings

Metric	Value	Source
% of customer abandonment poor solution	19.80%	Buyer Demand Survey
% of customer abandonment good solution	15.14%	Buyer Demand Survey
Average customer lifetime value	\$4,500	Forbes
Customer base	1	Placeholder number
Customer Retention Savings per Customer	\$210	Calculation



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

| www.liminal.co/linkplatform



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

www.liminal.co | info@liminal.co



©2024 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