Gartner Licensed for Distribution

Magic Quadrant for Identity Verification

21 October 2024 - ID G00811529 - 50 min read

By Akif Khan, James Hoover, **and 1 more**

The growing identity verification market helps deliver security, compliance and trust across onboarding and other use cases. This Magic Quadrant evaluates 11 vendors to help IAM leaders select the best choice to meet their core requirements and offer lasting value.

Market Definition/Description

Gartner defines identity verification (IDV) as the combination of activities during a digital interaction that brings a real-world identity claim within organizational risk tolerances. Identity verification capabilities — delivered as SaaS, software or an appliance — provide assurance that a real-world identity exists and that the individual claiming the identity is its true owner and is genuinely present during the digital interaction.

The purpose of identity verification is to establish confidence in the real-world identity of a person during a digital interaction when curated credentials do not exist, are not available or do not provide sufficient assurance.

Identity verification is used for a variety of business use cases, such as:

- Compliance (such as know-your-customer [KYC] obligations).
- Onboarding (customer registration, remote workforce hiring and employee onboarding processes, for example).
- Account security (including support for credential management processes, such as credential enrollment and account recovery).
- Mitigating fraud risk (preventing fraudulent registrations using stolen or synthetic identities, enabling remote proctoring/invigilation, and securing high-risk transactions, for example).
- Trust and safety (including improving accountability in marketplaces, providing assurance in the gig economy and establishing trust in larger portable digital identity networks).

Mandatory Features

The mandatory features for this market include:

- Capture of a person's photo and data from a photo identification document, followed by assessment of the document's authenticity to provide assurance that the real-world identity exists. Solutions must capture the document through one of the following technologies:
  - Optical capture and processing, including optical character recognition (OCR) or analysis of bar code or quick response (QR) code.
  - Data extraction from a chip using near-field communication (NFC).
- Image capture of the person's face, with integrated liveness detection to ensure human presence, followed by biometric face comparison with the photo from the identity document.
- The complete identity verification process must be carried out by a person on a normal user device (a laptop, tablet or smartphone, for example) with no requirement for the user to rely on specialized hardware.

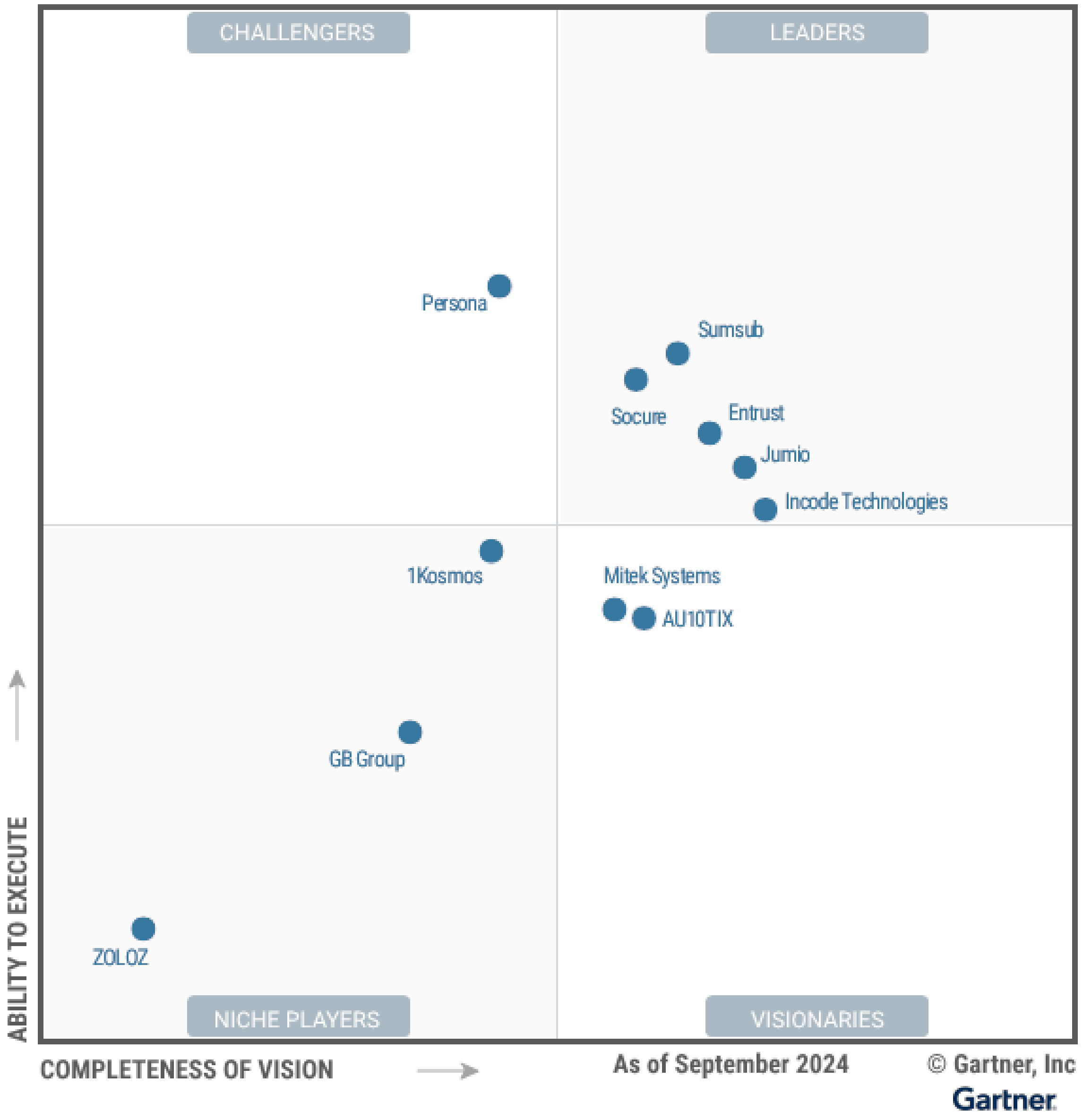
Common Features

The common features for this market include:

- Administrative portal with reporting, analytics and separation-of-duties frameworks.
- Configurable approaches for handling personal identifiable information (PII), such as retention periods.
- Connectivity with external data sources to corroborate information from the identity-verification process. Examples of these data sources include government document-issuing authorities, government biometric databases, vendor-managed identity graphs and credit bureaus.
- Support for video calls during the identity verification process, so that agents can interact with people to assess their identity claims (as required by regulation in some markets). The vendor may either supply the agents or simply provide platform features that enable organizations to use their own agents.
- Fraud detection via assessment of signals, such as location intelligence or attributes of the device being used in the identity verification process.
- Support for authentication and duplication checking using identity and biometric data (for example, by one-to-one biometric comparison and one-to-many searches of biometric data and/or identity attributes).
- Provision of an identity wallet, which enables people to store verified identity attributes and control their presentation to a relying party. Such an identity wallet could be vendor-branded or available for white labeling.

Magic Quadrant

Figure 1: Magic Quadrant for Identity Verification



Vendor Strengths and Cautions

1Kosmos

1Kosmos is a Niche Player in this Magic Quadrant. Its BlockID Verify product can be sold individually or bundled with its BlockID Workforce or BlockID Customer digital identity wallet and passwordless authentication solutions. Its operations are mostly focused in North America and APAC, and its clients tend to be large organizations in financial services, healthcare and telecom, with a small percentage in government. About one-third of clients use 1Kosmos for workforce use cases.

Recently added features include expanded coverage of more document types and the ability to configure more granular policies governing data retention. 1Kosmos' roadmap items include development of a database of fraudulent identity data and the addition of a live-agent video call to resolve exceptions in the IDV process.

Strengths

- Its IDV solution is tightly integrated with its digital identity wallet, which is widely deployed in both workforce and customer use cases. Its digital identity wallet offering is highly mature.

- It offers significant discounts for customers signing multiyear deals. As a result, it had a much higher than average number of customers who signed multiyear deals during 2023.

- The option to bundle provides additional features beyond IDV, including digital identity wallet and passwordless authentication solutions. Bundling makes it an effective solution for workforce use cases, such as onboarding and account recovery.

Cautions

- When carrying out optical character recognition (OCR) on identity documents, it is currently limited to supporting Latin, Cyrillic and Arabic character sets only. As a result, its IDV solution may not be suitable for organizations needing support for more diverse character sets.

- Its IDV product roadmap is not a point of differentiation. Several features implemented in 2023 and cited by 1Kosmos as being the most effective, such as those relating to document coverage and configurable data retention, are playing catch-up with the market. The same applies to several features expected in the coming 18 months.

- Its credible value proposition and differentiation stem from the coupling of IDV with its digital identity wallet and passwordless authentication capabilities. The value proposition for using 1Kosmos for IDV alone is somewhat diminished without these complementary capabilities.

AU10TIX

AU10TIX is a Visionary in this Magic Quadrant. Its IDV product is aimed solely at customer use cases. Its operations are geographically diversified, and its clients tend to be large organizations in financial services, cryptocurrency and the sharing economy.

Recent product developments include partnering with Microsoft (via the Microsoft Entra verified ID product) to deliver a reusable digital identity solution and introducing Serial Fraud Monitor to check presented identity data against previous identity presentations. AU10TIX's roadmap items include enhanced deepfake detection and enhanced tools for administrators.

Strengths

- It had an exceptionally low customer churn rate despite macroeconomic factors such as reduced venture capital funding and volatility in cryptocurrency markets affecting fintech firms and leading to churn elsewhere in the IDV market.

- Its customer base has a diverse geographic spread. It also has a highly diverse list of top document types processed in 2023, and it supports a wide range of character sets and languages for document OCR.

- It has a high level of accessibility, as evidenced by its voluntary product accessibility template (VPAT) and the accessibility features woven into its design and development processes. These features position it well in a market in which accessibility is increasingly important, and in some cases, a regulatory obligation.

Cautions

- It was unable to provide granular insights into user experience (UX) metrics, such as the number of image retakes that were due to poor quality. It may, therefore, lack sufficient data to address UX issues, should they arise.
- It had few examples of features that are industry-specific, and it was ineffective at demonstrating how its sales and marketing teams are structured to address different industry requirements.
- It does not have in-depth practices for assessing customer satisfaction (meaning the satisfaction of organizations contracting with them for IDV services), evaluating the maturity of customers' IDV processes or helping customers increase that maturity.

Entrust

Entrust is a Leader in this Magic Quadrant. Entrust completed an acquisition of IDV vendor Onfido in April 2024, which is now integrated with Entrust's heritage IDV solution (the combined solution was assessed for this Magic Quadrant). Its IDV product is used overwhelmingly in customer use cases. Its operations are geographically diversified, and its clients tend to be large organizations in financial services, cryptocurrency and travel.

Recently added features include the Studio no-code visual workflow editor tool and new Motion liveness detection solution. Entrust's roadmap items include enhanced deepfake detection and adding connections to government electronic identification (eID) schemes globally.

Strengths

- Its Studio no-code visual workflow editor easily allows customers to drag and drop "tasks" within the IDV journey and apply conditional logic to the outputs of those tasks. The interface is intuitive and enables users to create a single, flexible IDV journey definition.
- It has a very structured approach to researching the IDV market. In particular, it stands out for having a mature competitive intelligence function. It shows great candor and self-awareness in acknowledging factors that influence both positive and negative prospect decisions.
- Customers surveyed for this Magic Quadrant gave it a high score for customer satisfaction. It provides granular data on how it measures customer satisfaction and how this has changed over time. It can candidly identify areas for continual improvement of customer satisfaction.

Cautions

- The percentage of its IDV checks requiring a final decision from a human to drive up pass rates is high — even considering some markets' regulatory requirements for human involvement. In some cases, human involvement addresses shortcomings in its automated processing. For example, it does not offer full automation of OCR in non-Latin character sets. This high use of human involvement drives up average processing time.

- The pricing is higher for a global spread of documents than for U.S. documents only. This variance is unusual, and is likely due to its reliance on human involvement for document types it sees less often and with non-Latin character sets.
- Its discount offers for customers signing multiyear deals are low, which likely contributed to the low rate of customers signing multiyear deals in 2023.

GB Group

GB Group (GBG) is a Niche Player in this Magic Quadrant. Its IDScan product can be sold stand-alone or bundled with other services, such as its compliant onboarding solution ID3Global. Its operations are mostly focused in North America and Europe, and clients tend to be organizations of varying size in financial services, gambling and travel, mainly for customer use cases.

Recent product developments include enhancements to better detect screen replay attacks and document tampering, and deeper integration of know-your-customer and anti-money-laundering (AML) checks within the IDV process. GBG's roadmap items include combining all GBG services (including IDV) within a single API/software development kit (SDK) and portal, and extracting unstructured data from documents (e.g., utility bills).

Strengths

- It has a high level of connectivity to data sources to obtain additional signals about identity claims. Many of these come via integration with ID3Global. In addition, its GBG Trust product is an identity graph solution that can correlate signals from the IDV solution. This architecture is driven by a focus predominantly on compliance and onboarding use cases.
- The IDV solution is part of the identity division within the larger GB Group and is, thus, highly viable. Although it does not generate high revenue specifically from IDV, it has a large number of customers using its IDV solution. In addition, it had a high renewal rate in 2023.
- It offers quality image capture and verification, which reflects rigor in document capture and face matching. Notably it provides a credible, detailed explanation regarding its process for training and evaluating the machine learning (ML) models used for document assessment.

Cautions

- It is more expensive for processing IDV events in scenarios involving different volumes of only U.S. documents and scenarios involving a global spread of documents.
- Customers gave it a low score in overall customer satisfaction. It scored lowest in areas such as ease of administration for operational tasks, ability to detect fraudulent identity presentations, UX and conversion rate, and pace of innovation.
- Its VPAT showed that people with disabilities would find it hard or impossible to use the IDV solution, automated accessibility checks yielded poor results, and its SDK does not support

assistive technology (e.g., voice assistance for users with impaired vision). These findings may be a concern as accessibility becomes an increasingly important requirement, and in some markets, a regulatory obligation.

Incode Technologies

Incode Technologies is a Leader in this Magic Quadrant. Its IDV product is aimed mainly at customer use cases, with a modest percentage of clients using it in workforce use cases. Its operations are largely focused in North America and Latin America; clients are large organizations in financial services, travel and government.

Recently added features include its Workflows no-code orchestration tool and its age-estimation product. Incode's roadmap items include enhancing injection attack detection and building turnkey IDV features specifically for workforce use cases.

Strengths

- Its solution is easy to configure, with a clean and intuitive interface. This usability is largely driven by its Workflows no-code IDV journey editor, which allows users to drag and drop components of the IDV process and use conditional logic to control the user journey and potential step-up fraud checks.

- It offers a novel pricing model, with SLAs linked to conversion rate and fraud outcomes. Failure to meet the SLAs results in heavy discounts. This strategy is a potentially disruptive alternative to the standard per-verification pricing, which is decoupled from performance outcomes.

- Its product roadmap balances enhancements to core aspects (such as deepfake detection) with the addition of new features for workforce use cases. Its roadmap is also rich with features that complement its core IDV solution. Recently released features include a reusable digital identity product and an age-estimation tool that has been highly ranked by the U.S. National Institute of Standards and Technology (NIST).

Cautions

- It relies solely on a biannual Net Promoter Score (NPS) survey to assess customer satisfaction and did not provide the latest results. This approach neglects common metrics such as customer satisfaction (CSAT) scores, customer effort scores (CES) and time-to-resolution for support tickets.

- It had a high customer churn rate in 2023, which it attributes to macroeconomic factors related to customers in the fintech and cryptocurrency spaces missing growth targets or going out of business.

- It has below-average marketing execution, with a tendency to rely on promoting its AI and ML capabilities. However, as every vendor does this, focusing on AI and ML has become white noise in the market.

Jumio

Jumio is a Leader in this Magic Quadrant. Its IDV product is primarily targeted at customer use cases, with a small percentage of clients using it for workforce use cases. Its operations are geographically diversified; clients are large organizations in financial services, cryptocurrency and gambling, among others.

Recent product developments include becoming a data controller and offering an enhanced consent framework to build new features that leverage stored user data. Jumio's roadmap items include adding multimodal biometrics for user authentication and connecting to government eID schemes.

Strengths

- It can clearly articulate how its acquisitions have enhanced its IDV business and how market disruptors — such as government eID schemes, portable digital identity and the convergence of IDV with cybersecurity — will impact it.
- It has a clear sales methodology and shows strong alignment between the sales and product teams via an in-depth field enablement program. It has one of the most globally distributed direct sales teams, and it had a high deal-closing ratio in 2023.
- It has a high level of accessibility, as evidenced by its VPAT and the accessibility features woven into its design and development processes. These features position it well in a market in which accessibility is increasingly important, and in some cases, a regulatory obligation.

Cautions

- The percentage of its IDV checks requiring a final decision from a human to drive up pass rates is high — even considering some markets' regulatory requirements for human involvement. In some cases, human involvement addresses shortcomings in its automated processing, such as unsupported document types. This high use of human involvement drives up processing time.
- The pricing is higher for a global spread of documents than for U.S. documents only. This variance is unusual, and is likely due to its reliance on human involvement for document types it sees less often.
- Ease of configuration is low. While it does have a no-code visual workflow editor, it is part of Jumio's managed service, not customer-facing. This approach is out of step with the trend of empowering customers to build and manage their IDV journey workflows themselves.

Mitek Systems

Mitek Systems is a Visionary in this Magic Quadrant. Its Mitek Verified Identity Platform (MiVIP) product is aimed primarily at customer use cases, with a small percentage of clients using it for workforce use cases. Its operations are focused mainly in Europe and North America; clients are mostly large organizations in financial services, gambling and travel.

Recently added features include enhanced deepfake and injection attack detection and duplicate identity detection. Mitek Systems' roadmap items include adding the ability to issue verifiable credentials in its existing reusable identity wallet product, as well as improving the configurability and speed of its products.

Strengths

- It emphasizes innovation within the company culture. Examples include regular internal hackathon events, which are open to all employees and have been linked to over 30 new features released in the IDV solution.
- It has a particularly structured customer onboarding program, which has distinct phases of support from contract signing until 30 days after go-live. It also has a multifaceted approach to assessing customer satisfaction across six clear dimensions.
- It conducted a thorough analysis of its marketing activities in 2023 to inform its marketing approach for 2024. It also clearly articulated planned marketing campaigns, with a well-reasoned rationale for each.

Cautions

- It is more expensive to process IDV events in scenarios involving different volumes of only U.S. documents and scenarios involving a global spread of documents.
- It does not offer prebuilt integrations with customer relationship management, access management and IT service management platforms. It does not consider these to be included in the buying criteria for enterprise customers.
- Its business focuses on North America and Europe, with very minor activity in Latin America and no direct or indirect sales presence in any other regions. It processed identity documents from a limited range of countries in 2023 and supports relatively few character sets and languages for OCR.

Persona

Persona is a Challenger in this Magic Quadrant. Its IDV product is aimed mainly at customer use cases. Its operations are focused primarily in North America, with clients of varying sizes in financial services, marketplaces, social media and other areas.

Recent product developments include its Dynamic Flow no-code visual workflow editor and its Graph tool for linking and investigating identity data. Persona’s roadmap items include enhanced deepfake detection and a self-service query and analytics tool.

Strengths

- It offers strong fraud and risk controls, as well as native capabilities, such as location intelligence, device profiling and behavioral analysis, to provide contextual risk and trust signals. It also offers detailed insights via its Graph network feature and granular policy control, giving customers flexibility as to how they leverage the data.
- Its prices are low, and it does not offer multiyear contracts because it wants clients to renew by choice each year. It makes a contractual commitment to not increase pricing at renewal time. In

addition, it offers a permanent free tier (as opposed to a free trial) for low-volume customers with simple requirements.
- It has a high level of accessibility, as evidenced by its VPAT and the accessibility features woven into its design and development processes. These features position it well in a market in which accessibility is increasingly important, and in some cases, a regulatory obligation.

Cautions

- Its availability is below average; however, its uptime for 2023 was within its SLA. Its SaaS solution is hosted in Google Cloud Platform, and its uptime SLA was in line with the market average. The provided uptime data included legacy, shared tenancy deployments; however, new deployments can now be on more resilient single tenancy infrastructure.
- It is North America-focused. Most of its customers are in the U.S., and it has no sales presence outside North America or Mexico. Its strategy for acquiring customers in other countries is nascent. However, it did process a reasonably diverse set of global identity documents in 2023.
- It does not have a strategy to address the needs of customers in specific industries. Its sales and marketing efforts focus on use cases, and it aims to make its platform maximally configurable rather than develop industry-specific features.

Socure

Socure is a Leader in this Magic Quadrant. Its Predictive DocV product is aimed primarily at customer use cases, with a small percentage of clients using it for workforce use cases. Its operations are focused mainly in North America, where it is used by large organizations, but it also has some presence in Europe and Latin America, with smaller organizations via channel partners. Clients tend to be in financial services and marketplaces.

Recently added features include a new IDV forensic engine via its acquisition of Berbix. Socure's roadmap items include adding user authentication, by means of selfie reverification, and extracting unstructured data from documents, such as bank statements.

Strengths

- It offers strong fraud risk and controls. Its Digital Intelligence module gathers contextual signals related to location, device and user behavior. These data points can be assessed alone or checked against the SocureID identity graph, with the results then combined with the IDV check to reach an overall decision.
- It serves a wide range of industries, and its sales and marketing structure has a vertical focus, with a range of product features tailored to different verticals, such as reverification of delivery drivers. It is close to achieving Federal Risk and Authorization Management Program certification to serve U.S. public-sector customers.
- It has a flexible and data-driven approach to running proofs of concept with sales prospects. Its salespeople have a high closing rate, which it credits to a six-level training program for all teams selling IDV and an "extreme focus" on deal qualification.

Cautions

- Although it reports that about one-third of its customers are outside the U.S., almost all its processed documents are North American. It supports a wide range of character sets and languages for OCR, but it was unable to demonstrate actual experience in processing a diverse set of global identity documents at scale.
- Its proprietary liveness detection capability has not been tested in conformance with ISO/IEC 30107-3 (international standard for testing biometric presentation and attack detection), and its proprietary biometric face-matching algorithms have not been submitted to the U.S. NIST for testing.
- Its solution is fully automated. A case management system allows customers to provide their own agents, if needed, for exception handling. This approach may be an issue for customers in markets where review by a human agent is a regulatory requirement.

Sumsub

Sumsub is a Leader in this Magic Quadrant. Its IDV product is aimed primarily at customer use cases, with a small percentage of clients using it for workforce use cases. Its operations are geographically diversified with clients of varying sizes in financial services, cryptocurrency and gambling, among others.

Recent product developments include its Workflow Builder orchestration solution, as well as its Non-Doc product, which connects to a range of authoritative government databases. Sumsub's roadmap items include fully compliant eIDAS onboarding for European markets and source-of-funds verification for clients in the gambling industry.

Strengths

- It showed high diversity in the locations of its customer base and the top document types processed in 2023. It supports a wide range of character sets and languages for document OCR and offers out-of-the-box versions of its administrative portal in English, Spanish, Portuguese and Chinese. In addition, it has built a broad range of connections to authoritative government identity sources in different countries.
- It has a strong vertical/industry strategy, with product features tailored to verticals such as gambling and cryptocurrency exchanges. In addition, its sales and marketing teams are strongly vertically aligned, with industry champions responsible for disseminating expertise.
- In a survey of customer contacts, it scored high in overall customer satisfaction. It scored highest in areas such as ease of configuration, ease of administration, support in ensuring successful use of the solution, and pace of innovation.

Cautions

- It has not submitted its proprietary face-matching algorithms to the U.S. NIST for testing, stating that it prefers to rely on its own benchmarking.

- It delivered numerous IDV-specific features in 2023, but its stated roadmap for 2024 focuses more on IDV-adjacent features, such as AML and payment source verification, which lack relevance beyond compliance use cases. In addition, it failed to articulate a clear product strategy for portable digital identity.

- While an automated accessibility check showed strong results, it declined to provide a VPAT, which would have yielded more detailed insights. This finding may be a concern as accessibility becomes an increasingly important requirement, and in some markets, a regulatory obligation.

ZOLOZ

ZOLOZ is a Niche Player in this Magic Quadrant. Its IDV product is aimed only at customer or citizen use cases. Its operations are focused in China and other APAC markets with clients of varying sizes in financial services, marketplaces and government.

Recently added features include its ID Network identity graph product, to uncover fraud rings, and connectivity to the Chinese Ministry of Public Security's authoritative identity database. ZOLOZ's roadmap items include mobile app security assessments and being able to support on-premises deployments.

Strengths

- All of its customers are in APAC, with approximately half in China. Clients with a strong APAC focus may benefit from its expertise with APAC document types, regulation and — in particular — connectivity to authoritative government sources, such as the Chinese Ministry of Public Security.

- For market responsiveness, it presented clear examples of how it had adapted its product to meet new regulatory environments in markets such as Hong Kong and the Philippines.

- In a survey of customer contacts, it achieved an average score for overall customer satisfaction. It scored strongest in areas such as reliability and uptime, support in ensuring successful use of its IDV solution, and being a strong partner to support its customers' business growth.

Cautions

- It declined to provide pricing scenario information.

- It cited a relatively low conversion rate (the percentage of users successfully able to complete the IDV process), which may be a result of the fraud environment in some APAC markets. Customers are advised to review the ZOLOZ UX to ensure it meets their requirements.

- It failed to provide a VPAT, and automated accessibility checks yielded poor results. This finding may be a concern as accessibility becomes an increasingly important requirement, and in some markets, a regulatory obligation.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

As this is a new Magic Quadrant, no vendors were added.

Dropped

As this is a new Magic Quadrant, no vendors were dropped.

Inclusion and Exclusion Criteria

To qualify for inclusion in this Magic Quadrant, vendors had to meet the following must-have capabilities (also found in the identity verification Market Definition section):

- Capture of a person’s photo and data from a photo identification document, followed by assessment of the document’s authenticity to provide assurance that the real-world identity exists. Solutions must capture the document through one of the following technologies:
  - Optical capture and processing, including OCR, or analysis of bar code or quick response (QR) code.
  - Data extraction from a chip using near-field communication (NFC).
- Image capture of the person’s face, with integrated liveness detection to ensure human presence, followed by biometric face comparison with the photo from the identity document.
- The complete identity verification process must be carried out by a person on a normal user device (e.g., laptop, tablet or smartphone) with no requirement for the user to rely on specialized hardware.

Vendors may also receive components of the must-have capabilities from third parties. However, vendors were **excluded** if they obtained the full identity verification solution (all must-have capabilities) from a third-party and simply resold it, regardless of whether they were adding additional value with other capabilities.

Vendors also had to meet **one** of the following criteria:

- At least $100 million in identity verification revenue in fiscal year 2023
- At least $40 million in identity verification revenue in fiscal year 2023, and at least 15% year-over-year growth when compared to fiscal year 2022
- At least $30 million in identity verification revenue in fiscal year 2023, and at least 30% year-over-year growth when compared to fiscal year 2022

Honorable Mentions

ADVANCE.AI: ADVANCE.AI is headquartered in Singapore and has customers across a number of markets in APAC and Latin America. Its IDV capability can be used stand-alone or as part of its digital verification stack, which includes a range of contextual fraud signals and verification sources. ADVANCE.AI did not meet the revenue inclusion criteria.

Daon: Daon has a global customer base and offers IDV capability as part of its broader identity life cycle and authentication platform. The IDV capability can be deployed stand-alone, or it can be tightly coupled with other authentication capabilities, such as face and voice biometrics and FIDO/UAF passkeys. In addition to its SaaS offering, Daon has a software offering that's both cloud-based and self-managed, and extensive experience deploying it to meet complex implementation requirements. Daon did not meet the revenue inclusion criteria.

ID-Pal: ID-Pal is headquartered in Ireland, with a focus on the U.K., the U.S. and Europe, serving small, midtier and enterprise businesses. ID-Pal differentiates through its approach to privacy and ensuring user data can be decrypted and accessed only by its customers. ID-Pal did not meet the revenue inclusion criteria.

IDWise: IDWise is a newer vendor, founded in 2020 and headquartered in the U.K., which has built its IDV solution to focus on use cases in emerging markets globally. Its solution focuses on handling legacy devices, diverse and low-quality ID documents, accuracy with non-Latin character sets and strict data residency requirements. IDWise did not meet the revenue inclusion criteria.

Intellicheck: Intellicheck is a U.S.-focused IDV vendor that specializes in verifying U.S. drivers' licenses. Intellicheck is differentiated from other IDV vendors through its unique status as the sole "courtesy verification provider" for U.S. Departments of Motor Vehicles, which gives it privileged information regarding security features within the bar codes on U.S. drivers' licenses. Intellicheck did not meet the revenue inclusion criteria.

Inverid: Inverid is headquartered in the Netherlands and offers a differentiated IDV solution by means of its primary focus on use of NFC to assess chip-enabled documents. As a result, Inverid is often used in high-assurance use cases. Many other IDV vendors in the market partner with Inverid to source their NFC capabilities. Inverid did not meet the revenue inclusion criteria.

Nametag: Nametag is a newer IDV vendor, founded in 2020 and headquartered in the U.S. It differentiates itself in the market with a cryptographic approach to preventing injection attacks, and by focusing only on the account recovery use case for workforce and customers. It has built deep integrations with a range of access management and IT service management platforms to enable turnkey deployment. Nametag did not meet the revenue inclusion criteria.

Regula: Regula is headquartered in Latvia and its core business for decades has been manufacturing hardware and technology for document verification. It also has a complete IDV solution for remote verification. It is unusual in the IDV market for not having a SaaS platform and offering its solution only as software, which can meet requirements for customers who don't want their users' data being handled by a third party. Many other IDV vendors partner with Regula to leverage some or all of their IDV capabilities. Regula did not meet the revenue inclusion criteria.

Veridas: Veridas is headquartered in Spain. Its IDV platform features face and voice biometrics. Its IDV is also integrated with its own hardware for biometric physical access control. It offers its own reusable digital identity solution, as well as a patented biometric-within-a-QR-code solution. Veridas did not meet the revenue inclusion criteria.

Evaluation Criteria

Product or Service: Core product that competes in the defined IDV market, which can be offered natively or by using OEM components as defined in the market definition and inclusion criteria. Includes the following subcriteria:

- Image capture and verification
- Configuration, administration and reporting
- Implementation and integration
- Data management, control and privacy
- UX and accessibility
- Scalability and resiliency
- Risk and fraud controls
- External data sources and additional verification

Overall Viability: The organization's overall financial health, as well as the success of the IDV business unit if it is a subset of a larger organization. Examines the likelihood of continued investment in the IDV product and the significance of the IDV product within the vendor's broader portfolio. Includes the following subcriteria:

- General
- IDV business-specific

Sales Execution/Pricing: The vendor's capabilities in presales and sales activities. This includes pricing strategies to support different IDV use cases and overall efficacy of the sales channel when selling IDV to different industries with different IDV requirements. Additional subcriteria include:

- Sales execution
- Pricing
- Scenarios

Market Responsiveness and Track Record: The ability to respond to evolving customer needs for IDV, market and regulatory changes, and competitor activities.

Marketing Execution: The creation and delivery of marketing programs that differentiate a vendor's IDV solution within the market. Execution involves delivering the vendor's message with respect to IDV and creating mind share.

Customer Experience: Programs, processes and resources that help customers successfully use an IDV product. Includes technical support and account support, as well as mechanisms for measuring customer satisfaction as well as the following subcriteria:

- Customer relationship and services
- Customer satisfaction
- New customer survey

Operations: The ability to use people, processes and technology to meet goals and commitments in delivering an IDV solution. Includes acquisitions and divestitures that may impact delivery of the vendor's IDV product.

Ability to Execute

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	***Weighting*** ↓
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High

Evaluation Criteria ↓	***Weighting*** ↓
Operations	Medium

Source: Gartner (October 2024)

Completeness of Vision

Market Understanding: The ability to understand the needs of IDV buyers and translate these into IDV products and services. Includes processes for extracting insight from customer and sales data.

Marketing Strategy: The creation of clear and differentiated messaging about IDV and the vendor's IDV product. Includes metrics used to measure the impact of marketing activities.

Sales Strategy: The use of direct and indirect channels closely aligned with marketing to drive revenue and business growth.

Offering (Product) Strategy: An approach to product management and delivery of IDV features that is intentional and emphasizes differentiation and mapping to both current and future requirements. Includes assessing self-awareness and candor of areas in which a vendor's IDV product may be lagging the market. Includes the following subcriteria:

- Roadmap
- General

Business Model: The design, logic and execution of the vendor's business proposition to achieve continued growth and success.

Vertical/Industry Strategy: The strategy to direct investment and resources to meet the needs of IDV buyers in specific industry segments. Includes the following subcriteria:

- Applicability of offering to specific verticals, industries or sizes of organizations
- Strategy

Innovation: Demonstration of a systematic and intentional approach to innovation, both technical and nontechnical, with respect to delivering IDV.

Geographic Strategy: The approach to meeting the needs of IDV buyers and their specific needs in geographies outside the vendor's home market. These include differing regional requirements for storing personally identifiable information (PII), handling of document types specific to different regions and emerging market needs, such as the need to support legacy mobile devices.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	***Weighting*** ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2024)

Quadrant Descriptions

Leaders

Leaders deliver a broad and comprehensive IDV product that addresses a wide range of use cases and customer needs. They have successfully built a significant installed customer base and revenue stream. Leaders demonstrate a superior vision that goes beyond simply doing more of the same at a larger scale. They also demonstrate strong execution to bring that vision to fruition. They anticipate IDV requirements and in some ways help shape the market.

Challengers

Challengers show strong execution, complete and specialized product features, and have significant customer bases. They tend to have sales and brand presence within a particular region or industry. However, Challengers do not have the same breadth of vision as Leaders. Due to Challengers' smaller size, some potential buyers may have concerns regarding their long-term viability. Challengers have not yet demonstrated the same maturity, scale of deployment or vision for IDV as Leaders. Rather, their vision tends to be more focused on — or restricted to — specific geographies, industries or use cases.

Visionaries

Visionaries provide products that meet many IDV customer requirements, but they may not have the market penetration or maturity to execute as Leaders do. Visionaries are noted for their innovative approaches to addressing IDV challenges. They may have unique features, more so than vendors in other quadrants. Visionaries are often innovation leaders in maturing markets such as IDV, and enterprises that seek the latest solutions often look to Visionaries.

Niche Players

Niche players provide IDV technology that is a good match for specific use cases. They may focus only on certain geographic regions or provide IDV as part of a broader platform where it can be tightly coupled with complementary capabilities. They can outperform many competitors in their specific area of focus. They do not always compete purely on IDV capabilities. Brand awareness of them only as an IDV vendor is usually low relative to vendors in other quadrants. Vision and strategy entirely from an IDV perspective may not extend much beyond feature improvements to current offerings to keep pace with the market. However, inclusion in this quadrant does not reflect negatively on the vendor's value in the more narrowly focused spectrum. Niche solutions can be very effective in their areas of focus.

Context

The following commentary gives context and insight to support interpretation of the Magic Quadrant.

Comparing Vendor Accuracy Is Fraught With Difficulties

This Magic Quadrant does not compare vendors based on their product's accuracy, and is not a quantitative reflection on how well vendors assess document authenticity or perform liveness detection and then face-matching during the selfie step. Rather, it assesses vendors' possession of a broad range of capabilities and attributes.

Comparing vendors' accuracy in the IDV process is very challenging. Instead, buyers should seek data from vendors that is specific to:

- Their expected volumes and document types
- Their expectation or need for either fully automated flows or human agent involvement
- How vendors meet (and preferably exceed) current standards

In most cases, testing a vendor against live production data for the target population and use cases is the only way to obtain the reassurances buyers seek.

Issues in Comparing Accuracy of Document Assessment

The industry lacks a standard approach to benchmark document assessment. Any comparison of accuracy (e.g., false acceptance rate, false rejection rate) is hindered by several elements, and these were apparent in responses to this Magic Quadrant:

- **Vendors' methods of measurement —** The methods for measuring and reporting on the efficacy of a solution vary widely. Some vendors rely on fraud outcome data as reported by their customers, while others rely on testing against known good and bad documents. Still others have forensic document analysts perform random sampling on production data.

- **The number of document types —** Even for a given vendor, accuracy varied across different document types due to their relative volumes. ML models thrive on data and are typically more accurate for document types with larger datasets.

- **Geography —** Security features aiding document assessment vary globally. So, a vendor operating in regions with documents that have fewer security features will likely appear to be less accurate.

- **Inconsistent use of human agents —** Many vendors offer the ability to use human agents to make the final determination in an IDV check. The optional nature of this capability further complicates any measurement of accuracy, as the use of human agents would vary by customer of any given vendor.

However, there are some promising developments in this area. For example, the FIDO Alliance has introduced its Document Authenticity (DocAuth) Certification Program for Remote Identity Verification. Similarly, the U.S. Department of Homeland Security launched its 2023 Remote Identity Validation Technology Demonstration. Both programs have invited vendors to submit their technologies for testing. At the time of this assessment, neither had published any results.

Issues in Comparing Liveness Detection

Comparing liveness detection is similarly difficult. However, there is at least a standard in this area that serves as a point of reference. ISO/IEC 30107-3 "Information technology — Biometric presentation attack detection — Part 3: Testing and reporting" covers the assessment of presentation attack detection (see Note 1). Most vendors surveyed were assessed by iBeta testing labs in conformance with the standard.

However, iBeta's testing simply creates a baseline that all vendors meet and does not facilitate further quantitative vendor comparison.

iBeta's testing allows a generous false nonmatch rate (FNMR) (see Note 2). It was previously unconstrained, then set at 20%, then reduced to 15%. In reality, few (if any) IDV customers would tolerate 15% of their genuine users being declined in error. To demonstrate that they go over and above the requirements of the iBeta ISO/IEC 30107-3 conformant testing, vendors use widely varying internal testing approaches, which render comparison largely worthless.

In addition, ISO/IEC 30107-3 and other test regimens, such as NIST FATE PAD testing, focus on presentation attacks alone. The threat landscape now also involves injection attacks, and there are currently no standards for assessing injection attack detection (see Note 1). However, the current development of European standard FprCEN/TS 18099 for biometric data injection attack detection holds some promise for future standardized benchmarking in this area.

The Use of Human Agents Is Nuanced

Buyers are often surprised to learn that many IDV vendors offer varying degrees of human agent involvement behind the scenes to make a final decision after automated processes are complete. For example, vendors may offer:

- **Full automation for some document types —** Some vendors may offer fully automated flows on only some document types but rely on human agents for others. Typically, human agents are used for less common document types with fewer security features, or for documents containing character sets that the vendor does not support.

- **Human involvement for higher accuracy —** Some vendors may offer a fully automated flow for all document types but acknowledge that, for some document types, the use of human agents can improve accuracy without reducing pass rates. Customers of such a vendor must decide between automation with lower accuracy or the use of human agents for supposedly higher accuracy.

- **Human involvement for regulatory compliance —** Some vendors may offer the use of human agents, not to improve accuracy or pass rates but to help customers meet regulatory obligations. In some markets, notably within Europe, a human agent must review any automated decision involving IDV, particularly for financial services use cases.

- **Human involvement for exception handling —** Some vendors may offer a fully automated solution across -all document types, with a claim of consistently high accuracy, but also offer human agents to handle exceptions. For example, human agents may step in if an invalid identity document is presented or if images are low-quality.

Even vendors who do not offer any human agent capability still provide case management systems that allow customers to use their own agents to drive up pass rates, comply with regulation, or for exception handling. Thus, in today’s market, to varying degrees, IDV is still a process that melds machine and human.

The use of vendor-provided human agents has several implications buyers should consider:

- **Higher processing time —** Human involvement extends processing time and, thus, erodes UX. Vendors with a greater percentage of IDV checks involving human agents consistently show longer overall IDV processing times.

- **Concerns about protecting users' PII —** Vendors will need to demonstrate that appropriate controls are in place to prevent human agents from abusing their access to user PII. Requirements to keep user PII within certain geographic regions are more difficult to meet if that data is sent to human agents operating in a globally diversified model.

- **Higher pricing —** Vendors who rely on human agents across a greater percentage of their IDV checks often have higher pricing.

Fraud Detection Beyond IDV Better Identifies Deepfakes

Attacks against the IDV process are not new. A range of "analog" presentation attack vectors have been known for years (see Note 1), and IDV vendors have developed defenses against them. However, now IDV vendors must also defend against more "digital" approaches, such as injection attacks (see Note 2).

With the rapid evolution of generative AI, the risk of deepfake images and videos — of documents and/or faces — has become greater. In response, many IDV vendors have increased their investments in deepfake and injection attack detection. However, buyers remain uncertain whether vendors can keep up with attackers.

Vendors stand a better chance of detecting an attack involving a deepfake — even if they fail to detect the deepfake itself — by implementing a layered approach to fraud detection. Some vendors have invested in the ability to detect other contextual signals that could indicate a fraudulent identity presentation. For example:

- **Location —** Vendors can assess the location of a user's device and correlate it against the presented identity data. They can also look for anomalies in repeated locations across different identity presentations.

- **Device —** Vendors can profile a user's device to uniquely identify it and look for anomalies, such as the same device being used for different identity presentations.

- **Behavior —** Vendors can examine user behavior attributes — such as session duration, use of copy and paste, dwell time and device orientation — and compare them with the statistical norms for good and bad users to identify anomalies.

- **Repeated identity attributes —** Vendors can compare attributes from an identity presentation — such as a face, a document number or an address — with those from previous identity presentations to look for repeated occurrences. More sophisticated vendors perform "fuzzy matching," detecting when an attacker has attempted to alter its appearance, or when document numbers are sequential rather than identical. Such checks are typically performed within a single customer tenant, but some vendors allow customers to opt into a consortium. Note that this approach, while powerful, requires the vendor to store identity data from each IDV event. Some vendors do this in privacy-preserving ways involving hashed representations of identity data.

Ease of Configuration Is a Key Differentiator

IDV management is becoming more complex, with many available functionality combinations and permutations. Customers may have different requirements for different user types. Examples include permitting different document types, using different types of liveness detection that vary in their UX or level of security, deploying conditional logic for running additional checks against other data sources, and performing localization and branding within UI components.

The traditional approach to configuration gives customers a static menu where they can toggle options on and off and set thresholds. Customers may need to repeat this process several times to create different possible journeys, and there is little scope for flexibility or conditional logic.

A more intuitive approach is a drag-and-drop IDV workflow editor that allows customers to create journeys with conditional logic and different functional components. This approach makes it easier for customers to visualize the IDV journey and make changes to specific aspects of it — without having to jump between different screens of configuration menus. Vendors offering this approach typically received more positive responses in the MQ customer survey with respect to ease of configuration.

SaaS Is the Dominant Model

All vendors in this Magic Quadrant deliver IDV in a SaaS model, and most offer only a SaaS model. However, vendors are attempting to offer flexibility with their SaaS offerings. Most are hosted in Amazon Web Services (AWS), Microsoft Azure or GCP across several regions as the default option. If customers require SaaS processing in a given region only, some vendors are willing to set up new SaaS instances in those regions — though they may increase prices to justify the investment.

A small minority of vendors can also deploy their IDV solutions as software for customers to install and manage in their on-premises or private cloud environments. Customers may prefer this method to satisfy regulations that require them to keep user data within their infrastructure or within their geographic region. However, vendors that do offer software deployments express a strong caveat that it is not the preferred option. Besides the usual barriers to maintaining software (e.g., operational costs, managing upgrades and updates, support), IDV delivered via software lacks certain benefits, such as the updating of ML models in (near) real time with fraud attack vectors or correlation of IDV data against identity graphs.

Accessibility Varies Greatly by Vendor

Many government and public-sector organizations have long focused on accessibility out of a duty to ensure all citizens can use their services. However, there is urgent interest in accessibility from private-sector organizations — not only driven by a need to monetize as many users as possible but also growing regulatory pressure. [1] In response, this Magic Quadrant explores the accessibility of vendors' IDV products as well as how vendors integrate accessibility into their product management and development processes. Vendors were required to provide a VPAT (see Note 3) and a recorded demonstration of an automated accessibility scan, and to demonstrate how their SDK performed when used with assistive technologies.

The goal of these questions and tests was to assess compliance with the Web Content Accessibility Guidelines (WCAG), Version 2.1, Level “AA.” The results showed large variations among vendors. Some declined to provide VPAT reports, some believed they were compliant but testing results showed otherwise, and some openly acknowledged they were deficient in this area. Several vendors performed reasonably well.

IDV buyers should be clear about their own expectations regarding accessibility given that, from an end-user perspective, the IDV process will be seen as part of the organization’s interface and offering. With many vendors demonstrating barriers to accessibility, buyers must consider how this will impact user experience, their brand and their own regulatory obligations. To learn more, see 3 Digital Accessibility Steps to a More Inclusive User Experience.

Market Overview

This Magic Quadrant was produced in response to market conditions for IDV, including the following trends.

The market of vendors is growing. Gartner has observed that the number of vendors in the IDV market continues to grow, and is currently tracking over 100 vendors. While the core IDV process offered by them all is seemingly similar, there are many differences between vendors. IDV product capabilities aside, the most notable differentiation stems from geographic or industry focus. To add further complexity for buyers, IDV is also being offered as part of broader platforms. Many stand-alone IDV vendors focus on IDV alone. However, some vendors now offer IDV as part of an AM tool, or as part of a broader biometric authentication tool. Finally, future market consolidation is likely as IDV vendors consider acquiring competitors to buy market share in new geographies or gain a foothold in new industries.

IDV is being applied to broader use cases. Historically, the dominant use case for deploying IDV has been part of the customer onboarding process for regulated organizations to meet their know your customer (KYC) use-case obligations. However, Gartner has observed end-user organizations buying IDV solutions for an ever broader range of use cases, including fraud detection, trust and safety in marketplaces, workforce onboarding, age verification and account recovery. The latter example of account recovery, particularly in the workforce context, has seen a surge of interest since late 2023. A common requirement is to secure the account recovery process for users with privileged access, or for regular users when multifactor authentication (MFA) is not possible (e.g., the user has lost their device or token) to improve security and reduce the operational burden on IT help desks.

IDV is now complemented by government eID schemes and authoritative sources. While assessing the authenticity of a government-issued photo identity document and comparing it to a selfie remains the main focus of IDV vendors, three other types of checks are becoming more commonplace:

- **Use of government eID schemes —** Examples include SPID in Italy, FranceConnect in France, or Singpass in Singapore. These provide citizens with a secure way to authenticate themselves and assert their identity, and have varying degrees of adoption and assurance across public-

and private-sector relying parties. Some IDV vendors are beginning to integrate with such eID schemes and are offering platforms that allow customers to integrate IDV and/or eID acceptance.

- **Access to issuing authority databases to check data attributes —** Examples include AAMVA in the U.S., Serpro in Brazil or DVS in Australia. Some of these enable real-time checks of data attributes provided by a user or extracted from their identity document.
- **Access to issuing authority databases to check biometric data —** Examples include Aadhaar in India, Absher in Saudi Arabia or RENAPER in Argentina. The availability of these databases varies greatly across different countries, given varying public and political sensitivity to government handling of biometric data.

Some IDV vendors are now connecting to such eID schemes and authoritative sources to complement their standard IDV checks and add a further layer of defense against identity impersonation and to provide different options to customers.

IDV is transitioning to digital identity. The IDV market is entering a period of transition, as a broad and differing range of portable digital identity initiatives either mature, enter the market or undergo large-scale pilot programs. No single “winner” is likely to emerge in this race for portable digital identity adoption; what is more likely is a patchwork of competing and complementary schemes for many years to come. These solutions may or may not involve a dedicated digital identity wallet application for mobile devices. As the adoption of portable digital identity grows over time, the total addressable market for identity verification vendors will intuitively decrease as discrete identity verification events are replaced with events in which users present their already verified identity. An opportunity will still exist since most portable digital identity solutions will be bootstrapped by an initial automated identity verification event, which may also play a role in account recovery. However, today’s identity verification vendors will need to strategically evolve their offerings to remain relevant in this changing market.

This is Gartner’s first version of the Magic Quadrant for Identity Verification, replacing the Market Guide for Identity Verification.

Evidence

Gartner’s analysis in this Magic Quadrant is based on sources that include:

- Vendor briefings covering differentiation, customer use cases and product roadmaps.
- An extensive RFP questionnaire inquiring how each vendor delivers against the fifteen evaluation criteria and eight critical capabilities defined for this market.
- A survey of up to 10 customers per vendor, based on contacts provided by the vendors.

Additional evidence:

[1] Relevant legislation:

- EU — European Accessibility Act
- U.S. — The Americans With Disabilities Act
- U.K. — Equality Act 2010

Note 1: Presentation Attacks and Injection Attacks

A **presentation attack** on the IDV process consists of an attacker presenting a fraudulent artifact to the sensor (camera). Examples include using the device’s camera to take an image of:

- A color photocopy or printout of an identity document
- An existing identity document with a new headshot photo stuck onto it
- A headshot photograph of someone else in place of taking a selfie
- An image or video being displayed on a monitor screen in place of taking a selfie
- The attacker wearing a mask

An **injection attack** on the IDV process consists of an attacker introducing digital content into the process, bypassing the sensor (camera). This digital content could be images or videos, real or deepfake, of the identity document and/or the target’s face. Examples of how this is done include using:

- Virtual cameras
- Hardware video sticks
- JavaScript injection
- Smartphone emulators
- Interception of network traffic

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Note 2: False Nonmatch Rate

The false nonmatch rate (FNMR), also referred to as the bona fide presentation classification error rate (BPCER), is the percentage of genuine presentations during liveness testing that is wrongly classified as attacks. This value should be as low as possible. A higher value results in more genuine users being wrongly declined.

Note 3: Voluntary Product Accessibility Template (VPAT)

A VPAT is a document that helps buyers of IT products make informed decisions about a product's accessibility. The Information Technology Industry Council (ITIC) created the VPAT template to help vendors document how their products meet the accessibility standards of Section 508 of the Rehabilitation Act and other accessibility standards, such as the Web Content Accessibility Guidelines (WCAG). For further information see **VPAT — Information Technology Industry Council**.

objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.