Magic Quadrant for Identity Verification

25 August 2025 - ID G00824718 - 45 min read

By Akif Khan, Nayara Sangiorgio, and 1 more

Identity verification tools help deliver security, compliance and trust across customer and workforce use cases. This Magic Quadrant evaluates 11 vendors to help IAM leaders assess these solutions against their use cases and requirements.

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

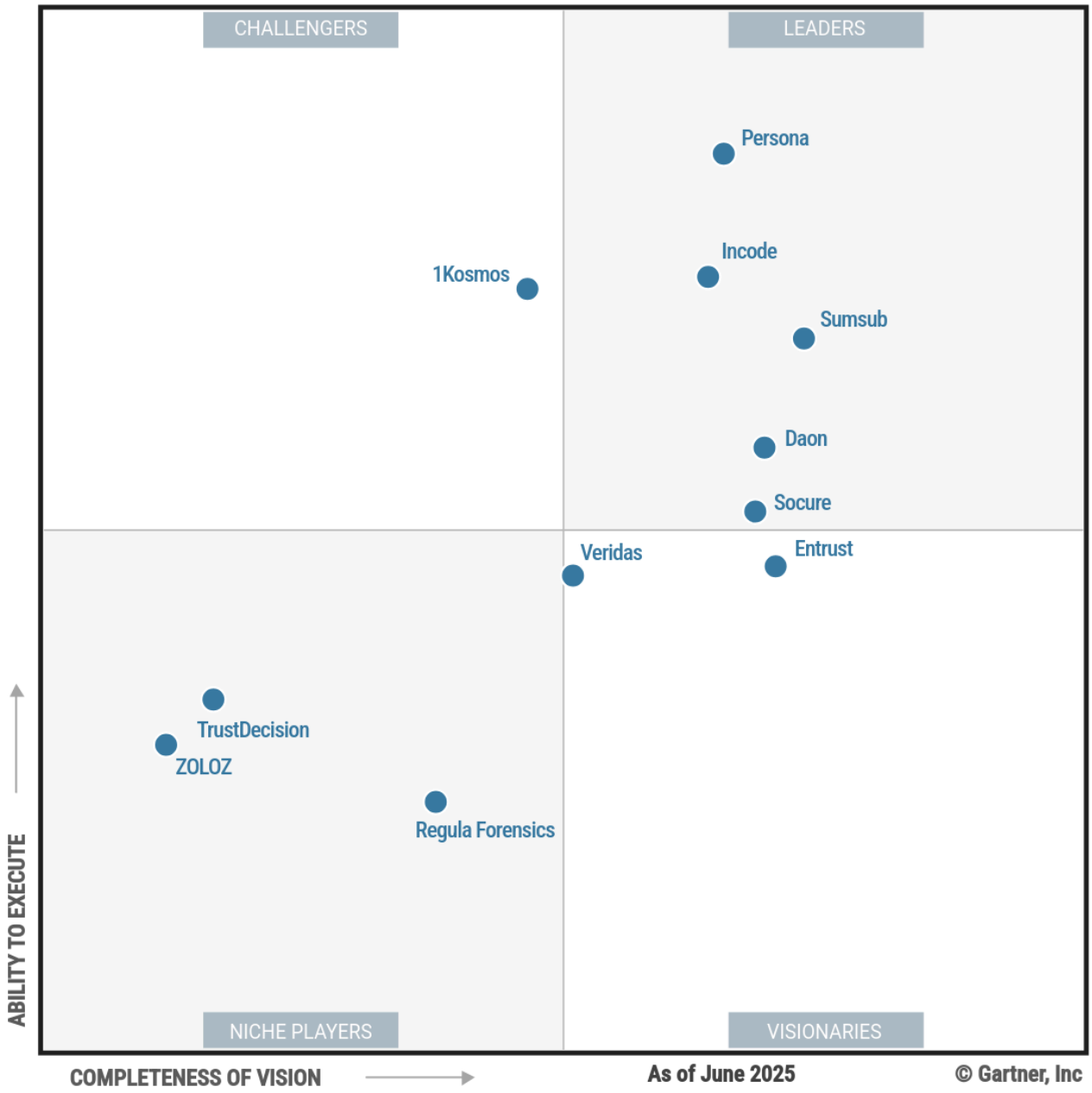
The common features for this market include:

- 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



Gartner

Vendor Strengths and Cautions

1Kosmos

1Kosmos is a Challenger in this Magic Quadrant. Its 1Kosmos Verify product can be bought individually or bundled with its 1Kosmos Workforce or Customer digital identity wallet and passwordless authentication solutions. The company operates globally, with most clients in financial services and retail. More than a third use 1Kosmos for workforce use cases.

Recent updates include risk signals, such as device profiling and velocity checks, as well as integration with handheld scanners for retail environments. 1Kosmos' roadmap includes

sharing anonymized risk signals across customer tenants and enhancing the risk policy engine with more granular controls.

Strengths

- 1Kosmos achieved FedRAMP High authorization for its IDV platform, which positions it well to serve U.S. federal and state agencies.
- The company offers a broad range of in-depth, prebuilt integrations for customer and workforce scenarios, including AM, IGA, ITDR, ITSM, HR and background-screening platforms.
- It has extensive experience with face biometrics for authentication, leveraging the selfie taken during an IDV event. It has demonstrated performance and scalability by successfully processing high volumes of these authentications in a range of workforce use cases.

Cautions

- Compared to other vendors in this research, 1Kosmos' pricing is higher for SaaS IDV deals, with fewer than 1 million annual checks, though pricing is competitive at higher volumes.
- The company shows a lack of candor and market insight when asked why prospects decide not to buy its IDV product, failing to cite any product deficiencies. This may result in misalignment of customer needs with the product and its roadmap.
- Its value proposition and differentiation stem from coupling IDV with its digital identity wallet and passwordless authentication. The value for using 1Kosmos for IDV alone is reduced without these complementary capabilities.

Daon

Daon is a Leader in this Magic Quadrant. Its xProof IDV product is part of a platform offering a broad range of authentication tools and orchestration capabilities. Its operations are geographically diversified, and its clients tend to be in financial services and government. Daon declined to say what proportion of clients use it for workforce use cases.

Recent updates include a no-code orchestration tool for building and managing complex IDV workflows, and a bring-your-own-key cloud security model that lets customers manage

their own encryption keys. Daon plans to improve its biometric face-matching algorithms and start adding third-party integrations relevant to workforce use cases.

Strengths

- Daon has undergone credible third-party testing of its document assessment capabilities, an uncommon practice among IDV vendors that is notably different from standard IDV conformity certifications.
- The company has significant experience deploying its IDV solution as software for clients who do not want a SaaS solution. While its main sales approach is a SaaS offering, one-fifth of its clients today have software deployments to meet specific needs, such as data-processing requirements.
- Compared to other vendors in this research, Daon's pricing is low for IDV deals with annual volumes greater than 1 million checks, applying to both SaaS and software implementations.

Cautions

- Daon does not help clients address workforce use cases with out-of-the-box integrations with platforms and capabilities such as AM, IGA, ITDR, ITSM or HR systems.
- The company was unable to provide granular insights into user experience (UX) metrics for its SDKs for software deployments, such as the number of image retakes needed due to poor quality. This may limit Daon's ability to address UX issues if they arise in software deployments.
- Its user-facing IDV UI is available in only a small number of languages in addition to English, although additional languages can be added upon request. Additionally, its back-end administration portal is only available in English.

Entrust

Entrust is a Visionary in this Magic Quadrant. Entrust completed an acquisition of IDV vendor Onfido in 2024 and has integrated it with its heritage IDV solution. The company's operations are geographically diversified, and its customers are mainly in financial services and cryptocurrency. Only a small number of customers use Entrust's IDV product for workforce use cases.

Recent updates include adding advanced electronic signature to its compliance suite and a policy validator tool that automatically checks IDV configurations against regulatory requirements. Entrust plans to add more eID integrations and make device intelligence signals more readily available in its Studio workflow editor.

Strengths

- Entrust has a global sales footprint, with both direct and channel partner sales operations in every region.
- The company self-reported a low percentage of end users in 2024 who needed to take second images of their face, indicating an optimized UX.
- It prioritizes accessibility in its end-user IDV interfaces, as shown by its voluntary product access templates (VPATs) and the accessible design and development processes. This focus is increasingly important as accessibility becomes a higher priority and in many cases, a regulatory requirement.

Cautions

- Entrust relies heavily on human involvement for IDV checks, beyond what is required by regulatory oversight in some markets. In some cases, human involvement compensates for gaps in automated processing, such as the lack of full OCR automation for non-Latin-character sets. This increases the average time to complete the IDV process.
- Compared to other vendors in this research, Entrust's pricing is higher for SaaS scenarios involving documents with non-Latin-character sets, though pricing is typical for Latin-only scenarios. This variance is unusual and likely due to the need for more human involvement in non-Latin OCR processing.
- Its hosted IDV user experience, in which a customer can simply provide end users with a URL to complete their IDV check, lacks some standard market features. For example, customers can use a subdomain they own, but cannot fully white-label or alias the experience to their own domain.

Incode

Incode is a Leader in this Magic Quadrant. Its operations are focused in North America and Latin America, and its customers are typically in financial services and government. Only a small number use Incode for workforce use cases.

Recent updates include a no-code orchestration tool for building and managing complex IDV workflows that involve branching and this-party call-outs, and capabilities that let customers install and run Incode's IDV solution within their own infrastructure. Incode plans to connect to more biometric authoritative issuing sources and create large vision models to improve the document assessment process.

Strengths

- Incode connects to a high number of authoritative issuing sources of identity data across several countries, particularly those that enable biometric data checks. These are becoming an increasingly important market requirement to complement or even replace the standard IDV process.
- The company has an innovative product roadmap, including the use of vision language models to improve document assessment and support for protocols such as Model Context Protocol and Agent2Agent, which anticipates the need to use IDV with AI agents.
- It has developed a strong understanding of IDV buying needs in workforce use cases and has built a large sales team dedicated to expanding its workforce business.

Cautions

- Incode's accessibility performance is low compared to other vendors in this research. The company's VPATs show only partial compliance with Web Content Accessibility Guidelines (WCAG) (version 2.1, Level AA) in both its user-facing IDV UI and back-end administration portal, which may make the solution difficult or impossible for people with disabilities to use. This may be a concern as accessibility becomes an increasingly important requirement, and in some markets, a regulatory obligation.
- The company has a high percentage of customers in one vertical, financial services, and relatively little experience in other industries driving IDV growth, such as online marketplaces, the gig economy, travel and social media.
- Incode does not hold any patents specific to its IDV technology, which is unusual from an innovation perspective in the IDV market.

Persona

Persona is a Leader in this Magic Quadrant. Its operations are focused primarily in North America, and its customers are mainly in online marketplaces, financial services and the gig

economy. Only a small number use Persona for workforce use cases.

Recent updates include adding mobile driver's license (mDL) verification via digital wallets and enhanced data residency options, including single-tenant hosting across multiple regions. Persona plans to enable anonymized sharing of risk signals across customer tenants and add AI agents to its case management tool to improve reviewer efficiency.

Strengths

- Persona has a comprehensive suite of risk signals, including location intelligence, device profiling and behavioral analysis, and uses a high number of attributes for velocity and cross-linking checks to help assess IDV risk. These are augmented by strong policy controls, allowing customers to control how data is used.
- The company offers single-tenant SaaS hosting across a high number of regions to support customers with specific data privacy requirements that do not want to manage software deployments. It also provides flexible and granular controls for managing PII retention and redaction, configurable at the attribute (rather than entire IDV event) level with conditional logic. Its SaaS pricing is lower than other vendors evaluated in this research, and it also provides a permanent free tier for low-volume customers.
- Its end-user IDV interfaces and back-end administration portal perform well for accessibility, as shown by its VPATs and accessibility-focused design and development processes. This is increasingly important as accessibility becomes a higher priority and sometimes a regulatory requirement.

Cautions

- Persona's customer base is concentrated in the U.S, Canada and Mexico; thus, its experience of being able to service clients in other geographies is limited. However, the company did process a diverse set of global identity documents in 2024, suggesting that its existing customers have global user bases.
- The company needs to increase UX optimization, as indicated by its self-report of a high percentage of end users in 2024 who needed to take second images of their documents.
- Its channel sales program is still immature, as indicated by a low percentage of new customers in 2024 compared to its direct sales. This could limit Persona's reach and ability to scale into new industries and regions until the program expands.

Regula Forensics

Regula Forensics is a Niche Player in this Magic Quadrant. Its IDV solution is not available as SaaS; it is software installed by customers on their own infrastructure. The company operates globally, and its customers are typically in financial services or are other IDV vendors or resellers. Regula Forensics does not track whether its solutions are used in workforce use cases.

Recent updates include document liveness checks that involve being able to examine visibly dynamic security features such as holograms or optically variable ink during document image capture. Regula Forensics plans to support mDL verification and introduce a SaaS version of its IDV solution.

Strengths

- Regula Forensics has strong experience deploying IDV as software, meeting client requirements to keep all data processing within their infrastructure, and serves customers in many regions.
- Compared to other companies in this research, it offers lower per-check pricing for software-deployment scenarios, although it only serves customers processing more than 1 million IDV checks annually.
- It earns a low percentage of its revenue from its top 10 customers, which improves overall viability and business resilience, reduces risk and minimizes the impact of customer churn.

Cautions

- Regula Forensics does not currently offer a SaaS solution, meaning that its solution is unsuitable for customers that do not want to manage the implementation and updates of IDV software themselves alongside the associated data processing and storage.
- The company has little insight into how customers use its IDV software and could not provide metrics such as volumes of different document types processed or the percentage of users requiring multiple attempts at image capture.
- It does not provide reporting or additional risk checks, such as velocity checking. Customers must use the outputs from the SDK to create such features themselves.

Socure

Socure is a Leader in this Magic Quadrant. Its Predictive DocV IDV solution is part of a broader suite of identity assurance products. The company focuses mainly on North America, and its customers are typically in financial services and online marketplaces. Only a small number use Socure for workforce use cases.

Socure acquired Effectiv in 2024 to improve orchestration capabilities, and the company has enhanced its models for deepfake detection. Socure plans to support mDL verification via digital wallets and expand its image alert list into a global consortium.

Strengths

- Socure provides a strong suite of risk signals, including location intelligence, device profiling and behavioral analysis, and uses a high number of attributes for velocity checks. These can be combined with other data-centric products in its portfolio, such as Sigma Identity Fraud or Graph Intelligence, to provide a deeper view of IDV event risk.
- The company had a low customer churn rate despite macroeconomic challenges and volatility in cryptocurrency markets that led to churn elsewhere in the IDV market.
- It achieved FedRAMP Moderate authorization for its IDV platform in addition to GovRAMP authorization, which positions it well to serve U.S. federal and state agencies.

Cautions

- Although Socure supports a wide range of character sets and languages for OCR, the company was unable to demonstrate experience processing a diverse set of global identity documents at scale. It reports that about one-third of its customers are outside the U.S., but almost all processed documents are North American.
- The company's multitenant SaaS solution is only hosted in the U.S., with no off-the-shelf solution for customers who require data processing and storage outside the U.S.
- It does not offer out-of-the-box integrations with platforms and capabilities such as AM, IGA, ITDR, ITSM or HR systems to help clients address workforce use cases.

Sumsub

Sumsub is a Leader in this Magic Quadrant. The company operates globally, and its customers are mainly in financial services and cryptocurrency. Only a small minority use Sumsub for workforce use cases.

Recent updates include the launch of its Non-Doc IDV suite, which connects eIDs and authoritative issuing sources, and Sumsub ID, its solution for enabling reuse of verified identity data. Sumsub plans to support mDL verification via digital wallets and introduce automation tools to improve the efficiency of anti-money-laundering (AML) investigations.

Strengths

- Sumsub shows high geographic diversity in its customer base and in the top document types processed in 2024. It supports its global customers by offering out-of-the-box versions of its administrative portal in English, Spanish, Portuguese and Chinese.
- The company connects to a high number of eID schemes and authoritative issuing sources, which are increasingly important to complement or replace standard IDV processes.
- It launched its Sumsub ID product, a portable digital identity solution that lets end users who complete IDV with Sumsub customers reuse their identity data, even for know-your-customer (KYC) compliance, reducing friction for users across Sumsub's customer network.

Cautions

- Sumsub's business is concentrated in financial services, crypto and gambling for compliance use cases, so it has less experience in other industries and with other use cases.
- The company does not help clients address workforce use cases with out-of-the-box integrations with platforms and capabilities such as AM, IGA, ITDR, ITSM or HR systems.
- It has not submitted its proprietary face-matching algorithms to the U.S. NIST for testing, preferring to rely on its own benchmarking, a practice which is unusual among IDV vendors.

TrustDecision

TrustDecision is a Niche Player in this Magic Quadrant. It offers only an API and SDK for its SaaS IDV solution, with no back-end administration portal. The company focuses mainly in Indonesia, the Philippines and Mexico, and its customers are typically in financial services and e-commerce. It has no customers using the solution for workforce use cases.

Recent updates include enhanced document assessment using large multimodal models and connectivity to Indonesia's government biometric verification service. TrustDecision plans to reduce the size of its SDK and improve support for Huawei's HarmonyOS, which is increasingly important in APAC.

Strengths

- TrustDecision primarily serves customers in its core markets of Indonesia, the Philippines and Mexico, and processes the majority of the documents from these countries, giving it deep regional expertise.
- Compared to other companies in this research, TrustDecision offers lower per-check pricing across SaaS scenarios.
- It has innovated with large multimodal models to improve OCR performance, resulting in a self-reported measurable uplift in OCR accuracy across a diverse range of document types that has helped the company win competitive deals.

Cautions

- TrustDecision offers its IDV solution only via API and mobile SDK, with no hosted user experience or back-end administration portal. Customers must configure the solution through the API and SDK, which may not suit clients that require easy configuration by business users.
- The company had a high churn rate in 2024, which it attributes to volatile business environments in the emerging markets it serves.
- It does not provide out-of-the-box integrations such as those with CIAM, e-commerce or banking platforms to serve customer use cases, nor with AM, IGA, ITDR, ITSM or HR platforms or capabilities for workforce use cases.

Veridas

Veridas is a Visionary in this Magic Quadrant. It only offers an API and SDK for its SaaS IDV solution, with no back-end administration portal. The company focuses on Europe, North America and Latin America, and its customers are mainly in financial services and ticketing or events. It also specializes in applying IDV to physical access contexts. Only a small number of customers use Veridas for workforce use cases.

Recent updates include enhanced injection attack detection and compatibility with incremental web browsers such as Opera and Samsung Internet. Veridas plans to comply with WCAG and seek certification of its injection attack detection against the new CEN/TS 18099:2024 standard.

Strengths

- Veridas had a low churn rate in 2024, which it attributes to proactive account management and mature processes for gathering customer feedback to inform its product roadmap.
- The company offers a smooth and user-friendly IDV experience. It self-reported a very low rate of end users needing to retake images of their documents or faces due to quality issues, and a high overall conversion rate for end users completing the IDV process.
- It applies its IDV solution in a range of contexts. These include integrations with several physical access control vendors and its ZeroData ID biometric QR code solution, which allows data from an IDV check to be stored in a privacy-preserving QR code for various use cases.

Cautions

- Veridas offers its IDV solution only via API and SDK, with no hosted user experience. In addition, its back-end portal is focused on search and reporting but does not offer configuration options, which may not suit clients that need easy configuration and management by business users.
- The company earns a high percentage of revenue from its top 10 customers, which increases risk if customer churn occurs.
- Its accessibility performance was low compared to other vendors in this research. Its VPATs showed only partial WCAG compliance in its user-facing IDV UI, suggesting people with disabilities may have difficulty using the solution as accessibility becomes a higher priority and regulatory requirement in some markets.

ZOLOZ

ZOLOZ is a Niche Player in this Magic Quadrant. Its operations focus on China and APAC, and its customers are mainly in financial services and cryptocurrency. Only a small number use ZOLOZ for workforce use cases.

Recent updates include the ZOLOZ ID Network to identify large-scale fraud attacks across customers and enhanced deepfake detection. ZOLOZ plans to automate testing tools to continually assess its own deepfake detection and add connections to authoritative issuing sources.

Strengths

- ZOLOZ serves the vast majority of its clients in China but processes documents issued in a broad range of countries, including Indonesia, Thailand and the Philippines, demonstrating expertise across the APAC region.
- Compared to other companies in this research, ZOLOZ's accessibility performance was above average for both its end-user IDV interfaces and back-end administration portal. Its VPATs showed it was largely compliant with WCAG requirements, and it has a credible roadmap to address remaining gaps.
- Its IDV business is viable, with a high number of customers, strong renewal rates and many multiyear deals.

Cautions

- ZOLOZ declined to provide pricing-scenario information. As a result, we are unable to assess its commercial value proposition.
- The company earns a high percentage of revenue from its top 10 customers, which increases risk if customer churn occurs.
- It does not offer prebuilt reports of aggregate IDV event information, or a custom query or BI interface, so customers must request reports through ZOLOZ customer support.

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

Daon

Regula Forensics

Trust Decision

Veridas

Dropped

AU10TIX: AU10TIX has globally distributed headquarters in London, New York and Singapore, and serves customers across many regions. Its IDV solution focuses on deepfake detection and serial fraud prevention. It is used by clients in a broad range of industries, including newer use cases in markets like the gig economy and digital assets. AU10TIX did not meet the commercial inclusion criteria.

GBG: GBG is headquartered in the U.K. and has customers mainly in North America, Europe and Asia. Its IDV solution can be used stand-alone or accessed via its global identity platform GBG Go. GBG did not meet the commercial inclusion criteria.

Jumio: Jumio is headquartered in the U.S. and serves customers across many regions. Its IDV solution has strong compliance features, leading to a large customer base in financial services and cryptocurrency, among other sectors. Jumio did not meet the commercial inclusion criteria.

Mitek: Mitek is headquartered in the U.S. and has customers mainly in Europe and North America. It has a strong customer presence in financial services, driven in part by its mobile deposit and fraud product lines. Mitek did not meet the commercial inclusion criteria.

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), and these must have been generally available in production by 1 April 2025:

- 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 receive components of the must-have capabilities from third parties. However, vendors are excluded if they obtain the full identity verification solution (all must-have capabilities) from a third-party and simply resell it, regardless of whether they are adding additional value with other capabilities.

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

- At least $100 million in identity verification revenue in fiscal year 2024, and at least 10% year-over-year growth when compared to fiscal year 2023.
- At least $45 million in identity verification revenue in fiscal year 2024, and at least 35% year-over-year growth when compared to fiscal year 2023.
- At least $15 million in identity verification revenue in fiscal year 2024, and at least 40% year-over-year growth when compared to fiscal year 2023.
- At least $3 million in identity verification revenue in fiscal year 2024, and at least 125% year-over-year growth when compared to fiscal year 2023.

Honorable Mentions

ADVANCE.AI: ADVANCE.AI is headquartered in Singapore and serves customers mainly across APAC and Latin America. Its IDV capability can be used as a stand-alone product or as part of its digital verification solution, AdvanGuard, which includes a range of contextual

fraud signals and verification sources. ADVANCE.AI did not meet the commercial inclusion criteria.

AU10TIX: AU10TIX has globally distributed headquarters in London, New York and Singapore and serves customers across many regions. Its IDV solution focuses on deepfake detection and serial fraud prevention. It is used by clients in a broad range of industries, including newer use cases in markets like the gig economy and digital assets. AU10TIX did not meet the commercial inclusion criteria.

Facephi: Facephi is headquartered in Spain and serves customers mainly in Latin America. Its IDV solution is part of a broader platform that includes biometric authentication capabilities such as voice and fingerprint. FacePhi did not meet the commercial inclusion criteria.

GBG: GBG is headquartered in the U.K. and has customers mainly in North America, Europe, and Asia. Its IDV solution can be used stand-alone or accessed via its global identity platform GBG Go. GBG did not meet the commercial inclusion criteria.

Inverid: Inverid is headquartered in the Netherlands and differentiates its IDV solution by focusing on NFC to assess chip-enabled documents. As a result, Inverid is often used in high-assurance use cases, and many other IDV vendors partner with Inverid to source their NFC capabilities. Inverid did not meet the commercial inclusion criteria. Inverid was acquired by Signicat in August 2025.

Jumio: Jumio is headquartered in the U.S. and serves customers across many regions. Its IDV solution has strong compliance features, leading to a large customer base in financial services and cryptocurrency, among other sectors. Jumio did not meet the commercial inclusion criteria.

Mitek: Mitek is headquartered in the U.S. and has customers mainly in Europe and North America. It has a strong customer presence in financial services, driven in part by its mobile deposit and fraud product lines. Mitek did not meet the commercial inclusion criteria.

Nametag: Nametag is headquartered in the U.S. and serves clients mainly in the U.S. It differentiates itself by focusing on workforce identity verification for use cases such as employee onboarding, account recovery and help desk verification, as well as some high-risk customer use cases. Nametag did not meet the commercial inclusion criteria.

Shufti: Shufti is headquartered in the U.K. and serves customers in many regions. It is differentiated by its ability to process a highly diverse set of identity documents from a large number of countries. Shufti did not meet the commercial inclusion criteria.

Veriff: Veriff is headquartered in Estonia and has customers mainly in North America and Europe, with many clients in the fintech industry. It has a strong suite of fraud intelligence capabilities that provide signals to detect attacks on the IDV process. Veriff did not meet the commercial inclusion criteria.

Evaluation Criteria

Product or Service: The capabilities, features and overall quality of the core goods and services that compete in and/or serve the defined market. Focus areas include document assessment, selfie and liveness assessment, workforce integrations and automation.

Overall Viability: The organization's overall financial health, as well as the financial and practical success of the relevant business unit. This includes the likelihood that the organization can continue to offer and invest in the product, as well as the product's position in the organization's portfolio. Focus areas include customer churn rate, proportion of revenue from top customers and employee attrition rate.

Sales Execution/Pricing: The organization's capabilities in all presales activities and the structures that support these activities. This includes deal management, pricing and negotiation, presales support and the overall effectiveness of the sales channel. Focus areas include specific pricing across a range of scenarios.

Market Responsiveness and Track Record: The ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This includes the provider's history of responsiveness to changing market demands.

Marketing Execution: The ability to deliver clear, high-quality, creative and effective messaging via publicity, promotional activity, thought leadership, social media, referrals and sales activities. This includes the organization's ability to influence the market, promote the brand, increase awareness of products and establish a positive reputation among customers.

Customer Experience: The degree to which a vendor's products, services and programs enable customers to achieve their desired results. This includes the quality of supplier/buyer interactions, technical support or account support, as well as ancillary tools, customer support programs, availability of user groups and service-level agreements.

Operations: The ability of the organization to meet its goals and commitments. This includes the quality of its organizational structure, skills, experiences, programs and systems that enable the organization to operate effectively and efficiently. Focus areas include identification of challenges in delivering the IDV service.

Ability to Execute

Ability to Execute Evaluation Criteria

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

Source: Gartner (August 2025)

Completeness of Vision

Market Understanding: The ability to understand customer needs and translate that understanding into products and services. Vendors with a clear vision of the market listen to and understand customer demands, and they can shape or enhance market changes with their vision. Focus areas include understanding why sales prospects choose not to buy an IDV product.

Marketing Strategy: The ability to clearly communicate differentiated messaging, both internally and externally, through social media, advertising, customer programs and positioning statements.

Sales Strategy: The ability to create a sound strategy for selling that uses the appropriate networks including direct and indirect sales, marketing, service and communication. This includes partnerships that extend the scope and depth of a provider's market reach, expertise, technologies, services and their customer base.

Offering (Product) Strategy: The ability to approach product development and delivery in a way that meets current and future requirements, with an emphasis on market differentiation, functionality, methodology and features. Focus areas include an understanding of the most impactful IDV product features that have been delivered and the shape of the IDV product roadmap.

Business Model: The design, logic and execution of the organization's business proposition. Focus areas include identifying possible disruptors in the IDV market.

Vertical/Industry Strategy: The ability to strategically direct resources (sales, product, development), skills and products to meet the specific needs of verticals and market segments. Focus areas include assessing the approach to dealing with IDV requirements in workforce use cases.

Innovation: Marshaling of resources, expertise or capital for competitive advantage, investment, consolidation or defense against acquisition.

Geographic Strategy: The ability to direct resources, skills and offerings to meet the specific needs of regions outside the providers' home region, either directly or through partners, channels and subsidiaries.

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	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (August 2025)

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 can act as thought leaders, driving market trends and investing in transformative technologies. While Visionaries may face challenges in execution, they can influence the market's direction and provide early access to breakthrough features.

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 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.

Automation Is Becoming a Higher Priority

Many IDV vendors do not offer fully automated IDV solutions and in fact, use human agents in their IDV processes for a variety of reasons:

- **Handling specific document types —** Some vendors offer fully automated flows for certain document types but rely on human agents for others, especially less common documents with fewer security features or those with unsupported character sets.
- **Improving accuracy —** Some vendors automate all document types but acknowledge that human agents can improve accuracy for specific cases. Customers may have to choose between full automation with lower accuracy or human involvement for higher accuracy.
- **Complying with regulations —** In some markets, particularly Europe, regulations require a human agent to review automated IDV decisions, especially in financial services. Some vendors include human review to help clients meet these obligations.
- **Handling exceptions —** Some vendors claim high accuracy with fully automated solutions but still use human agents for exceptions, such as invalid documents or low-quality images.

The use of human agents in IDV checks — and the corresponding lack of automation — is nuanced. While traditional KYC use cases for IDV did not always require real-time decisions, the expansion of IDV into new use cases has increased demand for automation to deliver faster responses and better user experience. Gartner clients also express concerns about sharing PII with human agents, particularly those offshore, and about meeting regional privacy requirements or contractual requirements for onshore processing.

Due to the following negative impacts of using human agents, automation has become a higher-priority buying criteria for organizations seeking IDV solutions:

- **Higher processing time —** Human involvement extends processing time and can erode user experience. Vendors with higher rates of human-agent use consistently show longer IDV processing times.
- **Concerns about protecting users' PII —** Vendors must have strong controls to prevent misuse of PII by human agents. Keeping data within required regions is harder when a vendor relies on globally distributed agents.
- **Higher pricing —** Vendors who rely heavily on human agents usually have higher pricing.

Threat Landscape Demands Broad and Deep Risk Signals

The threat landscape for IDV continues to evolve, with buyers increasingly concerned about sophisticated attacks. Vendors now regularly encounter deepfake content, both in the document and selfie steps, either presented directly to the camera or bypassing it entirely.

Today, the market expects all IDV vendors to have added measures such as presentation attack detection (PAD) and injection attack detection (IAD) to help mitigate these risks (see Note 1). While standards for PAD and IAD exist, the rapid pace of attacker innovation means some attacks will inevitably evade even the best defenses.

As a result, clients now expect vendors to deliver a broader and deeper approach to defending against deepfake threats. Many vendors have responded by adding multiple layers of risk-detection signals, including device, IP address, phone number and email insights. More sophisticated vendors also analyze user behavior during the IDV process and employ velocity checks across identity attributes.

While none of these additional signals can directly spot a deepfake, they can reveal signs of risk in an IDV event even if the deepfake itself is not detected. This layered approach is now seen as essential for robust IDV security.

Interest in IDV for Workforce Is Surging

Over the past year, Gartner has noted a significant increase in client interest in IDV for workforce applications. This trend is driven by high-profile security breaches involving attacks on IT help desk account-recovery processes and incidents of candidate fraud during remote hiring.

In response, IDV vendors are developing integrations with IAM services and other workforce IT infrastructure, and are increasing their sales and marketing focus on workforce opportunities. Clients evaluating IDV vendors for workforce use cases should ask about vendor integration capabilities with workforce systems to help maximize value as part of an IAM toolset.

Key workforce integrations examples include:

- **Access management (AM) tools —** Integrating IDV and AM tools enables real-time risk assessment by continuously verifying identities for high-risk interactions or access to sensitive systems and data, and by monitoring access patterns.

- **Identity governance and administration (IGA) tools —** Integrating IDV with IGA tools helps incorporate IDV into the broader identity life cycle, from onboarding to offboarding, and enforces stricter access controls.
- **IT service management (ITSM) tools —** Integrating IDV with ITSM tools helps verify the identity of users reporting incidents or requesting support, ensuring only verified users interact with IT services and reducing the need for manual checks.
- **Human resources management (HRM) —** integrating IDV with HRM platforms can help accurately verify new hires during onboarding, mitigate candidate fraud risk and ensure only verified employees access sensitive HR information and systems.

Hosted IDV UX Gaining Traction

Gartner clients across industries continue to evaluate IDV tools to establish trust in identity claims across a broad range of use cases. A common concern is the burden placed on IAM, cybersecurity and/or compliance teams to integrate yet another tool, especially when development resources are limited.

As a result, clients increasingly prefer IDV solutions that are easy and quick to implement, minimizing deployment time and resource requirements. Most vendors now offer a fully hosted IDV user experience, where end users receive a URL that directs them to a vendor-hosted IDV process, requiring no integration by the client organization.

This approach has gained significant traction since the previous edition of this Magic Quadrant, with most vendors reporting over a third of their clients now use hosted IDV UX. However, the depth and breadth of features vary across vendors. Differentiators include language localization, customization of look and feel, layout adjustability, white labeling, domain aliasing, expiring URLs and other features. Some vendors also support Apple App Clips and/or Android Instant Apps, allowing users to access an app-like experience without downloading a full application.

Reporting Is A Neglected Feature

Within most vendors' back-end administration portals, last year's differentiation was achieved by drag-and-drop workflow editors that made IDV tool configuration easier. This year, most vendors offer some level of workflow configuration, so client focus has shifted to reporting and analytics.

Vendors vary significantly in their reporting capabilities. Only a few provide comprehensive reporting suites that offer insights beyond counts of IDV events and aggregate outcomes. Some vendors offer self-service query or BI interfaces, while others still require clients to request custom insights through customer success teams, which then provide the data manually.

Accessibility Varies Greatly by Vendor

Many government and public-sector organizations have long focused on accessibility to ensure all citizens can use their services. Recently, private-sector organizations have shown urgent interest in accessibility, driven by the need to reach more users and comply with growing regulatory requirements. [1]

In response, this Magic Quadrant maintains and increases its focus on accessibility, evaluating both the end-user IDV products and the integration of accessibility into vendors' product management and development processes. Vendors were required to provide a VPAT (see Note 2) and a recorded demonstration of an automated accessibility scan for their end-user-facing IDV user interface, as well as show how their SDK performs with assistive technologies. This year, vendors also needed to provide a VPAT for their back-end administration portals.

The goal was to assess compliance with the Web Content Accessibility Guidelines (WCAG), version 2.1, Level AA — the recognised benchmark for compliance. Results showed wide variation. Some vendors declined to provide VPATs, some claimed full compliance but had VPATs or test results that showed otherwise, and some openly acknowledged deficiencies. Significant differences remain in vendors' performance on accessibility.

IDV buyers should clarify their own accessibility expectations, since end users will view the IDV process as part of the organization's interface and brand. With many vendors still demonstrating accessibility barriers, buyers must consider the impact on user experience, brand reputation and regulatory obligations. To learn more, see **3 Digital Accessibility Steps to a More Inclusive User Experience**.

Market Overview

This Magic Quadrant was developed in response to market conditions for IDV, reflecting several important trends.

The number of vendors in the IDV market continues to grow. Gartner has observed that while most vendors offer similar core IDV processes, significant differences exist, especially in geographic and industry focus. To add further complexity for buyers, some vendors provide IDV as a stand-alone product, while others include it as part of broader platforms, such as access management or biometric authentication tools. Market consolidation is likely in the future, as vendors look to acquire competitors to expand into new geographies or industries.

IDV is being applied to a broader range of use cases. Historically, IDV was primarily used for customer onboarding in regulated organizations to meet know-your-customer (KYC) requirements. Now, end-user organizations are buying IDV solutions for an ever broader range of use cases. Such use cases include fraud detection, trust and safety in marketplaces, social media, workforce applications, higher education for remote exam proctoring and student applications, 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, with strong and continuing client enthusiasm. 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 — such as when users have 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 verifying government-issued photo IDs and comparing them to selfies remains central, three additional types of checks are becoming more common:

- **Use of government eID schemes —** Examples include SPID in Italy, FranceConnect in France, or Singpass in Singapore. These provide citizens secure authentication and identity assertion, with varying adoption and assurance levels across sectors. Some IDV vendors now integrate with these schemes and offer platforms that combine IDV and 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, which enable real-time checks of user-provided or document-extracted data.

- **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 by country, depending on public and political attitudes about government handling of biometric data.

Some IDV vendors now connect to these eID schemes and authoritative sources to complement standard IDV checks, adding another layer of defense against identity impersonation and offering more options to customers.

IDV is a critical piece of wider digital identity initiatives. The IDV market is entering a period of transition, as portable digital identity initiatives mature, launch or undergo large-scale pilot programs. Projects like the EU digital identity wallet in Europe, which will require EU governments to offer identity wallets to its citizens by the end of 2026, are shaping the landscape. No single “winner” is likely to emerge; instead, a patchwork of competing and complementary schemes will persist for years. These solutions may or may not involve a dedicated digital identity wallet application for mobile devices. As portable digital identity adoption grows, the addressable market for IDV vendors may shrink, since verified identities will be reused rather than checked repeatedly. However, opportunities remain, as most portable digital identity solutions will still require an initial automated IDV event and IDV may play a role in account recovery and high-risk transactions. To stay relevant, IDV vendors must strategically evolve their offerings in this changing environment.

Acronym Key and Glossary Terms

AM	Access management
CIAM	Customer identity and access management
eID	Electronic identification
IAM	Identity and access management
IGA	Identity governance and administration
ITDR	Identity threat detection and response
ITSM	IT service management

OCR	Optical character recognition
PII	Personally identifiable information
SDK	Software development kit
NIST	National Institute of Standards and Technology
VPAT	Voluntary Product Accessibility Template

⊕ Evidence

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

Note 2: 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 of 1973 and other accessibility standards, such as the Web Content Accessibility Guidelines (WCAG). For further information see **VPAT — Information Technology Industry Council**.

⊕ Evaluation Criteria Definitions