

Magic Quadrant for Identity Verification

28 July 2026 - ID G00840985 - 48 min read

By Nayara Sangiorgio, Akif Khan, [and 1 more](#)

Identity verification tools are expanding beyond their original consumer fraud and compliance purposes and are increasingly deployed in workforce use cases. This Magic Quadrant evaluates 12 vendors to help leaders compare options and find the best fit for their identity verification 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 are delivered as SaaS or installable software, and provide assurance that a real-world identity exists through assessment of a government-issued photo identity document, 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 ability to complete the identity verification process on an end-user user device (a laptop, tablet, or smartphone, for example) with no requirement for the user to rely on specialized hardware.

Optional Features

The optional 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 Leader in this Magic Quadrant. Its 1Kosmos Verify product is available only as SaaS. Its operations are primarily concentrated in North America with a small presence in APAC and Europe. It has a strong presence across diverse industry verticals, including education, healthcare and retail/e-commerce. More than half of its customers use 1Kosmos for workforce use cases.

Recent updates feature an AI agent that analyzes and reports on identity verification patterns, including document-specific pass rates and trends in verification failures. Roadmap items include AI-based decision analysis and summary to assist human judgment in manual reviews.

Strengths

- 1Kosmos has 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 digital commerce, CIAM, CRM, ITSM, HR and background-screening platforms.
- It has demonstrated meaningful integration of AI into its back-end portal, with natural language workflow builders, risk configuration suggestions, and tailored reporting insights.

Cautions

- In 2025, the percentage of IDV checks requiring manual intervention became high relative to most other vendors in this Magic Quadrant, which 1Kosmos attributes to GenAI document fraud. This suggests that automated detection of such fraud can be improved.
- While it experienced some growth in Europe and Asia/Pacific, the majority of its customers are in North America, and so it is still building experience for servicing customers in other regions.
- Compared to other vendors in this research, 1Kosmos' pricing is higher for SaaS IDV deals, with fewer than 10 million annual checks, though pricing is competitive at higher volumes.

Daon

Daon is a Challenger in this Magic Quadrant. Its xProof IDV product is available as SaaS and software. Daon's operations are geographically diversified, and its customer base is mostly in financial services and government with a small proportion in telecom. Only a small minority of its customers use Daon for workforce use cases.

Recent updates include enhancements to its orchestration engine to support issuance and acceptance of wallet-based reusable identities and eIDs. Roadmap items include developing a proprietary technology for document recognition and classification.

Strengths

- It has a geographically diverse client base and is able to service prospects via a globally distributed sales force.

- Daon 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 deployed Daon as software, which they manage in their own environments to meet their own specific data processing requirements.
- The company connects to a wide range of eID schemes and authoritative data sources in different geographies, offering alternative approaches for users to assert their identity beyond just using IDV.

Cautions

- Daon self-reports a high percentage of end users in 2025 who needed to take second images of their document or face during the IDV process. Buyers should check the UX to ensure it meets their requirements.
- Its back-end portal and all of its support channels are available in English only.
- The company has very few customers in emerging sectors for IDV such as healthcare, the gig economy and workforce, and thus has little experience in these sectors. Instead, its customer base is concentrated in IDV sectors such as financial services and government.

Incode

Incode is a Leader in this Magic Quadrant. Its Incode Omni IDV product is available as SaaS and software. Its operations are primarily in the Americas with a small presence in Europe and Africa. Its customers are mostly in financial services, with a small proportion in other verticals such as cryptocurrency, government and gambling. Only a small minority of its customers use Incode for workforce use cases.

Recent updates include DMV Face Match, built on proprietary direct connections with some U.S. DMVs to check document and biometric data against the government-issuing authoritative source, with more state coverage planned for this year. Roadmap items include enhancements to its existing Trust Graph fraud signals to improve user experience.

Strengths

- Incode connects to a wide range of eID schemes and authoritative data sources in different geographies, offering alternative approaches for users to assert their identity beyond just using IDV. This includes direct connections to several U.S. state DMVs, going beyond the common basic connection to AAMVA.

- In 2025, it self-reported a high conversion rate for users going through IDV, suggesting an optimized UX.
- Its revenue is well-balanced across its customer base as 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

- Incode has few customers in emerging sectors for IDV, such as healthcare, the gig economy and marketplaces, and hence has little experience in these sectors. Its largest proportion of customers by far is in financial services.
- Incode's accessibility performance is low compared to other vendors in this research. The company's Voluntary Product Accessibility Template (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 for some people to use.
- Compared to other vendors in this research, it has a low ratio of technical presales consultants per salesperson, and a low deal-closing ratio. This suggests that sales processes must be improved.

LexisNexis Risk Solutions

LexisNexis Risk Solutions is a Niche Player in this Magic Quadrant. In 2025, LexisNexis Risk Solutions completed the acquisition of Australia-based IDV vendor IDVerse and it is now integrated into the LexisNexis Risk Solutions suite. Its IDVerse IDV product is available only as SaaS. Its customer base is primarily in Asia/Pacific with a notable presence in the Americas. Its customers are predominantly in financial services with a small proportion in other verticals such as healthcare and retail/e-commerce. Only a small minority of its customers use LexisNexis IDVerse for workforce use cases.

Recent updates include a proprietary active capture capability for document and biometric verification combining on-device and server-side validation. Roadmap items include IDVerse IDKit, a self-service SaaS identity verification platform to offer a mobile-friendly, no-code solution.

Strengths

- LexisNexis Risk Solutions' 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.
- It is able to service prospects via a globally distributed sales force.
- The company has a strong roadmap to address areas needing improvement to align with the needs of an evolving IDV market. These include integrations with eIDs and authoritative data sources, coupled with even deeper integration with other LexisNexis Risk Solutions products to consume a broader range of risk signals.

Cautions

- LexisNexis Risk Solutions adds implementation complexity by not offering meaningful out-of-the-box integrations with platforms across consumer or workforce use cases.
- It does not connect to any eID schemes and very few authoritative data sources, thus providing little alternative to the traditional document-based IDV process.
- The company earns a high percentage of IDV revenue from its top 10 customers, which increases risk if customer churn occurs.

Nametag

Nametag is a Visionary in this Magic Quadrant. Its IDV product is available only as SaaS. Its operations are aggregated in North America, and its customers are distributed among diverse industry verticals, including healthcare, education, and retail and e-commerce. An overwhelming majority of its customers use Nametag for workforce use cases.

Recent updates include proprietary technology to cryptographically attest GPS signals and create a record that binds the verified identity to a verified device and location. Roadmap items include developing an identity graph to link verified individuals with their accounts and actions across workforce applications.

Strengths

- Nametag has a strong vision for workforce IDV use cases and has demonstrable experience in this domain with the overwhelming majority of its customers using it in a workforce context.

- It self-reports a short duration for users to complete the IDV process, suggesting an optimized UX.
- It had a zero percent churn rate in 2025, with every customer that was up for renewal doing so.

Cautions

- Given its focus on workforce use cases, Nametag has little demonstrable experience in consumer use cases and lacks meaningful integrations for this market.
- All of Nametag's customers are in North America, and so it has limited experience and capability for servicing customers in other regions.
- Its accessibility performance is poor. The company's VPATs show definitive "Does Not Support" failures across standard WCAG Level A and AA criteria for its user-facing IDV UI, meaning the solution will be difficult for some people with disabilities to use.

Persona

Persona is a Leader in this Magic Quadrant. Its IDV product is available as SaaS. Its operations are predominantly in North America with a small presence in Europe. Its customers are mainly in online marketplaces, financial services and the gig economy. Only a small minority of its customers use Persona for workforce use cases.

Recent updates include achieving FedRAMP Moderate Authorization. Roadmap items include the launch of Relay, Persona's double-blind claims-based product that confirms claims like minimum age without exposing unnecessary personally identifiable information (PII) for use cases where a user does not need to go through full IDV.

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.
- Despite having a customer base concentrated in North America, the company processed a highly diverse set of global identity documents in 2025. It also plans for regional expansion by already offering its support channels and back-end portal in multiple languages today.

- Compared to other vendors in this research, Persona offers low per-check pricing across SaaS scenarios.

Cautions

- The company self-reported a conversion rate across all platforms and SDKs that is lower than other vendors in this research. Buyers should check the UX to ensure that it meets their requirements.
- While it experienced some growth in Europe and Asia/Pacific, the majority of its customers are in North America, and so it is still building experience for servicing customers in other regions.
- While Persona scored well for customer experience, 24/7 live support is limited to critical issues only. Customers with noncritical issues must rely on email and ticketing support.

Regula

Regula is a Niche Player in this Magic Quadrant. Its IDV solution is available exclusively as software installed by customers on their own infrastructure. Its operations are global, and its customers are notably in financial services with a small proportion in travel and government, as well as being used by other IDV vendors. Only a small minority of its customers use Regula for workforce use cases.

Recent updates include launching the Regula IDV platform with features such as a low-code orchestration layer, risk-based workflows and anti-money laundering (AML) screening.

Roadmap items include know-your-business (KYB) with capabilities to verify a company and create a company's business profile to help identify risks.

Strengths

- Regula has strong experience deploying IDV as software, meeting client requirements to keep all data processing within their infrastructure, and serving customers in many regions.
- Its revenue is well-balanced across its customer base as 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.
- The company self-reports a high conversion rate for users going through IDV, indicating that the UX has been optimized.

Cautions

- Regula 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.
- It does not provide additional risk checks such as velocity checks. Customers must use outputs from the SDK to create such features themselves.
- The company does not connect to any eID schemes or authoritative data sources which have become increasingly common in the market today, instead only narrowly focusing on document-based IDV.

Socure

Socure is a Leader in this Magic Quadrant. Its DocV IDV solution is available only as SaaS. Its operations are predominantly concentrated in North America, and its customers are primarily in financial services with a small proportion in online marketplaces, government and education. Only a small minority of its customers use Socure for workforce use cases, although these are high volume.

Recent updates include the expansion of its Identity Graph to continuously monitor identity risk through a subscription-based model for real-time identity intelligence. Roadmap items include a Resume Identity Graph to detect fraud patterns between resumes and identity attributes captured by its Identity Graph.

Strengths

- Socure connects to a high number of eID schemes and authoritative data sources to provide additional ways to verify user identity beyond traditional document-based IDV checks.
- It has 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.
- The company has invested heavily in prebuilt integrations for workforce use cases, most notably recruitment, and now has a large number of integrations to HR and background screening platforms.

Cautions

- The vast majority of Socure’s customers are in North America, so it has limited experience and capability for servicing customers in other regions.
- Its back-end portal and support channels are available in English only.
- The company was unable to demonstrate experience in processing a diverse set of global identity documents at scale, with the majority of its volume being North American identity documents. This may be a concern for prospective customers in other regions, or for those in North America with global IDV requirements.

TrustDecision

TrustDecision is a Niche Player in this Magic Quadrant. Its IDV product is available as SaaS and software, although the software-delivered version currently has no customers. Its operations are concentrated in Asia/Pacific, with a small presence in the Americas, and its customers are mostly in financial services, with a small proportion in social media. TrustDecision has no customers using its IDV solution for workforce use cases.

Recent updates include enhancements to device intelligence and deepfake detection capabilities. Roadmap items include expanding connections with government and authoritative issuing sources, including Indonesia’s Dukcapil and other official sources in the Philippines and Mexico.

Strengths

- TrustDecision’s revenue is well-balanced across its customer base as 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.
- Compared to other vendors in this research, it offers very low per-check pricing across SaaS scenarios.
- Given its strong focus on emerging markets in the Asia/Pacific region, the company has heavily optimized its IDV process to work on legacy devices and in low-bandwidth environments.

Cautions

- The company had a high churn rate in 2025.

- It does not reduce implementation complexity by offering meaningful out-of-the-box integrations with platforms across consumer or workforce use cases.
- TrustDecision did not submit VPATs for its end-user-facing UI or back-end portal, and thus was unable to demonstrate any conformance at all with accessibility requirements. This strongly suggests an immature approach to accessibility.

Veridas

Veridas is a Visionary in this Magic Quadrant. Its IDV product is available as SaaS and software, although the on-premises version has limited adoption with few live customer deployments. Its operations are mostly in Europe with a notable presence in the Americas, and its customers are largely in financial services with a small proportion in gambling and government. Only a small minority of its customers use Veridas for workforce use cases.

Recent updates include support for emerging markets with improvements to enable faster processing of IDV data on low-end devices. Roadmap items include creating a real-time risk engine by leveraging machine learning models in real-time risk signal analysis to produce a unified identity risk score.

Strengths

- Veridas had a low churn rate in 2025.
- The company demonstrates high technical inclusivity, investing heavily in ensuring that its IDV solution can work in emerging markets with legacy devices and low bandwidth. It is also unusual in supporting HarmonyOS for mobile devices in addition to the more standard iOS and Android.
- Veridas' decentralized identity wallet, Nexus, is a strategic asset that positions the company for relevance as the European market evolves under the eIDAS 2.0 regulation.

Cautions

- Veridas increases implementation complexity for customers by not offering meaningful out-of-the-box integrations with platforms across consumer or workforce use cases.
- The company earns a high percentage of revenue from its top 10 customers, which increases risk if customer churn occurs.

- Its accessibility performance is poor. The company's VPATs show definitive "Does Not Support" failures across standard WCAG Level A and AA criteria for its user-facing IDV UI, meaning the solution will be difficult for some people with disabilities to use.

Veriff

Veriff is a Visionary in this Magic Quadrant. Its IDV product is available only as SaaS. Its operations are mostly in North America and Europe with a small presence in LATAM and APAC. Its customers are mostly in financial services and online marketplaces with a small proportion in gambling. Only a small minority of its customers use Veriff for workforce use cases.

Recent updates include the acquisition of Vespia — a KYB intelligence platform — to include registry checks, ultimate beneficial owner (UBO) identification and risk screening. Roadmap items include a single IDV flow that supports eIDs, biometric registries and digital wallets with a fallback to physical IDs.

Strengths

- Veriff offers an innovative pricing model in which it refunds customers for any IDV events that are approved but in fact turn out to be fraudulent.
- The company is expanding its IDV business from individuals to businesses through the acquisition of Vespia, a KYB intelligence platform.
- It connects to a high number of authoritative data sources across different geographies, providing alternative means to check identity beyond just document-based IDV.

Cautions

- Veriff increases implementation complexity for customers by not offering any out-of-the-box integrations with platforms across consumer or workforce use cases.
- Compared to other vendors in this research, the company had a high churn rate and low renewal rate.
- It was unable to submit VPATs for its end-user-facing UI or back-end portal, and thus was unable to demonstrate conformance with accessibility requirements. However, it has an active accessibility program in place with VPATs due later in 2026.

ZOLOZ

ZOLOZ is a Niche Player in this Magic Quadrant. Its IDV product is available as SaaS and software. Its operations are largely concentrated in China and Asia/Pacific, and its customers are mostly in financial services with a small proportion in telecom, cryptocurrency and gambling. Only a small minority of its customers use ZOLOZ for workforce use cases.

Recent updates include the launch of an IDV product that enables KYC data to be reused and shared among customers, and RealDoc, an LLM-powered document processing product. Roadmap items include leveraging AI models to proactively analyze contextual and risk signals, and detect emerging fraudulent patterns in IDV journeys supporting adaptive risk decisions.

Strengths

- ZOLOZ has a strong roadmap to leverage AI — using it to analyze context, proactively detect new types of fraud, and make adaptive risk decisions.
- It implemented innovative use of LLMs to improve data extraction from documents, backed by metrics demonstrating the performance improvements.
- The company made significant improvements in accessibility during 2025. Its VPATs showed a high level of compliance with WCAG 2.1 Level AA, and even went beyond that standard measure by demonstrating strong compliance with Level AAA.

Cautions

- ZOLOZ declined to provide pricing-scenario information. As a result, we are unable to assess its commercial value proposition.
- The vast majority of the documents it processes are from a cluster of countries in Asia/Pacific. This may be a concern for prospective customers in other regions, or for those in APAC with global IDV requirements.
- Compared to other vendors in this research, its churn rate in 2025 was high.

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

- LexisNexis Risk Solutions
- Nametag
- Veriff

Dropped

- Entrust
- Sumsub

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 2026:

- 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 single 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 2025, and at least 25% year-on-year revenue growth when compared to fiscal year 2024, and at least 5% customer growth year-on-year in 2025 when compared to fiscal year 2024.
- At least \$50 million in identity verification revenue in fiscal year 2025, and at least 35% year-on-year revenue growth when compared to fiscal year 2024, and at least 10% customer growth year-on-year in 2025 when compared to fiscal year 2024.
- At least \$20 million in identity verification revenue in fiscal year 2025, and at least 40% year-on-year revenue growth when compared to fiscal year 2024, and at least 20% customer growth year-on-year in 2025 when compared to fiscal year 2024.
- At least \$3 million in identity verification revenue in fiscal year 2025, and at least 90% year-on-year revenue growth when compared to fiscal year 2024, and at least 50% customer growth year-on-year in 2025 when compared to fiscal year 2024.

Honorable Mentions

The following vendors did not meet the commercial inclusion criteria for the MQ. Their exclusion does not mean that they lack viability. The following are noteworthy providers not included in the formal analysis. These providers could be appropriate for clients, contingent on their requirements:

- **AU10TIX:** AU10TIX is headquartered in the Netherlands, with offices in the U.K., New York, Singapore, Bulgaria and Australia, and serves customers globally. Its identity verification solution includes deepfake detection and serial fraud prevention capabilities. It is used by clients in a broad range of industries, including emerging use cases in areas such as the gig economy and digital assets.
- **Entrust:** Entrust is headquartered in the U.S. Entrust completed an acquisition of IDV vendor Onfido in 2024 and has integrated it with its heritage IDV solution. Its operations are global, and its customers are mostly in financial services and cryptocurrency. It has strong

orchestration capabilities with its Studio Workflow editor, which includes integration with Mastercard's Ekata.

- **IDnow:** IDnow is headquartered in Munich, with offices in London, Paris, Rennes, Berlin and Iasi. Its operations are mostly in Europe. IDnow offers IDV from within its Trust Platform — alongside fraud prevention and compliance capabilities — offering automated, video, and eID verification capabilities, and EUDI Wallet integration. It offers global document coverage.
- **Jumio:** Jumio is headquartered in the U.S. It serves customers globally. Jumio has a strong foothold in financial services, and it processes a diverse set of global documents. Jumio recently introduced selfie.DONE — a reusable digital identity solution — worldwide.
- **Microblink:** Microblink is headquartered in the U.S. Its customer base spans a variety of industry verticals, and it is used by other IDV vendors that leverage Microblink's document assessment technology, which overall performed strongest in recent U.S. Department of Homeland Security (DHS) testing.
- **Mitek:** Mitek is headquartered in the U.S. Its operations are mainly in Europe and North America, with a strong presence in financial services. Mitek offers both mobile deposit and check fraud detection solutions for financial institutions, as well as biometric authentication and identity verification.
- **Shufti:** Shufti is headquartered in the U.K. and serves customers in many regions. It is differentiated by its demonstrable capability to process a highly diverse set of identity documents from a large number of countries.
- **Signicat:** Signicat is headquartered in Norway. In 2025, Signicat acquired Dutch NFC-focused IDV solution Inverid, and it integrated Inverid's ReadID solution into its IDV suite. Its operations are mostly in Europe, and it serves European customers, driven by its focus on meeting the diverse requirements of European countries.
- **Sumsub:** Sumsub is headquartered in Ireland. Its operations are global and its customers are mainly in financial services and cryptocurrency. Sumsub offers a portable digital identity solution called "Reusable KYC," which enables users who completed IDV with Sumsub to reuse their identity data in subsequent identity assertions, including KYC. It also has coverage of a diverse set of global documents.

- **Yoti:** Yoti is headquartered in the U.K. Its IDV solution can also orchestrate digital IDs from around the world, and it offers its own reusable digital identity wallet that enables users to verify their identity once and then control what data they share. It also has proprietary technology for age estimation.

Evaluation Criteria

Ability to Execute

Product or Service: The capabilities, features and overall quality of the core goods and services that compete in 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 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 (July 2026)

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 communications. 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 provider’s home region, either directly or through partners, channels and subsidiaries.

Completeness of Vision Evaluation Criteria	
Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium

<i>Evaluation Criteria</i>	<i>Weighting</i>
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Medium
Innovation	High

Source: Gartner (July 2026)

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.

Identity Impersonation Detection Demands Multilayered Risk Evaluation

Many Gartner clients have observed a rise in identity attacks driven by generative AI, raising an important question: "Can IDV keep pace with the new era of GenAI-created synthetic content?" This concern is well-founded, as synthetic media created using GenAI tools are rapidly transforming the threat landscape.

Concerns with deepfake attacks have raised the bar for the IDV market. IDV vendors are now expected to have their solutions tested for presentation attack detection (PAD) and injection attack detection (IAD) to mitigate the risk of a deepfake making its way successfully into an IDV flow (see Note 1).

PAD, IAD and inspection of images for signs of being GenAI created are not enough in the current aggressive threat landscape, however. The leading IDV vendors in the market have invested in a range of additional risk signals, such as those focused on device, phone number, email, behavior and location. These are assessed both in isolation and also as part of velocity checks. Further risk mitigation checks can involve checking identity data against authoritative data sources.

Some IDV vendors are also introducing industry vertical-specific signals — such as analyzing resume data and cross-referencing it with other user information to detect inconsistencies. Others are partnering with specialized risk signal platforms, including those focused on higher education fraud (see [Mitigate Fraudulent Student Applications Through Identity Verification](#)).

The authors of this Magic Quadrant have also observed that some IDV vendors are leveraging AI agents in risk assessments, enabling real-time evaluation of all collected risk signals as unified data points, which could simplify decision making for both customers and human agents.

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.

Demand Is Starting to Move Beyond Document Verification

Electronic identity (eID) schemes are digital identity systems, often provided by governments (trusted source), that let people prove who they are online using an official eID. If a user can log in and assert their identity using a trusted eID (like a government-issued digital ID), this could replace the traditional IDV process because there wouldn't be a need for the user to provide a document — since the user will have verified their identity when enrolling in the eID scheme.

Additionally, some IDV vendors verify the PII on a user's captured document by checking it against third-party identity attribute data sources. This helps confirm that the identity exists in the real world and isn't entirely fake. However, if a bad actor has stolen someone's identity or obtained their PII — such as name, address, date of birth, or Social Security Number (SSN) — they could still use that information to impersonate someone else.

To address this risk, innovative IDV vendors are going a step further by verifying users' PII — and, in some cases, biometric data — directly with authoritative issuing sources like

government databases or official registries. This approach allows for more reliable and direct validation of personal data.

When an IDV vendor connects with authoritative sources (such as AAMVA in the U.S., Serpro in Brazil, DVS in Australia, Aadhaar in India, or Dukcapil in Indonesia), they can confirm whether the information on a captured document or even just a captured biometric matches what's stored in official records. Any mismatches can indicate potential risk. This method provides a strong risk signal and enables decisions to be backed by evidence and direct corroboration from the issuing authority, making the verification process overall more robust and trustworthy.

As such, many IDV vendors are evolving into “identity assertion hubs” that offer document-based IDV, verification via eID, and corroborative checks against third-party data sources or authoritative issuing sources. This allows their customers to offer a range of verification offers to their end users, which may vary by demographic or geographic market.

IDV Faces Competition for Workforce Use Cases

Since the release of the 2025 Magic Quadrant for Identity Verification, Gartner has observed a continued rise in client interest in IDV for workforce use cases, such as remote account recovery and remote employee hiring and onboarding. Cybersecurity leaders continue to show interest in IDV, driven by concerns over attack scenarios that exploit weaknesses in remote security processes.

However, IDV tools can also introduce friction, increase costs, and raise concerns from employees about biometric data processing. Many IDV vendors are addressing workforce needs by enhancing their risk signal capabilities, integrating with authoritative sources, and offering prebuilt connections to workforce IAM and IT systems (see [Workforce Identity Verification Requires Unique Capabilities](#)). Despite these advancements, issues related to cost, user experience and privacy remain significant concerns for many customers.

The rise of deepfake-enhanced social engineering attacks and the exploitation of security gaps in remote and hybrid work environments present ongoing challenges. Importantly, not all impersonation attacks involve deepfakes. For example, while a deepfake was reportedly used in the Hong Kong fake CFO case that led to a \$25 million loss,¹ there is no publicly known evidence that deepfakes were involved in other successful attacks such as on the IT service desks at MGM Casinos or Marks & Spencer.^{2,3} Such challenges have led to an emerging ecosystem of “identity impersonation detection” vendors that are competing with IDV vendors to address workforce use cases.

For example, vendors such as TruSONA use a range of contextual signals based on a caller's location, device, and phone number, coupled with checks on the user's document alone, to protect IT service desks. Other vendors such as Imper.ai and HYPR have reimaged knowledge-based verification for employees, pulling on high recency data from workforce systems to create security questions to verify employees ("Who were the attendees in the meeting you joined at 11 a.m. this morning?").

IDV is now competing with these identity impersonation detection solutions for the budget of cybersecurity buyers who seek to address a broad range of workforce challenges.

Interest in Reusable Identity Is Emerging

The IDV market has evolved rapidly beyond compliance in recent years, being used in a diversity of use cases in a range of industry verticals. However, IDV as it stands today is typically a stand-alone process. Every time a user needs to verify their identity, they have to provide a government-issued document and take a selfie for biometric comparison. This process is repetitive and creates friction for users.

In the past year, Gartner clients have expressed mounting concern with the friction in repeated point-in-time IDV. The promise of reusable or portable digital identity models is to make verification faster and more convenient, benefiting both users and organizations by reducing friction and repetitive checks (see [Begin Portable Digital Identity Evaluation With Use Cases and Trends in Government Digital Policies and Adoption](#)).

Such portable digital identity schemes can be offered by governments, or by organizations such as banks or telcos. However, some IDV vendors also already offer reusable identity models. With reusable identities, typically users would only need to verify themselves once. After that, they can use their verified digital identity for future transactions, eliminating the need to repeat document and selfie capture for every new service. Reusable identities can be tied to authentication methods and are stored by the user often in secure digital wallets. This helps mitigate the risk of account takeover.

Some reusable identity schemes, like bank-based ones, are centralized in nature, while others, such as the European digital identity wallet (EUDIW), are decentralized in nature (see [Market Guide for Decentralized Identity](#)).

Reusable identities are the next step in the IDV market evolution for key reasons:

- **Better UX:** A one-time, reusable identity makes onboarding and accessing services much faster and easier for users, improving UX and reducing abandonment rates.
- **Operational efficiency:** Organizations save time and resources by not having to trigger document plus selfie events for each interaction or identity assertion challenge. They can trust the previously verified identity, streamlining operations.
- **Support for privacy and user control:** Theoretically, reusable identity solutions give users more control over their data, allowing them to share only the specific information needed for a transaction, rather than exposing all their personal details. For example, in age assurance requests, a user could share proof of age and no additional unnecessary data beyond what is needed.
- **Enables interoperability:** Reusable identities can be used across supporting platforms and services, making it easier for users to access a wide range of offerings with a single, trusted identity.

Whether an IDV vendor can develop a network of users with their portable digital identity solution that is of a size comparable to a government, bank or telco remains to be seen. Scale and size of network will be a critical determinant for driving adoption and ensuring the long-term success of any such solution.

Improving Administration Tasks With AI

In the first iteration of this Magic Quadrant, within most vendors' back-end administration portals, differentiation was achieved by drag-and-drop workflow editors that made IDV tool configuration easier. Last year, most vendors offered some level of workflow configuration; this year, reporting and analytics continue to be a focus for clients.

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.

This Magic Quadrant observes that some IDV vendors are enhancing their reporting and workflow capabilities through the integration of AI agents. By leveraging these agents, customers can simply input natural language prompts tailored to their specific needs or use cases — such as customer onboarding or blocking access from sanctioned locations — and

receive data insights or workflow suggestions automatically. This streamlines the process of building and configuring workflows — which are typically done manually or via APIs — and mining insights from different prebuilt reports, significantly reducing the time and effort required.

AI agents can also recommend decision logic for approvals or manual reviews and offer guidance for specialized or emerging scenarios, such as determining the appropriate level of IDV stringency in different regions. This evolution not only increases operational efficiency but also enables clients to adapt quickly to changing requirements and regulatory environments, ultimately saving valuable and scarce resources.

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.⁴

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

The goal was to assess compliance with the Web Content Accessibility Guidelines, version 2.1, Level AA — the recognized 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 [Market Guide for Digital Accessibility](#).

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, and strategic partnerships between IDV vendors and vendors in other markets are emerging. 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, and even to verify the legitimacy of other businesses (KYB). The example of account recovery, particularly in the workforce context, has seen a surge of interest since late 2023, with sustained client enthusiasm ever since. 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, and Singpass in Singapore. These provide citizens with 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, and 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, and RENAPER in Argentina. The creation and operation of these databases vary by country, depending on public and political attitudes about government handling of biometric data. Furthermore, the availability of these databases for commercial organizations such as IDV vendors to query also varies depending on legal and political contexts.

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 their citizens by the end of 2026, are shaping the landscape. Additionally, client demand for less friction in IDV processes for returning customers and employees could also help move this space forward. 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 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 more information, see [VPAT — Information Technology Industry Council](#).

⊕ Evaluation Criteria Definitions

Unlock more AI value

With unmatched, proprietary AI insights from Gartner

[Explore the AI Hub ↗](#)

© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and 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.

[About Us](#) [Search Careers](#) [Newsroom](#) [Policies](#) [Site Index](#) [Featured Insights](#)
[Contact Us](#) [Send Feedback](#)

Gartner

© 2026 Gartner, Inc. and/or its Affiliates. All Rights Reserved.