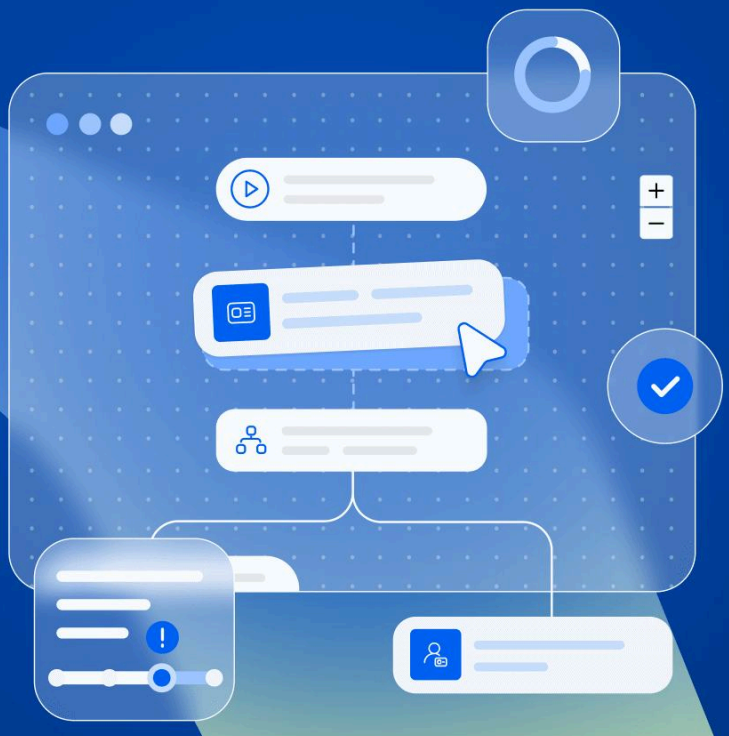
MICROBLINK

A Buyer's Checklist

How To Evaluate An Identity Platform

Choosing vendors for your identity stack is a time-consuming and opaque process. With non-standard industry terms out there and unverifiable marketing claims, it can be hard to know if what you're buying really matches your needs until after implementation.

To help minimize the guesswork, here are the 65 most common questions that buyers should be asking vendors. The Microblink team has compiled this from the questions that we see in RFPs and industry guides, as well as feedback from our own customers on their business needs and decision drivers. We hope it's useful!



MICROBLINK

Table of contents

1 Company

Questions to Ask	Positive Indicators	Concerns To Investigate
Describe your company's growth over the last 3 years.	A strong response will include concrete details on revenue growth, market expansion, and customer acquisition, as well as any major partnerships or strategic investments. It should highlight key acquisitions or structural changes in a way that reassures stability and demonstrates a commitment to innovation, such as increased R&D investment or hiring in critical areas like AI, security, and compliance.	Vague or evasive answers that lack specific metrics or trends are concerning, as are mentions of frequent leadership turnover or recent layoffs without a clear strategic explanation. Indications of stalled growth, declining revenue, or major customer losses suggest potential instability. Additionally, sudden acquisitions or restructuring without a clear long-term plan may indicate financial trouble.
Which technologies do you develop in-house and what parts of your solution rely on third-party solutions?	A good answer should clearly distinguish between proprietary technology and third-party components, justifying the use of external providers for specialized functions like OCR or biometric analysis.	If a vendor heavily relies on whitelabelled third-party services for core identity verification functions without clear differentiation or transparency, costs may be inflated and expertise may be lacking.
What are the key milestones on your upcoming product roadmap?	The response should outline a well-structured, forward-thinking roadmap aligned with industry trends, including milestones related to regulatory changes, AI advancements, or UX improvements. It should explain how planned features will support customer needs and market demands while providing realistic delivery timelines, demonstrating a proactive rather than reactive approach to innovation.	A vague or non-committal answer with no concrete milestones suggests a lack of strategic planning. If a vendor's priorities seem unclear or purely reactionary, that could indicate instability or a lack of vision. Promises of features without clear delivery dates or an absence of consideration for industry trends and compliance changes should also raise concerns.
What is your release cycle?	A well-structured response will detail a predictable release cadence, balancing frequent updates with stability for clients. The vendor should explain how releases are managed—whether through staged rollouts, A/B testing, or clear versioning—and emphasize transparent communication about new features and changes.	If a vendor has no clear release schedule or an inconsistent update pattern, that may indicate a lack of operational maturity. Frequent disruptive changes without proper notice can create business risks, while slow update cycles could signal stagnation.

2 Pricing

Questions to Ask	Positive Indicators	Concerns To Investigate
What is your cost structure?	A strong response will transparently explain whether pricing is per transaction, per user, or bundled, while also breaking down costs related to implementation, maintenance, and support. The vendor should highlight any volume discounts, overage fees, or optional add-ons and ensure the pricing model aligns with scalable business needs.	Hidden costs or an unclear fee structure can indicate financial unpredictability. Significant price jumps at higher usage tiers without added value or high setup and maintenance fees without justification should be viewed skeptically.
Is the contract and pricing all-inclusive or do you require additional agreements with 3rd party vendors?	A good answer will provide clarity on whether all services are included in the base price and, if third-party agreements are needed, explain which ones and why.	Unexpected third-party costs that complicate budgeting are a major concern, as is a requirement for customers to negotiate separate agreements with third parties.

3 ID Document Capture

Questions to Ask	Positive Indicators	Concerns To Investigate
What percentage of users complete the image capture process?	A strong answer will provide data on average completion rates, segmented by geography, document type, and integration method (web vs. SDK). The vendor should acknowledge that conversion rates vary due to factors like fraud deterrence, user friction, and regional user behavior while offering solutions to optimize completion rates through UX improvements.	A claim of an unrealistically high completion rate (e.g., near 100%) may indicate a lack of fraud controls or a misleading metric. If the vendor cannot provide segmented data or insights into why users drop out, they may not have the necessary analytics capabilities to optimize conversion.
What is the average time it takes for a user to complete the verification process?	A good response provides an average time for completion, broken down by workflow type (fully automated vs. human-in-the-loop), document type, and region. The vendor should explain how they optimize for speed while maintaining accuracy, and how their UX minimizes friction for users.	If a vendor cannot provide timing benchmarks, it suggests they do not track UX performance effectively. If their verification process is consistently slow or heavily reliant on manual reviews, it could cause delays and drop-offs in user onboarding.

Questions to Ask	Positive Indicators	Concerns To Investigate
What real-time feedback guides the user through successful image capture?	A good answer will describe interactive guidance features such as tilt adjustment prompts, lighting suggestions, or framing indicators, explaining how these improve capture success rates.	If the vendor offers no real-time feedback, users may struggle with poor-quality image submissions, leading to frustration and increased support costs. Generic or ineffective guidance, as well as overly complex feedback that confuses users rather than helping them, should be seen as weaknesses in the solution.
Is the image auto-captured or does the user manually tap a shutter button?	The vendor should describe an auto-capture feature that enhances UX by optimizing image quality through factors like lighting, clarity, and motion detection. If manual capture is also supported, they should explain when it is useful and how it integrates with the overall user experience.	If the vendor lacks an auto-capture feature and requires manual image capture, this could lead to a poor user experience and higher failure rates. A poorly implemented auto-capture system that frustrates users or does not effectively improve image quality should also be seen as a concern.
How do different image capture devices affect the perfomance of your solution?	The vendor should demonstrate that their solution is tested across a broad range of devices, from high-end smartphones to older models, and explain how they optimize performance based on camera quality, lighting conditions, and processing power. They should mention device compatibility testing and continuous improvements based on real-world data.	A lack of detail about testing on different devices suggests potential inconsistencies in image capture quality. If a vendor struggles with performance on lower-end or older devices, it could lead to higher failure rates for certain user segments.
Does your UI meet Web Content Accessibility Guidelines (WCAG) guidelines?	A strong answer will confirm compliance with WCAG standards and provide examples of accessibility features, such as screen reader compatibility, color contrast adjustments, and keyboard navigation support. The vendor should demonstrate a commitment to inclusivity by regularly testing and improving accessibility features.	If the vendor is unsure about WCAG compliance or lacks documentation, their UI may not be accessible to users with disabilities. A failure to address accessibility concerns could lead to compliance risks and limit usability for a diverse audience.
Do you support photo uploads/PDF uploads?	The vendor should clearly define supported input methods, including live capture, photo uploads, and PDFs, and explain fraud prevention measures such as metadata checks or liveness detection for uploaded images.	Unrestricted uploads without fraud mitigation could introduce security risks. If the vendor cannot clearly explain how they handle different document formats, that indicates a lack of sophistication in their verification process.
Do you support using NFC to read RFID chips in identity documents?	A vendor should confirm NFC support for reading RFID chips in identity documents and explain how it enhances security and data integrity. They should acknowledge that not all documents contain chips and not all devices have NFC capabilities, and describe how they handle fallback scenarios when NFC is unavailable.	A response that fails to address the limitations of NFC compatibility across different devices and document types suggests a lack of understanding of real-world deployment challenges.

Questions to Ask	Positive Indicators	Concerns To Investigate
Which character sets and languages are supported for OCR?	The vendor should provide a detailed list of supported languages and character sets, ensuring they cover the regions and document types relevant to your needs. They should also describe their approach to continuous improvement, such as expanding language support based on customer demand and leveraging machine learning for better OCR accuracy.	If a vendor gives a vague or incomplete response without listing supported languages, it suggests they may not fully understand the scope of their OCR capabilities. A lack of commitment to expanding language support or improving recognition for complex scripts (e.g., Arabic, Chinese, Cyrillic) is a potential concern.
Can the UI be customized to local languages?	The vendor should confirm that their UI supports localization, including language translation for both the user-facing experience and the admin portal. They should describe their approach to supporting multiple languages and how updates to translations are managed.	If the vendor only supports a limited set of languages or requires complex workarounds for localization, it may indicate a lack of flexibility in their UI. A lack of support for non-Latin scripts may also be a concern for global deployments.
How can the UX be adapted to match my company's brand?	A good response should outline the level of customization available, such as changing fonts, colors, and UI elements. Ideally, they should offer a no-code or low-code customization interface for easier branding adjustments without requiring developer intervention.	If branding options are rigid or require significant development effort, it may hinder seamless integration. A vendor that offers only minimal customization without explaining how deeper modifications can be achieved may not be the best fit for companies needing strong brand consistency.

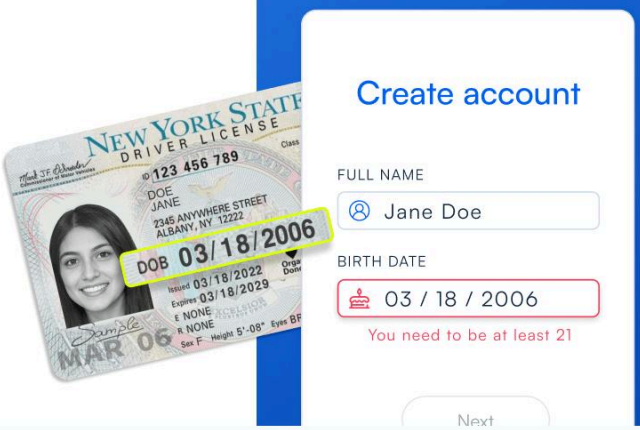
4 ID Document Verification

Questions to Ask	Positive Indicators	Concerns To Investigate
Which countries and document types are supported?	The vendor should provide a detailed and up-to-date list of supported countries and document types, ensuring that their coverage aligns with your business needs.	If a vendor does not have a comprehensive or regularly updated list of supported documents, they may struggle with maintaining global coverage.
Can the solution detect document liveness?	The vendor should confirm whether their solution can assess document liveness in addition to biometric liveness.	If the vendor does not support document liveness detection, their fraud detection capabilities may be weaker.

Questions to Ask	Positive Indicators	Concerns To Investigate
How frequently is support for new document types added?	A good answer will describe a structured approach to adding new documents, such as proactive monitoring for document updates, partnerships with issuing authorities, and an internal SLA for integrating new document templates. They should provide an estimate of how quickly they adapt to changes.	If a vendor lacks in-house capabilities to expand their supported document library, expect delays and limits in coverage.
What security checks are performed on an ID document?	A strong response will outline both document-specific security checks (such as color formatting and and watermark analysis) and document-agnostic checks (such as detecting photocopies, screen-presented images, or manipulated documents).	If a vendor provides a generic or vague response without listing specific security measures, it may indicate weak fraud detection capabilities. A lack of proactive fraud prevention mechanisms could lead to an increased risk of undetected identity fraud.
Can your solution extract identity data from the PDF417 barcode?	A well-prepared vendor will confirm support for reading identity data from the PDF417 barcode, explaining how it is used for fraud detection (e.g., detecting mismatches between barcode data and OCR-extracted text).	If a vendor does not support PDF417 barcode extraction or fails to validate barcode authenticity, they may lack a key fraud detection capability. A vague response about barcode processing suggests potential security gaps.
What is your average verification rate (of all the users that start the verification process, how many reach a pass/fail assessment)?	A good answer will provide an average verification rate and explain how it varies by geography, document type, and verification method (e.g., web vs. SDK). The vendor should also highlight efforts to improve verification rates, such as real-time feedback during image capture.	An unrealistically high verification rate may indicate weak fraud controls, while an extremely low rate could signal a poor UX. If a vendor cannot provide verification rate data, they may lack proper analytics capabilities.
What is the false acceptance rate (FAR) and false rejection rate (FRR)?	The vendor should provide FAR and FRR metrics, ideally segmented by document type and geography. They should also explain how these rates are benchmarked, how they optimize for both security and user experience, and whether customers can fine-tune thresholds to balance fraud prevention with accessibility.	If a vendor is unwilling to disclose these metrics or provides unrealistic figures, it suggests a lack of transparency. High FAR indicates a weak security system, while high FRR could lead to unnecessary user frustration and onboarding drop-offs.
What is the accuracy of your document verification and face matching?	The vendor should provide benchmarks on the accuracy of both document verification and face matching, ideally with third-party testing results. They should also explain how their models handle edge cases, such as poor lighting conditions, aging effects, or partial occlusions.	A vague or overgeneralized response without accuracy benchmarks suggests the vendor may not rigorously test their technology. If they do not account for real-world variability, their solution may struggle with diverse user conditions.

5 Biometrics

Questions to Ask	Positive Indicators	Concerns To Investigate
What checks do you perform on the selfie?	The vendor should confirm that selfies are checked for liveness and face matching against the ID document photo. They should also explain additional fraud detection mechanisms, such as AI-driven anomaly detection or checks for image manipulation.	A lack of liveness detection or weak face-matching capabilities increases the risk of fraud. If the vendor does not provide details on how they ensure selfie authenticity, their solution may be vulnerable to spoofing.
Is your solution iBeta tested, and what level of Presentation Attack Detection is available?	A vendor that has undergone iBeta testing should provide certification details, describing their PAD capabilities and how they perform against known spoofing attacks.	If a vendor lacks PAD benchmarks or is unwilling to share third-party testing results, their liveness detection may be unproven.
Do you offer active or passive liveness detection?	The vendor should be able to explain the mechanisms of liveness detection, and explain how they solve for friction and fraud.	The use of active liveness detection could negatively impact completion rates, accessibility and fraud prevention.
Can you detect if the same face has been used multiple times?	A strong response will confirm the ability to detect repeated face usage, either via biometric deduplication or cross-referencing verification events. They should describe their approach to identity clustering and how this feature helps prevent synthetic identity fraud.	A vague response without technical details suggests they do not actively monitor for repeat fraud attempts.
Can biometric information be re-used for authentication use-cases such as login?	The vendor should confirm support for biometric authentication beyond initial identity verification, describing how they enable secure re-authentication with liveness detection and encryption. They should also address compliance with data retention and privacy regulations.	If the vendor does not support biometric re-use or lacks a clear privacy framework, it could indicate lack of suitability for authentication use cases.



6 Age Verification and Estimation

Questions to Ask	Positive Indicators	Concerns To Investigate
Can your solution verify the age of a user?	The vendor should confirm support for age verification via document data extraction. They should provide accuracy benchmarks and compliance information for age-restricted use cases.	If the vendor cannot automate age verification, their solution may not be reliable for age-restricted applications
Is biometric age estimation available?	A strong response will describe the accuracy and confidence intervals of biometric age estimation, addressing potential bias concerns. They should explain how the algorithm determines age and provide validation data.	If a vendor does not provide accuracy benchmarks or cannot explain how their model works, it suggests potential reliability issues. A lack of transparency about bias mitigation is also problematic.

7 Additional Verification, Fraud and Risk Signals

Questions to Ask	Positive Indicators	Concerns To Investigate
What is the perfomance for PII data matching against official databases, and how does this vary by region?	A strong answer will describe the vendor's approach to PII matching with third-party data sources. They should explain how accuracy and coverage vary by region.	If a vendor lacks regional performance insights or does not clarify how they handle PII verification, they may not have robust global coverage. A lack of database integrations may limit identity validation capabilities.

Questions to Ask	Positive Indicators	Concerns To Investigate
Is a risk score available? How is it calculated?	The vendor should confirm whether they provide a risk score and explain how it is derived, detailing the factors considered (e.g., device signals, document anomalies, behavioral analytics). Transparency in model explainability is key.	If the vendor provides a black-box risk score without clarity on inputs, it may be difficult to interpret and use effectively. A lack of customization options for risk scoring could limit usability.
Describe how device geolocation is used in your solution?	A strong response will explain how geolocation data is collected, whether it is based on IP address, GPS, or Wi-Fi triangulation, and how it is used to assess risk. The vendor should highlight how they compare a user's location to expected locations based on the identity document provided and whether they factor in travel patterns, VPN detection, or known fraud hotspots.	If a vendor does not leverage geolocation at all, it may indicate weak risk assessment.
What device footprint signals are available?	A good response will outline the various device signals collected, such as browser fingerprinting, IP address, operating system, and hardware identifiers. The vendor should explain how these signals are analyzed to detect fraud patterns, such as multiple identities being verified from a single device.	If the vendor does not collect device footprint signals or only provides basic information without deeper fraud analytics, their solution may lack sophistication in detecting repeat fraud attempts. A failure to address data privacy and security concerns related to device tracking is also problematic.
Are email, address and phone signals available?	A strong answer will confirm whether the solution can analyze email, address, and phone signals, detailing sources such as telecom providers, postal databases, or fraud detection networks. The vendor should also explain how these signals contribute to risk scoring and identity verification.	If a vendor does not utilize any of these signals or cannot verify their authenticity, it may limit the depth of their identity verification. A lack of integration with external data sources for validating email, address, and phone details is also a concern.
Can the solution detect injection attacks?	A strong response will describe the mechanisms used to detect injection attacks, such as monitoring for screen recording software, analyzing pixel inconsistencies, or using challenge-response methods to ensure real-time image capture.	If the vendor does not have a strategy for detecting injection attacks or provides only a vague response, their system may be vulnerable to synthetic identity fraud and deepfakes. A lack of proactive monitoring against advanced fraud attempts is also concerning.

8 Results

Questions to Ask	Positive Indicators	Concerns To Investigate
What information is returned about the user after their verification?	The vendor should specify whether they return extracted OCR data, document authenticity scores, face match confidence levels, and additional risk indicators. They should also highlight whether they provide structured risk assessments rather than just pass/fail results.	If the vendor only returns basic extracted data without confidence scores or fraud indicators, it may limit your ability to make informed identity verification decisions. A lack of transparency in their scoring methodology is also problematic.
What determines if a user is accepted or rejected?	The vendor should clarify whether they provide a final decision on acceptance/rejection or if they provide raw verification data for customers to make their own decisions. They should also explain how decision-making thresholds can be customized.	If the vendor does not provide clarity on how decisions are made or if they enforce rigid rules without customization options, it could limit your control over the verification process. A lack of transparency in decision logic is a concern.
How can my team view and interact with the verification results?	A strong response will confirm whether a dedicated admin portal is available, allowing teams to review, audit, and override verification decisions.	If verification results are not easily accessible or if manual review capabilities are limited, it may indicate poor operational support.
Is it possible to export data?	A vendor should confirm data export capabilities and describe available formats (e.g., CSV, JSON, API access) while ensuring compliance with data security and privacy regulations.	If the vendor restricts or does not support data exports, it may limit your ability to conduct fraud investigations or meet compliance requirements. A lack of transparency on data access policies is also a concern.
Does your solution leverage fuzzy matching to improve results?	A well-prepared vendor will confirm their use of fuzzy matching for OCR and identity data comparisons, explaining how it improves accuracy for names, addresses, and other text fields with minor variations. They should provide evidence of NLP-driven performance improvements.	If the vendor lacks fuzzy matching capabilities, their system may struggle with minor data inconsistencies, leading to higher false rejection rates. A failure to demonstrate improved accuracy through fuzzy matching is also a concern.

9 Automation

Questions to Ask	Positive Indicators	Concerns To Investigate
Is the solution automated or are there human-in-the-loop checks?	The vendor should explain whether their solution is fully automated, human-reviewed, or a hybrid approach. They should describe how they balance speed with accuracy for edge cases	A fully automated workflow will give the quickest response without the bias of human error.
What is the difference in accuracy, fraud detection rates, processing times and costs between the automated and human-in-the-loop processes?	A good response will should highlight when manual review is necessary, if at all.	If costs and processing time escalates with human review, there is cause for concern.

10 Implementation

Questions to Ask	Positive Indicators	Concerns To Investigate
Is the solution available on-premises or via cloud?	The vendor should confirm whether they offer a cloud-based SaaS solution, on-premises deployment, or a hybrid model. They should outline the advantages and trade-offs of each approach, including data security, compliance, and operational effort.	If the vendor only offers a single deployment model without flexibility, it may limit your ability to meet regulatory or business requirements. A lack of clarity on data security for SaaS deployments is also a concern.
How do I orchestrate multiple identity checks into a workflow?	A strong answer will describe how the vendor enables customers to build custom verification workflows using multiple identity checks, such as document verification, biometric matching, and third-party data validation. They should also highlight any no-code orchestration tools or API flexibility.	If a vendor does not support workflow orchestration or requires complex integrations for combining different checks, it may reduce efficiency. A lack of dynamic risk-based verification options is also concerning.
Are mobile and web SDKs available for image capture?	The vendor should confirm support for both mobile and web SDKs, explaining how they optimize for different platforms and device capabilities. They should also describe their update cycle and developer support.	If a vendor lacks SDK support for either mobile or web, it may limit your deployment options. A poorly maintained SDK with infrequent updates is also a concern.

Questions to Ask	Positive Indicators	Concerns To Investigate
Can all the model thresholds be adjusted, self-serve?	The vendor should confirm that customers can adjust model thresholds for face matching, document verification, and fraud risk scoring, ideally through a self-serve dashboard without requiring vendor intervention.	If model thresholds are fixed or require extensive support requests to modify, it could limit flexibility in adapting the solution to different risk tolerances. A lack of customization options is problematic.
What team and resources are needed to successfully implement your solution?	A vendor should provide details on the roles and skills required for implementation, including whether a development team is needed and what technical expertise they require (e.g., RESTful APIs, SDK integration). They should offer examples of similar-sized companies that have successfully implemented their solution, outlining typical timelines, challenges, and best practices. A strong response will also include details on documentation, onboarding support, and professional services available.	If the vendor does not specify required resources or assumes implementation is straightforward without offering real-world case studies, it may indicate poor planning support. A lack of clarity on necessary development skills or an overly complex setup process without adequate documentation could lead to delays and increased costs.
What team and resources will I need to use and maintain your solution over time?	A good response will outline the ongoing resource requirements, such as developer involvement for updates, training needs for new team members, and expected backend maintenance efforts. The vendor should provide insights into how often changes occur, the learning curve for new users, and what level of support is included to assist with maintenance.	If the vendor does not clarify maintenance expectations or requires extensive development work for every update, it may indicate a high long-term operational burden. A lack of training resources or unclear support policies could make it difficult to onboard new team members effectively.

11 Service Level Agreement

Questions to Ask	Positive Indicators	Concerns To Investigate
Describe your account support philosophy	A strong answer will specify whether the vendor follows a self-serve or hands-on support model, detailing what level of assistance is included and what professional services cost extra. They should mention how many customers they serve, whether dedicated account managers are available, and their approach to proactive customer engagement.	If support is minimal or hidden behind expensive professional service fees, it could indicate a lack of commitment to customer success. A vague or one-size-fits-all approach without considering business size and complexity may also be a concern.

Questions to Ask	Positive Indicators	Concerns To Investigate
What is the escalation and resolution methodology your company uses when account issues arise?	The vendor should describe a structured, well-documented escalation process, including expected response times, key points of contact, and how issues are prioritized based on severity. They should also explain how they track and communicate resolution progress.	If the vendor lacks a formal escalation process or provides generic support without clear resolution timelines, it may lead to prolonged downtime or unresolved issues. A lack of transparency in issue tracking and updates is also concerning.
Describe your downtime, response times and resolution times.	A strong response will include historical uptime percentages (ideally above 99%), response time commitments for different support tiers, and average resolution times for common issues. The vendor should also explain how they minimize disruptions through proactive monitoring and redundancy measures.	If the vendor cannot provide realistic downtime or response metrics, it suggests a lack of reliability tracking. Claims of perfect uptime without historical evidence may be unrealistic, and slow response times could indicate weak support structures.

12 Data Security

Questions to Ask	Positive Indicators	Concerns To Investigate
Describe how roles and permissions are managed.	A vendor should provide granular role-based access controls, allowing organizations to define permissions for different user levels. They should ensure that access to sensitive PII data can be restricted and that administrative controls are intuitive and customizable.	If all users have the same access or if permission controls are rigid and non-configurable, it may create security and compliance risks. A lack of detailed documentation on role management is also problematic.
What data is collected and stored?	The vendor should provide a detailed list of collected data points, distinguishing between temporary and stored data. They should explain retention policies, consent management, and whether data is used for training AI models.	If a vendor collects excessive PII without clear justification or retains data indefinitely without customer control, it may create compliance risks. A lack of transparency on data usage is also concerning.
Where is PII stored and processed?	A good answer will specify the geographic locations of PII storage and processing, ensuring compliance with regional data protection laws.	If a vendor does not disclose where PII is stored or lacks the ability to comply with regional data laws, it may lead to compliance issues. A lack of transparency on data handling processes is also problematic.

Questions to Ask	Positive Indicators	Concerns To Investigate
Are regional endpoints available so that PII data can remain within a chosen territory (e.g. EU)	A strong response will confirm whether customers can choose regional endpoints for data processing, ensuring compliance with regulations such as GDPR. They should also provide details on data routing and storage policies.	If a vendor cannot support regional data residency requirements, it may limit adoption for organizations with strict compliance needs. A vague response on data flow and storage is also concerning.
What is the data retention period and is it customizable?	The vendor should confirm whether customers can define retention periods, with options for immediate purging, short-term storage, or long-term archiving. They should explain how retention settings align with compliance requirements.	If data retention policies are rigid or unclear, it may limit compliance flexibility. A vendor that retains PII indefinitely without customer control should raise concerns.
Is data encrypted in transit and at rest?	The vendor should confirm encryption protocols (e.g., AES-256 for storage, TLS 1.2/1.3 for transmission) and explain how they protect sensitive data against unauthorized access.	If encryption standards are outdated or unclear, it may indicate weak data security practices. A lack of end-to-end encryption should raise concerns.
How do you handle regional biometric data protection requirements (eg. BIPA)?	A strong response will explain how the vendor ensures compliance with biometric data protection laws. They should outline consent collection processes, data retention policies, and how they handle user opt-out requests.	If the vendor does not have a clear compliance strategy, it may create legal risks. A lack of transparency on how biometric data is stored and managed is a concern.

13 Resource Requests

Questions to Ask	Positive Indicators	Concerns To Investigate
Share customer references or testimonials	A reliable vendor should be able to provide references from businesses of similar size, industry, or use case. Case studies with measurable results (e.g., improved onboarding conversion rates, fraud reduction) indicate a strong track record. Testimonials from recognized brands, industry leaders, or regulated businesses suggest credibility. If a vendor can arrange direct conversations with existing customers, it's a sign of confidence in their solution and support.	If the vendor hesitates to share references, it may indicate a lack of satisfied customers or reluctance to expose weaknesses. Be wary if they only share outdated references or if customer feedback lacks measurable impact.

Questions to Ask	Positive Indicators	Concerns To Investigate
Share your developer documentation	A strong vendor will provide well-structured, publicly accessible developer documentation, preferably in an online portal with easy navigation, search functionality, and API references. The documentation should include clear integration guides, SDK instructions, code samples, and troubleshooting sections. Ideally, there should be versioning information to track updates, along with webhooks and customization options. If interactive API testing is available, such as a sandbox or Postman collection, it's a good sign of a developer-friendly experience.	If documentation is outdated, difficult to access, or only available on request, it may indicate a lack of transparency or insufficient developer support. Poorly structured or incomplete documentation, missing key details like authentication methods or response formats, suggests a higher risk of integration challenges. If there's no mention of SDK updates, breaking changes, or changelogs, it could indicate poor version control and maintenance.
Share your privacy and security policies	A reputable vendor should provide a well-documented privacy policy outlining data collection, processing, storage, and retention practices. They should also clarify compliance with GDPR, CCPA, BIPA, and other relevant data protection regulations. A strong security policy should detail encryption standards (e.g., AES-256, TLS 1.2/1.3), internal access controls, data minimization strategies, and breach response protocols. If they provide independent security audits, SOC 2, ISO 27001, or penetration test reports, that's a sign of robust security practices.	If privacy and security policies are vague, outdated, or difficult to obtain, it suggests a lack of transparency. A lack of mention of key regulations, such as GDPR compliance for European data processing, could indicate potential legal risks. If they avoid discussing security certifications or refuse to disclose how they handle breaches, it raises concerns about data protection. Vendors that retain user data indefinitely without clear justification should also be scrutinized.
Share a live demo	A strong vendor will offer a hands-on demo showcasing their user experience, fraud detection capabilities, and admin portal. The demo should include real-time document verification, selfie matching, and liveness detection, demonstrating accuracy and speed. Ideally, the vendor will allow you to test various document types and simulate different user scenarios (e.g., poor lighting conditions, edge cases). A sandbox or free trial where you can evaluate the solution independently is a positive indicator.	If the vendor is unwilling to provide a live demo or only offers pre-recorded videos without live interaction, it suggests they may be hiding performance issues. Poor UI/UX during the demo, frequent verification failures, or slow processing times indicate potential user friction. If they avoid letting you test edge cases, such as blurred images or fraud scenarios, it could mean their solution struggles with real-world conditions. A lack of transparency in demonstrating backend processes, decision logic, or admin controls should also be a concern.

Get in touch if you have any questions or suggestions.

Contact us >