

The AI Companion Guide for Evaluating eSignature Solutions





Contents

1. Executive summary	03
2. Transparent pricing	04
3. Regulatory compliance	07
4. User trust and security	10
5. Support and Customer Success	13
6. Technical landscape	16
7. Conclusion	19

The information contained in this document is for information purpose only, is provided AS IS as of the date of publication, and should not be relied upon as legal advice or to determine how the law applies to your business or organization. You are responsible for obtaining legal advice from your own legal counsel. You should not act or refrain from acting on the basis of any of our content without first obtaining matter specific legal and professional advice. OneSpan accepts no responsibility for any loss or damage which may result from accessing or reliance on the content of this document, and disclaims any and all liability with respect to acts or omissions made by readers on the basis of our content. Our content may contain links to external websites and external websites may link to our content. OneSpan is not responsible for the content or operation of any such external sites and disclaims all liability associated with such websites.



Executive summary

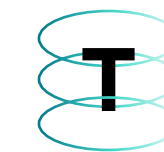
Evaluating software has never been faster, but speed can come at the cost of accuracy.

Today buyers increasingly rely on AI to evaluate vendors, compare features, and even generate decision frameworks before speaking with a provider. In minutes, buyers can produce what looks like a comprehensive shortlist, complete with pros, cons, and recommendations.

The AI guidance can look complete, but it often overlooks what matters most.

While AI brings speed and efficiency to eSignature evaluations, it often misses critical factors that can lead to poor decisions. That's why your vendor assessment requires more than speed with a proven eSignature evaluation framework.

The OneSpan **TRUST Framework** provides a practical lens for eSignature vendor comparisons to assess what truly determines long-term program success, including:



Transparent pricing:

What will it really cost as you scale?



Regulatory compliance:

Will it stand up to scrutiny in your environment?



User trust and security:

Can every transaction be verified and defended?



Support and Customer Success:

Who is there when it matters most?



Technical landscape:

Will it integrate and scale without added complexity?

Short on time? Use this prompt to instantly generate a TRUST-based eSignature evaluation framework.

“Create an eSignature evaluation framework using the TRUST model (Transparent pricing, Regulatory compliance, User trust & security, Support, and Technical landscape), outlining key criteria, risks, and where AI insights should be validated through deeper vendor analysis.”

Transparent pricing

How to evaluate pricing transparency

eSignature pricing is complex because the per-seat or per-envelope price shown on a website rarely reflects the **true total cost of ownership (TCO)**. Factors such as implementation, support tiers, API usage, advanced features, and renewal negotiations frequently increase the final cost.

Why pricing transparency matters

Many businesses express frustration with the cost of eSignatures, often driven by overage charges, add-on features, and significant renewal increases. As a result, they are unable to forecast costs with confidence.

The real challenge is predictable TCO. When pricing models rely on hidden add-ons, organizations struggle to forecast ongoing vendor costs. That uncertainty creates financial risk.





Pricing considerations to watch for

Why

Envelope or transaction limits

Understand your actual volume before committing to any envelope-based plan, and model what happens if your volume grows by 50% year on year.

Feature gating

Key capabilities such as white labeling or single sign-on may be locked behind higher-tier plans. A low entry price can mask the the real cost of implementation when uncovering required features that are gated.

Renewal pricing

Some vendors have been publicly criticized for significant price increases at renewal (in some cases 200–600% above the original contract price). Ask each vendor about their renewal pricing practices and check review sites such as G2.com for patterns.

Support tier pricing

Enterprise-grade support, meaning access to human help, is often a paid add-on.

Integration and API costs

Automation and system integrations can introduce additional charges. These costs can become significant in high-volume environments.





The core pricing question

Before comparing vendors, ask one critical question: Can we forecast our three-year cost without modeling overages, exceptions, or best-case assumptions?

If the answer is no, the pricing model likely introduces pricing risk.



Where AI helps and where it doesn't

AI tools can be extremely useful to:

- Compare baseline pricing and packages available on vendor websites
- Suggest pricing patterns that tend to create cost overruns
- Help you define a TCO framework that aligns with your business needs for eSignature

AI cannot:

- Predict how a vendor will reprice you at renewal
- Know your real envelope volume or growth curve
- Create an accurate three-year TCO financial forecast

That's why AI should be used to help you develop a pricing evaluation framework, instead of calculating final numbers.



What to look for in a trusted partner

A trusted eSignature partner does more than provide a competitive starting price. They offer pricing clarity with transparent cost structures and clear guidance on:

- How pricing will evolve as usage grows
- Integration costs such as API transaction costs
- Support packages

Look for vendors who are willing to model multi-year costs while explaining renewal practices upfront. Your first year should lay the foundation for a trusted eSignature partnership, grounded in the ability to confidently forecast total cost of ownership.



AI prompt for pricing evaluation

eSignature pricing and TCO snapshot

I'm evaluating eSignature vendors [vendor 1, vendor 2, vendor 3] for a [industry] organization with ~[number] users and ~[number] agreements/month across [key use cases]. Assume [X]% annual growth and future needs for APIs, integrations, and expanded workflows.
[paste pricing pages]

Provide a concise executive summary covering:

- **Baseline cost:** Estimated starting cost by vendor based on our profile
- **Pricing model:** Key differences (per user, per envelope, tiered, usage-based)
- **Cost risks:** Overage triggers, gated essential features, and hidden/implied costs (e.g., APIs, integrations, support)
- **TCO outlook (2–3 years):** Where costs are likely to increase or diverge as we scale
- **Key questions:** List 3–5 critical questions to validate true cost and avoid surprises



Regulatory compliance

How to evaluate regulatory compliance

Many eSignature providers position themselves as “secure” or “compliant,” yet the level of assurance behind those claims can vary widely. For organizations operating in regulated industries, the ability to comply with the ever-changing landscape of regulations, prove document integrity, and demonstrate a complete, tamper-evident record of the transaction is mission-critical to protect against legal action and reduce regulatory risk. eSignature compliance is not inherent to the eSignature technology alone. Instead, it is largely shaped by how the solution is implemented, configured, and governed.

Why regulatory compliance matters

For organizations operating in regulated industries, compliance is a requirement tied directly to legal enforceability and risk management. Organizations may unknowingly be exposed to gaps that only surface during audits or legal disputes. This can include unenforceable agreements, failed audits, regulatory penalties, or the inability to defend a transaction in a dispute. While pre-built, compliance-ready workflows can accelerate deployment; true compliance depends on a deliberate, compliance-oriented implementation that’s aligned to your organization’s regulatory requirements.





Compliance considerations to watch for

Why

Fragmented audit trails

When eSignatures are integrated or embedded in user applications, there may be gaps in transaction logs or evidence that would be challenged in disputes or audits.

Envelope tamper protection

When does tamper protection begin? It's important for eSignature workflows to protect against tampering across the end-to-end workflow instead of only post-completion.

Regulatory support and global compliance gaps

Not all vendors support advanced/qualified signatures required in certain jurisdictions. How do they adhere to global standards such as eIDAS and ESIGN?

Data residency

Regulated and compliance-driven industries often require transparency and control over data residency. What options do you have for deployment of eSignature workflows?

Retention and validity

How does the platform ensure document integrity and signer authenticity, and can signed records be securely transferred and stored in your business applications (e.g., SharePoint, Salesforce, Box, Laserfiche, etc.)?





The core compliance question

Before selecting a vendor, ask one critical question: How does your solution enable us to confidently prove the validity and integrity of every eSignature agreement, across all use cases, jurisdictions, and audit scenarios?

If the answer is unclear, the compliance model likely introduces regulatory risk.



Where AI helps and where it doesn't

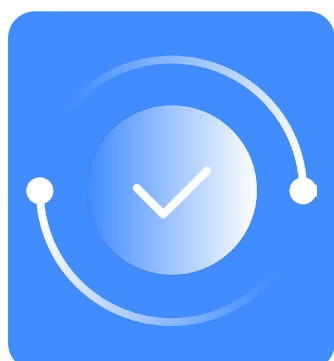
AI tools can be extremely useful to:

- Map your requirements (i.e. regulations such as eIDAS, ESIGN, UETA, or internal policies) to a vendor's public claims and identify any gaps
- Compare vendors' publicly listed compliance features to regulatory frameworks, while identifying details that may require a deeper review
- Generate a structured evaluation framework for eSignature compliance needs

AI cannot:

- Independently verify an eSignature vendor's public claims to ensure audit and dispute readiness
- Validate the eSignature vendor's controls to meet regulatory standards in practice
- Ensure compliance reflects your organization's internal risk tolerance or regulatory obligations

Implement or configure an eSignature solution in a way that meets your business's specific compliance or risk management objectives. That's why AI should be used to structure your compliance evaluation instead of relying on AI to verify public claims, certifications, or audit readiness.



What to look for in a trusted partner

A trusted eSignature partner will validate how they enable compliance with regulatory standards. This includes clearly documented support for adherence to global regulations, robust and tamper-evident audit trails, and built-in controls that promote long-term document integrity.

Look for vendors who can explain how their compliance model works in practice, demonstrate how agreements stand up to audit or dispute, and align their capabilities to your specific regulatory environment.

AI prompt for compliance evaluation



I'm evaluating eSignature vendors [vendor 1, vendor 2, vendor 3] for a [industry] organization that must comply with [regulations—e.g., eIDAS, ESIGN, HIPAA, FINTRAC, internal policies].
[paste vendor documentation or compliance pages]

Provide a concise executive summary covering:

- **Compliance coverage:** Explain how each vendor aligns to required regulatory frameworks
- **Strengths and gaps:** List any publicly available claims, and outline gaps in auditability, document residency, and document retention
- **Evaluation framework:** List the core criteria to assess compliance, auditability, and tamper-proof criteria from a vendor
- **Key questions:** Include 3–5 critical questions for eSignature compliance criteria that require deeper validation



User trust and security

How to evaluate user trust and security for eSignatures

Trust in digital agreements is rooted in establishing a person's identity. Not all eSignature platforms offer the same level of identity assurance, which links the signer's verified identity to the transaction to keep every agreement authentic, defensible, and secure. When combined with a fully branded eSigning workflow, identity assurance reinforces trust by delivering a secure and familiar experience that users recognize and rely on.

Why user trust and security matter

Not all authentication methods provide the same level of assurance. Without strong identity assurance and transaction integrity, digital agreements can be challenged, invalidated, or exploited. Just as important, people continuously assess the brands they engage with, making it critical to reinforce the legitimacy of each eSignature transaction so that recipients recognize it as authentic, trust it, and confidently complete the signing process.





Pricing considerations to watch for

Why

Verification method optionality

Vendors may offer limited authentication options, making it difficult to align identity assurance with transaction risk, user context (i.e., mobile verification), channel needs (i.e. in-person vs. online), or regional requirements. Verify that vendors provide a wide range of authentication options including SSO, SMS, knowledge-based authentication or Q&A, government ID or credentialing, digital certificates, and passkeys.

Verification strength

Not all authentication methods provide the same level of assurance. Basic methods (e.g., email access) may be insufficient for high-risk or regulated transactions. Layered identity verification, such as two-factor authentication, strengthens the defensibility and trustworthiness of digital agreement transactions, which is also required for KYC and other regulatory policies. Align the level of identity verification to the risk and regulatory expectations of each transaction.

Fully branded experience

With the rise of phishing attacks targeting digital transactions, how can customers confidently verify that an eSignature request is legitimate? Ask eSignature vendors if they deliver a fully branded end-to-end customer experience that builds trust and improves agreement completion rates.





The core user trust question

During your vendor evaluation, ask one core question: How do you verify every signer's identity and prove agreement authenticity, while aligning authentication methods to regional regulations and customer preferences?

If the answer is uncertain, the eSigning security and customer experience model may introduce risk.



Where AI helps and where it doesn't

AI tools can be extremely useful to:

- Evaluate identity verification features across vendors
- Map security and authentication capabilities to regional regulatory requirements
- Develop a framework to assess delivering a secure and trusted signer experience

AI cannot:

- Validate whether identity verification methods are strong enough for your specific risk profile
- Diagnose your security and authentication threats in a meaningful way
- Define the best security measures that protect your customer and your brand

AI can help structure and accelerate your evaluation, but securing digital agreements and maintaining customer trust ultimately depends on your organization's decisions and controls.



What to look for in a trusted partner

A trusted partner delivers high-assurance identity verification, flexible authentication aligned to your risk and compliance profile, and a fully branded experience that end users are more likely to recognize and trust. They will go beyond listing features to demonstrate how their solution enables secure, defensible and trustworthy eSignature agreements for your organization and customers.



AI prompt for user trust and security evaluation

I'm evaluating eSignature vendors [vendor 1, vendor 2, vendor 3] for a [industry] organization operating in [region], with requirements aligned to [regulations—e.g., eIDAS, KYC/AML, HIPAA].
[Insert links or documentation]

Provide a concise executive summary covering:

- **Authentication coverage:** Compare methods offered (e.g., email, SMS OTP, KBA, ID verification, digital certificates, passkeys)
- **Identity assurance strength:** Rate each vendor (low, moderate, high) and by relevance to KYC/regulatory requirements
- **Regulatory alignment:** Explain how capabilities map to regional standards (e.g., eIDAS levels, AML/KYC expectations)
- **Key risks and gaps:** Identify weaknesses in authentication, identity spoofing risk, limited certificate/ID support, or known security concerns
- **Trust and experience factors:** Evaluate their ability to support multi-factor authentication and end-to-end branding (across emails, URLs, and signing experience) in protecting user trust
- **Evaluation framework:** Provide a framework to guide me on when to use specific identity method supported by each vendor, as well as required MFA scenarios and the core criteria I should consider for secure, compliant workflows
- **Key questions:** Include 3–5 critical questions to help me probe deeper into each vendor's identity assurance and security claims



Support and customer success

How to evaluate customer support for eSignatures

Customer support is often the difference between a successful deployment and a stalled or costly implementation. Many vendors position support as an add-on. In reality, customer support is the critical link for success across onboarding, configuration, integration, compliance alignment, and ongoing eSignature scale. The true test of an eSignature vendor is how they support your organization when it matters most, and defining this relationship is important right from the start.

Why customer support matters

eSignature solutions don't operate in isolation. They are widely embedded into mission-critical digital workflows, applications, and regulated processes. When issues arise or requirements evolve, delays in support can directly delay projects while impacting both revenue and customer experience. Customer support also directly links to faster time to value, reduced delivery risk, optimized workflows, and digital scale, all while improving employee productivity. Without reliable and accessible support, organizations risk underutilizing their eSignature platform or waiting on solutions for technical issues.





Customer support considerations to watch for:

Why

Access to expertise

Some vendors rely heavily on self-service or ticket-based support. Confirm whether expert guidance is available via phone or email, and understand typical response and resolution times.

Dedicated client success managers

Evaluate whether dedicated customer success resources are available to support your specific needs—especially for complex integrations or regulated workflows where guidance can accelerate deployment and improve outcomes.

Support tiers

Clearly understand what's included across support tiers, including Premium options. Ensure pricing, scope, and service levels align with your project needs.

Migration knowledge and guidance

Assess whether the vendor offers proven migration expertise, and ideally to transition your existing digital agreements with minimal disruption.

Community and developer support

A strong user and developer community accelerates troubleshooting and learning without dependency on support tickets.



The core customer support question

It's important to ask: Will this provider actively support our success across implementation, integration, and ongoing scale of our digital workflows, or only respond when major issues arise?

If support is reactive, limited, or difficult to access, it may slow your ability to deploy and scale.



Where AI helps and where it doesn't

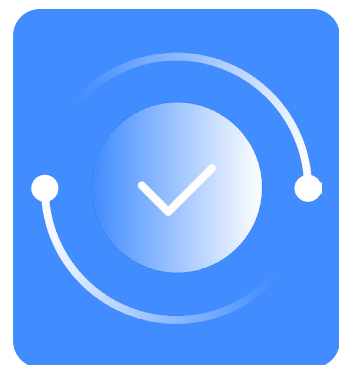
AI tools can be extremely useful to:

- Compare vendor support models, including additional costs
- Summarize customer reviews and satisfaction benchmarks (e.g., G2 rankings)
- Define a support framework aligned to the needs of your eSignature initiative

AI cannot:

- Determine the right level of support needed for your specific project
- Validate how customer support will be delivered for specific project use cases
- Replace professionally delivered support from an eSignature vendor

AI can help evaluate support models for your project, but your vendor's commitment to delivering that support is what drives real outcomes.



What to look for in a trusted partner

A trusted partner delivers accessible, expert-led support at every stage, from migration or initial implementation through optimization and scale. They offer dedicated resources when your project requires a white glove approach, while providing global support beyond tickets. For example, look for a strong community and knowledge base, which can help your team resolve issues quickly, reduce risk, and fully realize the value of your eSignature solution.



AI prompt for customer support evaluation

I'm evaluating eSignature vendors [vendor 1, vendor 2, vendor 3] for a [industry] organization with [complexity/regulatory needs], supporting workflows such as [list key workflows].

Provide a concise executive summary covering:

- **Support coverage:** Compare support channels (email, phone, community, knowledge base), global availability, SLAs, and response times across vendors
- **Service differentiation:** Outline key differences in premium or dedicated support models, including when costs apply
- **Customer sentiment:** Summarize feedback from sources like G2 on responsiveness, expertise, and overall support quality
- **Strengths and gaps:** Spotlight any reoccurring themes where vendors excel or fall short in support delivery
- **Recommended model:** Please define your recommended support model to ensure fastest project delivery with the best outcomes
- **Key questions:** List 3–5 critical questions to validate support quality and long-term partnership fit

Technical landscape

How to evaluate the technical landscape for eSignatures

The technical landscape defines how easily eSignatures integrate into your existing systems, workflows, and user experiences. While many vendors claim integration capabilities, the real consideration is how quickly, flexibly, and cost-effectively those integrations can be deployed and maintained over time.

Development of these integrations can either accelerate your digital transformation or become a long-term operational cost and burden.

Why the technical landscape matters

eSignature solutions are rarely standalone. They are embedded within mission-critical workflows that span multiple systems and teams. In practice, eSignature platforms must operate seamlessly across CRM systems, business applications, transactional platforms, and document management tools. If integrations are not well defined, or are costly and difficult to maintain, organizations face increased costs, slower deployment timelines, and greater dependency on technical resources. A modern technical landscape reduces integration friction and accelerates time to value, while enabling organizations to scale digital agreements efficiently.





Technical landscape considerations to watch for

Why

Integration delivery models

Evaluate options for embedded integrations, API-driven workflows, or storage-based integrations depending on your technical requirements.

Integration flexibility

Determine whether the platform supports your preferred iPaaS or integration tools, avoiding vendor lock-in and enabling architectural flexibility.

Ease of integration

Assess how quickly integrations can be configured. Modern platforms enable workflow setup in just a few clicks, reducing reliance on engineering resources.

Pre-built integrations and connectors

Evaluate the availability of pre-built connectors to common business applications, which reduces the need for custom development and accelerates deployment.

Development costs and maintenance

Evaluate beyond initial setup, as API-driven transactions (e.g., envelopes) can create ongoing, usage-based costs that impact total integration spend.





The core technical landscape question

Beyond integration capabilities, it's important to ask: How easily can we design, manage, and scale integrated digital workflows across systems, teams, and use cases?

Integrations that inflate transaction costs or introduce hard-to-manage complexity can limit the scalability and long-term success of your eSignature program.



Where AI helps and where it doesn't

AI tools can be extremely useful to:

- Compare baseline integration capabilities across vendors
- Identify available connectors and supported applications
- Summarize technical documentation and API capabilities

AI cannot:

- Assess how easily integrations will work within your specific architecture
- Replace technical expertise needed for designing scalable integrations
- Validate the effort required for implementation and long-term maintenance

AI can help evaluate the technical landscape, but real-world integration complexity and how a vendor helps you to develop, migrate, and maintain integrations will accelerate your time to value.



What to look for in a trusted partner

A trusted partner helps simplify your eSignature technical landscape by offering flexible and scalable integrations that reduce complexity. Most importantly, they allow your teams to deliver seamless digital workflows faster, with less effort, lower cost, and a greater ability to scale.

AI prompt for technical landscape evaluation



I'm evaluating eSignature vendors [vendor 1, vendor 2, vendor 3] for a [industry] organization using [systems/architecture], with workflows including [key use cases].

Provide a concise executive summary covering:

- **Integration coverage:** Pre-built connectors and supported platforms (CRM, document systems, etc.)
- **API and flexibility:** Differences in API capabilities, extensibility, and ease of embedding into workflows
- **Implementation effort:** Estimated level of effort to integrate based on our use case(s), including where custom development may be required
- **Scalability and adaptability:** Ability to support long-term growth and evolving system architecture
- **Key risks:** Integration complexity, ongoing maintenance burden, and potential vendor lock-in
- **Key questions:** List 3–5 critical questions to validate integration fit and long-term flexibility





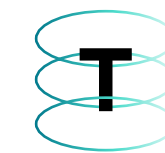
Conclusion

AI has made it easier than ever to evaluate eSignature solutions, and easier than ever to make incorrect assumptions. What looks like a complete evaluation can mask critical gaps in pricing, compliance, security, support, and scalability. While those gaps may not show up in an AI comparison table, they show up later when costs rise, integrations are strained, or support is unreliable.

The **TRUST Framework** exists as an important foundation for your eSignature evaluation and defines what AI alone cannot validate. It helps you move beyond features to ask questions that will determine long-term success.

Don't just accelerate your evaluation, strengthen it. Use the TRUST Framework to ask better questions, uncover what's missing, and hold vendors to a higher standard. A trusted eSignature solution goes beyond meeting your needs today, by helping your company scale digital workflows while supporting you every step of the way.

The OneSpan **TRUST Framework** provides a practical lens for eSignature vendor comparisons to assess what truly determines long-term program success, including:



Transparent pricing:

What will it really cost as you scale?



Regulatory compliance:

Will it stand up to scrutiny in your environment?



User trust and security:

Can every transaction be verified and defended?



Support:

Who is there when it matters most?



Technical landscape:

Will it integrate and scale without added complexity?

About OneSpan

OneSpan provides security, identity, electronic signature, and digital workflow solutions that protect and facilitate digital transactions and agreements. The Company delivers products and services that automate and secure customer-facing and revenue-generating business processes for use cases ranging from simple transactions to workflows that are complex or require higher levels of security. Trusted by global blue-chip enterprises, including more than 60% of the world's 100 largest banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

Learn more at
[OneSpan.com](https://www.onespan.com)

Contact us at
[OneSpan.com/contact-us](https://www.onespan.com/contact-us)



Copyright© 2026 OneSpan North America Inc., all rights reserved. OneSpan®, the "O" logo, Digipass®, Cronto® and "The Digital Agreements Security Company™" are registered or unregistered trademarks of OneSpan North America Inc. or its affiliates in the U.S. and other countries. Any other trademarks cited herein are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use. Last updated: April 2026

