TRUST e SOLUTIONS

Top 10 Things to Consider When Selecting a Cloud-based Software Provider

Cloud-based computing has quickly become the standard practice in legal technology. Working in the cloud offers convenience, efficiency and security—including anytime, anywhere access to case files and documentation; a secure place to safely collaborate with colleagues while uploading, downloading and sharing documents; robust data backup; and a plethora of other productivity-enhancing tools and benefits. In today's work-from-anywhere environment, it isn't just nice to have—it's a necessity.

So, how do you choose the right cloud-based software provider? Consider the following before making your move to the cloud or switching to a new provider from your current one.

1. Software Security

Security should be at the top of your list when considering a move to a cloud-based environment. You must feel confident that your data, documents and case files are protected in the cloud, especially in today's world where headlines warn of constant security breaches and server hacks. User-based security controlled by an Administrator is an absolute requirement for cloud-based systems. The workings of the software need to adhere to security permissions set by the Administrator.

In a 2022 Cloud Computing survey conducted by the American Bar Association, 36% of respondents indicated that cloud services provide the benefit of giving greater security than they provide on their own. Of those concerned about cloud security and confidentiality, 97% ranked the reputation of the vendor high in the decision-making process.

So, when you are reviewing your list of potential providers, be sure to ask these important security-based questions:

- Is your platform SOC-compliant?
- Does the application support commercially available data encryption standards?
- Does the application support two-factor user authentication as a double layer of security?

At Financial Software Solutions (FSS), all of our software platforms, including TrusteSolutions (TES), CORE and BlueStylus were built from the ground up in the cloud. We designed all of these safety protocols, and more, into our systems from the very beginning to ensure the utmost security for our clients and their data—because our reputation has depended on it from Day 1.

2. Service Level Agreement (SLA)

Your software provider will have a service level agreement that covers concerns such as uptime and support ticket handling. The SLA will be shared with you in the software license agreement or in a separate document. It is imperative that you carefully review this document to fully understand what the software vendor will be delivering to you on an ongoing basis.

3. Third-Party Audit

Most financial institutions require some level of third-party audit on at least an annual basis for those service providers that house financial data. Depending on the type of data that is being stored and the level of integration with financial data systems, this can be handled in various ways. Most common are SOC 1 Type 1 or Type 2 and SOC 2 audits. The report prepared by the outside audit firm can be made available to customers if license agreements contain strong confidentiality language.

4. Data Sharing & Data Privacy

You've seen the news stories and watched the documentaries about how social media giants use and abuse personal information. Your clients entrust you to keep their personally identifiable information (PII) safe and in turn, you trust your cloud-based provider to do the same. Even accidentally disclosing PII such as Social Security numbers and other protected information can have significant repercussions including financial liability and associated costs.

With large amounts of data being stored on the cloud in one place, you need to be aware of what your provider does with that data. Most software providers will include language in their license agreements that discuss data sharing policies, which can range from "no sharing" to "certain information." PII may not be shared. Some other data may be shared with third parties. You must review the license agreement and ask questions when necessary to be certain you understand a provider's data privacy and data sharing stance.

5. Disaster Recovery (DR)

Whether you house your software platform on a server in your office, or use a cloud-based provider, make sure a disaster recovery plan exists to ensure access to your data and systems during unexpected events. If you live in an area frequently impacted by Mother Nature, that's all the more reason to ensure you have a back-up plan ready to go so you never lose access to your data.

As you go through your cloud-based provider selection process, confirm the provider has a regularly tested DR plan. While the details of how DR is performed may be technical, and possibly proprietary, the most important questions to ask are:

1) When is the last time the DR was tested?

2) If there were negative results, were these addressed?

Learning important aspects of the provider's operation will give you peace of mind that you've made the best decision for your firm.

6. Service & Support

Even the best, most intuitive and user-friendly software will require some form of customer support from time to time. While chat and email are great tools for non-emergencies, the ability to get someone knowledgeable on the phone is essential. Confirm that a provider's customer support team is not only responsive, but experts when it comes to the software, so downtime is minimized and your productivity can soar.

As you review providers, inquire about their customer satisfaction scores. At FSS, we are pleased to report that more than 99% of TrusteSolutions customers were "very" or "extremely" satisfied with our customer support team in our 2023 annual customer satisfaction survey. The numbers speak for themselves. Make sure they do for the providers you're considering, as well.

7. Employee Training

When you evaluate and select a service provider that is concerned about data security, you can feel confident its employees will be trained to keep communications secure. This includes phone and written communications. Regular training of employees on current phishing trends, for example, will help keep the human side of data security safe. Additionally, regular training in confidentiality and accurately identifying a customer are also important.

8. Customer Training

As you look at cloud-based software providers, ensure they will provide your team with suitable customer training. It is imperative that you, as the customer, are aware of your responsibility in keeping data safe. Systems require regular password changes of certain complexity. Many cloud providers offer two-factor authentication for increased security. Ensuring customers, like you, are aware of the tools that are available to them is the responsibility of the cloud provider's training team. Choose a provider with proactive customer support and training teams that receive high marks from users.

9. Referrals & Testimonials

Referrals and customer testimonials can supply you with valuable insights about a cloud-based provider. Reach out to one or more attorneys you respect and trust to see who they use, and why. Ask them to give you a true account of their experiences with their providers and ask if they would recommend them. When TrusteSolutions' customers were asked if they would recommend TrusteSolutions to another trustee in the 2023 annual customer satisfaction survey, an overwhelming 100% replied "yes."

Visit the potential provider's website to view testimonials, case studies or reviews from customers. If you can't find any, this could be a red flag as to what kind of service you can expect to receive.

10. Vendor Longevity

In the 2022 Cloud Computing survey by the American Bar Association, current cloud users rated vendor longevity as a top concern. Research how long the cloud-based providers you are considering have been in business. Find out if their software platform originated on the web or not. If it did not, there is a possibility they are still in the process of moving to the cloud. Look for a tried and true provider with a proven platform so you can hit the ground running when you migrate to the cloud.

At TrusteSolutions, we are pleased to have customers that have been with us since we started our business in the cloud almost 25 years ago. We are also proud to have the highest customer retention rate in the industry. Our customers offer loyalty as well as feedback, helping us to continue innovating our products to make them more feature-rich so attorneys and businesses alike can experience more efficiency, more excellence, and more profit with better case management.

Clearly, choosing a cloud-based software provider (or switching to a new one) requires careful consideration of many important factors, 10 of which we have identified here. As you review cloud-based providers, set your standards high. With more and more people embracing hybrid and remote workplaces, choosing an efficient, reliable and secure cloud solution is key to increasing productivity and maintaining excellence.