alexi

Brief and Evaluation Checklist

Why Leading Law Firms Are Moving to Private Cloud Legal AI

In this brief, we'll examine the differences between various cloud options, explain why private clouds are ideal for law firms, and provide an evaluation checklist to help your firm select, implement, and optimize a private cloud solution.

Table of Contents

Why Leading Law Firms Are Moving to Private Cloud

Not long ago, law firms depended on paper-based records, physical storage like external hard drives, and local servers to manage their data. While these traditional methods were standard practice, they came with limitations: scalability was restricted, maintenance was cumbersome, and the risk of data loss was always looming. As client expectations for faster and more secure access to information grew, it became clear that these legacy systems could no longer keep up.

The shift toward cloud-based infrastructure provided law firms with the flexibility and resilience needed to meet modern demands. Among the available options, private cloud emerged as the ideal choice. Its dedicated infrastructure ensures sensitive client data is kept secure and fully compliant with stringent legal regulations.

In this brief, we'll explore the key differences between private, public, and hybrid clouds, outline why private cloud is best suited for law firms, and provide an evaluation checklist to guide your firm in selecting the right solution.

Private, Public, or Hybrid Cloud?

Choosing the right cloud infrastructure is crucial for law firms that handle sensitive data.

Below you'll find key differences involved when considering private, public, and hybrid cloud environments.

Category	Private Cloud	Public Cloud	Hybrid Cloud
Infrastructure Ownership	Dedicated, managed by the firm	Shared infrastructure managed by third-party (e.g., AWS, Azure)	Mix of on-premises, private, and public cloud environments
Data Control	Full control and customization	Limited control, standardized environments	Moderate control, flexibility to keep sensitive data private
Security & Compliance	High; easier to meet industry-specific compliance (e.g., GDPR, HIPAA)	Adequate but reliant on vendor security measures	Allows sensitive data to remain private while using public for less critical data
Cost Structure	High upfront cost, but predictable ongoing costs	Lower upfront cost, but potential for high costs based on usage	Flexible; costs vary based on resource allocation
Scalability	Scalable based on physical resource availability	Rapid; virtually unlimited scalability	Flexible; can scale public resources while keeping sensitive data secure
Maintenance and Management	Managed by the firm or private vendor	Managed entirely by the cloud provider	Split management; firm handles private, provider handles public
Integration Flexibility	High; full control over integration with existing systems	Moderate; dependent on API and service offerings	High; can integrate diverse systems
Accessibility	Internal or VPN access for high security	Global access from any internet connection	Configurable; private is restricted, public is accessible
Disaster Recovery	Firm-managed, customizable solutions	Managed by the provider; often included in service	Can be configured for optimal redundancy and backup

The Case for Private Cloud

While public and hybrid clouds may offer unique advantages, private cloud stands out as the ideal solution for law firms. Its dedicated infrastructure ensures sensitive client data is safeguarded, while providing the customization and reliability law firms need to operate with confidence

Compliance

A private cloud offers complete control over data location and jurisdiction, helping firms meet stringent data residency requirements, such as Canada's PIPEDA and the ABA's Model Rules for Professional Conduct in the United States. Unlike multi-tenant public clouds, private clouds provide firms with the ability to dictate encryption standards, access controls, and data retention policies – ensuring that sensitive client information is handled with the utmost care.

Security and Control

A private cloud offers an isolated, single-tenant environment dedicated exclusively to one firm. This isolation reduces exposure; sensitive data is not stored on shared servers, and the network is accessible only to the firm's authorized users.

Firms can implement custom security measures tailored to their specific needs, including:

- Dedicated firewalls that provide an added layer of protection against unauthorized access.
- Bespoke monitoring that allows for real-time threat detection and rapid incident response.
- Network segmentation to ensure that critical applications and confidential data are kept separate and secure from potential vulnerabilities.

In contrast, public clouds rely on shared infrastructure, increasing the risk of exposure during data transit or when access controls are misconfigured.

Cost-Efficiency

While private clouds may involve higher fixed costs compared to their public counterparts, they offer **predictability and long-term cost stability that is often easier to budget for.** Firms are not subject to fluctuating usage costs or unexpected data transfer fees, which are common challenges with public cloud environments.

Client Expectations and Trust

In an industry where trust is currency, a firm's choice to invest in a private cloud solution serves as a clear message to clients:

Your data is protected with the highest level of care and security.

Clients expect their legal partners to not only secure their data but also guarantee its privacy and availability at all times. Leveraging a private cloud signals to clients that the firm is dedicated to safeguarding their information with top-tier security and proactive measures against unauthorized access

Legal AI Vendor Checklist

Data Security

- ☐ Does the vendor use end-to-end encryption for data both in transit and at rest?
- ☐ Are multi-factor authentication (MFA) and role-based access controls (RBAC) available to secure sensitive information?
- ☐ How frequently are security audits and vulnerability assessments conducted?
- ☐ Are data backups encrypted and stored in secure locations?
- ☐ What threat detection and incident response protocols are in place?

Compliance

- ☐ Is the vendor fully compliant with jurisdiction-specific legal regulations? (e.g., PIPEDA, GDPR, HIPAA)
- ☐ Can they provide certification documentation for compliance standards?
- ☐ Does the vendor offer audit logs and reporting tools for easy compliance checks?
- ☐ Are data retention policies customizable to meet our firm's legal obligations?
- ☐ How do they handle data residency requirements for sensitive legal information?

Infrastructure Control and Customization

- ☐ Does the solution allow us to control where data is stored and how it is accessed?
- ☐ Are there options for scalable resource allocation as we grow?
- ☐ Can the infrastructure be custom-configured to meet specific security and compliance needs?

Integration and Interoperability

- ☐ Can the solution seamlessly integrate with our case management and billing systems?
- ☐ Does it support interoperability with existing IT infrastructure?
- ☐ Are APIs available for custom integrations?
- ☐ Does the vendor provide migration support for legacy applications and data?

Disaster Recovery and Uptime Guarantees

- ☐ What uptime guarantees does the vendor service-level agreement (SLA) provide?
- ☐ What is the vendor's disaster recovery plan, and how frequently is it tested?
- ☐ Are data backups automated, and how quickly can they be restored in the event of a failure?
- ☐ Are there real-time monitoring and alert systems for instant incident detection?

Support and Maintenance

- ☐ Is there 24/7 dedicated support for issue resolution?
- ☐ What is the average response time for critical issues?
- ☐ Are software updates and security patches included in the service agreement?

Final Thoughts

Adopting a private cloud signals a commitment to client trust and data integrity, demonstrating that the firm prioritizes both security and regulatory compliance. In an era where data breaches and cyber threats are constant concerns, moving to a private cloud is not just an upgrade – it's a strategic necessity to remain competitive, secure, and forward-thinking.

Ready to implement private cloud at your firm?

With Alexi Enterprise, you get AI designed specifically for the legal industry, housed in a private, secure environment that you fully control. Protect your data, meet compliance with confidence, and unlock the power of AI – on your terms.

Get in touch to see how Alexi Enterprise can secure your firm's data with private cloud technology.