LEGAL TECH

The Death of Public Cloud

alexi

Executive Summary

Public cloud provides legaltech vendors agility, affordability, and scale. But in the new AI era, those benefits come at a cost most law firms can no longer afford: control, security, and ownership. As AI becomes embedded in critical legal workflows, the case against public cloud deployments in law is no longer academic. It's existential.

Firms that continue to rely on public cloud platforms for AI tools and core legal applications are putting their reputations, client confidentiality, and competitive edge at risk. The next wave of transformation in legal tech is shifting from licensing AI to building on it and owning it.

This whitepaper lays out why firms must urgently reassess their infrastructure strategies and outlines the business, technical, and strategic case for moving to a private cloud architecture purpose-built for legal.

The Public Cloud Wasn't Built for Modern AI

The legal industry has unique needs when it comes to data sensitivity, confidentiality, and client expectations. Yet most business-critical AI-enabled software used by firms today is built on general-purpose, multi-tenant public cloud environments.

While modern cloud architecture includes significant innovations, it falls short for legal teams charged with safeguarding some of the most sensitive information in the professional world. Public cloud infrastructure doesn't allow firms to build onto it and truly own the resulting assets – only private, single-tenant clouds can provide the control, customization, and ownership that legal applications demand.

AI Changes Everything: New Threats, New Stakes

AI represents a new paradigm for legal work. And as law firms adopt AI to support research, analysis, and decision-making, the data these tools interact with becomes more valuable – and more vulnerable.

AI requires broad access to data to function effectively, but that same access introduces significant liability if not properly controlled. Public cloud AI products often co-mingle client work product, usage data, and even user prompts across customers, blurring boundaries that should remain distinct in legal contexts.

As well, when AI tools are built on public cloud, they often introduce additional exposure points from vendor dependencies to opaque data pipelines, making it difficult to ensure full visibility and control over where data resides and how it's used.

And as firms begin building AI-driven workflows tailored to their specific practice areas, the question of ownership becomes critical. If custom workflows are built and stored in large vendor, multi-tenant environments, then who really owns the IP of those workflows?

In a zero-trust environment where security must be assumed fragile by default, relying on infrastructure you don't own or fully understand means operating with a persistent risk to your most valuable data.

Critically, firms that adopt AI early within a secure, private infrastructure can create compounding advantage. As Alexi has noted, early adoption creates proprietary workflows, rich data feedback loops, and cultural fluency with AI tools. These advantages only deepen over time.

Clients Are Watching

The shift to private cloud is more than just an internal decision. Clients are increasingly asking tough questions about how law firms are protecting their data in the age of AI. Compliance with client demands, RFP standards, and industry best practices now requires more than vague assurances. It requires infrastructure designed for trust.

Most clients are demanding concrete evidence that law firms have secure infrastructure in place and are not relying on generative AI tools built on public cloud platforms. RFPs increasingly include detailed questions about AI governance, data segregation, and infrastructure control.

The message is clear: reputational risk has moved from theoretical to tangible, and for many firms, it's becoming a direct barrier to winning new business.

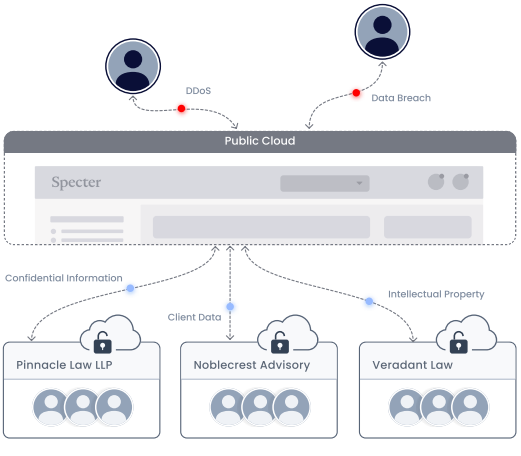
Private Cloud Is No Longer a Luxury

What was once considered a premium or niche solution is now table stakes for serious firms. Private cloud empowers law firms to retain full control over their data, customize deployments, and maintain a defensible security posture. And thanks to advances in deployment and vendor collaboration, it's never been easier to make the move.

Platforms like Alexi now offer private cloud deployment by default – fully isolated environments that meet strict compliance requirements. These are not hypothetical solutions; they're live today, running inside firms' own virtual networks.

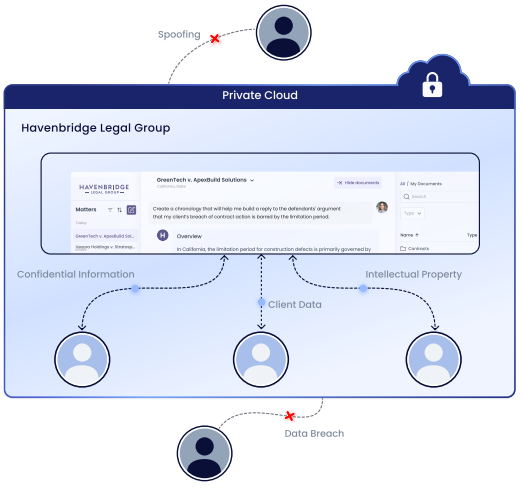
OTHER AI PLATFORMS

Traditional SaaS poses privacy risks with insecure data transfer over a single, shared deployment.



ALEXI PRIVATE DEPLOYMENT

Private firm deployment ensures **complete model and data isolation**.



It's Not Just About Security. It's About Strategic Ownership

Owning the infrastructure behind your AI stack means you get to shape how legal intelligence is built, protected, and delivered. This is a chance to differentiate – strengthening your position in the market while building infrastructure that aligns with your long-term strategy. It's about turning your AI capabilities into capital assets: building proprietary workflows, protecting firm-specific knowledge, and creating systems that reflect your unique approach to legal practice. In doing so, you position your firm as leaders in the future of legal AI.

Critically, the benefits of this ownership compound over time. Each AI-powered workflow you develop or model you fine-tune doesn't just solve an immediate problem – it lays the foundation for continuous improvement. The more your firm uses and refines its AI systems, the more effective and specialized they become.

Proprietary data accumulates, creating a defensible moat, while workflows evolve through trial and iteration. Your team gains fluency in working with AI, turning early adoption into lasting advantage

This is institutional transformation, and the sooner it begins, the wider the gap becomes – between firms that are compounding strategic advantage through ownership and learning, and those still catching up with tools they don't control.

What You Can Do Now

The shift away from public cloud requires decisive leadership across IT, risk, and practice management. Fortunately, firms can begin that journey today without disrupting core operations. Here are four concrete steps to get started.

1. **Audit Your Current Stack**
   Conduct a full review of all legal applications and AI tools used across the firm. Identify where each system is hosted and who has control over the underlying data.

2. **Initiate Internal Dialogue**
   Bring together IT, risk, and firm leadership to assess private deployment options. Align on security priorities, compliance obligations, and long-term infrastructure goals

3. **Engage Your Vendors**
   Ask each legal tech provider a simple but critical question: Can this run in my environment? Ensure your partners are equipped to support private cloud deployment.

4. **Elevate the Decision**
   Treat this as a strategic, board-level issue. The move to private infrastructure impacts more than IT – it's central to business continuity, client trust, and competitive positioning.

Conclusion

The Shift Is Inevitable. Be the First, Not the Last.

The firms who move first to secure, private, AI-ready cloud deployments will gain the trust of the market, unlock long-term strategic value, and avoid the compliance disasters looming for those clinging to legacy infrastructure.

The death of the public cloud in legal tech is not a prediction. It's a call to action.

*To learn how firms like yours are making the shift with our **IT Change Management Program**, request a strategic consultation with our team. Qualified firms can access **up to $100K in credits** to support a seamless move to private cloud.*

Check if you qualify