SOLUTION BRIEF

Airtight Data Security for Legal

Legal work runs on trust. Every M&A due diligence room, financial disclosure, multi-party agreement, and settlement negotiation depends on one unbreakable promise: what's shared stays privileged. Break that promise once, and the fallout isn't a compliance footnote — it's malpractice exposure, sanctions, escrow forfeiture, and a client relationship that doesn't survive discovery.

But privilege doesn't stay put. It moves through matter management systems, email threads, shared drives, e-discovery platforms, and now the AI tools associates use to draft memos, summarize depositions, or research precedent. Every one of those touchpoints is a potential waiver waiting to happen.

Layer on external counsel, opposing counsel, expert witnesses, and regulators, and privileged data is constantly moving outside your walls, often without anyone confirming it should be. Add a growing patchwork of data privacy regulation on top of your ethical obligations, and "we'll sort it out before the next audit" stops being a strategy.

Ask most legal teams where their privileged data actually sits, and you'll get a shrug. It's buried in matter folders, forwarded in email chains, pasted into AI prompts, and shared with outside counsel nobody's tracking anymore. Meanwhile, GC is expected to prove, on demand, that privilege was protected and that no client data leaked into a public AI tool. That's a hard case to argue with no evidence.

Key Benefits

- Enhanced visibility into privileged, confidential, and regulated legal data
- Matter-based access controls and ethical wall enforcement
- Guardrails for AI use across Copilot, ChatGPT, and other public AI tools
- Automated retention policies aligned to matter lifecycle
- Real-time remediation of risky sharing and over-permissioned access
- Audit-ready proof of regulatory and ethical compliance
- Purpose-built integration with iManage for matter-aware governance

The Verdict You Actually Want

What legal teams need is a way to find every privileged and confidential document without opening a research project. Something that understands a settlement agreement is different from a marketing deck, without a human tagging every file by hand.

Even better: a partner who helps you stand it up fast, tighten access before the next audit, and keep AI tools from becoming the newest form of privilege waiver.

Context, Not Just Keywords

Picture a solution that understands the difference between a signed NDA and a first-round term sheet — not because someone built a rule for it, but because it actually reads and understands the document. Concentric AI's Semantic Intelligence™ Engine scans structured and unstructured data across cloud and on-premises environments, in full, to identify privileged, confidential, and regulated content and IP with courtroom-grade accuracy.

No agents to deploy, no regex to maintain, no weeks of tuning. Point it at your matter files, DMS, email, and shared drives, and it gets to work identifying M&A documents, financial disclosures, litigation holds, and settlement terms. It then flags who has access, who shouldn't, and where it's been shared outside the firm.

When it's time to act, centralize sensitive matters, apply access restrictions and ethical walls directly in the platform, and set automated retention so closed-matter data doesn't linger past your document retention policy. And as attorneys turn to AI assistants like Copilot, Cowork or public tools like ChatGPT to draft and research, Concentric AI monitors what's shared — blocking or redacting privileged content before it ever leaves your environment.

Matter-aware Governance. Concentric AI's integration with iManage understands client and matter metadata natively, applies matching labels and access governance as data moves to SharePoint or OneDrive, and maps sensitive files to the right client and matter, even without an existing dictionary.

The Payoff: Privilege, Proven

- **What's privileged:** Full visibility into M&A, financial, litigation, and settlement data across every repository
- **Who can see it:** Access and ethical-wall enforcement down to the matter level
- **Where it's going:** Real-time monitoring and blocking of privileged data shared with AI tools
- **Proof it worked:** Audit-ready reporting for bar compliance, malpractice defense, and regulatory review

Securing the Data That Powers AI

Concentric AI enables organizations to accelerate safe AI adoption through its unified AI and data security governance platform. Powered by the Semantic Intelligence Engine's patented language models, the platform discovers, governs, and protects business-critical and compliance-sensitive data at rest, in motion, and used by AI through a consistent policy framework.

Schedule a Demo