

DÉTENTEIQ LLC

MEMORANDUM — Architecture, Security, and Data Handling

TO: Prospective firm clients and their IT / risk reviewers

FROM: Joseph V. Pumilia, DétenteIQ LLC

RE: How DétenteIQ is built, and how it protects your matter data

DATE: August 2026

Please accept this memorandum as a plain-English reference for the questions defense firms most often raise about how DétenteIQ is architected and how it handles firm data. It is written to be candid, including about the limits of each option, because a defense firm evaluating this tool is entitled to a straight answer rather than a marketing one. I am happy to walk your IT team through any of it in more detail and to complete a security questionnaire under NDA.

Executive Summary

DétenteIQ is hosted, multi-tenant software. Every firm's data is encrypted, isolated from every other firm on the platform, and accessible only to that firm's authorized users through role-based controls and single sign-on. We offer two encryption postures. The Standard option encrypts all data at rest and in transit and is protected by strict tenant isolation and audit logging; in that posture the application can decrypt your data server-side in order to display, search, and compute it for your own users. The Zero-Knowledge (end-to-end) option removes even that: your matter data is encrypted in your browser with a key we never hold, we store only ciphertext, and we cannot read your data or produce it in readable form in response to a subpoena served on us. The remainder of this memo explains both, compares them feature by feature, and answers the specific questions I expect to be asked.

Hosting and Technical Overview

DétenteIQ runs as a hosted application on Amazon Web Services, with a PostgreSQL database and a reverse proxy that terminates TLS using managed certificates. Each firm reaches the application over an encrypted connection, either at app.detenteiq.com or at the firm's own subdomain. The system is multi-tenant, which means firms share the same application but not the same data: every database query is scoped to the requesting firm's tenant identifier, and no interface returns another firm's records. Access to matter data is governed by user roles (administrator, attorney, and read-only) and, where a firm elects, by per-matter visibility so that an associate sees only the matters they are staffed on. Sign-in can be handled through the firm's own identity provider using single sign-on. Backups are taken on a daily schedule and stored encrypted.

The Two Encryption Options

The distinction between the two options comes down to a single question: who holds the key.

Under the Standard option, DétenteIQ holds a server-side key and encrypts all matter data at rest with AES-256. This protects your data against the theft of a database or a backup file, which would be unreadable ciphertext to anyone who obtained it. Because the application itself holds the key, it can decrypt your data on the server in order to render your matters, run searches, and perform the valuation and analytics your own users request. As a practical and honest matter, that means DétenteIQ has the technical ability to access matter content when the application runs. That ability is constrained by tenant isolation, by access controls, and by audit logging that records support access to your firm's own audit trail — but it is not eliminated. For most firms, Standard is more than sufficient, and it preserves full search and convenience.

Under the Zero-Knowledge (end-to-end) option, which a firm turns on at its election, matter data is encrypted and decrypted in your users' browsers using a key derived from your firm's own credentials. That key is never transmitted to us and never stored on our servers. What reaches our systems is ciphertext, together with a small set of searchable labels — the case name, number, and mediator — so the application can still list and open matters. We store only the ciphertext, we cannot decrypt it, and there is no server-side copy of your key to steal, to subpoena, or to misuse. Your whole team can still read the same matters, because the firm key is separately wrapped to each authorized user's login; but the key is never usable on our side. In this posture, a subpoena served on DétenteIQ for your matter data yields ciphertext, and we cannot produce it in readable form because we do not hold the means to read it.

Comparison Chart — Standard vs. Zero-Knowledge

Feature / Question	Standard (AES-256 at rest)	Zero-Knowledge (end-to-end)
Who holds the encryption key	DétenteIQ (server-side)	Your firm only — derived in-browser, never sent to us
Where data is encrypted / decrypted	On the server	In your users' browsers
Encrypted in transit (TLS)	Yes	Yes
Encrypted at rest	Yes (AES-256)	Yes (client-side ciphertext)
Can DétenteIQ technically read matter content	Yes — to display, search, and compute for your users (constrained by access controls and audit)	No — we hold only ciphertext
What a subpoena served on DétenteIQ yields	Data we would have to decrypt and respond to	Ciphertext we cannot produce in readable form
Protection against a stolen database or backup	Yes	Yes

Protection against a compromised operator or insider	Partial — access controls plus audit logging	Yes — cryptographic; there is no key on our side
Case name / number / mediator	Fully searchable	Kept as cleartext labels; all substantive content encrypted
Valuations, offers, demands, settlements, strategy, notes	Encrypted at rest; readable by the app	Encrypted end-to-end; unreadable to us
AI Assistant data path	Runs browser-direct to your chosen provider or on-device; may optionally route through our proxy	Runs browser-direct to your provider by default; matter content does not transit our servers
Cross-firm isolation	Yes	Yes
Single sign-on, roles, per-matter visibility	Yes	Yes
Operator password reset	Standard reset available	Cannot reset to gain access; key recovery is handled by your own firm administrator
Firm-wide, de-identified benchmarking	Available, opt-in	Available, opt-in; de-identified before anything leaves your firm
Recovery if a user forgets a password	Standard reset	Re-provisioned by your firm's administrator, who re-wraps the key; a fully lost firm key is unrecoverable by design
Best fit	Firms wanting strong protection with full search and convenience	Firms that require the vendor to be unable to read their data at all

Anticipated Questions and Answers

Where is our data hosted, and who can reach the servers? The application and database run on Amazon Web Services. Server access is limited to DétenteIQ operations, and any support access to a firm's data is recorded to that firm's audit trail. Under the Zero-Knowledge option there is nothing readable to reach in the first place.

Is our data encrypted? Yes, in both options and in both states. All data is encrypted in transit with TLS and at rest with AES-256. The difference between the options is who holds the key, as described above.

Can DétenteIQ, or another firm on the platform, see our valuations and settlements? No other firm can, in either option — tenant isolation ensures every firm is walled off from every other firm on the platform at the data layer, not merely in the interface. As for DétenteIQ itself: under Standard, the application can technically decrypt your data to serve your users, constrained by controls and audit; under Zero-Knowledge, we cannot read it at all.

What happens if you receive a subpoena for our matter data? Under Standard, we would be able to access the data and would respond to lawful process as required, and we would notify you

where permitted. Under Zero-Knowledge, a subpoena served on us yields ciphertext; we cannot produce your matter content in readable form because we do not hold the key. In either case, the confidential mediation and settlement material is best protected by process served on your firm, not on your vendor.

How does zero-knowledge actually work, in plain terms? A key is derived in your browser from your firm's credentials and never leaves your device. Data is encrypted before it is sent to us, stored by us only as ciphertext, and decrypted again only in the browser of an authorized user at your firm. We are never in the loop for the readable version.

What does the AI Assistant send, and to whom? You bring your own model provider or run on-device. The Assistant is designed to run browser-direct to that provider, so matter content need not pass through DétenteIQ's servers, and party names can be redacted on your device before a prompt is sent. Under the Zero-Knowledge option this is the default. The Assistant is also grounded — it draws only on the matter's own figures and flags any number it cannot support, so it does not introduce invented figures into a settlement discussion.

How are firms kept separate? Every query is scoped to your tenant. No screen, report, or export returns another firm's records, and under Zero-Knowledge the separation is cryptographic as well as logical.

Who at our firm can see what? Access is governed by roles — administrator, attorney, and read-only — and, if you choose, by per-matter visibility so associates see only the matters they are staffed on. Sign-in can run through your identity provider by single sign-on.

What happens when an attorney leaves? An administrator removes the user's access. Under Zero-Knowledge, that user's wrapped copy of the firm key is revoked with the account; the underlying data remains readable to your remaining authorized users and unreadable to us.

Do you have SOC 2 or a penetration test? Not yet, and I will not represent otherwise. An independent penetration test and a SOC 2 examination are on our roadmap, and we will state each publicly, with dates, as it is completed. What is in place today is set out above: AES-256 at rest, TLS in transit, the optional zero-knowledge encryption, tenant isolation, audited access, single sign-on, and browser-direct or on-device AI.

Do we own our data, and can we leave with it? Yes. Your matters are yours. We will export your firm's data on request, and deletion removes it from active systems and rolls out of backups on the normal retention cycle. Your data is never pooled with other firms; any benchmarking is opt-in and de-identified before anything leaves your firm.

What if DétenteIQ goes out of business? Your data is exportable at any time, so you are never locked in, and we are glad to address continuity terms — including data escrow or an export commitment — in the agreement.

Does using the software affect the confidentiality or privilege of our mediation communications? Mediation and settlement communications are confidential, protected by rule or statute in nearly every state, and that protection was a design input here rather than an afterthought. The tool is built so it does not widen the circle: your valuations, offers, demands, and strategy stay encrypted and isolated to your firm, and under Zero-Knowledge they are unreadable to us and do not transit our servers. DétenteIQ is built to support your confidentiality obligations; how privilege and the confidentiality rules apply to a given matter, of course, remains your firm's call.

What are the honest tradeoffs of Zero-Knowledge? Three. First, the searchable labels — case name, number, and mediator — remain cleartext so the application can find and open matters; if even a caption is too sensitive, name the matter by an internal code. Second, recovery depends on your own key custody: because we hold no key, a firm key that is entirely lost cannot be recovered, which is the point, so administrators manage recovery through the firm. Third, cross-firm benchmarking on a zero-knowledge firm works only on the de-identified data you opt to contribute. For most firms these are acceptable in exchange for a vendor that cannot read the file.

In sum, DétenteIQ gives a defense firm a hosted system of record that is encrypted, isolated, and access-controlled by default, with an end-to-end option for firms that require the vendor to be cryptographically unable to read their data. I am happy to take your IT and risk teams through any part of this in detail.

Sincerely,

Joseph V. Pumilia

DétenteIQ LLC

hello@detenteiq.com · (941) 800-1923