



QAXA BUYER BRIEF

Beyond the Data Room

VDRs protect formal disclosure. Qaxa protects the working layer around it — the conversations, drafts, tasks, notes, and decisions that move sensitive deals forward.

For lawyers, M&A counsel, deal advisors, corporate development teams, and professionals managing confidential external work.

Core argument

Virtual data rooms protect the formal document repository. Qaxa protects the live working layer around it - the messages, drafts, tasks, notes, questions, and decisions that often fall back into email, chat, cloud links, and spreadsheets.

Executive summary

Virtual data rooms have become standard infrastructure for serious transactions. They are good at what they were built to do: controlled disclosure, document permissioning, indexing, Q&A workflows, watermarking, and audit trails. For formal diligence, they remain essential.

The problem is not the VDR. The problem is the work that happens outside it.

In live deals, sensitive context rarely stays inside the formal repository. Questions move to email. Drafts and redlines move through cloud links. Negotiation context moves to messaging apps. Closing lists move to spreadsheets. Decisions are made in one place and executed in another.

The result is a fragmented working record, weaker access control, and avoidable operational risk.

Qaxa is an encrypted deal room for this working layer. It brings discussion, working files, notes, tasks, and decisions into one controlled room, protected with client-side end-to-end encryption.

Qaxa can sit beside an established VDR on larger transactions, or serve as a lighter encrypted room for matters where a full VDR is unnecessary.

Positioning in one sentence

Qaxa does not replace the formal VDR. It secures the confidential workstream that too often happens outside it.

1. What VDRs already do well

Virtual data rooms are built for controlled disclosure. In M&A, financing, litigation support, real estate transactions, and other high-stakes matters, they provide a disciplined environment for sharing formal documents with defined parties.

A well-run VDR helps deal teams manage:

- Structured document repositories and indexing.
- Granular access permissions for folders, documents, and user groups.

- Formal Q&A workflows with assigned owners and tracked responses.
- Watermarking, secure viewing, and download controls.
- Audit trails and reporting on document activity.
- Administrative controls required by sophisticated deal processes.

That infrastructure is valuable. This brief is not an argument against VDRs.

It is an argument for a clearer boundary: the VDR protects the formal document record. The working layer around the deal still needs a secure environment of its own.

2. The missing layer: live deal work

A transaction is not only a folder structure. It is a stream of questions, comments, revisions, assumptions, assignments, follow-ups, and decisions. Much of that work is informal, fast-moving, and highly sensitive.

In practice, the working layer often includes:

- Questions between counsel, advisors, clients, and counterparties before they become formal VDR Q&A.
- Drafts, redlines, models, exhibits, side letters, and working files that are not yet final disclosure documents.
- Internal strategy discussions inside the firm or advisor team.
- Client instructions and deal-positioning conversations.
- Task lists, open items, deadlines, and follow-ups across workstreams.
- Decision notes explaining why a term, exception, or risk was accepted.

This is where many deals become messy. The official documents may sit inside the VDR, while the deal itself is run across inboxes, chat messages, shared drives, spreadsheets, and side channels.

The practical question

The issue is not whether the VDR is secure. The issue is whether the rest of the deal is handled with the same level of control.

3. Where sensitive work goes today

When there is no dedicated working room, teams default to the tools already on their desks. Each tool is useful. None is designed to be the controlled workspace for a sensitive deal.

Email

Email is universal, but it is a poor system of record for live deal work. Attachments are forwarded, copied, downloaded, and stored in multiple inboxes. Threads split. People answer the wrong chain. Important context gets buried. Once a sensitive draft leaves the sender, practical control is limited.

Messaging apps and team chat

Messaging tools are fast, which is why people use them. But speed creates its own risk. Consumer messaging apps may protect message transport, yet they do not provide a complete deal workspace with controlled rooms, files, tasks, notes, participant governance, and post-close administration. Enterprise chat systems may also be retained, exported, or placed under legal hold depending on the organization and plan.

Cloud storage and shared documents

Cloud drives make collaboration easy, but they can also create link sprawl. Permissions can be too broad, inherited, forgotten, or forwarded. Version history may preserve material that was never intended to become part of the final record. A shared folder may hold the files, but it does not hold the discussion and decisions around them.

Spreadsheets and ad-hoc trackers

Spreadsheets often become the unofficial control tower for a deal: open items, owners, dates, missing documents, and closing deliverables. They are flexible, but they separate the checklist from the discussion, files, and decisions needed to complete the work.

The real risk

General-purpose tools do not automatically destroy confidentiality. But they can make confidentiality, access control, retention, and later reconstruction harder to manage — and harder to prove.

4. What an encrypted deal room should provide

A secure working room for sensitive deals should not be another file-sharing portal. It should reduce the number of places where sensitive context escapes, while giving teams one controlled place to work.

At minimum, it should provide:

1. One contained room per matter, deal, client, or workstream.
2. Client-side end-to-end encryption for room content before it reaches the server.
3. Controlled membership, with access granted only to invited participants.
4. The full working context: chat, files, notes, comments, tasks, and decisions.
5. Simple browser-based guest access, so clients and counterparties can join without buying seats or installing software.
6. Minimal data collection, with no advertising model and no AI training on room content.
7. Clear limits, so buyers know what the system protects against and what remains their responsibility.

5. How Qaxa works

Qaxa organizes sensitive external work into encrypted rooms. Each room has its own members, files, conversations, notes, tasks, and activity context. Access to one room does not create access to another.

Qaxa component	Purpose in a deal room
Chat	A shared room conversation for questions, updates, decisions, and day-to-day coordination.
Vault	Encrypted files and notes kept in the same place as the discussion around them.
Tasks	Open items, owners, deadlines, follow-ups, and workstream coordination.
Comments	Context attached to the relevant file, note, or task instead of buried in an inbox.
Guests	External participants can join the specific room they are invited to, without paid guest licenses.

Room content is protected with OpenPGP-based client-side encryption. In practical terms, content is encrypted before it leaves the user’s device. Qaxa stores ciphertext — encrypted data that is not readable without the relevant keys. The server can store and synchronize room content without needing plaintext access.

This matters because the privacy guarantee is not only a policy promise. It is part of the product architecture. If Qaxa cannot read room content, Qaxa cannot use it for advertising, train AI on it, or produce readable room content from its servers.

Qaxa still needs some operational data to run the service, such as account email addresses, billing records, plan status, timestamps, and support communications. That should be stated plainly. Zero-knowledge protection applies to encrypted room content, not to every operational fact required to operate a SaaS business.

6. Threat model: what Qaxa protects – and what it does not

A credible security claim should define its limits. Qaxa is designed to reduce exposure in the places where deal teams usually lose control: scattered working files, provider-accessible content, fragmented communication, and access that remains open longer than it should.

Risk	How Qaxa helps	Important limit
Provider access to room content	Room content is encrypted client-side; Qaxa stores ciphertext rather than readable content.	Operational metadata still exists. Qaxa also cannot protect content copied out of the room.
Server breach	A breach of stored room data should expose encrypted data rather than plaintext deal content.	Endpoint compromise, stolen passphrases, or compromised user devices are outside server-side protection.
Scattered deal context	Chat, files, notes, tasks, and comments live in one room instead of across email, cloud links, and spreadsheets.	Users can still choose to move material into external tools.
Uncontrolled guest access	Membership is room-based. Guests only enter rooms they were invited to.	A trusted participant can still screenshot, copy, summarize, or disclose what they can legitimately see.
Post-close access	Room owners can remove access when the matter ends.	Previously downloaded or copied material cannot be technically recalled from someone else's device.
Discovery and legal process served on the provider	If room content is encrypted and Qaxa does not hold decryption keys, server-side production should not reveal readable room content.	This is not legal advice. Obligations vary by jurisdiction, account data, and facts.

Plain-English security claim

Qaxa is designed so the room owner controls who enters the room, while Qaxa stores only encrypted room content it cannot read.

7. What Qaxa is not

Qaxa is strongest when the buyer understands its role clearly.

- Qaxa is not a traditional VDR replacement for large, formal diligence processes that require advanced document indexing, formal Q&A, watermarking, secure viewing rules, and detailed VDR audit reporting.
- Qaxa is not a legal privilege guarantee. It can support better confidentiality discipline, but privilege depends on law, facts, process, and counsel guidance.
- Qaxa is not a guarantee against human disclosure. Any invited participant who can read content can potentially copy, screenshot, summarize, or disclose it.
- Qaxa is not a substitute for endpoint security, passphrase hygiene, internal access policies, or legal retention policies.
- Qaxa is not designed to create a heavy enterprise permission maze. Its value is a simple encrypted room that external parties can actually use.

8. Coverage comparison

The point is not that one system should do everything. The point is to put each kind of deal work in the environment best suited to protect it.

Deal work	Traditional VDR	Email / cloud / chat	Qaxa
Formal document repository	Best fit	Poor fit	Useful for working files
Formal diligence Q&A	Best fit	Fragmented	Useful for informal questions
Watermarking / secure viewer controls	Best fit	Limited	Not the primary purpose
Detailed document audit reporting	Best fit	Fragmented	Room activity context
Live deal communication	Often secondary	Common but scattered	Best fit
Drafts, redlines, working files	Sometimes too formal	Common but exposed	Best fit
Task and deadline management	Limited or separate	Usually spreadsheet-based	Best fit

Deal work	Traditional VDR	Email / cloud / chat	Qaxa
Decision notes beside work	Limited	Scattered	Best fit
Provider unable to read room content	Depends on vendor architecture	Usually no for business cloud tools	Designed for this
Low-friction external guests	Varies	Easy but uncontrolled	Designed for browser-based guest access

9. Where Qaxa fits in the deal stack

Scenario	Best use of Qaxa
Large transaction with an established VDR	Use the VDR for formal disclosure and Qaxa for encrypted communication, working files, tasks, client instructions, and decision notes.
Mid-market transaction without heavy diligence infrastructure	Use Qaxa as a lightweight encrypted deal room for the full working process.
Legal matter involving external clients or advisors	Create one room for the matter so client communication, files, and open items stay together.
Sensitive negotiation or pre-deal exploration	Use Qaxa when the matter needs confidentiality, controlled access, and simple external participation — without the weight of a full VDR.

The adoption principle is simple: if the other side will not use the tool, the tool cannot protect the work.

That is why Qaxa is built around browser-based guest access and a host-paid model. The firm controls the room. External participants join without buying licenses.

10. Adoption: the external-party problem

A security tool only protects the work people actually do inside it.

That is why adoption matters in deal work. Clients, counterparties, advisors, and outside counsel may resist any system that requires a paid account, installation, procurement step, or IT approval. If the room is hard to enter, the deal will move back to email.

Qaxa is designed around that reality. The firm or deal owner creates the room, controls access, and pays for the workspace. External participants join invited rooms in the browser, without buying licenses or installing software.

The result is a controlled room that is easier to adopt: simple enough for the other side to use, but private enough for sensitive work.

11. Conclusion

The modern deal stack has a gap. The VDR protects the formal document set. But the working layer of the deal — the questions, drafts, decisions, tasks, and sensitive context — often escapes into tools built for convenience rather than controlled confidential work.

Qaxa closes that gap with one encrypted room per deal, matter, client, or workstream. It is simple enough for external parties to use, and private enough that Qaxa cannot read the room.

For teams that already use a VDR, Qaxa adds the missing encrypted working layer. For teams that do not need a full VDR, Qaxa provides a lighter way to run sensitive external work without falling back to scattered tools.

Final takeaway

Use the VDR for formal disclosure. Use Qaxa for the encrypted work around it. And when a formal VDR is more than the matter requires, use Qaxa as the controlled room for the full working process.

Selected source notes

The following references were consulted to keep the positioning fair and avoid overstating claims about VDRs, enterprise discovery, cloud productivity suites, consumer messaging, legal confidentiality obligations, and OpenPGP-based encryption.

- **Datasite virtual data room materials:** examples of VDR positioning around permissions, audit trails, Q&A, and deal activity <https://www.datasite.com/en/resources/faqs>
- **Intralinks virtual data room overview:** examples of VDR features including granular permissions, watermarking, audit trails, secure viewing, and Q&A workflows <https://www.intralinks.com/virtual-data-room>
- **Slack legal holds documentation:** official explanation of legal holds, retained message/file data, export, and Discovery API access <https://slack.com/help/articles/4401830811795-Create-and-manage-legal-holds>

- **Microsoft Purview eDiscovery documentation:** official explanation of identifying, preserving, reviewing, and exporting content from Microsoft 365 services including Exchange Online, Teams, OneDrive, and SharePoint <https://learn.microsoft.com/en-us/purview/edisc>
- **Google Vault documentation:** official explanation of retaining, holding, searching, and exporting Google Workspace data <https://support.google.com/vault/answer/2462365>
- **Google Workspace Client-side Encryption documentation:** official explanation of encrypting Workspace data with customer-controlled keys so Google servers cannot decrypt protected content <https://knowledge.workspace.google.com/admin/security/about-client-side-encryption>
- **Apple iCloud data security overview:** official explanation of which Apple data categories are end-to-end encrypted and how Advanced Data Protection changes iCloud protection <https://support.apple.com/en-us/102651>
- **WhatsApp encrypted backup documentation:** official explanation of end-to-end encrypted backups and user-controlled backup protection <https://faq.whatsapp.com/490592613091019>
- **Signal government requests page:** official examples showing the limited categories of data Signal can provide when legally compelled <https://signal.org/bigbrother/>
- **IETF RFC 9580:** current OpenPGP standard describing encryption, signatures, compression, and key management <https://datatracker.ietf.org/doc/rfc9580/>
- **OpenPGP.js project:** JavaScript implementation of the OpenPGP protocol used by browser-based applications <https://openpgpjs.org/>

Legal and security note

This document is provided for informational and commercial evaluation purposes only. It is not legal advice, security advice, or a compliance opinion.

Security architecture, legal privilege, discovery obligations, retention duties, regulatory requirements, and compliance obligations should be reviewed with qualified legal, security, and technical advisors in the relevant jurisdiction.

© Qaxa Labs s.r.o. All rights reserved.

www.qaxa.com