RingStor

RINGSTOR

VaultIQ

Private AI Document Intelligence

How organizations can deploy a secure, on-premises AI knowledge platform that answers questions from their own documents · without data ever leaving their control.

White Paper · 2025

RingStor, Inc. · Princeton, NJ · www.ringstor.com

Executive Summary

Organizations today are drowning in unstructured documents · contracts, policies, research reports, technical manuals, financial filings · spread across local drives, NAS devices, and cloud storage. Finding information within these silos is slow, error-prone, and increasingly a competitive liability.

Existing AI-powered search solutions require uploading sensitive documents to third-party cloud services, creating unacceptable privacy and compliance risk for industries such as finance, healthcare, legal, and defense.

VaultIQ, by RingStor, solves this by delivering a fully private, on-premises AI document intelligence platform. Built on a proven Retrieval-Augmented Generation (RAG) architecture, VaultIQ ingests documents from any source · local folders, NAS, OneDrive, Google Drive, SharePoint · indexes them into a secure private knowledge base, and lets authorized users query them in natural language. AI reasoning happens entirely within the customer's own infrastructure. No document content ever leaves.

> ***"Ask any question. Get precise answers. Your documents never leave your network."***

The Problem: Knowledge Locked in Documents

Modern organizations generate and accumulate enormous volumes of documents. IDC research estimates that unstructured data represents 80·90% of all enterprise data, yet the vast majority remains unsearchable beyond simple keyword matching.

Pain Points

· Employees spend 1.8·2.5 hours per day searching for information (McKinsey Global Institute)

· Critical knowledge is siloed across departments, systems, and geographies

· Keyword search returns documents, not answers · users still read entire files

· Regulated industries cannot use public AI tools that require cloud upload

· Onboarding new staff is slow because institutional knowledge is hard to surface

Why Public AI Tools Fall Short

Consumer-facing large language models such as ChatGPT and Copilot offer compelling general AI capabilities, but require data to be transmitted to external servers. For organizations handling confidential

contracts, patient records, financial models, or proprietary research, this is a hard stop. Beyond compliance, these tools lack the ability to reason over a specific organization's own document corpus with precision and attribution.

The Solution: VaultIQ Private AI Document Intelligence

VaultIQ is a two-tier, on-premises SaaS platform that brings AI document intelligence inside the customer's own network perimeter. It combines a lightweight sync agent installed on endpoints and servers with a centrally managed cloud controller · deployed on the customer's private cloud or on-premises servers · that handles indexing, AI reasoning, and access control.

Core Value Proposition

Private by Design	Source-Agnostic	LLM-Flexible	Enterprise-Ready
All AI processing on customer infrastructure. Zero data egress.	Sync from local files, NAS, OneDrive, SharePoint, Google Drive.	Use local Ollama models or connect OpenAI, Anthropic, Mistral APIs.	Role-based access, audit trails, and multi-tenant organization support.

Platform Architecture

VaultIQ is built around a clean two-tier architecture that separates document collection from AI processing · keeping data secure while enabling centralized management and querying.

Tier 1: VaultIQ Sync Agent

A lightweight agent installed on Windows workstations, file servers, and configured source locations, detects new or changed files, and securely the VaultIQ Controller. The agent supports:

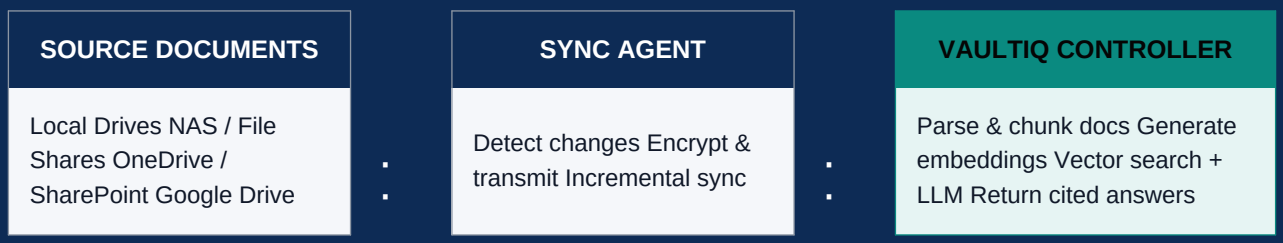
- Local folders and Windows file shares
- NAS devices (SMB/NFS)
- Microsoft OneDrive and SharePoint Online
- Google Drive
- Incremental sync · only changed files are transmitted
- TLS-encrypted transport to the VaultIQ Controller

Tier 2: VaultIQ Controller (Cloud or On-Premises)

The Controller is the intelligence hub of the platform. It receives documents from agents, processes and chunks them, generates vector embeddings, and stores the indexed knowledge base. When a user submits a query, the Controller retrieves the most semantically relevant document segments and passes them · along with the query · to the configured LLM to generate a precise, cited answer.

- · Powered by RAGFlow · an open-source, production-grade RAG engine
- · Embedding models run locally (no external calls required)
- · Answers include citations showing exactly which document and page answered the query
- · LLM selection: Ollama (fully local), or external API (OpenAI, Anthropic, Mistral, etc.)
- · REST API for integration with third-party applications

Architecture Flow



Key Features

I Natural Language Q&A;

Users ask questions in plain English (or any language) and receive direct, accurate answers with source citations · no more reading through stacks of documents to find a single fact.

I Semantic Search

VaultIQ understands meaning, not just keywords. Queries return the most relevant content even when exact terms differ, dramatically improving recall over traditional search.

I Full Citation and Attribution

Every answer references the specific document, section, and page that supports it. Users can verify answers and navigate directly to the source.

Private Vault Organization

Documents are organized into Vaults · logical containers corresponding to projects, departments, or document types. Access to each Vault is controlled through role-based permissions.

Multi-Source Ingestion

A single VaultIQ deployment can ingest from dozens of simultaneous sources: local file paths, NAS shares, OneDrive accounts, SharePoint sites, and Google Drive folders · via a single management interface.

LLM Flexibility

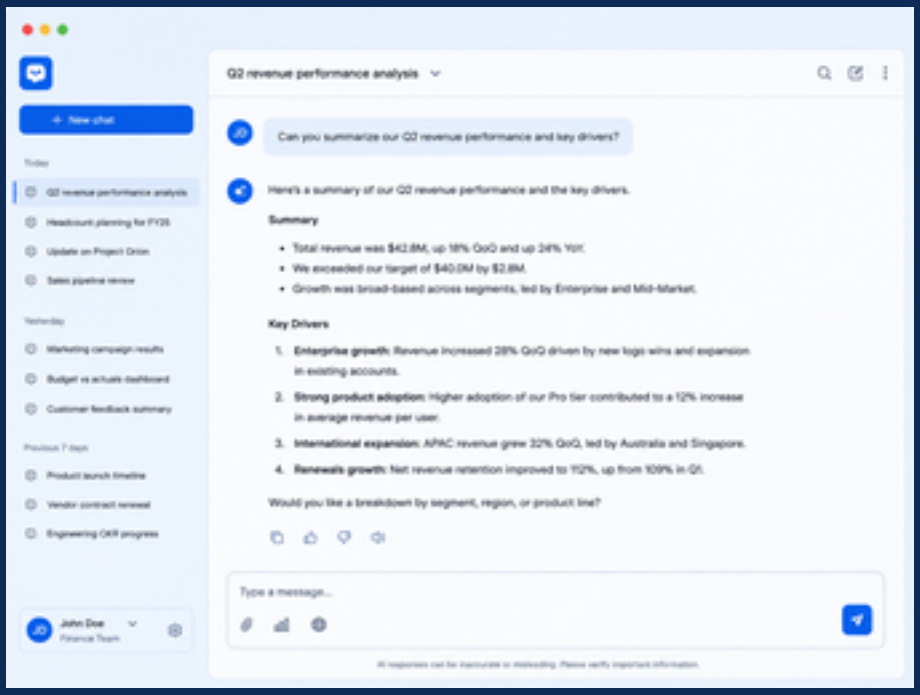
VaultIQ is LLM-agnostic. Organizations can run fully air-gapped with open-source models via Ollama (Llama 3, Mistral, Qwen, Gemma) or connect to external APIs for higher-capability models, depending on security and budget requirements.

Role-Based Access Control

Four granular roles · Admin, Vault Admin, Vault Contributor, and Vault Viewer · allow precise control over who can create Vaults, add data sources, and query results.

Audit and Compliance Logging

All user queries, document ingestions, and configuration changes are logged with timestamps, supporting compliance requirements and organizational accountability.



VaultIQ Chat Interface · instant cited answers from your own documents

Target Use Cases

Industry	Document Types	Key Benefit
Financial Services	Research reports, regulatory filings, client contracts	Instantly answer compliance questions without sharing data externally
Legal	Case files, contracts, precedents, discovery documents	Surface relevant precedents and clauses across thousands of documents
Healthcare	Clinical guidelines, formularies, SOPs, research papers	Clinicians get instant policy answers with citations · on-premise, HIPAA-aligned
Manufacturing & Engineering	Technical manuals, CAD specs, quality standards, BOMs	Field staff query manuals in natural language without IT support
Government & Defense	Classified and sensitive policy documents, procurement files	Fully air-gapped deployment with no external connectivity required
Professional Services	Engagement files, methodologies, proposals, client deliverables	Reuse institutional knowledge across engagements and accelerate onboarding

Competitive Differentiation

The enterprise AI search market includes well-funded players such as Glean, Microsoft Copilot, Guru, Onyx, and GoSearch. VaultIQ occupies a distinct position in this landscape:

Capability	VaultIQ	Glean / Copilot	Onyx / GoSearch
Fully on-premises / air-gapped	**Yes**	**No**	Partial
No per-seat cloud SaaS fees	**Yes**	**No**	**No**
SMB-accessible pricing	**Yes**	**No**	Partial
Local file / NAS ingestion	**Yes**	**No**	**No**

Bring your own LLM (local or API)	**Yes**	**No**	**Yes**
Source citations in every answer	**Yes**	Partial	**Yes**

Security and Data Privacy

VaultIQ was designed from the ground up with a privacy-first architecture. Unlike SaaS AI platforms that process customer data on shared infrastructure, VaultIQ ensures that all sensitive content remains within the customer's controlled environment.

Security Architecture Highlights

- All document content processed exclusively on customer-controlled servers
- TLS 1.2/1.3 encryption for all agent-to-controller communication
- No document content stored on RingStor infrastructure
- Optional fully air-gapped deployment with local LLM (no internet required)
- Role-based access control with per-Vault permission scoping
- Audit logging of all queries, ingestion events, and administrative actions
- Supports deployment on customer's private cloud (Azure, AWS, GCP) or on-premises bare metal

Compliance Alignment

VaultIQ's private-by-design model directly supports compliance with major regulatory frameworks. Because data does not leave the customer's perimeter, organizations avoid the data processing agreements, DPA reviews, and vendor risk assessments that SaaS AI tools require.

Framework	VaultIQ Alignment
HIPAA	Documents processed on-site; no PHI transmitted externally
SOC 2 / ISO 27001	Audit logs and access controls support trust service criteria
GDPR / CCPA	No personal data leaves organizational control
CMMC / FedRAMP	Air-gapped deployment option eliminates external data flows
SEC / FINRA	Confidential research and client data stays on-premises

Deployment and Pricing

Deployment Options

VaultIQ is designed to deploy quickly on existing infrastructure. The Controller runs in Docker containers, enabling deployment on any Linux server, VM, or managed container service. Minimum recommended specifications for production use:

- Controller server: 8-core CPU, 32 GB RAM, 500 GB SSD storage
- GPU (optional but recommended): NVIDIA with 8+ GB VRAM for faster local LLM inference
- Sync Agent: Windows 10/11 or Windows Server 2016+, 4 GB RAM, 10 GB disk
- Network: 100 Mbps minimum between agent endpoints and the controller

Subscription Tiers

Tier	Target	Vaults	Agents	Users	Price (Annual)
Starter	Small teams	Up to 3	Up to 3	Up to 10	Contact us
Professional	Growing SMBs	Up to 10	Up to 10	Up to 50	Contact us
Enterprise	Large organizations	Unlimited	Unlimited	Unlimited	Custom

All tiers include software updates, security patches, and email support. Priority support SLAs and on-site deployment assistance are available as add-ons. VaultIQ is sold as an annual subscription. Pricing is per-deployment, not per-seat, making it significantly more cost-effective than per-user SaaS alternatives at scale.

Implementation and Onboarding

VaultIQ is designed for straightforward deployment by IT teams without specialized AI expertise. The typical implementation timeline:

Phase	Activities	Duration
1. Controller Setup	Deploy Docker containers on target server; configure network, TLS, and admin account	1–2 days

2. Agent Rollout	Install Sync Agents on endpoint machines or servers; configure source paths	1·3 days
3. Vault Configuration	Define Vaults, assign permissions, configure LLM connection	1 day
4. Initial Indexing	First-time ingestion and embedding generation; time varies by document volume	Hours·days
5. User Training	Brief end-user orientation on the chat interface and Vault structure	Half day

Conclusion

The era of passive document storage is over. Organizations that can surface the right knowledge at the right moment will outperform those that cannot. But the transition to AI-powered document intelligence must not come at the cost of data security, privacy, or regulatory compliance.

VaultIQ delivers the full power of modern AI · natural language search, semantic retrieval, cited answers · running entirely inside your own infrastructure. No data leaves. No vendor lock-in. No per-seat pricing that scales against you as adoption grows.

RingStor has built VaultIQ on a foundation of production-grade open-source AI technology, hardened with the enterprise controls and deployment flexibility that security-conscious organizations require.

Ready to deploy private AI document intelligence?

Contact RingStor to schedule a technical demonstration or start a pilot deployment.

www.ringstor.com · info@ringstor.com · Princeton, NJ

RingStor, Inc. | Princeton, NJ | Founded 2011 | www.ringstor.com

RingStor