Agency — Canonical Product Overview

What is Agency?

Agency is a local-first, zero-knowledge knowledge base that lets individuals and teams ingest, search, and reason over their private documents and data using AI — **without plaintext ever leaving their control**.

Agency is designed for situations where cloud-first AI tools are unacceptable due to confidentiality, compliance, data ownership, or trust constraints. It delivers modern AI-assisted search and chat while preserving strict data sovereignty.

At its core, Agency gives users the power of AI over their own knowledge — **on their own machine, under their own keys, with optional and tightly constrained cloud participation**.

The Core Problem Agency Solves

Most AI tools force a tradeoff:

- Use powerful AI → upload sensitive data to third parties
- Keep data private → lose AI capabilities

Agency removes this tradeoff.

It enables: - AI-assisted search and chat over private data - Deterministic, auditable reasoning - Strong confidentiality guarantees - Flexible deployment models (offline, cloud-connected, BYOS)

All without requiring users to surrender control of their data.

Who Agency Is For

Agency is built for users and organizations that **cannot** or **will not** upload sensitive data to SaaS AI platforms.

Typical users include:

- Legal teams handling privileged or regulated material
- Security-conscious founders and engineering teams
- Enterprises with strict compliance or data residency requirements
- Researchers working with proprietary or embargoed data
- Organizations operating in air-gapped or offline environments
- Teams that need AI capabilities without vendor lock-in

If uploading documents to external AI services is not an option, Agency is designed for you.

What Makes Agency Different

Agency is not “another RAG app.” Its design starts from trust boundaries, not features.

1. Local-First by Default

All core operations run locally: - Document parsing and ingestion - Embedding generation - Hybrid search (semantic + keyword) - Knowledge graph construction - AI-assisted chat

Agency works fully offline. Cloud services are **optional** and never required for core functionality.

---

2. Zero-Knowledge by Design

Agency enforces a strict zero-knowledge model:

- Documents, filenames, and content are encrypted client-side
- Encryption keys never leave the user’s device
- Optional cloud components see **only encrypted blobs and metadata**
- No plaintext is accessible to Agency’s servers

Even in cloud-connected modes, Agency cannot read user data.

---

3. Multi-Paradigm AI (Not LLM-Only)

Agency deliberately avoids the “LLM for everything” approach.

Instead, it combines: - **Hybrid search** for fast, precise retrieval - **Knowledge graphs** for structured, explainable reasoning - **Traditional NLP and classifiers** for deterministic tasks - **LLMs** only where generative reasoning is appropriate

This results in: - Lower latency - Fewer hallucinations - Better explainability - Predictable behavior in high-stakes workflows

---

4. Flexible Trust & Deployment Models

Agency supports multiple operating modes:

- **Standalone (Local-Only):**
- No cloud account required
- Fully offline

- Always free for core functionality

- **Cloud-Connected (Optional):**

- Team collaboration
- Encrypted sync

- Share links and permissions

- **Bring Your Own Storage (BYOS):**

- Use your own AWS/GCP/Azure/S3-compatible buckets

- Client-side encryption enforced

- **Future: Trusted Execution Environments (TEEs):**

- Hardware-attested confidential compute for large datasets

Users choose their trust boundary; Agency adapts without changing its data model.

What You Can Do With Agency

Agency enables users to:

- Ingest large, heterogeneous document collections
- Search using semantic meaning, keywords, metadata, and filters
- Ask natural-language questions over their data
- Build and query knowledge graphs
- Track provenance and citations
- Collaborate securely with teams
- Maintain full control over storage and encryption

All while keeping sensitive data private.

What Agency Is Not

Agency is intentionally **not** designed for:

- Users comfortable uploading data to cloud AI services
- Lightweight note-taking or personal productivity apps
- Consumer chatbots or entertainment use
- Pure LLM experimentation without data governance concerns

If convenience outweighs confidentiality, simpler tools may be a better fit.

Why Agency Exists

AI is becoming a foundational interface for knowledge work — but trust, privacy, and control have not kept pace.

Agency exists to ensure that:

- AI can be powerful **without being invasive**

- Users retain sovereignty over their data
- Teams can adopt AI without violating policy or principle
- Advanced reasoning does not require blind trust in vendors

Agency's philosophy is simple:

> **Your data. Your machine. Your rules.**

The One-Sentence Summary

Agency is a local-first, zero-knowledge knowledge base that brings AI-powered search and reasoning to private data — without forcing users to give up control or confidentiality.