

VaultAI — Your Second Brain, Actually Private

Drop: Jan 31, 2026 • **Test Drop Category:** AI / Privacy / Personal Knowledge

The One-Liner

A local-first AI assistant that runs entirely on your device — your data never leaves your machine.

The Problem

Everyone wants AI assistants, but: - ChatGPT/Claude see everything you type - Enterprises can't use AI for sensitive docs (legal, medical, financial) - Privacy-conscious users are locked out of the AI revolution - Data breaches expose your most personal conversations

The fear is real: 11% of data pasted into ChatGPT is confidential (Samsung banned it after source code leak).

The Solution

VaultAI — A fully local AI that: 1. Runs 100% on your device (Mac, PC, phone) 2. Connects to your files, notes, emails — locally 3. Never sends data to any server 4. Open-source, auditable, trustworthy 5. Fine-tuned on YOUR data for personalized responses

The stack: - Local LLMs (Llama 3, Mistral, Phi) optimized for Apple Silicon / NVIDIA - Local vector DB (ChromaDB) for your knowledge base - Local RAG pipeline for document Q&A - Optional encrypted sync between YOUR devices only

Why Now?

1. **Local LLMs are finally good** — Llama 3 70B rivals GPT-4 for many tasks
 2. **Apple Silicon changed everything** — M3 MacBooks run 70B models smoothly
 3. **Privacy regulations tightening** — GDPR, CCPA, HIPAA forcing compliance
 4. **Enterprise demand exploding** — Legal/medical/finance need AI but can't use cloud
 5. **Trust in Big Tech collapsing** — Users want control
-

Market Size

- **TAM:** \$50B+ (AI assistant market)
- **SAM:** \$15B (privacy-conscious users + regulated industries)
- **SOM:** \$2B (early adopters willing to pay for privacy)

Target segments: - Lawyers, doctors, financial advisors (compliance-required) - Executives with sensitive communications - Journalists, activists, researchers - Privacy-first consumers (growing fast)

Business Model

Tier	Price	Features
Free	\$0	Basic local chat, 7B model
Pro	\$20/mo	All models, unlimited docs, priority support
Team	\$50/user/mo	Admin console, audit logs, on-prem deployment
Enterprise	Custom	Dedicated support, custom fine-tuning, compliance certs

Unit Economics: - No inference costs (runs on user hardware) - 90%+ gross margins - Revenue = pure software licensing

Competitive Landscape

Competitor	Approach	Gap
ChatGPT	Cloud, sees everything	No privacy
Ollama	Local but CLI-only	No UX, no ecosystem
Jan.ai	Local but limited	Early, not enterprise-ready
PrivateGPT	Document Q&A only	Not a full assistant

Our edge: Consumer-grade UX + Enterprise-grade privacy + Full second-brain features

Go-to-Market

Phase 1: Prosumer Launch (Month 1-6) - Launch on Product Hunt, Hacker News - Target: developers, privacy advocates - Price: Free tier + \$20/mo Pro - Goal: 10K users, 500 paid

Phase 2: Professional (Month 6-12) - Target: lawyers, doctors, financial advisors - Compliance certifications (SOC2, HIPAA-ready) - Direct sales + partnerships - Goal: 50K users, 5K paid, \$1M ARR

Phase 3: Enterprise (Year 2) - On-prem deployment option - Team management features - Goal: \$10M ARR

5-Year Projection

Year	Users	Paid	ARR
1	50K	5K	\$1M
2	200K	25K	\$8M
3	500K	80K	\$30M
4	1M	200K	\$80M
5	2M	500K	\$200M

Exit: \$2B+ acquisition by Apple, Microsoft, or privacy-focused player

Why This Wins

1. **Inevitable demand** — Privacy + AI intersection is unavoidable
 2. **Zero marginal cost** — Users bring their own compute
 3. **Trust moat** — Open source + local = verifiable privacy
 4. **Network effects** — Community plugins, shared prompts
 5. **Apple partnership potential** — Aligns with Apple's privacy brand
-

Action Items for Pradhith

- Download Ollama, test Llama 3 locally
 - Research Jan.ai and PrivateGPT as comps
 - Survey 10 lawyers/doctors about AI privacy concerns
 - Mock up the ideal UX in Figma
 - Buy domain: vaultai.com or getvault.ai
-

“The most powerful AI is the one you can trust with everything.”

— *The Godfather*