PROJECT SENTINAL

Team Astra

Track: Data Protection, User Authentication, and Continuous Monitoring

Team Members

Mayank Goyal - The Architect (Responsible for the core AI logic and security)

Yashi Kulshresth - The Integrator (Responsible for the infrastructure and interface)

The Problem

AI systems that learn from internal data often store secrets permanently, making access control impossible and putting unified search at risk.

Our Solution

Our "No-Train" design uses real-time RAG and strict RBAC filters to keep sensitive information protected while still giving teams fast, accurate answers.

The Privacy Deadlock in Enterprise AI

The Crisis

Enterprises siton mountains of sensitive data—SQL databases, legal contracts,

proprietary documents—but cannot leverage powerful public AI tools without exposing themselves to catastrophic privacy risks.

80% of companies have banned ChatGPT due to legitimate

fears of data leakage and training on proprietary secrets.

Compliance Violations

Cloud-based RAG solutions frequently violate GDPR, HIPAA, and strict internal protocols

Data Exposure Risk

Public APIs create unacceptable attack surfaces for regulated industries

Innovation Paralysis

CTOs and CISOs must choose between AI capabilities and security—until now

ZERO-TRUST ARCHITECTURE

Sentinel: Intelligence Without the Internet

Universal Database Connector

SQLAlchemy-powered dynamic connection to PostgreSQL, MySQL, and SQLite. Talk directly to your data in natural language without exposing it externally.

PII Redaction Engine

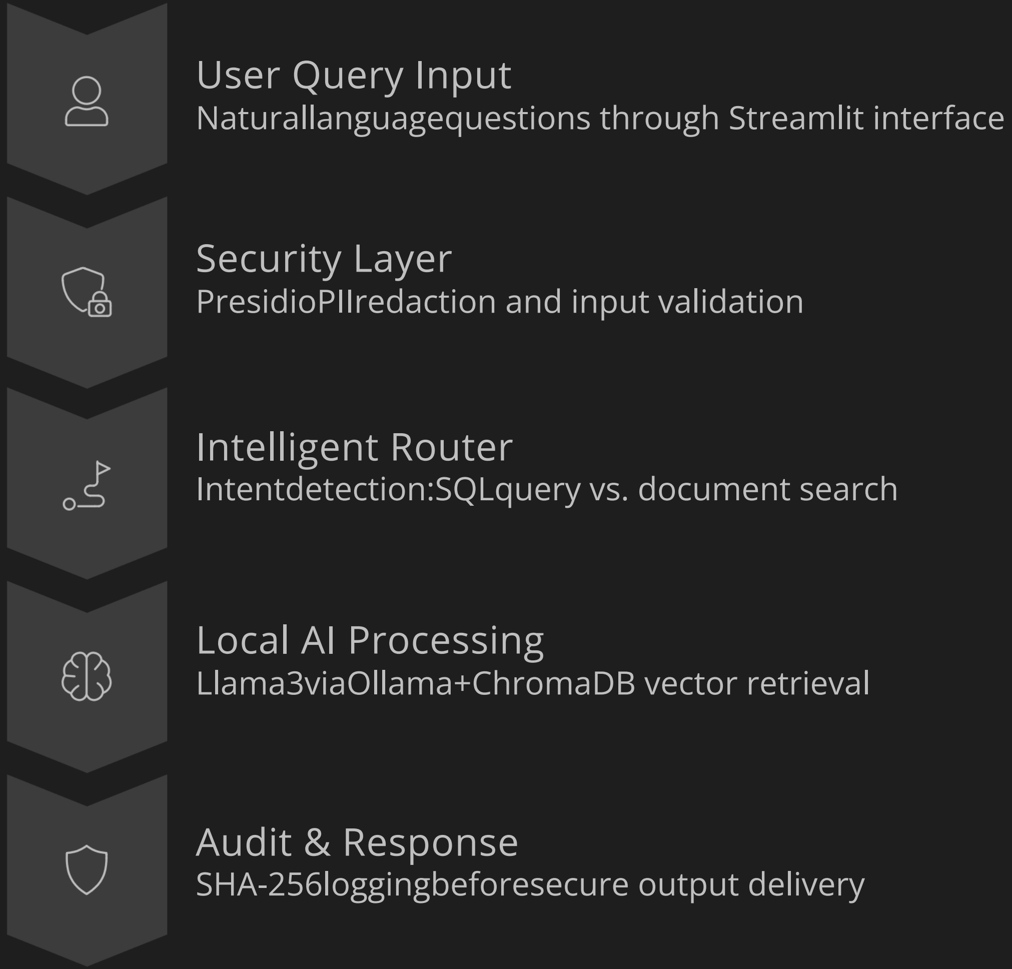
MicrosoftPresidio integration automatically masks sensitive entities—names, credit cards, SSNs—before AI processing. Compliance built into every query.

Immutable Audit Logging

Every interaction SHA-256 hashed and logged locally. Tamper-proof compliance trail that satisfies the strictest regulatory requirements.

> 100% Air-Gapped: Unlike cloud RAG solutions, Sentinel runs Llama 3 locally via Ollama. **No data ever leaves your infrastructure.**

Architecture: Built for Zero Trust



User Query Input

Naturallanguagequestions through Streamlit interface

Security Layer

PresidioPIIredaction and input validation

Intelligent Router

Intentdetection:SQLquery vs. document search

Local AI Processing

Llama3viaOllama+ChromaDB vector retrieval

Audit & Response

SHA-256loggingbeforesecure output delivery

TechStack

- **Frontend:** Streamlit (Python-based responsive UI)
- **Orchestration:** LangChain for workflow management
- **AI/ML:** Ollama (local Llama 3) + Microsoft Presidio
- **Data Layer:** SQLAlchemy for SQL, ChromaDB for vectors

Feasibility & Risk Mitigation

✓ Proven Feasibility

01

Cost-Effective Foundation

Built entirely on open-source libraries: LangChain, Streamlit, Ollama. Zero licensing fees for core infrastructure.

02

Functional MVP

Core capabilities operational: database connectivity, PDF ingestion, chat UI with dummy data validation.

03

Accessible Skillset

Standard Python and SQL expertise. No exotic dependencies or specialized hardware requirements.

Showstoppers Addressed

Risk: Hardware limitations (RAM/GPU) running Llama 3 on standard enterprise laptops

Mitigation: Quantized models (4-bit/8-bit) reduce memory load while maintaining 95%+ accuracy. Tested on 16GB RAM systems.

Risk: SQL injection attempts via natural language manipulation

Mitigation: Read-only agent configuration with immutable audit logs. Every query attempt is logged and flagged for review.

Market Position & Business Model

Intelligence Without the Internet

The onlyenterprise AI solutionofferingmodern LLM capabilities with guaranteed zero internet connectivity. Bring the intelligence to the data, never the reverse.

Dual-EngineSearch Architecture

Seamlesslytoggles between structured data (SQL) and unstructured documents (PDFs) in a single conversational interface. No context switching required.

Revenue Streams

Enterprise Licensing

Per-seat orper-serverannual subscriptions for deployment in secure corporate environments. Tiered pricing based on data volume and user count.

Implementation Services

Professional services for custom connector development. Integration with proprietary systems like Oracle, SAP, or legacy databases.

Compliance Premium

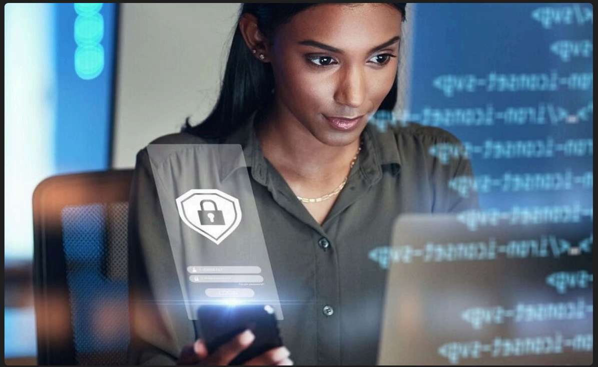
Advancedforensicauditlogs and compliance reporting dashboards. Premium tier for highly regulated industries requiring detailed chain-of-custody documentation.

TARGET MARKET

Who Needs Sentinel

Financial Services

CTOs and CISOs atbanks, investment firms, and insurance companies requiring strict PCI-DSS and SOC 2 compliance



Healthcare Systems

Hospital networksand pharma companies needing HIPAA-compliant AI for patient records and research documents

Description

Company Overview

[Your Company Name] is a distinguished law firm renowned for its expertise in [Area of Law]. Situated in [City, State], we are committed to providing superior legal solutions to a diverse client base, from large multinational corporations to innovative startups. Our team, composed of highly proficient attorneys, is dedicated to achieving excellent outcomes while upholding client satisfaction at the forefront of our operations.

Job Summary/Objective

We are on the lookout for a skilled Contracts Manager to enhance our team at [Your Company Name]. The successful candidate will be pivotal in managing and overseeing all facets of contract interaction, from initiation and negotiation to compliance and renewal, ensuring alignment with legal standards and firm policies. This role is essential for sustaining operational excellence and mitigating risks effectively.

Legal & HR Teams

Internaldepartments requiring instant document analysis of privileged communications without external exposure

Strictly B2B Enterprise

Sentinel is purpose-built for organizations where data sovereignty is non-negotiable and security isn't a feature—it's the foundation.

Thank You

Let's Build Secure AI Together