The Data Layer represents systems where raw data is stored, processed, and converted into datasets for model training and fine-tuning

Problems

- AI initiatives lack access to the most valuable enterprise data due to security and privacy concerns, hindering potential breakthroughs.
- Sensitive information movements risk exposing data to malicious actors and compromising your security posture.

Solved with Protopia

- Access to your most valuable data through Stained Glass, ensuring no raw data leaves your trusted environment.
- Transforms sensitive data into randomized representations, unlocking AI/LLM utility without exposing or leaking original data.

The Model Layer represents systems where data, training code and base models are processed in training and fine-tuning runs and deployed to serve user requests.

Problems

- Redacted or synthetic data lowers model accuracy, hampering AI initiatives.
- Efficacy hindered by limited access to data in hybrid execution environments, which are necessary due to GPU/compute constraints or data sovereignty requirements.

Solved with Protopia

- Securely transform and utilize more of your sensitive data for greater impact.
- Enables data availability across hybrid environments through directly usable, irreversible transformations, eliminating the need to transmit, decrypt, or locally copy actual data outside your trusted environment.

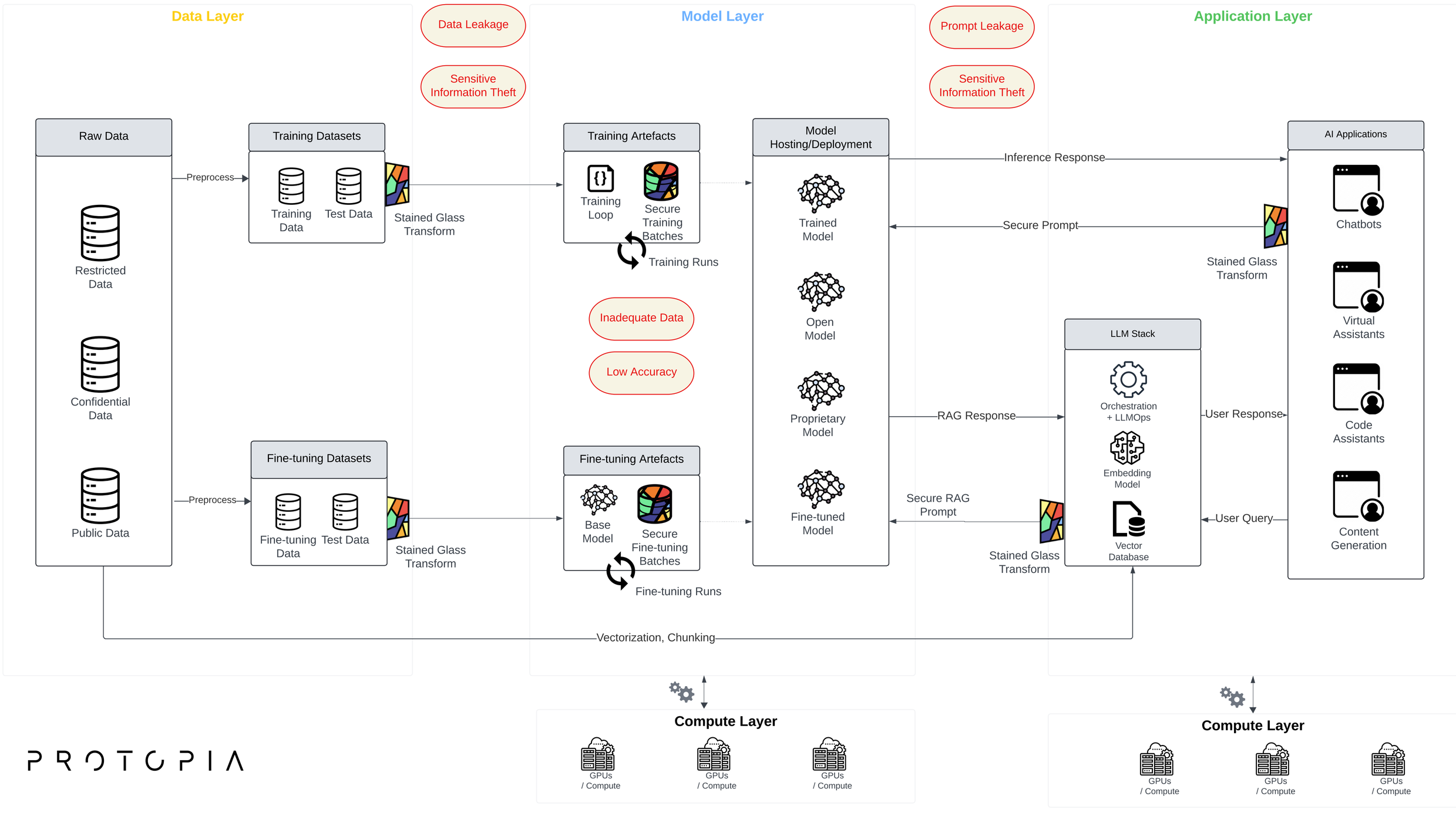
The Application Layer represent systems used to power end user applications like chatbots, virtual assistants, as well as technology components for Retreival Augmented Generation (RAG), including vector databases

Problems

- Inference traffic interception risks exposing sensitive or personally identifiable information (PII) to hackers.
- Malicious actors can compromise data, user, or model security by stealing prompts to extract sensitive details.

Solved with Protopia

- Enhances the security of prompts to model endpoints, ensuring consistent protection of sensitive user data.
- Strengthens the protection of prompts and sensitive data in Retrieval Augmented Generation (RAG) systems for enterprises.



PROTOPIA