PROTOPIA

www.protopia.ai

Data Privacy That Scales With Your AI Infrastructure

Deploy AI in Production While Protecting Sensitive Data

Organizations deploying AI with sensitive data face critical security challenges:

Inference Endpoints Create New Security Vulnerabilities

Traditional security measures protect data at rest and in transit—but not during AI processing. As inference scales, sensitive data remains exposed at endpoints.

Multi-tenant AI Applications Risk Data Leakage

This inference-stage vulnerability exposes sensitive data, raising privacy concerns for regulated industries and slowing AI adoption in high-security environments.

Traditional Data Protection Methods Are No Longer Sufficient

Alternatives like redaction and data masking reduces data utility and AI use-case accuracy, impacting performance, cost, and accuracy.

Protopia Stained Glass: The Lightweight Solution for AI Inference Security

Protopia's Stained Glass Transform (SGT) converts sensitive data into irreversible, AI-compatible stochastic representations, eliminating raw data exposure risks while maintaining full model accuracy and near-zero performance impact.

Expand Data Utilization

Leverage your full data spectrum across the entire AI lifecycle while mitigating data leakage and exposure risks.

Improve Infra Utilization

Securely use data across on-prem, hybrid, and cloud environments for efficiency and faster value realization.

Retain Data Ownership

Stochastic representations preserve accuracy for target models but are unintelligible to humans or other models.

Deploy Anywhere

SGTs add minimal latency (typically ms) and can even run on CPUs or embedded devices, including sensors.

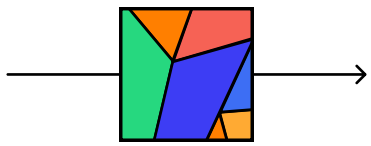
How Stained Glass Transforms Work

Unprotected Prompt (Without Protopia)

Context & Instruction

Summarize the below document:
COUNTRY: Warsaw Pact/USSR
SUBJECT: Armaments Planning Within the Framework of the Warsaw Pact
DOI: Late 1981.The following report is a detailed account of the...

Stained Glass Transform™



Protected Prompt (With Protopia)

Context & Instruction

}, // ', ');){ '); }); a>?[<}); "> });];]; >?[<});)); >?[< } s}; '); >?[< */ },]); }; >?[< '); KS}); }); '); ', ', }); */ // ', for'); our', "> s'); ', */ */ >?[< */ G }; >?[< '); };]); }; */ ', ',){ '; }); //){ ', */ >?[<}; ', });){ ', /** //){ >?[< */ ', ";]); */ ()); }, } '; }; ',]); }); ()); // }; }, ', (); } ', (); };){ };...

Maintain High Performance While Eliminating Plain-Text Data Exposure

Model	Average Tokens Transformed	Sentence Completion (HellaSwag)	Language Understanding (MMLU)	Model Truthfulness	Abstraction Reasoning (ARC)
Llama 3.1 70B W/ SGT	98.44%	77.97%	77.88%	62.33%	51.02%
Llama 3.1 70B without SGT	0% (ie., plain-text)	77.61%	80.52%	66.9%	50.94%

Secure AI Inference Without Performance Trade-Offs

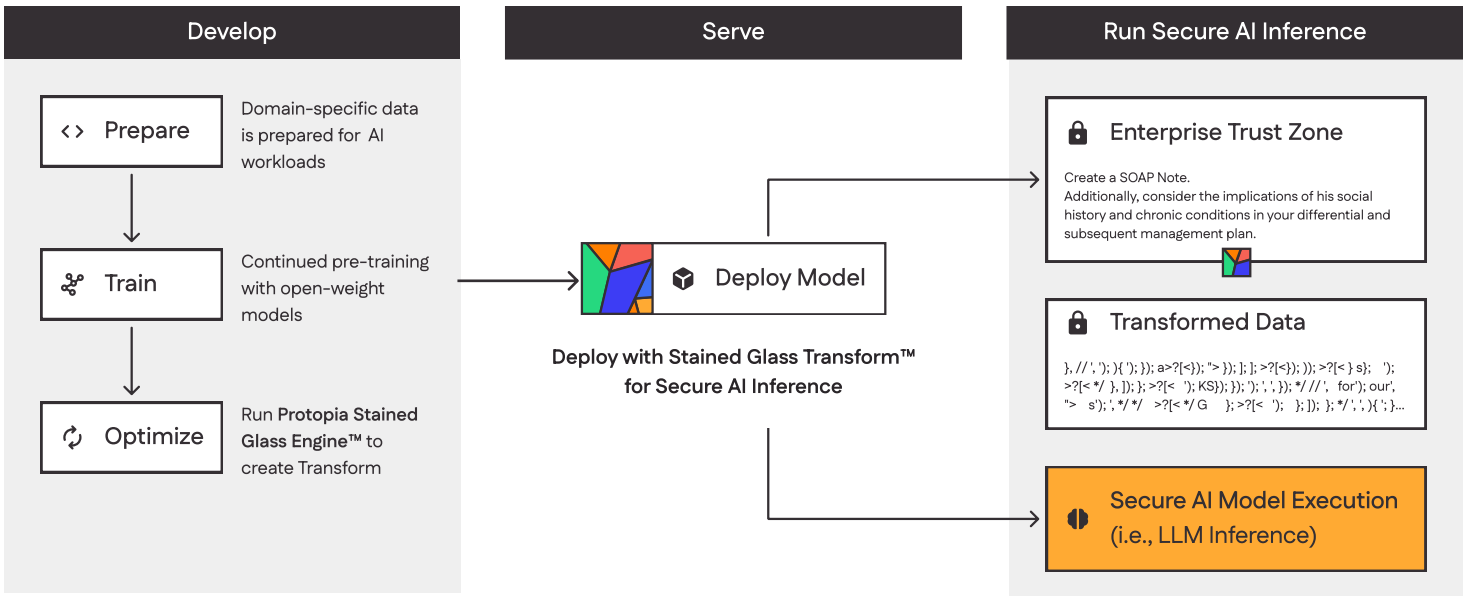
<1%
Added to inference time

~25 milliseconds
Latency for Llama 70B SGT for ~200 token

Data Protection Without Disruption
Model weights, accuracy, and AI workload performance rates remain intact

Secure AI Workloads Across Inference Ecosystems

Protopia Stained Glass integrates seamlessly into inference endpoints, AI pipelines, and LLM applications without modifying underlying models. SGT unlocks secure AI adoption without compromising accuracy or scalability.



End-to-End Protection Across Inputs, Outputs, and Embeddings

Protopia ensures that sensitive information never exists in plaintext outside of the enterprise zone of trust, securing data through every layer of the AI pipeline—from user inputs to model outputs. Stained Glass Transform seamlessly integrates with existing AI pipelines, maintaining peak accuracy and performance without compromising on latency or cost.

Open-Weights

No modifications to the weights of trained AI model being targeted.

Near-Zero Latency

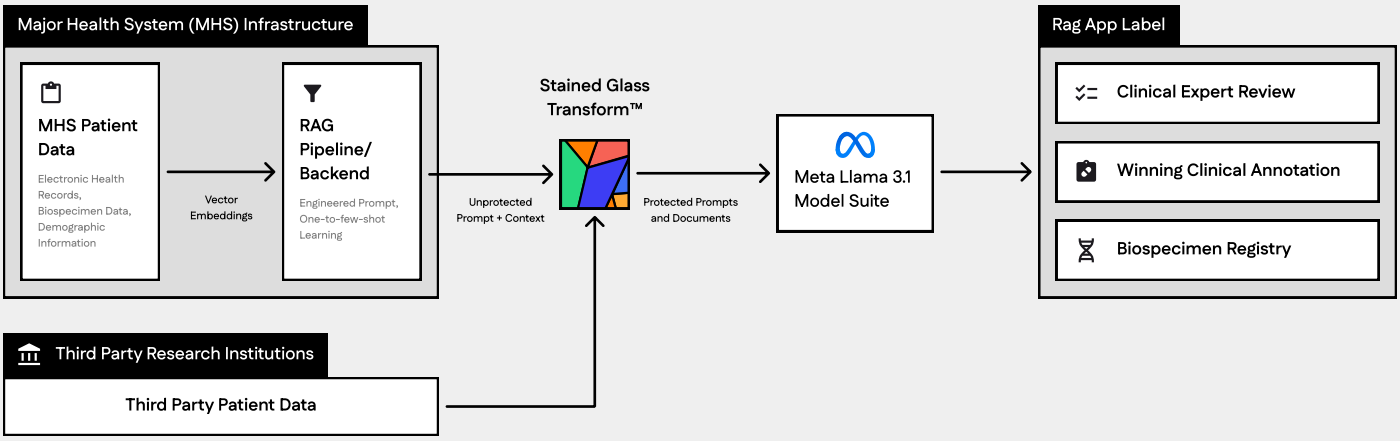
Minimal latency with Stained Glass during inference.

Model Agnostic

Applicable to LLM, computer vision, or other ML architectures.

RAG Case Study: Advancing Medical Research While Protecting Data

Protopia partnered with Meta and a leading Major Health System (MHS) to securely implement a RAG application for oncology research. By using Protopia SGT, the institution overcame strict privacy constraints, enabling secure AI-powered collaboration with third-party researchers.



Gartner

- Gartner AI TRiSM Market Guide
- Emerging Tech: Edge AI
- Emerging Tech: Data Privacy
- Gartner Hype Cycle x9

- U.S. Army XTech Scalable AI 1st Place ‘24
- U.S. Navy Trident Warrior ‘22

Partner to leading compute and data infra providers:

NVIDIA INCEPTION PROGRAM · aws · ORACLE PartnerNetwork · Lambda · NetApp · VAST