

Deploy AI in Production While Protecting Sensitive Data

Inference Endpoints Create New Security Vulnerabilities

Multi-tenant AI Applications

Risk Data Leakage

Traditional Data Protection Is No Longer Sufficient

Loss of Data Ownership with Third-Party Inference

When using third-party inference, enterprises lose control over where data is processed, undermining confidentiality and ownership.

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.



Improve Infra Utilization

Retain Data Ownership

Deploy Anywhere

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

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 }>?[< '};.];}>?/*,'}{');)// }{,/*
>?[<{'});){}/** //){}>?[< /*,'.];*/ ();
    } }{'};.];.});());// }{'};.();{'};.(); } }{;...

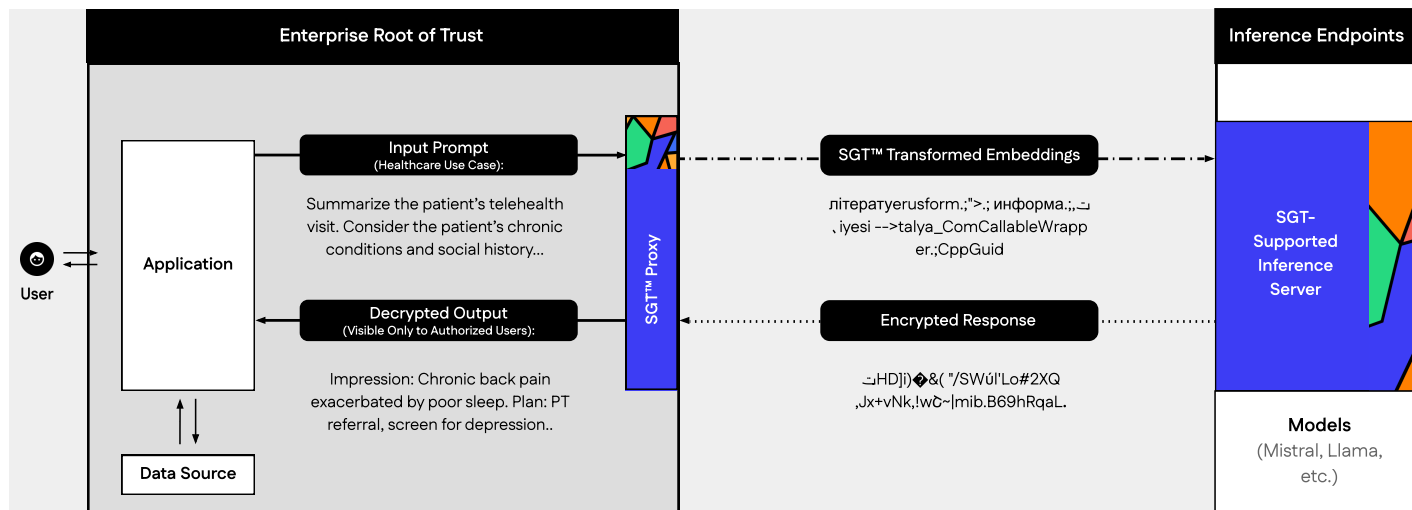
```

Model	Average Tokens Transformed	Sentence Completion (HellaSwag)	Language Understanding (MMLU)	Model Truthfulness	Abstraction Reasoning (ARC)	Secure AI Inference Without Performance Trade-Offs
-------	----------------------------	---------------------------------	-------------------------------	--------------------	-----------------------------	--

Llama 3.1 70B W/ SGT	98.44%	77.97%	77.88%	62.33%	51.02%	Added to inference time ~25 milliseconds Latency for Llama 70B SGT for ~200 token
Llama 3.1 70B without SGT	0% (ie., plain-text)	77.61%	80.52%	66.9%	50.94%	Data Protection Without Disruption Model weights, accuracy, and AI workload performance rates remain intact

Roundtrip Data Protection: Preserving Data Ownership in Managed Inference

Protopia's Stained Glass Transform (SGT) integrates with high-performance inference endpoints to protect sensitive data throughout the AI inference lifecycle. Data stays secure from input to output, even in multi-tenant environments. Only the client sees the full prompt and response in plaintext—preserving ownership without tradeoffs.



Deploy Secure Enterprise Use Cases

Transition from POC to production by unlocking proprietary data assets for secure enterprise workloads.

Maximize AI Infrastructure ROI

Securely scale up enterprise users and data sources to maximize utilization of cost-effective inference endpoints.

Quickly Adopt Cutting-Edge Models

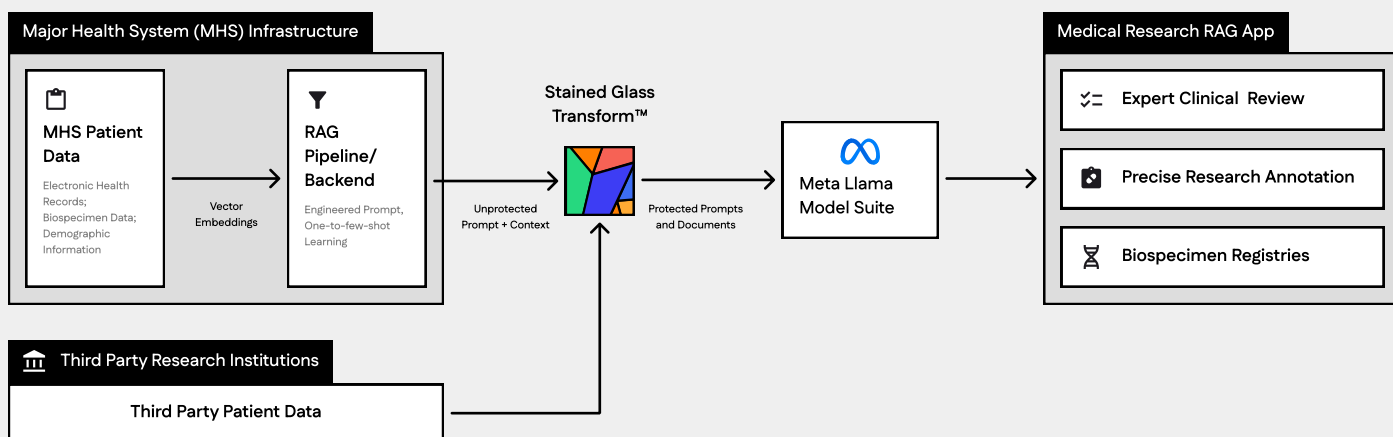
Access state-of-the-art models or your custom-deployed variants via serverless APIs, without exposing data in plaintext.

Secure AI Workloads Across the Full Inference Lifecycle

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

RAG Case Study: Advancing Medical Research While Protecting Data

Protopia partnered with Meta and a major U.S. 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

- AI TRISM Market Guide x3
- Emerging Tech: Edge AI
- Emerging Tech: Data Privacy
- Gartner Hype Cycle x9



- U.S. Air Force D2P2 SBIR for Secure Coding Assistants '25
- U.S. Army XTech Scalable AI 1st Place '24
- U.S. Navy Trident Warrior '22

Partner to leading compute and data infra providers:



PROTOPIA

[Learn More at Protopia.AI](https://Protopia.AI)