

Wand AI and Protopia AI Partner to Power Sovereign AI on Shared, Secure, High-Utilization Backend

Every ministry and agency in a nation can run its most sensitive workloads on a single sovereign AI back end, with plaintext never leaving the trust boundary.

AUSTIN, TX, UNITED STATES, July 21, 2026 /EINPresswire.com/ -- [Wand AI](#)

and [Protopia AI](#) today announced a partnership to deliver sovereign AI at national scale. The collaboration

combines Wand's operating system for

the hybrid human and AI workforce with Protopia AI's inference privacy layer, enabling a government or enterprise to run its most sensitive workloads across one shared sovereign backend at full utilization, without exposing data to the infrastructure operator or to other tenants.

The image shows the logos for Wand AI and Protopia AI. The Wand AI logo is in a dark purple color with a small pink star above the 'a'. The Protopia AI logo is in a light grey color. A horizontal line with a green-to-blue gradient is positioned below the logos.

“

Ministries and agencies can run their highest-value agentic workloads on one governed sovereign backend and make full use of the compute already in place.”

Jeff Brown, Chief Business Officer, Protopia AI

Real sovereignty requires the entire AI stack to run on sovereign soil and sensitive data. The agentic layer can be sovereign, but the moment an agent sends that sensitive data to a model, that data is exposed in plaintext across the entire serving environment: logs, caches, GPU memory, traces, and runtime infrastructure.

That creates a hard national-security problem. Secrets from different ministries, agencies, banks, and critical infrastructure operators cannot safely share the same

backend, so the default today is fragmentation, a separate infrastructure stack for each data owner. The result is massive waste: national compute investments sit underutilized because every sensitive workload requires its own isolated environment. At country scale, this "isolation tax" can reach tens of billions in infrastructure spend over time. The alternative is worse: data that is sovereign in name, but not sovereign in fact.

The Wand and Protopia AI partnership removes that tradeoff. Wand provides the sovereign agentic stack: country-level governance, a hybrid human and AI operating system, certified AI labor, and autonomous agents, attached to the sovereign compute base. Protopia AI provides the inference privacy layer. Its Stained Glass Transform™ (SGT), applied by the SafeCLAW subagent at the trust boundary, converts sensitive inputs into protected representations, so only the protected form ever crosses into the model and compute layers, with no decoder on the host and accuracy parity to plaintext. Because plaintext never leaves the trust boundary, every data owner can share one sovereign backend without exposing data to the operator or to one another.

“Too often, sovereign AI programs have had to fragment their agentic infrastructure into dedicated stacks whenever sensitive data enters the workflow,” said Jeff Brown, Chief Business Officer at Protopia AI. “Wand and Protopia AI remove that constraint. Protopia Stained Glass keeps plaintext inside each data owner’s trust boundary, so ministries and agencies can run their highest-value agentic workloads on one governed sovereign backend and make full use of the compute already in place.”

“Wand provides that foundational infrastructure: a governed operating system through which nations can deploy, operate, manage, and continuously evolve AI labor at scale. We are pleased to welcome Protopia AI into Wand’s sovereign technology ecosystem, adding a valuable privacy-preserving capability that enables ministries, institutions, and agencies to operate on a unified national stack while maintaining the security and control of their most sensitive data,” said Cristian Felix, Chief AI Architect, of Wand AI

HOW IT WORKS

The [joint reference architecture](#) supports two deployment points. Inference privacy uses SGT alone to make every model on the sovereign backend usable on sensitive data, with no enclave required. Confidential inference pairs SGT with Confidential Computing to protect the model and its execution environment as well, forming a zero-trust AI factory. While the two are complementary with compounding benefits, SGT does not depend on Confidential Computing.

Back end integration happens at a single point. Wand's Adaptive Router reduces every model call to one dispatch seam and selects models from an Open Model Registry. SGT plugs in at that seam, so privacy becomes a capability of every model on the backend rather than a property of any one deployment.

By allowing sovereign and regulated workloads to run on shared capacity instead of dedicated carveouts, the joint solution is designed to dramatically increase tenancy, and raise utilization of national compute from roughly 25 percent to more than 80 percent, lowering the cost per outcome for every ministry and agency it serves.

AVAILABILITY

The Wand AI and Protopia AI joint reference architecture is available to sovereign programs and enterprises now.

ABOUT PROTOPIA AI

Protopia AI delivers inference privacy for AI. Its Stained Glass technology protects the inference data path wherever AI runs, on-prem, in the cloud, serverless, sovereign, or across shared multi-tenant infrastructure. Stained Glass Transform converts sensitive inputs into protected representations before they leave the data owner's trust boundary, so the inference endpoint and its logs, caches, memory, and observability tooling never hold raw data. Stained Glass is software-only, needs no model retraining, and preserves accuracy and performance, which lets regulated and proprietary workloads run on shared infrastructure instead of dedicated carveouts. Organizations across financial services, defense, healthcare, and education use Stained Glass in production to put their most sensitive data to work with AI. Protopia AI is headquartered in Austin, Texas, with a global presence.

ABOUT WAND AI

Wand AI is building the sovereign infrastructure for AI labor. Wand's operating system enables governments and enterprises to deploy, manage, govern and continuously evolve AI agents alongside humans as trusted members of the workforce, with identity, objectives, authority, security, governance and auditability built into the platform.

For nations, Wand provides a unified foundation through which ministries, public institutions, and critical national organizations can deploy AI labor while maintaining sovereign control over models, compute, data, policies and operations. Wand powers production-scale deployments with some of the world's most consequential institutions including leading banks, asset management firms, hedge funds, consulting firms, and system integrators. Wand exists to power the biggest transition in human history: infinite labor – so that everything humanity can imagine, we can finally build.

Founded in 2023 and headquartered in Palo Alto, California, with offices in Palo Alto, New York and Abu Dhabi, Wand is backed by world-class investors, leaders, and a tier-one research team.

MEDIA CONTACTS

Wand AI

Hope Frank / Chief Marketing Officer / hope.f@wand.ai / 415.887.8448

Brittany Carambio

Protopia AI Inc

brittany@protopia.ai

Visit us on social media:

[LinkedIn](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/928162816>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.