

LATERALUS LABS

AI-POWERED, HUMAN-DRIVEN INFRASTRUCTURE

Danny Barbour, Principal Engineer

danny@lateraluslabs.com | g8e.ai

Portland, OR | Remote (US, EU)

Status: VOSB

CAGE: 13JA1

NAICS: 541511, 541512, 541519, 541715, 541690

PSC: DA10, DC10, DE01, R425, AC11

Lateralus Labs, LLC designs and builds sovereign agentic AI systems for mission-critical production environments, regulated sectors, and zero-downtime settings. We specialize in operationalizing active defense and advanced AI risk management for federal and defense infrastructure, replacing implicit trust with verifiable cryptographic proof at the edge.

CORE COMPETENCIES

- **Agentic AI Orchestration & Runtime Governance:** We deploy multi-agent consensus and ReAct reasoning while enforcing a strict **Zero-Trust Execution Substrate**. Our architecture guarantees **Fail-Closed Verification**, dropping any unauthorized or off-policy action at the boundary.
- **Data Protection & Shadow AI Governance:** We prevent unsanctioned model access and data spillage utilizing a **Sovereignty Boundary Plane** that dynamically scrubs PII and credentials prior to egress, rehydrating them only exactly at execution.
- **Hardware-Bound Authorization:** We enforce **Zero Standing Privileges**. Human intent is captured via **Out-of-Band (OOB) Suspension** and FIDO2/WebAuthn passkeys, binding cryptographic human approval to every state mutation.

TECHNICAL DIFFERENTIATORS

- **Co-Validation & Heterogeneous Consensus:** Execution requires a strict conjunction of machine-checkable consistency proofs and human intent proofs, eliminating shared AI blind spots.
- **Cryptographic Binding & State-Bound Transactions:** Mutations are bound to a deterministic hash. We verify expected vs. actual state roots, preventing time-of-check/time-of-use vulnerabilities.
- **Local-First Audit Architecture (LFAA):** The host operates as a **Sovereign Execution Boundary**—an untrusting, append-only, and tamper-evident source of truth for all commands.
- **Contextual Engineering & Data Sovereignty:** Models operate on a safe projection of reality. Our Sovereignty Boundary dynamically scrubs and tokenizes sensitive data before egress, rehydrating context locally only at the instant of execution.
- **Sovereign Agentic Infrastructure:** We design and build self-hosted, air-gapped, sovereign, and model-agnostic agentic systems that eliminate vendor lock-in and operate entirely within your perimeter.

RISK MANAGEMENT

- **Regulatory Alignment:** Architecture designed to support **NIST AI RMF Critical Infrastructure Profiles** and map directly to NSA Zero Trust pillars.
- **Accountability:** Delivering the "3 Ts"—**Trust, Transparency, and Traceability**—prioritizing auditable decision-making over raw model speed.
- **Supply Chain Security:** Architecturally hostile to vendor lock-in, enabling deep **AI Bill of Materials (AI-BOM) & Model Provenance** through replaceable reasoning engines.
- **Continuous Monitoring:** Providing **Full-Lifecycle Auditability** that integrates directly with existing SIEM/SOC pipelines for immutable runtime monitoring.

PROVEN EXPERIENCE

U.S. Navy | USS Bataan (LHD-5)

Commissioned IT infrastructure from bare steel. Administered UNIX systems in high-stakes operational environments.

Rubrik (NYSE: RBRK)

Owned service direction for NAS Cloud Direct in multi-petabyte enterprise environments. Automated observable workflows.

Nike Global Backup

Engineered and managed one of the world's largest enterprise backup environments in a zero-downtime, mission-critical setting.