Sovereignware™ + Trinary Bound™

Physical-Boundary Security Architecture for Sovereign AI

Hectec.ai Inc.

June 2026

Executive Summary

The Challenge
Highly regulated organizations face an impossible choice: adopt powerful public-cloud AI and expose sensitive data to telemetry and third-party processing, or remain fully air-gapped and sacrifice capability, scalability, and talent. Existing confidential computing solutions (TEEs, confidential VMs) still leave data exposed during transit, at rest outside attested environments, or subject to cloud-provider telemetry.

The Solution
Sovereignware™ + Trinary Bound™ introduces a **novel physical-boundary security architecture** that enforces data sovereignty through hardware-rooted controls and a formal multi-phasic data lifecycle. Sensitive information is never processed in unverified environments and is physically isolated when at rest.

Core Innovation
- **Physical-Boundary Model**: Data transitions through three verifiable states (Steam → Water → Stone) with corresponding physical isolation. Cold data can be completely disconnected from all networks. - **Tiered AI Execution**: Lightweight models run on the telemetry-free M5 edge device; sensitive orchestration executes locally on the Compute Node; heavy reasoning is dispatched only to remotely attested Trusted Execution Environments after cryptographic verification. - **Hardware-Rooted Trust Chain**: Every transition requires either physical human presence (YubiKey kinetic gate) or cryptographic remote attestation. - **Zero-Inbound Network Posture**: All external connectivity is strictly outbound-only via Cloudflare SASE, eliminating inbound attack surface.

Key Differentiators - Combines the performance of hybrid cloud AI with verifiable physical isolation of sensitive data. - Maps directly to regulatory requirements for data minimization, retention, and privilege protection (Florida FDBR, SEC 17a-4, attorney-client privilege). - Formal IP ownership is documented and assigned to Hectec.ai Inc. (Delaware C Corporation).

Target Users
Elite law firms, defense contractors, family offices, wealth managers, and government entities that require frontier AI capabilities without compromising data ownership or regulatory compliance.

Current Status
- Core architecture protected under U.S. Patent Application No. 19/458,785 (pending). - Functional prototypes validated with Apple Silicon + Thunderbolt 5 + CalDigit + OWC hardware stack. - Pilot program targeted for Q3–Q4 2026.

Contact
For pilot discussions or partnership inquiries:
hq.trinarybound.com | sovereignware.org