Technical Whitepaper

The Sovereignware™ + Trinary Bound™ Hybrid AI and Physical-Boundary Security Architecture

Hectec.ai Inc. (Delaware C Corporation) Founder & Inventor: Hector Jose Cabrera

June 11, 2026

Contents

Executive Summary

The integration of advanced generative artificial intelligence within enterprise operations has created a structural conflict between the reasoning power of public cloud models and the confidentiality, statutory, and privilege mandates of highly regulated industries. Traditional security perimeters have largely disintegrated, forcing organizations to choose between fully public cloud environments—which expose sensitive data to telemetry, unauthorized data scraping, and third-party processing—and fully air-gapped on-premises architectures, which are severely constrained by local hardware limitations and capital costs.

To resolve this conflict, the Sovereignware™ and Trinary Bound™ framework introduces a novel hybrid Software-as-a-Service (SaaS) and zero-cloud Hardware-as-a-Service (HaaS) architecture grounded in **physical-boundary security**. Unlike conventional confidential computing approaches that rely solely on Trusted Execution Environments or fully air-gapped systems, this architecture enforces data sovereignty through a hardware-rooted, multi-phasic state machine that transitions sensitive information through distinct physical and logical states.

Utilizing a hardware-rooted local orchestration unit (**Ark Citadel**) coupled with physically isolated, multi-drive local storage (**Ark Node**), the system executes a multi-phasic state machine that protects sensitive data at the physical boundary. AI workloads are strategically placed: lightweight inference and semantic processing occur on the telemetry-free M5 Ambassador edge device; sensitive orchestration and local reasoning execute on the Compute Node (Phase 0); and computationally intensive tasks are dispatched only to remotely attested Trusted Execution Environments after cryptographic verification. By combining telemetry-free local edge processing, secure outbound-only tunnels, hardware-token kinetic validation, and remote attestation before any data leaves the local boundary, this framework preserves client confidentiality, attorney-client privilege, and regulatory compliance while delivering enterprise-grade AI capabilities.

This whitepaper validates the engineering design and positions the architecture as a production-grade solution for elite enterprise, legal, defense, and government environments that demand both advanced AI capabilities and uncompromising data ownership and sovereignty.

Intellectual Property Ownership

Technical Foundations and the White Stone Protocol

The foundational mechanism of the Trinary Bound™ physical hardware platform is "The White Stone Protocol," the subject of U.S. Patent Application No. 19/458,785 [3], which claims priority to U.S. Provisional Application No. 63/926,688, filed on November 27, 2025. The utility non-provisional application was submitted on January 24, 2026, by inventor Hector Jose Cabrera under microentity status on a gross income basis. As of the date of this whitepaper, the application remains pending and no patent has been granted. This protocol describes a hardware-rooted local server architecture designed to govern the ingestion, processing, and permanent recordation of sensitive client data while ensuring zero digital trace of volatile decrypted materials.

The Multi-Phasic Logic State Machine

The White Stone Protocol models data processing by transitioning information through three distinct logical states that correspond to the physical states of matter. This multi-phasic transition function, denoted as $\mathbf{\Psi}$, is mathematically defined as the composition:

$$\mathbf{\Psi} = \text{Commit} \circ \text{Sanitize} : \mathcal{S}_{\text{Steam}} \rightarrow \mathcal{S}_{\text{Water}} \rightarrow \mathcal{S}_{\text{Stone}}$$

Where:

- $\mathcal{S}_{\text{Steam}}$ represents the volatile, encrypted, and networked state of data: In this state, data exists only as transient, encrypted packets moving through external networks, completely isolated from any plain-text processing engine.
- $\mathcal{S}_{\text{Water}}$ represents the sanitized, buffered, and authenticated local state: In this state, data flows into the local physical bridge, undergoing hardware-rooted sanitization via the M4 logic module inside the **Ark Citadel** platform.
- $\mathcal{S}_{\text{Stone}}$ represents the physical and cryptographically immutable archive state: In this final state, data is committed to the physically isolated storage vault (**Ark Node**), verified locally, and the volatile memory buffers are cleared, leaving no lingering plain-text digital trails on the host system.

The multi-phasic architecture ensures that digital information is human-authenticated, sanitized, and physically isolated. This sequence generates a forensically audited trail while destroying intermediate volatile media, establishing a highly secure environment for individual data sovereignty.

Hardware Topology and the CalDigit High-Speed Bus

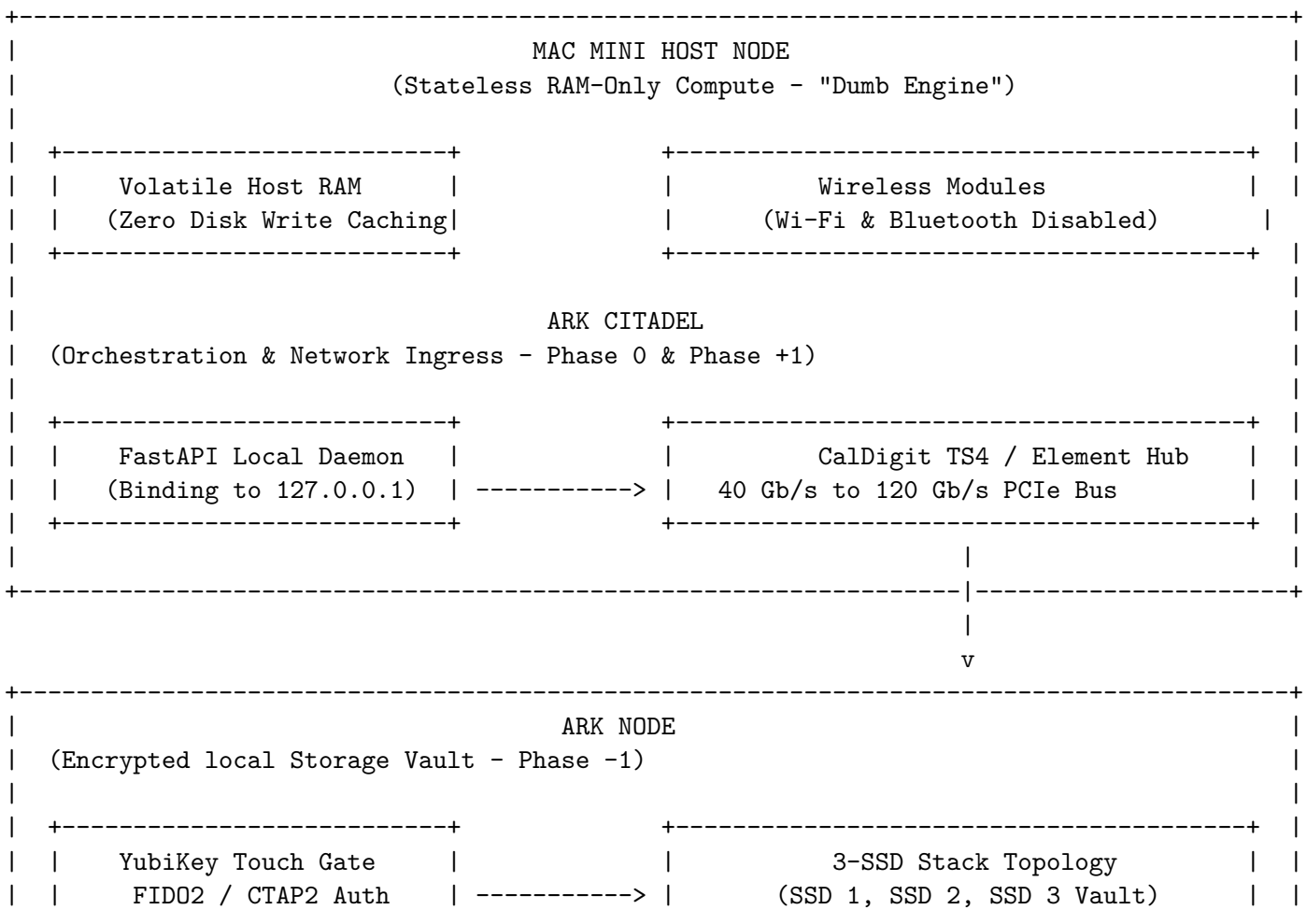
To eliminate performance, indexing, and protocol bottlenecks, routing between the **Ark Citadel** and the isolated **Ark Node** is managed via a dedicated, low-latency, PCIe-over-Thunderbolt hardware bridge featuring dynamic DMA protections and physical port isolation.

The system configuration uses the following reference components:

- **Primary Hardware Bus:** A multi-protocol Thunderbolt 4/5 docking and hub system (modeled on CalDigit's high-speed architectures) serves as the centralized high-speed communication bus.
- **Host Bandwidth Allocation:** The high-speed bus utilizes PCIe-over-Thunderbolt to achieve external storage speeds up to 6,200 MB/s and up to 64 Gb/s of dedicated PCI Express bandwidth, preventing system bottlenecks during intensive Vision-Language-Action (VLA) loops.
- **Decoupled Host Compute ("Dumb Engine"):** The host compute engine (specifically configured as an Apple Silicon Mac mini) operates as a stateless execution node or "dumb engine". To

guarantee complete telemetry containment, the Mac mini does not write persistent cache, indexing logs, or swap files to its internal storage; instead, the AI models and runtime software are loaded from the external storage stack directly into volatile host RAM with virtual memory swap disabled via system-level boot configurations.

- **Thunderbolt DMA Protections:** To defeat Direct Memory Access (DMA) attacks over the high-speed PCIe bus, the host compute engine's native Input-Output Memory Management Unit (IOMMU) is configured to enforce strict memory translation and hardware-isolated paging for all attached Thunderbolt channels. This blocks unauthorized external reads or writes to host system RAM.
- **SIP-Compliant Index Engine Bypass:** Because the physical drives connect via PCIe-over-Thunderbolt, they bypass the host operating system's default storage indexing utilities. To avoid raising the host's attack surface, the system does not disable System Integrity Protection (SIP). Instead, it touch-creates programmatic marker files directly on the root of each external volume and executes volume-specific command exclusions via the terminal. This disables both indexing and searching for the designated external storage blocks while keeping SIP fully active.
- **Hardware-Disconnection Air-Gap:** When the Thunderbolt physical cabling is disconnected, the isolated storage drives have zero active electrical signals. This provides a strong physical security boundary that renders the cold data significantly more resistant to remote network-based attacks and many electromagnetic, acoustic, or thermal covert-channel side-attacks, though organizations should still apply standard physical security controls.



```
|  +--------------------------+              +--------------------------------------+  |
+-------------------------------------------------------------------------------------+
```

The 3-SSD Stack Topology

The physical data states are isolated across three independent solid-state drives (SSDs) connected to the CalDigit Thunderbolt bus, representing a hardware realization of the phase-state model:

1. **SSD 1 (Phase +1 / Security Node):** Coordinates the network ingress tunnel. It hosts the Content Disarm and Reconstruction (CDR) pipeline, scanning for malware, stripping active scripts, and rebuilding clean "twin" document payloads while holding transient threat signatures.
2. **SSD 2 (Phase 0 / Compute Node):** Runs the local command surface and API routing, bound exclusively to local loopback interfaces (127.0.0.1) on ephemeral ports, ensuring it is entirely invisible to public network adapters. This is the primary location where AI models and orchestration logic execute.
3. **SSD 3 (Phase -1 / Vault Node):** Houses the dark local storage vault. It remains physically unaddressable to external network routes and executes a ledger-backed cryptographic handshake with SSD 2, requiring physical hardware-key touching to release raw blocks. This node is designed to host long-term immutable storage, including vector databases such as ChromaDB for retrieval-augmented generation workloads.

Hybrid SaaS + Zero-Cloud HaaS Configuration

To deliver advanced artificial intelligence capabilities without compromising data containment, the Sovereignware™ and Trinary Bound™ framework integrates a hybrid Software-as-a-Service (SaaS) and zero-cloud Hardware-as-a-Service (HaaS) topology. This architecture is built upon four primary security pillars designed to enforce localized data control while utilizing remote, high-performance cloud-based computing resources.

Telemetry-Free iPad M5 Ambassador AI

The primary interface and edge processing coordinator is a customized M5-powered display terminal operating as an "Ambassador AI". This terminal runs a highly restricted mobile operating system with all commercial diagnostic, crash-reporting, and usage telemetry disabled. This is achieved through firmware-level profile restrictions and local network loopback isolation, ensuring that zero operational metadata is transmitted to the operating system provider.

The M5 Neural Engine hosts lightweight on-device foundation models that handle initial natural language processing, semantic parsing, and biometric verification locally. These on-device models integrate with broader system capabilities via App Intents. By using App Intents, the local system can parse user context and orchestrate tasks across applications without sending raw, un-sanitized client documents to external servers.

Vertex AI and Google Distributed Cloud Sandbox Integration

For computationally intensive reasoning and agentic workloads that exceed local edge capacity, the architecture leverages Google Distributed Cloud (GDC) Sandbox environments. The GDC Sandbox acts as a secure, virtualized emulator of air-gapped systems. This configuration uses standard cloud APIs of the Vertex AI machine learning platform, authenticated securely via service accounts or API keys. No public cloud foundation models are executed locally; instead, all remote inference runs in Google

Cloud servers using NVIDIA GPUs inside Trusted Execution Environments (TEEs). These TEEs utilize hardware-level isolation, such as AMD SEV-SNP or Intel TDX, combined with TPU hardware featuring Google's Titanium security architecture, to encrypt and isolate memory and processing from the host OS and hypervisor.

To run these workloads securely, prompt payloads are sanitized locally on the M4 server, and a Kubernetes Job is initiated within the GDC Sandbox user cluster to manage the secure API dispatch. The container image is pulled from a secure local registry, and the GCP API key is mounted into the container as an environment variable via a Kubernetes secret:

```
apiVersion: batch/v1
kind: Job
metadata:
  name: secure-inference-dispatch-job
spec:
  template:
    spec:
      containers:
      - name: inference-client-container
        image: secure-registry.internal/sovereign-ai/inference-app:latest
        envFrom:
        - secretRef:
            name: gcp-api-key-secret
      restartPolicy: Never
```

The job status is monitored via standard orchestration tools. This workflow ensures that remote cloud servers function as stateless inference engines, maintaining no persistent records of inputs or outputs.

Remote Attestation Cryptographic Protocol

Before SSD 2 (Water) dispatches any sanitized prompt payload to the GDC Sandbox via the Cloudflare tunnel, it enforces a remote attestation "Background Check" protocol to cryptographically verify the integrity of the remote execution environment.

1. The local client issues an attestation challenge containing a cryptographically secure, single-use, short-lived random nonce to the GDC Sandbox, preventing replay attacks.
2. The GDC Sandbox TEE-kernel reads the hardware measurements from the AMD SEV-SNP/Intel TDX module (such as the Measurement of the Trust Domain, or MRTD), combines it with the nonce, and signs it using the hardware-embedded chip key.
3. The signed evidence is dispatched to an authorized, hardware-rooted verification authority (such as Intel Trust Authority) for validation. Once a cryptographically signed attestation token is returned, the local Citadel verifies the measurement against its local security policy. Only upon successful verification of the environment is the transient, end-to-end encrypted payload delivered to the TEE.

Cloudflare SASE Tunnels

Network egress from the local server unit to the GDC Sandbox is managed by the Cloudflare One Secure Access Service Edge (SASE) architecture. The connection is established via a secure daemon utility installed directly on the local server operating system. This design creates an outbound-only

connection to the nearest Cloudflare data center, rendering the local server completely invisible to the public internet.

The tunnel integration uses several key SASE mechanisms:

- **Outbound-Only Egress:** By establishing persistent, outbound UDP connections to Cloudflare's edge, the local server requires no open inbound ports on the local firewall, neutralizing external network scanning vectors.
- **Zero Trust Access Control:** Every connection routed through the tunnel is evaluated at the Cloudflare edge based on identity, device posture, and network context.
- **Persistent Session Resilience:** The tunnel software uses Dynamic Path MTU Discovery (PMTUD) to maintain active session persistence at the edge even during local network transitions.
- **Single-Pass Architecture:** Cloudflare's single-pass engine executes security checks, DDoS protection, and Web Application Firewall (WAF) inspections simultaneously, minimizing routing latency.

YubiKey Physical Touch Kinetic Gate

To prevent remote exploitation or unauthorized administrative overrides of the server unit, the system requires physical hardware-token validation using a YubiKey security key. This key enforces User Verification (UV) through two distinct cryptographic protocols:

FIDO2 / CTAP2 Protocol

The FIDO2 protocol secures web-based and application-level access. The YubiKey requires a physical capacitive touch to release private keys and authorize transactions, ensuring that remote actors cannot bypass local authorization. The YubiKey FIDO2 application requires that the PIN be supplied as the UTF-8 representation of the Unicode characters in Normalization Form C (Form C), preventing character encoding mismatches during authentication.

PIV (Smart Card) Operational Authentication

For local root operations and cryptographic key signing within the server, the PIV application is utilized. This mechanism restricts critical operations (such as generating new key pairs, importing private certificates, and modifying system retry limits) to local operators possessing both the PIV PIN and the physical management key.

For hardware versions utilizing firmware 5.7 and above, the default Triple-DES management key algorithm is replaced with AES-192, and the physical PUK is restricted to Unicode characters within the 0x00 to 0x7F range, enforcing a robust cryptographic boundary at the hardware layer.

The table below outlines the hardware token specifications and limitations for the platform, highlighting specific quirks of the YubiKey Bio Multi-protocol Edition (MPE):

Hardware Token Parameter	Standard FIDO2/PIV Specifications	YubiKey Bio MPE Quirks & Limitations
PIN Requirements	Up to 63 alphanumeric characters. Normalization Form C in UTF-8.	Supports fingerprint biometric auth; PIV PIN is set to "123456" by default.

Hardware Token Parameter	Standard FIDO2/PIV Specifications	YubiKey Bio MPE Quirks & Limitations
PUK Capabilities	6 to 8 characters used to unblock PIV PIN.	**No PUK support:** PIN cannot be unblocked if blocked; requires device-wide reset.
Session Reset	Standard PivSession.Reset() resets the PIV application.	**Reset Blocked:** PivSession.Reset() is not supported; requires device-wide reset.
Management Key	Triple-DES (firmware <= 5.6); AES-192 (firmware >= 5.7).	Cryptographic operations must use the default management key algorithms for firmware 5.7+.
Retry Counter	Configurable from 1 to 255; default set to 3.	PIN block occurs after maximum retries; if blocked, device-wide reset is required.

Hardware-Level Lockout and alwaysUV Configuration To completely safeguard against physical theft or coercion, the YubiKey is programmed with an **Always-On User Verification** (alwaysUV) policy. This forces the authenticator to demand biometrics or PIN verification for all cryptographic transactions.

The YubiKey firmware enforces a strict security limit: if the biometric scanner or PIN is failed 8 consecutive times, the FIDO2/PIV application permanently locks the interface. This action instantly deletes and destroys all stored private keys and credentials, neutralizing any physical brute-force attempts on the hardware token.

Phishing-Resistant Identity Federation & Cellular/SIM Defenses

To shield the hybrid control plane (accessible via endpoints such as hq.trinarybound.com, trinarybound.com, sovereign-ware.com, and sovereignware.org) from advanced session hijacking and telecom-based intercepts, the gateway layers FIDO2-compliant authentication directly into the Cloudflare Zero Trust Access policies.

This integration actively mitigates two critical remote attack vectors:

- **Neutralization of SIM Swapping:** Standard multi-factor methods like SMS one-time passwords (OTPs) are highly vulnerable to SIM-swapping attacks, where an adversary exploits carrier-level social engineering to port the user's telephone number to an attacker-controlled device. By enforcing mandatory WebAuthn/FIDO2 hardware-token policies through the Cloudflare Tunnel, shared secrets are eliminated entirely. Authentication is executed via asymmetric public-key cryptography where the private key resides exclusively inside the tamper-resistant secure element of the YubiKey and cannot be cloned or intercepted over a cellular network.
- **Defeating Device ID and Browser Fingerprint Spoofing:** Software-defined device IDs and browser user-agent fingerprints are easily spoofed by local malware or session-replay frameworks. The Trinary Bound™ architecture defeats this by requiring a device-bound cryptographic handshake. When logging in through the Cloudflare SASE gateway, a cryptographic challenge is bound directly to the legitimate domain origin (e.g., hq.trinarybound.com). Even if a remote attacker has spoofed the local machine's device ID, simulated its MAC address, or built a convincing Adversary-in-the-Middle (AiTM) phishing proxy, the authentication attempt will fail because the physical

YubiKey will only complete the cryptographic handshake with the genuine, registered origin. It is mathematically impossible to complete the handshake without physical possession of the hardware token and a physical touch to verify human presence.

The Steel Briefcase Engineering Specifications & Viewport Design

The stationary **Ark Citadel** configuration is integrated into a custom-designed, heavy-duty steel briefcase that acts as a secure, physical-boundary Faraday cage. This design protects the system from external physical and electronic threats during transit and operation, while maintaining the warranty and origin of the internal Apple hardware components.

Lexan Viewport and Trademark Protection

To maintain the active warranty of the Apple Mac mini, the host compute engine is never opened, unscrewed, or physically modified. Instead, it is housed within a custom-beveled baseplate under a transparent Lexan (polycarbonate) viewport.

- **First Sale Doctrine Alignment:** Under the First Sale Doctrine (17 U.S.C. § 109), the purchase of a genuine, retail-sold hardware item grants the purchaser the right to resell or incorporate that unmodified item into a higher-level assembly.
- **Lanham Act Compliance & First Sale Doctrine:** Section 43(a) of the Lanham Act (15 U.S.C. § 1125(a)) prohibits "reverse passing off." By keeping the Apple logo fully visible through the transparent Lexan viewport, the Ark Citadel explicitly displays the unmodified, genuine product origin in accordance with the First Sale Doctrine (17 U.S.C. § 109). Hectec.ai Inc. and its affiliates are not affiliated with, endorsed by, or sponsored by Apple Inc. The Apple Mac mini and its trademarks are used solely to identify the unmodified, commercially purchased hardware component integrated into the custom Ark Citadel enclosure. All Apple trademarks, logos, and product names remain the exclusive property of Apple Inc.
- **Aperture EMI Shielding:** Polycarbonate is naturally transparent to radio frequencies. To maintain the integrity of the Faraday cage, a conductively electroplated wire mesh (85 to 125 mesh copper grid with a wire diameter of 0.0012 inches) is laminated between two sheets of Lexan. This micro-mesh provides up to 50 dB to 60 dB of RF attenuation over the 30 MHz to 1 GHz range. The mesh terminates at the viewport perimeter via a conductive copper foil tape bonded to the steel bezel, preventing RF leakage through the window seams.

Active Thermal Management inside the Steel Shell

Enclosing a high-performance system like the M4 Mac mini in a small, unventilated space presents severe thermal risks. The Mac mini's metal casing is designed to act as a heat sink, and its internal power supply generates significant heat on the upper chassis under heavy loads. The system draws in cool air through the circular bottom ventilation grille and expels hot air out of the back. If the briefcase is completely sealed, a "greenhouse effect" will cause the internal air temperature to rise rapidly, triggering thermal throttling and performance degradation.

To evaluate the shielding performance of the steel briefcase, the skin depth of electromagnetic waves in the metal hull must be calculated. The skin depth, denoted as δ, is mathematically defined as:

$$\delta = \sqrt{\frac{2}{\omega\mu\sigma}} = \frac{1}{\sqrt{\pi f \mu\sigma}}, \quad \omega = 2\pi f$$

Where:

- δ is the skin depth (meters),
- f is the electromagnetic frequency (Hz),
- μ is the magnetic permeability (H/m) of the steel alloy,
- σ is the electrical conductivity (S/m) of the metal.

This formula ensures that the thickness of the 16 GA steel shell (1.52 mm) exceeds the required skin depth for target RF frequencies (e.g., up to several GHz), guaranteeing that external signals are completely blocked by the metal enclosure.

- **Segmented Thermal Zones:** The briefcase baseplate features a physical gasket cutout that isolates the Mac mini's bottom intake from the rear exhaust, preventing the system from recycling its own warm air.
- **Active Cooling Ventilation:** The steel shell cannot rely solely on passive heat dissipation. We integrate active, military-grade DC vaneaxial fans (STRONGAIR series engineered to meet MIL-STD-810 environmental standards) to draw ambient air into the enclosure and expel heated air out.
- **Chassis Star Grounding:** To completely eliminate the risk of the metal case acting as an antenna, the platform uses a **Single-Point Grounding (Star Grounding)** design. Connecting the system's logic ground to the metal cage in more than one place can turn the cage into an active dipole antenna. All internal components (the Mac mini chassis, CalDigit hub, and SSD bays) are electrically isolated from the metal briefcase shell and are routed to a single, low-impedance threaded brass ground stud.
- **Honeycomb Waveguide Vents:** To protect open air-vent apertures from RF leaks, we utilize honeycomb waveguide vents. These metal grilles are designed so that the diameter of each honeycomb cell is significantly smaller than the wavelength of the RF signals we want to block (e.g., maintaining cell openings under 3 mm to block frequencies up to 10 GHz).
- **Thermal Control Loop:** We configure the host machine's internal fan speed using thermal monitoring software (such as custom system fan modifiers) to adjust the internal fan speed up to 5,000 RPM during continuous computing tasks, keeping CPU temperatures below critical thresholds.
- **Conductive Seam Gasketing:** To prevent RF leakage, all seams, case openings, and lock latches must use conductive elastomeric gaskets conforming to MIL-DTL-83528 specifications. These gaskets must maintain a low volume resistivity (<= 0.10 ohm-cm) to ensure electrical continuity across the briefcase joints.
- **Grounding Infrastructure:** The metal layers of the briefcase must be grounded to neutralize external or internal electromagnetic fields. We terminate the conductive chassis to a dedicated, low-impedance threaded brass ground stud. This ground connection eliminates capacitive coupling and prevents static charge build-up.

Tiered Product Architecture (Ark Citadel vs. Ark Node)

To support diverse operational requirements and budget constraints, the platform is productized across two distinct tiers:

1. Ark Citadel (High-Assurance Enterprise/Government Tier)

The **Ark Citadel** is the flagship HaaS configuration, designed for high-risk corporate, legal, and governmental environments that demand absolute physical containment.

- **Enclosure:** Ruggedized, NEMA 3RX-rated steel briefcase with integrated active cooling and honeycomb waveguide vents.
- **Physical Protection:** Laminated blackened copper mesh Lexan window preserving Apple logo visibility and warranty.
- **Kinetic Actuator:** Class I mechanical foot-pedal acting as a physical power-gating relay.
- **Data Destruction:** High-Assurance Enterprise Materialization loop (thermal printer, gravity accumulator, optical scanner, and cross-cut shredder).
- **Target Audience:** Defense contractors, elite law firms, and financial institutions managing sensitive intellectual property or classified data.

2. Ark Node (Commercial Broad Market Tier)

The **Ark Node** is a streamlined, single-SSD hardware deployment designed to make secure local AI accessible to the broader commercial market. It offers a highly competitive price point while remaining substantially more secure than standard consumer or cloud AI setups.

- **Enclosure:** High-durability, compact desktop stand with passive heat dissipation, designed to be portable and easily packed for travel.
- **Physical Protection:** Relies on physical disconnection (dynamic physical decoupling) for cold data storage, ensuring that the drive is completely offline and un-hackable when unplugged from the CalDigit bus.
- **Kinetic Actuator:** FIDO2-based cryptographic capacitive touch gate via a roaming YubiKey token.
- **Security Profile:** While it lacks the physical Faraday cage and mechanical shredder of the Citadel, it retains the core zero-trust software properties—specifically the loopback-only APIs, stateless host RAM execution, and local cryptographic ledger handshakes.
- **Target Audience:** Independent consultants, boutique firms, and decentralized enterprise teams requiring strong, phishing-resistant local AI and GDPR compliance without the capital-intensive cost of a full Faraday briefcase.

Physical Construction, Bill of Materials (BOM), and Commercial Pricing Strategy

To translate the Sovereignware™ and Trinary Bound™ architecture into a viable commercial product, this section establishes the physical manufacturing tolerances, exact Bill of Materials (BOM), and financial projections for both the high-assurance enterprise and broad-market tiers.

Enclosure Mechanical Tolerances & Machining Guide

For the **Ark Citadel Briefcase**, the metal fabrication must adhere to strict tolerances to guarantee both NEMA 3RX ingress protection and MIL-STD-461 EMI shielding:

- **Chassis Deflection:** The 16 GA steel casing must maintain a maximum planar deflection of <= 0.05 mm across the mating seams to ensure uniform compression of the MIL-DTL-83528 conductive gaskets.
- **Vent Aperture Tolerances:** The honeycomb waveguide vent cells must be machined to a hexagonal cell diameter of 3.175 mm (± 0.05 mm) to block frequencies up to 10 GHz.
- **Airflow Clearances:** The internal mounting plate must hold the Mac mini exactly 63.5 mm (2.5 inches) above the briefcase floor, aligning the bottom intake grille with the isolated cool-air chamber.

Projected Production Costs & Bill of Materials (BOM)

The tables below detail the estimated Cost of Goods Sold (COGS) for both tiers, based on a low-volume pilot run (100–500 units).

Tier 1: The Ark Citadel Briefcase Unit (COGS Breakdown)

Component / Material Description	Unit Cost (USD)	Function / Security Role
Compute Node: Apple Mac mini M4 (Base Model)	599.00	Stateless "dumb engine" loaded directly into host RAM.
High-Speed Bus: CalDigit Element 5 Hub (TB5)	250.00	Low-latency 120 Gb/s routing with PCIe isolation.
Chassis: Custom 16 GA Steel Briefcase Shell	550.00	Ruggedized NEMA 3RX physical shield and Faraday cage.
Viewport: Polycarbonate + 100-Mesh Copper Grid PET	120.00	Shielded Lexan window keeping the Apple logo visible.
Shielding: Gaskets, Honeycomb Vents, Star Studs	85.00	Conductive sealing and ground loop elimination.
Thermal: Dual STRONGAIR 80mm Vaneaxial Fans	90.00	Active, MIL-STD-810 certified system cooling.
Secure Storage: 3x Samsung 990 Pro 2TB (Custom Bays)	350.00	Physically isolated Phase -1, 0, and +1 drive stack.
Authentication: YubiKey 5 Series / Bio MPE Tokens	85.00	Phishing-resistant FIDO2 hardware-token verification.
Assembly, Integration, & RF Attestation Testing	450.00	Professional assembly, wiring, and certified RF leak audits.
Total Estimated Tier 1 COGS	**2,579.00**	

Tier 2: The Ark Node Desktop Unit (COGS Breakdown)

Component / Material Description	Unit Cost (USD)	Function / Security Role
Compute Node: Apple Mac mini M4 (Base Model)	599.00	Stateless host RAM execution with wireless modules disabled.
High-Speed Bus: CalDigit Element Hub (TB4)	180.00	Low-latency 40 Gb/s Thunderbolt 4 routing.
Chassis: Custom-Machined Desktop Aluminum Stand	65.00	Compact, portable desktop stand with 2.5-inch elevation.

Component / Material Description	Unit Cost (USD)	Function / Security Role
Storage: 1x Samsung 990 Pro 2TB (Custom Enclosure)	120.00	Cold-vault storage with dynamic physical decoupling.
Authentication: YubiKey 5 Series / Bio MPE Tokens	85.00	FIDO2 user verification with alwaysUV PIN lockout.
Assembly & Quality Assurance	100.00	Stand testing, OS pre-loading, and QA verification.
Total Estimated Tier 2 COGS	**1,149.00**	

Commercial Pricing and Market Strategy

Because the physical construction costs are high, the platform utilizes a value-based, enterprise-targeted pricing model. This model is designed to offset hardware costs while maintaining high recurring profit margins.

- **Ark Citadel (Enterprise/Gov Tier):**
  - **Unit Price:** $14,500 upfront purchase (or a monthly lease of $650/month under a Hardware-as-a-Service model).
  - **SaaS Subscription:** Mandates a $1,500/month enterprise subscription for Sovereignware™ software licenses, local daemon updates, and Cloudflare SASE tunnel access.
  - **Target Sectors:** Defense contractors (CMMC compliance), corporate legal teams, elite family offices, and sovereign wealth funds.
- **Ark Node (Commercial Broad-Market Tier):**
  - **Unit Price:** $3,499 upfront purchase (one-time fee).
  - **SaaS Subscription:** Optional $250/month subscription for automated secure GDC Sandbox processing, remote backup ledgers, and secure software updates.
  - **Target Sectors:** Independent legal consultants, boutique financial advisors, small medical practices, and traveling corporate executives.

Regulatory Compliance and Legislative Analysis

The Sovereignware™ + Trinary Bound™ architecture is designed to address complex regional and federal regulatory environments. The table below maps specific physical and digital modules to their corresponding statutory requirements under Florida and federal laws.

Platform Component	Primary Regulatory Standard	Statutory Provisions & Mandates	Compliance Mapping & Verification
M4 Sanitization Module (104)	Florida SB 482 (Artificial Intelligence Bill of Rights), Florida Digital Bill of Rights (FDBR)	**SB 482:** NIL commercial protections. **FDBR § 501.711:** Data minimization and sensitive data processing rules.	Automatically strips PII, tracking pixels, and unauthorized synthetic media assets before printing or external API routing.

Platform Component	Primary Regulatory Standard	Statutory Provisions & Mandates	Compliance Mapping & Verification
Secure RAID Archive (106)	SEC Rule 17a-4 (Electronic Recordkeeping Requirements)	**17 CFR § 240.17a-4(f):** Immutable storage, indexed retrieval, and 3-year retention of business communication.	Captures and stores high-fidelity digital images of all printed client correspondence in a local, indexed, WORM-compliant storage array.
Ark Citadel & Ark Node	Florida HB 473 (Cybersecurity Incident Liability Act), FDBR Data Security Mandates	**HB 473:** Data breach safe harbor and tort liability protections for aligned entities.	Implements a physical-boundary security program that aligns with NIST CSF and CIS Controls, satisfying the burden of proof for tort safe harbor.
M5 Display Terminal (110)	Florida SB 482 (AI Transparency Rules)	**SB 482:** Right to know when communicating with an artificial intelligence system or chatbot.	Displays persistent on-screen notices and disclosures to the local operator during active AI sessions, fully satisfying transparency requirements.
YubiKey physical validation	FDBR Access Controls, SEC Rule 17a-4 Audit Integrity	**FDBR § 501.702:** Implement appropriate technical and administrative security measures.	Restricts cluster access and Cloudflare SASE tunnel authorization to physically present, hardware-token verified operators.

Florida Senate Bill 482 (Artificial Intelligence Bill of Rights)

The legislative landscape surrounding artificial intelligence in Florida is defined by Senate Bill 482, titled the "Artificial Intelligence Bill of Rights" [1]. Sponsored by Senator Tom Leek, the bill was filed on December 22, 2025, and passed the Senate Commerce and Tourism and Appropriations Committees favorably. On March 4, 2026, the bill passed the Senate floor by a vote of 35–2 as amended [1]. However, it died in Messages in the House of Representatives on March 13, 2026, upon the conclusion of the regular session [1]. Despite failing to pass into law, the bill's provisions represent a key compliance benchmark for modern AI systems:

- **Companion Chatbots and Minors:** The bill proposed that companion chatbot platforms must prohibit minors under 17 from creating accounts without verified parental or guardian consent. It also mandated that platforms provide parents with access to interaction histories and provide options to limit use. Furthermore, the platform would be required to display periodic pop-up reminders and hourly warnings informing the user that the companion chatbot is artificially generated.
- **Governmental Procurement Restrictions:** Starting July 1, 2026, governmental entities would be prohibited from extending or renewing contracts for AI technologies with vendors owned by, controlled by, or headquartered in foreign countries of concern (including China, Russia, Iran, North Korea, Cuba, Venezuela, and Syria). Such vendors would be required to submit sworn affidavits attesting to compliance.
- **Commercial NIL Protections:** The bill proposed amending Florida's existing Name, Image,

and Likeness (NIL) statute to prohibit the unauthorized use of generative AI to create or publish synthetic depictions of an individual for commercial purposes without written consent.

- **Educational AI Tool Framework:** The bill outlined structured guidelines for AI instructional tools in educational settings, restricting access before Grade 6 unless directed and supervised by school personnel. It also required educational entities (including private schools and VPK providers) to provide parents with read-only access to student AI interactions.

By using the **Ark Citadel** M4 Logic Module to sanitize data and strip executable code or synthetic images before routing, the Sovereignware™ and Trinary Bound™ architecture allows organizations to meet these standards. This localized control ensures that no synthetic likenesses or unverified student metadata can be transmitted to external cloud systems.

Florida House Bill 473 (Cybersecurity Incident Liability Act)

Originally passed by the Florida Legislature on March 5, 2024, but vetoed by Governor Ron DeSantis on June 26, 2024 [2], due to concerns about limiting consumer recourse after data breaches, House Bill 473 remains a key framework for cybersecurity compliance planning in Florida. The bill proposed a legal safe harbor (immunity from tort claims like negligence) for counties, municipalities, and private "covered entities" or third-party agents that experience a data breach, provided they meet specific criteria:

1. **Notification Compliance:** The entity must substantially comply with the individual, regulatory, and consumer reporting agency notice requirements of Florida's data breach notification law, the Florida Information Protection Act (FIPA).
2. **Framework Alignment:** The entity must adopt and maintain a cybersecurity program that "substantially aligns" with a recognized industry standard or framework, such as NIST CSF, CIS Critical Security Controls, ISO 27001, HITRUST CSF, FedRAMP, HIPAA Security Rule, or GLBA Title V.
3. **Prompt Updates:** The cybersecurity program must be updated within one year of any revisions to the selected industry standard or framework.

Importantly, the bill noted that the failure of an entity to implement such a program is not admissible as evidence of negligence and does not constitute negligence per se. The burden of proof remains on the defendant to establish substantial compliance, which can be demonstrated through internal or third-party assessment documentation. The Sovereignware™ and Trinary Bound™ platform is designed to align with NIST CSF and CIS Controls, helping firms meet the documentation requirements necessary to claim safe harbor protections under these standards.

SEC Rule 17a-4 Electronic Recordkeeping Requirements

For wealth management firms and broker-dealers, maintaining compliant electronic records is governed by SEC Rule 17a-4 under the Securities Exchange Act of 1934. Amended in October 2022, the rule modernized recordkeeping by replacing rigid technical requirements with two distinct compliance pathways:

- **WORM Format:** Maintaining records on Write-Once, Read-Many (WORM) storage media, where data cannot be overwritten or deleted.
- **Audit-Trail Method:** Utilizing an electronic recordkeeping system that maintains a complete, unalterable log of all modifications and deletions, with the ability to reconstruct accurate audit trails throughout the record lifecycle.

The rule mandates specific retention periods (typically 3–6 years depending on record type). Additionally, any third party maintaining these records must file a written undertaking with the SEC promising to permit examinations and promptly furnish complete copies. Alternatively, larger firms may appoint a Designated Executive Officer (DEO) to assume personal responsibility for record accessibility. All records and audit trails must be furnished in a "human-readable and reasonably usable electronic format" upon regulatory request.

The Trinary Bound™ platform meets these electronic recordkeeping requirements through its integrated, physically isolated SSD volume. By maintaining an indexed, tamper-proof audit trail of processed queries, the local storage node satisfies the audit-trail pathway, while the optional High-Assurance Enterprise Materialization loop satisfies the WORM pathway by committing indexed scans directly to the secure RAID archive.

Architectural Comparison Matrix

To evaluate the operational differences between the Sovereignware™ + Trinary Bound™ hybrid HaaS models, standard centralized cloud SaaS architectures, and fully localized air-gapped systems, the table below provides a structured technical comparison:

Architectural Metric	Centralized Cloud SaaS Model	Fully Air-Gapped Local System	Sovereignware™ + Trinary Bound™ Hybrid HaaS
Physical Isolation Boundary	None; data is processed in multi-tenant cloud data centers.	Absolute; system is physically disconnected from external networks.	**Hardened Boundary:** Ephemeral physical-path processing with local 3-SSD isolation.
Outbound Port Exposure	Open inbound/outbound ports; prone to remote network attacks.	Zero; no network connections are permitted.	**Zero Inbound Ports:** Uses outbound-only Cloudflare SASE tunnels.
Compute Scaling Capacity	Elastic cloud-scale compute utilizing advanced GPU ensembles.	Constrained by local on-premises hardware and thermal limitations.	**SaaS-HaaS Hybrid:** Integrates sandboxed GDC remote GPU compute with local edge models.
Metadata & Telemetry Security	Voluminous telemetry is collected by platform and OS providers.	Zero telemetry leakage.	**Telemetry-Free:** Stateless host RAM execution cuts off all out-of-band diagnostics.
Regulatory Compliance Fit	Low; data exposure risks complicate compliance with SB 482 and FDBR.	Compliant with local mandates but lacks off-site replication and searchability.	**High Compliance:** Meets SB 482 disclosures, HB 473 security safe harbor, and SEC 17a-4 WORM mandates.

Targeted Peer-Review Publication Recommendations

To establish broader scientific validation for the Sovereignware™ and Trinary Bound™ architecture, this whitepaper is prepared for submission to peer-reviewed journals. Four publication venues across the legal, cybersecurity, and data protection fields are recommended:

International Data Privacy Law (IDPL)

- **Editorial Scope:** Published by Oxford University Press, this journal focuses on data protection, privacy law, and technical policy implementations worldwide.
- **Analytical Alignment:** Highly suited for evaluating the hybrid SaaS + HaaS state-machine transition model against regional data governance laws (such as the Florida Digital Bill of Rights and the EU GDPR).
- **Indexing Metrics:** Indexed in Scopus, legal databases, and major academic directories.

Computer Law & Security Review

- **Editorial Scope:** A premier international journal examining the intersection of computer law, cybersecurity, forensic engineering, and data security standards.
- **Analytical Alignment:** Ideal for publishing the physical path mechanics of "The White Stone Protocol," including the kinetic touch gate, CalDigit hardware bus, and Cloudflare SASE tunnel integrations.
- **Indexing Metrics:** h5-index of 48, h5-median of 83.

Berkeley Technology Law Journal (BTLJ)

- **Editorial Scope:** A leading technology-focused law review exploring intellectual property, patent litigation, state-level technology regulation, and emerging technical policy.
- **Analytical Alignment:** Well-suited for analyzing U.S. Patent Application No. 19/458,785 in relation to Florida's SB 482 and HB 473 legislative histories.
- **Indexing Metrics:** Ranked highly among US law and technology journals; h5-index of 23, h5-median of 35.

Journal of Data Protection & Privacy

- **Editorial Scope:** Published by Henry Stewart Publications, this peer-reviewed journal focuses on applied research, regulatory compliance audits, and practical data protection frameworks.
- **Analytical Alignment:** Excellent fit for demonstrating compliance with SEC Rule 17a-4 electronic recordkeeping requirements and the HB 473/NIST CSF security alignment for financial and legal services.
- **Indexing Metrics:** Listed and indexed in Cabell's Directories and Scopus.

Novel Contribution and Positioning

The Sovereignware™ + Trinary Bound™ architecture introduces a distinct paradigm that differentiates it from existing approaches:

- **Physical-Boundary Security Model**: Rather than relying exclusively on software-based TEEs or complete network disconnection, the architecture enforces security through verifiable physical state transitions and hardware-rooted controls (YubiKey kinetic gate, physical air-gap disconnection, and outbound-only zero-trust networking).
- **Hybrid Intelligence Placement**: AI execution is deliberately tiered — lightweight models run on the edge M5 Ambassador, sensitive orchestration remains on the local Compute Node,

and heavy reasoning is offloaded only to cryptographically attested remote TEEs after remote attestation succeeds.
- **Formal Multi-Phasic Data Lifecycle**: Data is explicitly transitioned through Steam → Water → Stone states with corresponding physical isolation, providing auditable boundaries that map directly to regulatory requirements for data minimization, retention, and privilege protection.
- **Hardware-Rooted Trust Chain**: From YubiKey physical presence validation to remote attestation of cloud TEEs, every transition point requires either physical human verification or cryptographic proof of environment integrity.

This combination positions the platform as a production-ready solution for organizations that require both frontier AI capabilities and verifiable data sovereignty — a segment currently underserved by pure cloud confidential computing offerings and traditional air-gapped systems.

Limitations and Trade-offs

While the Sovereignware™ + Trinary Bound™ architecture offers significant security advantages through physical-boundary controls, it also introduces important trade-offs that organizations should consider:

- **Increased Complexity and Cost:** The hybrid SaaS + HaaS model, physical hardware requirements (custom Faraday briefcase, active cooling, YubiKey authentication, multi-SSD topology), and specialized configuration increase both capital and operational expenditure compared to standard cloud SaaS deployments.
- **Scalability Constraints:** Local edge processing and physically isolated storage inherently limit horizontal scaling and geographic elasticity relative to public cloud environments.
- **New Failure Modes:** Reliance on physical components (Thunderbolt cabling, YubiKey tokens, briefcase hardware, power and cooling systems) introduces logistical and single-point-of-failure risks not present in fully cloud-native architectures.
- **Regulatory Uncertainty:** Several Florida legislative measures referenced in this paper (including SB 482 and HB 473) did not become law. Organizations should treat referenced compliance pathways as illustrative rather than guaranteed and monitor ongoing legislative developments.
- **Patent Status:** The core architecture described herein is the subject of a pending U.S. patent application and has not yet been granted patent protection.

These limitations do not negate the security and compliance benefits of the design but should inform risk assessments and deployment decisions, particularly for high-volume or geographically distributed use cases.

Conclusions and Strategic Roadmap

The Sovereignware™ + Trinary Bound™ architecture demonstrates that the seemingly contradictory demands of advanced artificial intelligence and strict data sovereignty can be resolved through physical-boundary security design. By utilizing the **Ark Citadel** and **Ark Node** topology, the platform establishes a hardware-rooted boundary that isolates data processing within a physically verifiable environment.

Through the integration of telemetry-free edge interfaces, secure outbound tunnels, sandboxed cloud-based inference, and physical authentication keys, the platform allows highly regulated enterprises to utilize modern AI capabilities while remaining compliant with regional and federal regulations. This hybrid design provides a robust, verifiable framework for secure data processing, ensuring that sensitive information remains protected at the physical boundary.

About Hectec Labs / Sovereignware™

Hectec Labs develops sovereign AI infrastructure that combines physical-boundary hardware security with hybrid cloud intelligence. The Trinary Bound™ platform is protected under U.S. Patent Application No. 19/458,785 and related filings. For enterprise inquiries, pilot deployments, or regulatory alignment consultations, contact the architecture team via the secure portals at hq.trinarybound.com or sovereignware.org.

This document is provided for technical and compliance evaluation purposes. All specifications, pricing, and regulatory mappings are subject to change based on final manufacturing validation and legislative developments.

References

1. Florida Senate, CS/SB 482: Artificial Intelligence Bill of Rights (2026 Regular Session), https://www.flsenate.gov/Session/Bill/2026/482 (last visited June 11, 2026) (bill passed Senate 35–2 on March 4, 2026; died in House Messages on March 13, 2026).
2. Florida House of Representatives, HB 473: Cybersecurity Incident Liability (2024 Regular Session), https://www.flsenate.gov/Session/Bill/2024/473 (vetoed by Governor Ron DeSantis on June 26, 2024).
3. U.S. Patent Application No. 19/458,785 (filed January 24, 2026), claiming priority to U.S. Provisional Application No. 63/926,688 (filed November 27, 2025) (application pending; no patent has been granted as of the date of this whitepaper).
4. Securities and Exchange Commission, Electronic Recordkeeping Requirements for Broker-Dealers, 17 C.F.R. § 240.17a-4 (as amended 2022).
5. Florida Digital Bill of Rights, Fla. Stat. §§ 501.701–501.722 (2023) (data minimization and sensitive data processing requirements).
6. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0 (2024).
7. U.S. Copyright Office, First Sale Doctrine, 17 U.S.C. § 109.
8. Lanham Act § 43(a), 15 U.S.C. § 1125(a) (prohibition on reverse passing off and false designation of origin).
9. AMD, SEV-SNP: Strengthening VM Isolation with Integrity Protection and More, AMD Technical Document (2023).
10. Cloudflare, Cloudflare One SASE Architecture Documentation, https://developers.cloudflare.com/cloudflare-one/ (accessed June 2026).

Conflicts of Interest / Author Affiliation

Hector Jose Cabrera is the founder and sole director of Hectec.ai Inc., the Delaware C Corporation that owns the intellectual property described in this whitepaper. This document reflects both technical design decisions and the commercial interests of the author's company. All technical claims are presented in good faith but should be independently verified by readers prior to deployment in production environments.

Document Information

Version: 1.0
Date: June 11, 2026
Owner: Hectec.ai Inc. (Delaware C Corporation)
Intellectual Property Status: Formal assignment from the inventor, Hector Jose Cabrera, to Hectec.ai Inc. has been executed and documented through an Intellectual Property Assignment Agreement and Unanimous Written Consent of the Sole Director and Shareholder (dated June 2026), ratifying prior corporate actions taken in December 2025.