

Trinarybound.com

Sovereignware.org

sovereign-ware.com

DMHfl.com

hectec.ai

Security was the foundation. The assistant was built on top of it.

“We let the AI work the outside. The proof stays inside.”

Publisher: HecTec.ai Inc. (Delaware C-Corp) · **Deployment & Stewardship:** DMH (DMHFL.com | Winter Park, FL) · **Intellectual Property:** U.S. Utility Patent Application 19/458,785 (Trinary Bound™) · **Key Trademarks:** Sovereignware™, Trinary Bound™, Embassy Tunnel™, Steward Marketing™, Steward Key™

The Core Thesis: “Security was the foundation. The assistant was built on top of it.”

“We let the AI work the outside. The proof stays inside.”

The enterprise AI boom presented regulated industries and national security environments with an untenable bargain: surrender sensitive client files, privileged financial ledgers, litigation work product, or mission telemetry to multi-tenant cloud data centers, or fall permanently behind in operational velocity.

For wealth advisors, multi-family offices, defense contractors, medical practices, and boutique law firms, commercial Software-as-a-Service (SaaS) AI is an existential liability. Terms of service are not cryptographic guarantees. Data loss prevention (DLP) filters applied post-hoc are leaky abstractions.

Most software vendors spend their initial years shipping features and promise to reach “secure-by-design” later. HecTec.ai inverted that timeline: spending its first eight months engineering a zero-trust, client-owned security substrate—and only then building the autonomous AI assistant on top of it.

Your documents never leave your building. A sanitized forensic twin—containing only logic, mathematical abstractions, and de-identified code—is the only artifact that ever encounters a frontier cloud model. The response returns home and is reconstructed locally.

Mathematical certainty replaces corporate trust.

Executive Summary: Autonomous Intelligence on Iron You Own

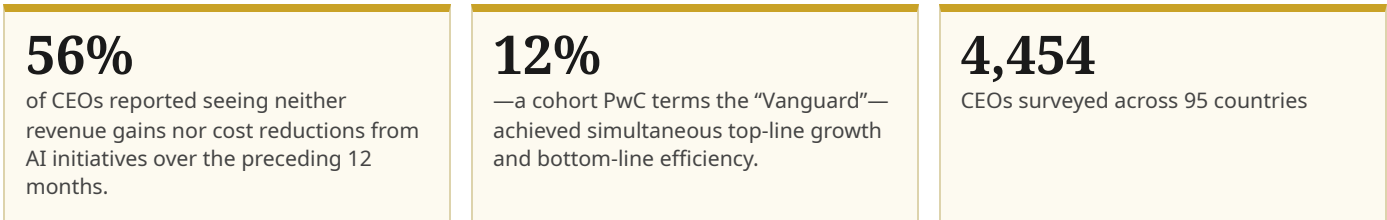
Sovereignware™ is an on-premises AI operating system engineered exclusively for organizations that cannot afford to leak.

Unlike SaaS wrappers that ingest confidential enterprise records into multi-tenant clusters, Sovereignware™:

- Runs entirely on client-owned physical hardware (standardized today on Apple Silicon; Dell and NVIDIA substrate variants currently in engineering).
- Integrates directly into existing legacy infrastructure (email, document management, practice suites, operational ledgers) without migration, re-platforming, or staff retraining.
- Over-achieves regulatory and defense compliance mandates, structurally fulfilling statutory requirements for the SEC (Rule 17a-4 / 206(4)-7), FINRA (Rule 4511), and Department of the Air Force / AFWERX dual-use zero-trust standards (NIST SP 800-171, CMMC 2.0 Level 2/3, DoD Zero Trust Reference Architecture).
- Is managed by dedicated, named human stewards—licensed HecTec Sovereign AI Engineers accountable for uptime, custom integrations, and system hygiene. Stewards are there to help build apps and integrations with legacy platforms to automate the executive’s and enterprise’s bottlenecks.
- Eliminates vendor hostage-taking: If you part ways with us, the hardware, software instances, and cryptographic journals remain in your custody, fully functional.

Why Most Enterprise AI Deployments Stall

According to PwC’s 29th Global CEO Survey (surveying 4,454 CEOs across 95 countries):



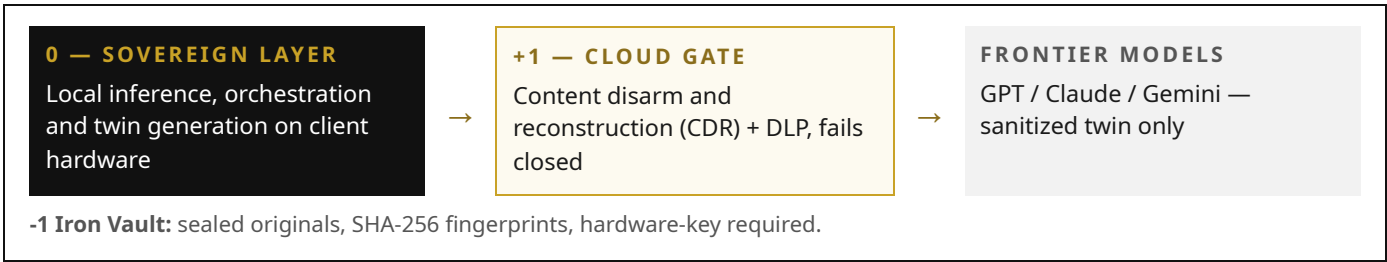
The root cause identified by the survey is decisive: isolated, tactical AI pilots and generic SaaS chatbots fail to move the needle because they are severed from actual workflows and forbidden from touching core, confidential records.

Sovereignware™ was engineered to bridge that exact divide: enterprise-grade agentic automation wired directly into production data, operating on owned hardware behind ironclad security boundaries, overseen by accountable human operators.

Architectural Breakthrough: Trinary Bound™

The fundamental vulnerability of modern cloud architecture is the single-boundary model: if an attacker or prompt injection breaches the container, the entire database is exposed.

The Trinary Bound™ architecture (patent-pending, U.S. Utility Patent Application 19/458,785) physically isolates every deployment across three distinct nodes: Node -1 Iron Vault (sealed originals, SHA-256 fingerprints, hardware-key required), Node 0 Sovereign Layer (local inference, orchestration and twin generation on client hardware), Node +1 Cloud Gate (content disarm and reconstruction (CDR) + DLP, fails closed), connecting to frontier cloud models (GPT/Claude/Gemini).



- Node +1: The Cloud Gate (The DMZ).** Every inbound and outbound byte is intercepted. Inbound files are scanned across six distinct threat vectors using Content Disarm and Reconstruction (CDR). Outbound requests are stripped of all Personally Identifiable Information (PII), client names, matter numbers, and sensitive context. If the de-identification stripper fails for any reason, the gate fails closed—no data escapes.
- Node 0: The Sovereign Layer (The Engine).** Hosted on client-owned premises. Local inference models and orchestration run directly on local silicon. This layer accepts queries, references local indices, generates the anonymous “forensic twin” (logic, code, and math only), routes the sanitized payload through the Cloud Gate, and re-stitches the returned intelligence with local records at the Sovereign Bridge.
- Node -1: The Iron Vault (The Fortress).** Original, unaltered source records are sealed here under SHA-256 cryptographic fingerprints. The Vault is decoupled from remote execution environments. Retrieving or exporting original records requires a physical hardware-key touch (FIDO2/U2F). Even in the event of a remote takeover of Node +1 or Node 0, the compromise is contained; the Vault cannot be scraped over a network socket.

Field Scenario: How It Works in Practice

Consider a partner at a boutique law firm reviewing an unannounced cross-border acquisition:

- **Intake & Hashing** — the partner drops a confidential 180-page draft purchase agreement into their existing document repository. Node -1 seals the PDF, computing an immutable SHA-256 hash.
- **De-Identification** — Node 0 extracts the core covenants, indemnification caps, and antitrust formulas, replacing real party names, transaction amounts, and geographic markers with structured cryptographic tokens.
- **Frontier Reasoning** — Node +1 validates that no PII exists and forwards the abstract mathematical and structural logic to frontier cloud models (e.g., Claude, GPT) to analyze clause parity.
- **Local Re-Stitching** — the cloud models deliver structural feedback. Node 0 re-maps the confidential entity names back to the text on the firm’s physical machine.
- **Human Approval** — Sovereignware™ drafts the redlined counter-proposal. The system halts. It does not send, file, or export the document until the partner provides an explicit one-touch signature. The cloud vendor processed the legal logic. They never learned who was buying whom, for how much, or under which jurisdiction.

Auditory Over-Achievement: SEC, FINRA & Military/AFWERX Alignment

Standard enterprise software attempts compliance through administrative policy, non-disclosure agreements, and post-event human attestations. Sovereignware™ was engineered to over-achieve statutory and military compliance requirements by replacing human promise with deterministic, mathematical boundaries.

Statutory / regulatory mapping	Sovereignware™ implementation
SEC Rule 17a-4 / 206(4)-7 (WORM Storage)	Immutable Append-Only SHA-256 Hash Chain
FINRA Rule 4511 (Tamper-Proof Records)	Physical FIDO2 Hardware-Key Retrieval
DoD / AFWERX Zero Trust Pillars	Trinary Bound™ Physical Node Segregation
NIST SP 800-171 / CMMC 2.0 (CUI Defense)	Outbound-Only Embassy Tunnel™ (Zero Inbound)

1. SEC & Financial Auditory Standards (SEC Rule 17a-4, Rule 206(4)-7, FINRA 4511)

- **Cryptographic WORM Architecture:** Sovereignware™ commits every transaction, prompt payload, document revision, and agentic action to a local, append-only SHA-256 hash chain — tamper-evident proof that exceeds SEC Rule 17a-4(f) requirements.
- **Immediate, Unmediated Retrieval:** records and verification ledgers reside entirely on client-owned iron; compliance officers extract complete audit histories in real time.
- **Privileged Fiduciary Isolation (ABA Model Rule 1.6(c)):** external cloud APIs analyze only synthetic forensic twins — client confidences never cross public multi-tenant networks.

2. Department of the Air Force / AFWERX & DoD Zero Trust Alignment

- **CUI & ITAR Defense:** Node -1 enforces cryptographic isolation of raw schematics and mission data.
- **Hardware-Bound Authentication (DoD User Pillar):** FIDO2/U2F physical touch required for raw data egress.
- **Outbound-Only Perimeters (DoD Network & Environment Pillar):** the Embassy Tunnel™ operates exclusively on outbound TLS tunnels with zero open inbound listening ports.
- **Blast-Radius Containment (DoD Workload Pillar):** fails closed; lateral movement physically blocked at hardware boundaries.
- **DDIL:** local inference continues in contested or air-gapped environments even when cloud connectivity is severed.

Adversarial Threat Model & Blast-Radius Containment

Threat	Containment
Indirect Prompt Injection (Node +1)	CDR strips executable macros/scripts; gate fails closed.
PII/CUI Exfiltration (Node +1)	air-gapped tokenization; cloud models cannot leak what they never receive.
Physical Hardware Theft (Node -1)	hardware enclave encryption; decryption requires physical FIDO2 biometrics.
Rogue Steward / Remote Takeover (Embassy Tunnel™)	outbound-only pull protocol; zero inbound listeners; HMAC-verified signed work orders.
Audit Ledger Tampering (System Logs)	append-only SHA-256 hash chaining; tampering corrupts the chain and alerts compliance immediately.

Cryptographic Proof, Not Legal Promises

- **SHA-256 Hash Chain:** every action committed locally; verification is standard arithmetic (shasum -a 256), no proprietary tooling required.
- **HMAC-Signed Bridge:** signed unidirectional bridge to enterprise ecosystems (Google Workspace, Microsoft 365); the sovereign node holds zero third-party credentials.
- **Embassy Tunnel™:** approved remote steward diagnostics through a single guarded door — outbound-only Cloudflare Tunnels, zero inbound firewall ports; remote agents pull cryptographically signed work orders; client entities leave only as de-identified placeholders.
- **100% Audit-Ready Evidence:** locally generated logs provide court-admissible chain-of-custody evidence.

Steward Marketing™: Thought Leadership Impact, Attribution & Leads Without Surveillance

- HecTec.ai operationalized Steward Marketing™ — a zero-surveillance growth and telemetry architecture measuring thought-leadership impact and verifiable lead attribution on 100% first-party infrastructure. Four stages:
1. **Deterministic Attribution & Active Workflows** — cryptographically signed first-party UTM parameters; Cloudflare R2 + database engine instantiate stateful workflows. Zero ad pixels.
 2. **The Authenticator Anchor (Steward Key™)** — identity bound through a Steward Cryptographic Key in the user's own authenticator app; self-sovereign identity, no cookies.
 3. **Behavioral Telemetry Without Surveillance** — touchpoints logged against the active workflow; no IP dossiers, no device fingerprints.
 4. **Verified Attribution & Thought Leadership ROI** — mathematically provable lead origin, pipeline velocity, and conversion attribution.

Trust by Design: Operationalizing the CISA Principles

CISA Secure by Design pledge goal	Sovereignware™ implementation
Increase MFA	FIDO2 hardware-key touch for vault retrieval; authenticator-anchored steward keys.
Eliminate Default Passwords	zero default credentials; client-generated, client-held keys from day one.
Reduce Vulnerability Classes	three-tier physical segregation; fail-closed PII stripper.
Make Patching Seamless	named human stewards (licensed HecTec Sovereign AI Engineers) maintain deployments directly.
Radical Transparency	arithmetic audit trails; plain statements of what we do not claim.
Intrusion Evidence	append-only SHA-256 hash chaining makes tampering mathematically obvious.

What We Do Not Claim

CISA does not endorse or certify commercial products, and HecTec.ai has not sought third-party government accreditation. We claim structural alignment with secure-by-design guidelines. We supply tamper-evident forensic tools; your firm remains the ultimate custodian of its compliance obligations.

The Sovereign Continuity Covenant: Zero Dead-Man Switches

- **Hardware Ownership:** deployments run on client-owned hardware; end the engagement and your system keeps running.
- **No Remote Kill Switches:** zero remote kill switches, timed de-authorization, or cloud license heartbeats.
- **Open Verification:** every ledger verified with open-source arithmetic (shasum -a 256).
- **Approval-First Operations:** agents prepare, draft, calculate, and stage — then pause. Nothing is submitted, charged, or dispatched without explicit approval from your designated team. Note: approval rests with the client's own designated approver, never with DMH — stewards are the build team and safety net, not a checkpoint.

Deployment & Economics: The Sovereign Model

- **Executive Pilot Cohort:** Fall Cohort enrollment closes Saturday, October 31, 2026 — seven seats. Your ArkNode is live as soon as 7 days after enrollment, and no later than 14.
- **Deployment Fee:** \$1,999 one-time setup (includes ArkNode provisioning; client supplies Mac mini or DMH procures at cost + \$75 installation and travel).
- **Subscription:** \$333/month or \$999/quarter Managed Retainer, charged at enrollment with your package so your steward is active from day one.
- **Steward Key™:** issued at enrollment into your own authenticator app; your steward checks its 6-digit code before acting on your requests.
- **Inclusions:** complete on-premises deployment, legacy software integration, swarm agent workflows, local/connected CRM with Steward Marketing™ attribution, dedicated steward engineering support.
- **Enroll:** dmhfl.com/cohort

Media Inquiries & Private Briefings: DMH Systems & Engineering, Winter Park, Florida. Direct: (407) 329-4499. Executive Portal: DMHFL.com. Corporate: HecTec.ai Inc. (Delaware C-Corp | HecTec.ai). Briefing inquiries: briefing@dmhfl.com | press@hectec.ai.

THE SOVEREIGNWARE™ ECOSYSTEM

hectec.ai — HecTec.ai Inc., the company (Delaware C-Corp)

sovereign-ware.com · sovereignware.org — the Sovereignware™ operating system product site (white papers live here)

trinarybound.com — the Trinary Bound™ architecture, patent, and licensing

dmhfl.com — DMH Florida, deployment & stewardship partner (Winter Park, FL)

Sources: PwC, 29th Global CEO Survey — [pwc.com/gx/en/issues/c-suite-insights/ceo-survey.html](https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey.html). CISA Secure by Design Pledge — [cisa.gov](https://www.cisa.gov). Sovereignware™ / Trinary Bound™ / Embassy Tunnel™ / Steward Marketing™ / Steward Key™ are trademarks of HecTec.ai Inc.; deployed & stewarded by DMH.