INTRODUCTION: PROOF OF WORK

A Technical Portfolio by David Culp

In an industry often defined by fleeting certifications and vendor-specific exams, I have spent the last 35 years focused on a different standard: **Demonstrable Results.**

This portfolio serves as a "Technical Binder" of my career. It is a curated collection of architectures, codebases, and case studies that document my journey from the physical foundations of networking in 1992 to the deployment of local, privacy-first Artificial Intelligence in 2025.

The Philosophy of the "Sovereign Architect"

My approach to IT is guided by three core principles:

1. **Resilience is Mandatory:** Whether it is a 32-site SD-WAN failover or a High-Availability Proxmox cluster, I build systems that survive.
2. **Data Sovereignty:** In healthcare, privacy isn't just a policy; it's a moral obligation. I specialize in building "Local-First" tools (OpenClinical-AI, OpenCompliance-AI) that keep sensitive data out of the cloud and under the owner's control.
3. **Resourceful Engineering:** I believe the best solution isn't always the most expensive one. My "Conference Room" project demonstrates how E-waste can be transformed into high-fidelity A/V-over-IP infrastructure through pure technical ingenuity.

How to Navigate This Document

Each section of this binder corresponds to a pillar of modern enterprise IT. You will find more than just summaries; you will find the **logic** behind the work—including IP schemas, network diagrams, and code architecture.

- **Exhibits I–III (Infrastructure):** Standardized networking at scale and private cloud resilience.
- **Exhibits IV–V (Intelligence):** Software engineering using Python and Local LLMs to solve GRC and Clinical needs.
- **Exhibit VI (Ingenuity):** A case study in maximizing ROI through hardware repurposing and MDM management.

> *"The pulse of a network is felt at Layer One, but its value is realized at the Application Layer. I have spent my career mastering everything in between."*

DAVID CULP: ARCHITECTURAL PORTFOLIO (2025)

35 Years of Infrastructure, Security, and AI Proof-of-Work

Exhibit	**Focus Area**	**Industry Benchmark Equivalent**
I. Enterprise SD-WAN Transformation	Large-Scale Networking & Resilience	**CCNP / Fortinet NSE-7**
II. The Autonomous Datacenter	SecOps, Identity & Orchestration	**CISSP / CISM**
III. High-Availability (HA) Compute	Private Cloud & BC/DR Logic	**VCP (VMware) / Nutanix**
IV. OpenCompliance-AI (GRC Tool)	Software Engineering & GRC	**CISA / CISM**
V. OpenClinical-AI (Medical LLM)	Clinical Informatics & AI Engineering	**Azure/AWS AI Specialist**
VI. The $1 Conference Suite	Resourceful Engineering & MDM	**A/V-over-IP Specialist**

Exhibit I: Enterprise SD-WAN & Network Standardization

- **The Work:** Architected a 32-site healthcare network utilizing **Fortinet SD-WAN** and **AT&T FirstNet 5G** failover.
- **Evidence:** [32-Location MPLS Map] | [Global IPAM Schema Spreadsheet]
- **Result:** Achieved 100% clinical uptime and established a "Clinic-in-a-Box" deployment model that reduced site launch time by 80%.

Exhibit II: The Autonomous Hybrid-Cloud Datacenter

- **The Work:** A 6-layer implementation of **Zero-Trust** security using **Ansible** for self-healing automation and **ELK Stack** for SIEM visibility.
- **Evidence:** [The Autonomous Datacenter Deployment Guide] | [GCP Secure Email Gateway SOP]
- **Result:** Eliminated manual configuration drift and centralized identity across all endpoints via FreeIPA/RADIUS.

Exhibit III: High-Availability Proxmox Cluster Engineering

- **The Work:** Engineered a 3-node HA cluster using **ZFS Replication** and **Fencing/Quorum** logic.
- **Evidence:** [Proxmox HA Lab Demo & "Pull-the-Plug" Failover Test Documentation]
- **Result:** Verified <120 second automated failover for mission-critical VMs without a shared SAN.

Exhibit IV: OpenCompliance-AI (NIST 800-53 Engine)

- **The Work:** Built a local-first GRC tool using **Python (FastAPI)** and **Ollama (Mistral-Nemo)** to automate NIST assessments.
- **Evidence:** [GitHub Repository: OpenCompliance-AI]
- **Result:** Replaced expensive cloud GRC tools with a private, AI-assisted auditing engine that ensures 100% data sovereignty.

Exhibit V: OpenClinical-AI (Deterministic Medical Analyst)

- **The Work:** Developed a privacy-first AI workstation that uses **SQL-Augmented Generation** to analyze C-CDA XML medical records.
- **Evidence:** [GitHub Repository: OpenClinical-AI] | [LinkedIn Proof-of-Concept]
- **Result:** Solved the "Context Wall" hallucination problem in healthcare AI by utilizing deterministic lookups instead of standard vector RAG.

Exhibit VI: The $1 Professional Conference Suite (NDI)

- **The Work:** Engineered a professional A/V-over-IP suite by repurposing E-waste mobile hardware via **NDI** and **Hexnode MDM**.
- **Evidence:** [Conference Room Tests Presentation]
- **Result:** Delivered $20k+ functionality at near-zero cost while maintaining absolute network isolation on a dedicated media VLAN.

Digital Access & Contact

- **GitHub:** github.com/davidculp-tech
- **LinkedIn:** linkedin.com/in/david-c-13682186/
- **Contact:** david.culp@davidculp.tech | (205) 340-4549

EXHIBIT I: Enterprise SD-WAN Transformation & Zero-Trust Architecture

Organization: Cahaba Medical Care (FQHC)

Scale: 32 Multi-State Clinical Locations | 2500+ Endpoints

Architect: David Culp, Principal Solutions Architect

---

1. EXECUTIVE SUMMARY

In response to a hyper-growth phase (expanding from 7 to 32 sites), I architected a unified, resilient network infrastructure to replace a fragmented patchwork of consumer-grade DSL and cable connections. The objective was to eliminate downtime, ensure HIPAA/HITECH compliance, and create a scalable "Clinic-in-a-Box" deployment model.

---

2. THE CHALLENGE

- **Operational Risk:** Clinical sites faced frequent "dark periods" due to unreliable local ISPs, stopping patient care and EHR access.
- **Security Gaps:** Lack of centralized visibility made consistent firewall policy enforcement and threat detection impossible.
- **Scaling Bottlenecks:** Manual configuration of new sites was slow, prone to "configuration drift," and required excessive on-site engineering hours.

---

3. THE ARCHITECTURAL SOLUTION

I engineered a **Zero-Trust SD-WAN** utilizing the **Fortinet Security Fabric** and **AT&T FirstNet** as the backbone for healthcare continuity.

A. Connectivity & Resiliency

- **Primary Path:** Dedicated AT&T MPLS Fiber.
- **High-Availability Path:** Integrated FirstNet LTE/5G Cellular gateways.
- **Logic:** Implemented sub-second automated failover. During a primary fiber cut, the SD-WAN orchestrator maintains active VoIP sessions and EHR data streams without user intervention.

B. Standardized Network Segmentation (The "Clinic-in-a-Box")

To ensure security and auditability, I developed a standardized 6-VLAN logical schema deployed identically across all 32 sites:

VLAN ID	Name	Purpose	Access Control
VLAN 10	Clinical	EHR & Medical Imaging	Zero-Trust (Internal Only)
VLAN 20	Admin	Staff Workstations	RADIUS/MFA Protected
VLAN 100	Servers	Local Proxmox HA Clusters	Isolated / Mgmt Only
VLAN 172	Test	Sandbox & Dev	Air-gapped from Clinical
VLAN 192	BYOD	Guest/Patient Wi-Fi	Internet Only; No LAN Access
VLAN 200	Backup	Offsite ZFS Replication	High-Bandwidth Dedicated

C. Global IP Management (IPAM)

I implemented a hierarchical IP addressing scheme to allow for massive scale and simplified routing. By utilizing a predictable "Golden Schema" (e.g., 10.[Site_ID].x.0/24), we achieved:

- **Global Firewall Policies:** One security policy could be pushed to 32 sites simultaneously.
- **Predictable Troubleshooting:** IT staff can identify device types and locations instantly based on the IP address.

---

4. KEY TECHNOLOGIES

- **Edge Security:** FortiGate Next-Generation Firewalls (NGFW).
- **Wireless:** Ubiquiti UniFi managed access points with WPA3-Enterprise.
- **Identity:** Duo MFA integrated with FreeIPA/RADIUS for "Road Warrior" VPN access.
- **Monitoring:** Centralized "Single Pane of Glass" via FortiManager and ELK Stack for real-time threat maps.

---

5. BUSINESS OUTCOMES

- **100% Uptime:** Successfully maintained clinic operations through regional ISP outages and severe weather events.
- **Deployment Velocity:** Reduced "Time-to-Online" for new clinics from **3 weeks to 48 hours**.

- **Audit Compliance:** Passed all external security audits with zero findings related to network segmentation or unauthorized access.
- **Cost Efficiency:** Repurposed existing hardware for local "Drop Box" vulnerability scanning (OpenVAS), saving thousands in licensing fees.

---

6. TECHNICAL DOCUMENTATION INDEX

- **Network Diagram:** [Link to 32-Site MPLS Map]
- **VLAN Logic:** [Link to Remote Clinic PDF]
- **Configuration Data:** [Link to IPAM Spreadsheet]
- **Code Base:** [GitHub.com/davidculp-tech/OpenClinical-AI]

EXHIBIT II: The Autonomous Hybrid-Cloud Datacenter

Project Scope: 6-Layer Zero-Trust Infrastructure & Automated SecOps

Architect: David Culp, Principal Solutions Architect

Core Objective: To eliminate manual "human-element" errors through Infrastructure as Code (IaC) and self-healing architecture.

---

1. EXECUTIVE SUMMARY

I engineered a production-grade, private-cloud ecosystem designed for maximum autonomy. This architecture integrates **on-premise High-Availability (HA)** clusters with **Cloud-Native security gateways** and **automated vulnerability scanning**. The result is a "Self-Healing" datacenter that manages its own identity, security patching, and disaster recovery failover.

---

2. THE ARCHITECTURAL STACK (The 6-Layer Model)

The environment is structured into six interlocking layers to ensure no single point of failure:

- **Layer 1-2 (Resilient Networking):** Managed via **OPNsense** with strict VLAN segmentation.
- **Layer 3 (Identity & Access):** Centralized **FreeIPA (LDAP/Kerberos)** and **FreeRADIUS** for 802.1X, gated by an **Apache Guacamole** clientless gateway with MFA.
- **Layer 4 (Observability):** A full **ELK Stack (Elasticsearch, Logstash, Kibana)** providing a "Single Pane of Glass" for GeoIP threat maps and patch status.
- **Layer 5-6 (Automation): Ansible** orchestration for drift management and automated Sunday 3 AM maintenance windows.

---

3. CORE TECHNICAL PILLARS

A. High-Availability (HA) Compute Logic

To ensure zero downtime for critical services, I deployed a 3-node **Proxmox HA Cluster**.

- **The "Plug-Pull" Test:** I implemented **ZFS Replication** with 1-minute sync intervals.
- **Result:** Verified sub-120-second automated failover. If a physical node loses power, the cluster detects the loss (Fencing/Quorum) and automatically reboots mission-critical VMs on healthy nodes.

B. Remote Security Operations (The OpenVAS "Drop Box")

I developed a "Headless" vulnerability management solution for remote site auditing.

- **The Hardware:** Repurposed ultra-small form factor nodes (Acer CX13) running **Dockerized Greenbone (OpenVAS)**.
- **The Logic:** A "Call Home" **WireGuard** tunnel that bypasses client-side NAT/Firewalls, allowing for remote internal security audits without on-site configuration.

C. Secure Email Gateway (SEG) on GCP

To bridge local infrastructure with the cloud, I architected a **Proxmox Mail Gateway** on Google Cloud Platform.

- **Innovation:** Bypassed GCP's Port 25 restrictions by leveraging Google’s SMTP Relay (Port 587/TLS).
- **Impact:** Created a secure, authenticated mail pipeline that provides granular, self-hosted security inspection for Google Workspace Enterprise.

---

4. ACHIEVEMENTS & PROOF OF CONCEPT

- **Zero-Trust Identity:** Every service in the datacenter—from SSH to Wi-Fi—requires **LDAP/MFA** authentication.
- **Autonomous Maintenance:** Achieved 100% automated patching across the fleet via **Ansible**, reducing manual admin overhead by an estimated **80%**.
- **Hardened Compliance:** Created a **HIPAA Hardening Script** that validates BitLocker, SMBv1 status, and Audit logging, providing an instant "Pass/Fail" report for auditors.

---

5. TECHNICAL DOCUMENTATION INDEX

- **Deployment Guide:** [Link to The Autonomous Datacenter Guide]
- **HA Logic & POC:** [Link to Proxmox HA Lab Demo]
- **Vulnerability Scanning:** [Link to OpenVAS Drop Box Guide]
- **Cloud Mail Security:** [Link to Google-Native SEG on GCP]

EXHIBIT III: Enterprise High-Availability (HA) Cluster Engineering

Project Scope: 3-Node Hyperconverged Infrastructure (HCI) with ZFS Replication

Architect: David Culp, Principal Solutions Architect

Key Value: Verified <120 second automated failover for mission-critical medical workloads using zero-shared-storage architecture.

---

1. EXECUTIVE SUMMARY

To eliminate hardware single points of failure in a resource-constrained environment, I engineered a **3-node High-Availability cluster** using **Proxmox VE**. Unlike traditional clusters that require an expensive, centralized SAN (Storage Area Network), this architecture utilizes **ZFS Replication** to maintain data synchronization across local NVMe storage. The result is an enterprise-grade "Self-Healing" private cloud built on high-performance, cost-effective hardware.

---

2. THE CHALLENGE

- **Hardware Fragility:** In a standard single-server setup, a motherboard or power supply failure results in a total blackout of clinical services.
- **Storage Bottlenecks:** Centralized SANs are often a single point of failure themselves and introduce significant latency and cost.
- **The "Split-Brain" Risk:** In cluster engineering, if nodes lose communication but stay powered on, they may attempt to write to the same data simultaneously, causing catastrophic corruption.

---

3. THE ARCHITECTURAL SOLUTION

I implemented a robust HA logic stack that prioritizes data integrity and automated recovery.

A. Storage: ZFS Replication (The "No-SAN" Strategy)

- **Frequency:** Configured ZFS-to-ZFS replication jobs to run every **60 seconds**.

- **Benefit:** Ensures that a near-identical copy of the virtual machine's disk exists on all nodes at all times, allowing for rapid recovery without waiting for multi-terabyte data transfers.

B. The Logic: Quorum & Fencing

- **Quorum:** Established a 3-node minimum to ensure a mathematical majority is required before the cluster can make "life or death" decisions about a VM.
- **Fencing (Watchdog):** Configured hardware-level fencing. If a node becomes unresponsive, the cluster "fences" the node to prevent data corruption before restarting services on a healthy node.

---

4. THE "PULL-THE-PLUG" VALIDATION

To prove the resilience of this architecture, I conducted a physical stress test:

1. **Baseline:** Mission-critical VM (EHR Database) running on `pve-01`.
2. **The Event:** Manually disconnected the power supply from `pve-01` during a simulated high-load period.
3. **The Recovery:**
   - **0-60s:** Cluster detects "Node Down" state; Quorum remains maintained by `pve-02` and `pve-03`.
   - **60-120s:** HA Manager marks the node as dead and initiates the boot sequence on `pve-02`.
   - **Result:** Services restored and reachable via network in **under 2 minutes** with zero manual intervention.

---

5. TECH STACK

- **Hypervisor:** Proxmox VE 9.x (Debian-based)
- **Filesystem:** ZFS (RAID-Z1 for local redundancy)
- **Management:** Proxmox Datacenter Manager (PDM) for multi-cluster visibility.
- **Backup:** Proxmox Backup Server (PBS) with deduplication and encryption.

EXHIBIT IV: OpenCompliance-AI (Governance as Code)

Project Scope: Open-Source, Local-First GRC Assessment Engine

Tech Stack: Python (FastAPI), SQLModel, Tailwind CSS, Ollama (Mistral-Nemo)

Core Objective: To replace expensive, cloud-dependent GRC tools with a private, AI-assisted compliance auditor.

---

1. THE PROBLEM: The "Compliance Tax"

Standard GRC platforms are often "security-through-cloud," requiring organizations to upload their most sensitive security gaps to a third-party vendor. For small-to-medium teams, the cost of these tools and the risk of data leakage often lead to "Compliance by Spreadsheet," which is difficult to audit and version control.

2. THE SOLUTION: Local-First AI Auditing

I developed **OpenCompliance-AI**, a lightweight engine designed specifically for **NIST 800-53 Rev. 5** assessments.

Key Architectural Pillars:

- **AI-Assisted Expert Review:** Integrated **Ollama (Mistral-Nemo)** to act as a virtual auditor. The AI evaluates implementation statements against NIST requirements and provides a 2-sentence sufficiency opinion—all running locally to ensure 100% data sovereignty.
- **Maturity-Based Scoring:** Implemented a 5-tier maturity model (Initial to Optimized) that automatically generates "PASS/FAIL/PARTIAL" status badges.
- **Dynamic NIST Catalog Integration:** Developed a custom ingestion engine that seeds a local SQLite database directly from the official NIST CSV catalog, providing instant tooltips and supplemental guidance for auditors.

3. TECH STACK & INTEGRATION

- **Backend Autonomy:** Built with **FastAPI** and **SQLModel**, allowing for sub-millisecond database queries and a clean, interactive API documentation (Swagger/OpenAPI).

- **Frontend Simplicity:** Utilized **Tailwind CSS** and Vanilla JS to maintain a high-performance, framework-agnostic dashboard that can be served from any internal web server.
- **Remediation Mapping:** Built-in tracking for failed controls, allowing teams to document and export **Plan of Action and Milestones (POA&M)** reports directly to PDF.

---

4. IMPACT ON THE "AUTONOMOUS DATACENTER"

OpenCompliance-AI serves as the **Governance Layer** of my 6-Layer Datacenter model.

- While **Ansible** manages the *state* of the servers...
- And **OpenVAS** scans for *vulnerabilities*...
- **OpenCompliance-AI** tracks the *policy maturity*, providing the "Paper Trail" required for HIPAA, SOC2, and NIST audits.

---

5. TECHNICAL DOCUMENTATION INDEX

- **GitHub Repository:** github.com/davidculp-tech/OpenCompliance-AI
- **Demo/SOP:** Included in the *Autonomous Datacenter Deployment Guide*.

EXHIBIT V: OpenClinical-AI (Deterministic Clinical Intelligence)

Project Scope: Local-First Clinical Data Analyst for C-CDA XML

Tech Stack: Python (Streamlit), SQLite, Ollama (Mistral-Nemo), HL7/XML Parsing

Core Objective: To provide clinicians with a queryable, 100% offline "Assistant" that analyzes patient records without risking PHI leakage or hallucination.

---

1. THE PROBLEM: The "RAG" Context Wall

Most AI projects use Vector Databases to "chunk" data. In healthcare, if you chunk a C-CDA file, you might separate a **Medication** from its **Allergy Contraindication**, leading to life-threatening hallucinations. Furthermore, cloud-based LLMs (OpenAI/Claude) are often non-starters for smaller clinics due to the complexity of Business Associate Agreements (BAA) and data sovereignty risks.

2. THE SOLUTION: SQL-Augmented Generation

I abandoned the standard RAG approach in favor of a **Deterministic SQL Lookup** model.

Key Innovations:

- **HL7 Noise Reduction:** Developed a custom XML parser that strips 90% of HL7 syntax noise. This "clean" clinical data ensures the LLM sees only relevant encounters, meds, and labs, maximizing the efficiency of the **Mistral-Nemo** context window.
- **Context Preservation:** By feeding the *entire* cleaned patient record into the model rather than random "chunks," the AI maintains the full clinical context, resulting in **100% accuracy on medication and allergy reconciliation tests.**
- **Local Data Sovereignty:** Powered by **Ollama**, the entire pipeline runs on-premise. This satisfies HIPAA's most stringent privacy requirements because the data never touches the internet.

---

3. INTEGRATION WITH THE "AUTONOMOUS DATACENTER"

OpenClinical-AI is the functional result of the layers below it:

1. **Hardware Layer:** Runs on the **Proxmox HA Cluster** (GPU-accelerated nodes).
2. **Storage Layer:** Data is protected by **ZFS Replication**.
3. **Security Layer:** Access is gated by **Guacamole MFA** and **VLAN Segmentation**.
4. **Application Layer: OpenClinical-AI** turns that raw infrastructure into a life-saving clinical tool.

---

4. IMPACT & AUDIENCE

- **For Clinicians:** Reduces "chart review" time from 20 minutes to 20 seconds.
- **For IT Directors:** Provides a "Doomsday Protocol" for EHR access during ISP outages.
- **For Compliance Officers:** Eliminates the risk of "Cloud PHI" leaks.

---

5. TECHNICAL DOCUMENTATION INDEX

- **GitHub Repository:** github.com/davidculp-tech/OpenClinical-AI
- **Demo:** [Link to LinkedIn Post]

EXHIBIT VI: The $1 Professional Conference Suite

Project Scope: Secure A/V-over-IP via Repurposed Mobile Hardware

Organization: Cahaba Medical Care (FQHC)

Architect: David Culp, Principal Solutions Architect

Key Value: Delivered $20k+ professional conferencing functionality at near-zero hardware cost.

---

1. EXECUTIVE SUMMARY

Faced with the need for high-fidelity, multi-endpoint conferencing in a non-profit environment, I architected a custom **A/V-over-IP (AoIP)** solution. By repurposing "E-waste" (Samsung S21FE mobile devices) and leveraging the **NDI (Network Digital Interface)** protocol, I built a modular, broadcast-quality conference suite. The system provides sub-millisecond latency and professional-grade audio/video without the five-figure price tag of proprietary hardware.

---

2. THE CHALLENGE

- **Budgetary Constraints:** Commercial-grade conferencing solutions (Polycom/Logitech) for 30+ sites were cost-prohibitive.
- **Hardware Waste:** The organization had a surplus of "outdated" FirstNet mobile devices and network switches slated for E-waste.
- **Technical Complexity:** Delivering synchronized, low-latency audio and video over a standard clinical network without causing congestion or security vulnerabilities.

---

3. THE ENGINEERING SOLUTION

I transformed discarded mobile phones into high-definition NDI endpoints, controlled by a central production hub.

A. The NDI & A/V-over-IP Pipeline

- **Visuals:** Each mobile device was configured as an **NDI Camera HX** source, delivering high-bitrate video over the network.
- **Audio:** Integrated USB-C gooseneck and lavalier microphones into the mobile units to serve as distributed "mic arrays."
- **Production Hub:** A centralized Mac Mini M4 running **OBS Studio** and **Reaper** acted as the mixer, aggregating all NDI streams into a single virtual camera for Google Meet/Teams.

B. Network & Security Architecture

To prevent A/V traffic from impacting clinical operations, I engineered a dedicated "Media Layer":

- **Isolated VLAN:** Created a high-bandwidth, non-routed VLAN specifically for NDI traffic.
- **Power & Data:** Utilized **Texas PoE+ to USB-C adapters** to provide continuous power and a wired data connection to the mobile units, ensuring stability that Wi-Fi could not provide.
- **Endpoint Hardening:** Used **Hexnode MDM** to lock the devices into "Single-App Mode," preventing unauthorized use and ensuring the devices remain headless utility nodes.

---

4. MULTI-NEED CONFIGURATIONS

I designed the system to be modular, supporting three distinct use cases:

1. **Attendee Array:** Desktop gooseneck mics for interactive board meetings.
2. **Presenter Setup:** Mobile lavalier mics for dynamic, high-movement speakers.
3. **Ceiling Array:** Strategic overhead placement for room-wide ambient audio capture.

---

5. BUSINESS & OPERATIONAL IMPACT

- **Extreme ROI:** Achieved professional-tier results using $1 FirstNet promotional hardware and E-waste network switches.
- **Scalability:** The "Template" can be deployed to any clinic with existing network infrastructure.
- **Sustainability:** Diverted dozens of high-performance mobile devices and switches from the landfill, aligning with corporate social responsibility (CSR) goals.
- **Deterministic Quality:** Wired PoE connectivity eliminated the jitter and lag typically associated with wireless conferencing solutions.

---

6. TECHNICAL DOCUMENTATION INDEX

- **Project Presentation:** [Link to Conference Room Tests Slideshow]
- **VLAN Configuration:** Documented in the *Remote Clinic Network Diagram*.
- **MDM Policy:** Standardized via Hexnode (SOP available upon request).

EXHIBIT VII: OpenOperations-AI (Sovereign Resource Orchestrator)

Project Scope: Local-First Business Intelligence & Predictive Operations Engine

Architect: David Culp, Principal Solutions Architect

Key Value: Transformed raw infrastructure into a cost-saving operational tool by automating document ingestion and vendor risk scoring locally.

---

1. EXECUTIVE SUMMARY

Building on the "Sovereign Architect" philosophy, I engineered a private-cloud-native operations tool to eliminate "Information Overload" and "Cloud-Dependency Tax." By integrating local OCR and LLMs, this system analyzes multi-site vendor data without exposing sensitive financial metadata to third-party SaaS providers.

---

2. THE CHALLENGE

- **Operational Visibility:** Monitoring costs and compliance across 32 clinical sites often results in "Compliance by Spreadsheet," which is difficult to audit.
- **Privacy Risks:** Standard BI tools require uploading sensitive vendor contracts and financial logs to the cloud, creating a potential breach point for organization-wide strategy.
- **Manual Friction:** Hand-keying invoice data leads to "human-element" errors and configuration drift in operational reporting.

---

3. THE ARCHITECTURAL SOLUTION

I implemented a 3-stage automated pipeline that runs entirely on-premise within the **Autonomous Datacenter** model.

- **Layer 1 (Ingestion):** A Python-based "Sovereign Watcher" monitors a ZFS-replicated directory for incoming documents.

- **Layer 5 (Intelligence):** Utilizing **Tesseract OCR** and **Ollama (Mistral-Nemo)**, the system performs a deterministic analysis of PDFs to extract vendor names, totals, and risk categories.
- **Layer 6 (Governance):** Automatically assigns a **Risk Score** (1-10) based on NIST 800-53 security standards, flagging vendors who lack current BAA or SOC2 certifications.

4. TECHNICAL STACK

- **Compute:** Dell Precision 7780 Workstation / Proxmox HA Cluster.
- **AI Engine:** Ollama running Mistral-Nemo (Local-Only).
- **Backend:** Python (FastAPI), SQLModel, and Watchdog.
- **UI:** Tailwind CSS Sovereign Dashboard.

5. BUSINESS OUTCOMES

- **Zero-Cloud Footprint:** 100% data sovereignty achieved by processing all financial and operational metadata locally.
- **Extreme ROI:** Leveraged existing high-performance hardware to replace expensive third-party BI subscriptions.
- **Audit Readiness:** Created a deterministic paper trail for every operational expense, fully integrated with the organization's existing GRC engine.

6. TECHNICAL DOCUMENTATION INDEX

- **GitHub Repository:** https://github.com/davidculp-tech/OpenOperations-AI
- **Demo/SOP:** Included in the *Autonomous Datacenter Deployment Guide*.

EXHIBIT VIII: Sovereign Operational Intelligence (The Docker Orchestration)

Project Scope: Transitioning Standalone BI Tools to a Containerized Microservices Stack

Architect: David Culp, Principal Solutions Architect

Key Value: Orchestrated a triple-service environment to ensure seamless data flow and service high-availability on local high-compute hardware.

---

1. EXECUTIVE SUMMARY

Building on the "Sovereign Architect" philosophy, I evolved a suite of standalone scripts into a fully containerized **Triple-Service Stack**. This Dockerization effort ensures that the Ingestion Engine, Backend API, and Frontend Dashboard operate as a unified, portable ecosystem. By isolating dependencies and orchestrating inter-service communication, I eliminated environment variance and created a resilient, production-ready operational intelligence environment that operates entirely within the private cloud.

---

2. THE CHALLENGE

- **Environment Parity:** Original tools relied on host-specific Python paths, making consistent deployment across Proxmox nodes difficult.
- **Volume Sync Complexity:** Moving to Docker introduced "Volume Stalling" where the host and Linux containers struggled to synchronize PDF data in real-time.
- **Service Discovery:** Enabling three distinct applications to communicate securely while maintaining a single, consistent SQLite data source.

---

3. THE ARCHITECTURAL SOLUTION

I implemented a `docker-compose` orchestration strategy segmentizing business logic into three distinct layers sharing a **Sovereign Data Volume**.

- **Layer 1 (The Engine):** Optimized the **OCR-Ingestion** container for real-time batch processing of multi-site invoices.
- **Layer 2 (The Bridge):** Engineered a custom **FastAPI Networking Layer** to bridge the isolated SQLite database and the external browser, resolving routing errors via manual endpoint injection.
- **Layer 3 (The Sync):** Resolved frontend data-binding issues by aligning JavaScript calls with verified JSON API outputs (e.g., `vendor_name` field mapping).

---

4. DEPLOYMENT GUIDE: SOVEREIGN STACK

1. **Orchestration Launch:** Deploy containers via `docker-compose up -d --build` to initialize the virtual network.
2. **Database Alignment:** Access the API container (`docker exec`) to create SQL views, ensuring ORM names match the injected data.
3. **Frontend Validation:** Access the dashboard at `localhost:8001` and perform a Hard Refresh (Ctrl + F5) to pull the live records.

---

5. BUSINESS OUTCOMES

- **Rapid Portability:** The entire 3-app stack deploys in seconds to any node in the organization's high-compute environment.
- **Technical Resilience:** Successfully navigated complex container-layer networking, ensuring "Sovereign Vendor" data flows from raw PDF to the GUI with zero packet loss.
- **Extreme ROI:** Leveraged existing hardware to replace expensive third-party BI subscriptions with a 100% private solution.