Zero-Trust Infrastructure Provisioning

Engineering Air-Gapped Deployments with Create-V

1. Executive Summary

In modern high-security environments—such as defense, banking, and critical infrastructure—the concept of 'Air-Gapping' is no longer optional. Datacenters must operate completely disconnected from the public internet.

However, traditional Infrastructure as Code (IaC) tools like Terraform or Microsoft System Center Virtual Machine Manager (SCVMM) often introduce heavy dependencies, require external module downloads, or demand complex database backends that violate strict Zero-Trust policies. This whitepaper explores how Create-V solves this paradox by delivering a 100% client-side, zero-install orchestration engine.

2. The Danger of 'Connected' Provisioning

Most provisioning engines require an 'Agent' installed on the Hyper-V host, continuously polling a central server or a cloud endpoint. This creates a massive attack surface. If the central orchestrator is compromised, the attacker instantly gains SYSTEM-level access to every Hyper-V node in the cluster.

Furthermore, auditing closed-source agents is nearly impossible for internal CISO teams. Security teams are forced to blindly trust the vendor's telemetry practices.

3. The Create-V Architecture (Offline-First)

Create-V flips the traditional IaC model. Instead of a heavy backend, the entire orchestration intelligence is compiled into a single 200KB HTML file. An architect can place this file on an encrypted USB drive, walk into a Faraday-caged datacenter, and open it in any modern browser without internet access.

Because all JSON blueprinting and PowerShell generation happens locally in the browser's memory, absolutely zero bytes are transmitted over the network. There is no database to hack, no API keys to steal, and no cloud telemetry to block.

4. Transparent, Auditable Execution

Security teams despise 'black boxes'. When Create-V generates a deployment script, it outputs raw, heavily commented, and human-readable PowerShell. Before a single VM is provisioned, the CISO or Lead Engineer can read exactly what the script will do.

Additionally, Create-V scripts automatically generate native PowerShell Transcripts. Every command executed, every VHDX created, and every vSwitch attached is immutably logged into a local text file, satisfying compliance and auditing requirements instantly.