ZeroLock® Compliance Overview for NIST 800-171

Designed to align with NIST 800-171, ZeroLock® delivers preemptive, runtime security purpose-built to protect hypervisors against evolving threats. By integrating advanced access controls, AI-driven behavioral detection, and automated threat response into the hypervisor layer, ZeroLock proactively prevents unauthorized access, detects malicious activity, and enforces compliance with federal security standards.

Function	Control	Applicable Features
Access Control & Authentication	3.1.1 - Account Management 3.1.5 – Least Privilege 3.1.12 – Remote Access 3.5.1 – User Identification and Authentication 3.5.3 – Multi-Factor Authentication	• Network Access Rules • File Access Rules • CLI MFA
Configuration Management	3.4.2 – Configuration Settings 3.4.6 – Least Functionality 3.4.8 – Authorized Software – Allow by Exception	• Application Filtering • Automated File Rollback • Program Execution Rules
System Integrity, Protection & Threat Monitoring	3.13.1 – Boundary Protection 3.13.11 – Cryptographic Protection 3.13.15 – Session Authenticity 3.14.2 – Malicious Code Protection 3.14.6 – System Monitoring	• Endpoint Quarantine • Ransomware Detection • Tampering Detection • Cryptojacking Detection • Use of Cryptography • Canary Files
Incident Response	3.6.1 – Incident Handling	• Remote Shell

valicyber®

ZeroLock

ZeroLock Endpoint Agent Requirements for Hypervisors

OS	• VMware Cloud Foundation 9.X • VMware ESXi, 6.7+ (Older versions supported upon request.) • Nutanix-managed ESXi, 6.7+ • Nutanix AHV 2017+* • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization, 3.6+ • HPE Morpheus, 8.0+ • Dell VxRail, 4.8+ • KVM, Kernel 3.5 *Note, Nutanix does not currently support third-party products running on AHV.
Processor	x86-64, ARM-64 (coming soon)
Memory	50MB
Disk Space	100MB
Kernel Mods	No kernel modification or modules required
Installation Methods	• One-line, web-based deployment (Wget) • File-based deployment (Tar.gz or Bash) • ESXi: Signed VIB and deployable via vCenter

ZeroLock Server Requirements (Only required for on-prem deployment.)

RAM	16GB
Disk Space	128GB (Dependent on number of endpoints and data retention period.)
CPU Cores	6 or more recommended
Installation Reqs.	• Self-deployment: Latest version of Docker installed • OVA-deployment: ESXi 7.0 or later

ZeroLock Bidirectional API-First Architecture

Documentation	Visit api.zerolock.com for a full API
Existing Integrations	• SIEM: Splunk, Sumo Logic, Elastic, Google SecOps • SOAR: Swimlane • Incident API: Veeam

About Vali Cyber

Vali Cyber® secures where attacks have the most impact: mission critical systems. While most defenses focus on endpoints, Vali Cyber identified Linux and hypervisors as critical yet under protected. Built for this reality, ZeroLock® is the only Broadcom-certified solution that delivers preemptive security with CLI-MFA, exploit prevention, and AI-driven behavioral detection. By operating at the hypervisor layer, ZeroLock stops threats in real time without performance impact. If incidents occur, automated rollback restores workloads in seconds, ensuring uptime. Recognized by Gartner as a Key Startup in Security Software, Vali Cyber leads by protecting the foundation of modern infrastructure others overlook.

MADE IN THE U.S.A.

valicyber®