ZeroLock® Compliance Overview for NIST 800-171

Designed to align with NIST 800-171, ZeroLock® delivers a comprehensive, multilayered defense strategy tailored for securing 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 • SSH 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	• ESXi, 6.7+ (Older versions supported upon request.) • Nutanix, AHV-2017+ • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization (RHEV), 3.6+ • KVM, Kernel 3.5+
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 • SOAR: Swimlane • Incident API: Veeam

About Vali Cyber

Vali Cyber, Inc. was founded in 2020 with the mission of addressing the specific security needs of Linux and its derivatives. By focusing on creating a Linux-first security solution with increased efficacy and reduced Total Cost of Ownership (TCO), we created the ZeroLock platform. Our approach puts clients in control of their hypervisor & Linux security by reducing analyst and computational overhead, while simultaneously ensuring uptime with state-of-the-art AI behavioral techniques to stop attacks and automated file rollback to restore your most critical data in milliseconds. Imagine detecting and fully remediating a ransomware attack on your hypervisor in real-time...that dream has become reality.

MADE IN THE U.S.A.

valicyber®