ZeroLock® Compliance Overview for NIST CSF 2.0

Designed to align with the five core functions of NIST Cybersecurity Framework (CSF) 2.0, ZeroLock® delivers a preemptive, runtime protection purpose-built for hypervisors. By integrating advanced attack prevention, AI-driven behavioral detection, and automated remediation, ZeroLock proactively secures your hypervisors against emerging threats at runtime, helping organizations streamline compliance while fortifying their cybersecurity posture.

Function	Category	Applicable Features
Identify (ID)	Asset Management (ID.AM) Risk Assessment (ID.RA) Improvement (ID.IM)	• Network Access Rules • Program Execution Rules • Application Filtering • API Integration
Protect (PR)	Identity Management, Authentication, and Access Control (PR.AA) Data Security (PR.DS) Platform Security (PR.PS) Technology Infrastructure Resilience (PR.IR)	• CLI MFA • File Access Rules • SSO Integration • Use of Cryptography • Canary Files
Detect (DE)	Continuous Monitoring (DE.CM) Adverse Event Analysis (DE.AE)	• Ransomware Detection • Cryptojacking Detection • Tampering Detection • Email Alerts
Respond (RS)	Incident Management (RS.MA) Incident Analysis (RS.AN) Incident Mitigation (RS.MI)	• Automated Process Trees • Endpoint Quarantine • Virtual Patching
Recover (RC)	Incident Recovery Plan Execution (RC.RP)	• Automated File Rollback

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