# 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 comprehensive, multilayered defense strategy. By integrating advanced attack prevention, AI-driven behavioral detection, and automated remediation, ZeroLock proactively secures your hypervisors against emerging threats. With real-time threat intelligence and adaptive security controls, ZeroLock helps organizations streamline compliance while fortifying their cybersecurity posture.**

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

valicyber®

ZeroLock

# ZeroLock Endpoint Agent Requirements for Hypervisors

| | |
|---|---|
| **OS** | • ESXi, 6.7+ (Older versions supported upon request.)<br>• Nutanix, AHV-2017+<br>• XenServer, 6.5+<br>• Citrix Hypervisor, 8.0+<br>• Proxmox, 3.0+<br>• Red Hat Enterprise Virtualization (RHEV), 3.6+<br>• 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)<br>• File-based deployment (Tar.gz or Bash)<br>• 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<br>• 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<br>• SOAR: Swimlane<br>• 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