ZeroLock® Protecting Hypervisors for Healthcare Institutions

FINALLY, HYPERVISOR RANSOMWARE PROTECTION IS HERE.

Designed to align with the controls of SOC-2 and NIST Cybersecurity Framework (CSF) 2.0, ZeroLock® offers a multilayered approach to security by combining attack prevention with AI behavioral detection and automated remediation to secure your hypervisors and ensure the confidentiality, integrity, & availability of personal health information (PHI).

Prevent attacks with SSH-MFA and application allowlisting.

ZeroLock goes beyond traditional access control capabilities outlined in SOC-2 by offering easily configured and universally applied rules and policies that can be deployed across your hypervisor environment. Examples of our control capabilities include:

- **SSH Multifactor Authentication (MFA)**
- **Application Allowlisting**
- **Process Behavior Controls**
- **Network Access Controls**
- **File Access Controls**
- **Canary Files**
- **Tamper Protection**

Ensure uptime with AI detection and automated remediation.

ZeroLock's AI behavioral detection identifies malware in real-time. Our proprietary algorithms support NIST Detect and Respond functions by detecting and stopping traditional and fileless ransomware attacks with >98% efficacy, and offer the ability to automatically remediate file damage and remove attackers with no user intervention required—helping you to ensure zero downtime.

- **Ransomware Protection**
- **Wiperware Protection**
- **Real-time Threat Remediation**
- **Automated File Rollback & Attacker Persistence Removal**
- **Fully Automated Process Tree Creation**

Enable transparency with data management and audit trails.

Satisfy data retention policies and NIST Asset Management by ensuring that e-PHI is not improperly altered or destroyed based on predefined rules. ZeroLock's audit trails and logging capabilities enhance operational transparency and ensure regulatory compliance through detailed data handling records.

Deploy and manage flexibly.

With ZeroLock, no modification to the hypervisor itself is required, and deployment is as simple as one line in the terminal, or through a partner portal like VCenter. ZeroLock is configured to work while also maintaining system stability and performance.

> "Healthcare institutions have been looking for a security solution to their vulnerable hypervisors for years with no luck. It's our mission to provide solutions to the unique challanges that critical Linux systems face, and we're pleased to announce the first ever hypervisor ransomware protection solution."
>
> **—Austin Gadient, CTO & Cofounder, Vali Cyber**

For the 14th year in a row, healthcare saw the costliest breaches across industries, reaching $9.77 million.

IBM
Costs of a Data Breach 2024

valicyber®

Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.
Linux® is the registered trademark of Linus Torvalds.

©Vali Cyber, Inc. | valicyber.com

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	512GB (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

Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.
Linux® is the registered trademark of Linus Torvalds.

©Vali Cyber, Inc. | valicyber.com