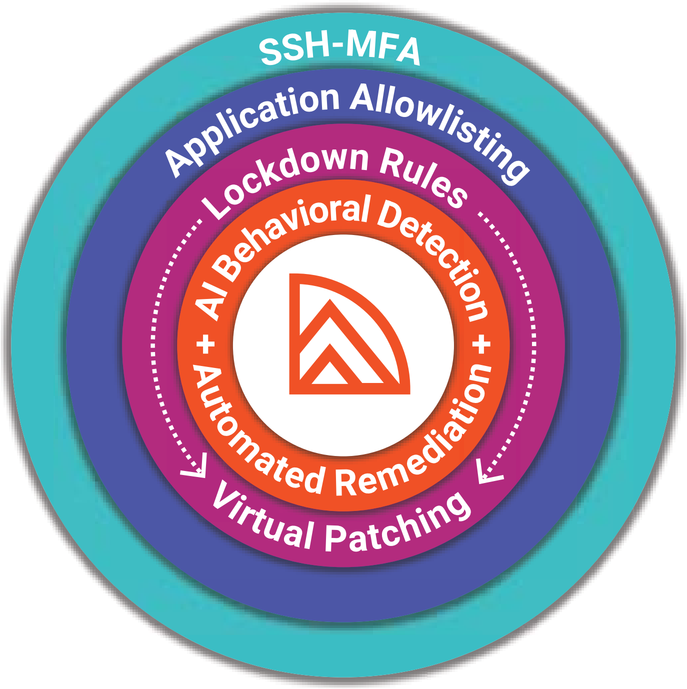
ZeroLock®

Hypervisor Ransomware Protection

Defense-in-depth

Recognized by Gartner as a Key Startup in Security Software, Vali Cyber has expanded our ZeroLock® platform to take a multilayered approach to hypervisor defense to provide a comprehensive security solution.



SSH-MFA

Application Allowlisting

Lockdown Rules

AI Behavioral Detection + Automated Remediation +

Virtual Patching

Prevent attacks with SSH-MFA, virtual patching, and more.

ZeroLock goes beyond traditional mandatory access control capabilities by offering easily configured and universally applied rules and policies that can be deployed across your hypervisor environment.

- SSH-MFA
- Lockdown Rules & Virtual Patching
- Application Allowlisting
- 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 detect and stop 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

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.

- Compatible with all Linux-based hypervisors, including VMware ESXi
- API-based architecture
- Single agent
- One-line deployment
- Minimal overhead (50MB RAM)

Schedule your demo today! info@valicyber.com

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®