ZeroLock®

# Defense-in-Depth for Hypervisors and vCenter

## PREEMPT: Stop attacks before they start.

As enterprises grow their private cloud, threat actors have locked in on the hypervisor. Recognized by Gartner as a Key Startup in Security Software, Vali Cyber® has expanded our ZeroLock® platform to take a proactive, multilayer approach to hypervisor defense—answering this critical security gap.

ZeroLock leads with preventative best practices, going beyond traditional mandatory access control capabilities by offering features like easily configured and universally applied rules and policies that can be deployed across your hypervisor environment, helping you stop attacks before they even start.

### Key Capabilities

**CLI-MFA:** Attackers often compromise hypervisors using stolen credentials. Without CLI-MFA on access points like SSH or the DCUI, these sessions go unchallenged and unseen. Microsoft estimates MFA can block over 99% of account-compromise attempts, yet most hypervisor access still relies on passwords alone. Enforcing CLI-MFA adds a critical zero-trust control, stopping ransomware before attackers ever reach the hypervisor.

**Data Exfiltration & File Access Prevention:** Unrestricted file operations allow attackers to encrypt, delete, or exfiltrate entire environments in minutes. Data exfiltration and file access prevention stop this by enforcing strict controls. By restricting access to VMX, VMDK, and snapshot files, security teams prevent ransomware execution, tampering, and persistence, hardening the hypervisor environment.

**Exploit Prevention & Virtual Patching:** Zero-day vulnerabilities can enable VM escape, remote code execution, and full hypervisor takeover—impacting every workload on the host. Traditional patching is often delayed by downtime, reboots, or unavailable vendor fixes, leaving critical systems exposed. Virtual patching closes this gap by blocking exploit behavior at runtime without modifying system code or taking hosts offline. Protect against zero-days, secure unsupported ESX versions, and maintain uptime for mission-critical environments.

**Application Allowlisting:** Application allowlisting for hypervisors protects from unauthorized code execution. Instead of trying to detect malicious activity after it occurs, allowlisting enforces a zero trust “default deny” posture. This dramatically reduces the attack surface, blocking ransomware, living-off-the-land techniques, and zero-day exploits that attempt to introduce new or modified code.

**Canary Files:** Canary files provide an early-warning mechanism for detecting attacks against hypervisors and the virtual machines they manage. These decoy files are placed in sensitive directories and are triggered on behavior rather than known signatures. They can expose zero-day attacks and insider threats to help surface malicious activity that traditional EDR tools miss.

**Tamper Protection:** Tamper protection enforces safeguards that lock down files, processes, memory, and configurations so only authorized actions are allowed—even from privileged accounts. This stops attackers from exposing every hosted workload and turning a local compromise into a systemic failure.

## Schedule your demo today! info@valicyber.com

valicyber®

Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.
All other trademarks are the property of their respective owners.

©Vali Cyber, Inc. | valicyber.com

ZeroLock

# ZeroLock Endpoint Agent Requirements for Hypervisors

| | |
|---|---|
| **OS** | • VMware Cloud Foundation 9.X<br>• VMware ESX, 6.7+<br>(Older versions supported on request.)<br>• Nutanix-managed ESX, 6.7+<br>• Nutanix AHV 2017+*<br>• XenServer, 6.5+<br>• Citrix Hypervisor, 8.0+<br>• XCP-ng 8.3+<br>• Proxmox, 3.0+<br>• Red Hat Enterprise Virtualization, 3.6+<br>• HPE Morpheus, 8.0+<br>• Dell VxRail, 4.8+<br>• KVM, Kernel 3.5+<br>*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)<br>• File-based deployment (Tar.gz or Bash)<br>• VCF & 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, Google SecOps, CrowdStrike Next-Gen<br>• SOAR: Swimlane<br>• Incident API: Veeam |

## About Vali Cyber

Vali Cyber® secures the core of enterprise infrastructure: the hypervisor and the management plane that controls it. Most defenses stop at the endpoint, but attackers have moved below it, where one compromise can take down every workload. A pioneer of preemptive hypervisor security, Vali Cyber built ZeroLock® for defense-in-depth: CLI-MFA and exploit prevention stop attacks before they start, AI behavioral detection catches what can get past, and automated rollback restores workloads in seconds. One lightweight agent protects most major hypervisors and streams every event into the SIEM and SOAR tools teams already use. Recognized by Gartner as a Key Startup in Security Software, Vali Cyber protects the layer others overlook.



MADE IN THE U.S.A.

valicyber®

Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.
All other trademarks are the property of their respective owners.

©Vali Cyber, Inc. | valicyber.com