ZeroLock®

Preemptive Hypervisor Security

Defense-in-depth: Prevention first.

As enterprises grow their private cloud, threat actors have locked in on the hypervisor. Attacks on ESX are up 700%, at times resulting in hundreds of millions of dollars lost in a single attack. 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 by covering 100% of MITRE ESX TTPs.

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®

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) • 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 • 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® 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® delivers preemptive security with CLI-MFA, exploit prevention, deep hypervisor visibility, and AI-driven behavioral detection. By operating at the hypervisor layer, ZeroLock stops threats in real time without performance impact or added overhead. 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®