ZeroLock®

Defense-in-Depth for Hypervisors and vCenter

PROTECT: Detect and undo what could get through.

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.

No security strategy is static, which is why resilience matters as much as prevention. With patented AI Detection and Automated Remediation, you gain the ability to detect and respond to threats in real time—limiting blast radius, accelerating recovery, and keeping the business running.

Key Capabilities

AI Detection for Ransomware & Wiperware: Stop attacks in real-time—before you even know something is wrong. ZeroLock instantly detects anomalous behavior like suspicious hypercalls, unauthorized process execution, or abnormal VM interactions. Instead of waiting for known signatures or post-breach indicators, ZeroLock acts at machine-speed to surface and contain ransomware and wiperware threats the moment they deviate from expected behavior. The result is faster detection, fewer configuration gaps, and protection where other tools can't see, making ZeroLock a critical pillar of a true Zero Trust strategy for virtualization security.

Automated File Remediation & Attacker Persistence Removal: An actual "easy" button, ZeroLock provides security teams with an instant recovery option by restoring critical hypervisor files to a known-good state automatically—eliminating the need for manual rebuilds, lengthy downtime, or risky reinstallation. This capability is unique to ZeroLock, allowing teams to rapidly reverse malicious changes made by ransomware, insider abuse, or zero-day exploits. By pairing real-time detection with immediate rollback, ZeroLock not only stops attacks in progress but dramatically shortens recovery time, helping organizations maintain uptime, operational continuity, and confidence in their virtual infrastructure.

Attacker Persistence Removal: Going beyond stopping malicious activity, ZeroLock automatically identifies and eliminates the mechanisms attackers use to survive reboots, patches, and restores, such as rogue services, scheduled tasks, modified binaries, or abused management functions. By removing persistence at the hypervisor layer, ZeroLock ensures recovery is complete and durable, preventing attackers from quietly re-establishing access and turning a "resolved" incident into a recurring one.

Fully Automated Process Tree Creation: ZeroLock's automated process tree capabilities provide you with insight and understanding as to how an attack happened. This post-incident visibility is critical for validating that remediation was effective, explaining impact to auditors and executives, refining security policy, and strengthening future defenses. Process trees turn automated response into provable resilience, not just assumed protection.

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 • VMware ESX, 6.7+ (Older versions supported on request.) • Nutanix-managed ESX, 6.7+ • Nutanix AHV 2017+* • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • XCP-ng 8.3+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization, 3.6+ • HPE Morpheus, 8.0+ • Dell VxRail, 4.8+ • KVM, Kernel 3.5+ *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, Google SecOps, CrowdStrike Next-Gen • SOAR: Swimlane • 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