ZeroLock®

Hypervisor Exploit Prevention

The problem with patching in an AI world

A patch cycle measured in days can't defend a threat measured in hours. With hypervisors becoming a higher targeted critical attack surface, this is the new threat landscape security and infrastructure teams are facing:

48,244 CVEs
published in 2025 (+20% YoY); remote code execution CVEs alone up 39%

~10 hrs
median disclosure-to-exploit window for internet-facing infrastructure, down from 56 days in 2024

29%
of exploited CVEs in 2025 hit before disclosure was even public

5 Days
from patch to mass exploitation of vCenter's CVE-2026-59310

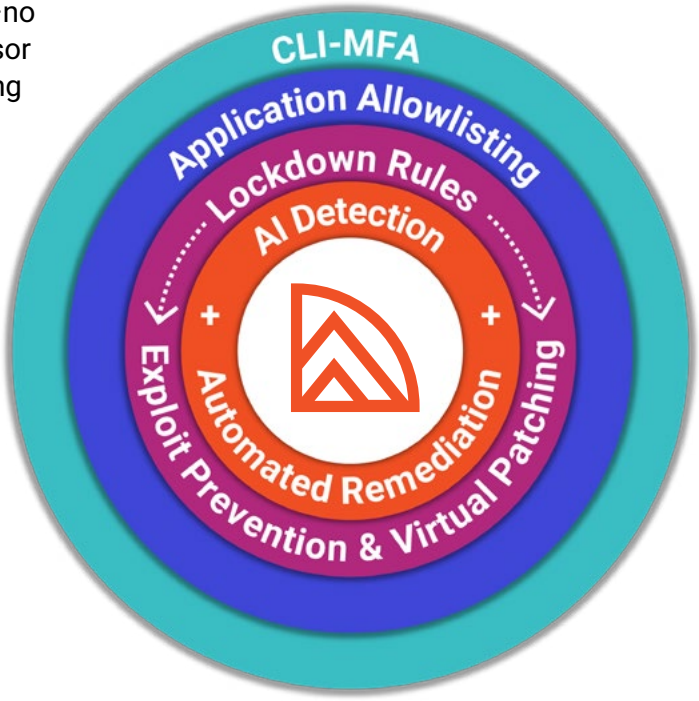
8x
rise in hypervisor ransomware encryption in 2025, even as exposed ESXi hosts fell ~90%

ZeroLock closes the patching gap at runtime

Preemptive hypervisor security doesn't wait for a CVE, a patch, or a signature. It enforces prevention at the hypervisor control plane itself, the moment an attacker tries to act.

Exploit Prevention & Lockdown Rules

Close the exploit pathways of a vulnerability within hours—no reboot, no waiting on a vendor fix. This means the hypervisor is never exposed during the disclosure-to-patch gap, helping to ensure business resiliency.



CLI-MFA

Requires verified authorization for privileged hypervisor commands. A valid credential or an abused trust relationship stops being enough to reach host admin.

AI Behavioral Detection

Watches what an attack does (unusual command sequences, encryption behavior, lateral movement) not what it's signed as. Catches novel and zero-day activity no CVE-based tool can recognize yet.

Automated Remediation

Contains and stops in-progress activity in real time. No analyst triage required before the bleeding stops.

What is your plan to keep your most critical infrastructure running?
Schedule your demo today! info@valicyber.com

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	• VMware Cloud Foundation 9.X • VMware ESXi, 6.7+ (Older versions supported on request.) • Nutanix-managed ESXi, 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 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®

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

©Vali Cyber, Inc. | valicyber.com