HOW ARE YOU HANDLING TODAY'S HYPERVISOR RISKS?

AI has shifted the target to the hypervisor. Most continuity plans haven't caught up.

The hypervisor has quietly become one of the highest-value targets in the enterprise. Private AI and the most sensitive workloads increasingly run on it, and attackers have noticed:

8x
rise in hypervisor ransomware in 2025, even as internet-exposed ESX hosts fell 90%

~10 hrs
from disclosure to exploitation, now that attackers use AI

0 lines of code
needed to exploit CVE-2024-37085; creating a domain group named "ESX Admins" gets full admin on every vulnerable AD-joined ESX host

When one host falls, every VM on it goes down, breaking the two assumptions continuity plans rely on: time to react and contained failures. Yet hypervisor security often has no clear owner. The hypervisor is the one layer that can take down the entire business, and no one is accountable for its protection.

ZeroLock®: Take control of hypervisor risk

Certified by Broadcom, ZeroLock's Hypervisor Security doesn't wait for a CVE or patch. It enforces prevention at the hypervisor control plane itself, keeping your most critical infrastructure running.

Close trust-relationship gaps, not just technical ones.

CLI-MFA requires verified authorization for privileged hypervisor commands, so an abused AD group or a stolen credential alone can't reach host admin, extending zero trust to the hypervisor.

Contain the blast radius.

Stop encryption, tampering, and unauthorized escalation at the host in real time, so one compromised host can't take down every workload with it. Plus, attacker persistence removal keeps threat actors from getting back in.

See what perimeter tools can't.

AI-behavioral detection watches activity at the hypervisor itself, the one layer most security stacks can't see. Suspicious actions are stopped at machine speed, and automated process trees show how the attack unfolded.

Shrink recovery from weeks to seconds.

Automated remediation reverses in-progress activity immediately—not on the timeline a real incident response takes to spin up—so an attack doesn't turn into weeks of downtime and lasting costs.

Ensure business continuity without adding to your workload.

ZeroLock is configured to deploy at scale quickly, often in under 6 hours, and SIEM/SOAR integrations put alerts where your team already works, keeping hands-on management down to as little as 1 hour a week.

WHO OWNS YOUR HYPERVISOR RISK PLAN?

Let's work on it together: info@valicyber.com

Sources: https://aiweekly.co/alerts/synack-ai-collapses-cve-exploit-window-to-10-hours
https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
https://www.huntress.com/blog/hypervisor-defenses-against-ransomware-targeting-esxi
https://www.forescout.com/blog/vmware-esxi-servers-a-major-attack-vector-for-ransomware/
https://cyberunit.com/insights/cve-exploit-window-10-hours-ai-attackers-2026/

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 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 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