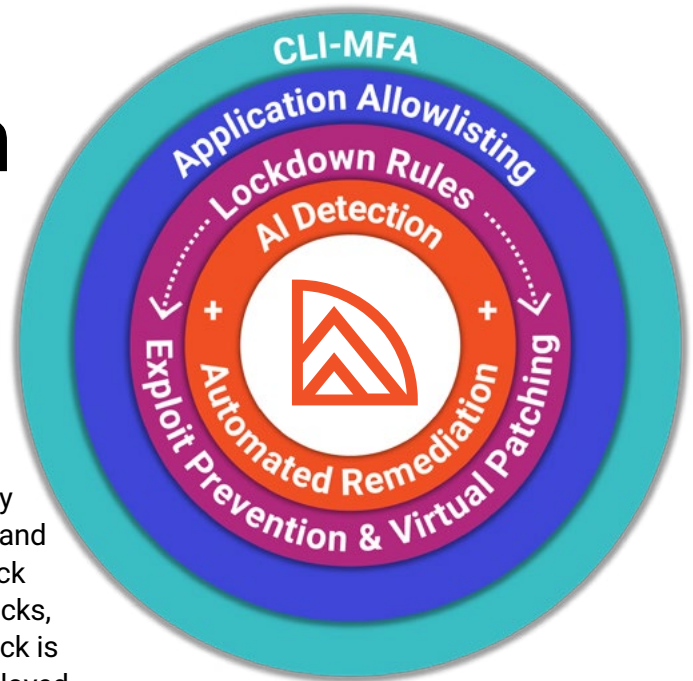




Defense-In-Depth for Hypervisors

Cover your core.

Compromise one hypervisor and every workload on it goes dark, which is exactly why attackers want it. In 2025, the hypervisor's share of ransomware encryption grew 8x, and AI now turns a new flaw into a working exploit in roughly 15 minutes for \$1. Many skip the exploit entirely, logging in and using the host's own tools where no SOC is looking. ZeroLock brings defense-in-depth to the hypervisor itself: it stops attacks, catches what can get past and undoes the damage. ZeroLock is Broadcom-certified. When properly configured and fully deployed, it mitigates 100% of MITRE ATT&CK ESXi TTPs. Vali Cyber is recognized by Gartner as a Key Startup in Security Software.



Sources: <https://cybersecuritynews.com/ai-generate-cve-exploits/>
<http://www.huntress.com/blog/hypervisor-defenses-against-ransomware-targeting-esxi>

PREEMPT: Stop attacks before they start.

Attackers increasingly arrive with valid credentials or a fresh exploit. ZeroLock requires MFA on the commands you choose at the moment of action, not just at login. It also hardens vulnerable code paths with virtual patching, so you patch on your own schedule instead of in a fire drill.

- CLI-MFA
- Data Exfiltration & File Access Prevention
- Exploit Prevention & Virtual Patching
- Application Allowlisting
- Canary Files & Tamper Protection

PROTECT: Undo whatever can get through.

No security strategy is static, which is why resilience matters as much as prevention. Patented AI behavioral detection runs inside the agent and catches what can get past, even attacks no rule anticipates. It stops them in real time and rolls back encrypted files automatically, with no human in the loop, so workloads are restored in seconds.

- Ransomware Protection
- Wiperware Protection
- Real-time Threat Remediation
- Automated File Rollback
- Attacker Persistence Removal
- Fully Automated Process Tree Creation

PERFORM: Designed for how your team actually works.

Attackers aren't limited to one platform, and your SOC can't defend what it can't see. One lightweight ZeroLock agent protects most major hypervisors, deploys quickly with just a single command line, and streams every event into the SIEM and SOAR tools you already run, all while preserving performance, uptime, and control.

- ESX, VCF 9.x, Nutanix, Proxmox & more
- Certified CrowdStrike Falcon integration
- API-first for SIEM/SOAR integration
- Lightweight single agent (50MB RAM)
- One-line deployment, no kernel modules
- Signed Broadcom VIB to deploy via vCenter
- Works in air-gapped environments

Schedule your demo today! info@valicyber.com



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 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+ *Nutanix does not currently support third-party products running on AHV.	• 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+
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.



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