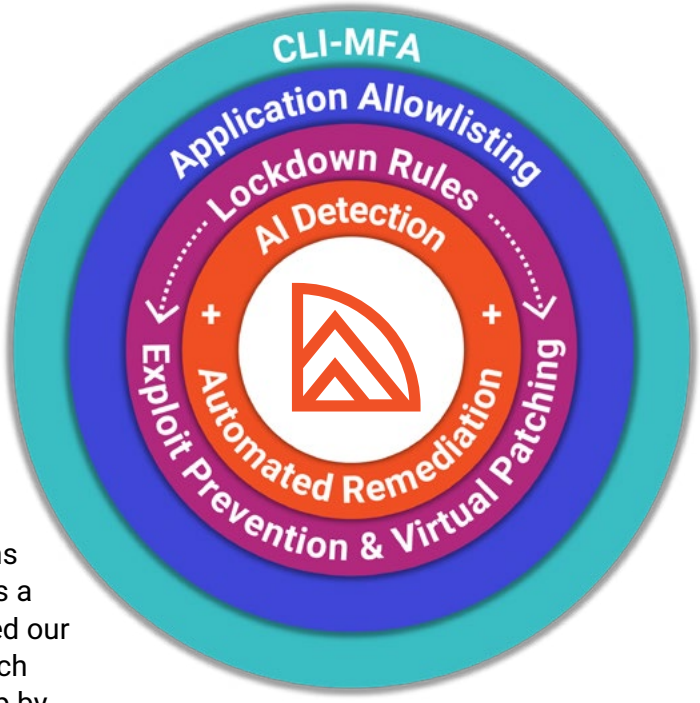
ZeroLock®

Preemptive Hypervisor Security



Defense-in-depth

As enterprises grow their private cloud, threat actors have locked in on the hypervisor. Ransomware ttacks 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—and it's certified by Broadcom.

PREEMPT: Prevention first with CLI-MFA, virtual patching, and more.

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.

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

PROTECT: Business continuity with machine-speed detection & remediation.

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.

- 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.

ZeroLock was designed to deliver enterprise-grade hypervisor security without the operational friction that typically slows adoption. From rapid deployment to broad platform support, it integrates seamlessly into existing environments while preserving performance, uptime, and control.

- Compatible with VMkernel and KVM-based hypervisors, including VCF 9.X
- API-first for SIEM/SOAR integration
- Lightweight single agent (50MB RAM)
- One-line deployment
- Signed Broadcom VIB to deploy via vCenter
- Works in air-gapped environments

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