ZeroLock®

Preemptive Hypervisor Security

vs. Traditional Hypervisor Security Approaches

As enterprises grow their private cloud, threat actors have locked in on the hypervisor. Attacks on ESX are up 700%, circumventing traditional security and 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.

Traditional Hypervisor Security

Hardening + Segmentation + Monitoring

Core Characteristics

- Hardening procedures are more manual and cumbersome, but can reduce vulnerability risk
- Segmentation can serve as a preventative control to reduce blast radius, but can miss key attack tactics like lateral movement
- Detection is implied, but is likely using logs that must be reviewed after the fact
- Cannot stop attacks once access is gained
- Relies on multiple tools that are likely agent-based and network-based

The overall security posture is reactive. In the event an environment is breached, the user must rely on back-ups (that may have the attacker still inside) or start anew.

ZeroLock

Preemptive Hypervisor Security

Core Differentiators

- Preventative layers, including hardening procedures, CLI-MFA, anti-tampering, and virtual patching are automated to quickly and effectively enforce zero-trust exploit prevention
- Complements segmentation by being able to detect tactics like lateral movement at runtime for fast response
- Emphasis is on multiple prevention points, but detection and remediation exist as a last resort and happen in real-time automatically
- Stops ransomware, living-off-the land attacks, zero-days, and tampering
- Single tool that runs in user space, does not alter the hypervisor kernel, does not require connectivity for effectiveness, and plugs into existing SIEMs/SOARs for simplified management

The overall security posture is preventative and proactive. In the event an environment is breached, the attack can be stopped, and the system restored in seconds, helping to ensure business continuity.

Traditional hypervisor security is reactive—focused on hardening, segmentation, and logs after compromise. ZeroLock's Preemptive Hypervisor Security stops attacks before they start, giving your team peace of mind and ensured business continuity.

Schedule your demo today! info@valicyber.com

valicyber®

ZeroLock

ZeroLock Endpoint Agent Requirements for Hypervisors

OS	• VCF 9.X and ESXi, 6.7+ (Older versions supported upon request.) • Nutanix, AHV-2017+ • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization (RHEV), 3.6+ • 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) • 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 • 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 SSH-MFA, virtual patching, 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.

valicyber