ZeroLock®

Virtual Patching for Hypervisors

Zero-Day Exploit & Instant Shield: Proactive Security as Easy and Effective as Turning Your Deadbolt

Are you prepared for the next VMware vulnerability announcement? Waiting on official patches can take weeks—leaving your infrastructure dangerously exposed, especially when hyperjacking threats are escalating and downtime for patching can grind productivity to a halt.

Introducing Vali Cyber's ZeroLock®:

Instant Vulnerability Shield
ZeroLock acts like a deadbolt for zero-day threats, keeping emergent vulnerabilities out—right when you need protection the most.

No Times, No Delays.
Traditional patching often demands ESXi server reboots and waits for official fixes. ZeroLock's rule-based patching deploys within hours, without forcing system reboots or interrupting operations.

AI-Driven Detection & Response
Advanced heuristics and AI continuously scan your environment for suspicious behavior, neutralizing exploits before they have a chance to cause damage.

Faster, Safer Protection
ZeroLock shields you from zero-day exploits faster than any firewall or EDR solution, securing your critical infrastructure and providing true peace of mind.

Proven & Cost-Efficient
Automated remediation and efficient resource utilization help reduce total cost of ownership—no more scrambling to patch or restore systems after an incident.

Real-World Threat: ESXiArgs Attack
A stark reminder of why immediate protection is paramount is the notorious EsxiArgs attack—a ransomware campaign that spread rapidly by exploiting vulnerabilities in unpatched ESXi servers. Organizations that lacked quick-response solutions found themselves at the mercy of widespread data encryption and downtime. Attackers seized on these ideal windows of vulnerability, locking critical systems and demanding exorbitant ransoms. For teams unprepared to respond instantly, it underscored how delays in patching—even brief ones—can lead to devastating operational and financial losses.

Schedule your demo today: info@valicyber.com

valicyber®

How It Works:

Instant Vulnerability Shield
We push new rules to identify and contain zero-day vulnerabilities the moment they're uncovered.

Day-One Vulnerability Detection
ZeroLock's security intelligence identifies potential exploits as soon as they emerge.

Instant Shield Activation
ZeroLock's virtual patches deploy in 12–24 hours after discovery—no server reboots required.

Virtual Patching
Temporary rule-based fixes that lock out exploits until VMware releases an official patch. No more "white-knuckle" waiting periods.

Quick, Scalable Deployment
Even across large, distributed virtual environments, ZeroLock's shield can be deployed within hours.

Offering You Peace of Mind

Why a Deadbolt?
A deadbolt is a seemingly simple, but highly effective, mechanism to keep unwanted intruders from strolling through your doors. Similarly, ZeroLock proactively locks out hypervisor threats that leverage emerging vulnerabilities, helping your organization evolve from a reactionary mindset.

Thoroughly Tested & Trusted
Every virtual patch undergoes rigorous testing to ensure reliability under real-world conditions.

See Virtual Patching in Action!
Click the image or visit valicyber.com/resources/virtual-patching-video/

Ready to Secure Your Hypervisors?

Don't wait for the next vulnerability to compromise your critical infrastructure.
Eliminate costly downtime, protect your entire virtual environment, and gain the peace of mind you deserve. **Contact us today** to discover how ZeroLock can instantly shield your ESXi environments from zero-day exploits—no waiting, no downtime, and no hassle.

Schedule your demo today: info@valicyber.com

valicyber®

ZeroLock

ZeroLock Endpoint Agent Requirements for Hypervisors

OS	• 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	512GB (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, Inc. was founded in 2020 with the mission of addressing the specific security needs of Linux and its derivatives. By focusing on creating a Linux-first security solution with increased efficacy and reduced Total Cost of Ownership (TCO), we created the ZeroLock platform. Our approach puts clients in control of their hypervisor & Linux security by reducing analyst and computational overhead, while simultaneously ensuring uptime with state-of-the-art AI behavioral techniques to stop attacks and automated file rollback to restore your most critical data in milliseconds. Imagine detecting and fully remediating a ransomware attack on your hypervisor in real-time...that dream has become reality.

MADE IN THE U.S.A.

valicyber®