ZeroLock® + VCF

Extending Security Across the Full Stack

Organizations are modernizing on VMware Cloud Foundation (VCF) to support hybrid cloud, AI initiatives, and mission-critical applications. VCF delivers several security components:

- **vDefend provides network security and segmentation**
- **Advanced Cyber Compliance (ACC) enforces continuous compliance**
- **Live Patching reduces downtime for critical updates, minimizing exposure**

These capabilities strengthen workload and network security, but they overlook the hypervisor itself—the privileged control layer beneath every virtual machine. Adversaries are increasingly targeting that layer; ransomware targeting hypervisors surged roughly 700% in the second half of 2025. When the hypervisor is compromised, controls applied inside individual workloads can be bypassed, putting the entire environment at risk.

Extending Protection to the Hypervisor Layer

While vDefend, ACC, and Live Patching secure workloads and networks, they have limited visibility into runtime behavior at the hypervisor layer.

ZeroLock extends protection directly into this layer. Running on the hypervisor, it continuously monitors execution in real time and enforces what is allowed, blocking unauthorized activity as it occurs. This introduces behavioral, runtime security where attacks ultimately converge.

From Reactive to Preemptive Security on the Hypervisor

Patching and compliance are essential but inherently reactive, relying on known vulnerabilities and remediation cycles. ZeroLock complements these controls by:

- **Detecting anomalous hypervisor behavior tied to exploitation techniques**
- **Blocking attacks in real time without requiring prior CVE knowledge**
- **Enforcing MFA across SSH, the dCUI, and the CLI**

This shifts protection from detection and remediation to active prevention at runtime.

Defending Against Modern Techniques

Modern attackers increasingly use fileless and “living-off-the-land” techniques, leveraging trusted system tools to carry out malicious activity and often evading traditional controls. ZeroLock addresses this by:

- **Enforcing behavioral controls on native ESXi processes**
- **Blocking unauthorized configuration changes at execution time**
- **Preventing ransomware activity at the hypervisor before it reaches workloads**

Stronger Together: Complete Coverage Across Layers

VCF and ZeroLock combine into a layered security architecture:

- **VCF provides the foundation for modern infrastructure and secures workloads and network traffic with vDefend, ACC, and Live Patching.**
- **ZeroLock keeps that foundation secure continuously and at runtime by protecting the hypervisor itself.**

Together, they extend modern security principles across the full stack, closing a critical gap and enabling true defense-in-depth.

Schedule your demo today! info@valicyber.com

valicyber®

ZeroLock

ZeroLock Endpoint Agent Requirements for Hypervisors

OS	• VMware Cloud Foundation 9.X • VMware ESXi, 6.7+ (Older versions supported upon request.) • Nutanix-managed ESXi, 6.7+ • Nutanix AHV 2017+* • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization, 3.6+ • HPE Morpheus, 8.0+ • Dell VxRail, 4.8+ • KVM, Kernel 3.5+ *Note, 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 • 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®