ZeroLock®

Defense-in-Depth for Hypervisors and vCenter

PERFORM: Built for how your team works.

As enterprises grow their private cloud, threat actors have locked in on the hypervisor. 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.

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.

Key Capabilities

Streamlined Management: ZeroLock is configured to work without compromising system stability or performance. With an API-first architecture, ZeroLock can easily fit into your existing SIEM/SOAR—including CrowdStrike Next-Gen SIEM—ensuring protection without adding extra management cycles to your plate.

Ubiquitous Coverage: ZeroLock is compatible with VMkernel and KVM-based hypervisors, including VCF 9.X. For a full list, please see the back of this sheet. Because of ZeroLock's wide coverage capabilities it provides a lot of flexibility to lift and shift with customers, should they decide to change the makeup of their stack.

Signed Broadcom VIB: Vali Cyber is an approved Broadcom VMware partner, allowing VMware Cloud Foundation (VCF) and other VMware users to deploy ZeroLock from vCenter with just one-line in the terminal and no impact to their existing Broadcom support contract.

Minimal Hypervisor Impact: With ZeroLock, no kernel module or modification to the hypervisor itself is required. ZeroLock requires just 50MB of memory, 100MB of disc space, and less than 5% of one CPU core per hypervisor—allowing you to keep resources available for the work that matters to you.

Air-Gapped or SaaS Deployment: The ZeroLock server can be self-hosted in your environment, including your public/private cloud, air-gapped and embedded environments, all with the same level of protection no matter your connectivity abilities. If you choose to take advantage of our ZeroLock SaaS backend, you can be up and running in minutes. Deployment is as simple as one line in the terminal and can also happen through a partner portal like vCenter.

24-7 Support: Vali Cyber prides itself in offering best-in-class support. Our team is there for you every step of the way through deployment and continues to be available to answer questions any time of day as you manage ZeroLock in your environment. We also schedule periodic check-ins to make sure you are getting the most out of your ZeroLock purchase.

Schedule your demo today! info@valicyber.com

valicyber®

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

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+ • 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 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.



MADE IN THE U.S.A.

valicyber®

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