



# Preemptive Hypervisor Security

## Defense-in-depth: Designed for how your team actually works.

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

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

**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.

**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, ensuring protection without adding extra management cycles to your plate.

**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.

**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.

**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](mailto:info@valicyber.com)**



Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.  
Linux® is the registered trademark of Linus Torvalds.

©Vali Cyber, Inc. | [valicyber.com](http://valicyber.com)



## ZeroLock Endpoint Agent Requirements for Hypervisors

<b>OS</b>	<ul style="list-style-type: none"><li>• VMware Cloud Foundation 9.X</li><li>• VMware ESXi, 6.7+ (Older versions supported upon request.)</li><li>• Nutanix-managed ESXi, 6.7+</li><li>• Nutanix AHV 2017+*</li><li>• XenServer, 6.5+</li></ul> <ul style="list-style-type: none"><li>• Citrix Hypervisor, 8.0+</li><li>• Proxmox, 3.0+</li><li>• Red Hat Enterprise Virtualization, 3.6+</li><li>• HPE Morpheus, 8.0+</li><li>• Dell VxRail, 4.8+</li><li>• KVM, Kernel 3.5+</li></ul> <p>*Note, Nutanix does not currently support third-party products running on AHV.</p>
<b>Processor</b>	x86-64, ARM-64 (coming soon)
<b>Memory</b>	50MB
<b>Disk Space</b>	100MB
<b>Kernel Mods</b>	No kernel modification or modules required
<b>Installation Methods</b>	<ul style="list-style-type: none"><li>• One-line, web-based deployment (Wget)</li><li>• File-based deployment (Tar.gz or Bash)</li><li>• VCF &amp; ESXi: Signed VIB and deployable via vCenter</li></ul>

## ZeroLock Server Requirements (Only required for on-prem deployment.)

<b>RAM</b>	16GB
<b>Disk Space</b>	128GB (Dependent on number of endpoints and data retention period.)
<b>CPU Cores</b>	6 or more recommended
<b>Installation Reqs.</b>	<ul style="list-style-type: none"><li>• Self-deployment: Latest version of Docker installed</li><li>• OVA-deployment: ESXi 7.0 or later</li></ul>

## ZeroLock Bidirectional API-First Architecture

<b>Documentation</b>	Visit <a href="https://api.zerolock.com">api.zerolock.com</a> for a full API
<b>Existing Integrations</b>	<ul style="list-style-type: none"><li>• SIEM: Splunk, Sumo Logic, Elastic</li><li>• SOAR: Swimlane</li><li>• Incident API: Veeam</li></ul>

## 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.



Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.  
Linux® is the registered trademark of Linus Torvalds.

©Vali Cyber, Inc. | [valicyber.com](https://valicyber.com)