ZeroLock® Protecting Hypervisors for Healthcare Institutions

Secure Patient Care Starts at the Hypervisor

Healthcare organizations are required to safeguard ePHI — but ePHI doesn't exist in isolation. It lives across virtualized environments where a single compromised hypervisor can take down the infrastructure supporting patient care. Across HIPAA, NIST CSF 2.0, HITRUST, HICP, and NIST SP 800-53, the expectation is consistent: protect not just the data, but the systems that enable access to it. ZeroLock® addresses that requirement at the hypervisor layer with preemptive capabilities.

Access Control & Identity

Framework requirements mandate that organizations limit access to systems handling ePHI to authorized users only, including privileged administrative access to underlying infrastructure. ZeroLock enforces CLI multifactor authentication for SSH and policy-based process controls at the hypervisor layer, directly addressing the admin credential gap these controls are designed to close.

HIPAA §164.312(a)(1) · NIST CSF PR.AA · NIST SP 800-53 AC-2/IA-2 · HICP

Threat Detection & Malware Protection

HIPAA requires covered entities to identify and respond to suspected security incidents. NIST and HITRUST further require continuous monitoring and malware protection across systems that store or process sensitive data. ZeroLock's behavioral runtime monitoring detects fileless and in-memory attacks at the hypervisor layer in real time.

HIPAA §164.308(a)(6) · NIST CSF DE.CM · NIST SP 800-53 SI-3 · HITRUST Endpoint Protection

Data Integrity & Incident Response

HIPAA integrity controls require that ePHI not be improperly altered or destroyed. Incident response requirements — across HIPAA, NIST, and Joint Commission resilience expectations — call for the ability to contain and recover from security events without extended downtime. ZeroLock's automated rollback restores affected VMs in milliseconds, while tamper protection and persistence removal prevent reinfection.

HIPAA §164.312(c)(1) · §164.308(a)(6) · NIST CSF RS/RC · NIST SP 800-53 SI-7 · Joint Commission

Risk Analysis & Audit Readiness

HIPAA requires a thorough assessment of risks to systems that store, transmit, or process ePHI — including the virtual infrastructure those systems run on. ZeroLock provides continuous visibility into hypervisor activity and generates audit trails and security logs that support risk documentation and compliance reporting.

HIPAA §164.308(a)(1) · NIST CSF GV/ID · HITRUST Vulnerability Management · NIST SP 800-53 SI-7

Layered Defense & Compensating Controls

HITRUST and HICP both emphasize defense-in-depth — particularly for environments running legacy or unpatched systems where traditional controls cannot be applied. ZeroLock's runtime controls and virtual patching provide a documented compensating layer at the hypervisor, supporting HITRUST certification efforts and HICP ransomware mitigation guidance.

HITRUST CSF · HICP · NIST SP 800-53

> "We had nothing protecting us at the hypervisor level, and until ZeroLock, there really wasn't anything available at that level. We moved hypervisor security up the list once we found that there was a product… from discovery to implementation, this may be one of our quickest turnarounds."
>
> **—Executive Director of IT**
> **A US-based large-scale healthcare institution**

For the 15th year in a row, healthcare saw the costliest breaches across industries, reaching $7.42 million.

IBM
Costs of a Data Breach 2025

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) • 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® is the only Broadcom-certified solution that delivers preemptive security with CLI-MFA, exploit prevention, and AI-driven behavioral detection. By operating at the hypervisor layer, ZeroLock stops threats in real time without performance impact. 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