ZeroLock® Compliance Overview for SOC 2

Designed to support SOC 2's stringent security, availability, and confidentiality requirements, ZeroLock® delivers preemptive, runtime protection purpose-built for hypervisors. By combining AI-driven behavioral detection, real-time threat prevention, and automated remediation, ZeroLock safeguards virtualized environments against advanced attacks and helps organizations maintain compliance, reduce risk exposure, and ensure the integrity of their hypervisors.

Function	Common Criteria Principles	Applicable Features
Change & Risk Management	CC2.1 – Quality Information for Internal Control CC3.4 – Identifies & Assesses System Changes	• Code Validation Checks • Canary Files
Access Control & Authentication	CC6.1 – Logical Access Security CC6.2 – User Registration CC6.3 – Role-Based Access Control (RBAC)	• CLI MFA • Program Execution Rules • File & Network Access Rules
Threat Detection & Prevention	CC5.2 – Control Activities Over Technology CC6.6 – Boundary Protection CC6.8 – Unauthorized and Malicious Code Protection CC7.1 – Configuration and Vulnerability Management CC7.2 – Security Event & Anomaly Detection CC7.3 – Incident Detection & Response	• Tampering Detection • Ransomware Detection • Cryptojacking Detection • Virtual Patching • Email Alerts
Data Protection & Encryption	CC6.7 – Secure Data Transmission	• Use of Cryptography • SSO Integration
Incident Response & Recovery	CC7.4 – Incident Containment & Remediation CC7.5 – Recovery & Preventive Measures CC9.1 – Business Continuity & Risk Mitigation	• Automated File Rollback • Endpoint Quarantine • Remote Shell

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