ZeroLock® Compliance Overview for SOC 2

ZeroLock® is designed to meet SOC 2's stringent security, availability, and confidentiality requirements while providing comprehensive hypervisor protection. By combining AI-driven behavioral detection, real-time threat prevention, and automated remediation, ZeroLock safeguards virtualized environments against advanced attacks. Its proactive defense framework 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)	• SSH-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	• ESXi, 6.7+ (Older versions supported upon request.) • Nutanix, AHV-2017+ • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization (RHEV), 3.6+ • KVM, Kernel 3.5+
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	512GB (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 • SOAR: Swimlane • Incident API: Veeam

About Vali Cyber

Vali Cyber, Inc. was founded in 2020 with the mission of addressing the specific security needs of Linux and its derivatives. By focusing on creating a Linux-first security solution with increased efficacy and reduced Total Cost of Ownership (TCO), we created the ZeroLock platform. Our approach puts clients in control of their hypervisor & Linux security by reducing analyst and computational overhead, while simultaneously ensuring uptime with state-of-the-art AI behavioral techniques to stop attacks and automated file rollback to restore your most critical data in milliseconds. Imagine detecting and fully remediating a ransomware attack on your hypervisor in real-time...that dream has become reality.

MADE IN THE U.S.A.

valicyber