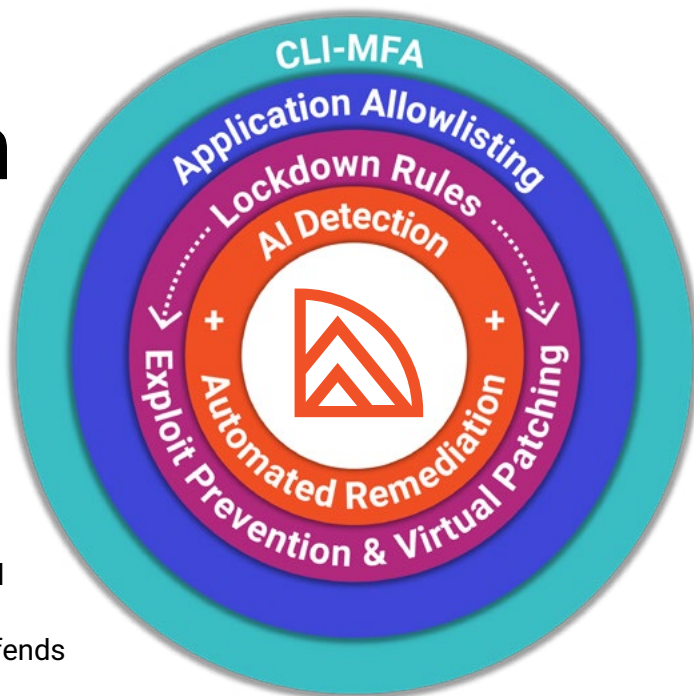


ZeroLock[®]

Defense-in-Depth for vCenter

Securing the Management Plane

vCenter is under attack, with high severity CVEs being found more often and more quickly by AI. Disclosure-to-exploitation windows are collapsing to minutes. Why vCenter? Just one vulnerability or compromised credential in the hands of an attacker delivers them administrative privileges across the entire VMware estate. ZeroLock[®] defends vCenter with novel techniques that preserve performance and stability while helping to ensure uptime. This capability works seamless with our Hypervisor Security to allow for true defense-in-depth protection of your virtualized infrastructure.



Sources: <https://labs.cloudsecurityalliance.org/research/csa-research-note-vmware-vcenter-cve-2026-59310-exploitation/>

PREEMPT: Stop attacks before they have a name.

Traditional defenses are reactive, waiting for a patch or an alert. By then, the attacker already has the keys to the infrastructure. ZeroLock enforces prevention at the control plane itself, closing off attack pathways and protecting the vCenter appliance before a CVE is ever assigned a number.

- Exploit Prevention & Virtual Patching
- Lockdown Rules for execution and file paths
- Application Allowlisting
- CLI-MFA on appliance shell access
- Data Exfiltration & File Access Prevention
- Canary Files & Tamper Protection

PROTECT: Ensuring business continuity when the console is the target.

With AI-driven attacks continuing to evolve, resilience matters as much as prevention. Patented AI Detection and Automated Remediation catch malware implants, log tampering, and hypervisor access behavior in real time. They also automatically remove malicious files and restore altered data in seconds, keeping the brain of your operation running under attack.

- Ransomware Protection
- Wiperware Protection
- Real-time Threat Remediation
- Automated File Rollback
- Attacker Persistence Removal
- Fully Automated Process Tree Creation

PERFORM: Designed for how your team actually works.

ZeroLock installs onto vCenter in one line and runs as a single lightweight agent with no kernel modules. Detection is behavioral, so there are no signatures to chase, and every event is available to the SIEM and SOAR you already run, streamlining your management overhead.

- No kernel modification or modules required
- Behavior-based, no signatures to update
- Lightweight single agent (50MB RAM)
- One-line deployment
- API-first for SIEM/SOAR integration
- Works in air-gapped environments

Schedule your demo today! info@valicyber.com



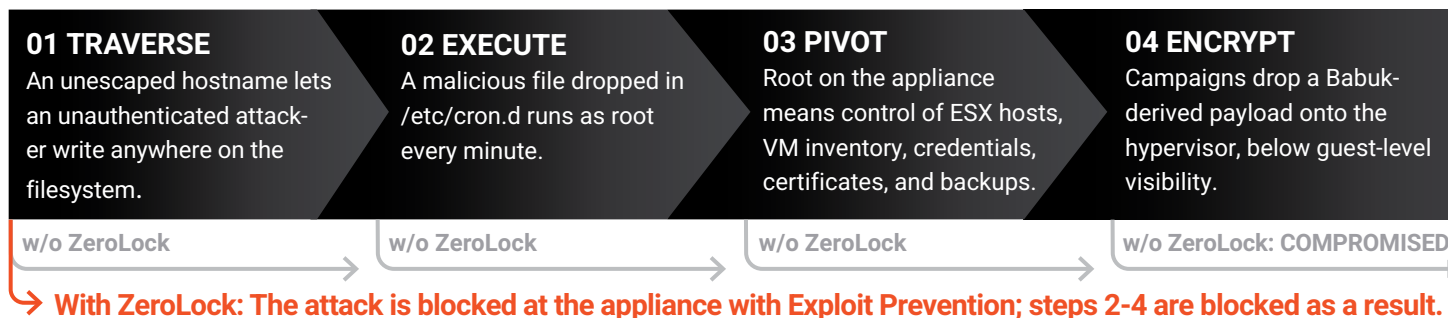
Vali Cyber[®] and ZeroLock[®] are trademarks of Vali Cyber, Inc.
All other trademarks are the property of their respective owners.

©Vali Cyber, Inc. | valicyber.com



The Case for Preemptive vCenter Security: CVE-2026-59310

Directory traversal in the vCenter Syslog Server enabling unauthenticated RCE as root. CVSS 9.8. Disclosed 29 July 2026 (VMSA-2026-0006). No vendor workaround available; patch only...unless you have ZeroLock:



ZeroLock Agent Requirements for vCenter

OS	VMware vCenter Server Appliance (VCSA)*, 6.7+ (Older versions supported upon request.)
Processor	x86-64
Footprint	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)

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

Footprint & Cores	RAM: 16GB; Disk Space: 128GB; 6 or more CPU cores 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

*Broadcom does not currently support third party software installed on vCenter. If vCenter support is ever needed, ZeroLock can be removed with a one-click uninstall and reinstalled afterward with a single-line deployment.

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.



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