ZeroLock

Stopping the Fairlife Playbook on ESXi

Reports indicate the attack that halted Fairlife's US production targeted the Nutanix hypervisor[1], the one place in the technology stack with no runtime security. The same playbook works against VMware ESXi. Each attack stage below maps to a ZeroLock control that prevents it.

Threat Actions

01 Enable SSH
Turn on administrative services to gain command line access to the host.

02 Reach the Host
SSH straight into ESXi. ESXi and Nutanix have no native MFA on shell access.

03 Shut Down VMs
Turn off VMs to enable encryption of virtual hard disk files.

04 Encrypt Data
Delete the snapshots, then encrypt every VM on the datastore.

COMPROMISED → COMPROMISED → COMPROMISED → COMPROMISED

With ZeroLock: Tamper Prevention
ZeroLock prevents tampering with hardened configurations.
THREAT BLOCKED.

With ZeroLock: CLI-MFA
Every shell session requires MFA using a secure, rotating time-based token.
THREAT BLOCKED.

With ZeroLock: Lockdown Rules
Fine-grained access control rules block activity, like maliciously killing VMs.
THREAT BLOCKED.

With ZeroLock: Ransomware Detection
State-of-the-art AI-behavioral models prevent encryption before it does damage.
THREAT BLOCKED.

Real-World Threat: The Anubis Attack on Fairlife

What Is Confirmed

On July 16, 2026, Coca-Cola disclosed unauthorized access to Fairlife systems, including production systems. US production was suspended.[1]

What the Actor Claims

On July 20, Anubis listed Fairlife on its leak site, claiming it encrypted the Nutanix hypervisor infrastructure and stole 1 TB of data.[1] Those claims are unverified.

Why the Pattern Matters

The same pattern Anubis applied to Nutanix also works on VMware ESXi. These attacks are highly disruptive. When the hypervisor goes down, every workload goes with it.

SOURCE

[1] https://www.bleepingcomputer.com/news/security/anubis-ransomware-claims-coca-cola-fairlife-attack-threatens-data-leak/

See it stopped in your environment today! info@valicyber.com

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) • VCF & 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® 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.

MADE IN THE U.S.A.

valicyber®