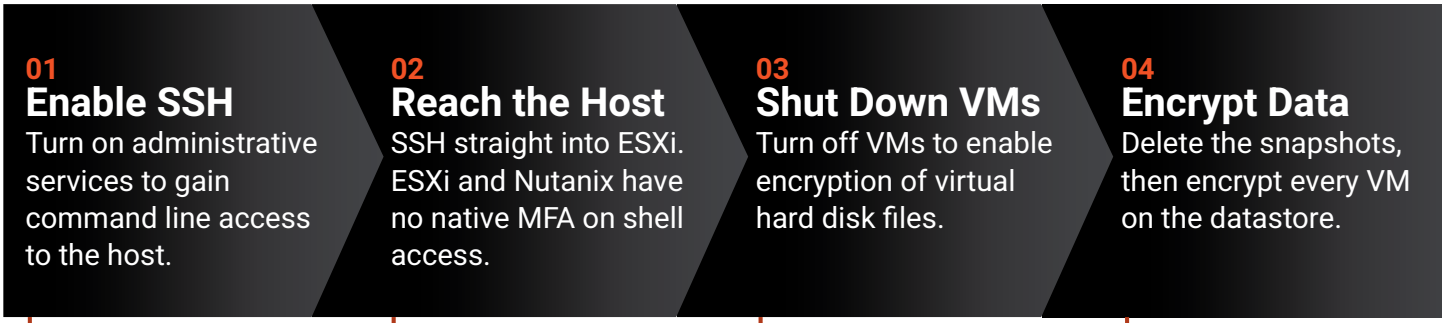
ZeroLock

Stopping the Fairlife Playbook on ESX

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 ESX. Each attack stage below maps to a ZeroLock control that prevents it.

Threat Actions



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 ESX. 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

Vali Cyber® and ZeroLock® are trademarks of Vali Cyber, Inc.
Linux® is the registered trademark of Linus Torvalds.

©Vali Cyber, Inc. | valicyber.com

ZeroLock

ZeroLock Endpoint Agent Requirements for Hypervisors

OS	• VMware Cloud Foundation 9.X • VMware ESX, 6.7+ (Older versions supported on request.) • Nutanix-managed ESX, 6.7+ • Nutanix AHV 2017+* • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • XCP-ng 8.3+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization, 3.6+ • HPE Morpheus, 8.0+ • Dell VxRail, 4.8+ • KVM, Kernel 3.5+ *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, CrowdStrike Next-Gen • SOAR: Swimlane • Incident API: Veeam

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.



MADE IN THE U.S.A.

valicyber®

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