MITRE ATT&CK ESXi: Vali Cyber® ZeroLock® Quick Map

INITIAL ACCESS

- **T1190: Exploit Public-Facing Application** — Resolved with: Exploit Prevention, Virtual Patching
- **T1078: Valid Accounts** — Resolved with: CLI MFA

EXECUTION

- **T1059: Command & Scripting Interpreter** — Resolved with: Application Filtering, Exploit Prevention
- **T1675: ESXi Administration Command** — Resolved with: CLI MFA, Exploit Prevention
- **T1053: Scheduled Task/Job** — Resolved with: AI Behavioral Detection, Application Filtering, Exploit Prevention

PERSISTENCE

- **T1098: Account Manipulation** — Resolved with: CLI MFA, AI-Behavioral Detection, Exploit Prevention
- **T1037: Boot or Logon Initialization Scripts** — Resolved with: Application Filtering, Exploit Prevention
- **T1554: Compromise Host Software Binary** — Resolved with: Application Filtering, Exploit Prevention
- **T1136: Create Account** — Resolved with: Application Filtering, Exploit Prevention
- **T1053: Scheduled Task/Job** — Resolved with: AI-Behavioral Detection, Application Filtering, Exploit Prevention
- **T1505: Server Software Component** — Resolved with: Application Filtering, Exploit Prevention
- **T1078: Valid Accounts** — Resolved with: CLI MFA

PRIVILEGE ESCALATION

- **T1098: Account Manipulation** — Resolved with: CLI MFA, AI-Behavioral Detection, Exploit Prevention
- **T1037: Boot or Logon Initialization Scripts** — Resolved with: Application Filtering, Exploit Prevention
- **T1611: Escape to Host** — Resolved with: Exploit Prevention Virtual Patching
- **T1053: Scheduled Task/Job** — Resolved with: AI Behavioral Detection, Application Filtering, Exploit Prevention
- **T1078: Valid Accounts** — Resolved with: CLI MFA

DEFENSE EVASION

- **T1140: Decode/ Deobfuscate Files or Info** — Resolved with: Application Filtering, Exploit Prevention
- **T1480: Execution Guardrails** — Resolved with: Application Filtering, Exploit Prevention
- **T1222: File & Directory Permission Mod.** — Resolved with: AI-Behavioral Detection Exploit Prevention
- **T1564: Hide Artifacts** — Resolved with: Application Filtering, Exploit Prevention
- **T1562: Impair Defenses** — Resolved with: AI-Behavioral Detection, Exploit Prevention
- **T1070: Indicator Removal** — Resolved with: Exploit Prevention Virtual Patching
- **T1036: Masquerading** — Resolved with: Application Filtering, Exploit Prevention
- **T1027: Obfuscated Files or Information** — Resolved with: CLI MFA, Application Filtering, Exploit Prevention
- **T1078: Valid Accounts** — Resolved with: CLI MFA

CREDENTIAL ACCESS

- **T1110: Brute Force** — Resolved with: CLI MFA

DISCOVERY

- **T1087: Account Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1083: File & Directory Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1654: Log Enumeration** — Resolved with: Exploit Prevention, Virtual Patching
- **T1057: Process Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1018: Remote System Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1518: Software Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1082: System Information Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1016: System Network Configuration Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1049: System Network Connections Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1124: System Time Discovery** — Resolved with: Exploit Prevention, Virtual Patching
- **T1673: Virtual Machine Discovery** — Resolved with: Exploit Prevention, Virtual Patching

LATERAL MOVEMENT

- **T1210: Exploit. of Remote Services** — Resolved with: Exploit Prevention, Virtual Patching
- **T1570: Lateral Tool Transfer** — Resolved with: Application Filtering, Exploit Prevention
- **T1021: Remote Services** — Resolved with: CLI MFA, Exploit Prevention

COLLECTION

- **T1005: Data from Local System** — Resolved with: Exploit Prevention, Virtual Patching
- **T1074: Data Staged** — Resolved with: Exploit Prevention, Virtual Patching

COMMAND & CONTROL

- **T1071: Application Layer Protocol** — Resolved with: CLI MFA, Exploit Prevention
- **T1132: Data Encoding** — Resolved with: Exploit Prevention, Virtual Patching
- **T1001: Data Obfuscation** — Resolved with: Exploit Prevention, Virtual Patching
- **T1568: Dynamic Resolution** — Resolved with: Exploit Prevention, Virtual Patching
- **T1573: Encrypted Channel** — Resolved with: Exploit Prevention, Virtual Patching
- **T1105: Ingress Tool Transfer** — Resolved with: Application Filtering, Exploit Prevention
- **T1104: Multi-Stage Channels** — Resolved with: Application Filtering, Exploit Prevention
- **T1095: Non-Application Layer Protocol** — Resolved with: Exploit Prevention, Virtual Patching
- **T1571: Non-Standard Port** — Resolved with: Exploit Prevention, Virtual Patching
- **T1572: Protocol Tunneling** — Resolved with: Exploit Prevention, Virtual Patching
- **T1008: Fallback Channels** — Resolved with: Exploit Prevention, Virtual Patching
- **T1090: Proxy** — Resolved with: Exploit Prevention, Virtual Patching
- **T1665: Hide Infrastructure** — Resolved with: Exploit Prevention, Virtual Patching
- **T1102: Web Service** — Resolved with: Application Filtering, Exploit Prevention

EXFILTRATION

- **T1030: Data Transfer Size Limits** — Resolved with: Application Filtering, Exploit Prevention
- **T1048: Exfiltration Over Alt. Protocol** — Resolved with: Application Filtering, Exploit Prevention
- **T1041: Exfiltration Over C2 Channel** — Resolved with: Exploit Prevention, Virtual Patching
- **T1567: Exfiltration Over Web Service** — Resolved with: Exploit Prevention, Virtual Patching

IMPACT

- **T1531: Account Access Removal** — Resolved with: CLI MFA, AI-Behavioral Detection, Exploit Prevention
- **T1485: Data Destruction** — Resolved with: CLI MFA, AI-Behavioral Detection, Automated Remediation
- **T1486: Data Encrypted for Impact** — Resolved with: AI-Behavioral Detection, Automated Remediation
- **T1491: Defacement** — Resolved with: Exploit Prevention, Automated Remediation
- **T1490: Inhibit System Recovery** — Resolved with: AI-Behavioral Detection, Automated Remediation, Exploit Prevenetion
- **T1489: Service Stop** — Resolved with: Exploit Prevention, AI-Behavioral Detection
- **T1529: System Shutdown/Reboot** — Resolved with: AI-Behavioral Detection, Automated Remediation, Exploit Prevention

100% of TTPs
mitigated with ZeroLock*

Quick Color Key

- CLI MFA
- Application Filtering
- Exploit Prevention
- Virtual Patching
- AI-Behavioral Detection
- Automated Remediation

Multiple feature coverage depicted by corresponding color gradients

***When properly configured and fully deployed.**

valicyber.com

valicyber

Assess Your ESX and vCenter Risk

For each statement, select: Yes = Confident, validated control in place (2 points) | Somewhat = Partial, inconsistent, or untested (1 point) | No = Not in place / unknown (0 points)

INITIAL ACCESS

___ Access to ESX hosts and management interfaces is restricted and not directly exposed.

___ MFA is enforced across all hypervisor and vCenter access paths.

___ We can detect unauthorized access attempts to ESXi in real time.

___ Our vCenter and ESX hypervisors are fully patched and up to date.

Score: ___ / 8

DEFENSE EVASION

___ We maintain security visibility at the hypervisor layer (not just inside VMs).

___ We can detect tampering with security controls on ESX in real time.

___ We can identify attacker activity that mimics legitimate behavior as it occurs.

Score: ___ / 6

COLLECTION

___ We monitor access to VM disks, snapshots, and memory in real time.

___ Bulk or unusual data access across VMs is detectable as it occurs.

___ Snapshot and backup access is controlled and audited.

Score: ___ / 6

EXECUTION

___ We have visibility into commands executed directly on ESX hosts in real time.

___ We can detect suspicious or unauthorized execution at the hypervisor layer as it occurs.

___ We can distinguish legitimate admin activity from malicious behavior in real time.

Score: ___ / 6

CREDENTIAL ACCESS

___ ESX and vCenter credentials are securely stored and regularly rotated.

___ We detect suspicious authentication or credential misuse in real time.

___ Service accounts and automation credentials are tightly controlled.

Score: ___ / 6

COMMAND & CONTROL

___ Outbound communication from ESXi hosts is restricted and monitored in real time.

___ We can detect abnormal external connections or beaconing as it occurs.

___ Management channels are monitored for misuse in real time.

Score: ___ / 6

PERSISTENCE

___ We monitor for unauthorized changes to ESX configurations and services in real time.

___ We can detect persistence mechanisms that survive reboot.

___ We regularly validate the integrity of hypervisor configurations.

Score: ___ / 6

DISCOVERY

___ We can detect enumeration of VMs, datastores, and infrastructure in real time.

___ Access to infrastructure metadata is restricted by role.

___ Abnormal discovery activity would trigger alerts as it occurs.

Score: ___ / 6

EXFILTRATION

___ Data movement from ESX hosts is monitored in real time.

___ Large or unusual exports (VMs, snapshots) trigger alerts as they occur.

___ Backup/replication channels are secured against misuse.

Score: ___ / 6

PRIVILEGE ESCALATION

___ Least privilege is enforced across ESX and vCenter access.

___ Privileged accounts are segmented to limit blast radius.

___ We detect abnormal privilege changes or misuse in real time.

Score: ___ / 6

LATERAL MOVEMENT

___ ESX hosts and management planes are segmented to limit movement.

___ We can detect pivoting across hosts, clusters, or vCenter in real time.

___ A single host compromise can be contained.

Score: ___ / 6

IMPACT

___ We can detect and stop actions impacting multiple VMs simultaneously as they occur.

___ We can isolate a compromised host quickly.

___ Backups and recovery mechanisms are protected from tampering.

___ We can recover critical workloads rapidly after a hypervisor incident.

Score: ___ / 8

TOTAL POINTS: ___ / 76

What does your score mean?

0–19: HIGH RISK
Hypervisor-level controls are limited or absent.
An attacker could gain access and impact multiple workloads with little resistance—and minimal real-time visibility.

20-38: EXPOSED
Controls exist, but not where or when it matters.
Without real-time enforcement at the hypervisor layer, attackers can bypass defenses using valid credentials and native tools. **This is where most organizations sit and what most modern attack playbooks are built for.**

39-57: PARTIALLY SECURE
Some areas are well-defended, but coverage is inconsistent.
Gaps in real-time detection and hypervisor-layer control leave paths for attackers to operate and achieve broad impact before containment.

58-76: PREEMPTIVELY SECURE
Controls operate in real time at the hypervisor layer.
Threats can be stopped early, limiting spread, impact, and time to containment.

valicyber.com

valicyber