MITRE ATT&CK v17 ESXi Matrix: ZeroLock® Quick Map

INITIAL **ACCESS**

T1190: Exploit T1059: Command & Public-Facing Applica Scripting Interpreter Resolved with: Lockdown Rules Application Filtering **Virtual Patching Lockdown Rules**

T1078: Valid Accounts

T1675: ESXi SSH MFA,

> Task/Job Resolved with: Application Filtering. Lockdown Rules

T1554: Compromise **Host Software Binary** Resolved with: **Application Filtering Lockdown Rules**

Application Filtering

T1136: Create Accoun Resolved with Application Filtering

T1053: Scheduled Application Filtering. Lockdown Rule

T1505: Server **Software Component** Resolved with: Application Filtering, **Lockdown Rules**

T1078: Valid Accounts **SSH MFA**

Resolved with: havioral Detec

Lockdown Rules T1037: Boot or Logon Initialization Scripts Resolved with:

Task/Job Resolved with: **Al Behavioral Detection Application Filtering** Lockdown Rules

Virtual Patching

T1078: Valid Accounts **SSH MFA**

> Resolved with: **Lockdown Rules**

Resolved with: Application Filtering

SSH MFA

EXECUTION

PERSISTENCE PRIVILEGE ESCALATION

AI-Behavioral Detec

Lockdown Rules T1037: Boot or Logon Initialization Scripts Resolved with:

Resolved with: Application Filtering **Application Filtering Lockdown Rules Lockdown Rules** T1222: File & T1611: Escape to Hos

Directory Permission Mod. Lockdown Rules,

DEFENSE

EVASION

T1140: Decode/

Deobfuscate Files or Info

Resolved with:

Lockdown Rules

T1480: Execution

Guardrails

T1564: Hide Artifacts Resolved with: lication Filtering Lockdown Rules

T1562: Impair Defenses **AI-Behavioral Detection** Lockdown Rules

T1070: Indicator

Lockdown Rules

Γ1027: Obfuscated Files or Information Resolved with: SSH MFA, Application Filtering Lockdown Rules

T1078: Valid Accounts

100% of ESXi TTPs mitigated with ZeroLock*

Quick Map Color Key

SSH MFA

Application Filtering

Lockdown Rules

Virtual Patching **AI-Behavioral Detection**

Automated Remediation

Multiple feature coverage depicted by corresponding color gradients

CREDENTIAL **DISCOVERY** ACCESS

> T1110: Brute Force **SSH MFA**

T1087: Account Discovery **Virtual Patching**

T1083: File &

Directory Discover

T1654: Log

Enumeration

Lockdown Rules

Virtual Patching

T1210: Exploit. of **Remote Services** Resolved with: **Virtual Patching**

T1570: Lateral

Tool Transfer

Resolved with

Application Filtering

Lockdown Rules

LATERAL

MOVEMENT

Services Resolved with: SSH MFA,

T1057: Process Discovery **Lockdown Rules** Virtual Patching

T1018: Remote **Lockdown Rules**

T1518: Software Discovery **Lockdown Rules**

Information Discovery Resolved with: Lockdown Rules, **Virtual Patching**

T1016: System Networl Configuration Discovery Resolved with **Lockdown Rules Virtual Patching**

T1049: System Networl Resolved with: Lockdown Rules,

> T1124: System **Lockdown Rules**

T1673: Virtual **Machine Discovery** Lockdown Rules, **Virtual Patching**

COLLECTION COMMAND

T1005: Data from **Local System Virtual Patching**

Resolved with:

Lockdown Rules

T1074: Data Staged T1132: Data Encoding Resolved with Lockdown Rules, Virtual Patching

> T1001: Data Resolved with

Layer Protocol

Resolved with: SSH MFA,

T1568: Dynamic Lockdown Rules, Virtual Patching

Channe

Lockdown Rules Virtual Patching

T1573: Encrypted Resolved with: Lockdown Rules, Virtual Patching

Channels Resolved with: Virtual Patching

T1665: Hide Infrastructure Resolved with: **Virtual Patching**

T1105: Ingress Tool Transfer Resolved with: **Application Filtering** Lockdown Rules

T1104: Multi-Stage Channels Application Filtering **Lockdown Rules**

T1095: Non-Applicati Resolved with: Lockdown Rules. Virtual Patching

T1571: Non-Standar Port Resolved with: **Virtual Patching**

T1572: Protocol Tunneling Resolved with Lockdown Rules, **Virtual Patching**

T1090: Proxy Lockdown Rules, **Virtual Patching**

T1102: Web Service Resolved with: **Application Filtering** Lockdown Rules



T1030: Data **Transfer Size Limits** Resolved with: **Application Filtering**

T1048: Exfiltration

Over Alt. Protocol

Resolved with:

Lockdown Rules

T1041: Exfiltration

Over C2 Channel

Lockdown Rules

T1567: Exfiltration

Over Web Service

Access Removal Resolved with: Al-Behavioral Detection

IMPACT

SSH MFA, Al-Behaviora

Encrypted for Impact AI-Behavioral Detecti

T1491: Defacement Lockdown Rules, Automated Remediati

T1490: Inhibit System Recovery **AI-Behavioral Detection**

T1489: Service Stop Lockdown Rules, AI-Behavioral Detection

T1529: System Resolved with:

