Rimini Protect™

Advanced Hypervisor Security (AHS)

Powered by Vali Cyber®

KEY BENEFITS

- Realtime file remediation
- Automated protection
- Maintained system stability
- Less than 5% performance impact
- Flexible access control

r_mod.use_y = True
r_mod.use_z = False
eration == "MIRROR_Z":
r_mod.use_x = False
r_mod.use_y = False
r_mod.use_z = True
ection at the end -add back the deselected mirror modifier
.select= 1
_ob.select=1
ext.scene.objects.active = modifier_ob
elected" + str(modifier_ob)) # modifier ob is the active ob
ror_ob.select = 0

The Business Challenge

Hypervisors — the software responsible for creating, running, and managing virtual machines — face significant risk in the current landscape. Common attacks on hypervisors include not only the growing list of known vulnerabilities maintained by NIST in the National Vulnerability Database[1] but also ransomware, compromised credentials, and misconfigurations of enterprise software.

Exploits leveraging known vulnerabilities are on the rise

Exploits against hypervisors can be particularly devastating. One hypervisor typically manages dozens of virtual machines[2], which are essential for handling critical business workflows and processes. If an exploit compromises a hypervisor, it could gain access to all the virtual machines on that host and their data. CrowdStrike reaffirmed this risk in a recent blog post:

> "More and more threat actors are recognizing that the lack of security tools, lack of adequate network segmentation of ESXi interfaces, and ITW vulnerabilities for ESXi create a target-rich environment."[3]

The number of groups targeting ESXi continues to grow, with attacks ranging from ransomware-as-a-service groups such as Eldorado[4] emerging in mid-2024, to ESXiArgs[5] successfully leveraging existing unpatched vulnerabilities, which compromised nearly 2,000 servers within 24 hours of release.[6]

Ransomware is growing in popularity

Ransomware attacks are at an all-time high as of December of 2024.[7] The number of victims has risen by 43% from Q3 to Q4 of 2024 and is up 47% YoY from 2023 to 2024. Well-known companies have suffered almost a dozen attacks in December of 2024 alone (that we know of), including UK telecommunications giant BT Group, hospitals, and energy companies.[8] Ransomware payments have also shot up from a median of $199 thousand in early 2023 to $1.5 million in June of 2024, with the largest single ransom payment ever revealed coming in at a staggering $75 million.[9]

[1] National Vulnerability Database

[2] ESXi Host Maximums

[3] Hypervisor Jackpotting, Part 3: Lack of Antivirus Support Opens the Door to Adversary Attacks

[4] New Eldorado ransomware targets Windows, VMware ESXi VMs

[5] VMware: VMware Security Response Center (vSRC) Response to 'ESXiArgs' Ransomware Attacks

[6] CyberSecurity Dive: What's known about the ESXiArgs ransomware hitting VMware servers

[7] Reliaquest: Ransomware and Cyber Extortion in Q4 2024

[8] Cyber Management Alliance: December 2024: Major Cyber Attacks, Data Breaches, Ransomware Attacks

[9] Roundup: The top ransomware stories of 2024

STOLEN CREDENTIALS ARE STILL OUR BIGGEST PROBLEM

- Even with the rise in ransomware vulnerability exploits, the 2024 Verizon DBIR report still indicates that credential use is the largest attack vector.[10] Risk and vulnerability assessments conducted by CISA revealed that infiltration of valid accounts were the most common successful attack technique.[11] The group “Codefinger” attacked Amazon in January 2025 by exploiting valid credentials.[12]

MISCONFIGURATIONS ARE EASY TO MISS

- As software enterprise ecosystems grow in complexity and scope, ensuring that the appropriate configurations are applied becomes a challenge. In May of 2024, a massive data leak exposed the biometric information on millions of Indian police, military personnel, and civilians. The cause? A misconfigured (non-password protected) database.[13] Even Microsoft was recently breached due to misconfigured OAuth configurations.[14]

The Rimini Street Solution

Rimini Protect Advanced Hypervisor Security (AHS) powered by Vali Cyber is the industry’s first purpose-built hypervisor security solution. It’s specifically designed to help defend against ransomware and other common malware-based attacks targeting Linux-based hypervisors, including VMware ESXi.

EXPLOIT PROTECTION

Lockdown rules associated with this zero-day protection are designed to prevent the exploitation of "Escape to Host" vulnerabilities. These vulnerabilities allow processes to access resources outside their designated virtual machine or container, potentially enabling attacks on multiple virtual machines simultaneously and even allowing for the encryption or export of entire filesystems.

RANSOMWARE PROTECTION

Rimini Protect AHS leverages AI/ML technology to detect malware by the actions it performs, instead of just scanning for easily defeated file hashes. Proprietary algorithms detect and stop traditional and in-memory attacks in real-time with greater than 98% efficacy.

MULTI-FACTOR AUTHENTICATION

Rimini Protect AHS also provides MFA to management interfaces such as SSH as a security control to protect and alert against the attempted use of stolen credentials.

Included with Standard Rimini Support™

Rimini Protect AHS is embedded into Rimini Street’s industry-leading Rimini Support for VMware, offering protection against zero-day vulnerabilities and safeguarding against ransomware and other common malware attacks for VMware’s ESXi hypervisor. Rimini Protect AHS is included with our standard Rimini Support for VMware offering.

[10] Verizon 2024 Data Breach Investigations Report
[11] CISA Analysis: Fiscal Year 2023 Risk and Vulnerability Assessments
[12] Forbes: New Amazon Ransomware Attack—‘Recovery Impossible’ Without Payment
[13] Hackread: Data Leak Exposes 500GB of Indian Police, Military Biometric Data
[14] WIZ: Midnight Blizzard attack on Microsoft corporate environment

Rimini Protect AHS clients leverage the same industry-leading support process and SLAs as Rimini Support, including:

- 10-minute guaranteed response time for P1 critical issues
- Frequent cadence of update communications for every case
- Root-cause analysis to help prevent future issues

Solution Benefits

Realtime file remediation/recovery: Automatically copies and caches deleted or changed (including encrypted) files, helping to ensure zero downtime during and after an attack

Automated protection: Enables quick, easy deployment of lockdown rules to safeguard hypervisors against new attack vectors

Greater access control: Allows granular and flexible access rules to be custom created and applied for filesystems, network access, and program execution

Minimal performance impact: Monitors process behavior to detect attacks, with less than 5% impact on performance

Maintained stability: No modification to the operating system ensures stability

Installation and Managed Service Options

Rimini Protect AHS is easy to leverage with our security professional services team, a global team of over 60 full-time employees dedicated to enterprise software security. With our deep familiarity of your enterprise ecosystems through the everyday support that we provide, Rimini Protect security solutions can also be delivered as fully managed services, providing you with efficient and effective security and risk management outcomes tailored to your business needs.

Need to transition to a new environment as your business needs evolve? Rimini Protect professional security services can assist you with migration, and Rimini Protect Advanced Hypervisor Security offers protection for Linux-based hypervisors currently available on the market!

LET US SHOW YOU HOW THIS WORKS

Contact us for a 30-minute demonstration today!

Rimini Street®

riministreet.com | info@riministreet.com | linkedin.com/company/rimini-street | x.com/riministreet