Rimini Protect™

Advanced Hypervisor Security (AHS)

Propulsé par Vali Cyber®

PRINCIPAUX AVANTAGES

- Remédiation des fichiers en temps réel
- Protection automatisée
- Maintien de la stabilité du système
- Impact sur les performances inférieures à 5 %
- Contrôle d'accès flexible

Le défi professionnel

Les hyperviseurs, c'est-à-dire les logiciels responsables de la création, de l'exécution et de la gestion des machines virtuelles, sont confrontés à des risques importants dans l'environnement actuel. Les attaques courantes contre les hyperviseurs comprennent non seulement la liste croissante de vulnérabilités connues gérées par le NIST dans la base de données nationale de vulnérabilités[1], mais aussi les ransomwares, les informations d'identification compromises et les erreurs de configuration des logiciels d'entreprise.

Les exploits tirant parti de vulnérabilités connues se multiplient

Les exploits contre les hyperviseurs peuvent être particulièrement dévastateurs. Un hyperviseur gère généralement des dizaines de machines virtuelles[2], qui sont essentielles pour gérer les flux de travail et les processus critiques des entreprises. Si un exploit compromet un hyperviseur, il peut accéder à toutes les machines virtuelles de cet hôte et à leurs données. CrowdStrike a rappelé ce risque dans un récent billet de blog :

> « De plus en plus d'acteurs malveillants reconnaissent que le manque d'outils de sécurité, l'absence de segmentation adéquate du réseau des interfaces ESXi et les vulnérabilités informatiques pour ESXi créent un environnement avec de nombreuses cibles. »[3]

Le nombre de groupes ciblant ESXi continue d'augmenter, avec des attaques allant de groupes de ransomware-as-a-service tels qu'Eldorado[4] apparu à la mi-2024, à ESXiArgs[5] tirant parti avec succès des vulnérabilités existantes non corrigées, qui a compromis près de 2 000 serveurs dans les 24 heures suivant leur publication.[6]

Les rançongiciels gagnent en popularité

Le nombre d'attaques par ransomware a atteint un niveau record en décembre 2024.[7] Le nombre de victimes a augmenté de 43 % entre le troisième et le quatrième trimestre de 2024 et de 47 % d'une année sur l'autre de 2023 à 2024. Des entreprises bien connues ont été victimes de près d'une douzaine d'attaques rien qu'en décembre 2024 (à notre connaissance), notamment le géant britannique des télécommunications BT Group, des hôpitaux et des entreprises énergétiques.[8] Les paiements de ransomware ont également grimpé d'une médiane de 199 000 dollars au début de 2023 à 1,5 million de dollars en juin 2024, le paiement de rançon le plus important jamais révélé s'élevant à 75 millions de dollars.[9]

---

[1] Base de données nationale des vulnérabilités
[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 : Ce que l'on sait du ransomware ESXiArgs qui frappe les serveurs VMware
[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

LES IDENTIFIANTS VOLÉS RESTENT NOTRE PRINCIPAL PROBLÈME

› Malgré l'augmentation des exploits de vulnérabilités de ransomware, le rapport DBIR 2024 de Verizon indique toujours que l'utilisation d'identifiants est le plus grand vecteur d'attaque.[10] Les évaluations des risques et des vulnérabilités menées par la CISA ont révélé que l'infiltration de comptes valides était la technique d'attaque réussie la plus courante.[11] Le groupe « Codefinger » a attaqué Amazon en janvier 2025 en exploitant des identifiants valides.[12]

LES ERREURS DE CONFIGURATION SONT FACILES À MANQUER

› À mesure que les écosystèmes d'entreprises logicielles gagnent en complexité et en portée, il devient difficile de s'assurer que les configurations appropriées sont appliquées.

› En mai 2024, une fuite massive de données a révélé les informations biométriques de millions de policiers, militaires et civils indiens. La cause ? Une base de données mal configurée (non protégée par un mot de passe).[13] Même Microsoft a récemment subi une violation en raison de configurations OAuth mal configurées.[14]

La solution de Rimini Street

Rimini Protect Advanced Hypervisor Security (AHS) de Vali Cyber est la première solution de sécurité d'hyperviseur spécifique au secteur. Il est spécifiquement conçu pour aider à se défendre contre les ransomwares et autres attaques courantes basées sur des logiciels malveillants ciblant les hyperviseurs basés sur Linux, y compris VMware ESXi.

PROTECTION CONTRE LES EXPLOITS

Les règles de verrouillage associées à cette protection zero-day sont conçues pour empêcher l'exploitation des vulnérabilités « Escape to Host ». Ces vulnérabilités permettent aux processus d'accéder à des ressources en dehors de leur machine virtuelle ou conteneur désigné, ce qui peut potentiellement permettre des attaques sur plusieurs machines virtuelles simultanément et même permettre le chiffrement ou l'exportation de systèmes de fichiers entiers.

PROTECTION CONTRE LES RANSOMWARE

Rimini Protect AHS s'appuie sur la technologie d'IA et d'apprentissage automatique pour détecter les logiciels malveillants en fonction des actions qu'ils effectuent, au lieu de se contenter d'analyser les hachages de fichiers faciles à contourner. Les algorithmes propriétaires détectent et arrêtent les attaques traditionnelles et en mémoire en temps réel avec une efficacité supérieure à 98%.

AUTHENTIFICATION MULTIFACTORIELLE

Rimini Protect AHS fournit également l'authentification multifacteur aux interfaces de gestion telles que SSH en tant que contrôle de sécurité pour protéger et alerter contre la tentative d'utilisation de données d'identification volées.

Inclus dans le support standard de Rimini™

Rimini Protect AHS est intégré à Rimini Support for VMware, le support de Rimini Street leader du secteur, offrant une protection contre les vulnérabilités zero-day et une protection contre les ransomwares et autres attaques de logiciels malveillants courantes pour l'hyperviseur ESXi de VMware. Rimini Protect AHS est inclus sans frais supplémentaires dans notre offre standard Rimini Support for VMware.

[10] Verizon 2024 Data Breach Investigations Report
[11] CISA Analysis: Fiscal Year 2023 Risk and Vulnerability Assessments
[12] Forbes: Nouvelle attaque de ransomware Amazon — « récupération impossible » sans paiement
[13] Hackread: Data Leak Exposes 500GB of Indian Police, Military Biometric Data
[14] WIZ: WIZ: Midnight Blizzard attack on Microsoft corporate environment

Rimini Street®

Les clients de Rimini Protect AHS bénéficient du même processus de support et des mêmes accords de niveau de service de pointe que Rimini Support, notamment :

- Temps de réponse garanti de 10 minutes pour les problèmes critiques P1
- Fréquence accélérée de mise à jour des communications pour chaque cas
- Analyse des causes profondes pour aider à prévenir les problèmes futurs

Avantages de la solution

Correction et restauration de fichiers en temps réel: copie et met en cache automatiquement les fichiers supprimés ou modifiés (y compris les fichiers chiffrés), afin de garantir zéro interruption pendant et après une attaque

Protection automatisée: permet de déployer rapidement et facilement des règles de verrouillage pour protéger les hyperviseurs contre les nouveaux vecteurs d'attaque

Contrôle d'accès amélioré: Apermet de créer et d'appliquer des règles d'accès précises et flexibles aux systèmes de fichiers, à l'accès au réseau et à l'exécution de programmes

Impact minimal sur les performances: surveille le comportement des processus pour détecter les attaques, avec un impact inférieur à 5 % sur les performances

Stabilité maintenue: aucune modification du système d'exploitation ne garantit la stabilité

Options d'installation et de services infogérés

Rimini Protect AHS est facile à exploiter grâce à notre équipe de services professionnels de sécurité, une équipe mondiale de plus de 60 employés à temps plein dédiée à la sécurité des logiciels d'entreprise. Grâce à notre connaissance approfondie de vos écosystèmes d'entreprise acquise par le biais du support quotidien que nous fournissons, les solutions de sécurité Rimini Protect peuvent également être fournies sous forme de services entièrement gérés, vous offrant ainsi des résultats efficaces en matière de sécurité et de gestion des risques, adaptés aux besoins de votre entreprise.

Vous avez besoin de passer à un nouvel environnement au fur et à mesure que les besoins de votre entreprise évoluent ?

Les services de sécurité professionnels de Rimini Protect peuvent vous aider à effectuer la migration, et Rimini Protect Advanced Hypervisor Security protège les hyperviseurs basés sur Linux actuellement disponibles sur le marché !

LAISSEZ-NOUS VOUS MONTRER COMMENT CELA FONCTIONNE

Contactez-nous dès aujourd'hui pour une démonstration de 30 minutes !

Rimini Street

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