McAfee Server Security Suite Essentials

Protection essentielle des serveurs pour les déploiements physiques, virtuels et dans le cloud

Ces dernières années, le centre de données a connu un changement radical au niveau du stockage, des serveurs, des réseaux et des applications qu'il héberge. La nature hétérogène du centre de données et la transition rapide vers le cloud exigent de nouvelles méthodes pour sécuriser cet environnement. Les professionnels de la sécurité et de l'informatique en entreprise se trouvent ainsi confrontés à un important défi : celui de mettre en place une sécurité unifiée et robuste pour les environnements physiques, virtuels et dans le cloud afin de garantir agilité et rentabilité de l'investissement. McAfee® Server Security Suite Essentials, de la gamme Intel® Security, résout ces problèmes par l'intégration des composants de sécurité essentiels pour la détection des charges de traitement dans le cloud, la protection des serveurs et l'extension de la sécurité dans le cloud.

Principaux avantages

- Détection de tous les serveurs physiques et virtuels, y compris ceux hébergés dans le cloud, et gestion unifiée à partir d'une console centrale
- Sécurité des environnements virtualisés, optimisée de façon à limiter l'impact sur les performances grâce à McAfee MOVE AntiVirus
- Visibilité complète sur l'état de sécurité de toutes les machines virtuelles hébergées dans des clouds publics et privés grâce à McAfee Data Center Connector for VMware vSphere, Amazon Web Services, OpenStack et Microsoft Azure

Détection de toutes les charges de traitement

L'identification des charges de traitement et l'application des stratégies de sécurité adéquates posent souvent des difficultés considérables. Nos rapports d'analyse facilitent la gestion en vous aidant à détecter les terminaux non protégés et à déterminer si les réglementations en matière de sécurité sont respectées. Grâce à des connecteurs pour le logiciel McAfee ePolicy Orchestrator® (McAfee ePO™), McAfee Server Security Suite Essentials vous permet de détecter tous les serveurs physiques et virtuels, y compris ceux hébergés dans des clouds privés et publics. La suite est fournie avec les connecteurs McAfee Data Center Connector for VMware vSphere, Amazon AWS, OpenStack et Microsoft Azure. Ceux-ci vous permettent de surveiller chaque machine virtuelle sur et hors site, et de renforcer son niveau de sécurité par une gestion granulaire des stratégies. Vous bénéficiez d'une visibilité accrue, pour déterminer l'état de protection de la mémoire du système d'exploitation, l'hôte sur lequel s'exécute chaque machine virtuelle, le centre de données ou le cloud qui héberge chaque machine virtuelle, etc.

Protection des serveurs

La suite McAfee Server Security Suite Essentials comprend le logiciel McAfee VirusScan® Enterprise, classé numéro un par NSS Labs pour sa protection contre les exploits « jour zéro » et les attaques par contournement[1]. Outre la protection antimalware classique, elle offre une solution distincte spécialement conçue pour les environnements virtuels. McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus optimise la technologie antivirus pour ces environnements particuliers, en limitant l'impact sur les performances même pour les environnements dynamiques de très grande taille, et en assurant une prise en charge des principaux hyperviseurs.

intel Security

McAfee MOVE AntiVirus est disponible sous forme de solution personnalisée sans agent pour les environnements VMware ou sous forme de solution multiplate-forme compatible avec les environnements équipés d'un hyperviseur KVM, Microsoft Hyper-V, VMware ou Xen.

Bien que l'antivirus soit essentiel à la sécurité, des solutions supplémentaires peuvent s'avérer nécessaires pour neutraliser les menaces avancées. McAfee Host Intrusion Prevention est inclus afin de protéger l'entreprise contre les menaces complexes susceptibles d'être introduites ou autorisées involontairement.

Extension dans le cloud

À mesure que votre entreprise s'étend dans le cloud, il est toujours plus difficile de faire en sorte que les stratégies de sécurité adéquates soient appliquées aux nouvelles charges de traitement activées. McAfee résout ces difficultés en détectant automatiquement les machines virtuelles à mesure qu'elles sont activées dans les clouds publics et privés, qu'elles soient en cours d'exécution ou à l'arrêt. Pour ce faire, il vous suffit d'enregistrer un compte de cloud public dans le logiciel McAfee ePO. Les machines virtuelles peuvent alors être protégées automatiquement à l'aide des stratégies de sécurité appropriées. Le tableau de bord pour la sécurité du centre de données de McAfee offre en outre une visibilité complète sur l'état de la protection et sur les incidents de sécurité survenus dans vos clouds publics et privés.

Optimisation de vos serveurs, optimisation de votre entreprise

L'immense potentiel de la virtualisation et du cloud ne peut être pleinement exploité que si ces environnements sont correctement sécurisés. McAfee propose des solutions de sécurité des serveurs qui n'entravent pas les possibilités de croissance des entreprises tout au long de leur transition. La suite McAfee Server Security Suite Essentials protège les serveurs, qu'ils soient physiques, virtuels ou hébergés dans le cloud, tout en préservant la flexibilité. Elle conjugue les éléments essentiels nécessaires à la protection des serveurs au sein des déploiements physiques, virtuels et dans le cloud.

Pour en savoir plus sur les avantages de McAfee Server Security Suite Essentials, consultez notre site à l'adresse : **www.mcafee.com/fr/products/server-security-suite-essentials.aspx**.

Fonctionnalité	Avantage pratique
Gestion à l'aide d'une console unique	• Gestion unifiée via une seule console pour les serveurs physiques et virtuels, y compris ceux hébergés dans des clouds privés et publics, pour une visibilité accrue sur la sécurité • Aspects opérationnels simplifiés et investissement en temps réduit pour le personnel administratif • Coûts en matériel réduits en raison du nombre limité de serveurs nécessaires
Protection du serveur principal	• Protection antimalware pour les serveurs physiques classée numéro un par NSS Labs pour sa protection contre les exploits « jour zéro » et les attaques par contournement • Grâce à Host Intrusion Prevention, protection des entreprises contre les menaces complexes susceptibles d'être introduites ou autorisées involontairement
Sécurité de la virtualisation	• Protection optimisée des charges de traitement déployées dans les infrastructures virtuelles sans préjudice au niveau des performances et de l'utilisation des ressources • Protection pour plusieurs hyperviseurs dans le centre de données afin d'assurer un niveau de sécurité commun pour tous les types d'hyperviseurs utilisés • Déploiement sans agent optimisé pour les environnements VMware afin d'offrir des performances et une densité de machines virtuelles hors pair
Visibilité complète sur les machines virtuelles au sein des clouds privés et publics	• Détection non seulement des serveurs physiques, mais également des hyperviseurs et des machines virtuelles présentes dans les environnements VMware vSphere, Amazon AWS, OpenStack et Microsoft Azure pour une visibilité complète sur les ordinateurs devant être sécurisés • Découverte des machines virtuelles activées, celles-ci pouvant être automatiquement protégées par des stratégies de sécurité afin de leur assurer le niveau de protection approprié

1. NSS Labs, Inc., Protection & Evasion Test (Test sur la protection et les techniques de contournement), 2013

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com

62336ds_sss-essentials_0316