McAfee Server Security Suite Advanced

Protection avancée des serveurs pour les déploiements physiques, virtuels et dans le cloud, avec listes blanches

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
- Combinaison de listes noires et de listes blanches pour une protection des serveurs physiques et virtuels contre les logiciels malveillants
  - Placement sur liste blanche dynamique pour une protection contre les menaces inconnues qui assure la sécurité permanente des hôtes en empêchant l'exécution d'applications indésirables via McAfee Application Control for Servers
  - Détection continue des modifications apportées aux systèmes sur les sites distants et distribués pour assurer le respect les exigences en matière de conformité

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 Advanced, de la gamme Intel® Security, offre la solution de gestion et de protection des serveurs la plus complète pour les déploiements physiques, virtuels et dans le cloud. Cette suite propose en outre des fonctions avancées de sécurité des serveurs supplémentaires, telles que les listes blanches et le contrôle des modifications, pour aider les entreprises à préserver leur conformité.

Détection de toutes les charges de traitement

L'identification des charges de traitement et l'application des stratégies de sécurité adéquates au sein des déploiements physiques, virtuels et dans le cloud posent souvent des difficultés considérables. Les 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 Advanced vous permet de détecter tous les serveurs physiques et virtuels, y compris ceux hébergés dans des clouds privés et publics. La solution est fournie avec les connecteurs McAfee Data Center Connector for VMware vSphere, Amazon AWS, OpenStack et Microsoft Azure. Ensemble, ceux-ci vous permettent de surveiller toutes les machines virtuelles sur et hors site, et de renforcer leur niveau de protection grâce à des stratégies de sécurité granulaires. Les tableaux de bord offrent des informations sur l'état de la sécurité, notamment sur la protection de la mémoire du système d'exploitation, les relations entre l'hôte de l'hyperviseur et les machines virtuelles, l'emplacement de chaque machine virtuelle, etc.

Principaux avantages (suite)

- Sécurité des environnements virtualisés, optimisée de façon à limiter le plus possible 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

Protection des serveurs

McAfee Server Security Suite Advanced assure à vos serveurs la protection la plus complète qui soit, qu'ils soient physiques, virtualisés ou hébergés dans le cloud. La solution offre en outre un contrôle des modifications et une combinaison unique de technologies de protection par listes noires et listes blanches sans équivalent sur le marché.

McAfee Server Security Suite Advanced inclut McAfee Application Control for Servers, une solution de listes blanches qui permet uniquement aux logiciels approuvés de s'exécuter sur les systèmes. Cette solution de gestion centralisée de listes blanches conjugue un modèle d'approbation dynamique et des fonctionnalités de sécurité innovantes qui bloquent les applications non autorisées et déjouent les menaces persistantes avancées (APT), en vous évitant la lourde tâche de gérer les listes. Les listes blanches réduisent l'impact sur les performances des hôtes en garantissant une protection contre les attaques de type « jour zéro » et les menaces APT sans exiger de mises à jour de signatures.

Afin d'assurer la protection de base du serveur, la suite comprend des solutions antimalware traditionnelles pour les serveurs Microsoft Windows et Linux, notamment McAfee VirusScan® Enterprise, classé numéro un par NSS Labs pour sa protection contre les exploits « jour zéro » et les attaques par contournement. Elle offre en outre 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. 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 protège les entreprises 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 la plate-forme 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 favorisent les possibilités de croissance des entreprises tout au long de leur transition. La suite McAfee Server Security Suite Advanced protège les serveurs, qu'ils soient physiques, virtuels ou hébergés dans le cloud, tout en préservant la flexibilité. Elle assure la protection des serveurs dans ces trois types de déploiements via des solutions avancées afin d'instaurer et de maintenir un niveau de sécurité élevé dans l'ensemble de l'entreprise.

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

Fonctionnalité	Avantage pratique
Listes blanches d'applications	• Réduction considérable de l'impact sur les performances des hôtes par rapport aux contrôles de sécurité appliqués aux terminaux traditionnels • Protection contre les attaques de type « jour zéro » et les menaces APT sans mise à jour des signatures pour un délai de protection réduit • Charge opérationnelle réduite des listes blanches dynamiques par rapport aux anciennes techniques de listes blanches
Contrôle des modifications	• Blocage des modifications non autorisées des configurations, des répertoires et des fichiers système critiques pour empêcher les tentatives d'altération, permettant ainsi aux administrateurs de gagner du temps lors de la résolution des violations de sécurité • Suivi et validation de chaque tentative de modification en temps réel sur le serveur, grâce à la mise en œuvre de la stratégie de modifications par période, source ou ticket d'approbation de modifications • Réduction de l'impact des changements ad hoc ou non autorisés grâce à un contrôle continu
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[1] pour sa capacité à refouler 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 protection 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 qui peuvent se voir automatiquement appliquer 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

62337ds_sss-adv_0316