McAfee Server Security Suite Advanced

Protection complète pour les déploiements physiques, virtuels et dans le cloud, avec listes blanches et contrôle des modifications.

Dans les environnements informatiques complexes actuels, il devient de plus en plus difficile de protéger les nouveaux serveurs et les charges de travail de cloud contre les menaces, toujours plus sophistiquées. Une approche globale est essentielle. McAfee® Server Security Suite Advanced assure une protection cohérente et continue dans l'ensemble des déploiements physiques, virtuels et de cloud public. Cette solution de sécurité complète offre non seulement des fonctions essentielles telles qu'un antivirus, un pare-feu, la prévention des intrusions et des listes blanches pour contrer les attaques de type « jour zéro », mais aussi un contrôle des modifications pour assurer le respect des obligations réglementaires. Son architecture avancée limite l'impact sur les performances des serveurs physiques et virtuels et s'adapte automatiquement aux charges de travail dynamiques exécutées dans le cloud.

Découverte et contrôle instantanés

Grâce à Cloud Workload Discovery, une fonctionnalité clé de McAfee Server Security Suite Advanced, rechercher les failles de sécurité de votre centre de données hybride en constante expansion devient un jeu d'enfant. Destiné aux déploiements de cloud hybride, cet outil prend en charge VMware, OpenStack, AWS et Microsoft Azure. Il offre ainsi une visibilité de bout en bout sur toutes les charges de travail et les plates-formes sous-jacentes. L'identification de contrôles de sécurité trop faibles, de paramètres de pare-feu et de chiffrement peu sûrs et d'indicateurs de compromission tels que le trafic suspect permet une détection plus rapide. Quant au logiciel McAfee® ePolicy Orchestrator® (McAfee ePO™) et aux outils DevOps, ils assurent une neutralisation sans délai des menaces.

La sécurité du cloud peut se révéler complexe, car les charges de travail de cloud sont très diverses et présentent des profils de risques et des exigences de protection qui leur sont propres. L'évaluation réalisée par Cloud Workload Discovery se base sur les stratégies. Elle permet de déterminer facilement les exigences de sécurité des différentes charges de travail, puis de dresser un état des lieux comparatif afin de garantir la protection et la conformité. Une fois les risques de sécurité décelés, vous pouvez optimiser votre protection en seulement quelques clics.

Principaux avantages

- Unification de la gestion de la sécurité des terminaux, des réseaux, des données et des solutions de conformité de McAfee et d'autres éditeurs grâce au logiciel McAfee ePO
- Visibilité, évaluation des risques et mesures correctives grâce à Cloud Workload Discovery pour les déploiements en clouds hybrides
- Listes noires et prévention des intrusions combinées à des listes blanches et au contrôle des modifications, pour la protection antimalware des serveurs physiques et virtuels
  - Protection contre les menaces inconnues grâce au blocage de l'exécution d'applications indésirables
  - Détection continue des modifications apportées aux systèmes, même sur les sites distants et distribués, pour assurer le respect des obligations réglementaires

L'intégration de Cloud Workload Discovery avec la console de gestion McAfee ePO offre aux entreprises un contrôle efficace pour implémenter des solutions de sécurité dans les environnements physiques, virtuels et de cloud. Cette intégration permet aux administrateurs de la sécurité d'utiliser une plate-forme de gestion unique, avec workflows simplifiés, pour gérer les alertes et appliquer les stratégies. Le délai d'identification et de correction des problèmes de sécurité s'en trouve fortement réduit.

Grâce à McAfee Server Security Suite Advanced, les environnements de cloud dynamiques prenant en charge l'architecture DevOps n'ont plus à sacrifier la sécurité au profit de l'agilité. La sécurité est étendue de façon élastique avec les charges de travail de cloud pour assurer une protection continue. En outre, le provisionnement élastique des ressources dans les clouds privés permet d'ajouter ou de supprimer automatiquement des serveurs d'analyse hors ligne du pool des ressources, selon les fluctuations de la demande. Pour les charges de travail AWS et Azure, les utilisateurs peuvent configurer la sécurité au niveau du modèle afin qu'elle s'adapte automatiquement aux variations des charges de travail.

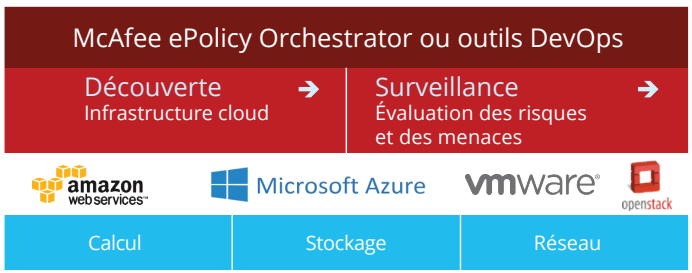

Figure 1. Profitez d'avantages durables grâce à Cloud Workload Discovery.

Protection complète

McAfee Server Security Suite Advanced assure à vos serveurs une protection optimale, qu'ils soient physiques, virtuels ou dans le cloud. La solution offre en outre une protection contre les attaques par débordement de mémoire tampon sur les systèmes Windows 32 et 64 bits, une combinaison unique de technologies de protection par listes noires et listes blanches, et une fonctionnalité de contrôle des modifications sans équivalents sur le marché. Composants de la suite :

- **McAfee Application Control for Servers :** Cette solution de gestion centralisée des listes blanches permet aux seuls logiciels autorisés de s'exécuter sur les serveurs, pour protéger ces derniers contre les logiciels malveillants inconnus, les attaques de type « jour zéro » et les menaces avancées. Son modèle d'approbation dynamique permet de réduire la charge de travail des administrateurs.
- **McAfee Change Control for Servers :** Cette solution offre une détection continue des modifications système sur les sites distants et distribués, de manière à garantir la conformité aux différentes lois et réglementations telles que Sarbanes-Oxley et PCI DSS (Payment Card Industry Data Security Standard).
- **McAfee Endpoint Security — Prévention contre les menaces :** Ce module fait partie intégrante d'un cadre collaboratif et évolutif qui protège les serveurs Microsoft Windows et Linux contre les exploits de type « jour zéro » et les attaques avancées.

Principaux avantages (suite)

- Blocage des menaces inconnues de type « jour zéro » en quelques secondes grâce aux fonctions locales d'analyse de la réputation et d'analyse sandbox
- Sécurité physique et virtuelle optimisée avec impact minimal sur les performances

- **McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) :** Cette solution antimalware est spécialement conçue pour les environnements virtuels. Elle est disponible sous forme d'option personnalisée sans agent pour les environnements VMware NSX et VMware vCNS, ou encore sous forme d'option multiplate-forme compatible avec les principaux hyperviseurs (Microsoft Hyper-V, VMware, KVM, Xen).
- **McAfee Host Intrusion Prevention for Server :** Cette solution protège votre entreprise contre les menaces complexes en surveillant le comportement des codes sur votre serveur et en traquant les activités suspectes.
- **McAfee Endpoint Security — Pare-feu :** Ce module surveille le trafic réseau et Internet, et intercepte les communications suspectes.

McAfee Server Security Suite Advanced peut compléter les informations mondiales sur la réputation de McAfee Global Threat Intelligence (McAfee GTI) par les données locales de McAfee Threat Intelligence Exchange (module vendu séparément). Cette complémentarité permet d'identifier et de neutraliser instantanément les nouveaux malwares. Grâce à McAfee Threat Intelligence Exchange, les solutions de la suite peuvent également collaborer avec McAfee Advanced Threat Defense pour analyser de manière dynamique le comportement des applications inconnues dans un environnement sandbox et immuniser automatiquement tous les terminaux contre les nouveaux logiciels malveillants détectés.

Par ailleurs, McAfee a conclu un partenariat avec Rapid7 pour la gestion des vulnérabilités. La solution Nexpose de Rapid7 détecte et priorise les vulnérabilités, puis envoie une confirmation lorsque toute menace est écartée.

Impact minimal sur les performances

Bien que la sécurité soit un enjeu primordial pour la plupart des entreprises, certaines hésitent à renforcer la protection de leurs serveurs, de peur de nuire aux performances. Grâce à McAfee Server Security Suite Advanced, il est désormais possible de protéger vos serveurs physiques et virtuels sans en sacrifier les performances, même lors de l'analyse antimalware.

Contrairement à la plupart des produits antimalware, McAfee Endpoint Security et McAfee MOVE AntiVirus ne sont pas gourmands en ressources informatiques. McAfee Endpoint Security effectue des analyses rapides et optimise son utilisation du processeur et de la mémoire tout en offrant une protection bien supérieure à toute autre solution antimalware. Quant à l'agent McAfee MOVE AntiVirus, il transfère la charge de l'analyse antimalware des machines virtuelles, pour une protection instantanée avec impact minimal sur la mémoire et le traitement. Enfin, les stratégies distinctes pour l'analyse à la demande et à l'accès confèrent un contrôle plus précis sur les performances et la sécurité.

Optimisation de la sécurité 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. Que vos serveurs soient physiques, virtuels ou hébergés dans le cloud, notre suite de solutions protège leurs charges de travail dans des environnements toujours plus dynamiques.

FICHE TECHNIQUE

Fonctionnalité	Avantage pratique
Gestion à l'aide d'une console unique	▪ Les déploiements physiques, virtuels et dans le cloud sont gérés de manière centralisée pour assurer des contrôles de sécurité plus performants sur l'ensemble des plates-formes (gestion des stratégies, déploiements, visibilité, sécurité). ▪ Les aspects opérationnels sont simplifiés et l'investissement en temps du personnel administratif est réduit.
Découverte et contrôle instantanés	▪ La solution effectue la découverte des serveurs physiques et assure une vue complète sur les charges de travail et plates-formes VMware vSphere, OpenStack, AWS et Microsoft Azure. ▪ La solution évolue avec vos besoins en s'adaptant à vos charges de travail dynamiques exécutées dans le cloud.
Sécurité de la virtualisation	▪ La sécurité des charges de travail est améliorée, sans impact sur les performances et l'utilisation des ressources. ▪ Vous avez le choix entre un déploiement multiplate-forme (principaux hyperviseurs) et un déploiement sans agent pour VMware NSX et VMware vCNS, qui garantit des performances et une densité optimales des machines virtuelles.
Sécurité des clouds publics	▪ Vous pouvez contrôler les paramètres de sécurité de la plate-forme pour AWS et Microsoft Azure, notamment en ce qui concerne le pare-feu et le chiffrement. ▪ Vous disposez de visibilité sur le trafic et les menaces réseau pour sécuriser AWS de manière optimale.
Listes blanches d'applications	▪ L'impact sur les performances des hôtes est très limité comparé aux mécanismes de sécurité traditionnels appliqués aux serveurs. ▪ La protection contre les attaques de type « jour zéro » et les menaces APT n'exige aucune mise à jour des signatures, ce qui réduit le délai de protection. ▪ La charge opérationnelle est réduite grâce aux listes blanches dynamiques.
Contrôle des modifications	▪ La solution bloque les modifications non autorisées au niveau des configurations, des répertoires et des fichiers système critiques pour empêcher toute altération, permettant ainsi aux administrateurs de gagner du temps lors de la résolution des violations de sécurité. ▪ Vous suivez et validez chaque tentative de modification en temps réel sur le serveur, en mettant en œuvre la stratégie de modifications par période, source ou ticket d'approbation de modifications.
Protection du serveur principal	▪ La fonction de protection antimalware bloque les exploits de type « jour zéro » et les attaques avancées. ▪ McAfee Host Intrusion Prevention System protège les entreprises contre les menaces complexes susceptibles d'être introduites ou autorisées involontairement.
Informations locales sur la réputation	▪ La solution bloque les menaces inconnues de type « jour zéro » en quelques secondes grâce à l'intégration avec McAfee Threat Intelligence Exchange (module vendu séparément).

En savoir plus

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**.

McAfee™
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr