

McAfee Server Security

Optimisation de la sécurité avec une incidence minimale sur les performances

Les solutions de sécurité de la génération précédente ne sont pas adaptées aux exigences de sécurité propres aux clouds hybrides. Comme les outils de sécurité traditionnels offrent une visibilité limitée sur l'infrastructure de cloud, il devient difficile de protéger des ressources qui ne sont pas toujours visibles. Faut-il sacrifier la sécurité afin de bénéficier de l'agilité d'une infrastructure de cloud décentralisée, nécessaire à la prise en charge DevOps ? Ou devrez-vous choisir entre la sécurisation des serveurs virtuels et l'optimisation de leurs performances ? En optant pour la sécurité, vous gardez la disponibilité élevée de votre environnement, la protection de vos données et la réussite de votre prochain audit de conformité. En favorisant les performances, vous pourrez sans doute obtenir un retour plus élevé sur vos investissements en technologies, sans oublier les félicitations de votre directeur financier. Entre sécurité ou agilité et performances, le choix est difficile.

Principaux avantages

- Grâce à une découverte et à un contrôle instantanés, vous bénéficiez d'une protection cohérente et continue dans l'ensemble des déploiements physiques, virtuels et de cloud.
- Les serveurs et les charges de travail dans le cloud sont protégés contre les menaces actuelles, toujours plus sophistiquées, avec un impact minimal sur les performances et un ajustement à la demande dans les environnements de cloud dynamiques.
- McAfee Server Security Suite Essentials assure la protection essentielle des serveurs et des charges de travail dans le cloud, avec notamment des fonctions antivirus et de prévention des intrusions optimisées pour les environnements virtualisés.
- Encore plus complète, McAfee Server Security Suite Advanced offre des fonctionnalités supplémentaires, telles que les listes blanches et le contrôle des modifications.

PRÉSENTATION DE SOLUTION

À l'intersection de la sécurité traditionnelle et des exigences liées au cloud

Confrontés à la difficulté de protéger les environnements cloud modernes avec des solutions de sécurité d'ancienne génération, de nombreux directeurs informatiques ont dû faire ce choix. La sécurité doit être aussi agile que les clouds dynamiques où les charges de travail sont ajustées à la demande. Les outils de sécurité conventionnels sont par nature trop statiques pour s'adapter et laissent de larges failles dans la protection du cloud. Confrontés à la charge de traitement que les contrôles de sécurité des serveurs physiques classiques imposent aux systèmes virtuels, ou à la charge d'administration que représentent plusieurs solutions isolées sans interface de gestion centrale, bon nombre d'entreprises décident tout simplement de désactiver leurs outils de protection des terminaux et de placer tous leurs espoirs dans les systèmes de défense du périmètre.

Les exigences complexes de la sécurité des serveurs d'aujourd'hui

Priver les serveurs de cloud stratégiques d'une protection intégrée risque bien de vous mener à la catastrophe, mais force est de constater que les anciennes technologies de sécurité ont été développées dans le but de protéger des serveurs physiques dédiés. Elles ne sont pas adaptées à la virtualisation et ne répondent plus aux besoins des environnements de centre de données hétérogènes actuels. Les solutions de sécurité des serveurs et des charges de travail dans le cloud doivent désormais répondre aux impératifs suivants :

- Offrir une visibilité sur l'infrastructure de cloud et étendre automatiquement la protection avec des charges de travail de cloud dynamiques

- Fournir une protection optimisée, spécialement conçue pour limiter l'impact sur les environnements virtuels
- Proposer une gestion de l'ensemble des contrôles de sécurité de l'environnement de serveurs (physiques, virtuels et dans le cloud) au sein d'une même console

Suites McAfee Server Security

McAfee® Server Security Suite Essentials offre une protection essentielle des serveurs et des charges de travail de cloud, avec notamment des fonctions antivirus et IPS optimisées. McAfee® Server Security Suite Advanced propose une protection encore plus complète des serveurs et des charges de travail dans le cloud grâce à des fonctions supplémentaires telles que les listes blanches avancées pour mettre en échec les attaques de type « jour zéro » et les fonctions de contrôle des modifications pour assurer le respect des obligations réglementaires.

McAfee Server Security Suite Essentials	McAfee Server Security Suite Advanced
Console McAfee ePolicy Orchestrator® (McAfee ePO™)	Console McAfee ePO
Cloud Workload Discovery pour le cloud hybride	Cloud Workload Discovery pour le cloud hybride
Protection antimalware (optimisée pour les machines virtuelles)	Protection antimalware (optimisée pour les machines virtuelles)
Pare-feu	Pare-feu
Prévention des intrusions sur l'hôte	Prévention des intrusions sur l'hôte
	Listes blanches d'applications
	Surveillance de l'intégrité des fichiers

PRÉSENTATION DE SOLUTION

Visibilité sur l'infrastructure de cloud

Rechercher les failles de sécurité de votre centre de données hybride en constante expansion devient un jeu d'enfant grâce à Cloud Workload Discovery, une fonctionnalité clé de McAfee Server Security Suite Advanced et de McAfee Server Security Suite Essentials. 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. En outre, McAfee ePO et les outils DevOps assurent une neutralisation sans délai des menaces.

Protection optimisée des environnements virtuels

McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) offre à vos postes de travail et serveurs virtuels une protection avancée et optimisée contre les logiciels malveillants afin que vous n'ayez plus à choisir entre sécurité et performances. Pour éliminer les goulots d'étranglement et les retards d'analyse, McAfee MOVE AntiVirus transfère les opérations d'analyse, de configuration et de mise à jour des fichiers DAT, normalement exécutées sur les systèmes invités, vers un serveur d'analyse de déchargement. McAfee conçoit et entretient un cache global de fichiers analysés pour garantir qu'une fois un fichier contrôlé et son absence de contamination confirmée, les machines virtuelles qui y accéderont par la suite seront dispensées d'attendre l'exécution d'une analyse. Les ressources de mémoire allouées

à chaque machine virtuelle sont ainsi réduites et peuvent être réaffectées au pool de ressources en vue d'une utilisation plus efficace.

Extension automatique

Grâce à notre solution de sécurité des serveurs et des clouds hybrides, 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. Grâce au provisionnement élastique des ressources dans les clouds privés, McAfee MOVE AntiVirus peut automatiquement ajouter ou supprimer 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.

Gestion unifiée

Le logiciel McAfee ePO offre une gestion unifiée via une seule console pour les serveurs physiques et virtuels, y compris ceux hébergés dans des clouds privés et publics. Bénéficiez d'une sécurité plus robuste et cohérente, et diminuez votre coût total de possession en gérant toute votre infrastructure de terminaux à l'aide d'une console unique. Tous les composants de chaque suite sont étroitement intégrés avec la plate-forme de gestion de la sécurité McAfee ePO. L'objectif est de permettre une évaluation des risques, une administration de la sécurité et une résolution des incidents à la fois centralisées et efficaces.

PRÉSENTATION DE SOLUTION

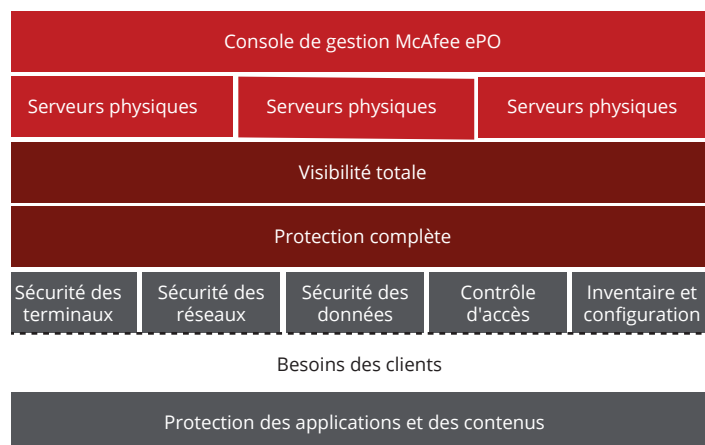


Figure 1. Gestion unifiée des solutions McAfee pour tous les clouds et les serveurs.

Sécurité irréprochable pour les serveurs

Les suites McAfee Server Security constituent la première solution complète pour la sécurité des services stratégiques au sein des environnements hétérogènes modernes, à la fois physiques et virtuels. Ces suites allient plusieurs technologies de sécurité des serveurs pour réduire la charge de traitement. Elles fournissent des jeux complets de contrôles de sécurité pour toutes les charges de travail essentielles, prennent en charge les principaux environnements de virtualisation et centralisent la gestion de la sécurité au sein d'une console d'administration unique. Pour plus d'informations, visitez le site web de McAfee :

<http://www.mcafee.com/fr/products/data-center-security/server-security.aspx>.



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

McAfee et le logo McAfee, ePolicy Orchestrator et McAfee ePO sont des marques commerciales ou des marques commerciales déposées de McAfee, LLC ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs.
Copyright © 2017 McAfee, LLC. 2722_0317
MARS 2017