

# Solutions McAfee pour la **sécurité des serveurs**

**Sécurisez les charges de travail des serveurs avec une incidence minimale sur les performances et toute l'efficacité d'une gestion intégrée.**

Imaginez que vous ayez à choisir entre la sécurisation de tous les serveurs physiques et virtuels de votre centre de données et l'optimisation de leurs performances ? En optant pour la sécurité, vous gardez la disponibilité élevée de vos services informatiques, 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 matériel et en logiciels, sans oublier les félicitations de votre directeur financier. Entre sécurité et performances, la décision est difficile. Et si vous n'aviez plus à faire un choix ?

## À l'intersection de la sécurité et des performances

Avec la virtualisation rapide des centres de données, de nombreux directeurs informatiques ont été confrontés à ce dilemme. Lorsqu'elles ont dû choisir entre la charge de traitement élevée imposée par les contrôles de sécurité des serveurs physiques classiques aux systèmes virtuels et la charge d'administration de plusieurs solutions isolées sans interface de gestion centrale, beaucoup d'entreprises ont tout simplement décidé 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 stratégiques d'une protection intégrée est une invitation au désastre mais force est de constater que la plupart des technologies de sécurité disponibles 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 sécurisation des serveurs doivent désormais répondre aux impératifs suivants :

- Respecter les exigences de sécurité particulières des charges de travail des centres de données, pour tous types de serveurs (bases de données, web, applications, messagerie, collaboration ou stockage). Selon une récente étude du SANS Institute<sup>1</sup>, la sécurisation complète des serveurs nécessite le déploiement de « diverses technologies pour assurer une mise en service sécurisée des serveurs, gérer les vulnérabilités de façon suivie, protéger l'accès aux informations, identifier rapidement les menaces émergentes et améliorer les opérations de sécurité du réseau ».
- Éviter de consommer des ressources de traitement nécessaires aux services métier. Les solutions de sécurité classiques utilisent une part importante des ressources de traitement disponibles, essentiellement en raison de leur dépendance excessive vis-à-vis

## Principaux avantages

### Optimisation de la sécurité avec une incidence minimale sur les performances

Avec McAfee Server Security Suite Essentials et McAfee Server Security Suite Advanced, vous n'avez plus à faire de compromis entre la sécurité des serveurs et leurs performances dans les centres de données virtualisés d'aujourd'hui.

Chaque suite allie diverses technologies, dont les listes noires et la prise en charge de la virtualisation, pour garantir la protection complète des principales charges de travail des serveurs physiques et virtuels avec un temps total de traitement processeur de 5 % ou moins. McAfee Server Security Suite Advanced offre une protection supplémentaire, notamment les listes blanches et le contrôle des modifications.

Toutes les suites prennent en charge la gestion centralisée à l'aide du logiciel McAfee ePO.

Suites disponibles :

- McAfee Server Security Suite Essentials
- McAfee Server Security Suite Advanced
- McAfee Security Suite for VDI
- McAfee Data Center Security Suite for Databases

---

## Présentation de solution

des technologies de listes noires, basées sur les signatures, qui doivent constamment analyser toute l'image système pour détecter les menaces.

- Offrir une prise en charge optimisée des principaux environnements de virtualisation.
- Proposer une gestion de l'ensemble des contrôles de sécurité de l'environnement de serveurs, physiques et virtuels, au sein d'une même console.

### Suites McAfee pour la sécurité des serveurs

Pour satisfaire ces exigences et assurer la sécurité des centres de données virtualisés d'aujourd'hui, McAfee propose plusieurs suites de sécurisation des serveurs conçues tout spécialement pour répondre aux besoins des charges de travail spécifiques sur les serveurs Microsoft Windows et Linux.

Pour garantir une protection optimale des serveurs, McAfee Server Security Suite Advanced associe des technologies de listes blanches (par exemple, le contrôle des applications) aux technologies de listes noires, comme un antivirus et un système de prévention des intrusions basé sur l'hôte. Cette suite de contrôle intégrée protège les systèmes récemment analysés contre les intrusions des logiciels malveillants (*malware*) en limitant l'exécution de code aux applications autorisées. Cela réduit considérablement la fréquence d'analyse des signatures et réduit la charge de traitement au minimum, ce qui représente un avantage de taille pour une entreprise. Cette combinaison unique de listes blanches, de listes noires et de prise en charge de la virtualisation permet d'optimiser considérablement les opérations du centre de données. Elle garantit une protection maximale des serveurs physiques et virtuels avec une incidence minimale sur leurs performances. Tous les composants de chaque suite sont étroitement intégrés avec la plate-forme de gestion McAfee® ePolicy Orchestrator® (McAfee ePO™) afin de permettre une évaluation des risques, une administration de la sécurité et une résolution des incidents à la fois centralisées et efficaces.

McAfee Data Center Security Suite for Databases combine la découverte globale des bases de données, l'évaluation des vulnérabilités et la surveillance non intrusive et en temps réel de l'activité sur l'ensemble des vecteurs de menaces. Elle comprend les composants suivants :

- McAfee Database Activity Monitoring
- McAfee Vulnerability Manager for Databases

McAfee Server Security Suite Essentials propose des fonctionnalités complètes de listes noires, avec une prise en charge optimisée de la virtualisation pour assurer une protection essentielle aux serveurs de tous types. McAfee Server Security Suite Advanced offre en plus des fonctions de listes blanches et de contrôle des modifications.

McAfee Security Suite for VDI assure une sécurité complète pour les déploiements de postes de travail virtuels sans incidence sur les performances ou l'expérience utilisateur. Elle comprend les composants suivants :

- McAfee Application Control for Desktops
- McAfee VirusScan® Enterprise
- McAfee VirusScan Enterprise for Linux
- McAfee MOVE AntiVirus for Virtual Desktops (VDI)
- Logiciel McAfee ePO

D'autres solutions de sécurité sont également disponibles :

- McAfee Security for Microsoft SharePoint
- McAfee Security for Email Servers
- McAfee VirusScan Enterprise for Storage

### Solutions McAfee pour la sécurité des centres de données

	McAfee Server Security Suite Essentials	McAfee Server Security Suite Advanced	McAfee Security Suite for VDI	McAfee Data Center Security Suite for Databases
Logiciel McAfee VirusScan Enterprise	■	■	■	
McAfee VirusScan Enterprise for Linux – Postes de travail			■	
McAfee VirusScan Enterprise for Linux – Serveurs	■	■		
McAfee VirusScan Command Line	■	■		
McAfee Application Control for Servers		■		
McAfee Application Control for Desktops			■	
McAfee MOVE AntiVirus for Virtual Desktops (VDI)			■	
McAfee MOVE AntiVirus for Virtual Servers	■	■		
McAfee MOVE Scheduler	■	■		
McAfee Data Center Connector for VMware vSphere	■	■		
McAfee Data Center Connector for Amazon AWS	■	■		
McAfee Data Center Connector for OpenStack	■	■		
McAfee Data Center Connector for Microsoft Azure	■	■		
McAfee Host Intrusion Prevention	■	■		
McAfee Deep Defender for Servers	■	■		
McAfee Change Control		■		
McAfee Agentless Firewall		■		
Logiciel McAfee ePO	■	■	■	
McAfee File and Removable Media Protection			■	
McAfee Database Activity Monitoring				■
McAfee Vulnerability Manager for Databases				■
Formule de licence	Par instance de système d'exploitation (par machine virtuelle)	Par instance de système d'exploitation (par machine virtuelle)	Par machine virtuelle	Par instance de base de données

### Le portefeuille de technologies de sécurisation des serveurs le plus complet du secteur

Seul McAfee peut offrir un éventail aussi complet de solutions de sécurité des serveurs car il possède tout l'arsenal des technologies nécessaire à la sécurisation des serveurs physiques et virtuels et à la gestion centralisée de solutions de sécurité complexes dans des environnements hétérogènes. Ces suites se fondent sur le riche portefeuille de technologies de sécurisation de McAfee, dont les suivantes :

- **McAfee VirusScan Enterprise** — Allie des technologies de défense antivirus, antispyware, de pare-feu et de prévention des intrusions pour bloquer et supprimer les logiciels malveillants. Il assure également une protection étendue contre les nouveaux risques de sécurité et réduit les coûts qu'implique la réponse aux attaques avec un impact minimal sur les performances système, sans équivalent sur le marché.
- **McAfee VirusScan Enterprise for Linux** — Assure une protection continue irréfutable contre le nombre croissant de virus, de vers et autres types de code malveillant qui ciblent les systèmes Linux. Conçu pour répondre aux besoins actuels des entreprises en évolution rapide, McAfee VirusScan Enterprise for Linux bénéficie d'une évolutivité élevée et d'une fonction de mise à jour automatique, et peut être géré de façon centralisée à partir d'une console unique, la plate-forme McAfee ePO.
- **McAfee Application Control** — Offre un moyen efficace pour bloquer les applications et le code non autorisés sur les serveurs, les postes de travail d'entreprise et les équipements à fonction fixe. Cette solution de gestion centralisée de listes blanches conjugue un modèle d'approbation dynamique et des fonctionnalités de sécurité innovantes qui contrent les menaces persistantes avancées. Et ce, sans nécessiter de mises à jour des signatures ni la gestion de listes qui exigerait de nombreuses heures de travail.
- **McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus** — Optimise la protection antivirus de McAfee pour les serveurs et les postes de travail virtuels sans nuire aux performances ni à la sécurité. Elle vous aide à obtenir les retours sur investissement escomptés et à gérer plus efficacement votre sécurité. La solution protège votre environnement virtuel, notamment vos machines virtuelles dans le cloud.
- **McAfee Data Center Connector** — Garantit une visibilité complète de vos machines virtuelles. La solution permet de détecter non seulement les serveurs physiques, mais aussi les hyperviseurs et les machines virtuelles dans les environnements VMware vSphere, Amazon Web Services, OpenStack et Microsoft Azure. Lorsque vous détectez les nouvelles machines virtuelles mises en service dans votre cloud public, vous pouvez identifier celles qui peuvent être protégées automatiquement à l'aide des stratégies de sécurité appropriées.
- **McAfee Host Intrusion Prevention for Server** — Offre une protection proactive contre les attaques connues et de type « jour zéro ». Il renforce la sécurité et diminue les coûts en réduisant la fréquence et l'urgence de l'application de patchs. McAfee Host Intrusion Prevention s'intègre avec la plate-forme McAfee ePO afin d'offrir des fonctions centralisées de gestion et de génération de rapports. Précises, évolutives et conviviales, celles-ci fonctionnent avec d'autres produits McAfee ou des produits d'autres fournisseurs.
- **McAfee Deep Defender for Servers** — Représente la nouvelle génération de solutions de sécurisation des terminaux assistées par le matériel et fondées sur la technologie McAfee DeepSAFE™. Conçue pour détecter, bloquer et neutraliser les attaques furtives avancées, la solution agit à un niveau plus profond que le système d'exploitation. Fondé sur une approche novatrice de la sécurité, McAfee Deep Defender est le premier produit inspiré de la technologie McAfee DeepSAFE développée en collaboration avec Intel.
- **McAfee Change Control** — Élimine l'application de modifications dans les environnements serveur susceptibles d'entraîner des compromissions de sécurité, des fuites de données ainsi que des pannes et défaillances. McAfee Change Control facilite le respect des obligations réglementaires.

---

## Présentation de solution

- **McAfee Agentless Firewall** — Offre une visibilité sur tous les réseaux virtuels. Il offre la possibilité de contrôler et d'isoler les données et les machines virtuelles grâce à son intégration avec VMware vCNS App Firewall.
- **McAfee File and Removable Media Protection** — Assure la sécurité en chiffrant les données stockées passivement sur des supports internes et amovibles. Il permet aux utilisateurs de chiffrer les clés USB amovibles et de transférer les informations en toute sécurité.
- **McAfee Database Activity Monitoring** — Détecte automatiquement les bases de données sur votre réseau, les protège au moyen d'un ensemble de mécanismes de défense préconfigurés et vous aide à développer une stratégie de sécurité personnalisée pour votre environnement. Il protège, à un coût abordable, vos données contre toutes les menaces en assurant le suivi des activités localement, sur chaque serveur de base de données, et en signalant ou en bloquant tout comportement malveillant en temps réel, même lorsque le serveur tourne dans un environnement cloud ou virtualisé.
- **McAfee Vulnerability Manager for Databases** — Offre un aperçu précis, instantané et complet des vulnérabilités de tous les actifs de votre réseau. Il vous permet de garder une longueur d'avance sur les menaces en constante évolution et de déterminer les mesures à appliquer en priorité grâce à une vue unique et corrélée des vulnérabilités détectées.
- **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. 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 afin de permettre une évaluation des risques, une administration de la sécurité et une résolution des incidents à la fois centralisées et efficaces.

### Le succès de la sécurisation des serveurs

Les suites McAfee pour la sécurité des serveurs offrent la première solution complète du secteur pour la sécurisation des services stratégiques au sein des environnements physiques et virtuels d'aujourd'hui. Ces suites allient plusieurs technologies de sécurisation des serveurs pour réduire la charge de traitement. Elles fournissent des jeux complets de contrôles de sécurité pour toutes les charges de traitement essentielles, prennent en charge les principaux environnements de virtualisation et centralisent la gestion de la sécurité via une console d'administration unique. Pour plus d'informations, visitez le site web de McAfee :

[www.mcafee.com/fr/products/data-center-security/index.aspx](http://www.mcafee.com/fr/products/data-center-security/index.aspx).

---

1. [www.sans.org/reading\\_room/analysts\\_program](http://www.sans.org/reading_room/analysts_program)