# McAfee Host Intrusion Prevention for Server

## Protection avancée des serveurs et des applications contre les vulnérabilités

Les serveurs d'entreprise hébergent les informations stratégiques de celle-ci et sont essentiels à son bon fonctionnement. L'un des principaux défis auxquels sont confrontés les services informatiques est la protection de ces serveurs et des applications qu'ils hébergent contre les attaques connues et inconnues qui menacent de perturber les activités de l'entreprise.

### Principaux avantages

**Protection renforcée**

- Mise en œuvre des mesures de prévention des intrusions et de protection contre les menaces de type « jour zéro » les plus étendues à tous les niveaux : réseau, applications et exécution

**Réduction des coûts**

- Réduction du temps et des coûts grâce à une console puissante unifiée pour le déploiement, la gestion, la génération de rapports et l'audit des événements, des stratégies et des agents
- Application de patchs aux terminaux moins fréquente et plus rationnelle, plutôt que dans l'urgence

**Mise en conformité simplifiée**

- Gestion de la conformité à l'aide de vues exploitables faciles à comprendre, ainsi que de fonctionnalités de workflow, de surveillance des événements et de génération de rapports pour des enquêtes et des analyses post-mortem précises et rapides

### McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Server offre une protection spécialisée aux serveurs web et de base de données permettant de préserver la disponibilité des systèmes et la continuité des activités de l'entreprise. Équipée du seul pare-feu dynamique du marché, cette solution assure en outre une protection contre les menaces avancées et le trafic malveillant, et associe un système de prévention des intrusions (IPS) basé sur les signatures et les comportements. McAfee Host Intrusion Prevention for Server diminue l'urgence et la fréquence d'application des patchs, assure la continuité des activités de l'entreprise, préserve la productivité du personnel, protège la confidentialité des données et simplifie la conformité réglementaire.

**Protection des serveurs et des applications contre les attaques et prévention des fuites de données**

Parce qu'ils hébergent d'importants volumes de données et sont essentiels aux activités quotidiennes des entreprises, les serveurs sont devenus une cible privilégiée des cyberattaques. McAfee Host Intrusion Prevention for Server sécurise les serveurs stratégiques afin de préserver la disponibilité des systèmes et la productivité.

- Protection des serveurs web :
  - Filtrez les requêtes HTTP pour prévenir les attaques de type traversée de répertoires, par caractères Unicode et par déni de service.
  - Utilisez des stratégies et des règles de protection prédéfinies pour prévenir les attaques et les fuites de données.
- Protection des serveurs de base de données :
  - Examinez les requêtes de base de données pour prévenir des attaques telles que l'injection SQL.
  - Utilisez des stratégies et des règles de protection prédéfinies pour garantir un comportement normal et prévenir l'altération des données.

**Protection contre les menaces avancées grâce à un pare-feu système dynamique**

Contrairement aux pare-feux système traditionnels qui reposent sur des règles spécifiques, McAfee Host Intrusion Prevention for Server intègre les services de réputation des

intel Security

## Configuration système requise

**Configuration matérielle minimale**

- Intel ou AMD x86 et x64
- Espace disque disponible (client) : 15 Mo, mais 100 Mo pendant l'installation
- Mémoire : 256 Mo de RAM
- Environnement réseau : Réseaux Microsoft ou Novell NetWare (les réseaux NetWare nécessitent TCP/IP)
- Carte réseau : carte réseau 10 Mbit/s ou supérieure

**Systèmes d'exploitation pris en charge**

- Microsoft Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (toutes éditions, 32 et 64 bits)
- Microsoft Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (toutes éditions, 32 et 64 bits)
- SPARC Solaris 9 sun4u (32 et 64 bits)
- SPARC Solaris 10 sun4u, sun4v (32 et 64 bits)
- Red Hat Linux Enterprise 4, 32 bits
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, 64 bits
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, 32 bits
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5, 64 bits
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10, 32 bits
  - 2.6.16.21-0.8-bigsmp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp

connexions réseau de McAfee Global Threat Intelligence (McAfee GTI) pour protéger les serveurs contre les menaces avancées que sont les réseaux de robots, les attaques par déni de service distribué et le trafic malveillant, avant qu'une attaque survienne. Face à la multiplication des menaces avancées, McAfee GTI constitue la protection la plus sophistiquée qui soit.

**Appliquez des patchs au système d'exploitation et aux applications moins souvent, avec moins d'urgence et selon votre propre calendrier**

Un pourcentage important d'exploits est distribué dans les trois jours suivant la divulgation de vulnérabilités. Or, il faut parfois 30 jours à bon nombre d'entreprises pour tester et déployer des patchs sur l'ensemble des terminaux.

McAfee Host Intrusion Prevention for Server comble cette brèche de sécurité tout en simplifiant le processus d'application des patchs et en le rendant plus efficace.

- McAfee Host Intrusion Prevention for Server vous protège contre les vulnérabilités Microsoft et Adobe. La protection contre les vulnérabilités met automatiquement à jour les signatures pour préserver les terminaux des attaques résultant de l'exploitation de vulnérabilités.
- Les mises à jour de signatures peuvent être téléchargées automatiquement et régulièrement pour garantir une protection totale.

**Protection des serveurs au démarrage**

Les serveurs sont particulièrement vulnérables au moment du démarrage, car les stratégies de sécurité ne sont pas encore actives. Ce court laps de temps suffit aux cybercriminels pour lancer une attaque réseau et désactiver les services de sécurité. McAfee Host Intrusion Prevention for Server bloque ce type d'attaque au démarrage grâce à un pare-feu et à un système de prévention des intrusions (IPS) dédiés.

- La protection par pare-feu au démarrage autorise uniquement le trafic en sortie jusqu'à la mise en œuvre complète de la stratégie de pare-feu.
- Le système de prévention des intrusions au démarrage empêche la désactivation de nos services de sécurité jusqu'à la mise en œuvre complète de la stratégie IPS.

**Gestion simplifiée et rationalisée**

La création et la gestion de plusieurs stratégies de pare-feu et IPS sont nécessaires dans le cas de grandes entreprises, mais ces tâches fastidieuses exigent généralement de nombreuses heures de travail. Les catalogues IPS et de stratégies de McAfee Host Intrusion Prevention for Server simplifient ce processus, en vous permettant de créer et de gérer plusieurs stratégies de pare-feu et IPS, que vous pourrez ensuite appliquer à votre convenance.

Optimisez et simplifiez davantage encore la gestion grâce à McAfee® ePolicy Orchestrator® (McAfee ePO™), notre console centralisée unique qui vous permet de superviser et d'administrer l'ensemble de vos dispositifs de protection. En vous permettant de gagner du temps et de l'argent, l'intégration complète avec McAfee ePO est la garantie d'une efficacité opérationnelle optimale.

Pour plus d'informations, contactez un représentant commercial ou visitez notre site à l'adresse : **www.mcafee.com/fr**.

**Systèmes d'exploitation pris en charge** (suite)

- SUSE Linux Enterprise 10, 64 bits
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11, 32 bits
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11, 64 bits
  - 2.6.27.19-5-default

**Serveurs web pris en charge**

- Microsoft Windows
  - IIS 6.0 et 7.0
- SPARC Solaris
  - Apache 1.3.6 et serveurs web ultérieurs
  - Apache 2.0.42 et serveurs web ultérieurs
  - Apache 2.2.3 et serveurs web ultérieurs
  - Sun Java Web Server 6.1
  - Sun Java Web Server 7.0
- Linux (RHEL et SUSE)
  - Apache 1.3.6 et serveurs web ultérieurs
  - Apache 2.0.42 et serveurs web ultérieurs
  - Apache 2.2.3 et serveurs web ultérieurs

**Serveurs de base de données pris en charge**

- Microsoft SQL Server 2005 et 2008

## Compatibilité avec les principales plates-formes de virtualisation

La virtualisation étant désormais largement adoptée par les services informatiques, la compatibilité des produits avec les principales plates-formes de virtualisation constitue un aspect essentiel. McAfee Host Intrusion Prevention for Server 8.0 est compatible avec les trois principales plates-formes de virtualisation, à savoir VMware, Citrix et Microsoft Hyper-V. Le tableau ci-après répertorie les produits pris en charge par chacune de ces trois plates-formes.

| VMware | Citrix | Microsoft |
|---|---|---|
| VMware ESX 3.5 et 4.0 | Citrix XenServer 5.0 et 5.5 | Microsoft Hyper-V Server 2008 et 2008 R2 |
| VMware vSphere 4.0 | Citrix XenDesktop 3.0 et 4.0 | Microsoft VDI |
| VMware View 3.1 et 4.0 | Citrix XenApp 5.0 et 6.0 | Microsoft App-V 4.5 et 4.6 |
| VMware ThinApp 4.0 et 4.5 | | XP Mode sur Windows 7 |
| VMware ACE 2.5 et 2.6 | | |
| VMware Workstation 6.5 et 7.0 | | |
| VMware Player 2.5 et 3.0 | | |

**McAfee. Part of Intel Security.**
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com


17802ds_hips-server_1110B