

Suite McAfee Endpoint Protection – Advanced

Protection contre les attaques de type « jour zéro » et conformité réglementaire simplifiée

La conjonction d'une main-d'œuvre de plus en plus mobile et d'un durcissement des réglementations peut transformer la sécurité en un réel cauchemar. Assurez votre tranquillité d'esprit en adoptant la suite McAfee® Endpoint Protection – Advanced. Grâce à ses mécanismes de sécurité proactifs intégrés qui arrêtent net les logiciels malveillants sophistiqués et les menaces de type « jour zéro », cette suite protège les postes clients lorsqu'ils quittent votre réseau et prémunissent ce dernier contre les risques auxquels ils peuvent l'exposer lorsqu'ils s'y reconnectent. Sa technologie de prévention des intrusions intégrée protège les postes clients Windows, y compris ceux qui ne quittent pas le bureau, contre les menaces persistantes évoluées. Une gestion centralisée basée sur les stratégies, le contrôle de l'accès et l'audit permettent de sécuriser l'ensemble des postes clients et de garantir leur conformité.

Points essentiels

- Protection des postes clients contre les menaces visant les systèmes, les données, la messagerie électronique et l'environnement web, ainsi que les risques de non-conformité
- Solution intégrée de protection des données et des postes clients proposée par un fournisseur unique, qui garantit une sécurité plus efficace à moindre coût
- Protection renforcée instantanée, basée sur un agent unique pour plus de simplicité et d'efficacité

Fin 2008, pour la première fois, il s'est vendu plus d'ordinateurs portables que d'ordinateurs de bureau fixes et de type tour. L'informatique est entrée dans l'ère du « portable ».

— IDC : *Notebooks Finally Outsell Desktops in U.S.* (Aux Etats-Unis, les ordinateurs portables finissent par dépasser les ordinateurs de bureau en termes de ventes) ; <http://www.pcmag.com/article2/0,2817,2333549,00.asp>



Meilleure solution antimalware et meilleure solution de sécurité pour entreprises

Seuls des mécanismes de protection par analyse comportementale et au niveau des systèmes peuvent prémunir les postes clients contre les logiciels malveillants (*malwares*) les plus insidieux, conçus pour échapper à la détection par signatures et frapper avant la distribution de patches. Même si tous les postes clients sont aujourd'hui menacés en raison des technologies sophistiquées élaborées par les criminels, nul doute que les ordinateurs portables sont en première ligne. Ces systèmes nomades sont en effet emportés d'hôtels en cafés ainsi qu'au domicile de l'utilisateur, alors qu'ils peuvent être dépourvus des niveaux de protection traditionnels qu'offrent les passerelles web et de messagerie, les pare-feux réseau ou encore les systèmes de prévention des intrusions réseau. Et une fois connectés à un réseau Wi-Fi, ils sont sujets à l'écoute clandestine qui permet à quiconque de mettre la main sur des informations importantes.

Il suffit que vous vous absentiez du bureau pour que votre ordinateur manque l'application de patches et d'autres mises à jour, devenant ainsi une cible toute désignée pour les menaces de type « jour zéro ». Or, ces patches et mises à jour sont de plus en plus indispensables à la conformité réglementaire. Non seulement les réglementations sectorielles deviennent toujours plus strictes, mais il se peut que vos contrôles de gouvernance exigent la mise en place de politiques en matière de distribution des données sensibles et d'utilisation responsable d'Internet, tant sur site qu'en déplacement. Avec la suite McAfee Endpoint Protection – Advanced, c'est vous qui êtes aux commandes, grâce à ses mécanismes de protection étendus, à ses contrôles de conformité et à sa gestion unifiée. Que vous souhaitiez tenir à distance les virus, les pirates, les spammeurs et les voleurs de données, ou encore éviter les audits, cette solution transparente combine, à la perfection, richesse fonctionnelle et économies de coûts.

Protection en temps réel permanente contre les logiciels malveillants

Avec la croissance sans précédent des menaces évoluées persistantes, les entreprises ne peuvent plus compter sur des solutions qui utilisent uniquement l'analyse des signatures pour protéger les postes clients. Il s'écoule toujours de 24 à 72 heures entre l'identification d'une menace et le moment où sa signature est appliquée sur les postes clients. Dans l'intervalle, vos données et vos systèmes sont vulnérables. Le service intégré de réputation des fichiers de McAfee Global Threat Intelligence comble ce délai en offrant une protection en temps réel et permanente basée sur les informations recueillies par McAfee Labs™.

Protection avancée contre le spam et les virus propagés par e-mail

Notre solution analyse le trafic de messagerie à l'entrée et en sortie pour y détecter la présence éventuelle de spam, de contenu indésirable ou de virus. Les e-mails suspects peuvent être mis en quarantaine afin d'empêcher les menaces qu'ils véhiculent d'affecter le réseau et les utilisateurs. De plus, la protection antivirus du serveur de messagerie intercepte les logiciels malveillants (*malwares*) avant qu'ils n'atteignent les boîtes aux lettres des utilisateurs.

Un rempart contre les menaces de type « jour zéro » et les vulnérabilités

L'application de patches dans l'urgence appartient désormais au passé. Le système de prévention des intrusions sur l'hôte surveille sans relâche les postes clients à la recherche de logiciels malveillants et empêche le code nuisible de pirater les applications. De plus, il fournit automatiquement des signatures mises à jour qui protègent les postes de travail et les ordinateurs portables contre les attaques. Vous avez par ailleurs le temps d'implémenter et de tester les patches selon le calendrier établi. Ajoutons à cela notre technologie de protection par analyse comportementale brevetée, qui bloque les attaques par Buffer Overflow, et vous obtenez la solution d'immunisation contre les vulnérabilités la plus performante du marché.

McAfee, « la référence du secteur »

- Classé parmi les leaders du Magic Quadrant de Gartner dans les catégories sécurisation des postes clients et protection des données mobiles pendant quatre années consécutives
- Premier produit capable de gérer un large éventail de produits de sécurisation (postes clients, réseau, données, environnement web et messagerie électronique), le tout à partir d'une seule et même console
- Premier produit de gestion de la sécurité des postes clients doté d'un agent unique et d'une console unique
- Première plate-forme de gestion unifiée pour la sécurisation des postes clients et la gestion de la conformité
- Premier produit à gérer des produits de sécurité de McAfee et d'éditeurs tiers
- Premier produit combinant l'audit et la mise en œuvre des stratégies en un seul moteur
- Premier fournisseur à allier la sécurisation des postes clients et la protection des données au sein d'une suite véritablement intégrée

Plates-formes d'exploitation prises en charge

Postes de travail (remarque : la prise en charge de la version 64 bits est disponible pour certaines technologies)

- Windows 7 ou Embedded
- Windows Vista
- Windows XP Edition familiale, Professionnel, Embedded (WEPOS), Tablet PC
- Windows 2000 Professionnel avec Service Pack 2 ou version ultérieure

Serveurs (remarque : la prise en charge de la version 64 bits est disponible pour certaines technologies)

- Windows Server 2008 : versions standard, avec technologie Hyper-V, Server Core, Datacenter, Storage Server, Cluster Server et Small Business Server
- Windows Server 2003 : versions standard, Storage Server, Cluster Server, Datacenter et Small Business Server
- Windows Server 2000 : versions standard, Advanced Server et Small Business Server

Configuration requise pour le serveur de messagerie

- Microsoft Exchange 2003 avec Service Pack 1, 2007 (64 bits), 2010 (7.0.2)
- Microsoft Small Business Server 2000, Microsoft Exchange Server 2003 ou version ultérieure
- Lotus Domino 6.0.3 à 6.0.5, 7.0, 8.0 (32 bits), 8.5 (32 bits)



McAfee S.A.S.
 Tour Franklin, La Défense 8
 92042 Paris La Défense Cedex
 France
 +33 1 47 62 56 00 (standard)
 www.mcafee.com/fr

Pare-feu dynamique pour postes clients

Vous pouvez contrôler les applications pouvant accéder au réseau afin de bloquer les attaques propagées via ce dernier et de réduire les périodes d'indisponibilité. Vous pouvez déployer et gérer des stratégies de pare-feu selon l'emplacement afin d'offrir une protection absolue et une conformité totale aux dispositions réglementaires.

Contrôle souple de l'accès au réseau

Lorsque les utilisateurs nomades se reconnectent au réseau de l'entreprise, vous êtes assuré qu'ils ne ramènent aucun « passager clandestin ». La fonction de contrôle d'accès au réseau limite l'accès au réseau d'entreprise aux seuls systèmes conformes que vous avez autorisés. Quelle que soit la manière dont les postes clients se connectent au réseau, cette fonction identifie et évalue leur état de conformité, met en œuvre les stratégies d'accès au réseau appropriées et applique automatiquement les actions correctives nécessaires.

Solution efficace de conformité et d'audit des stratégies

La fonction d'audit des stratégies basée sur l'agent analyse vos postes clients et atteste que toutes les stratégies sont à jour. Les entreprises peuvent mesurer leur conformité aux cadres de meilleures pratiques (ISO 27001 et COBIT) ainsi qu'aux principales réglementations sectorielles.

Contrôle total des périphériques

Empêchez les données critiques de quitter votre entreprise via des clés USB, des iPod, des périphériques Bluetooth, ainsi que des CD et DVD enregistrables. Nous vous offrons les outils nécessaires pour surveiller et contrôler les transferts de données depuis l'ensemble des postes de travail et ordinateurs portables. Et ce, quelle que soit la destination des données confidentielles, où que l'utilisateur se trouve et qu'il soit connecté ou non au réseau de l'entreprise.

Sécurisation proactive de l'environnement web

Assurez votre conformité et limitez le risque posé par la navigation web grâce à des avertissements signalant aux utilisateurs la présence de sites web malveillants avant qu'ils n'y accèdent. Le filtrage web au niveau de l'hôte vous permet d'autoriser et de bloquer l'accès aux sites web, de protéger les utilisateurs et de garantir la conformité aux stratégies lorsqu'ils naviguent sur Internet et d'où qu'ils se connectent.

Réduction des coûts opérationnels grâce à une gestion centralisée

Afin d'améliorer l'efficacité et de vous offrir une visibilité complète sur votre état de protection et de conformité, McAfee ePolicy Orchestrator® (ePO™) fournit une plate-forme centrale unique qui gère la sécurité, met en œuvre les stratégies de protection et diminue le coût des opérations de sécurité. Accessible en permanence via une interface web conviviale, ePO offre une sécurité intelligente afin d'accélérer et d'optimiser la prise de décisions tout en garantissant un contrôle accru.

Il est possible de mettre en corrélation les événements et les informations sur les attaques et les menaces communiqués par les solutions de sécurisation du réseau, des postes clients et des données d'une part, et résultant des audits de conformité d'autre part, afin d'améliorer la pertinence et l'efficacité des opérations de sécurité et des rapports de conformité. Aucun autre fournisseur ne peut prétendre offrir une plate-forme de gestion intégrée qui couvre l'ensemble de ces domaines de sécurité. McAfee ePolicy Orchestrator simplifie véritablement la gestion de la sécurité.

En savoir plus

Pour plus d'informations, consultez le site www.mcafee.com/endpoint ou appelez le +33 1 47 62 56 00 (standard) – numéro accessible aux heures de bureau.

Caractéristiques	Avantage pratique
Gestion intégrée unifiée	Visibilité instantanée sur l'état de protection de l'entreprise et les événements, ainsi qu'accès direct à l'interface de gestion grâce à McAfee ePolicy Orchestrator (ePO), afin de vous garantir un contrôle unifié sur tous les outils de conformité et de sécurité
Contrôle des périphériques	Surveillance et limitation de l'accès aux données copiées sur les supports et périphériques de stockage amovibles afin de les empêcher de quitter la société
Prévention des intrusions sur l'hôte et pare-feu pour postes de travail	Protection de type « jour zéro » contre les nouvelles vulnérabilités, qui diminue l'urgence de l'application de patches aux systèmes existants, et contrôle des applications de poste de travail autorisées à accéder au réseau afin de mettre un terme aux attaques propagées via le réseau et de réduire les périodes d'indisponibilité consécutives
Protection antimalware	Blocage des virus, des chevaux de Troie, des vers, des logiciels publicitaires (adwares), des logiciels espions (spywares) et autres programmes potentiellement indésirables qui volent des données confidentielles et nuisent à la productivité des utilisateurs finaux
Protection antisпам	Élimination du spam qui mène des utilisateurs trop confiants à des sites conçus pour distribuer des logiciels malveillants et extorquer des données personnelles et financières
Recherche et navigation en toute sécurité	Garantie de conformité et limitation du risque posé par la navigation web grâce à la génération d'alertes qui signalent aux utilisateurs la présence de sites web malveillants et à une fonctionnalité permettant aux administrateurs de bloquer ou d'autoriser l'accès aux sites web
Filtrage de contenu web sur l'hôte	Contrôle des utilisateurs lorsqu'ils naviguent sur Internet à partir du réseau d'entreprise ou d'ailleurs grâce au filtrage de contenu et à la mise en œuvre de stratégies d'accès aux sites web basées sur les utilisateurs et les groupes
Sécurisation du serveur de messagerie	Protection du serveur de messagerie et interception des logiciels malveillants avant qu'ils n'atteignent les boîtes aux lettres des utilisateurs
Contrôle d'accès au réseau	Limitation des infections par logiciels malveillants en empêchant les systèmes non conformes d'accéder au réseau
Audit des stratégies	Génération de rapports de conformité étroitement intégrés pour diverses normes et réglementations telles que PCI, HIPAA et bien d'autres

McAfee, le logo McAfee, McAfee ePolicy Orchestrator, McAfee ePO, McAfee Global Threat Intelligence et McAfee Labs sont des marques commerciales déposées ou des marques commerciales de McAfee, Inc. et/ou de ses sociétés affiliées aux États-Unis et/ou dans d'autres pays. Les autres noms et marques peuvent être la propriété d'autres sociétés. Les plans, les spécifications et les descriptions des produits mentionnés dans le présent document sont donnés à titre indicatif uniquement. Ils peuvent être modifiés sans préavis et sont fournis sans aucune garantie, implicite ou explicite. Copyright © 2010 McAfee, Inc. 14100ds_epa_0910_fnl_ASD