

Suite McAfee Endpoint Protection

Protection en temps réel des ordinateurs Windows contre les logiciels malveillants et les périphériques non autorisés

Les postes de travail traditionnels et les systèmes fixes de votre réseau local sont probablement protégés par des mécanismes de sécurité au niveau du réseau ou de la passerelle. Pourtant, il leur manque encore un niveau de sécurité essentiel pour bloquer les logiciels malveillants sophistiqués, empêcher les fuites de données, contrôler les risques de conformité que représentent les supports amovibles et assurer un accès sécurisé aux applications web et de messagerie critiques. La suite McAfee® Endpoint Protection intègre ces fonctions de base dans un environnement unique facile à gérer, parfaitement adapté à la protection des postes de travail traditionnels et autres systèmes peu exposés aux menaces Internet.

Points essentiels

- Protection essentielle qui consolide la sécurité des données et des postes clients
- Déploiement et gestion de la sécurité plus simples et plus rapides
- Solution tout en un offrant les fonctions de protection adaptées aux postes de travail traditionnels et aux systèmes fixes



Meilleure solution antimalware et meilleure solution de sécurité pour entreprises

Quel est le point commun entre un centre d'appels, un bureau de conception technique et un cabinet médical ? Toutes les personnes qui y travaillent utilisent des ordinateurs de type tour et des postes de travail traditionnels qui ne quittent jamais le bureau. De par leur nature sédentaire, ces systèmes ne se connectent pas à des points d'accès sans fil, ils n'accompagnent pas vos enfants lors de leurs pérégrinations nocturnes sur Internet et ne sont pas oubliés dans le hall d'un aéroport. Aussi, le risque est-il faible qu'ils soient piratés, qu'ils téléchargent des applications malveillantes ou que les données sensibles qu'ils hébergent soient volées.

Cependant, en raison de l'utilisation massive de la messagerie électronique et des applications web sur le lieu de travail, même ces systèmes fixes ont besoin d'une protection sophistiquée et en temps réel contre les logiciels malveillants (*malwares*) ciblés véhiculés par ces outils. Votre serveur de messagerie doit lui aussi être doté d'une protection antimalware, de même que chacun des postes clients.

Pour corser le tout, les ordinateurs dernier cri sont, pour la plupart, équipés de plusieurs ports USB et lecteurs DVD. Dans le cas des centres d'appels, bureaux de conception technique et cabinets médicaux, un travailleur mécontent peut utiliser ces équipements pour rapporter chez lui des bases de données clients, des conceptions techniques et d'autres éléments de propriété intellectuelle ou encore des dossiers médicaux et des données financières. Le contrôle des périphériques peut toutefois vous aider à limiter l'utilisation de supports amovibles et de dispositifs de stockage portables afin d'éviter toute fuite de données.

La suite McAfee Endpoint Protection intègre, de manière transparente, des technologies de sécurité éprouvées pour vous aider à gérer tous ces risques. Et en plus d'offrir les avantages d'une solution unique, elle améliore l'efficacité opérationnelle et vous permet de réaliser des économies substantielles.

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 en danger.

Le service 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 sur les menaces multivectorielles recueillies par McAfee Labs™. Il met en quarantaine ou bloque les virus, les chevaux de Troie, les vers, les logiciels publicitaires (*adwares*), les logiciels espions (*spywares*) et autres programmes potentiellement indésirables qui volent des données confidentielles et nuisent à la productivité des utilisateurs finaux.

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 avant qu'ils n'atteignent les boîtes aux lettres des utilisateurs.

Contrôle total des périphériques

Empêchez les données critiques de quitter votre société via des périphériques amovibles, tels que des lecteurs USB, des iPod, des périphériques Bluetooth ou encore des CD et DVD enregistrables. Vous disposez des outils nécessaires pour surveiller et contrôler les transferts de données depuis l'ensemble des postes de travail, même si un périphérique est déconnecté physiquement du réseau de l'entreprise.

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 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 Windows 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)

Pare-feu dynamique pour postes clients

Contrôlez les applications autorisées à accéder au réseau afin de bloquer les attaques se propageant 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.

Sécurisation proactive de l'environnement web

Internet dissimule de nombreuses menaces silencieuses et invisibles aux internautes. 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. Vous pouvez également autoriser ou bloquer l'accès à des sites web en fonction des utilisateurs et des groupes, en contrôlant l'accès à des sites sensibles ou inadaptés (sites de jeux ou pour adultes, par exemple).

Réduction des coûts opérationnels grâce à une gestion centralisée

Toutes les fonctionnalités de la suite McAfee Endpoint Protection sont administrées par McAfee ePolicy Orchestrator® (ePO™), une plate-forme centralisée qui gère la sécurité, met en œuvre la 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.

McAfee ePO peut réduire de plus de 60 % les coûts associés à la gestion de la conformité et de la sécurité informatique (source : étude de MSI International portant sur 488 grandes et moyennes entreprises).

Cette conception ouverte de l'infrastructure de gestion repose sur une console et un agent uniques. En comparaison des solutions individuelles des générations précédentes, notre approche optimisée simplifie considérablement l'installation et la maintenance des systèmes de protection, de même que celles de leurs règles et stratégies. C'en est fini des nombreux agents qui dégradent les performances système et les consoles multiples à l'origine de décisions disparates et inefficaces. Lorsque les stratégies doivent être revues, les mises à jour sont rapides, précises et systématiques.

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.

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
Pare-feu pour postes de travail	Blocage des attaques réseau et autorisation du trafic réseau légitime uniquement
Protection antimalware	Blocage des virus, des chevaux de Troie, des vers, des logiciels publicitaires, des logiciels espions 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
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
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

