

McAfee VirusScan Mobile Enterprise

Extension de la sécurité éprouvée des postes clients aux périphériques mobiles

Principaux avantages

Protection des équipements mobiles de l'entreprise contre les logiciels malveillants à tous les points d'entrée

- Analyse et nettoyage du code malveillant des e-mails entrants et sortants, des messages texte, des pièces jointes et des fichiers
- Prise en charge des principaux modes de connexion : réseaux de données des opérateurs de téléphonie mobile, Bluetooth, Wi-Fi et infrarouge

Sérénité garantie par des mises à jour de sécurité automatiques

- Envoi de mises à jour des signatures des équipements mobiles par liaison radio
- Mise à jour des stratégies et des logiciels des systèmes à l'aide d'un nœud managé via une méthode ActiveSync pratique, de même que des stratégies via une connexion Wi-Fi

Diminution de la charge d'administration informatique et gestion simplifiée

- Gestion de la sécurité des équipements mobiles à l'aide de McAfee ePO pour améliorer l'efficacité et réduire les coûts
- Automatisation des mises à jour des signatures, des logiciels système et des stratégies à partir d'une console de gestion centralisée

Le défi

Les entreprises du monde entier considèrent aujourd'hui les périphériques mobiles intelligents comme des outils essentiels à la productivité de leurs effectifs. L'accès en tout lieu et à toute heure aux informations de la société favorise la réactivité des employés et permet de communiquer 24 heures sur 24. Les périphériques mobiles intelligents seront bientôt aussi répandus que les ordinateurs portables. Plus de 100 millions de smartphones ont été vendus en 2007 et, d'après les prévisions, ce chiffre devrait frôler les 400 millions d'ici 2012¹. Malheureusement, cette croissance rapide associée à la disponibilité généralisée des kits d'outils de développement incite les cybercriminels à s'intéresser de près à ces appareils. Les informations d'entreprise contenues dans les e-mails, les téléchargements et les données de contact des clients stockés sur les smartphones sont susceptibles d'être compromises et de tomber entre de mauvaises mains. Par conséquent, la sécurisation des périphériques mobiles intelligents est devenue aussi essentielle que la protection des ordinateurs portables et des postes de travail.

McAfee VirusScan Mobile Enterprise

Protégez tous les périphériques mobiles intelligents qui exécutent le système d'exploitation Microsoft Windows Mobile avec McAfee® VirusScan® Mobile Enterprise (VSME). Cette solution antimalware gérée de façon centralisée analyse et élimine les virus, les vers, les numéroteurs (*dialers*), les chevaux de Troie, le code malveillant et les programmes malveillants qui vident votre batterie. Les périphériques mobiles sont protégés au niveau de la plupart des points d'exposition potentielle, notamment les e-mails entrants et sortants,

les messages texte, les pièces jointes, les fichiers et les téléchargements Internet, sur une multitude de modes de connexion (Bluetooth, Wi-Fi et infrarouge, notamment). McAfee VirusScan Mobile Enterprise prend en charge les mises à jour de signatures planifiées par liaison radio et assure ainsi une protection instantanée contre les menaces émergentes. Gérez la sécurité de votre environnement mobile à l'aide de McAfee ePolicy Orchestrator® (ePO™) pour réduire sensiblement la charge d'administration informatique et améliorer l'efficacité de vos opérations.

Gestion simplifiée au niveau de l'entreprise

McAfee VirusScan Mobile Enterprise est géré par McAfee ePO, la console de gestion de la sécurité primée qui assure à l'entreprise une défense coordonnée et proactive contre les menaces et les attaques malveillantes. Véritable tour de contrôle des solutions de gestion des risques de sécurité (SRM) de McAfee, ePO permet aux administrateurs de minimiser les risques liés aux systèmes non fiables et non conformes, de maintenir leur protection à jour, de configurer et de mettre en œuvre des stratégies de sécurité et de surveiller l'état de sécurisation de l'entreprise en continu, 24 heures sur 24 et 7 jours sur 7 — le tout à partir d'une console web centrale unique. Déployez ePO et gérez toutes vos nouvelles solutions de sécurité ou dopez les investissements consacrés à la gestion de la sécurité de l'entreprise en ajoutant McAfee VirusScan Mobile Enterprise à l'infrastructure ePO existante. McAfee ePO facilite le déploiement, la configuration et la gestion de McAfee VirusScan Mobile Enterprise. De ce fait, elle est la solution idéale pour gérer tous vos périphériques mobiles Windows d'entreprise ainsi que les postes clients.

¹ Rapport IDC n° 211431, *WW Converged Mobile Device 2008-2012 Forecast and Analysis: A Category Comes of Age* (Analyse et prévisions relatives aux équipements mobiles convergents pour 2008-2012 : la maturité des équipements mobiles), mars 2008.

Spécifications

Poste managé

- McAfee Agent version 3.5.5 patch 1 (ou ultérieur)
- Microsoft ActiveSync version 4.1 (ou ultérieure) pour les systèmes Windows XP
- Microsoft Windows Mobile Device Center (WMDC) version 6.1 (ou ultérieure) pour les systèmes Windows Vista

McAfee VirusScan Mobile Enterprise

- Appareils Microsoft Windows Mobile 5.0 pour Smartphone et pour Pocket PC
- Appareils Microsoft Windows Mobile 6.0 Professionnel et Standard
- Au moins 4 Mo d'espace de stockage disponible pour l'installation de McAfee VirusScan Mobile Enterprise

McAfee ePolicy Orchestrator 4.0

- Configuration standard requise pour le serveur telle qu'établie pour McAfee ePO 4.0

Fonctionnalités et avantages

Protection des actifs de l'entreprise et respect des exigences de conformité

- Protection des informations confidentielles contre les vols de données potentiels
- Respect de la législation et des réglementations sectorielles imposant aux entreprises de protéger leurs données sensibles

Maintien d'une productivité élevée des employés

Les virus et d'autres menaces peuvent compromettre la disponibilité des périphériques mobiles et perturber les communications de votre entreprise. Il est donc primordial de sécuriser les smartphones de l'entreprise afin de préserver la productivité du personnel et d'assurer la continuité de vos activités.

Mise à jour automatique afin de garantir la protection des utilisateurs contre les menaces actuelles et émergentes

- Les signatures sont mises à jour par liaison radio grâce à une connexion sans fil au serveur de mises à jour lorsque les périphériques sont connectés au réseau ou au serveur public McAfee lorsqu'ils sont déconnectés du réseau.
- Les stratégies et les logiciels du système sont mis à jour avec un nœud managé (poste de travail ou ordinateur portable, par exemple) via Microsoft ActiveSync. En outre, il est possible de mettre à jour les stratégies via une connexion LAN sans fil à ePO, si elle est disponible.

Protection contre la corruption et les infections grâce à des analyses des messages et des fichiers à la demande ou déclenchées par des événements

- Analyse planifiée de tous les types de fichiers (images, photos, vidéos, etc.) et des messages (messages texte, e-mails et pièces jointes)
- Analyse des fichiers en temps réel lors de leur ajout ou de leur modification et des messages à l'envoi ou à la réception
- Nettoyage, suppression ou mise en quarantaine des fichiers et des messages infectés

Contrôle total de la sécurité

- Réception d'une notification d'équipement non protégé en cas d'échec de la mise à jour des stratégies ou des signatures
- Réception d'alertes en cas d'infection de l'équipement par des logiciels malveillants

Gestion centralisée de la sécurité de l'environnement mobile à l'aide du logiciel primé McAfee ePO

- Pour simplifier la gestion, les administrateurs ePO peuvent envoyer des SMS aux périphériques mobiles pour les informer des mises à jour de produits et des actions que l'utilisateur doit effectuer.
- Limitez le contrôle local et les modifications des paramètres de sécurité avec l'agent du client verrouillé.
- Utilisez un mot de passe à usage unique dans le cas où l'agent du client doit être désinstallé au moyen du mot de passe généré par ePO.
- Consignez les entrées d'événement sur le périphérique à des fins d'administration.

