McAfee Security for Email Servers

Sécurisation robuste du contenu de vos serveurs Microsoft Exchange et Lotus Domino

McAfee® Security for Email Servers permet d'identifier et de bloquer les virus, les vers, les chevaux de Troie et les programmes potentiellement indésirables. Compatible avec les serveurs Microsoft Exchange et Lotus Domino, la solution peut également stopper le spam et filtrer les messages pour bloquer les informations inappropriées ou sensibles à l'entrée ou à la sortie du réseau, ce qui facilite le respect des stratégies et des obligations en matière de conformité.

Pour protéger votre infrastructure de messagerie électronique, McAfee allie l'inspection du contenu, l'analyse de la réputation et la protection antimalware. Nous proposons plusieurs niveaux de défense et options de déploiement de la sécurisation de la messagerie électronique : serveur Edge Transport au niveau du périmètre réseau, serveur Hub Transport ou serveur de boîtes aux lettres.

Principaux avantages

- *Système opérationnel en permanence* — Empêchez les vers et les virus de s'introduire via les e-mails ou de se propager en interne via Microsoft Exchange ou Lotus Domino.
- *Productivité du personnel garantie* — Bloquez le spam et les attaques par phishing.
- *Gestion à l'aide d'une console unique* — Le logiciel McAfee ePO offre une console de gestion puissante unique permettant le contrôle, la gestion et l'affichage des rapports.
- *Protection des données critiques* — Filtrez les e-mails à l'entrée et en sortie pour préserver la sécurité des informations et limiter la responsabilité légale de votre entreprise au moyen de technologies de prévention des fuites de données et d'analyse de la réputation (adresses IP, messages et fichiers).
- *Interface utilisateur graphique intuitive* — L'interface conviviale permet d'accéder à des rapports d'une grande richesse, à des graphiques ainsi qu'à des statistiques en temps réel sur le trafic de messagerie.

McAfee Security for Email Servers offre une protection multiniveau de la messagerie électronique à l'entrée et en sortie, notamment grâce à des analyses antimalware à la demande et à la mise en œuvre de stratégies visant à prévenir l'utilisation abusive ou les fuites de données sensibles.

- *Protection de premier plan* — S'appuie sur la technologie primée d'analyse en mémoire et incrémentielle à la demande de McAfee pour éliminer les virus, les vers, les chevaux de Troie et autres menaces des messages électroniques entrants et sortants.
- *Mesures de protection internes efficaces* — Détecte les menaces qui pourraient avoir trompé vos défenses périmétriques ou atteint le réseau via la messagerie interne ou des ordinateurs portables infectés. Le module antispam permet en outre de bloquer le courrier indésirable.
- *Filtrage de contenu puissant* — Garantit la mise en œuvre des stratégies de sécurité de l'entreprise en matière d'utilisation de la messagerie électronique en bloquant les types de fichiers interdits et le contenu inapproprié ainsi qu'en empêchant les fuites de données sensibles.
- *Gestion à l'aide d'une console unique* — Utilise la plate-forme McAfee ePolicy Orchestrator® (McAfee ePO™) pour le déploiement et la gestion de la sécurité, et pour l'affichage de rapports graphiques détaillés.

Protection de la messagerie électronique multiniveau

Protection antimalware complète

McAfee Security for Email Servers recourt à des fonctionnalités antimalware avec analyse de la réputation des fichiers en temps réel qui réduisent considérablement votre exposition aux menaces émergentes. Au travers de son réseau mondial de renseignements sur les menaces hébergé dans le cloud McAfee Global Threat Intelligence™ (McAfee GTI™), McAfee envoie une empreinte de tout fichier suspect détecté à McAfee Labs, à des fins d'analyse instantanée de la réputation. Si une correspondance est établie avec un logiciel malveillant connu, une réponse appropriée est renvoyée au bout de quelques millisecondes seulement, afin de bloquer le fichier ou de le mettre en quarantaine. Le service de réputation des messages de McAfee GTI est un service dans le cloud complet en temps réel qui analyse la réputation des expéditeurs et des messages afin de permettre aux produits McAfee de protéger les clients contre les menaces véhiculées par la messagerie électronique, telles que le spam, qu'elles soient connues ou émergentes.

Réputation des messages

La réputation des messages est combinée à des facteurs tels que les modèles d'envoi de spam et le comportement IP pour déterminer la probabilité que le message en question soit malveillant. Le score de réputation repose non seulement sur les renseignements collectifs recueillis par les sondes qui interrogent le cloud McAfee et les analyses réalisées par McAfee Labs, mais également sur la mise en corrélation d'informations sur les menaces émanant de divers vecteurs : le Web, la messagerie électronique et le réseau.

Réputation des adresses IP

La solution détecte les menaces dans les e-mails en fonction de l'adresse IP du serveur d'envoi. La fonction de réputation des adresses IP prévient les dommages et le vol de données en bloquant les e-mails au niveau de la passerelle.

Protection des serveurs 24h/24 et 7j/7

McAfee Security for Email Servers vérifie dans les e-mails entrants et sortants la présence de virus, de vers, de chevaux de Troie et d'autres logiciels malveillants. La solution analyse également tous les e-mails internes afin d'empêcher la propagation d'un ver au sein de l'entreprise. Elle télécharge automatiquement les fichiers de signatures de virus (DAT) les plus récents via HTTP, FTP, un partage de fichiers réseau ou la console de gestion centralisée McAfee ePO.

Mise en conformité

Les messages sont filtrés en fonction de leur taille, de leur contenu ou du type des pièces jointes. Ceux qui contiennent des termes spécifiques dans leur ligne d'objet, dans le corps de message ou dans les pièces jointes sont bloqués ou mis en quarantaine.

Spécifications

Pour faire face à la croissance exponentielle des e-mails et des données partagées sur les serveurs de messagerie, McAfee Security for Email Servers prend en charge à la fois les environnements Microsoft Exchange et Lotus Domino, assurant la productivité des employés et la continuité permanente des activités de l'entreprise.

McAfee Security for Microsoft Exchange — Configuration requise

Systèmes d'exploitation pris en charge

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

Serveurs Microsoft Exchange pris en charge

- Exchange Server 2003, y compris la version 32 bits
- Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013
- Serveurs Exchange Server avec cluster

McAfee Security for Lotus Domino sous Windows — Configuration requise

- Microsoft Windows Server 2008 ou 2008 R2
- Lotus Domino version 8.5.x (32 ou 64 bits)

McAfee Security for Lotus Domino sous Linux — Configuration requise

- Novell SUSE Linux Enterprise Server (SLES) 10 ou 11
- Red Hat Enterprise Linux (RHEL) 5.x ou 6.x
- Lotus Domino 8.5 (32 ou 64 bits)

Gain de temps et de ressources

Des filtres de contenu prédéfinis simplifient la création et la mise en œuvre des stratégies. Créez des règles globales et ajoutez les exceptions nécessaires pour chaque individu et département. Pour la gestion, utilisez l'interface HTML intégrée ou la plate-forme McAfee ePO.

Filtrage de contenu

La solution analyse le contenu et le texte dans la ligne d'objet ou le corps d'un e-mail et ses pièces jointes. Vous pouvez créer vos propres règles de filtrage de contenu sur la base d'expressions régulières.

Prévention des fuites de données et conformité

La prévention des fuites de données (DLP, *Data Loss Prevention*) garantit que les e-mails envoyés (en transit) ou stockés (au repos) respectent les règles de confidentialité et de conformité de votre entreprise. La configuration est rapide grâce aux dictionnaires prédéfinis associés aux règles de conformité propres aux entreprises et au pays. Le workflow intégré transfère automatiquement les e-mails en quarantaine aux auditeurs pour analyse.

Filtrage du spam et productivité accrue

Préservez le niveau de productivité du personnel et évitez tout gaspillage inutile de la capacité de stockage des serveurs de messagerie en interceptant le spam et les e-mails de phishing grâce au module antispam. Les utilisateurs peuvent également créer leurs propres listes de blocage et d'autorisation. Grâce à une solution de quarantaine unique partagée avec les solutions McAfee de sécurisation de la messagerie électronique pour passerelles, ils peuvent facilement accéder à une seule et même zone de quarantaine.

Alertes sur l'état de fonctionnement du produit

McAfee Security for Email Servers envoie des notifications concernant l'état du produit à l'administrateur désigné. Ces notifications peuvent être configurées et leur envoi peut être planifié en fonction de vos besoins.

Mise à jour en toute facilité

Les mises à jour automatiques vous permettent de bénéficier des dernières informations de sécurité fournies par McAfee Labs, le premier centre de recherche au monde en matière de menaces informatiques.

Centralisation et consolidation de vos zones de quarantaine d'e-mails

Intégré avec McAfee Security for Email Servers, McAfee Quarantine Manager consolide les fonctionnalités de gestion antispam et de mise en quarantaine au sein d'une solution unique. McAfee Quarantine Manager permet d'envoyer des échantillons à McAfee Labs. Facile à gérer, il associe des contrôles d'administration granulaires, la synchronisation automatique des utilisateurs à partir des serveurs LDAP, la gestion des listes d'autorisation et de blocage définies par l'utilisateur ou globales ainsi que la génération de rapports d'une grande précision — le tout administré à partir de la plate-forme McAfee ePO.

Prise en charge de l'ensemble des serveurs

Protégez vos serveurs de messagerie utilisant les principaux systèmes d'exploitation, notamment Microsoft Windows ou Linux sur des plates-formes 32 et 64 bits.

Analyse et sécurisation des banques d'e-mails

McAfee Security for Email Servers prend en charge les analyses à la demande planifiées avec des options de configuration granulaires qui permettent de les exécuter plus rapidement que les analyses complètes traditionnelles. La solution offre la possibilité d'analyser uniquement certains e-mails grâce à la sélection de critères : messages avec pièces jointes, messages non lus, période à laquelle ils ont été reçus, objet, expéditeur, destinataire, destinataire en copie, identifiant de message ou encore taille du message.

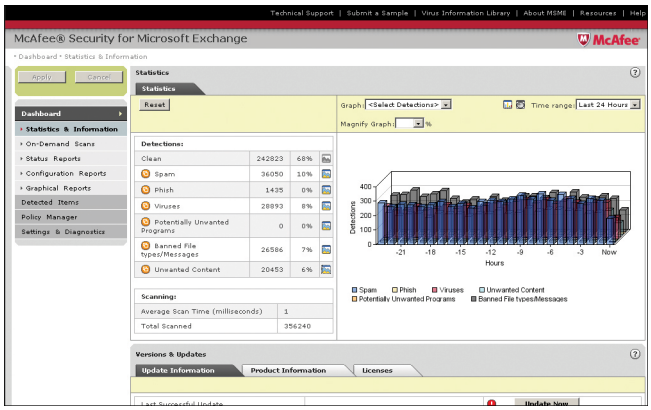

Figure 1 — L'interface conviviale permet d'accéder à des rapports d'une grande richesse, à des graphiques ainsi qu'à des statistiques en temps réel sur le trafic de messagerie.

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

60079ds_security-email-servers_0213_fnl_ASD