McAfee Email Gateway

Protection de la messagerie d'entreprise

Principaux avantages

Protection complète du trafic à l'entrée et en sortie

- Protection complète à l'entrée contre les menaces transmises par la messagerie électronique
- Chiffrement des messages intégré
- Modèles de conformité prédéfinis et fonction de prévention des fuites de données intégrée pour éviter la perte d'informations sensibles

Évolutivité élevée et fonctions avancées de gestion et de protection

- Solution disponible dans plusieurs formats : appliance virtuelle, appliance matérielle, serveur lame ou solution hybride intégrée avec McAfee SaaS Email Protection
- Gestion centralisée, recherche de messages, génération de rapports et mise en quarantaine
- Clustering et équilibrage de charge intégré évolutifs pour répondre aux impératifs des déploiements sur site les plus exigeants

Profitez des avantages offerts par Security Connected grâce à McAfee® ePolicy Orchestrator® (McAfee ePO™), à McAfee Global Threat Intelligence (McAfee GTI), à McAfee Advanced Threat Defense et à une approche hybride de protection de la messagerie électronique.

La messagerie électronique est devenue un moyen de communication indispensable et l'un des services les plus stratégiques de tout environnement d'entreprise. Sa capacité à distribuer instantanément un large éventail d'informations au-delà des frontières organisationnelles, géographiques et politiques fait d'elle un outil essentiel, mais aussi un défi énorme en termes de sécurité. McAfee® Email Gateway vous aide à améliorer la sécurité de votre système de messagerie et combine dans une appliance unique, facile à déployer, plusieurs niveaux de défense tels que la protection contre les menaces à l'entrée, la prévention des fuites de données en sortie, le chiffrement, la mise en conformité avancée et l'administration centralisée.

Les défis inhérents à la sécurité de la messagerie électronique

À l'heure actuelle, la sécurité de la messagerie électronique pose de graves problèmes aux entreprises :

- Les attaques liées au courrier entrant sont de plus en plus souvent le fait de cybercriminels organisés en quête d'informations à exploiter dans un but lucratif. Ces attaques font appel à des techniques sophistiquées d'ingénierie sociale et mutent rapidement afin de déjouer les défenses traditionnelles basées sur les signatures.
- La messagerie électronique est un important vecteur de fuites d'informations sensibles et confidentielles, que ce soit à cause d'employés bien intentionnés mais négligents ou d'utilisateurs internes malveillants.
- À cause de son importance opérationnelle et de sa grande vulnérabilité, la messagerie électronique fait désormais l'objet d'une surveillance étroite de la part d'organismes de régulation au-delà des frontières politiques et sectorielles. C'est ainsi que les réglementations couvrent les cartes de paiement (PCI DSS), les services financiers (GLBA), les soins de santé (HIPAA) et toutes les sociétés publiques américaines (SOX).
- Le spam représente environ 75 % du volume mondial d'e-mails, avec des différences marquées selon le pays. Les attaques par spear phishing deviennent de plus en plus ciblées, efficaces et motivées par l'appât du gain.
- McAfee Labs a identifié environ 2 250 URL de phishing par jour au 4e trimestre 2013, et cette valeur est restée constante au fil de l'année.

intel Security

Distinctions reçues en 2013

- Leader du Magic Quadrant de Gartner pour la catégorie de passerelles de protection de la messagerie électronique
- Leader du classement Forrester Wave dans la catégorie de solutions de protection du contenu des e-mails
- Cinq étoiles et prix du meilleur rapport qualité-prix (« Best Buy ») décernés par *SC Magazine* dans la catégorie des meilleures solutions de protection du contenu des e-mails
- McAfee nommé parmi les innovateurs du secteur par *SC Magazine* pour la protection des données

Pourquoi vous contenter d'une protection fragmentée et inadéquate ?

La protection de la messagerie déployée dans les entreprises à l'heure actuelle a évolué. Malheureusement, la plupart des solutions ciblent uniquement le courrier entrant et n'offrent aucune protection contre les fuites de données en sortie. Les systèmes de défense regroupent souvent diverses solutions isolées (antivirus, antispam, antiphishing, antimalware, chiffrement, prévention des fuites de données), achetées auprès de différents fournisseurs, déployées individuellement et reconfigurées à maintes reprises. Beaucoup ne respectent pas les normes actuelles en matière de performances.

Ainsi, si les principales solutions antispam enregistrent un taux de détection d'au moins 99 %, bon nombre n'atteignent que 95 % ou moins. Si cette différence de 4 % peut paraître insignifiante de prime abord, elle représente en réalité une différence de 400 % en termes de pénétration du spam et d'infections potentielles des systèmes. En outre, dans la mesure où le spam se compte en milliards d'e-mails, une augmentation de 4 % peut avoir un impact non négligeable sur les activités, en encombrant la bande passante et en surchargeant l'infrastructure de messagerie électronique. La moindre infiltration de courrier indésirable peut détourner les utilisateurs de leurs activités normales dès lors qu'ils doivent faire le tri dans leur boîte de réception pour en supprimer le spam. Les risques d'infections par des logiciels malveillants augmentent avec, pour conséquence, une hausse des coûts, une diminution de la productivité et des pertes potentielles de données.

Inéluctablement, la plupart des départements informatiques consacrent trop de temps et d'argent à gérer des défenses fragmentées, à empêcher les fuites d'informations sensibles, à prouver la conformité aux réglementations et à réparer les dégâts causés par une sécurité insuffisante de la messagerie électronique. Une solution complète intégrant des défenses à l'entrée et en sortie, simplifiant l'administration et la mise en conformité, apparaît donc comme un atout important pour l'entreprise. McAfee Email Gateway offre tous ces avantages.

Protection complète de la messagerie électronique

Niveau de sécurité de pointe

McAfee Email Gateway intègre une protection évoluée contre les menaces à l'entrée, à laquelle s'ajoutent des fonctionnalités telles que la prévention des fuites de données en sortie, la mise en conformité avancée, le chiffrement des e-mails, la génération de rapports et la gestion unifiée, dans une plate-forme robuste tout-en-un proposée à un prix unique.

- La combinaison des informations réseau locales et des données sur la réputation fournies par McAfee GTI lui permet d'offrir la protection la plus complète contre les menaces entrantes, le spam et les logiciels malveillants.
- Les fonctions de McAfee Gateway Anti-Malware Engine telles que l'analyse des liens au moment du clic avec émulation comportementale bloquent les attaques recourant aux URL malveillantes.
- L'intégration avec McAfee Advanced Threat Defense permet la détection des logiciels malveillants les plus sophistiqués et difficiles à identifier, grâce à l'association innovante d'une analyse dynamique (*sandbox*) avec une analyse statique du code.
- Ses technologies sophistiquées d'analyse du contenu, l'association de plusieurs techniques de chiffrement et la gestion des messages granulaire et basée sur des stratégies empêchent les fuites de données en sortie et simplifient le respect de la conformité.
- L'intégration complète avec le logiciel McAfee ePO assure une gestion complète de la solution, au sein des clusters ou entre ceux-ci, couplée à des fonctions de journalisation et de génération de rapports d'entreprise visant à simplifier les tâches d'administration et de mise en conformité, tout en réduisant considérablement les coûts.

Protection complète contre les menaces à l'entrée
McAfee Email Gateway identifie et bloque le spam entrant avec un taux de fiabilité de plus de 99 %. Parallèlement, il offre une protection intégrée contre les virus, les logiciels malveillants, le phishing, la collecte d'adresses e-mail et les attaques par déni de service et par retours de courrier (*bounce-back attack*). Il prévient les menaces « jour zéro » ainsi que les attaques ciblées et combinées, et réduit considérablement l'impact des pics de spam grâce à une classification dynamique du courrier indésirable alliée à la réponse aux menaces. McAfee Email Gateway fournit des mises à jour grâce aux informations de réputation sur les expéditeurs, les messages et les URL transmises par McAfee GTI.

Un moteur antivirus secondaire intégré permet aux clients de disposer d'une protection multiniveau contre les logiciels malveillants et de satisfaire les impératifs de conformité.

Analyse des liens au moment du clic pour bloquer les attaques capables d'évoluer
McAfee ClickProtect, une fonctionnalité de McAfee Email Gateway, élimine les menaces utilisant comme vecteur des URL incorporées dans les e-mails. Elle recherche les modifications de l'intention d'une URL susceptibles de survenir entre le moment où le message est analysé, même si ce dernier semble inoffensif, et le moment où l'utilisateur clique sur l'URL. Cette « réinspection » comprend un contrôle de la réputation des URL et une émulation proactive s'appuyant sur la même technologie antimalware de pointe intégrée à McAfee Web Protection pour protéger les passerelles. Les administrateurs peuvent configurer des stratégies déclenchées au moment de l'analyse et au moment du clic, et activer l'émulation d'URL pour protéger les utilisateurs contre les clics inopportuns. Safe Preview propose un aperçu des pages qui seront affichées et fait donc appel au bon sens de l'utilisateur pour renforcer encore la sécurité. Pour bloquer entièrement tout accès au Web à partir des e-mails, il est possible de détecter et de supprimer les URL des messages, ou de les remplacer par un texte d'explication.

Détection des logiciels malveillants sophistiqués et difficiles à identifier grâce à McAfee Advanced Threat Defense
McAfee Advanced Threat Defense recourt à une approche multiniveau innovante pour détecter les logiciels malveillants de type « jour zéro » furtifs. La solution combine des fonctions d'analyse statique de code et d'analyse dynamique en environnement restreint (*sandboxing*) pour décortiquer le comportement réel du malware. L'intégration étroite entre McAfee Email Gateway et McAfee Advanced Threat Defense permet de réaliser cette analyse sur les pièces jointes suspectes, bloquant ainsi les e-mails identifiés comme malveillants avant même qu'ils ne puissent atteindre la boîte de réception.

D'une part, les méthodes d'analyse moins intensives telles que l'analyse des signatures ou l'émulation en temps réel préservent les performances. D'autre part, l'ajout de l'analyse statique complète de code à l'analyse dynamique fournit des informations détaillées pour la classification des logiciels malveillants et étend la protection aux menaces extrêmement bien dissimulées et employant des techniques de contournement, tout en permettant l'identification de logiciels malveillants associés à la menace principale grâce à la détection de code recyclé. Les chemins d'exécution différés ou conditionnels, qui ne sont généralement pas exécutés en environnement dynamique, peuvent être détectés grâce à la décompression et à l'analyse statique complète du code.

Ensemble, l'analyse statique du code et l'analyse dynamique offrent une méthode d'évaluation complète et des informations détaillées — par exemple, une synthèse du comportement, la gravité des logiciels malveillants détectés, les associations entre familles de logiciels malveillants, les chemins d'exécution ou encore le pourcentage de code exécuté pendant l'analyse dynamique.

Filtrage par liste grise pour limiter encore le courrier indésirable
Le courrier indésirable peut consister en des messages légitimes mais diffusés en masse, c'est-à-dire des e-mails que l'utilisateur a un jour sollicités mais ne souhaite plus recevoir (newsletters, notifications, etc.). Les e-mails sur liste grise ne sont généralement pas considérés comme du spam mais ils constituent une nuisance considérable pour leurs destinataires. Des filtres déclenchant des actions comme le blocage et la mise en quarantaine contribuent à désencombrer vos boîtes de réception.

Protection complète à la sortie pour sécuriser le contenu

Chiffrement des e-mails intégré

La solution inclut en standard un chiffrement des e-mails basé sur des stratégies qui fait appel à un ensemble de technologies B-to-B (TLS, S/MIME et OpenPGP) et B-to-C (Push/Pull). Ainsi, même les destinataires ne disposant pas de fonctionnalités de chiffrement peuvent recevoir des messages sécurisés et y répondre. La technologie Push/Pull inclut un client de messagerie web personnalisable, sur lequel vous pouvez apposer votre marque, et permet d'extraire et d'afficher des messages chiffrés sur les équipements mobiles. Puisque le chiffrement est appliqué au niveau de la passerelle plutôt qu'au niveau du poste de travail, les utilisateurs n'ont plus à déterminer eux-mêmes si et de quelle manière ils doivent chiffrer leurs messages, et, surtout, ne risquent plus d'oublier de chiffrer des données sensibles.

Conformité et prévention des fuites de données

La solution comprend en outre en standard une bibliothèque étendue de modèles de conformité intégrés, identiques à ceux proposés par McAfee Data Loss Prevention. Des techniques de détection des empreintes, d'analyse lexicale et de clustering viennent compléter la mise en correspondance des mots clés et des modèles pour permettre une détection complète des données structurées et non structurées. La passerelle identifie avec précision le contenu réglementé (HIPAA, SOX, GLBA) et les informations d'identification personnelle, telles que les numéros de carte de crédit, les numéros de sécurité sociale, les identifiants propres aux régions et d'autres données sur les clients et le personnel. McAfee Email Gateway est également à même de détecter les données non structurées et les éléments de propriété intellectuelle, comme le code source, les brevets, les informations financières et les projets d'entreprise, et de prendre les mesures appropriées. En cas de détection d'une fuite, la solution exécute une série d'actions déterminées par des stratégies, dont le chiffrement forcé (Push/Pull, TLS), le déclenchement d'alertes, le réacheminement, la mise en quarantaine, le blocage et d'autres actions personnalisées.

Autonomisation administrative totale

McAfee Email Gateway aide les administrateurs à mettre en place une protection optimale de la messagerie électronique et offre la possibilité de documenter celle-ci à l'aide de rapports d'entreprise, de journaux exportables complets, d'alertes et de tableaux de bord configurables en temps réel, et de rapports détaillés. Il allie performances, évolutivité, stabilité et modèle de diffusion flexible pour garantir un retour sur investissement maximal et une charge administrative minimale. La solution peut être gérée depuis la console d'administration McAfee Email Gateway ou le logiciel McAfee ePO. Elle offre également les fonctionnalités suivantes :

Contrôles sophistiqués basés sur les stratégies et l'utilisation pour une administration simplifiée

- Interface élégante et intuitive ; installation et configuration à l'aide d'Assistants
- Intégration d'annuaire et du protocole LDAP (Lightweight Directory Access Protocol)
- Gestion centralisée et complète de la sécurité de votre messagerie, qui inclut une mise en œuvre granulaire des stratégies, la recherche de messages et des journaux de conversations détaillés
- Rapports générés en temps réel, notamment des tableaux de bord interactifs et des fonctionnalités de rapports détaillés

Hautes performances grâce à une architecture de pointe

- Analyse en mémoire asynchrone
- Mise en cluster et équilibrage de la charge intégrés pour bénéficier d'une disponibilité élevée
- Le serveur McAfee Quarantine Manager, hautement évolutif et proposé en version indépendante ou embarquée, assure des services de mise en quarantaine consolidée pour plusieurs appliances McAfee Email Gateway. Il offre des files d'attente de mise en quarantaine personnalisées et soulage la charge de stockage et de traitement grâce à une capacité pouvant atteindre 1,5 million de messages et à la prise en charge de jusqu'à 200 000 utilisateurs.

Certifications et support

- Certification Common Criteria niveau EAL2+, y compris la conformité NDPP
- Certification et validation logicielle FIPS 140-2 L1
- Prise en charge de la carte d'accès commun (CAC x.509)
- Prise en charge d'IPv6

Pérennité garantie : protection totale de la messagerie électronique pour toutes les entreprises

Souplesse de déploiement

Vous pouvez déployer McAfee Email Gateway sous la forme d'une machine virtuelle, d'une appliance matérielle (quatre formats différents) ou au sein d'une architecture de serveur lame. Une telle souplesse offre une protection et une évolutivité à prix abordable, adaptées aux environnements de messagerie professionnelle les plus exigeants. En outre, McAfee Email Gateway fait partie de la solution McAfee Email Protection, qui vous permet de déployer la protection de votre messagerie sous la forme d'une passerelle de messagerie sur site (matérielle ou virtuelle), d'un service de cloud SaaS (Security-as-a-Service) ou d'une solution hybride intégrée, pour un montant d'abonnement unique.

Les entreprises qui cherchent à tirer parti des avantages du cloud tout en maintenant un contrôle sur site peuvent déployer la solution hybride intégrée, qui utilise McAfee Email Gateway comme console d'administration pour gérer les stratégies, générer des rapports consolidés, rechercher des messages et les mettre en quarantaine sur site et dans le cloud. La solution hybride convient parfaitement aux entreprises qui veulent empêcher le contenu malveillant ou indésirable d'accéder au réseau et diminuer la bande passante tout en gérant la manipulation des informations sensibles et le chiffrement à partir d'une appliance installée sur site.

Security Connected

Le cadre d'implémentation Security Connected aide les clients à améliorer leur niveau de sécurité, à optimiser leur protection pour une meilleure rentabilité de l'investissement en sécurité et à bénéficier d'un alignement stratégique de leur sécurité avec les initiatives d'ordre commercial. L'intégration avec le logiciel McAfee ePO permet d'associer la gestion et la génération de rapports au sein des solutions de sécurité et entre celles-ci. McAfee Global Threat Intelligence (McAfee GTI), qui tire parti de l'ensemble de la gamme de solutions McAfee, collecte des renseignements collectifs sur tous les vecteurs de menaces couverts par nos solutions. Ces données et connaissances corrélées sont partagées avec nos produits et solutions, si bien que les solutions de protection de la messagerie électronique fournies par McAfee, division d'Intel Security, disposent en permanence et instantanément d'informations parfaitement à jour. McAfee Advanced Threat Defense recourt à une approche multiniveau innovante pour détecter les logiciels malveillants de type « jour zéro » furtifs et s'intègre de façon transparente à de nombreux produits, dont McAfee Email Gateway. Agissant à l'instar d'une ressources partagée par plusieurs solutions, McAfee Advanced Threat Defense peut être déployé de façon optimale et économique sur tout le réseau, réduisant de ce fait les coûts d'exploitation.

Vous bénéficiez de fonctionnalités puissantes adaptées aux environnements d'entreprise, capables d'évoluer pour répondre aux charges de traitement les plus exigeantes, le tout avec une charge d'administration minimale. La combinaison unique de fonctionnalités, de performances, de fiabilité et de valeur ajoutée de McAfee Email Gateway explique que plus de la moitié des sociétés informatiques du classement Fortune 500 utilisent cette solution de protection de la messagerie électronique. Pour plus d'informations sur McAfee Email Gateway et les autres solutions McAfee de protection de la messagerie électronique, visitez notre site à l'adresse **www.mcafee.com/fr/products/email-and-web-security/email-security.aspx**.

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