Mail-SeCure sur une plateforme VMware

APERÇU

Les menaces liées aux messages électroniques sont un problème connu depuis longtemps. La plupart des entreprises prennent des mesures de protection contre ces menaces, utilisant des solutions dédiées de filtrage de courrier (relais de messagerie)

Les récents changements du marché mondial et les tendances émergentes dans l'économie internationale forcent les responsables des services informatiques à penser à des solutions créatives qui leur permettront de maximiser l'efficacité et à réduire les dépenses de leur service.

Les salles de serveur modernes sont surchargées de plateformes matérielles dédiées, exigeant l'installation et la maintenance de systèmes de refroidissement, d'ondulateurs et d'autres systèmes de surveillance matérielle.

C'est la raison pour laquelle les dépenses liées au matériel sont les plus lourdes dans le budget d'une entreprise, en particulier si l'on considère la hausse des coûts de consommation et des dépenses d'électricité.
Le besoin d'une baisse globale de la consommation d'énergie est une question importante lorsque l'on prévoit de mettre en place des solutions de sécurité de réseau, nouvelles et existantes.

Mail-SeCure de PineApp sur une plateforme VMware est une solution logicielle de filtrage et de gestion de courrier électronique, conçue pour fournir une réponse rentable et éprouvée aux clients recherchant une solution VMware de filtrage et de gestion de courrier électronique

La plateforme Mail-SeCure est équipée de moteurs haute-technologie de sécurisation du périmètre dont la mission est de stopper la grande majorité des menaces en vérifiant la crédibilité de leur source avant qu'elles ne pénètrent dans le réseau du client. L'approche de sécurisation du périmètre de PineApp permet d'économiser une quantité importante de ressources système qui étaient auparavant gâchées dans des contrôles de contenu inutiles.
Mail-SeCure fournit aux administrateurs système les outils nécessaires à la gestion des menaces et d'une série de tâches administratives liées aux messages électroniques.

Mail-SeCure de PineApp a récemment obtenu la certification Anti-Spam Checkmark, au niveau premium, grâce à un taux de détection de plus de 99 %.

FONCTIONNALITÉS

Protection avancée anti-spam basée sur le périmètre

Mail-SeCure est équipé d'un module avancé anti-spam, à couches multiples, qui stoppe la plupart des menaces (jusqu'à 90 %), au niveau du périmètre (avant le réseau de l'entreprise), permettant ainsi d'importantes économies sur la bande passante et les ressources système ainsi qu'un meilleur taux de détection (moins de données sont lues par le système) et un taux inférieur de faux positifs.

La protection post-périmètre comprend l'analyse en profondeur par différents moteurs anti-spam d'inspection du contenu.

Le module anti-spam de Mail-SeCure est enrichi d'une technologie éprouvée stoppant tous les spams connus, y compris les spams image. Mail-SeCure est ainsi capable d'identifier 99 % des spams entrants, de les bloquer ou de les baliser immédiatement comme spam, conformément à la stratégie de l'entreprise.

En combinant des technologies anti-spam et une gestion stratégique avancée, PineApp a réduit le taux de faux positifs à presque zéro.

FEATURES
(continued)

Solution de chiffrement de courrier

Mail-SeCure propose un service de chiffrement de courrier électronique robuste, complet et géré centralement qui garantit que tout message privé demeure confidentiel. Aussi facile à utiliser qu'un courrier électronique standard, il permet aux utilisateurs de chiffrer des messages de façon transparente, suivant la stratégie de sécurité de l'entreprise.

L'appliance vérifie tous les messages sortants pour détecter des correspondances avec les règles stratégiques configurées de chiffrement du contenu. Elle achemine automatiquement tous les messages détectés sur une route sécurisée (SSL), vers le centre SES (Secure Encryption Service) dédié de PineApp, afin qu'ils ne soient signés, chiffrés et envoyés à leur expéditeur d'origine, au format PDF ou HTML. Un accusé de réception certifié confirme que la bonne personne a ouvert le message électronique. Les clients peuvent maintenant chiffrer uniquement les messages nécessaires (messages liés à la sécurité ou d'ordre financier, par exemple) via une route sécurisée (SSL). L'usage d'un centre de chiffrement externe, entièrement sécurisé (SES de PineApp), en plus de la suppression de la charge de la clé et du certificat pour le service informatique de l'entreprise, constitue des économies considérables de ressources réseau et financières.

Gestion avancée

Mail-SeCure propose un ensemble d'outils de gestion, sophistiqués et souples, qui permettent aux administrateurs système, aux postmasters et aux utilisateurs finaux de concevoir des mesures intelligentes et efficaces d'application des stratégies pour avoir ainsi un contrôle complet sur l'audit et la gestion.

Prévention des fuites de données et Package de conformité du contenu

Pour aider les administrateurs système à maintenir une stratégie de sécurité des données entièrement conforme à la règlementation du contenu nationale et internationale, Mail-SeCure propose un jeu d'outils complet permettant une analyse en profondeur de plus de 300 types de fichiers, de manière à bloquer toute fuite de données et tentative de vol.

Rapports du trafic personnel quotidien de l'utilisateur

En envoyant un rapport de trafic quotidien par courrier, Mail-SeCure permet aux clients de gérer leurs propres listes noires et blanches et à libérer tout message ayant été bloqué comme spam. L'appliance envoie un rapport contenant un récapitulatif de tous les messages entrants destinés à ce client spécifique depuis l'envoi du dernier rapport quotidien.

Mail-SeCure peut envoyer des rapports horaires avec une fonctionnalité personnalisable (c'est à dire avec/sans la capacité d'inscrire sur une liste blanche ou noire un certain domaine ou une adresse, avec/sans un lien à la quarantaine personnelle, etc.).

Cela fait économiser à l'administrateur système des tâches inutiles car les utilisateurs peuvent gérer leurs propres listes sans nuire à la stratégie de sécurité générale de l'entreprise.

Contrôle des contenus inappropriés (ICC)

Mail-SeCure propose, en option, un module d'analyse d'image, défini pour détecter, bloquer et consigner toute image inappropriée (comportant de la pornographie, de la nudité, etc.), intégrée ou jointe aux messages entrants, selon une échelle personnalisable.

Le module ICC de Mail-SeCure offre également une fonctionnalité de synchronisation comprenant la liste noire d'URL établie par IWF (Internet Watch Foundation), empêchant tout site au contenu malveillant de s'insérer dans des liens de messages entrants.

L'utilisation d'ICC permet de renforcer considérablement l'efficacité et la couverture du champ de contrôle du contenu de l'appliance.

Prévention de la rétrodiffusion

La rétrodiffusion est un avis de non-remise reçu soit de personnes à qui aucun membre de l'entreprise n'a envoyé de message ou d'une source inconnue. Elle est causée par des virus qui infectent les ordinateurs en dehors du réseau, remplissant la ligne «De» d'un message électronique en sélectionnant des adresses de façon aléatoire dans le carnet d'adresses d'un poste infecté. La rétrodiffusion est également causée par des spammeurs qui inscrivent l'adresse électronique d'une personne dans l'adresse de retour de leur spam. Cela peut entraîner l'envoi de centaines voire de milliers de messages électroniques au serveur de messagerie d'une personne. Mail-SeCure réduit considérablement le volume de rétrodiffusion via une fonctionnalité unique qui empêche la rétrodiffusion et bloque l'entrée des messages retournés indésirables dans le réseau.

AVANTAGES

Efficacité économique optimisée
L'implémentation d'une solution de sécurité virtualisée permet aux entreprises de réduire considérablement les dépenses liées au matériel informatique telles que l'électricité, l'affectation d'espace de stockage physique, la maintenance, la surveillance, etc.

Processus d'installation transparent
Les plateformes virtualisées améliorent la mobilité du produit. Au besoin, il est possible d'effectuer une démonstration virtualisée d'un produit sur des sites distants, même à partir d'un poste de travail générique !

Contribution à un environnement vert
La réduction du nombre de plateformes matérielles dans l'entreprise et, par conséquent, de la consommation totale d'électricité, est en accord avec la nouvelle tendance internationale visant à sensibiliser les entreprises à l'environnement.

Préservation du coeur du système d'exploitation
Alors que toutes les solutions sont en générale installées sur un système central unique, les solutions VMware préservent leur propre coeur opérationnel. Cela signifie que les produits sont séparés les uns des autres et qu'en cas de dysfonctionnement sur une solution, l'activité des autres solutions ne sera pas affectée.

Une solution conforme au contenu
Grâce au package complet de prévention contre les fuites de données, Mail-SeCure propose maintenant une conformité de contenu répondant aux normes nationales et internationales les plus strictes telles que HIAA, SOX, GLBA, Bâle-II, etc. !

Une solution conviviale de ressources système et réseau
Le volume des ressources enregistrées par le biais de la plateforme virtuelle ainsi que le recours à des requêtes sur la base de données externe et le tableau de sécurisation du périmètre de Mail-SeCure permettent de conserver les ressources système et d'améliorer considérablement les performances réseau.

Implémentation technologique en temps réel
Les mises à jour du logiciel de Mail-SeCure consistent non seulement à contrer les menaces de sécurité émergentes mais aussi à mettre en place, en temps réel, de nouvelles fonctionnalités sur demande et des améliorations pour tous les moteurs et les services de l'appliance.

CONFIGURATION MINIMALE

Références de commande	Nbre d'utilisateurs est.	Processeur	Mémoire	Taille du lecteur système	Ports réseau
PA-VM-MS-25	25	Processeur Celeron double cœur E1400	2 G	80 Go SATA2	2xGoE
PA-VM-MS-50	50	Processeur Celeron double cœur E1400	2 G	80 Go SATA2	2xGoE
PA-VM-MS-150	150	Processeur Celeron double cœur E1400	2 G	80 Go SATA2	2xGoE
PA-VM-MS-300	300	Processeur Intel double cœur Duo E7400	2 G	80 Go SATA2	2xGoE
PA-VM-MS-600	600	Processeur Intel double cœur Duo E7400	2 G	160 Go SATA2	2xGoE
PA-VM-MS-850	850	Processeur Intel double cœur Duo E7400	2 G	160 Go SATA2	2xGoE
PA-VM-MS-1K	1,000	Processeur Intel double cœur Duo E8400	4 G	160 Go SATA2	2xGoE
PA-VM-MS-2K	2,000	Xeon E5405 (4 cœurs)	4 G	146 Go SAS	2xGoE
PA-VM-MS-3K	3,000	Xeon E5405 (4 cœurs)	4 G	146 Go SAS	2xGoE
PA-VM-MS-4K	4,000	Xeon E5405 (4 cœurs)	4 G	146 Go SAS	2xGoE
PA-VM-MS-5K	5,000	Xeon E5405 (4 coeurs)	4 G	146 Go SAS	2xGoE
PA-VM-MS-10K	10,000	Xeon E5405 (4 cœurs)	4 G	146 Go SAS	2xGoE
PA-VM-MS-25K	25,000	2x Xeon E5405 (4 cœurs)	4 G	146 Go SAS	2xGoE
PA-VMDR-850 (Directeur jusqu'à 850 utilisateurs)		Processeur Intel double cœur Duo E7400	2 G	160 Go SATA2	2xGoE
PA-VMDR-3 K (Directeur jusqu'à 3 000 utilisateurs)		Xeon E5405 (4 cœurs)	4 G	146 Go SAS	2xGoE
PA-VMDR-25K (Directeur jusqu'à 25 000 utilisateurs)		2x Xeon E5405 (4 cœurs)	4 G	146 Go SAS	2xGoE

Remarques :

- ✓ Lecteur système recommandé @ RAID 1 au-dessus de 1 500 utilisateurs.
- ✓ Système recommandé avec mémoire maximum >=4 Go

GAMME DE PRODUITS

Mail-SeCure est un produit de sécurisation du périmètre du courrier électronique qui protège les entreprises de toutes tailles contre les menaces liées aux messages électroniques, ciblés et non ciblés. Mail-Secure se décline sur différentes plateformes logicielles et d'appliance.

La gamme Mail-SeCure 1000 protège les petites entreprises et les bureaux à domicile (de 1 à 50 utilisateurs de messagerie).

La gamme Mail-SeCure 2000 protège les entreprises de taille moyenne (de 100 à 500 utilisateurs de messagerie).

La gamme Mail-SeCure 3000 protège les entreprises de taille moyenne plus grandes (de 500 à 1 500 utilisateurs de messagerie).

La gamme Mail-SeCure 5000 protège les entreprises plus grandes (de 2 500 à 25 000 utilisateurs de messagerie). Mail-SeCure as Software protège les sociétés de toutes tailles (de 1 à 25 000 utilisateurs de messagerie).

Mail-SeCure sur une plateforme VMware protège les sociétés de toutes tailles (de 1 à 25 000 utilisateurs de messagerie).

RÉCAPITULATIF

Mail-SeCure sur une plateforme VMware est la solution de sécurité de messagerie électronique la plus efficace disponible aujourd'hui sur le marché pour les réseaux VMware. Elle est largement représentée dans le monde entier, sans dysfonctionnement ou temps d'arrêt et un taux de blocage de spam exceptionnellement élevé.

La facilité d'utilisation et d'accès de Mail-SeCure et le système d'autorisations détaillé permettent aux utilisateurs finaux de gérer leur propre boîte de réception, sans nuire à la sécurité de la messagerie électronique (ou de l'entreprise) et sans détourner les règlementations stratégiques en matière de messagerie électronique appliquées par l'administrateur.

Les moteurs de sécurisation du périmètre de Mail-SeCure, robustes et précis, permettent de conserver intactes les ressources système et réseau.

Une stratégie intelligente de sécurisation du périmètre de courrier électronique permet non seulement de renforcer la qualité des services de messagerie électronique mais également les services réseau.

La conception souple et novatrice de Mail-SeCure, ainsi que ses mises à jour fréquentes et autonomes, permettent de protéger l'entreprise de toute menace liée au courrier électronique, existante ou émergente, et en temps réel !

Les entreprises de toutes tailles et de tous domaines, cherchant à solution efficace et complète de sécurité de messagerie électronique, adaptée à leur taille, trouveront dans Mail-SeCure sur une plateforme VMware la solution répondant le mieux à leurs besoins en matière de sécurité de messagerie électronique.

CONTACT

Les solutions de la gamme Mail-SeCure de PineApp sont disponibles en version d'essai gratuite pour les clients souhaitant acheter le produit.

Pour vous inscrire à une version d'essai gratuite de 30 jours, appelez le +972-4-8212321 ou rendez-vous sur notre site Web à l'adresse : http://www.pineapp.com/try.

P32V05/10-F-L

PineApp LTD.
8 Hata'asia Street, Nesher Israël 36601 POB 136
Tél. : +972-4-821-2321 Fax : +972-4-820-3676
Courriel : info@pineapp.com Web : www.pineapp.com

PineApp est l'un des principaux fournisseurs de solutions de sécurité pour les services informatiques. PineApp propose des solutions complètes de sécurité de messagerie électronique, d'archivage de messagerie électronique et de filtrage de contenu web, disponibles en tant que module d'appliance ou logiciel (sur un serveur ou sur la plateforme VMware). Les solutions PineApp sont également disponibles pour les fournisseurs d'accès Internet (FAI) souhaitant offrir des services en ligne et une solution de plan de reprise après sinistre à leurs clients.