FICHE PRODUIT

Symantec® Messaging Gateway

Sécurité des messages entrants et sortants

EN RÉSUMÉ

Symantec® Messaging Gateway (SMG) protège vos communications électroniques contre les spams, malwares et attaques ciblées.

PRINCIPAUX AVANTAGES

- Arrêtez les menaces avancées
- Bloquez les messages électroniques indésirables
- Protégez vos données sensibles
- Développez une visibilité approfondie sur les menaces véhiculées par la messagerie électronique

PRINCIPALES FONCTIONNALITÉS

- Technologies de détection à plusieurs niveaux
- Filtrage de contenu avancé
- Protection contre la perte de données
- Audits détaillés
- Intégrations de sécurité puissantes

Présentation

La messagerie électronique est l'un des principaux canaux de communication de l'entreprise. Elle est aussi l'un des vecteurs d'attaque les plus populaires des pirates informatiques qui l'utilisent pour lancer et distribuer des attaques par spear phishing, ransomware ou encore des courriers électroniques frauduleux. L'humain est généralement considéré comme étant le maillon faible de la chaîne de sécurité : de fait, un simple clic sur le mauvais lien ou l'envoi d'un fichier contenant des données sensibles peut avoir des effets désastreux pour l'entreprise. Que votre système de messagerie électronique soit géré sur site, dans le cloud ou de manière hybride, pour sécuriser efficacement le courrier électronique de votre entreprise, vous devez d'abord prévenir la survenue de ces événements. Il s'agit de bloquer et de mettre en quarantaine les messages suspects avant qu'ils n'atteignent vos utilisateurs, et de surveiller les messages sortants, pour veiller à ce que les données de votre entreprise soient protégées.

Symantec® Messaging Gateway (SMG) est une solution de sécurisation de la messagerie électronique sur site qui s'appuie sur les capacités suivantes pour assurer la sécurité des messages entrants et sortants de l'entreprise :

- Technologies de détection à plusieurs niveaux
- Filtrage de contenu avancé
- Protection contre la perte de données
- Audits détaillés
- Intégrations de sécurité puissantes

Ces fonctionnalités centrales protègent vos communications électroniques contre les spams, malwares et attaques ciblées. SMG prévient également les fuites de données, que celles-ci soient accidentelles ou le résultat d'actions malveillantes. Elle peut être implémentée sous la forme d'une appliance virtuelle ou physique. Vous avez la possibilité d'ajouter facilement des capacités, afin que le volume des spams n'affecte pas les performances de votre système de messagerie.

Des technologies de détection à plusieurs niveaux pour bloquer les menaces avancées

Pour bloquer et mettre en quarantaine les messages suspects, SMG associe des technologies de détection à plusieurs niveaux qui exploitent les données du plus grand réseau civil de renseignement au monde.

- **Messages électroniques frauduleux (attaques BEC) :** la solution s'appuie sur des analyses heuristiques avancées, un moteur d'analyse des messages frauduleux, l'authentification des expéditeurs et les informations sur les domaines pour prévenir les vols d'URL et les usurpations d'identité.
- **Attaques de spear phishing :** la solution protège les utilisateurs contre les liens malveillants utilisés dans les campagnes de spear phishing à l'aide d'un filtrage de réputation d'URL. Basé sur la base de données globale de Symantec, ce filtrage permet d'identifier les liens similaires à ceux utilisés dans le cadre d'attaques de phishing connues.
- **Attaques par ransomware :** la solution protège les utilisateurs contre les attaques par ransomware ciblées en supprimant les menaces Zero Day dans les pièces jointes Microsoft Office et PDF. Tout contenu actif potentiellement malveillant détecté dans une pièce jointe est supprimé de celle-ci. Le fichier est ensuite reconstruit, puis de nouveau joint au message initial avant d'être envoyé à l'utilisateur final.
- **Attaques d'annuaire (DHA) :** la solution exploite une combinaison de bases de données d'expéditeurs Symantec globales et locales, des analyses heuristiques et des règles de spam définies spécifiquement pour le client afin de bloquer jusqu'à 99 % des messages électroniques indésirables avant qu'ils n'atteignent votre réseau. La limitation des expéditeurs sortants permet de prévenir les attaques de spam qui proviendraient de comptes utilisateurs internes compromis, ce qui aurait pour effet de dégrader la réputation de l'entreprise.
- **Attaques d'emprunt d'identité :** la solution s'intègre avec Symantec Email Fraud Protection pour automatiser la création de protocoles d'authentification des expéditeurs (DMARC, DKIM et SPF) et ainsi protéger l'ensemble des destinataires des attaques d'emprunt d'identité.

Le filtrage de contenu pour bloquer les messages électroniques indésirables

Les contrôles de filtrage de contenu avancé de SMG empêchent des messages électroniques indésirables tels que des newsletters et autres messages marketing de parvenir aux utilisateurs de votre entreprise. SMG exploite aussi une combinaison de bases de données d'expéditeurs Symantec globales et locales, des analyses heuristiques et des règles de spam définies spécifiquement pour votre entreprise afin de bloquer jusqu'à 99 % des spams avant qu'ils n'atteignent votre réseau.

La prévention contre la perte de données pour protéger vos données sensibles

SMG intègre des politiques de prévention contre la perte de données qui facilitent la protection des données contenues dans les messages sortants ou leurs pièces jointes. Les administrateurs peuvent s'appuyer sur 100 dictionnaires, schémas et modèles de politiques préconçus pour développer et implémenter des politiques d'application et de protection automatisées de vos données. La solution propose également des fonctionnalités de chiffrement SMTP over TLS automatique qui permettent de sécuriser le trajet de l'ensemble des communications électroniques.

Des audits détaillés pour une gestion approfondie de la sécurité de la messagerie électronique

SMG intègre une console web unique qui fournit des fonctionnalités de configuration et de contrôle affiné des politiques et de reporting détaillé, ainsi qu'une vue consolidée des tendances en matière de menaces, de statistiques sur les attaques et des incidents de non-conformité.

- **Outils d'audit :** les rapports au format tableau de bord, synthétique ou détaillé, créés sur la base des 50 rapports prédéfinis disponibles dans l'application et personnalisés en fonction de vos propres critères de contenu et de planification, permettent de mettre en lumière les tendances en matière de menaces et les problèmes de conformité potentiels.
- **Intégration avec les SIEM :** vous pouvez exporter les données syslog générées par l'application dans des outils de gestion des informations et des événements de sécurité (SIEM) tiers pour réaliser des analyses de corrélation.
- **Convivialité :** le suivi des messages basé sur une interface d'audit graphique permet de déterminer rapidement la disposition et l'état de livraison des messages.

L'architecture de SMG permet la gestion de plusieurs appliances dans un environnement IPv4 et IPv6 mixte.

Intégrations de sécurité puissantes

Pour une protection encore plus renforcée, SMG peut transférer le contenu du fichier des messages vers Symantec Content Analysis pour permettre leur inspection poussée. Cette inspection porte sur des données exploitables combinant analyses statistiques, apprentissage machine et techniques d'analyse comportementale. Un environnement de test (sandbox) adaptatif et personnalisable assure une détonation complète des malwares, pour analyser rapidement les fichiers suspects, interagir avec les malwares en cours d'exécution de façon à révéler leur comportement et exposer les menaces Zero Day et malwares inconnus. SMG s'intègre avec Symantec DLP pour étendre la mise en œuvre des politiques au canal de la messagerie électronique. Enfin, le module additionnel Symantec Content Encryption vous donne la possibilité de chiffrer les messages en fonction de politiques définies.

Flexibilité de déploiement

Le logiciel SMG est disponible sur différentes plates-formes et peut être déployé dans des rôles flexibles pour mettre à la disposition de l'entreprise une architecture modulaire et évolutive qui s'adapte à ses besoins.

Fonctionnalité	Description
Plates-formes prises en charge	*VMware, HyperV, KVM, Microsoft Azure, Appliance Symantec Messaging Gateway 8390 Hardware*
Rôles de déploiement	*Tout-en-un, centre de contrôle, analyseur pour mise en quarantaine uniquement ; mise en quarantaine uniquement*
Facteur de forme flexible	*Montage en rack 1U*
UC	*Processeur double cœur 20*
Mémoire : Disque dur/RAID	*192 Go RAM, 6 x 2,4 To (RAID 10)*
NIC	*Port onboard double 1 Go, adaptateur Base-T pour port 10GbE double*

Résumé

SMG fournit un éventail complet de capacités de détection des menaces pour sécuriser les messages électroniques entrants et sortants de l'entreprise. Ces capacités bloquent les menaces véhiculées par la messagerie électronique, telles que la compromission des comptes de messagerie, les ransomwares et les spams, et empêche vos utilisateurs de diffuser des données sensibles de l'entreprise sans le vouloir. La solution s'intègre également avec d'autres solutions de sécurité Symantec leaders pour renforcer la sécurité de votre entreprise face aux menaces qui touchent à la sécurité de sa messagerie électronique.

Pour plus d'informations, visitez le site broadcom.com/symantec-iam.

BROADCOM
connecting everything®

Pour plus d'informations, visitez notre site web à l'adresse suivante : www.broadcom.com

19D214107-PB101_FR 11 août 2023