Google Message Security

À PROPOS DES SERVICES GOOGLE DE SÉCURITÉ ET D'ARCHIVAGE

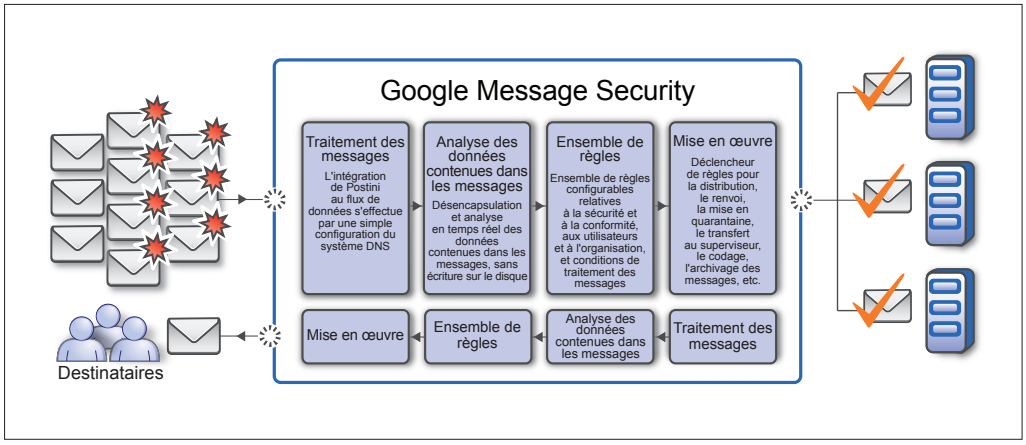
Les services Google de sécurité et d'archivage, fournis par Postini, renforcent la sécurité et la conformité de votre système de messagerie. Basés sur une plate-forme d'hébergement de services, ces produits bloquent le spam, les attaques de phishing et les logiciels malveillants, entre autres types d'intrusions, avant qu'ils n'atteignent votre réseau. Ils proposent également des fonctionnalités de gestion et d'archivage de contenu qui vous aident à remplir vos obligations légales. Le modèle hébergé de Google offre différents avantages. Grâce à «l'effet réseau» lié aux dizaines de milliers de réseaux de messagerie protégés, la technologie Google peut identifier les nouvelles menaces en temps réel et les bloquer à l'échelle du réseau de sécurité Google, sans qu'il soit nécessaire de procéder à des mises à jour sur site. De la même façon, les économies d'échelle réalisées en stockage, la simplicité de déploiement et l'absence de maintenance ont pour corollaire un faible coût total de possession.

Pour plus d'informations, consultez la page
www.google.com/postini

Google Message Security, service de sécurité des messages fourni par Postini, assure une protection efficace lors de la réception et de l'envoi d'e-mails. S'adressant aux organisations de toutes tailles, il simplifie la gestion de la sécurité et de la conformité des e-mails et permet de libérer des ressources informatiques précieuses. Google Message Security étant toujours actif et à jour, les organisations sont sûres de bénéficier en permanence d'une protection fiable et efficace de leurs systèmes de messagerie.

S'appuyant sur une architecture à la demande, brevetée, Google Message Security bloque le spam, les tentatives de phishing et les virus, entre autres types de menaces touchant les e-mails, avant qu'ils n'atteignent votre organisation. Ce service permet ainsi d'alléger la charge de vos serveurs de messagerie, d'économiser la bande passante et d'améliorer les performances de l'infrastructure de messagerie existante. Google Message Security est fourni en tant que modèle SaaS (Software-as-a-Service), ce qui permet d'économiser les ressources financières et informatiques puisqu'il n'est pas nécessaire d'installer ni d'entretenir du matériel ou des logiciels.

En éliminant l'obligation d'installer régulièrement les correctifs et les mises à jour qu'exigent les autres solutions matérielles ou logicielles, Google Message Security limite le recours aux ressources informatiques. Ce service réduit également la charge de travail de votre centre d'assistance informatique en permettant aux utilisateurs finals de gérer leurs propres paramètres de messagerie et de mise en quarantaine dans une interface Web très simple à utiliser. Plutôt que de faire appel au centre d'assistance, les utilisateurs finals peuvent inspecter la liste des messages mis en quarantaine et traiter les messages de leur choix. Les utilisateurs reçoivent régulièrement un e-mail résumant les mises en quarantaine, avec tous les détails nécessaires. Ils peuvent également paramétrer précisément la protection anti-spam et en définir eux-mêmes le niveau. Toutes ces commandes destinées aux utilisateurs finals étant entièrement configurables, vous contrôlez très exactement les opérations qu'ils sont autorisés à effectuer.



Graphique 1 : Google Message Security protège efficacement les e-mails reçus et envoyés dans toutes les organisations, quelle qu'en soit la taille.

Google Message Security vous permet d'automatiser l'application de vos règles de sécurité en matière de messagerie. Cette application des règles vous aide à assurer la conformité légale et réglementaire des e-mails reçus et envoyés, à tous les niveaux de votre organisation. La prise en charge TLS (Transport Layer Security) permet le cryptage des communications sensibles envoyées par e-mail et peut être appliquée automatiquement à toutes les communications entre des domaines définis. La transmission des communications sensibles ou soumises à certaines règles s'effectue donc toujours avec le niveau de sécurité approprié.

Google Message Security fournit également une console Web d'administration conviviale. Cette console permet de modifier en temps réel la configuration et les règles. Elle inclut un système de surveillance et d'alerte, ainsi qu'une fonctionnalité complète de génération de rapports à l'intention des administrateurs. Les utilisateurs peuvent être définis au niveau de la console. Le service Google Message Security peut également être intégré à la structure d'annuaire de votre organisation à des fins de synchronisation des utilisateurs.

Google Message Security associe de nombreux composants pour fournir une protection efficace contre les menaces affectant les systèmes de messagerie. Ce service comprend les fonctionnalités spécifiques suivantes :

- L'identification en temps réel des menaces, rendue possible par le traitement quotidien de plus de deux milliards d'e-mails, fournit une visibilité globale des menaces émergentes. Cet « effet réseau » identifie et suit automatiquement les adresses IP (Internet Protocol) à l'origine de spam, de la diffusion de virus ou d'attaques DoS (déni de service), etc. Dès qu'une menace est identifiée, elle est bloquée pour tous les clients utilisant Google Message Security. En outre, le système d'identification des menaces se met à jour automatiquement. Lorsque les adresses IP repérées cessent leurs attaques, elles sont à nouveau autorisées à établir des connexions SMTP (Simple Mail Transfer Protocol) afin d'envoyer des e-mails valides.
- Notre technologie brevetée de détection en temps réel du spam examine des milliers d'éléments dans chaque e-mail afin de déterminer s'il s'agit effectivement de spam. Elle assure un filtrage anti-spam extrêmement efficace et affiche des taux de faux positifs exceptionnellement faibles.
- Le système de protection antivirus s'appuie sur l'identification du spam et inclut des méthodes de détection heuristique et basée sur les signatures, à « l'heure zéro », ainsi que plusieurs moteurs antivirus commerciaux.
- Le système de gestion de contenu vous permet de définir des règles pour les e-mails reçus et envoyés, qui fournissent une couche supplémentaire de protection contre les menaces extérieures. Il offre également une protection contre les fuites accidentelles ou délibérées de données confidentielles par le biais des e-mails envoyés et de leurs pièces jointes.
- La technologie de gestion des pièces jointes vous permet de définir des règles spécifiques pour les fichiers en pièce jointe. Elle peut ainsi bloquer ou mettre en quarantaine les messages en fonction du type ou de la taille des fichiers qui leur sont joints. Le système de gestion des pièces jointes inspecte les fichiers d'archives tels que les fichiers .zip ou .rar afin d'évaluer leur contenu. Il vous permet également de définir des règles spécifiques relatives au traitement des fichiers d'archives cryptés.

Fonction	Avantages
Architecture d'intercommunication brevetée	Filtrage extrêmement efficace du spam et taux de faux positifs exceptionnellement faible
Protection antivirus multicouche et système de détection heuristique, basée sur les signatures	Protection à l' « heure zéro » contre les virus à mutation rapide 100 %
Plate-forme SaaS hautement évolutive, avec SLA garantissant une disponibilité du service de filtrage de 99,999 %	Protection toujours active et à jour pour un faible coût total de possession
Console d'administration Web	Mise à jour des utilisateurs et des règles, modifications de configuration et génération des rapports en temps réel
Blocage des attaques DHA (pillage d'annuaire)/DoS (déni de service)	Prévention des attaques grâce à un système breveté d'analyse du comportement
Cryptage TLS basé sur des règles	Transmission sécurisée des e-mails
Filtrage des pièces jointes	Mise en application des règles relatives aux pièces jointes des e-mails
Gestion des règles relatives au contenu	Mise en application des règles relatives aux utilisations autorisées et à la conformité du contenu
Mise en file d'attente des e-mails	Réception ininterrompue des e-mails, même en cas de défaillance du serveur de messagerie

Revendeur et intégrateur Google™ Apps

112 bis rue Jean Jaurès 92800 Paris La Défense, France
Tél. : 01 71 12 60 32
Fax : +33 179 75 90 21
Mail : contact@econsulting.fr

www.econsulting.fr

Google™