blackspider technologies

Présentation de la technologie MailControl Spam

BlackSpider MailControl Spam est un service géré haute performance qui identifie le spam de manière intelligente et bloque sa transmission. S'appuyant sur de multiples techniques, MailControl Spam intercepte en permanence plus de 98 % de vos courriers non sollicités.

Du fait de la nature dynamique du pollupostage, le filtrage de spam constitue un défi complexe à plusieurs égards.

Pour être efficace, un filtre spam doit bloquer un maximum de courriers indésirables avec un minimum de «faux positifs» (courrier valide identifié comme étant un spam).

Pour faire face à ces difficultés, MailControl Spam utilise un moteur anti-spam intelligent qui apprend ce que l'organisation considère être du spam et adapte ses filtres en conséquence.

En combinant cette approche avec une fonction de définition des seuils de spam par utilisateur ou par domaine, MailControl Spam se positionne comme la technologie de filtrage de spam la plus efficace du marché.

Autonomie de l'utilisateur

MailControl Spam reconnaît que l'utilisateur est seul juge pour décider de ce qui est ou n'est pas du spam.

L'utilisateur peut choisir de recevoir régulièrement des rapports sur les messages, d'accéder à son propre espace de mise en quarantaine et de gérer ses propres listes noires et blanches.

Tirant parti du moteur anti-spam adaptatif, cette approche libère les utilisateurs et administrateurs e-mail des problèmes liés aux faux positifs, d'où une totale confiance de leur part.

Vue d'ensemble de la technologie

Le processus d'analyse ne prend en tout que quelques secondes. Une fois analysé au moyen des neuf différentes techniques de MailControl, chaque message reçoit une "note spam" globale.

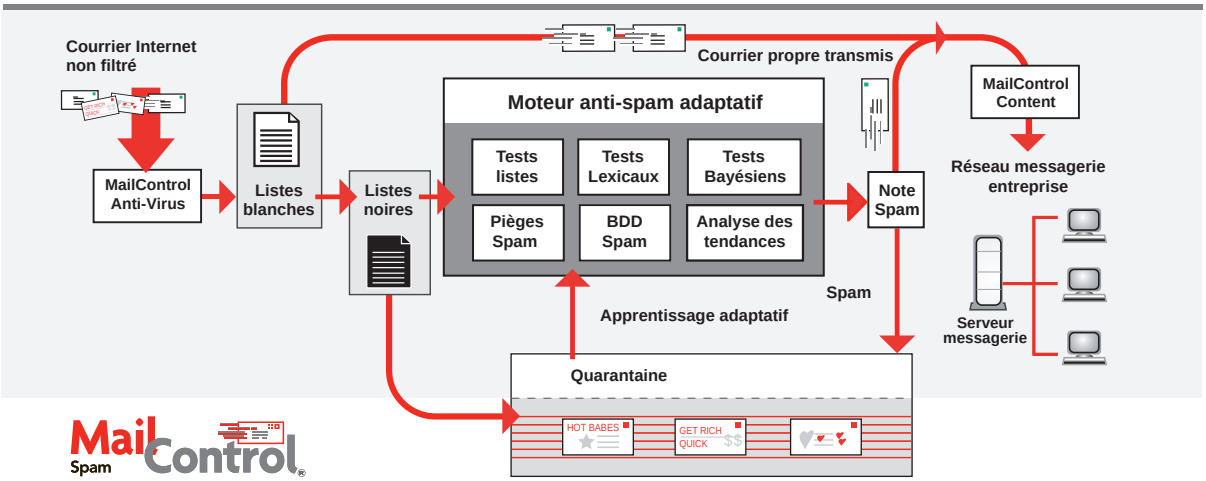
Cette note est alors comparée à un seuil de spam paramétrable ; le courrier dont la note se trouve en dessous du seuil est considéré comme normal et transmis, tandis que le courrier dont la note se situe au-dessus du seuil est mis en quarantaine en tant que spam.

Moteur anti-spam adaptatif

MailControl Spam est conçu autour du moteur anti-spam adaptatif. Ce moteur exploite une combinaison de différentes techniques pour analyser chaque message électronique et lui attribuer sa note spam, laquelle permet ensuite de déterminer la probabilité pour que ce message soit un spam. Parmi les techniques utilisées pour l'attribution de la note spam :

- **Tests Réseau** : ceux-ci comportent un certain nombre de d'analyses dont la technique du SPF (Sender Policy Framework – recherche de l'authenticité de l'émetteur) combinée à celle des RBL (Real Time Black List – Listes Noires en temps réel) afin de définir l'identité et la réputation de l'émetteur du message.
- **L'analyse lexicale** : Analyse détaillée de la totalité d'un courrier électronique, dont l'enveloppe, les en-têtes, le sujet et le corps du texte. L'analyse lexicale recherche des mots-clés et des expressions afin d'évaluer la probabilité pour le message d'être un spam.
- **Base de données partagée** : Un certain nombre de bases de données spam sont disponibles sur Internet (dont Vipul's Razor). Ces bases s'appuient sur une approche collaborative d'identification des spams. Les utilisateurs soumettent individuellement les messages spam à la base, qui associe une signature ou une clé unique à chaque message.

Processus de filtrage adaptatif de MailControl Spam



- **Filtrage bayésien** : Le concept de filtrage bayésien repose sur la création de deux bases de données ou «corpus» de courrier électronique : un corpus de courrier spam et un second de courrier valide. Chaque corpus est «marqué» puis soumis à une analyse visant à repérer les marques récurrentes dans chaque type de courrier. Un niveau de probabilité est ensuite associé à chaque marque afin de déterminer si celle-ci est plutôt susceptible d'apparaître dans le spam ou dans le courrier valide.

- **Pièges à spam** : Les pièges à spam (ou "pots de miel") sont des comptes de courrier électronique configurés pour recueillir le spam. Il suffit qu'un même message apparaisse dans un très petit nombre de pièges à spam pour que ce message soit clairement identifié comme spam, avec un très faible risque d'erreur quant à sa classification. Une fois le message identifié, une signature (ou clé) peut être créée et utilisée pour détecter et bloquer tout nouveau message similaire.

- **Analyse des tendances** : L'analyse des tendances est une technique qui peut contribuer à limiter les faux positifs et à accroître les taux de détection de spam. Cette technique efficace consiste à analyser l'historique du courrier électronique transmis par un individu donné puis à dégager les tendances, ce qui peut aider à estimer la probabilité pour qu'un courrier soit valide ou non.

- **Listes blanches & noires** : Il s'agit de listes configurables regroupant des adresses électroniques (ou des domaines) que les organisations peuvent bloquer ou accepter de façon explicite. Ces listes peuvent être établies au niveau du domaine, du groupe ou de l'utilisateur final.

Les points forts

- *Une protection accrue, des coûts opérationnels ré-duits*
- *Des taux de détection maximaux, un minimum de faux positifs*
- *Une technologie de filtrage spam adaptative et autorégulée*
- *Maintien du contrôle via un portail de gestion sûr*
- *Configuration par domaine et par utilisateur*
- *Intervention minimale du service assistance*

Les principales fonctionnalités de MailControl Spam

	Gestion
☑	Portail de gestion client en ligne
☑	Gestion en ligne du courrier en quarantaine
☑	Mise en quarantaine du courrier jusqu'à 30 jours
☑	Rapports de gestion du spam synthétisant tous les messages traités avec leurs « notes spam »
☑	Rapports sur la composition des courriers
☑	Granularisation des droits d'administration sur le portail
☑	Possibilité pour l'administrateur d'afficher tous les journaux de messages et rapports de transmission
☑	Notifications HTML ou Texte configurables pour des utilisateurs spécifiques, des groupes d'utilisateurs en entrée et en sortie
☑	Suivi en ligne des messages avec journaux SMTP détaillés via le portail
☑	Possibilité de définition d'un seuil de confiance spam par utilisateur, domaine ou groupe
	Détection du spam
☑	Analyse des listes noires en temps réel
☑	Analyse lexicale incluant les en-têtes, le sujet et le corps du message
☑	Analyse et réputation réseau associant les RBL (Real Time Black List) et SPF (Sender Policy Framework)
☑	Filtrage bayésien
☑	Bases de données spam partagées
☑	Analyse des tendances
☑	Analyse DDC (Distributed Checksum Clearinghouse)
☑	Pièges à spam («pots de miel»)
☑	Taux de détection de spam publié
☑	Listes blanches paramétrées par domaine ou par utilisateur
☑	Listes noires paramétrées par domaine ou par utilisateur
	Déploiement du spam
☑	Le spam peut être mis en quarantaine sans transmission vers les réseaux de l'entreprise
☑	Le spam peut être marqué au niveau de l'objet et transmis
☑	Le spam peut être redirigé vers une boîte aux lettres spécifique
	Autonomie de l'utilisateur final
☑	L'utilisateur final dispose de rapports récapitulant tous les messages traités avec leur «notes spam»
☑	Si autorisé, l'utilisateur peut visualiser les messages en quarantaine
☑	Si autorisé, l'utilisateur final peut accéder à une interface Web pour libérer des messages spam placés dans l'espace de mise en quarantaine
☑	Si autorisé, l'utilisateur final peut configurer ses propres listes blanches et noires pour adapter le service à ses besoins

MailControl Spam

Evaluation gratuite pendant 28 jours

pour plus d'informations ...

Appelez +33 1 60 01 59 87
Email contact@mak2.fr