

HOSTED WEB SECURITY

LE POINT DE VUE

“Le Web est devenu le vecteur de prédilection des pirates et cybercriminels pour la distribution de logiciels malveillants, le vol d'identité, la fraude financière et l'espionnage industriel.”

IDC Worldwide IT Security Software, Hardware, and Services 2009–2012 Forecast and 2007 Vendor Shares : The Big Picture

LA SINGULARITE DE MESSAGELABS

- Architecture avancée, garantissant une protection sans équivalent avec un temps de latence minimale
- Accords de niveau de service de référence : possibilité de remboursement si les niveaux de performance ne sont pas atteints.
- Console de gestion unique et partage des informations sur les menaces entre messagerie électronique, Web et messagerie instantanée pour une protection, une visibilité et un contrôle accrus
- Support global gratuit 24h/24 et 7j/7 en 10 langues délivré par les spécialistes de SaaS

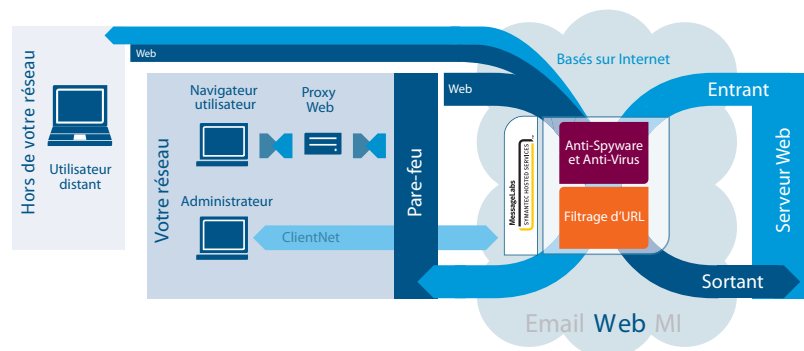
COMMENT ASSUREZ-VOUS LE CONTROLE ET LA SECURITE DU TRAFIC WEB AU SEIN DE VOTRE ENTREPRISE ?

Internet est devenu un outil essentiel pour l'entreprise et pourtant il n'a jamais été aussi dangereux de naviguer sur le Web. Pour les pirates, le Web est devenu le premier vecteur de diffusion de virus et de logiciels espions. Les Internautes qui visitent des sites infectés peuvent télécharger à leur insu un logiciel malveillant capable de voler des informations confidentielles.

Les entreprises sont également en train de réaliser qu'il faut impérativement définir et mettre en application des politiques d'utilisation acceptable du Web afin d'optimiser la productivité, de limiter les pertes de données et de réduire au maximum les risques juridiques. Les cas d'usages abusifs du Web augmentent sans cesse avec l'utilisation de plus en plus fréquente de Web 2.0 et l'engouement pour les sites de média sociaux.

MessageLabs Web Security bloque les virus, logiciels espions et menaces de phishing véhiculés par le Web et contrôle le trafic Web via le filtrage des URL, tout en assurant la mise en application de politiques d'utilisation acceptable du Web. Agissant au niveau d'Internet, MessageLabs Web Security bloque les menaces avant qu'elles n'aient pu atteindre votre réseau et utilise le filtrage des URL pour limiter les accès Web en fonction de la catégorie, de l'utilisateur, de l'heure de la journée, de l'URL ou du type de fichier. La prise en charge des utilisateurs itinérants permet d'étendre la protection et la mise en application des politiques aux employés qui se connectent à Internet à partir d'un point d'accès à l'extérieur du réseau de l'entreprise.

WEB SECURITY AND CONTROL – LA SOLUTION MESSAGELABS



MessageLabs Web Security fonctionne avec un temps de latence minimum à travers notre réseau global de datacenters à équilibrage de charge hautement disponibles, ce qui permet de bénéficier d'une protection rapide, efficace et permanente, sans aucun impact sur la productivité de vos utilisateurs. Notre solution est facile à déployer, facile à gérer. Elle s'appuie sur l'accord de niveau de service le plus exigeant de l'industrie, et s'accompagne d'un support globale gratuit dispensé 24h/24 et 7j/7 en 10 langues par les spécialistes de SaaS.

FONCTIONNEMENT DU SERVICE

- Les demandes de trafic Web sont acheminées via MessageLabs et vérifiées par rapport à vos politiques d'usage acceptables.
- Si aucune règle de politique n'est déclenchée, la demande passe.
- Si une règle de politique est déclenchée, la demande est enregistrée ou autorisée à passer ou l'accès à la page Web est refusé.
- Les demandes de page Web sont extraites par MessageLabs avant diffusion sur votre réseau et sont analysées pour rechercher des menaces Web connues et émergentes.
- Les menaces nouvelles et convergentes de type logiciel malveillant sont identifiées par Skeptic™, tandis que les menaces connues sont identifiées par plusieurs moteurs de signature de logiciels malveillants.
- Quand une menace est identifiée, l'accès à la page demandée est refusé.
- Si aucune menace n'est identifiée, la page est remise à l'utilisateur sans délai perceptible.

ACCORD DE NIVEAU DE SERVICE

MessageLabs Web Security s'appuie sur les niveaux de performance d'accord de niveau de service suivants :

- Protection Web Anti-Virus - Protection à 100 % contre les virus connus
- Temps de latence - Temps moyen d'analyse du contenu Web sous 100 millisecondes
- Disponibilité du service - Temps de fonctionnement à 100 %
- Support technique - Temps de réponse pour les appels critiques, majeurs et mineurs

ETAPES SUIVANTES

Contactez un spécialiste produit :
 France: +33 (0)6 8089 8886
 Belgique: +32 (0) 2 531 11 40
 info@messagelabs.com

Pour connaître les coordonnées des bureaux dans un pays spécifique, consultez la page :
www.messagelabs.be/contact



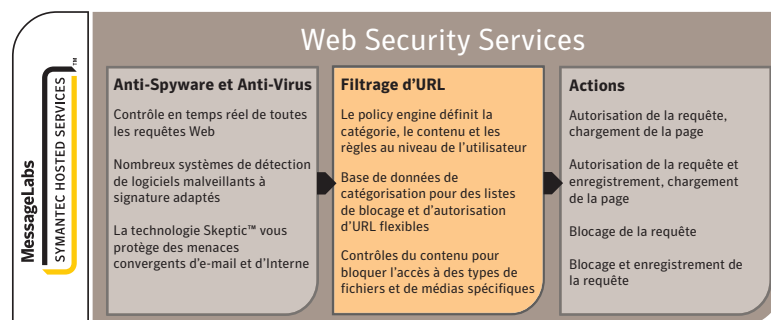
Confidence in a connected world.

MessageLabs Web Security est constitué de deux composants principaux :

Sécurité multicouches – Plusieurs moteurs d'antivirus et d'antispyware du commerce recherchent des logiciels malveillants dans le contenu Web. Ces moteurs sont continuellement mis à jour par MessageLabs, pour une détection précise des menaces connues. En outre, la technologie heuristique Skeptic™ propriétaire de MessageLabs vous protège contre les menaces nouvelles et convergentes, capables de cibler les utilisateurs Web via d'autres protocoles tels que ceux du courrier électronique et de la messagerie instantanée.

Filtrage des URL - Toutes les demandes Web sont vérifiées par rapport à un moteur de politiques sophistiqué et une base de données de catégorisation d'URL afin de s'assurer que le contenu approprié reste accessible tandis que le contenu restreint est soigneusement contrôlé. Hautement flexible et intuitif, le moteur de politique permet aux entreprises de créer des politiques et de surveiller le comportement pour des utilisateurs et groupes spécifiques.

MessageLabs offre une console de gestion unique et intégrée pour le courrier électronique, le Web et la messagerie instantanée, ce qui simplifie l'administration et abaisse le coût total de possession tout en procurant une visibilité accrue du comportement de l'utilisateur. L'information sur les menaces est partagée entre les protocoles de communication pour une protection accrue.



FONCTIONNALITÉS	AVANTAGES
Défenses antivirus et antispyware multicouches fonctionnant au niveau d'Internet	Blocage des virus et des logiciels espions avant qu'ils n'atteignent votre réseau
Fonction heuristique Skeptic™ propriétaire avec toute la puissance du grid computing	Protection contre des menaces nouvelles et convergentes visant le courrier électronique, le Web et la messagerie instantanée
Architecture globale distribuée assurant un temps de latence minimal	Navigation sécurisée sans retard perceptible
Moteur de génération de politiques de filtrage d'URL hautement configurable	Permet aux entreprises d'empêcher l'usage abusif du Web en restreignant l'accès à des sites et contenus indésirables.
Support pour les utilisateurs itinérants	Extension de l'application de la protection et des politiques aux employés se trouvant à l'extérieur du réseau de l'entreprise
Filtrage du cache du moteur de recherche	Identification de l'origine du contenu mis en cache et application des politiques de contrôle appropriées
Tableau de bord, récapitulatif, rapports détaillés et planifiés	Visibilité, responsabilité et garantie d'un service irréprochable
Console de gestion unique pour la sécurité du courrier électronique, du Web et de la messagerie instantanée	Simplification de l'administration avec protection, contrôle et visibilité accrues