

Principe intelligent

- MailInBlack vérifie l'identité des expéditeurs et délivre instantanément au destinataire les emails en provenance de ses correspondants connus. Tout email malveillant (spyware, virus...) est stoppé, quel que soit l'expéditeur, connu ou inconnu.
- Si un utilisateur protégé reçoit un emailing publicitaire ou un message provenant d'un nouveau contact, MailInBlack renvoie une invitation en son nom, proposant à l'expéditeur d'intégrer sa liste de correspondants connus. Aucune invitation n'est envoyée lorsque l'adresse d'expédition est usurpée.
- Simple et rapide, l'acceptation de cette invitation ne se fait qu'une seule fois. L'expéditeur prouve ainsi qu'il est légitime. Son email est délivré et son adresse est ajoutée à la liste des correspondants connus de l'utilisateur protégé.

- Les spammeurs n'acceptent pas les invitations : tous les spams sont stoppés. Ce principe est imparable et s'adapte à toutes les situations : newsletters, réponses automatiques, double utilisateurs protégés...

Bénéfices uniques

- garantie de recevoir tous ses emails : aucun email valide bloqué par erreur (faux-positif)
- gage de protection absolue : 100% des spams sont stoppés
- élimination de tout travail d'administration lié au spam et de support aux utilisateurs
- pérennité de la technologie face aux futures techniques de spamming
- antivirus de mail inclus (entrant et sortant)
- meilleure solution antispam du marché : études comparatives publiées dans L'Express (n°2866) et Micro Hebdo (n°424)

Nouveautés V4

Exclusivités
V4 !

Fonctionnalités

Allègement du rapport des emails stoppés !

- ↳ Facilité de lecture et d'utilisation

Gestion granulaire par groupe d'utilisateurs

- ↳ Partage de la white-list pour tous les membres du groupe (Q12010)!
- ↳ Possibilités accrues et facilité d'administration

Mobilité

- ↳ Adaptation smartphones et PDA
- ↳ Partenariat technologique exclusif avec BlackBerry France

Reconnaissance des invitations entre deux utilisateurs MailInBlack !

Statistiques par utilisateur

- ↳ Top 10 des expéditeurs, destinataires, spammeurs, virus, sujets...

Administration

- ↳ Mesure anti-spoofing d'un domaine par déclaration de sa plage d'adresses IP
- ↳ Stratégie de gestion des pièces jointes (Q42009)



Moteur et architecture

Scalabilité dispo V4.2

- ↳ Protection de 5 à 500 000 utilisateurs !

Sécurité

- ↳ Noyau *hardened*

Nouveaux outils tiers embarqués

Efficacité et sécurité

Contrôle de l'envoi des invitations :

- . Mesures anti DOS (*deny of service*)
- . DKIM (*Domain Keys Identified Mail*) V4.1
- . BATV (*Bounced Address Tag Validation*)
- . SPF (*Sender Policy Framework*) V4.1
- . RBL (*Realtime Blackhole List*)

La solution antispam MailInBlack-ASP

MailInBlack-Asp est une solution antispam professionnelle. Cette solution est offerte en mode ASP : par un changement de Mx, les emails sont dirigés vers l'une des Mibox administrées par la société MailInBlack. Les emails provenant d'expéditeurs autorisés sont poussés vers le serveur de messagerie de l'organisme (ou de son hébergeur de boîtes aux lettres). En mode ASP, l'organisme est libéré du travail d'administration relatif aux paramètres généraux. Ce travail, ainsi que la maintenance et la supervision sont réalisés par le service technique de MailInBlack.

Fonctionnalités spécifiques MailInBlack-ASP

- Mibox ASP mutualisée ou dédiée
- Synchronisation avec un ou plusieurs annuaires d'entreprise (Ldap ou AD) pour tenir à jour les utilisateurs protégés possible en ASP dédié
- Personnalisation de l'invitation et du test de Turing (logo)
- Traitement des spams externalisés, en amont du réseau du client
- Conservation des emails en cas d'indisponibilité du serveur de messagerie pendant 4 jours
- Réduction du besoin en bande passante
- Monitoring et redondance assurés par MailInBlack
- Filtrage antispam assuré sur Mx secondaire
- Continuité de service : redirection de tous les emails (sauf virus) vers le client en cas d'incident majeur
- Délai de garde des emails stoppés : 30 jours
- Interface d'administration des comptes protégés (modification, pré-autorisation, personnalisation...)
- Sauvegarde assurée par MailInBlack tous les jours
- Protection multi-domaines
- 50% minimum requis de licences
- Interface d'administration de l'appliance et des comptes protégés (modification, pré-autorisation, personnalisation...) en https



Fonctionnalités communes

- Gestion des emails automatiques (newsletters...)
- Gestion personnalisée des correspondants pour chaque utilisateur
- Gestion possible par groupe d'utilisateurs
 - Partage de la white-list par groupe utilisateurs V4.1
 - Gestion de privilèges par groupe d'utilisateurs
- Système anti-usurpation : BATV, RBL, (DKIM ; SPF) V4.1
- Jusqu'à 3 récapitulatifs interactifs et individuels des emails stoppés (Digest) par mail à heures souhaitées : aucun message perdu
- Blocage des spams pour des destinataires inconnus
- Convergence mobile : adapté smartphones / PDA
- Espace utilisateur privatif (accès en temps réel aux mails stoppés, pré-autorisation...)
- Limitation du nombre d'invitations envoyées :
 - protection des adresses tierces usurpées
 - limitations vers un même expéditeur
 - protection anti-DOS
- Personnalisation de l'invitation et des interfaces
- 6 alias ou groupes de diffusion par licence
- Pré-autorisation possible de contacts connus (par adresse email, domaine ou liste de diffusion)
- Usage multilingue français ou anglais)
- Reconnaissance des invitations entre 2 utilisateurs
- Confidentialité de l'email de l'utilisateur
- Statistiques utilisateur et administrateur

Datacenter

Les Mibox MailInBlack sont domiciliés au DataCentre Neuf/SFR de Marseille, l'un des datacenters les plus modernes d'Europe. Cet hébergement, associé à l'architecture sécurisée des Mibox, garantit une disponibilité maximale :

- **Connectivité** : réseau IP: transit IP dédié en BGP-4 via de la bande passante fournie par plusieurs opérateurs permettant d'éviter totalement les suspensions de service internet ; niveau de bande passante librement évolutif en cas de montées en charge ; équipements réseaux en redondance
- **Applicatif** : supervision SNMP ; sauvegarde des données journalière ; supervision et alerte externes Redondance machines avec bascule en service dégradé en cas d'incident bloquant
- **Matériel** : hardware IBM ; supervision IBM director (certifications MailInBlack « IBM Optimized Partner »); double processeur ; redondance des disques en Raid 1 ; double alimentation
- **Energie et climatisation** : redondance électricité et climatisation
- **Sécurité incendie** : détection précoce et extinction automatique au gaz Argonite
- **Sécurité physique** : surveillance vidéo ; gardiennage 24h/24 ; anti-intrusion ; habilitation règlementée par badge

Architecture

Après redirection du Mx, MailInBlack traite tous les emails à destination du domaine puis pousse uniquement les messages validés vers le serveur de messagerie, situé chez le client ou chez son hébergeur.

Un serveur dédié reçoit le flux de messagerie sur le Mx secondaire pour lutter contre ce spam particulier et offrir une continuité de service email permanente.

