

# bitdefender® SECURITY FOR MAIL SERVERS

## DES BOÎTES AUX LETTRES SÉCURISÉES ET SANS SPAM : UNE NÉCESSITÉ

Le courrier électronique est devenu un service indispensable que les entreprises doivent protéger – quel qu'en soit le prix. Quand le serveur de messagerie cesse de fonctionner, ce sont vos employés qui cessent de travailler. Les conséquences d'une perte de productivité associée à une attaque virale propagée par e-mail peuvent pratiquement paralyser une entreprise. Beaucoup d'entreprises réfléchissent à l'impact potentiel que peuvent avoir les virus transportés par e-mail, mais il est encore plus important de penser à la mauvaise réputation et aux préjudices que peuvent causer l'envoi accidentel par un employé d'un e-mail infecté à des partenaires extérieurs ou des clients. Plus que tout autre dégât, la mauvaise image véhiculée par une entreprise, peut se révéler irréversible.

Le système de messagerie d'une entreprise constitue sur un réseau, le principal point d'entrée et de sortie pour la propagation de codes malveillants et la fuite de données. Les solutions de sécurité pour la messagerie doivent donc pouvoir protéger le système de messagerie de l'entreprise contre un grand nombre de menaces différentes, parmi lesquelles :

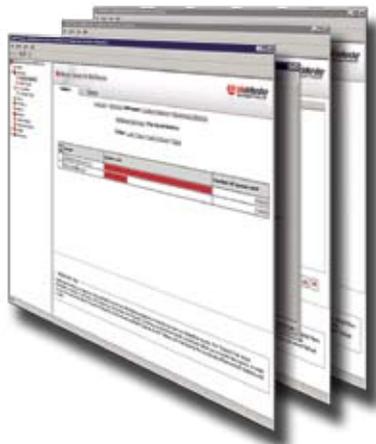
- L'envoi ou la réception de codes malveillants contenus dans des pièces jointes
- Le courrier non sollicité sous la forme de spam
- Les tentatives de phishing pour récupérer des informations confidentielles
- La divulgation d'informations confidentielles par e-mail
- Les attaques de type DHA (Directory Harvesting Attacks)

Les méthodes de diffusion des menaces par e-mail sont devenues de plus en plus virulentes, les bloquer au niveau du poste de travail peut se révéler trop tardif. Dans ces conditions, une solution déployée aux limites du réseau et sur le serveur de messagerie lui-même peut limiter l'impact des malwares, en nettoyant les documents infectés et en protégeant le bien le plus précieux de votre entreprise – sa capacité à communiquer.

## SÉCURISATION DES SERVICES DE MESSAGERIE AVEC BITDEFENDER

BitDefender Security for Mail Servers protège les serveurs de messagerie de type Windows ou UNIX contre les menaces connues ou inconnues, grâce à des technologies primées de détection proactive antivirus, antispyware, antispam, antiphishing, et de filtrage des contenus et des pièces jointes.

Cette solution sécurise les services de messagerie de l'entreprise et assure une productivité accrue grâce au blocage des spams et à ses outils d'administration centralisée. BitDefender Security for Mail Servers analyse les courriers électroniques à de multiples niveaux en vérifiant d'abord que le serveur de l'expéditeur du courrier n'est ni suspect ni bloqué, puis que ni le contenu du courrier ni ses pièces jointes ne contiennent de codes malveillants ou ne correspondent à une règle du filtre antispam.



## PRINCIPALES FONCTIONNALITÉS ET AVANTAGES-CLÉS

- Analyse du trafic e-mails entrants pour assurer une protection antimalware en temps réel et minimiser le risque de propagation sur le réseau interne.
- Analyse des e-mails sortants pour empêcher la propagation des menaces de sécurité chez vos partenaires et clients.
- Analyse chaque e-mail une seule fois, en utilisant la méthode d'analyse sélectionnée pour minimiser la charge du serveur.
- Analyse du contenu des e-mails entrants et sortants afin de détecter des mots clés spécifiques définis par l'administrateur, par exemple des numéros de cartes bancaires.
- Filtres antispam et antiphishing de haute précision, utilisant la technologie heuristique NeuNet.
- Protection du répertoire des utilisateurs contre les attaques de type DHA utilisées par les spameurs pour récupérer des adresses e-mail valides, en utilisant des techniques de force brute.
- Permet la configuration à distance depuis n'importe quel ordinateur du réseau de l'entreprise à travers la console d'administration, centralisée BitDefender.
- Réduction des frais de gestion et des frais généraux permettant d'améliorer globalement la productivité de l'entreprise.
- Limitation du temps d'arrêt du réseau pour améliorer l'efficacité opérationnelle.

## LES TECHNOLOGIES BITDEFENDER

**b-have** Toutes les solutions BitDefender incorporent B-HAVE, qui analyse le comportement des codes potentiellement malveillants au sein d'un ordinateur virtuel, élimine les faux positifs et augmente de manière significative le taux de détection des malwares inconnus.

**NeuNet** Pour mieux traiter le nouveau spam, Les Laboratoires BitDefender ont créé NeuNet, un puissant filtre antispam. Les Laboratoires Antispam assurent l'entraînement préalable de NeuNet au moyen de divers messages de spam, afin qu'il puisse reconnaître le spam en percevant les ressemblances avec les messages déjà examinés.

## CONFIGURATION NÉCESSAIRE

### Systèmes d'exploitation de type Windows :

- Windows Server 2000 SP4 + Update Rollup 1
- Windows Server 2003 avec SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2, Windows Small Business Server (SBS) 2008
- Windows Exchange Server 2000+SP3, 2003, 2007
- Internet Explorer version 6.0 ou supérieure

### Systèmes d'exploitation de type UNIX :

Système d'exploitation : Linux, FreeBSD, Solaris Linux Kernel 2.6.18 ou plus récent, glibc 2.3.1 ou plus récent, libstdc++ de gcc 4 ou plus récent Samba version 3.0 ou plus récent

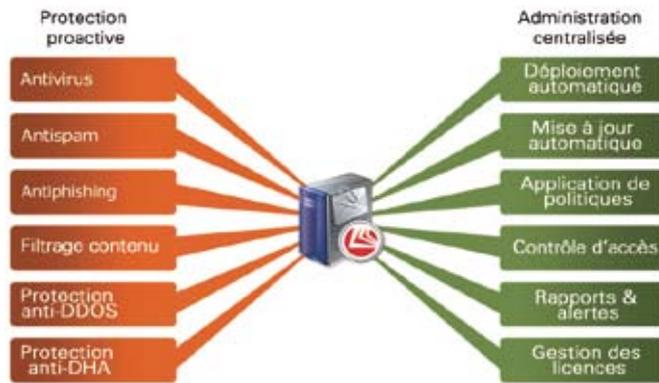
### Compatible avec les distributions :

- Debian GNU/Linux 3.1 ou plus récent
- Fedora Core 1 ou plus récent
- FreeBSD: 5 (ou plus récent avec compat5x)
- Novell SuSE Linux Enterprise Server 9, Linux 8.2 ou plus récent
- Mandrake/Mandriva 9.1 ou plus récent
- OpenSolaris 2008 ou 2009 (plateforme x86)
- RedHat Enterprise Linux 3, Linux 9 ou plus récent
- Solaris 9 or 10 (plateforme x86)
- Slackware 9.x ou plus récent



Toutes les marques, noms commerciaux et produits cités dans ce document sont la propriété exclusive de leurs détenteurs respectifs. Tous droits réservés.

© 2010 BitDefender.



BitDefender Security for Mail Servers fournit une protection proactive et permet l'administration centralisée des services de messagerie

## DÉTECTION ET PROTECTION PROACTIVE AVANCÉE

Les moteurs d'analyse primés de BitDefender ont été récompensés par les principaux organismes de certification – y compris ICSA Labs, Virus Bulletin et West Coast Labs – pour leur protection proactive antimalware inégalée. BitDefender offre de multiples niveaux de protection avancée.

**Antivirus & Antispyware** - Outre la détection basée sur la signature, BitDefender offre une détection heuristique qui émule un ordinateur virtuel dans l'ordinateur, afin de vérifier tous les fichiers et les codes pour déceler les comportements malveillants. Cette technique produit moins de faux positifs et des taux de détection nettement plus élevés des menaces inconnues ou de type "Zero-day".

**Antispam & Antiphishing** - En utilisant de façon permanente les mises à jour des listes noires et blanches des sites de spam connus, le moteur d'apprentissage bayésien fournit un niveau de détection supplémentaire, qui s'adapte aux modifications imaginées par les spammeurs pour contourner les filtres antispam statiques.

**Filtrage du contenu** - Le filtrage de contenu permet la détection d'informations prédéfinies, telles que les numéros de carte ou de compte bancaire, noms de rapports, bases de données clients, etc. et d'empêcher qu'elles échappent au contrôle de la société.

**Protection anti-DHA** - La DHA (Directory Harvesting Attack) est utilisée par les spammeurs pour trouver des adresses valides ou existantes. Cette technique est d'autant plus efficace pour récupérer les e-mails d'entreprises que les adresses qu'elle se conforme à certaines normes. Des e-mails peuvent ainsi être spécialement conçus pour contourner les filtres antispam et arriver dans la boîte aux lettres des utilisateurs ciblés.

**Liste blanche/Liste noire** - Elles permettent d'exclure ou d'autoriser des serveurs de messagerie en ayant la possibilité de valider la correspondance de leur adresse IP en fonction du nom de domaine de l'expéditeur.

## DE MULTIPLES MÉTHODES CONFIGURABLES D'ANALYSE

BitDefender Security for Mail Servers offre des méthodes d'analyse : complète, en continu, à la demande, au niveau de la couche "transport", pour détecter les codes malveillants et protéger l'intégrité des services de messagerie électronique. Chaque e-mail est analysé une seule fois suivant la méthode sélectionnée, et un pied de page entièrement configurable peut être intégré à tout courrier analysé. Des méthodes supplémentaires d'analyse peuvent être configurées pour éviter que des informations confidentielles puissent être divulguées par certains groupes d'utilisateurs.



## INTÉGRATION À LA PLATEFORME D'ADMINISTRATION CENTRALISÉE

BitDefender Security for Mail Servers s'intègre à la console d'administration de BitDefender Management Server, ce qui donne aux administrateurs la visibilité de l'ensemble de leurs ressources réseau et de la sécurité globale.