Bitdefender®
Security for Mail Servers

DES BOÎTES AUX LETTRES SECURISÉES 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 peut pratiquement paralyser une entreprise. Beaucoup de sociétés réfléchissent à l'impact en interne que peuvent avoir les virus véhiculés par e-mail, mais il est encore plus important de penser à la perte de réputation et aux préjudices que peut causer l'envoi accidentel par un employé d'un e-mail infecté à des partenaires extérieurs ou des clients.

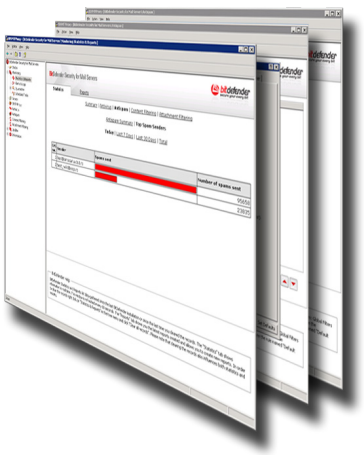
Le système de messagerie d'une entreprise constitue sur un réseau le principal point d'entrée et de sortie pour la propagation de codes malveillants et la fuite de données. Les solutions de sécurité doivent donc pouvoir protéger le système de messagerie de l'entreprise contre un grand nombre de menaces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

- L'envoi ou la réception de codes malveillants contenus dans des documents joints
- Courrier non sollicité sous la forme de spam
- Tentatives de hameçonnage pour récupérer des informations confidentielles
- Utilisateurs légitimes divulguant des informations confidentielles par e-mail
- Les attaques de type DHA (Dictionary 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.

SÉCURISATION DES SERVICES DE MESSAGERIE AVEC BITDEFENDER

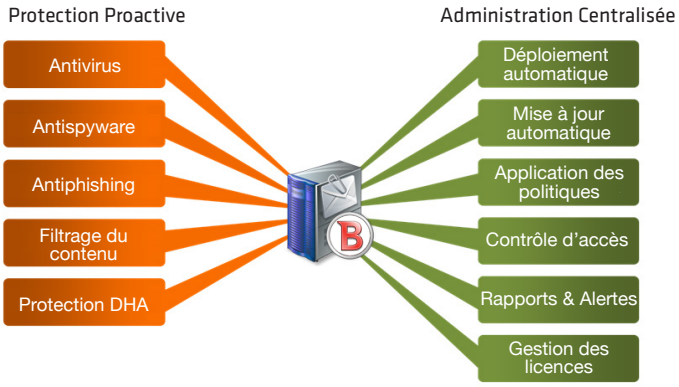
Bitdefender Security for Mail Servers protège les serveurs de messagerie fonctionnant sous Windows ou UNIX contre les menaces de sécurité connues et inconnues grâce à ses technologies proactives antivirus, antispyware, antispam, antiphishing, de filtrage des pièces jointes et du contenu. Cette solution assure la sécurité des services de messagerie des organisations et permet une meilleure productivité en bloquant le spam et en fournissant des 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, ensuite que ni le contenu du courrier ni ses pièces jointes ne contiennent de codes malveillants ou ne possèdent des propriétés caractéristiques du spam.

AVANTAGES CLÉS

- Analyse le trafic d'e-mails entrants pour assurer une protection antimalware en temps réel et minimiser le risque de propagation sur le réseau interne
- Analyse les e-mails sortants pour empêcher les menaces à la sécurité de se propager chez vos partenaires et clients
- Analyse chaque e-mail une seule fois en utilisant la méthode d'analyse sélectionnée pour minimiser la charge sur le 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 haute précision antispam et antiphishing utilisant la technologie heuristique NeuNet
- Protection du répertoire des utilisateurs contre les attaques DHA des spammeurs qui tentent de récupérer des adresses e-mail valides en utilisant des techniques de force brute
- Permet, à distance, la configuration, l'audit, l'installation et la suppression des applications et des paramètres de toute station ou serveur administré(e) sur le réseau
- Réduction des frais de personnels et des frais généraux pour améliorer globalement la productivité de l'entreprise
- Limitation du temps d'arrêt du réseau pour améliorer l'efficacité opérationnelle



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

DÉTECTION ET PRÉVENTION PROACTIVE AVANCÉE

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

Antivirus - Outre la détection basée sur la signature, Bitdefender offre une détection heuristique qui émule un ordinateur-dans-l'ordinateur virtuel qui contrôle 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 - 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.

Antispyware - Bitdefender détecte les spywares et adwares connus empêchant ainsi les fuites de données.

Antiphishing - Bien qu'ils soient considérés comme une menace visant plutôt les particuliers que les entreprises, les sites de phishing peuvent recueillir des informations auprès des employés de votre entreprise. Grâce à l'utilisation de listes noires constamment mises à jour et de règles configurables d'inspection des contenus, Bitdefender bloque les messages incitant les utilisateurs à se connecter à des sites de phishing.

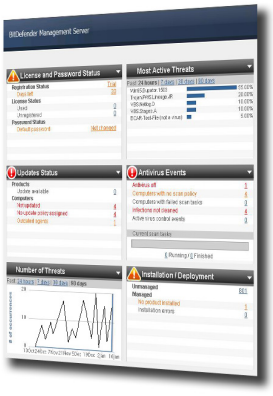
Filtrage de contenu - Le filtrage de contenu permet la détection d'informations prédéfinies, telles que les numéros de carte ou de compte bancaire, noms de rapports, bases de données clients, etc. et d'empêcher qu'elles échappent au contrôle de l'entreprise.

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 leurs adresses suivent 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.

OPTIONS D'ANALYSE FIABLES ET CONFIGURABLES

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.



TECHNOLOGIES BITDEFENDER

b-have Toutes les solutions Bitdefender intègrent 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 les nouveaux spams, 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.

DÉFENSE EN PROFONDEUR

Bitdefender Security for Mail Servers n'est qu'un des éléments d'un ensemble complet de solutions assurant la protection globale du réseau, depuis la passerelle jusqu'à la station de travail. Les produits proactifs et multi-plateformes de Bitdefender détectent et bloquent les menaces que les virus, les spywares, les adwares et les chevaux de Troie peuvent faire peser sur l'intégrité de votre réseau.

CONFIGURATION REQUISE

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 Server 2012
- Internet Explorer version 6.0 ou supérieure

Systèmes d'exploitation de type UNIX :
- Linux, FreeBSD, Solaris
- Linux Kernel : 2.6.18 ou plus récent
- glibc: version 2.3.1 ou plus récent, et libstdc++ gcc4 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)
- Mandrake/Mandriva 9.1 ou plus récent
- Novell SuSE Linux Enterprise Server 9, Linux 8.2 ou plus récent
- OpenSolaris 2008 ou 2009 (plateforme x86)
- Oracle Linux 5 ou plus récent
- RedHat Enterprise Linux 3, Linux 9 ou plus récent
- Slackware 9.x ou plus récent
- Solaris 9 ou 10 (plateforme x86)

vb 100 VIRUS virusbtn.com
vb VERIFIED SPAM + virusbtn.com

ÉDITIONS PROFIL

Plus de **500 millions d'utilisateurs** sont protégés par **les technologies Bitdefender.**

Bitdefender

Bitdefender est édité en France et dans les pays francophones par la société EDITIONS PROFIL S.A., spécialiste de la sécurité des systèmes d'information et du filtrage de contenus numériques.