BITDEFENDER CLIENT SECURITY

LES BASES DE LA SÉCURITE DE L'ENTREPRISE

Pour toutes les entreprises, qu'elles soient anciennes ou récentes, les exigences de sécurité sont les mêmes – quelle que soit leur taille. En protégeant la propriété intellectuelle de votre entreprise et en sécurisant les données de vos clients, vous adoptez de bonnes pratiques, car les conséquences de l'arrivée de n'importe quel virus peuvent affecter l'efficacité opérationnelle de l'entreprise et entraîner une perte de productivité du personnel. Cette perte de productivité peut paralyser une petite entreprise et au minimum, entraver sa croissance.

L'ANTIVIRUS NE SUFFIT PLUS

Les menaces sont en constante évolution pour déjouer les solutions de sécurité mises en place et peuvent se propager rapidement. Même si l'antivirus reste la base d'une bonne politique de sécurité, il n'est plus suffisant pour protéger vos employés des malveillances. Parmi les menaces susceptibles de perturber gravement l'activité de l'entreprise, on peut citer :

Virus : Ils se transmettent en infectant des fichiers exécutables, en se dissimulant dans des archives compressées, ou sous la forme de macros dans des documents légitimes. Leur nuisance peut aller jusqu'à la suppression de fichiers, le cryptage de données, l'effacement du disque dur, etc.

Adware/Spyware : Presque aussi perturbant et dangereux que les virus, le spyware peut se révéler difficile à identifier et à supprimer. La perte de données personnelles et professionnelles constitue un risque majeur, auquel s'ajoute celui d'une dégradation de la performance des stations de travail, de l'installation inopinée de logiciels, et de la réorientation des navigateurs. La grave infection d'un système peut nécessiter sa réinstallation complète, assortie de la perte de temps et d'argent qu'elle implique.

Vers : Ces programmes capables de s'auto-reproduire utilisent les réseaux pour se propager, ralentir leur fonctionnement et contaminer les systèmes en exploitant leurs vulnérabilités. Ils peuvent aller jusqu'à supprimer ou crypter des fichiers, expédier des documents par e-mails, installer des portes dérobées (backdoors), des zombies et des chevaux de Troie.

Chevaux de Troie et **rootkits** apparemment légitimes, ces programmes sont conçus pour permettre un accès distant à un ordinateur. La détection et la prévention manuelles de ce type de menaces prennent beaucoup de temps et peuvent nécessiter la réinstallation complète du système, si ces opérations ne sont pas effectuées correctement

Spam et phishing : les messages publicitaires non sollicités diffusés par courrier électronique constituent plus qu'un simple désagrément. Ils sont à l'origine de considérables pertes de temps s'ils ne sont pas correctement gérés. Certaines attaques de type spam ou hameçonnage peuvent également véhiculer du malware en pièces jointes (des parenthèses ce qui expose à des risques internes si elles sont ouvertes) des parenthèses ou des liens vers des sites web sollicitant des informations privées. Le hameçonnage utilise le même genre de techniques mais dirige l'utilisateur vers des sites apparemment légitimes pour lui soutirer des informations personnelles, par exemple le numéro de sa carte ou de son compte bancaire, ou dépose des enregistreurs de frappe (keyloggers) susceptibles de recueillir sur la société des informations sensibles.

Les conséquences d'une invasion de malwares peuvent sérieusement perturber l'activité générale d'une entreprise, mais les services informatiques sont ceux qui en souffrent le plus. Les administrateurs qui ont été confrontés à la nécessité de supprimer un vers ou un virus se propageant rapidement en infectant un grand nombre de systèmes peuvent témoigner qu'ils agit d'un travail très compliqué. Malheureusement, cette tâche est prioritaire pour limiter la perte de données et rétablir l'activité normale de l'entreprise le plus rapidement possible.

PRINCIPALES FONCTIONNALITÉS ET AVANTAGES-CLÉS

- Détection primée des virus, nettoyage et mise en quarantaine
- Souplesse d'utilisation, permettant de planifier des analyses ou d'en déclencher d'immédiates pour s'assurer de l'absence d'infection.
- Analyse et marque les fichiers « en lecture seule » une seule fois au cours de la même session et n'effectue qu'une nouvelle analyse en cas de nouvelle session, de mise à jour ou d'infection du système.
- Mise en quarantaine des fichiers infectés ou suspects, minimisant le risque de propagation
- Configuration et administration utilisant des politiques
- Protection pare-feu personnelle pour les utilisateurs à distance ou itinérants
- Analyse des périphériques amovibles et politiques de contrôle d'accès
- Protection antispam au niveau du système avec mise à jour permanente des listes blanches / listes noires et un moteur d'apprentissage bayésien pour identifier le nouveau spam qui contourne les filtres traditionnels
- Filtrage personnalisé du contenu pour identifier les informations sensibles et minimiser les fuites de données
- Imposer la sécurité grâce aux profils limitant l'accès à l'interface et aux désinstallations protégées par mot de passe
- Réduction des frais de gestion liés à l'administration de nombreux postes clients grâce à une console d'administration centralisée
- 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

bitdefender

TECHNOLOGIES BITDEFENDER

BitDefender AVC BitDefender Active Virus Control est une technologie de détection proactive innovante qui utilise des méthodes heuristiques de pointe pour détecter de nouvelles menaces potentielles en temps réel. Elle surveille de façon continue chaque programme en cours d'exécution sur le PC, et donne des notes à toutes les actions ressemblant à des actions malveillantes. Chacune de ces actions obtient un score, et lorsqu'un certain pallier est franchi, le processus est bloqué car considéré comme malveillant.

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.

CONFIGURATION REQUISE

La solution BitDefender Client Security est livrée avec une administration centralisée côté serveur et des composants de protection des postes de travail côté client. Deux composants concernent l'aspect client : BitDefender Business Client pour le contrôle des postes de travail Windows, et BitDefender Agent pour permettre la centralisation de l'administration. Les composants clients se déploient en utilisant la plateforme d'administration centralisée de BitDefender.

BitDefender Business Client et Management Agent

Processeur compatible Intel Pentium :

- 500 MHz pour Windows 2000
- 800 MHz pour Windows XP
- 1 GHz pour Windows Vista, Windows 7

Mémoire RAM :

- 512 Mo pour Windows 2000, Windows XP
- 1 Go (100 Mo pour Management Agent)

Espace disque minimum disponible :

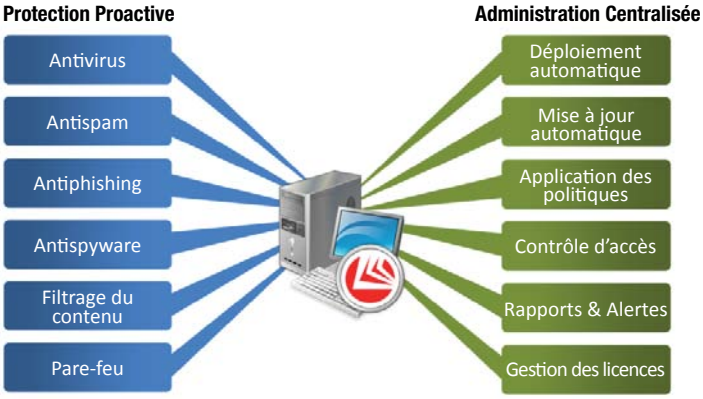
- 1 GB (100 MB for Management Agent)

Système d'exploitation :

- **Business Client and Management Agent** for Windows 7, Windows Vista SP1, Windows XP (SP2), Windows Home Server, Windows 2000 Professional (SP4 Rollup 1 v2)
- **Management Agent** Windows 2008 / 2008 SBS / 2008 R2, Windows Server 2003 (SP2), Windows 2000 Server (SP4 Rollup 1 v2), Mac OS X 10.4.6 ou plus récent, Linux 2.4.x or 2.6.x with glibc 2.3.1 ou plus récent et libstdc++5 from gcc 3.2.2 ou plus récent

vb 100 VIRUS virusbtn.com

Compatible with Windows 7



BitDefender Client Security fournit de multiples niveaux de protection et de fonctionnalités d'administration des clients

DÉTECTION PROACTIVE AVANCÉE

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

BitDefender Client Security offre de multiples niveaux de protection avancée : antivirus, antispam, antispyware, antiphishing, filtrage de contenu, détection des chevaux de Troie/Rootkits et un pare-feu personnel complet. Toutes les fonctions sont configurables à distance, y compris les politiques de sécurité avancées pour contrôler l'accès des utilisateurs aux périphériques amovibles et aux applications locales, et à Internet pendant certaines plages horaires.

CONFIGURATION ET ADMINISTRATION GRANULAIRE DES ANALYSES

BitDefender Client Security fournit différentes méthodes d'analyse pour détecter les codes malveillants et sauvegarder l'intégrité des ordinateurs portables et des stations de travail déployés sur votre réseau. Différentes options d'analyse contribuent au maintien de l'intégrité du système sans déranger les utilisateurs.

A l'accès moteur d'analyse en temps réel, détectant les virus au moment même où un utilisateur accède à un document ou l'ajoute à une bibliothèque ou une liste.

Les fonctionnalités d'analyse à la demande permettent d'effectuer des analyses du système planifiées en dehors des heures de travail, sans affecter les performances globales ni la disponibilité du système.

Configuration des analyses planifiées permet de configurer la planification des analyses à la demande et des tâches de mise à jour, en limitant leur impact éventuel sur le serveur et le système au cours des heures de pointe d'activité.

Mise en quarantaine des fichiers infectés ou suspects les fichiers suspects sont isolés dans des zones de quarantaine. Ils peuvent être au choix : nettoyés ou conservés en quarantaine pour être analysés, restaurés vers leur emplacement d'origine une fois validés, ou envoyés directement aux Laboratoires antivirus de BitDefender pour évaluation.

INTÉGRATION À LA PLATEFORME D'ADMINISTRATION CENTRALISÉE

Un grand nombre de stations de travail peuvent être rapidement et facilement gérées à partir de la console d'adminstration centralisée de BitDefender. Les administrateurs informatiques peuvent ainsi avoir une vision globale des menaces et protéger proactivement les ressources de leurs réseaux. BitDefender Management Server permet de centraliser la gestion à distance des installations, la configuration et la génération de rapports de tous les produits clients, serveurs et passerelles BitDefender déployés dans l'entreprise. Elle permet également de notifier aux administrateurs les résultats des analyses, des infections et des tâches de mise à jour grâce à son module d'alertes.

bitdefender