

BitDefender for File Servers

GUIDE DE DEMARRAGE RAPIDE

Comment est-ce que cela fonctionne?

BitDefender for File Servers est une solution implémentée spécialement pour serveurs fonctionnant sur la plateforme Windows. Ses principaux traits couvrent les besoins de sécurité d'un serveur file-sharing, tandis que son objectif est de réduire le poids apporté par une solution d'administration des logiciels du serveur. Facile à installer et à configurer, mais avec un gros tas de fonctionnalités, il vise des petites et grandes compagnies.

Il stocke, partage et distribue des données comme majeure tâche de gestion, mais ceux-ci échoueraient sans l'accès facile à l'information, l'intégrité des données et une idéale mise à jour du système. BitDefender for File Servers vise les problèmes de sécurité des données et la disponibilité du système par:

Technologies avancées antivirus

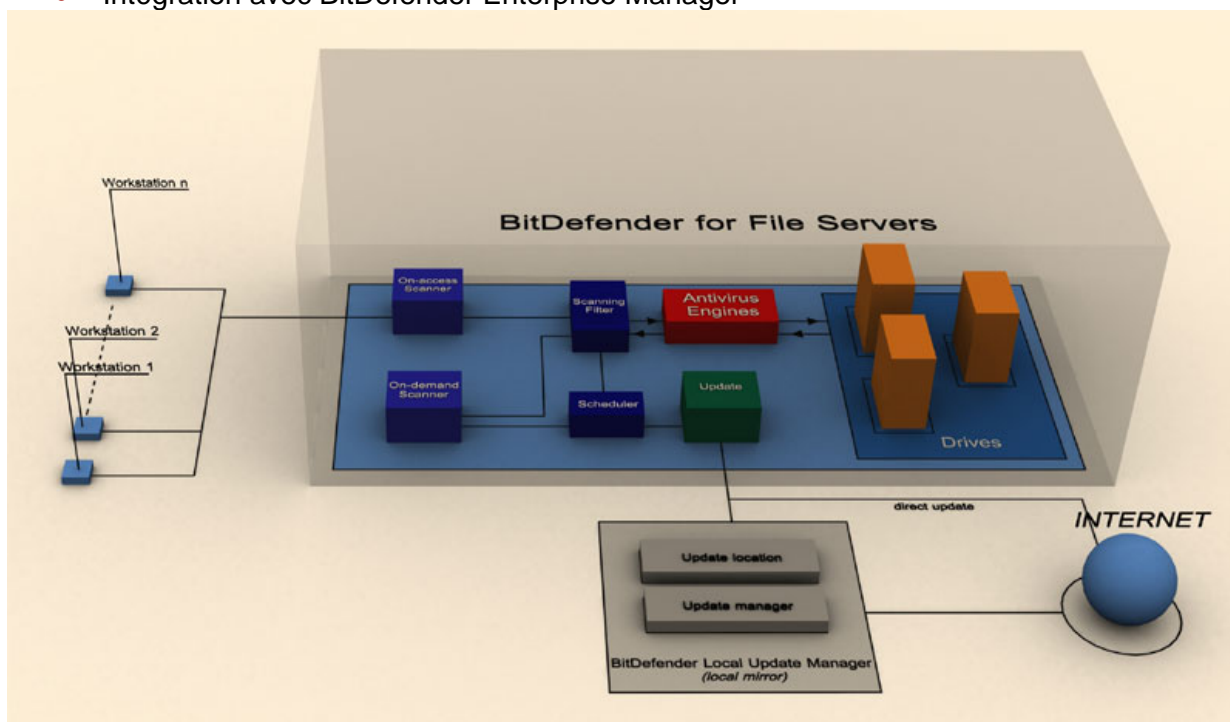
- La technologie HiVE et moteurs certifiés
- Analyse optimisée et multithread

Fonctionnalités puissantes

- Analyse antivirus on-access et on-demand
- Mise à jour automatique

Usabilité élargie

- Système de programmation
- Système de logging, reporting et alerting
- Intégration avec BitDefender Enterprise Manager



Dans le diagramme ci-dessus sont décrits les principaux processus, analyse antivirus et mise à jour

Pour mieux servir sa fonction de solution de sécurité pour serveurs, **BitDefender for File Servers** a été implémenté à base d'une architecture modulaire. Ses modules principaux sont:

- Analyse on-access
- Analyse on-demand
- Mise-à-jour
- Programmeur
- Filtre d'analyse
- Moteurs antivirus

La protection en temps réel

Comme les fichiers sont écrits sur un disque ou accés le module **Analyse On-access** intercepte l'évènement et démarre le processus d'analyse.

Les pas suivants peuvent décrire le processus d'analyse:

1. Le filtre d'analyse vérifie le fichier. L'extension, la taille, la voie du fichier sont successivement vérifiés pour répondre aux configurations de l'administrateur. Le résultat du Filtre d'analyse est ANALYSE ou PAS D'ANALYSE.
2. Si le résultat du Filtre d'analyse est Analyse, le fichier est analysé par les moteurs antivirus. D'abord le fichier est vérifié dans la base de données de signatures antivirus. Si n'importe quelle partie du fichier répond à une signature, le fichier est déclaré comme infecté. Si aucune des signatures ne s'y retrouve, le fichier est analysé avec la technologie HIVE. Au cas où le comportement du fichier est similaire au comportement d'un malveillant, le fichier est déclaré comme suspect. Le résultat du module des Moteurs Antivirus peut être INFECTE ou PROPRE.
3. Si le résultat du module des Moteurs Antivirus est INFECTE, l'une des actions suivantes peut être prise: désinfecter, effacer, ignorer, quarantaine. Si ces actions échouent d'être appliqués, on applique "Accès refusé". De cette manière l'utilisateur ne sera pas capable d'exécuter le code infecté.

La protection on-demand

Ce type de protection est utile pour les buts de maintenance usuelle et pour vérifier le serveur après une période où la protection antivirus on-access a été désaffectée.

Le module d'**analyse on-demand** peut être activé en cliquant "Analyser maintenant" depuis l'interface utilisateur ou par un une tâche d'analyse programmeur on-demand. Le processus d'analyse est le même, mais il vérifie tous les fichiers qui sont soumis à l'analyse et non pas les fichiers qui sont accésés.

Le processus de mise à jour

Le module de Mise à jour effectue le processus de mise à jour et sa principale fonction est de télécharger les derniers fichiers BitDefender. Trois types de fichiers sont valables:

- **Signatures antivirus.** Ces fichiers sont constamment mis à jour car BitDefender Lab analyse chaque jour des nouveaux virus.
- **Moteurs antivirus.** Ces fichiers sont mis à jour aussi fréquemment que les signatures antivirus. HIVE, la technologie propriété BitDefender a été implémentée dans les moteurs antivirus.
- **Fichiers produit.** Les mises à jour des fichiers produit diffèrent des mises à jour des signatures antivirus et leur fonction est de livrer des solutions pour les bugs et des améliorations de la performance du produit. Les mises à jour du produit sont téléchargées, mais non pas installées automatiquement. Merci de noter que l'installation des mises à jour du produit peuvent solliciter le redémarrage du système.

Le processus de Mise à jour est effectué automatiquement tous les 3 heures, mais l'intervalle de temps peut être configuré aussi bien que les tâches de mise à jour, à tout moment.

Le téléchargement des plus récents fichiers BitDefender sollicite une location de Mise à jour approuvée BitDefender. Le produit met à jour par défaut les fichiers depuis les sites BitDefender, mais les miroirs locaux des locations de Mise à jour BitDefender peuvent s'effectuer en installant **BitDefender Local Update Manager**. Le kit d'installation pour **BitDefender for File Servers** inclut également **BitDefender Local Update Manager**. De cette manière, les produits **BitDefender for File Servers** peuvent être chargés depuis une location dans le même réseau.

PRINCIPALES CARACTERISTIQUES

AVANTAGES

HiVE

HiVE, pour Heuristics in Virtual Environment ; concrètement, il émule un ordinateur virtuel dans l'ordinateur, où des parties de logiciels seront exécutées afin de rechercher des comportements potentiels de codes malveillants. Cette technologie propriétaire de BitDefender représente une nouvelle couche de sécurité qui garde le système d'exploitation protégé contre des virus inconnus en détectant des parties de codes potentiellement malicieuses pour lesquelles des signatures n'ont pas encore été préparées. Il complète les habituelles techniques de recherche par signature et par comportement, augmentant l'efficacité globale de votre solution antivirus. HiVE est un composant des moteurs antivirus BitDefender qui ont été certifiés par **ICSA Labs**, **CheckMark**, **CheckVir**, **Virus Bulletin**, **AV Comparatives** et **TüV**.

Optimisation de l'analyse

Le scanner antivirus de BitDefender antivirus scanner « marque », lors de chaque session, tous les fichiers en "lecture-seule" analysés. La permission "lecture-seule" assure que le fichier ne sera pas modifié ou infecté durant la session concernée. Une base de données des fichiers récemment analysés et trouvés sains est alors créée. Ces fichiers ne sont pas ré-analysés jusqu'à un nouvel accès. Si une mise à jour est réalisée ou si une infection est détectée sur le système, la base de données est réinitialisée. Cette mesure de sécurité assure que l'ensemble des fichiers est re-contrôlé avec les dernières signatures antivirus.

Analyse Multithread

L'analyse multithread implémente une méthode bien connue qui simule l'exécution en parallèle d'un programme. De multiples instances des moteurs sont utilisés afin de réduire le temps d'analyse.

Analyse à l'accès

L'analyse à l'accès assure une protection en temps réel du serveur de fichiers en analysant chaque fichier à l'accès sur le disque. C'est la principale fonction d'un serveur orienté application antivirus dont le but est de maintenir le serveur de fichiers libre de tout code malveillant.

Analyse à la demande

L'analyse à la demande est un outil puissant spécialement conçu pour les administrateurs. Son but est de fournir un second niveau de défense contre les codes malicieux qui pourraient infecter le serveur de fichiers. Nous vous recommandons d'analyser périodiquement le serveur de fichiers avec les nouvelles signatures de virus en programmant une tâche d'analyse antivirus ou en réalisant une tâche d'analyse immédiate.

Mise à jour automatique

Les mises à jour automatiques des signatures et du produit, secondées par la technologie HiVE, réduisent la fenêtre de vulnérabilité de votre système. Les mises à jour sont automatiquement téléchargées TOUTES LES HEURES depuis les serveurs BitDefender ou des sites miroirs approuvés.

Programmeur	Des options de programmation ont été ajoutées à BitDefender for File Servers. Les tâches d'analyse antivirus à la demande et de mises à jour peuvent être programmées depuis l'interface utilisateur du produit. Ce système a été couplé au module d'alertes pour fournir des notifications aux administrateurs lorsqu'une analyse à la demande ou une mise à jour ont été réalisées.
Logs et Statistiques	Le système de contrôle a également été amélioré. Des rapports sur l'activité du produit peuvent être créés et un module spécifique de statistiques est fourni. De plus, le système d'alertes inclut de nouvelles fonctions comme la personnalisation des alertes pour différents types d'événements: mise à jour des signatures antivirus, mise à jour du produit, analyse à la demande, virus détectés.
Nouvelle interface	BitDefender for File Servers a une interface utilisateur basée sur MMC qui offre un environnement de travail convivial. Un système d'assistants est intégré dans l'interface et le système de composant logiciel enfichable fournit les fonctionnalités de gestion actuelles.
Gestion centralisée	BitDefender for File Servers est totalement compatible avec BitDefender Enterprise Manager, assurant aux sociétés une gestion de type centralisée de la protection antivirus et des politiques de sécurité sur des réseaux complexes. L'installation à distance, la configuration à distance et le contrôle de l'état de BitDefender for File Servers peuvent être réalisés de manière centralisée depuis une console d'administration sur votre réseau.

Demandes de système:

Minimum Processor: Pentium II 300MHz

Minimum 75 MB espace disque disponible

Minimum RAM Memory: 64 MB (128 MB recommandés pour une performance supérieure)

Système d'exploitation: Windows NT 4.0 SP6 + IE 5.5 +MMC v1.2

Windows 2000, Windows XP or Windows 2003 Server

Meilleurs pratiques

1. Après la fin du processus d'installation, enregistrer le produit. Vous devez accéder la section **Enregistrement**, sélectionner le produit, introduire le numéro sérial et cliquer sur le bouton **Appliquer**.
2. Activer votre Compte Support. Pour gérer le feedback et sollicitations / demandes d'analyse des bugs vous envoyez à BitDefender, entrez dans la section **Information\Enregistrement** et cliquez sur **Enregistrement en ligne** depuis le menu d'Aide BitDefender
3. Configurer la mise à jour. Entrez dans la section **Paramétrages Mise à jour** et configurez les paramètres de la mise à jour. Par défaut, BitDefender fera une Mise à jour automatique tous les 3 heures. Cliquez **Analysez maintenant!** pour immédiatement mettre à jour les moteurs d'analyse.

INDICATION: Si **BitDefender for File Servers** a été installé sur un ordinateur qui n'a pas d'accès à Internet, configurez **BitDefender Local Update Manager** pour garder le moteur antivirus mis à jour.

4. Mettre en application les **Mises-à-jour Produit** disponibles. Entrez dans la section **Mises-à-jour Produit**. Entrez dans la section **Mise-à-jour\Mises-à-jour Produit** et installez les mises-à-jour disponibles pour le produit. Les mises-à-jour produit diffèrent des mises-à-jour des signatures antivirus et leur fonction est de livrer des solutions aux bugs et améliorations de la performance du produit. Les mises à jour produit sont téléchargées, mais non pas installées automatiquement. Merci de noter que l'installation des mises à jour produit peut solliciter le redémarrage du système. Nous vous conseillons d'installer la dernière version des mises à jour produit.
5. Sélectionner l'action à prendre contre les fichiers infectés durant l'analyse on-access. Entrez dans la section **Antivirus/Analyse on-access** et sélectionnez l'action désirée: désinfecter, effacer, mettre en Quarantine ou ignorer (pas d'action). Pour désinfecter vous pouvez sélectionner une seconde action au cas où la désinfection échoue.

INDICATION: Au cas où les deux actions échouent, **BitDefender for File Servers** refuse l'accès au fichier infecté afin de prévenir le système d'être infecté.

6. Vérifier que BitDefender fonctionne avec le test EICAR. Ce test consiste à créer un fichier utilisant l'éditeur de texte, à condition que le fichier soit sauvé en format standard MS-DOS ASCII et soit long de 68 bytes. Il peut également être de 70 bytes si l'éditeur met un CR/LF à la fin. Le fichier doit contenir seulement la ligne suivante:
X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*. Sauvez le fichier sous n'importe quel nom avec extension COM, par exemple EICAR.COM sur le serveur protégé par BitDefender. BitDefender doit traiter ce fichier comme un fichier infecté.
7. Effectuer l'analyse manuelle du file server. Entrez dans la section **Antivirus/Analyse on-demand**, configurez les paramètres d'analyse et cliquez sur **Analyser maintenant**.
8. Exclure les fichiers/directoires de l'analyse on-access. Entrez dans la section **Antivirus/Analyse on-access** et sélectionnez les fichiers désirés et /ou directoires. Vous pouvez exclure de l'analyse autant de directoires que vous voulez.

INDICATION: Pour une meilleure performance, configurez les options d'analyse des extensions en sélectionnant la case à cocher correspondant aux **Extensions Applications** pour analyser seulement les fichiers qui peuvent être exécutés.

9. Configurer les alertes BitDefender. Si un virus est détecté ou une situation inattendue apparaît, il est possible d'envoyer des messages d'alarme par e-mail ou par net send. Entrez dans la section **Alertes Mail** ou **Alertes Net Send** pour configurer BitDefender d'envoyer ces notifications.