

# BITDEFENDER SECURITY FOR SAMBA



## PROTECTION DES RESSOURCES RÉSEAU MULTIPLATEFORMES

Les serveurs de fichiers Samba sont souvent présents dans les grands réseaux hétérogènes car ils proposent un ensemble d'outils économiques et permettent de créer des interfaces entre les stations de travail et les serveurs de type Windows ou Linux/UNIX. Samba fournit des services stables et sécurisés pour fichiers et imprimantes sur toutes les plateformes utilisant le protocole SMB/CIFS, y compris celles des systèmes DOS, Windows, OS/2 et Linux.

Samba est aussi un composant important qui s'intègre parfaitement dans les stations de travail et les serveurs Linux/UNIX et à l'environnement Active Directory de Microsoft. Du fait de cette intégration, les services Samba peuvent facilement véhiculer des codes malveillants ciblant la plateforme Windows.

Parmi les services cruciaux que fournit un serveur de fichiers sur un réseau, on trouve :

- Serveurs web (Apache)
- Serveurs de fichiers et d'imprimantes (Samba)
- Serveurs d'accès à distance/VPN
- Serveur DNS

Les serveurs de fichier Samba peuvent transmettre les menaces suivantes :

- Codes malveillants dans les fichiers partagés
- Archives compressées infectées
- Virus, chevaux de Troie et rootkits
- Vers et spywares

Les fichiers stockés sur des partages Samba peuvent infecter d'autres systèmes avec du spyware, du adware ou un cheval de Troie/virus. Les vers peuvent également se propager sur l'ensemble du réseau et contaminer un serveur. Si ce dernier n'est pas protégé, les services essentiels du réseau deviennent inutilisables pour l'ensemble des utilisateurs, ayant pour conséquence des répercussions graves sur la productivité de l'entreprise.

## SÉCURISATION DES SERVEURS DE FICHIERS SAMBA AVEC BITDEFENDER

Les entreprises peuvent protéger leurs serveurs de fichiers Samba contre les attaques grâce à la capacité que possède BitDefender de détecter les codes malveillants se trouvant dans des fichiers, de maintenir l'intégrité du système, de contribuer à la conformité avec les politiques de sécurité et d'empêcher que des données sensibles sortent de l'entreprise.

BitDefender Security for Samba permet aux entreprises de déployer une protection antivirus et antispyware sur les partages réseau Samba tournant sous les systèmes d'exploitation Linux, FreeBSD ou Solaris. Déployé et géré de façon centralisé au sein du réseau, Security for Samba analyse les structures de données et les dossiers de fichiers multi-plateformes à la recherche de malwares et protège les utilisateurs du réseau contre les infections virales.



## PRINCIPALES FONCTIONNALITÉS ET AVANTAGES-CLÉS

- Détection primée des virus, nettoyage et mise en quarantaine
- Limitation du temps d'arrêt du réseau et des risques de propagation des malwares grâce à l'analyse des fichiers partagés assurant une protection antimalware en temps réel
- Souplesse de planification des analyses à la demande ou immédiates
- Mise en quarantaine des fichiers infectés ou suspects pour minimiser le risque de propagation
- Permet la configuration à distance à partir de n'importe quel ordinateur de l'entreprise via une interface web d'administration à distance
- Parfaitement conforme à la norme FHS (Filesystem Hierarchy Standard), fonctionne de manière non intrusive
- Fonctionne avec toutes les versions de Samba et peut être facilement compilé avec toutes les versions, grâce à son module vfs open source
- Compatible avec toutes les principales plateformes UNIX grâce aux empaquetages rpm, deb et .tar.run générique

## CARACTÉRISTIQUES AVANCÉES

- S'intègre à BitDefender Management Server
- Le tableau de bord centralisé affiche un résumé de l'état des déploiements et les seuils d'alerte
- Mise en quarantaine des fichiers suspects en toute sécurité, avec option de restauration à l'emplacement d'origine
- Personnalisation des notifications par e-mail et alertes SNMP concernant son activité : nombre de fichiers analysés, désinfectés, supprimés, infectés ou filtrés.

## 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.

## DÉFENSE EN PROFONDEUR

BitDefender Security for Samba 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, le spyware, le adware et les chevaux de Troie peuvent faire peser sur l'intégrité de votre réseau.

## CONFIGURATION REQUISE

### Système d'exploitation :

- 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

### Samba :

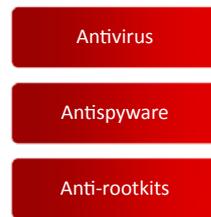
- Version 3.0 ou plus récent

### Compatible avec les distributions :

- Debian GNU/Linux 3.1 ou plus récent
- Fedora Core 1 ou plus récent
- FreeBSD: 5.4-RELEASE (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)



### Protection Proactive



### Administration Centralisée



BitDefender Security for Samba fournit une protection proactive et une administration centralisée

## DÉTECTION PROACTIVE AVANCÉE

Optimisés pour le serveur de fichiers Samba, 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 For Samba offre 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".

**Antispyware** – BitDefender détecte les spywares et adwares connus empêchant ainsi les fuites de données.

**Les Chevaux de Troie et les Rootkits** sont conçus pour un accès distant à un ordinateur. Lorsqu'un Cheval de Troie ou un Rootkit est installé, un pirate peut accéder à l'ordinateur à distance et voler des données. 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.

## CONFIGURATION ET ADMINISTRATION GRANULAIRE DES ANALYSES

BitDefender Security for Samba fournit des méthodes d'analyse à l'accès, à la demande ou planifiées, pour détecter les codes malveillants et préserver l'intégrité des dossiers de stockage de fichiers. Les fichiers suspects sont isolés dans des zones de quarantaine. Les fichiers peuvent être supprimés ou conservés pour analyse dans la zone de quarantaine, restaurés à leur emplacement d'origine une fois validés, ou directement envoyés aux Laboratoires antivirus BitDefender pour évaluation.

## INTÉGRATION À LA CONSOLE D'ADMINISTRATION CENTRALISÉE

BitDefender Security for Samba s'intègre au tableau de bord de sécurité de BitDefender Management Server, ce qui donne aux administrateurs la visibilité de l'ensemble de leurs ressources réseau et de la sécurité globale. 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.

