Sommaire

Utilisation de F-Secure Anti-Virus

Présentation
F-Secure Anti-Virus Gatekeeper
Recherche manuelle de virus
Assistant de nettoyage

Paramètres utilisateur de F-Secure Anti-Virus

Paramètres
Protection en temps réel
Analyse manuelle
Mises à jour
Statistiques

Support technique

Support technique

A propos de F-Secure Corporation

Informations sur F-Secure Corporation
La gamme de produits F-Secure

Présentation

F-Secure Anti-Virus est conçu pour les environnements réseau des entreprises. La fonction de détection des virus s'exécute en temps réel et de manière transparente. Ce programme ne nécessite quasiment aucune intervention de l'utilisateur, ce qui réduit les besoins en formation et en assistance technique. La gestion centralisée par stratégies est une solution antivirus peu coûteuse et d'une maintenance simple.

F-Secure Anti-Virus Gatekeeper

Le fonctionnement de F-Secure Anti-Virus Gatekeeper repose sur la technologie DVP (protection virale dynamique). Cette technologie repose sur un pilote de périphérique qui contrôle les services utilisés par le système d'exploitation lors de l'ouverture des fichiers et de la gestion des partitions de disques.

La fonction de protection en temps réel de F-Secure Anti-Virus Gatekeeper fournit une protection antivirus continue lorsque les fichiers sont ouverts, copiés, déplacés, renommés ou téléchargés depuis Internet.

La protection en temps réel fonctionne de manière transparente en tâche de fond. Elle recherche la présence éventuelle de virus lorsque vous accédez à des fichiers stockés sur disque dur, sur disquettes ou sur lecteurs réseau. Si vous tentez d'accéder à un fichier infecté, la protection en temps réel interrompt automatiquement l'exécution du virus. En fonction de la stratégie de sécurité définie, le virus est supprimé du fichier ou un message d'avertissement s'affiche.

F Afin d'empêcher les virus de secteur d'amorçage de se propager, la protection en temps réel analyse également les disquettes à l'arrêt ou au redémarrage de l'ordinateur. Si aucune disquette ne se trouve dans le lecteur, ce dernier peut émettre un bourdonnement. Il s'agit là d'un phénomène normal.

Pour savoir si la protection en temps réel est active, cliquez deux fois sur l'icône Paramètres et statistiques de F-Secure Manager dans la barre d'état système, située dans l'angle inférieur droit de l'écran. Si l'état de F-Secure Anti-Virus est « Activé », la protection en temps réel est active et fournit une protection continue.

Recherche manuelle de virus

Il n'est pas nécessaire d'analyser les fichiers manuellement. Les options de détection en temps réel de F-Secure Anti-Virus Gatekeeper garantissent en effet une protection automatique maximale contre les virus. Par conséquent, les informations figurant dans cette section ne sont données qu'à titre indicatif au cas où vous souhaiteriez lancer une analyse manuelle.

Vous pouvez lancer une analyse à partir de l'un des menus suivants :

- menu contextuel (cliquez avec le bouton droit de la souris sur un fichier, un dossier ou un disque),
- menu Paramètres et statistiques de F-Secure dans la barre d'état système (cliquez avec le bouton droit de la souris sur l'icône « F » (F-Secure) de la barre d'état système),
- menu Démarrer de Windows (cliquez avec le bouton droit de la souris sur le menu).

Au cours d'une analyse manuelle, la boîte de dialogue *Statistiques de l'analyse manuelle* affiche un indicateur d'avancement, ainsi que des statistiques sur l'analyse en cours. Pour interrompre l'analyse, cliquez sur **Arrêter**. A la fin de l'analyse, un rapport est généré. Vous pouvez visualiser ce rapport dans votre navigateur Web. Il suffit de cliquer sur le bouton **Afficher le rapport**.

Autres :

Menu contextuel

Menu Paramètres et statistiques de F-Secure dans la barre d'état système

Lancement d'une analyse à partir du menu Démarrer de Windows

Menu contextuel

Pour rechercher des virus dans un fichier, un dossier ou une disquette, cliquez avec le bouton droit de la souris sur l'icône appropriée, puis sélectionnez l'option « Rechercher des virus dans les dossiers » dans le menu contextuel. Tout fichier, dossier ou lecteur peut être analysé de cette manière, quelle que soit son extension.

Menu Paramètres et statistiques de F-Secure dans la barre d'état système

Pour afficher le menu F-Secure Manager, cliquez avec le bouton droit de la souris sur l'icône « F » (F-Secure) de la barre d'état système.

Pour lancer une analyse, sélectionnez l'une des options d'analyse figurant dans le menu.

Si vous sélectionnez l'option *Analyser la cible*, vous devez sélectionner le dossier ou le disque à analyser.

Lancement d'une analyse à partir du menu Démarrer de Windows

Le groupe de programmes de F-Secure Anti-Virus contient des raccourcis permettant d'analyser les disques durs, les disquettes et les dossiers.

Pour lancer une analyse, sélectionnez l'une des commandes d'analyse disponibles dans le menu : *Analyser tous les disques durs locaux, Analyser la disquette* ou *Analyser le dossier*. Si vous sélectionnez l'option *Analyser le dossier*, vous devez sélectionner le dossier ou le disque à analyser.

Assistant de nettoyage

Lorsque vous utilisez l'ordinateur et qu'un virus est détecté, F-Secure Anti-Virus lance automatiquement l'Assistant de nettoyage car cette option est définie par défaut.

1. Le premier écran affiche le nom des virus détectés.
   Pour obtenir de plus amples informations sur un virus, cliquez sur son nom, puis sur le bouton **Infos virus**. La page d'informations sur les virus répertorie les virus détectés.
   Pour parcourir l'ensemble de la base de données d'informations sur les virus, cochez la case appropriée. Si le virus est très récent, il n'y figure peut-être pas. Lorsqu'aucune description n'est disponible, consultez la base de données d'informations sur les virus, accessible à partir de notre site Web.
   La base de données F-Secure d'informations sur les virus est une base de connaissances qui rassemble une masse considérable d'informations sur des milliers de virus différents. Cette base de données est mise à jour quotidiennement. Pour y accéder, cliquez sur le bouton **Web Club**.
2. La liste des fichiers infectés s'affiche.
   Dans la zone ***Action***, sélectionnez l'opération à exécuter sur les fichiers infectés.
3. Les fichiers sont alors nettoyés et les résultats de la tâche de nettoyage s'affichent.
4. Un rapport de nettoyage est ensuite généré. Si vous ne souhaitez pas obtenir de rapport, ne cochez pas la case **Créer le rapport**.

Le rapport de nettoyage s'affiche automatiquement dans votre navigateur Web par défaut. Ce rapport est envoyé à l'administrateur si le programme est géré de manière centralisée.

> F Remarque : L'administrateur peut configurer F-Secure Anti-Virus de sorte que les virus soient supprimés automatiquement sans qu'aucune intervention de l'utilisateur ne soit nécessaire. Dans ce cas, l'Assistant de nettoyage ne s'exécute pas.

Paramètres

Pour afficher et modifier les paramètres de F-Secure Anti-Virus, cliquez deux fois sur l'icône « F » de la barre d'état système pour ouvrir la boîte de dialogue *Paramètres et statistiques* de F-Secure. La boîte de dialogue *Paramètres et statistiques* de F-Secure s'ouvre et affiche la liste des produits F-Secure installés.

Vous pouvez ensuite cliquer deux fois sur l'application *F-Secure Anti-Virus* ou cliquer sur **Propriétés** pour ouvrir la boîte de dialogue *Propriétés de F-Secure Anti-Virus*. Dans cette boîte de dialogue, différents paramètres sont disponibles pour les trois types d'analyses suivants : Protection en temps réel, Analyse manuelle et Mises à jour. La boîte de dialogue *Propriétés de F-Secure Anti-Virus* contient également des informations sur les statistiques de l'analyse.

Statistiques

Affiche les résultats de l'analyse en temps réel.

Protection en temps réel

Paramètres définissant la protection continue et transparente assurée par F-Secure Anti-Virus en tâche de fond : les fichiers sont analysés lors de leur accès.

Analyse manuelle

Paramètres définissant les tâches d'analyse lancées manuellement.

Mises à jour

Paramètres activant les rappels automatiques de mise à jour des bases de données de définition des virus pour les mises à jour manuelles. Le bouton **Mettre à jour maintenant** permet d'effectuer des mises à jour immédiates.

Il est nécessaire de limiter le champ d'action des analyses en temps réel afin de ne pas trop solliciter les ressources système, notamment dans le cadre d'analyses de fichiers compressés ou d'autres fichiers non standard.

Etant donné que les analyses manuelles sont effectuées au cas par cas en fonction de besoins spécifiques, il est possible de concentrer l'analyse sur un nombre important de fichiers, ce qui sollicite toutefois davantage de ressources système.

Protection en temps réel

Pour activer ou désactiver la protection en temps réel assurée par F-Secure Anti-Virus, cochez ou non la case ***Activer la protection***.

Autres :

Action à appliquer aux fichiers infectés

Options d'analyse

Action à appliquer aux fichiers infectés

Dans la zone ***Action à appliquer aux fichiers infectés***, sélectionnez l'action exécutée par F-Secure Anti-Virus lors de la détection d'un fichier infecté. Sélectionnez l'une des actions suivantes :

Interroger l'utilisateur après l'analyse
Lance l'Assistant de nettoyage lorsqu'un fichier infecté est détecté.

Nettoyer automatiquement
Nettoie le fichier automatiquement lorsqu'un virus est détecté.

Renommer automatiquement
Renomme le fichier automatiquement lorsqu'un virus est détecté.

Supprimer automatiquement
Supprime le fichier automatiquement lorsqu'un virus est détecté.

Options d'analyse

Dans la zone ***Options d'analyse***, sélectionnez les fichiers à analyser en temps réel.
Les options suivantes sont disponibles :

Tous les fichiers

Tous les fichiers sont analysés, quelle que soit leur extension. Cette option est déconseillée car elle risque de ralentir considérablement les performances du système.

Fichiers avec ces extensions

Seuls les fichiers portant les extensions définies sont analysés. Pour indiquer des fichiers sans extension, tapez « . ». Vous pouvez également utiliser le caractère générique « ? ». Séparez chaque extension de fichier par un espace. Cette option est recommandée pour la protection en temps réel.

Exclure les fichiers avec ces extensions

Les fichiers portant l'une des extensions définies ne sont pas analysés.

Exclure les objets

Permet de spécifier quels fichiers ou dossiers spécifiques ne doivent pas être analysés. Cliquez sur le bouton **Sélectionner**, puis recherchez dans l'arborescence les fichiers et dossiers à exclure de l'analyse.

Analyser les fichiers compressés

Cochez cette case pour analyser les fichiers compressés, tels que les fichiers ZIP, ARJ ou LZH. L'analyse de fichiers compressés volumineux sollicite de nombreuses ressources système et risque donc de ralentir le système. Cette option s'accorde mal avec la protection en temps réel.

Analyse manuelle

Les paramètres des opérations d'analyse manuelle peuvent être spécifiés dans la page *Analyse manuelle* de la boîte de dialogue *Propriétés de F-Secure Anti-Virus*.

Autres :

Action à appliquer aux fichiers infectés

Options d'analyse

Action à appliquer aux fichiers infectés

Dans la zone ***Action à appliquer aux fichiers infectés***, sélectionnez l'action exécutée par F-Secure Anti-Virus lors de la détection d'un fichier infecté.

Les options suivantes sont disponibles :

Interroger l'utilisateur après l'analyse

Lance l'Assistant de nettoyage lorsqu'un fichier infecté est détecté.

Nettoyer automatiquement

Nettoie le fichier automatiquement lorsqu'un virus est détecté.

Renommer automatiquement

Renomme le fichier automatiquement lorsqu'un virus est détecté.

Supprimer automatiquement

Supprime le fichier automatiquement lorsqu'un virus est détecté.

Options d'analyse

Dans la zone ***Options d'analyse***, sélectionnez les fichiers à analyser manuellement.
Les options suivantes sont disponibles :

Tous les fichiers

Tous les fichiers sont analysés, quelle que soit leur extension. Cette option est déconseillée car elle risque de ralentir considérablement les performances du système.

Fichiers avec ces extensions

Seuls les fichiers portant les extensions définies sont analysés. Séparez chaque extension de fichier par un espace. Vous pouvez également utiliser le caractère générique « ? ».

Exclure les fichiers avec ces extensions

Les fichiers portant l'une des extensions définies ne sont pas analysés.

Exclure les objets

Permet de spécifier quels fichiers ou dossiers spécifiques ne doivent pas être analysés. Cliquez sur le bouton **Ajouter**, puis recherchez dans l'arborescence les fichiers et dossiers à exclure de l'analyse.

Analyser les fichiers compressés

Cochez cette case pour analyser les fichiers compressés, tels que les fichiers ZIP, ARJ ou LZH. Etant donné que les tâches d'analyse manuelle n'affectent pas les performances du système, cette option peut être utilisée sans risque.

Le bouton **Analyser maintenant** permet de rechercher à tout moment des virus dans un dossier.

Mises à jour

La page Mises à jour contient des informations sur les moteurs d'analyse installés, ainsi que sur les mises à jour de la base de données de virus. Elle comporte également un lien direct vers le site Web de F-Secure ou vers le site d'un fournisseur d'accès à Internet, à partir du bouton **Autres informations**.

Autres :

Moteurs d'analyse installés

Mises à jour de la base de données de définition des virus

Rappel des mises à jour

Mettre à jour maintenant

Mise à jour manuelle

Autres informations

Moteurs d'analyse installés

La zone ***Moteurs d'analyse installés*** contient des informations sur les noms de moteurs d'analyse installés, la date des bases de données individuelles et leurs numéros de révision. Les moteurs d'analyse utilisés sont F-Secure F-Prot, F-Secure AVP et F-Secure Orion.

Mises à jour de la base de données de définition des virus

La section ***Mises à jour de la base de données de définition des virus*** vous informe sur l'état courant des bases de données de définition de virus. Elle vous indiquera, par exemple, les mises à jour à effectuer si les bases de données de définition de virus sont anciennes.

Rappel des mises à jour

Grâce à la case à cocher ***Rappel des mises à jour***, vous pouvez activer les rappels automatiques de mise à jour des bases de données de définition des virus. Vous pouvez déterminer la fréquence d'affichage de la boîte de dialogue de mise à jour en insérant un nombre dans la zone ***jours***.

La disponibilité de la fonctionnalité de rappel de mise à jour est déterminée par les paramètres de stratégie. Si les mises à jour manuelles sont interdites dans les paramètres de stratégie, la case ***Rappel des mises à jour*** et la zone ***[X] jours*** ne sont pas disponibles. L'administrateur peut modifier l'état d'autorisation de ces options à partir de la stratégie F-Secure Administrator :

`FSAV\Data Fellows\F-Secure Anti-Virus\Settings\Virus Database Updates\Update Reminder\Reminder Status`

L'état par défaut du mode autonome est **autorisé**. Pour le mode de gestion centralisée, il est **non autorisé**.

Mettre à jour maintenant

Le bouton **Mettre à jour maintenant** lance la mise à jour manuelle des bases de données de définition de virus. La disponibilité de cette fonction est déterminée par les paramètres de stratégie.

Si le paramètre de stratégie F-Secure Administrator suivant :

`FSAV\Data Fellows\F-Secure Anti-Virus\Settings\Virus Database Updates\Allow Manual Updates`

est défini sur **true**, vous pouvez utiliser le bouton **Mettre à jour maintenant**. Si F-Secure Anti-Virus a été installé en configuration de gestion centralisée, il lancera une interrogation de mise à jour normale à partir du Management Server ou depuis les bases de données de définition des virus. Le mode autonome commence à télécharger les nouvelles bases de données depuis le site de F-Secure ou depuis le site d'un fournisseur d'accès à Internet.

Une boîte de dialogue s'affiche pendant le processus de téléchargement. Pour annuler la mise à jour, il suffit de cliquer sur le bouton **Cancel Update (Annuler la mise à jour)**.

Mise à jour manuelle

Si les mises à jour manuelles des bases de données de définition des virus sont autorisées, les rappels de mises à jour sont également activés. Si la case ***Rappel des mises à jour tous les [X] jours*** est cochée et si X jours sont passés depuis la dernière mise à jour, ou le dernier rappel de mise à jour, une boîte de dialogue s'affiche.

Si vous appuyez sur le bouton **Mettre à jour maintenant** de cette boîte de dialogue, la mise à jour manuelle des bases de données de définition de virus commence. Si vous cliquez sur le bouton **Rappeler ultérieurement**, le rappel de mise à jour est reporté du nombre de jours défini en tant qu'intervalle de rappel. Si vous cliquez sur le bouton **Options de mise à jour**, la boîte de dialogue *Propriétés de F-Secure Anti-Virus* s'ouvre sur l'onglet *Database Management (Gestion de la base de données)*.

Autres informations

Le bouton **Autres informations** ouvre le navigateur Web par défaut sur le site de F-Secure ou sur le site d'un fournisseur de services Internet. L'adresse peut être modifiée dans F-Secure Administrator :

`FSAV\Data Fellows\F-Secure Anti-Virus\Settings\Virus Database Updates\Information Site`

Notez que l'adresse doit comporter le nom de protocole et de site, par exemple, http://www.company.com.

Statistiques

La page *Statistiques* de la boîte de dialogue *Propriétés de F-Secure Anti-Virus* affiche les résultats de l'analyse en temps réel pour la session en cours.

Support technique

Le support technique de F-Secure est disponible par courrier électronique et depuis notre site Web. Vous pouvez y accéder depuis F-Secure Anti-Virus ou depuis votre navigateur Web.

Autres :

Web Club

Descriptions de virus sur le Web

Assistance par courrier électronique

Web Club

Le Web Club F-Secure Anti-Virus propose une assistance aux utilisateurs du programme F-Secure Anti-Virus. Pour y accéder, choisissez la commande Web Club du menu Aide. A la première utilisation de cette option, entrez le chemin d'accès à votre navigateur Web et votre pays de résidence.

Pour vous connecter directement au Web Club depuis votre navigateur Web, entrez l'adresse suivante :
http://www.F-Secure.com/webclub/

Pour obtenir une aide plus personnelle, le centre d'assistance F-Secure Anti-Virus est disponible à l'adresse suivante :
http://www.F-Secure.com/support/

Descriptions de virus sur le Web

F-Secure Corporation met régulièrement à jour une base de données complète d'informations sur les virus informatiques sur son site Web. Pour consulter cette base de données, choisissez la commande Virus Descriptions On the Web (Descriptions de virus sur le Web) du menu Aide.

Vous pouvez également y accéder à l'adresse suivante :
http://www.F-Secure.com/vir-info/

Assistance par courrier électronique

Si vous avez des questions sur F-Secure Anti-Virus qui n'ont pas été abordées dans ce manuel ou dans les services en ligne sur le site *www.F-Secure.com*, contactez votre revendeur F-Secure ou directement F-Secure Corporation.

Pour obtenir l'assistance technique de base, veuillez contacter votre partenaire F-Secure. Envoyez votre courrier électronique à l'adresse suivante :

Anti-Virus-<pays>@F-Secure.com

Exemple : Anti-Virus-France@F-Secure.com

Si aucun partenaire F-Secure Anti-Virus ne se trouve dans votre pays, vous pouvez tout de même obtenir de l'aide à l'adresse suivante :

Anti-Virus-Support@F-Secure.com

Veuillez inclure les informations suivantes avec votre demande :

Numéro de version de F-Secure Anti-Virus (y compris le numéro de révision).

Nom et numéro de version de votre système d'exploitation (DOS, Windows). Numéro de révision du système d'exploitation.

Description détaillée du problème, y compris tout message d'erreur affiché par le programme, ainsi que tout détail susceptible de nous aider à reproduire le problème.

Lorsque vous contactez F-Secure par téléphone, procédez comme suit pour gagner du temps :

Tenez-vous à proximité de votre ordinateur afin de pouvoir suivre les instructions fournies par le technicien ou apprêtez-vous à noter les instructions.

Mettez l'ordinateur sous tension et, si possible, dans l'état où il se trouvait lorsque le problème est survenu. Le cas échéant, vous devrez pouvoir reproduire le problème sur l'ordinateur avec un minimum d'efforts.

Si vous êtes victime d'une infection virale, assurez-vous d'avoir exécuté la toute dernière mise à jour fsupdate. Vous pouvez télécharger le fichier fsupdate depuis le Web Club.

Informations sur F-Secure Corporation

F-Secure Corporation (anciennement Data Fellows) est l'un des plus grands développeurs mondiaux de produits de protection des données. Notre société développe, commercialise et assure l'assistance technique de logiciels antivirus, de protection de données et de cryptographie pour les réseaux informatiques d'entreprise. Nos principaux sièges se trouvent à San Jose en Californie et à Espoo en Finlande. Nous possédons des bureaux dans plusieurs pays, notamment au Royaume-Uni, en France, en Allemagne, au Japon, à Hong Kong et au Canada. Nos partenaires, revendeurs et autres distributeurs sont situés dans plus de 80 pays de par le monde. Les produits F-Secure ont été traduits dans plus de 20 langues.

Les logiciels F-Secure ont reçu de nombreux prix et citations dans le monde entier. Notre société a figuré parmi les 100 meilleures entreprises du domaine technique du monde du magazine Red Herring dans son numéro de septembre 1998. F-Secure Workstation Suite 4.0 s'est vu décerner cinq étoiles, la plus haute distinction, par le magazine SECURE Computing dans son numéro de juillet 1999. F-Secure Anti-Virus a été élu Choix de la rédaction par le magazine allemand PC Professionell dans son numéro de juillet 1999. D'autres récompenses nous ont été décernées, telles que Produit de l’année 1997 (Data Communications Magazine), Meilleur produit antivirus (SVM Magazine, mai 1997) et le prix européen des technologies de l'information en 1996.

F-Secure Corporation compte des dizaines de milliers de clients dans plus de 100 pays. Parmi nos clients, nous comptons les plus grandes entreprises industrielles mondiales et les compagnies de télécommunication les plus prestigieuses, des compagnies aériennes importantes, plusieurs services gouvernementaux, services postaux et forces de défense européens, ainsi que plusieurs banques de renom. Nous comptons également parmi nos clients la NASA, l'US Air Force, la branche médicale du ministère de la défense américain, l'US Naval Warfare Center, le San Diego Supercomputer Center, le Lawrence-Livermore National Laboratory, IBM, Unisys, Siemens-Nixdorf, EDS, Cisco, Nokia, Sonera (anciennement Telecom Finland), UUNet Technologies, Boeing, Bell Atlantic et MCI.

La gamme de produits F-Secure

Tous les produits F-Secure sont intégrés dans F-Secure Framework qui propose une infrastructure à trois niveaux, adaptable et stratégique, afin de minimiser le coût de gestion de la sécurité.

F-Secure Workstation Suite permet la détection et la suppression de codes malveillants, le cryptage discret de fichiers et de réseaux et propose un firewall personnel. Toutes ces fonctions s'intègrent dans une architecture de gestion par stratégies.

F-Secure Anti-Virus, doté de plusieurs moteurs d'analyse (dont F-PROT et AVP), est le système de protection et d'analyse en temps réel le plus complet, adapté à toutes les principales plates-formes, serveurs ou postes de travail. Il s'agit d'une solution à trois niveaux destinées aux entreprises, qui comporte de nombreuses fonctions adaptées à la gestion de réseau et au déploiement centralisé.

F-Secure Content Scanner protège les réseaux des virus entrant par courrier électronique, téléchargements sur Internet et réplication de base de données. Il fonctionne avec Microsoft Exchange Server, Lotus Domino, les produits firewall de Check Point et autres éditeurs importants.

F-Secure VPN+ propose une solution logicielle pour réseaux privés virtuels, conforme à IPSec aussi bien pour les grands réseaux d'entreprises que pour les petits. Grâce à l'utilisation des divers produits F-Secure VPN+, les entreprises de toute taille peuvent utiliser les réseaux publics ou Internet pour créer des réseaux privés virtuels sécurisés sans devoir installer de matériel particulier.

F-Secure FileCrypto est le premier (et unique) produit intégrant un cryptage en temps réel puissant directement dans le système de fichiers Windows. Il crypte automatiquement les données avant de les stocker sur le disque dur, protégeant ainsi les informations sensibles dans les situations les plus exigeantes. FileCrypto permet également aux utilisateurs d'envoyer à d'autres utilisateurs des ensembles de fichiers cryptés auto-extractibles par courrier électronique.

FSecure SSH propose des connexions distantes, des fonctions de terminal et autres connexions sécurisées sur des réseaux non protégés. Ce produit est l'outil d'administration distante sécurisée le plus fréquemment utilisé.

F-Secure NameSurfer est la solution adaptée à l'administration distante des DNS Internet et intranet. Son interface Web facile d'utilisation permet d'automatiser et de simplifier l'administration des DNS.

F-Secure Distributed FireWall est une solution logicielle qui offre une protection globale des utilisateurs itinérants, où qu’ils se trouvent, depuis un emplacement de gestion centralisée.

Glossaire

Amorçage à froid
Amorcer
AUTOEXEC.BAT
BIOS
Bit
CMOS
CONFIG.SYS
Contrôle de l'accès
CounterSign
CPU
CRC
DOS
Fichier BAT
Fichier COM
Fichier EXE
HPFS
Kilo-octet
LAN (réseau local d'entreprise)
MBR
Méga-octet
Modem
NFS
NTFS
Octet
Programme d'analyse à la demande
Programme d'analyse en temps réel
Programme d'analyse lors de l'accès
RAM
Réinitialiser
Secteur d'amorçage
Somme de contrôle
Tâche de fond
Virus multipartite
Virus mutant

Contrôle de l'accès

Procédure qui accorde ou refuse l'utilisation d'un système à des utilisateurs ou à des traitements. Généralement, il consiste à authentifier l'utilisateur, à vérifier les droits d'accès, ainsi qu'à assurer la surveillance et la connexion.

AUTOEXEC.BAT

Fichier de commande exécuté automatiquement au démarrage du système dans DOS.

Tâche de fond

Tâche exécutée, mais qui n'apparaît pas dans la fenêtre active.

Fichier BAT

Fichier contenant les commandes DOS utilisées pour l'automatisation des tâches répétitives.

BIOS

Basic Input/Output System. Partie du système d'exploitation qui gère la plupart des tâches propres au matériel. Sur la majorité des PC, le BIOS est stocké dans la ROM.

Bit

Plus petite unité de taille de mémoire reconnaissable par un ordinateur. Les jeux de bits constituent des octets, ordonnés en motif séquentiel afin d'exprimer du texte, des nombres ou d'autres informations détaillées.

Amorcer

Redémarrer l'ordinateur.

Secteur d'amorçage

Enregistrement d'amorçage. Zone située sur la première piste des disquettes et des disques logiques. Les informations du secteur d'amorçage permettent à l'ordinateur de lire un système d'exploitation (tel que MS-DOS, par exemple).

Octet

Petite unité de taille de mémoire suffisante pour stocker un caractère alphabétique ou numérique. Chaque octet est composé de « bits », c'est-à-dire d'unités binaires regroupées en ensembles (par exemple, 00101101) qui permettent de stocker les plus petites informations.

Somme de contrôle

Numéro d'identification calculé à partir des caractéristiques d'un fichier. Si le fichier est modifié, même peu, cette identité est changée.

CMOS

Complementary Metal Oxide Semiconductor. Mémoire à pile des ordinateurs de type PC. La taille de cette mémoire est généralement comprise entre 32 et 50 octets. Le CMOS contient des informations sur les détails externes, tels que les disques, la date et les périphériques. Il ne se vide pas lorsque l'ordinateur est mis hors tension, tant que la pile fonctionne.

Amorçage à froid

Redémarrage de l'ordinateur, par mise hors tension, puis sous tension.

Fichier COM

Programme DOS exécutable dont la structure est simple. Sa taille maximum est de 64 kilo-octets.

CONFIG.SYS

Fichier de configuration exécuté automatiquement au démarrage du système dans DOS.

CounterSign

Cadre qui intègre divers moteurs d'analyse afin d'offrir une protection à plusieurs niveaux, pour tous les schémas possibles de compression et de cryptage et servant de protection totale contre les virus pouvant toucher une entreprise dans une seule interface.

CPU

Central Processing Unit. Le « cerveau » de l'ordinateur. Elle se trouve généralement dans une « boîte » qui peut être séparée du moniteur.

CRC

Cyclic Redundancy Check. Méthode de somme de contrôle parmi les plus fréquemment utilisées. CRC utilise une signature 32 bits calculée à partir du contenu d'un fichier.

DOS

Disk Operating System. Type de système le plus élémentaire. Il était, à l'origine, utilisé sur tous les ordinateurs personnels.

Fichier EXE

Fichier « exécutable » ou fichier de programme. Type de fichier qui « s'exécute », contrairement à un document ou à un fichier de données.

HPFS

High Performance File System. Système de fichiers utilisé par OS/2.

Kilo-octet

1024 octets.

LAN (réseau local d'entreprise)

Local Area Network. Petit réseau se trouvant dans une pièce, un édifice ou un groupe qui peut ou non être connecté au réseau mondial Internet.

MBR

Master Boot Record. Zone située sur la piste zéro des disques durs physiques. Il contient le programme d'amorçage principal, ainsi que la table de partition. L'enregistrement d'amorçage principal est indépendant des systèmes d'exploitation et est toujours exécuté en premier, une fois que l'ordinateur a effectué l'autotest de mise sous tension (POST - Power-On-Self-Test). La taille de l'enregistrement d'amorçage principal est de 512 octets. Il permet de traduire la table de partition qui contient des informations relatives à la division en entités logiques du disque physique (partitions). Après cela, le programme d'amorçage principal exécute le secteur d'amorçage de la partition active.

Méga-octet

1024 kilo-octets (un million d'octets)

Modem

Matériel téléphonique utilisé pour connecter un ordinateur ou un réseau local (LAN) à un réseau plus vaste, tel qu'Internet.

Virus multipartite

Virus composé de plusieurs parties. Chaque partie d'un tel virus doit être nettoyée afin d'être certain qu'aucune infection ne se produira.

Virus mutant

Virus qui se transforme (mute) dès qu'il passe par des fichiers hôtes. Le nettoyage d'un tel virus est un véritable défi.

NFS

Système de fichiers réseau (Network File System) utilisé par de nombreuses variantes d'UNIX.

NTFS

Système de fichiers de Windows NT.

Programme d'analyse lors de l'accès

Programme d'analyse en temps réel, dont le processus est en tâche de fond et qui procure une protection constante contre les virus.

Programme d'analyse à la demande

Programme de recherche de virus lancé manuellement.

RAM

Random Access Memory (mémoire vive). Mémoire dynamique utilisée par le processeur.

Programme d'analyse en temps réel

Programme d'analyse qui fonctionne en tâche de fond, permettant ainsi à l'utilisateur de continuer à travailler à une vitesse normale, sans ralentissement notable.

Réinitialiser

Amorcer le système à chaud.