McAfee®

VirusScan® 2008

Virus and Spyware Protection

Guide de l'utilisateur

Table des matières

CHAPITRE 1

McAfee VirusScan

VirusScan avec SiteAdvisor offre des services avancés de détection et de protection qui optimisent les défenses de votre ordinateur contre les menaces les plus récentes contre la sécurité : virus, chevaux de Troie, cookies de suivi, logiciels espions, logiciels publicitaires et autres programmes potentiellement indésirables. Avec VirusScan, la protection s'étend au-delà des fichiers et dossiers de votre ordinateur de bureau ou portable, pour contrer les menaces provenant de différents points d'entrée, dont le courrier électronique, la messagerie instantanée et le Web. Avec McAfee SiteAdvisor, des classifications de sécurité Internet vous permettent d'éviter les sites Web à risque.

Contenu de ce chapitre

CHAPITRE 2

McAfee SecurityCenter

McAfee SecurityCenter vous permet de surveiller l'état de la sécurité de votre ordinateur, de savoir instantanément si vos services de protection contre les virus, logiciels espions et messages électroniques et de protection par pare-feu sont à jour et d'agir sur certaines failles de sécurité. Il fournit les outils de navigation et commandes nécessaires et contrôle votre besoin de coordonner et gérer tous les secteurs de la protection de votre ordinateur.

Avant de commencer à configurer et gérer la protection de votre ordinateur, étudiez l'interface de SecurityCenter et veillez à bien distinguer état de protection, catégories de protection et services de protection. Ensuite, mettez à jour SecurityCenter pour disposer de la protection McAfee la plus récente disponible.

Après la configuration initiale, vous utilisez SecurityCenter pour surveiller l'état de protection de votre ordinateur. Si SecurityCenter détecte un problème de protection, il vous alerte pour que vous puissiez corriger ou ignorer le problème (selon sa gravité). Vous pouvez aussi analyser les événements liés à SecurityCenter, comme les changements de configuration de l'analyse antivirus, dans un journal des événements.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de SecurityCenter

SecurityCenter propose les fonctionnalités suivantes :

État de protection simplifié

Consultez facilement le niveau de protection de votre ordinateur, vérifiez la présence de mises à jour et réglez les problèmes de protection potentiels.

Mises à jour et mises à niveau automatisées

Téléchargez et installez automatiquement les mises à jour de vos programmes enregistrés. Lorsqu'une nouvelle version d'un programme McAfee enregistré est disponible, vous l'obtenez sans frais pendant toute la durée de votre abonnement. Vous bénéficiez ainsi d'une protection à jour en permanence.

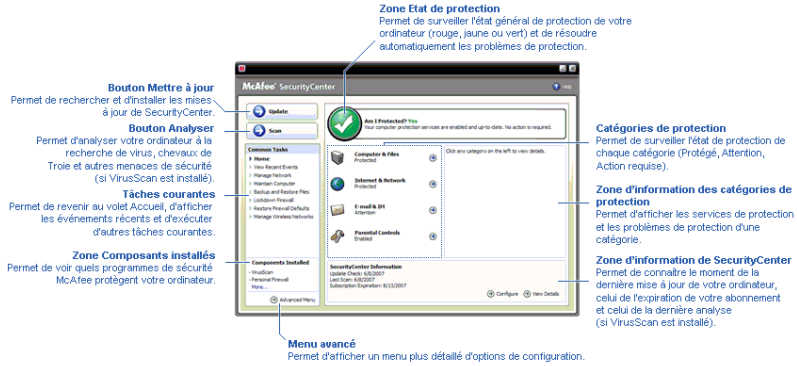
Alertes en temps réel

Les alertes de sécurité vous avertissent des nouvelles épidémies virales et des menaces de sécurité, et permettent de supprimer, neutraliser ou mieux connaître la menace.

CHAPITRE 3

Utilisation de SecurityCenter

Avant de commencer à utiliser SecurityCenter, passez en revue les composants et domaines de configuration que vous allez utiliser pour gérer l'état de protection de votre ordinateur. Pour plus d'informations sur la terminologie utilisée dans cette image, consultez Explications sur l'état de protection (page 8) et Explications sur les catégories de protection (page 9). Ensuite, vous pouvez contrôler les données de votre compte McAfee et vérifier la validité de votre abonnement.



Contenu de ce chapitre

Explications sur l'état de protection

L'état de protection de votre ordinateur s'affiche dans la zone d'état de protection dans le volet Accueil de SecurityCenter. Il indique si votre ordinateur est entièrement protégé contre les menaces les plus récentes et peut être influencé par des attaques externes, d'autres programmes de sécurité et des programmes accédant à Internet.

L'état de protection de votre ordinateur peut être rouge, jaune ou vert.

Etat de protection	Description
Rouge	Votre ordinateur n'est pas protégé. La zone d'état de protection du volet Accueil de SecurityCenter est rouge et indique que vous n'êtes pas protégé. SecurityCenter rapporte au moins un problème de sécurité critique. Pour obtenir une protection complète, vous devez corriger tous les problèmes de sécurité critiques dans chaque catégorie de protection (l'état de la catégorie de problèmes est mis à **Action requise**, également en rouge). Pour plus d'informations sur la correction des problèmes de protection, consultez Résolution des problèmes de protection (page 18).
Jaune	Votre ordinateur est partiellement protégé. La zone d'état de protection du volet Accueil de SecurityCenter est jaune et indique que vous n'êtes pas protégé. SecurityCenter rapporte au moins un problème de sécurité non critique. Pour obtenir une protection complète, vous devez corriger ou ignorer les problèmes de sécurité non critiques associés à chaque catégorie de protection. Pour plus d'informations sur la façon de corriger ou ignorer des problèmes de protection, consultez Résoudre ou ignorer des problèmes de protection (page 17).
Vert	Votre ordinateur est entièrement protégé. La zone d'état de protection du volet Accueil de SecurityCenter est verte et indique que vous êtes protégé. SecurityCenter ne rapporte aucun problème de sécurité, critique ou non critique. Chaque catégorie de protection énumère les services qui protègent votre ordinateur.

Explications sur les catégories de protection

Les services de protection de SecurityCenter sont divisés en quatre catégories : ordinateur & fichiers, internet & réseau, e-mail & messagerie instantanée et contrôle parental. Ces catégories vous aident à parcourir et configurer les services de sécurité qui protègent votre ordinateur.

Cliquez sur le nom d'une catégorie pour en configurer les services de protection et voir les problèmes de sécurité éventuels détectés pour ces services. Si l'état de protection de votre ordinateur est rouge ou jaune, une ou plusieurs catégories affichent un message *Action requise* ou *Attention*, indiquant que SecurityCenter a détecté un problème dans les catégories en question. Pour plus d'informations sur l'état de protection, consultez Explications sur l'état de protection (page 8).

Catégorie de protection	Description
Ordinateur & fichiers	La catégorie Ordinateur & fichiers permet de configurer les services de protection suivants : ▪ Protection antivirus ▪ Protection PUP ▪ Moniteurs système ▪ Protection Windows
Réseau & Internet	La catégorie Réseau & Internet permet de configurer les services de protection suivants : ▪ Protection par pare-feu ▪ Protection des données personnelles
E-mail & IM	La catégorie E-mail & IM permet de configurer les services de protection suivants : ▪ Protection des e-mails ▪ Protection antispam
Contrôle parental	La catégorie Contrôle parental permet de configurer les services de protection suivants : ▪ Blocage de contenu

Explications sur les services de protection

Les services de protection sont les composants essentiels de SecurityCenter que vous configurez pour protéger votre ordinateur. Les services de protection correspondent directement à des programmes McAfee. Par exemple, lorsque vous installez VirusScan, les services de protection suivants deviennent disponibles : Protection antivirus, Protection PUP, Moniteurs système et Protection Windows. Pour des informations détaillées sur ces services de protection particuliers, consultez l'aide de VirusScan.

Par défaut, tous les services de protection associés à un programme sont activés lorsque vous installez ce programme ; cependant, vous pouvez désactiver un service de protection à tout moment. Par exemple, si vous installez Privacy Service, les services Blocage de contenu et Protection des données personnelles sont tous deux activés. Si vous ne souhaitez pas utiliser le service de protection Blocage de contenu, vous pouvez le désactiver entièrement. Vous pouvez aussi désactiver temporairement un service de protection pendant des tâches de configuration ou de maintenance.

Gestion de votre compte McAfee

À partir de SecurityCenter, vous pouvez facilement accéder aux données de votre compte pour les consulter et vérifier l'état actuel de votre abonnement.

Remarque : Si vous avez installé vos programmes McAfee à partir d'un CD, vous devez les enregistrer sur le site Web de McAfee pour configurer ou mettre à jour votre compte McAfee. C'est indispensable pour pouvoir bénéficier des mises à jour régulières automatiques des programmes.

Gérer votre compte McAfee

Vous pouvez facilement accéder aux données de votre compte McAfee (Mon compte) à partir de SecurityCenter.

1. Sous **Tâches courantes**, cliquez sur **Mon compte**.
2. Connectez-vous à votre compte McAfee.

Vérifier votre abonnement

Vous pouvez vérifier votre abonnement pour vous assurer qu'il n'a pas encore expiré.

- Cliquez avec le bouton droit sur l'icône de SecurityCenter dans la zone de notification à l'extrême droite de la barre des tâches, puis cliquez sur **Vérifier l'abonnement**.

CHAPITRE 4

Mise à jour de SecurityCenter

SecurityCenter garantit la mise à jour permanente de vos programmes McAfee enregistrés en vérifiant toutes les quatre heures si des mises à jour sont disponibles en ligne et en les installant le cas échéant. Selon les programmes installés et enregistrés, les mises à jour en ligne peuvent inclure les définitions de virus les plus récentes ainsi que les mises à jour des protections contre les pirates, le spam et les logiciels espions et la protection de votre confidentialité. Si vous souhaitez vérifier l'existence de mises à jour avant l'échéance de l'intervalle par défaut, vous pouvez le faire à tout moment. Pendant que SecurityCenter recherche des mises à jour, vous pouvez continuer à travailler.

Bien que cela ne soit pas recommandé, vous pouvez modifier la façon dont SecurityCenter recherche et installe les mises à jour. Par exemple, vous pouvez configurer SecurityCenter pour qu'il télécharge les mises à jour sans les installer ou qu'il vous avertisse avant de télécharger ou d'installer des mises à jour. Vous pouvez aussi désactiver la mise à jour automatique.

Remarque : Si vous avez installé vos programmes McAfee à partir d'un CD, vous ne pourrez bénéficier des mises à jour régulières automatiques de ces programmes que lorsque vous les aurez enregistrés sur le site Web de McAfee.

Contenu de ce chapitre

Rechercher des mises à jour

Par défaut, SecurityCenter recherche automatiquement des mises à jour toutes les quatre heures lorsque votre ordinateur est connecté à Internet ; cependant, si vous souhaitez rechercher des mises à jour avant que les quatre heures soient écoulées, vous pouvez le faire. Si vous avez désactivé les mises à jour automatiques, il vous incombe de vérifier régulièrement si des mises à jour sont disponibles.

- Dans le volet Accueil de SecurityCenter, cliquez sur **Mettre à jour**.

Conseil : Vous pouvez rechercher des mises à jour sans lancer SecurityCenter en cliquant avec le bouton droit sur l'icône de SecurityCenter dans la zone de notification à l'extrême droite de la barre des tâches, puis en cliquant sur **Mises à jour**.

Configurer les mises à jour automatiques

Par défaut, SecurityCenter vérifie et installe automatiquement les mises à jour à intervalles de quatre heures lorsque vous êtes connecté à Internet. Si vous souhaitez modifier ce comportement par défaut, vous pouvez configurer SecurityCenter pour qu"il télécharge automatiquement les mises à jour puis vous avertisse lorsqu'elles sont prêtes à être installées ou pour qu'il vous avertisse avant de télécharger les mises à jour.

Remarque : SecurityCenter vous avertit par des alertes lorsque des mises à jour sont prêtes à être téléchargées ou installées. Ces alertes vous permettent de télécharger ou installer les mises à jour, ou de les postposer. Lorsque vous mettez à jour vos programmes à partir d'une alerte, vous serez peut-être invité à vérifier votre abonnement avant de télécharger et installer les mises à jour. Pour plus d'informations, consultez Utilisation des alertes (page 23).

1. Ouvrez le volet de configuration SecurityCenter.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.

2. Dans le volet Configuration de SecurityCenter, sous **Des mises à jour automatiques sont désactivées**, cliquez sur **Activé**, puis sur **Avancé**.
3. Selon le cas, cliquez sur l'un des boutons suivants :

   - **Installer automatiquement les mises à jour de mes services et m'avertir de l'opération une fois terminée (recommandé)**

- **Télécharger automatiquement les mises à jour et m'avertir de la possibilité de les installer**
- **M'avertir avant de télécharger une mise à jour**

4 Cliquez sur **OK**.

Désactiver les mises à jour automatiques

Si vous désactivez les mises à jour automatiques, il vous incombe de vérifier régulièrement si des mises à jour sont disponibles, faute de quoi votre ordinateur ne disposera pas de la protection la plus récente. Pour plus d'informations sur la recherche manuelle de mises à jour, consultez Rechercher des mises à jour (page 14).

1 Ouvrez le volet de configuration SecurityCenter.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.

2 Dans le volet Configuration de SecurityCenter, sous **Des mises à jour automatiques sont activées**, cliquez sur **Désactivé**.

Conseil : Pour activer les mises à jour automatiques, cliquez sur le bouton **Activé** ou désélectionnez **Désactiver les mises à jour automatiques et me laisser les vérifier manuellement** dans le volet Options de mise à jour.

CHAPITRE 5

Résoudre ou ignorer des problèmes de protection

SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Les problèmes de protection critiques exigent une action immédiate et compromettent votre état de protection (qui passe au rouge). Les problèmes de protection non critiques n'exigent pas d'action immédiate et peuvent ou non compromettre votre état de protection (selon le type de problème). Pour obtenir un état de protection vert, vous devez corriger tous les problèmes critiques et résoudre ou ignorer tous les problèmes non critiques. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician. Pour plus d'informations sur McAfee Virtual Technician, consultez l'aide de McAfee Virtual Technician.

Contenu de ce chapitre

Résolution des problèmes de protection

La plupart des problèmes de sécurité peuvent être corrigés automatiquement ; cependant, certains problèmes peuvent exiger une action de votre part. Par exemple, si le programme Protection par pare-feu est désactivé, SecurityCenter peut l'activer automatiquement ; en revanche, s'il n'est pas installé, c'est vous qui devez l'installer. Le tableau qui suit décrit certaines autres actions que vous pouvez entreprendre lors de la résolution manuelle de problèmes de protection :

Problème	Action
L'analyse complète de votre ordinateur n'a pas été exécutée depuis au moins 30 jours.	Analysez manuellement votre ordinateur. Pour plus d'informations, consultez l'aide de VirusScan.
Vos fichiers de signatures de détection ne sont pas à jour.	Actualisez manuellement votre protection. Pour plus d'informations, consultez l'aide de VirusScan.
Un programme n'est pas installé.	Installez le programme à partir du site Web ou du CD de McAfee.
Des composants d'un programme sont manquants.	Réinstallez le programme à partir du site Web ou du CD de McAfee.
Un programme n'est pas enregistré et ne peut pas bénéficier d'une protection complète.	Enregistrez le programme sur le site Web de McAfee.
Un programme a expiré.	Vérifiez l'état de votre compte sur le site Web de McAfee.

Remarque : Souvent, un même problème de protection affecte plusieurs catégories de protection. Dans ce cas, sa résolution dans une catégorie résout le problème dans toutes les autres catégories.

Résolution automatique des problèmes de protection

SecurityCenter peut résoudre automatiquement la plupart des problèmes de protection. Les changements de configuration effectués par SecurityCenter lors de la résolution automatique de problèmes de protection ne sont pas enregistrés dans le journal des événements. Pour plus d'informations sur les événements, consultez Affichage des événements (page 29).

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, dans la zone d'état de protection, cliquez sur **Corriger**.

Résolution manuelle des problèmes de protection

Si un ou plusieurs problèmes de protection persistent après une tentative de correction automatique, vous pouvez les résoudre manuellement.

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur la catégorie de protection où SecurityCenter a rapporté le problème.
3. Cliquez sur le lien qui suit la description du problème.

Ignorer des problèmes de protection

Si SecurityCenter détecte un problème non critique, vous pouvez le corriger ou l'ignorer. D'autres problèmes non critiques (par exemple, si Antispam ou Privacy Service ne sont pas installés) sont automatiquement ignorés. Les problèmes ignorés n'apparaissent dans la zone d'information des catégories de protection dans le volet Accueil de SecurityCenter que si l'état de protection de votre ordinateur est vert. Si vous ignorez un problème, mais décidez ensuite de l'afficher dans la zone d'information des catégories de problème alors que l'état de protection de votre ordinateur n'est pas vert, vous pouvez l'y faire apparaître.

Ignorer un problème de protection

Si SecurityCenter détecte un problème non critique que vous ne souhaitez pas corriger, vous pouvez l'ignorer. Un problème ignoré est supprimé de la zone d'information des catégories de protection dans SecurityCenter.

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur la catégorie de protection où est rapporté le problème.
3. Cliquez sur le lien **Ignorer** face au problème de protection.

Afficher ou masquer des problèmes ignorés

Selon sa gravité, vous pouvez afficher ou masquer un problème de protection ignoré.

1. Ouvrez le volet Options d'alerte.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
   3. Sous **Alertes**, cliquez sur **Avancé**.
2. Dans le volet Configuration de SecurityCenter, cliquez sur **Problèmes ignorés**.
3. Dans le volet Problèmes ignorés, effectuez l'une des opérations suivantes :
   - Pour ignorer un problème, activez sa case à cocher.
   - Pour faire apparaître un problème dans la zone d'information des catégories de protection, désactivez sa case à cocher.

4 Cliquez sur **OK**.

Conseil : Vous pouvez aussi ignorer un problème en cliquant sur le lien **Ignorer** face au problème en question dans la zone d'information des catégories de protection.

CHAPITRE 6

Utilisation des alertes

Les alertes sont des petites boîtes de dialogue en superposition qui apparaissent dans l'angle inférieur droit de l'écran lorsque certains événements se produisent dans SecurityCenter. Une alerte fournit des informations détaillées sur un événement ainsi que des recommandations et des options de résolution des problèmes éventuellement associés à l'événement. Certaines alertes contiennent également des liens vers des informations complémentaires sur l'événement. Ces liens permettent d'ouvrir le site Web global de McAfee ou d'envoyer des informations à McAfee à des fins de dépannage.

Il y a trois types d'alertes : rouge, jaune et verte.

Type d'alerte	Description
Rouge	Une alerte rouge constitue une indication critique qui nécessite une réponse de votre part. Elle se produit lorsque SecurityCenter ne peut pas déterminer comment résoudre automatiquement un problème de protection.
Jaune	Une alerte jaune constitue une indication non critique qui nécessite généralement une réponse de votre part.
Verte	Une alerte verte constitue une indication non critique qui ne nécessite pas de réponse de votre part. Les alertes vertes fournissent des informations de base sur un événement.

Les alertes jouent un rôle important dans la surveillance et la gestion de votre état de protection ; c'est pourquoi vous ne pouvez pas les désactiver. En revanche, vous pouvez définir si certains types d'alertes d'information doivent apparaître et configurer d'autres options d'alerte (par exemple l'émission ou non d'un son lorsque SecurityCenter produit une alerte ou l'affichage ou non de l'écran d'accueil de McAfee au démarrage).

Contenu de ce chapitre

Affichage et masquage d'alertes d'information

Les alertes d'information font état d'événements qui ne menacent pas la sécurité de l'ordinateur. Par exemple, si vous avez configuré la Protection par pare-feu, une alerte d'information s'affiche par défaut lorsqu'un programme installé sur votre ordinateur reçoit l'autorisation d'accéder à Internet. Si vous ne voulez pas afficher un type d'alerte d'information spécifique, vous pouvez la masquer. Si vous ne voulez afficher aucune alerte d'information, vous pouvez les masquer toutes. Vous pouvez aussi masquer toutes les alertes d'information lorsque vous jouez à un jeu en plein écran sur votre ordinateur. Lorsque vous avez terminé de jouer et quittez le mode plein écran, SecurityCenter recommence à afficher les alertes d'information.

Si vous masquez involontairement une alerte d'information, vous pouvez la réafficher à tout moment. Par défaut, SecurityCenter affiche toutes les alertes d'information.

Afficher ou masquer des alertes d'information

Vous pouvez configurer SecurityCenter pour qu'il affiche certaines alertes d'information et pas d'autres, ou pour qu'il masque toutes les alertes d'information.

1 Ouvrez le volet Options d'alerte.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
   3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Configuration de SecurityCenter, cliquez sur **Alertes d'information**.

3 Dans le volet Alertes d'information, effectuez l'une des opérations suivantes :

   - Pour afficher une alerte d'information, désactivez sa case à cocher.
   - Pour masquer une alerte d'information, activez sa case à cocher.
   - Pour masquer toutes les alertes d'information, activez la case à cocher **Ne pas afficher les alertes d'information**.

4 Cliquez sur **OK**.

Conseil : Vous pouvez également masquer une alerte d'information en activant la case **Ne plus afficher cette alerte** dans l'alerte même. Dans ce cas, vous pouvez réafficher l'alerte d'information en désactivant la case à cocher appropriée dans le volet Alertes d'information.

Afficher ou masquer des alertes d'information pendant un jeu

Vous pouvez masquer les alertes d'information lorsque vous jouez à un jeu en plein écran sur votre ordinateur. Lorsque vous avez terminé de jouer et quittez le mode plein écran, SecurityCenter recommence à afficher les alertes d'information.

1 Ouvrez le volet Options d'alerte.

   Comment ?

   1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
   2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
   3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Options d'alerte, activez ou désactivez la case **Afficher les alertes d'information en mode jeu**.

3 Cliquez sur **OK**.

Configuration des options d'alerte

L'apparence et la fréquence des alertes sont configurées par SecurityCenter ; cependant, vous pouvez régler certaines options de base des alertes. Par exemple, vous pouvez activer l'émission d'un son lorsqu'une alerte est produite ou masquer l'écran d'accueil au démarrage de Windows. Vous pouvez aussi masquer les alertes qui vous avertissent des épidémies virales et des autres menaces pour la sécurité dans la communauté en ligne.

Emettre un son en cas d'alerte

Si vous souhaitez recevoir une indication audible qu'une alerte s'est produite, vous pouvez configurer SecurityCenter pour qu'il produise un son à chaque alerte.

1 Ouvrez le volet Options d'alerte.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Options d'alerte, sous **Son**, activez la case à cocher **Emettre un son en cas d'alerte**.

Masquer l'écran d'accueil au démarrage

Par défaut, l'écran d'accueil de McAfee apparaît brièvement au démarrage de Windows, vous indiquant que SecurityCenter protège votre ordinateur. Cependant, vous pouvez masquer l'écran d'accueil si vous ne voulez pas qu'il apparaisse.

1 Ouvrez le volet Options d'alerte.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Options d'alerte, sous **Écran d'accueil**, désactivez la case à cocher **Afficher l'écran d'accueil McAfee au démarrage de Windows**.

Conseil : Vous pouvez réafficher l'écran d'accueil à tout moment en activant la case à cocher **Afficher l'écran d'accueil McAfee au démarrage de Windows**.

Masquer les alertes d'attaque virale

Vous pouvez masquer les alertes qui vous avertissent des épidémies virales et des autres menaces pour la sécurité dans la communauté en ligne.

1 Ouvrez le volet Options d'alerte.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet de droite, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
3. Sous **Alertes**, cliquez sur **Avancé**.

2 Dans le volet Options d'alerte, désactivez la case **M'avertir en cas d'apparition d'un virus ou d'une menace informatique**.

Conseil : Vous pouvez afficher les alertes d'attaque virale à tout moment en activant la case **M'avertir en cas d'apparition d'un virus ou d'une menace informatique**.

CHAPITRE 7

Affichage des événements

Un événement est une action ou un changement de configuration qui se produit dans une catégorie de protection et les services de protection correspondants. Différents services de protection enregistrent différents types d'événements. Par exemple, SecurityCenter enregistre un événement si un service de protection est activé ou désactivé ; Virus Protection enregistre un événement chaque fois qu'un virus est détecté et supprimé ; et Firewall Protection enregistre un événement chaque fois qu'une tentative de connexion à Internet est bloquée. Pour plus d'informations sur les catégories de protection, consultez Explications des catégories de protection (page 9).

Vous pouvez afficher les événements lorsque vous tentez de résoudre des problèmes de configuration et analysez les opérations effectuées par les autres utilisateurs. Nombre de parents utilisent le journal des événements pour surveiller le comportement de leurs enfants sur Internet. Vous affichez les événements récents si vous ne souhaitez examiner que les 30 derniers événements survenus. Vous affichez tous les événements si vous souhaitez examiner une liste complète des événements survenus. Lorsque vous visualisez tous les événements, SecurityCenter lance le journal des événements, qui trie les événements selon la catégorie de protection dans laquelle ils se sont produits.

Contenu de ce chapitre

Afficher les événements récents

Vous affichez les événements récents si vous ne souhaitez examiner que les 30 derniers événements survenus.

- Sous **Tâches courantes**, cliquez sur **Afficher les événements récents**.

Afficher tous les événements

Vous affichez tous les événements si vous souhaitez examiner une liste complète des événements survenus.

1. Sous **Tâches courantes**, cliquez sur **Afficher les événements récents**.
2. Dans le volet Evénements récents, cliquez sur **Afficher le fichier journal**.
3. Dans le volet gauche du journal des événements, cliquez sur le type d'événements à afficher.

CHAPITRE 8

McAfee VirusScan

VirusScan offre des services avancés de détection et de protection défendant votre ordinateur contre les menaces les plus récentes contre la sécurité : virus, chevaux de Troie, cookies de suivi, logiciels espions, logiciels publicitaires et autres programmes potentiellement indésirables. La protection s'étend au-delà des fichiers et dossiers de votre ordinateur de bureau, pour contrer les menaces provenant de différents points d'entrée, dont le courrier électronique, la messagerie instantanée et le Web.

Avec VirusScan, la protection de votre ordinateur est immédiate et constante (pas d'administration fastidieuse). Pendant que vous travaillez, jouez, naviguez sur le Web ou contrôlez votre courrier électronique, la protection s'exécute à l'arrière-plan pour surveiller, analyser et détecter des risques en temps réel. Des analyses complètes sont exécutées à intervalles programmés pour vérifier votre ordinateur avec un ensemble plus sophistiqué d'options. VirusScan vous offre la possibilité de personnaliser ce comportement si vous le souhaitez ; dans le cas contraire, votre ordinateur reste protégé.

Utilisé normalement, votre ordinateur est exposé aux virus, vers et autres menaces potentielles. Si une menace se présente, VirusScan vous en avertit, mais y fait normalement face pour vous en nettoyant ou en mettant en quarantaine les éléments infectés avant que votre ordinateur puisse subir un quelconque dommage. Dans de rare cas, une action complémentaire de votre part peut être exigée. Dans ces cas, VirusScan vous laisse décider que faire (réanalyser au prochain démarrage de l'ordinateur, conserver l'élément détecté ou le supprimer).

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de VirusScan

VirusScan propose les fonctionnalités suivantes.

Protection complète anti-virus

VirusScan offre des services avancés de détection et de protection défendant votre ordinateur contre les menaces les plus récentes contre la sécurité : virus, chevaux de Troie, cookies de suivi, logiciels espions, logiciels publicitaires et autres programmes potentiellement indésirables. La protection s'étend au-delà des fichiers et dossiers de votre ordinateur de bureau, pour contrer les menaces provenant de différents points d'entrée, dont le courrier électronique, la messagerie instantanée et le Web. Aucune administration fastidieuse.

Options d'analyse économes en ressources

Si l'analyse est lente, vous pouvez désactiver l'option afin de minimiser l'utilisation des ressources de l'ordinateur, mais sachez qu'une plus haute priorité sera accordée à la protection anti-virus qu'aux autres tâches. VirusScan vous offre la possibilité de personnaliser les options d'analyse en temps réel et manuelle si vous le souhaitez ; dans le cas contraire, votre ordinateur reste protégé.

Réparations automatiques

Si VirusScan détecte une menace lors d'une analyse en temps réel ou d'une analyse manuelle, il tente de la traiter automatiquement en fonction du type de menace. De cette façon, la plupart des menaces peuvent être détectées et neutralisées sans que vous deviez intervenir. Dans de rares cas, VirusScan ne pourra peut-être pas neutraliser lui-même une menace. Dans ces cas, VirusScan vous laisse décider que faire (réanalyser au prochain démarrage de l'ordinateur, conserver l'élément détecté ou le supprimer).

Suspension de tâches en mode plein écran

Lorsque vous regardez un film, jouez ou effectuez toute autre activité sur votre ordinateur qui occupe la totalité de l'écran, VirusScan suspend un certain nombre de tâches, y compris les mises à jour automatiques et les analyses manuelles.

Démarrage de la protection antivirus en temps réel

VirusScan offre deux types de protection antivirus : en temps réel et manuelle La protection antivirus en temps réel surveille en permanence votre ordinateur pour déceler toute activité virale, en analysant les fichiers chaque fois que vous ou votre ordinateur y accédez. La protection antivirus manuelle vous permet d'analyser des fichiers à la demande. Pour garantir que votre ordinateur reste protégé contre les menaces les plus récentes, laissez la protection antivirus en temps réel activée et programmez des analyses manuelles régulières plus complètes. Par défaut, VirusScan effectue une analyse programmée une fois par semaine. Pour en savoir plus sur l'analyse en temps réel et l'analyse manuelle, consultez Analyse de votre ordinateur (page 57).

Exceptionnellement, vous voudrez suspendre temporairement l'analyse en temps réel (par exemple, pour changer certaines options d'analyse ou résoudre un problème de performance). Lorsque la protection antivirus en temps réel est désactivée, votre ordinateur n'est pas protégé et votre état de protection SecurityCenter passe au rouge. Pour plus d'informations sur l'état de protection, consultez « Explications sur l'état de protection » dans l'aide de SecurityCenter.

Démarrer la protection antivirus en temps réel

Par défaut, la protection antivirus en temps réel est activée et protège votre ordinateur contre les virus, chevaux de Troie et autres menaces pour la sécurité. Si vous désactivez la protection antivirus en temps réel, vous devez la réactiver pour rester protégé.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

   Comment ?

   1. Dans le volet gauche, cliquez sur **Menu Avancé**.
   2. Cliquez sur **Configurer**.
   3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection anti-virus**, cliquez sur **Activé**.

Arrêter la protection antivirus en temps réel

Vous pouvez désactiver temporairement la protection antivirus en temps réel et spécifier quand elle doit reprendre. La protection peut être automatiquement réactivée après 15, 30, 45 ou 60 minutes, au redémarrage de l'ordinateur ou jamais.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection anti-virus**, cliquez sur **Désactivé**.

3 Dans la boîte de dialogue, sélectionnez l'option de reprise de l'analyse en temps réel.

4 Cliquez sur **OK**.

CHAPITRE 9

Démarrage de la protection supplémentaire

Outre la protection antivirus en temps réel, VirusScan offre une protection avancée contre les scripts, logiciels espions et les pièces jointes potentiellement nocives dans le courrier électronique et la messagerie instantanée. Par défaut, l'analyse de scripts, la protection contre les logiciels espions et la protection du courrier électronique et des messages instantanés sont activées et protègent votre ordinateur.

Analyse de scripts

L'analyse de scripts détecte les scripts potentiellement nocifs et les empêche de s'exécuter sur votre ordinateur. Elle surveille votre ordinateur pour déceler toute activité suspecte de scripts, comme les scripts qui créent, copient ou suppriment des fichiers ou qui ouvrent votre registre Windows, et vous avertit avant que votre ordinateur puisse subir un quelconque dommage.

Protection contre les logiciels espions

La protection contre les logiciels espions détecte les logiciels espions, logiciels publicitaires et autres applications potentiellement indésirables. Les logiciels espions sont des logiciels qui peuvent être installés à votre insu sur votre ordinateur pour surveiller votre comportement, collecter des informations personnelles et même interférer dans le contrôle de l'ordinateur en installant d'autres logiciels ou en redirigeant l'activité du navigateur.

Protection des e-mails

La protection des e-mails détecte toute activité suspecte dans les e-mails et les pièces jointes que vous envoyez et recevez.

Protection de la messagerie instantanée

La protection de la messagerie instantanée détecte des menaces potentielles pour la sécurité provenant de pièces jointes à des messages instantanés que vous recevez. Elle empêche aussi les programmes de messagerie instantanée de partager des informations personnelles.

Contenu de ce chapitre

Lancer l'analyse de scripts

Activez la protection par analyse de scripts pour détecter les scripts potentiellement nocifs et les empêcher de s'exécuter sur votre ordinateur. Cette protection vous avertit lorsqu'un script tente de créer, copier ou supprimer des fichiers sur votre ordinateur, ou d'effectuer des modifications dans le registre de Windows.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection des analyses de scripts**, cliquez sur **Activé**.

Remarque : Bien que vous puissiez désactiver l'analyse des scripts à tout moment, cela laisse l'ordinateur vulnérable aux scripts nuisibles.

Démarrer la protection contre les logiciels espions

Activez la protection contre les logiciels espions pour détecter et supprimer les logiciels espions et publicitaires ainsi que tout programme potentiellement indésirable qui collecte et transmet des informations à votre insu ou sans votre autorisation.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection des analyses de scripts**, cliquez sur **Activé**.

Remarque : Bien que vous puissiez désactiver la protection contre les logiciels espions à tout moment, cela laisse l'ordinateur vulnérable aux programmes potentiellement indésirables.

Démarrer la protection des e-mails

Activez la protection des e-mails pour détecter les vers ainsi que les menaces potentielles dans les messages électroniques sortants (SMTP) et entrants (POP3) et leurs pièces jointes.

1 Ouvrez le volet Configuration E-mail & IM.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.

2 Sous **Protection de la messagerie**, cliquez sur **Activé**.

Remarque : Bien que vous puissiez désactiver la protection des e-mails à tout moment, cela laisse l'ordinateur vulnérable aux menaces par e-mail.

Démarrer la protection de la messagerie instantanée

Activez la protection de la messagerie instantanée pour détecter les menaces pour la sécurité se cachant dans les pièces jointes aux messages instantanés.

1 Ouvrez le volet Configuration E-mail & IM.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.

2 Sous **Protection de la messagerie instantanée**, cliquez sur **Activé**.

Remarque : Bien que vous puissiez désactiver la protection de la messagerie instantanée à tout moment, cela laisse l'ordinateur vulnérable aux pièces jointes nuisibles des messages instantanés.

CHAPITRE 10

Configuration de la protection antivirus

VirusScan offre deux types de protection antivirus : en temps réel et manuelle La protection antivirus en temps réel analyse les fichiers à chaque fois que vous ou votre ordinateur y accédez. La protection antivirus manuelle vous permet d'analyser des fichiers à la demande. Vous pouvez définir différentes options pour chaque type de protection. Par exemple, puisque la protection en temps réel surveille en permanence votre ordinateur, vous pourriez sélectionner un certain ensemble d'options d'analyse de base et garder un choix d'options plus complet pour la protection manuelle à la demande.

Contenu de ce chapitre

Configuration des options d'analyse en temps réel

Lorsque vous activez la protection antivirus en temps réel, VirusScan utilise un ensemble d'options par défaut pour analyser les fichiers ; cependant, vous pouvez changer les options par défaut pour les adapter à vos besoins.

Pour changer les options d'analyse en temps réel, vous devez prendre des décisions concernant la cible des contrôles effectués par VirusScan, ainsi que l'emplacement et les types de fichiers analysés. Par exemple, vous pouvez déterminer si VirusScan doit vérifier les virus inconnus ou les cookies que les sites Web peuvent utiliser pour suivre vos activités, et s'il doit analyser les disques réseau mappés sur votre ordinateur ou uniquement les disques locaux. Vous pouvez aussi définir les types de fichiers à analyser (tous les fichiers ou uniquement les fichiers programmes et les documents, car c'est là que se trouvent la plupart des virus).

Lorsque vous changez les options d'analyse en temps réel, vous devez aussi spécifier s'il est important de protéger votre ordinateur contre les débordements de mémoire tampon. Une mémoire tampon est une section de mémoire utilisée pour stocker temporairement des informations. Les débordements de mémoire tampon peuvent survenir lorsque la masse d'informations que des processus ou programmes suspects stockent dans une mémoire tampon dépasse la capacité de la mémoire. Lorsque cela se produit, l'ordinateur devient plus vulnérable aux attaques.

Configurer les options d'analyse en temps réel

Vous configurez les options d'analyse en temps réel pour personnaliser la cible des contrôles effectués par VirusScan lors d'une analyse en temps réel, ainsi que l'emplacement et les types de fichiers à analyser. Les options comprennent l'analyse des virus inconnus et des cookies ainsi que la protection contre les débordements de mémoire tampon. Vous pouvez aussi configurer l'analyse en temps réel pour vérifier les disque réseau mappés sur votre ordinateur.

1 Ouvrez le volet Analyse en temps réel.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.

2 Spécifiez les options d'analyse en temps réel, puis cliquez sur **OK**.

Pour...	Opération à exécuter...
Détecter les virus inconnus et les nouvelles variantes de virus connus	Activez la case à cocher **Recherche heuristique de virus inconnus**.
Détecter les cookies	Activez la case à cocher **Rechercher et supprimer les cookies de suivi**.
Détecter les virus et autres menaces potentielles sur les disques connectés à votre réseau	Activez la case à cocher **Analyser les lecteurs réseau**.
Protéger votre ordinateur contre les débordements de mémoire tampon	Activez la case à cocher **Activer la protection contre le débordement de tampon**.
Préciser les types de fichiers à analyser	Cliquez sur **Tous les fichiers (recommandé)** ou sur **Fichiers programme et documents uniquement**.

Configuration des options d'analyse manuelle

La protection antivirus manuelle vous permet d'analyser des fichiers à la demande. Lorsque vous lancez une analyse manuelle, VirusScan cherche sur votre ordinateur les virus et autres éléments potentiellement nuisibles en utilisant une palette d'options d'analyse plus complète. Pour changer les options d'analyse manuelle, vous devez décider ce que VirusScan doit rechercher lors d'une analyse. Par exemple, vous pouvez déterminer si VirusScan doit rechercher les virus inconnus, les programmes potentiellement indésirables tels que les logiciels espions ou publicitaires, les programmes furtifs tels que les rootkits qui peuvent octroyer un accès non autorisé à votre ordinateur, et les cookies que les sites Web peuvent utiliser pour suivre vos activités. Vous devez aussi spécifier les types de fichiers à vérifier. Par exemple, vous pouvez spécifier si VirusScan doit vérifier tous les fichiers ou uniquement les fichiers programmes et les documents (car c'est là que se trouvent la plupart des virus). Vous pouvez aussi déterminer si l'analyse doit inclure les fichiers d'archive (par exemple les fichiers .zip).

Par défaut, VirusScan analyse tous les disques et dossiers de votre ordinateur chaque fois qu'il effectue une analyse manuelle ; vous pouvez cependant modifier les emplacements par défaut pour les adapter à vos besoins. Par exemple, vous pouvez limiter l'analyse aux fichiers système critiques, aux éléments placés sur votre bureau ou à ceux de votre dossier Program Files. À moins de vouloir lancer vous-même chaque analyse manuelle, vous pouvez programmer des analyses régulières. Les analyses programmées vérifient toujours la totalité de l'ordinateur avec les options d'analyse par défaut. Par défaut, VirusScan effectue une analyse programmée une fois par semaine.

Si vous trouvez que l'analyse est lente, vous pouvez envisager de désactiver l'option afin de minimiser l'utilisation des ressources de l'ordinateur, mais sachez qu'une plus haute priorité sera accordée à la protection antivirus qu'aux autres tâches.

Remarque : Lorsque vous regardez un film, jouez ou effectuez toute autre activité sur votre ordinateur qui occupe la totalité de l'écran, VirusScan suspend un certain nombre de tâches, y compris les mises à jour automatiques et les analyses manuelles.

Configurer les options d'analyse manuelle

Vous configurez les options d'analyse manuelle pour personnaliser la cible des contrôles effectués par VirusScan lors d'une analyse manuelle, ainsi que l'emplacement et les types de fichiers à analyser. Les options comprennent la recherche de virus inconnus, l'analyse des fichiers d'archive, la recherche de logiciels espions, de programmes potentiellement indésirables, de cookies de suivi, de rootkits et de programmes furtifs.

1 Ouvrez le volet Analyse manuelle.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.
5. Dans la fenêtre Protection antivirus, cliquez sur **Analyse manuelle**.

2 Spécifiez les options d'analyse manuelle, puis cliquez sur **OK**.

Pour...	Opération à exécuter...
Détecter les virus inconnus et les nouvelles variantes de virus connus	Activez la case à cocher **Recherche heuristique de virus inconnus**.
Détecter et supprimer les virus dans les fichiers .zip et autres fichiers d'archive	Activez la case à cocher **Analyse des fichiers .zip et autres fichiers d'archive**.
Détecter les logiciels espions, logiciels publicitaires et autres applications potentiellement indésirables.	Activez la case à cocher **Rechercher les logiciels espions et les programmes potentiellement indésirables**.
Détecter les cookies	Activez la case à cocher **Rechercher et supprimer les cookies de suivi**.
Détecter les rootkits et les programmes furtifs pouvant altérer et exploiter les fichiers système Windows existants	Activez la case à cocher **Rechercher les rootkits et autres programmes furtifs**.

Réduire l'utilisation du processeur pour les analyses tout en donnant une plus haute priorité aux autres tâches (comme la navigation Web ou l'ouverture de documents)	Activez la case à cocher **Analyser en utilisant un minimum de ressources informatiques**.
Préciser les types de fichiers à analyser	Cliquez sur **Tous les fichiers (recommandé)** ou sur **Fichiers programme et documents uniquement**.

Configurer l'emplacement de l'analyse manuelle

Vous définissez l'emplacement de l'analyse manuelle pour spécifier où VirusScan doit rechercher des virus et autres éléments nuisibles lors d'une analyse manuelle. Vous pouvez analyser tous les fichiers, dossiers et disques de votre ordinateur ou limiter l'analyse à des dossiers et disques spécifiques.

1 Ouvrez le volet Analyse manuelle.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.
5. Dans la fenêtre Protection antivirus, cliquez sur **Analyse manuelle**.

2 Cliquez sur **Emplacement par défaut à analyser**.

3 Spécifiez l'emplacement d'analyse manuelle, puis cliquez sur **OK**.

Pour...	Opération à exécuter...
Analyser tous les fichiers et dossiers de votre ordinateur	Activez la case à cocher **Poste de travail**.
Analyser des fichiers, dossiers et disques spécifiques sur votre ordinateur	Désactivez la case à cocher **Poste de travail** et sélectionnez un ou plusieurs dossiers ou disques.

Analyser les fichiers système critiques	Désactivez la case à cocher **Poste de travail** et activez la case à cocher **Fichiers système critiques**.

Programmer une analyse

Programmez des analyses pour procéder à une analyse approfondie de votre ordinateur à la recherche de virus et d'autres menaces à tout moment de la semaine. Les analyses programmées vérifient toujours la totalité de l'ordinateur avec les options d'analyse par défaut. Par défaut, VirusScan effectue une analyse programmée une fois par semaine. Si vous trouvez que l'analyse est lente, vous pouvez envisager de désactiver l'option afin de minimiser l'utilisation des ressources de l'ordinateur, mais sachez qu'une plus haute priorité sera accordée à la protection antivirus qu'aux autres tâches.

1 Ouvrez le volet Analyse programmée.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.
5. Dans le volet Protection antivirus, cliquez sur **Analyse programmée**.

2 Sélectionnez **Autoriser une analyse programmée**.

3 Pour réduire la puissance de calcul normalement utilisée pour une analyse, sélectionnez **Analyser en utilisant un minimum de ressources informatiques**.

4 Sélectionnez un ou plusieurs jours.

5 Spécifiez une heure de début.

6 Cliquez sur **OK**.

Conseil : Vous pouvez rétablir le programme par défaut en cliquant sur **Réinitialiser**.

Utilisation des options SystemGuards

SystemGuards permet de surveiller, consigner, rapporter et gérer les modifications potentiellement non autorisées apportées au registre de Windows ou à des fichiers système critiques sur votre ordinateur. Les modifications non autorisées apportées au registre et aux fichiers risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.

Les modifications du registre et des fichiers sont courantes et se produisent fréquemment sur votre ordinateur. La plupart de ces modifications étant inoffensives, les réglages par défaut de SystemGuards sont configurés pour offrir une protection fiable, intelligente et réaliste contre les modifications non autorisées présentant un risque significatif. Par exemple, lorsque SystemGuards détecte des changements inhabituels et présentant une menace potentiellement importante, cette activité est immédiatement signalée et consignée. Les modifications plus courantes mais constituant néanmoins un risque potentiel sont uniquement consignées. En revanche, la surveillance des changements standard à faible risque est désactivée par défaut. La technologie SystemGuards peut être configurée pour étendre sa protection à tout environnement que vous souhaitez.

Il y a trois types de SystemGuards : SystemGuards Programme, SystemGuards Windows et SystemGuards Navigateur.

SystemGuard Programme

Les SystemGuards Programme détectent les modifications potentiellement non autorisées apportées au registre de votre ordinateur et à d'autres fichiers critiques essentiels pour Windows. Ces éléments du registre et fichiers importants comprennent les installations ActiveX, les éléments de démarrage, les shell execute hooks de Windows et les shell service object delay loads. En surveillant ces éléments, la technologie SystemGuards Programme bloque les programmes ActiveX suspects (téléchargés depuis Internet) en plus des logiciels espions et des applications potentiellement indésirables pouvant se lancer automatiquement au démarrage de Windows.

SystemGuards Windows

Les SystemGuards Windows détectent aussi les modifications potentiellement non autorisées apportées au registre de votre ordinateur et à d'autres fichiers critiques essentiels pour Windows. Ces éléments du registre et fichiers importants comprennent les gestionnaires de menus contextuels, les DLL appInit et le fichier hosts Windows. En surveillant ces éléments, la technologie SystemGuards Windows vous aide à éviter que votre ordinateur envoie et reçoive des informations non autorisées ou personnelles via Internet. Elle peut aussi aider à bloquer les programmes suspects pouvant modifier l'apparence et le comportement des programmes importants pour vous et votre famille.

SystemGuard Navigateur

Comme les SystemGuards Programme et Windows, les SystemGuards Navigateur détectent les modifications potentiellement non autorisées apportées au registre de votre ordinateur et à d'autres fichiers critiques essentiels pour Windows. Ces SystemGuards surveillent cependant les modifications apportées à des éléments du registre et fichiers importants tels que les extensions pour Internet Explorer, les URL Internet Explorer et les zones de sécurité Internet Explorer. En surveillant ces éléments, la technologie SystemGuards Navigateur aide à empêcher les activités non autorisées dans le navigateur, comme la redirection vers des sites Web suspects, les modifications des paramètres et options du navigateur à votre insu, et l'approbation indésirable de sites Web suspects.

Activer la protection SystemGuards

Activez la protection SystemGuards pour détecter et signaler les modifications potentiellement non autorisées du registre Windows et des fichiers système sur votre ordinateur. Les modifications non autorisées apportées au registre et aux fichiers risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.

1 Ouvrez le volet Configuration Ordinateur & fichiers.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans la fenêtre de configuration, cliquez sur **Ordinateur & fichiers**.

2 Sous **Protection SystemGuard**, cliquez sur **Activé**.

Remarque : Vous pouvez désactiver la protection SystemGuards en cliquant sur **Désactivé**.

Configuration des options SystemGuards

Utilisez le volet SystemGuards pour configurer les options de protection, consignation et alerte contre les modifications non autorisées du registre et des fichiers liées aux fichiers et programmes Windows ainsi qu'à Internet Explorer. Les modifications non autorisées apportées au registre et aux fichiers risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.

1 Ouvrez le volet SystemGuards.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection SystemGuard est activée, puis cliquez sur **Avancé**.

2 Sélectionnez un type de protection SystemGuards dans la liste.

- **SystemGuard Programme**
- **SystemGuards Windows**
- **SystemGuard Navigateur**

3 Sous **Je souhaite**, effectuez l'une des actions suivantes :

- Pour détecter, consigner et signaler les modifications non autorisées du registre et des fichiers liées aux SystemGuards Programme, Windows et Navigateur, cliquez sur **Afficher les alertes.**
- Pour détecter et consigner les modifications non autorisées du registre et des fichiers liées aux SystemGuards Programme, Windows et Navigateur, cliquez sur **Consigner uniquement les modifications.**
- Pour désactiver la détection de modifications non autorisées du registre et des fichiers liées aux SystemGuards Programme, Windows et Navigateur, cliquez sur **Désactiver SystemGuard.**

Remarque : Pour plus d'informations sur les types de SystemGuards, consultez À propos des types de SystemGuards (page 49).

À propos des types de SystemGuards

Les SystemGuards détectent les modifications potentiellement non autorisées apportées au registre de votre ordinateur et à d'autres fichiers critiques essentiels pour Windows. Il y a trois types de SystemGuards : SystemGuards Programme, SystemGuards Windows et SystemGuards Navigateur

SystemGuard Programme

La technologie SystemGuards Programme bloque les programmes ActiveX suspects (téléchargés depuis Internet) en plus des logiciels espions et des applications potentiellement indésirables pouvant se lancer automatiquement au démarrage de Windows.

SystemGuard	Détection
Installations ActiveX	Les modifications non autorisées apportées au registre des installations ActiveX risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.
Éléments de démarrage	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant apporter des modifications de fichiers dans les éléments de démarrage pour permettre à des programmes suspects de s'exécuter au démarrage de votre ordinateur.
Shell Execute Hooks de Windows	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant installer des programmes dans le Shell Windows (Shell Execute Hooks) pour empêcher le bon fonctionnement des programmes de sécurité.
Shell Service Object Delay Load	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant apporter des modification de registre à la charge de retard de l'objet de service du Shell pour permettre à des fichiers nuisibles de s'exécuter au démarrage de votre ordinateur.

SystemGuards Windows

La technologie SystemGuards Windows vous aide à éviter que votre ordinateur envoie et reçoive des informations non autorisées ou personnelles via Internet. Elle peut aussi aider à bloquer les programmes suspects pouvant modifier l'apparence et le comportement des programmes importants pour vous et votre famille.

SystemGuard	Détection
Gestionnaires de menus contextuels	Modifications de registre non autorisées apportées aux gestionnaires de menus contextuels et pouvant affecter l'apparence et le comportement des menus Windows. Les menus contextuels permettent d'effectuer diverses actions sur votre ordinateur, comme un clic droit sur un fichier.
DLL AppInit	Modifications de registre non autorisées apportées aux DLL AppInit de Windows et pouvant entraîner l'exécution de fichiers potentiellement nuisibles au démarrage de votre ordinateur.
Fichier Hosts Windows	Logiciels espions, publicitaires et programmes potentiellement indésirables pouvant apporter des modifications non autorisées à votre fichier Hosts Windows pour permettre la redirection de votre navigateur vers des sites Web suspects et bloquer les mises à jour de logiciels.
Shell Winlogon	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre du Shell Winlogon pour permettre à d'autres programmes de se substituer à l'Explorateur Windows.
Clé UserInit de Winlogon	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre de Winlogon User Init pour permettre à des programmes suspects de s'exécuter lorsque vous vous connectez à Windows.
Protocoles Windows	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre des protocoles Windows et affecter ainsi la manière dont votre ordinateur envoie et reçoit des informations sur Internet.
Fournisseurs de services en couche (Layered Service Providers ou LSP) Winsock	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre des fournisseurs de services en couche (Winsock Layered Service Providers - LSP) pour intercepter et modifier les informations envoyées et reçues sur Internet.

Commandes Open Shell Windows	Modifications non autorisées aux commandes Open Shell de Windows pouvant entraîner l'exécution de vers ou d'autres programmes nuisibles sur votre ordinateur.
Gestionnaire de tâches programmées	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant apporter des modifications au registre et aux fichiers du gestionnaire de tâches partagées pour autoriser des fichiers nuisibles à s'exécuter au démarrage de votre ordinateur.
Windows Messenger Service	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre de Windows Messenger Service et ouvrir la voie aux publicités intempestives et aux programmes exécutés à distance.
Fichier Windows Win.ini	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le fichier Win.ini et permettre à des programmes suspects de s'exécuter au démarrage de votre ordinateur.

SystemGuard Navigateur

La technologie SystemGuards Navigateur aide à empêcher les activités non autorisées dans le navigateur, comme la redirection vers des sites Web suspects, les modifications des paramètres et options du navigateur à votre insu, et l'approbation indésirable de sites Web suspects.

SystemGuard	Détection
Browser Helper Objects (BHO)	Logiciels espions, publicitaires ou autres programmes potentiellement indésirables pouvant utiliser les "browser helper objects" pour suivre les actions de navigation et afficher des publicités de manière intempestive.
Barres Internet Explorer	Modifications non autorisées apportées au registre des programmes de la barre Internet Explorer, tels que Rechercher et Favoris, pouvant affecter l'apparence et le comportement d'Internet Explorer.
Modules Internet Explorer complémentaires	Logiciels espions, publicitaires ou autres programmes potentiellement indésirables pouvant installer des modules Internet Explorer complémentaires pour suivre les actions de navigation et afficher des publicités de manière intempestive.
ShellBrowser Internet Explorer	Modifications non autorisées apportées au registre du ShellBrowser Internet Explorer et pouvant affecter l'apparence et le comportement de votre navigateur Web.

WebBrowser Internet Explorer	Modifications non autorisées apportées au registre du navigateur Web Internet Explorer et pouvant affecter l'apparence et le comportement de votre navigateur Web.
URL Search Hooks Internet Explorer	Logiciels espions, publicitaires ou programmes potentiellement indésirables pouvant modifier le registre des "Internet Explorer URL Search Hooks" et autoriser ainsi la redirection de votre navigateur vers des sites Web suspects lorsque vous effectuez des recherches sur Internet.
URL Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement nuisibles pouvant modifier le registre des URL d'Internet Explorer et affecter ainsi les paramètres du navigateur.
Restrictions Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement nuisibles pouvant modifier le registre des restrictions d'Internet Explorer et affecter ainsi les paramètres et options du navigateur.
Zones de sécurité Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre des zones de sécurité d'Internet Explorer et permettre à des fichiers nuisibles de s'exécuter au démarrage de votre ordinateur.
Sites de confiance d'Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement indésirables pouvant modifier le registre des sites autorisés d'Internet Explorer pour permettre à votre navigateur d'afficher des sites Web suspects.
Stratégie Internet Explorer	Logiciels espions, publicitaires et autres programmes potentiellement nuisibles pouvant modifier le registre des stratégies d'Internet Explorer et affecter ainsi l'apparence et le comportement du navigateur.

Utilisation des listes approuvées

Si VirusScan détecte une modification de fichier ou de registre (SystemGuard), un programme suspect ou un débordement de mémoire tampon, il vous invite à l'approuver ou à le supprimer. Si vous approuvez l'élément et indiquez que vous ne voulez plus être alerté de son activité, l'élément est ajouté à une liste approuvée et VirusScan ne le détecte plus ou ne vous avertit plus de son activité. Si un élément a été ajouté à une liste approuvée, mais que vous décidez d'en bloquer les activités, vous pouvez le faire. Le blocage de l'élément l'empêche de s'exécuter ou de modifier votre ordinateur sans que vous soyez averti de chaque tentative. Vous pouvez aussi supprimer un élément d'une liste approuvée. La suppression d'un élément permet à VirusScan de détecter à nouveau les activités de cet élément.

Gestion des listes approuvées.

Utilisez le volet Listes approuvées pour approuver ou bloquer des éléments qui ont été précédemment détectés et approuvés. Vous pouvez aussi supprimer un élément d'une liste approuvée afin que VirusScan le détecte à nouveau.

1 Ouvrez le volet Listes approuvées.

Comment ?

1. Sous **Tâches courantes**, cliquez sur **Page d'accueil**.
2. Dans le volet Accueil de SecurityCenter, cliquez sur **Ordinateur & fichiers**.
3. Dans la zone d'informations Ordinateurs & Fichiers, cliquez sur **Configurer**.
4. Dans le volet Configuration Ordinateur & fichiers, vérifiez que la protection antivirus est activée, puis cliquez sur **Avancé**.
5. Dans le volet Protection antivirus, cliquez sur **Listes approuvées**.

2 Sélectionnez un des types de listes approuvées suivants :

- **SystemGuard Programme**
- **SystemGuards Windows**
- **SystemGuard Navigateur**
- **Programmes autorisés**
- **Débordements de mémoire tampon approuvés**

3 Sous **Je souhaite**, effectuez l'une des actions suivantes :

- Pour autoriser l'élément détecté à modifier le registre de Windows ou des fichiers système critiques sur votre ordinateur sans que vous en soyez averti, cliquez sur **Autoriser**.

- Pour bloquer l'élément détecté et l'empêcher de modifier le registre de Windows ou des fichiers système critiques sur votre ordinateur sans que vous en soyez averti, cliquez sur **Bloquer**.
- Pour supprimer l'élément des listes approuvées, cliquez sur **Supprimer**.

4 Cliquez sur **OK**.

Remarque : Pour plus d'informations sur les types de listes approuvées, consultez À propos des types de listes approuvées (page 54).

À propos des types de listes approuvées

Les SystemGuards dans le volet Listes approuvées représentent des modifications non autorisées au registre et aux fichiers que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Il y a cinq types de listes approuvées que vous pouvez gérer dans le volet Listes approuvées : SystemGuards Programme, SystemGuards Windows, SystemGuards Navigateur, Programmes approuvés et Débordements de mémoire tampon approuvés.

Option	Description
SystemGuard Programme	Les SystemGuards Programme dans le volet Listes approuvées représentent des modifications non autorisées au registre et aux fichiers que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Les SystemGuards Programme détectent les modifications du registre et des fichiers système associées aux installations ActiveX, éléments de démarrage, shell execute hooks de Windows et shell service object delay loads. Ces types de modifications non autorisées du registre et des fichiers système risquent de nuire à votre ordinateur, de compromettre la sécurité informatique et d'endommager de précieux fichiers système.

SystemGuards Windows	Les SystemGuards Windows dans le volet Listes approuvées représentent des modifications non autorisées au registre et aux fichiers que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Les SystemGuards Windows détectent les les modifications du registre et des fichiers système associées aux gestionnaires de menus contextuels, aux DLL appInit, au fichier Hosts de Windows, au shell Winlogon, aux Winsock Layered Service Providers (LSP), etc. Ces types de modifications non autorisées du registre et des fichiers système peuvent affecter la façon dont votre ordinateur envoie et reçoit des informations via Internet, changer l'apparence et le comportement de programmes et autoriser des programmes suspects à s'exécuter sur votre ordinateur.
SystemGuard Navigateur	Les SystemGuards Navigateur dans le volet Listes approuvées représentent des modifications non autorisées au registre et aux fichiers que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Les SystemGuards Navigateur détectent les modifications non autorisées du registre et autres comportements indésirables associés aux Browser Helper Objects, aux extensions Internet Explorer, aux URL Internet Explorer, aux zones de sécurité Internet Explorer, etc. Ces types de modifications non autorisées peuvent entraîner des activités indésirables dans le navigateur, comme la redirection vers des sites Web suspects, les modifications des paramètres et options du navigateur, et l'approbation de sites Web suspects.
Programmes autorisés	Les programmes approuvés sont des programmes potentiellement indésirables que VirusScan a détectés précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse.

Débordements de mémoire tampon approuvés	Les débordements de mémoire tampon approuvés représentent des activités indésirables que VirusScan a détectées précédemment, mais que vous avez choisi d'autoriser à partir d'une alerte ou du volet Résultats de l'analyse. Les débordements de mémoire tampon peuvent nuire à votre ordinateur et endommager des fichiers. Les débordements de mémoire tampon surviennent lorsque la masse d'informations que des processus ou programmes suspects stockent dans une mémoire tampon dépasse la capacité de la mémoire.

CHAPITRE 11

Analyse de votre ordinateur

Lorsque vous lancez SecurityCenter pour la première fois, la protection antivirus en temps réel de VirusScan commence à protéger votre ordinateur contre les virus, chevaux de Troie et autres menaces potentiellement nuisibles. À moins que vous désactiviez la protection antivirus en temps réel, VirusScan surveille en permanence votre ordinateur pour déceler toute activité virale, en analysant les fichiers chaque fois que vous ou votre ordinateur y accédez, en utilisant les options d'analyse en temps réel que vous avez définies. Pour garantir que votre ordinateur reste protégé contre les menaces les plus récentes, laissez la protection antivirus en temps réel activée et programmez des analyses manuelles régulières plus complètes. Pour en savoir plus sur la configuration des options d'analyse en temps réel et d'analyse manuelle, consultez Configuration de la protection antivirus (page 39).

VirusScan offre une palette plus détaillée d'options d'analyse pour la protection antivirus manuelle, vous permettant ainsi d'exécuter périodiquement des analyses plus poussées. Vous pouvez lancer des analyses manuelles à partir de SecurityCenter, en ciblant des emplacement spécifiques selon un programme défini. Cependant, vous pouvez aussi exécuter des analyses manuelles en cours de travail directement dans l'Explorateur Windows. L'analyse dans SecurityCenter offre l'avantage de permettre de changer les options d'analyse sur le moment. L'analyse à partir de l'Explorateur Windows, en revanche, offre une approche pratique de la sécurité informatique.

Que vous lanciez une analyse manuelle à partir de SecurityCenter ou de l'Explorateur Windows, vous pouvez consulter les résultats de l'analyse une fois celle-ci terminée. Vous pouvez consulter les résultats d'une analyse pour déterminer si VirusScan a détecté, réparé ou mis en quarantaine des virus, chevaux de Troie, logiciels espions, logiciels publicitaires, cookies et autres programmes potentiellement indésirables. Les résultats d'une analyse peuvent s'afficher de différentes manières. Par exemple, vous pouvez afficher un résumé des résultats ou des informations détaillées telles que le statut et le type de l'infection. Vous pouvez aussi afficher des statistiques générales d'analyse et de détection.

Contenu de ce chapitre

Analyser votre ordinateur

Vous pouvez exécuter une analyse manuelle à partir du menu Avancé ou du menu de base de SecurityCenter. Si vous lancez une analyse à partir du menu Avancé, vous pouvez confirmer les options d'analyse manuelle avant de commencer. Si vous lancez une analyse à partir du menu de base, VirusScan lance immédiatement l'analyse, en utilisant les options d'analyse existantes. Vous pouvez aussi exécuter une analyse dans l'Explorateur Windows en utilisant les options d'analyse existantes.

- Effectuez l'une des opérations suivantes :

  Analyser dans SecurityCenter

Pour...	Opération à exécuter...
Analyser avec les paramètres existants	Cliquez sur **Analyser** dans le menu de base.
Analyser avec des paramètres différents	Cliquez sur **Analyser** dans le menu Avancé, sélectionnez les emplacements à analyser, sélectionnez les options d'analyse et cliquez sur **Analyser maintenant**.

  Analyser dans l'Explorateur Windows

  1. Ouvrez l'Explorateur Windows.
  2. Cliquez avec le bouton droit sur un fichier, dossier ou disque, puis cliquez sur **Analyser**.

Remarque : Les résultats d'analyse apparaissent dans l'alerte Analyse terminée. Ces résultats comprennent le nombre d'éléments analysés, détectés, réparés, mis en quarantaine et supprimés. Cliquez sur **Afficher les détails de l'analyse** pour en savoir plus sur les résultats d'analyse ou gérer les éléments infectés.

Afficher les résultats de l'analyse

Lorsqu'une analyse manuelle se termine, vous pouvez en afficher les résultats pour déterminer ce que l'analyse a décelé et connaître l'état de protection actuel de votre ordinateur. Les résultats d'analyse indiquent si VirusScan a détecté, réparé ou mis en quarantaine des virus, chevaux de Troie, logiciels espions, logiciels publicitaires, cookies et autres programmes potentiellement indésirables.

- Dans le menu de base ou le menu avancé, cliquez sur **Analyser**, puis effectuez l'une des opérations suivantes :

Pour...	Opération à exécuter...
Afficher les résultats d'analyse dans l'alerte	Affichez les résultats d'analyse dans l'alerte Analyse terminée.
Afficher davantage d'informations sur les résultats d'analyse	Cliquez sur **Afficher les détails de l'analyse** dans l'alerte Analyse terminée.
Afficher un bref résumé des résultats d'analyse	Pointez sur l'icône **Analyse terminée** dans la zone de notification de votre barre des tâches.
Afficher des statistiques d'analyse et de détection	Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification de votre barre des tâches.
Afficher des détails sur les éléments détectés, l'état d'infection et le type d'infection.	Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification de votre barre des tâches, puis cliquez sur **Afficher les résultats** dans le volet Progression de l'analyse : Analyse manuelle.

CHAPITRE 12

Exploitation des résultats d'analyse

Si VirusScan détecte une menace lors d'une analyse en temps réel ou d'une analyse manuelle, il tente de la traiter automatiquement en fonction du type de menace. Par exemple, si VirusScan détecte un virus, un cheval de Troie ou un cookie de suivi sur votre ordinateur, il tente de nettoyer le fichier infecté. S'il n'y parvient pas, il le met en quarantaine.

Pour certaines menaces, il se peut que VirusScan ne réussisse pas à nettoyer ni à mettre en quarantaine un fichier. Dans ce cas, VirusScan vous invite à gérer la menace en question. Vous avez le choix entre différentes actions selon le type de menace. Par exemple, si un virus est détecté dans un fichier, mais que VirusScan ne parvient pas à nettoyer ce fichier ni à le mettre en quarantaine, il y refuse tout accès. Si des cookies de suivi sont détectés, mais que VirusScan ne réussit pas à nettoyer ou mettre en quarantaine les cookies, vous pouvez décider de les supprimer ou de les autoriser. Si des programmes potentiellement indésirables sont détectés, VirusScan n'effectue aucune action automatique ; il vous laisse décider de les mettre en quarantaine ou de les autoriser.

Lorsque VirusScan met des éléments en quarantaine, il les chiffre et les isole dans un dossier pour empêcher les fichiers, programmes ou cookies de nuire à votre ordinateur. Vous pouvez restaurer ou supprimer les éléments mis en quarantaine. Dans la plupart des cas, vous pouvez supprimer un cookie en quarantaine sans affecter votre système ; en revanche, si VirusScan a mis en quarantaine un programme que vous connaissez et utilisez, envisagez de le restaurer.

Contenu de ce chapitre

Gérer les virus et chevaux de Troie

Si VirusScan détecte un virus ou un cheval de Troie sur votre ordinateur lors d'une analyse en temps réel ou d'une analyse manuelle, il tente de nettoyer le fichier. S'il n'y parvient pas, VirusScan tente de le mettre en quarantaine. Si cette tentative échoue également, il bloque l'accès au fichier (uniquement lors d'une analyse en temps réel).

1 Ouvrez le volet Résultats de l'analyse.

   Comment ?

   1. Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification à l'extrême droite de votre barre des tâches.
   2. Dans le volet Progression de l'analyse : Analyse manuelle, cliquez sur **Afficher les résultats**.

2 Dans la liste des résultats d'analyse, cliquez sur **Virus et chevaux de Troie**.

Remarque : Pour gérer les fichiers mis en quarantaine par VirusScan, consultez Gérer les fichiers mis en quarantaine (page 63).

Gérer les programmes potentiellement indésirables

Si VirusScan détecte un programme potentiellement indésirable sur votre ordinateur lors d'une analyse en temps réel ou manuelle, vous avez le choix de supprimer ou d'autoriser le programme. La suppression du programme potentiellement indésirable ne l'efface pas de votre système. Elle met le programme en quarantaine pour l'empêcher d'endommager votre ordinateur ou vos fichiers.

1 Ouvrez le volet Résultats de l'analyse.

   Comment ?

   1. Double-cliquez sur l'icône **Analyse terminée** dans la zone de notification à l'extrême droite de votre barre des tâches.
   2. Dans le volet Progression de l'analyse : Analyse manuelle, cliquez sur **Afficher les résultats**.

2 Dans la liste des résultats d'analyse, cliquez sur **Programmes potentiellement indésirables**.

3 Sélectionnez un programme potentiellement indésirable.

4 Sous **Je souhaite**, cliquez sur **Supprimer** ou **Autoriser**.

5 Confirmez votre choix.

Gérer des fichiers en quarantaine

Lorsque VirusScan met en quarantaine des fichiers infectés, il les chiffre et les isole dans un dossier pour empêcher les fichiers de nuire à votre ordinateur. Vous pouvez ensuite choisir de restaurer ou de supprimer les fichiers en quarantaine.

1 Ouvrez le volet Fichiers mis en quarantaine.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Restaurer**.
3. Cliquez sur **Fichiers**.

2 Sélectionnez un fichier en quarantaine.

3 Effectuez l'une des opérations suivantes :

- Pour réparer le fichier infecté et le remettre à son emplacement d'origine sur votre ordinateur, cliquez sur **Restaurer**.
- Pour supprimer le fichier infecté de votre ordinateur, cliquez sur **Supprimer**.

4 Cliquez sur **Oui** pour confirmer votre choix.

Conseil : Vous pouvez restaurer ou supprimer plusieurs fichiers à la fois.

Gérer des programmes et cookies en quarantaine

Lorsque VirusScan met en quarantaine des programmes potentiellement indésirables ou des cookies de suivi, il les chiffre et les isole dans un dossier protégé pour empêcher ces programmes ou cookies de nuire à votre ordinateur. Vous pouvez ensuite choisir de restaurer ou de supprimer les éléments mis en quarantaine. Le plus souvent, vous pouvez supprimer un élément en quarantaine sans affecter votre système.

1 Ouvrez le volet Programmes mis en quarantaine et cookies de suivi.

Comment ?

1. Dans le volet gauche, cliquez sur **Menu Avancé**.
2. Cliquez sur **Restaurer**.
3. Cliquez sur **Programmes et cookies**.

2 Sélectionnez un programme ou cookie en quarantaine.

3 Effectuez l'une des opérations suivantes :

- Pour réparer le fichier infecté et le remettre à son emplacement d'origine sur votre ordinateur, cliquez sur **Restaurer**.
- Pour supprimer le fichier infecté de votre ordinateur, cliquez sur **Supprimer**.

4 Cliquez sur **Oui** pour confirmer l'opération.

Conseil : Vous pouvez restaurer ou supprimer plusieurs programmes et cookies à la fois.

CHAPITRE 13

McAfee QuickClean

QuickClean améliore les performances de votre ordinateur en supprimant des fichiers qui peuvent l'encombrer. Il vide votre Corbeille et supprime les fichiers temporaires, raccourcis, fragments de fichiers perdus, fichiers de registre, fichiers en mémoire cache, cookies, fichiers d'historique du navigateur, messages envoyés et supprimés, fichiers récemment utilisés, fichiers Active-X et fichiers de point de restauration système. QuickClean protège également votre confidentialité en utilisant le composant McAfee Shredder pour supprimer en toute sécurité et de manière définitive des éléments pouvant contenir des informations personnelles confidentielles telles que vos nom et adresse. Pour des informations sur le broyage de fichiers, voir McAfee Shredder.

Defragmenteur de disques organise les fichiers et dossiers de votre ordinateur de manière à éviter leur éparpillement (fragmentation) lors de leur enregistrement sur le disque dur de votre ordinateur. En défragmentant périodiquement votre disque dur, vous garantissez le regroupement des fichiers et dossiers fragmentés, ce qui permet de les récupérer plus rapidement ensuite.

Si vous ne souhaitez pas effectuer manuellement la maintenant de votre ordinateur, vous pouvez demander l'exécution automatique programmée de QuickClean et Défragmenteur de disques, indépendamment et à la fréquence de votre choix.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de QuickClean

QuickClean fournit différents outils de nettoyage qui suppriment les fichiers inutiles de manière sûre et efficace. En supprimant ces fichiers, vous augmentez l'espace disponible sur le disque dur de votre ordinateur et en améliorez les performances.

Nettoyage de votre ordinateur

QuickClean supprime les fichiers susceptibles d'encombrer votre ordinateur. Il vide votre Corbeille et supprime les fichiers temporaires, raccourcis, fragments de fichiers perdus, fichiers de registre, fichiers en mémoire cache, cookies, fichiers d'historique du navigateur, messages envoyés et supprimés, fichiers récemment utilisés, fichiers Active-X et fichiers de point de restauration système. QuickClean supprime ces éléments sans toucher aux autres informations essentielles.

Vous pouvez utiliser les nettoyeurs de QuickClean pour supprimer des fichiers inutiles de votre ordinateur. Le tableau suivant décrit les nettoyeurs QuickClean :

Nom	Fonction
Nettoyeur de la Corbeille	supprime les fichiers contenus dans la Corbeille.
Nettoyeur de fichiers temporaires	supprime les fichiers stockés dans des dossiers temporaires.
Nettoyeur de raccourcis	supprime les raccourcis inutilisables et les raccourcis auxquels aucun programme n'est associé.
Nettoyeur de fragments de fichiers perdus	supprime de l'ordinateur les fragments de fichiers perdus.
Nettoyeur du registre	supprime du registre Windows® les informations correspondant à des programmes désormais inexistants. Le registre est une base de données dans laquelle Windows stocke ses données de configuration. Il contient des profils pour chaque utilisateur de l'ordinateur ainsi que des informations sur le matériel du système, les programmes installés et les paramètres des propriétés. Windows se réfère continuellement à ces informations en cours de travail.
Nettoyeur du cache	supprime les fichiers mis en cache qui s'accumulent lorsque vous naviguez sur des pages Web. Ces fichiers sont habituellement des fichiers temporaires stockés dans un dossier cache. Un dossier cache est une zone de stockage temporaire de votre ordinateur. Pour augmenter la vitesse et l'efficacité de la navigation sur le Web, votre navigateur peut extraire une page Web de son cache (plutôt que d'un serveur distant) lorsque vous souhaitez la revoir.

Cookie Cleaner (Nettoyeur de cookies)	supprime les cookies. Ces fichiers prennent généralement la forme de fichiers temporaires. Un cookie est un petit fichier contenant des informations, dont généralement un nom d'utilisateur et les date et heures du moment, stocké sur l'ordinateur d'une personne naviguant sur le Web. Les cookies sont essentiellement utilisés par des sites Web pour identifier des utilisateurs qui se sont déjà enregistrés ou ont déjà visité le site ; toutefois, ils peuvent aussi être une source d'informations pour les hackers.
Nettoyeur de l'historique du navigateur	supprime l'historique de votre navigateur Web.
Nettoyeur d'e-mails Outlook Express et Outlook (éléments envoyés et supprimés)	supprime les messages envoyés et supprimés d'Outlook® et Outlook Express.
Nettoyeur récemment utilisé	supprime les fichiers récemment utilisés créés avec l'un des programmes suivants : ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Historique de Windows ▪ Lecteur Windows Media ▪ WinRAR® ▪ WinZip®
Nettoyeur de contrôles ActiveX	supprime les contrôles ActiveX. ActiveX est un composant logiciel utilisé par des programmes ou des pages Web pour ajouter des fonctionnalités qui se fondent dans le programme ou la page Web et y apparaissent comme des éléments normaux. Les plupart des contrôles ActiveX sont inoffensifs ; toutefois, certains peuvent subtiliser des informations sur votre ordinateur.
Nettoyeur de points de restauration système	supprime les anciens points de restauration système (hormis le plus récent) de votre ordinateur. Les points de restauration système sont créés par Windows pour noter les modifications apportées à votre ordinateur afin que vous puissiez revenir à une situation antérieure en cas de problème.

Nettoyage de votre ordinateur

Vous pouvez utiliser les nettoyeurs de QuickClean pour supprimer des fichiers inutiles de votre ordinateur. Lorsque vous avez terminé, sous **Résumé QuickClean**, vous pouvez voir la quantité d'espace disque récupérée après le nettoyage, le nombre de fichiers supprimés, et les date et heure de dernière exécution de QuickClean sur votre ordinateur.

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **McAfee QuickClean**, cliquez sur **Démarrer**.
3. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Suivant** pour utiliser les nettoyeurs par défaut de la liste.
   - Sélectionnez ou désactivez les nettoyeurs appropriés, puis cliquez sur **Suivant**. Si vous sélectionnez Nettoyeur récemment utilisé, vous pouvez cliquer sur **Propriétés** pour sélectionner ou désélectionner les fichiers qui ont été récemment créés par les programmes de la liste, puis cliquer sur **OK**.
   - Cliquez sur **Paramètres par défaut** pour rétablir les nettoyeurs par défaut, puis cliquez sur **Suivant**.
4. Lorsque l'analyse est terminée, cliquez sur **Suivant**.
5. Cliquez sur **Suivant** pour confirmer la suppression des fichiers.
6. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Suivant** si vous acceptez l'option par défaut **Non, je souhaite supprimer les fichiers à l'aide de la fonction Windows standard**.
   - Cliquez sur **Oui, je souhaite procéder à la suppression sécurisée de mes fichiers à l'aide de Shredder**, spécifiez le nombre de passages (jusqu'à 10) et cliquez sur **Suivant**. Le broyage de fichiers peut être long s'il y a beaucoup d'informations à effacer.
7. Si des fichiers ou éléments ont été verrouillés pendant le nettoyage, vous pouvez être invité à faire redémarrer l'ordinateur. Cliquez sur **OK** pour fermer le message.
8. Cliquez sur **Terminer**.

Remarque : Les fichiers supprimés à l'aide de Shredder ne peuvent pas être récupérés. Pour des informations sur le broyage de fichiers, voir McAfee Shredder.

Défragmentation de votre ordinateur

Defragmenteur de disques organise les fichiers et dossiers de votre ordinateur de manière à éviter leur éparpillement (fragmentation) lors de leur enregistrement sur le disque dur de votre ordinateur. En défragmentant périodiquement votre disque dur, vous garantissez le regroupement des fichiers et dossiers fragmentés, ce qui permet de les récupérer plus rapidement ensuite.

Défragmenter votre ordinateur

Vous pouvez défragmenter votre ordinateur pour améliorer l'accès aux fichiers et dossiers et leur récupération.

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Défragmenteur de disque**, cliquez sur **Analyse**.
3. Suivez les instructions à l'écran.

Remarque : pour plus d'informations sur Défragmenteur de disque, consultez l'aide de Windows.

Programmation d'une tâche

Le Planificateur de tâches automatise l'exécution régulière de QuickClean ou de Défragmenteur de disque sur votre ordinateur. Par exemple, vous pouvez programmer une tâche QuickClean qui vide la Corbeille tous les dimanches à 21h00 ou une tâche Défragmenteur de disque qui défragmente le disque dur de votre ordinateur le dernier jour de chaque mois. Vous pouvez créer, modifier ou supprimer une tâche à tout moment. Vous devez être connecté à l'ordinateur pour qu'une tâche programmée puisse s'exécuter. Si une tâche n'est pas exécutée pour une raison quelconque, elle sera reprogrammée cinq minutes après votre reconnexion.

Programmer une tâche QuickClean

Vous pouvez programmer une tâche QuickClean qui nettoie automatiquement votre ordinateur à l'aide d'un ou plusieurs nettoyeurs. Lorsque l'opération est terminée, sous **Résumé QuickClean**, vous pouvez voir les date et heure auxquelles l'exécution de la tâche est à nouveau programmée.

1. Ouvrez le volet Planificateur de tâches.

   Comment ?

   1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
   2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2. Dans la liste **Sélectionner une opération à planifier**, cliquez sur **McAfee QuickClean**.
3. Entrez le nom à donner à la tâche dans la zone **Nom de la tâche**, puis cliquez sur **Créer**.
4. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Suivant** pour utiliser les nettoyeurs de la liste.
   - Sélectionnez ou désactivez les nettoyeurs appropriés, puis cliquez sur **Suivant**. Si vous sélectionnez Nettoyeur récemment utilisé, vous pouvez cliquer sur **Propriétés** pour sélectionner ou désélectionner les fichiers qui ont été récemment créés par les programmes de la liste, puis cliquer sur **OK**.
   - Cliquez sur **Paramètres par défaut** pour rétablir les nettoyeurs par défaut, puis cliquez sur **Suivant**.
5. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Planification** pour accepter l'option par défaut **Non, je souhaite supprimer les fichiers à l'aide de la fonction Windows standard**.

- Cliquez sur **Oui, je souhaite procéder à la suppression sécurisée de mes fichiers à l'aide de Shredder**, spécifiez le nombre de passages (jusqu'à 10) et cliquez sur **Planification**.

6 Dans la boîte de dialogue **Planification**, sélectionnez la fréquence à laquelle la tâche doit être exécutée, puis cliquez sur **OK**.

7 Si vous avez apporté des modifications aux propriétés du Nettoyeur récemment utilisé, vous serez peut-être invité à faire redémarrer votre ordinateur. Cliquez sur **OK** pour fermer le message.

8 Cliquez sur **Terminer**.

Remarque : Les fichiers supprimés à l'aide de Shredder ne peuvent pas être récupérés. Pour des informations sur le broyage de fichiers, voir McAfee Shredder.

Modifier une tâche QuickClean

Vous pouvez modifier une tâche QuickClean programmée pour changer les nettoyeurs utilisés ou sa fréquence d'exécution automatique sur votre ordinateur. Lorsque l'opération est terminée, sous **Résumé QuickClean**, vous pouvez voir les date et heure auxquelles l'exécution de la tâche est à nouveau programmée.

1 Ouvrez le volet Planificateur de tâches.

Comment ?

1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **McAfee QuickClean**.

3 Sélectionnez la tâche dans la liste **Sélectionner une tâche existante**, puis cliquez sur **Modifier**.

4 Effectuez l'une des opérations suivantes :

- Cliquez sur **Suivant** pour utiliser les nettoyeurs sélectionnés pour la tâche.
- Sélectionnez ou désactivez les nettoyeurs appropriés, puis cliquez sur **Suivant**. Si vous sélectionnez Nettoyeur récemment utilisé, vous pouvez cliquer sur **Propriétés** pour sélectionner ou désélectionner les fichiers qui ont été récemment créés par les programmes de la liste, puis cliquer sur **OK**.
- Cliquez sur **Paramètres par défaut** pour rétablir les nettoyeurs par défaut, puis cliquez sur **Suivant**.

5 Effectuez l'une des opérations suivantes :

- Cliquez sur **Planification** pour accepter l'option par défaut **Non, je souhaite supprimer les fichiers à l'aide de la fonction Windows standard**.
- Cliquez sur **Oui, je souhaite procéder à la suppression sécurisée de mes fichiers à l'aide de Shredder**, spécifiez le nombre de passages (jusqu'à 10) et cliquez sur **Planification**.

6 Dans la boîte de dialogue **Planification**, sélectionnez la fréquence à laquelle la tâche doit être exécutée, puis cliquez sur **OK**.

7 Si vous avez apporté des modifications aux propriétés du Nettoyeur récemment utilisé, vous serez peut-être invité à faire redémarrer votre ordinateur. Cliquez sur **OK** pour fermer le message.

8 Cliquez sur **Terminer**.

Remarque : Les fichiers supprimés à l'aide de Shredder ne peuvent pas être récupérés. Pour des informations sur le broyage de fichiers, voir McAfee Shredder.

Supprimer une tâche QuickClean

Vous pouvez supprimer une tâche QuickClean programmée si vous ne souhaitez plus son exécution automatique.

1 Ouvrez le volet Planificateur de tâches.

Comment ?

1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **McAfee QuickClean**.

3 Sélectionnez la tâche dans la liste **Sélectionner une tâche existante**.

4 Cliquez sur **Supprimer**, puis sur **Oui** pour confirmer la suppression.

5 Cliquez sur **Terminer**.

Programmer une tâche Défragmenteur de disque

Vous pouvez programmer une tâche Défragmenteur de disque pour planifier la fréquence à laquelle le disque dur de votre ordinateur doit être automatiquement défragmenté. Lorsque l'opération est terminée, sous **Défragmenteur de disque**, vous pouvez voir les date et heure auxquelles l'exécution de la tâche est à nouveau programmée.

1 Ouvrez le volet Planificateur de tâches.

   Comment ?

   1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
   2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **Défragmenteur de disque**.

3 Entrez le nom à donner à la tâche dans la zone **Nom de la tâche**, puis cliquez sur **Créer**.

4 Effectuez l'une des opérations suivantes :

   - Cliquez sur **Planification** pour accepter l'option par défaut **Procéder à la défragmentation même si l'espace disque est insuffisant**.
   - Désélectionnez **Procéder à la défragmentation même si l'espace disque est insuffisant**, puis cliquez sur **Planification**.

5 Dans la boîte de dialogue **Planification**, sélectionnez la fréquence à laquelle la tâche doit être exécutée, puis cliquez sur **OK**.

6 Cliquez sur **Terminer**.

Modifier une tâche Défragmenteur de disque

Vous pouvez modifier une tâche Défragmenteur de disque programmée pour changer sa fréquence d'exécution automatique sur votre ordinateur. Lorsque l'opération est terminée, sous **Défragmenteur de disque**, vous pouvez voir les date et heure auxquelles l'exécution de la tâche est à nouveau programmée.

1 Ouvrez le volet Planificateur de tâches.

   Comment ?

1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **Défragmenteur de disque**.

3 Sélectionnez la tâche dans la liste **Sélectionner une tâche existante**, puis cliquez sur **Modifier**.

4 Effectuez l'une des opérations suivantes :

- Cliquez sur **Planification** pour accepter l'option par défaut **Procéder à la défragmentation même si l'espace disque est insuffisant**.
- Désélectionnez **Procéder à la défragmentation même si l'espace disque est insuffisant**, puis cliquez sur **Planification**.

5 Dans la boîte de dialogue **Planification**, sélectionnez la fréquence à laquelle la tâche doit être exécutée, puis cliquez sur **OK**.

6 Cliquez sur **Terminer**.

Supprimer une tâche Défragmenteur de disque

Vous pouvez supprimer une tâche Défragmenteur de disque programmée si vous ne souhaitez plus son exécution automatique.

1 Ouvrez le volet Planificateur de tâches.

Comment ?

1. Dans McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Planificateur de tâches**, cliquez sur **Démarrer**.

2 Dans la liste **Sélectionner une opération à planifier**, cliquez sur **Défragmenteur de disque**.

3 Sélectionnez la tâche dans la liste **Sélectionner une tâche existante**.

4 Cliquez sur **Supprimer**, puis sur **Oui** pour confirmer la suppression.

5 Cliquez sur **Terminer**.

CHAPITRE 14

McAfee Shredder

McAfee Shredder supprime (broie) de manière définitive des éléments se trouvant sur le disque dur de votre ordinateur. Même lorsque vous supprimez manuellement des fichiers et des dossiers, puis que vous videz la Corbeille ou que vous supprimez votre dossier Fichiers Internet temporaires, vous pouvez encore récupérer ces informations à l'aide d'outils d'expertise informatique judiciaire. De même, un fichier supprimé peut être récupéré, car certains programmes effectuent des copies temporaires masquées des fichiers ouverts. Shredder protège votre confidentialité en supprimant en toute sécurité et de manière définitive ces fichiers indésirables. Il importe de ne pas oublier que des fichiers broyés ne peuvent plus être restaurés.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctions de Shredder

Shredder supprime des éléments du disque dur de votre ordinateur de sorte que les informations y associées ne puissent plus être récupérées. Il protège votre confidentialité en supprimant en toute sécurité et de manière définitive des fichiers et dossiers, des éléments contenus dans la Corbeille et le dossier Fichiers Internet temporaires, ainsi que le contenu entier de disques tels que des CD réinscriptibles, des disques durs externes et des disquettes.

Broyage de fichiers, dossiers et disques

Shredder veille à ce que les informations contenues dans les fichiers supprimés placés dans votre Corbeille et dans votre dossier Fichiers Internet temporaires ne puissent plus être récupérées, même avec des outils spéciaux. Avec Shredder, vous pouvez spécifier combien de fois (jusqu'à 10) vous voulez qu'un élément soit broyé. Un nombre élevé de broyages augmente le niveau de sécurité de suppression des fichiers.

Broyer les fichiers et les dossiers

Vous pouvez broyer des fichiers et dossiers du disque dur de votre ordinateur, y compris des éléments de la Corbeille et du dossier Fichiers Internet temporaires.

1 Ouvrez **Shredder**.

   Comment ?

   1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Menu Avancé**.
   2. Dans le volet gauche, cliquez sur **Outils**.
   3. Cliquez sur **Shredder**.

2 Dans le volet Broyer les fichiers et les dossiers, sous **Je souhaite**, cliquez sur **Effacer des fichiers et des dossiers**.

3 Sous **Niveau de broyage**, cliquez sur l'un des niveaux de broyage suivants :

   - **Rapide** : broie une seule fois les éléments sélectionnés.
   - **Complet** : broie 7 fois les éléments sélectionnés.
   - **Personnalisé** : broie jusqu'à 10 fois les éléments sélectionnés.

4 Cliquez sur **Suivant**.

5 Effectuez l'une des opérations suivantes :

   - Dans la liste **Sélectionner le(s) fichier(s) à broyer**, cliquez sur **Contenu de la Corbeille** ou sur **Fichiers Internet temporaires**.
   - Cliquez sur **Parcourir**, naviguez jusqu'aux fichiers à broyer, puis cliquez sur **Ouvrir**.

6 Cliquez sur **Suivant**.

7 Cliquez sur **Démarrer**.

8 Lorsque Shredder a terminé, cliquez sur **Terminé**.

Remarque : N'utilisez aucun fichier tant que Shredder n'a pas terminé sa tâche.

Broyer un disque entier

Vous pouvez broyer en une fois le contenu entier d'un disque. Seuls des disques amovibles, comme des disques durs externes, des CD réinscriptibles et des disquettes peuvent être broyés.

1 Ouvrez **Shredder**.

Comment ?

1. Dans le volet McAfee SecurityCenter, sous **Tâches courantes**, cliquez sur **Menu Avancé**.
2. Dans le volet gauche, cliquez sur **Outils**.
3. Cliquez sur **Shredder**.

2 Dans le volet Broyer des fichiers et des dossiers, sous **Je souhaite**, cliquez sur **Effacer un disque entier**.

3 Sous **Niveau de broyage**, cliquez sur l'un des niveaux de broyage suivants :

- **Rapide** : broie une seule fois le disque sélectionné.
- **Complet** : broie 7 fois le disque sélectionné.
- **Personnalisé** : broie jusqu'à 10 fois le disque sélectionné.

4 Cliquez sur **Suivant**.

5 Dans la liste **Sélectionnez le disque**, cliquez sur le disque à broyer.

6 Cliquez sur **Suivant**, puis sur **OK** pour confirmer.

7 Cliquez sur **Démarrer**.

8 Lorsque Shredder a terminé, cliquez sur **Terminé**.

Remarque : N'utilisez aucun fichier tant que Shredder n'a pas terminé sa tâche.

CHAPITRE 15

McAfee Network Manager

Network Manager présente sous forme graphique les ordinateurs et les autres composants de votre réseau. Vous pouvez utiliser Network Manager pour surveiller à distance l'état de protection de chaque ordinateur géré de votre réseau, mais aussi pour corriger à distance les points faibles de la sécurité de ces ordinateurs.

Avant d'utiliser Network Manager, nous vous conseillons de vous familiariser avec certaines de ses fonctionnalités. Pour plus de détails sur la configuration et l'utilisation de ces fonctionnalités, consultez l'aide de Network Manager.

Remarque : SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician.

Contenu de ce chapitre

Fonctionnalités de Network Manager

Network Manager propose les fonctionnalités suivantes.

Carte graphique du réseau

La carte du réseau de Network Manager est une représentation graphique du niveau de protection des ordinateurs et des composants de votre réseau domestique. Lorsque vous modifiez votre réseau (lorsque vous ajoutez un ordinateur, par exemple), la carte du réseau identifie ces changements. Vous pouvez actualiser la carte du réseau, renommer le réseau, ou encore afficher ou masquer des composants de la carte du réseau. Vous pouvez également afficher les détails associés aux composants de la carte du réseau.

Gestion à distance

Utilisez la carte du réseau de Network Manager pour gérer le niveau de protection des ordinateurs qui constituent votre réseau domestique. Vous pouvez inviter un ordinateur à s'affilier au réseau géré, surveiller le niveau de protection des ordinateurs gérés et régler les problèmes connus de failles de sécurité du réseau à partir d'un ordinateur distant.

Présentation des icônes de Network Manager

Le tableau suivant décrit les icônes les plus utilisées sur la carte du réseau Network Manager.

Icône	Description
	Représente un ordinateur géré connecté au réseau
	Représente un ordinateur géré non connecté au réseau
	Représente un ordinateur non géré sur lequel SecurityCenter est installé
	Représente un ordinateur non géré non connecté au réseau
	Représente un ordinateur connecté au réseau sur lequel SecurityCenter n'est pas installé ou un matériel inconnu sur le réseau
	Représente un ordinateur non connecté au réseau sur lequel SecurityCenter n'est pas installé ou un matériel inconnu non connecté au réseau
	Signifie que l'élément correspondant est protégé et connecté
	Signifie que l'élément correspondant nécessite peut-être votre attention
	Signifie que l'élément correspondant nécessite votre attention immédiate
	Représente un routeur personnel sans fil
	Représente un routeur personnel standard
	Représente Internet en mode connexion
	Représente Internet en mode déconnexion

CHAPITRE 16

Configuration d'un réseau géré

Pour configurer un réseau géré, vous triez les éléments de la carte de votre réseau et vous ajoutez des membres (des ordinateurs) au réseau. Pour qu'un ordinateur puisse être géré à distance ou recevoir les autorisations nécessaires pour gérer d'autres ordinateurs à distance sur le réseau, il doit devenir membre autorisé du réseau. L'appartenance au réseau est accordée aux nouveaux ordinateurs par ceux qui sont déjà membres du réseau et qui possèdent des autorisations d'administration.

Vous pouvez voir les détails associés à un composant de la carte du réseau, même après avoir modifié votre réseau (par exemple, en ajoutant un ordinateur).

Contenu de ce chapitre

Utilisation de la carte du réseau

Lorsque vous connectez un ordinateur au réseau, Network Manager analyse l'état du réseau afin de déterminer s'il y a des membres gérés ou non gérés, quels sont les attributs du routeur et quel est l'état d'Internet. Si aucun membre n'est trouvé, Network Manager suppose que l'ordinateur actuellement connecté est le premier du réseau et en fait automatiquement un membre géré avec des autorisations d'administration. Par défaut, le nom du réseau inclut le nom du groupe de travail ou du domaine du premier ordinateur qui se connecte au réseau équipé de SecurityCenter. Vous pouvez modifier le nom du réseau à tout moment.

Lorsque vous modifiez votre réseau (lorsque vous ajoutez un ordinateur, par exemple), vous pouvez personnaliser la carte du réseau. Ainsi, vous pouvez actualiser la carte du réseau, renommer le réseau et afficher/masquer des composants de la carte. Vous pouvez également afficher les détails associés aux composants de la carte du réseau.

Accéder à la carte du réseau

La carte du réseau propose une représentation graphique des ordinateurs et des autres composants de votre réseau.

- Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.

Remarque : vous devez commencer par autoriser les autres ordinateurs du réseau au premier accès à la carte.

Actualiser la carte du réseau

Vous pouvez actualiser la carte du réseau à tout moment, lorsqu'un nouvel ordinateur est affilié au réseau géré par exemple.

1. Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.
2. Cliquez sur **Actualiser la carte du réseau** sous **Je souhaite**.

Remarque : le lien **Actualiser la carte du réseau** n'est disponible que si aucun élément n'est sélectionné sur la carte du réseau. Pour désélectionner un élément, cliquez sur l'élément sélectionné ou sur une zone vide de la carte du réseau.

Attribution d'un nouveau nom au réseau

Par défaut, le nom du réseau inclut le nom du groupe de travail ou du domaine du premier ordinateur qui se connecte au réseau équipé de SecurityCenter. Si vous préférez utiliser un autre nom, vous pouvez le changer.

1. Dans le menu de base ou avancé, cliquez sur **Gérer un réseau**.
2. Cliquez sur **Renommer le réseau** sous **Je souhaite**.
3. Saisissez le nom du réseau dans la zone **Nom du réseau**.
4. Cliquez sur **OK**.

Remarque : Le lien **Attribution d'un nouveau nom au réseau** n'est disponible que si aucun élément n'est sélectionné sur la carte du réseau. Pour désélectionner un élément, cliquez sur l'élément sélectionné ou sur une zone vide de la carte du réseau.

Afficher ou masquer un élément de la carte du réseau

Par défaut, tous les ordinateurs et les autres composants de votre réseau apparaissent sur la carte du réseau. Si vous avez masqué des éléments, vous pouvez les réafficher à tout moment. Seuls les éléments non gérés peuvent être masqués. Les ordinateurs gérés ne peuvent pas être masqués.

Pour...	Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**, puis...
Masquer un élément de la carte du réseau	Cliquez sur un élément de la carte du réseau, puis sur **Masquer cet élément** sous **Je souhaite**. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.
Afficher des éléments masqués de la carte du réseau	Sous **Je souhaite**, cliquez sur **Afficher les éléments masqués**.

Afficher les détails d'un élément

Sélectionnez un composant de votre réseau dans la carte du réseau pour afficher des informations détaillées le concernant. Ces informations comprennent le nom du composant, l'état de sa protection et d'autres informations nécessaires pour gérer le composant.

1. Cliquez sur l'icône d'un élément sur la carte du réseau.
2. Sous **Détails**, affichez des informations sur l'objet.

Affiliation au réseau géré

Pour qu'un ordinateur puisse être géré à distance ou recevoir les autorisations nécessaires pour gérer d'autres ordinateurs à distance sur le réseau, il doit devenir membre autorisé du réseau. L'appartenance au réseau est accordée aux nouveaux ordinateurs par ceux qui sont déjà membres du réseau et qui possèdent des autorisations d'administration. Pour garantir que seuls les ordinateurs autorisés s'affilient au réseau, les utilisateurs des ordinateurs qui accordent les autorisations et ceux qui s'affilient au réseau doivent s'authentifier mutuellement.

Lorsqu'un ordinateur s'affilie au réseau, il est invité à indiquer l'état de sa protection McAfee aux autres ordinateurs du réseau. Si un ordinateur accepte d'afficher l'état de sa protection, il devient un membre géré du réseau. Si un ordinateur refuse d'afficher l'état de sa protection, il devient un membre non géré du réseau. Les membres non gérés du réseau sont généralement des invités qui souhaitent accéder à d'autres fonctionnalités du réseau (par exemple, envoyer des fichiers ou partager des imprimantes).

Remarque : après vous être affilié, si d'autres programmes réseau McAfee sont installés (EasyNetwork, par exemple), l'ordinateur est également reconnu comme étant un ordinateur géré pour ces programmes. Le niveau d'autorisation affecté à un ordinateur dans Network Manager s'applique à tous les programmes réseau McAfee. Pour obtenir des informations sur la signification des autorisations de type Invité, Complet ou Administration dans un autre programme réseau McAfee, reportez-vous à sa documentation.

Affiliation à un réseau géré

Lorsque vous êtes invité à vous affilier à un réseau géré, vous pouvez accepter ou refuser l'invitation. Vous pouvez également déterminer si vous voulez que cet ordinateur et les autres ordinateurs du réseau surveillent mutuellement leurs paramètres de sécurité (pour savoir par exemple si les services de protection antivirus d'un ordinateur sont à jour).

1. Dans la boîte de dialogue Réseau géré, assurez-vous que la case **Autoriser tous les ordinateurs de ce réseau à surveiller les paramètres de sécurité** est sélectionnée.
2. Cliquez sur l'option d'**affiliation**.
   Lorsque vous acceptez l'invitation, deux cartes à jouer s'affichent.
3. Vérifiez que ces cartes sont identiques à celles affichées sur l'ordinateur qui vous a invité à vous affilier au réseau géré.
4. Cliquez sur **OK**.

Remarque : si l'ordinateur qui vous a invité à vous affilier au réseau géré n'affiche pas les mêmes cartes que celles de la boîte de dialogue de confirmation de la sécurité, le réseau géré est victime d'une faille de sécurité. Le fait de vous affilier au réseau risque de compromettre la sécurité de votre ordinateur. Par conséquent, nous vous conseillons de cliquer sur **Annuler** dans la boîte de dialogue Réseau géré.

Inviter un ordinateur à s'affilier au réseau géré

Si un ordinateur est ajouté au réseau géré ou si un autre ordinateur non géré est déjà présent sur le réseau, vous pouvez inviter cet ordinateur à s'affilier au réseau géré. Seuls les ordinateurs avec des autorisations d'administration sur le réseau peuvent en inviter d'autres à s'y affilier. Lorsque vous envoyez l'invitation, vous spécifiez également le niveau d'autorisation que vous affectez à cet ordinateur.

1. Cliquez sur l'icône d'un ordinateur non géré sur la carte du réseau.
2. Cliquez sur **Surveiller cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue d'invitation à l'affiliation au réseau géré, effectuez l'une des opérations suivantes :
   - Cliquez sur **Accorder un accès invité aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau (vous pouvez utiliser cette option pour des utilisateurs temporaires chez vous).
   - Cliquez sur **Accorder un accès total aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau.

- Cliquez sur **Accorder un accès administrateur aux programmes du réseau géré** pour permettre à l'ordinateur d'accéder au réseau avec des droits d'administration. L'ordinateur a par ailleurs la possibilité d'accorder un accès aux autres ordinateurs qui veulent s'affilier au réseau.

4 Cliquez sur **OK**.
Une invitation à s'affilier au réseau géré est envoyée à l'ordinateur. Lorsque l'ordinateur accepte l'invitation, deux cartes à jouer s'affichent.

5 Vérifiez que ces cartes sont identiques à celles affichées sur l'ordinateur que vous avez invité à s'affilier au réseau.

6 Cliquez sur **Autoriser l'accès**.

Remarque : si l'ordinateur qui vous a invité à vous affilier au réseau géré n'affiche pas les mêmes cartes que celles de la boîte de dialogue de confirmation de la sécurité, le réseau géré est victime d'une faille de sécurité. Le fait d'autoriser l'ordinateur à s'affilier au réseau risque de compromettre la sécurité des autres ordinateurs. Par conséquent, nous vous conseillons de cliquer sur **Refuser l'accès** dans la boîte de dialogue de confirmation de la sécurité.

Ne plus approuver les ordinateurs du réseau

Si vous avez approuvé d'autres ordinateurs par erreur, vous pouvez arrêter de les approuver.

- Cliquez sur **Arrêter de faire confiance aux ordinateurs du réseau** sous **Je souhaite**.

Remarque : Le lien **Arrêter de faire confiance aux ordinateurs du réseau** n'est disponible que si vous avez des droits d'administration et qu'il y a d'autres ordinateurs gérés sur le réseau.

CHAPITRE 17

Gestion à distance du réseau

Une fois que vous avez configuré votre réseau géré, vous pouvez gérer à distance les ordinateurs et les autres composants de votre réseau. Vous pouvez surveiller l'état et les niveaux de permission des ordinateurs et des autres composants, mais aussi corriger la plupart des problèmes de vulnérabilité, le tout à distance.

Contenu de ce chapitre

Surveillance de l'état et des autorisations

Un réseau géré comporte des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à surveiller l'état de leur protection McAfee, contrairement aux membres non gérés. Les membres non gérés sont généralement des invités qui souhaitent accéder à d'autres fonctionnalités du réseau (par exemple, envoyer des fichiers et partager des imprimantes). Un ordinateur non géré peut être invité à devenir géré à tout moment par un autre ordinateur géré du réseau. De même, un ordinateur géré peut devenir non géré à tout moment.

Les ordinateurs gérés ont des autorisations de type Administration, Complet ou Invité. Les autorisations de type Administration permettent à l'ordinateur géré de gérer l'état de protection de tous les autres ordinateurs gérés du réseau, mais aussi d'accorder une appartenance aux autres ordinateurs du réseau. Les autorisations de type Complet et Invité ne permettent que l'accès au réseau. Vous pouvez modifier le niveau d'autorisation d'un ordinateur à tout moment.

Un réseau géré pouvant aussi comporter du matériel (des routeurs, par exemple), vous pouvez utiliser Network Manager pour les gérer. Vous pouvez aussi configurer et modifier les propriétés d'affichage d'un matériel sur la carte du réseau.

Surveillance de l'état de protection d'un ordinateur

Si l'état de protection d'un ordinateur n'est pas surveillé sur le réseau (l'ordinateur n'est pas un membre ou est un membre non géré), vous pouvez demander sa surveillance.

1. Cliquez sur l'icône d'un ordinateur non géré sur la carte du réseau.
2. Cliquez sur **Surveiller cet ordinateur** sous **Je souhaite**.

Arrêt de la surveillance de l'état de protection d'un ordinateur

Vous pouvez arrêter de surveiller l'état de protection d'un ordinateur géré de votre réseau ; cependant, l'ordinateur devient alors non géré et vous ne pouvez pas en contrôler l'état de protection à distance.

1. Cliquez sur l'icône d'un ordinateur géré sur la carte du réseau.
2. Cliquez sur **Arrêter de surveiller cet ordinateur** sous **Je souhaite**.
3. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.

Modification des autorisations d'un ordinateur géré

Vous pouvez modifier les autorisations d'un ordinateur géré à tout moment. Ainsi, vous pouvez changer les ordinateurs qui vont surveiller l'état de protection des autres ordinateurs du réseau.

1. Cliquez sur l'icône d'un ordinateur géré sur la carte du réseau.
2. Cliquez sur **Modifier les autorisations de cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue de modification des autorisations, sélectionnez ou désélectionnez la case à cocher afin de déterminer si cet ordinateur et les autres ordinateurs du réseau géré peuvent surveiller mutuellement l'état de leur protection.
4. Cliquez sur **OK**.

Gestion d'un matériel

Pour gérer un matériel, accédez à sa page Web d'administration depuis Network Manager.

1. Cliquez sur l'icône d'un matériel sur la carte du réseau.
2. Cliquez sur **Gérer ce matériel** sous **Je souhaite**.
   Un navigateur Web s'ouvre pour afficher la page Web d'administration du matériel.
3. Dans votre navigateur Web, fournissez vos informations de connexion, puis configurez les paramètres de sécurité du matériel.

Remarque : si le matériel est un point d'accès ou un routeur sans fil protégé par Wireless Network Security, vous devez utiliser Wireless Network Security pour en configurer les paramètres de sécurité.

Modification des paramètres d'affichage d'un matériel

Lorsque vous modifiez les paramètres d'affichage d'un matériel, vous pouvez le renommer sur la carte du réseau et spécifier s'il s'agit d'un routeur sans fil.

1. Cliquez sur l'icône d'un matériel sur la carte du réseau.
2. Cliquez sur **Modifier les propriétés du matériel** sous **Je souhaite**.
3. Pour spécifier le nom d'affichage du matériel, saisissez un nom dans la zone **Nom**.
4. Pour spécifier le type de matériel, cliquez **Routeur standard** s'il ne s'agit pas d'un routeur sans fil ou **Routeur sans fil** dans le cas contraire.
5. Cliquez sur **OK**.

Réparation des failles de sécurité

Les ordinateurs gérés avec des autorisations de type Administration peuvent surveiller l'état de protection McAfee des autres ordinateurs gérés du réseau, mais aussi corriger à distance toute défaillance détectée en matière de sécurité. Ainsi, si l'état de protection McAfee d'un ordinateur géré indique que VirusScan est désactivé, un autre ordinateur géré avec des autorisations de type Administration peut activer VirusScan à distance.

Lorsque vous corrigez à distance des défaillances en matière de sécurité, Network Manager répare la plupart des problèmes rencontrés. Dans certains cas, une intervention manuelle directement sur l'ordinateur peut être nécessaire. Dans ce cas, Network Manager corrige tous les problèmes qui peuvent être réglés à distance, puis vous invite à corriger les problèmes restants. Connectez-vous alors à SecurityCenter sur l'ordinateur vulnérable et suivez les recommandations fournies. Dans certains cas, la solution suggérée consiste à installer la dernière version de SecurityCenter sur les ordinateurs distants du réseau.

Réparation automatique des failles de sécurité

Network Manager permet de corriger la plupart des problèmes de sécurité sur les ordinateurs gérés distants. Par exemple, si VirusScan est désactivé sur un ordinateur distant, vous pouvez le réactiver.

1. Cliquez sur l'icône d'un élément sur la carte du réseau.
2. Sous **Détails**, affichez l'état de protection de l'élément.
3. Cliquez sur **Réparer les failles de sécurité** sous **Je souhaite**.
4. Une fois les problèmes de sécurité réglés, cliquez sur **OK**.

Remarque : bien que Network Manager corrige automatiquement la plupart des failles de sécurité, il peut parfois être nécessaire d'ouvrir SecurityCenter sur l'ordinateur vulnérable et de suivre les recommandations fournies.

Installation de McAfee Security sur les ordinateurs distants

Si des ordinateurs de votre réseau n'utilisent pas la dernière version de SecurityCenter, leur état de protection ne peut pas être surveillé à distance. Pour surveiller ces ordinateurs à distance, vous devez installer la dernière version de SecurityCenter sur chacun d'entre eux.

1. Sur l'ordinateur où vous souhaitez installer le logiciel de sécurité, ouvrez SecurityCenter.
2. Sous **Tâches courantes**, cliquez sur **Mon compte**.
3. Connectez-vous avec l'adresse électronique et le mot de passe que vous avez utilisés pour enregistrer votre logiciel de sécurité la première fois que vous l'avez installé.
4. Sélectionnez le produit approprié, cliquez sur l'icône **Télécharger/Installer**, puis suivez les instructions à l'écran.

Référence

Le glossaire répertorie et définit les termes de sécurité les plus utilisés dans les produits McAfee.

Glossaire

8

802.11

Ensemble de standards IEEE pour la transmission de données sur un réseau sans fil. 802.11 est communément connu sous le nom de Wi-Fi.

802.11a

Extension de 802.11 qui transmet des données à un débit pouvant atteindre 54 Mbits/s dans la bande des 5 GHz. Même si le débit de transmission est plus rapide que celui du 802.11b, la distance couverte est inférieure.

802.11b

Extension de 802.11 qui transmet des données à un débit pouvant atteindre 11 Mbits/s dans la bande des 2,4 GHz. Même si le débit de transmission est plus lent que celui du 802.11a, la distance couverte est supérieure.

802.1x

Standard IEEE pour l'authentification sur les réseaux câblés et sans fil. 802.1x est couramment utilisé avec les réseaux sans fil 802.11.

A

adaptateur sans fil

Appareil qui ajoute une capacité de communication sans fil à un ordinateur ou un PDA. L'adaptateur est connecté via un port USB, un connecteur pour carte PC (CardBus), un connecteur de carte mémoire ou, à l'intérieur, sur le bus PCI.

Adresse IP

Identifiant d'un ordinateur ou d'un périphérique au sein d'un réseau TCP/IP. Les réseaux qui utilisent le protocole TCP/IP acheminent les messages en fonction de l'adresse IP de leur destination. Une adresse IP est au format numérique. Elle est codée sur 32 bits, sous la forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre zéro et 255 (par exemple : 192.168.1.100).

Adresse MAC

(adresse Media Access Control) Numéro de série unique attribué à un appareil physique accédant au réseau.

Analyse à la demande

Analyse lancée à la demande (c'est-à-dire lorsque vous lancez l'opération). A la différence de l'analyse en temps réel, les analyses à la demande ne se lancent pas automatiquement.

analyse en temps réel

Permet d'analyser les fichiers et les dossiers, à la recherche de virus et d'autres activités, lorsque vous ou votre ordinateur y accédez.

archivage complet

Archiver un jeu complet de données en fonction des types des fichiers et des emplacements que vous avez déjà configurés. Voir aussi archivage rapide.

archivage rapide

Archivage des seuls fichiers modifiés depuis le dernier archivage complet ou rapide. Voir aussi archivage complet.

archiver

Créer une copie de fichiers importants sur CD, DVD, lecteur USB, disque dur externe ou disque réseau.

attaque en force

Méthode de décodage de données chiffrées, comme des mots de passe, basée sur un effort exhaustif (force brute) plutôt que sur une stratégie intellectuelle. La force brute est jugée comme une méthode d'attaque infaillible, mais longue. Aussi appelée craquage en force.

attaque par dictionnaire

Type d'attaque en force qui utilise des mots courants pour tenter de découvrir un mot de passe.

attaque par immixtion

Méthode visant à intercepter et éventuellement modifier des messages entre deux parties sans que celles-ci sachent que leur communication a été infiltrée.

authentification

Processus d'identification d'une personne, généralement par un nom unique et un mot de passe.

B

bande passante

Quantité de données pouvant être transmise sur une période donnée.

base de registre

Base de données où Windows stocke ses informations de configuration. Il contient des profils pour chaque utilisateur de l'ordinateur ainsi que des informations sur le matériel du système, les programmes installés et les paramètres des propriétés. Windows se réfère continuellement à ces informations en cours de travail.

bibliothèque

Zone de stockage en ligne pour des fichiers que vous avez sauvegardés et publiés. La bibliothèque Data Backup est un site Web sur Internet, accessible à toute personne disposant d'un accès Internet.

C

cache

Zone de stockage temporaire sur votre ordinateur. Par exemple, pour accélérer et augmenter l'efficacité de la navigation sur le Web, votre navigateur peut extraire une page Web de sa mémoire cache (plutôt que d'un serveur distant) la prochaine fois que vous l'affichez.

carte adaptateur sans fil USB

Carte adaptateur sans fil qui se connecte à un logement USB dans l'ordinateur.

carte du réseau

Représentation graphique des ordinateurs et des autres composants de votre réseau domestique.

cartes adaptateur sans fil PCI

(Peripheral Component Interconnect) Carte adaptateur sans fil qui se branche sur un connecteur d'extension PCI à l'intérieur de l'ordinateur.

certifié Wi-Fi

Testé et approuvé par la Wi-Fi Alliance. Les produits certifiés Wi-Fi sont réputés interopérables même s'ils proviennent de fabricants différents. Un utilisateur disposant d'un produit certifié Wi-Fi peut utiliser n'importe quelle marque de point d'accès avec toute autre marque de matériel client également certifié.

Cheval de Troie

Programmes qui semblent légitimes mais qui peuvent endommager de précieux fichiers, perturber les performances et permettre des accès non autorisés à votre ordinateur.

chiffrement

Processus de transformation de données, de texte en code, qui les obscurcit pour les rendre illisibles par les personnes ne sachant pas les déchiffrer. On dit aussi texte crypté.

Clé

Voir clé USB.

clé

Série de lettres et de chiffres utilisée par deux périphériques pour authentifier une communication. Les deux doivent disposer de la clé. Voir aussi WEP, WPA, WPA2, WPA-PSK et WPA2- PSK.

clé USB

Petit lecteur mémoire qui se branche sur un port USB de l'ordinateur. Un lecteur USB agit comme un petit lecteur de disque et facilite le transfert de fichiers entre deux ordinateurs.

client

Application qui s'exécute sur un ordinateur personnel ou une station de travail et qui s'appuie sur un serveur pour certaines de ses opérations. Un client de messagerie, par exemple, est une application qui permet d'envoyer et de recevoir du courrier électronique.

client de messagerie

Programme que vous exécutez sur votre ordinateur pour envoyer et recevoir des e-mails (par exemple, Microsoft Outlook).

code d'authentification des messages (MAC)

Code de sécurité utilisé pour chiffrer des messages transmis entre des ordinateurs. Le message est accepté si l'ordinateur reconnaît la validité du code déchiffré.

compression

Processus permettant de compresser des fichiers dans un format qui réduit l'espace nécessaire pour les stocker ou les transmettre.

compte de messagerie standard

Voir POP3.

Contrôle ActiveX

Composant logiciel utilisé par des programmes ou des pages Web pour ajouter une fonctionnalité qui apparaît comme une partie normale du programme ou de la page Web. Les plupart des contrôles ActiveX sont inoffensifs ; toutefois, certains peuvent subtiliser des informations sur votre ordinateur.

Contrôle parental

Réglages qui déterminent ce que vos enfants peuvent voir et faire sur le Web. Pour configurer le contrôle parental, vous pouvez activer ou désactiver le filtrage d'images, choisir un groupe de classification du contenu et définir des heures limites de navigation sur le Web.

cookie

Petit fichier contenant des informations, dont généralement un nom d'utilisateur et les date et heure actuelles, stocké sur l'ordinateur d'une personne naviguant sur le Web. Les cookies sont essentiellement utilisés par des sites Web pour identifier des utilisateurs qui se sont déjà enregistrés ou ont déjà visité le site ; toutefois, ils peuvent aussi être une source d'informations pour les hackers.

Corbeille

Imitation d'une corbeille à papiers, utilisée pour stocker les fichiers et dossiers supprimés dans Windows.

D

DAT

(Fichiers de signature de données) Fichiers contenant les définitions employées pour détecter des virus, des chevaux de Troie, des logiciels espions, des logiciels publicitaires et d'autres programmes potentiellement indésirables sur votre ordinateur ou votre lecteur USB.

débordement de la mémoire tampon

Condition qui se produit lorsque des programmes ou processus suspects tentent de stocker davantage de données dans une mémoire tampon (zone de stockage temporaire) de votre ordinateur que celle-ci peut en contenir. Les débordements de mémoire tampon endommagent ou écrasent les données contenues dans les tampons adjacents.

déni de service

Type d'attaque qui ralentit ou paralyse le trafic sur un réseau. Une attaque par déni de service se produit lorsqu'un réseau est inondé de requêtes supplémentaires au point que le trafic ordinaire est ralenti ou complètement bloqué. Il n'entraîne généralement aucun vol d'informations ni aucune autre vulnérabilité.

disque dur externe

Disque dur conservé en dehors de l'ordinateur.

DNS

(Système de noms de domaines) Système qui convertit les noms d'hôtes ou noms de domaines en adresses IP. Sur le Web, DNS est utilisé pour convertir une adresse Web facilement lisible (par exemple, www.monhote.com) en une adresse IP (par exemple, 111.2.3.44) pour permettre d'aller chercher la page Web. Sans DNS, vous devriez taper vous-même l'adresse IP dans votre navigateur Web.

domaine

Sous-réseau local ou descripteur de sites sur Internet.

Sur un réseau local (LAN), un domaine est un sous-réseau composé d'ordinateurs clients et serveurs contrôlés par une seule base de données de sécurité. Dans ce contexte, les domaines peuvent améliorer les performances. Sur Internet, un domaine est une partie de toute adresse Web (par exemple, dans www.abc.com, abc est le domaine).

E

e-mail

(courrier électronique) Messages envoyés et reçus électroniquement, à travers un réseau d'ordinateurs. Voir aussi Webmail.

emplacement de surveillance accrue

Dossier de votre ordinateur dont les changements sont surveillés par Data Backup. Si vous définissez un emplacement de surveillance accrue, Data Backup sauvegarde les types de fichiers de surveillance dans ce dossier ou ses sous-dossiers.

emplacements de surveillance de premier niveau

Dossier de votre ordinateur dont les changements sont surveillés par Data Backup. Si vous définissez un emplacement surveillé de premier niveau, Data Backup sauvegarde les types de fichiers de surveillance dans ce dossier, mais n'inclut pas ses sous-dossiers.

emplacements surveillés

Dossiers surveillés par Data Backup sur votre ordinateur.

ESS

(Extended Service Set) Ensemble de deux réseaux ou plus formant un même sous-réseau.

É

événement

Action entreprise par l'utilisateur, un périphérique ou l'ordinateur lui-même, qui déclenche une réponse. McAfee consigne les événements dans son journal des événements.

F

fenêtres instantanées

Petites fenêtres qui apparaissent au-dessus d'autres fenêtres plus grandes, sur l'écran de l'ordinateur. Les fenêtres instantanées servent souvent à afficher des publicités dans les navigateurs Web.

fichier temporaire

Fichier utile le temps d'une session, que le système d'exploitation ou un autre programme crée en mémoire ou sur disque, avant de le supprimer.

filtrage d'images

Option de contrôle parental qui empêche l'affichage d'images Web potentiellement inappropriées.

fragments de fichier

Restes d'un fichier éparpillés sur un disque. La fragmentation se produit à mesure que des fichiers sont ajoutés ou supprimés, et peut ralentir votre ordinateur.

G

groupe d'évaluation de contenu

Dans le contrôle parental, groupe d'âge auquel appartient un utilisateur. Le contenu est mis à disposition ou bloqué en fonction du groupe auquel appartient l'utilisateur. Les groupes d'évaluation du contenu incluent : les jeunes enfants, les enfants, les pré-adolescents, les adolescents et les adultes.

I

Internet

Ensemble d'un grand nombre de réseaux interconnectés qui utilisent le protocole TCP/IP pour localiser et transférer des données. Initialement, il s'agissait d'une liaison entre des ordinateurs d'universités (à la fin des années 1960 et au début des années 1970) financée par le Ministère de la Défense des États-Unis et appelée ARPANET. Aujourd'hui, Internet est un réseau mondial qui regroupe près de 100 000 réseaux indépendants.

intranet

Réseau d'ordinateurs privé, généralement au sein d'une organisation, qui n'est accessible qu'aux utilisateurs autorisés.

itinérance

Déplacement d'une zone de couverture d'un point d'accès à une autre, sans interruption du service, ni perte de connexion.

L

LAN

(Local Area Network - Réseau local) Réseau d'ordinateurs qui s'étend sur une zone relativement petite (par exemple, un seul bâtiment). Les ordinateurs connectés via un LAN peuvent communiquer entre eux et partager des ressources telles que des imprimantes et des fichiers.

Launchpad

Composant de l'interface U3 qui agit comme point de départ pour lancer et gérer les programmes USB U3.

lecteur réseau

Disque ou lecteur de bande relié à un serveur sur un réseau partagé par plusieurs utilisateurs. Les lecteurs réseau sont quelquefois appelés lecteurs distants.

liste approuvée

Contient des éléments que vous avez autorisés et ne sont donc plus détectés. Si vous autorisez par erreur un élément (par exemple, un programme potentiellement indésirable ou une modification du registre) ou si vous souhaitez à nouveau qu'il soit détecté, vous devez le supprimer de cette liste.

liste d'autorisation

Liste de sites Web auxquels les utilisateurs sont autorisés à accéder car ils ne sont pas considérés comme frauduleux.

liste de blocage

Dans la protection anti-hameçonnage, liste de sites Web considérés comme frauduleux.

M

MAPI

(Messaging Application Programming Interface) Spécification d'interface de Microsoft permettant à différentes applications de messagerie et de groupes de travail (messagerie électronique, messagerie vocale, télécopie...) de fonctionner sur un seul client, comme le client Exchange.

mot clé

Mot pouvant être affecté à un fichier sauvegardé pour établir une relation ou une connexion avec d'autres fichiers auxquels le même mot clé a été affecté. Les mots clés facilitent la recherche des fichiers publiés sur Internet.

mot de passe

Code (généralement composé de lettres et de chiffres) qui permet d'accéder à votre ordinateur, à un programme ou à un site Web.

MSN

(Microsoft Network) Groupe de services basés sur le Web offerts par Microsoft Corporation ; ce groupe comprend un moteur de recherche, une messagerie Web, une messagerie instantanée et un portail.

N

navigateur

Programme utilisé pour afficher des pages Web sur Internet. Les navigateurs Web les plus populaires sont Microsoft Internet Explorer et Mozilla Firefox.

NIC

(Network Interface Card - Carte d'interface réseau) Carte qui se branche sur un ordinateur portable ou un autre périphérique pour le relier au réseau local.

nœud

Ordinateur unique relié à un réseau.

numéroteur

Logiciel qui aide à établir une connexion Internet. Utilisé de manière malveillante, il peut rediriger vos connexions Internet vers quelqu'un d'autre que votre fournisseur d'accès (FAI) par défaut, sans vous informer du coût supplémentaire que cela implique.

P

pare-feu

Système (matériel et/ou logiciel) conçu pour empêcher les accès non autorisés à un réseau privé ou à partir de ce dernier. Ils sont fréquemment utilisés pour empêcher les utilisateurs non autorisés d'accéder à des réseaux privés connectés à Internet, en particulier des intranets. Tous les messages qui pénètrent ou quittent l'intranet passent par le pare-feu, qui étudie chaque message et bloque ceux qui ne répondent pas aux critères de sécurité spécifiés.

partager

Permettre aux destinataires d'e-mails d'accéder à certains fichiers sauvegardés pendant une certaine période. Lorsque vous partagez un fichier, vous en envoyez la copie sauvegardée aux destinataires que vous choisissez. Ces derniers reçoivent un courrier électronique de Data Backup leur signalant que des fichiers ont été partagés avec eux. Le courrier comporte également un lien vers ces fichiers partagés.

passerelle intégrée

Dispositif qui associe les fonctions d'un point d'accès, d'un routeur et d'un pare-feu. Certains peuvent aussi comporter des améliorations de sécurité et des fonctions de pont.

Password Vault

Zone de stockage sécurisée des mots de passe personnels. Ainsi, vous êtes assuré que personne ne peut accéder à vos mots de passe (pas même un administrateur).

phishing

Tromperie sur Internet visant à obtenir des informations précieuses (comme un numéro de carte de crédit ou de sécurité sociale, un nom d'utilisateur et des mots de passe) de personnes naïves en vue d'un usage frauduleux.

Pixels invisibles

Petits fichiers graphiques pouvant s'insérer dans vos pages HTML et permettant à une source non autorisée de placer des cookies sur votre ordinateur. Ces cookies peuvent ensuite transmettre des informations à la source non autorisée. Les pixels invisibles sont aussi appelés balises Web, GIF transparents ou GIF invisibles.

plug-in

Petit logiciel qui collabore avec un programme de plus grande taille pour fournir des fonctionnalités supplémentaires. Par exemple, des plug-ins permettent à un navigateur Web d'exécuter des fichiers incorporés dans des documents HTML, dans des formats qu'il ne reconnaîtrait pas normalement (par exemple, fichiers vidéo, audio et d'animation).

Point d'accès

Périphérique réseau (couramment appelé routeur sans fil) qui se connecte à un concentrateur ou commutateur Ethernet pour étendre la portée physique du service pour un utilisateur sans fil. Lorsque des utilisateurs sans fil se déplacent avec leur appareil mobile, la transmission passe d'un point d'accès à un autre pour maintenir la connectivité.

point d'accès non fiable

Point d'accès non autorisé. Des points d'accès non fiables peuvent être installés sur un réseau d'entreprise sûr pour permettre à des tiers non autorisés d'accéder au réseau. Ils peuvent aussi être créés pour permettre à un agresseur de mener une attaque par immixtion.

point d'accès sans fil

Zone géographique couverte par un point d'accès Wi-Fi (802.11). Un utilisateur qui y pénètre avec un portable sans fil peut se connecter à Internet, à condition que le point d'accès diffuse sa présence et n'exige pas d'authentification. Les points d'accès sans fil (hotspots) se situent souvent dans des zones très fréquentées (p. ex. aéroports).

point de restauration système

Instantané (image) du contenu de la mémoire d'un ordinateur ou d'une base de données. Windows crée des points de restauration périodiquement ainsi qu'au moment d'événements système significatifs (p. ex. lors de l'installation d'un programme ou d'un pilote). Vous pouvez également créer et nommer à tout moment vos propres points de restauration.

POP3

(Post Office Protocol 3) Interface entre un client de messagerie et le serveur de messagerie. La plupart des utilisateurs domestiques ont un compte POP3, qui est leur compte de messagerie standard.

port

Lieu par où des informations entrent et/ou sortent d'un ordinateur. Par exemple, un modem analogique conventionnel est connecté à un port série.

PPPoE

(Point-to-Point Protocol Over Ethernet) Méthode utilisant le protocole PPP (Point-to-Point Protocol) avec Ethernet comme moyen de transport.

programme potentiellement indésirable (PUP)

Programme qui recueille et transmet des informations personnelles sans votre autorisation (par exemple logiciel espion ou publicitaire).

protocole

Format (matériel ou logiciel) de transmission de données entre deux périphériques. Votre ordinateur ou périphérique doit prendre en charge le protocole approprié pour pouvoir communiquer avec d'autres ordinateurs.

proxy

Ordinateur (ou logiciel s'exécutant sur cet ordinateur) qui agit comme une barrière entre un réseau et Internet en présentant une adresse réseau unique aux sites externes. En représentant tous les ordinateurs internes, le proxy protège les identités réseau tout en fournissant un accès à Internet. Voir également serveur proxy.

publier

Mettre à disposition du public, sur Internet, un fichier sauvegardé. Vous pouvez accéder à des fichiers publiés en feuilletant la bibliothèque Data Backup.

Q

quarantaine

Isolement. Par exemple, dans VirusScan, les fichiers suspects sont détectés et mis en quarantaine afin qu'ils ne puissent pas nuire à votre ordinateur ni à vos fichiers.

R

raccourci

Fichier contenant uniquement l'emplacement d'un autre fichier sur votre ordinateur.

RADIUS

(Remote Access Dial-In User Service) Protocole qui permet l'authentification des utilisateurs, généralement dans le contexte d'un accès à distance. Initialement défini pour être utilisé avec des serveurs d'accès distant à commutation, le protocole RADIUS sert maintenant dans divers environnements d'authentification, notamment l'authentification 802.1x d'un secret partagé de l'utilisateur d'un WLAN.

référentiel de sauvegarde en ligne

Emplacement sur le serveur en ligne pour stocker les fichiers après leur sauvegarde.

réseau

Ensemble de points d'accès et de leurs utilisateurs associés, qui équivaut à un ESS (jeu de service étendu).

réseau domestique

Plusieurs ordinateurs connectés dans une maison pour permettre le partage de fichiers et de l'accès à Internet. Voir aussi Réseau local.

réseau géré

Un réseau domestique comporte deux types de membres : des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à surveiller l'état de leur protection, contrairement aux membres non gérés.

restauration

Récupération d'une copie d'un fichier à partir du référentiel de sauvegarde en ligne ou d'une archive.

rootkit

Ensemble d'outils (programmes) qui octroient à un utilisateur le niveau administrateur pour accéder à un ordinateur ou un réseau d'ordinateurs. Les rootkits peuvent comprendre des logiciels espions et d'autres programmes potentiellement indésirables qui peuvent engendrer des risques pour la sécurité et la confidentialité des données de votre ordinateur ou de vos informations personnelles.

routeur

Périphérique réseau qui transmet des paquets de données d'un réseau à un autre. Sur la base de tables de routage internes, les routeurs lisent les paquets entrants et décident comment les transférer d'après la combinaison d'adresses source et destination ainsi que les conditions de trafic actuelles (par exemple, charge, coût de la ligne et mauvaises lignes). Un routeur est parfois appelé Point d'accès (AP).

S

sauvegarder

Copier des fichiers importants sur un serveur sécurisé en ligne.

script

Liste de commandes qui peuvent être exécutées automatiquement (sans intervention de l'utilisateur). À la différence des programmes, les scripts sont généralement stockés en texte clair et compilés à chaque exécution. Les macros et fichiers batch sont aussi appelés scripts.

secret partagé

Chaîne ou clé (généralement un mot de passe) qui a été partagé entre deux interlocuteurs avant d'entamer une communication. Un secret partagé est utilisé pour protéger des parties sensibles de messages RADIUS.

serveur

Ordinateur ou programme qui accepte les connexions d'autres ordinateurs ou programmes et renvoie des réponses appropriées. Par exemple, votre programme de messagerie se connecte à un serveur de messagerie chaque fois que vous envoyez ou recevez des e-mails.

serveur DNS

Ordinateur qui renvoie l'adresse IP associée à un nom d'hôte ou de domaine. Voir aussi DNS.

serveur proxy

Composant du pare-feu qui gère le trafic Internet vers et depuis un réseau local (LAN). L'utilisation d'un serveur proxy améliore les performances par deux aspects : d'une part, il fournit des données fréquemment demandées, telles qu'une page Web, et d'autre part, il filtre les demandes et ignore celles que le propriétaire considère comme inappropriées (par exemple, les demandes d'accès non autorisées à des fichiers propriétaires).

SMTP

(Simple Mail Transfer Protocol) Protocole TCP/IP permettant de transmettre des messages d'un ordinateur à un autre sur un réseau. Ce protocole sert à router les courriers électroniques sur Internet.

SSID

(Service Set Identifier) Jeton (clé secrète) qui identifie un réseau Wi-Fi (802.11). Le SSID est défini par l'administrateur du réseau et doit être fourni par les utilisateurs qui souhaitent s'y joindre.

SSL

(Secure Sockets Layer) Protocole développé par Netscape pour transmettre des documents privés sur Internet. SSL utilise une clé publique pour chiffrer des données transférées sur une connexion SSL. Les URL qui exigent une connexion SSL commencent par https au lieu de http.

synchroniser

Résoudre les incohérences entre des fichiers sauvegardés et ceux stockés sur votre ordinateur local. La synchronisation des fichiers a lieu lorsque la version du fichier dans le référentiel de sauvegarde en ligne est plus récente que la version du fichier sur d'autres ordinateurs.

SystemGuard

Alertes McAfee qui détectent les modifications non autorisées apportées à votre ordinateur et vous en avertissent.

T

texte brut

Texte non chiffré. Voir aussi chiffrement.

texte chiffré

Texte codé par chiffrement. Le texte chiffré est illisible tant qu'il n'a pas été converti en texte brut (déchiffré).

TKIP

(Temporal Key Integrity Protocol) Protocole qui surmonte les faiblesses inhérentes à la sécurité WEP, notamment pour la réutilisation des clés de chiffrement. TKIP modifie les clés temporaires tous les 10 000 paquets, pour offrir une méthode de distribution dynamique qui améliore considérablement la sécurité du réseau. Le processus TKIP (sécurité) démarre par une clé temporaire à 128 bits partagée entre les clients et les points d'accès. Il associe la clé temporaire à l'adresse MAC du client, puis ajoute un vecteur d'initialisation de 16 octets relativement large pour produire la clé qui chiffre les données. Cette procédure permet de s'assurer que chaque station utilise des flux de clé différents pour chiffrer les données. TKIP utilise le RC4 pour procéder au chiffrement.

types de fichiers de surveillance

Types de fichiers (par exemple, .doc, .xls, etc.) que Data Backup sauvegarde ou archive dans les emplacements surveillés.

U

U3

(Plus simple, plus intelligent et mobile.) Plate-forme permettant d'exécuter Windows 2000 ou Windows XP directement depuis un lecteur USB. L'initiative U3 a été lancée en 2004 par M-Systems et SanDisk. Elle permet aux utilisateurs d'exécuter des programmes U3 sur un ordinateur Windows, sans installer ni stocker de données ou de paramètres sur l'ordinateur.

URL

(Uniform Resource Locator) Format standard des adresses Internet.

USB

(Bus série universel) Interface informatique série standardisée permettant de connecter des périphériques tels que des claviers, des joysticks et des imprimantes à votre ordinateur.

usurpation d'adresse IP

Action de falsifier les adresses IP dans un paquet IP. Ceci est utilisé dans de nombreux types d'attaques, notamment la prise de contrôle des sessions, et sert souvent à falsifier les en-têtes des courriers électroniques de spam pour empêcher leur traçage.

V

ver

Virus qui se propage automatiquement et qui se fixe dans la mémoire active et peut utiliser les e-mails pour envoyer des copies de lui-même. Les vers reproduisent et consomment les ressources du système, ce qui ralentit les performances ou interrompt les tâches.

Virus

Programmes qui se propagent et peuvent endommager vos fichiers et données. En général, leur expéditeur semble digne de foi ou leur contenu apparaît comme fiable.

VPN

(Virtual Private Network) Réseau privé configuré au sein d'un réseau public afin de profiter des fonctions de gestion du réseau public. Les VPN sont utilisés par les entreprises pour créer des réseaux WAN (wide area networks) s'étendant sur de grandes régions géographiques, afin de fournir des connexions de site à site avec leurs filiales ou pour permettre à des utilisateurs mobiles de se connecter au LAN de l'entreprise par numérotation.

W

wardriver

Personne qui cherche des réseaux Wi-Fi (802.11) en se déplaçant dans les villes équipé d'un ordinateur Wi-Fi et d'un matériel ou logiciel spécial.

Webmail

Messages envoyés et reçus électroniquement via Internet. Voir aussi e-mail.

WEP

(Wired Equivalent Privacy) Protocole de chiffrement et d'authentification défini dans le cadre de la norme Wi-Fi (802.11). Les premières versions sont basées sur des chiffrements RC4 et présentent des faiblesses considérables. WEP tente d'apporter un minimum de sécurité en chiffrant les données sur des ondes radio pour qu'elles soient protégées lors de leur transfert d'un point d'extrémité à un autre. On a toutefois découvert que WEP n'est pas aussi sûr qu'on le pensait.

Wi-Fi

(Wireless Fidelity) Terme utilisé par la Wi-Fi Alliance pour faire référence à tout type de réseau 802.11.

Wi-Fi Alliance

Organisation composée des grands fournisseurs de matériels et logiciels sans fil. La Wi-Fi Alliance cherche à certifier l'interopérabilité de tous les produits basés sur 802.11 et à promouvoir le terme Wi-Fi comme nom de marque global sur tous les marchés pour tout produit LAN sans fil basé sur 802.11. L'organisation agit comme un consortium, un laboratoire de test et un centre d'informations pour les fournisseurs qui veulent promouvoir la croissance du marché.

WLAN

(Wireless Local Area Network) Réseau local (LAN) utilisant une connexion sans fil. Un réseau local sans fil utilise des ondes radio hautes fréquences à la place des fils pour permettre aux ordinateurs de communiquer entre eux.

WPA

(Wi-Fi Protected Access) Norme de spécification qui augmente fortement le niveau de protection des données et le contrôle d'accès des systèmes de réseau local sans fil actuels et futurs. Conçu pour fonctionner sur le matériel existant sous la forme d'une mise à niveau du logiciel, le WPA est issu de la norme IEEE 802.11i avec laquelle il est compatible. Lorsqu'il est correctement installé, il offre aux utilisateurs d'un réseau local sans fil un niveau de certitude élevé sur le fait que leurs données sont protégées et que seuls les utilisateurs autorisés à utiliser le réseau y auront accès.

WPA-PSK

Mode WPA spécial, conçu pour les utilisateurs à domicile qui n'ont pas besoin de la sécurité nécessaire aux entreprises et n'ont pas accès à des serveurs d'authentification. Avec ce mode, l'utilisateur à domicile entre manuellement le mot de passe de départ pour activer l'accès Wi-Fi protégé en mode clé pré-partagée et doit régulièrement modifier le mot de passe sur chaque ordinateur sans fil et point d'accès. Voir aussi WPA2-PSK et TKIP.

WPA2

Mise à jour de la norme de sécurité WPA, basée sur la norme 802.11i IEEE.

WPA2-PSK

Mode spécial de WPA, similaire à WPA-PSK, basé sur la norme WPA2. Cette norme établit, parmi ses fonctions générales, que les périphériques acceptent souvent plusieurs modes de chiffrement (comme AES, TKIP) simultanément, tandis que les plus anciens n'acceptent généralement qu'un mode de chiffrement à la fois (tous les clients doivent utiliser le même mode de chiffrement).

A propos de McAfee

McAfee, Inc., leader mondial en gestion des risques de sécurité et prévention des intrusions et dont le siège social est basé à Santa Clara, Californie, propose des solutions et services proactifs et éprouvés de sécurisation des systèmes et réseaux dans le monde entier. Avec son expérience de la sécurité et son engagement à l'innovation sans égal, McAfee donne aux particuliers, aux entreprises, au secteur public et aux prestataires de service la capacité de bloquer les attaques, de prévenir les perturbations et d'assurer et d'améliorer régulièrement leur sécurité.

Copyright

Licence

A L'ATTENTION DE TOUS LES UTILISATEURS : LISEZ ATTENTIVEMENT L'ACCORD JURIDIQUE CORRESPONDANT A LA LICENCE QUE VOUS AVEZ ACHETEE. IL DEFINIT LES CONDITIONS GENERALES D'UTILISATION DU LOGICIEL SOUS LICENCE. SI VOUS IGNOREZ LE TYPE DE LICENCE QUE VOUS AVEZ ACQUIS, REPORTEZ-VOUS AUX DOCUMENTS COMMERCIAUX ET AUTRES DOCUMENTS D'OCTROI DE LICENCE, OU AU BON DE COMMANDE, QUI ACCOMPAGNENT VOTRE PROGICIEL OU QUI VOUS ONT ÉTÉ TRANSMIS SÉPARÉMENT DANS LE CADRE DE VOTRE ACHAT (SOUS LA FORME D'UN LIVRET, D'UN FICHIER INCLUS DANS LE CD DU PRODUIT OU D'UN FICHIER DISPONIBLE SUR LE SITE WEB A PARTIR DUQUEL VOUS AVEZ TÉLÉCHARGÉ LE PROGICIEL). SI VOUS N’ÊTES PAS D’ACCORD AVEC CERTAINS TERMES DE CET ACCORD, N’INSTALLEZ PAS LE LOGICIEL. LE CAS ECHEANT, VOUS POUVEZ RENVOYER LE PRODUIT A MCAFEE, INC. OU A L’ENDROIT OU VOUS L’AVEZ ACHETE AFIN D’EN OBTENIR LE REMBOURSEMENT INTEGRAL.

CHAPITRE 18

Service clientèle et support technique

SecurityCenter rapporte les problèmes de protection, qu'ils soient critiques ou non, dès qu'il les détecte. Les problèmes de protection critiques exigent une action immédiate et compromettent votre état de protection (qui passe au rouge). Les problèmes de protection non critiques n'exigent pas d'action immédiate et peuvent ou non compromettre votre état de protection (selon le type de problème). Pour obtenir un état de protection vert, vous devez corriger tous les problèmes critiques et résoudre ou ignorer tous les problèmes non critiques. Si vous avez besoin d'aide dans le diagnostic de vos problèmes de protection, vous pouvez exécuter McAfee Virtual Technician. Pour plus d'informations sur McAfee Virtual Technician, consultez l'aide de McAfee Virtual Technician.

Si vous avez acheté votre logiciel de sécurité chez un partenaire ou un fournisseur autre que McAfee, ouvrez un navigateur Web et accédez à www.mcafeeaide.com. Sous Partner Links, sélectionnez votre partenaire ou fournisseur pour accéder à McAfee Virtual Technician.

Remarque : Pour installer et exécuter McAfee Virtual Technician, vous devez vous connecter à votre ordinateur en tant qu'administrateur Windows. Si vous ne le faites pas, MVT sera peut-être dans l'impossibilité de résoudre vos problèmes. Pour plus d'informations sur la connexion en tant qu'administrateur Windows, consultez l'aide de Windows. Dans Windows Vista™, une invite s'affiche lorsque vous lancez MVT. Cliquez alors sur **Accepter**. Virtual Technician ne fonctionne pas avec Mozilla® Firefox.

Contenu de ce chapitre

Utilisation de McAfee Virtual Technician

À la manière d'un technicien d'assistance personnel, Virtual Technician collecte des informations sur vos programmes SecurityCenter pour résoudre les problèmes de protection de votre ordinateur. Lorsque vous exécutez Virtual Technician, il s'assure que vos programmes SecurityCenter fonctionnent correctement. S'il découvre des problèmes, il propose de les corriger pour vous ou dispense des informations détaillées à leur sujet. Lorsqu'il a terminé, Virtual Technician affiche les résultats de son analyse et vous permet de demander une aide technique supplémentaire de McAfee, le cas échéant.

Pour maintenir la sécurité et l'intégrité de votre ordinateur et de vos fichiers, Virtual Technician ne collecte pas d'informations personnelles identifiables.

Remarque : Pour plus d'informations sur Virtual Technician, cliquez sur l'icône **Aide** dans Virtual Technician.

Lancez Virtual Technician

Virtual Technician collecte des informations sur vos programmes SecurityCenter pour vous aider à résoudre vos problèmes de protection. Afin de préserver votre confidentialité, ces informations ne comprennent pas de données personnelles identifiables.

1. Sous **Tâches courantes**, cliquez sur **McAfee Virtual Technician**.
2. Suivez les instructions à l'écran pour télécharger et exécuter Virtual Technician.

Assistance et téléchargements

Consultez les tableaux suivants pour trouver les sites Assistance et téléchargements McAfee de votre pays, y compris les Guides de l'utilisateur.

Assistance et téléchargements

Pays	Assistance McAfee	Téléchargements McAfee
Australie	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brésil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (anglais)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canada (français)	www.mcafeeaide.com	ca.mcafee.com/root/downloads.asp
Chine (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Chine (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
République tchèque	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Danemark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlande	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
France	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Allemagne	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Grande-Bretagne	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italie	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japon	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Corée	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Mexique	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norvège	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Pologne	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Espagne	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Suède	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turquie	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Etats-Unis	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

Guides de l'utilisateur de McAfee Total Protection

Pays	Guides de l'utilisateur McAfee
Australie	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brésil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (anglais)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canada (français)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Chine (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Chine (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
République tchèque	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlande	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Allemagne	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Grande-Bretagne	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italie	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japon	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Corée	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexique	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Pologne	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Guides de l'utilisateur McAfee Internet Security

Pays	Guides de l'utilisateur McAfee
Australie	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brésil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canada (anglais)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canada (français)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Chine (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Chine (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
République tchèque	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlande	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Allemagne	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Grande-Bretagne	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italie	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japon	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexique	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Pologne	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Guides de l'utilisateur de McAfee VirusScan Plus

Pays	Guides de l'utilisateur McAfee
Australie	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brésil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (anglais)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canada (français)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Chine (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Chine (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
République tchèque	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Danemark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlande	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Allemagne	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Grande-Bretagne	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italie	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japon	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexique	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Pologne	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Guides de l'utilisateur de McAfee VirusScan

Pays	Guides de l'utilisateur McAfee
Australie	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brésil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canada (anglais)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Canada (français)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Chine (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Chine (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
République tchèque	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Danemark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlande	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Allemagne	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Grande-Bretagne	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Pays-Bas	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italie	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japon	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Corée	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexique	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norvège	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Pologne	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Espagne	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Suède	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turquie	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Etats-Unis	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Consultez le tableau suivant pour connaître les sites d'informations Centre de menaces et Informations sur les virus McAfee dans votre pays.

Pays	Siège social du service de sécurité	Informations sur les virus
Australie	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brésil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (anglais)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (français)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Chine (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Chine (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
République tchèque	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Danemark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlande	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
France	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Allemagne	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Grande-Bretagne	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Pays-Bas	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italie	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japon	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Corée	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Mexique	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norvège	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Pologne	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo

Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Espagne	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Suède	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turquie	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Etats-Unis	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Consultez le tableau suivant puor connaître les sites HackerWatch dans votre pays.

Pays	HackerWatch
Australie	www.hackerwatch.org
Brésil	www.hackerwatch.org/?lang=pt-br
Canada (anglais)	www.hackerwatch.org
Canada (français)	www.hackerwatch.org/?lang=fr-ca
Chine (chn)	www.hackerwatch.org/?lang=zh-cn
Chine (tw)	www.hackerwatch.org/?lang=zh-tw
République tchèque	www.hackerwatch.org/?lang=cs
Danemark	www.hackerwatch.org/?lang=da
Finlande	www.hackerwatch.org/?lang=fi
France	www.hackerwatch.org/?lang=fr
Allemagne	www.hackerwatch.org/?lang=de
Grande-Bretagne	www.hackerwatch.org
Pays-Bas	www.hackerwatch.org/?lang=nl
Italie	www.hackerwatch.org/?lang=it
Japon	www.hackerwatch.org/?lang=jp
Corée	www.hackerwatch.org/?lang=ko
Mexique	www.hackerwatch.org/?lang=es-mx
Norvège	www.hackerwatch.org/?lang=no
Pologne	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Espagne	www.hackerwatch.org/?lang=es

Suède	www.hackerwatch.org/?lang=sv
Turquie	www.hackerwatch.org/?lang=tr
Etats-Unis	www.hackerwatch.org

Index

V

W