F-Secure Anti-Virus 2013

Sommaire

Chapitre 1: Installation.....5

Avant la première installation.....6
Première installation du produit.....6
Installation et mise à niveau des applications.....6
Aide et assistance.....7

Chapitre 2: Prise en main.....9

Comment utiliser les mises à jour automatiques ?.....10
Vérifier l'état de la mise à jour.....10
Modifier les paramètres de la connexion Internet.....10
Vérifier le statut du réseau de protection en temps réel.....11
Comment voir l'action du produit.....11
Afficher l'historique des notifications.....11
Modifier les paramètres de notification.....11
Réseau de protection en temps réel.....12
Définition du réseau de protection en temps réel.....12
Avantages du réseau de protection en temps réel.....13
Cadre de contribution de vos données.....13
Comment nous protégeons votre confidentialité.....14
Participer au réseau de protection en temps réel.....15
Questions à propos du réseau de protection en temps réel.....15
Comment savoir si mon abonnement est valable.....15
Centre d'action.....16
Activer un abonnement.....16

Chapitre 3: Présentation.....17

Afficher le statut général de ma protection.....18
Afficher les statistiques du produit.....18
Gérer les mises à jour du produit.....19
Afficher les versions de base de données.....19
Changer les paramètres de la bande passante mobile.....19
Comment fonctionnent les virus et autres programmes malveillants ?.....20
Virus.....20
Logiciels espions.....21
Programmes de base.....21
Programmes à risque.....21

Chapitre 4: Protection contre les programmes malveillants.....23
Comment analyser mon ordinateur ?.....24
Analyser les fichiers automatiquement.....24
Analyser les fichiers manuellement.....26
Analyser les e-mails.....29
Afficher les résultats de l'analyse.....30
Comment exclure des fichiers de l'analyse ?.....31
Exclure des types de fichiers.....31
Exclure des fichiers par emplacement.....31
Afficher les applications exclues.....32
Comment fonctionne la mise en quarantaine ?.....33
Afficher les éléments mis en quarantaine.....33
Restaurer les éléments mis en quarantaine.....33
Qu'est-ce que DeepGuard ?.....34
Activer ou désactiver DeepGuard.....34
Autoriser les applications bloquées par DeepGuard.....34
Utiliser DeepGuard en mode de compatibilité.....35
Que faire en cas d'avertissements pour comportements suspects ?.....35

Chapitre

1

Installation

Sujets :

- *Avant la première installation*
- *Première installation du produit*
- *Installation et mise à niveau des applications*
- *Aide et assistance*

Avant la première installation

Merci d'avoir choisi F-Secure.

Pour installer le produit, il vous faut :

- Le CD d'installation ou un package d'installation. Si vous utilisez un netbook sans lecteur CD, vous pouvez télécharger le package d'installation depuis *www.f-secure.com/netbook*.
- Votre clé d'abonnement.
- Une connexion Internet.

Si vous avez un produit de sécurité d'un autre fournisseur, le programme d'installation va tenter de le supprimer automatiquement. Dans le cas contraire, veuillez le supprimer manuellement.

Remarque: Si vous avez plusieurs comptes sur l'ordinateur, connectez-vous avec vos droits d'administrateur pour l'installation.

Première installation du produit

Instructions pour installer le produit.

Pour installer le produit, procédez comme suit :

1. Insérez le CD ou double-cliquez sur le programme d'installation que vous avez téléchargé.

   Si le CD ne démarre pas automatiquement, allez dans l'Explorateur Windows et double-cliquez sur l'icône du CD-ROM. Double-cliquez ensuite sur le fichier d'installation pour lancer l'installation.

2. Suivez les instructions affichées à l'écran.

   - Si vous avez acheté le produit dans un magasin sur support CD, vous trouverez la clé d'abonnement sur la page de couverture du guide d'installation rapide.
   - Si vous avez téléchargé le produit depuis l'eStore de F-Secure, la clé d'abonnement vous a été fournie dans le message de confirmation du bon de commande.

   Vous devrez probablement redémarrer votre ordinateur pour valider votre abonnement et télécharger les dernières mises à jour depuis Internet. Si vous effectuez l'installation depuis le CD, n'oubliez pas de sortir le CD d'installation avant de redémarrer l'ordinateur.

Installation et mise à niveau des applications

Instructions pour activer le nouvel abonnement.

Suivez ces instructions pour activer votre nouvel abonnement ou pour installer une nouvelle application depuis la zone de lancement :

Remarque: Vous trouverez l'icône de la zone de lancement dans la barre d'état de Windows.

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite.
   Un menu contextuel s'affiche.
2. Sélectionnez**Afficher mes abonnements**
3. Dans**Mes abonnements**, allez à la page **Status de l'abonnement** et cliquez sur **Activer abonnement**.
   La fenêtre **Activer abonnement** s'affiche.

4. Saisissez votre clé d'abonnement pour l'application et cliquez sur **OK**.
5. Une fois votre abonnement validé et activé, cliquez sur **Fermer**.
6. Dans**Mes abonnements**, allez à la page **Statut de l'installation**. Si l'installation ne démarre pas automatiquement, suivez ces instructions:
   a) Cliquez sur **Installer**.
      La fenêtre d'installation s'affiche.
   b) Cliquez sur **Suivant**.
      L'application est téléchargée et l'installation démarre.
   c) Une fois l'installation terminée, cliquez sur **Fermer**.

Le nouvel abonnement est activé.

Aide et assistance

Vous pouvez accéder à l'aide en ligne du produit en cliquant sur l'icône Aide ou en appuyant sur la touche F1 depuis n'importe quel écran du produit.

Une fois que vous avez enregistré votre licence, vous avez accès à de nouveaux services tels que les mises à jour produit gratuites et l'assistance produit. Vous pouvez vous enregistrer sur la page*www.f-secure.com/register*.

Chapitre

2

Prise en main

Sujets :

- *Comment utiliser les mises à jour automatiques ?*
- *Comment voir l'action du produit*
- *Réseau de protection en temps réel*
- *Comment savoir si mon abonnement est valable*

Informations sur la prise en main du produit

Cette section vous explique comment modifier les paramètres et gérer vos abonnements par le biais de la zone de lancement.

Les paramètres communs de la zone de lancement s'appliquent à tous les programmes installés dans la zone de lancement. Vous n'avez pas besoin de modifier les paramètres pour chaque programme, il suffit de modifier un paramètre commun qui sera appliqué à tous les programmes installés.

Les paramètres communs de la zone de lancement comprennent :

- Téléchargements, où vous pouvez consulter les informations sur les mises à jour téléchargées et vérifier manuellement si de nouvelles mises à jour sont disponibles.
- Paramètres de connexion, où vous pouvez changer le mode de connexion de votre ordinateur à Internet.
- Notifications, où vous pouvez afficher les anciennes notifications et définir le type de notifications que vous souhaitez afficher.
- Paramètres de confidentialité, où vous pouvez autoriser ou non votre ordinateur à se connecter au réseau de protection en temps réel.

Vous pouvez également gérer vos abonnements aux programmes installés dans la zone de lancement.

Comment utiliser les mises à jour automatiques ?

Assurez la protection de votre ordinateur grâce aux mises à jour automatiques.

Le produit récupère les dernières mises à jour pour votre ordinateur lorsque vous êtes connecté à Internet. Il détecte le trafic réseau et ne dérange aucune utilisation d'Internet, même si votre connexion est lente.

Vérifier l'état de la mise à jour

Affichez la date et l'heure de la dernière mise à jour.

Si vous avez activé les mises à jour automatiques, le produit reçoit automatiquement les dernières mises à jour dès que vous êtes connecté à Internet.

Pour s'assurer de disposer des dernières mises à jour :

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite.
   Un menu contextuel s'affiche.
2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez **Mises à jour automatiques** > **Téléchargements**.
4. Cliquez sur **Maintenant**.
   Le produit se connecte à Internet et recherche les dernières mises à jour. Il récupère les dernières mises à jour si la protection est obsolète.

   Remarque: Si vous utilisez un modem ou que vous disposez d'une connexion ISDN à Internet, la connexion doit être active pour rechercher des mises à jour.

Modifier les paramètres de la connexion Internet

En général, vous n'avez pas besoin de modifier les paramètres par défaut, mais vous pouvez configurer la connexion du serveur à internet, afin de recevoir automatiquement les mises à jour.

Pour modifier les paramètres de la connexion Internet :

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite.
   Un menu contextuel s'affiche.
2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez **Mises à jour automatiques** > **Connexion**.
4. Dans la liste **Connexion Internet**, sélectionnez la méthode de connexion de votre ordinateur à Internet.
   - Sélectionnez **Considérer la connexion permanente** si vous disposez d'une connexion réseau permanente.

     Remarque: Si votre ordinateur ne dispose pas de la connexion réseau permanente et qu'il est configuré pour une composition à la demande, la sélection de **Considérer la connexion permanente** peut entraîner plusieurs compositions.
   - Sélectionnez **Détecter la connexion** pour ne récupérer des mises à jour que lorsque le produit détecte une connexion réseau active.
   - Sélectionnez **Détecter le trafic** pour ne récupérer des mises à jour que lorsque le produit détecte un autre trafic réseau.

     Astuce: Si vous disposez d'une configuration matérielle atypique entraînant le paramètre **Détecter la connexion** à détecter une connexion réseau active alors qu'il en existe déjà une, sélectionnez plutôt **Détecter le trafic**.

5. Dans la liste **proxy HTTP**, choisissez si votre ordinateur utilisera ou non un *serveur proxy* pour se connecter à Internet.
   - Sélectionnez**Pas de proxy HTTP** si votre ordinateur est connecté directement à Internet.
   - Sélectionnez **Configurer manuellement le proxy HTTP** pour configurer les paramètres de *proxy HTTP*.
   - Sélectionnez **Utiliser le proxy HTTP de mon navigateur** pour utiliser les mêmes paramètres de *proxy HTTP* que ceux configurés dans votre navigateur Web.

Vérifier le statut du réseau de protection en temps réel

Pour un bon fonctionnement, de nombreuses fonctions du produit dépendent de la connectivité du réseau de protection en temps réel.

En cas de problèmes de réseau ou si votre pare-feu bloque le trafic du réseau de protection en temps réel, le statut est « Déconnecté ». Si vous n'avez installé aucune fonction du produit nécessitant un accès au réseau de protection en temps réel, le statut est « Non utilisé ».

Pour vérifier le statut :

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite.
   Un menu contextuel s'affiche.
2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez **Mises à jour automatiques** > **Connexion**.

Dans **Réseau de protection en temps réel**, vous pouvez voir le statut actuel de ce dernier.

Comment voir l'action du produit

Vous pouvez voir les actions effectuées par le produit pour protéger votre ordinateur à la page **Notifications**.

Ce produit affichera une notification lorsqu'il exécutera une action, par ex. lorsqu'il trouvera un virus qu'il bloquera. Certaines notifications peuvent provenir de votre fournisseur de services, par ex. pour vous informer de l'existence de nouveaux services.

Afficher l'historique des notifications

Vous pouvez voir les notifications affichées dans l'historique des notifications

Pour afficher l'historique des notifications :

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite.
   Un menu contextuel s'affiche.
2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez **Autre** > **Notifications**.
4. Cliquez sur **Afficher l'historique des notifications**.
   La liste de l'historique des notifications s'affiche.

Modifier les paramètres de notification

Vous pouvez choisir le type de notifications affichées.

Pour modifier les paramètres de notification :

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite.

Un menu contextuel s'affiche.

2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez **Autre** > **Notifications**.
4. Sélectionnez ou désélectionnez **Autoriser les messages de programmes** pour activer ou désactiver les messages de programmes.

   Lorsque ce paramètre est activé, le produit affiche les notifications des programmes installés.
5. Sélectionnez ou désélectionnez **Autoriser les messages publicitaires** pour activer ou désactiver les messages publicitaires.
6. Cliquez sur **OK**.

Réseau de protection en temps réel

Ce document décrit le réseau de protection en temps réel, un service en ligne de F-Secure Corporation qui identifie les applications et sites Web propres, tout en assurant la protection contre les programmes malveillants et les exploits de sites Web.

Définition du réseau de protection en temps réel

Le réseau de protection en temps réel est un service en ligne qui permet de réagir rapidement face aux dernières menaces Internet.

En participant au réseau de protection en temps réel, vous pouvez nous aider à renforcer la protection contre les menaces, qu'elles soient nouvelles ou émergeantes. Le réseau de protection en temps réel collecte des statistiques sur certaines applications inconnues, malveillantes ou suspectes et sur ce qu'elles font sur votre appareil. Ces informations sont anonymes et sont envoyées à F-Secure Corporation pour une analyse de données combinée. Nous utilisons les informations analysées pour améliorer la sécurité de votre appareil contre les menaces les plus récentes et les fichiers malveillants.

Principe de fonctionnement du réseau de protection en temps réel

En participant au réseau de protection en temps réel, vous nous fournissez des informations sur des applications et des sites web inconnus, ou encore sur des applications malveillantes et des codes malveillants exploitant une faille de sécurité. La protection en temps réel ne suit pas votre activité sur le web et ne collecte aucune information sur des sites web qui ont déjà été analysés. Elle ne collecte pas d'informations sur les applications saines installées sur votre ordinateur.

Si vous ne souhaitez pas participer, la protection en temps réel ne collectera pas d'informations sur les applications intallées ou sur les sites web consultés. Cependant, le produit doit envoyer des requêtes aux serveurs F-Secure sur la réputation des applications, des sites web, des messages et d'autres éléments. La requête est envoyée par le biais d'un total de contrôle cryptographique, l'objet étant sujet de la requête n'étant pas envoyé à F-Secure. Nous ne suivons pas les données en fonction des utilisateurs, mais seulement si le compteur de fichiers ou de sites web augmente.

Il est impossible d'arrêter totalement tout le trafic réseau vers le réseau de protection en temps réel, parce qu'il s'agit d'une composante de la protection assurée par le produit.

Avantages du réseau de protection en temps réel

Le réseau de protection en temps réel vous permet de disposer d'une protection plus rapide et plus précise contre les dernières menaces et vous ne serez pas alerté inutilement en cas d'applications suspectes qui ne sont pas malveillantes.

En participant au réseau de protection en temps réel, vous pouvez nous aider à détecter de nouveaux programmes malveillants inconnus et supprimer des faux positifs de notre définition de base de données de virus.

Tous les participants sur le réseau de protection en temps réel s'entraident. Lorsque le réseau de protection en temps réel trouve une application suspecte sur votre périphérique, vous bénéficiez des résultats de l'analyse quand la même application a déjà été trouvée sur d'autres périphériques. Le réseau de protection en temps réel améliore les performances globales de votre périphérique, parce que le produit de sécurité installé n'analyse pas inutilement des applications qui ont déjà été analysées et jugées propres. De même, les informations sur les sites Web malveillants et les messages en masse non sollicités sont partagées par le réseau de protection en temps réel et nous pouvons vous assurer une protection plus précise contre les exploits de sites Web et les messages indésirables.

Plus vous êtes nombreux à participer au réseau de protection en temps réel, plus nous serons en mesure de protéger efficacement chaque participant.

Cadre de contribution de vos données

En tant que participant au réseau de protection en temps réel, vous fournissez des informations sur les applications stockées sur votre appareil et sur les sites web que vous consultez. Le réseau de protection en temps réel peut ainis offrir une protection contre les applications malveillantes les plus récentes et les sites web suspects.

Analyse de la réputation des fichiers

Le réseau de protection en temps réel recueille uniquement des informations sur des applications sans réputation connue et sur des fichiers suspects ou connus pour être malveillants.

Le réseau de protection en temps réel collecte des informations anonymes sur les applications propres et suspectes de votre appareil. Le réseau de protection en temps réel collecte des informations uniquement sur les fichiers exécutables (les fichiers Portable Executable de la plateforme Windows par ex., dont l'extension de fichier est .cpl, .exe, .dll, .ocx, .sys, .scr et .drv).

Les informations recueillies sont les suivantes :

- le chemin d'accès de l'application sur votre périphérique,
- la taille du fichier et sa date de création ou de modification,
- attributs et privilèges du fichier,
- les informations de signature du fichier,
- la version actuelle du fichier et le nom de l'éditeur qui l'a créé,
- l'origine du fichier ou son URL de téléchargement et
- Résultats des analyses DeepGuard et anti-virus de F-Secure des fichiers analysés et
- d'autres informations similaires.

Le réseau de protection en temps réel ne collecte jamais aucune information sur vos documents personnels, sauf s'ils sont infrectés. Pour tout fichier malicieux, il collecte le nom de l'infection et le statut de désinfection du fichier.

Le réseau de protection en temps réel permet également d'analyser des applications suspectes. Les applications soumises correspondent uniquement à des fichiers exécutables portables. Il ne recueille jamais d'informations concernant vos documents personnels, qui ne sont jamais téléchargés automatiquement pour être analysés.

Fichiers à analyser

Le réseau de protection en temps réel vous permet d'envoyer des applications suspectes pour les faire analyser.

Vous pouvez envoyer des applications suspectes manuellement lorsque le produit vous invite à le faire. Vous pouvez uniquement envoyer des fichiers exécutables portables. Le réseau de protection en temps réel ne charge jamais vos documents personnels.

Analyse de la réputation des sites Web

Le réseau de protection en temps réel ne conserve pas la trace de votre activité sur le Web ni ne recueille d'informations sur les sites Web déjà analysés. Il s'assure que les sites Web consultés sont sûrs lorsque vous naviguez sur le Web. Lorsque vous consultez un site Web, le réseau de protection en temps réel vérifie sa sécurité et vous signale si le site est considéré comme suspect ou dangereux.

Si le site Web que vous consultez contient des éléments malveillants ou suspects ou un exploit connu, le réseau de protection en temps réel recueille l'intégralité de l'URL du site, pour que le contenu de la page Web puisse être analysé.

Si vous consultez un site qui n'a pas encore été évalué, le réseau de protection en temps réel recueille les noms du domaine et sous-domaine et dans certains cas, le chemin d'accès à la page consultée, pour que le site puisse être analysé et évalué. Tous les paramètres de l'URL susceptibles de contenir des informations qui permettent de vous identifier personnellement sont supprimés pour protéger votre vie privée.

Remarque: Le réseau de protection en temps réel n'évalue pas ni n'analyse les pages Web de réseaux privés, il ne recueille donc jamais d'informations sur les adresses de réseau IP privées (par exemple, les intranets d'entreprises).

Analyse des informations système

Le réseau de protection en temps réel recueille le nom et la version de votre système d'exploitation, des informations sur la connexion Internet et les statistiques d'utilisation du réseau de protection en temps réel (par exemple, le nombre de fois que la réputation de sites Web a été interrogée et la durée moyenne pour que l'interrogation retourne un résultat), afin que nous puissions contrôler et améliorer le service.

Comment nous protégeons votre confidentialité

Nous transférons les informations de manière sécurisée et supprimons automatiquement toutes les informations personnelles que les données peuvent contenir.

Le réseau de protection en temps réel supprime les données d'identification avant l'envoi à F-Secure et crypte toutes les informations collectées au cours du transfert pour les protéger contre tout accès non autorisé. Les informations ne sont pas traitées individuellement mais elles sont groupées avec des informations d'autres participants au réseau de protection en temps réel. Toutes les données sont analysées au niveau statistique et de manière anonyme, c'est-à-dire qu'aucune donnée ne pourra être rapportée à vous d'aucune manière.

Toute information qui pourrait vous identifier personnellement est omise dans les données recueillies. Le réseau de protection en temps réel ne recueille aucune adresse IP privée ou des informations privées comme des adresses de courriel, des noms d'utilisateur ou des mots de passe. Même si nous nous efforçons de supprimer toutes les données d'identification personnelles, l'éventualité que les informations recueillies contiennent certaines données d'identification n'est pas à exclure. Dans ce cas, nous n'exploiterons pas ces données recueillies par inadvertance pour vous identifier.

Nous appliquons des mesures de sécurité strictes et des mesures de protection physiques, administratives et techniques pour protéger les informations recueillies, lorsqu'elles sont transférées, enregistrées et traitées. Les informations sont enregistrées dans des emplacements sécurisés et sur des serveurs que nous contrôlons, qui sont situés dans nos bureaux ou dans les bureaux de nos sous-traitants. L'accès aux informations recueillies est réservé aux seuls membres accrédités du personnel.

F-Secure est en droit de partager les données recueillies avec d'autres entités du groupe, ses sous-traitants, ses distributeurs et partenaires, mais toujours dans un format non identifiable et anonyme.

Participer au réseau de protection en temps réel

Vous pouvez nous aider à améliorer la protection du réseau de protection en temps réel en nous fournissant des informations sur des programmes et sites Web malveillants.

Vous pouvez choisir de participer au réseau de protection en temps réel au moment de l'installation. Les paramètres par défaut sont ainsi configurés que vous participez au réseau de protection en temps réel. Vous pouvez les modifier plus tard en utilisant le produit.

Suivez ces instructions pour modifier les paramètres du réseau de protection en temps réel :

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite.
   Un menu contextuel s'affiche.
2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez **Autre** > **Confidentialité**.
4. Cochez la case pour participer au réseau de protection en temps réel.

Questions à propos du réseau de protection en temps réel

Contactez le service d'informations pour toute question à propos du réseau de protection en temps réel.

Si vous avez d'autres questions à propos du réseau de protection en temps réel, veuillez contacter :

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finlande

http://www.f-secure.com/en/web/home_global/support/contact

La dernière version de cette stratégie est toujours disponible sur notre site Web.

Comment savoir si mon abonnement est valable

Le type et le statut de votre abonnement sont affichés dans la page **Statut de l'abonnement**.

Lorsqu'un abonnement est sur le point d'expirer ou si un abonnement a expiré, le statut général de protection du programme change dans l'icône correspondante de la zone de lancement.

Pour vérifier la validité de votre abonnement :

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite.
   Un menu contextuel s'affiche.
2. Sélectionnez **Afficher mes abonnements**.
3. Sélectionnez **Status de l'abonnement** pour afficher les informations sur les abonnements aux programmes installés.
4. Sélectionnez **Statut de l'installation** pour afficher les programmes pouvant être installés.

Le statut et la date d'expiration de votre abonnement sont également affichés dans la page **Statistiques** du programme. Si votre abonnement a expiré, vous devez le renouveler pour recevoir les nouvelles mises à jour et utiliser le produit.

Remarque: Lorsque votre abonnement arrive à expiration, l'icône du statut du produit clignote sur votre zone de notification.

Centre d'action

Le centre d'action vous indique les notifications importantes qui requièrent votre attention.

Si votre abonnement a expiré ou est sur le point d'expirer, le centre d'action vous informe. La couleur d'arrière-plan et le contenu du message du centre d'action dépend du type et du statut de l'abonnement :

- Si votre abonnement a expiré et qu'aucun abonnement graduit n'est disponible, le message a un arrière-plan blanc et un bouton **Activer**.
- Si votre abonnement a expiré et qu'aucun abonnement graduit n'est disponible, le message a un arrière-plan rouge et les boutons **Acheter** et **Saisir clé**. Si vous avez déjà acheté un nouvel abonnement, vous pouvez cliquer sur le bouton **Saisir clé** pour saisir la clé d'abonnement et activer votre nouvel abonnement.
- Si votre abonnement a expiré et qu'aucun abonnement graduit n'est disponible, le message a un arrière-plan rouge et un bouton **Activer**.
- Si votre abonnement a expiré et qu'aucun abonnement gratuit n'est disponible, le message a un arrière-plan rouge et dispose de boutons **Acheter** et **Saisir clé**. Si vous avez déjà acheté un nouvel abonnement, vous pouvez cliquer sur le bouton **Saisir clé** pour saisir la clé d'abonnement et activer votre nouvel abonnement.

Remarque: Le lien **Afficher l'historique des notifications** du centre d'action vous indique une liste de messages de notification, et non pas les anciens messages du centre d'action.

Activer un abonnement

Lorsque vous avez reçu une nouvelle clé d'abonnement ou un code de campagne pour un produit, vous devez l'activer.

Pour activer un abonnement :

1. Dans la zone de lancement, cliquez sur le bouton droit de la souris sur l'icône le plus à droite. Un menu contextuel s'affiche.
2. Sélectionnez **Afficher mes abonnements**.
3. Sélectionnez une des options suivantes :
   - Cliquez sur **Activer l'abonnement**.
   - Cliquez sur **Activer le code de campagne**.
4. Dans la boîte de dialogue qui s'affiche, saisissez votre nouvelle clé d'abonnement ou votre code de campagne et cliquez sur **OK**.

   Astuce: Si vous avez reçu votre clé d'abonnement par courriel, vous pouvez copier la clé du message en question et la coller dans le champ correspondant.

Lorsque vous avez saisi la nouvelle clé d'abonnement, la nouvelle date de validité de l'abonnement est affichée dans la page **Statut de l'abonnement**.

Chapitre

3

Présentation

Sujets :

- *Afficher le statut général de ma protection*
- *Afficher les statistiques du produit*
- *Gérer les mises à jour du produit*
- *Comment fonctionnent les virus et autres programmes malveillants ?*

Ce produit protège votre ordinateur des virus et autres applications nuisibles.

Il analyse les fichiers et les applications et applique des mises à jour automatiquement. Vous n'avez rien à faire.

Afficher le statut général de ma protection

La page **Statut** contient également un aperçu des fonctions du produit installé et leur statut.

Pour ouvrir la page **Statut** :

Sur la page principale, cliquez sur **Statut**.

La page **Statut** s'affiche.

L'icône vous indique le statut du programme et ses fonctions de sécurité.

Icône de statut	Nom du statut	Description
	OK	Votre ordinateur est protégé. La fonction est activée et fonctionne correctement.
	Informations	Le produit vous informe sur le statut spécial d'une fonction. Par exemple, la fonction a été mise à jour.
	Avertissement	Votre ordinateur n'est pas entièrement protégé. Par exemple, le produit n'a pas reçu de mises à jour depuis un certain temps, ou le statut d'une fonctionnalité mérite votre attention.
	Erreur	Votre ordinateur n'est pas protégé Par exemple, votre abonnement a expiré ou une fonctionnalité cruciale est désactivée.
	Désactivée	Une fonction non critique est désactivée.

Afficher les statistiques du produit

Vous pouvez voir l'action du produit depuis son installation dans la page **Statistiques**.

Pour ouvrir la page **Statistiques** :

Sur la page principale, cliquez sur **Statistiques**.

La page **Statistiques** s'ouvre.

- **Dernière recherche de mise à jour réussie** indique la date de la dernière mise à jour.

- **Recherche de virus et logiciels espions** indique le nombre de fichiers analysés et nettoyés depuis l'installation.
- **Applications** indique le nombre de programmes que DeepGuard a autorisés ou bloqués depuis l'installation.
- **Connexions du pare-feu** indique le nombre de connexions autorisées et bloquées depuis l'installation.
- **Filtrage anti-spam et anti-phishing** indique le nombre d'e-mails valides et indésirables que le produit a détectés.

Gérer les mises à jour du produit

Le produit applique automatiquement des mises à jour de la protection.

Afficher les versions de base de données

Vous pouvez voir les dernières heures de mise à jour et les numéros des versions sur la page **Mises à jour de la base de données**.

Pour ouvrir la page **Mises à jour de la base de données** :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Autres paramètres** > **Versions de la base de données**.

La page **Versions de la base de données** affiche la date des dernières mises à jour des définitions de virus et logiciels espions, de DeepGuard et du filtrage anti-spam et anti-phishing, de même que leurs numéros de version.

Changer les paramètres de la bande passante mobile

Indiquez si vous souhaitez télécharger les mises à jour de sécurité lorsque vous utilisez de la bande passante mobile.

Remarque: Cette fonction est diponible uniquement dans Microsoft Windows 7.

Par défaut, les mises à jour de sécurité sont toujours téléchargées sur le réseau de votre opérateur personnel. Cependant, les mises à jour sont suspendues lorsque vous êtes sur le réseau d'un autre opérateur, parce que les tarifs des connexions varient d'un opérateur à l'autre, d'un pays à l'autre. Vous pouvez conserver les paramètres pour économiser de la bande passante et éventuellement des frais supplémentaires lors de votre déplacement.

Remarque: Ce paramère s'applique uniquement aux connexions mobiles à la bande passante. Lorsque l'ordinateur est branché à un réseau fixe ou sans fil, le produit est automatiquement mis à jour.

Pour modifier les paramètres :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Autres paramètres** > **Bande passante mobile** > **Télécharger les mises à jour de sécurité**.
3. Sélectionnez votre option de mise à jour pour les connexions mobiles :
   - **Uniquement dans le réseau de mon opérateur**

Les mises à jour sont toujours téléchargées vers votre réseau d'exploitation privé. Lorsque vous vous trouvez sur le réseau d'un autre opérateur, les mises à jour sont suspendues. Nous vous conseillons de choisir cette option afin de garantir la sécurité de vos produits sans frais supplémentaires.

- **Jamais**

  Les mises à jour ne sont pas téléchargées lorsque vous utilisez de la bande passante mobile.

- **Toujours**

  Les mises à jour sont toujours téléchargées, quel que soit le réseau que vous utilisez. Choisissez cette option pour garantir la sécurité de votre ordinateur, quels que soient les frais.

4. Si vous souhaitez décider à chaque fois que vous quittez le réseau de votre fournisseur, sélectionnez **Me demander à chaque fois que je quitte le réseau de mon opérateur**.

Mises à jour de sécurité suspendues

Les mises à jour de sécurité peuvent être suspendues lorsque vous utilisez de la bande passante mobile en dehors du réseau de votre opérateur privé.

Dans ce cas, la notification **Suspendu** s'affichera dans le coin inférieur droit de votre écran. Les mises à jour sont suspendues parce que les tarifs des connexions varient d'un opérateur à l'autre, notamment selon les pays. Vous pouvez laisser ce paramètre tel quel, si vous souhaitez économiser de la bande passante et par conséquent faire des économies d'argent pendant votre séjour. Si vous souhaitez néanmoins modifier le paramètre, cliquez sur le lien **Changer**.

Remarque:

Cette fonction est diponible uniquement dans Microsoft Windows 7.

Comment fonctionnent les virus et autres programmes malveillants ?

Les programmes malveillants sont des programmes tout particulièrement conçus pour endommager votre ordinateur, l'utiliser à des fins illégales sans que vous le sachiez ou dérober des informations sur votre ordinateur.

Les programmes malveillants peuvent :

- prendre le contrôle de votre navigateur Web,
- rediriger vos tentatives de recherche,
- afficher des publicités indésirables,
- conserver la trace des sites Web visités,
- dérober des informations personnelles comme vos données bancaires,
- utiliser votre ordinateur pour envoyer du courrier indésirable, et
- utiliser votre ordinateur pour attaquer d'autres ordinateurs.

Ils peuvent également ralentir votre ordinateur et le rendre instable. Vous pouvez suspecter un *programme malveillant* sur votre ordinateur s'il devient soudainement très lent et s'il plante souvent.

Virus

Un virus est généralement un programme pouvant se greffer sur des fichiers et se dupliquer plusieurs fois. Il peut altérer et remplacer le contenu d'autres fichiers d'une manière telle qu'ils peuvent endommager votre ordinateur.

Un *virus* est un programme généralement installé sur votre ordinateur sans que vous le sachiez. Le virus tente alors de se dupliquer. Le virus :

- utilise des ressources système de votre ordinateur,
- peut altérer ou endommager des fichiers sur votre ordinateur,
- tente éventuellement d'utiliser votre ordinateur pour en infecter d'autres,
- peut amener votre ordinateur à être utilisé à des fins illégales.

Logiciels espions

Les logiciels espions sont des logiciels qui peuvent enregistrer vos informations personnelles.

Les logiciels espions peuvent collecter des informations personnelles, telles que :

- sites Internet que vous avez visités,
- adresses électroniques sur votre ordinateur,
- mots de passe ou
- numéros de carte bancaire.

Un logiciel espion s'installe dans la plupart des cas de lui-même, sans votre accord. L'installation d'un logiciel espion peut s'effectuer lorsque vous installez un autre programme utile ou lorsque vous cliquez sur une option dans une fenêtre contextuelle trompeuse.

Programmes de base

Les programmes de base sont des programmes compliquant la recherche d'un *programme malveillant*.

Les programmes de base masquent les fichiers et processus. En général, ils procèdent ainsi pour masquer une activité malveillante sur votre ordinateur. Lorsqu'un programme de base masque un *programme malveillant*, vous ne le détectez pas facilement.

Ce produit est doté d'un moteur d'analyse de programmes de base qui recherche tout particulièrement ce type de programme. Un *programme malveillant* peut ainsi difficilement être masqué.

Programmes à risque

Un riskware (programme à risque) n'est pas conçu spécifiquement pour endommager votre ordinateur, mais il peut le faire s'il est mal utilisé.

Les riskwares (programmes à risque) ne correspondent pas forcément à des programmes malveillants. Les programmes « riskware » effectuent certaines opérations utiles, mais potentiellement dangereuses.

Exemples de programmes à risque :

- programmes de messagerie instantanée (IRC, Internet relay chat, par exemple),
- programmes de transfert de fichiers sur Internet d'un ordinateur à un autre,
- ou programmes téléphoniques sur Internet (VoIP, *Voix sur IP (Internet Protocol)*).
- Logiciel d'accès à distance, tel que VNC,
- les programmes « scareware », dont le but est d'effrayer ou d'escroquer les utilisateurs afin qu'ils achètent des logiciels de sécurité fictifs ou
- les logiciels conçus afin de contourner les analyses de CD ou protections des copies.

Si vous avez installé et configuré correctement le programme, sa dangerosité est moindre.

Si le programme à risque est installé sans que vous le sachiez, il peut s'agir d'une intention malveillante et doit être supprimé.

Chapitre

4

Protection contre les programmes malveillants

Sujets :

- *Comment analyser mon ordinateur ?*
- *Comment exclure des fichiers de l'analyse ?*
- *Comment fonctionne la mise en quarantaine ?*
- *Qu'est-ce que DeepGuard ?*

La recherche de virus et logiciels espions protège votre ordinateur de programmes pouvant dérober des informations personnelles, endommager le serveur ou utiliser ces données à des fins illégales.

Par défaut, tous les types de logiciels malveillants sont traités dès leur détection. Ils ne peuvent ainsi causer aucun dégât.

Par défaut, toutes les recherches de virus et de logiciels espions analysent automatiquement vos disques durs locaux, les supports amovibles (lecteurs portables, disques compact, etc.) et le contenu téléchargé. Vous pouvez configurer l'analyse pour qu'elle analyse automatiquement vos e-mails.

La recherche de virus et logiciels espions surveille tout changement sur votre ordinateur pouvant indiquer la présence de *logiciels malveillants*. Si un système dangereux change la configuration système par exemple ou tente de modifier d'importants processus système, DeepGuard empêche ce programme de fonctionner car il s'agit probablement d'un *logiciel malveillant*.

Comment analyser mon ordinateur ?

Lorsque la recherche de virus et logiciels espions est activée, les fichiers nuisibles sont recherchés automatiquement. Vous pouvez également analyser les fichiers manuellement et configurer des analyses planifiées.

Nous vous conseillons de toujours laisser la recherche de virus et logiciels espions activée. Analysez vos fichiers manuellement quand vous voulez vous assurer qu'aucun fichier nuisible ne se trouve sur votre ordinateur ou quand vous voulez analyser des fichiers exclus des analyses en temps réel.

En configurant une analyse planifiée, la recherche de virus et logiciels espions supprime les fichiers nuisibles de votre ordinateur à des moments précis.

Analyser les fichiers automatiquement

L'analyse en temps réel protège l'ordinateur en analysant tous les accès aux fichiers et en bloquant cet accès aux fichiers contenant des *programmes malveillants*.

Lorsque votre ordinateur essaie d'accéder à un fichier, l'analyse en temps réel recherche d'éventuels logiciels malveillants avant d'autoriser votre ordinateur à y accéder. Si l'analyse en temps réel découvre du contenu nuisible, elle place le fichier en quarantaine avant qu'il ne puisse causer de problèmes.

Est-ce que l'analyse en temps réel affecte les performances de mon ordinateur ?

Normalement, vous ne remarquez pas le processus d'analyse car il ne prend que très peu de temps et de ressources système. La durée et les ressources système utilisées par l'analyse en temps réel dépend, par exemple, du contenu, de l'emplacement et du type de fichier.

Fichiers dont l'analyse est longue :

- Fichiers sur disques amovibles tels que lecteurs CD, DVD et USB portables.
- Fichiers compressés, tels que les*fichiers .zip*.

  Remarque: Les fichiers comprimés ne sont pas comprimés par défaut.

L'analyse en temps réel peut ralentir votre ordinateur si :

- vous disposez d'un ordinateur qui ne respecte pas les conditions requises, ou
- vous accédez à de nombreux fichiers simultanément. Par exemple, quand vous ouvrez un répertoire qui contient de nombreux fichiers à analyser.

Activer ou désactiver l'analyse en temps réel

Laissez l'analyse en temps réel activée pour bloquer tout *logiciel malveillant* avant qu'il n'endommage votre ordinateur.

Pour activer ou désactiver l'analyse en temps réel :

1. Sur la page principale, cliquez sur **Statut**.
2. Cliquez sur **Modifier les paramètres de cette page**.

   Remarque: Vous devez disposer de droits d'administrateur pour désactiver les fonctionnalités de sécurité.

3. Activez ou désactivez **la recherche de virus et logiciels espions**.
4. Cliquez sur **Fermer**.

Gérer les fichiers nuisibles automatiquement

L'analyse en temps réel peut gérer les fichiers nuisibles automatiquement sans vous consulter.

Pour laisser l'analyse en temps réel gérer les fichiers nuisibles automatiquement :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Sécurité de l'ordinateur** > **Recherche de virus et logiciels espions**.
3. Sélectionnez **Gérer les fichiers nuisibles automatiquement**.

Si vous décidez de gérer les fichiers nuisibles automatiquement, l'analyse en temps réel vous demande ce qu'il convient de faire lorsqu'un fichier nuisible est découvert.

Gérer les logiciels espions

La recherche de virus et logiciels espions bloque immédiatement tout logiciel espion qui essaie de démarrer.

Avant qu'une application espion ne puisse démarrer, le produit la bloque et vous demande ce que vous voulez faire.

Choisissez l'une des actions suivantes lorsqu'un logiciel espion est détecté :

Action à entreprendre	Action effectuée sur le logiciel espion
Gérer automatiquement	Laisser le produit décider de la meilleure action à effectuer en fonction du logiciel espion trouvé.
Mettre le logiciel espion en quarantaine	Déplacer le logiciel espion en quarantaine où il ne peut pas provoquer de dégâts.
Supprimer le logiciel espion	Supprimer tous les fichiers liés au logiciel espion de votre ordinateur.
Bloquer uniquement le logiciel espion	Bloquer l'accès au logiciel espion, mais le conserver sur votre ordinateur.
Exclure le logiciel espion de l'analyse	Autoriser le logiciel espion à s'exécuter, mais l'exclure de l'analyse à l'avenir.

Gérer les programmes à risque

La recherche de virus et logiciels espions bloque immédiatement tout programme à risque qui essaie de démarrer.

Avant qu'une application à risque ne puisse démarrer, le produit la bloque et vous demande ce que vous voulez faire.

Choisissez l'une des actions suivantes lorsqu'un programme à risque est détecté :

Action à entreprendre	Action effectuée sur le programme à risque
Bloquer uniquement le programme à risque	Bloquer l'accès au programme à risque, mais le conserver sur votre ordinateur.
Mettre le programme à risque en quarantaine	Déplacer le programme à risque en quarantaine où il ne peut pas provoquer de dégâts.
Supprimer le programme à risque	Supprimer tous les fichiers liés au programme à risque de votre ordinateur.

Action à entreprendre	Action effectuée sur le programme à risque
Exclure le programme à risque de l'analyse	Autoriser l'exécution du programme à risque, mais l'exclure de l'analyse à l'avenir.

Supprimer automatiquement les cookies de suivi

En supprimant les cookies de suivi, vous empêchez les sites Web de suivre les sites que vous visitez sur Internet.

Les cookies de suivi sont de petits fichiers qui permettent aux sites Web d'enregistrer les sites que vous avez visités. Suivez ces instructions pour éliminer les cookies de suivi de votre ordinateur.

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Sécurité de l'ordinateur** > **Recherche de virus et logiciels espions**.
3. Sélectionnez **Supprimer les cookies de suivi**.
4. Cliquez sur **OK**.

Analyser les fichiers manuellement

Vous pouvez analyser vos fichiers manuellement, par exemple quand vous connectez un périphérique externe à votre ordinateur, pour vous assurer qu'il ne contient pas de logiciel malveillant.

Démarrage de l'analyse manuelle

Vous pouvez analyser l'ordinateur entier ou un type spécifique de *programme malveillant* ou un emplacement spécifique.

Si vous suspectez un certain type de *programme malveillant* , vous pouvez n'analyser que ce type. Si vous suspectez un emplacement donné de l'ordinateur, vous pouvez n'analyser que cet emplacement. Ces analyses seront plus rapides qu'une analyse complète de l'ordinateur.

Pour lancer manuellement l'analyse de votre ordinateur :

1. Sur la page principale, cliquez sur la flèche située sous **Analyse**.

   Les options d'analyse s'affichent.

2. Sélectionnez le type d'analyse.

   Sélectionnez **Modifier les paramètres d'analyse** pour optimiser la manière dont l'analyse manuelle recherche des virus et autres applications nuisibles sur votre ordinateur.

3. Si vous avez choisi **Sélectionner les éléments à analyser**, vous pouvez indiquer l'emplacement à analyser dans la fenêtre qui s'ouvre.
   L' **Assistant d'analyse** s'ouvre.

Types d'analyses

Vous pouvez analyser l'ordinateur entier ou un type spécifique de programme malveillant ou un emplacement spécifique.

Voici les différents types d'analyses :

Type d'analyse	Sur quoi porte l'analyse ?	Quand utiliser ce type ?
Recherche de virus et logiciels espions	Certaines parties de votre ordinateur sont analysées pour	Ce type d'analyse est beaucoup plus rapide qu'une analyse complète. Il ne recherche que les parties de votre système contenant des fichiers programmes

Type d'analyse	Sur quoi porte l'analyse ?	Quand utiliser ce type ?
	détecter la présence éventuelle de virus, logiciels espion et riskware.	installés. Ce type d'analyse est recommandé si vous souhaitez vérifier rapidement que votre ordinateur est propre, car il permet de rechercher et de supprimer efficacement tout programme malveillant installé sur votre ordinateur.
Analyse complète de l'ordinateur	Recherche de virus, de logiciels espions et de riskware dans l'intégralité de votre ordinateur (disques durs internes et externes)	Lorsque vous voulez être sûr qu'il n'y a aucun programme malveillant ou programme à risque sur votre ordinateur. Ce type d'analyse est celui qui prend le plus de temps. Il associe la détection rapide des programmes malveillants et l'analyse du disque dur. Il recherche également les éléments susceptibles d'être dissimulés derrière un rootkit.
Sélectionner les éléments à analyser	Analyser un fichier, dossier ou lecteur particulier pour détecter la présence éventuelle de virus, logiciels espions et riskware	Vous suspectez la présence d'un programme malveillant à un emplacement précis de votre ordinateur, tel que le dossier contenant des téléchargements provenant de sources potentiellement dangereuses (par exemple les réseaux peer-to-peer de partage de fichiers). La durée de l'analyse dépend de la taille de la cible à analyser. L'analyse se fait rapidement si vous analysez un dossier contenant uniquement quelques petits fichiers.
Analyse du rootkit	Emplacements système importants où un élément suspect peut entraîner un problème de sécurité. Analyse les fichiers, dossiers, lecteurs et processus cachés.	Lorsque vous soupçonnez la présence d'un rootkit sur votre ordinateur. Par exemple, si un programme a été récemment détecté sur votre ordinateur et vous souhaitez vous assurer qu'il n'a pas installé de rootkit.

Analyse dans l'Explorateur Windows

Vous pouvez analyser des disques, dossiers et fichiers à la recherche de *virus*, *logiciels espions* et *programmes à risque* dans l'Explorateur Windows.

Pour analyser un disque, un dossier ou un fichier :

1. Placez le pointeur de la souris et cliquez avec le bouton droit sur le disque, dossier ou fichier à analyser.
2. Dans le menu contextuel, sélectionnez **Analyser des dossiers à la recherche de virus**. Le nom de l'option dépend de l'élément analysé : disque, dossier ou fichier.
   La fenêtre **Assistant d'analyse** s'ouvre et l'analyse démarre.

Si un *virus* ou un *logiciel espion* est détecté, l'**Assistant d'analyse** vous guide dans les étapes de nettoyage.

Sélectionner des fichiers à analyser

Sélectionnez les types de fichiers à analyser à la recherche de *virus* et de *logiciel espion* lors d'analyses manuelles ou planifiées.

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Autres paramètres** > **Analyse manuelle**.
3. Dans **Options d'analyse**, sélectionnez parmi les paramètres suivants :

Analyser uniquement des types de fichiers connus	Pour analyser uniquement les fichiers suscpetibles de présenter des infections, par exemple les fichiers exécutables. Cette option permet également d'accélérer l'analyse. Elle prendra en compte les fichiers ayant les extensions suivantes : `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` et `.hqx`.
Analyser le contenu des fichiers compressés	Analyser des fichiers et dossiers compressés :
Utiliser une heuristique avancée	Lors de l'analyse, utilisez toute l'heuristique disponible afin d'optimiser la découverte de programmes malveillants inconnus ou nouveaux. **Remarque:** Si vous optez pour cette option, l'analyse prend plus de temps et peut indiquer davantage de faux positifs (des fichiers inoffensifs signalés comme suspects).

4. Cliquez sur **OK**.

Remarque: Les fichiers figurant dans la liste des exclusions ne sont pas analysés, même si vous les sélectionnez pour l'analyse.

Que faire si des fichiers nuisibles sont détectés ?

Choisissez comment traiter les fichiers nuisibles détectés.

Pour déterminer l'action à entreprendre si du contenu dangereux est découvert pendant l'analyse manuelle :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Autres paramètres** > **Analyse manuelle**.
3. Dans **Lorsqu'un virus ou un logiciel espion est détecté**, sélectionnez une des options suivantes :

Option	Description
Me demander (par défaut)	Vous pouvez choisir une mesure à prendre pour chaque élément découvert lors d'une analyse manuelle.
Nettoyer les fichiers	Le produit tente de nettoyer automatiquement les fichiers infectés détectés lors de l'analyse manuelle. **Remarque:** Si le produit ne peut pas nettoyer le fichier infecté, ce dernier est placé en quarantaine (sauf s'il se trouve sur le réseau ou des disques amovibles) afin de ne pas endommager l'ordinateur.
Mettre les fichiers en quarantaine	Le produit déplace tout fichier nuisible découvert pendant l'analyse manuelle en quarantaine où il ne peut pas endommager l'ordinateur.
Supprimer les fichiers	Le produit supprime tout fichier nuisible découvert pendant l'analyse manuelle.

Option	Description
Signaler uniquement	Le produit laisse les fichiers nuisibles découverts pendant l'analyse manuelle tels qu'ils sont et signale la détection dans le rapport d'analyse. **Remarque:** Lorsque l'analyse en temps réel est désactivée, les programmes malveillants peuvent nuire à votre ordinateur si vous sélectionnez cette option.

Remarque: Lorsque des fichiers nuisibles sont détectés pendant l'analyse manuelle, ils sont nettoyés automatiquement.

Planifier une analyse

Configurez votre ordinateur de sorte à rechercher et supprimer automatiquement les virus et autres applications nuisibles quand vous ne l'utilisez pas. Vous pouvez aussi définir une exécution régulière d'analyses pour vous assurer que votre ordinateur est exempt de tels programmes.

Pour planifier une analyse :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Autres paramètres** > **Analyse planifiée**.
3. Activez l'**analyse planifiée**.
4. Choisissez à quel moment vous voulez lancer l'analyse.

Option	Description
Tous les jours	Analysez votre ordinateur tous les jours.
Toutes les semaines	Analysez votre ordinateur certains jours de la semaine. Choisissez les jours dans la liste.
Tous les mois	Analysez votre ordinateur certains jours du mois. Pour choisir des jours : 1. Sélectionnez parmi les options **Jour**. 2. Sélectionnez le jour du mois dans la liste en regard du jour sélectionné.

5. Sélectionnez le moment souhaité pour démarrer l'analyse les jours sélectionnés.

Option	Description
Heure début	Commencez l'analyse à l'heure spécifiée.
Si l'ordinateur est inutilisé pendant	Commencez l'analyse lorsque vous n'avez pas utilisé votre ordinateur pendant l'intervalle spécifié.

L'analyse planifiée exploite les mêmes paramètres que l'analyse manuelle, sauf qu'elle analyse systématiquement les archives et nettoie automatiquement les fichiers nuisibles.

Analyser les e-mails

L'analyse du courrier électronique vous protège contre les fichiers nuisibles contenus dans les messages qui vous sont envoyés.

La recherche de virus et logiciels espions doit être activée pour pouvoir rechercher des virus dans les e-mails.

Pour activer l'analyse du courrier électronique :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Sécurité de l'ordinateur** > **Recherche de virus et logiciels espions**.
3. Sélectionnez **Supprimer les pièces jointes nuisibles**.
4. Cliquez sur **OK**.

Quand les e-mails et les pièces jointes sont-ils analysés ?

L'analyse de virus et de logiciels espions permet de supprimer les contenus dangereux des courriels que vous recevez.

L'analyse de virus et logiciels espions supprime les courriels dangereux arrivant dans les boîtes aux lettres de vos programmes de messagerie tels que Microsoft Outlook et Outlook Express, Microsoft Mail ou Mozilla Thunderbird. Elle analyse les courriels et les pièces jointes à chaque fois que votre programme de messagerie reçoit un courriel du serveur au moyen du protocole POP3.

La recherche de virus et logiciels espions ne peut pas analyser les e-mails des messageries Web qui englobent des applications exécutées dans votre navigateur Web, comme Hotmail, Yahoo! mail ou Gmail. Vous êtes toujours protégé contre les *virus*, même si vous ne supprimez pas les pièces jointes nuisibles ou si vous utilisez une messagerie Web. Lorsque vous ouvrez vos pièces jointes, l'analyse en temps réel supprime tout fichier nuisible avant qu'il ne provoque de dégâts.

Remarque: L'analyse en temps réel protège votre ordinateur, mais pas vos amis. L'analyse en temps réel n'analyse les pièces jointes que si vous les ouvrez. Cela signifie que si vous utilisez une messagerie Web et que vous transférez un e-mail avant d'ouvrir la pièce jointe, vous pouvez envoyer des fichiers infectés à vos amis.

Afficher les résultats de l'analyse

L'historique de la recherche de virus et logiciels espions répertorie tous les fichiers nuisibles détectés par le produit.

Il arrive que le produit ne puisse pas effectuer l'action choisie lorsqu'il détecte du contenu indésirable. Par exemple, si vous décidez de nettoyer des fichiers et si un fichier ne peut pas l'être, le produit l'envoie en quarantaine. Vous avez accès à ces informations dans l'historique.

Pour afficher l'historique :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Sécurité de l'ordinateur** > **Recherche de virus et logiciels espions**.
3. Cliquez sur **Afficher l'historique des suppressions**.

L'historique de recherches de virus et logiciels espions présente les informations suivantes :

- date et heure à laquelle le fichier nuisible a été détecté,
- nom du logiciel malveillant et emplacement sur l'ordinateur, et
- action entreprise.

Comment exclure des fichiers de l'analyse ?

Vous voudrez parfois exclure certains fichiers ou certaines applications d'une analyse. Les éléments exclus ne seront pas analysés sauf si vous les retirez de la liste des exclusions.

Remarque: Il existe des listes des exclusions distinctes pour les analyses manuelles et en temps réel. Par exemple, si vous excluez un fichier de l'analyse en temps réel, il sera analysé lors d'une analyse manuelle sauf si vous l'excluez également de ce deuxième type d'analyse.

Exclure des types de fichiers

Lorsque vous excluez des fichiers en fonction de leur type, le produit ne recherche pas de contenu nuisible dans les fichiers portant l'extension spécifiée.

Pour ajouter ou supprimer des types de fichiers à exclure :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Choisissez si vous voulez exclure le type de fichier de l'analyse manuelle ou en temps réel :
   - Sélectionnez **Sécurité de l'ordinateur** > **Recherche de virus et logiciels espions** pour exclure le type de fichier de l'analyse en temps réel.
   - Sélectionnez **Autres paramètres** > **Analyse manuelle** pour exclure le type de fichier de l'analyse manuelle.
3. Cliquez sur **Exclure des fichiers de l'analyse**.
4. Pour exclure un type de fichier :
   a) Sélectionnez l'onglet **Types de fichiers**.
   b) Sélectionnez **Exclure les fichiers avec ces extensions**.
   c) Saisissez une extension de fichier qui identifie le type de fichiers à exclure dans le champ se trouvant à côté du bouton **Ajouter**.

      Pour indiquer des fichiers sans extension, saisissez « . ». Vous pouvez également utiliser le caractère générique « ? » pour représenter un caractère quelconque ou « * » pour représenter un nombre quelconque de caractères.

      Pour exclure par exemple les fichiers exécutables, saisissez `exe` dans le champ.
   d) Cliquez sur **Ajouter**.
5. Répétez l'étape précédente pour toute autre extension que vous voulez exclure de l'analyse de recherche de virus.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Exclure de l'analyse**.
7. Cliquez sur **OK** pour appliquer les nouveaux paramètres.

Les types de fichiers sélectionnés sont exclus des analyses futures.

Exclure des fichiers par emplacement

Lorsque vous excluez des fichiers selon leur emplacement, le produit ne recherche pas de contenu nuisible dans les fichiers se trouvant dans les dossiers ou sur les disques spécifiés.

Pour ajouter ou supprimer des emplacements de fichiers à exclure :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Choisissez si vous voulez exclure l'emplacement de l'analyse manuelle ou en temps réel :
   - Sélectionnez **Système** > **Recherche de virus et logiciels espions** pour exclure un emplacement de l'analyse en temps réel.
   - Sélectionnez **Système** > **Analyse manuelle** pour exclure un emplacement de l'analyse manuelle.
3. Cliquez sur **Exclure des fichiers de l'analyse**.
4. Pour exclure un fichier, lecteur ou dossier :
   a) Cliquez sur l'onglet **Objets**.
   b) Sélectionnez **Exclure les objets (fichiers, dossiers, ...)**.
   c) Cliquez sur **Ajouter**.
   d) Sélectionnez le fichier, le lecteur ou le dossier que vous souhaitez exclure de l'analyse de virus.

      Remarque: Certains lecteurs sont peut-être amovibles, tels qu'un lecteur de CD, de DVD, ou des lecteurs réseau. Les lecteurs réseau sont vides et les lecteurs amovibles ne peuvent être exclus.

   e) Cliquez sur **OK**.
5. Répétez l'étape précédente pour exclure d'autres fichiers, lecteurs ou dossiers de l'analyse de virus.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Exclure de l'analyse**.
7. Cliquez sur **OK** pour appliquer les nouveaux paramètres.

Les fichiers, lecteurs ou dossiers sélectionnés sont exclus des analyses futures.

Afficher les applications exclues

Vous pouvez afficher les applications que vous avez exclues de l'analyse et les supprimer de la liste des exclusions, afin qu'elles soient prises en compte à l'avenir.

Si l'analyse en temps réel ou manuelle détecte une application qui se comporte comme un logiciel espion ou à risque, mais si vous savez qu'il s'agit d'un programme sûr, vous pouvez l'exclure de l'analyse pour que le produit n'émette plus d'avertissement.

Remarque: Si l'application se comporte tel un virus ou un autre logiciel malveillant, il est impossible de l'exclure.

Vous ne pouvez pas exclure d'applications directement. Les nouvelles applications apparaissent dans la liste des exclusions uniquement si vous les excluez lors de l'analyse.

Pour afficher les applications exclues de l'analyse :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Choisissez si vous voulez afficher les applications exclues de l'analyse manuelle ou en temps réel :
   - Sélectionnez **Système** > **Recherche de virus et logiciels espions** pour afficher les applications exclues de l'analyse en temps réel.
   - Sélectionnez **Système** > **Analyse manuelle** pour afficher les applications exclues de l'analyse manuelle.
3. Cliquez sur **Exclure des fichiers de l'analyse**.
4. Sélectionnez l'onglet **Applications**.

   Remarque: Seules des applications de logiciels espions et de programmes à risque peuvent être exclues, pas les virus.

5. Si vous voulez à nouveau analyser une application exclue :

a) Sélectionnez l'application que vous voulez à nouveau inclure dans l'analyse.
b) Cliquez sur **Supprimer**.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Exclure de l'analyse**.
7. Cliquez sur **OK** pour quitter.

Comment fonctionne la mise en quarantaine ?

La quarantaine est un référentiel sûr de fichiers pouvant être dangereux.

Les fichiers mis en quarantaine ne peuvent pas être diffusés ou endommager votre ordinateur.

Le produit peut mettre en quarantaine les *programmes malveillants*, *logiciels espions* et *riskwares* afin de les neutraliser. Vous pouvez restaurer les applications ou fichiers mis en quarantaine, en cas de besoin.

Si vous n'avez pas besoin d'un élément mis en quarantaine, vous pouvez le supprimer. La suppression d'un élément en quarantaine le supprime définitivement de l'ordinateur.

- En général, vous pouvez supprimer un *programme malveillant* mis en quarantaine.
- Dans la plupart des cas, vous pouvez supprimer un *logiciel espion* mis en quarantaine. Il est possible que le *logiciel espion* en quarantaine fasse partie d'un programme légitime et sa suppression empêche le programme de fonctionner correctement. Pour conserver le programme, vous pouvez restaurer le *logiciel espion* en quarantaine.
- Un *programme à risque* en quarantaine peut être un programme légitime. Si vous avez installé et configuré le programme, vous pouvez le restaurer de la quarantaine. Si le *programme à risque* est installé sans que vous le sachiez, il peut s'agir d'une intention malveillante et doit être supprimé.

Afficher les éléments mis en quarantaine

Vous pouvez afficher plus d'informations concernant les éléments en quarantaine.

Pour afficher des informations détaillées sur les éléments en quarantaine :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Sécurité de l'ordinateur** > **Recherche de virus et logiciels espions**.
3. Cliquez sur **Afficher le dossier de quarantaine**.
   La page **Quarantaine** récapitule le nombre total d'éléments mis en quarantaine.
4. Pour afficher des informations détaillés sur les éléments de la quarantaine, cliquez sur **Détails**.

   Vous pouvez trier le contenu soit par nom de logiciel malveillant soit par chemin de fichier.

   Une liste des 100 premiers éléments s'affiche avec le type et le nom des objets mis en quarantaine, ainsi que le chemin vers les fichiers qui les contiennent.
5. Pour plus d'informations sur un élément mis en quarantaine, cliquez sur l'icône en regard de l'élément dans la colonne **Statut**.

Restaurer les éléments mis en quarantaine

Vous pouvez restaurer des éléments mis en quarantaine dont vous avez besoin.

Vous pouvez restaurer des applications ou des fichiers de la quarantaine si vous en avez besoin. Ne restaurez des éléments de la quarantaine que si vous êtes convaincu qu'ils n'entraînent aucune menace. Les éléments restaurés retrouvent leur emplacement d'origine de l'ordinateur.

Restaurer les éléments mis en quarantaine

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Sécurité de l'ordinateur** > **Recherche de virus et logiciels espions**.
3. Cliquez sur **Afficher le dossier de quarantaine**.
4. Sélectionnez les éléments mis en quarantaine que vous souhaitez restaurer.
5. Cliquez sur **Restaurer**.

Qu'est-ce que DeepGuard ?

DeepGuard analyse le contenu des fichiers et le comportement des applications, et surveille les applications qui ne sont pas sûres.

DeepGuard bloque les nouveaux *virus* et les virus inconnus, les *vers* et les autres applications dangereuses essayant de modifier votre ordinateur, et empêche toute application suspecte d'accéder à Internet.

Lorsque DeepGuard détecte une nouvelle application qui essaie d'effectuer des changements potentiellement nuisibles à votre système, il autorise l'exécution de l'application dans une zone sécurisée. L'application ne peut donc pas endommager votre ordinateur. DeepGuard analyse les modifications que l'application voulait apporter et décide ensuite si cette application est susceptible d'être un *logiciel malveillant*. Si l'application est un *logiciel malveillant* potentiel, DeepGuard la bloque.

DeepGuard détecte les modifications système potentiellement nuisibles suivantes :

- la modification de paramètres système (registre Windows),
- les tentatives de désactivation de programmes système importants, des programmes de sécurité comme ce produit par exemple, et
- les tentatives de modification de fichiers système importants.

Activer ou désactiver DeepGuard

Laissez DeepGuard activé pour empêcher les applications suspectes d'apporter des modifications potentiellement dangereuses à votre système.

Si vous êtes équipé de Windows XP, assurez-vous d'avoir installé le Service Pack 2 avant d'activer DeepGuard.

Pour activer ou désactiver DeepGuard :

1. Sur la page principale, cliquez sur **Statut**.
2. Cliquez sur **Modifier les paramètres de cette page**.

   Remarque: Vous devez disposer de droits d'administrateur pour désactiver les fonctionnalités de sécurité.

3. Activez ou désactivez **DeepGuard**.
4. Cliquez sur **Fermer**.

Autoriser les applications bloquées par DeepGuard

Vous pouvez contrôler le blocage ou l'autorisation des applications par DeepGuard.

Il arrive que DeepGuard bloque une application fiable, alors que vous voulez l'utiliser et que vous savez qu'elle n'est pas dangereuse. Vous êtes confronté à cette situation lorsqu'une application essaie d'apporter des changements potentiellement nuisibles au système. Vous avez aussi peut-être bloqué une application par mégarde via une fenêtre contextuelle DeepGuard.

Pour autoriser une application bloquée par DeepGuard :

1. Dans la page principale, cliquez sur **Outils**.
2. Cliquez sur **Applications**.
   La liste **Applications surveillées** s'affiche.
3. Recherchez l'application à autoriser.

   Remarque: Vous pouvez cliquer sur les titres de colonnes pour trier la liste. Cliquez par exemple sur la colonne **Autorisation** pour classer la liste en groupes de programmes autorisés et refusés.

4. Sélectionnez **Autoriser** dans la colonne **Autorisation**.
5. Cliquez sur **Fermer**.

DeepGuard autorise à nouveau l'application à apporter des modifications au système.

Utiliser DeepGuard en mode de compatibilité

Pour une protection optimale, DeepGuard modifie temporairement les programmes en cours d'exécution. Certains programmes vérifient qu'ils n'ont pas été corrompus ou modifiés et peuvent donc être incompatibles avec cette fonctionnalité. Par exemple, les jeux en ligne dotés d'outils évitant la triche s'assurent qu'ils n'ont pas été modifiés lorsqu'ils sont exécutés. Dans ce cas, vous pouvez activer le mode de compatibilité.

Pour activer le mode de compatibilité :

1. Sur la page principale, cliquez sur **Paramètres**.

   Remarque: Vous devez disposer des droits administratifs pour modifier les paramètres.

2. Sélectionnez **Sécurité de l'ordinateur** > **DeepGuard**.
3. Sélectionnez **Utiliser le mode de compatibilité**.
4. Cliquez sur **OK**.

Que faire en cas d'avertissements pour comportements suspects ?

DeepGuard surveille les applications qui ne sont pas sûres. DeepGuard bloque toute application surveillée qui tente d'accéder à Internet, de modifier votre système ou montre un autre comportement suspect.

Lorsque vous avez sélectionné le paramètre DeepGuard **Me signaler tout comportement suspect**, DeepGuard vous informe s'il détecte une application potentiellement dangereuse ou si vous lancez une application inconnue.

Pour déterminer l'action à entreprendre quand DeepGuard bloque une application :

1. Cliquez sur **Détails** pour en savoir plus sur le programme.
   La section des détails vous présente les données suivantes :
   - l'emplacement de l'application,
   - la réputation de l'application sur le réseau de protection en temps réel, et
   - si l'application est répandue.
2. Précisez si vous faites confiance à l'application bloquée par DeepGuard :
   - Choisissez **Je fais confiance à cette application. Poursuivre son exécution.** si vous ne souhaitez pas bloquer l'application.

     L'application est susceptible d'être sûre si :

     - DeepGuard a bloqué l'application suite à une de vos actions,
     - vous connaissez l'application, ou

    - vous avez obtenu cette application d'une source fiable.

  - Choisissez **Je ne fais pas confiance à cette application. La bloquer.** si vous souhaitez bloquer l'application.

    L'application est susceptible de ne pas être sûre si :

    - l'application n'est pas très répandue,
    - la réputation de l'application n'est pas connue, ou
    - vous ne connaissez pas l'application.

3. Si vous voulez faire analyser une application suspecte :
   a) Cliquez sur **Signaler l'application à F-Secure**.
      Le produit affiche les conditions d'envoi.
   b) Cliquez sur **Accepter** si vous approuvez les conditions et si vous voulez envoyer un échantillon.

   Nous vous conseillons d'envoyer un échantillon quand :

   - DeepGuard bloque une application qui est fiable selon vous, ou
   - vous suspectez l'application d'être un *logiciel malveillant*.