F-Secure Anti-Virus 2013

Contenu

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:Comment démarrer.....9

Utilisation des mises à jour automatiques.....10
Vérification de l'état des mises à jour.....10
Modification des paramètres de connexion Internet.....10
Vérifier l'état du réseau de protection en temps réel.....11
Comment afficher les activités du produit?.....11
Affichage de l'historique des notifications.....11
Modification des paramètres de notification.....11
Le réseau de protection en temps réel.....12
Qu'est-ce que le réseau de protection en temps réel?.....12
Avantages du réseau de protection en temps réel.....12
Quelles données fournissez-vous?.....13
Protection de votre vie privée.....14
Contribution au réseau de protection en temps réel.....15
Questions à propos du réseau de protection en temps réel.....15
Placement du pointeur de la souris sur l'icône d'état pour afficher l'info bulle de l'état.....15
Centre d'action.....16
Activation d'un abonnement.....16

Chapitre 3:Présentation.....17

Affichage de l'état général de ma protection.....18
Affichage des statistiques du produit.....18
Gérer les mises à jour du produit.....19
Affichage des versions de bases de données.....19
Changement des paramètres du haut débit mobile.....19
Virus et autres maliciels.....20
Virus.....20
Logiciels espions.....21
Rootkits.....21
Programmes à risque.....21

Chapitre 4:Protection de l'ordinateur contre les maliciels.....23
Analyse de l'ordinateur.....24
Analyse automatique des fichiers.....24
Analyse manuelle de fichiers.....26
Analyse des courriels.....29
Affichage des résultats de l'analyse.....30
Exclusion des fichiers de l'analyse.....30
Exclusion des types de fichiers.....30
Exclusion des fichiers en fonction de l'emplacement.....31
Affichage des applications exclues.....32
Utilisation de la quarantaine.....32
Affichage des articles mis en quarantaine.....33
Restauration des articles mis en quarantaine.....33
Que'est-ce que DeepGuard?.....34
Activer ou désactiver DeepGuard.....34
Autorisation des applications bloquées par DeepGuard.....34
Utilisation de DeepGuard en mode de compatibilité.....35
Que faire lors d'avertissements de comportement suspect.....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

Nous vous remercions de choisir F-Secure.

Pour installer le produit, vous avez besoin de ce qui suit :

- Le CD d'installation ou une trousse d'installation. Si vous utilisez un netbook sans lecteur de CD, vous pouvez télécharger la trousse d'installation du site *www.f-secure.com/netbook*.
- Votre clé d'abonnement.
- Une connexion Internet.

Si vous utilisez un produit de sécurité d'un autre fournisser est installé, l'installateur tentera de le désinstaller automatiquement. Si ce processus ne fonctionne pas, veuillez effectuer une désinstallation manuelle.

Nota: Si vous avez plus d'un compte sur l'ordinateur, connectez-vous sur le compte avec privilèges d'administrateur pour exécuter l'installation.

Première installation du produit

Instructions d'installation du produit

Veuillez suivre ces instructions pour installer le produit :

1. Insérez le CD ou cliquez deux fois sur l'installateur que vous avez téléchargé.

   Si le CD ne démarre pas automatiquement, ouvrez Windows Explorer, cliquez deux fois sur l'icône du CD-ROM, puis deux fois sur le fichier d'installation pour lancer l'installation.

2. Suivez les instructions à l'écran.

   - Si vous avez acheté le produit sur un CD chez un détaillant, vous trouverez la clé d'abonnement sur la couverture du Guide d'installation rapide.
   - Si vous avez téléchargé le produit d'un magasin en ligne de F-Secure, la clé d'abonnement est incluse dans le courriel de confirmation de votre commande d'achat.

   Il faudra peut-être redémarrer l'ordinateur avant de valider l'abonnement et de télécharger les mises à jour de l'Internet. Si vous installez à partir d'un CD, n'oubliez pas de le retirer avant de redémarrer l'ordinateur.

Installation et mise à niveau des applications

Instructions d'activation d'un nouvel abonnement

Suivez ces instructions pour activer votre nouvel abonnement ou pour installer une nouvelle application à l'aide de la zone de lancement :

Nota: L'icône de zone de lancement se trouve dans la barre d'état système.

1. Dans la zone de lancement, cliquez sur l'icône la plus à droite.
   Un menu contextuel apparaît.
2. Sélectionnez **Afficher mes abonnements**
3. Sous **Mes abonnements**, accédez à la page **État de l'abonnement** et cliquez sur **Activer l'abonnement**.
   La fenêtre **Activer l'abonnement** apparaît.

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

Le nouvel abonnement a été activé.

Aide et assistance

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

Après avoir enregistré votre licence, vous avez droit à des services supplémentaires comme des mises à jour de produits gratuites et un support pour le produit. Vous pouvez vous inscrire sur le site *www.f-secure.com/register*.

Chapitre

2

Comment démarrer

Sujets :

- *Utilisation des mises à jour automatiques*
- *Comment afficher les activités du produit?*
- *Le réseau de protection en temps réel*
- *Placement du pointeur de la souris sur l'icône d'état pour afficher l'info bulle de l'état.*

Informations sur la première utlisation du produit.

Cette section décrit la manière de modifier les paramètres communs et de gérer vos abonnements par l'entremise de la zone de lancement.

Les paramètres communs de la zone de lancement s'appliquent à tous les programmes installés dans cette zone. Plutôt que de modifier les paramètres séparément pour chaque programme, il vous suffit de modifier les paramètres communs, qui sont alors utilisés par tous les programmes installés.

Les paramètres communs de la zone de lancement incluent ce qui suit :

- Téléchargements, où vous pouvez afficher des renseignements sur les mises à jour téléchargées et vérifier manuellement si de nouvelles mises à jour sont offertes.
- Paramètres de connexion, où vous pouvez modifier la manière dont votre ordinateur se connecte à Internet.
- Notifications, où vous pouvez afficher les anciennes notifications et définir les 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 pour les programmes installés au moyen de la zone de lancement.

Utilisation des mises à jour automatiques

Les mises à jour automatiques permettent de garder à jour la protection de votre ordinateur.

L'agent de mise à jour automatique F-Secure récupère les dernières mises à jour lorsque vous êtes connecté à Internet. Il détecte le trafic réseau et ne pertube pas les autres utilisations d'Internet même si la connexion réseau est lente.

Vérification de l'état des mises à jour

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

Lorsque la fonction de mises à jour automatique est activée, le produit reçoit automatiquement les mises à jour les plus récentes 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 l'icône la plus à droite.
   Un menu contextuel apparaît.
2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez **Mises à jour automatiques** > **Téléchargements**.
4. Cliquez sur **Vérifier maintenant**.
   Le produit se connecte à Internet et vérifie la disponibilité des mises à jour les plus récentes. Il récupère les dernières mises à jour si la protection est obsolète.

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

Modification des paramètres de connexion Internet

Il n'est généralement pas nécessaire de modifier les paramètres par défaut, mais vous pouvez configurer la manière dont le serveur est connecté à Internet afin de recevoir automatiquement des mises à jour.

Pour modifier les paramètres de connexion Internet :

1. Dans la zone de lancement, cliquez sur l'icône la plus à droite.
   Un menu contextuel apparaît.
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 comme permanente** si vous disposez d'une connexion réseau permanente.

     Nota: 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.

     Conseil: 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 **proxy HTTP**, sélectionnez si oui ou non votre ordinateur utilise un *serveur proxy* pour se connecter à Internet.
   - Sélectionnez **Pas de proxy HTTP** si votre ordinateur est directement connecté à Internet.
   - Sélectionnez **Configurer manuellement le proxy HTTP** pour configurer les paramètres de *serveur proxy HTTP*.
   - Sélectionnez **Utiliser le proxy HTTP de mon navigateur** > **Utiliser le proxy HTTP**du navigateur pour utiliser les mêmes paramètres de serveur *proxy HTTP* que ceux configurés dans votre navigateur Web.

Vérifier l'état du réseau de protection en temps réel

Le bon fonctionnement de plusieurs fonctions dépend 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 l'état passe à « déconnecté ». Si aucune des fonctions du produit installé n'exige un accès au réseau de protection en temps réel, l'état passe à « non utilisé ».

Pour vérifier l'état :

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

Sous **Réseau de protection en temps réel**, vous pouvez voir l'état actuel du réseau de protection en temps réel.

Comment afficher les activités du produit?

Vous pouvez afficher les actions exécutées par le produit pour protéger votre ordinateur en accédant à la page **Notifications**.

Le produit affichera une notification lorsqu'il exécute une action, par exemple lorsqu'il détecte un virus et qui le bloque. Certaines notifications peuvent également être envoyées par votre fournisseur de services, par exemple pour vous informer sur de nouveaux services offerts.

Affichage de l'historique des notifications

Vous pouvez voir les notifications qui ont été affichées dans l'historique des notifications

Pour afficher l'historique des notifications :

1. Dans la zone de lancement, cliquez sur l'icône la plus à droite.
   Un menu contextuel apparaît.
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 apparaît.

Modification des paramètres de notification

Vous pouvez sélectionner le type de notifications affichées par le produit.

Pour modifier les paramètres de notification :

1. Dans la zone de lancement, cliquez sur l'icône la plus à droite.
   Un menu contextuel apparaît.
2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez **Autre** > **Notifications**.
4. Sélectionnez ou effacez **Autoriser les messages de programmes** pour activer ou désactiver les messages de programmes.

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

Le 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 les sites Web fiables tout en offrant une protection contre les maliciels et les attaques des sites Web.

Qu'est-ce que le réseau de protection en temps réel?

Le réseau de protection en temps réel est un service en ligne qui réagit rapidement aux menaces les plus récentes provenant d'Internet.

En tant que contributeur au réseau de protection en temps réel, vous pouvez nous aider à renforcer la protection contre les menaces nouvelles et émergentes. Le réseau de protection en temps réel collecte les statistiques de certaines applications inconnues, malicieuses ou suspectes et leurs activités sur votre machine. Ces renseignements sont anonymes et sont envoyés à F-Secure Corporation pour être soumis à une analyse de données combinées. Nous utilisons les renseignements analysés pour améliorer la sécurité de votre machine contre les menaces les plus récentes et contre les fichiers malicieux.

Principes de fonctionnement du réseau de protection en temps réel

En tant que contributeur au réseau de protection en temps réel, vous pouvez fournir des renseignements sur des applications et des sites Web inconnus, ainsi que sur des applications malicieuses et des attaques vers des sites Web. Le réseau de protection en temps réel n'effectue pas le suivi de vos activités sur le Web ni ne collecte de renseignements sur les sites Web qui ont déjà été analysés, en outre, il ne collecte aucun renseignement sur les applications propres installées sur votre ordinateur.

Si vous ne souhaitez pas contribuer, le réseau de protection en temps réel ne collecte pas les renseignements sur des applications installées ou des sites Web visités. Toutefois, le produit doit envoyer des requêtes au serveur de F-Secure au sujet de la réputation des applications, des sites Web, des messages ou d'autres objets. La requête est effectuée en utilisant un total de contrôle chiffré où l'objet de la requête est envoyé à F-Secure. Nous n'effectuons aucun suivi des données pour les utilisateurs; seul le compteur d'accès du fichier ou du site Web affiche une augmentation.

Il est impossible d'arrêter complètement tout le trafic vers le réseau de protection en temps réel, car il fait partie intégrale de la protection fournie par le produit.

Avantages du réseau de protection en temps réel

Le réseau de protection en temps réel offre une protection plus rapide et plus précise contre les menaces les plus récentes sans vous envoyer d'alerte inutile sur des applications suspectes, mais non malicieuses.

En tant que contributeur au réseau de protection en temps réel, vous pouvez nous aider à détecter des maliciels nouveaux et non détectés et à éliminer les fausses alarmes de notre base de données de définition de virus.

Tous les participants au réseau de protection en temps réel s'aident mutuellement. Lorsque le réseau de protection en temps réel détecte une application suspecte sur votre machine, vous bénéficiez de l'analyse des résultats lorsque la même application a été déjà détectée sur d'autres machines. Le réseau de protection en temps réel améliore la performance générale de votre machine, car les produits de sécurité installés n'exigent pas une nouvelle analyse des applications déjà analysées par le réseau de protection en temps réel et considérées comme fiables. En outre, les renseignements sur les sites Web malicieux et sur les messages en vrac non sollicités sont partagés par le réseau de protection en temps réel; nous sommes ainsi en mesure de vous offrir une protection plus précise contre les attaques des sites Web et contre le courrier indésirable.

Plus les gens contribuent au réseau de protection en temps réel, mieux les participants sont protégés.

Quelles données fournissez-vous?

En tant que contributeur au réseau de protection en temps réel, vous fournissez des renseignements sur les applications stockées sur votre machine et sur les sites Web que vous avez visités, de sorte que le réseau de protection en temps réel soit en mesure de fournir une protection contre les applications malveillantes et les sites Web suspects les plus récents.

Analyse du statut des fichiers

Le réseau de protection en temps réel collecte des renseignements uniquement sur les applications dont le statut n'est pas connu et sur des fichiers suspects ou qui ont la réputation d'être des maliciels.

Le réseau de protection en temps réel collecte des renseignements anonymes sur des applications propres et suspectes présentes sur votre machine. Le réseau de protection en temps réel collecte des renseignements sur des fichiers exécutables seulement (ayant les extensions suivantes : .cpl, .exe, .dll, .ocx, .sys, .scr et .drv).

Les renseignements collectés incluent ce qui suit :

- le chemin des fichiers indiquant l'emplacement de l'application sur votre machine;
- la taille du fichier et la date de sa création ou modification;
- attributs de fichiers et privilèges,
- les renseignements de signature;
- la version courante du fichier et l'entreprise qui l'a créé;
- l'origine du fichier ou son URL téléchargée, et
- les résultats d'analyse de F-Secure DeepGuard et de l'anti-virus et
- d'autres renseignements similaires.

Le réseau de protection en temps réel ne collecte jamais de renseignements à partir de vos documents personnels, à moins qu'ils n'aient été infectés. Dans le cas d'un fichier malveillant, il collecte le nom de l'infection et l'état de désinfection du fichier.

Le réseau de protection en temps réel vous permet également de soumettre des applications suspectes pour les faire analyser. Les applications que vous pouvez soumettre sont uniquement des fichiers exécutables et portables. Réseau de protection en temps réel ne collecte jamais de renseignements de vos documents personnels et ils ne sont jamais téléchargés automatiquement pour être analysés.

Soumission de fichiers aux fins d'analyse

Le réseau de protection en temps réel vous permet également de soumettre des applications suspectes pour analyse.

Vous pouvez soumettre des applications suspectes individuelles manuellement, lorsque le produit vous invite à le faire. Vous pouvez seulement soumettre des fichiers portables exécutables. Le réseau de protection en temps réel ne télécharge jamais vos documents personnels.

Analyse de la réputation d'un site Web

Le réseau de protection en temps réel n'effectue pas le suivi de vos activités sur le Web, ni ne collecte de renseignements sur les sites Web déjà analysés. Il s'assure que les sites Web visités sont sécuritaires alors que vous naviguez sur le Web. Lorsque vous visitez un site Web, le réseau de protection en temps réel vérifie sa sécurité et vous avise s'il est coté suspect ou malveillant.

Si le site Web visité contient des programmes malicieux ou suspects, ou une attaque connue, le réseau de protection en temps réel collecte l'intégralité de l'URL du site pour en analyser le contenu.

Si vous visitez un site Web qui n'a pas encore été analysé, le réseau de protection en temps réel collecte les noms de domaine et de sous-domaine, et dans certains cas le chemin de la page visitée, aux fins d'analyse et d'évaluation. Tous les paramètres des URL pouvant contenir des renseignements permettant de vous identifier personnellement sont supprimés pour protéger votre vie privée.

Nota: Le réseau de protection en temps réel n'évalue pas ou n'analyse pas les pages Web de réseaux privés; il ne collecte donc aucun renseignement sur des adresses de réseau IP privées (comme les intranets des entreprises).

Analyse des informations système

Le réseau de protection en temps réel collecte le nom et la version de votre système d'exploitation, des renseignements sur la connexion Internet et des statistiques du réseau de protection en temps réel (comme le nombre de demandes de vérification de la réputation d'un site Web et le temps moyen de réponse pour ces demandes) afin de surveiller et d'améliorer le service.

Protection de votre vie privée

Nous transférerons les renseignements de manière sûre et supprimons automatiquement tous les renseignements personnels pouvant être contenus dans ces données.

Réseau de protection en temps réel supprime les données permettant l'identification avant de les faire parvenir à F-Secure et, pendant le transfert, chiffre tous les renseignemets collectés afin de les protéger contre un accès non autorisé. Les renseignements collectés ne sont pas traités individuellement; ils sont regroupés avec des renseignements d'autres contributeurs du réseau de protection en temps réel. Toutes les données sont analysées sous forme statistique et anonyme; autrement dit, aucune donnée ne peut être associée directement à vous, en aucune manière.

Tout renseignement susceptible de vous identifier personnellement n'est pas inclus dans les données collectées. Le réseau de protection en temps réel ne collecte par les adresses IP personnelles ou vos renseignements personnels, comme des adresses de courriel, des noms d'utilisateur et des mots de passe. Bien que nous prenions toutes les mesures nécessaires pour supprimer les données pouvant mener à une identification personnelle, il est possible que certaines données d'identification puissent rester dans les renseignements collectés. Dans de tels cas, nous ne chercherons pas à utiliser intentionnellement ces données collectées en vue de vous identifier.

Nous appliquons des mesures de sécurité, des mesures physiques et des protections techniques strictes afin de protéger les données collectées lorsqu'elles sont transférées, stockées et traitées. Les renseignements sont stockés dans des emplacements sécurisés, sur des serveurs contrôlés par nous, situés soit dans nos bureaux, soit dans des bureaux de sous-traitants. Seul le personnel autorisé peut avoir accès aux renseignements collectés.

F-Secure pourrait partager les données collectées avec ses affiliés, sous-traitants, distributeurs et partenaires, mais toujours dans un format non identifiable et anonyme.

Contribution au réseau de protection en temps réel

Vous pouvez nous aider à améliorer le réseau de protection en temps réel en contribuant des renseignements sur des programmes et des sites Web malicieux

Vous pouvez décider de participer au réseau de protection en temps réel pendant l'installation. Les paramètres par défaut de l'installation vous enregistrent comme contributeur au réseau de protection en temps réel. Vous pouvez modifier ces paramètres plus tard.

Suivez ces instructions pour modifier les paramètres de Real-time Protection :

1. Dans la zone de lancement, cliquez sur l'icône la plus à droite.
   Un menu contextuel apparaît.
2. Sélectionnez **Ouvrir les paramètres communs**.
3. Sélectionnez**Autre** > **Confidentialité**.
4. Cochez la case de participation pour devenir un contributeur au réseau de protection en temps réel.

Questions à propos du réseau de protection en temps réel

Informations de contact 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 communiquer avec :

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finlande

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

La version la plus récente de cette politique est toujours disponible sur notre site Web.

Placement du pointeur de la souris sur l'icône d'état pour afficher l'info bulle de l'état.

Le type et l'état de votre abonnement sont affichées sur la page **État de l'abonnement**.

Lorsqu'un abonnement est sur le point d'expirer ou si votre abonnement a déjà expiré, l'icône de l'état global de protection du programme dans la zone de lancement change.

Pour vérifier la validité de votre abonnement :

1. Dans la zone de lancement, cliquez sur l'icône la plus à droite.
   Un menu contextuel apparaît.
2. Sélectionnez **Afficher mes abonnements**.
3. Sélectionnez **État de l'abonnement** pour afficher les renseignements sur les abonnements des programmes installés.
4. Sélectionnez **État de l'installation** pour afficher les programmes prêts à être installés.

L'état et la date d'expiration de votre abonnement sont indiqués dans la page **Statistiques**. Si votre abonnement a expiré, vous devez le renouveler pour continuer à recevoir des mises à jour et utiliser le produit.

Nota: Lorsque votre abonnement à expiré, l'icône d'état clignote dans votre barre d'état système.

Centre d'action

Le centre d'action affiche tous les avis importants qui exigent votre attention.

Si votre abonnement a expiré ou est sur le point d'expirer, le centre d'action vous en avise. La couleur de fond et le contenu du message du centre d'action dépendent de votre type d'abonnement et de votre état :

- Si votre abonnement est sur le point d'expirer et que des abonnements gratuits sont offerts, l'arrière-plan du message est blanc et affiche un bouton **Activer**.
- Si votre abonnement est sur le point d'expirer et qu'aucun abonnement gratuit n'est offert, l'arrière-plan du message et de couleur jaune et affiche les boutons **Acheter** et **Saisir la clé**. Si vous avez déjà acheté un nouvel abonnement, cliquez sur **Saisir la clé** pour fournir une clé d'abonnement et activer votre nouvel abonnement.
- Si votre abonnement a expiré et que des abonnements gratuits sont offerts, l'arrière-plan est de couleur rouge et affiche un bouton **Activer**.
- Si votre abonnement a expiré et qu'aucun abonnement gratuit n'est offert, l'arrière-plan du message est rouge et affiche les boutons **Acheter** et **Saisir la clé**. Si vous avez déjà acheté un nouvel abonnement, vous pouvez cliquer sur **Saisir la clé** pour fournir une clé d'abonnement et activer votre nouvel abonnement.

Nota: Le lien **Afficher l'historique des avis** dans le centre d'action affiche la liste des messages d'avis sur les produits, mais pas les messages antérieurs du centre d'action.

Activation d'un abonnement

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

Pour activer un abonnement :

1. Dans la zone de lancement, cliquez sur l'icône la plus à droite.
   Un menu contextuel apparaît.
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'ouvre, saisissez votre nouvelle clé d'abonnement et cliquez sur **OK**.

   Conseil: Si vous avez reçu la clé d'abonnement par courriel, vous pouvez la copier et la coller du message dans le champ.

Après avoir saisi la nouvelle clé d'abonnement, la date de validation du nouvel abonnement est affichée sur la page **État de l'abonnement**.

Chapitre

3

Présentation

Sujets :

- *Affichage de l'état général de ma protection.*
- *Affichage des statistiques du produit*
- *Gérer les mises à jour du produit*
- *Virus et autres maliciels*

Ce produit protège votre ordinateur contre les virus et autres applications dangereuses.

Le produit analyse des fichiers, les applications et effectue automatiquement des mises à jour. Il n'exige aucune intervention de votre part.

Affichage de l'état général de ma protection.

La page d'**État** affiche un aperçu rapide des fonctions du produit installé, ainsi que leur état actuel.

Pour ouvrir la page d'**État** :

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

La page d'**État** s'ouvre.

Les icônes indiquent l'état du programme et ses fonctions de sécurité.

Icône d'état	Nom de l'état	Description
	OK	Votre ordinateur est protégé. La fonction est activée et s'exécute correctement.
	Information	Le produit vous informe sur un état ou sur une fonction particulière. Par exemple, la fonction est mise à jour.
	Avertissement	Votre ordinateur n'est pas complètement protégé. Par exemple, le produit n'a pas reçu de mises à jour depuis une longue période de temps, ou l'état d'une fonction exige de l'attention.
	Erreur	Votre ordinateur n'est pas protégé Par exemple, votre abonnement a expiré ou une fonction critique est désactivée.
	Désactivée	Une fonction non critique est désactivée.

Affichage des statistiques du produit

Vous pouvez afficher les activités du produit depuis son installation dans la page **Statistiques**.

Pour ouvrir la page **Statistiques** :

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

La page **Statistiques** apparaît.

- **Dernière mise à jour réussie** affiche l'heure de la mise à jour la plus récente.

- **Recherche de virus et logiciels espions** affiche le nombre de fichiers analysés et nettoyés par le produit depuis son l'installation.
- **Applications** affiche le nombre de programmes autorisés ou bloqués par DeepGuard depuis l'installation.
- **Connexionx de pare-feu** affiche le nombre de connexions autorisées est bloquées depuis l'installation.
- **Spam and phishing filtering** shows how many e-mail messages the product has detected as valid e-mail messages and as spam messages.

Gérer les mises à jour du produit

Le produit met à jour automatiquement la protection.

Affichage des versions de bases de données

Vous pouvez afficher les heures et les numéros de versions les plus récentes dans la page **Mise à jour de bases de données** .

Pour ouvrir la page **Mise à jour de bases de données** :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. Sélectionnez **Autres paramètres** > **Versions de base de donnée**.

La page **Versions de bases de données** affiche la date la plus récente lorsque les définitions de virus et de logiciels espions, DeepGuard et le filtrage des courriers indésirables et de hameçonnage ont été mis à jour, ainsi que leur numéro de version.

Changement des paramètres du haut débit mobile

Sélectionnez si vous souhaitez ou non télécharger les mises à jour de sécurité lorsque vous utilisez le haut débit mobile.

Nota: Cette fonction est uniquement disponible dans Windows 7 de Microsoft.

Les mises à jour de sécurité sont téléchargées par défaut lorsque vous êtes situé dans le réseau de votre opérateur d'origine. Toutefois, les mises à jour sont suspendues lorsque vous visitez le réseau d'un autre opérateur, car le prix des connexions peut varier entre opérateurs comme, par exemple, entre différents pays. Vous pourriez considérer de ne pas changer ce paramètre si vous souhaitez économiser de la bande passante et, possiblement, des frais pendant votre visite.

Nota: Ce paramètre s'applique uniquement aux connexions à haut débit mobile. Lorsque l'ordinateur est connecté à un réseau fixe ou sans fil, le produit est mis à jour automatiquement.

Pour modifier les paramètres :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. > > Sélectionnez Autres paramètresHaut débit mobileTélécharger les mises à jour de sécurité.
3. Sélectionnez l'option de mises à jour préférée pour les connexions mobiles :
   - **Seulement dans le réseau de mon opérateur**

Les mises à jour sont toujours téléchargées dans le réseau de votre opérateur d'origine. Lorsque vous visitez le réseau d'un autre opérateur, les mises à jour sont suspendues. Nous vous recommandons de sélectionner cette option pour conserver la mise à jour de votre produit à des coûts prévus.

- **Jamais**

  Aucune mise à jour téléchargée pendant l'utilisation du haut débit mobile

- **Toujours**

  Les mises à jour sont toujours téléchargées, peu importe le réseau utilisé. Sélectionnez cette option si vous souhaitez vous assurer que la sécurité de votre ordinateur est toujours à jour, peu importent les coûts.

4. Si vous souhaitez décider à chaque fois que vous quittez le réseau de votre opérateur d'origine, sélectionnez **Demander chaque fois que le réseau de l'opérateur d'origine est quitté**.

Mises à jour de sécurité suspendues

Les mises à jour de sécurité pourraient être suspendues lorsque vous utilisez le haut débit mobile à l'extérieur du réseau de votre opérateur.

Dans ce cas, vous pouvez voir l'avis **Suspendu** dans le coin inférieur droit de l'écran. Les mises à jour sont suspendues, car les prix des connexions peuvent varier parmi les opérateurs; par exemple dans différents pays. Vous pourriez envisager de laisser ce paramètre non changé si vous souhaitez économiser de la bande passante et peut-être aussi des frais au cours de votre visite. Toutefois, si vous souhaitez tout de même changer vos paramètres, cliquez sur le lien **Modifier**.

Nota:

Cette fonction est uniquement disponible dans Windows 7 de Microsoft.

Virus et autres maliciels

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

Les maliciels 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 *maliciel* 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 sans que vous le sachiez sur votre ordinateur. 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 programmes qui recueillent vos informations personnelles.

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

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

Un logiciel espion s'installe quasiment toujours de lui-même sans votre accord. Les logiciels espions peuvent être installés en même temps qu'un programme utile ou en vous incitant à cliquer sur une option dans une fenêtre trompeuse.

Rootkits

Les rootkits sont des programmes compliquant la recherche d'un *maliciel*.

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

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

Programmes à risque

Les programmes à risque ne sont pas conçus spécifiquement pour endommager votre ordinateur, mais ils risquent de le faire s'ils sont mal utilisés.

Les programmes à risque ne sont pas, à strictement parler, les maliciels; ils exécutent des fonctions utiles, mais potentiellement dangereuses.

Voici des 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 comme VoIP (*Protocole voix sur IP*).
- logiciels d'accès distant comme VNC,
- programmes alarmistes de canulars qui tentent d'alarmer ou de duper des individus pour qu'ils achètent des logiciels de sécurité factices, ou
- programmes conçus pour contourner les vérifications de CD ou la protection contre les 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 de l'ordinateur contre les maliciels

Sujets :

- *Analyse de l'ordinateur*
- *Exclusion des fichiers de l'analyse*
- *Utilisation de la quarantaine*
- *Que'est-ce que DeepGuard?*

L'analyse de détection des virus et des logiciels espions protège votre ordinateur contre des programmes susceptibles de dérober vos informations personnelles, endommager votre ordinateur ou de l'utiliser pour des fins illégales.

Par défaut, tous les types de maliciels sont immédiatement pris en charge lorsqu'ils sont détectés, afin qu'ils ne posent pas de risques.

Par défaut, la recherche de virus et de logiciels espions analyse automatiquement vos disques durs locaux, tous les médias amovibles (comme des disques durs portables ou des disques compacts) ainsi que du contenu téléchargé. Vous pouvez la configurer pour qu'elle analyse automatiquement les courriels.

La recherche de virus et de logiciels espions surveille également votre ordinateur pour y détecter des modifications susceptibles d'indiquer la présence de *maliciels*. Si une modification dangereuse a lieu dans le système, par exemple dans la configuration système ou des tentatives de modifier un processus important du système, DeepGuard bloque l'exécution de ce programme, car c'est probablement un *maliciel*.

Analyse de l'ordinateur

Lorsque l'analyse des virus et des logiciels est est activée, elle analyse votre ordinateur pour y détecter automatiquement des fichiers dangereux. Vous pouvez également analyser manuellement les fichiers et programmer des horaires d'analyse.

Nous recommandons de laisser toujours activée l'analyse des virus et des logiciels. Analysez vos fichiers manuellement lorsque vous voulez vous assurer qu'aucun fichier dangereux n'est sur votre ordinateur ou si vous souhaitez analyser les fichiers que vous avez exclus de l'analyse en temps réel.

En configurant des analyses programmées, l'analyse des virus et des logiciels espions élimine de votre ordinateur les fichiers dangereux à des heures spécifiées.

Analyse automatique des fichiers

L'analyse en temps réel protège votre ordinateur en analysant tous les fichiers lorsque vous y accédez et en bloquant l'accès aux fichiers contenant un *maliciel*.

Lorsque votre ordinateur cherche à accéder à un fichier, l'analyse en temps réel analyse les fichiers pour y détecter des maliciels avant d'autoriser votre ordinateur à accéder à ce fichier. Si l'analyse en temps réel détecte un contenu dangereux, elle place automatiquement le fichier en quarantaine avant qu'il ne puisse causer des dommages.

L'analyse en temps réel affecte-t-elle la performance de l'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 dépendent, par exemple, du contenu, de l'emplacement et du type de fichier.

Fichiers dont l'analyse est longue :

- Les fichiers sur des disques amovibles, comme les CDs, les DVD et les clés USB portables.
- Fichiers compressés, comme *.zip*.

  Nota: Les fichiers comprimés ne sont pas analysés par défaut.

L'analyse en temps réel peut ralentir votre ordinateur dans les cas suivants :

- votre ordinateur n'est pas conforme aux exigences système, ou
- vous accédez à un grand nombre de fichiers en même temps. Par exemple lorsque vous ouvrez un répertoire qui contient de nombreux fichiers devant être analysés.

Activation ou désactivation de l'analyse en temps réel

Vous pouvez activer l'analyse en temps réel pour arrêter un *maliciel* Evant qu'il endommage votre ordinateur.

Activation ou désactivation de l'analyse en temps réel :

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

   Nota: Vous devez gérer les droits administratifs pour désactiver les fonctions de sécurité.

3. Activer ou désactiver **l'analyse des virus et des logiciels espions** .
4. Cliquez sur **Fermer**.

Gestion automatique des fichiers dangereux

L'analyse en temps réel peut gérer automatiquement les fichiers dangereux, sans vous poser aucune question.

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

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. Sélectionnez **Sécurité ordinateur** > **Recherche des virus et logiciels espions**.
3. Sélectionnez **Gérer automatiquement les fichiers**.

Si vous choisissez de ne pas gérer automatiquement les fichiers dangereux, l'analyse en temps réel vous demande ce qu'il faut faire lorsqu'un fichier dangereux est détecté.

Gestion des logiciels espions

L'analyse des virus et des logiciels espions bloque immédiatement les logiciels espions lorsqu'ils tentent de démarrer.

Avant qu'une application de logiciel espion ne puisse démarrer, le produit la bloque et vous laisse décider ce qu'il faut faire.

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

Action à entreprendre	Action effectuée sur le logiciel espion
Décider automatiquement la meilleure action	Laisser le produit décider de la meilleure action à prendre, en fonction du logiciel espion détecté.
Mettre le logiciel espion en quarantaine	Déplacer le logiciel espion vers la quarantaine, où il ne peut plus nuire à votre ordinateur.
Supprimer le logiciel espion	Supprimer de votre ordinateur tous les fichiers associés au logiciel espion.
Simplement bloquer le logiciel espion	Bloquer l'accès au logiciel espion, mais le laisser sur votre ordinateur.
Exclure le logiciel espion de l'analyse	Autoriser le logiciel espion à s'exécuter et l'exclure de l'analyse à l'avenir.

Gestion des logiciels à risque

L'analyse des virus et des logiciels espions bloque immédiatement les logiciels à risque lorsqu'ils tentent de démarrer.

Avant qu'une application de logiciel à risque ne puisse démarrer, le produit la bloque et vous laisse décider ce qu'il faut faire.

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

Action à entreprendre	Action effectuée sur le programme à risque
Simplement bloquer le logiciel à risque	Bloquer l'accès au logiciel à risque, mais le laisser sur votre ordinateur.
Mettre en quarantaine le logiciel à risque	Déplacer le logiciel à risque vers la quarantaine, où il ne peut plus nuire à votre ordinateur.
Supprimer le logiciel à risque	Supprimer de votre ordinateur tous les fichiers associés au logiciel à risque.
Exclure le logiciel à risque de l'analyse	Autoriser le logiciel à risque à s'exécuter et l'exclure de l'analyse à l'avenir.

Suppression automatique des témoins de suivi de navigation

En supprimant les témoins de suivi vous empêchez les sites Web de garder une trace des sites visités sur Internet.

Les témoins de suivi sont de petits fichiers permettant aux sites Web d'enregistrer les sites que vous visitez. Suivez ces instructions pour bloquer l'installation des témoins de suivi sur votre ordinateur.

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

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

Analyse manuelle de fichiers

Vous pouvez analyser manuellement vos fichiers; par exemple, lorsque vous connectez un appareil externe à votre ordinateur, pour vous assurer qu'il ne contient aucun maliciel.

Lancement de l'analyse manuelle

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

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

Pour lancer manuellement l'analyse de votre ordinateur :

1. Dans la page principale, cliquez sur la flèche sous **Analyser**.

   Les options d'analyse s'affichent.

2. Sélectionnez le type d'analyse.

   Sélectionnez **Modifier les paramètres d'analyse** pour optimiser l'analyse manuelle de votre ordinateur dans la recherche de virus et d'autres applications dangereuses.

3. Si vous avez sélectionné **Sélectionner les éléments à analyser**, une fenêtre s'ouvre dans laquelle vous pouvez sélectionner l'emplacement que vous souhaitez analyser.
   L'**Assistant d'analyse** s'ouvre.

Types d'analyse

Vous pouvez analyser l'ordinateur entier, un type spécifique de maliciel ou un emplacement spécifique.

Voici la liste des différents types d'analyse :

Type d'analyse	Qu'est-ce qui doit être analysé?	Quand utiliser ce type?
Recherche de virus et logiciels espions	Des parties de votre ordinateur sont analysées pour y détecter des virus, des logiciels espions et des logiciels à risque	Ce type d'analyse est plus rapide qu'une analyse complète. Elle vérifie seulement des parties de votre système qui contiennent des fichiers de programmes installés. Ce type d'analyse est recommandé si vous voulez effectuer une analyse rapide pour vérifier que votre ordinateur est propre, car elle peut détecter et supprimer efficacement tout maliciel actif dans l'ordinateur.
Analyse complète	Tout l'ordinateur (en les disques internes et externes) pour y détecter	Lorsque vou voulez être sûr qu'il n'y a aucun maliciel ou programme à risque sur votre ordinateur. Ce type

Type d'analyse	Qu'est-ce qui doit être analysé?	Quand utiliser ce type?
	les virus, les logiciels espions et les logiciels à risque.	d'analyse prend le plus de temps. Il combine de l'analyse rapide de détection de maliciels et l'analyse du disque dur. Il vérifie également si des articles pourraient être eux cachés dans un rootkit.
Sélectionner les éléments à analyser	Analyse spécifique d'un fichier, d'un dossier ou d'un disque dur pour y détecter des virus, des logiciels espions et des logiciel à risque	Lorsque vous suspectez qu'un emplacement spécifique de votre ordinateur contient un maliciel s'il contient, par exemple, des téléchargements de sources potentiellement dangereuses comme des réseaux de partage de fichiers poste-à-poste. La durée de l'analyse dépend de la taille de la cible qui doit être analysée. L'analyse est rapide si, par exemple, vous analysez un dossier qui contient seulement quelques petits fichiers.
Analyse des rootkits	Analyse des emplacements système importants où un élément suspect peut entraîner un problème de sécurité. Recherche des fichiers, des dossiers, des disques ou des processus dissimulés	Lorsque vous soupçonnez qu'un rootkit pourrait être installé dans votre ordinateur. Par exemple, si un maliciel a été détecté récemment dans votre ordinateur et que vous voulez vous assurer qu'il n'a pas installé un rootkit.

Analyse dans Windows Explorer

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 **Analyse de détection de virus dans les dossiers**. (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.

Sélection des fichiers à analyser

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

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. Sélectionnez **Autres paramètres** > **Analyse manuelle**.
3. Sous **Options d'analyse**, sélectionnez un des éléments suivants :

Analyser seulement les fichiers dont le type est connu	Pour analyser seulement les types de fichiers les plus susceptibles d'être infectés, comme les fichiers exécutables. Le choix de cette options accélère l'analyse : `.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`, and `.hqx`.
Analyser les fichiers comprimés	Pour analyser des archives et des dossiers.
Utiliser l'heuristique évoluée	Pour utiliser toute l'heuristique disponible pendant l'analyse afin de mieux détecter un maliciel inconnu. **Nota:** Si vous sélectionnez cette option, l'analyse prend plus de temps et risque de détecter de faux dangers (des fichiers inoffensifs rapportés comme suspects).

4. Cliquez sur **OK**.

Nota: Les fichiers exclus de la liste des éléments exclus ne sont pas analysés, même si vous les sélectionnez pour les analyser ici.

Que faire lorsque des fichiers dangereux sont détectés

Choisissez comment traiter les fichiers dangereux lorsqu'ils sont détectés.

Pour sélectionner une action lorsque du contenu dangereux est détecté pendant une analyse manuelle :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

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

Option	Description
Me demander (par défaut)	Vous pouvez sélectionner l'action à prendre pour chaque élément détecté pendant une analyse manuelle.
Nettoyer les fichiers	Le produit essaie automatiquement de désinfecter les fichiers infectés qui ont été détectés pendant une analyse manuelle. **Nota:** Si le produit ne peut nettoyer le fichier infecté, ce dernier est mis en quarantaine (sauf s'il est détecté sur un réseau ou sur des disques durs amovibles), afin qu'il ne puisse causer des dommages à l'ordinateur.
Mettre les fichiers en quarantaine	Le produit déplace tout fichier infecté détecté pendant l'analyse manuelle dans le dossier de quarantaine, où il ne peut nuire à l'ordinateur.
Supprimer les fichiers	Le produit supprime automatiquement un fichier infecté rencontré lors d'une analyse manuelle.
Rapporter uniquement	Le produit laisse tout fichier infecté tel qu'il a été trouvé pendant une analyse manuelle et se contente d'enregistrer la détection du virus ou du logiciel espion dans le rapport d'analyse. **Nota:** Si l'analyse en temps réel n'est pas activée et que cette option est sélectionnée, tout maliciel peut encore endommager l'ordinateur.

Nota: Lorsque des fichiers dangereux sont détectés pendant une analyse programmée, ils sont nettoyés automatiquement.

Programmation d'une analyse

Programmez votre ordinateur pour qu'il analyse et supprime automatiquement les virus et autres applications malveillantes lorsque vous ne l'utilisez pas, ou programmez une analyse régulière pour vous assurer que votre ordinateur est nettoyé.

Pour programmer une analyse :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. Sélectionnez **Autres paramètres** > **Analyse programmée**.
3. Activez l'**Analyse programmée**.
4. Sélectionnez l'heure du début de l'analyse.

Option	Description
Tous les jours	Analysez votre ordinateur chaque jour.
Toutes les semaines	Analysez votre ordinateur les jours de semaine sélectionnés. Sélectionnez les jours à partir de la liste.
Tous les mois	Analysez votre ordinateur les jours du mois sélectionné. Pour sélectionner les 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 où lancer l'analyse pendant les journées sélectionnées.

Option	Description
Heure début	Lancer l'analyse à l'heure spécifiée.
Si l'ordinateur est inutilisé pendant	Lancer l'analyse après avoir utilisé votre ordinateur pendant une période de temps spécifiée.

L'analyse programmée utilise les paramètres d'analyse manuelle lorsqu'elle analyse votre ordinateur, sauf qu'elle analyse chaque fois des archives et nettoie automatiquement les fichiers dangereux.

Analyse des courriels

L'analyse des courriels vous protège contre l'intrusion de fichiers malveillants dans des courriels qui vous sont envoyés.

L'analyse des virus et des logiciels espions doit être activée pour que les courriels soient analysés contre les virus.

Pour activer l'analyse des courriels :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. Sélectionnez **Sécurité ordinateur** > **Recherche des virus et logiciels espions**.
3. Sélectionnez **Supprimer les pièces jointes de courriel dangereuses**.
4. Cliquez sur **OK**.

À quel moment les messages du courriel et les pièces jointes sont-ils analysés

La recherche de virus de logiciels espions peut supprimer du contenu nuisible des courriels que vous recevez.

La recherche de virus et de logiciels espions supprimes les messages de courriel nuisibles reçus par des programmes de courriel, comme Microsoft Outlook et Outlook Express, Microsoft Mail, ou Mozilla Thunderbird. Cette recherche analyse les messages de courriel et les attachements non chiffrés chaque fois que votre programme de courriel reçoit de tels messages du serveur de courriel utilisant le protocole POP3.

L'analyse des virus les logiciels espions ne peut analyser les messages de courriel de la messagerie Web, qui inclut des applications de courriel exécutées dans votre navigateur Web comme Hotmail, Yahoo! mail, ou Gmail. Vous êtes toujours protégés contre les *virus*, même si vous n'enlevez pas les pièces jointes dangereuses ou si vous utilisez la messagerie Web. Lorsque vous ouvrez une pièce jointe courriel, l'analyse en temps réel élimine toutes les pièces jointes dangereuses avant qu'elles ne puissent causer des dommages.

Nota: L'analyse en temps réel protège seulement votre ordinateur, mais pas vos amis. L'analyse en temps réel n'analyse pas les pièces jointes tant que vous ne les ouvrez pas. Autrement dit, si vous utilisez la messagerie Web et que vous faites suivre un message avant d'ouvrir sa pièce jointe, vous pourriez faire suivre à vos amis un courriel infecté.

Affichage des résultats de l'analyse

L'historique des virus et des logiciels espions affichent tous les fichiers dangereux détectés par le produit.

Il arrive parfois que le produit ne puisse exécuter l'action sélectionnée lorsqu'un élément dangereux est détecté. Par exemple, si vous sélectionnez de nettoyer les fichiers et que le fichier ne peut être nettoyé, le produit le met en quarantaine. Vous pouvez afficher ces renseignements dans l'historique des virus et des logiciels espions.

Pour afficher l'historique :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

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

L'historique des virus et des logiciels espions affiche les renseignements suivants :

- la date et l'heure à laquelle le fichier dangereux a été détecté,
- le nom du maliciel et son emplacement sur votre ordinateur, et
- l'action exécutée.

Exclusion des fichiers de l'analyse

Vous pourriez parfois souhaiter exclure certains fichiers ou certaines applications de l'analyse. Les éléments exclus ne sont pas analysés, à moins qu'ils ne soient retirés de la liste des éléments exclus.

Nota: Les listes d'exclusion de l'analyse en temps réel et de l'analyse manuelle sont distinctes. Par exemple, si vous excluez un fichier de l'analyse en temps réel, il est analysé pendant une analyse manuelle, à moins qu'il ne soit également exclu de l'analyse manuelle.

Exclusion des types de fichiers

Lorsque vous excluez des types de fichiers, les fichiers avec des extensions particulières sont pas s'analysés pour y détecter du contenu malveillant.

Pour ajouter ou supprimer des types de fichiers que vous souhaitez exclure :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. Choisissez si vous souhaitez exclure le type de fichier de l'analyse en temps réel ou manuelle :
   - Sélectionnez **Sécurité ordinateur** > **Recherche des virus et logiciels espions** pour exclure le fichier de l'analyse en temps réel.
   - Sélectionnez **Autres paramètres** > **Analyse manuelle** pour exclure le fichier de l'analyse manuelle.
3. Cliquez sur **Exclure les 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) Tapez une extension de fichier qui identifie le type de fichier que vous souhaitez exclure, dans le champ à côté du bouton **Ajouter**.

      Pour spécifier les fichiers sans extension, saisissez '.'. Vous pouvez utiliser le métacaractère '?' Pour représenter un caractère unique, ou '*' pour représenter n'importe quelle quantité de caractères.

      Par exemple, pour exclure les fichiers exécutables, saisissez `exe` dans le champ.
   d) Cliquez sur **Ajouter**.
5. Répétez l'étape précédente pour toute autre extension que vous souhaitez exclure de l'analyse de détection de virus.
6. Cliquez sur **OK** pour fermer le dialogue **Exclure de l'analyse**.
7. Cliquez sur **OK** pour appliquer les nouveaux réglages.

Les types fichiers sélectionnés sont exclus des analyses futures.

Exclusion des fichiers en fonction de l'emplacement

Lorsque vous excluez des fichiers en fonction de l'emplacement, les fichiers dans des disques durs ou des dossiers spécifiés ne sont pas analysés pour y détecter des contenus malveillants.

Pour ajouter ou supprimer des emplacements de fichiers que vous souhaitez exclure :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

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

Nota: Certains lecteurs pourraient être amovibles, comme des lecteurs de disques CD, DVD, ou des disques de réseaux. Les disques de réseaux et des lecteurs amovibles vides ne peuvent pas être exclus.

e) Cliquez sur **OK**.

5. Répéter l'étape précédente pour exclure d'autres fichiers, lecteurs ou dossiers de l'analyse de détection des virus.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Exclure de l'analyse**.
7. Cliquez sur **OK** pour appliquer la nouvelle configuration.

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

Affichage des applications exclues

Vous pouvez afficher les applications exclues de l'analyse et les supprimer de la liste des éléments exclus si vous souhaitez les analyser à l'avenir.

Si l'analyse en temps réel ou l'analyse manuelle détecte une application qui se comporte comme un logiciel espion ou un logiciel à risque, mais que vous savez que celle-ci est sécuritaire, vous pouvez l'exclure de l'analyse de sorte que le produit n'affiche plus un avertissement pour cette application.

Nota: Si l'application se comporte comme un virus ou un autre logiciel malicieux, elle ne peut être exclue.

Vous ne pouvez exclure des applications directement. Les nouvelles applications apparaissent sur la liste d'exclusion seulement si vous les excluez pendant l'analyse.

Pour afficher des applications exclues de l'analyse :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

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

   Nota: Seuls les logiciels espions et les logiciels à risque peuvent être exclus, mais pas les virus.

5. Si vous souhaitez analyser encore une fois l'application exclue :
   a) Sélectionnez l'application que vous souhaitez inclure dans l'analyse.
   b) Cliquez sur **Supprimer**.
6. Cliquez sur **OK** pour fermer le dialogue **Exclure de l'analyse**.
7. Cliquez sur **OK** pour quitter.

Utilisation de la 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.

Vous pouvez mettre en quarantaine des *maliciel*, *logiciel espion* et des *programmes à risque* pour les rendre inoffensifs. Vous pouvez restaurer des applications ou des fichiers de la quarantaine ultérieurement si nécessaire.

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 *maliciel* 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.

Affichage des articles mis en quarantaine

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

Pour afficher des informations détaillées sur les éléments dans la quarantaine :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. Sélectionnez **Sécurité ordinateur** > **Recherche des virus et logiciels espions**.
3. Cliquez sur **Afficher la quarantaine**.
   La page **Quarantaine** affiche le nombre total d'éléments stockés en quarantaine.
4. Pour afficher des renseignements détaillés sur la quarantaine, cliquez sur **Détails**.

   Vous pouvez trier le contenu par nom de maliciel ou par chemin de fichier.

   Une liste des 100 premiers articles est affichée, avec le type d'articles en quarantaine, leur nom et le chemin menant à l'emplacement où les fichiers ont été installés.
5. Pour afficher plus d'information sur un article en quarantaine, cliquez sur l'icône Située à côté de la colonne **État**.

Restauration des articles 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 sur l'ordinateur.

Restauration des articles mis en quarantaine

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

2. Sélectionnez **Sécurité ordinateur** > **Recherche des virus et logiciels espions**.
3. Cliquez sur **Afficher la quarantaine**.
4. Sélectionnez les articles en quarantaine que vous souhaitez restaurer.
5. Cliquez sur **Restaurer**.

Que'est-ce que DeepGuard?

DeepGuard analyse le contenu des fichiers, le comportement des applications et surveille les applications non fiables.

DeepGuard bloque les *virus* et les *vers* nouveaux et non découverts, ainsi que d'autres applications nuisibles qui tentent d'effectuer des modifications dans votre ordinateur; il empêche également les applications suspectes d'accéder à Internet.

Lorsque DeepGuard ne détecte une nouvelle application qui tente d'effectuer des modifications potentiellement dangereuses pour le système, il laisse l'application s'exécuter dans une zone sécuritair, où elle ne peut nuire à l'ordinateur et annalyse les modifications qu'elle tenté d'effectuer et, en fonction de ces données, décide si l'application a des chances d'être un *maliciel*. Si l'application ressemble effectivement à un *maliciel*, DeepGuard la bloque.

Voici les modifications de système potentiellement dangereuses détectées par DeepGuard :

- 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

En laissant DeepGuard activé vous pouvez prévenir des programmes suspects d'effectuer des modifications potentiellement dangereuses dans votre ordinateur.

Si vous exécutez Windows XP, assurez-vous d'avoir installé le Service Pack 2 installed avant d'activer DeepGuard.

Pour activer ou désactiver DeepGuard :

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

   Nota: Vous devez gérer les droits administratifs pour désactiver les fonctions de sécurité.

3. Activer ou désactiver **DeepGuard**.
4. Cliquez sur **Fermer**.

Autorisation des applications bloquées par DeepGuard

Vous pouvez contrôler les applications autorisées est bloquées par Deepguard.

DeepGuard pourrait parfois bloquer l'exécution d'une application sécuritaire, même si vous souhaitez utiliser cette application et savez qu'elle ne pose aucun danger. Ceci peut se produire si l'application tente d'effectuer des modifications du système pouvant être potentiellement dangereuses. Vous pourriez également avoir bloqué cette application par inadvertance lors de l'affichage de la fenêtre éclair de DeepGuard.

Pour autoriser une application bloquée par DeepGuard :

1. Dans la page principale, cliquez sur **Outils**.
2. Cliquez sur **Applications**.
   La liste des **Applications surveillées** apparaît.
3. Repérez l'application que vous souhaitez autoriser.

   Nota: Vous pouvez cliquer sur l'en-tête de colonnes trier la liste. Par exemple, cliquez sur la colonne **Autorisation** Pour trier la liste en groupes de programmes autorisés et refusés.

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

DeepGuard autorise l'application à effectuer des modifications au système.

Utilisation de DeepGuard en mode de compatibilité

Afin d'assurer une protection maximale, DeepGuard modifie temporairement les programmes en cours d'exécution. Certains programmes vérifient qu'ils ne sont pas corrompus ou modifiés et pourraient donc ne pas être compatibles avec cette fonction. Par exemple, les jeux en ligne dotés d'outils anti tricherie vérifient qu'ils n'ont pas été modifiés en quelque manière lorsqu'ils sont exécutés. Dans ces cas, vous pouvez activer le mode de compatibilité.

Pour activer le mode de compatibilité :

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

   Nota: Vous devez posséder des droits d'administrateur pour modifier les paramètres.

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

Que faire lors d'avertissements de comportement suspect

DeepGuard surveille les applications non fiables. Si une application surveillée tente d'accéder à Internet, d'effectuer des modifications dans votre système ou affiche un comportement suspect, DeepGuard la bloque.

Lorsque vous avez sélectionné **M'avertir à propos d'un comportement suspect** dans les paramètres de DeepGuard, celui-ci vous avise lorsqu'il détecte une application potentiellement dangereuse ou lorsque vous lancez une application dont la réputation est inconnue.

Pour décider ce que vous souhaitez faire avec l'application bloquée par DeepGuard :

1. Cliquez sur **Détails** pour afficher plus de renseignements sur le programme.
   La section des détails indique :
   - l'emplacement de l'application,
   - la réputation de l'application dans Real-time Protection Network, et
   - le degré de popularité de l'application.
2. Décider si vous souhaitez faire confiance à l'application bloquée par DeepGuard :
   - Choisissez **J'approuve l'application. Continuer.** si vous souhaitez ne pas bloquer l'application.

     L'application a plus de chances d'être sécuritaire dans les cas suivants :
     - DeepGuard a bloqué l'application en réaction à une action de votre part,
     - vous reconnaissez l'application, ou
     - vous avez obtenu l'application d'une source sûre.
   - Choisissez **Je n'approuve pas l'application. Continuer à la bloquer.** Si vous souhaitez continuer à bloquer l'application.

     L'application a plus de chances d'être dangereuse dans les cas suivants :
     - l'application est peu connue,
     - l'application n'a aucune réputation, ou
     - vous ne connaissez pas l'application.

3. Si vous souhaitez soumettre une application suspecte pour analyse :

a) Cliquez sur **Rapporter cette application à F-Secure**.
Le produit affiche les conditions de soumission.

b) Cliquez sur **J'accepte** si vous acceptez les conditions et souhaitez soumettre l'échantillon.

Nous vous recommandons d'envoyer un échantillon dans les cas suivants :

- DeepGuard bloque une application que vous pensez être sure, ou
- vous soupçonnez que l'application pourrait être en *maliciel*.