Bitdefender®

ANTIVIRUS PLUS 2016

MANUEL D'UTILISATION

Bitdefender Antivirus Plus 2016
Manuel d'utilisation

Date de publication 05/02/2016

Mentions Légales

Bitdefender

Table des matières

INSTALLATION

1. PRÉPARATION DE L'INSTALLATION

Avant d'installer Bitdefender Antivirus Plus 2016, procédez comme suit pour faciliter l'installation :

- Vérifiez que l'ordinateur où vous prévoyez d'installer Bitdefender dispose de la configuration minimale requise. Si l'ordinateur ne dispose pas de la configuration minimale requise, Bitdefender ne pourra pas être installé, ou, une fois installé, il ne fonctionnera pas correctement, ralentira le système et le rendra instable. Pour des informations détaillées sur la configuration requise, veuillez consulter « *Configuration requise* » (p. 3).
- Connectez-vous à l'ordinateur en utilisant un compte administrateur.
- Désinstallez tous les autres logiciels similaires sur l'ordinateur. L'exécution de deux programmes de sécurité à la fois peut affecter leur fonctionnement et provoquer d'importants problèmes sur le système. Windows Defender sera désactivé pendant l'installation.
- Il est recommandé que votre ordinateur soit connecté à Internet pendant l'installation, même pour une installation à partir d'un CD ou DVD. Si des versions plus récentes des fichiers d'applications du package d'installation sont disponibles, Bitdefender peut les télécharger et les installer.

2. CONFIGURATION REQUISE

Vous pouvez installer Bitdefender Antivirus Plus 2016 uniquement sur les ordinateurs fonctionnant avec les systèmes d'exploitation suivants :

- Windows 7 avec Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Avant d'installer le produit, vérifiez que votre ordinateur dispose de la configuration minimale requise.

Note

Pour connaître le système d'exploitation Windows de votre ordinateur et obtenir des informations sur le matériel, procédez comme suit :

- Dans **Windows 7**, faites un clic droit sur **Poste de travail** sur le bureau, puis sélectionnez **Propriétés** dans le menu.
- Dans **Windows 8 et Windows 8.1**, sur l'écran d'accueil Windows, localisez « Ordinateur » (vous pouvez, par exemple, taper « Ordinateur » directement sur l'écran d'accueil), puis faites un clic droit sur son icône. Sélectionnez Propriétés dans le menu inférieur. Regardez sous Système pour connaître le type de système.
- Dans **Windows 10**, tapez "Système" dans le champ de recherche de la barre des tâches cliquez sur son icône. Regardez sous Système pour connaître le type de système.

2.1. Configuration système minimale

- 1 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- Processeur 1,6 GHz
- 1 Go de mémoire (RAM)

2.2. Configuration système recommandée

- 2 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- Intel CORE Duo (2 GHz) ou processeur équivalent
- 2 Go de mémoire (RAM)

2.3. Configuration logicielle requise

Pour pouvoir utiliser Bitdefender et l'ensemble de ses fonctionnalités, votre ordinateur doit disposer de la configuration logicielle suivante :

- Internet Explorer 10 ou version supérieure
- Mozilla Firefox 14 ou version supérieure
- Google Chrome version 20 ou supérieure
- Skype 6.3 ou version supérieure
- Yahoo! Messenger 9 ou version supérieure

3. INSTALLER BITDEFENDER

Vous pouvez installer Bitdefender à partir du disque d'installation ou en utilisant un programme d'installation téléchargé sur votre ordinateur à partir du compte Bitdefender Central.

Si votre achat protège plus d'un ordinateur (si, par exemple, vous avez acheté Bitdefender Antivirus Plus 2016 pour 3 PC), répétez le processus d'installation et activez votre produit avec le même compte sur chaque ordinateur. Le compte que vous devez utiliser est celui qui contient votre abonnement actif Bitdefender.

3.1. Installer à partir de Bitdefender Central

A partir du compte Bitdefender Central vous pouvez télécharger le kit d'installation correspondant à l'abonnement acheté. Une fois le processus d'installation terminé, Bitdefender Antivirus Plus 2016 est activé.

Pour télécharger Bitdefender Antivirus Plus 2016 à partir de votre compte Bitdefender Central, suivez ces étapes :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionnez le panneau **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
4. Sélectionnez l'une des deux actions disponibles :
   - **TÉLÉCHARGER**

     Cliquez sur le bouton pour sauvegarder le fichier d'installation.
   - **Sur un autre appareil**

     Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER**.
5. Attendez que le téléchargement soit terminé, puis lancez l'installation.

Validation de l'installation

Bitdefender vérifiera d'abord votre système pour valider l'installation.

Si votre système ne dispose pas de la configuration minimale requise pour l'installation de Bitdefender, vous serez informé des zones devant être améliorées avant de pouvoir poursuivre.

Si un programme antivirus incompatible ou une version antérieure de Bitdefender est détecté, on vous demandera de le désinstaller de votre système. Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite. Il est parfois nécessaire de redémarrer l'ordinateur pour terminer la désinstallation des programmes antivirus détectés.

Le package d'installation de Bitdefender Antivirus Plus 2016 est constamment mis à jour.

Note
Le téléchargement des fichiers d'installation peut être long, en particulier sur des connexions Internet plus lentes.

Une fois l'installation validée, l'assistant de configuration s'affichera. Suivez les étapes pour installer Bitdefender Antivirus Plus 2016.

Étape 1 - Installation de Bitdefender

L'écran d'installation de Bitdefender vous permet de choisir le type d'installation que vous souhaitez effectuer.

Pour une installation simplifiée, cliquez simplement sur le bouton **Installer**. Bitdefender sera installé dans l'emplacement par défaut avec les paramètres par défaut et vous passerez directement à l'Étape 3 de l'assistant.

Si vous souhaitez configurer les paramètres d'installation, cliquez sur **Personnalisé**.

Deux tâches supplémentaires peuvent être réalisées au cours de cette étape :

- Veuillez lire l'Accord de licence de l'utilisateur final avant de procéder à l'installation. L'Accord de Licence contient les termes et conditions d'utilisation de Bitdefender Antivirus Plus 2016.

  Si vous n'acceptez pas ces conditions, fermez la fenêtre. Le processus d'installation sera abandonné et vous quitterez l'installation.

- Gardez l'option **Envoyer rapports d'utilisation anonymes** activée. Si vous activez cette option, les rapports contenant des informations sur votre utilisation du produit seront envoyés aux serveurs de Bitdefender. Ces

informations sont essentielles pour améliorer le produit et nous aider à vous offrir la meilleure expérience possible. Veuillez noter que ces rapports ne comportent aucune donnée confidentielle, comme votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Étape 2 - Personnaliser les paramètres d'installation

> **Note**
> Cette étape apparaît uniquement si vous avez choisi de personnaliser l'installation lors de l'étape précédente.

Voici les options proposées :

Chemin d'installation

Par défaut, la Bitdefender Antivirus Plus 2016 sera installé dans C:\Program Files\Bitdefender\Bitdefender2016\. Si vous souhaitez choisir un autre répertoire, cliquez sur **Modifier** et choisissez le répertoire d'installation de Bitdefender.

Configurer les paramètres du proxy

Bitdefender Antivirus Plus 2016 nécessite un accès à Internet pour l'activation du produit, le téléchargement de mises à jour du produit et de sécurité, les composants de détection "in the cloud", etc. Si vous utilisez une connexion via un proxy au lieu d'une connexion Internet directe, vous devez sélectionner cette options et configurer les paramètres du proxy.

Les paramètres peuvent être importés à partir du navigateur par défaut ou vous pouvez les indiquer manuellement.

Cliquez sur **Installer** pour confirmer vos préférences et commencer l'installation. Si vous changez d'avis, cliquez sur le bouton **Par défaut** correspondant.

Étape 3 - Installation en cours

Patientez jusqu'à la fin de l'installation. Des informations détaillées sur la progression sont affichées.

Les zones critiques de votre système font l'objet d'une analyse antivirus, les dernières versions des fichiers d'applications sont téléchargées et installées et les services de Bitdefender sont lancés. Cette étape peut prendre quelques minutes.

Étape 4 - Installation terminée

Votre produit Bitdefender a été installé avec succès.

Un résumé de l'installation s'affiche. Si des logiciels malveillants actifs ont été détectés et supprimés pendant l'installation, un redémarrage du système peut être nécessaire. Cliquez sur **OK** pour continuer.

Étape 5 - Pour commencer

Dans la fenêtre Pour commencer vous pouvez vérifier la validité de votre abonnement.

Deux tâches supplémentaires peuvent être réalisées au cours de cette étape :

- Acheter un nouvel abonnement - ce lien vous redirige vers la page Bitdefender, où vous pourrez acheter un nouvel abonnement.
- J'ai un code d'activation - ce lien vous redirige vers votre compte Bitdefender Central. Saisissez le code d'activation dans le champ correspondant puis cliquez sur **SOUMETTRE**. Sinon, vous pouvez saisir une clé de licence valide qui sera convertie en abonnement avec les mêmes attributs : nombre d'appareils et disponibilité restante.

Cliquez sur **Terminer** pour accéder à l'interface de Bitdefender Antivirus Plus 2016.

3.2. Installer à partir du disque d'installation

Pour installer Bitdefender à partir du disque d'installation, insérez le disque dans le lecteur optique.

Un écran d'installation s'affiche peu après. Suivez les instructions pour démarrer l'installation.

Note

L'écran d'installation fournit une option pour copier le package d'installation à partir du disque d'installation sur un support de stockage USB. C'est utile si vous avez besoin d'installer Bitdefender sur un ordinateur ne disposant pas d'un lecteur de disque (sur un netbook, par exemple). Branchez votre périphérique USB, puis cliquez sur **Copier vers un disque USB**. Ensuite, branchez votre disque USB sur le PC ne disposant pas de lecteur de disque et double-cliquez sur runsetup.exe depuis le répertoire dans lequel se trouve le package d'installation.

Si l'écran d'installation ne s'affiche pas, utilisez l'Explorateur Windows pour vous rendre au répertoire racine du disque et double-cliquez sur le fichier autorun.exe.

Validation de l'installation

Bitdefender vérifiera d'abord votre système pour valider l'installation.

Si votre système ne dispose pas de la configuration minimale requise pour l'installation de Bitdefender, vous serez informé des zones devant être améliorées avant de pouvoir poursuivre.

Si un programme antivirus incompatible ou une version antérieure de Bitdefender est détecté, on vous demandera de le désinstaller de votre système. Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite. Il est parfois nécessaire de redémarrer l'ordinateur pour terminer la désinstallation des programmes antivirus détectés.

Le package d'installation de Bitdefender Antivirus Plus 2016 est constamment mis à jour.

> **Note**
> Le téléchargement des fichiers d'installation peut être long, en particulier sur des connexions Internet plus lentes.

Une fois l'installation validée, l'assistant de configuration s'affichera. Suivez les étapes pour installer Bitdefender Antivirus Plus 2016.

Étape 1 - Installation de Bitdefender

L'écran d'installation de Bitdefender vous permet de choisir le type d'installation que vous souhaitez effectuer.

Pour une installation simplifiée, cliquez simplement sur le bouton **Installer**. Bitdefender sera installé dans l'emplacement par défaut avec les paramètres par défaut et vous passerez directement à l'Étape 3 de l'assistant.

Si vous souhaitez configurer les paramètres d'installation, cliquez sur **Personnalisé**.

Deux tâches supplémentaires peuvent être réalisées au cours de cette étape :

- Veuillez lire l'Accord de licence de l'utilisateur final avant de procéder à l'installation. L'Accord de Licence contient les termes et conditions d'utilisation de Bitdefender Antivirus Plus 2016.

  Si vous n'acceptez pas ces conditions, fermez la fenêtre. Le processus d'installation sera abandonné et vous quitterez l'installation.

- Gardez l'option **Envoyer rapports d'utilisation anonymes** activée. Si vous activez cette option, les rapports contenant des informations sur votre utilisation du produit seront envoyés aux serveurs de Bitdefender. Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir la meilleure expérience possible. Veuillez noter que ces rapports ne comportent aucune donnée confidentielle, comme votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Étape 2 - Personnaliser les paramètres d'installation

> **Note**
> Cette étape apparaît uniquement si vous avez choisi de personnaliser l'installation lors de l'étape précédente.

Voici les options proposées :

Chemin d'installation

Par défaut, la Bitdefender Antivirus Plus 2016 sera installé dans C:\Program Files\Bitdefender\Bitdefender2016\. Si vous souhaitez choisir un autre répertoire, cliquez sur **Modifier** et choisissez le répertoire d'installation de Bitdefender.

Configurer les paramètres du proxy

Bitdefender Antivirus Plus 2016 nécessite un accès à Internet pour l'activation du produit, le téléchargement de mises à jour du produit et de sécurité, les composants de détection "in the cloud", etc. Si vous utilisez une connexion via un proxy au lieu d'une connexion Internet directe, vous devez sélectionner cette options et configurer les paramètres du proxy.

Les paramètres peuvent être importés à partir du navigateur par défaut ou vous pouvez les indiquer manuellement.

Cliquez sur **Installer** pour confirmer vos préférences et commencer l'installation. Si vous changez d'avis, cliquez sur le bouton **Par défaut** correspondant.

Étape 3 - Installation en cours

Patientez jusqu'à la fin de l'installation. Des informations détaillées sur la progression sont affichées.

Les zones critiques de votre système font l'objet d'une analyse antivirus, les dernières versions des fichiers d'applications sont téléchargées et installées et les services de Bitdefender sont lancés. Cette étape peut prendre quelques minutes.

Étape 4 - Installation terminée

Un résumé de l'installation s'affiche. Si des logiciels malveillants actifs ont été détectés et supprimés pendant l'installation, un redémarrage du système peut être nécessaire. Cliquez sur **OK** pour continuer.

Étape 5 - Bitdefender Central

Une fois que vous avez fini le paramétrage initial, la fenêtre Bitdefender Central apparaît. Un compte Bitdefender Central est nécessaire pour activer le produit et utiliser ses fonctionnalités en ligne. Pour plus d'informations, reportez-vous à « *Bitdefender Central* » (p. 39).

Procédez selon votre situation.

J'ai déjà un compte Bitdefender Central

Saisissez l'adresse e-mail et le mot de passe de votre compte Bitdefender Central, puis cliquez sur **CONNEXION**.

Si vous avez oublié le mot de passe de votre compte ou que vous souhaitez simplement reconfigurer celui déjà existant, cliquez sur le lien **Réinitialiser mot de passe**. Saisissez votre adresse e-mail, puis cliquez sur le bouton **RÉINITIALISER MOT DE PASSE**

Je souhaite créer un compte Bitdefender Central

Pour créer un compte Bitdefender Central, cliquez sur le lien **Inscription** qui se trouve en bas de la fenêtre. Saisissez les informations nécessaires dans les champs correspondants, puis cliquez sur le bouton **CRÉER COMPTE**

Les informations fournies resteront confidentielles.

Le mot de passe doit contenir au moins 8 caractères et contenir un chiffre.

> **Note**
> Une fois le compte créé, vous pouvez utiliser l'adresse courriel et le mot de passe indiqués pour vous connecter à votre compte sur https://central.bitdefender.com.

Je souhaite me connecter à l'aide de mon compte Microsoft, Facebook ou Google

Pour vous connecter avec votre compte Microsoft, Facebook ou Google, procédez comme suit :

1. Sélectionnez le service que vous souhaitez utiliser. Vous serez redirigé vers la page de connexion de ce service.
2. Suivez les instructions du service sélectionné pour lier votre compte à Bitdefender.

> **Note**
> Bitdefender n'accède à aucune information confidentielle telle que le mot de passe du compte que vous utilisez pour vous connecter, ou les informations personnelles de vos amis et contacts.

Étape 6 - Pour commencer

Dans la fenêtre Pour commencer vous pouvez vérifier la validité de votre abonnement.

Deux tâches supplémentaires peuvent être réalisées au cours de cette étape :

- Acheter un nouvel abonnement - ce lien vous redirige vers la page Bitdefender, où vous pourrez acheter un nouvel abonnement.
- J'ai un code d'activation - ce lien vous redirige vers votre compte Bitdefender Central. Saisissez le code d'activation dans le champ correspondant puis cliquez sur **SOUMETTRE**. Sinon, vous pouvez saisir une clé de licence valide qui sera convertie en abonnement avec les mêmes attributs : nombre d'appareils et disponibilité restante.

Cliquez sur **Terminer** pour accéder à l'interface de Bitdefender Antivirus Plus 2016.

COMMENCER

4. FONCTIONS DE BASE

Une fois Bitdefender Antivirus Plus 2016 installé, votre ordinateur est protégé contre tous les types de malwares (tels que les virus, spywares et chevaux de Troie).

L'application utilise la technologie Photon pour améliorer la vitesse et les performances du processus d'analyse antimalware. Elle fonctionne en apprenant les modèles d'utilisation de vos applications système afin de savoir quoi analyser et quand, ce qui réduit l'impact sur les performances du système.

Vous pouvez activer la fonction Autopilot pour bénéficier d'une protection complètement silencieuse. Vous n'aurez ainsi aucun paramètre à configurer. Cependant, vous pouvez souhaiter profiter des paramètres de Bitdefender pour ajuster et améliorer votre protection.

Bitdefender peut vous permettre de travailler, jouer ou regarder des films sans être dérangé en reportant les tâches de maintenance, en supprimant les interruptions et en ajustant les effets visuels du système. Vous pouvez bénéficier de tout ceci en activant et en configurant les Profils.

Bitdefender prendra pour vous la plupart des décisions de sécurité et affichera rarement des alertes pop-up. Des détails sur les actions prises et des informations sur le fonctionnement du programme sont disponibles dans la fenêtre Événements. Pour plus d'informations, reportez-vous à « *Événements* » (p. 17).

Il est recommandé d'ouvrir Bitdefender de temps en temps et de corriger les problèmes existants. Vous pouvez avoir à configurer des composants Bitdefender spécifiques ou appliquer des actions préventives afin de protéger votre ordinateur et vos données.

Pour utiliser les fonctionnalités en ligne de Bitdefender Antivirus Plus 2016 et gérez vos abonnements et appareils, accédez à votre compte Bitdefender Central. Pour plus d'informations, reportez-vous à « *Bitdefender Central* » (p. 39).

La section « Comment faire pour » (p. 49) vous fournit des instructions détaillées pour utiliser les fonctionnalités les plus courantes. Si vous rencontrez des problèmes lors de l'utilisation de Bitdefender, recherchez dans la section « *Résoudre les problèmes les plus fréquents* » (p. 138) des solutions possibles aux problèmes les plus courants.

4.1. Ouverture de la fenêtre de Bitdefender

Pour accéder à l'interface principale de Bitdefender Antivirus Plus 2016, suivez les étapes ci-dessous :

- Dans **Windows 7** :
  1. Cliquez sur **Démarrer** et allez dans **Programmes**.
  2. Cliquez sur **Bitdefender 2016**.
  3. Cliquez sur **Bitdefender Antivirus Plus 2016** ou faites un double clic sur Bitdefender dans la zone de notification.
- Dans **Windows 8 et Windows 8.1** :

  Localisez Bitdefender Antivirus Plus 2016 dans l'écran d'accueil Windows (vous pouvez par exemple taper « Bitdefender » directement dans l'écran d'accueil) puis cliquez sur son icône. Vous pouvez également ouvrir le Bureau puis double-cliquer sur Bitdefender de la zone de notification.
- Dans **Windows 10** :

  Tapez "Bitdefender" dans le champ de recherche de la barre des tâches puis cliquez sur son icône. Vous pouvez également double-cliquer sur l'icône Bitdefender dans la zone de notification.

Pour plus d'informations sur la fenêtre de Bitdefender et l'icône de la zone de notification, reportez-vous à « *Interface de Bitdefender* » (p. 26).

4.2. Correction des problèmes

Bitdefender utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous en informer. Par défaut, il surveille uniquement un ensemble de problèmes considérés comme très importants. Cependant, vous pouvez le configurer selon vos besoins en sélectionnant les problèmes spécifiques que vous souhaitez surveiller.

Les problèmes détectés comprennent la désactivation d'importants paramètres de protection et d'autres conditions pouvant constituer un risque pour la sécurité. Ils sont regroupés en deux catégories :

- **Problèmes critiques** - ils empêchent Bitdefender de vous protéger contre les malwares ou constituent un risque majeur pour la sécurité.

- **Problèmes mineurs (non critiques)** - ces problèmes pourraient éventuellement affecter votre protection.

L'icône de Bitdefender de la zone de notification signale les problèmes en attente en changeant de couleur comme suit :

Des problèmes critiques affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.
Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.

Si vous faites glisser le curseur de la souris sur l'icône, une fenêtre de notification confirmera la présence de problèmes en attente.

Lorsque vous ouvrez l'interface de Bitdefender, la zone d'état de Sécurité de la barre d'outils supérieure indique la nature des problèmes affectant votre système.

4.2.1. Assistant de correction des problèmes

Pour corriger les problèmes détectés, suivez l'assistant de **Correction des problèmes**.

1. Pour ouvrir l'assistant, procédez comme suit :
   - Faites un clic droit sur l'icône de Bitdefender dans la zone de notification et sélectionnez **Voir les problèmes de sécurité**.
   - Ouvrez l'interfaceBitdefender et cliquez dans la zone d'état de sécurité de la barre d'outils supérieure (vous pouvez, par exemple, cliquer sur le lien **Tout corriger**).
2. Vous pouvez voir les problèmes affectant la sécurité de votre ordinateur et de vos données. Tous les problèmes présents sont sélectionnés pour être corrigés.

   Si vous ne souhaitez pas corriger un problème spécifique immédiatement, décochez la case correspondante. On vous demandera de spécifier pendant combien de temps vous souhaitez reporter la correction du problème. Sélectionnez l'option souhaitée dans le menu et cliquez sur **OK**. Pour cesser de surveiller cette catégorie de problème, sélectionnez **En permanence**.

   L'état du problème deviendra **Reporté** et aucune action ne sera adoptée pour corriger le problème.

3. Pour corriger les problèmes sélectionnés, cliquez sur **Corriger**. Certains problèmes sont corrigés immédiatement. Pour d'autres, un assistant vous aide à les corriger.

Les problèmes que cet assistant vous aide à corriger peuvent être regroupés dans les catégories suivantes :

- **Paramètres de sécurité désactivés.** Ces problèmes sont corrigés immédiatement en activant les paramètres de sécurité correspondants.
- **Tâches de sécurité préventives devant être réalisées.** Un assistant vous aide à corriger ces problèmes.

4.2.2. Configurer les alertes d'état

Bitdefender peut vous avertir lorsque des problèmes sont détectés lors du fonctionnement des composants de programmes suivants :

- Antivirus
- Mettre à jour
- Sécurité du navigateur

Vous pouvez configurer le système d'alertes afin de répondre à vos besoins spécifiques en choisissant les problèmes à propos desquels vous souhaitez être informé. Suivez ces étapes :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Avancé**.
3. Cliquez sur le lien **Configurer les alertes d'état**.
4. Cliquez sur les boutons pour activer ou désactiver les alertes d'état en fonction de vos préférences.

4.3. Événements

Bitdefender tient un journal détaillé des événements concernant son activité sur votre ordinateur. Lorsqu'un événement concernant la sécurité de votre système ou de vos données a lieu, un nouveau message est ajouté aux Événements de Bitdefender, comme lorsqu'un nouvel e-mail arrive dans votre boîte de réception.

Les événements sont un outil très important pour la surveillance et la gestion de votre protection Bitdefender. Par exemple, vous pouvez facilement vérifier qu'une mise à jour s'est effectuée correctement, s'il y a eu des malwares détectés sur votre ordinateur, etc. Vous pouvez également adopter d'autres actions si nécessaire ou modifier les actions appliquées par Bitdefender.

Pour accéder au journal des Événements, procédez comme suit :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Événements** dans le menu déroulant.

Les messages sont regroupés en fonction du module Bitdefender dont ils sont liés à l'activité :

- **Mettre à jour**
- **Antivirus**
- **Protection Web**
- **Vulnérabilité**
- **Protection ransomware**

À chaque fois qu'un événement se produit, un point bleu apparaît sur l'icône  en haut de l'interface Bitdefender.

Une liste d'événements est disponible pour chaque catégorie. Pour trouver des informations sur un événement spécifique de la liste, cliquez sur l'icône  et sélectionnez **Événements** dans le menu déroulant. Des détails sur l'événement s'affichent alors dans la partie droite de la fenêtre. Chaque événement est accompagné des informations suivantes : une brève description, l'action que Bitdefender a appliqué et la date et l'heure de l'événement. Des options peuvent permettre d'appliquer une action supplémentaire si nécessaire.

Vous pouvez filtrer les événements en fonction de leur importance et de l'ordre dans lequel ils ont eu lieu. Il y a trois types d'événements filtrés en fonction de leur importance, chacun étant signalé par une icône spécifique :

■ Les événements **critiques** signalent des problèmes critiques. Nous vous recommandons de les vérifier immédiatement.
■ Les événements **avertissement** signalent des problèmes non critiques. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
■ Les événements **Informations** indiquent des opérations réussies.

Pour voir les événements ayant eu lieu au cours d'une période donnée, sélectionnez la période souhaitée dans le champ correspondant.

Pour vous aider à gérer facilement les événements enregistrés, chaque section de la fenêtre Événements fournit des options permettant de supprimer ou de marquer comme lus tous les événements de cette section.

4.4. Autopilot

Pour les utilisateurs qui souhaitent que leur solution de sécurité les protège sans les interrompre, Bitdefender Antivirus Plus 2016 dispose d'un mode Autopilote intégré.

En Autopilot, Bitdefender applique une configuration de sécurité optimale et prend pour vous toutes les décisions de sécurité. Cela signifie qu'aucune fenêtre contextuelle ni alerte ne s'affichera et que vous n'aurez aucun paramètre à configurer.

En mode Autopilot, Bitdefender corrige automatiquement les problèmes critiques, active et gère silencieusement :

- La protection antivirus, fournie par l'analyse à l'accès et l'analyse en continu.
- Protection Web.
- Les mises à jour automatiques.

Pour activer ou désactiver **Autopilote**, cliquez sur le bouton dans la barre d'outils de l'interface Bitdefender.

Tant que l'Autopilot est activé, l'icône de Bitdefender de la zone de notification est .

Important
Lorsque le mode Autopilot est activé, modifier l'un des paramètres qu'il gère conduit à sa désactivation.

Pour afficher un historique des actions réalisées par Bitdefender alors que l'Autopilot était en cours, ouvrez la fenêtre Événements.

4.5. Profils et Mode Batterie

Certaines utilisations de l'ordinateur comme les jeux en ligne ou les présentations vidéo nécessitent plus de performance et de réactivité du

système et aucune interruption. Lorsque votre ordinateur portable est alimenté par sa batterie, il vaut mieux que les opérations non indispensables, qui consomment de l'énergie supplémentaire, soient reportées jusqu'au moment où l'ordinateur portable sera branché sur secteur.

Pour s'adapter à ces situations particulières, Bitdefender Antivirus Plus 2016 comprend deux modes de fonctionnement spéciaux :

- Profils
- Mode Batterie

4.5.1. Profils

Les profils de Bitdefender allouent davantage de ressources système aux applications en cours d'exécution en modifiant momentanément les paramètres de protection et en adaptant la configuration du système. L'impact du système sur vos activités est donc réduit.

Pour s'adapter à différentes activités, Bitdefender dispose des profils suivants :

Profil Travail
: Optimise votre efficacité lorsque vous travaillez en identifiant et en ajustant la configuration du logiciel et du système.

Profil Film
: Améliore les effets visuels et supprime les interruptions lorsque vous regardez des films.

Profil Jeu
: Améliore les effets visuels et supprime les interruptions lorsque vous jouez.

Activer et désactiver les profils

Pour activer ou désactiver les profils, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Profils**, sélectionnez l'onglet **Paramètres des profils**.

5. Activez et désactivez les profils en cliquant sur le bouton correspondant.

Configurer Autopilot pour surveiller les profils

Pour une utilisation simple, vous pouvez configurer l'Autopilote afin qu'il gère votre profil actif. Dans ce mode, Bitdefender détecte automatiquement les activités que vous effectuez et applique les paramètres d'optimisation du système et du produit.

Pour permettre à Autopilot de gérer les profils, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Profils**, sélectionnez l'onglet **Paramètres des profils**.
5. Cochez la case **Laisser Autopilot gérer mes profils** correspondante.

Si vous ne souhaitez pas que votre Profil soit géré automatiquement, ne cochez pas la case et effectuez la sélection manuellement dans la liste déroulante **PROFILE** de l'interface de Bitdefender.

Pour plus d'informations sur les Profils, reportez-vous à« *Profils* » (p. 131)

4.5.2. Mode Batterie

Le mode Batterie est spécialement conçu pour les utilisateurs d'ordinateurs portables et de tablettes. Son rôle est de limiter à la fois l'impact du système et de Bitdefender sur la consommation électrique lorsque le niveau de charge de la batterie est inférieur à celui par défaut ou que vous avez sélectionné.

Les paramètres du produit suivants s'appliquent lorsque Bitdefender fonctionne en Mode Batterie :

- La Mise à jour Automatique de Bitdefender est reportée.
- Les analyses planifiées sont reportées.
- Le Widget Windows est désactivé.

Bitdefender détecte le passage d'une alimentation secteur à une alimentation sur batterie et, en fonction du niveau de charge de la batterie, passe automatiquement en Mode Batterie. De la même manière, Bitdefender quitte

automatiquement le Mode Batterie lorsqu'il détecte que l'ordinateur portable ne fonctionne plus sur batterie.

Pour activer ou désactiver le mode Batterie, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils**, puis sélectionnez l'onglet **Mode Batterie**.
4. Activez ou désactivez le mode Batterie automatique en cliquant sur le bouton correspondant.

   Faites glisser le curseur correspondant le long de l'échelle pour déterminer quand le système doit passer en Mode Batterie. Le mode est activé par défaut lorsque le niveau de charge de batterie est inférieur à 30%.

Note
Le Mode Batterie est activé par défaut sur les ordinateurs portables et les tablettes.

Configurer le Mode Batterie

Pour configurer le mode Batterie, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils**, puis sélectionnez l'onglet **Mode Batterie**.
4. Désactivez la fonctionnalité en cliquant sur le bouton correspondant.
5. Cliquez sur le bouton **Configurer**.
6. Sélectionnez les réglages du système à appliquer en cochant les options suivantes :
   - Optimiser les paramètres du produit pour le mode Batterie.
   - Reporter les tâches des programmes en arrière-plan et de maintenance.
   - Reporter les mises à jour automatiques de Windows.
   - Ajuster les paramètres du plan d'alimentation pour le mode Batterie.

- Désactiver les appareils externes et les ports du réseau.

7. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

4.6. Paramètres de Bitdefender de la protection par mot de passe

Si vous n'êtes pas le seul utilisateur avec des droits d'administrateur qui utilise cet ordinateur, il vous est recommandé de protéger vos paramètres de Bitdefender par un mot de passe.

Pour configurer la protection par mot de passe des paramètres de Bitdefender, suivez ces étapes :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Configurations générales**.
3. Activez la protection mot de passe en cliquant sur le bouton correspondant.
4. Entrez le mot de passe dans les deux champs puis cliquez sur **OK**. (8 caractères minimum)

Une fois que vous avez défini un mot de passe, toute personne essayant de modifier les paramètres de Bitdefender devra indiquer ce mot de passe.

Important

N'oubliez pas votre mot de passe ou conservez-le en lieu sûr. Si vous oubliez le mot de passe, vous devrez réinstaller le programme ou contacter le support Bitdefender.

Pour supprimer la protection par mot de passe, suivez ces étapes :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Configurations générales**.

3. Désactivez la protection mot de passe en cliquant sur le bouton correspondant. Entrez le mot de passe puis cliquez sur **OK**.

> **Note**
> Pour modifier le mot de passe de votre produit, cliquez sur le lien **Changer de mot de passe**.

4.7. Rapports d'utilisation anonymes

Par défaut, Bitdefender envoie des rapports contenant des informations sur votre utilisation aux serveurs Bitdefender. Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir un meilleur service à l'avenir. Veuillez noter que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Si vous souhaitez cesser d'envoyer des rapports d'utilisation anonymes, procédez comme suit :

1. Cliquez sur l'icône en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Avancé**.
3. Cliquez sur le bouton pour désactiver les rapports d'utilisation anonymes.

4.8. Offres spéciales et notifications du produit

Le produit Bitdefender est configuré pour vous signaler via une fenêtre pop-up les offres promotionnelles disponibles. Cela vous donne la possibilité de bénéficier de tarifs avantageux et de protéger vos appareils plus longtemps.

Des notifications du produit peuvent apparaître également lorsque vous effectuez des modifications dans le produit.

Pour activer ou désactiver les offres spéciales et les notifications du produit, procédez comme suit :

1. Cliquez sur l'icône en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Configurations générales**.

3. Activez ou désactivez les offres spéciales et les notifications du produit en cliquant sur le bouton correspondant.

L'option des offres spéciales et des notifications du produit est activée par défaut.

Note
Après avoir désactivé les offres spéciales et les notifications du produit, Bitdefender continuera à vous signaler les offres spéciales lorsque vous utiliserez une version d'évaluation, lorsque votre abonnement arrivera à expiration ou lorsque vous utiliserez une version du produit ayant expiré.

5. INTERFACE DE BITDEFENDER

Bitdefender Antivirus Plus 2016 répond aux besoins de tous les utilisateurs, qu'ils soient débutants ou armés de solides connaissances techniques. Son interface utilisateur graphique est conçue pour s'adapter à chaque catégorie d'utilisateurs.

Pour afficher l'état du produit et effectuer des tâches essentielles, l'icône de la zone de notification de Bitdefender est disponible à tout moment.

La fenêtre principale vous donne accès à d'importantes informations sur le produit, aux modules du programme et vous permet d'effectuer des tâches courantes. La fenêtre principale vous permet d'accéder aux Bitdefender modules pour une configuration détaillée et des tâches d'administration avancées, et de gérer le comportement du produit à l'aide d'Autopilot et des Profils.

Si vous souhaitez garder en permanence un œil sur les informations de sécurité essentielles et disposer d'un accès rapide aux principaux paramètres, ajoutez le Widget Window à votre bureau.

5.1. Icône de la zone de notification

Pour gérer l'ensemble du produit plus rapidement, vous pouvez utiliser l'icône Bitdefender de la zone de notification.

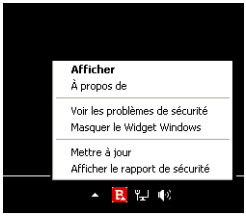
Note

L'icône de Bitdefender ne sera peut-être pas visible en permanence. Pour que l'icône soit présente en permanence, procédez comme suit :

- Dans **Windows 7, Windows 8 et Windows 8.1** :
  1. Cliquez sur la flèche dans l'angle inférieur droit de l'écran.
  2. Cliquez sur **Personnaliser...** pour ouvrir la fenêtre Icônes de la Zone de Notification.
  3. Sélectionnez l'option **Afficher les icônes et les notifications** pour l'icône **Agent Bitdefender**.
- Dans **Windows 10** :
  1. Faites un clic droit sur la barre des tâches et sélectionnez **Propriétés**.
  2. Cliquez sur **Personnaliser...** dans la fenêtre de la barre des tâches.
  3. Cliquez sur le lien **Choisir quelles icônes apparaissent dans la barre des tâches** dans la fenêtre **Notifications & actions**.

4. Activez le bouton à côté de **BitdefenderAgent**.

Double-cliquez sur cette icône pour ouvrir Bitdefender. Un clic droit sur l'icône donne également accès à un menu contextuel qui vous permettra de rapidement administrer le produit Bitdefender.



Icône de la barre d'état

- **Afficher** - ouvre la fenêtre principale de Bitdefender.
- **À propos de** - Affichage d'une fenêtre contenant des informations relatives à Bitdefender, ainsi que des éléments d'aide si vous rencontrez une situation anormale.
- **Voir les problèmes de sécurité** - vous aide à résoudre les problèmes de vulnérabilité en matière de sécurité. Si l'option n'est pas disponible, c'est qu'il n'y a pas de problème à corriger. Pour plus d'information, consultez « *Correction des problèmes* » (p. 15).
- **Afficher / Masquer le Widget Windows** - permet d'activer / de désactiver le Widget Windows.
- **Mettre à jour** - lance immédiatement une mise à jour. Vous pouvez suivre l'état de mise à jour dans le panneau Mise à jour de la fenêtre principale de Bitdefender.
- **Afficher le rapport de sécurité** - ouvre une fenêtre où vous pouvez voir un rapport hebdomadaire et des recommandations pour votre système. Vous pouvez suivre les recommandations pour améliorer la sécurité de votre système.

L'icône de la zone de notification de Bitdefender vous informe de la présence de problèmes affectant la sécurité de votre ordinateur et du fonctionnement du programme en affichant un symbole spécial :

Des problèmes critiques affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.
Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
L'Autopilot de Bitdefender est activé.

Si Bitdefender ne fonctionne pas, l'icône de la zone de notification apparaît sur un fond gris : . Cela se produit généralement lorsque l'abonnement est

expiré. Cela peut également avoir lieu lorsque les services Bitdefender ne répondent pas ou lorsque d'autres erreurs affectent le fonctionnement normal de Bitdefender.

5.2. Fenêtre principale

La fenêtre principale de Bitdefender permet d'effectuer des tâches courantes, de corriger rapidement des problèmes de sécurité, d'afficher des informations sur le fonctionnement du produit et accéder aux panneaux à partir desquels vous configurez le produit. Tout se trouve à quelques clics.

La fenêtre est organisée en deux zones principales :

Barre d'outils supérieure
: Cette section vous permet de connaître l'état de sécurité de votre ordinateur, de configurer le comportement de Bitdefender dans certains cas et d'accéder à des tâches importantes.

Zone Boutons d'action
: Vous pouvez accéder ici aux tableaux de bord du compte Bitdefender Central et exécuter différentes tâches pour assurer la protection de votre système et son fonctionnement à une vitesse optimale.

L'icône  dans le coin en bas à gauche de l'interface principale vous donne accès aux modules du produit afin que vous puissiez commencer la configuration du produit.

L'icône  en haut de l'interface principale vous permet de gérer votre compte et d'accéder aux fonctionnalités en ligne de votre produit depuis le tableau de bord du compte. Vous pouvez également accéder ici aux Événements, au Rapport de sécurité hebdomadaire et à la page Aide & Support.

Lier	Description
Nombre de jours restants	Le temps restant avant l'expiration de votre abonnement actuel est indiqué. Cliquez sur le lien pour ouvrir une fenêtre dans laquelle vous pouvez voir plus d'informations sur votre clé de licence ou activer votre produit avec une nouvelle clé de licence.

5.2.1. Barre d'outils supérieure

La barre d'outils supérieure contient les éléments suivants :

- La **Zone d'état de sécurité** à gauche de la barre d'outils vous indique si des problèmes affectent la sécurité de votre ordinateur et vous aide à les corriger.

  La couleur de la zone d'état de la sécurité change en fonction des problèmes détectés et différents messages s'affichent :

  - **La zone est en vert.** Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.
  - **La zone est en jaune.** Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
  - **La zone est en rouge.** Des problèmes critiques affectent la sécurité de votre système. Nous vous recommandons de vous occuper de ces problèmes immédiatement.

  En cliquant sur la zone d'état de la sécurité, vous pouvez accéder à un assistant qui vous aidera à supprimer facilement toutes les menaces de votre ordinateur. Pour plus d'information, consultez « *Correction des problèmes* » (p. 15).

- **Autopilot** vous permet de lancer l'Autopilot et de profiter d'une sécurité totalement silencieuse. Pour plus d'informations, consultez « *Autopilot* » (p. 19).

- Les **Profils** vous permettent de travailler, de jouer ou de regarder des films et vous font gagner du temps en configurant le système afin qu'il remette à plus tard les tâches de maintenance. Pour plus d'informations, consultez « *Profils* » (p. 131).

5.2.2. Boutons d'action

A l'aide des boutons d'action, vous pouvez accéder rapidement à votre compte Bitdefender Central et exécuter des tâches importantes.

Les boutons d'action dans cette zone sont :

- **Aller à Bitdefender Central** Accéder à votre compte Bitdefender Central pour vérifier votre abonnement et effectuer des tâches de sécurité sur les appareils que vous gérez.

- **Analyse rapide**. Exécutez une analyse rapide pour vérifier qu'aucun virus n'est présent sur votre ordinateur.
- **Analyse de vulnérabilités**. Analysez votre ordinateur à la recherche de vulnérabilités pour vous assurer que toutes les applications, ainsi que le système d'exploitation, sont mis à jour et fonctionnent correctement.
- **Safepay**. Ouvrez Bitdefender Safepay™ pour protéger vos données sensibles lorsque vous effectuez des transactions en ligne.
- **Mise à jour**. Mettez à jour votre Bitdefender pour vous assurer de disposer des dernières signatures de malwares.

5.3. Les modules Bitdefender

Le produit Bitdefender présente un grand nombre de modules utiles pour vous aider à rester protégé pendant que vous travaillez, naviguez sur le web, jouez, ou souhaitez réaliser des paiements en ligne.

Lorsque vous souhaitez accéder aux modules ou commencer à configurer votre produit, cliquez sur l'icône  dans le coin en bas à gauche de l'interface de Bitdefender.

Les modules sont séparés en trois onglets, selon les fonctionnalités qu'ils offrent :

- Protection
- Vie privée
- Outils

5.3.1. Protection

Cet onglet vous permet de configurer votre niveau de sécurité et de configurer les vulnérabilités du système à corriger.

Les modules que vous pouvez gérer dans le panneau Protection sont les suivants :

Antivirus

La protection antivirus est la base de votre sécurité. Bitdefender vous protège en temps réel et à la demande contre toutes sortes de malwares tels que les virus, les chevaux de Troie, les spywares, les adwares etc.

Le module Antivirus vous permet d'accéder facilement aux tâches d'analyse suivantes :

- Analyse rapide

- Analyse du système
- Gestion des analyses
- Mode de secours

Pour plus d'informations sur les tâches d'analyse et sur comment configurer la protection antivirus, consultez « *Protection antivirus* » (p. 76).

Protection Web

La protection web vous aide à être protégé contre les attaques de phishing, les tentatives de fraude et les fuites de données personnelles lorsque vous naviguez sur Internet.

Pour plus d'informations sur comment configurer Bitdefender pour protéger vos activités en ligne, reportez-vous à « *Protection Web* » (p. 102).

Vulnérabilité

Le module Vulnérabilité vous aide à maintenir actualisés le système d'exploitation et les applications que vous utilisez régulièrement.

Cliquez sur **Analyse de Vulnérabilité** dans le module Vulnérabilité pour commencer à identifier les mises à jour critiques de Windows, les mises à jour d'applications et les mots de passe vulnérables appartenant à des comptes Windows.

Pour plus d'informations sur la configuration de la protection contre les vulnérabilités, reportez-vous à « *Vulnérabilité* » (p. 107).

Protection ransomware

Le module Ransomware Protection garantit que vos fichiers personnels restent protégés contre l'extorsion en ligne.

Pour plus d'informations sur comment configurer la Ransomware Protection pour protéger les activités du système contre les attaques de ransomwares, reportez-vous à « *Protection ransomware* » (p. 111).

5.3.2. Vie privée

L'onglet Vie privée vous permet de protéger vos transactions en ligne et de continuer à naviguer sur Internet en toute sécurité.

Les modules que vous pouvez gérer dans le panneau Vie privée sont les suivants :

Protection des données

Le module Protection des données vous permet de supprimer des fichiers de façon permanente.

Cliquez sur **Destructeur de Fichiers** dans le module Protection des données pour lancer un assistant qui vous permettra de supprimer complètement des fichiers de votre système.

Pour plus d'informations sur la configuration de la protection des données, reportez-vous à « *Protection des données* » (p. 105).

Password Manager

Bitdefender gestionnaire de mots de passe vous aide à conserver vos mots de passe, protège votre vie privée et vous offre une expérience de navigation sécurisée.

Le module Password Manager vous permet de sélectionner les tâches suivantes :

- **Ouvrir Portefeuille** - ouvre la base de données d'un Portefeuille existant.
- **Verrouiller Wallet** - verrouille la base de données d'un Wallet existant.
- **Exporter Portefeuille** - sauvegarde la base de données existante sur votre système.
- **Créer un Portefeuille** - lance un assistant qui vous permet de créer une nouvelle base de données Portefeuille.
- **Supprimer** - vous permet de supprimer une base de données Wallet.
- **Paramètres** - ici, vous pouvez modifier le nom de votre base de données Wallet et configurer de façon à ce que la synchronisation soit faite entre les informations existantes et tous vos appareils, ou non.

Pour plus d'informations sur la configuration du Gestionnaire de mots de passe, consultez « *Protection Password Manager de vos identifiants* » (p. 120).

Safepay

Le navigateur Bitdefender Safepay™ vous aide à assurer la confidentialité et la sécurité de vos transactions bancaires, de vos achats en ligne et de tout autre type de transaction sur Internet.

Cliquez sur le bouton d'action **Safepay** dans l'interface Bitdefender pour commencer à effectuer des transactions en ligne dans un environnement sécurisé.

Pour plus d'informations sur Bitdefender Safepay™, reportez-vous à « *La sécurité SafePay pour les transactions en ligne* » (p. 115).

5.3.3. Outils

Dans l'onglet Outils, vous pouvez configurer votre profil.

Les modules que vous pouvez gérer dans l'onglet Outils sont les suivants :

Profils

Les Profils Bitdefender vous aident à profiter d'une expérience utilisateur simplifiée lorsque vous travaillez, regardez un film ou jouez en surveillant le logiciel et les outils de travail du système. Cliquez sur **Enregistrer** sur la barre d'outils supérieure dans l'interface de Bitdefender pour commencer à utiliser cette fonctionnalité.

Bitdefender vous permet de configurer les profils suivants :

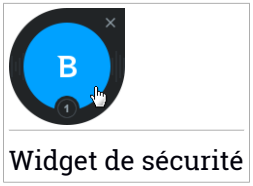
- Profil Travail
- Profil Film
- Profil Jeu

Pour plus d'informations sur comment configurer le module profils, reportez-vous à « *Profils* » (p. 131).

5.4. Widget de sécurité

Le **Widget Windows** est une façon simple et rapide de surveiller et de contrôler Bitdefender Antivirus Plus 2016. Ajouter ce petit widget discret à votre bureau vous permet de voir des informations critiques et d'effectuer des tâches essentielles à tout moment :

- ouvrir la fenêtre principale de Bitdefender.
- surveiller l'activité d'analyse en temps réel.
- surveiller l'état de sécurité de votre système et corriger tout problème existant.
- voir quand une mise à jour est en cours.
- afficher des notifications et accéder aux derniers événements signalés par Bitdefender.
- analyser des fichiers ou des dossiers en glissant-déposant un ou plusieurs éléments sur le widget.



Widget de sécurité

L'état de sécurité global de votre ordinateur s'affiche **au centre** du widget. L'état est indiqué par la couleur et la forme de l'icône qui s'affiche dans cette zone.

Des problèmes critiques affectent la sécurité de votre système.

Ils requièrent votre attention immédiate et doivent être réglés dès que possible. Cliquez sur l'icône d'état pour commencer à corriger les problèmes signalés.

Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps. Cliquez sur l'icône d'état pour commencer à corriger les problèmes signalés.

Votre système est protégé.

Lorsqu'une tâche d'analyse à la demande est en cours, cette icône animée apparaît.

Lorsque des problèmes sont signalés, cliquez sur l'icône d'état pour lancer l'assistant de correction des problèmes.

La partie inférieure du widget affiche le compteur d'événements non lus (le nombre d'événements importants signalés par Bitdefender, s'il y en a). Cliquez sur le compteur d'événements, par exemple 1 pour un événement non lu, pour ouvrir la fenêtre Événements. Pour plus d'informations, reportez-vous à « *Événements* » (p. 17).

5.4.1. Analyse des fichiers et des dossiers

Vous pouvez utiliser le Widget Windows pour analyser rapidement des fichiers et des dossiers. Faites glisser tout fichier ou dossier que vous souhaitez analyser et déposez-le sur le **Widget Windows**.

L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse. Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible et ne peuvent pas être modifiées. Si des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (de supprimer les codes malveillants). Si la désinfection échoue, l'Assistant d'analyse antivirus vous proposera d'indiquer d'autres moyens d'intervenir sur les fichiers infectés.

5.4.2. Masquer / afficher le Widget Windows

Lorsque vous ne souhaitez plus voir le widget, cliquez sur .

Pour restaurer le Widget Windows, utilisez l'une des méthodes suivantes :

- Dans la zone de notification :
  1. Faites un clic droit sur l'icône de Bitdefender dans la zone de notification.
  2. Cliquez sur **Afficher le Widget Windows** dans le menu contextuel qui apparaît.
- À partir de l'interface de Bitdefender :
  1. Cliquez sur l'icône en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
  2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Configurations générales**.
  3. Activez **Afficher le Widget Windows** en cliquant sur le bouton correspondant.

5.5. Rapport de sécurité

Le rapport de sécurité fournit un rapport hebdomadaire pour votre produit et plusieurs conseils pour améliorer la protection du système. Ces conseils sont importants pour gérer la protection globale et vous pouvez voir facilement les actions que vous pouvez appliquer sur votre système.

Le rapport est généré une fois par semaine et résume les principales informations sur l'activité de votre produit afin que vous puissiez comprendre facilement ce qui s'est passé pendant cette période.

Les informations fournies par le rapport de sécurité sont divisées en deux catégories :

- Zone **Protection** - permet d'afficher des informations liées à la protection de votre système.
  - **Fichiers analysés**

    Vous permet de voir les fichiers analysés par Bitdefender pour la semaine. Vous pouvez afficher des informations comme le nombre de fichiers analysés et le nombre de fichiers nettoyés par Bitdefender.

    Pour plus d'informations sur la protection antivirus, reportez-vous à « *Protection antivirus* » (p. 76).
  - **Pages Web analysées**

    Vous permet de consulter le nombre de pages web analysées et bloquées par Bitdefender. Pour vous protéger contre la divulgation d'informations personnelles lorsque vous êtes sur Internet, Bitdefender sécurise votre trafic web.

    Pour plus d'informations sur la protection Web, reportez-vous à « *Protection Web* » (p. 102).
  - **Vulnérabilités**

    Vous permet d'identifier et de corriger facilement les vulnérabilités du système afin de renforcer la protection de votre ordinateur contre les malwares et les pirates informatiques.

    Pour plus d'informations sur l'analyse de vulnérabilité, consultez « *Vulnérabilité* » (p. 107).
  - **Chronologie des événements**

    Vous permet d'avoir une image globale des processus d'analyse et des problèmes corrigés par Bitdefender au cours de la semaine. Les événements sont séparés par jours.

    Pour plus d'informations sur un journal détaillé d'événements concernant l'activité sur votre ordinateur, consultez Événements.
- La zone **Optimisation** - affiche des informations au sujet de l'espace libéré, des applications optimisées et de la quantité de batterie économisée avec le Mode Batterie.
  - **Batterie économisée**

    Vous permet de voir la quantité de batterie économisée lorsque le système fonctionnait en Mode Batterie.

Pour plus d'informations sur le Mode Batterie, reportez-vous à « *Mode Batterie* » (p. 21).

- **Application(s) optimisée(s)**

  Vous permet de voir le nombre d'applications que vous avez utilisées sous les Profils.

  Pour plus d'informations sur les Profils, reportez-vous à « *Profils* » (p. 131).

5.5.1. Consulter le rapport de sécurité

Le rapport de sécurité utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous en informer. Les problèmes détectés comprennent la désactivation d'importants paramètres de protection et d'autres conditions pouvant constituer un risque pour la sécurité. Utiliser le rapport vous permet de configurer des composants de Bitdefender spécifiques ou d'appliquer des actions préventives afin de protéger votre ordinateur et vos données confidentielles.

Pour consulter le rapport de sécurité, procédez comme suit :

1. Accédez au rapport :
   - Cliquez sur l'icône  en haut de l'interface Bitdefender puis sélectionnez **Security Report** dans le menu déroulant.
   - Faites un clic droit sur l'icône de Bitdefender dans la zone de notification et sélectionnez **Afficher le rapport de sécurité**.
   - Lorsqu'un rapport est terminé, vous serez averti par une fenêtre contextuelle. Cliquez sur **Afficher** pour accéder au rapport de sécurité.

     Une page Web s'ouvrira dans votre navigateur Web où vous pourrez voir le rapport généré.
2. Consultez la partie supérieure de la fenêtre pour voir l'état de sécurité global.
3. Consultez nos recommandations en bas de la page.

La couleur de la zone d'état de la sécurité change en fonction des problèmes détectés et différents messages s'affichent :

- **La zone est en vert.** Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.
- **La zone est en jaune.** Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
- **La zone est en rouge.** Des problèmes critiques affectent la sécurité de votre système. Nous vous recommandons de vous occuper de ces problèmes immédiatement.

5.5.2. Activer ou désactiver la notification Rapport de Sécurité

Pour activer ou désactiver la notification Rapport de sécurité, procédez comme suit :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Configurations générales**.
3. Cliquez sur le bouton correspondant pour activer ou désactiver la notification Rapport de sécurité.

   La notification Rapport de sécurité est activée par défaut.

6. BITDEFENDER CENTRAL

Bitdefender Central est la plateforme web à partir de laquelle vous avez accès aux fonctionnalités et services en ligne du produit, et peut effectuer d'importantes tâches sur les appareils sur lesquels Bitdefender est installé. Vous pouvez vous connecter à votre compte Bitdefender Central à partir de n'importe quel ordinateur ou appareil mobile connecté à Internet en allant dans https://central.bitdefender.com. Une fois que vous êtes connectés, vous pouvez commencer à faire ce qui suit :

- Télécharger et installer Bitdefender sur les systèmes d'exploitation OS X, Windows et Android. Les produits disponibles au téléchargement sont :
  - Bitdefender Antivirus Plus 2016
  - Antivirus Bitdefender pour Mac
  - Bitdefender Mobile Security
- Gérer et renouveler vos abonnement Bitdefender.
- Ajouter de nouveaux appareils à votre réseau et les gérer où que vous soyez.

6.1. Accéder à votre compte Bitdefender Central.

Il existe plusieurs façons d'accéder à votre compte Bitdefender Central. Selon la tâche que vous souhaitez effectuer, vous pouvez utiliser n'importe laquelle des possibilités suivantes :

- À partir de l'interface principale de Bitdefender :
  1. Cliquer sur le lien **Aller à Bitdefender Central** dans la partie gauche de l'interfaceBitdefender.
- A partir d'Informations du compte :
  1. Cliquez sur l'icône  en haut de l'interface Bitdefender puis sélectionnez **Infos Compte** dans le menu déroulant.
  2. Cliquer sur le lien **Aller à Bitdefender Central** dans la partie basse de la fenêtre qui apparaît.
- A partir de votre navigateur web :
  1. Ouvrir un navigateur web sur chaque appareil ayant accès à Internet.

2. Allez à : https://central.bitdefender.com.
3. Connectez-vous à votre compte à l'aide de votre adresse courriel et de votre mot de passe.

6.2. Mes licences

La plateforme Bitdefender Central vous donne la possibilité de gérer facilement vos abonnements pour tous vos appareils.

6.2.1. Vérifier les abonnements disponibles

Pour vérifier vos abonnements disponibles :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionner le panneau **Mes Abonnements**.

Vous trouverez ici des informations sur la disponibilité des abonnements que vous avez et le nombre d'appareils qui les utilisent.

Vous pouvez ajouter un nouvel appareil à un abonnement ou le renouveler en sélectionnant une carte d'abonnement.

Note
Vous pouvez avoir un ou plusieurs abonnements sur votre compte, pourvu qu'ils soient pour différentes plateformes (Windows, Mac OS X, ou Android).

6.2.2. Ajouter un nouvel appareil

Si votre abonnement couvre plus d'un appareil, vous pouvez ajouter un nouvel appareil et y installer votre Bitdefender Antivirus Plus 2016, comme suit :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionnez le panneau **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
4. Sélectionnez l'une des deux actions disponibles :
   - **TÉLÉCHARGER**

     Cliquez sur le bouton pour sauvegarder le fichier d'installation.
   - **Sur un autre appareil**

Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER**.

5. Attendez que le téléchargement soit terminé, puis lancez l'installation.

6.2.3. Renouveler abonnement

Si vous n'avez pas choisi le renouvellement automatique pour votre abonnement Bitdefender, vous pouvez le faire manuellement en suivant ces étapes :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionner le panneau **Mes Abonnements**.
3. Sélectionnez la carte d'abonnement souhaitée.
4. Cliquez sur **Renouveler** pour poursuivre.

Une page web s'ouvre dans votre navigateur, sur laquelle vous pouvez renouveler votre abonnement Bitdefender.

6.2.4. Activer abonnement

Un abonnement peut être activé pendant le processus d'installation à l'aide de votre compte Bitdefender Central. En même temps que le processus d'activation, sa validité commence le compte à rebours.

Si vous avez acheté un code d'activation chez l'un de nos revendeurs ou que vous l'avez reçu en cadeau, vous pouvez ajouter sa disponibilité à tout abonnement Bitdefender existant disponible sur le compte, s'ils sont pour le même produit.

Pour activer l'abonnement avec un code d'activation, suivez ces étapes :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionner le panneau **Mes Abonnements**.
3. Cliquez sur le bouton **CODE D'ACTIVATION**, puis saisissez le code dans le champs correspondant.
4. Cliquez sur **SOUMETTRE**.

L'abonnement est désormais activé. Allez dans le panneau **Mes Appareils**, et sélectionnez **INSTALLER Bitdefender** pour installer le produit sur l'un de vos appareils.

6.3. Mes appareils

La zone **Mes Appareils** dans votre compte Bitdefender Central vous donne la possibilité d'installer, gérer et exécuter des actions à distance sur votre produit Bitdefender sur n'importe quel appareil, pourvu qu'il soit allumé et connecté à Internet. Les cartes appareils affichent le nom de l'appareil, le statut de protection et la disponibilité restante de votre abonnement.

Pour identifier vos appareils facilement, vous pouvez personnaliser le nom de l'appareil :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionnez le panneau **Mes Appareils**.
3. Cliquez sur l'icône ⋮ sur la carte appareil souhaitée, puis sélectionnez **Paramètres**.
4. Changez le nom de l'appareil dans le champs correspondant, puis sélectionnez **Sauvegarder**.

Si Autopilot est désactivé, vous pouvez l'activer en cliquant sur le bouton. Cliquez sur **Enregistrer** pour appliquer les configurations.

Vous pouvez créer et assigner un propriétaire pour chacun de vos appareils pour une meilleure gestion :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionnez le panneau **Mes Appareils**.
3. Cliquez sur l'icône ⋮ sur la carte appareil souhaitée, puis sélectionnez **Profil**.
4. Cliquez sur **Ajouter propriétaire**, puis remplissez les champs correspondants, configurer le sexe, la date de naissance, et ajoutez une photo de profil si vous le souhaitez.
5. Cliquez sur **AJOUTER** pour sauvegarder le profil.
6. Sélectionnez le propriétaire souhaité à partir de la liste **Propriéaire appareil**, puis cliquez sur **ASSIGNER**.

Pour mettre à jour Bitdefender à distance sur un appareil, suivez ces étapes :

1. Accédez à votre compte Bitdefender Central.

2. Sélectionnez le panneau **Mes Appareils**.
3. Cliquez sur l'icône ⋮ sur la carte appareil souhaitée, puis sélectionnez **Mise à jour**.

Pour plus d'actions à distance et d'informations concernant votre produit Bitdefender sur un appareil spécifique, cliquez sur la carte appareil souhaitée.

Une fois que vous avez cliqué sur une carte appareil, les onglets suivants sont disponibles :

- **Tableau de bord**. Dans cette fenêtre, vous pouvez vérifier le statut de protection de vos produits Bitdefenderet le nombre de jours restants pour votre abonnement. Le statut de protection peut être vert lorsque aucun problème n'affecte votre produit, ou rouge si le produit est en danger. Quand des problèmes affectent votre produit, cliquez sur **Voir problèmes** pour en savoir plus. A partir de là, vous pouvez réparer manuellement les problèmes qui affectent la sécurité de vos appareils.
- **Protection**. A partir de cette fenêtre, vous pouvez lancer à distance une Analyse rapide ou une Analyse système sur vos appareils. Cliquez sur le bouton **ANALYSE** pour commencer le processus. Vous pouvez également vérifier à quelle date la dernière analyse a été faite sur l'appareil, et un rapport de l'analyse la plus récente contenant les informations importantes est à votre disposition.Pour plus d'informations sur les deux processus d'analyse, reportez-vous à « *Exécuter une analyse du système* » (p. 85) et à « *Exécuter une Analyse Rapide* » (p. 84) .
- **Vulnérabilité**. Pour vérifier les vulnérabilités sur un appareil (comme les mises à jour Windows manquantes, les applications obsolètes, ou les mots de passe faibles) cliquez sur le bouton **ANALYSE** dans l'onglet Vulnérabilité. Les vulnérabilités ne peuvent pas être réparées à distance. Dans le cas où une vulnérabilité est trouvée, vous devez exécuter une nouvelle analyse sur l'appareil puis effectuer les actions recommandées. Pour plus de détails sur cette fonctionnalité, reportez-vous à « *Vulnérabilité* » (p. 107).

7. MAINTENIR BITDEFENDER À JOUR

De nouveaux virus sont trouvés et identifiés chaque jour. C'est pourquoi il est très important que Bitdefender soit à jour dans les signatures de codes malveillants.

Si vous êtes connecté à Internet par câble ou DSL, Bitdefender s'en occupera automatiquement. Par défaut, des mises à jour sont recherchées au démarrage de votre ordinateur puis toutes les **heures** après cela. Si une mise à jour est détectée, elle est automatiquement téléchargée et installée sur votre ordinateur.

Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

Important
Pour être protégé contre les dernières menaces, maintenez la mise à jour automatique activée.

Votre intervention peut être nécessaire, dans certains cas, pour maintenir la protection de Bitdefender à jour :

- Si votre ordinateur se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy comme indiqué dans « *Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?* » (p. 69).
- Des erreurs peuvent se produire lors du téléchargement de mises à jour avec une connexion à Internet lente. Pour savoir comment éviter ces erreurs, veuillez consulter « *Comment mettre à jour Bitdefender avec une connexion Internet lente ?* » (p. 144).
- Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour à la demande de Bitdefender. Pour plus d'informations, reportez-vous à « *Mise à jour en cours* » (p. 45).

7.1. Vérifier que Bitdefender est à jour

Pour vérifier l'heure de la dernière mise à jour de votre Bitdefender, regardez la **Zone état sécurité**, sur le côté gauche de la barre d'outils.

Pour des informations détaillées sur les dernières mises à jour, vérifiez les événements de mise à jour :

1. Dans la fenêtre principale, cliquez sur l'icône  en haut de l'interfaceBitdefender et sélectionnez **Événements** dans le menu déroulant.
2. Dans la fenêtre **Événements**, sélectionnez **Mise à jour** dans le menu déroulant correspondant.

Vous pouvez savoir quand des mises à jour ont été lancées et obtenir des informations à leur sujet (si elles ont été ou non réussies, si elles nécessitent un redémarrage pour que leur installation se termine). Si nécessaire, redémarrez le système dès que possible.

7.2. Mise à jour en cours

Pour effectuer des mises à jour, une connexion à Internet est requise.

Pour lancer une mise à jour, choisissez l'une des options suivantes :

- Ouvrez l'interfaceBitdefender et cliquez sur le bouton d'action **Mise à jour**.
- Faites un clic droit sur l'icône de Bitdefender  de la zone de notification et sélectionnez **Mettre à jour maintenant**.

Le module de Mise à jour se connectera au serveur de mise à jour de Bitdefender et recherchera des mises à jour. Si une mise à jour est détectée, elle sera installée automatiquement ou il vous sera demandé de confirmer son installation, selon les paramètres de mise à jour.

Important
Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Il est recommandé de le faire dès que possible

Vous pouvez également réaliser des mises à jour à distance sur vos appareils, pourvu qu'ils soient allumés et connectés à Internet.

Pour mettre à jour Bitdefender à distance sur un appareil, suivez ces étapes :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionnez le panneau **Mes Appareils**.

3. Cliquez sur l'icône ⋮ sur la carte appareil souhaitée, puis sélectionnez **Mise à jour**.

7.3. Activer ou désactiver la mise à jour automatique

Pour activer ou désactiver la mise à jour automatique, procédez comme suit :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Mise à jour**.
3. Cliquez sur le bouton pour activer ou désactiver la mise à jour automatique.
4. Une fenêtre d'avertissement s'affiche. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactivez la mise à jour automatique. Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

Avertissement
Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la mise à jour automatique pendant le moins de temps possible. Si Bitdefender n'est pas régulièrement mis à jour, il ne pourra pas vous protéger contre les dernières menaces.

7.4. Réglage des paramètres de mise à jour

Les mises à jour peuvent être réalisées depuis le réseau local, depuis Internet, directement ou à travers un serveur proxy. Par défaut, Bitdefender recherche les mises à jour chaque heure sur Internet et installe celles qui sont disponibles sans vous en avertir.

Les paramètres de mise à jour par défaut sont adaptés à la plupart des utilisateurs et vous n'avez normalement pas besoin de les modifier.

Pour régler les paramètres de mise à jour, suivez ces étapes :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.

2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Mise à jour** et ajustez les paramètres en fonction de vos préférences.

Fréquence de la mise à jour

Bitdefender est configuré pour chercher des mises à jour toutes les jours. Pour changer la fréquence des mises à jour, bougez le curseur le long de l'échelle pour configurer la période durant laquelle la mise à jour doit se faire.

Emplacement de mise à jour

Bitdefender est configuré pour se mettre à jour à partir des serveurs de mise à jour de Bitdefender sur Internet. L'emplacement de mise à jour est une adresse Internet générique qui est automatiquement redirigée vers le serveur de mise à jour Bitdefender le plus proche de votre région.

Ne modifiez pas l'emplacement de mise à jour sauf sur demande d'un représentant de Bitdefender ou de votre administrateur réseau (si vous êtes connecté à un réseau d'entreprise).

Vous pouvez revenir à l'emplacement de mise à jour Internet générique en cliquant sur **Par défaut**.

Règles de traitement

Vous disposez de trois façons de télécharger et d'installer des mises à jour :

- **Mise à jour silencieuse** - Bitdefender télécharge et implémente automatiquement la mise à jour.
- **Demander avant de télécharger les mises à jour** - à chaque fois qu'une mise à jour sera disponible, le système demandera votre autorisation avant de la télécharger.
- **Demander avant l'installation** - à chaque fois qu'une mise à jour est téléchargée, le système demande votre autorisation avant de l'installer.

Certaines mises à jour nécessitent un redémarrage pour terminer l'installation. Par défaut, si une mise à jour nécessite un redémarrage, Bitdefender continuera à fonctionner avec les anciens fichiers jusqu'à ce que l'utilisateur redémarre volontairement l'ordinateur. Cela évite que le processus de mise à jour de Bitdefender interfère avec le travail de l'utilisateur.

Si vous souhaitez être averti lorsqu'une mise à jour nécessite un redémarrage, désactivez l'option **Reporter le redémarrage** en cliquant sur le bouton correspondant.

COMMENT FAIRE POUR

8. INSTALLATION

8.1. Comment installer Bitdefender sur un deuxième ordinateur ?

Si l'abonnement que vous avez acheté couvre plus d'un seul ordinateur, vous pouvez utiliser votre compte Bitdefender Central pour enregistrer un second PC.

Pour installer Bitdefender correctement sur un second ordinateur, suivez les étapes suivantes :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionnez le panneau **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
4. Sélectionnez l'une des deux actions disponibles :
   - **TÉLÉCHARGER**

     Cliquez sur le bouton pour sauvegarder le fichier d'installation.
   - **Sur un autre appareil**

     Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER**.
5. Exécutez le produit Bitdefender que vous avez installé. Attendez la fin du processus d'installation et fermez la fenêtre.

Le nouvel appareil sur lequel vous avez installé le produit Bitdefender apparaîtra désormais sur le tableau de bord Bitdefender Central.

8.2. Quand devrais-je réinstaller Bitdefender ?

Dans certains cas, vous pouvez avoir besoin de réinstaller votre produit Bitdefender.

Quelques situations typiques nécessitant de réinstaller Bitdefender :

- vous avez réinstallé le système d'exploitation.
- vous avez acheté un nouvel ordinateur.

- vous souhaitez modifier la langue d'affichage de l'interface de Bitdefender .

Pour réinstaller Bitdefender, vous pouvez utiliser le disque d'installation que vous avez acheté ou télécharger une nouvelle version à partir de votre compte Bitdefender Central.

Pour plus d'informations sur le processus d'installation de Bitdefender, reportez-vous à « *Installer Bitdefender* » (p. 5).

8.3. Où est-ce que je peux télécharger mon produit Bitdefender ?

Vous pouvez installer Bitdefender à partir du disque d'installation ou en utilisant un programme d'installation téléchargé sur votre ordinateur à partir de la plateforme Bitdefender Central.

Note
Avant de lancer le kit, nous vous recommandons de désinstaller toutes les solutions antivirus présentes sur votre système. Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, le système devient instable.

Pour installer Bitdefender à partir du compte Bitdefender Central, suivez ces étapes :

1. Accédez à votre compte Bitdefender Central.
2. Sélectionnez le panneau **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
4. Sélectionnez l'une des deux actions disponibles :
   - **TÉLÉCHARGER**

     Cliquez sur le bouton pour sauvegarder le fichier d'installation.
   - **Sur un autre appareil**

     Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER**.
5. Exécutez le produit Bitdefender que vous avez installé.

8.4. Comment utiliser mon abonnementBitdefender après une mise à niveau Windows ?

Cette situation se produit lorsque vous mettez à niveau votre système d'exploitation et souhaitez continuer à utiliser votre abonnement Bitdefender.

Si vous utilisez une version antérieure de Bitdefender vous pouvez la mettre à niveau, gratuitement, vers la dernière version de Bitdefender en procédant comme suit :

- D'une ancienne version de Bitdefender Antivirus vers la dernière version de Bitdefender Antivirus disponible.
- D'une ancienne version de Bitdefender Internet Security vers la dernière version de Bitdefender Internet Security disponible.
- D'une ancienne version de Bitdefender Total Security vers la dernière version de Bitdefender Total Security disponible.

Deux situations peuvent se produire :

- Vous avez mis à niveau le système d'exploitation à l'aide de Windows Update et vous remarquez que Bitdefender ne fonctionne plus.

  Dans ce cas, vous avez besoin de réinstaller le produit avec la dernière version disponible.

  Pour résoudre cette situation, suivez ces étapes :

  1. Supprimez Bitdefender en procédant comme suit :
     - Dans **Windows 7** :
       a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
       b. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
       c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
       d. Cliquez sur **Suivant** pour continuer.
       e. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
     - Dans **Windows 8 et Windows 8.1** :

a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.

b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.

c. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.

d. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

e. Cliquez sur **Suivant** pour continuer.

f. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

- Dans **Windows 10** :

a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".

b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.

c. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.

d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.

e. Cliquez sur **Supprimer** puis sélectionnez **Je souhaite le réinstaller**.

f. Cliquez sur **Suivant** pour continuer.

g. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

2. Téléchargez le fichier d'installation :

a. Accédez à votre compte Bitdefender Central.

b. Sélectionnez le panneau **Mes Appareils**.

c. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.

d. Sélectionnez l'une des deux actions disponibles :

- **TÉLÉCHARGER**

  Cliquez sur le bouton pour sauvegarder le fichier d'installation.

- **Sur un autre appareil**

  Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER**.

3. Exécutez le produit Bitdefender que vous avez installé.

- Vous avez changé de système et souhaitez continuer à utiliser la protection Bitdefender.

  Vous avez donc besoin de réinstaller le produit avec la dernière version.

  Pour résoudre cette situation :

  1. Téléchargez le fichier d'installation :
     a. Accédez à votre compte Bitdefender Central.
     b. Sélectionnez le panneau **Mes Appareils**.
     c. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
     d. Sélectionnez l'une des deux actions disponibles :

     - **TÉLÉCHARGER**

       Cliquez sur le bouton pour sauvegarder le fichier d'installation.

     - **Sur un autre appareil**

       Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER**.

  2. Exécutez le produit Bitdefender que vous avez installé.

  Pour plus d'informations sur le processus d'installation de Bitdefender, reportez-vous à « *Installer Bitdefender* » (p. 5).

8.5. Comment réparer Bitdefender ?

Si vous souhaitez réparer votre produit Bitdefender Antivirus Plus 2016 à partir du menu Démarrer de Windows, procédez comme suit :

- Dans **Windows 7** :

  1. Cliquez sur **Démarrer** et allez dans **Programmes**.
  2. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
  3. Cliquez sur **Réparer** dans la fenêtre qui s'affiche.

Cela prendra quelques minutes.

4. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.

- Dans **Windows 8 et Windows 8.1** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
4. Cliquez sur **Réparer** dans la fenêtre qui s'affiche.

   Cela prendra quelques minutes.
5. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.

- Dans **Windows 10** :

1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **& Fonctionnalités Applications**.
3. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Cliquez sur **Réparer**.

   Cela prendra quelques minutes.
6. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.

9. LICENCE(S)

9.1. Quel est le produit Bitdefender que j'utilise ?

Pour voir quel programme Bitdefender vous avez installé :

1. Ouvrir l'interface de Bitdefender.
2. En haut de la fenêtre devrait apparaître l'un des éléments suivants :
   - Bitdefender Antivirus Plus 2016
   - Bitdefender Internet Security 2016
   - Bitdefender Total Security 2016

9.2. Comment activer l'abonnement Bitdefender à l'aide d'une clé de licence ?

Si vous avez une clé de licence valide et que vous souhaitez l'utiliser pour activer votre abonnement pour Bitdefender Antivirus Plus 2016, il y a deux cas possibles :

- Vous avez fait une mise à niveau à partir d'une version précédente de Bitdefender vers la nouvelle :
  1. Une fois que la mise à niveau vers Bitdefender Antivirus Plus 2016 est terminée, vous devez vous connecter à votre compte Bitdefender Central.
  2. Saisissez vos identifiants de connexion,puis cliquez sur **CONNEXION**.
  3. Une notification vous informant qu'un abonnement a été créé apparaît sur l'écran de votre compte. L'abonnement créé sera valide pour la période restante sur votre clé de licence et pour le même nombre d'utilisateurs.

     Les appareils qui utilisent les versions précédentes de Bitdefender et sont enregistrés avec la clé de licence que vous avez convertie en abonnement doivent enregistrer le produit avec le même compte Bitdefender Central.
- Bitdefender n'était pas précédemment installé sur le système :
  1. Dès que le processus d'installation est terminé, vous devez vous connecter à votre compte Bitdefender Central.

2. Saisissez vos identifiants de connexion,puis cliquez sur **CONNEXION**.
3. Sélectionner le panneau **Mes Abonnements**.
4. Cliquez sur le bouton **CODE D'ACTIVATION**, et saisissez votre clé de licence.
5. Cliquez sur **SOUMETTRE**. Un abonnement avec la même disponibilité et nombre d'utilisateurs pour votre clé de licence est associée à votre compte.

10. BITDEFENDER CENTRAL

10.1. Comment me connecter à Bitdefender Central à l'aide d'un autre compte en ligne ?

Vous avez créé un nouveau compte Bitdefender Central et souhaitez l'utiliser à partir de maintenant.

Pour créer un autre compte, suivez ces étapes :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Infos Compte** dans le menu déroulant.
2. Cliquez sur le bouton **Changer de compte** pour changer le compte lié à l'ordinateur.
3. Tapez l'adresse courriel et le mot de passe de votre compte dans les champs correspondants, puis cliquez sur **Connexion**.

> **Note**
> Le produit Bitdefender de votre appareil change automatiquement selon l'abonnement associé au nouveau compte Bitdefender Central.
> S'il n'y a pas d'abonnement disponible associé au nouveau compte Bitdefender Central, ou que vous souhaitez le transférer à partir du compte précédent, vous pouvez contacter le support Bitdefender comme décrit dans la rubrique « *Demander de l'aide* » (p. 162).

10.2. Comment redéfinir le mot de passe du compte Bitdefender Central ?

Pour définir un nouveau mot de passe pour votre compte Bitdefender Central, procédez comme suit :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Infos Compte** dans le menu déroulant.
2. Cliquez sur le bouton **Changer de compte** pour changer le compte lié à l'ordinateur.

   Une nouvelle fenêtre apparaît.
3. Cliquez sur le lien **Reconfigurer mot de passe**.

4. Saisissez l'adresse courriel utilisée pour créer votre compte Bitdefender Central puis cliquez sur le bouton **Réinitialiser mot de passe**.
5. Consultez votre courriel et cliquez sur le lien indiqué.
6. Saisissez votre adresse e-mail dans le champ correspondant.
7. Saisissez le nouveau mot de passe. Le mot de passe doit contenir au moins 8 caractères et contenir des chiffres.
8. Cliquez sur **Se connecter**.

Pour accéder à votre compte Bitdefender Central, saisissez votre adresse courriel et le nouveau mot de passe que vous venez de définir.

11. ANALYSER AVEC BITDEFENDER

11.1. Comment analyser un fichier ou un dossier ?

La méthode la plus simple pour analyser un fichier ou un dossier consiste à faire un clic droit sur l'objet que vous souhaitez analyser, à pointer sur Bitdefender et à sélectionner **Analyser avec Bitdefender** dans le menu.

Pour terminer l'analyse, suivez l'assistant d'analyse antivirus. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés.

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

Cette méthode d'analyse est à utiliser dans des situations courantes qui englobent les cas suivants :

- Vous soupçonnez un fichier ou un dossier donné d'être infecté.
- Quand vous téléchargez sur Internet des fichiers dont vous pensez qu'ils pourraient être dangereux.
- Analysez un dossier partagé sur le réseau avant de copier des fichiers sur votre ordinateur.

11.2. Comment analyser mon système ?

Pour effectuer une analyse complète du système, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Analyse du Système**.
4. Suivez les indications de l'Assistant d'analyse système pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés.

   Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 88).

11.3. Comment programmer une analyse ?

Vous pouvez configurer le produit Bitdefender pour commencer à analyser les localisations systèmes importantes quand vous n'êtes pas devant votre ordinateur.

Pour programmer une analyse, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Gestion des analyses**.
4. Choisissez le type d'analyse que vous souhaitez programmer, Analyse système ou Analyse rapide, puis cliquez sur **Options Analyse**.

   Alternativement, vous pouvez créer un type d'analyse qui correspond à vos besoins en cliquant sur **Nouvelle tâche personnalisée**.
5. Activer le bouton **Programme**.

   Sélectionnez l'une des options correspondantes pour définir une planification :

   - Au démarrage du système
   - Une fois
   - Périodiquement

Dans la fenêtre **Cibles analyse** vous pouvez choisir les localisations que vous souhaitez analyser.

11.4. Comment créer une tâche d'analyse personnalisée ?

Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

Pour créer une tâche d'analyse personnalisée, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.

2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Gestion des analyses**.
4. Cliquez sur **Nouvelle tâche personnalisée**. Saisissez un nom pour l'analyse dans l'onglet **Standard** et sélectionnez les emplacements à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**.

   Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour choisir le niveau d'analyse souhaité.

   Vous pouvez également choisir d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée. N'oubliez pas qu'il s'agira du comportement par défaut à chaque fois que vous exécuterez cette tâche.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
7. Utilisez le bouton correspondant si vous souhaitez définir une planification pour cette tâche d'analyse.
8. Cliquez sur **Démarrer l'analyse** et suivez l'Assistant d'analyse pour terminer l'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
9. Si vous le souhaitez, vous pouvez relancer rapidement une analyse personnalisée en cliquant sur le bouton correspondant dans la liste.

11.5. Comment exclure un dossier de l'analyse ?

Bitdefender vous permet d'exclure de l'analyse certains fichiers, dossiers ou extensions de fichiers.

Les exclusions doivent être employées par des utilisateurs ayant un niveau avancé en informatique et uniquement dans les situations suivantes :

- Vous avez un dossier important sur votre système où se trouvent des films et de la musique.
- Vous avez une archive importante sur votre système où se trouvent différentes données.
- Vous gardez un dossier où vous installez différents types de logiciels et applications à des fins de test. L'analyse du dossier peut conduire à la perte de certaines données.

Pour ajouter le dossier à la liste d'exceptions, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus** puis sélectionnez l'onglet **Exclusions**.
4. Veillez à ce qu'**Exclusions pour les fichiers** soit activé en cliquant sur le bouton.
5. Cliquez sur le lien **Fichiers et dossiers exclus**.
6. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
7. Cliquez sur **Parcourir**, sélectionnez le dossier à exclure de l'analyse, puis cliquez sur **OK**.
8. Cliquez sur **Ajouter** puis sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

11.6. Que faire lorsque Bitdefender a détecté un fichier sain comme infecté ?

Il arrive parfois que Bitdefender indique par erreur qu'un fichier légitime est une menace (une fausse alerte). Pour corriger cette erreur, ajoutez le fichier à la zone des exclusions de Bitdefender :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
   b. Sélectionnez l'onglet **Protection**.
   c. Cliquez sur le module **Antivirus**.
   d. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
   e. Cliquez sur le bouton pour désactiver l'**Analyse à l'accès**.

      Une fenêtre d'avertissement s'affiche. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactivez la protection en temps- réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 71).
3. Restaurer le fichier à partir de la zone de quarantaine :
   a. Cliquer sur l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
   b. Sélectionnez l'onglet **Protection**.
   c. Cliquez sur le module **Antivirus** puis sélectionnez l'onglet **Quarantaine**.
   d. Sélectionnez le fichier et cliquez sur **Restaurer**.
4. Ajouter le fichier à la liste d'exceptions. Pour savoir comment faire cela, consultez « *Comment exclure un dossier de l'analyse ?* » (p. 62).
5. Activez la protection antivirus en temps réel de Bitdefender.
6. Contactez les représentants de notre soutien technique afin que nous puissions supprimer la signature de détection. Pour savoir comment faire cela, consultez « *Demander de l'aide* » (p. 162).

11.7. Comment connaître les virus détectés par Bitdefender ?

À chaque fois qu'une analyse est effectuée, un journal d'analyse est créé et Bitdefender enregistre les problèmes détectés.

Le rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises à l'encontre de ces menaces.

Vous pouvez ouvrir le journal d'analyse directement à partir de l'assistant d'analyse, une fois l'analyse terminée, en cliquant sur **Afficher le Journal**.

Pour consulter ultérieurement un journal d'analyse ou toute infection détectée, procédez comme suit :

1. Cliquez sur l'icône en haut de l'interface Bitdefender et sélectionnez **Événements** dans le menu déroulant.
2. Dans la fenêtre **Événements**, sélectionnez **Antivirus** dans le menu déroulant correspondant.

Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.

3. Dans la liste des événements, vous pouvez consulter les analyses ayant été réalisées récemment. Cliquez sur un événement pour afficher des informations à son sujet.
4. Pour ouvrir un journal d'analyse, cliquez sur **Afficher le journal**.

   Si vous souhaitez exécuter la même analyse encore une fois, cliquez sur le bouton **Ré analyser**

12. PROTECTION DE LA VIE PRIVÉE

12.1. Comment vérifier que ma transaction en ligne est sécurisée ?

Pour assurer la confidentialité de vos opérations en ligne, vous pouvez utiliser le navigateur fourni par Bitdefender pour protéger vos transations et applications bancaires.

Bitdefender Safepay™ est un navigateur sécurisé conçu pour protéger vos informations bancaires, votre numéro de compte et toutes les autres données confidentielles que vous pouvez saisir lorsque vous accédez à différents sites en ligne.

Pour assurer la sécurité et la confidentialité de vos activités en ligne, procédez comme suit :

1. Cliquez sur le bouton d'action **Safepay** à partir de l'interface Bitdefender.
2. Cliquez sur le bouton pour accéder au **Clavier virtuel**.
3. Utilisez le **Clavier virtuel** lorsque vous tapez des informations confidentielles telles que des mots de passe.

12.2. Comment supprimer définitivement un fichier avec Bitdefender ?

Si vous souhaitez supprimer définitivement un fichier de votre système, vous avez besoin de supprimer physiquement les données de votre disque dur.

Le Destructeur de fichiers Bitdefender vous aidera à détruire rapidement des fichiers ou dossiers de votre ordinateur à l'aide du menu contextuel de Windows, en procédant comme suit :

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement, pointez sur Bitdefender et sélectionnez **Destructeur de fichiers**.
2. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour lancer l'assistant du destructeur de fichiers.
3. Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
4. Les résultats sont affichés. Cliquez sur **Fermer** pour quitter l'assistant.

13. INFORMATIONS UTILES

13.1. Comment tester ma solution antivirus ?

Pour vérifier que votre produit Bitdefender fonctionne correctement, nous vous recommandons d'utiliser le test Eicar.

Le test Eicar vous permet de vérifier votre protection antivirus à l'aide d'un fichier sûr développé à cet effet.

Pour tester votre solution antivirus, procédez comme suit :

1. Téléchargez le test à partir de la page Web officielle de l'organisme EICAR http://www.eicar.org/.
2. Cliquez sur l'onglet **Anti-Malware Testfile**.
3. Cliquez sur **Download** dans le menu de gauche.
4. Dans **Download area using the standard protocol http** cliquez sur le fichier de test **eicar.com**.
5. Vous serez informé que la page à laquelle vous essayez d'accéder contient « EICAR-Test-File (not a virus) ».

   Si vous cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**, le téléchargement du test débutera et une fenêtre pop-up de Bitdefender vous indiquera qu'un virus a été détecté.

   Cliquez sur **Plus de détails** pour obtenir plus d'informations sur cette action.

Si vous ne recevez pas d'alerte Bitdefender, nous vous recommandons de contacter Bitdefender pour obtenir de l'aide comme indiqué dans la section « *Demander de l'aide* » (p. 162).

13.2. Comment désinstaller Bitdefender ?

Si vous souhaitez désinstaller Bitdefender Antivirus Plus 2016, procédez comme suit :

- Dans **Windows 7** :
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
  2. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.

3. Sélectionnez **Remove**, puis **Je souhaite le désinstaller définitivement**.
4. Cliquez sur **Suivant** pour continuer.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

- Dans **Windows 8 et Windows 8.1** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
4. Sélectionnez **Remove**, puis **Je souhaite le désinstaller définitivement**.
5. Cliquez sur **Suivant** pour continuer.
6. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

- Dans **Windows 10** :

1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
3. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Sélectionnez **Remove**, puis **Je souhaite le désinstaller définitivement**.
6. Cliquez sur **Suivant** pour continuer.
7. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

13.3. Comment éteindre automatiquement l'ordinateur une fois l'analyse terminée ?

Bitdefender propose plusieurs tâches d'analyse que vous pouvez utiliser pour vérifier que votre système n'est pas infecté par des malwares. L'analyse

de l'ensemble de l'ordinateur peut prendre plus de temps en fonction de la configuration matérielle et logicielle de votre système.

C'est pourquoi Bitdefender vous permet de configurer Bitdefender pour éteindre votre système dès que l'analyse est terminée.

Prenons l'exemple suivant : vous avez terminé d'utiliser l'ordinateur et souhaitez aller dormir. Vous aimeriez que l'ensemble de votre système fasse l'objet d'une analyse antimalware par Bitdefender.

Voici comment configurer Bitdefender pour éteindre votre système à la fin de l'analyse :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Gestion des analyses**.
4. Dans la fenêtre **Gérer les tâches d'analyse**, cliquez sur **Nouvelle tâche personnalisée** pour saisir un nom pour l'analyse et sélectionnez les emplacements à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**.
6. Choisissez d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
8. Cliquez sur le bouton **Démarrer analyse** pour analyser votre système.

Si aucune menace n'est détectée, l'ordinateur sera éteint.

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 88).

13.4. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?

Si votre ordinateur se connecte à Internet via un serveur proxy, vous devez configurer Bitdefender avec les paramètres du proxy. Normalement,

Bitdefender détecte et importe automatiquement les paramètres proxy de votre système.

Important
Les connexions résidentielles à Internet n'utilisent normalement pas de serveur proxy. En règle générale, vérifiez et configurez les paramètres de connexion proxy de Bitdefender lorsque aucune mise à jour n'est en cours. Si Bitdefender peut effectuer des mises à jour, alors il est correctement configuré pour se connecter à Internet.

Pour gérer les paramètres proxy, procédez comme suit :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Avancé**.
3. Activez l'utilisation du proxy en cliquant sur le bouton.
4. Cliquez sur le lien **Gérer proxy**.
5. Deux options permettent de définir les paramètres du proxy :
   - **Importer les paramètres proxy à partir du navigateur par défaut** - paramètres du proxy de l'utilisateur actuel provenant du navigateur par défaut. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.

     Note
     Bitdefender peut importer les paramètres proxy des principaux navigateurs, y compris des dernières versions d'Internet Explorer, de Mozilla Firefox et d'Opera.

   - **Paramètres proxy personnalisés** - paramètres proxy que vous pouvez configurer vous-même. Voici les paramètres à spécifier:
     - **Adresse** - saisissez l'adresse IP du serveur proxy.
     - **Port** - saisissez le port utilisé par Bitdefender pour se connecter au serveur proxy.
     - **Nom d'utilisateur** - entrez le nom d'utilisateur reconnu par le serveur proxy.
     - **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Bitdefender utilisera les paramètres proxy disponibles jusqu'à ce qu'il parvienne à se connecter à Internet.

13.5. Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?

Pour savoir si vous disposez d'un système d'exploitation de 32 ou de 64 bits, suivez les étapes ci-dessous :

- Dans **Windows 7** :
  1. Cliquez sur **Démarrer**.
  2. Repérez **Ordinateur** dans le menu **Démarrer**.
  3. Faites un clic droit sur **Ordinateur** et sélectionnez **Propriétés**.
  4. Consultez ce qui est indiqué sous **Système** afin de vérifier les informations concernant votre système.
- Dans **Windows 8 et Windows 8.1** :
  1. Dans l'écran d'accueil Windows, localisez l'**Ordinateur** (vous pouvez, par exemple, taper « Ordinateur » directement dans l'écran d'accueil), puis faites un clic droit sur son icône.
  2. Sélectionnez **Propriétés** dans le menu inférieur.
  3. Regardez sous Système pour connaître le type de système.
- Dans **Windows 10** :
  1. Tapez "Système" dans le champ de recherche de la barre des tâches et cliquez sur son icône.
  2. Regardez sous Système pour connaître le type de système.

13.6. Comment afficher des objets cachés dans Windows ?

Ces étapes sont utiles en cas de malwares, si vous avez besoin de détecter et de supprimer les fichiers infectés, qui peuvent être cachés.

Suivez ces étapes pour afficher les objets cachés dans Windows :

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration**.

Dans **Windows 8 et Windows 8.1** : Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil), puis cliquez sur son icône.

2. Sélectionnez **Options des dossiers**.
3. Allez dans l'onglet **Afficher**.
4. Sélectionnez **Afficher les fichiers et les dossiers cachés**.
5. Décochez **Masquer les extensions des fichiers dont le type est connu**.
6. Décochez **Masquer les fichiers protégés du système d'exploitation**.
7. Cliquez sur **Appliquer** puis sur **OK**.

Dans **Windows 10** :

1. Tapez "Afficher les fichiers et les dossiers cachés" dans le champ de recherche de la barre des tâches puis cliquez sur son icône.
2. Sélectionnez **Afficher les fichiers et les dossiers cachés**.
3. Décochez **Masquer les extensions des fichiers dont le type est connu**.
4. Décochez **Masquer les fichiers protégés du système d'exploitation**.
5. Cliquez sur **Appliquer** puis sur **OK**.

13.7. Comment supprimer les autres solutions de sécurité ?

La principale raison à l'utilisation d'une solution de sécurité est d'assurer la protection et la sécurité de vos données. Mais qu'arrive-t-il quand vous avez plus d'un produit de sécurité sur le même système ?

Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, le système devient instable. Le programme de désinstallation de Bitdefender Antivirus Plus 2016 détecte d'autres programmes de sécurité et vous permet de les désinstaller.

Si vous n'avez pas supprimé les autres solutions de sécurité au cours de l'installation initiale, suivez ces étapes :

- Dans **Windows 7** :

  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.

2. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
3. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
4. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

- Dans **Windows 8 et Windows 8.1** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
4. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

- Dans **Windows 10** :

1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
3. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

Si vous ne parvenez pas à supprimer l'autre solution de sécurité de votre système, obtenez l'outil de désinstallation sur le site web de l'éditeur ou contactez-les directement afin qu'ils vous indiquent la procédure de désinstallation.

13.8. Comment redémarrer en mode sans échec ?

Le mode sans échec est un mode de fonctionnement de diagnostic, utilisé principalement pour résoudre des problèmes affectant le fonctionnement normal de Windows. Ce type de problèmes peut intervenir lors de conflits de pilotes et de virus empêchant Windows de démarrer normalement. En mode sans échec, seules quelques applications fonctionnent et Windows ne charge que les pilotes de base et un minimum de composants du système d'exploitation. C'est pourquoi la plupart des virus sont inactifs lorsque Windows est en mode sans échec et qu'ils peuvent être supprimés facilement.

Pour démarrer Windows en mode sans échec :

1. Redémarrez votre système.
2. Appuyez plusieurs fois sur la touche **F8** avant que Windows ne démarre afin d'accéder au menu de démarrage.
3. Sélectionnez **Mode sans échec** dans le menu de démarrage ou **Mode sans échec avec prise en charge réseau** si vous souhaitez avoir accès à Internet.
4. Cliquez sur **Entrée** et patientez pendant que Windows se charge en mode sans échec.
5. Ce processus se termine avec un message de confirmation. Cliquez sur **OK** pour valider.
6. Pour démarrer Windows normalement, il suffit de redémarrer le système.

GÉRER VOTRE SÉCURITÉ

14. PROTECTION ANTIVIRUS

Bitdefender protège votre ordinateur contre tous les types de logiciels malveillants (virus, chevaux de Troie, spywares, rootkits, etc.). La protection offerte par Bitdefender est divisée en deux catégories:

- Analyse à l'accès - empêche les nouvelles menaces d'infecter votre système. Bitdefender analysera par exemple un document Word quand vous l'ouvrez, et les e-mails lors de leur réception.

  L'analyse à l'accès assure une protection en temps réel contre les malwares, et constitue un composant essentiel de tout programme de sécurité informatique.

  Important
  Pour empêcher l'infection de votre ordinateur par des virus, maintenez l'**analyse à l'accès** activée.

- Analyse à la demande - permet de détecter et de supprimer les codes malveillants déjà présents dans le système. C'est l'analyse classique antivirus déclenchée par l'utilisateur – vous choisissez le lecteur, dossier ou fichier que Bitdefender doit analyser Bitdefender le fait – à la demande.

Bitdefender analyse automatiquement tout support amovible connecté à l'ordinateur afin de s'assurer que son accès ne pose pas de problème de sécurité. Pour plus d'informations, reportez-vous à « *Analyse automatique de supports amovibles* » (p. 93).

Les utilisateurs avancés peuvent configurer des exceptions d'analyse s'ils ne souhaitent pas que certains fichiers ou types de fichiers soient analysés. Pour plus d'informations, reportez-vous à « *Configurer des exceptions d'analyse* » (p. 95).

Lorsqu'il détecte un virus ou un autre malware, Bitdefender tente automatiquement de supprimer le code du malware du fichier infecté et de reconstruire le fichier d'origine. Cette opération est appelée désinfection. Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 98).

Si votre ordinateur a été infecté par des malwares, veuillez consulter « *Suppression des malwares de votre système* » (p. 152). Pour vous aider à supprimer les malwares qui ne peuvent pas l'être à partir du système

d'exploitation Windows, Bitdefender vous fournit le Mode de secours. Il s'agit d'un environnement de confiance, spécialement conçu pour la suppression de malwares, qui vous permet de faire redémarrer votre ordinateur indépendamment de Windows. Lorsque l'ordinateur s'exécute en Mode de Secours, les malwares Windows sont inactifs, ce qui rend leur suppression facile.

Pour vous protéger contre les applications malveillantes inconnues, Bitdefender utilise Active Threat Control, une technologie heuristique avancée, qui surveille en permanence les applications en cours d'exécution sur votre système. Active Threat Control bloque automatiquement les applications ayant un comportement similaire à celui des malwares afin de les empêcher d'endommager votre ordinateur. Des applications légitimes sont parfois bloquées. Vous pouvez dans ce cas configurer Active Threat Control afin qu'il ne bloque plus ces applications en créant des règles d'exclusion. Pour en savoir plus, consultez « *Active Threat Control* » (p. 99).

14.1. Analyse à l'accès (protection en temps réel)

Bitdefender fournit une protection continue, en temps réel, contre une large gamme de malwares en analysant tous les fichiers et e-mails auxquels vous accédez.

Le réglage par défaut de la protection en temps réel assure un bon niveau de protection contre les malwares, avec un impact minimal sur les performances système. Vous pouvez facilement modifier les paramètres de la protection en temps réel selon vos besoins en choisissant un des niveaux de protection prédéfinis. Si vous êtes un utilisateur avancé, vous pouvez également configurer les paramètres d'analyse en détail en créant un niveau de protection personnalisé.

14.1.1. Activer ou désactiver la protection en temps réel

Pour activer ou désactiver la protection en temps réel contre les malwares, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus**, puis sélectionnez l'onglet **Résident**

4. Cliquez sur le bouton pour activer ou désactiver l'analyse à l'accès.
5. Si vous tentez de désactiver la protection en temps réel, une fenêtre d'avertissement apparaît. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactivez la protection en temps- réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système. La protection en temps réel sera automatiquement activée lorsque la durée sélectionnée expirera.

> **Avertissement**
> Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la protection en temps réel pendant le moins de temps possible. Si la protection en temps réel est désactivée, vous ne serez pas protégé contre les menaces de codes malveillants.

14.1.2. Régler le niveau de protection en temps réel

Le niveau de protection en temps réel détermine les paramètres d'analyse pour la protection en temps réel. Vous pouvez facilement modifier les paramètres de la protection en temps réel selon vos besoins en choisissant un des niveaux de protection prédéfinis.

Pour régler le niveau de protection en temps réel, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus**, puis sélectionnez l'onglet **Résident**
4. Déplacez le curseur sur l'échelle pour choisir le niveau de protection souhaité. Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.

14.1.3. Configurer les paramètres de protection en temps réel

Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Bitdefender. Vous pouvez configurer les paramètres de protection en temps réel en détail en créant un niveau de protection personnalisé.

Pour configurer les paramètres de la protection en temps réel, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus**, puis sélectionnez l'onglet **Résident**
4. Cliquez sur **Personnaliser**.
5. Configurez les paramètres d'analyse selon vos besoins.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiarisé avec certains des termes, consultez le glossaire. Vous pouvez également rechercher des informations sur Internet.
- **Options d'analyse à l'accès des fichiers.** Vous pouvez régler Bitdefender pour analyser tous les types de fichiers auxquels vous accédez ou uniquement les applications (fichiers programmes). L'analyse de tous les fichiers accédés offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour obtenir de meilleures performances du système.

  Par défaut, les dossiers locaux et les partages réseau sont sujets à l'analyse à l'accès. Pour de meilleures performances du système, vous pouvez exclure certains emplacements du réseau de l'analyse à l'accès.

  Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Cette catégorie comprend les extensions de fichiers suivantes :

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam;

pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analyser le contenu compressé.** L'analyse des fichiers compressés est un processus lent et consommant beaucoup de ressources, qui n'est donc pas recommandé pour une protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée.

  Si vous décidez d'utiliser cette option, vous pouvez définir une limite de taille pour les archives à analyser à l'accès. Cochez la case correspondante et tapez la taille maximale des archives (en Mo).

- **Options d'analyse pour les trafics e-mails et HTTP.** Afin d'éviter que des malwares soient téléchargés sur votre ordinateur, Bitdefender analyse automatiquement les points d'entrée des malwares suivants :
  - courriels entrants et sortants
  - Trafic HTTP

  L'analyse du trafic Web peut ralentir un peu la navigation sur Internet, mais elle bloquera les malwares provenant d'Internet, y compris les téléchargements de type "drive-by".

  Bien que ce ne soit pas recommandé, vous pouvez désactiver l'analyse antivirus de messagerie ou web pour améliorer les performances du système. Si vous désactivez les options d'analyse correspondantes, les courriels et les fichiers reçus ou téléchargés sur Internet ne seront pas analysés, ce qui permettra aux fichiers infectés d'être enregistrés sur votre ordinateur. Il ne s'agit pas d'une menace critique, car la protection en temps réel bloquera le malware lorsque vous tenterez d'accéder (ouvrir, déplacer, copier ou exécuter) aux fichiers infectés.

- **Analyser les secteurs d'amorçage.** Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.

- **Analyser que les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Analyse des enregistreurs de frappe.** Sélectionnez cette option pour analyser la présence d'enregistreurs de frappe sur votre système. Les enregistreurs de frappe enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur Internet à une personne malveillante (un pirate informatique). Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.
- **Analyser au redémarrage.** Sélectionnez l'option d'analyse Early boot pour analyser votre système au démarrage dès que tous ses services critiques ont été téléchargés. La mission de cette fonctionnalité est d'améliorer la détection des virus au démarrage et redémarrage de votre système.

Actions appliquées à l'encontre des malwares détectés

Vous pouvez configurer les actions appliquées par la protection en temps réel.

Pour configurer les actions, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus**, puis sélectionnez l'onglet **Résident**
4. Cliquez sur **Personnaliser**.
5. Sélectionnez l'onglet **Actions**, et configurez les options d'analyse comme souhaité.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Les actions suivantes peuvent être appliquées par la protection en temps réel dans Bitdefender :

Action automatique

Bitdefender appliquera les actions recommandées en fonction du type de fichier détecté :

- **Fichier(s) infecté(s).** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender. Bitdefender tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer le fichier d'origine. Cette opération est appelée désinfection.

  Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 98).

  ! **Important**
  Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Fichier(s) suspect(s).** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter une infection potentielle.

  Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Archives contenant des fichiers infectés.**
  - Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.
  - Si une archive contient à la fois des fichiers infectés et des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Déplacer en quarantaine
Déplace les fichiers détectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 98).

Refuser l'accès
Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.

14.1.4. Restauration des paramètres par défaut

Le réglage par défaut de la protection en temps réel assure un bon niveau de protection contre les malwares, avec un impact minimal sur les performances système.

Pour restaurer les paramètres de protection en temps réel par défaut, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus**, puis sélectionnez l'onglet **Résident**
4. Cliquez sur **Par défaut**.

14.2. Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre PC sans virus. Cela s'effectue en protégeant votre ordinateur des nouveaux virus par l'analyse des courriels que vous recevez et des nouveaux fichiers que vous téléchargez ou copiez sur votre système.

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de Bitdefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de Bitdefender. Et il encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

L'analyse à la demande est fondée sur les tâches d'analyse. Les tâches d'analyse permettent de spécifier les options d'analyse et les objets à analyser. Vous pouvez analyser l'ordinateur quand vous le souhaitez en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Si vous souhaitez analyser certains emplacements

de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

14.2.1. Rechercher des malwares dans un fichier ou un dossier

Il est conseillé d'analyser les fichiers et les dossiers chaque fois que vous soupçonnez qu'ils peuvent être infectés. Faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser, pointez sur **Bitdefender** et sélectionnez **Analyser avec Bitdefender**. L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

14.2.2. Exécuter une Analyse Rapide

Quick Scan utilise l'analyse 'in-the-cloud' pour détecter les malwares présents sur votre système. La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

Pour effectuer une analyse rapide, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Analyse Rapide**.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

Vous pouvez également cliquer sur le bouton d'action **Analyse rapide** dans l'interface de Bitdefender.

14.2.3. Exécuter une analyse du système

La tâche d'analyse du système analyse l'ensemble de votre ordinateur en vue de détecter tous les types de logiciels malveillants menaçant sa sécurité : virus, logiciels-espions, publiciels, rootkits et autres.

Note
L'**analyse du système** effectue une analyse approfondie de l'ensemble du système, elle peut donc prendre un certain temps. Il est donc recommandé d'exécuter cette tâche lorsque vous n'utilisez pas votre ordinateur.

Avant d'exécuter une analyse du système, nous vous recommandons ceci :

- Vérifiez que Bitdefender dispose de signatures de malwares à jour. Analyser votre ordinateur en utilisant une base de données de signatures non à jour peut empêcher Bitdefender de détecter le nouveau malware identifié depuis la mise à jour précédente. Pour plus d'informations, reportez-vous à « *Maintenir Bitdefender à jour* » (p. 44).
- Fermez tous les programmes ouverts.

Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée. Pour plus d'informations, reportez-vous à « *Configurer une analyse personnalisée* » (p. 85).

Pour exécuter une analyse du système, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Analyse du Système**.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

14.2.4. Configurer une analyse personnalisée

Pour configurer une analyse antimalware en détail et l'exécuter, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Gestion des analyses**.
4. Cliquez sur **Nouvelle tâche personnalisée**. Saisissez un nom pour l'analyse dans l'onglet **Standard** et sélectionnez les emplacements à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**. Une nouvelle fenêtre apparaît. Suivez ces étapes :
   a. Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour choisir le niveau d'analyse souhaité. Reportez-vous à la description à droite de l'échelle pour identifier le niveau d'analyse le plus adapté à vos besoins.

      Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Bitdefender. Pour configurer les options d'analyse en détail, cliquez sur **Personnaliser**. Vous trouverez des informations à leur sujet à la fin de la section.

   b. Vous pouvez aussi configurer ces options générales :
      - **Exécuter la tâche en priorité basse .** Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.
      - **Réduire l'assistant d'analyse dans la zone de notification .** Réduit la fenêtre d'analyse dans la zone de notification. Double-cliquez sur l'icône de Bitdefender pour l'ouvrir.
      - Spécifiez l'action à mener si aucune menace n'a été trouvée.

   c. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
6. Si vous souhaitez paramétrer une heure pour votre tâche d'analyse, utilisez le bouton **Horaires** Sélectionnez l'une des options correspondantes pour définir une planification :
   - Au démarrage du système
   - Une fois
   - Périodiquement

7. Cliquez sur **Démarrer l'analyse** et suivez l'Assistant d'analyse antivirus pour terminer l'analyse. En fonction des emplacements à analyser, l'analyse peut prendre quelque temps. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
8. Si vous le souhaitez, vous pouvez relancer rapidement une analyse personnalisée en cliquant sur le bouton correspondant dans la liste.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiarisé avec certains des termes, consultez le glossaire. Vous pouvez également rechercher des informations sur Internet.
- **Analyser les fichiers.** Vous pouvez régler Bitdefender pour analyser tous les types de fichiers ou uniquement les applications (fichiers programmes). L'analyse de tous les fichiers fournit la meilleure protection, alors que l'analyse des applications uniquement peut être utilisée pour effectuer une analyse plus rapide.

  Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Cette catégorie comprend les extensions de fichiers suivantes : 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Options d'analyse pour les archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette

option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.

> **Note**
> L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

- **Analyser les secteurs d'amorçage.** Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
- **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.
- **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.
- **Analyser les témoins.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur votre ordinateur.
- **Analyser que les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Ignorer les enregistreurs de frappe commerciaux.** Sélectionnez cette option si vous avez installé et utilisez un keylogger commercial sur votre ordinateur. Les keyloggers commerciaux sont des logiciels de surveillance légitimes dont la fonction principale consiste à enregistrer tout ce qui est tapé au clavier.
- **Rechercher les rootkits.** Sélectionnez cette option pour rechercher des rootkits et des objets cachés à l'aide de ce logiciel.

14.2.5. Assistant d'analyse antivirus

À chaque fois que vous lancerez une analyse à la demande (par exemple en faisant un clic droit sur un dossier, en pointant sur Bitdefender et en

sélectionnant **Analyser avec Bitdefender**), l'assistant de l'analyse antivirus Bitdefender s'affichera. Suivez l'assistant pour terminer le processus d'analyse.

Note

Si l'assistant d'analyse ne s'affiche pas, il est possible que l'analyse soit paramétrée pour s'exécuter invisiblement, en tâche de fond. Recherchez l'icône de l'avancement de l'analyse dans la zone de notification. Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Étape 1 - Effectuer l'analyse

Bitdefender commence à analyser les objets sélectionnés. Vous pouvez voir des informations en temps réel sur l'état et les statistiques de l'analyse (y compris le temps écoulé, une estimation du temps restant et le nombre de menaces détectées).

Patientez jusqu'à ce que Bitdefender ait terminé l'analyse. L'analyse peut durer un certain temps, suivant sa complexité.

Arrêt ou pause de l'analyse. Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Arrêter**. Vous vous retrouverez alors à la dernière étape de l'assistant. Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

Archives protégées par mot de passe. Lorsqu'une archive protégée par mot de passe est détectée, en fonction des paramètres de l'analyse, on peut vous demander d'indiquer son mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe. Voici les options proposées :

- **Mot de passe.** Si vous souhaitez que Bitdefender analyse l'archive, sélectionnez cette option et entrez le mot de passe. Si vous ne connaissez pas le mot de passe, choisissez l'une des autres options.
- **Ne pas demander le mot de passe et ne pas analyser cet objet.** Sélectionnez cette option pour ne pas analyser cette archive.
- **Ne pas analyser les éléments protégés par mot de passe.** Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe. Bitdefender ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

Sélectionnez l'option souhaitée et cliquez sur **OK** pour poursuivre l'analyse.

Étape 2 - Sélectionner des actions

À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

Note

Si vous lancez une analyse rapide ou une analyse complète du système, Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés pendant l'analyse. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

Les objets infectés sont affichés dans des groupes, basés sur les malwares les ayant infectés. Cliquez sur le lien correspondant à une menace pour obtenir plus d'informations sur les éléments infectés.

Vous pouvez sélectionner une action globale à mener pour l'ensemble des problèmes de sécurité ou sélectionner des actions spécifiques pour chaque groupe de problèmes. Une ou plusieurs des options qui suivent peuvent apparaître dans le menu :

Action automatique

Bitdefender appliquera les actions recommandées en fonction du type de fichier détecté :

- **Fichier(s) infecté(s).** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender. Bitdefender tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer le fichier d'origine. Cette opération est appelée désinfection.

  Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 98).

Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Fichier(s) suspect(s).** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter une infection potentielle.

  Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Archives contenant des fichiers infectés.**
  - Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.
  - Si une archive contient à la fois des fichiers infectés et des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Supprimer
Supprime du disque les fichiers détectés.

Si des fichiers infectés sont contenus dans une archive avec des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés et de reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Ignorer
Aucune action ne sera menée sur les fichiers détectés. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.

Cliquez sur **Continuer** pour appliquer les actions spécifiées.

Étape 3 - Récapitulatif

Une fois que les problèmes de sécurité auront été corrigés par Bitdefender, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre. Si vous souhaitez consulter des informations complètes sur le processus d'analyse, cliquez sur **Afficher journal** pour afficher le journal d'analyse.

Cliquez sur **Fermer** pour fermer la fenêtre.

Important

Dans la plupart des cas, Bitdefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte. Il y a toutefois des problèmes qui ne peuvent pas être résolus automatiquement. Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation. Pour plus d'informations et d'instructions sur la méthode permettant de supprimer des malwares manuellement, reportez-vous à « *Suppression des malwares de votre système* » (p. 152).

14.2.6. Consulter les journaux d'analyse

À chaque fois qu'une analyse est effectuée, un journal d'analyse est créé et Bitdefender enregistre les problèmes détectés dans la fenêtre Antivirus. Le rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises à l'encontre de ces menaces.

Vous pouvez ouvrir le journal d'analyse directement à partir de l'assistant d'analyse, une fois l'analyse terminée, en cliquant sur **Afficher le Journal**.

Pour consulter ultérieurement un journal d'analyse ou toute infection détectée, procédez comme suit :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Événements** dans le menu déroulant.
2. Dans la fenêtre **Événements**, sélectionnez **Antivirus** dans le menu déroulant correspondant.

   Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.
3. Dans la liste des événements, vous pouvez consulter les analyses ayant été réalisées récemment. Cliquez sur un événement pour afficher des informations à son sujet.
4. Pour ouvrir le journal d'analyse, cliquez sur **Journal**. Si vous souhaitez exécuter la même analyse encore une fois, cliquez sur le bouton **Ré analyser**

14.3. Analyse automatique de supports amovibles

Bitdefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre ordinateur et l'analyse en tâche de fond. Ceci est recommandé afin d'empêcher que des virus ou autres malwares n'infectent votre ordinateur.

Les périphériques détectés appartiennent à l'une des catégories suivantes :

- CD ou DVD
- Des supports USB, tels que des clés flash et des disques durs externes
- disques réseau (distants) connectés

Vous pouvez configurer l'analyse automatique séparément pour chaque catégorie de périphériques de stockage. L'analyse automatique des disques réseau connectés est désactivée par défaut.

14.3.1. Comment cela fonctionne-t-il ?

Lorsqu'il détecte un périphérique de stockage amovible, Bitdefender commence à l'analyser en tâche de fond à la recherche de malwares (à condition que l'analyse automatique soit activée pour ce type de périphérique). Une icône d'analyse de Bitdefender apparaîtra dans la zone de notification. Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Si la fonction Autopilot est activée, vous n'aurez pas à vous soucier de l'analyse. L'analyse sera seulement enregistrée et des informations à son sujet seront disponibles dans la fenêtre Événements.

Si Autopilot est désactivé :

1. Vous serez averti via une fenêtre contextuelle qu'un nouveau périphérique a été détecté et est en cours d'analyse.
2. Dans la plupart des cas, Bitdefender supprime automatiquement les malwares détectés ou isole les fichiers infectés en quarantaine. S'il y a des menaces non résolues après l'analyse, on vous demandera de choisir les actions à appliquer.

> **Note**
> Veuillez prendre en compte le fait qu'aucune mesure ne sera prise à l'encontre des fichiers infectés ou suspects détectés sur des CD ou DVD.

De plus, aucune action ne sera appliquée à l'encontre des fichiers suspects détectés sur des lecteurs mappés du réseau si vous ne disposez pas des privilèges appropriés.

3. Lorsque l'analyse est terminée, la fenêtre des résultats de l'analyse s'affiche afin de vous informer si vous pouvez accéder aux fichiers en toute sécurité sur le support amovible.

Ces informations peuvent vous être utiles :

- Soyez prudent lorsque vous utilisez un CD ou DVD infecté par des malwares, car ces malwares ne peuvent pas être supprimés du disque (le support est en lecture seule). Vérifiez que la protection en temps réel est activée pour empêcher la diffusion de malwares sur votre système. Il est recommandé de copier toutes les données essentielles du disque sur le système avant de se séparer du disque.
- Bitdefender n'est parfois pas en mesure de supprimer les malwares de certains fichiers en raison de contraintes légales ou techniques. C'est le cas par exemple des fichiers archivés à l'aide d'une technologie propriétaire (car l'archive ne peut pas être recréée correctement).

  Pour savoir comment traiter les malwares, reportez-vous à « *Suppression des malwares de votre système* » (p. 152).

14.3.2. Gérer l'analyse des supports amovibles

Pour gérer l'analyse automatique de supports amovibles, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus** puis sélectionnez l'onglet **Exclusions**.

Pour une meilleure protection, nous vous recommandons d'activer l'analyse automatique de tous les types de périphériques de stockage amovibles.

Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible. Si des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (supprimer le code malveillant) ou de les placer en quarantaine. Si ces actions échouent, l'assistant d'analyse antivirus vous

permettra de spécifier d'autres actions à appliquer aux fichiers infectés. Les options d'analyse sont standard et vous ne pouvez pas les modifier.

14.4. Configurer des exceptions d'analyse

Bitdefender vous permet d'exclure de l'analyse certains fichiers, dossiers ou extensions de fichiers. Cette fonctionnalité est conçue pour éviter d'interférer avec votre travail et peut également contribuer à améliorer les performances du système. Les exclusions doivent être employées par des utilisateurs ayant un niveau avancé en informatique ou, sinon, selon les recommandations d'un représentant de Bitdefender.

Vous pouvez configurer des exclusions à appliquer uniquement à l'analyse à l'accès ou à la demande, ou aux deux. Les objets exclus d'une analyse à l'accès ne sont pas analysés, que ce soit vous-même ou une application qui y accédiez.

Note

Les exclusions ne sont PAS appliquées pour l'analyse contextuelle. L'analyse contextuelle est un type d'analyse à la demande : vous faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser et vous sélectionnez **Analyser avec Bitdefender**.

14.4.1. Exclure de l'analyse des fichiers ou des dossiers

Pour exclure de l'analyse des fichiers ou des dossiers, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Activez les exceptions d'analyse pour les fichiers à l'aide du bouton correspondant.
6. Cliquez sur le lien **Fichiers et dossiers exclus**. La fenêtre qui s'affiche vous permet de gérer les fichiers et dossiers exclus de l'analyse.
7. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.

b. Cliquez sur **Parcourir**, sélectionnez le fichier ou le dossier à exclure de l'analyse, puis cliquez sur **OK**. Vous pouvez également taper (ou copier-coller) le chemin vers le fichier ou le dossier dans le champ de saisie.

c. Par défaut, le fichier ou dossier sélectionné est exclu à la fois de l'analyse à l'accès et à la demande. Pour modifier les conditions d'application de l'exclusion, sélectionnez l'une des autres options.

d. Cliquez sur **Ajouter**.

8. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

14.4.2. Exclure de l'analyse des extensions de fichiers

Lorsque vous excluez de l'analyse une extension de fichier, Bitdefender n'analysera plus les fichiers avec cette extension, quel que soit leur emplacement sur votre ordinateur. L'exclusion s'applique également aux fichiers de supports amovibles tels que les CD, les DVD, les périphériques de stockage USB ou les disques réseau.

Important
Soyez prudent lorsque vous excluez de l'analyse des extensions car celles-ci peuvent rendre votre ordinateur vulnérable aux malwares.

Pour exclure de l'analyse des extensions de fichiers, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Activez les exceptions d'analyse pour les fichiers à l'aide du bouton correspondant.
6. Cliquez sur le lien **Extensions exclues**. La fenêtre qui s'affiche vous permet de gérer les extensions de fichiers exclues de l'analyse.
7. Ajoutez des exclusions en suivant ces étapes :

   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.

b. Indiquez les extensions que vous ne souhaitez pas analyser, en les séparant par des points-virgules (;). Voici un exemple :

txt;avi;jpg

c. Par défaut, tous les fichiers ayant les extensions indiquées sont exclus à la fois de l'analyse à l'accès et à la demande. Pour modifier les conditions d'application de l'exclusion, sélectionnez l'une des autres options.

d. Cliquez sur **Ajouter**.

8. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

14.4.3. Gérer les exceptions d'analyse

Si les exceptions d'analyse configurées ne sont plus nécessaires, il est recommandé de les supprimer ou de les désactiver.

Pour gérer les exceptions d'analyse, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus** puis sélectionnez l'onglet **Exclusions**. Utilisez les options de la section **Fichiers et dossiers** pour gérer les exceptions d'analyse.
4. Pour supprimer ou éditer des exceptions d'analyse, cliquez sur l'un des liens. Procédez comme suit :
   - Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Supprimer**.
   - Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la et cliquez sur le bouton **Modifier**.) Une nouvelle fenêtre apparaît vous permettant de modifier l'extension ou le chemin à exclure et le type d'analyse dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **Modifier**.
5. Pour désactiver les exceptions d'analyse, cliquez sur le bouton correspondant.

14.5. Gérer les fichiers en quarantaine

Bitdefender isole les fichiers infectés par des malwares qu'il ne peut pas désinfecter et les fichiers suspects dans une zone sécurisée nommée quarantaine. Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté, ni être lu.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

Bitdefender analyse également les fichiers en quarantaine après chaque mise à jour de signatures de malware. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Pour consulter et gérer les fichiers de la quarantaine, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus** puis sélectionnez l'onglet **Quarantaine**.
4. Les fichiers en quarantaine sont gérés automatiquement par Bitdefender en fonction des paramètres de quarantaine par défaut. Bien que ce ne soit pas recommandé, vous pouvez régler les paramètres de quarantaine en fonction de vos préférences.

   Analyser la quarantaine après la mise à jour des définitions de virus
   Maintenez cette option activée pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour des définitions de virus. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

   Envoyer les fichiers suspects de la quarantaine pour analyse
   Maintenez cette option activée pour envoyer automatiquement les fichiers de la quarantaine aux laboratoires de Bitdefender. Les échantillons seront analysés par les spécialistes malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

Supprimer le contenu datant de plus de {30} jours
Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés. Si vous souhaitez modifier ce délai, entrez une nouvelle valeur dans le champ correspondant. Pour désactiver la suppression automatique des fichiers de la quarantaine selon la date, tapez 0.

5. Pour supprimer un fichier en quarantaine, sélectionnez-le, puis cliquez sur le bouton **Supprimer**. Si vous souhaitez restaurer un fichier mis en quarantaine à son emplacement d'origine, sélectionnez-le, puis cliquez sur **Restaurer**.

14.6. Active Threat Control

Bitdefender Active Threat Control est une technologie de détection proactive innovante qui utilise des méthodes heuristiques de pointe pour détecter de nouvelles menaces potentielles en temps réel.

Active Threat Control surveille en permanence les applications en cours d'exécution sur l'ordinateur, à la recherche d'actions ressemblant à celles des malwares. Chacune de ces actions est notée et un score global est calculé pour chaque processus. Lorsque la note globale d'un processus atteint un seuil donné, le processus est considéré comme malveillant et est automatiquement bloqué.

Si la fonction Autopilot est désactivée, vous serez averti via une fenêtre contextuelle sur l'application bloquée. Sinon, l'application sera bloquée sans notification. Vous pouvez vérifier les applications détectées par Active Threat Control dans la fenêtre Événements.

14.6.1. Vérifier des applications détectées

Pour contrôler les applications détectées par Active Threat Control, procédez comme suit :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Événements** dans le menu déroulant.
2. Dans la fenêtre **Événements**, sélectionnez **Antivirus** dans le menu déroulant correspondant.
3. Cliquez sur un événement pour afficher des informations à son sujet.

4. Si vous considérez que l'application est fiable, vous pouvez configurer Active Threat Control afin qu'il ne la bloque plus en cliquant sur **Autoriser et surveiller**. Active Threat Control continuera à surveiller les applications exclues. Si les activités suspectes d'une application exclue sont détectées, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

14.6.2. Activer ou désactiver Active Threat Control

Pour activer ou désactiver Active Threat Control, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur le bouton pour activer ou désactiver Active Threat Control.

14.6.3. Régler la protection Active Threat Control

Si vous remarquez qu'Active Threat Control détecte souvent des applications légitimes, optez pour un niveau de protection moins strict.

Pour ajuster la protection Active Threat Control, faites monter ou descendre le curseur sur l'échelle afin de déterminer le niveau de protection désiré.

Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.

> **Note**
> Si vous élevez le niveau de protection, Active Threat Control aura besoin de moins de signes de comportements similaires à ceux des malwares pour signaler un processus. Cela conduira au signalement d'un nombre plus important d'applications et, en même temps, à un risque plus élevé de faux positifs (des applications saines détectées comme étant malveillantes).

14.6.4. Gérer les processus exclus

Vous pouvez configurer des règles d'exceptions pour les applications de confiance afin qu'Active Threat Control ne les bloque pas si elles effectuent des actions ressemblant à celles de malwares. Active Threat Control

continuera à surveiller les applications exclues. Si les activités suspectes d'une application exclue sont détectées, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

Pour gérer les exclusions de processus Active Threat Control, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus** puis sélectionnez l'onglet **Exclusions**.
4. Cliquez sur le lien **Processus exclus**. Dans la fenêtre qui apparaît, vous pouvez gérer les exclusions de processus Active Threat Control.
5. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Cliquez sur **Parcourir**, sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.
   c. Gardez l'option **Autoriser** sélectionnée pour empêcher Active Threat Control de bloquer l'application.
   d. Cliquez sur **Ajouter**.
6. Pour supprimer ou éditer des exclusions, procédez comme suit :
   - Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **Effacer**.
   - Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la) et cliquez sur le bouton **Modifier**. Effectuez les modifications nécessaires, puis cliquez sur **Modifier**.
7. Enregistrer les modifications et fermer la fenêtre.

15. PROTECTION WEB

La protection Web de Bitdefender vous garantit une navigation sur Internet en toute sécurité en vous signalant les pages web présentant un risque de phishing.

Bitdefender fournit une protection web en temps réel pour :

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Pour configurer les paramètres de la protection Web, les étapes sont les suivantes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Protection Web**.

Cliquez sur les boutons pour activer ou désactiver :

- Conseiller de recherche, un composant qui évalue les résultats de vos requêtes sur les moteurs de recherche et les liens postés sur les sites Web de réseaux sociaux en plaçant une icône à côté de chaque résultat :

  Nous vous déconseillons de consulter cette page Web.

  Cette page Web peut contenir du contenu dangereux. Soyez prudent si vous décidez de le consulter.

  Cette page peut être consultée en toute sécurité.

  Conseiller de recherche évalue les résultats de recherche des moteurs de recherche Web suivants :
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Conseiller de recherche évalue les liens postés sur les sites de réseaux sociaux suivants :
  - Facebook

- Twitter
- Analyse du trafic web SSL.

  Des attaques plus sophistiquées peuvent utiliser le trafic Web sécurisé pour induire en erreur leurs victimes. Nous vous recommandons donc d'activer l'analyse SSL.
- Protection contre les escroqueries.
- Protection contre l'hameçonnage.

Vous pouvez créer une liste de sites Web qui ne seront pas analysés par les moteurs antimalware, antiphishing et antifraude de Bitdefender. La liste ne doit contenir que des sites Web de confiance. Par exemple, ajoutez les sites Web sur lesquels vous avez l'habitude de faire vos achats en ligne.

Pour configurer et administrer les sites web à l'aide de la protection web fournie par Bitdefender, cliquez sur le lien **Liste blanche**. Une nouvelle fenêtre apparaît.

Pour ajouter un site à la liste blanche, entrez son adresse dans le champ correspond et cliquez sur **Ajouter**.

Pour supprimer un site Web de la liste, sélectionnez-le dans la liste et cliquez sur le lien **Supprimer**.

Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

15.1. Alertes Bitdefender dans le navigateur

Lorsque vous essayez de consulter un site Web considéré comme non sûr, ce site web est bloqué et une page d'avertissement s'affiche dans votre navigateur.

La page contient des informations telles que l'URL du site web et la menace détectée.

Vous devez décider quoi faire ensuite. Voici les options proposées :

- Quittez la page Web en cliquant sur **Retour en toute sécurité**.
- Désactivez le blocage des pages d'hameçonnage en cliquant sur **Désactiver le filtre anti-hameçonnage**.
- Désactivez le blocage des pages contenant des malwares en cliquant sur **Désactiver le filtre antimalware**.

- Ajoutez la page à la liste blanche anti-hameçonnage en cliquant sur **Ajouter à la liste blanche**. Cette page ne sera plus analysée par les moteurs Antiphishing de Bitdefender.
- Pour vous rendre sur le site Web, malgré l'avertissement, cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**.

16. PROTECTION DES DONNÉES

16.1. Supprimer définitivement des fichiers

Lorsque vous supprimez un fichier, vous ne pouvez plus y accéder par le chemin habituel. Toutefois, ce fichier continue d'être stocké sur le disque dur jusqu'à ce qu'il soit remplacé lors de la copie de nouveaux fichiers.

Le Destructeur de Fichiers Bitdefender vous aidera à supprimer définitivement des données en les supprimant physiquement de votre disque dur.

Vous pouvez détruire rapidement des fichiers ou dossiers de votre ordinateur à l'aide du menu contextuel de Windows, en procédant comme suit :

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement.
2. Sélectionnez **Bitdefender** > **Destructeur de fichiers** dans le menu contextuel qui apparaît.
3. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour lancer l'assistant du destructeur de fichiers.
4. Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
5. Les résultats sont affichés. Cliquez sur **Fermer** pour quitter l'assistant.

Vous pouvez également détruire des fichiers à partir de l'interface de Bitdefender.

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Sous le module **Données**, sélectionnez **Destructeur de fichiers**.
4. Suivez l'assistant du destructeur de fichiers :
   a. **Ajouter**

      Ajoutez les fichiers ou les dossiers que vous souhaitez supprimer définitivement.

   b. Cliquez sur **Suivant** et confirmez que vous souhaitez continuer le processus.

      Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.

c. **Résultats**

Les résultats sont affichés. Cliquez sur **Fermer** pour quitter l'assistant.

17. VULNÉRABILITÉ

Une étape importante permettant de préserver votre ordinateur contre les actions malveillantes et les menaces est de maintenir à jour votre système d'exploitation et vos principales applications. Vous devriez également envisager de désactiver les paramètres Windows qui rendent le système plus vulnérable aux malwares. De plus, afin de prévenir tout accès physique non autorisé à votre ordinateur, il est recommandé d'utiliser des mots de passe complexes (qui ne peuvent pas être devinés trop facilement) pour chaque compte utilisateur Windows.

Bitdefender recherche automatiquement les vulnérabilités de votre système et vous les signale. Les vulnérabilités du Système peuvent être :

- la présence sur votre ordinateur d'applications non à jour
- des mises à jour Windows manquantes
- des mots de passe non sécurisés de comptes utilisateurs Windows

Bitdefender fournit deux manières simples de corriger les vulnérabilités de votre système :

- Vous pouvez rechercher des vulnérabilités sur votre système et les corriger pas à pas à l'aide de l'option **Analyse de Vulnérabilité**.
- La surveillance des vulnérabilités automatique vous permet de vérifier et de corriger les vulnérabilités détectées dans la fenêtre Événements.

Nous vous recommandons de vérifier et de corriger les vulnérabilités du système toutes les semaines, ou une fois toutes les deux semaines.

17.1. Analyser votre système à la recherche de vulnérabilités

Pour corriger les vulnérabilités du système à l'aide de l'option Analyse de Vulnérabilité, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Vulnérabilité**, sélectionnez **Analyse de Vulnérabilité**.

4. Patientez jusqu'à ce que Bitdefender ait analysé votre système à la recherche de vulnérabilités. Pour arrêter le processus d'analyse, cliquez sur le bouton **Ignorer** en haut de la fenêtre.

   Vous pouvez également cliquer sur le bouton d'action **Analyse vulnérabilité** dans l'interface de Bitdefender.

   - **Mises à jour critiques Windows**

     Cliquez sur **Afficher les détails** pour voir la liste des mises à jour Windows critiques qui ne sont pas installées sur votre ordinateur.

     Pour lancer l'installation des mises à jour sélectionnées, cliquez sur **Installer les mises à jour**. Veuillez noter que l'installation des mises à jour peut durer un certain temps et que certaines peuvent nécessiter un redémarrage du système. Si nécessaire, redémarrez le système dès que possible.

   - **Mises à jour d'applications**

     Si une application n'est pas à jour, cliquez sur le lien **Télécharger nouvelle version** pour télécharger la dernière version.

     Cliquez sur **Afficher les détails** pour voir des informations sur l'application ayant besoin d'être mise à jour.

   - **Mots de passe de comptes Windows vulnérables**

     Vous pouvez voir une liste des comptes utilisateur Windows configurés sur votre ordinateur ainsi que le niveau de protection que leur mot de passe respectif apportent.

     Cliquez sur **Changer mot de passe à la connexion** pour configurer un nouveau mot de passe pour votre système.

     Cliquez sur **Afficher les détails** pour modifier les mots de passe vulnérables. Vous pouvez choisir entre demander à l'utilisateur de modifier le mot de passe lors de sa prochaine connexion ou modifier le mot de passe par vous-même immédiatement. Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

L'angle supérieur droit de la fenêtre vous permet de filtrer les résultats en fonction de vos préférences.

17.2. Utiliser la surveillance des vulnérabilités automatique

Bitdefender analyse régulièrement votre système à la recherche de vulnérabilités, en tâche de fond, et enregistre les problèmes détectés dans la fenêtre Événements.

Pour vérifier et corriger les problèmes détectés, suivez ces étapes :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Événements** dans le menu déroulant.
2. Dans la fenêtre **Événements**, sélectionnez **Vulnérabilité** à partir de la liste Sélectionner événements.
3. Vous pouvez consulter des informations détaillées au sujet des vulnérabilités du système détectées. En fonction du problème, procédez comme suit pour corriger une vulnérabilité spécifique :
   - Si des mises à jour Windows sont disponibles, cliquez sur **Mettre à jour**.
   - Si la mise à jour Windows automatique est désactivée, cliquez sur **Activer**.
   - Si une application n'est pas à jour, cliquez sur **Mettre à jour maintenant** pour trouver un lien vers la page Web du fournisseur d'où vous pourrez installer la dernière version de l'application.
   - Si un compte utilisateur Windows a un mot de passe vulnérable, cliquez sur **Changer de mot de passe** pour obliger l'utilisateur à modifier son mot de passe lors de la prochaine connexion ou pour changer le mot de passe par vous-même. Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).
   - Si la fonctionnalité AutoRun de Windows est activée, cliquez sur **Corriger** pour la désactiver.

Pour configurer les paramètres de surveillance des vulnérabilités, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.

3. Cliquez sur le module **Vulnérabilité**.
4. Cliquez sur le bouton pour activer ou désactiver l'analyse de vulnérabilité.

> **Important**
> Pour être automatiquement averti(e) en cas de vulnérabilités du système ou des applications, veuillez garder l'option **Analyse de Vulnérabilité** activée.

5. Choisissez les vulnérabilités du système que vous souhaitez vérifier régulièrement à l'aide des boutons correspondants.

Mises à jour critiques Windows
Vérifiez que votre système d'exploitation Windows dispose des dernières mises à jour de sécurité critiques de Microsoft.

Mises à jour d'applications
Vérifiez que les applications installées sur votre système sont à jour. Des applications non à jour peuvent être exploitées par des logiciels malveillants, rendant votre PC vulnérable aux attaques extérieures.

Mots de passe vulnérables
Vérifiez si les mots de passe des comptes Windows configurés sur le système sont faciles à deviner. Choisir des mots de passe difficiles à deviner rend difficile l'introduction dans votre système de pirates informatiques. Un mot de passe sécurisé est constitué d'une association de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

Exécution automatique des supports amovibles
Vérifiez l'état de la fonctionnalité AutoRun de Windows. Cette fonctionnalité permet aux applications d'être automatiquement lancées à partir de CD, DVD, lecteurs USB ou autres périphériques externes.

Certains types de malwares utilisent la fonction AutoRun pour passer automatiquement des supports amovibles vers le PC. Nous vous recommandons donc de désactiver cette fonctionnalité Windows.

> **Note**
> Si vous désactivez la surveillance d'une certaine vulnérabilité, les problèmes qui y sont liés ne seront plus enregistrés dans la fenêtre Événements.

18. PROTECTION RANSOMWARE

Un ransomware est un code malveillant qui attaque les systèmes vulnérables en bloquant l'accès et en demandant de l'argent pour redonner le contrôle de son système à l'utilisateur. Ces softwares malveillants sont intelligents, car ils envoient de faux messages pour faire peur à l'utilisateur, le pressant à payer.

L'infection peut se répandre par des e-mails spams, en téléchargeant des pièces jointes, en visitant des sites web corrompus ou en téléchargeant des applications malveillantes à l'insu de l'utilisateur.

Les ransowmares peuvent se comporter des façons suivants, pour empêcher l'utilisateur d'accéder à son système :

- Ils chiffrent les fichiers sensibles et personnels sans laisser de possibilité de décryptage jusqu'à ce qu'une rançon soit payée par la victime.
- Ils verrouillent l'écran de l'ordinateur et affichent un message demandant de l'argent. Dans ce cas, aucun fichier n'est chiffré, mais l'utilisateur est simplement forcé à payer.
- Ils bloquent le lancement des applications.

Grâce aux dernières technologies, la Protection Bitdefender contre les ransomwares garantit l'intégrité du système en protégeant les zones critiques du système contre les dommages, sans répercussions sur le système. Vous pouvez également souhaiter protéger vos fichiers personnels tels que les documents, photos, films, ou les fichiers que vous conservez dans le cloud.

18.1. Activer ou désactiver la protection contre les ransomwares

Pour désactiver le protection contre les ransomwares, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur **Protection contre les ransomwares**.

4. Cliquez sur le bouton pour activer ou désactiver la **Protection contre les ransomwares**..

Chaque fois qu'une application tentera d'accéder à un fichier protégé, un pop-up Bitdefender s'affichera. Vous pouvez autoriser ou refuser l'accès.

18.2. Protégez vos fichiers personnels contre les attaques de ransomwares

Si vous souhaitez mettre à l'abri des fichiers personnels, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Protection contre les ransomwares** , puis cliquez sur le bouton **Ajouter**.
4. Allez dans le dossier que vous souhaitez protéger, puis cliquez sur **OK** pour ajouter le dossier sélectionné à l'environnement de protection.

Par défaut, les dossiers Mes Documents, Mes images, Documents publiques, et Images publiques sont protégés contre les attaques de malwares. Les données personnelles stockées dans des services d'hébergement de fichiers en ligne tels que Box, Dropbox, Google Drive et OneDrive sont également inclus dans l'environnement de protection, à condition que leurs applications soient installées sur le système.

Note
Les dossiers personnalisés ne peuvent être protégés que pour les utilisateurs actuels. Les fichiers systèmes et d'applications ne peuvent pas être ajoutés aux exceptions.

18.3. Configuration des applications fiables

Désactiver la protection contre les ransomwares pour certaines applications spécifiques, mais seulement celles que vous jugez fiables peuvent être ajoutées à la liste.

Pour ajouter des applications fiables aux exclusions, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Dans le module **Protection contre les ransomwares**, sélectionnez **Applications fiables**.
4. Cliquez sur **Ajouter** pour sélectionner les applications que vous voulez protéger.
5. Cliquez sur **OK** pour ajouter l'application sélectionnée à l'environnement de protection.

18.4. Configuration des applications bloquées

Parmi les applications que vous avez ajoutées sur votre ordinateur, certaines souhaitent accéder à vos fichiers personnels.

Pour limiter ces applications, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Dans le module **Protection contre les ransomwares**, sélectionnez **Applications bloquées**.
4. Cliquez sur **Ajouter** pour sélectionner les applications que vous voulez limiter.
5. Cliquez sur **OK** pour ajouter l'application sélectionnée à la liste de restriction.

18.5. Protection au démarrage

Il est connu que plusieurs applications malwares sont configurées pour s'exécuter au démarrage, ce qui peut sérieusement abîmer une machine. La protection au démarrage Bitdefender analyse tous les zones systèmes critiques avant que tous les fichiers ne soient chargés, sans impact sur le système. Dans le même temps, la protection est assurée contre certaines attaques se basant sur l'exécution de code au niveau de la pile ou du tas, les injections de code ou les hooks à l'intérieur de certaines bibliothèques logicielles dynamiques.

Pour désactiver la protection du démarrage, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur **Protection contre les ransomwares**.
4. Cliquez sur le bouton pour activer ou désactiver la **Protection du démarrage**.

19. LA SÉCURITÉ SAFEPAY POUR LES TRANSACTIONS EN LIGNE

L'ordinateur devient rapidement indispensable pour les achats et les transactions bancaires. Payer vos factures, virer de l'argent, et acheter quasiment tout ce que vous pouvez imaginer n'a jamais été aussi rapide ni aussi simple.

Cela implique l'envoi sur Internet d'informations personnelles, de données de comptes et de cartes bancaires, de mots de passe et d'autres types d'informations confidentielles, en d'autres termes exactement le type d'informations qui intéressent tout particulièrement les cybercriminels. Les pirates ne sont pas avares d'efforts lorsqu'il s'agit de voler ces informations, et vous n'êtes donc jamais trop prudent pour ce qui est de la sécurisation des transactions en ligne.

Bitdefender Safepay™ est avant tout un navigateur protégé, un environnement sécurisé conçu pour assurer la confidentialité et la sécurité des opérations bancaires, achats en ligne et autres types de transactions sur Internet.

Pour une meilleure protection de la vie privée, Bitdefender Password Manager est intégré à Bitdefender Safepay™ afin de protéger vos identifiants lorsque vous essayez d'accéder à des espaces en ligne confidentiels. Pour plus d'informations, reportez-vous à « *Protection Password Manager de vos identifiants* » (p. 120).

Bitdefender Safepay™ dispose des fonctions suivantes :

- Il bloque l'accès à votre bureau et toute tentative de prise d'instantanés de votre écran.
- Il protège vos mots de passe confidentiels lorsque vous naviguez sur Internet avec Password Manager.
- Il est accompagné d'un clavier virtuel, qui, lorsqu'il est utilisé, empêche les pirates de lire vos frappes au clavier.
- Il est complètement indépendant de vos autres navigateurs.
- Il contient une protection hotspot intégrée à utiliser lorsque votre ordinateur est connecté à des réseaux Wifi non sécurisés.
- Il supporte les marque-pages et vous permet de consulter vos sites bancaires et boutiques en ligne préférés.

- Il ne se limite pas aux sites bancaires et boutiques en ligne. Tout site web peut être ouvert dans Bitdefender Safepay™.

19.1. Utiliser Bitdefender Safepay™

Par défaut, Bitdefender détecte que vous naviguez sur un site bancaire ou une boutique en ligne dans tout navigateur sur votre ordinateur et vous invite à le lancer dans Bitdefender Safepay™.

Pour accéder à l'interface principale de Bitdefender Safepay™, utilisez l'une des méthodes suivantes :

- À partir de l'interface de Bitdefender :
  1. Cliquez sur le bouton d'action **Safepay** à partir de l'interface Bitdefender.
- À partir de Windows :
  - Dans **Windows 7** :
    1. Cliquez sur **Démarrer** et allez dans **Programmes**.
    2. Cliquez sur **Bitdefender**.
    3. Cliquez sur **Bitdefender Safepay™**.
  - Dans **Windows 8 et Windows 8.1** :

    Localisez Bitdefender Safepay™ dans l'écran d'accueil Windows (vous pouvez, par exemple, taper « Bitdefender Safepay™ » directement dans l'écran d'accueil) puis cliquez sur l'icône.
  - Dans **Windows 10** :

    Tapez "Bitdefender Safepay™" dans le champ de recherche de la barre des tâches et cliquez sur son icône.

> **Note**
> Si le plugin Adobe Flash Player n'est pas installé ou n'est pas à jour, un message Bitdefender apparaîtra. Cliquez sur le bouton correspondant pour poursuivre.
> Une fois le processus d'installation terminé, vous pourrez rouvrir manuellement le navigateur Bitdefender Safepay™ pour poursuivre votre travail.

Si vous êtes habitués aux navigateurs web, vous n'aurez pas de problème pour utiliser Bitdefender Safepay™ - il ressemble et se comporte comme un navigateur standard :

- saisissez les URL que vous souhaitez consulter dans la barre d'adresses.
- ajoutez des onglets pour visiter plusieurs sites web dans la fenêtre de Bitdefender Safepay™ en cliquant sur .
- naviguez d'une page à l'autre et actualisez les pages à l'aide de respectivement.
- Accédez aux paramètres Bitdefender Safepay™ en cliquant et sélectionnant **Paramètres**.
- protégez vos mots de passe avec Password Manager en cliquant sur .
- gérez vos marque-pages en cliquant sur à côté de la barre d'adresses.
- ouvrez le clavier virtuel en cliquant sur .
- augmentez ou diminuez la taille du navigateur en appuyant simultanément sur les touches **Ctrl** et **+/-** du clavier numérique.
- Voir les informations de votre produit Bitdefender en cliquant sur puis sélectionnez **A propos**.
- Imprimer des informations importantes en cliquant .

19.2. Configurer les paramètres

Cliquer sur puis sélectionnez **Paramètres** pour configurerBitdefender Safepay™ :

Paramètres généraux

Choisissez ce qui se passera lorsque vous accéderez à une boutique ou à un site bancaire en ligne dans un navigateur Web standard :

- Ouvrir automatiquement les sites Web dans Safepay.
- Me recommander d'utiliser Safepay.
- Ne pas me recommander d'utiliser Safepay.

Liste des domaines

Choisissez comment Bitdefender Safepay™ se comportera lorsque vous consulterez les sites web de certains domaines dans votre navigateur Web standard en les ajoutant à la liste de domaines et en sélectionnant son comportement pour chacun d'entre eux :

- Ouvrir automatiquement dans Bitdefender Safepay™.
- Faire en sorte que Bitdefender vous consulte pour l'action à chaque fois.

- Ne jamais utiliser Bitdefender Safepay™ lors de la consultation d'une page de ce domaine dans un navigateur standard.

Bloquer les pop-up

Vous pouvez choisir de bloquer les fenêtres pop-up en cliquant sur le bouton correspondant.

Vous pouvez également créer une liste de sites web dont vous autorisez les fenêtres pop-up. La liste ne doit contenir que des sites Web de confiance.

Pour ajouter un site à la liste, saisissez son adresse dans le champ correspond et cliquez sur **Ajouter un domaine**.

Pour supprimer un site Web de la liste, sélectionnez-le dans la liste et cliquez sur le lien **Supprimer**.

Activer la protection Hotspot

Vous pouvez activer une couche de sécurité supplémentaire pour quand vous êtes connectés à des réseaux Wifi non sécurisés en activant cette fonctionnalité.

Accéder à « *Protection hotspot pour les réseaux non sécurisés* » (p. 119) pour plus d'informations.

19.3. Gérer les marque-pages

Si vous avez désactivé la détection automatique de certains ou de tous les sites web, ou si Bitdefender ne détecte simplement pas certains sites web, vous pouvez ajouter des marque-pages à Bitdefender Safepay™ afin de pouvoir lancer facilement vos sites web favoris à l'avenir.

Suivez ces étapes pour ajouter une URL aux marque-pages de Bitdefender Safepay™ :

1. Cliquez sur l'icône à côté de la barre d'adresses pour ouvrir la page Marque-pages.

   Note
   La page Marque-pages s'ouvre par défaut lorsque vous lancez Bitdefender Safepay™.

2. Cliquez sur le bouton **+** pour ajouter un nouveau marque-pages.

3. Indiquez l'URL et le titre du marque-pages et cliquez sur **Créer**. Cochez l'option **Ouvrir automatiquement dans Safepay** si vous souhaitez que la page mise en favori s'ouvre dans Bitdefender Safepay™ chaque fois que vous y accédez. L'URL est également ajoutée à la Liste de domaines sur la page paramètres.

19.4. Protection hotspot pour les réseaux non sécurisés

Lorsque vous utilisez Bitdefender Safepay™ en étant connecté à des réseaux Wifi non sécurisés (par exemple, à un point d'accès public), un niveau de sécurité supplémentaire est fourni par la fonctionnalité Protection Hotspot. Ce service chiffre la communication Internet sur des connexions non sécurisées, vous aidant à assurer la protection de votre vie privée quel que soit le réseau auquel vous êtes connecté.

La protection Hotpsot ne fonctionne que si votre ordinateur est connecté à un réseau non sécurisé.

La connexion sécurisée sera initialisée et un message s'affichera dans la fenêtre Bitdefender Safepay™ lorsque la connexion sera établie. Le symbole apparaît en face de l'URL dans la barre d'adresses pour vous aider à identifier facilement les connexions sécurisées.

Pour améliorer votre expérience de navigation visuellement, vous pouvez choisir d'activer les plugins **Adobe Flash** et **Java** en cliquant sur **Afficher les paramètres avancés**.

Vous aurez peut-être besoin de confirmer l'action.

20. PROTECTION PASSWORD MANAGER DE VOS IDENTIFIANTS

Nous utilisons l'ordinateur pour effectuer des achats en ligne ou payer nos factures, pour nous connecter à des plateformes de réseaux sociaux ou à des applications de messagerie instantanée.

Mais comme chacun le sait, ce n'est pas toujours facile de se souvenir des mots de passe !

Et si nous ne sommes pas prudents sur Internet, nos informations confidentielles telles que notre adresse courriel, nos identifiants de messagerie instantanée ou les données de notre carte bancaire peuvent être compromises.

Noter vos mots de passe ou vos données confidentielles sur une feuille de papier ou dans votre ordinateur peut être dangereux car cela les rend accessibles à des personnes qui souhaitent les dérober et les utiliser. Et vous souvenir de tous les mots de passe que vous avez définis pour vos comptes en ligne ou pour vos sites Web préférés n'est pas une tâche facile.

Y a-t-il un moyen de nous garantir de trouver nos mots de passe au moment où nous en avons besoin ? Et pouvons-nous être sûrs que nos mots de passe confidentiels sont en sécurité ?

Password Manager vous aide à conserver vos mots de passe, protège votre vie privée et vous offre une expérience de navigation sécurisée.

En utilisant un mot de passe principal unique pour accéder à vos identifiants, Password Manager vous permet de conserver facilement vos mots de passe en sécurité dans un Wallet.

Pour fournir la meilleure protection possible à vos activités en ligne, Password Manager est intégré à Bitdefender Safepay™ et offre une solution intégrée pour répondre aux différentes façons dont vos données confidentielles peuvent être compromises.

Password Manager protège les informations confidentielles suivantes :

- Des informations personnelles, telles que l'adresse courriel ou le numéro de téléphone
- Les identifiants de connexion aux sites Web
- Les informations bancaires sur les comptes et les numéros de carte

- Les données permettant d'accéder aux comptes de messagerie
- Les mots de passe des applications
- Les mots de passe des réseaux Wifi

20.1. Configurer Password Manager

Une fois l'installation terminée, lorsque vous ouvrirez votre navigateur, une fenêtre contextuelle vous indiquera que vous pouvez utiliser Portefeuille pour faciliter votre navigation sur Internet.

BitdefenderWallet est l'endroit où vous pouvez stocker vos données personnelles.

Cliquez sur **Explorer** pour lancer l'assistant de configuration de Portefeuille. Suivez l'assistant pour terminer le processus de configuration.

Deux tâches peuvent être réalisées au cours de cette étape :

- Créer une nouvelle base de données Portefeuille pour protéger vos mots de passe.

  Lors de la configuration, vous serez invité à protéger votre Portefeuille avec un mot de passe principal. Le mot de passe doit être sécurisé et contenir au moins 7 caractères.

  Pour créer un mot de passe sécurisé, utilisez au moins un chiffre ou un symbole et une majuscule. Une fois que vous aurez défini un mot de passe, toute personne essayant d'accéder au Portefeuille devra indiquer ce mot de passe.

  Après avoir configuré le mot de passe principal, vous pouvez synchroniser les informations du Wallet dans le cloud pour l'utiliser sur tous vos appareils.

  À la fin de la configuration, les paramètres suivants de Portefeuille sont activés par défaut :

  - **Enregistrer automatiquement les identifiants dans Portefeuille**.
  - **Me demander mon mot de passe principal lorsque j'ouvre mes navigateurs et applications**.
  - **Verrouiller automatiquement Portefeuille lorsque mon PC n'est pas utilisé**.
  - **Saisir automatiquement les identifiants de connexion**.

- **Me demander mes options de saisie lorsque je consulte une page contenant des formulaires**.
- Importez une base de données existante si vous avez déjà utilisé Portefeuille sur votre système.

Exporter la base de données du Portefeuille

Pour exporter la base de données de votre Portefeuille, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Cliquez sur le module **Password Manager**, puis sélectionnez l'onglet **Wallets**.
4. Sélectionnez la base de données Wallet souhaitée à partir de la section **Mes Wallets**, puis cliquez sur le bouton **Exporter**.
5. Suivez ces étapes pour exporter la base de données du Portefeuille vers votre système.

Note
Le wallet doit être ouvert pour que le bouton **Exporter** soit disponible.

Créer une nouvelle base de données Portefeuille

Pour créer une nouvelle base de données du Portefeuille, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Cliquez sur le module **Password Manager**, puis sélectionnez l'onglet **Wallets**.
4. Cliquez sur l'icône + dans la fenêtre qui apparaît.
5. Dans la zone **Partir de zéro**, cliquez sur **Créer nouveau**.
6. Tapez les informations requises dans les champs correspondants.

- Nom Wallet - saisissez un nom unique pour votre base de données Wallet.
- Mot de passe principal - saisissez un mot de passe pour votre Wallet.
- Saisissez le mot de passe à nouveau - saisissez à nouveau le mot de passe que vous avez configuré.
- Indice - saisissez un indice pour vous souvenir du mot de passe.

7. Cliquez sur **Continuer**.
8. A cette étape, vous pouvez choisir de stocker vos informations dans le cloud. Si vous choisissez Oui, vos informations bancaires seront conservées localement sur votre appareil. Choisissez les options souhaitées, puis cliquez sur **Continuer**.
9. Sélectionnez le navigateur web à partir duquel vous souhaitez importer vos identifiants.
10. Cliquez sur **Terminer**.

Synchroniser vos Wallets dans le cloud.

Pour activer ou désactiver la synchronisation des Wallets dans le cloud, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Cliquez sur le module **Password Manager**, puis sélectionnez l'onglet **Wallets**.
4. Sélectionnez la base de données Wallet souhaitée à partir de la section **Mes Wallets**, puis cliquez sur le bouton **Paramètres**
5. Choisissez l'option désirée dans la fenêtre qui apparaît, puis cliquez sur **Sauvegarder**.

Note
Le wallet doit être ouvert pour que le bouton **Paramètres** soit disponible.

Gérer les identifiants de votre Portefeuille

Pour gérer vos mots de passe, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Cliquez sur le module **Password Manager**, puis sélectionnez l'onglet **Wallets**.
4. Sélectionnez la base de données Wallet souhaitée à partir de la section **Mes Wallets**, puis cliquez sur le bouton **Ouvrir**.

Une nouvelle fenêtre apparaît. Sélectionnez la catégorie souhaitée dans la partie supérieure de la fenêtre :

- Identité
- Sites Web
- Banques
- Courriels
- Applications
- Réseaux Wifi

Ajouter/ modifier les identifiants

- Pour ajouter un nouveau mot de passe, choisissez la catégorie souhaitée en haut, cliquez sur **+ Ajouter un élément**, insérez les informations dans les champs correspondants et cliquez sur le bouton Enregistrer.
- Pour éditer un objet de la liste, sélectionnez le et cliquez sur le bouton **Editer**.
- Pour quitter, cliquez sur **Annuler**.
- Pour supprimer une entrée, sélectionnez-la, cliquez sur le bouton **Modifier** et sélectionnez **Supprimer**.

20.2. Activer ou désactiver la protection du Password Manager

Pour activer ou désactiver la protection du Password Manager, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Cliquez sur le module **Password Manager**.
4. Cliquez sur le bouton **Statut Module** pour activer ou désactiver le Password Manager.

20.3. Gestion des configurations du Password Manager

Pour configurer le mot de passe principal en détail, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Cliquez sur le module **Password Manager**, puis sélectionnez l'onglet **Configuration de la sécurité**.

Voici les options proposées :

- **Me demander mon mot de passe principal lorsque je me connecte à mon PC** - vous devrez indiquer votre mot de passe principal lorsque vous accéderez à l'ordinateur.
- **Me demander mon mot de passe principal lorsque j'ouvre mes navigateurs et applications** - vous devrez indiquer votre mot de passe principal lorsque vous accéderez à un navigateur ou à une application.
- **Verrouiller automatiquement Portefeuille lorsque mon PC n'est pas utilisé** - vous devrez saisir votre mot de passe principal lorsque vous utiliserez votre ordinateur après 15 minutes d'inactivité.

> **Important**
> N'oubliez pas votre mot de passe principal ou conservez-le en lieu sûr. Si vous oubliez le mot de passe, vous devrez réinstaller le programme ou contacter le support Bitdefender.

Améliorer votre expérience

Pour sélectionner les navigateurs ou les applications où vous souhaitez intégrer le Password Manager, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Cliquez sur le module **Password Manager**, puis sélectionnez l'onglet **Plugins**.

   Cochez une application pour utiliser le Password Manager et améliorer votre expérience :

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay
   - Skype
   - Yahoo! Messenger

Configurer la saisie automatique

La fonctionnalité Saisie automatique vous permet d'accéder facilement à vos sites web préférés ou de vous connecter à vos comptes en ligne. Lorsque vous saisissez vos informations d'identification et données personnelles dans votre navigateur web pour la première fois, celles-ci sont automatiquement conservées en toute sécurité dans Portefeuille.

Pour configurer les paramètres de la **Saisie automatique**, les étapes sont les suivantes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Vie privée**.
3. Cliquez sur le module **Password Manager**, puis sélectionnez l'onglet **Configuration Autofill**.
4. Configurez les options suivantes :

   - **Saisir automatiquement les identifiants de connexion**:

- **Saisir automatiquement les identifiants de connexion à chaque fois** - les identifiants de connexion sont insérés automatiquement dans le navigateur.
- **Me laisser choisir quand je souhaite que mes identifiants de connexion soient saisis automatiquement** - vous pouvez choisir quand les identifiants seront saisis automatiquement dans le navigateur.

- **Configurer la façon dont Password Manager sécurise vos identifiants**:
  - **Enregistrer automatiquement les identifiants dans Portefeuille** - les identifiants de connexion et autres informations identifiables telles que vos données personnelles et bancaires sont automatiquement enregistrées et mises à jour dans le Portefeuille.
  - **Me demander à chaque fois** - on vous demandera à chaque fois si vous souhaitez ajouter vos identifiants au Portefeuille.
  - **Ne pas enregistrer, je mettrai les informations à jour manuellement** - les identifiants peuvent être ajoutés uniquement manuellement dans le Portefeuille.
- **Compléter automatiquement les formulaires**:
  - **Me demander mes options de saisie lorsque je consulte une page contenant des formulaires** - une fenêtre avec les options de remplissage apparaîtra à chaque fois que Bitdefender détectera que vous souhaitez effectuer un paiement en ligne ou vous connecter.

Gérer les informations de Password Manager à partir de votre navigateur

Vous pouvez facilement gérer les détails de Password Manager directement à partir de votre navigateur afin d'avoir toutes vos données importantes à portée de main. L'extension Bitdefender Wallet est compatible avec les navigateurs suivants : Google Chrome, Internet Explorer et Mozilla Firefox et est également intégré à Safepay.

Pour accéder à l'extension Bitdefender Wallet, ouvrez votre navigateur web, autorisez l'installation de l'add-on et cliquez sur l'icône  de la barre d'outils.

L'extension Bitdefender Wallet présente les options suivantes :

- Ouvrir Portefeuille - ouvre le Portefeuille.

- Verrouiller Wallet - verrouille le Wallet.
- Sites web - ouvre un sous-menu avec tous les identifiants de sites web contenus dans Portefeuille. Cliquez sur **Ajouter un site web** pour ajouter de nouveaux sites web à la liste.
- Remplir les formulaires - ouvre un sous-menu contenant les informations que vous avez ajoutées pour une catégorie spécifique. Vous pouvez ajouter ici de nouvelles données à votre Portefeuille.
- Générateur de mot de passe - vous permet de générer des mots de passe au hasard que vous pourrez utiliser pour des comptes existants. Cliquez sur **Afficher configurations avancées** pour personnaliser la complexité du mot de passe.
- Configuration - ouvre la fenêtre des paramètres de Password Manager.
- Signaler un problème - permet de signaler tout problème rencontré avec Bitdefender Password Manager.

21. PROTECTION USB

La fonction AutoRun intégrée aux systèmes d'exploitation Windows est très utile car elle permet aux ordinateurs d'exécuter automatiquement un fichier depuis un support qui y est connecté. Par exemple, les installations de logiciels peuvent démarrer automatiquement lorsqu'un CD est inséré dans le lecteur optique.

Malheureusement, cette fonctionnalité peut également être utilisée par des malwares pour se lancer automatiquement et infiltrer votre ordinateur depuis des supports réinscriptibles tels que des lecteurs flash USB et des cartes mémoire connectés via des lecteurs de cartes. De nombreuses attaques exploitant la fonctionnalité AutoRun ont été créées ces dernières années.

Avec la protection USB, vous pouvez empêcher tout lecteur flash formaté en NTFS, FAT32 ou FAT d'exécuter des malwares. Lorsqu'un périphérique USB est immunisé, les malwares ne peuvent plus le configurer pour qu'il exécute une application spécifique lorsqu'il est connecté à un ordinateur fonctionnant sous Windows.

Pour immuniser un périphérique USB, procédez comme suit :

1. Connectez le lecteur flash à votre ordinateur.
2. Localisez sur votre ordinateur le périphérique de stockage amovible et faites un clic droit sur son icône.
3. Dans le menu contextuel, pointez sur **Bitdefender** et sélectionnez **Immuniser ce lecteur**.

> **Note**
> Si le lecteur a déjà été immunisé, le message **Le périphérique USB est protégé contre les malwares AutoRun** s'affichera au lieu de l'option Immuniser.

Pour empêcher que votre ordinateur ne lance des malwares depuis des lecteurs USB non immunisés, désactivez la fonction Exécution automatique des médias. Pour plus d'informations, reportez-vous à « *Utiliser la surveillance des vulnérabilités automatique* » (p. 109).

OPTIMISATION DU SYSTÈME

22. PROFILS

Effectuer des activités professionnelles quotidiennes, regarder des films ou jouer peut ralentir le système, en particulier si des processus de mise à jour Windows et des tâches de maintenance ont lieu simultanément. Bitdefender vous permet désormais de choisir et d'appliquer le profil de votre choix, qui fait les réglages nécessaires pour améliorer les performances de certaines applications installées sur le système.

Bitdefender propose les profils suivants :

- Profil Travail
- Profil Film
- Profil Jeu

Si vous décidez de ne pas utiliser les **Profils**, un profil par défaut nommé **Standard** est activé et n'apporte aucune optimisation à votre système.

En fonction de votre activité, les paramètres du produit suivants s'appliquent lorsqu'un profil est activé :

- Toutes les alertes et fenêtres pop-up de Bitdefender sont désactivées.
- La Mise à jour Automatique est reportée.
- Les analyses planifiées sont reportées.
- Search Advisor est désactivé.
- Les offres spéciales et notifications du produit sont désactivées.

En fonction de votre activité, les paramètres du système suivants s'appliquent lorsqu'un profil est activé :

- Les mises à jour automatiques de Windows sont reportées.
- Les alertes et fenêtres pop-up de Windows sont désactivées.
- Les programmes inutiles en arrière-plan sont interrompus.
- Les effets visuels sont ajustés pour de meilleures performances.
- Les tâches de maintenance sont reportées.
- Les paramètres du plan d'alimentation sont adaptés.

22.1. Profil Travail

Effectuer plusieurs tâches au travail comme envoyer des e-mails, avoir une communication vidéo avec des collègues ou utiliser des applications de conception graphique peut affecter les performances de votre système. Le profil Travail est conçu pour vous aider à améliorer votre efficacité en désactivant certaines tâches de maintenance et services d'arrière-plan.

Configurer le Profil Travail

Pour configurer les actions à appliquer lorsque le Profil Travail est activé, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Paramètres des profils**, cliquez sur le bouton **Configurer** dans la zone Profil Travail.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :
   - Améliorer les performances pour les applications de bureautique
   - Optimiser les paramètres du produit pour le profil Travail
   - Reporter les tâches de maintenance et les programmes en arrière-plan
   - Reporter les mises à jour automatiques de Windows
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des applications à la liste du Profil Travail

Si Bitdefender ne passe pas automatiquement en Profil Travail lorsque vous lancez une application de travail spécifique, vous pouvez ajouter manuellement cette application à la **Liste des applications**.

Pour ajouter manuellement des applications à la Liste des applications dans le Profil Travail :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils** puis sélectionnez le bouton **Configurer** dans la zone Profil Travail.
4. Dans la fenêtre **Profil Travail**, cliquez sur le lien **Liste des applications**.
5. Cliquez sur **Ajouter** pour ajouter une nouvelle application à la **Liste des applications**.

   Une nouvelle fenêtre apparaît. Localisez le fichier exécutable de l'application, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

22.2. Profil Film

Afficher du contenu vidéo de grande qualité comme des films haute définition nécessite d'importantes ressources système. Le Profil Film ajuste la configuration du système et du logiciel afin que vous puissiez regarder des films sans interruptions.

Configurer le Profil Film

Pour configurer les actions à appliquer lorsque le profil Film est activé :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Paramètres des profils**, cliquez sur le bouton **Configurer** dans la zone Profil Film.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :
   - Améliorer les performances pour les lecteurs vidéo
   - Optimiser les paramètres du produit pour le profil Film
   - Reporter les tâches de maintenance et les programmes en arrière-plan
   - Reporter les mises à jour automatiques de Windows

- Ajuster les paramètres du plan d'alimentation pour les films

6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des lecteurs vidéo à la liste du Profil Film

Si Bitdefender ne passe pas automatiquement en Profil Film lorsque vous lancez un lecteur vidéo spécifique, vous pouvez ajouter manuellement cette application à la **Liste des lecteurs vidéo**.

Pour ajouter manuellement des lecteurs vidéo à la Liste des lecteurs vidéo dans le Profil Film :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils** puis sélectionnez le bouton **Configurer** dans la zone Profil Film.
4. Dans la fenêtre **Profil Film**, cliquez sur le lien **Liste des lecteurs vidéo**.
5. Cliquez sur **Ajouter** pour ajouter une nouvelle application à la **Liste des lecteurs vidéo**.

   Une nouvelle fenêtre apparaît. Localisez le fichier exécutable de l'application, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

22.3. Profil Jeu

Pour une meilleure expérience de jeu, il suffit de réduire la charge du système et de diminuer les ralentissements. En associant des techniques heuristiques comportementales à une liste de jeux connus, Bitdefender détecte automatiquement les jeux en cours d'exécution et optimise les ressources du système afin que vous puissiez profiter pleinement de vos pauses.

Configurer le Profil Jeu

Pour configurer les actions à appliquer lorsque le Profil Jeu est activé, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Paramètres des profils**, cliquez sur le bouton **Configurer** dans la zone Profil Jeu.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :
   - Améliorer les performances pour les jeux
   - Optimiser les paramètres du produit pour le profil Jeu
   - Reporter les tâches de maintenance et les programmes en arrière-plan
   - Reporter les mises à jour automatiques de Windows
   - Ajuster les paramètres du plan d'alimentation pour les jeux
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des jeux à la Liste des jeux.

Si Bitdefender ne passe pas automatiquement en Profil Jeu lorsque vous lancez un jeu ou une application spécifique, vous pouvez ajouter manuellement cette application à la **Liste des Jeux**.

Pour ajouter manuellement des jeux à la liste des Jeux dans le Profil Jeu :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils** puis sélectionnez le bouton **Configurer** dans la zone Profil Jeu.
4. Dans la fenêtre **Profil Jeu**, cliquez sur le lien **Liste des Jeux**.
5. Cliquez sur **Ajouter** pour ajouter un nouveau jeu à la **Liste des Jeux**.

   Une nouvelle fenêtre apparaît. Localisez le fichier exécutable du jeu, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

22.4. Optimisation en temps réel

L'Optimisation en temps réel de Bitdefender est un plugin qui améliore les performances de votre système discrètement, en arrière-plan, en veillant à ce que vous ne soyez pas interrompu lorsque vous êtes en mode profil. En fonction de la charge du processeur, le plugin surveille tous les processus, en particulier ceux qui ont une charge plus élevée, afin de les adapter à vos besoins.

Pour activer ou désactiver l'Optimisation en temps réel, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Outils**.
3. Cliquez sur le module **Profils** puis sélectionnez l'onglet **Configuration Profils**.
4. Activez ou désactivez l'Optimisation en temps réel en cliquant sur le bouton correspondant.

RÉSOLUTION DES PROBLÈMES

23. RÉSOUDRE LES PROBLÈMES LES PLUS FRÉQUENTS

Ce chapitre présente certains problèmes que vous pouvez rencontrer lorsque vous utilisez Bitdefender et vous fournit des solutions possibles à ces problèmes. La plupart de ces problèmes peuvent être résolus via la configuration appropriée des paramètres du produit.

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du soutien technique Bitdefender comme indiqué dans le chapitre « *Demander de l'aide* » (p. 162).

23.1. Mon système semble lent

Généralement, après l'installation d'un logiciel de sécurité, on assiste à un léger ralentissement du système, qui est normal dans une certaine mesure.

Si vous remarquez un ralentissement important, ce problème peut apparaître pour les raisons suivantes :

- **Bitdefender n'est pas le seul logiciel de sécurité installé sur le système.**

  Bien que Bitdefender recherche et supprime les programmes de sécurité trouvés pendant l'installation, il est recommandé de supprimer tout programme antivirus que vous utilisiez avant d'installer Bitdefender. Pour

plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 72).

- **Vous ne disposez pas de la configuration système minimale pour l'exécution de Bitdefender.**

  Si votre machine ne dispose pas de la configuration système minimale, l'ordinateur deviendra lent, notamment lorsque plusieurs applications s'exécuteront simultanément. Pour plus d'informations, reportez-vous à « *Configuration système minimale* » (p. 3).

- **Vous avez installé des applications que vous n'utilisez pas**.

  Tous les ordinateurs ont des programmes ou des applications qui ne sont pas utilisés. Et de nombreux programmes indésirables s'exécutent en tâche de fond, utilisant de l'espace disque et de la mémoire. Si vous n'utilisez pas un programme, désinstallez-le. Cela s'applique également à tout autre logiciel préinstallé ou version d'évaluation d'une application que vous avez oublié de désinstaller.

  ! **Important**
  Si vous pensez qu'un programme ou qu'une application pourrait constituer un élément essentiel de votre système d'exploitation, ne les désinstallez pas et contactez le Service Client de Bitdefender pour obtenir de l'aide.

- **Votre système peut être infecté**.

  La vitesse de votre système et son comportement général peuvent également être affectés par des malwares. Les logiciels espions, les virus, les chevaux de Troie et les publiciels nuisent tous aux performances de votre ordinateur. Veillez à analyser votre système régulièrement, au moins une fois par semaine. Il est recommandé d'utiliser l'Analyse du système Bitdefender car elle recherche tous les types de malwares menaçant la sécurité de votre système.

  Pour lancer l'analyse du système, procédez comme suit :

  1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
  2. Sélectionnez l'onglet **Protection**.
  3. Sous le module **Antivirus**, sélectionnez **Analyse du Système**.
  4. Suivez les étapes de l'assistant.

23.2. L'analyse ne démarre pas

Ce type de problème peut avoir deux causes principales :

- **Une installation précédente de Bitdefender qui n'a pas été complètement supprimée ou une installation défectueuse de Bitdefender**.

  Dans ce cas, procédez comme suit :

  1. Désinstaller complètement Bitdefender du système :
     - Dans **Windows 7** :
       a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
       b. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
       c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
       d. Cliquez sur **Suivant** pour continuer.
       e. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
     - Dans **Windows 8 et Windows 8.1** :
       a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
       b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
       c. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
       d. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
       e. Cliquez sur **Suivant** pour continuer.
       f. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
     - Dans **Windows 10** :

a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".

b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.

c. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.

d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.

e. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

f. Cliquez sur **Suivant** pour continuer.

g. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

2. Réinstallez votre produit Bitdefender.

- **Bitdefender n'est pas la seule solution de sécurité installée sur votre système**.

  Dans ce cas, procédez comme suit :

  1. Supprimer l'autre solution de sécurité. Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 72).
  2. Désinstaller complètement Bitdefender du système :
     - Dans **Windows 7** :
       a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
       b. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
       c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
       d. Cliquez sur **Suivant** pour continuer.
       e. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
     - Dans **Windows 8 et Windows 8.1** :
       a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de

configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.

b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.

c. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.

d. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

e. Cliquez sur **Suivant** pour continuer.

f. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

- Dans **Windows 10** :

a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".

b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.

c. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.

d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.

e. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

f. Cliquez sur **Suivant** pour continuer.

g. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

3. Réinstallez votre produit Bitdefender.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 162).

23.3. Je ne peux plus utiliser une application

Ce problème se produit lorsque vous essayez d'utiliser un programme qui fonctionnait normalement avant d'installer Bitdefender.

Après l'installation de Bitdefender vous pouvez vous trouver dans l'une des situations suivantes :

- Vous pourriez recevoir un message de Bitdefender indiquant que le programme essaie d'apporter une modification au système.
- Il est possible que vous receviez un message d'erreur du programme que vous tentez d'utiliser.

Ce type de situation se produit quand Active Threat Control détecte à tort certaines applications comme étant malveillantes.

Active Threat Control est un module Bitdefender qui surveille en permanence les applications s'exécutant sur votre système et signale celles au comportement potentiellement malveillant. Étant donné que la fonction est basée sur un système heuristique, des applications légitimes peuvent, dans certains cas, être signalées par Active Threat Control.

Lorsque cette situation se produit, vous pouvez empêcher l'application correspondante d'être surveillée par Active Threat Control.

Pour ajouter le programme à la liste d'exceptions, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Antivirus** puis sélectionnez l'onglet **Exclusions**.
4. Cliquez sur le lien **Processus Exclus**. Dans la fenêtre qui apparaît, vous pouvez gérer les exclusions de processus Active Threat Control.
5. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Cliquez sur **Parcourir**, sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.
   c. Gardez l'option **Autoriser** sélectionnée pour empêcher Active Threat Control de bloquer l'application.
   d. Cliquez sur **Ajouter**.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 162).

23.4. Que faire lorsque Bitdefender bloque un site web ou une application en ligne sûre

Bitdefender permet de naviguer sur Internet en toute sécurité en filtrant l'ensemble du trafic web et en bloquant tout contenu malveillant. Il est toutefois possible que Bitdefender considère à tort qu'un site web ou une application en ligne n'est pas sûr, et que l'analyse du trafic HTTP de Bitdefender les bloque par erreur.

Si une page ou une application est bloquée de façon répétée, elle peut être ajoutée à une liste blanche afin de ne pas être analysée par les moteurs de Bitdefender et de permettre une navigation sans interruptions.

Pour ajouter un site web à la **Liste blanche**, procédez comme suit :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Cliquez sur le module **Protection Web**.
4. Dans l'onglet **Paramètres**, cliquez sur le lien **Liste blanche**.
5. Indiquez l'adresse du site web ou d'une application en ligne bloquée dans le champ correspondant et cliquez sur **Ajouter**.
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Seuls les sites web et les applications en lesquels vous avez pleinement confiance devraient être ajoutés à cette liste. Ils ne seront pas analysés par les moteurs suivants : malwares, phishing et fraude.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 162).

23.5. Comment mettre à jour Bitdefender avec une connexion Internet lente ?

Si votre connexion Internet est lente (RTC ou RNIS, par exemple), des erreurs peuvent se produire pendant le processus de mise à jour.

Pour maintenir votre système à jour avec les dernières signatures de malwares Bitdefender, suivez les étapes suivantes :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Configurations générales** dans le menu déroulant.
2. Dans la fenêtre **Configurations générales**, sélectionnez l'onglet **Mise à jour**.
3. À côté de **Règles de traitement**, sélectionnez **Demander avant le téléchargement** dans le menu déroulant.
4. Retournez dans la fenêtre principale et cliquez sur le bouton d'action **Mise à jour** dans l'interface Bitdefender.
5. Sélectionnez uniquement **Mises à jour de signatures**, puis cliquez sur **OK**.
6. Bitdefender ne téléchargera et n'installera que les mises à jour des signatures de malwares.

23.6. Le Services Bitdefender ne répondent pas

Cet article vous aide à régler l'erreur **Les Services Bitdefender ne répondent pas**. Vous pouvez rencontrer cette erreur de la façon suivante :

- L'icône Bitdefender de la zone de notification est grisée et vous informe que les services Bitdefender ne répondent pas.
- La fenêtre Bitdefender indique que les services Bitdefender ne répondent pas.

L'erreur peut être causée par :

- erreurs de communication temporaires entre les services Bitdefender.
- certains services Bitdefender sont interrompus.
- d'autres solutions de sécurité sont en cours d'exécution sur votre ordinateur en même temps que Bitdefender.

Pour régler cette erreur, essayez ces solutions :

1. Attendez quelques instants et voyez si quelque chose change. L'erreur peut être temporaire.
2. Redémarrez l'ordinateur et attendez quelques instants jusqu'à ce que Bitdefender soit chargé. Ouvrez Bitdefender pour voir si l'erreur persiste. Redémarrer l'ordinateur règle habituellement le problème.
3. Vérifiez que vous n'avez pas d'autre solution de sécurité installée car cela pourrait affecter le fonctionnement normal de Bitdefender. Si c'est le cas,

nous vous recommandons de supprimer toutes les autres solutions de sécurité et de réinstaller ensuite Bitdefender.

Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 72).

Si l'erreur persiste, veuillez contacter les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la section « *Demander de l'aide* » (p. 162).

23.7. La fonctionnalité saisie automatique de mon Portefeuille ne fonctionne pas

Vous avez enregistré vos identifiants en ligne dans votre Bitdefender Portefeuille et avez remarqué que la saisie automatique ne fonctionne pas. Ce problème se produit généralement lorsque l'extension de Bitdefender Password Manager n'est pas installée dans votre navigateur.

Pour résoudre cette situation, suivez ces étapes :

- Dans **Internet Explorer :**
  1. Ouvrez Internet Explorer.
  2. Cliquez sur Outils.
  3. Cliquez sur Gérer les modules.
  4. Cliquez sur Barres d'outils et Extensions.
  5. Pointez sur **Bitdefender Password Manager** et cliquez sur Permettre.
- Dans **Mozilla Firefox :**
  1. Ouvrez Mozilla Firefox.
  2. Cliquez sur Outils.
  3. Cliquez sur Modules.
  4. Cliquez sur Extensions.
  5. Pointez sur **Bitdefender Password Manager** et cliquez sur Permettre.
- Dans **Google Chrome :**
  1. Ouvrez Google Chrome.
  2. Allez sur l'icône du Menu.
  3. Cliquez sur Paramètres.

4. Cliquez sur Extensions.
5. Pointez sur **Bitdefender Password Manager** et cliquez sur Permettre.

> **Note**
> Le module sera activé une fois que vous aurez redémarré votre navigateur Web.

Vérifiez maintenant que la fonctionnalité de saisie automatique de Portefeuille fonctionne pour vos comptes en ligne.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 162).

23.8. La désinstallation de Bitdefender a échoué

Si vous souhaitez supprimer votre produit Bitdefender et remarquez que le processus se bloque ou que le système se fige, cliquez sur **Annuler** pour annuler l'action. Si cela ne fonctionne pas, redémarrez le système.

Lorsque la désinstallation échoue, certaines clés de registre et fichiers de Bitdefender peuvent demeurer sur votre système. De tels restes peuvent empêcher une nouvelle installation de Bitdefender. Ils peuvent aussi affecter la performance du système et sa stabilité.

Afin de désinstaller complètement Bitdefender de votre système, procédez comme suit :

- Dans **Windows 7** :
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
  2. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
  3. Sélectionnez **Remove**, puis **Je souhaite le désinstaller définitivement**.
  4. Cliquez sur **Suivant** pour continuer.
  5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Dans **Windows 8 et Windows 8.1** :
  1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.

2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
4. Sélectionnez **Remove**, puis **Je souhaite le désinstaller définitivement**.
5. Cliquez sur **Suivant** pour continuer.
6. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

- Dans **Windows 10** :

1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
3. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Sélectionnez **Remove**, puis **Je souhaite le désinstaller définitivement**.
6. Cliquez sur **Suivant** pour continuer.
7. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

23.9. Mon système ne démarre pas après l'installation de Bitdefender

Si vous venez d'installer Bitdefender et ne pouvez plus redémarrer votre système en mode normal, il peut y avoir plusieurs raisons à ce problème.

Cela est sans doute dû à une installation précédente de Bitdefender qui n'a pas été désinstallée correctement ou à une autre solution de sécurité toujours présente sur le système.

Voici comment faire face à chaque situation :

- **Vous aviez Bitdefender et vous ne l'avez pas désinstallé correctement.**

  Pour résoudre cela, suivez ces étapes :

  1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 74).

2. Désinstallez Bitdefender de votre système :
   - Dans **Windows 7** :
     a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
     b. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
     c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
     d. Cliquez sur **Suivant** pour continuer.
     e. Patientez jusqu'à la fin du processus de désinstallation.
     f. Redémarrez votre système en mode normal.
   - Dans **Windows 8 et Windows 8.1** :
     a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
     b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
     c. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.
     d. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
     e. Cliquez sur **Suivant** pour continuer.
     f. Patientez jusqu'à la fin du processus de désinstallation.
     g. Redémarrez votre système en mode normal.
   - Dans **Windows 10** :
     a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
     b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
     c. Localisez **Bitdefender Antivirus Plus 2016** et sélectionnez **Désinstaller**.

d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.

e. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

f. Cliquez sur **Suivant** pour continuer.

g. Patientez jusqu'à la fin du processus de désinstallation.

h. Redémarrez votre système en mode normal.

3. Réinstallez votre produit Bitdefender.

- **Vous aviez une autre solution de sécurité auparavant et vous ne l'avez pas désinstallée correctement.**

  Pour résoudre cela, suivez ces étapes :

  1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 74).
  2. Désinstallez l'autre solution de sécurité de votre système :
     - Dans **Windows 7** :
       a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
       b. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.
       c. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
     - Dans **Windows 8 et Windows 8.1** :
       a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
       b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
       c. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.
       d. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

- Dans **Windows 10** :
  a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
  b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
  c. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
  d. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

  Afin de désinstaller correctement les autres logiciels, allez sur leur site Internet et exécutez leur outil de désinstallation, ou contactez-les directement afin qu'ils vous indiquent la procédure de désinstallation.

3. Redémarrez votre système en mode normal et réinstallez Bitdefender.

Vous avez déjà suivi les étapes ci-dessus et la situation n'est pas résolue.

Pour résoudre cela, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 74).
2. Utilisez l'option Restauration du Système de Windows pour restaurer l'ordinateur à une date antérieure à l'installation du produit Bitdefender.
3. Redémarrez le système en mode normal et contactez les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la section « *Demander de l'aide* » (p. 162).

24. SUPPRESSION DES MALWARES DE VOTRE SYSTÈME

Les malwares peuvent affecter votre système de nombreuses manières et l'approche de Bitdefender dépend du type d'attaque de malware. Les virus changeant souvent de comportement, il est difficile de définir leur comportement et leurs actions.

Il s'agit des situations où Bitdefender ne peut supprimer automatiquement l'infection de malwares de votre système. Dans ce cas, votre intervention est nécessaire.

- « *Mode de Secours de Bitdefender* » (p. 152)
- « *Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?* » (p. 155)
- « *Comment nettoyer un virus dans une archive ?* » (p. 156)
- « *Comment nettoyer un virus dans une archive de messagerie ?* » (p. 157)
- « *Que faire si je suspecte un fichier d'être dangereux ?* » (p. 159)
- « *Que sont les fichiers protégés par mot de passe du journal d'analyse ?* » (p. 159)
- « *Que sont les éléments ignorés du journal d'analyse ?* » (p. 160)
- « *Que sont les fichiers ultra-compressés du journal d'analyse ?* » (p. 160)
- « *Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?* » (p. 160)

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du soutien technique Bitdefender comme indiqué dans le chapitre « *Demander de l'aide* » (p. 162).

24.1. Mode de Secours de Bitdefender

Le **Mode de secours** est une fonctionnalité de Bitdefender qui vous permet d'analyser et de désinfecter toutes les partitions de votre disque dur hors de votre système d'exploitation.

Une fois Bitdefender Antivirus Plus 2016 installé, le Mode de Secours peut être utilisé même si vous ne pouvez plus démarrer sous Windows.

Démarrer votre système en mode de secours

Vous pouvez entrer en mode de secours de l'une des deux façons suivantes :

À partir de l'interface de Bitdefender

Pour entrer en Mode de Secours directement à partir de Bitdefender, suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
2. Sélectionnez l'onglet **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Mode de secours**.

   Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour redémarrer votre ordinateur.
4. Après le redémarrage de l'ordinateur, un menu apparaîtra vous demandant de sélectionner un système d'exploitation. Sélectionnez **Mode de Secours de Bitdefender** et appuyez sur la touche **Entrée** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.
5. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.

   Le Mode de Secours de Bitdefender se chargera dans quelques instants.

Démarrez votre ordinateur directement en mode de secours

Si Windows ne démarre plus, vous pouvez démarrer directement votre ordinateur en Mode de Secours de Bitdefender en suivant les étapes ci-dessous:

1. Démarrez / redémarrez votre ordinateur et appuyez sur la touche **espace** de votre clavier avant que n'apparaisse le logo Windows.
2. Un menu apparaîtra vous demandant de sélectionner un système d'exploitation à démarrer. Cliquez sur **ONGLET** pour vous rendre dans la zone d'outils. Sélectionnez **Image de Secours de Bitdefender** et appuyez sur la touche **Entrée** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.

3. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.

   Le Mode de Secours de Bitdefender se chargera dans quelques instants.

Analyser votre système en mode de secours

Pour analyser votre système en mode de secours, procédez comme suit :

1. Entrez en mode de secours, comme indiqué dans « Démarrer votre système en mode de secours » (p. 153).
2. Le logo Bitdefender apparaîtra et les moteurs antivirus commenceront à être copiés.
3. Une fenêtre d'accueil apparaîtra. Cliquez sur **Continuer**.
4. Une mise à jour des signatures antivirus a démarré.
5. Une fois la mise à jour terminée, la fenêtre du Scanner Antivirus à la demande Bitdefender s'affiche.
6. Cliquez sur **Analyser**, sélectionnez la cible de l'analyse dans la fenêtre qui s'affiche et cliquez sur **Ouvrir** pour lancer l'analyse.

   Nous vous recommandons l'analyse de la totalité de votre partition Windows.

   > **Note**
   > En mode de secours, les noms de partitions sont de type Linux. Des partitions de disque apparaîtront, sda1 correspondant probablement à la partition de type Windows (C:), sda2 correspondant à (D:), etc.

7. Patientez jusqu'à la fin de l'analyse. Si un malware est détecté, suivez les instructions pour supprimer la menace.
8. Pour quitter le mode de secours, faites un clic droit sur une zone vide du bureau, sélectionnez **Quitter** dans le menu qui apparaît puis choisissez de redémarrer ou d'éteindre l'ordinateur.

24.2. Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?

Il est possible que vous découvriez qu'un virus se trouve sur votre ordinateur de l'une des manières suivantes :

- Vous avez analysé votre ordinateur et Bitdefender y a détecté des éléments infectés.
- Une alerte de virus vous informe que Bitdefender a bloqué un ou plusieurs virus sur votre ordinateur.

Dans de telles situations, mettez à jour Bitdefender pour vous assurer de disposer des dernières signatures de malwares puis exécutez une analyse du système.

Dès que l'analyse du système est terminée, sélectionnez l'action souhaitée à appliquer aux éléments infectés (Désinfecter, Supprimer, Quarantaine).

Avertissement
Si vous pensez que le fichier fait partie du système d'exploitation Windows ou qu'il ne s'agit pas d'un fichier infecté, ne suivez pas ces étapes et contactez le Service Client de Bitdefender dès que possible.

Si l'action sélectionnée ne peut être appliquée et que le journal d'analyse révèle une infection qui ne peut être supprimée, vous devez supprimer le(s) fichier(s) manuellement :

La première méthode peut être utilisée en mode normal :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquer sur l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
   b. Sélectionnez l'onglet **Protection**.
   c. Cliquez sur le module **Antivirus**, puis sélectionnez l'onglet **Résident**
   d. Cliquez sur le bouton pour désactiver l'**Analyse à l'accès**.
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 71).

3. Accédez à l'emplacement du fichier infecté (consultez le journal d'analyse), puis supprimez-le.
4. Activez la protection antivirus en temps réel de Bitdefender.

Si la première méthode ne parvient pas à supprimer l'infection, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 74).
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 71).
3. Accédez à l'emplacement du fichier infecté (consultez le journal d'analyse), puis supprimez-le.
4. Redémarrez votre système et entrez en mode normal.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 162).

24.3. Comment nettoyer un virus dans une archive ?

Une archive est un fichier ou un ensemble de fichiers compressés sous un format spécial pour réduire l'espace nécessaire sur le disque pour stocker les fichiers.

Certains de ces formats sont des formats ouverts, permettant ainsi à Bitdefender de les analyser, puis de mener les actions appropriées pour les supprimer.

D'autres formats d'archive sont fermés partiellement ou totalement, et Bitdefender peut uniquement détecter la présence de virus dans ceux-ci, mais n'est pas capable de mener d'autres actions.

Si Bitdefender indique qu'un virus a été détecté dans une archive et qu'aucune action n'est disponible, cela signifie qu'il n'est pas possible de supprimer le virus en raison de restrictions sur les paramètres d'autorisation de l'archive.

Voici comment nettoyer un virus stocké dans une archive :

1. Identifiez l'archive où se trouve le virus en réalisant une analyse du système.
2. Désactivez la protection antivirus en temps réel de Bitdefender :

a. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.

b. Sélectionnez l'onglet **Protection**.

c. Cliquez sur le module **Antivirus**, puis sélectionnez l'onglet **Résident**

d. Cliquez sur le bouton pour désactiver l'**Analyse à l'accès**.

3. Rendez-vous à l'emplacement de l'archive et décompressez-la à l'aide d'une application d'archivage, comme WinZip.
4. Identifier le fichier infecté et le supprimer.
5. Supprimez l'archive d'origine afin de vous assurer que l'infection est totalement supprimée.
6. Recompressez les fichiers dans une nouvelle archive à l'aide d'une application d'archivage, comme WinZip.
7. Activez la protection antivirus en temps réel de Bitdefender et exécutez une analyse complète du système afin de vous assurer qu'aucune autre infection n'est présente sur le système.

Note
Il est important de noter qu'un virus contenu dans une archive ne représente pas de menace immédiate pour votre système, puisque, pour infecter votre système, le virus doit être décompressé et exécuté.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 162).

24.4. Comment nettoyer un virus dans une archive de messagerie ?

Bitdefender permet également de repérer les virus dans les bases de données d'e-mails et les archives d'e-mails stockées sur le disque.

Il est parfois nécessaire d'identifier le message infecté à l'aide des informations du rapport d'analyse, et de le supprimer manuellement.

Voici comment nettoyer un virus stocké dans une archive de messagerie électronique :

1. Analysez la base de données des e-mails avec Bitdefender.

2. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquer sur  l'icône dans le coin en bas à gauche de l'interfaceBitdefender.
   b. Sélectionnez l'onglet **Protection**.
   c. Cliquez sur le module **Antivirus**, puis sélectionnez l'onglet **Résident**
   d. Cliquez sur le bouton pour désactiver l'**Analyse à l'accès**.
3. Ouvrez le rapport d'analyse et utilisez les informations d'identification (Sujet, Expéditeur, Destinataire) des messages infectés pour les localiser dans le client de messagerie.
4. Supprimez les messages infectés. La plupart des clients de messagerie placent les messages supprimés dans un dossier de récupération permettant de les restaurer. Il est recommandé de vous assurer que le message a été supprimé également dans ce dossier de récupération.
5. Compressez le dossier contenant le message infecté.
   - Dans Outlook Express : Dans le menu Fichier, cliquez sur Dossier, puis sur Compacter tous les dossiers.
   - Dans Microsoft Outlook 2007 : Dans le menu Fichier, cliquez sur Gestion des fichiers de données. Sélectionnez les dossiers de fichiers personnels (.pst) que vous souhaitez compresser, puis cliquez sur Configuration. Cliquez sur Compresser.
   - Dans Microsoft Outlook 2010 / 2013 : Dans le menu Fichier, cliquez sur Infos puis sur Paramètres du compte (Ajouter et supprimer des comptes ou modifier les paramètres de connexion existants). Cliquez ensuite sur Fichier de données, sélectionnez les fichiers des dossiers personnels (.pst) que vous souhaitez compacter puis cliquez sur Paramètres. Cliquez sur Compresser.
6. Activez la protection antivirus en temps réel de Bitdefender.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 162).

24.5. Que faire si je suspecte un fichier d'être dangereux ?

Vous pouvez suspecter qu'un fichier de votre système est dangereux, même si votre produit Bitdefender ne l'a pas détecté.

Pour vérifier que votre système est protégé, suivez ces étapes :

1. Exécuter une **Analyse du Système** avec Bitdefender. Pour savoir comment faire cela, reportez-vous à « *Comment analyser mon système ?* » (p. 60).
2. Si le résultat de l'analyse n'indique pas d'infection, mais que vous avez encore des doutes et souhaitez vérifier le fichier, contactez les représentants de notre soutien technique afin que nous puissions vous aider.

   Pour savoir comment faire cela, consultez « *Demander de l'aide* » (p. 162).

24.6. Que sont les fichiers protégés par mot de passe du journal d'analyse ?

Il ne s'agit que d'une notification qui indique que Bitdefender a détecté que ces fichiers sont soit protégés par un mot de passe soit par une forme de chiffrement .

Les éléments protégés par un mot de passe sont généralement :

- Fichiers appartenant à une autre solution de sécurité.
- Fichiers appartenant au système d'exploitation.

Afin que le contenu soit analysé, ces fichiers auront besoin d'être extraits ou déchiffrés.

Si ce contenu était extrait, le moteur d'analyse en temps réel de Bitdefender l'analyserait automatiquement pour que votre ordinateur reste protégé. Si vous souhaitez analyser ces fichiers avec Bitdefender, vous devez contacter le fabricant du produit afin d'obtenir plus d'informations sur ces fichiers.

Nous vous recommandons d'ignorer ces fichiers car ils ne constituent pas une menace pour votre système.

24.7. Que sont les éléments ignorés du journal d'analyse ?

Tous les fichiers apparaissant comme ignorés dans le rapport d'analyse sont sains.

Pour de meilleures performances, Bitdefender n'analyse pas les fichiers n'ayant pas été modifiés depuis la dernière analyse.

24.8. Que sont les fichiers ultra-compressés du journal d'analyse ?

Les éléments ultra-compressés sont des éléments qui n'ont pas pu être extraits par le moteur d'analyse ou des éléments dont le temps de déchiffrement aurait été trop long et aurait rendu le système instable.

Surcompressé signifie que Bitdefender a ignoré l'analyse dans cette archive car sa décompression consommait trop de ressources système. Le contenu sera analysé à l'accès en temps réel si nécessaire.

24.9. Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?

Si un fichier infecté est détecté, Bitdefender tente automatiquement de le désinfecter. Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection.

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

C'est généralement le cas avec les fichiers d'installation qui sont téléchargés depuis des sites non fiables. Si vous vous trouvez dans une telle situation, téléchargez le fichier d'installation sur le site Web du fabricant ou sur un autre site de confiance.

NOUS CONTACTER

25. DEMANDER DE L'AIDE

Bitdefender fournit à ses clients une aide hors pair, rapide et efficace. Si vous rencontrez le moindre problème ou si vous avez des questions sur votre produit Bitdefender, vous pouvez utiliser plusieurs ressources en ligne pour trouver rapidement une solution ou une réponse. Vous pouvez également contacter l'équipe du Service Client de Bitdefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.

La section « *Résoudre les problèmes les plus fréquents* » (p. 138) fournit les informations nécessaires concernant les problèmes les plus fréquents que vous pouvez rencontrer lors de l'utilisation de ce produit.

Si vous ne trouvez pas de réponse à votre question dans les ressources fournies, vous pouvez nous contacter directement :

- « Contactez-nous directement à partir de votre produit Bitdefender » (p. 162)
- « Contactez-nous via notre Centre de Support en ligne » (p. 163)

Contactez-nous directement à partir de votre produit Bitdefender

Si vous disposez d'une connexion Internet, vous pouvez contacter l'assistance de Bitdefender directement à partir de l'interface du produit.

Suivez ces étapes :

1. Cliquez sur l'icône  en haut de l'interface Bitdefender et sélectionnez **Aide& Support** dans le menu déroulant.
2. Vous disposez des options suivantes :
   - **Documentation du produit**

     Accédez à notre base de données et recherchez les informations nécessaires.
   - **Communiquer avec le soutien**

     Utilisez le bouton **Contacter le Support** pour lancer l'Outil Support de Bitdefender et contacter le Support Client. Vous pouvez naviguer dans

l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

a. Cochez la case d'accord et cliquez sur **Suivant**.

b. Compléter le formulaire de soumission avec les données nécessaires :

   i. Saisissez votre adresse e-mail.

   ii. Indiquez votre nom complet.

   iii. Décrivez le problème que vous avez rencontré.

   iv. Sélectionnez l'option **Essayer de reproduire le problème avant la soumission** si vous rencontrez un problème avec le produit. Poursuivez avec les étapes requises.

c. Veuillez patienter pendant quelques minutes pendant que Bitdefender recueille les informations sur le produit. Ces informations aideront nos ingénieurs à trouver une solution à votre problème.

d. Cliquez sur **Terminer** pour envoyer les informations au Service Client de Bitdefender. Nous vous contacterons dès que possible.

Contactez-nous via notre Centre de Support en ligne

Si vous ne parvenez pas à accéder aux informations nécessaires à l'aide du produit Bitdefender, consultez notre Centre de Support en ligne :

1. Allez à http://www.bitdefender.fr/support/consumer.html.

   Le Centre de Support de Bitdefender contient de nombreux articles apportant des solutions aux problèmes liés à Bitdefender.

2. Utilisez la barre de recherche en haut de la fenêtre pour trouver des articles susceptibles d'apporter une solution à votre problème. Pour effectuer une recherche, saisissez simplement un terme dans la barre de recherche et cliquez sur **Rechercher**.

3. Consultez les articles et les documents pertinents et essayez les solutions proposées.

4. Si la solution ne règle pas votre problème, allez dans

   http://www.bitdefender.fr/support/nous-contacter.htmlet contactez nos représentants du support.

25.1. Support Technique Profil Technology / Bitdefender

Centre d'Assistance des Laboratoires Technologiques et Scientifiques

Les Laboratoires de Profil Technology et de Bitdefender assurent un niveau d'assistance sur tous les produits maintenus par l'équipe de développement. La résolution d'un problème peut nous amener à vous proposer de mettre gratuitement à niveau la version de votre produit.

Ce service offre une assistance pour les questions ou problèmes liés à des applications courantes pour l'utilisateur final ou les entreprises, telles que :

- Des configurations personnalisées des produits Bitdefender.
- Des conseils de prise en main en monoposte ou en relation avec des réseaux simples.
- Des problèmes techniques après l'installation des produits Bitdefender.
- Des aides afin de contrer les activités de codes malicieux présents sur un système.
- L'accès à notre site internet de maintenance personnalisée et de FAQ en ligne 24h/24 et 7j/7 : http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/.
- L'accès aux informations des centres de support internationaux, qui permettent de gérer les situations par chat online – Accessible 7j/7 – 365j/an. Pour y accéder, veuillez saisir l'adresse ci-dessous dans votre navigateur : http://www.bitdefender.fr/site/KnowledgeBase/getSupport/. Attention : ce module est un service international, assuré majoritairement en Anglais.

Assistance téléphonique :

Les Laboratoires Profil Technology et Bitdefender mettent en oeuvre tous les efforts commercialement envisageables pour maintenir l'accès à l'assistance téléphonique de ce service, pendant les heures ouvrées locales du lundi au vendredi, sauf pendant les jours fériés.

Accès téléphoniques aux Laboratoires Profil Technology et Bitdefender :

- **Pour la France et les DOM-TOM** : 0892 561 161 (0.34 euros / minute)
- **Pour la Belgique** : 070 35 83 04

- **Pour la Suisse** : 0900 000 118 (0,60 FS / minute)

Avant de nous appeler, munissez-vous :

- du numéro de licence du produit Bitdefender. Communiquez le à un de nos analystes afin qu'il vérifie votre niveau d'assistance.
- de la version actuelle du système d'exploitation.
- des informations sur les marques et modèles de tous les périphériques et des logiciels chargés en mémoire ou utilisés.

En cas d'infection, l'analyste pourra demander une liste d'informations techniques à fournir ainsi que certains fichiers, qui pourront être nécessaires à son diagnostic.

Lorsqu'un analyste vous le demande, précisez les messages d'erreurs reçus et le moment où ils apparaissent, les activités qui ont précédées le message d'erreur et les démarches déjà entreprises pour résoudre le problème.

L'analyste suivra une procédure de dépannage stricte afin de tenter de diagnostiquer le problème.

Le Service n'inclut pas les éléments suivants :

- Ce service d'assistance ne comprend pas les applications, les installations, la désinstallation, le transfert, la maintenance préventive, la formation, l'administration à distance ou configurations logicielles autres que celles spécifiquement notifiées par l'analyste des Laboratoires Profil Technology et Bitdefender lors de l'intervention.
- L'installation, le paramétrage, l'optimisation et la configuration en réseau ou à distance d'applications n'entrant pas dans le cadre de l'assistance actuelle.
- Sauvegarde des logiciels/données. Il incombe au Client d'effectuer une sauvegarde de toutes les données, des logiciels et des programmes existants sur les systèmes d'information pris en charge avant toute prestation de service par Profil Technology et de Bitdefender.

Profil Technology ou Bitdefender NE PEUVENT ÊTRE TENUS RESPONSABLE DE LA PERTE OU DE LA RÉCUPÉRATION DE DONNÉES, DE PROGRAMMES, OU DE LA PRIVATION DE JOUISSANCE DES SYSTÈME(S) OU DU RÉSEAU.

Les conseils sont strictement limités aux questions demandées et basées sur les informations fournies par le client. Les problèmes et les solutions peuvent dépendre de la nature de l'environnement du système et d'une variété d'autres paramètres qui sont inconnus à Profil Technology ou Bitdefender.

Par conséquent, Profil Technology ou Bitdefender ne peuvent en aucun cas être tenus responsable de dommages résultant de l'utilisation de ces informations.

Il est possible que l'état du système sur lequel les produits Bitdefender doivent être installés soit instable (infection préalable, installation d'antivirus ou solutions de sécurité multiples, etc.). Dans ces cas précis, il est possible que l'analyste vous propose une prestation de maintenance auprès de votre revendeur avant de pouvoir régler votre problème.

Les informations techniques peuvent changer lorsque des nouvelles données deviennent disponibles, par conséquent, Profil Technology et Bitdefender recommandent que vous consultiez régulièrement notre site "Produits" à l'adresse suivante : http://www.bitdefender.fr pour des mises à jour, ou notre site internet de FAQ à l'adresse http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/.

Tout dommage direct, indirect, spécial, accidentel ou conséquent en relation avec l'usage des informations fournies ne peuvent pas être imputés à Profil Technology et Bitdefender.

Si une intervention sur site est nécessaire, l'analyste vous donnera de plus amples instructions concernant votre revendeur le plus proche.

26. RESSOURCES EN LIGNE

De nombreuses ressources en ligne sont disponibles pour vous aider à résoudre vos questions et problèmes liés à Bitdefender.

- Centre de Support de Bitdefender :

  http://www.bitdefender.fr/support/consumer.html

- Forum du Support Bitdefender :

  http://forum.bitdefender.com/index.php?showforum=59

- le portail de sécurité informatique Bitdefender blog :

  http://www.bitdefender.fr/blog/

Vous pouvez également utiliser votre moteur de recherche favori pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

26.1. Centre de Support de Bitdefender

Le Centre de Support de Bitdefender est une base en ligne d'informations concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus et constatés par le support technique, les équipes de réparation des bugs de Bitdefender. Ainsi que des articles généraux sur la prévention antivirus, la gestion des solutions Bitdefender, des informations détaillées et beaucoup d'autres articles.

Le Centre de Support de Bitdefender est accessible au public et consultable gratuitement. Cet ensemble d'informations est une autre manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'informations ou de rapports de bugs provenant de clients Bitdefender trouvent une réponse dans le Centre de Support Bitdefender, comme les rapports de corrections de bugs, les solutions de rechange, ou les articles d'informations venant compléter les fichiers d'aide des produits.

Le Centre de Support de Bitdefender est disponible en permanence sur

http://www.bitdefender.fr/support/consumer.html.

26.2. Forum du Support Bitdefender

Le Forum du Support Bitdefender fournit aux utilisateurs de Bitdefender une manière simple d'obtenir de l'aide et d'aider les autres.

Si votre produit Bitdefender ne fonctionne pas correctement, s'il ne peut pas supprimer certains virus de votre ordinateur ou si vous avez des questions sur son mode de fonctionnement, exposez votre problème ou posez vos questions sur le forum.

Les techniciens du support Bitdefender surveillent le forum à la recherche de nouvelles publications afin de vous aider. Vous pouvez également obtenir une réponse ou une solution d'un utilisateur Bitdefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de Bitdefender est disponible à http://forum.bitdefender.com/index.php?showforum=59, dans 5 langues différentes : français, anglais, allemand, espagnol et roumain. Cliquez sur le lien **Protection des indépendants & des petites entreprises** pour accéder à la section dédiée aux produits de consommation.

26.3. Portail Bitdefender blog

Bitdefender blog comprend de nombreuses informations sur la sécurité informatique. Vous pouvez découvrir ici les différentes menaces auxquelles votre ordinateur est exposé lorsqu'il est connecté à Internet (malwares, phishing, spam, cybercriminels).

De nouveaux articles sont régulièrement publiés pour vous tenir au courant des dernières menaces découvertes, des tendances actuelles en matière de sécurité et vous fournir encore d'autres informations sur le secteur de la sécurité informatique.

La page web de Bitdefender blog est http://www.bitdefender.fr/blog/.

27. POUR NOUS JOINDRE

Une communication efficace est la clé d'une relation réussie. Au cours des dix dernières années, BITDEFENDER s'est bâti une réputation incontestable dans sa recherche constante d'amélioration de la communication pour dépasser les attentes de ses clients et de ses partenaires. N'hésitez pas à nous contacter pour toute question.

27.1. Adresses Web

Ventes : bitdefender@profiltechnology.com
Centre de support :http://www.bitdefender.fr/support/consumer.html
Documentation : documentation@bitdefender.com
Distributeurs locaux : http://www.bitdefender.fr/partenaires/trouver-un-partenaire.html
Programme de partenariat : partners@bitdefender.com
Relations médias : pr@bitdefender.com
Emplois : jobs@bitdefender.com
Soumissions de virus : virus_submission@bitdefender.com
Envoi de spams : spam_submission@bitdefender.com
Signaler un abus : abuse@bitdefender.com
Site web : http://www.bitdefender.fr

27.2. Distributeurs locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Allez à http://www.bitdefender.fr/partenaires/trouver-un-partenaire.html.
2. Choisissez vos pays et ville à l'aide des options correspondantes.
3. Si vous ne trouvez pas de distributeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse sales@gdata.de. Merci de nous contacter par email pour optimiser le traitement de votre demande.

27.3. Bureaux de Bitdefender

Les bureaux de Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux. Leur adresse respective et contacts sont listés ci-dessous.

France

Profil Technology
49, Rue de la Vanne
92120 Montrouge
Téléphone : +33 (0)1 47 35 72 73
Ventes : bitdefender@profiltechnology.com
Support technique : http://www.bitdefender.fr/site/Main/nousContacter
Site Web : http://www.bitdefender.fr

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Téléphone (services administratif et commercial) : 1-954-776-6262
Ventes : sales@bitdefender.com
Support technique : http://www.bitdefender.com/support/consumer.html
Site Web : http://www.bitdefender.com

Allemagne

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Service administratif : +49 2304 9 45 - 162
Fax : +49 2304 9 45 - 169
Ventes : vertrieb@bitdefender.de
Support technique : http://www.bitdefender.de/support/consumer.html
Site Web : http://www.bitdefender.de

Espagne

Bitdefender España, S.L.U.

C/Bailén, 7, 3-D
08010 Barcelona
Fax : +34 93 217 91 28
Téléphone : +34 902 19 07 65
Ventes : comercial@bitdefender.es
Support technique : http://www.bitdefender.es/support/consumer.html
Site Web : http://www.bitdefender.es

Roumanie

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax : +40 21 2641799
Téléphone du service commercial : +40 21 2063470
Email du service commercial : sales@bitdefender.ro
Support technique : http://www.bitdefender.ro/support/consumer.html
Site Web : http://www.bitdefender.ro

Émirats arabes unis

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Téléphone du service commercial : 00971-4-4588935 / 00971-4-4589186
Email du service commercial : mena-sales@bitdefender.com
Support technique : http://www.bitdefender.com/support/consumer.html
Site Web : http://www.bitdefender.com

Glossaire

Abonnement

Achetez une licence qui donne à l'utilisateur le droit d'utiliser un produit ou service particulier sur un nombre spécifique d'appareils et pour un certain laps de temps. Un abonnement expiré peut être renouvelé automatiquement en utilisant les informations données par l'utilisateur lors du premier achat.

ActiveX

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour créer des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent poser ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est connu pour son manque total de commandes de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Advanced Persistent Threats (menaces persistantes avancées)

Les Advanced persistent threat (APT) exploitent les vulnérabilités des systèmes pour voler des informations importantes et les livrer à la source. Les grands groupes tels que les entreprises, les sociétés ou les gouvernements sont ciblés par ce malware.

L'objectif d'une Advanced persistent threat est de passer inaperçue pendant le plus de temps possible, tout en surveillant et regroupant des informations importantes sans endommager les machines ciblées. La méthode utilisée pour injecter le virus dans le réseau consiste à faire ouvrir un fichier PDF ou un document Office qui a l'air inoffensif, pour que chaque utilisateur puisse exécuter les fichiers.

Adware

Les adwares sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces adwares étant généralement installés une fois que l'utilisateur en a accepté le principe

dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant, les « pop up » publicitaires peuvent devenir contrariants et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des termes de l'accord de licence.

Applet Java

Il s'agit d'un programme Java conçu pour s'exécuter uniquement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Backdoor

Il s'agit d'une faille dans la sécurité d'un système délibérément laissée en place par des développeurs ou des personnes chargées de la maintenance. Les intentions ne sont pas toujours malveillantes ; quelques systèmes d'exploitation, par exemple, permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Chemin

Directions exactes vers un fichier d'un ordinateur. Ces directions sont généralement décrites par arborescence, de haut en bas.

La connexion entre deux points, comme le canal de communication entre deux ordinateurs.

Client de messagerie

Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (courriels).

Code d'activation

Clé unique qui peut être achetée chez un revendeur et utilisée pour activer un produit ou service spécifique. Un code d'activation permet l'activation de l'abonnement valide pour un certain laps de temps et pour certains appareils, et peut également être utilisé pour prolonger un abonnement avec pour seule condition d'être utilisé pour le même produit ou service.

Cookies

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (le code barres se trouvant au dos des produits). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Dossier de démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage de l'ordinateur. Par exemple, un écran de démarrage, un fichier son pour le démarrage de l'ordinateur, un calendrier, des programmes, peuvent être placés dans ce dossier. C'est généralement un raccourci vers le fichier qui est placé dans le dossier, et pas le fichier.

E-mail

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme le manque de mémoire.

Extension de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS-DOS. Elles comportent communément une à trois lettres (certains anciens OS n'en supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Fausse alerte

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Fichier journal (Log)

Fichier qui enregistre les actions ayant eu lieu. Bitdefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Hameçonnage

Action d'envoyer un courriel à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du courriel. Cet courriel oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Heuristique

Méthode basée sur des règles permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter

les variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Keylogger

Application qui enregistre tout ce qui est tapé.

Les keyloggers ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros de sécurité sociale).

Lecteur de disque

C'est un appareil qui lit et écrit des données sur un disque.

Une unité de disque dur lit et écrit sur un disque dur.

Un lecteur de disquette accède à des disquettes.

Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Logiciel espion

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels sharewares ou freewares pouvant être téléchargés sur Internet. Notons toutefois que la plupart des applications sharewares ou freewares ne comportent pas de spywares. Une fois installé, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement ces informations à une tierce personne. Les logiciels espions peuvent également récupérer des informations sur les adresses courriel, les mots de passe ou même, les numéros de cartes de crédit.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'être victime de spywares est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les spywares volent les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

Mettre à jour

Nouvelle version d'un logiciel ou d'un produit hardware, destinée à remplacer une version antérieure du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, et si ce n'est pas le cas, la mise à jour ne se fait pas.

Bitdefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les principaux navigateurs comprennent Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Ce sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.

Non-heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être un virus et ne génère donc pas de fausses alertes.

Photon

Photon est une technologie Bitdefender innovante et discrète, conçue pour limiter l'impact de la protection antivirus sur les performances. En surveillant l'activité de votre PC en tâche de fond, elle crée des modèles d'utilisation qui aident à optimiser les processus de démarrage et d'analyse.

Port

Une interface sur un ordinateur auquel vous pouvez connecter un appareil. Les ordinateurs comportent plusieurs sortes de ports. Il existe plusieurs ports internes permettant de connecter des lecteurs de disques, des écrans et des claviers. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Pourriel

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des courriels non sollicités.

Programmes empaquetés

Fichier dans un format compressé. Beaucoup de systèmes d'exploitation et d'applications contiennent des commandes vous permettant de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide" à la suite. Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui compresse des fichiers remplace la série d'espaces par un caractère spécial pour les séries d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. Il s'agit d'une technique de compression - il en existe plusieurs autres.

Ransomware

Le ransomware est un programme malveillant qui essaye de soutirer de l'argent aux utilisateurs en fermant leur système vulnérable. CryptoLocker, CryptoWall, et TeslaWall n'en sont que des variantes qui recherchent les systèmes personnels des utilisateurs.

L'infection peut se répandre via e-mail, le téléchargement de pièces jointes, ou l'installation d'applications, sans prévenir l'utilisateur de ce qui se passe dans son système. Les utilisateurs quotidiens et les entreprises sont ciblées par les pirates ransomwares.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant un accès de niveau administrateur à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs système.

Le principal rôle des rootkits est de masquer des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des logs et passer inaperçus.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur de boot :

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge le système d'exploitation.

Signature de virus

La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.

TCP/IP

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Télécharger

Copie des données (généralement un fichier entier) d'une source principale vers un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. Contrairement aux virus, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout aussi destructeurs. Un des types de chevaux de Troie les plus insidieux est un logiciel qui prétend désinfecter votre PC mais qui au lieu de cela l'infecte.

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Utilisation de la Mémoire

Zones de stockage internes dans l'ordinateur. Le terme mémoire définit le stockage de données sous la forme de composants électroniques, le mot stockage étant utilisé pour définir le stockage de données sur bande magnétique ou disques amovibles. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Ver

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure de sa propagation. Il ne peut pas se joindre à d'autres programmes.

Virus

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des virus peuvent également se répliquer. Tous les virus informatiques sont créés par des personnes. Un virus simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Virus de boot

Virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Virus Macro

Type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Virus polymorphique

Virus qui change de forme avec chaque fichier qu'il infecte. Ces virus n'ayant pas de forme unique bien définie, ils sont plus difficiles à identifier.

Zone de notification

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.