Bitdefender ANTIVIRUS PLUS

MANUEL D'UTILISATION

Bitdefender Antivirus Plus
Manuel d'utilisation

Date de publication 19/07/2020

Mentions légales

Bitdefender

Table des matières

INSTALLATION

1. PRÉPARATION DE L'INSTALLATION

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

- Vérifiez que l'appareil sur lequel vous prévoyez d'installer Bitdefender dispose de la configuration requise. Si l'appareil ne dispose pas de la configuration 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'appareil en utilisant un compte administrateur.
- Désinstallez tous les autres logiciels similaires sur l'appareil. Si un logiciel est détecté pendant le processus d'installation de Bitdefender, vous recevrez une notification pour le désinstaller. 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 appareil soit connecté à Internet pendant l'installation, même pour une installation à partir d'un CD/DVD. Si des versions plus récentes des fichiers d'applications du logiciel d'installation sont disponibles, Bitdefender peut les télécharger et les installer.

2. CONFIGURATION REQUISE

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

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

- 2,5 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- 2 Go de mémoire (RAM)

Important
Les performances système peuvent être impactées sur les appareils équipés d'anciennes générations de processeurs.

Note
Pour connaître le système d'exploitation Windows de votre appareil et obtenir des informations sur le matériel :

- Dans **Windows 7**, faites un clic droit sur **Poste de travail** sur le bureau, puis sélectionnez **Propriétés** dans le menu.
- Dans **Windows 8**, 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. Dans **Windows 8.1**, localisez **Ce PC**.

  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 logicielle requise

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

- Microsoft Edge 40 et supérieur
- Internet Explorer 10 ou version supérieure
- Mozilla Firefox 51 et version supérieure

- Google Chrome 34 et supérieur

3. INSTALLER BITDEFENDER

Vous pouvez installer Bitdefender à partir du disque d'installation ou en téléchargeant le programme depuis Bitdefender Central.

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

3.1. Installation depuis Bitdefender Central

A partir de Bitdefender Central vous pouvez télécharger le kit d'installation correspondant à l'abonnement auquel vous avez souscrit. Une fois le processus d'installation terminé, Bitdefender Antivirus Plus est activé.

Pour télécharger Bitdefender Antivirus Plus depuis Bitdefender Central:

1. Accéder à Bitdefender Central.
2. Sélectionnez le panneau **Mes appareils**, puis cliquez sur **INSTALLER LA PROTECTION**.
3. Sélectionnez l'une des deux actions disponibles :
   - **Protéger cet appareil**
     a. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
     b. Enregistrez le fichier d'installation.
   - **Protéger d'autres appareils**
     a. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
     b. Cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**.
     c. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR COURRIEL**.

Attention, le lien de téléchargement généré ne sera valide que pendant 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes instructions.

d. Depuis l'appareil sur lequel vous voulez installer votre produit Bitdefender, consultez la boite de messagerie que vous avez précédemment saisie, et cliquez sur le bouton de téléchargement.

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

Validation de l'installation

Bitdefender vérifie 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(e) des éléments devant être mis à niveau avant de pouvoir poursuivre.

Si une solution de sécurité 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'appareil pour terminer la désinstallation des solutions de sécurité détectées.

Le paquet d'installation de Bitdefender Antivirus Plus 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'affiche. Suivez les étapes pour installer Bitdefender Antivirus Plus.

Étape 1 - Installation de Bitdefender

Pour poursuivre l'installation, vous devez accepter les Conditions d'utilisation de l'abonnement. Veuillez prendre le temps de lire les Conditions d'utilisation de l'abonnement, car elles contiennent les termes et conditions dans le cadre desquels vous pouvez utiliser Bitdefender Antivirus Plus.

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

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

- Gardez l'option **Envoyer des rapports sur les produits** 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.
- Sélectionnez la langue dans laquelle vous souhaitez installer le produit.

Cliquez sur **INSTALLER** pour démarrer la procédure d'installation de votre produit Bitdefender.

Étape 2 - Installation en cours

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

Étape 3 - 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.

Étape 4 - Analyse de l'appareil

Vous allez maintenant être invité(e) à effectuer une analyse de votre appareil, afin de vérifier qu'il est protégé. Lors de cette étape, Bitdefender va analyser les zones critiques du système. Cliquez sur **Commencer l'analyse de l'appareil** pour lancer l'analyse.

Vous pouvez masquer l'interface d'analyse en cliquant sur **Exécuter l'analyse en arrière-plan**. Après cela, choisissez si vous souhaitez ou non être informé(e) une fois que l'analyse sera terminée.

Une fois l'analyse terminée, cliquez sur **Ouvrir l'Interface Bitdefender**.

Note

Sinon, si vous ne souhaitez pas effectuer l'analyse, vous pouvez simplement cliquer sur **Passer**.

Étape 5 - Pour commencer

Dans la fenêtre **Pour commencer**, vous pouvez consulter les détails de votre abonnement en cours.

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

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.

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.

Si votre connexion internet est lente, ou que votre système n'est pas connecté à internet, cliquez sur le bouton **Installer à partir du CD/DVD**. Dans ce cas, le produit Bitdefender disponible sur le disque sera installé et une version plus récente sera téléchargée à partir des serveurs Bitdefender via la mise à jour des produits.

Validation de l'installation

Bitdefender vérifie 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(e) des éléments devant être mis à niveau avant de pouvoir poursuivre.

Si une solution de sécurité 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'appareil pour terminer la désinstallation des solutions de sécurité détectées.

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'affiche. Suivez les étapes pour installer Bitdefender Antivirus Plus.

Étape 1 - Installation de Bitdefender

Pour poursuivre l'installation, vous devez accepter les Conditions d'utilisation de l'abonnement. Veuillez prendre le temps de lire les Conditions d'utilisation de l'abonnement, car elles contiennent les termes et conditions dans le cadre desquels vous pouvez utiliser Bitdefender Antivirus Plus.

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

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

- Gardez l'option **Envoyer des rapports sur les produits** 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.
- Sélectionnez la langue dans laquelle vous souhaitez installer le produit.

Cliquez sur **INSTALLER** pour démarrer la procédure d'installation de votre produit Bitdefender.

Étape 2 - Installation en cours

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

Étape 3 - 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.

Étape 4 - Analyse de l'appareil

Vous allez maintenant être invité(e) à effectuer une analyse de votre appareil, afin de vérifier qu'il est protégé. Lors de cette étape, Bitdefender va analyser

les zones critiques du système. Cliquez sur **Commencer l'analyse de l'appareil** pour lancer l'analyse.

Vous pouvez masquer l'interface d'analyse en cliquant sur **Exécuter l'analyse en arrière-plan**. Après cela, choisissez si vous souhaitez ou non être informé(e) une fois que l'analyse sera terminée.

Une fois l'analyse terminée, cliquez sur **Poursuivre avec la création d'un compte**.

Note
Sinon, si vous ne souhaitez pas effectuer l'analyse, vous pouvez simplement cliquer sur **Passer**.

Étape 5 - compte Bitdefender

Une fois que vous avez fini le paramétrage initial, la fenêtre compte Bitdefender apparaît. Un compte Bitdefender est nécessaire pour activer le produit et utiliser ses fonctionnalités en ligne. Pour plus d'informations, reportez-vous à « *Bitdefender Central* » (p. 31).

Procédez selon votre situation.

- **Je souhaite créer un compte Bitdefender**

  1. Tapez les informations requises dans les champs correspondants. Les informations fournies resteront confidentielles. Le mot de passe doit compter au moins 8 caractères, et au moins un chiffre ou symbole et des caractères en majuscule et en minuscule.
  2. Pour continuer, vous devez accepter les Conditions d'utilisation. Lisez attentivement nos Conditions d'utilisation car elles contiennent les termes et conditions selon lesquels vous pouvez utiliser Bitdefender.

     Vous pouvez également consulter notre Politique de confidentialité.
  3. Cliquez sur **Créer un compte**.

     Note
     Une fois le compte créé, vous pouvez utiliser l'adresse e-mail et le mot de passe indiqués pour vous connecter à votre compte sur https://central.bitdefender.com, ou via l'application Bitdefender Central si elle est installée sur un de vos appareils Android ou iOS. Pour installer l'application Bitdefender Central sur Android, rendez-vous sur Google Play, recherchez Bitdefender Central, puis appuyez sur le bouton d'installation. Pour installer l'application Bitdefender Central sur iOS, rendez-vous sur

l'App Store, recherchez Bitdefender Central, puis appuyez sur le bouton d'installation.

- **J'ai déjà un compte Bitdefender**

  1. Cliquez sur **Se connecter**.
  2. Saisissez l'adresse e-mail dans le champ correspondant, puis cliquez sur **SUIVANT**.
  3. Saisissez votre mot de passe puis cliquez sur **CONNEXION**.

     Si vous avez oublié le mot de passe de votre compte ou que vous souhaitez simplement reconfigurer celui déjà existant :

     a. cliquez sur le lien **Mot de passe oublié**.

     b. Saisissez votre adresse e-mail, puis cliquez sur **SUIVANT**.

     c. Consultez votre boite e-mail, saisissez le code de sécurité que vous venez de recevoir, et cliquez sur **SUIVANT**.

     Vous pouvez aussi cliquer sur **Changer de mot de passe** dans l'e-mail que nous vous avons envoyé.

     d. Saisissez votre nouveau mot de passe, puis confirmez-le. Cliquez sur **Enregistrer**.

     Note
     Si vous possédez déjà un compte MyBitdefender, vous pouvez l'utiliser afin de vous connecter à votre compte Bitdefender. Si vous avez oublié votre mot de passe, cliquez tout d'abord sur le lien https://my.bitdefender.com afin de le réinitialiser. Ensuite, utilisez les nouveaux identifiants pour vous connecter à votre compte Bitdefender.

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

  Pour vous connecter à l'aide de votre compte Microsoft, Facebook ou Google :

  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 - Activer votre produit

Note
Cette étape apparaît si vous avez choisi de créer un nouveau compte Bitdefender lors de l'étape précédente, ou si vous vous êtes connecté en utilisant un compte lié à un abonnement ayant expiré.

Une connexion internet active est nécessaire pour terminer l'enregistrement de votre produit.

Procédez selon votre situation :

- J'ai un code d'activation

  Dans ce cas, enregistrez le produit en procédant comme suit :

  1. Saisissez le code d'activation dans le champ **J'ai un code d'activation** puis cliquez sur **CONTINUER**.

     Note
     Pour trouver votre code d'activation :
     - sur l'étiquette du CD ou DVD.
     - sur le manuel du produit.
     - sur le courriel de confirmation d'achat en ligne.

  2. **Je veux évaluer la Bitdefender**

     Dans ce cas, vous pouvez utiliser le produit pendant une période de 30 jours. Pour commencer la période d'essai, sélectionnez **Je n'ai pas d'abonnement, je souhaite essayer le produit gratuitement** puis cliquez sur **CONTINUER**.

Étape 7 - Pour commencer

Dans la fenêtre **Pour commencer** vous pouvez vérifier les détails de votre abonnement actuel.

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

INTRODUCTION

4. FONCTIONS DE BASE

Une fois Bitdefender Antivirus Plus installé, votre apareil est protégé contre tous les types de menaces (tels que les programmes malveillants, logiciels espion, rançongiciels, exploits, botnets et chevaux de Troie).

L'application utilise la technologie Photon pour améliorer la vitesse et les performances du processus d'analyse des menaces. 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.

La connexion à des réseaux sans-fil publics tels que ceux des aéroports, des commerces, des cafés ou des hôtels, sans protection peut s'avérer dangereux pour votre appareil et vos données. Le principal risque est que des pirates surveillent vos activités et découvrent le moment optimal pour voler vos données personnelles. En outre, tout le monde peut voir votre adresse IP, rendant ainsi votre machine vulnérable à de futures cyberattaques. Pour éviter de vous retrouver dans cette situation délicate, vous pouvez installer et utiliser l'application « *VPN* » (p. 130).

Vous pouvez retenir vos mots de passe et comptes en ligne en les enregistrant dans « *Le Password Manager protège vos identifiants* » (p. 119) un Wallet. Avec un seul mot de passe maître, vous pouvez protéger votre vie privée des intrus susceptibles de s'en prendre à votre argent.

Pour vous préserver de potentiels espions lorsque votre appareil est connecté à un réseau sans fil non sécurisé, Bitdefender analyse son niveau de sécurité, et si nécessaire, propose des recommandations pour améliorer la sécurité de vos activités en ligne. Pour des instructions sur comment protéger vos données personnelles, veuillez vous référer à votre « *Sécurité du Wi-Fi* » (p. 111).

Les fichiers chiffrés par un ransomware peuvent maintenant être récupérés sans avoir à payer de demande de rançon. Pour en savoir plus sur la manière de récupérer vos fichiers chiffrés, rendez-vous sur« *Remédiation des ransomwares* » (p. 116).

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* » (p. 141).

Bitdefender prendra pour vous la plupart des décisions de sécurité et affichera rarement des alertes contextuelles. Des détails sur les actions prises et des informations sur le fonctionnement du programme sont disponibles dans la fenêtre Notifications. Pour plus d'informations, reportez-vous à « *Notifications* » (p. 16).

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 appareil et vos données.

Pour utiliser les fonctionnalités en ligne de Bitdefender Antivirus Plus et gérez vos abonnements et appareils, accédez à votre compte Bitdefender. Pour plus d'informations, reportez-vous à « *Bitdefender Central* » (p. 31).

La section « Comment faire pour » (p. 48) 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. 152) 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, cliquez sur l'icône présente sur votre bureau.

Si nécessaire, vous pouvez également suivre les étapes ci-dessous :

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

  Localisez Bitdefender 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. 21).

4.2. Notifications

Bitdefender tient un journal détaillé des événements concernant son activité sur votre appareil. 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 nouveau courriel arrive dans votre boîte de réception.

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

Pour accéder au journal des Notifications, cliquez sur **Notifications** dans le menu de navigation de l'interface de Bitdefender. Chaque fois qu'un événement critique se produit, un compteur apparaît dans l'icône .

Selon leur type et leur gravité, les notifications sont regroupées en :

- 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.

Cliquez sur chaque onglet pour obtenir plus de détails sur les événements générés. De brefs détails sont affichés en un clic sur chaque titre d'événement, à savoir : une courte description, l'action effectuée par Bitdefender lorsqu'il s'est produit, et la date et l'heure a laquelle il s'est produit. Des options peuvent être proposées pour effectuer d'autres actions, si nécessaire.

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

4.3. Profils

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.

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.

Profil Wi-Fi public
: Applique les paramètres du produit afin de bénéficier de la protection complète lorsque vous êtes connecté à un réseau sans fil non sécurisé.

Profil Mode batterie
: Applique les paramètres du produit et limite l'activité en arrière-plan afin d'économiser la durée de vie de la batterie.

4.3.1. Configurer l'activation automatique des profils

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

La première fois que vous accéderez aux **Profils**, il vous sera demandé d'activer les profils automatiques. Pour ce faire, cliquez simplement sur le bouton **ACTIVER** dans la fenêtre qui s'affiche.

Vous pouvez cliquer sur **PAS MAINTENANT** si vous souhaitez activer la fonctionnalité plus tard.

Pour permettre à Bitdefender d'activer les profils automatiquement :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton pour activer l'**Activation automatique des profils**.

Si vous ne souhaitez pas que les Profils soient activés automatiquement, désactivez le bouton.

Pour activer manuellement un profil, cliquez sur le bouton correspondant. Seul un des trois premiers profils peut être activé manuellement à la fois.

Pour plus d'informations sur les profils, reportez-vous à « *Profils* » (p. 141)

4.4. 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 appareil, il vous est recommandé de protéger vos paramètres de Bitdefender par un mot de passe.

Pour configurer la protection par mot de passe pour les paramètres de Bitdefender :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Dans la fenêtre **Généraux**, activez la **Protection par mot de passe**.

3. Saisissez 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 :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Dans la fenêtre **Généraux**, désactivez la **Protection par mot de passe**.
3. Saisissez le mot de passe puis cliquez sur **OK**.

Note

Pour modifier le mot de passe de votre produit, cliquez **Changer de mot de passe**. Entrez votre mot de passe actuel puis cliquez sur **OK**. Dans la nouvelle fenêtre, saisissez le nouveau mot de passe que vous voulez utiliser à partir de maintenant pour restreindre l'accès à vos réglages de Bitdefender.

4.5. Rapports sur les produits

Les rapports sur les produits contiennent des informations sur la manière d'utiliser le produit Bitdefender que vous avez installé. 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 comportent aucune donnée confidentielle, comme votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Si, pendant le processus d'installation, vous avez choisi d'envoyer ces rapports aux serveurs de Bitdefender, mais que vous avez changé d'avis :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Avancé**.
3. Désactivez les **Rapports sur les produits**.

4.6. Notifications sur les promotions

Le produit Bitdefender est configuré pour vous informer des offres promotionnelles disponibles via une fenêtre contextuelle. Cela vous donne la possibilité de bénéficier de tarifs avantageux et de protéger vos appareils plus longtemps.

Pour activer ou désactiver les notifications sur les promotions :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Dans la fenêtre **Généraux**, activez ou désactivez le bouton correspondant.

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

5. INTERFACE DE BITDEFENDER

Bitdefender Antivirus Plus 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 parcourir l'interface de Bitdefender, un assistant d'introduction présentant des informations sur la manière d'interagir et de configurer le produit est affiché dans la partie supérieure gauche. Cliquez sur la flèche pour continuer à être guidé, ou sur **Passer le tour** pour fermer l'assistant.

L'icône de la zone de notification Bitdefender est disponible à tout moment, que vous souhaitiez ouvrir la fenêtre principale, réaliser une mise à jour, ou consulter les informations relatives à la version installée.

La fenêtre principale vous donne des informations sur l'état de votre sécurité. En fonction de votre utilisation de l'appareil et de vos besoins, l'Autopilot affiche ici divers types de recommandations pour vous aider à améliorer la sécurité et les performances de votre appareil. En outre, vous pouvez ajouter les actions rapides que vous utilisez le plus fréquemment, pour toujours les avoir sous la main.

Depuis le menu de navigation situé à gauche, vous pouvez accéder aux paramètres, aux notifications et aux rubriques Bitdefender sur la configuration détaillée et les tâches administratives avancées.

Depuis la partie supérieure de l'interface principale, vous pouvez accéder à votre compte Bitdefender. Vous pouvez également nous contacter pour obtenir de l'aide si vous avez des questions ou si vous rencontrez une situation anormale.

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 apparaisse en permanence :

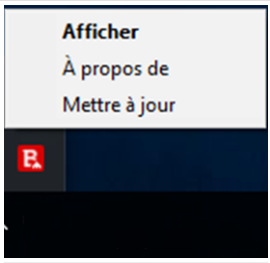
- Dans **Windows 7, Windows 8 et Windows 8.1** :
  1. Cliquez sur la flèche dans l'angle inférieur droit de l'écran.

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 **Paramètres de la barre des tâches**.
2. Faites défiler le menu déroulant et cliquez sur le lien **Sélectionner les icônes apparaissant dans la barre des tâches** situé sous **Zone de notification**.
3. Activez le bouton à côté de **Bitdefender agent**.

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

- **Afficher** - ouvre la fenêtre principale de Bitdefender.
- **À propos** - ouvre une fenêtre sur laquelle vous trouverez des informations sur Bitdefender, où trouver de l'aide en cas d'imprévu, où consulter les Conditions d'utilisation de l'abonnement, les composants de tiers et la Politique de confidentialité.
- **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.

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

Aucun problème n'affecte la sécurité de votre système.
D'importants problèmes affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.

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. Menu de navigation

Le menu de navigation, situé à gauche de l'interface de Bitdefender, vous permet de rapidement accéder aux fonctionnalités et outils de Bitdefender dont vous avez besoin pour utiliser votre produit. Les onglets disponibles dans cette zone sont les suivants :

- **Tableau de bord**. D'ici, vous pouvez rapidement corriger les problèmes de sécurité, voir des recommandations adaptées aux besoins de votre système et à vos habitudes d'utilisation, et exécuter des actions rapides.
-
- **Protection**. D'ici, vous pouvez lancer et configurer des analyses antivirus, récupérer des données qui auraient été chiffrées par un ransomware et configurer la protection tout en naviguant sur Internet.
- **Vie privée**. D'ici, vous pouvez créer des gestionnaires de mots de passe pour vos comptes en ligne, effectuer des paiements en ligne dans un environnement sécurisé et ouvrir l'application VPN.
- **Utilitaires**. D'ici, vous pouvez gérer les profils et accéder à la fonctionnalité de Protection des données.
- **Notifications**. Là, vous pouvez accéder aux notifications générées.
- **Configuration**. Ici, vous pouvez accéder aux Paramètres généraux.

Dans la partie supérieure de l'interface principale, vous trouverez les fonctionnalités **Mon compte** et **Assistance**.

- **Assistance**. Ici, lorsque vous avez besoin d'assistance pour régler un problème avec votre Bitdefender Antivirus Plus, vous pouvez contacter le service d'assistance de Bitdefender.
- **Mon compte**. D'ici, vous pouvez accéder à votre compte Bitdefender pour vérifier votre abonnement et effectuer des tâches de sécurité sur les appareils que vous gérez. Les détails à propos du compte Bitdefender et les abonnements en cours sont également disponibles.

5.3. Tableau de bord

La fenêtre du Tableau de bord 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 trois catégories :

Zone de l'état de sécurité
: Ici, vous pouvez consulter l'état de la sécurité de votre appareil.

Autopilot
: Ici, vous pouvez consulter les recommandations de l'Autopilot pour assurer le bon fonctionnement de votre système.

Actions rapides
: Ici, vous pouvez exécuter différentes tâches pour protéger votre système.

5.3.1. Zone de l'état de sécurité

Bitdefender utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre appareil 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.

Lorsque des problèmes affectent la sécurité de votre appareil, l'état affiché en haut de l'interface de Bitdefender devient rouge. L'état affiché indique la nature des problèmes affectant votre système. En outre, l'icône de la zone de notification devient , et si vous faites glisser le curseur de la souris sur l'icône, une fenêtre de notification confirmera la présence de problèmes en attente.

Comme les problèmes détectés sont susceptibles d'empêcher Bitdefender de vous protéger contre les menaces, ou de représenter un risque majeur en matière de sécurité, nous vous recommandons d'y prêter attention et de les corriger au plus vite. Pour corriger un problème, cliquez sur le bouton situé à côté de celui-ci.

5.3.2. Autopilot

Pour assurer une protection efficace peu importe vos activités, la fonction Autopilot de Bitdefender agit comme un conseiller personnel de sécurité. En fonction de vos activités, qu'il s'agisse de travailler, de procéder à des paiements en ligne, de regarder un film, ou de jouer aux jeux de vidéo, Bitdefender Autopilot vous proposera des recommandations contextuelles en fonction de votre utilisation de l'appareil et de vos besoins. Les recommandations peuvent également concerner des mesures que vous devez prendre pour assurer le bon fonctionnement de votre produit.

Pour commencer à utiliser une fonctionnalité suggérée, ou améliorer votre produit, cliquez sur le bouton correspondant.

Désactiver les notifications de l'Autopilot

Pour attirer votre attention aux recommandations de l'Autopilot, le produit Bitdefender est configuré en sorte que les notifications apparaissent par une fenêtre contextuelle.

Pour désactiver les notifications de l'Autopilot :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Dans la fenêtre **Généraux**, désactivez **Affichage de recommandations**.

5.3.3. Actions rapides

Grâce aux actions rapides, vous pouvez rapidement exécuter des tâches jugées importantes pour maintenir la protection de votre système tout en améliorant la manière dont vous travaillez.

Bitdefender propose des actions rapides par défaut qui peuvent être remplacées par celles que vous utilisez fréquemment. Pour remplacer une action rapide :

1. Cliquez l'icône dans le coin supérieur droit de la carte que vous voulez supprimer.
2. Sélectionnez la tâche que vous voulez ajouter à l'interface principale, puis cliquez sur **AJOUTER**.

Les tâches que vous pouvez ajouter à l'interface principale sont les suivantes :

- **Analyse rapide**. Exécuter une analyse rapide pour détecter rapidement les menaces potentiellement présentes sur votre appareil.
- **Analyse du système**. Exécutez une analyse du système pour vérifier qu'aucune menace n'est présente sur votre appareil.
- **Analyse de vulnérabilités**. Analysez votre appareil 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.
- **Assistant de sécurité du Wi-Fi**. Ouvrez la fenêtre de l'Assistant de sécurité du Wi-Fi dans le module Vulnérabilité.
- **Wallets**. Voir et gérer vos Wallets.
- **Ouvrir Safepay**. Ouvrez Bitdefender Safepay™ pour protéger vos données sensibles lorsque vous effectuez des transactions en ligne.
- **Ouvrir le VPN**. Activez le VPN Bitdefender pour ajouter une couche supérieure de protection lorsque vous êtes connecté à Internet.
- **Destructeur de fichiers**. Utiliser l'outil Destructeur de fichiers pour supprimer toute trace de données sensibles de votre appareil.

Pour commencer à protéger d'autres appareils avec Bitdefender:

1. Cliquez sur **Installer sur un autre appareil**.

   Une nouvelle fenêtre s'affiche à l'écran.

2. Cliquez sur **PARTAGER LE LIEN DE TÉLÉCHARGEMENT**.

3. Suivez les étapes figurant à l'écran pour installer Bitdefender.

En fonction de votre choix, les produits Bitdefender suivants seront installés :

- Bitdefender Antivirus Plus pour les appareils Windows.
- Bitdefender Antivirus for Mac pour les appareils macOS.
- Bitdefender Mobile Security pour les appareils sur Android.
- Bitdefender Mobile Security pour les appareils iOS.

5.4. Les rubriques Bitdefender

Le logiciel Bitdefender dispose de trois rubriques divisées en fonctionnalités utiles qui vous aident notamment à travailler, à surfer sur Internet ou à effectuer des paiements en ligne en toute sécurité ainsi qu'à améliorer la rapidité de votre système, et bien plus.

Chaque fois que vous souhaitez accéder aux fonctionnalités pour une raison spécifique ou pour commencer à configurer votre produit, accédez aux icônes suivantes localisées dans le menu de navigation de l'interface Bitdefender:

- Protection
- Vie privée
- Utilitaires

5.4.1. Protection

Dans la rubrique Protection, vous pouvez configurer vos réglages de sécurité avancés, paramétrer les fonctionnalités de Prévention des menaces en ligne, vérifier et réparer les éventuelles vulnérabilités du système et évaluer la sécurité des réseaux sans fil auxquels vous vous connectez.

Les fonctionnalités que vous pouvez gérer dans la rubrique Protection sont les suivantes :

ANTIVIRUS

La protection antivirus est la base de votre sécurité. Bitdefender vous protège en temps réel et à la demande contre toutes sortes de menaces tels que les programmes malveillants, les chevaux de Troie, les logiciels espions, les publiciels, etc.

La fonctionnalité 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. 79).

PRÉVENTION DES MENACES EN LIGNE

La Prévention des menaces en ligne 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, consultez « *Prévention menaces en ligne* » (p. 104).

ADVANCED THREAT DEFENSE

Advanced Threat Defense protège activement votre système des menaces, notamment des ransomwares, logiciels espions et chevaux de Troie, en analysant le comportement des applications installées. Les processus suspects sont identifiés et si nécessaire bloqués.

Pour plus d'informations sur la manière de protéger votre système des menaces, veuillez vous référer à « *Advanced Threat Defense* » (p. 101).

VULNÉRABILITÉ

Le module Vulnérabilité vous aide à maintenir à jour votre système d'exploitation et les applications que vous utilisez régulièrement et à identifier les réseaux sans fil non sécurisés auxquels vous vous connectez. Cliquez sur le bouton **Ouvrir** dans le module de Vulnérabilité pour accéder à ses fonctionnalités.

La fonctionnalité **Analyse de vulnérabilité** vous permet d'identifier les mises à jour critiques de Windows, les mises à jour d'applications, les mots de passe faibles associés à des comptes Windows et les réseaux sans fil non sécurisés. Cliquez sur **Commencer l'analyse** pour effectuer une analyse sur votre appareil.

Cliquez sur **Assistant de sécurité du Wi-Fi** pour visualiser la liste des réseaux sans fil auxquels vous vous connectez, ainsi que notre évaluation de réputation pour chacun d'entre eux et les actions que vous pouvez effectuer pour vous protéger d'éventuels espions.

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

NETTOYAGE DES RANSOMWARES

La fonctionnalité de Rémédiation des ransomwares vous aide à récupérer les fichiers chiffrés par un ransomware.

Pour en savoir plus sur la manière de récupérer vos fichiers chiffrés, rendez-vous sur« *Remédiation des ransomwares* » (p. 116).

5.4.2. Vie privée

La rubrique Vie privée vous permet d'ouvrir l'application VPN Bitdefender, de protéger vos transactions en ligne et de continuer à naviguer sur Internet en toute sécurité.

Les fonctionnalités que vous pouvez gérer dans la rubrique Vie privée sont les suivantes :

VPN

Le VPN sécurise vos activités en ligne et masque votre adresse IP lorsque vous vous connectez à des réseaux sans-fil non sécurisés dans les aéroports, les commerces, les cafés ou les hôtels. Il vous permet en outre d'accéder à des contenus qui ne seraient normalement pas disponibles dans votre région.

Pour plus d'informations sur cette fonctionnalité, reportez-vous à « *VPN* » (p. 130).

PASSWORD MANAGER

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

Pour plus d'informations sur la configuration du Password Manager, consultez « *Le Password Manager protège vos identifiants* » (p. 119).

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.

Pour plus d'informations sur Bitdefender Safepay™, reportez-vous à « *La sécurité Safepay pour les transactions en ligne* » (p. 133).

ANTI-TRACKER

La fonctionnalité Anti-tracker vous aide à éviter les trackers, afin que vos données restent privées lorsque vous naviguez en ligne, tout en réduisant le temps de chargement des sites Internet.

Pour plus d'informations sur la fonctionnalité Anti-tracker, référez-vous à « *Anti-tracker* » (p. 127).

5.4.3. Utilitaires

Protection des données

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

Pour plus d'informations à ce sujet, reportez-vous à « *Protection des données* » (p. 149).

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.

Pour plus d'informations sur cette fonctionnalité, reportez-vous à « *Profils* » (p. 141).

5.5. Changer la langue du produit

L'interface de Bitdefender est disponible en plusieurs langues qu'il est possible de changer en suivant ces instructions :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Dans la fenêtre **Général**, cliquez sur **Changer la langue**.
3. Sélectionnez la langue souhaitée dans la liste puis cliquez sur **ENREGISTRER**.
4. Attendez quelques instants que les paramètres soient appliqués.

6. BITDEFENDER CENTRAL

Bitdefender Central est la plateforme 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 depuis n'importe quel appareil connecté à Internet en vous rendez sur https://central.bitdefender.com, ou directement depuis l'application Bitdefender Central sur les appareils Android et iOS.

Pour installer l'application Bitdefender Central sur vos appareils :

- **Sur Android** - recherchez Bitdefender Central sur Google Play, puis téléchargez et installez l'application. Suivez les étapes requises pour terminer l'installation :
- **Sur iOS** - recherchez Bitdefender Central sur l'App Store, puis téléchargez et installez l'application. Suivez les étapes requises pour terminer l'installation :

Une fois que vous êtes connectés, vous pouvez commencer à faire ce qui suit :

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

6.1. Accès à Bitdefender Central

Il existe plusieurs façons d'accéder à Bitdefender Central:

- À partir de l'interface principale de Bitdefender :

1. Cliquez sur **Mon compte** dans le menu de navigation de l'interface de Bitdefender.
2. Cliquez sur **Se rendre sur Bitdefender Central**.
3. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse courriel et de votre mot de passe.

- 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 Bitdefender à l'aide de votre adresse courriel et de votre mot de passe.
- Depuis votre appareil Android ou iOS :

  Ouvrez l'application Bitdefender Central que vous venez d'installer.

> **Note**
> Ce document reprend les options et instructions disponibles sur la plateforme web.

6.2. Authentification à 2 facteurs

La méthode d'authentification à deux facteurs ajoute une couche de sécurité supplémentaire à votre compte Bitdefender, en requérant un code d'authentification en plus de vos identifiants de connexion. De cette façon, vous préviendrez la prise de contrôle de votre compte et vous préserverez de différents types de cyberattaques, telles que les attaques de type keyloggers, les attaques par force brute, ou les attaques par dictionnaire.

Activer l'authentification à deux facteurs

En activant l'authentification à deux facteurs, vous rendrez votre compte Bitdefender bien plus sûr. Votre identité sera vérifiée chaque fois que vous vous connecterez à partir d'appareils différents, que ce soit pour installer l'un des produits Bitdefender, pour contrôler le statut de votre abonnement ou pour exécuter des tâches à distance sur vos appareils.

Pour activer l'authentification à deux facteurs :

1. Accéder à Bitdefender Central.
2. Cliquez sur l'icône dans l'angle supérieur droit de l'écran.

3. Cliquez sur **Compte Bitdefender** dans le menu coulissant.
4. Sélectionnez l'onglet **Mot de passe et sécurité**.
5. Cliquez sur **Authentification à 2 facteurs**.
6. Cliquez sur **COMMENCER**.

   Choisissez l'une des deux méthodes suivantes :

   - **Application d'authentification** - utilise une application d'authentification pour générer un code chaque fois que vous souhaitez vous connecter à votre compte Bitdefender.

     Si vous souhaitez utiliser une application d'authentification, mais que vous ne savez pas laquelle choisir, nous mettons à votre disposition une liste des applications d'authentification que nous recommandons.

     a. Cliquez sur **UTILISER UNE APPLICATION D'AUTHENTIFICATION** pour commencer.

     b. Pour vous connecter sur un appareil Android ou iOS, utilisez votre appareil pour scanner le QR code.

        Pour vous connecter depuis un ordinateur portable ou depuis un ordinateur de bureau, vous pouvez saisir manuellement le code qui s'affiche.

        Cliquez sur **CONTINUER**.

     c. Saisissez le code fourni par l'application ou celui affiché lors de l'étape précédente, puis cliquez sur **ACTIVER**.

   - **E-mail** - chaque fois que vous vous connecterez à votre compte Bitdefender, un code de vérification vous sera envoyé par e-mail. Consultez votre compte de messagerie, puis saisissez le code que vous avez reçu.

     a. Cliquez sur **UTILISER UNE ADRESSE E-MAIL** pour commencer.

     b. Consultez votre compte de messagerie et saisissez le code fourni.

        Notez que vous disposez de cinq minutes pour consulter votre boîte de réception et saisir le code généré. Passé ce délai, il vous faudra générer un nouveau code en suivant les mêmes étapes.

     c. Cliquez sur **ACTIVER**.

     d. 10 codes d'activation vous sont fournis. Vous pouvez copier, télécharger ou imprimer la liste et l'utiliser en cas d'oubli de votre

adresse e-mail ou d'impossibilité de vous connecter à votre messagerie. Chaque code est à usage unique.

e. Cliquez sur **TERMINÉ**.

Dans le cas où vous souhaiteriez cesser d'utiliser l'authentification à deux facteurs :

1. Cliquez sur **DÉSACTIVER L'AUTHENTIFICATION À 2 FACTEURS**.
2. Consultez votre application ou votre compte de messagerie et saisissez le code que vous avez reçu.

   Dans le cas où vous auriez choisi de recevoir le code d'authentification par e-mail, vous disposez de cinq minutes pour consulter votre boîte de réception et saisir le code généré. Passé ce délai, il vous faudra générer un nouveau code en suivant les mêmes étapes.
3. Confirmez votre choix.

6.2.1. Ajouter des appareils approuvés

Afin de vous assurer que vous seul(e) pourrez accéder à votre compte Bitdefender, nous pouvons commencer par vous demander un code de sécurité. Si vous souhaitez passer cette étape chaque fois que vous vous connectez à partir d'un même appareil, nous vous recommandons de le désigner comme appareil approuvé.

Pour ajouter des appareils aux appareils approuvés :

1. Accéder à Bitdefender Central.
2. Cliquez sur l'icône dans l'angle supérieur droit de l'écran.
3. Cliquez sur **Compte Bitdefender** dans le menu coulissant.
4. Sélectionnez l'onglet **Mot de passe et sécurité**.
5. Cliquez sur **Appareils approuvés**.
6. La liste des appareils sur lesquels Bitdefender est installé s'affiche. Cliquez sur l'appareil de votre choix.

Vous pouvez ajouter autant d'appareils que vous le souhaitez, sous réserve que Bitdefender soit installé sur ces derniers et que votre abonnement soit valide.

6.3. Mes abonnements

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

6.3.1. Vérifier les abonnements disponibles

Pour vérifier vos abonnements disponibles :

1. Accéder à 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, macOS, iOS ou Android).

6.3.2. nouvel appareil

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

1. Accéder à Bitdefender Central.
2. Sélectionnez le panneau **Mes appareils**, puis cliquez sur **INSTALLER LA PROTECTION**.
3. Sélectionnez l'une des deux actions disponibles :
   - **Protéger cet appareil**

     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
   - **Protéger d'autres appareils**

     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.

Cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR COURRIEL**. Attention, le lien de téléchargement généré ne sera valide que pendant 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes instructions.

Depuis l'appareil sur lequel vous voulez installer votre produit Bitdefender, consultez la boite de messagerie que vous avez précédemment saisie, et cliquez sur le bouton de téléchargement.

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

6.3.3. Renouveler abonnement

Si vous avez désactivé le renouvellement automatique de votre abonnement Bitdefender, vous pouvez le renouveler manuellement en suivant ces étapes :

1. Accéder à 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.

6.3.4. Activer abonnement

Un abonnement peut être activé pendant le processus d'installation à l'aide de votre compte Bitdefender. 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 un abonnement avec un code d'activation :

1. Accéder à 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 **ACTIVER** pour poursuivre.

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

6.4. Mes appareils

La zone **Mes Appareils** dans Bitdefender Central vous donne la possibilité d'installer, gérer et exécuter des actions à distance sur votre Bitdefender sur n'importe quel appareil, pourvu qu'il soit allumé et connecté à internet. Les cartes des appareils présentent le nom de l'appareil, l'état de sa protection et s'il court un risque potentiel de sécurité.

Pour voir la liste des appareils triés selon leur état ou utilisateurs, cliquez sur le menu déroulant situé dans le coin supérieur droit de l'écran.

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

1. Accéder à Bitdefender Central.
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur la carte de l'appareil désiré, puis sur l'icône ⋮ dans l'angle supérieur droit de l'écran.
4. Sélectionnez **Configuration**.
5. Saisissez le nouveau nom dans le champ **Nom de l'appareil** puis cliquez sur **ENREGISTRER**.

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

1. Accéder à Bitdefender Central.
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur la carte de l'appareil désiré, puis sur l'icône ⋮ dans l'angle supérieur droit de l'écran.
4. Sélectionnez **Profil**.

5. Cliquez sur **Ajouter un propriétaire**, puis remplissez les champs correspondants. Vous pouvez personnaliser votre profil en ajoutant une photo et en indiquant votre date de naissance.
6. Cliquez sur **AJOUTER** pour sauvegarder le profil.
7. Sélectionnez le propriétaire souhaité à partir de la liste **Propriétaire appareil**, puis cliquez sur **ASSIGNER**.

Pour mettre à jour Bitdefender à distance sur un appareil Windows :

1. Accéder à Bitdefender Central.
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur la carte de l'appareil désiré, puis sur l'icône ⋮ dans l'angle supérieur droit de l'écran.
4. Sélectionner **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**. Sur cette fenêtre, vous pouvez voir des informations détaillées sur l'appareil sélectionné, contrôler l'état de sa sécurité, l'état du VPN de Bitdefender et la quantité de menaces bloquées ces sept derniers jours. Le statut de protection peut être vert lorsqu'aucun problème n'affecte votre appareil, jaune quand un sujet mérite votre attention, ou rouge si l'appareil est en danger. En cas de problème sur l'un de vos appareils, cliquez sur le menu déroulant situé en haut de la zone des états pour obtenir des informations détaillées. 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 Section 14.2.3, « *Exécuter une analyse du système* » et à « *Exécuter une analyse rapide* » (p. 85) .

- **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. Cliquez sur **Plus de détails** pour accéder à un rapport détaillé sur les problèmes trouvés. Pour obtenir plus d'information sur cette fonctionnalité, rendez-vous sur « *Vulnérabilité* » (p. 107).

6.5. Activités

Dans la zone Activité, vous avez accès à des informations sur les appareils sur lesquels Bitdefender est installé.

Une fois que vous avez accédé à la fenêtre **Activité**, les cartes suivantes sont disponibles :

- **Mes appareils**. Vous pouvez ici voir le nombre d'appareils actuellement connectés ainsi que l'état de leur protection. Pour corriger à distance les problèmes sur les appareils connectés, cliquez sur **Corriger les problèmes**, puis sur **ANALYSER ET CORRIGER LES PROBLÈMES**.

  Pour visualiser les détails des problèmes détectés, cliquez sur **Afficher les problèmes**.

  Les informations sur les menaces détectées ne peuvent pas être récupérées sur les appareils iOS.

- **Menaces bloquées**. Vous pouvez ici voir un graphique présentant une statistique générale avec des informations sur les menaces bloquées ces dernières 24 heures et au cours des sept derniers jours. Les informations affichées sont récupérées en fonction du comportement malveillant détecté sur les fichiers, applications et URL.

- **Utilisateurs avec le plus de menaces bloquées**. Ici, vous pouvez visualiser un classement indiquant quels utilisateurs ont été le plus confrontés à des menaces.

- **Appareils avec le plus de menaces bloquées**. Vous pouvez voir ici un classement des appareils sur lesquels le plus de menaces ont été détectés.

6.6. Notifications

L'icône 🔔 vous aide à rester informé des activités des appareils associés à votre compte. Après avoir cliqué sur celle-ci, un aperçu général contenant des informations sur les activités de produits Bitdefender installés sur vos appareils.

7. MAINTENIR BITDEFENDER À JOUR

De nouvelles menaces sont trouvées et identifiées chaque jour. C'est pourquoi il est très important que la base de données d'information sur les menaces de Bitdefender soit à jour.

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 appareil puis toutes les **heures** après cela. Si une mise à jour est détectée, elle est automatiquement téléchargée et installée sur votre appareil.

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 appareil 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. 72).
- 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 manuelles de Bitdefender. Pour plus d'informations, reportez-vous à « *Mise à jour en cours* » (p. 42).

7.1. Vérifier que Bitdefender est à jour

Pour consulter la date de la dernière mise à jour de votre Bitdefender :

1. Cliquez sur **Notifications** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant la dernière mise à jour.

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, faites un clic droit sur l'icône de Bitdefender de la zone de notification puis sélectionnez **Mettre à jour maintenant**.

La fonctionnalité 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 appareil 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 Windows :

1. Accéder à Bitdefender Central.
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur la carte de l'appareil désiré, puis sur l'icône dans l'angle supérieur droit de l'écran.
4. Sélectionner **Mise à jour**.

7.3. Activer ou désactiver la mise à jour automatique

Activer ou désactiver la mise à jour automatique :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Mise à jour**.
3. Activez ou désactivez le bouton correspondant.

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, 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 ajuster les paramètres de mise à jour :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Mise à jour**, 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.

Règles de traitement des mises à jour

À chaque fois qu'une mise à jour est disponible, Bitdefender téléchargera et installera automatiquement la mise à jour, sans aucune notification. Désactivez l'option **Mise à jour silencieuse** si vous voulez être averti à chaque fois qu'une nouvelle mise à jour est disponible.

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'appareil. 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, activez l'option **Notification de redémarrage**.

7.5. Mises à jour continues

Pour être certain d'utiliser la dernière version, votre Bitdefender vérifie automatiquement l'existence de mises à jour de produits. Ces mises à jour peuvent apporter de nouvelles fonctionnalités ou des améliorations, corriger des problèmes du produit, ou permettre de passer automatiquement à une nouvelle version. Lorsqu'une nouvelle version de Bitdefender s'installe via une mise à jour, les réglages personnalisés sont enregistrés et la procédure de désinstallation et de réinstallation sont passé.

Ces mises à jour nécessitent un redémarrage du système pour lancer l'installation de nouveaux fichiers. Lorsqu'une mise à jour du produit est terminée, une fenêtre contextuelle vous demande de redémarrer le système. Si vous manquez cette notification, vous pouvez soit cliquer sur **Redémarrer maintenant** sur la fenêtre Notifications où la mise à jour la plus récente est mentionnée, ou redémarrer manuellement le système.

Note

Les mises à jour contenant de nouvelles fonctionnalités et améliorations ne seront proposées qu'aux utilisateurs ayant Bitdefender 2020 d'installé.

8. ASSISTANCE VOCALE

Que vous utilisiez l'assistant Amazon Alexa ou l'application Google Assistant, vous pouvez configurer des commandes vocales pour exécuter des analyses rapides sur les appareils sur lesquels Bitdefender est installé, ou pour consulter l'état de votre abonnement. Pour voir la liste complète des commandes vocales possibles, rendez-vous sur « *Commandes vocales pour interagir avec Bitdefender* » (p. 46).

8.1. Configurer les commandes vocales

Les commandes vocales de Bitdefender peuvent être configurées pour :

- **Application Google Home**
  - Android 5.0 et supérieur
  - iOS 10.0 et plus
  - Chromebooks
- **Application Amazon Alexa sur**
  - Echo
  - Echo Dot
  - Echo Show
  - Echo Spot
  - Fire TV Cube

Configurer les commandes vocales d'Amazon Alexa pour Bitdefender

Pour configurer les commandes vocales de Bitdefender sur Amazon Alexa :

1. Ouvrez l'application Amazon Alexa.
2. Appuyez sur l'icône **Menu**, puis sur **Skills**.
3. Recherchez Bitdefender.
4. Appuyez sur **Bitdefender** puis sur **ACTIVER**.
5. Il vous est demandé de vous connecter à votre compte Bitdefender.

Saisissez votre nom d'utilisateur et votre mot de passe puis appuyez sur **CONNEXION**.

Dès que la synchronisation de Bitdefender avec Amazon Alexa est terminé, les commandes vocales que vous pouvez utiliser pour commander Bitdefender ou consulter des informations vous sont présentées.

Si vous voulez que l'assistant vous donne la liste de toutes les commandes vocales et skills, dites **AIDE MOI**.

Configurer les commandes vocales de Google Home pour Bitdefender

Pour configurer les commandes vocales sur Google Home :

1. Ouvrez l'application Google Home.
2. Appuyez sur Menu dans le coin supérieur gauche de l'écran accueil, puis appuyez sur **Explorer**.
3. Recherchez Bitdefender.
4. Appuyez sur **Bitdefender** puis sur **Lier**.
5. Il vous est demandé de vous connecter à votre compte Bitdefender.

   Saisissez votre nom d'utilisateur et votre mot de passe puis appuyez sur **CONNEXION**.

Dès que la synchronisation de Bitdefender avec Google Home est terminé, les commandes vocales que vous pouvez utiliser pour commander Bitdefender ou consulter des informations vous sont présentées.

Si vous voulez que l'assistant vous donne la liste de toutes les commandes vocales et skills, dites **AIDE MOI**.

8.2. Commandes vocales pour interagir avec Bitdefender

Pour ouvrir les commandes vocales de Bitdefender :

- Sur Amazon Alexa : **Alexa, ouvre Bitdefender**
- Pour Google Home : **OK, Google, parle avec Bitdefender**

Pour exécuter les commandes vocales de Bitdefender :

- Sur Amazon Alexa : **Alexa, demande à Bitdefender**

- Sur Google Home: **OK, Google, demande à Bitdefender**

Les questions et tâches que vous pouvez initier une fois l'assistant Bitdefender est ouvert sont les suivantes :

Comment est mon activité aujourd'hui?

Quel est le statut de mon abonnement ?

Exécuter une analyse rapide sur mon [type d'appareil]. (un type d'appareil peut être un ordinateur portable ou un ordinateur de bureau).

COMMENT FAIRE POUR

9. INSTALLATION

9.1. Comment installer Bitdefender sur un second appareil ?

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

Pour installer Bitdefender sur un second appareil :

1. Cliquez sur **Installer sur un autre appareil**dans le coin inférieur gauche de l'interface Bitdefender.

   Une nouvelle fenêtre s'affiche à l'écran.

2. Cliquez sur **PARTAGER LE LIEN DE TÉLÉCHARGEMENT**.
3. Suivez les instructions qui apparaissent à l'écran pour installer Bitdefender.

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

9.2. Comment réinstaller Bitdefender ?

Quelques situations typiques nécessitant de réinstaller Bitdefender :

- vous avez réinstallé le système d'exploitation.
- vous voulez résoudre les problèmes qui peuvent être à l'origine de ralentissements et de plantages.
- votre produit Bitdefender ne démarre pas ou ne fonctionne pas correctement.

Dans le cas où vous êtes touchés par une situation mentionnée, suivez les instructions suivantes :

- Dans **Windows 7** :

  1. Cliquez sur **Démarrer** et allez dans **Programmes**.
  2. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
  3. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
  4. Vous aurez besoin de redémarrer l'appareil 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** et sélectionnez **Désinstaller**.
4. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
5. Vous aurez besoin de redémarrer l'appareil 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** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Cliquez sur **RÉINSTALLER**.
6. Vous aurez besoin de redémarrer l'appareil pour terminer le processus.

Note
En suivant la procédure de réinstallation, les réglages personnalisés sont enregistrés et disponibles sur le nouveau produit installé. D'autres réglages peuvent être repassés à leur configuration par défaut.

9.3. 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 appareil à partir de la plateforme Bitdefender Central.

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

Pour installer Bitdefender à partir de Bitdefender Central :

1. Accéder à Bitdefender Central.
2. Sélectionnez le panneau **Mes appareils**, puis cliquez sur **INSTALLER LA PROTECTION**.
3. Sélectionnez l'une des deux actions disponibles :

   - **Protéger cet appareil**

     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.

   - **Protéger d'autres appareils**

     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.

     Cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR COURRIEL**. Attention, le lien de téléchargement généré ne sera valide que pendant 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes instructions.

     Depuis l'appareil sur lequel vous voulez installer votre produit Bitdefender, consultez la boite de messagerie que vous avez précédemment saisie, et cliquez sur le bouton de téléchargement.
4. Exécutez le produit Bitdefender que vous avez installé.

9.4. Comment changer la langue de mon produit Bitdefender ?

L'interface de Bitdefender est disponible en plusieurs langues qu'il est possible de changer en suivant ces instructions :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Dans la fenêtre **Général**, cliquez sur **Changer la langue**.
3. Sélectionnez la langue souhaitée dans la liste puis cliquez sur **ENREGISTRER**.
4. Attendez quelques instants que les paramètres soient appliqués.

9.5. Comment utiliser mon abonnement Bitdefender après une mise à jour 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 devez réinstaller le produit en procédant 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** et sélectionnez **Désinstaller**.
    3. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
    4. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

       Ouvrez l'interface de votre nouveau produit Bitdefender installé pour avoir accès à ses fonctionnalités.

  - 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** et sélectionnez **Désinstaller**.
4. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

   Ouvrez l'interface de votre nouveau produit Bitdefender installé pour avoir accès à ses fonctionnalités.

- Dans **Windows 10** :

1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications**.
3. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
6. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

   Ouvrez l'interface de votre nouveau produit Bitdefender installé pour avoir accès à ses fonctionnalités.

> **Note**
> En suivant la procédure de réinstallation, les réglages personnalisés sont enregistrés et disponibles sur le nouveau produit installé. D'autres réglages peuvent être repassés à leur configuration par défaut.

- 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. Accéder à Bitdefender Central.
   b. Sélectionnez le panneau **Mes appareils**, puis cliquez sur **INSTALLER LA PROTECTION**.
   c. Sélectionnez l'une des deux actions disponibles :
      - **Protéger cet appareil**

Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.

- **Protéger d'autres appareils**

  Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.

  Cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR COURRIEL**. Attention, le lien de téléchargement généré ne sera valide que pendant 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes instructions.

  Depuis l'appareil sur lequel vous voulez installer votre produit Bitdefender, consultez la boite de messagerie que vous avez précédemment saisie, et cliquez sur le bouton de téléchargement.

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).

9.6. Comment puis-je passer à la dernière version de Bitdefender ?

La mise à jour vers la nouvelle version est désormais possible sans suivre la procédure de désinstallation et réinstallation. Plus exactement, le nouveau produit contenant de nouvelles fonctionnalités et des améliorations majeures de produits sont diffusé via la mise à jour du produit, et si vous avez déjà un abonnement actif à Bitdefender, le produit s'active automatiquement.

Si vous utilisez la version 2020, vous pouvez passer à la dernière version en suivant ces instructions :

1. Cliquez sur **REDÉMARRER MAINTENANT** dans la notification que vous avez reçue avec les informations de mise à jour. Si vous l'avez manqué, rendez-vous dans la fenêtre Notifications, sélectionnez la mise à jour la plus récente, puis cliquez sur le bouton **REDÉMARRER MAINTENANT**. Attendez que l'appareil redémarre.

   La fenêtre **Nouveautés** contenant des informations sur les améliorations et nouvelles fonctionnalités apparait.

2. Cliquez sur le lien **En apprendre plus** pour être redirigé vers notre page dédiée avec plus d'informations et d'articles sur le sujet.
3. Fermer la fenêtre **Nouveautés** pour accéder à l'interface de la nouvelle version.

Les utilisateurs souhaitant mettre à niveau gratuitement leur Bitdefender 2016 ou mettre à jour vers la dernière version de Bitdefender doivent supprimer leur version actuelle depuis le Panneau de configuration, puis télécharger le dernier fichier d'installation depuis le site Internet de Bitdefender à l'adresse suivante : http://www.bitdefender.fr/Downloads/. L'activation n'est possible que si un abonnement est actif.

10. BITDEFENDER CENTRAL

10.1. Comment me connecter à un compte Bitdefender avec un autre compte ?

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

Pour vous connecter avec un autre compte Bitdefender :

1. Cliquez sur le nom de votre compte dans la partie supérieure de l'interface Bitdefender.
2. Cliquez sur le bouton **Changer de compte** dans le coin supérieur droit pour changer le compte lié à l'appareil.
3. Saisissez l'adresse e-mail dans le champ correspondant, puis cliquez sur **SUIVANT**.
4. Saisissez votre mot de passe puis cliquez sur **CONNEXION**.

> **Note**
> Le produit Bitdefender de votre appareil change automatiquement selon l'abonnement associé au nouveau compte Bitdefender.
> S'il n'y a pas d'abonnement disponible associé au nouveau compte Bitdefender, ou que vous souhaitez le transférer à partir du compte précédent, vous pouvez contacter le support Bitdefender comme décrit dans la rubrique « *Assistance* » (p. 175).

10.2. Comment désactiver les messages d'aide Bitdefender Central ?

Pour vous aider à comprendre à quoi sert chaque option dans Bitdefender Central, des messages d'aide sont affichés dans le tableau de bord.

Si vous souhaitez ne plus voir ces messages :

1. Accéder à Bitdefender Central.
2. Cliquez sur l'icône dans l'angle supérieur droit de l'écran.
3. Cliquez sur **Mon compte** dans le menu déroulant.
4. Cliquez sur **Paramètres** dans le menu coulissant.

5. Désactivez l'option **Activez/désactivez les messages d'aide**.

10.3. J'ai oublié le mot de passe de mon compte Bitdefender. Comment le réinitialiser ?

Il existe deux manières de définir un nouveau mot de passe pour votre compte Bitdefender :

- À partir de l'interface de Bitdefender :
  1. Cliquez sur **Mon compte** dans le menu de navigation de l'interface de Bitdefender.
  2. Cliquez sur le bouton **Changer de compte** dans le coin supérieur droit.

     Une nouvelle fenêtre apparaît.
  3. Saisissez votre adresse e-mail puis cliquez sur **SUIVANT**.

     Une nouvelle fenêtre apparaît.
  4. cliquez sur le lien **Mot de passe oublié**.
  5. Cliquez sur **SUIVANT**.
  6. Consultez votre boite e-mail, saisissez le code de sécurité que vous venez de recevoir, et cliquez sur **SUIVANT**.

     Vous pouvez aussi cliquer sur **Changer de mot de passe** dans l'e-mail que nous vous avons envoyé.
  7. Saisissez votre nouveau mot de passe, puis confirmez-le. Cliquez sur **Enregistrer**.
- A partir de votre navigateur web :
  1. Allez à : https://central.bitdefender.com.
  2. Cliquez sur **SE CONNECTER**.
  3. Saisissez votre adresse e-mail, puis cliquez sur **SUIVANT**.
  4. cliquez sur le lien **Mot de passe oublié**.
  5. Cliquez sur **SUIVANT**.
  6. Allez voir vos emails et suivez les instructions fournies pour configurer un nouveau mot de passe pour votre compte Bitdefender.

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

10.4. Comment gérer les sessions de connexion de mon compte Bitdefender ?

Dans votre compte Bitdefender, vous pouvez voir les dernières sessions de connexion actives et inactives ouvertes sur les appareils associés à votre compte. Vous pouvez également vous déconnecter à distance en procédant comme suit :

1. Accéder à Bitdefender Central.
2. Cliquez sur l'icône dans l'angle supérieur droit de l'écran.
3. Cliquez sur **Sessions** dans le menu coulissant.
4. Dans la zone **Sessions actives**, sélectionnez l'option **DÉCONNEXION** située à côté de l'appareil dont vous voulez terminer la session de connexion.

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 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.
- Lorsque vous téléchargez des fichiers sur Internet que vous soupçonnez d'être dangereux.
- Analysez un dossier partagé sur le réseau avant de copier des fichiers sur votre appareil.

11.2. Comment analyser mon système ?

Pour réaliser une analyse complète sur le système :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Cliquez sur le bouton **Lancer l'analyse** à côté d'**Analyse 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 appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 90).

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 appareil.

Pour programmer une analyse :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Cliquez sur • • • à côté du type d'analyse que vous souhaitez programmer, Analyse système ou Analyse rapide, dans la partie inférieure de l'interface, puis sélectionnez **Éditer**.

   Sinon, vous pouvez créer un type d'analyse qui correspond à vos besoins en cliquant sur **+Créer une analyse** à côté de **Gérer les analyses**.
4. Personnalisez l'analyse en fonction de vos besoins, puis cliquez sur **Suivant**.
5. Cochez la case à côté de **Choisir quand programmer cette tâche**.

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

   - Au démarrage du système
   - Tous les jours
   - Toutes les semaines
   - Tous les mois

   Pour sélectionner Quotidien, Hebdomadaire ou Mensuel, bougez le curseur le long de l'échelle pour configurer la période durant laquelle l'analyse planifiée doit débuter.

Si vous choisissez de créer une nouvelle analyse personnalisée, la fenêtre **Tâche d'analyse** apparait. D'ici, vous pouvez choisir les emplacements que vous souhaitez analyser.

11.4. Comment créer une tâche d'analyse personnalisée ?

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

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

1. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
2. Cliquez sur **+Créer une analyse** à côté de **Gérer les analyses**.
3. Dans le champ correspondant au nom de la tâche, saisissez un nom pour l'analyse, sélectionnez les emplacements que vous souhaitez analyser, puis cliquez sur **SUIVANT**.
4. Configurez les options générales suivantes :
   - **Analyser uniquement les applications**. Vous pouvez configurer Bitdefender de sorte à analyser uniquement les applications auxquelles vous avez accédé.
   - **Priorité de la tâche d'analyse**. Vous pouvez sélectionner quel impact peut avoir une analyse sur les performances de votre système.
     - Auto - La priorité du processus d'analyse dépendra de l'activité de votre système. Pour veiller à ce que le processus d'analyse ne nuise pas à l'activité du système, Bitdefender décidera si le processus d'analyse doit être exécuté avec une priorité haute ou basse.
     - Haute - La priorité de la tâche d'analyse sera élevée. En choisissant cette option, vous permettez à d'autres programmes de fonctionner plus lentement, et diminuez le temps nécessaire pour que l'analyse soit finie.
     - Basse - La priorité de la tâche d'analyse sera basse. En choisissant cette option, vous permettez à d'autres programmes de fonctionner plus rapidement, et augmentez le temps nécessaire pour que l'analyse soit finie.
   - **Actions post-analyse**. Spécifiez quelle mesure doit être prise par Bitdefender si aucune menace n'a été détectée.
     - Fermer la fenêtre de résumé
     - Éteindre l'appareil

- Fermer la fenêtre d'analyse

5. Si vous souhaitez configurer les options d'analyse en détail, cliquez sur **Afficher les options avancées**.

   Cliquez sur **Suivant**.

6. Si vous le souhaitez, vous pouvez activer l'option **Programmer la tâche d'analyse**, puis choisir le moment où l'analyse personnalisée que vous avez créée devra démarrer.

   - Au démarrage du système
   - Tous les jours
   - Tous les mois
   - Toutes les semaines

   Pour sélectionner Quotidien, Hebdomadaire ou Mensuel, bougez le curseur le long de l'échelle pour configurer la période durant laquelle l'analyse planifiée doit débuter.

7. Cliquez sur **Enregistrer** pour enregistrer les réglages et fermer la fenêtre de configuration.

   En fonction des emplacements à analyser, l'analyse peut prendre quelque temps. Si des menaces sont trouvées pendant le processus d'analyse, il vous sera demandé de sélectionner les actions à appliquer aux fichiers détectés.

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 exceptions 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 un dossier à la liste d'exceptions :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Cliquez sur l'onglet **Paramètres**.
4. Cliquez sur **Gérer les exceptions**.
5. Cliquez sur **+Ajouter une exception**.
6. Saisissez le chemin du dossier que vous souhaitez exclure de l'analyse dans le champ correspondant.

   Sinon, vous pouvez naviguer jusqu'au dossier en cliquant sur le bouton Parcourir situé sur la droite de l'interface, le sélectionner puis cliquer sur **OK**.
7. Activez l'interrupteur situé à côté de la fonctionnalité de protection qui ne devrait pas analyser le dossier. Il existe trois options :
   - Antivirus
   - Prévention menaces en ligne
   - Advanced Threat Defense
8. Cliquez sur **Enregistrer** 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 exceptions de Bitdefender :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
   b. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.

c. Dans la fenêtre **Avancé**, désactivez **Bouclier Bitdefender**.

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. 74).
3. Restaurer le fichier à partir de la zone de quarantaine :
   a. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
   b. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
   c. Ouvrez la fenêtre **Paramètres** puis cliquez sur **Gérer la quarantaine**.
   d. Sélectionnez le fichier, puis 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).

   Par défaut, Bitdefender est programmé pour ajouter automatiquement les fichiers restaurés à la liste des exceptions.
5. Activez la protection antivirus en temps réel de Bitdefender.
6. Contactez les représentants de notre service d'assistance afin que nous puissions supprimer la détection de la mise à jour d'information sur les menaces. Pour savoir comment faire cela, consultez « *Assistance* » (p. 175).

11.7. Comment connaître les menaces détectées 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 vérifier un journal d'analyse ou toute autre infection détectée plus tard :

1. Cliquez sur **Notifications** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant la dernière analyse.

   Cette section vous permet de trouver tous les événements d'analyse des menaces, 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 notifications, vous pouvez consulter les analyses ayant été réalisées récemment. Cliquez sur une notification pour afficher des informations à son sujet.
4. Pour ouvrir un journal d'analyse, cliquez sur **Afficher le journal**.

12. PROTECTION VIE PRIVÉE

12.1. Comment vérifier si 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 garder vos activités en ligne privées et en sécurité :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **SAFEPAY**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Safepay**, cliquez sur **Lancer Safepay**.
4. Cliquez sur le bouton pour accéder au **Clavier virtuel**.

   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 appareil 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. Cliquez sur **Supprimer de façon permanente**, puis confirmez que vous voulez poursuivre cette procédure.

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

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

12.3. Comment restaurer manuellement les fichiers chiffrés en cas d'échec de la procédure de restauration ?

Si les fichiers chiffrés ne peuvent pas être automatiquement restaurés, vous pouvez le faire manuellement en suivant les instructions suivantes :

1. Cliquez sur **Notifications** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification relative au dernier comportement de ransomware détecté, puis cliquez sur **Fichiers chiffrés**.
3. Une liste des fichiers chiffrés apparaît.

   Cliquez sur **Récupérer des fichiers** pour continuer.

4. Si tout ou une partie de la procédure de restauration échoue, vous devez choisir un emplacement où enregistrer les fichiers déchiffrés. Cliquez sur **Emplacement de restauration**, puis choisissez un emplacement sur votre ordinateur.
5. Une fenêtre de confirmation s'affichera.

   Cliquez sur **Terminer** pour achever le processus de restauration.

Les fichiers présentant les extensions suivantes peuvent être restaurés s'ils venaient à être chiffrés :

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

13. INFORMATIONS UTILES

13.1. Comment tester ma solution de sécurité ?

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

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

Pour tester votre solution de sécurité :

1. Téléchargez le test à partir de la page web officielle de l'organisme EICAR http://www.eicar.org/.
2. Cliquez sur l'onglet **Fichier test programmes malveillants**.
3. Cliquez sur **Télécharger** dans le menu de gauche.
4. Dans **zone de téléchargement utilisant le protocole HTTP standard** 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 threat) ».

   Si vous cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**, le téléchargement du test débutera et une fenêtre contextuelle de Bitdefender vous indiquera qu'une menace a été détectée.

   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 « *Assistance* » (p. 175).

13.2. Comment désinstaller Bitdefender ?

Si vous souhaitez supprimer votre Bitdefender Antivirus Plus :

- Dans **Windows 7** :
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
  2. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
  3. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.

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. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
4. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.
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**.
3. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.
6. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

Note
Cette procédure de réinstallation supprimera de manière permanente les réglages personnalisés.

13.3. Comment désinstaller le VPN Bitdefender ?

La procédure de suppression du VPN Bitdefender est similaire à celle des autres programmes de votre appareil :

- Dans **Windows 7** :

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

2. Localisez **VPN Bitdefender** et sélectionnez **Désinstaller**.

   Patientez jusqu'à la fin du processus de désinstallation.

- 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 **VPN Bitdefender** et sélectionnez **Désinstaller**.

   Patientez jusqu'à la fin du processus de désinstallation.

- 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 **VPN Bitdefender** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.

   Patientez jusqu'à la fin du processus de désinstallation.

13.4. Comment retirer l'extension Bloqueur de trackers Bitdefender ?

Suivez les instructions suivantes pour supprimer l'extension Bloqueur de trackers Bitdefender en fonction du navigateur que vous utilisez :

- Internet Explorer

1. Cliquez sur  à côté de la barre de recherche, puis sélectionnez Gérer les modules.

   Une liste des extensions installées apparait.
2. Cliquez sur Bloqueur de trackers Bitdefender.
3. Cliquez sur **Désactiver** en bas à droite.

- Google Chrome

1. Cliquez sur à côté de la barre de recherche.

2. Sélectionnez **Plus d'outils**, puis **Extensions**.

   Une liste des extensions installées apparait.

3. Cliquez sur **Supprimer** sur la fiche du Bloqueur de trackers Bitdefender.
4. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.

- Firefox

1. Cliquez sur ☰ à côté de la barre de recherche.
2. Sélectionnez **Add-ons**, puis **Extensions**.

   Une liste des extensions installées apparait.

3. Cliquez sur ••• puis sélectionnez **Supprimer**.

13.5. Comment éteindre automatiquement l'appareil 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 menaces. L'analyse de l'ensemble de l'appareil peut prendre plus de temps en fonction de la configuration matérielle et logicielle de votre système.

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

Prenons l'exemple suivant : vous avez terminé votre travail et souhaitez aller vous coucher. Vous aimeriez que l'ensemble de votre système fasse l'objet d'une analyse des menaces par Bitdefender.

Pour éteindre l'appareil quand l'Analyse rapide ou l'Analyse du système est terminée :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Analyses**, cliquez sur ••• à côté d'Analyse rapide ou d'Analyse système, puis sélectionnez **Éditer**.
4. Personnalisez l'analyse en fonction de vos besoins puis cliquez sur **Suivant**.

5. Cochez la case située à côté de **Choisir quand programmer cette tâche**, puis choisissez quand la tâche devra démarrer.

   Pour sélectionner Quotidien, Hebdomadaire ou Mensuel, bougez le curseur le long de l'échelle pour configurer la période durant laquelle l'analyse planifiée doit débuter.

6. Cliquez sur **Enregistrer**.

Pour éteindre l'appareil lorsqu'une analyse personnalisée est terminée :

1. Cliquez sur ••• à côté de l'analyse personnalisée que vous avez créée.
2. Cliquez sur **Suivant** puis cliquez de nouveau sur **Suivant**.
3. Cochez la case située à côté de **Choisir quand programmer cette tâche**, puis choisissez quand la tâche devra démarrer.
4. Cliquez sur **Enregistrer**.

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

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 90).

13.6. Comment configurer Bitdefender pour utiliser une connexion internet par proxy ?

Si votre appareil 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, il est correctement configuré pour se connecter à internet.

Pour gérer les paramètres du proxy :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.

2. Sélectionnez l'onglet **Avancé**.
3. Activez **Serveur proxy**.
4. Cliquez sur **Changement de 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 de Microsoft Edge, d'Internet Explorer, de Mozilla Firefox et de Google Chrome.

   - **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.

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

Pour savoir si votre système d'exploitation est un 32 ou 64 octets :

- 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** :

  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.

     Dans **Windows 8.1**, localisez **Ce PC**.

  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.

13.8. Comment afficher des objets cachés dans Windows ?

Ces étapes sont utiles en cas de menaces, 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**.

13.9. 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 appareil, le système devient instable. Le programme de désinstallation de Bitdefender Antivirus Plus 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 :

- 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**.
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.

13.10. 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 menaces 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 menaces sont inactives lorsque Windows est en mode sans échec et qu'elles peuvent être supprimées facilement.

Pour démarrer Windows en mode sans échec :

- Dans **Windows 7** :

1. Redémarrez l'appareil.

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.

- Dans **Windows 8, Windows 8.1 et Windows 10** :

1. Exécutez **Configuration système** dans Windows en appuyant simultanément sur les touches **Windows + R** de votre clavier.
2. Tapez **msconfig** dans la boîte de dialogue **Ouvrir** puis cliquez sur **OK**.
3. Sélectionnez l'onglet **Démarrage**.
4. Dans la zone **Options de démarrage**, cochez la case **Démarrage sécurisé**
5. Cliquez sur **Réseau** puis **OK**.
6. Cliquez sur **OK** dans la fenêtre **Configuration système** qui vous informe que le système doit être redémarré pour pouvoir faire les changements que vous souhaitez.

   Votre système redémarre en mode sécurisé avec le réseau.

Pour redémarrer en mode normal, changer à nouveau les paramètres en relançant l'**Opération système** et en décochant la case **Démarrage sécurisé**. Cliquez sur **OK** puis **Redémarrer**. Attendez que les nouveaux paramètres soient appliqués.

GÉRER VOTRE SÉCURITÉ

14. PROTECTION ANTIVIRUS

Bitdefender protège votre appareil contre tous les types de logiciels malveillants (programmes malveillants, chevaux de Troie, logiciels espions, trousses administrateur pirates, 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 courriels lors de leur réception.

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

  Important
  Pour empêcher l'infection de votre appareil par des menaces, 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 et Bitdefender le fait – à la demande.

Bitdefender analyse automatiquement tout support amovible connecté à l'appareil 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. 94).

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. 96).

Lorsqu'il détecte une menace, Bitdefender tente automatiquement de supprimer le code malveillant 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. 99).

Si votre appareil a été infecté par des logiciels malveillants, consultez-vous « *Suppression des menaces de votre système* » (p. 166). Pour vous aider à supprimer les logiciels malveillants qui ne peuvent pas l'être à partir du système d'exploitation Windows, Bitdefender vous fournit le« *Mode de secours* » (p. 166). Il s'agit d'un environnement de confiance, spécialement conçu pour la suppression de logiciels malveillants, qui vous permet de faire redémarrer votre appareil indépendamment de Windows. Lorsque l'appareil s'exécute dans un environnement de secours, les menaces Windows sont inactives, rendant leur suppression facile.

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

Bitdefender fournit une protection en temps réel contre une large gamme de logiciels malveillants en analysant tous les fichiers et courriels auxquels vous accédez.

14.1.1. Activer ou désactiver la protection en temps réel

Pour activer ou désactiver la protection contre les logiciels malveillants en temps réel :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Avancé**, activez ou désactivez **Bouclier Bitdefender**.
4. 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.

14.1.2. Configurer les paramètres avancés 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 avancés de protection en temps réel :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Avancé**, vous pouvez configurer les paramètres d'analyse en fonction de vos besoins.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- **Analyser uniquement les applications.** Vous pouvez configurer Bitdefender de sorte à analyser uniquement les applications auxquelles vous avez accédé.
- **Analyser les applications potentiellement indésirables.** Sélectionnez cette option pour n'analyser que les applications indésirables. Une application potentiellement indésirable (PUA), ou programme potentiellement indésirable (PIP), est un logiciel habituellement intégré à un logiciel gratuit qui provoque l'apparition de fenêtres publicitaires ou installe une barre d'outils sur le navigateur par défaut. Certains changent la page d'accueil ou le moteur de recherche utilisé, d'autres exécutent plusieurs processus en tâche de fond qui ralentissent l'ordinateur ou provoquent l'apparition de nombreuses publicités. Ces programmes peuvent être installés sans votre consentement (alors appelés publiciels) ou sont inclus par défaut dans le logiciel d'installation rapide.
- **Analyser les scripts.** La fonctionnalité Analyse de scripts permet à Bitdefender d'analyser des scripts PowerShell et des documents Office pouvant contenir des malwares basés sur des scripts.
- **Analyser les volumes partagés.** Pour accéder en toute sécurité à un réseau à distance depuis votre appareil, nous vous recommandons de maintenir activée l'option Analyser les volumes partagés.

- **Analyser dans les archives.** 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 menaces 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, activez-la puis déplacez le curseur sur l'échelle pour exclure de l'analyse les archives dont le poids est supérieur à une valeur en Mo (Mégaoctets).

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

- **Analyser uniquement les nouveaux fichiers et les fichiers 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.

- **Rechercher les 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 **Début du démarrage** pour analyser votre système au démarrage dès que tous ses services critiques ont été initialisés. La mission de cette fonctionnalité est d'améliorer la détection des menaces au démarrage et redémarrage de votre système.

Actions appliquées aux menaces détectées :

Vous pouvez configurer les actions appliquées par la protection en temps réel en suivant les étapes suivantes :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Avancé**, faites défiler vers le bas jusqu'à ce que vous voyiez l'option **Actions contre les menaces**.
4. Configurez les paramètres d'analyse selon vos besoins.

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 partiellement à des informations de la base de données d'information sur les menaces de 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. 99).

  Important

  Pour certains types de menaces, 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 en menaces de Bitdefender. Si la présence de menaces

est confirmée, une mise à jour des informations sur les menaces 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.

Mettre 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. 99).

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

14.1.3. Restauration des paramètres par défaut

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

Pour restaurer les paramètres de protection en temps réel par défaut :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Avancé**, faites défiler vers le bas jusqu'à ce que vous voyiez l'option **Réinitialiser les paramètres avancés**. Sélectionnez cette option pour réinitialiser les réglages par défaut de l'antivirus.

14.2. Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre appareil sans logiciel malveillant. Cela s'effectue en protégeant votre appareil des nouvelles menaces 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'une menace soit déjà logée dans votre système, avant même l'installation de Bitdefender. C'est pourquoi il est prudent d'analyser votre appareil après l'installation de Bitdefender. Et il encore plus prudent d'analyser régulièrement votre appareil contre les menaces.

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'appareil 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 appareil ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

14.2.1. Rechercher des menaces 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

L'analyse rapide utilise l'analyse dans le cloud pour détecter les logiciels malveillants 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 démarrer une analyse rapide :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Analyses**, cliquez sur le bouton **Lancer l'analyse** situé à côté d'**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 appliquer.

14.2.3. Exécuter une analyse du système

La tâche d'analyse du système analyse l'ensemble de votre appareil en vue de détecter tous les types de logiciels malveillants menaçant sa sécurité : programmes malveillants, logiciels espions, publiciels, trousses administrateur pirates 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 appareil.

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

- Vérifiez que la base de données d'information sur les menaces de Bitdefender est à jour. Analyser votre appareil en utilisant une base de données d'information sur les menaces non à jour peut empêcher Bitdefender de détecter les logiciels malveillants identifié depuis la mise à jour précédente. Pour plus d'informations, reportez-vous à « *Maintenir Bitdefender à jour* » (p. 41).
- Fermez tous les programmes ouverts.

Si vous souhaitez analyser certains emplacements de votre appareil ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée. Pour plus d'informations, reportez-vous à « *Configurer une analyse personnalisée* » (p. 87).

Pour exécuter un analyse système :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Analyses**, cliquez sur le bouton **Lancer l'analyse** situé à côté d'**Analyse système**.
4. La fonctionnalité Analyse du système vous sera présentée lors de sa première exécution. Cliquez sur **OK, j'ai compris** pour continuer.
5. 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 appliquer.

14.2.4. Configurer une analyse personnalisée

Dans la fenêtre **Gérer les analyses**, vous pouvez configurer Bitdefender pour qu'il exécute des analyses quand vous estimez que votre appareil peut potentiellement contenir des menaces. Vous pouvez choisir de planifier une Analyse du système ou une Analyse rapide, ou bien créer une analyse personnalisée en fonction de vos préférences.

Pour configurer une nouvelle analyse personnalisée en détails :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Analyses**, cliquez sur **+Créer une analyse**.
4. Dans le champ **Nom de la tâche**, saisissez un nom pour l'analyse, sélectionnez les emplacements que vous souhaitez analyser, puis cliquez sur **Suivant**.
5. Configurez les options générales suivantes :
   - **Analyser uniquement les applications**. Vous pouvez configurer Bitdefender de sorte à analyser uniquement les applications auxquelles vous avez accédé.
   - **Priorité de la tâche d'analyse**. Vous pouvez sélectionner quel impact peut avoir une analyse sur les performances de votre système.
     - Auto - La priorité du processus d'analyse dépendra de l'activité de votre système. Pour veiller à ce que le processus d'analyse ne nuise pas à l'activité du système, Bitdefender décidera si le processus d'analyse doit être exécuté avec une priorité haute ou basse.
     - Haute - La priorité de la tâche d'analyse sera élevée. En choisissant cette option, vous permettez à d'autres programmes de fonctionner plus lentement, et diminuez le temps nécessaire pour que l'analyse soit finie.
     - Basse - La priorité de la tâche d'analyse sera basse. En choisissant cette option, vous permettez à d'autres programmes de fonctionner

plus rapidement, et augmentez le temps nécessaire pour que l'analyse soit finie.

- **Actions post-analyse**. Spécifiez quelle mesure doit être prise par Bitdefender si aucune menace n'a été détectée.
  - Fermer la fenêtre de résumé
  - Éteindre l'appareil
  - Fermer la fenêtre d'analyse

6. Si vous souhaitez configurer les options d'analyse en détail, cliquez sur **Afficher les options avancées**. Vous trouverez des informations sur les analyses listées à la fin de cette section.

   Cliquez sur **Suivant**.

7. Si vous le souhaitez, vous pouvez activer l'option **Programmer la tâche d'analyse**, puis choisir le moment où l'analyse personnalisée que vous avez créée devra démarrer.
   - Au démarrage du système
   - Tous les jours
   - Tous les mois
   - Toutes les semaines

   Pour sélectionner Quotidien, Hebdomadaire ou Mensuel, bougez le curseur le long de l'échelle pour configurer la période durant laquelle l'analyse planifiée doit débuter.

8. Cliquez sur **Enregistrer** pour enregistrer les réglages et fermer la fenêtre de configuration.

   En fonction des emplacements à analyser, l'analyse peut prendre quelque temps. Si des menaces sont trouvées pendant le processus d'analyse, il vous sera demandé de sélectionner les actions à appliquer aux fichiers détectés.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiers avec certains de ces termes, consultez le glossaire. Vous pouvez également rechercher des informations sur Internet.

- **Analyser les applications potentiellement indésirables.** Sélectionnez cette option pour n'analyser que les applications indésirables. Une application potentiellement indésirable (PUA), ou programme potentiellement indésirable (PIP), est un logiciel habituellement intégré à un logiciel gratuit qui provoque l'apparition de fenêtres publicitaires ou installe une barre d'outils sur le navigateur par défaut. Certains changent la page d'accueil ou le moteur de recherche utilisé, d'autres exécutent plusieurs processus en tâche de fond qui ralentissent l'ordinateur ou provoquent l'apparition de nombreuses publicités. Ces programmes peuvent être installés sans votre consentement (alors appelés publiciels) ou sont inclus par défaut dans le logiciel d'installation rapide.
- **Analyser dans les archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Les menaces 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.

  Déplacez le curseur sur l'échelle pour exclure de l'analyse les archives doit le poids est supérieur à une valeur en Mo (Mégaoctets).

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

- **Analyser uniquement les nouveaux fichiers et les fichiers 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.
- **Analyser les secteurs d'amorçage.** Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs d'amorçage de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour faire lancer le processus de démarrage du système. Quand une menace infecte le secteur de démarrage, 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 temoins stockés par les navigateurs sur votre appareil.
- **Rechercher les 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.

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 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 appliquer.

Les objets infectés sont affichés dans des groupes, basés sur les menaces 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 partiellement à des informations de la base de données d'information sur les menaces de 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. 99).

  > **Important**
  > Pour certains types de menaces, 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 en menaces de Bitdefender. Si la présence de menaces est confirmée, une mise à jour des informations 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.

Ne rien faire

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.

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 logiciels malveillants manuellement, reportez-vous à « *Suppression des menaces de votre système* » (p. 166).

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 vérifier un journal d'analyse ou toute autre infection détectée plus tard :

1. Cliquez sur **Notifications** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant la dernière analyse.

   Cette section vous permet de trouver tous les événements d'analyse des menaces, 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 notifications, vous pouvez consulter les analyses ayant été réalisées récemment. Cliquez sur une notification pour afficher des informations à son sujet.
4. Pour ouvrir le journal d'analyse, cliquez sur **Journal**.

14.3. Analyse automatique de supports amovibles

Bitdefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre appareil et l'analyse en tâche de fond lorsque l'analyse automatique est activée. Ceci est recommandé afin d'empêcher que des logiciels malveillants n'infectent votre appareil.

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 à la recherche de logiciels malveillants (à condition

que l'analyse automatique soit activée pour ce type de périphérique). Vous serez averti via une fenêtre contextuelle qu'un nouveau périphérique a été détecté et est en cours d'analyse.

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.

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.

Dans la plupart des cas, Bitdefender supprime automatiquement les menaces détectées 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.

Ces informations peuvent vous être utiles :

- Soyez prudent lorsque vous utilisez un CD ou DVD infecté par des menaces, car ces menaces ne peuvent pas être supprimées du disque (le support est en lecture seule). Vérifiez que la protection en temps réel est activée pour empêcher la diffusion de menaces 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 menaces 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 menaces, reportez-vous à « *Suppression des menaces de votre système* » (p. 166).

14.3.2. Gérer l'analyse des supports amovibles

Pour gérer l'Analyse automatique de supports amovibles :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Sélectionnez la fenêtre **Paramètres**.

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.

Pour une meilleure protection, nous vous recommandons de laisser activée l'option **analyse automatique** de tous les types de périphériques de stockage amovibles.

14.4. Analyse du fichier hosts

Le fichier hosts est livré par défaut avec l'installation de votre système d'exploitation et est utilisé pour associer des noms d'hôtes à des adresses IP à chaque fois que vous accédez à une nouvelle page Web, que vous vous connectez à un serveur FTP ou à d'autres serveurs internet. C'est un fichier en texte brut et des programmes malveillants pourraient le modifier. Les utilisateurs avancés savent l'utiliser pour bloquer les publicités intempestives, ainsi que les bannières, les témoins tiers et les pirates informatiques.

Pour configurer l'analyse du fichier hosts :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Avancé**.
3. Activez ou désactivez **Analyse du fichier hosts**.

14.5. 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 exceptions 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 exceptions 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**.

14.5.1. Exclure de l'analyse des fichiers et des dossiers

Pour exclure des fichiers et des dossiers spécifiques de l'analyse :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres**, cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez le chemin du dossier que vous souhaitez exclure de l'analyse dans le champ correspondant.

   Sinon, vous pouvez naviguer jusqu'au dossier en cliquant sur le bouton Parcourir situé sur la droite de l'interface, le sélectionner puis cliquer sur **OK**.
6. Activez l'interrupteur situé à côté de la fonctionnalité de protection qui ne devrait pas analyser le dossier. Il existe trois options :
   - Antivirus
   - Prévention menaces en ligne
   - Advanced Threat Defense
7. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

14.5.2. Exclure des extensions de fichiers de l'analyse

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 appareil. L'exception 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 appareil vulnérable aux menaces.

Pour exclure des extensions de fichiers de l'analyse :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres**, cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez les extensions que vous souhaitez exclure de l'analyse en les précédant d'un point et en les séparant par des points-virgules (;).

   txt;avi;jpg
6. Activez l'interrupteur situé à côté de la fonctionnalité de protection qui ne devrait pas analyser l'extension.
7. Cliquez sur **Enregistrer**.

14.5.3. 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 des exceptions d'analyse :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres**, cliquez sur **Gérer les exceptions**. La liste de toutes vos exceptions va s'afficher.
4. Pour supprimer ou éditer des exceptions d'analyse, cliquez sur l'un des boutons disponibles. Procédez comme suit :

- Pour supprimer une entrée de la liste, cliquez sur le bouton situé à côté de celle-ci.
- Pour éditer une entrée du tableau, cliquez sur le bouton **Éditer** situé à côté de celle-ci. Une nouvelle fenêtre apparaît dans laquelle vous pouvez modifier l'extension ou le chemin à exclure ainsi que la fonctionnalité de sécurité dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **MODIFIER**.

14.6. Gérer les fichiers en quarantaine

Bitdefender isole les fichiers infectés par des menaces qu'il ne peut pas désinfecter et les fichiers suspects dans une zone sécurisée nommée quarantaine. Quand une menace est en quarantaine, elle ne peut faire aucun dégât car elle ne peut ni être exécutée, ni être lue.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes en menaces de Bitdefender. Si la présence de menaces est confirmée, une mise à jour des informations est publiée afin de permettre de les supprimer.

Bitdefender analyse également les fichiers en quarantaine après chaque mise à jour de la base de données d'information sur les menaces. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Pour consulter et gérer les fichiers en quarantaine :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Paramètres**.

   Vous pouvez ici voir le nom des fichiers en quarantaine, leur emplacement d'origine et le nom des menaces détectées.
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 en cliquant sur **Voir les paramètres**.

   Cliquez sur les boutons pour activer ou désactiver :

Analyser la quarantaine après la mise à jour des informations
Maintenez cette option activée pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour de la base de données d'information sur les menaces Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Supprimer le contenu datant de plus de 30 jours
Les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés.

Créer des exceptions pour les fichiers restaurés
Les fichiers que vous restaurez de la quarantaine sont déplacés vers leur emplacement d'origine sans être réparés et automatiquement exclus des analyses suivantes.

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**.

15. ADVANCED THREAT DEFENSE

Bitdefender Advanced Threat Defense est une technologie de détection proactive innovante qui utilise des méthodes heuristiques de pointe pour détecter des ransomwares ou d'autres nouvelles menaces potentielles en temps réel.

Advanced Threat Defense surveille en permanence les applications en cours d'exécution sur l'appareil, à la recherche d'actions ressemblant à celles des menaces. Chacune de ces actions est notée et un score global est calculé pour chaque processus.

Par mesure de sécurité, vous serez notifié à chaque fois que des menaces et des processus potentiellement malveillants sont détectés et bloqués.

15.1. Activer ou désactiver Advanced Threat Defense

Pour activer ou désactiver Advanced Threat Defense :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **DÉFENSE CONTRE LES MENACES AVANCÉES**, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Paramètres** et cliquez sur l'interrupteur situé à côté de **Défense Bitdefender contre les menaces avancées**.

> **Note**
> Pour maintenir la protection de votre système contre les ransomwares et les autres menaces, nous vous recommandons de désactiver Advanced Threat Defense pour des durées aussi brèves que possible.

15.2. Vérification des attaques malveillantes détectées

Dès qu'une menace ou un processus malveillant est détecté, Bitdefender le bloquera pour empêcher votre appareil d'être infecté par un ransomware ou un autre malware. Vous pouvez vérifier à tout moment la liste des attaques malveillantes détectées en suivant les étapes suivantes :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.

2. Dans le panneau **DÉFENSE CONTRE LES MENACES AVANCÉES**, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Défense contre les menaces**.

   Les attaques détectées ces 90 derniers jours sont affichées. Pour en apprendre plus sur le type d'un ransomware détecté, le chemin du processus malveillant ou si la désinfection a été une réussite, cliquez sur celui-ci.

15.3. Ajout de processus aux exceptions

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

Pour commencer à ajouter des processus à la liste d'exceptions d'Advanced Threat Defense :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **DÉFENSE CONTRE LES MENACES AVANCÉES**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres**, cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez le chemin du dossier que vous souhaitez exclure de l'analyse dans le champ correspondant.

   Sinon, vous pouvez naviguer jusqu'à l'exécutable en cliquant sur le bouton Parcourir situé sur la droite de l'interface, le sélectionner puis cliquer sur **OK**.
6. Activez l'interrupteur situé à côté de **Défense contre les menaces avancées**.
7. Cliquez sur **Enregistrer**.

15.4. Détection des exploits

L'une des manières utilisées par les pirates pour pénétrer sur un ordinateur est de profiter de certains bugs ou de vulnérabilités présents dans les logiciels (applications ou plug-ins) ou le matériel de celui-ci. Pour veiller à ce que votre appareil soit protégé des attaques de ce type, connues pour se répandre très

rapidement, Bitdefender utilise ce qui se fait de plus récent en termes de technologies anti-exploit.

Activer ou désactiver la détection des exploits

Pour activer ou désactiver la détection des exploits :

- Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
- Dans le panneau **DÉFENSE CONTRE LES MENACES AVANCÉES**, cliquez sur **Ouvrir**.
- Ouvrez la fenêtre **Paramètres** puis cliquez sur l'interrupteur situé à côté de **Détection des exploits** pour activer ou désactiver la fonctionnalité.

Note

L'option Détection des exploits est activée par défaut.

16. PRÉVENTION MENACES EN LIGNE

La Prévention des menaces en ligne de Bitdefender vous garantit une navigation sur Internet en toute sécurité en vous signalant les pages web présentant un risque.

Bitdefender assure la Prévention des menaces en ligne en temps réel pour :

- Internet Explorer
- Microsoft Edge
- Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Pour configurer les paramètres de la Prévention des menaces en ligne :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PRÉVENTION DES MENACES EN LIGNE**, cliquez sur **Paramètres**.

Dans la section **Protection web**, cliquez sur les interrupteurs pour activer ou désactiver :

- La Prévention d'attaques réseaux bloque les menaces provenant d'Internet, y compris les téléchargements intempestifs.
- L'Assistant de recherche, un composant qui évalue les résultats de vos requêtes sur les moteurs de recherche et les liens publiés 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.

  L'Assistant de recherche évalue les résultats de recherche des moteurs de recherche Web suivants :
  - Google
  - Yahoo!

- Bing
- Baidu

L'Assistant de recherche évalue les liens publiés sur les sites de réseaux sociaux suivants :

- Facebook
- Twitter

- Analyse Web chiffrée.

  Des attaques plus sophistiquées peuvent utiliser le trafic Web sécurisé pour induire en erreur leurs victimes. Nous vous recommandons donc de laisser l'option Analyse web chiffrée activée.

- Protection contre la fraude.
- Protection antiphishing.

Faites défiler vers le bas jusqu'à atteindre la section **Prévention des menaces réseau**. Ici apparaît l'option **Prévention des menaces réseau**. Pour protéger votre appareil des attaques de malwares complexes (comme les ransomwares) qui profitent de vulnérabilités, gardez cette option activée.

Vous pouvez créer une liste de sites Web, domaines et adresses IP qui ne seront pas analysés par les moteurs anti-malware, antiphishing et antifraude de Bitdefender. La liste ne doit contenir que des sites web, domaines et adresses IP en lesquels vous avez entièrement confiance.

Pour configurer et gérer les sites Internet, domaines et adresses IP en utilisant la fonctionnalité de Prévention des menaces en ligne fournie par Bitdefender :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PRÉVENTION DES MENACES EN LIGNE**, cliquez sur **Paramètres**.
3. Cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez dans le champ correspondant le nom du site Internet, le nom du domaine ou l'adresse IP que vous souhaitez ajouter aux exceptions.
6. Cliquez sur l'interrupteur situé à côté de **Prévention des menaces en ligne**.

7. Pour supprimer une entrée de la liste, cliquez sur le bouton situé à côté de celle-ci.

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

16.1. 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 le site web en cliquant sur **RETOUR EN TOUTE SÉCURITÉ**.
- Pour vous rendre sur le site web, malgré l'avertissement, cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**.
- Si vous êtes certain que le site web détecté est sûr, cliquez sur **VALIDER** pour l'ajouter aux exceptions. Nous vous recommandons de n'ajouter que les sites auxquels vous vous fiez entièrement.

17. VULNÉRABILITÉ

Une étape importante permettant de préserver votre appareil contre les actions malveillantes et les menaces est de maintenir à jour votre système d'exploitation et vos principales applications. En outre, pour empêcher l'accès physique non autorisé à votre appareil, des mots de passe forts (mots de passe qui ne peuvent pas être facilement déchiffrés) doivent être configurés pour chaque compte d'utilisateur Windows ainsi que pour les réseaux Wi-Fi auxquels vous vous connectez.

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 Notifications.

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 détecter les vulnérabilités d'un système, Bitdefender nécessite une connexion à Internet.

Analyser votre système à la recherche de vulnérabilités

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **VULNÉRABILITÉ**, cliquez sur **Ouvrir**.
3. Dans l'onglet **Analyse des vulnérabilités**, cliquez sur **Commencer l'analyse**, puis patientez pendant que Bitdefender recherche des vulnérabilités dans votre système. Les vulnérabilités détectées sont regroupées en trois catégories :
   - **SYSTÈME D'EXPLOITATION**
     - **Sécurité du système d'exploitation**

       A modifié des réglages système pouvant compromettre votre appareil et vos données, par exemple en ne permettant pas l'affichage d'alertes

lorsque des fichiers exécutés modifient votre système sans votre permission ou lorsque que des appareils MTP tels que des téléphones ou des appareils-photo se connectent et exécutent différentes opérations sans que vous le sachiez.

- **Mises à jour critiques Windows**

  Une liste des mises à jour critiques de Windows qui ne sont pas installées sur votre ordinateur apparait. Un redémarrage du système peut être nécessaire pour permettre à Bitdefender de terminer l'installation du correctif. Attention, l'installation de ces mises à jour peut prendre du temps.

- **Comptes Windows vulnérables**

  Vous pouvez visualiser la liste des comptes utilisateur Windows configurés sur votre appareil ainsi que le niveau de protection que leur confèrent leurs mots de passe. 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 définir un nouveau mot de passe pour votre système, sélectionnez **Changer de mot de passe maintenant**.

  Pour créer un mot de passe sécurisé, nous vous recommandons d'utiliser un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

- **APPLICATIONS**
  - **Sécurité du navigateur**

    Modification des paramètres de votre appareil permettant l'exécution de fichiers et de programmes téléchargés via Internet Explorer sans que leur intégrité ait été validée, pouvant entraîner une compromission de votre appareil.

  - **Mises à jour d'applications**

    Pour voir les informations sur une application devant être mise à jour, cliquez sur son nom dans la liste.

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

- **RÉSEAU**
  - **Réseau et informations d'authentification**

A modifié les paramètres système afin de permettre la connexion automatique à des points d'accès de réseaux ouverts sans que vous le sachiez ou le non chiffrement du trafic sortant sur un canal sécurisé.

- **Réseaux Wi-Fi et routeurs**

  Pour en apprendre plus sur le réseau sans fil et le routeur sur lesquels vous êtes connectés, cliquez sur son nom dans la liste. Il est recommandé de choisir un mot de passe complexe pour votre réseau domestique. Veuillez suivre nos instructions pour ne plus avoir à vous inquiéter pour votre vie privée quand vous êtes connecté.

  Lorsque d'autres recommandations sont disponibles, suivez les instructions fournies pour vous assurer que votre réseau domestique reste protégé des pirates informatiques.

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 Notifications.

Pour consulter et corriger les problèmes détectés :

1. Cliquez sur **Notifications** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant la vulnérabilité.
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 **Installer**.
   - Si la mise à jour Windows automatique est désactivée, cliquez sur **Activer**.
   - Si une application n'est pas à jour, cliquez sur **Mettre a 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.
- Si le routeur que vous avez configuré a défini un mot de passe faible, cliquez sur **Modifier le mot de passe** pour accéder à son interface à partir de laquelle vous pouvez en définir un plus fort.
- Si le réseau auquel vous êtes connecté a des vulnérabilités qui peuvent exposer votre système à des risques, cliquez sur **Modifier les paramètres WIFI**.

Pour configurer les paramètres de surveillance de la vulnérabilité :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **VULNÉRABILITÉ**, cliquez sur **Ouvrir**.

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

3. Ouvrez l'onglet **Paramètres**.
4. Choisissez les vulnérabilités du système que vous souhaitez vérifier régulièrement à l'aide des boutons correspondants.

   Mises à jour 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 utilisateur
   Vérifiez si les mots de passe des comptes Windows et des routeurs 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 @).

Autoplay

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

Sécurité du Wi-Fi

Vérifiez si le réseau sans fil domestique auquel vous êtes connecté et fiable ou non et s'il a des vulnérabilités. De plus, vérifiez que le mot de passe de votre routeur domestique est suffisamment fort, ou sinon comment le rendre plus sûr.

La plupart des réseaux non protégés sans fil ne sont pas sécurisés, permettant ainsi aux pirates d'accéder à vos activités privées.

Note

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

17.3. Sécurité du Wi-Fi

Lorsque vous êtes en déplacement, dans un café, ou attendez à l'aéroport, la connexion à un réseau sans fil public pour effectuer des paiements, vérifier vos courriels ou vos comptes de réseaux sociaux peut être la solution la plus rapide. Mais les regards indiscrets qui tentent de détourner vos données personnelles ne sont peut être pas loin et surveillent comment les informations fuitent du réseau.

Les données personnelles signifient les mots de passe et noms d'utilisateur que vous utilisez pour accéder à vos comptes en ligne, tels que les courriels, comptes bancaires, comptes de réseaux sociaux, mais aussi les messages que vous envoyez.

Habituellement, les réseaux sans fil publics sont plus susceptibles d'être dangereux car ils ne nécessitent pas de mot de passe lors de la connexion,

et si c'est le cas, le mot de passe peuvent être mis à disposition de toute personne qui veut se connecter. De plus, il peut s'agir de réseaux malveillants ou de pots de miel, faisant d'eux une cible pour les cybercriminels.

Pour vous protéger contre les dangers des hotspots sans fil publics non fiables ou non chiffrés, Wifi Security Advisor Bitdefender analyse le degré de protection du réseau sans fil, et si nécessaire, il vous recommande d'utiliser le VPN Bitdefender.

L'Assistant de sécurité Wi-Fi Bitdefender donne des informations sur :

- Réseaux Wifi domestiques
- Réseaux Wifi professionnels
- Réseaux Wifi publics

17.3.1. Activer ou désactiver les notifications de l'Assistant de sécurité Wi-Fi

Pour activer ou désactiver les notifications de l'Assistant de sécurité Wi-Fi :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **VULNÉRABILITÉ**, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Paramètres** et activez ou désactivez l'option **Assistant de sécurité du Wi-Fi**.

17.3.2. Configuration du réseau Wi-Fi domestique

Pour commencer à configurer votre réseau domestique :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **VULNÉRABILITÉ**, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Assistant de sécurité du Wi-Fi** puis cliquez sur **Wi-Fi domestique**.
4. Dans l'onglet **WI-FI domestique**, cliquez sur **SÉLECTIONNER WI-FI DOMESTIQUE**.

   Une liste avec les réseaux sans fil auxquels vous vous êtes connectés jusqu'à ce jour s'affiche.

5. Cherchez votre réseau domestique, puis cliquez sur **Sélectionner**.

Si un réseau domestique est considéré non protégé ou non fiable, les recommandations de configuration pour améliorer sa sécurité s'affichent.

Pour supprimer le réseau sans fil que vous avez défini comme réseau domestique, cliquez sur le bouton **SUPPRIMER**.

Pour ajouter un nouveau réseau sans fil domestique, cliquez sur **Sélectionner un nouveau Wi-Fi domestique**.

17.3.3. Configuration du réseau Wi-Fi professionnel

Pour commencer à configurer votre réseau professionnel :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **VULNÉRABILITÉ**, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Assistant de sécurité du Wi-Fi** puis cliquez sur **Wi-Fi du bureau**.
4. Dans l'onglet **WI-FI professionnel**, cliquez sur **SÉLECTIONNER WI-FI DOMESTIQUE**.

   Une liste avec les réseaux sans fil auxquels vous vous êtes connectés jusqu'à ce jour s'affiche.
5. Cherchez votre réseau professionnel, puis cliquez sur **Sélectionner**.

Si un réseau professionnel est considéré non protégé ou non fiable, les recommandations de configuration pour améliorer sa sécurité s'affichent.

Pour supprimer le réseau sans fil que vous avez défini comme réseau professionnel, cliquez sur **SUPPRIMER**.

Pour ajouter un nouveau réseau sans fil professionnel, cliquez sur **Sélectionner un nouveau Wi-Fi professionnel**.

17.3.4. Wi-Fi public

Lorsque vous êtes connecté à un réseau sans fil non sécurisé ou dangereux, le Profil Wifi public est activé. Lorsque vous êtes sous ce profil, Bitdefender Antivirus Plus est réglé pour accomplir automatiquement les paramètres de programme suivants :

- Advanced Threat Defense est activé

- Les paramètres suivants de la Prévention des menaces en ligne sont activés :
  - Analyse Web chiffrée
  - Protection contre la fraude
  - Protection contre le phishing
- Un bouton qui ouvre Bitdefender Safepay™ est disponible. Dans ce cas, la protection des points d'accès Wi-Fi pour les réseaux non sécurisés est activée par défaut.

17.3.5. Vérifier les informations à propos des réseaux Wifi

Pour vérifier les informations sur les réseaux sans fil auxquels vous vous connectez habituellement :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **VULNÉRABILITÉ**, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Assistant de sécurité du Wi-Fi**.
4. Selon les informations dont vous avez besoin, sélectionnez l'une des trois balises, **Wi-Fi domestique**, **Wi-Fi professionnel** ou **Wi-Fi public**.
5. Cliquez sur **Voir les détails** à côté du réseau à propos duquel vous souhaitez avoir plus d'informations.

Il y a trois types de réseaux sans fil filtrés en fonction de leur importance, chacun étant signalé par une icône spécifique :

Wifi dangereux - indique que le niveau de sécurité du réseau est faible. Cela signifie qu'il y a un risque élevé à l'utiliser et il est recommandé de ne pas effectuer de paiements ou de regarder vos comptes bancaires sans protection supplémentaire. Dans de telles situations, nous vous recommandons d'utiliser Bitdefender Safepay™ avec la protection Hotspot pour les réseaux non sécurisés.

Wifi dangereux - indique que le niveau de sécurité du réseau est moyenne. Cela signifie qu'il peut avoir des vulnérabilités et il est recommandé de ne pas effectuer de paiements ou consulter vos comptes bancaires sans protection supplémentaire. Dans de telles situations, nous vous recommandons d'utiliser Bitdefender Safepay™ avec la protection Hotspot pour les réseaux non sécurisés.

Wifi protégé - indique que le réseau que vous utilisez est sûr. Dans ce cas, vous pouvez utiliser des données sensibles pour faire des opérations en ligne.

En cliquant sur le lien **Afficher les détails** à proximité de chaque réseau, les informations suivantes sont affichées :

- **Sécurisé** - vous pouvez ici voir si le réseau sélectionné est sécurisé ou non. Les réseaux non chiffrés peuvent exposer vos données.
- **Type de chiffrement** - ici vous pouvez voir le type de chiffrement utilisé par le réseau sélectionné. Certains types de chiffrement peuvent ne pas être sécurisés. Par conséquent, nous vous recommandons vivement de vérifier les informations sur le type de chiffrement affiché pour être sûr que vous êtes protégé en naviguant sur le Web.
- **Canal/fréquence** - ici vous pouvez voir la fréquence du canal utilisé par le réseau sélectionné.
- **Force du mot de passe** - ici vous pouvez voir la force du mot de passe. Notez que les réseaux protégés par des mots de passe faibles représentent des cibles de choix pour les cybercriminels.
- **Type de connexion** - ici vous pouvez voir si le réseau sélectionné est protégé par un mot de passe ou non. Il est fortement recommandé de se connecter uniquement aux réseaux qui ont mis en place des mots de passe forts.
- **Type d'authentification** - ici vous pouvez voir le type d'authentification utilisé par le réseau sélectionné.

18. REMÉDIATION DES RANSOMWARES

La rémédiation des ransomwares Bitdefender réalise des sauvegardes des fichiers, par exemple les documents, images, vidéos, ou musiques pour assurer leur protection s'ils sont endommagés ou perdus en cas de chiffrement par un ransomware. Dès qu'une attaque de ransomware est détectée, Bitdefender bloque tous les processus impliqués dans l'attaque et commence la procédure de nettoyage. De cette manière, vous pourrez récupérer le contenu de tous vos fichiers sans avoir à payer la rançon.

18.1. Activer ou désactiver la Rémédiations des Ransomwares

Pour activer ou désactiver la Rémédiations des ransomwares:

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **REMEDIATION DES RANSOMWARES**, cliquez sur le bouton pour activer ou désactiver la fonctionnalité.

> **Note**
> Pour garantir que vos fichiers sont protégés contre les ransomwares, nous vous recommandons de maintenir le Nettoyage des ransomwares activé.

18.2. Activer ou désactiver la Restauration automatique

La Restauration automatique veille à ce que vos fichiers soient automatiquement restaurés en cas de chiffrement par un ransomware.

Pour activer ou désactiver la restauration automatique :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ÉLIMINATION DES RANSOMWARES**, cliquez sur **Gérer**.
3. Dans la fenêtre Paramètres, activez ou désactivez l'interrupteur **Restauration automatique**.

18.3. Voir les fichiers qui ont été restaurés automatiquement

Quand l'option **Restauration automatique** est activée, Bitdefender restaurera automatiquement les fichiers qui ont été chiffrés par un ransomware. Vos fichiers y sont en sécurité, quoi que vous fassiez.

Pour voir les fichiers qui ont été restaurés automatiquement :

1. Cliquez sur **Notifications** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification relative à la dernière remédiation du comportement des ransomwares, puis cliquez sur **Fichiers restaurés**.

   La liste des fichiers restaurés apparait. Vous pouvez également voir où les fichiers ont été restaurés.

18.4. Restaurer manuellement des fichiers chiffrés

Dans le cas où vous devez restaurer manuellement les fichiers chiffrés par un ransomware, suivez les étapes suivantes :

1. Cliquez sur **Notifications** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification relative au dernier comportement de ransomware détecté, puis cliquez sur **Fichiers chiffrés**.
3. Une liste des fichiers chiffrés apparaît.

   Cliquez sur **Récupérer des fichiers** pour continuer.
4. Si tout ou une partie de la procédure de restauration échoue, vous devez choisir un emplacement où enregistrer les fichiers déchiffrés. Cliquez sur **Emplacement de restauration**, puis choisissez un emplacement sur votre ordinateur.
5. Une fenêtre de confirmation s'affichera.

   Cliquez sur **Terminer** pour achever le processus de restauration.

Les fichiers présentant les extensions suivantes peuvent être restaurés s'ils venaient à être chiffrés :

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

18.5. Ajout d'applications aux exceptions

Vous pouvez configurer des exceptions pour les applications de confiance de façon à ce que la fonctionnalité de remédiation ne les bloque pas si elles ont des comportements similaires aux ransomwares.

Pour ajouter des applications à la liste d'exceptions de la Remédiation des ransomwares :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ÉLIMINATION DES RANSOMWARES**, cliquez sur **Gérer**.
3. Ouvrez la fenêtre **Exceptions** puis cliquez sur **+Ajouter une exception**.

19. LE PASSWORD MANAGER PROTÈGE VOS IDENTIFIANTS

Nous utilisons l'appareil 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 ?

Le Password Manager vous aide à conserver vos mots de passe, protège votre vie privée et vous offre une navigation sécurisée.

En utilisant un mot de passe maître unique pour accéder à vos identifiants, le 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, le Password Manager est intégré à Bitdefender Safepay™ et offre une solution unifiée pour répondre aux différentes situation pouvant mettre en péril la sécurité de vos données.

Le 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
- Mots de passe des applications
- Les mots de passe des réseaux Wi-Fi

19.1. Créer une nouvelle base de données

Bitdefender Wallet est l'endroit où vous pouvez sauvegarder vos données personnelles. Pour simplifier l'expérience de navigation, vous devez créer une base de données Wallet :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Mes portefeuilles**, cliquez sur **Ajouter un portefeuille**
4. Cliquez sur **Créer nouveau**.
5. Tapez les informations requises dans les champs correspondants.
   - Nom du portefeuille - saisissez un nom unique pour votre base de données (portefeuille).
   - Mot de passe maître - saisissez un mot de passe pour votre Wallet.
   - Indice - saisissez un indice pour vous souvenir du mot de passe.
6. Cliquez sur **Continuer**.
7. Lors de cette étape, vous pouvez choisir de stocker vos informations dans le Cloud, en activant l'interrupteur situé à côté de **Synchroniser sur tous mes appareils** Choisissez les options souhaitées, puis cliquez sur **Continuer**.
8. Sélectionnez le navigateur Web à partir duquel vous souhaitez importer vos identifiants.
9. Cliquez sur **Terminer**.

19.2. Importer une base de données existante

Pour importer une base de données de Wallet stockée localement :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.

2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Mes portefeuilles**, cliquez sur **Ajouter un portefeuille**
4. Cliquez sur **Importer une base de données existante**.
5. Rendez-vous à l'emplacement de votre appareil où vous avez enregistré la base de données de Wallet puis choisissez un nom.
6. Cliquez sur **Ouvrir**.
7. Donnez un nom à votre Wallet et saisissez le mot de passe attribué lors de sa création.
8. Cliquez sur **Importer**.
9. Sélectionnez les programmes desquels le Wallet doit importer les identifiants, puis cliquez sur le bouton **Terminer**.

19.3. Exporter la base de données du Wallet

Pour exporter votre base de données du Wallet :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Mes portefeuilles**.
4. Cliquez sur l'icône ••• du Wallet désiré, puis sélectionnez **Exporter**.
5. Rendez-vous à l'emplacement de votre appareil où vous voulez enregistrer la base de données de Wallet puis choisissez un nom.
6. Cliquez sur **Enregistrer**.

> **Note**
> Le Wallet doit être ouvert pour que l'option **Exporter** soit disponible.
> Si le portefeuille que vous souhaitez exporter est verrouillé, cliquez sur **Activer le portefeuille**, puis saisissez le mot de passe qui lui a été assigné lors de sa création.

19.4. Synchroniser vos Wallets dans le cloud.

Pour activer ou désactiver la synchronisation du Wallet dans le cloud :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Mes portefeuilles**.
4. Cliquez sur l'icône ••• du Wallet désiré, puis sélectionnez **Configuration**.
5. Choisissez l'option désirée dans la fenêtre qui apparaît, puis cliquez sur **Sauvegarder**.

Note
Le Wallet doit être ouvert pour que l'option **Exporter** soit disponible.
Si le Wallet que vous souhaitez synchroniser est verrouillé, cliquez sur **ACTIVER LE WALLET**, puis entrez le mot de passe.

19.5. Gérer les identifiants de votre Wallet

Pour gérer vos mots de passe :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Mes portefeuilles**.
4. Sélectionnez la base de données portefeuille désirée, puis cliquez sur **Activer le portefeuille**.
5. Entrez le mot de passe maître puis cliquez sur **OK**.

Une nouvelle fenêtre apparaît. Sélectionnez la catégorie souhaitée dans la partie supérieure de la fenêtre :

- Identité
- Pages Web
- Banques
- E-mails
- Applications
- Réseaux Wi-Fi

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 une entrée du tableau, sélectionnez-la puis cliquez sur le bouton **Éditer** situé sur le côté droit.
- Pour effacer une entrée, sélectionnez-la puis cliquez sur le bouton  **Supprimer**.

19.6. Activer ou désactiver la protection du Password Manager

Pour activer ou désactiver le Password Manager :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, activez ou désactivez le bouton correspondant.

19.7. Gestion des configurations du Password Manager

Pour configurer le mot de passe maître en détail :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Paramètres**.

Dans la section **Paramètres de sécurité**, les options suivantes sont disponibles :

- **Me demander mon mot de passe maître lorsque je me connecte à mon appareil** - vous devrez indiquer votre mot de passe maître lorsque vous accéderez à l'appareil.
- **Me demander mon mot de passe maître lorsque j'ouvre mes navigateurs et applications** - vous devrez indiquer votre mot de passe maître lorsque vous accéderez à un navigateur ou à une application.

- **Ne pas me demander mon mot de passe maître** - il ne vous sera pas demandé de saisir votre mot de passe maître lorsque vous accéder à l'appareil, à un navigateur ou à une application.
- **Verrouiller automatiquement mon Wallet lorsque mon appareil n'est pas utilisé** - vous devrez entrer votre mot de passe maître après 15 minutes d'inactivité sur votre appareil.

Important
N'oubliez pas votre mot de passe maître 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 :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Paramètres**.
3. Sélectionnez la fenêtre **Paramètres**.

   Activez l'interrupteur situé à côté d'une application pour utiliser le Gestionnaire de mots de passe et améliorer votre expérience :

   - Internet Explorer
   - Firefox
   - Google Chrome
   - Safepay

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 entrez vos informations d'identification et données personnelles dans votre navigateur Web pour la première fois, celles-ci sont automatiquement conservées en toute sécurité dans le Wallet.

Pour configurer les paramètres **Saisie automatique** :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Paramètres**, sélectionnez l'onglet **Paramètres de remplissage automatique**.
4. Configurez les options suivantes :
   - **Configurer la façon dont le Password Manager sécurise vos identifiants**:
     - **Enregistrer automatiquement les identifiants dans le Wallet** - les identifiants de connexion et autres informations identifiables telles que vos données personnelles et bancaires sont automatiquement enregistrées et mises à jour dans le Wallet.
     - **Me demander à chaque fois** - on vous demandera à chaque fois si vous souhaitez ajouter vos identifiants au Wallet.
     - **Ne pas enregistrer, je mettrai les informations à jour manuellement** - les identifiants peuvent être ajoutés uniquement manuellement dans le Wallet.
   - **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.
   - **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 du Password Manager à partir de votre navigateur

Vous pouvez gérer le 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 du module complémentaire et cliquez sur l'icône de la barre d'outils.

L'extension Bitdefender Wallet présente les options suivantes :

- Ouvrir Wallet - ouvre le Wallet.
- Verrouiller Wallet - verrouille le Wallet.
- Pages Web - ouvre un sous-menu avec tous les identifiants de sites Web contenus dans le Wallet. Cliquez sur **Ajouter une page 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 Wallet.
- 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 du Password Manager.
- Signaler un problème - permet de signaler tout problème rencontré avec Bitdefender Password Manager.

20. ANTI-TRACKER

De nombreux sites sur lesquels vous vous rendez utiliser des trackers pour collecter des informations sur votre comportement, soit pour les communiquer à des tiers, soit pour vous proposer des publicités ciblées. Les propriétaires de sites web gagnent ainsi de l'argent, ce qui leur permet de vous proposer gratuitement des contenus, ou même de continuer à exploiter leur site. En plus de collecter des informations, les trackers peuvent également ralentir votre expérience de navigation et utiliser de la bande passante.

Une fois l'extension Bloqueur de trackers Bitdefender activée sur votre navigateur, vous n'avez plus à vous soucier des trackers, et vos données restent privées tandis que vous naviguez encore plus vite sur Internet.

Cette extension de Bitdefender est compatible avec les navigateurs suivants :

- Internet Explorer
- Google Chrome
- Firefox

Les trackers que nous détectons sont classés selon les catégories suivantes :

- **Publicité** - utilisé pour analyser le trafic du site web, le comportement de l'utilisateur ou les modèles de trafic des visiteurs.
- **Interaction avec le client** - utilisé pour mesurer l'interaction de l'utilisateur avec les différents moyens de communication tels que les chats et supports.
- **Essentiel** - utilisé pour surveiller des fonctionnalités critiques du site web.
- **Statistiques sur le site** - utilisé pour collecter des données relatives à l'utilisation de la page web.
- **Réseaux sociaux** - utilisé pour surveiller l'audience sociale, l'activité et l'engagement de l'utilisateur sur diverses plateformes de réseaux sociaux.

20.1. Interface du Bloqueur de trackers

Lorsque l'extension Bloqueur de trackers Bitdefender est activée, l'icône apparait en haut de votre navigateur, à côté de la barre de recherche. Chaque fois que vous visitez un site web, un compteur apparait sur l'icône pour indiquer le nombre de trackers détectés et bloqués. Pour en apprendre plus sur les trackers bloqués, cliquez sur l'icône pour ouvrir l'interface. En plus du nombre de trackers bloqués, vous pouvez voir le temps nécessaire au chargement de la page et les catégories auxquelles les trackers détectés appartiennent. Pour voir la liste des sites web réalisant du tracking, cliquez sur la catégorie désirée.

Pour empêcher Bitdefender de bloquer les trackers sur le site web que vous êtes en train de parcourir, cliquez sur **Interrompre la protection sur ce site web**. Ce paramètre ne s'applique que tant que le site web est ouvert, et sera réinitialisé quand vous fermerez le site web.

Pour autoriser les trackers de certaines catégories à surveiller votre activité, cliquez sur l'activité désirée, puis sur le bouton correspondant. Si vous changez d'avis, cliquez de nouveau sur le même bouton.

20.2. Désactiver le Bloqueur de trackers Bitdefender

Pour désactiver le Bloqueur de trackers Bitdefender :

- A partir de votre navigateur web :
  1. Ouvrez votre navigateur web.
  2. Cliquez sur l'icône à côté de la barre d'adresses de votre navigateur.
  3. Cliquez sur l'icône dans l'angle supérieur droit.
  4. Utilisez le bouton correspondant pour désactiver la fonctionnalité.

     L'icône de Bitdefender devient grise.
- À partir de l'interface de Bitdefender :
  1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans le panneau **BLOQUEUR DE TRACKERS**, cliquez sur **Paramètres**.
  3. Désactivez le bouton correspondant au navigateur pour lequel vous voulez désactiver l'extension.

20.3. Autoriser le tracking d'un site web

Pour autoriser le tracking lorsque vous visitez un site web en particulier, vous pouvez ajouter son adresse aux exceptions, comme suit :

1. Ouvrez votre navigateur web.
2. Cliquez sur l'icône  située à côté de la barre de recherche.
3. Cliquez sur l'icône  dans l'angle supérieur droit.
4. Si vous êtes sur le site web que vous voulez ajouter aux exceptions, cliquez sur **Ajouter le site web actuel à la liste**.

   Si vous voulez ajouter un autre site web, saisissez son adresse dans le champ correspondant, puis cliquez sur  .

21. VPN

L'application VPN peut être installée depuis votre produit Bitdefender et utilisée à chaque fois que vous voulez ajouter une couche supplémentaire de protection à votre connexion. Le VPN fait office de tunnel entre votre appareil et le réseau que vous utilisez pour sécuriser votre connexion, chiffrer vos données à l'aide d'une technologie comparable à celle utilisée par les banques et masquer votre adresse IP. L'intégralité du trafic est redirigée vers un serveur séparé, rendant ainsi votre appareil presque impossible à identifier par la multitude d'autres appareils qui utilise nos serveurs. En outre, quand vous êtes connecté à Internet via le VPN Bitdefender, vous pouvez accéder à des contenus qui ne seraient normalement pas disponibles dans votre région.

Note
Certains pays pratiquent la cybercensure. L'utilisation de VPN sur leur territoire est donc interdite par la loi. Pour éviter les conséquences juridiques, un message d'avertissement apparait lors de votre première utilisation du VPN de Bitdefender. En continuant à utiliser l'application, vous confirmez avoir connaissance des réglementations applicables dans le pays où vous êtes et des risques auxquels vous vous exposez.

21.1. Ouvrir l'application VPN

Pour accéder à l'interface principale du VPN Bitdefender, utilisez l'une des méthodes suivantes :

- Dans la zone de notification
  1. Faites un clic droit sur l'icône  de la zone de notification, puis sélectionnez **Afficher**.
- À partir de l'interface de Bitdefender :
  1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans le panneau **VPN**, cliquez sur **Ouvrir le VPN**.

21.2. Interface du VPN

L'interface du VPN affiche l'état de l'application, connectée ou déconnectée. Pour les utilisateurs de la version gratuite, l'emplacement du serveur le plus

approprié est automatiquement défini par Bitdefender, tandis que les utilisateurs de la version Premium peuvent changer l'emplacement du serveur. Pour plus d'informations sur les abonnements au VPN, reportez-vous à « *Abonnements* » (p. 132).

Pour vous connecter ou vous déconnecter, cliquez simplement sur l'état affiché en haut de l'écran, ou faites un clic droit sur l'icône de la zone de notification. L'icône de la zone de notification présente une coche verte lorsque le VPN est connecté, et une coche rouge lorsqu'il est déconnecté.

La durée de connexion et l'utilisation de bande passante sont affichées dans la partie inférieure de l'interface.

Pour visualiser l'intégralité de la zone du **Menu**, cliquez sur l'icône ☰ située en haut à gauche. Vous disposez des options suivantes :

- **Mon compte** - affiche des informations sur votre compte Bitdefender et sur votre abonnement au VPN. Cliquez sur **Changer de compte** si vous voulez vous connecter avec un autre compte.

  Cliquez sur **Ajouter ici** pour ajouter un code d'activation pour Bitdefender Premium VPN.

- **Paramètres** – vous pouvez personnaliser le produit en fonction de vos besoins . Les paramètres sont regroupés en deux catégories :

  - **Généraux**
    - Notifications
    - Démarrage - choisissez d'exécuter ou non le VPN Bitdefender au démarrage.
    - Rapports produits - envoyer des rapports produits anonymes pour nous aider à améliorer votre expérience
    - Mode sombre
    - Langue
  - **Avancés**
    - Kill Switch Internet - cette fonctionnalité suspend temporairement tout le trafic Internet si la connexion VPN s'interrompt accidentellement. Dès que vous êtes de retour en ligne, la connexion VPN est rétablie.

- Autoconnect - Connecte automatiquement le VPN Bitdefender lorsque vous accédez à un réseau Wi-Fi public/non sécurisé ou lorsqu'une application de partage de fichiers entre pairs est lancée

- **Assistance** - vous pouvez accéder à notre plateforme d'assistance sur laquelle vous pourrez consulter un article utile sur la façon d'utiliser le VPN Bitdefender ou nous faire part de vos commentaires.

- **À propos** - Informations sur la version installée de l'appli.

21.3. Abonnements

Le VPN Bitdefender vous offre gratuitement 200 Mo de trafic par appareil pour sécuriser votre connexion quand vous le souhaitez, et vous connecte automatiquement au meilleur serveur disponible.

Pour bénéficier d'un trafic illimité et d'un accès total aux contenus du monde entier en choisissant vous-même l'emplacement de votre serveur, passez à la version Premium.

Vous pouvez passer à la version de Bitdefender Premium VPN en cliquant sur le bouton **Mettre à niveau** sur l'interface du produit.

L'abonnement de Bitdefender Premium VPN est indépendant de l'abonnement gratuit à Bitdefender Antivirus Plus, et vous pourrez donc l'utiliser pendant toute sa période de validité, quel que soit l'état de votre abonnement à la solution de sécurité. Lorsque l'abonnement de Bitdefender Premium VPN expire, mais que celui de Bitdefender Antivirus Plus est toujours actif, vous repassez automatiquement à la version gratuite.

Le VPN Bitdefender est un produit multiplateforme disponible dans les produits Bitdefender compatibles avec Windows, macOS, Android, et iOS. Avec un abonnement Premium, vous pourrez utiliser votre abonnement sur tous les produits, si vous vous vous connectez avec le même compte Bitdefender.

22. 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 lésinent pas 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 privés. Pour plus d'informations, reportez-vous à « *Le Password Manager protège vos identifiants* » (p. 119).

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 le 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 appareil est connecté à des réseaux Wi-Fi 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™.

22.1. Utiliser Bitdefender Safepay™

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

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

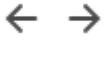
- À partir de l'interface de Bitdefender :
  1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans le panneau **SAFEPAY**, cliquez sur **Paramètres**.
  3. Dans la fenêtre **Safepay**, cliquez sur **Lancer Safepay**.
- À partir de Windows :
  - Dans **Windows 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.

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 sur et en sélectionnant **Imprimer**.

Note
Pour basculer entre Bitdefender Safepay™ et le bureau de Windows, appuyez sur les touches **Alt+Tab**, ou cliquez sur l'option **Passer au Bureau** située en haut à gauche de la fenêtre.

22.2. Configurer les paramètres

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

Appliquer les règles de Bitdefender Safepay aux domaines visités

Les sites web que vous avez ajoutés aux Marque-pages avec l'option **Ouvrir automatiquement dans Safepay** apparaitront ici. Si vous ne voulez plus ouvrir automatiquement un site web de la liste avec Bitdefender Safepay™, cliquez sur la croix dans la colonne **Supprimer**.

Bloquer les fenêtres publicitaires

Vous pouvez choisir de bloquer les fenêtres publicitaires en cliquant sur le bouton correspondant.

Vous pouvez également créer une liste de sites Web dont vous autorisez les fenêtres publicitaires. 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 retirer un site Web de la liste, sélectionnez le X correspondant à l'entrée désirée.

Gérer les plugins

Vous pouvez choisir si vous souhaitez activer ou désactiver des plugins spécifiques dans Bitdefender Safepay™.

Gérer les certificats

Vous pouvez importer des certificats de votre système dans un stockage de certificats.

Cliquez sur **IMPORTER** et suivez l'assistant pour utiliser les certificats dans Bitdefender Safepay™.

Utiliser le clavier virtuel

Le clavier virtuel va apparaître automatiquement lorsqu'un champ mot de passe est sélectionné.

Utilisez le bouton correspondant pour activer ou désactiver la fonctionnalité.

Confirmation de l'impression

Activez cette option si vous souhaitez avoir à confirmer le lancement d'une impression.

22.3. 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 ••• et choisissez **Marque-pages** pour ouvrir la page des 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. Saisissez l'URL et le titre du marque-pages puis 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.

22.4. Désactiver les notifications de Safepay

Le produit Bitdefender est configuré de sorte à vous avertir via une fenêtre contextuelle lorsqu'un site bancaire est détecté.

Pour désactiver les notifications de Safepay:

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **SAFEPAY**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Paramètres**, désactivez l'interrupteur situé à côté de **Notifications Safepay**.

22.5. Utilisation du VPN avec Safepay

Pour procéder à des paiements dans un environnement sécurisé lorsque vous êtes connecté à des réseaux non protégés, le produit Bitdefender peut être configuré de sorte à activer automatiquement le VPN en même temps que Safepay.

Pour activer l'application VPN lors de l'utilisation de Safepay :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **SAFEPAY**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Paramètres**, activez l'interrupteur situé à côté de **Utiliser le VPN avec Safepay**.

23. PROTECTION USB

La fonction AutoRun intégrée aux systèmes d'exploitation Windows est très utile car elle permet aux appareils 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 menaces pour se lancer automatiquement et infiltrer votre appareil 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 menaces. Lorsqu'un périphérique USB est immunisé, les menaces ne peuvent plus le configurer pour qu'il exécute une application spécifique lorsqu'il est connecté à un appareil fonctionnant sous Windows.

Pour immuniser un appareil USB :

1. Connectez le lecteur flash à votre appareil.
2. Localisez sur votre appareil 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 menaces de type AutoRun** s'affichera au lieu de l'option Immuniser.

Pour empêcher que votre appareil ne lance des menaces 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).

UTILITAIRES

24. 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
- Profil Wi-Fi public
- Profil Mode batterie

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 lorsque les profils Travail, Film et Jeu sont activés :

- Toutes les alertes et fenêtres de notification de Bitdefender sont désactivées.
- La Mise à jour automatique est reportée.
- Les analyses planifiées sont reportées.
- Assistant de recherche est désactivé.
- Les notifications sur les promotions sont désactivées.

En fonction de votre activité, les paramètres du système suivants s'appliquent lorsque les profils Travail, Film et Jeu sont activés :

- Les mises à jour automatiques de Windows sont reportées.
- Les alertes et fenêtres contextuelles 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.

Lorsqu'il fonctionne sous le profil Wi-Fi public, Bitdefender Antivirus Plus est configuré pour exécuter les paramètres de programme suivants :

- Advanced Threat Defense est activé
- Les paramètres suivants de la Prévention des menaces en ligne sont activés :
  - Analyse Web chiffrée
  - Protection contre la fraude
  - Protection contre le phishing

24.1. Profil Travail

Effectuer plusieurs tâches au travail comme envoyer des courriels, lancer 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 :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone profil Travail.
4. 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
5. Cliquez sur **ENREGISTRER** pour sauvegarder les modifications et fermez 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 d'applications professionnelles**.

Pour ajouter manuellement des applications à la Liste d'applications professionnelles dans le profil Travail :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone profil Travail.
4. Dans la fenêtre **Paramètres du profil Travail**, cliquez sur **Liste des applications**.
5. Cliquez sur **AJOUTER**.

   Une nouvelle fenêtre apparaît. Localisez le fichier exécutable du jeu, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

24.2. 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. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Film.
4. 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

5. Cliquez sur **ENREGISTRER** pour sauvegarder les modifications et fermez la fenêtre.

Ajouter manuellement des lecteurs vidéo à la liste du profil Film

Si Bitdefender ne passe pas automatiquement au profil Film lorsque vous lancez un lecteur vidéo spécifique, vous pouvez ajouter manuellement cette application à la **Liste d'applications de films**.

Pour ajouter manuellement des lecteurs vidéo à la liste d'applications de films dans le profil Film :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Film.
4. Dans la fenêtre **Paramètres du profil Film**, cliquez sur **Liste des lecteurs vidéo**.
5. Cliquez sur **AJOUTER**.

   Une nouvelle fenêtre apparaît. Localisez le fichier exécutable du jeu, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

24.3. 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 :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton **Configurer** dans la zone Profil Jeu.
4. 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
5. Cliquez sur **ENREGISTRER** pour sauvegarder les modifications et fermez la fenêtre.

Ajouter manuellement des jeux à la Liste des jeux.

Si Bitdefender ne passe pas automatiquement au profil Jeu lorsque vous lancez un jeu ou une application spécifique, vous pouvez ajouter manuellement cette application à la **Liste d'applications de jeu**.

Pour ajouter manuellement des jeux à la Liste d'applications de jeu dans le profil Jeu :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Jeu.
4. Dans la fenêtre **Paramètres du profil Jeu**, cliquez sur **Liste d'applications de jeu**.
5. Cliquez sur **AJOUTER**.

   Une nouvelle fenêtre apparaît. Localisez le fichier exécutable du jeu, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

24.4. Profil Wi-Fi public

Envoyer des courriels, saisir des identifiants sensibles ou faire des achats en ligne lorsque vous êtes connecté à des réseaux sans fil non sécurisés peut présenter un risque pour la sécurité de vos données personnelles. Le profil Wi-Fi public ajuste les paramètres du produit afin de vous donner la possibilité d'effectuer des paiements en ligne et d'utiliser des informations sensibles dans un environnement protégé.

Configurer le profil Wi-Fi public

Pour configurer Bitdefender afin qu'il applique les paramètres du produit lorsque vous êtes connecté à un réseau sans fil non sécurisé :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone profil Wi-Fi public.
4. Laissez cochée la case **Ajuster les paramètres du produit pour renforcer la protection en cas de connexion à un réseau Wi-Fi public non sécurisé**.
5. Cliquez sur **Enregistrer**.

24.5. Profil 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.

Configurer le mode Batterie

Pour configurer le mode Batterie :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton **Configurer** dans la zone Profil Mode Batterie.
4. 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.

5. Cliquez sur **ENREGISTRER** pour sauvegarder les modifications et fermez la fenêtre.

Saisissez une valeur correcte dans la case ou choisissez-en une à l'aide des flèches bas et haut pour indiquer lorsque le système doit commencer à fonctionner en mode Batterie. Le mode est activé par défaut lorsque le niveau de charge de batterie est inférieur à 30 %.

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.

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.

24.6. 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 :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans l'onglet **Profils**, cliquez sur **Paramètres**.

3. Descendez jusqu'à voir l'option d'Optimisation en temps réel, puis utiliser le bouton Activer/Désactiver correspondant.

25. PROTECTION DES DONNÉES

25.1. 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 appareil 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. Cliquez sur **Supprimer de façon permanente**, puis confirmez que vous souhaitez poursuivre cette procédure.

   Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
4. Les résultats sont affichés. Cliquez sur **Terminer** pour quitter l'assistant.

Vous pouvez également détruire des fichiers depuis l'interface de Bitdefender, comme suit :

1. Cliquez sur **Utilitaires** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **Protection des données**, cliquez sur **Destructeur de fichiers**.
3. Suivez l'assistant du destructeur de fichiers :
   a. Cliquez sur le bouton **Ajouter des dossiers** pour ajouter les fichiers ou dossiers que vous souhaitez supprimer définitivement.

      Sinon, glissez-déposez les fichiers ou dossiers vers cette fenêtre.
   b. Cliquez sur **Supprimer de façon permanente**, puis confirmez que vous voulez poursuivre cette procédure.

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

c. **Résumé des résultats**

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

RÉSOLUTION DE PROBLÈMES

26. 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 le service d'assistance de Bitdefender comme indiqué dans le chapitre « *Assistance* » (p. 175).

26.1. 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 toute solution de sécurité que vous utilisiez avant d'installer Bitdefender. Pour

plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 75).

- **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'appareil deviendra lent, notamment lorsque plusieurs applications s'exécuteront simultanément. Pour plus d'informations, reportez-vous à « *Configuration requise* » (p. 3).

- **Vous avez installé des applications que vous n'utilisez pas**.

  Tout appareil possède des programmes ou des applications que vous n'utilisez pas. 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 logiciels malveillants. Les logiciels espions, les programmes malveillants, les chevaux de Troie et les publiciels nuisent tous aux performances de votre appareil. 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 logiciels malveillants menaçant la sécurité de votre système.

  Pour commencer l'Analyse du système :

  1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
  3. Dans la fenêtre **Analyses**, cliquez sur le bouton **Lancez l'analyse** situé à côté d'**Analyse système**.
  4. Suivez les étapes de l'assistant.

26.2. 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, réinstallez Bitdefender :

  - Dans **Windows 7** :
    1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
    2. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
    3. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
    4. Attendez la fin du processus de réinstallation, 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** et sélectionnez **Désinstaller**.
    4. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
    5. Attendez la fin du processus de réinstallation, 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** et sélectionnez **Désinstaller**.
    4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
    5. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.

6. Attendez la fin du processus de réinstallation, puis redémarrez votre système.

> **Note**
> En suivant la procédure de réinstallation, les réglages personnalisés sont enregistrés et disponibles sur le nouveau produit installé. D'autres réglages peuvent être repassés à leur configuration par défaut.

- **Bitdefender n'est pas la seule solution de sécurité installée sur votre système**.

  Dans ce cas :

  1. Supprimer l'autre solution de sécurité. Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 75).
  2. Réinstaller Bitdefender :
     - Dans **Windows 7** :
       a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
       b. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
       c. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
       d. Attendez la fin du processus de réinstallation, 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** et sélectionnez **Désinstaller**.
       d. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
       e. Attendez la fin du processus de réinstallation, 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** et sélectionnez **Désinstaller**.
  d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
  e. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
  f. Attendez la fin du processus de réinstallation, puis redémarrez votre système.

> **Note**
> En suivant la procédure de réinstallation, les réglages personnalisés sont enregistrés et disponibles sur le nouveau produit installé. D'autres réglages peuvent être repassés à leur configuration par défaut.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 175).

26.3. 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 Advanced Threat Defense détecte à tort certaines applications comme étant malveillantes.

Advanced Threat Defense est une fonctionnalité de 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 Advanced Threat Defense.

Lorsque cette situation se produit, vous pouvez empêcher l'application correspondante d'être surveillée par Advanced Threat Defense.

Pour ajouter un programme à la liste d'exceptions :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **DÉFENSE CONTRE LES MENACES AVANCÉES**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres**, cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez le chemin de l'exécutable que vous souhaitez exclure de l'analyse dans le champ correspondant.

   Sinon, vous pouvez naviguer jusqu'à l'exécutable en cliquant sur le bouton Parcourir situé sur la droite de l'interface, le sélectionner puis cliquer sur **OK**.
6. Activez l'interrupteur situé à côté de **Défense contre les menaces avancées**.
7. Cliquez sur **Enregistrer**.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 175).

26.4. Que faire quand Bitdefender bloque un site web, un domaine, une adresse IP ou une application en ligne pourtant sûr

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, un domaine, une adresse IP 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, un domaine, une adresse IP ou une application est bloquée de façon répétée, elle peut être ajoutée à une liste d'exceptions afin de ne pas être analysée par les moteurs de Bitdefender et de permettre une navigation sans interruptions.

Pour ajouter un site Web aux **Exceptions** :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PRÉVENTION DES MENACES EN LIGNE**, cliquez sur **Paramètres**.
3. Cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez dans le champ correspondant le nom du site Internet, le nom du domaine ou l'adresse IP que vous souhaitez ajouter aux exceptions.
6. Cliquez sur l'interrupteur situé à côté de **Prévention des menaces en ligne**.
7. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Seuls les sites web, domaines, adresses IP et les applications en lesquels vous avez pleinement confiance devraient être ajoutés à cette liste. Ils ne seront pas analysés par les moteurs suivants : menaces, phishing et fraude.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 175).

26.5. 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 la dernière base de données d'information sur les menaces de Bitdefender :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Mise à jour**.
3. Activez le bouton **Mise à jour silencieuse**.
4. La prochaine fois qu'une mise à jour sera disponible, il vous sera demandé de sélectionner la mise à jour que vous voulez télécharger. Sélectionnez uniquement **Mise à jour des signatures**.
5. Bitdefender ne téléchargera et n'installera que la base de données d'information sur les menaces.

26.6. Les services Bitdefender ne répondent pas

Cet article vous aide à réparer 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 appareil en même temps que Bitdefender.

Pour réparer cette erreur, essayez ces solutions :

1. Attendez quelques instants et voyez si quelque chose change. L'erreur peut être temporaire.
2. Redémarrez l'appareil et attendez quelques instants jusqu'à ce que Bitdefender soit chargé. Ouvrez Bitdefender pour voir si l'erreur persiste. Redémarrer l'appareil 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. 75).

Si l'erreur persiste, veuillez contacter les représentants de notre service d'assistance pour obtenir de l'aide, comme indiqué dans la section « *Assistance* » (p. 175).

26.7. La fonctionnalité Saisie automatique de mon Wallet ne fonctionne pas

Vous avez enregistré vos identifiants en ligne dans votre Bitdefender Password Manager et avez remarqué que la saisie automatique ne fonctionne

pas. Ce problème se produit généralement lorsque l'extension de Bitdefender Wallet 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 Wallet** et cliquez sur **Permettre**.
- Dans **Mozilla Firefox :**
  1. Ouvrez Mozilla Firefox.
  2. Cliquez sur le bouton **Ouvrir le menu** situé dans le coin supérieur droit de l'écran.
  3. Cliquez sur Modules.
  4. Cliquez sur Extensions.
  5. Sélectionnez **Portefeuille Bitdefender**, puis cliquez sur l'interrupteur qui se trouve à côté.
- Dans **Google Chrome :**
  1. Ouvrez Google Chrome.
  2. Allez sur l'icône du Menu.
  3. Cliquez sur Plus d'outils.
  4. Cliquez sur Extensions.
  5. Sélectionnez **Portefeuille Bitdefender**, puis cliquez sur l'interrupteur correspondant.

Note
Le module sera activé une fois que vous aurez redémarré votre navigateur Web.

Vérifiez maintenant si la fonctionnalité de saisie automatique de Wallet 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 « *Assistance* » (p. 175).

26.8. 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 supprimer complètement Bitdefender de votre système :

- Dans **Windows 7** :
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
  2. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
  3. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.
  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. Localisez **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
  4. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.
  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 **Bitdefender Antivirus Plus** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.
6. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

26.9. 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 le résoudre :

  1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 76).
  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** et sélectionnez **Désinstaller**.
       c. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.
       d. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
       e. 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** et sélectionnez **Désinstaller**.

d. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.

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

f. 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** et sélectionnez **Désinstaller**.

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

e. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.

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

g. 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 le résoudre :

  1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 76).
  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 le résoudre :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 76).
2. Utilisez l'option Restauration du système de Windows pour restaurer l'appareil à une date antérieure à l'installation du produit Bitdefender.
3. Redémarrez le système en mode normal et contactez les représentants de notre service d'assistance pour obtenir de l'aide, comme indiqué dans la section « *Assistance* » (p. 175).

27. SUPPRESSION DES MENACES DE VOTRE SYSTÈME

Les menaces peuvent affecter votre système de nombreuses manières et l'approche de Bitdefender dépend du type d'attaque. Les menaces 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 la menace de votre système. Dans ce cas, votre intervention est nécessaire.

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter le service d'assistance de Bitdefender comme indiqué dans le chapitre « *Assistance* » (p. 175).

27.1. Mode de secours

L'**Environnement de secours** est une fonctionnalité Bitdefender qui vous permet d'analyser et de désinfecter toutes les partitions de disques durs existantes qui se trouvent dans votre système d'exploitation ou en dehors de celui-ci.

L'Environnement de secours Bitdefender est intégré à Windows RE,

Démarrer votre système en mode Environnement de secours

Vous pouvez uniquement passer sur l'Environnement de récupération depuis votre produit Bitdefender, comme suit :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Cliquez sur le bouton **Ouvrir** situé à côté d'**Environnement de secours**.
4. Cliquez sur **REDÉMARRER** dans la fenêtre qui s'affiche.

   L'Environnement de récupération de Bitdefender se chargera dans quelques instants.

Analyser votre système en mode Environnement de secours

Pour analyser l'Environnement de secours de votre système :

1. Entrez dans l'Environnement de récupération, comme indiqué dans « Démarrer votre système en mode Environnement de secours » (p. 167).
2. Le processus d'analyse de Bitdefender commence automatiquement quand le système charge l'Environnement de récupération.
3. Patientez jusqu'à la fin de l'analyse. Si une menace est détectée, suivez les instructions pour la supprimer.
4. Pour quitter l'Environnement de secours, cliquez sur le bouton **Fermer** situé dans la fenêtre contenant les résultats de l'analyse.

27.2. Que faire lorsque Bitdefender trouve des menaces sur votre appareil ?

Vous découvrirez peut-être qu'une menace est présente sur votre appareil par l'un des moyens suivants :

- Vous avez analysé votre appareil et Bitdefender y a détecté des éléments infectés.
- Une alerte de menaces vous informe que Bitdefender a bloqué une ou plusieurs menaces sur votre appareil.

Dans de telles situations, mettez à jour Bitdefender pour vous assurer de disposer de la dernière base de données d'information sur les menaces 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. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
   b. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
   c. Dans la fenêtre **Avancé**, désactivez **Bouclier Bitdefender**.
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 74).
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 n'a pas réussi à supprimer l'infection :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 76).
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 74).
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 « *Assistance* » (p. 175).

27.3. Comment nettoyer un menace 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 menaces dans ceux-ci, mais n'est pas capable de mener d'autres actions.

Si Bitdefender indique qu'une menace a été détectée dans une archive et qu'aucune action n'est disponible, cela signifie qu'il n'est pas possible de supprimer la menace en raison de restrictions sur les paramètres d'autorisation de l'archive.

Voici comment nettoyer une menace stockée dans une archive :

1. Identifiez l'archive où se trouve la menace en réalisant une analyse du système.
2. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
   b. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
   c. Dans la fenêtre **Avancé**, désactivez **Bouclier Bitdefender**.
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 du système afin de vous assurer qu'aucune autre infection n'est présente sur le système.

> **Note**
> Il est important de noter qu'une menace contenue dans une archive ne représente pas de menace immédiate pour votre système, puisque, pour infecter votre système, elle doit être décompressée et exécutée.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 175).

27.4. Comment nettoyer une menace dans une archive de messagerie ?

Bitdefender permet également de repérer les menaces dans les bases de données de courriels et les archives de courriels 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 une menace stockée dans une archive de messagerie électronique :

1. Analysez la base de données des courriels avec Bitdefender.
2. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
   b. Dans le panneau **ANTIVIRUS**, cliquez sur **Ouvrir**.
   c. Dans la fenêtre **Avancé**, désactivez **Bouclier Bitdefender**.
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 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/ 2016: 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 « *Assistance* » (p. 175).

27.5. Que faire si je soupçonne 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 vous assurer que votre système est protégé :

1. Exécuter une **Analyse du système** avec Bitdefender. Pour savoir comment faire cela, reportez-vous à « *Comment analyser mon système ?* » (p. 59).
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 service d'assistance afin que nous puissions vous aider.

   Pour savoir comment faire cela, consultez « *Assistance* » (p. 175).

27.6. 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 est extrait, le moteur d'analyse en temps réel de Bitdefender l'analyse automatiquement pour que votre appareil 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.

27.7. 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.

27.8. 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.

Ultra-compressé 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.

27.9. 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 menaces, 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

28. ASSISTANCE

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. 152) 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 depuis Bitdefender Antivirus Plus » (p. 175)
- « Contactez-nous via notre Centre de Support en ligne » (p. 176)

Contactez-nous directement depuis Bitdefender Antivirus Plus

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 le bouton **Assistance**, représenté par un **point d'interrogation** et situé dans la partie supérieure de l'interface Bitdefender.
2. Vous disposez des options suivantes :
   - **GUIDE D'UTILISATION**

     Accédez à notre base de données et recherchez les informations nécessaires.
   - **SUPPORT EN LIGNE**

     Consulter nos articles et vidéos en ligne.
   - **NOUS CONTACTER**

     Cliquez sur **CONTACTER LE SUPPORT** pour lancer l'Outil Support de Bitdefender et contacter le Support Client.

a. Compléter le formulaire de soumission avec les données nécessaires :
   i. Sélectionnez le type de problème que vous rencontrez.
   ii. Décrivez le problème que vous avez rencontré.
   iii. Cliquez sur **ESSAYER DE REPRODUIRE LE PROBLÈME** si vous rencontrez un problème avec le produit. Reproduisez le problème, puis cliquez sur **TERMINER** dans le cadre REPRODUCTION DU PROBLÈME.
   iv. Cliquez sur **CONFIRMER LE TICKET**.
b. Continuez à compléter le formulaire de soumission avec les données nécessaires :
   i. Saisissez votre nom complet.
   ii. Saisissez votre adresse e-mail.
   iii. Cochez la case d'acceptation de l'accord.
   iv. Cliquez sur **CRÉER UN PAQUET DE DÉBOGAGE**.

   Veuillez patienter pendant que Bitdefenderrecueille les informations sur le produit. Ces informations aideront nos ingénieurs à trouver une solution à votre problème.
c. Cliquez sur **FERMER** pour quitter l'assistant. Un de nos représentants vous contactera 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 https://www.bitdefender.fr/support/consumer/.

   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

   https://www.bitdefender.fr/support/nous-contacter.html et contactez nos représentants du support.

28.1. Assistance téléphonique :

Les Laboratoires 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.

Contacter l'assistance par téléphone :

- **Pour la France** : 0 800 961 161
- **Pour la Belgique** : +32 28 91 98 90

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 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 Bitdefender.

Bitdefender NE PEUT 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 Bitdefender. Par conséquent, Bitdefender ne peut 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, Bitdefender recommande que vous consultiez régulièrement notre site "Produits" à l'adresse suivante : https://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 Bitdefender.

Si une intervention sur site est nécessaire, l'analyste vous donnera de plus amples instructions concernant votre revendeur le plus proche.

29. 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 :

  https://www.bitdefender.fr/support/consumer/

- Forum du Support Bitdefender :

  https://forum.bitdefender.com/index.php?showforum=59

- Le portail de sécurité informatique Bitdefender blog :

  https://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.

29.1. 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 contre les menaces, 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

https://www.bitdefender.fr/support/consumer/.

29.2. 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 menances de votre appareil 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 https://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.

29.3. Portail Bitdefender blog

Bitdefender blog comprend de nombreuses informations sur la sécurité informatique. Vous pouvez découvrir ici les différentes menaces auxquelles votre ordinateurappareil 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 https://www.bitdefender.fr/blog/.

30. NOUS CONTACTER

Une communication efficace est la clé d'une relation réussie. Depuis 2001, 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.

30.1. Adresses Web

Ventes : sales@bitdefender.fr
Centre de support en ligne :https://www.bitdefender.fr/support/consumer/
Documentation : documentation@bitdefender.com
Distributeurs locaux : https://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 menace : virus_submission@bitdefender.com
Envoi de spams : spam_submission@bitdefender.com
Signaler un abus : abuse@bitdefender.com
Site Internet :https://www.bitdefender.fr

30.2. 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 https://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@bitdefender.fr. Veuillez rédiger votre e-mail en anglais pour optimiser le traitement de votre demande.

30.3. 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

Bitdefender SAS
49, Rue de la Vanne
92120 Montrouge
Téléphone : +33 (0)1 47 35 72 73
Ventes : sales@bitdefender.fr
Support technique : https://www.bitdefender.fr/support/nous-contacter.html
Site Web : https://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 : https://www.bitdefender.com/support/consumer.html
Site Web : https://www.bitdefender.com

Royaume-Uni et Irlande

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-mail : info@bitdefender.co.uk
Téléphone : (+44) 2036 080 456
Ventes : sales@bitdefender.co.uk
Support technique : https://www.bitdefender.co.uk/support/
Site Web : https://www.bitdefender.co.uk

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 : https://www.bitdefender.de/support/consumer.html
Site Web : https://www.bitdefender.de

Danemark

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Service administratif : +45 7020 2282
Support technique : http://bitdefender-antivirus.dk/
Site Web : http://bitdefender-antivirus.dk/

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 : https://www.bitdefender.es/support/consumer.html
Site Internet : https://www.bitdefender.es

Roumanie

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
Bucharest
Fax : +40 21 2641799
Téléphone du service commercial : +40 21 2063470
Email du service commercial : sales@bitdefender.ro
Support technique : https://www.bitdefender.ro/support/consumer.html
Site Internet : https://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 : https://www.bitdefender.com/support/consumer.html
Site Internet : https://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 Menaces persistantes avancées 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 cette menace.

L'objectif d'une menace persistante avancée 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 la menace 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.

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.

Attaque par dictionnaire

Les attaques qui essayent de pénétrer un système informatique en saisissant une combinaison de mots communs pour générer des mots de passe potentiels. La même méthode est utilisée pour deviner les clés de chiffrements des messages ou documents chiffrés. Les attaques par dictionnaire fonctionnent car de nombreuses personnes ont tendance à choisir des mots de passe simples à deviner et ne contenant qu'un seul mot.

Attaque par force brute

Les attaques qui essayent de pénétrer un système informatique en saisissant toutes les combinaisons de mots de passe possible, ce en commençant par les mots de passe les plus faciles à deviner.

Botnet

Le terme « botnet » est un mot composé de robot et de network (réseau). Les botnets sont des appareils connectés à Internet infectés par une menace et pouvant servir à envoyer des spams, voler des données, contrôler à distance les appareils vulnérables ou diffuser des logiciels espions, ransomwares, ou tout autre type de menace. Leur objectif est d'infecter autant d'appareils connectés que possible, comme les PC, serveurs, mobiles ou appareils de l'IoT appartenant à des grandes entreprises.

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.

Cheval de Troie

Programme destructeur qui prétend être une application normale. À la différence des programmes malveillants comme les vers, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout autant destructeurs. L'un des types les plus pernicieux de chevaux de Troie est un programme qui, sous couvert de supprimer les menaces de votre ordinateur, en installe en fait de nouvelles.

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.

Client de messagerie

Un client de messagerie est une application qui vous permet d'envoyer et recevoir des e-mails.

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.

Courriel

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

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.

Enregistreur de frappe

Un enregistreur de frappe est une application qui enregistre tout ce qui est saisi avec le clavier.

Les enregistreurs de frappe 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 d'assurance sociale).

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.

Exploits

Une manière de tirer profit des bugs et vulnérabilités (logicielles ou matérielles) qui sont présents sur un ordinateur. Les pirates peuvent ainsi prendre le contrôle des ordinateurs ou réseaux.

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.

Harcèlement en ligne

Lorsque des camarades ou des inconnus mènent des actions abusives envers des enfants dans le but de les blesser physiquement. Pour leur nuire sur le plan émotionnel, les assaillants envoient des messages malveillants ou des photos peu flatteuses, provoquant l'isolation de leurs victimes ou un sentiment de frustration.

Heuristique

Méthode basée sur des règles permettant d'identifier de nouvelles menaces. Cette méthode d'analyse ne s'appuie pas sur une base de données d'information sur les menaces spécifique. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'une menace existante. 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.

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.

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.

Menace

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des menaces peuvent également se répliquer. Toutes les menaces informatiques sont créées par des personnes. Une menace simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même une menace simple comme celle décrite est dangereuse puisqu'elle remplit vite la mémoire et bloque le système. Une menace plus dangereuse encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Mise à jour

Nouvelle version d'un logiciel ou d'un produit matériel, 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 sa propre fonctionnalité de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

Mise à jour des informations sur les menaces

La signature binaire de la menace, utilisée par la solution de sécurité pour détecter et éliminer la menace.

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 plugins pour certains formats.

Non-heuristique

Cette méthode d'analyse s'appuie sur une base de données d'information sur les menaces spécifique. L'avantage de l'analyse non-heuristique est

qu'elle n'est pas trompée par ce qui peut sembler être une menace et ne génère donc pas de fausses alertes.

Phishing

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.

Photon

Photon est une technologie Bitdefender innovante et discrète, conçue pour limiter l'impact de la solution de sécurité 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.

Portes dérobées

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.

Pot de miel

Un faux système d'ordinateur est créé pour attirer mes pirates afin d'étudier la façon dont ils agissent et identifient les méthodes hérétiques qu'ils utilisent pour collecter des informations sur le système. Les sociétés et les entreprises sont plus intéressées par la mise en place et l'utilisation de honeypots pour améliorer leur état de sécurité global.

Prédateurs en ligne

Individus cherchant à discuter avec des mineurs et des adolescents dans le but de les impliquer dans des activités sexuelles illégales. Les réseaux sociaux sont l'endroit idéal pour traquer les enfants vulnérables et les séduire dans le but de les faire se livrer à des activités sexuelles, en ligne ou en face à face.

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.

Publiciels

Les publiciels sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces publiciels 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 fenêtres publicitaires peuvent devenir contrariantes et, dans certains cas, nuire aux performances du système. De plus, les informations recueillies peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des conditions de l'accord de licence.

Ransomware

Les ransomwares sont des programmes malveillants qui tentent de soutirer de l'argent aux utilisateurs en bloquant leurs systèmes vulnérables. CryptoLocker, CryptoWall, et TeslaWall n'en sont que des variantes qui recherchent les systèmes personnels des utilisateurs.

L'infection peut se répandre via courriel, le téléchargement de pièces jointes, ou l'installation d'applications, sans prévenir l'utilisateur de ce qui se passe dans son système. Les utilisateurs réguliers et les entreprises sont ciblés par les pirates derrière les ransomwares.

Réseau privé virtuel (VPN)

C'est une technologie qui permet une connexion temporaire et chiffrée à un certain réseau plutôt qu'à un autre moins sécurisé. De cette façon, l'envoi et la réception de données sont protégés et chiffrés et plus difficiles à intercepter pour les pirates. Une preuve de sécurité est l'identification, qui ne peut se faire que via un identifiant et un mot de passe.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur d'amorçage

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 d'amorçage contient aussi un programme qui charge le système d'exploitation.

Spam

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des courriels non sollicités.

Spywares

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les logiciels espions sont généralement cachés dans des partagiciels et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des partagiciels et logiciels gratuits ne contiennent pas de logiciels espions. Une fois installé, le logiciel espion 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 bancaires.

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 logiciels espions 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 logiciels espions 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.

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 normes 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.

Témoins

Sur Internet, les témoins 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 témoins est encore en développement. Son but est de cibler directement les intérêts que vous avez exprimés. 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 "code SKU" (ce code barres se trouvant au dos des produits de consommation). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Trousse administrateur pirate (rootkit)

Une trousse administrateur 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 de ces trousses est de masquer des processus, des fichiers, des identifiants et des journaux. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les trousses administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des trousses administrateur. Cependant, ils sont principalement utilisés pour camoufler des menaces ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des menaces, les trousses administrateur pirates 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 journaux et passer inaperçus.

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 d'amorçage

Menace qui infecte le secteur d'amorçage d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus d'amorçage rendra la menace active en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez la menace active en mémoire.

Virus macro

Type de menace codée 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

Menace qui change de forme avec chaque fichier qu'elle infecte. Ces menaces n'ayant pas de forme unique bien définie, elles 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 : télécopieur, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.