Bitdefender INTERNET SECURITY

MANUEL D'UTILISATION

Bitdefender Internet Security
Manuel d'utilisation

Date de publication 12/07/2018

Mentions légales

Bitdefender

Table des matières

INSTALLATION

1. PRÉPARATION DE L'INSTALLATION

Avant d'installer Bitdefender Internet Security, procédez comme suit pour faciliter l'installation :

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

2. CONFIGURATION REQUISE

Vous pouvez installer Bitdefender Internet Security uniquement sur les ordinateurs fonctionnant avec les systèmes d'exploitation suivants :

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

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

Note

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

- 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 système minimale

- 2 Go d'espace disque disponible
- Dual Core 1.6 GHz
- 1 Go de mémoire (RAM)

2.2. Configuration système recommandée

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

2.3. Configuration logicielle requise

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

- Microsoft Edge 40 et supérieur
- Internet Explorer 10 ou version supérieure
- Mozilla Firefox 51 et version supérieure
- Google Chrome 34 et supérieur
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 ou version supérieure

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

3.1. 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 Internet Security est activé.

Pour télécharger Bitdefender Internet Security 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**

     Sélectionnez cette option et sauvegardez le fichier d'installation.

   - **Protéger d'autres appareils**

     Sélectionnez cette option, puis cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR E-MAIL**. 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.

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 des zones devant être améliorées 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'ordinateur pour terminer la désinstallation des solutions de sécurité détectées.

Le paquet d'installation de Bitdefender Internet Security 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 Internet Security.

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 Internet Security.

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.

Les zones critiques de votre système font l'objet d'une analyse des menaces, les dernières versions des fichiers d'applications sont téléchargées et installées et les services de Bitdefender sont lancés. Cette étape peut prendre quelques minutes. Cliquez sur **PASSER L'ANALYSE** si vous voulez analyser plus tard votre système. Pour plus d'informations sur l'exécution d'une analyse du système, reportez-vous à « *Exécuter une analyse du système* » (p. 94).

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. Cliquez sur **COMMENCER À UTILISER Bitdefender** pour continuer.

Étape 4 - 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 Internet Security.

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 des zones devant être améliorées 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'ordinateur 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 Internet Security.

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 Internet Security.

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.

Les zones critiques de votre système sont analysées et les services Bitdefender sont lancés. Cette étape peut prendre quelques minutes. Cliquez sur **PASSER L'ANALYSE** si vous voulez analyser plus tard votre système. Pour plus d'informations sur l'exécution d'une analyse du système, reportez-vous à « *Exécuter une analyse du système* » (p. 94).

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. Cliquez sur **COMMENCER À UTILISER Bitdefender** pour continuer.

Étape 4 - 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. 34).

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 contenir au moins 8 caractères et contenir un chiffre.
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 le lien **Se Connecter** puis tapez l'adresse email et le mot de passe de votre compte Bitdefender.

   Cliquez sur **Se connecter** pour poursuivre.
2. Si vous avez oublié le mot de passe de votre compte ou que vous souhaitez simplement reconfigurer celui déjà existant, cliquez sur **Mot de passe oublié**. Saisissez votre adresse e-mail, puis cliquez sur **MOT DE PASSE OUBLIÉ**. Allez voir vos emails et suivez les instructions fournies pour configurer un nouveau mot de passe pour votre compte Bitdefender.

> **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 5 - 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 6 - 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 Internet Security.

INTRODUCTION

4. FONCTIONS DE BASE

Une fois Bitdefender Internet Security installé, votre ordinateur est protégé contre toutes sortes de menaces (comme les malwares, les spywares, les ransomwares, les exploits, les botnets et les chevaux de Troie) et les menaces Internet (comme les pirates, le phishing et le spam).

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 vos données personnelles, faisant ainsi de votre machine une victime de potentielles futures cyberattaques. Pour éviter de vous retrouver dans cette situation délicate, vous pouvez installer et utiliser l'application « *VPN* » (p. 161).

Vous pouvez retenir vos mots de passe et comptes en ligne en les enregistrant dans « *Protection Password Manager de vos identifiants* » (p. 153) un wallet. Avec un seul mot de passe principal, vous pouvez protéger votre vie privée des intrus susceptibles de s'en prendre à votre argent.

« *Protection de webcam* » (p. 138)empêche les applications inconnues d'accéder à votre caméra vidéo, empêchant ainsi toute tentative de piratage. L'accès des applications populaires à votre webcam sera autorisé ou bloqué en fonction du choix des utilisateurs de Bitdefender.

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 « *Wi-Fi Security Advisor* » (p. 134).

Vos fichiers personnels stockés en local ou dans le cloud tels que vos documents, photos ou films, restent bien protégés des menaces les plus dangereuses du moment, notamment des ransomwares. Pour en savoir plus

sur la manière de mettre à l'abri vos fichiers, rendez-vous sur« *Safe Files* » (p. 141).

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. 144).

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. 189).

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 ordinateur et vos données.

Pour utiliser les fonctionnalités en ligne de Bitdefender Internet Security et gérez vos abonnements et appareils, accédez à votre compte Bitdefender. Pour plus d'informations, reportez-vous à « *Bitdefender Central* » (p. 34).

La section « Comment faire pour » (p. 45) 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. 198) des solutions possibles aux problèmes les plus courants.

4.1. Ouverture de la fenêtre de Bitdefender

Pour accéder à l'interface principale de Bitdefender Internet Security, suivez les étapes ci-dessous :

- Dans **Windows 7** :
  1. Cliquez sur **Démarrer** et allez dans **Programmes**.
  2. Cliquez sur **Bitdefender**.

3. Cliquez sur **Bitdefender Internet Security** 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 ordinateur. Lorsqu'un événement concernant la sécurité de votre système ou de vos données a lieu, un nouveau message est ajouté aux Événements de Bitdefender, comme lorsqu'un nouvel email 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 ordinateur, 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 permettre d'appliquer une action supplémentaire 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.

Pour autoriser Bitdefender à activer les profils :

1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
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 profil peut être manuellement activé à la fois.

Pour plus d'informations sur les Profils, reportez-vous à « *Profils* » (p. 189)

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 ordinateur, 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 signaler via une fenêtre pop-up les offres promotionnelles disponibles. Cela vous donne la possibilité de bénéficier de tarifs avantageux et de protéger vos appareils plus longtemps.

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.

4.7. Service analyse antimalware

Bitdefender intègre Microsoft Antimalware Scan Interface (AMSI), afin de vous permettre de vous protéger contre les malwares dynamiques basés sur des scripts, et les cyberattaques inhabituelles. AMSI est une interface générique qui permet aux applications et services de s'intégrer aux produits Bitdefender.

Pour activer ou désactiver l'intégration avec Antimalware Scan Interface :

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 d'intégration avec Antimalware Scan Interface est activée par défaut, et uniquement disponible sur Windows 10.

5. INTERFACE DE BITDEFENDER

Bitdefender Internet Security 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 à votre compte Bitdefender, aux paramètres, aux notifications et aux rubriques Bitdefender sur la configuration détaillée et les tâches administratives avancées. Vous pouvez également nous contacter pour obtenir de l'aide si vous avez des questions ou si vous rencontrez une situation anormale.

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

5.1. Icône de la zone de notification

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

Note
L'icône de Bitdefender ne sera peut-être pas visible en permanence. Pour que l'icône apparaisse en permanence :

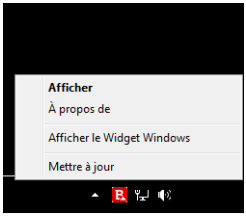
- Dans **Windows 7, Windows 8 et Windows 8.1** :

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 **Propriétés**.
2. Cliquez sur **Personnaliser...** dans la fenêtre de la barre des tâches.
3. Cliquez sur le lien **Choisir quelles icônes apparaissent dans la barre des tâches** dans la fenêtre **Notifications & actions**.
4. Activez le bouton à côté de **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 de la barre d'état

- **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.
- **Afficher / Masquer le Widget Windows** - permet d'activer / de désactiver le Widget Windows.
- **Mettre à jour** - lance immédiatement une mise à jour. Vous pouvez suivre l'état de mise à jour dans le panneau Mise à jour de la fenêtre principale de Bitdefender.

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

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 configurer et lancer des analyses antivirus, accéder aux paramètres du Pare-feu, protéger vos fichiers et applications des attaques de ransomware, récupérer les données éventuellement chiffrées par un ransomware, et configurer la protection de votre navigation sur Internet.
- **Vie privée**. D'ici, vous pouvez créer des gestionnaires de mots de passe pour vos comptes en ligne, empêcher les regards indiscrets d'accéder à votre webcam, procéder à des paiements en ligne dans un environnement sécurisé, ouvrir l'application VPN, et protéger vos enfants en consultant et en limitant leurs activités en ligne.
- **Notifications**. Là, vous pouvez accéder aux notifications générées.
- **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.
- **Configuration**. Là, vous pouvez accéder aux Paramètres généraux.
- **Support**. Là, quand vous avez besoin d'assistance pour régler un problème avec votre Bitdefender Internet Security, vous pouvez contacter le service de support technique de Bitdefender.

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 ordinateur.

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

Actions rapides
: Là, 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 ordinateur et de vos données et vous en informer. Les problèmes détectés comprennent la désactivation d'importants paramètres de protection et d'autres conditions pouvant constituer un risque pour la sécurité.

Lorsque des problèmes affectent la sécurité de votre ordinateur, l'état affiché en haut de l'interface de Bitdefender devient rouge. L'état indique la nature des problèmes dont souffre 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 pendant que vous vaquez à d'autres tâches, Bitdefender Autopilot joue le rôle de 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 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 sur les recommandations de l'Autopilot, le produit Bitdefender est configuré de sorte à faire apparaitre des notifications via une fenêtre pop-up.

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 ordinateur.
- **Analyse du système**. Exécutez une analyse du système pour vérifier qu'aucune menace n'est présente sur votre ordinateur.
- **Analyse de vulnérabilités**. Analysez votre ordinateur à la recherche de vulnérabilités pour vous assurer que toutes les applications, ainsi que le système d'exploitation, sont mis à jour et fonctionnent correctement.
- **Vérifier la sécurité du Wi-Fi**. Ouvrez Wi-Fi Security Advisor pour vérifier si le réseau sans fil domestique auquel vous êtes connecté est fiable ou non et s'il a des vulnérabilités.
- **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 ordinateur.
- **Coffres-forts**. Créez des coffres-forts dans lesquels stocker vos documents sensibles et confidentiels.

Pour commencer à protéger d'autres appareils avec Bitdefender:

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

   Vous êtes redirigé vers la page web compte Bitdefender. Assurez-vous que vous êtes connectés avec vos identifiants.

2. Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT** dans la fenêtre qui apparait.

3. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR E-MAIL**. 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 Bitdefender, consultez la boite de messagerie que vous avez précédemment saisie, et appuyez sur le bouton de téléchargement.

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

- Bitdefender Internet Security 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.
- Contrôle parental Bitdefender pour macOS, iOS et Android.

5.4. Les rubriques Bitdefender

Le produit Bitdefender est composé de deux sections divisées en fonctionnalités utiles pour vous aider à rester protégé pendant que vous travaillez, naviguez sur le web, jouez ou lors de vos paiements en ligne.

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

5.4.1. Protection

Dans la rubrique Protection, vous pouvez configurer les réglages de sécurité avancés, gérer vos amis et les spammeurs, afficher et modifier les paramètres de connexion réseau, configurer les fonctions Prévention des menaces en ligne et Safe Files, vérifier et corriger les vulnérabilités potentielles du système et évaluer la sécurité du réseau sans fil auquel vous êtes connecté.

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 malwares, 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 (Environnement de récupération Windows 10)

Pour plus d'informations sur les tâches d'analyse et sur comment configurer la protection antivirus, consultez « *Protection antivirus* » (p. 87).

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 des menaces en ligne* » (p. 111).

Pare-feu bidirectionnel

Le pare-feu vous protège lorsque vous êtes connecté à des réseaux et à internet en filtrant toute tentative de connexion.

Pour plus d'informations sur la configuration du pare-feu, consultez « *Pare-feu* » (p. 124).

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. 109).

ANTIPOURRIEL

La fonctionnalité antispam Bitdefender protège votre boîte de réception contre les e-mails indésirables en filtrant le trafic de messagerie POP3.

Pour plus d'informations sur la protection antispam, reportez-vous à « *Antispam* » (p. 114).

VULNÉRABILITÉ

La fonctionnalité Vulnérabilité vous aide à maintenir à jour votre système d'exploitation et les applications que vous utilisez régulièrement, ainsi qu'à identifier les réseaux sans fil non protégés auxquels vous vous connectez.

Cliquez sur **Analyse de Vulnérabilité** dans la fonctionnalité Vulnérabilité pour commencer à identifier les mises à jour critiques de Windows, les

mises à jour d'applications, les mots de passe vulnérables appartenant à des comptes Windows et les réseaux sans fil qui ne sont pas sûrs.

Cliquez sur **Wi-fi security** pour voir la liste de 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 des éventuels espions.

Pour plus d'informations sur la configuration de la protection contre les vulnérabilités, reportez-vous à « *Vulnérabilité* » (p. 130).

SAFE FILES

La fonctionnalité Safe Files garantit que vos fichiers personnels restent protégés des attaques de ransomware.

Pour plus d'informations sur la manière de configurer Safe Files pour protéger vos fichiers personnels contre les attaques de ransomwares, reportez-vous à « *Safe Files* » (p. 141).

NETTOYAGE DES RANSOMWARES

La fonctionnalité de Nettoyage 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. 144).

5.4.2. Vie privée

La rubrique Vie privée vous permet d'ouvrir l'application VPN Bitdefender, de chiffrer vos données confidentielles, de protéger vos transactions en ligne, de sécuriser votre webcam et votre navigation sur Internet et de protéger vos enfants en vous offrant la possibilité de voir et de limiter leurs activités en ligne.

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. 161).

CHIFFREMENT

Créer des disques (ou coffres) chiffrés, protégés par mot de passe, sur votre ordinateur, dans lesquels vous pouvez stocker vos documents confidentiels ou sensibles en toute sécurité.

Pour plus d'informations sur comment créer des disques logiques (ou des coffres-forts) chiffrés, protégés par mot de passe sur votre ordinateur, veuillez vous reporter à « *Chiffrement de fichiers* » (p. 147).

PROTECTION DE WEBCAM

La Protection de Webcam Bitdefender protège votre webcam des dangers en bloquant l'accès des applications auxquelles vous ne vous fiez pas.

Pour plus d'informations sur la manière de protéger votre webcam des accès malveillants, rendez-vous sur « *Protection de webcam* » (p. 138).

WALLET

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

Pour plus d'informations sur la configuration du Gestionnaire de mots de passe, consultez « *Protection Password Manager de vos identifiants* » (p. 153).

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. 164).

CONTRÔLE PARENTAL

Le Contrôle Parental Bitdefender vous permet de surveiller ce que vos enfants font sur leur ordinateur. En cas de contenu inapproprié vous pouvez décider de limiter son accès à internet ou à certaines applications.

Cliquez sur **Configurer** dans le panneau du Contrôle parental afin de commencer à configurer les appareils de vos enfants et ainsi suivre leurs activités en ligne.

Pour plus d'informations sur la configuration du Contrôle parental, consultez « *Contrôle Parental* » (p. 172).

PROTECTION DES DONNÉES

La fonctionnalité Protection des données vous permet de supprimer des fichiers de façon permanente.

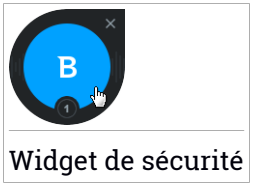
Cliquez sur **Destructeur de Fichiers** dans le panneau Protection des données pour lancer un assistant qui vous permettra de supprimer complètement des fichiers de votre système.

Pour plus d'informations sur la configuration de la protection des données, reportez-vous à « *Protection des données* » (p. 170).

5.5. Widget de sécurité

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

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



Widget de sécurité

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

 Des problèmes critiques affectent la sécurité de votre système.

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

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

 Votre système est protégé.

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

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

La partie inférieure du widget affiche le compteur d'événements non lus (le nombre d'événements importants signalés par Bitdefender, s'il y en a). Cliquez sur le compteur d'événements, par exemple 1 pour un événement non lu, pour ouvrir la fenêtre Notifications. Pour plus d'informations, reportez-vous à « *Notifications* » (p. 16).

5.5.1. Analyse des fichiers et des dossiers

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

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

5.5.2. Masquer / afficher le Widget Windows

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

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

- Dans la zone de notification :
  1. Faites un clic droit sur l'icône de Bitdefender dans la zone de notification.
  2. Cliquez sur **Afficher le Widget Windows** dans le menu contextuel qui apparaît.
- À partir de l'interface de Bitdefender :
  1. Cliquez sur **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans la fenêtre **Généraux**, activez le **Widget de sécurité**.

Le Widget Windows Bitdefender est désactivé par défaut.

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 ordinateur 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 Internet Security
  - Antivirus Bitdefender pour Mac
  - Bitdefender Mobile Security pour Android
  - Bitdefender Mobile Security pour iOS
  - Contrôle Parental Bitdefender
- Gérer et renouveler vos abonnement Bitdefender.
- Ajouter de nouveaux appareils à votre réseau et les gérer où que vous soyez.
- Configurez le Contrôle parental pour les appareils de vos enfants et surveillez leurs activités d'où que vous soyez.

6.1. Accéder 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 e-mail 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 e-mail 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. Mes abonnements

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

6.2.1. Vérifier les abonnements disponibles

Pour vérifier vos abonnements disponibles :

1. 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).

6.2.2. nouvel appareil

Si votre abonnement couvre plus d'un appareil, vous pouvez ajouter un nouvel appareil et y installer votre Bitdefender Internet Security, 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 et sauvegardez le fichier d'installation.

   - **Protéger d'autres appareils**

     Sélectionnez cette option, puis cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR E-MAIL**. 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.

6.2.3. Renouveler abonnement

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

1. 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.

6.2.4. 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.

6.3. 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 **Propriéaire 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 « *Exécuter une analyse du système* » (p. 94) et à « *Exécuter une analyse rapide* » (p. 94) .
- **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. 130).

6.4. Mon compte

Dans **Mon compte**, vous pouvez personnaliser votre profil, changer le mot de passe associé à votre compte, gérer les sessions de connexion et les messages d' aide Bitdefender Central.

Après avoir cliqué sur l'icône dans la partie supérieure droite de l'écran et sélectionnez **Mon compte**, les onglets suivants apparaissent :

- **Profil** - vous pouvez ici ajouter et modifier les informations relatives au compte.
- **Changer de mot de passe** - vous pouvez ici modifier le mot de passe associé à votre compte.

- **Gestion de session** - vous pouvez ici voir et gérer les dernières sessions de connexion actives et inactives ouvertes sur les appareils associés à votre compte.
- **Configuration** - vous pouvez ici activer ou désactiver les messages d'aide Bitdefender Central et décider si vous voulez être notifié ou non lorsque des photos sont prises depuis vos appareils Android.

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

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

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

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

- Si votre ordinateur se connecte à internet via un serveur proxy, vous devez configurer les paramètres du proxy comme indiqué dans « *Comment configurer Bitdefender pour utiliser une connexion internet par proxy ?* » (p. 80).
- 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 PC lorsque vous avez terminé une mise à jour. Il est recommandé de le faire dès que possible

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

Pour mettre à jour Bitdefender à distance sur un appareil 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, en permanence ou jusqu'au redémarrage du système.

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

7.4. Réglage des paramètres de mise à jour

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

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

Pour 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'ordinateur. Cela évite que le processus de mise à jour de Bitdefender interfère avec le travail de l'utilisateur.

Si vous souhaitez être averti lorsqu'une mise à jour nécessite un redémarrage, 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 pop-up 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 2018 d'installé.

COMMENT FAIRE POUR

8. INSTALLATION

8.1. Comment installer Bitdefender sur un deuxième ordinateur ?

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

installer Bitdefender sur un deuxième ordinateur :

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

   Vous êtes redirigé vers la page web compte Bitdefender. Assurez-vous que vous êtes connectés avec vos identifiants.

2. Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT** dans la fenêtre qui apparait.

3. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR E-MAIL**. 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 Bitdefender, consultez la boite de messagerie que vous avez précédemment saisie, et appuyez sur le bouton de téléchargement.

4. Exécutez le produit Bitdefender que vous avez installé.

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

8.2. 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 Internet Security** et sélectionnez **Désinstaller**.
  3. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
  4. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.
- Dans **Windows 8 et Windows 8.1** :
  1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
  2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
  3. Localisez **Bitdefender Internet Security** et sélectionnez **Désinstaller**.
  4. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
  5. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.
- Dans **Windows 10** :
  1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
  2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **& Fonctionnalités Applications**.
  3. Localisez **Bitdefender Internet Security** et sélectionnez **Désinstaller**.
  4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
  5. Cliquez sur **RÉINSTALLER**.
  6. Vous aurez besoin de redémarrer l'ordinateur 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.

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

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

Note
Avant de lancer le kit, nous vous recommandons de désinstaller toutes les solutions de sécurité présentes sur votre système. Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, 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 et sauvegardez le fichier d'installation.
   - **Protéger d'autres appareils**

     Sélectionnez cette option, puis cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR E-MAIL**. 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.

8.4. Comment changer la langue de mon produit Bitdefender ?

Si vous souhaitez utiliser Bitdefender dans une autre langue, vous devrez réinstaller le produit avec la langue souhaitée.

Pour utiliser Bitdefender dans une autre langue :

1. Supprimez Bitdefender en procédant comme suit :
   - Dans **Windows 7** :
     a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
     b. Localisez **Bitdefender Internet Security** 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.
   - 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 Internet Security** 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.
   - 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 Internet Security** 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.

2. Modifier la langue de Bitdefender Central :
   a. Accéder à Bitdefender Central.
   b. Cliquez sur l'icône dans l'angle supérieur droit de l'écran.
   c. Cliquez sur **Mon compte** dans le menu déroulant.
   d. Sélectionnez l'onglet **Profil**.
   e. Sélectionnez une langue à partir de la liste déroulante **Langue**, puis cliquez sur **ENREGISTRER**.
3. Téléchargez le fichier d'installation :
   a. Sélectionnez le panneau **Mes appareils**, puis cliquez sur **INSTALLER LA PROTECTION**.
   b. Sélectionnez l'une des deux actions disponibles :
      - **Protéger cet appareil**

        Sélectionnez cette option et sauvegardez le fichier d'installation.
      - **Protéger d'autres appareils**

        Sélectionnez cette option, puis cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR E-MAIL**. 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 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.

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

8.5. 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 Internet Security** 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 Internet Security** 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 installées**.
3. Localisez **Bitdefender Internet Security** 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 et sauvegardez le fichier d'installation.

- **Protéger d'autres appareils**

  Sélectionnez cette option, puis cliquez sur **ENVOYER UN LIEN DE TÉLÉCHARGEMENT**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER PAR E-MAIL**. 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).

8.6. 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 2018, 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'ordinateur 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.

9. ABONNEMENTS

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

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

- Vous avez fait une mise à niveau à partir d'une version précédente de Bitdefender vers la nouvelle :
  1. Une fois que la mise à niveau vers Bitdefender Internet Security est terminée, vous devez vous connecter à votre compte Bitdefender.
  2. Cliquez sur le lien **Se Connecter** puis tapez l'adresse email et le mot de passe de votre compte Bitdefender.
  3. Cliquez sur **Se connecter** pour poursuivre.
  4. Une notification vous informant qu'un abonnement a été créé apparaît sur l'écran de votre compte. L'abonnement créé sera valide pour la période restante sur votre clé de licence et pour le même nombre d'utilisateurs.

     Les appareils qui utilisent les versions précédentes de Bitdefender et sont enregistrés avec la clé de licence que vous avez convertie en abonnement doivent activer le produit avec le même compte Bitdefender.
- Bitdefender n'était pas précédemment installé sur le système :
  1. Dès que le processus d'installation est terminé, vous devez vous connecter à votre compte Bitdefender.
  2. Cliquez sur le lien **Se Connecter** puis tapez l'adresse email et le mot de passe de votre compte Bitdefender.
  3. Cliquez sur **CONNEXION** pour continuer, puis sur le bouton **TERMINER** pour accéder à l'interface Bitdefender Internet Security.
  4. Cliquez sur **Mon compte** dans le menu de navigation de l'interface de Bitdefender.
  5. Cliquez sur **Activer**.

Une nouvelle fenêtre apparaît.

6. Cliquez sur le lien **Obtenez votre mise à niveau gratuite maintenant !**.
7. Saisissez votre clé de licence dans le champ correspondant et cliquez sur **METTRE A NIVEAU MON PRODUIT**. Un abonnement avec la même disponibilité et nombre d'utilisateurs pour votre clé de licence est associée à votre compte.

10. BITDEFENDER CENTRAL

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

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

Pour ajouter un nouveau compte :

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 pour changer le compte lié à l'ordinateur.
3. Tapez l'adresse courriel et le mot de passe de votre compte dans les champs correspondants, puis cliquez sur **CONNEXION**.

> **Note**
> Le produit Bitdefender de votre appareil change automatiquement selon l'abonnement associé au nouveau compte Bitdefender.
> 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. 233).

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. Sélectionnez l'onglet **Paramètres**.
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. Cliquez sur **Mot de passe oublié**.
  4. Saisissez l'adresse courriel utilisée pour créer votre compte Bitdefender puis cliquez sur **MOT DE PASSE OUBLIÉ**.
  5. Consultez votre courriel et cliquez sur le bouton indiqué.

     La fenêtre RÉINITIALISATION DU MOT DE PASSE de Bitdefender apparait.
  6. Saisissez votre adresse e-mail et le nouveau mot de passe dans le champ correspondant. Le mot de passe doit contenir au moins 8 caractères et contenir des chiffres.
  7. Cliquez **RÉINITIALISER LE MOT DE PASSE**.
- A partir de votre navigateur web :
  1. Allez à : https://central.bitdefender.com.
  2. Cliquez sur **Mot de passe oublié**.
  3. Saisissez votre adresse e-mail, puis cliquez sur **MOT DE PASSE OUBLIÉ**.
  4. 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 **Mon compte** dans le menu déroulant.
4. Sélectionnez l'onglet **Gestion de session**.
5. 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 leur appliquer.

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

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

11.2. Comment analyser mon système ?

Pour 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 **Analyse système**.
3. Suivez les indications de l'Assistant d'analyse système pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés.

   Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 98).

11.3. Comment programmer une analyse ?

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

Pour programmer une analyse :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Gérer analyses**.
3. Choisissez le type d'analyse que vous voulez planifier, Analyse complète du système ou Analyse rapide, puis cliquez sur **OPTIONS D'ANALYSE**.

   Alternativement, vous pouvez créer un type d'analyse qui correspond à vos besoins en cliquant sur **NOUVELLE TÂCHE PERSONNALISÉE**.
4. Activer l'option **Planification**.

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

   - Au démarrage du système
   - Une fois
   - Périodiquement

Dans la fenêtre **Cibles analyse** vous pouvez choisir les localisations que vous souhaitez analyser. Cette option est seulement disponible si vous choisissez de créer une nouvelle analyse personnalisée.

11.4. Comment créer une tâche d'analyse personnalisée ?

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

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

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

3. Cliquez sur **NOUVELLE TÂCHE PERSONNALISÉE**. Saisissez un nom pour l'analyse dans la fenêtre **Standard** et sélectionnez les emplacements à analyser.
4. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**.

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

   Vous pouvez également choisir d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée. N'oubliez pas qu'il s'agira du comportement par défaut à chaque fois que vous exécuterez cette tâche.
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
6. Utilisez le bouton correspondant si vous souhaitez définir une planification pour cette tâche d'analyse.
7. Cliquez sur **DÉMARRER L'ANALYSE** et suivez l'Assistant d'analyse pour terminer l'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
8. 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 **Paramètres**.
3. Cliquez sur l'onglet **Exceptions**.
4. Cliquez sur le menu déroulant **Liste des fichiers et dossiers exclus de l'Analyse**, puis sur **Ajouter**.
5. Cliquez sur **PARCOURIR**, sélectionnez le dossier que vous voulez exclure de l'analyse, puis choisissez le type d'analyse duquel il doit être exclu.
6. Cliquez sur **AJOUTER** pour sauvegarder les modifications et fermez 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 **Paramètres**.
   c. Dans la fenêtre **Protection**, désactivez **Protection - 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. 82).
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 **Quarantaine**.

c. 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).
5. Activez la protection antivirus en temps réel de Bitdefender.
6. Contactez les représentants de notre soutien technique afin que nous puissions supprimer détection de la mise à jour d'information sur les menaces. Pour savoir comment faire cela, consultez « *Assistance* » (p. 233).

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. CONTRÔLE PARENTAL

12.1. Comment protéger mes enfants des menaces sur Internet ?

Le Contrôle parental Bitdefender vous permet de limiter l'accès à Internet et à certaines applications, empêchant ainsi vos enfants de visualiser du contenu inapproprié en votre absence.

Pour configurer le Contrôle parental :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **CONTRÔLE PARENTAL**, cliquez sur **Configurer**.

   Vous êtes redirigé vers la page web compte Bitdefender. Assurez-vous que vous êtes connectés avec vos identifiants.
3. Le tableau de bord du Contrôle Parental apparait. Vous pouvez consulter et configurer ici les paramètres du contrôle parental.
4. Cliquez sur **AJOUTER PROFIL** sur le côté droit de la fenêtre **Mes enfants**
5. Saisissez les informations demandées dans chaque champ, par exemple : nom et date de naissance. Pour ajouter une photo de profil, cliquez sur le lien **Choisir un fichier**. Cliquez sur **ÉTAPE SUIVANTE** pour continuer.

   Basée sur les standards de développement des enfants, la configuration de la date de naissance de l'enfant charge automatiquement les paramètres de recherche sur Internet considérés comme appropriés pour sa catégorie d'âge.
6. Si Bitdefender Internet Security est déjà installé sur l'appareil de votre enfant, sélectionnez le dans la liste puis sélectionnez le compte que vous souhaitez surveiller. Cliquez sur **Enregistrer**.

   Si votre enfant utilise un appareil Android ou iOS mais que l'application Contrôle parental Bitdefender n'est pas installée sur celui-ci, cliquez sur **AJOUTER UN APPAREIL**. Si votre enfant utilise un appareil Mac mais que l'application Antivirus for Mac Bitdefender n'est pas installée sur celui-ci, cliquez sur le même bouton. Sélectionnez le système d'exploitation sur lequel vous voulez installer l'application, puis cliquez sur **ÉTAPE SUIVANTE** pour continuer.

7. Saisissez l'adresse e-mail sur laquelle nous enverrons le lien de téléchargement du fichier d'installation de l'application Bitdefender, puis cliquez sur **ENVOYER UN LIEN D'INSTALLATION**.

Vérifiez les activités de vos enfants et modifiez les paramètres du Contrôle parental à l'aide de compte Bitdefender depuis tout ordinateur ou appareil mobile connecté à internet.

Important
Sur les appareils Windows, le Bitdefender Internet Security que vous avez inclus dans votre abonnement doit être téléchargé et installé.
Sur les appareils macOS, le produit Antivirus for Mac Bitdefender doit être téléchargé et installé.
Sur les appareils Android et iOS, l'application Contrôle parental Bitdefender doit être téléchargée et installée.

12.2. Comment empêcher mon enfant d'accéder à un site Web ?

Le Contrôle parental de Bitdefender vous permet de contrôler les contenus auxquels votre enfant accède en utilisant son appareil et vous permet de bloquer l'accès à un site web.

Pour bloquer l'accès à un site web, vous devez l'ajouter à la liste d'exceptions, comme suit :

1. Allez à : https://central.bitdefender.com.
2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
4. Sélectionnez le profil de votre enfant à partir de la fenêtre **Mes enfants**.
5. Sélectionnez l'onglet **Sites Web**.
6. Cliquez sur le bouton **GÉRER**.
7. Saisissez la page web que vous souhaitez bloquer dans le champ correspondant.
8. Sélectionnez **Autoriser** ou **Bloquer**.
9. Cliquez **FINISH** pour sauvegarder les changements.

Note
Les restrictions ne peuvent être définies que pour les appareils Android et Windows.

12.3. Comment empêcher mon enfant d'utiliser certaines applications ?

Le Contrôle Parental de Bitdefender vous permet de contrôler le contenu auquel votre enfant accède lorsqu'il utilise l'appareil.

Pour bloquer l'accès à une application :

1. Allez à : https://central.bitdefender.com.
2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
4. Sélectionnez le profil de votre enfant à partir de la fenêtre **Mes enfants**.
5. Sélectionnez l'onglet **Applications**.
6. Une liste des appareils affectés apparaît.

   Sélectionnez la carte correspondant à l'appareil sur lequel vous voulez restreindre l'accès à des applications.
7. Cliquez sur **Gérer les applications utilisées par...**.

   Une liste des applications installées apparait.
8. Sélectionnez **Bloquée** à côté des applications que vous ne voulez plus que votre enfant utilise.

12.4. Comment empêcher mon enfant d'être en contact avec des personnes malveillantes ?

Le Contrôle parental Bitdefender vous offre la possibilité de bloquer les appels venant de numéros inconnus ou d'amis à partir de la liste du téléphone de votre enfant.

Pour bloquer un contact spécifique sur un appareil Android sur lequel l'application Contrôle parental Bitdefender est installée :

1. Allez à : https://central.bitdefender.com.

2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
4. Sélectionnez le profil de l'enfant que vous souhaitez limiter.

   Vérifiez que l'appareil Android est bien affecté au profil sélectionné.
5. Sélectionnez l'onglet **Contacts téléphone**.

   Une liste avec des cartes s'affiche. Les cartes représentent les contacts provenant du téléphone de votre enfant.
6. Sélectionnez la carte avec le numéro de téléphone que vous souhaitez bloquer.

   Le symbole qui apparaît indique que votre enfant ne pourra plus être contacté par ce numéro de téléphone.

   Les SMS seront bloqués uniquement si, lors de la configuration de l'application Contrôle parental Bitdefender sur l'appareil de votre enfant, vous avez choisir d'utiliser l'application SMS du Contrôle parental au lieu de l'application par défaut.

Pour bloquer un contact spécifique sur un appareil Android sur lequel l'application Contrôle parental Bitdefender n'est pas installée :

1. Allez à : https://central.bitdefender.com.
2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
4. Sélectionnez le profil de l'enfant que vous souhaitez limiter.
5. Cliquez sur le lien **Installer le Contrôle parental sur un appareil** de la carte désirée.
6. Cliquez sur **AJOUTER UN APPAREIL** dans la fenêtre qui s'affiche.
7. Sélectionnez Android dans la liste, puis cliquez sur **ÉTAPE SUIVANTE** pour continuer.
8. Saisissez l'adresse e-mail sur laquelle nous enverrons le lien de téléchargement du fichier d'installation de l'application Bitdefender, puis cliquez sur **ENVOYER UN LIEN D'INSTALLATION**.

9. Installez l'application sur l'appareil désiré en suivant les instructions indiquées dans l'e-mail que vous avez reçu de notre part.
10. Sélectionnez l'onglet **Contacts téléphone** de Bitdefender Central.

    Une liste avec des cartes s'affiche. Les cartes représentent les contacts provenant du smartphone Android de votre enfant.
11. Sélectionnez la carte avec le numéro de téléphone que vous souhaitez bloquer.

    Le symbole qui apparaît indique que votre enfant ne pourra plus être contacté par ce numéro de téléphone.

    Les SMS seront bloqués uniquement si, lors de la configuration de l'application Contrôle parental Bitdefender sur l'appareil de votre enfant, vous avez choisir d'utiliser l'application SMS du Contrôle parental au lieu de l'application par défaut.

Les appels entrants et sortants depuis ou vers un numéro inconnu peuvent être bloqués en activant le bouton **Bloquer les appels des numéros privés inconnus sans identification de l'appelant**.

Note
Les restrictions d'appel ne peuvent être définies que pour les appareils Android ajoutés sur le profil de votre enfant, et s'appliquent aussi bien aux appels entrants que sortants.

12.5. Comment puis-je configurer une localisation aussi sécurisée ou limitée pour mon enfant ?

Le Contrôle parental de Bitdefender vous permet de définir un emplacement comme sécurisé ou limité pour votre enfant.

Pour configurer un emplacement :

1. Allez à : https://central.bitdefender.com.
2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
4. Sélectionnez le profil de votre enfant à partir de la fenêtre **Mes enfants**.
5. Sélectionnez l'onglet **Localisation de l'enfant**.

6. Cliquez sur **Appareils** dans le cadre qui se trouve dans la fenêtre **Localisation de l'enfant**.
7. Cliquez sur **CHOISIR APPAREILS** puis sélectionnez l'appareil que vous souhaitez configurer.
8. Dans la fenêtre **Zones**, cliquez sur le bouton **AJOUTER ZONE**.
9. Choisissez le type de lieu, **Sécurisé** ou **Limité**.
10. Saisissez un nom valide pour la zone où votre enfant a la permission d'aller ou non.
11. Configurez la portée qui devrait être appliquée pour la surveillance à partir du curseur **Rayon**.
12. Cliquez sur **AJOUTER ZONE** pour sauvegarder vos configurations.

Chaque fois que vous voulez configurer un lieu limité comme sécurisé, ou un lieu sécurisé comme limité, cliquez dessus, puis sélectionnez le bouton **ÉDITER ZONE**. Selon la modification que vous souhaitez opérer, sélectionnez l'option **SÉCURISÉ** ou **LIMITÉ**, puis cliquez sur **METTRE LA ZONE A JOUR**.

12.6. Comment bloquer l'accès de mon enfant aux appareils attribués pendant les activités du quotidien ?

Le Contrôle parental Bitdefender vous permet de restreindre l'accès de votre enfant aux appareils attribués pendant les activités du quotidien, comme les heures où il est à l'école ou doit faire ses devoirs, ou bien lorsqu'il devrait dormir.

Pour ajouter de nouvelles limites de temps :

1. Accédez au panneau Contrôle parental depuis Bitdefender Central.
2. Dans la fenêtre **Mes enfants** sélectionnez le profil de l'enfant pour lequel vous souhaitez définir des restrictions.
3. Sélectionnez l'onglet **Temps passé devant l'écran**.
4. Cliquez sur **Voir les restrictions de temps**.
5. Dans la zone **Définir des limites de temps**, cliquez sur **Ajouter une nouvelle restriction**.

6. Donnez un nom à la restriction que vous souhaitez définir (par exemple sommeil, devoirs, cours de tennis, etc.).
7. Définissez la plage horaire à restreindre, puis cliquez sur **AJOUTER** pour enregistrer les réglages.

12.7. Comment bloquer l'accès de mon enfant aux appareils attribués en journée ou pendant la nuit ?

Le Contrôle parental Bitdefender vous permet de restreindre l'accès de votre enfant aux appareils attribués à différents moments de la journée.

Pour définir une limite quotidienne :

1. Accédez au panneau Contrôle parental depuis Bitdefender Central.
2. Dans la fenêtre **Mes enfants** sélectionnez le profil de l'enfant pour lequel vous souhaitez définir des restrictions.
3. Sélectionnez l'onglet **Temps passé devant l'écran**.
4. Cliquez sur **Voir les restrictions de temps**.
5. Dans la zone **Définir une limite quotidienne**, cliquez sur **Ajouter une nouvelle limite quotidienne**.
6. Définissez la plage horaire et les jours à restreindre, puis cliquez sur **SAUVEGARDER** pour enregistrer les réglages.

12.8. Comment supprimer un profil enfant

Si vous souhaitez supprimer un profil enfant existant :

1. Allez à : https://central.bitdefender.com.
2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
4. Cliquez sur l'icône ⋮ dans le profil de l'enfant que vous souhaitez supprimer, puis choisissez **Supprimer**.

13. PROTECTION DE LA VIE PRIVÉE

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

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

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

Pour 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 **Ouvrir Safepay**.
3. 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.

13.2. Comment utiliser les coffres-forts ?

La fonction Coffre-fort de Bitdefender vous permet de créer des disques logiques chiffrés et protégés par mot de passe (appelés « coffres-forts ») sur votre ordinateur, afin d'y stocker vos documents confidentiels et sensibles. Physiquement, le coffre-fort est un fichier stocké sur le disque dur en local et ayant une extension .bvd.

Lorsque vous créez un coffre-fort, deux éléments sont importants : la taille et le mot de passe. La taille par défaut de 100 Mo devrait suffire pour vos documents personnels, fichiers Excel et autres données similaires. Vous pouvez cependant avoir besoin de plus d'espace pour des vidéos ou d'autres fichiers volumineux.

Pour stocker en toute sécurité vos fichiers ou dossiers confidentiels ou sensibles dans des coffres-forts Bitdefender :

- **Créez un coffre-fort et définissez un mot de passe sécurisé pour celui-ci.**

Pour créer un coffre-fort, faites un clic droit sur une zone vide du bureau ou dans un dossier de votre ordinateur, pointez sur **Bitdefender** > **Coffre-fort Bitdefender** et sélectionnez **Créer un coffre-fort** .

Une nouvelle fenêtre apparaît. Procédez comme suit :

1. Cliquez sur **Parcourir** pour sélectionner l'emplacement du coffre-fort et sauvegardez le coffre-fort sous le nom que vous souhaitez.
2. Choisissez une lettre de lecteur à partir du menu. Quand vous ouvrez le coffre, un disque virtuel indexé avec la lettre choisie apparaît dans **Poste de travail**.
3. Saisissez le mot de passe du coffre-fort dans les champs **Mot de passe** et **Confirmer**.
4. Si vous souhaitez modifier la taille par défaut du coffre-fort (100 Mo), utiliser les touches des flèches haut et bas dans le champ **Taille du coffre-fort (Mo)**.
5. Cliquez sur **Créer**.

Note

Quand vous ouvrez le coffre, un disque virtuel apparaît dans **Poste de travail**. Le disque se voit attribuer la lettre correspondant au coffre.

- **Ajoutez les fichiers ou les dossiers que vous voulez protéger au coffre-fort.**

  Vous devez d'abord ouvrir le coffre-fort pour y ajouter un fichier.

  1. Parcourir pour sélectionner le fichier coffre-fort .bvd.
  2. Faites un clic droit sur le coffre-fort, pointez sur Coffre-fort Bitdefender et sélectionnez **Ouvrir**.
  3. Dans la fenêtre qui apparaît, saisissez le mot de passe, sélectionnez une lettre de lecteur à attribuer au coffre-fort et cliquez sur **OK**.

  Vous pouvez maintenant effectuer des opérations sur le lecteur correspondant au coffre-fort souhaité en utilisant Windows Explorer, comme vous le feriez avec un lecteur normal. Pour ajouter un fichier à un coffre-fort ouvert, vous pouvez également faire un clic droit sur le fichier, pointer sur Coffre-fort Bitdefender, puis sélectionner **Ajouter au coffre-fort**.

- **Maintenez toujours le coffre-fort verrouillé.**

Ouvrez uniquement les coffres-forts lorsque vous avez besoin d'y accéder ou de gérer leur contenu. Pour verrouiller un coffre-fort, faites un clic droit sur le disque dur virtuel correspondant dans **Poste de travail**, sélectionnez **Coffre-fort Bitdefender**, puis choisissez **Verrouiller**.

- **Veillez à ne pas supprimer le fichier coffre-fort .bvd.**

  En supprimant le fichier vous supprimez également le contenu du coffre-fort.

Pour plus d'informations sur l'utilisation des coffres-forts, consultez « *Chiffrement de fichiers* » (p. 147).

13.3. Comment supprimer définitivement un fichier avec Bitdefender ?

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

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

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement, pointez sur Bitdefender et sélectionnez **Destructeur de fichiers**.
2. 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.

13.4. Comment protéger ma webcam des pirates ?

Vous pouvez régler votre produit Bitdefender de sorte à autoriser ou à bloquer l'accès des applications installées à votre webcam en suivant ces instructions :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PROTECTION WEBCAM**, cliquez sur **Accès à la Webcam**.

   La liste des applications ayant accès à votre webcam apparait.

3. Cliquez sur l'application dont vous voulez autoriser ou bannir l'accès, puis cliquez sur le bouton correspondant.

   Pour savoir ce que les autres utilisateurs de Bitdefender ont décidé de faire de l'application sélectionnée, cliquez sur l'icône . Vous recevrez une notification à chaque fois qu'une des applications de la liste est bloquée par les utilisateurs de Bitdefender.

Pour ajouter manuellement des applications à cette liste, cliquez sur le lient **Ajouter une nouvelle application à la liste**.

13.5. 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 **RESTAURER 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 terminer la procédure 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;

14. INFORMATIONS UTILES

14.1. 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 **Anti-Malware Testfile**.
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 pop-up 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. 233).

14.2. Comment désinstaller Bitdefender ?

Si vous souhaitez supprimer votre Bitdefender Internet Security :

- Dans **Windows 7** :
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
  2. Localisez **Bitdefender Internet Security** 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 Internet Security** 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 Internet Security** 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.

14.3. Comment désinstaller le VPN Bitdefender ?

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

- 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.

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

Bitdefender propose plusieurs tâches d'analyse que vous pouvez utiliser pour vérifier que votre système n'est pas infecté par des menaces. L'analyse de l'ensemble de l'ordinateur peut prendre plus de temps en fonction de la configuration matérielle et logicielle de votre système.

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

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

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

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Gérer analyses**.
3. Dans la fenêtre **Gérer les tâches d'analyse**, cliquez sur **NOUVELLE TÂCHE PERSONNALISÉE** pour saisir un nom pour l'analyse et sélectionnez les emplacements à analyser.
4. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**.
5. Choisissez d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
7. Cliquez sur **DÉMARRER L'ANALYSE** pour analyser votre système.

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

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 98).

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

Si votre ordinateur se connecte à internet via un serveur proxy, vous devez configurer Bitdefender avec les paramètres du proxy. Normalement, Bitdefender détecte et importe automatiquement les paramètres proxy de votre système.

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

Pour gérer les paramètres 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.

14.6. 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.

14.7. 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**.

14.8. Comment supprimer les autres solutions de sécurité ?

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

Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, le système devient instable. Le programme de désinstallation de Bitdefender Internet Security 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 installées**.
3. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

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

14.9. 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 votre système.

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

- 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

15. PROTECTION ANTIVIRUS

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

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

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

  Important
  Pour empêcher l'infection de votre ordinateur 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 Bitdefender le fait – à la demande.

Bitdefender analyse automatiquement tout support amovible connecté à l'ordinateur afin de s'assurer que son accès ne pose pas de problème de sécurité. Pour plus d'informations, reportez-vous à « *Analyse automatique de supports amovibles* » (p. 102).

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. 105).

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. 107).

Si votre ordinateur a été infecté par des logiciels malveillants, consultez-vous « *Suppression des menaces de votre système* » (p. 221). 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 Bitdefender (Environnement de récupération sur Windows 10)* » (p. 221). Il s'agit d'un environnement de confiance, spécialement conçu pour la suppression de logiciels malveillants, qui vous permet de faire redémarrer votre ordinateur indépendamment de Windows. Lorsque l'ordinateur s'exécute en Mode de Secours (Environnement de récupération sur Windows 10), les menaces de Windows sont inactives, ce qui rend leur suppression facile.

15.1. 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.

15.1.1. 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 **Paramètres**.
3. Dans la fenêtre **Protection**, activez ou désactivez **Protection - 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.

15.1.2. 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 **Paramètres**.
3. Dans la fenêtre **Protection** cliquez sur le menu déroulant **Afficher les paramètres avancés**.

   Une fenêtre s'affiche.
4. Faites défiler la fenêtre pour 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 programmes potentiellement indésirables (PIP) est un logiciel habituellement intégré à un logiciel gratuit qui provoque l'apparition de pop-up 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 Adware) ou sont inclus par défaut dans le kit d'installation rapide.
- **Analyser les volumes partagés.** Pour accéder en toute sécurité à un réseau à distance depuis votre ordinateur, nous vous recommandons de maintenir activée l'option Analyser les volumes partagés.

- **Analyser le contenu compressé.** L'analyse des fichiers compressés est un processus lent et consommant beaucoup de ressources, qui n'est donc pas recommandé pour une protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Les 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 définir la limite de taille maximum (en Mo) des archives à analyser à l'accès.

- **Analyser les e-mails.** Afin d'éviter que des menaces soient téléchargées sur votre ordinateur, Bitdefender analyse automatiquement les e-mails entrants et sortants.

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

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

- **Analyser 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 des enregistreurs de frappe.** Sélectionnez cette option pour analyser la présence d'enregistreurs de frappe sur votre système. Les enregistreurs de frappe enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur internet à une personne malveillante (un pirate informatique). Le pirate peut récupérer des informations sensibles à partir

des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.

- **Analyser au redémarrage.** Sélectionnez l'option d'analyse **Early boot** pour analyser votre système au démarrage dès que tous ses services critiques ont été téléchargés. La mission de cette fonctionnalité est d'améliorer la détection des 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 **Paramètres**.
3. Dans la fenêtre **Protection** cliquez sur le menu déroulant **Afficher les paramètres avancés**.

   Une fenêtre s'affiche.
4. Faites défiler la fenêtre jusqu'à voir l'option **Actions de menaces**.
5. 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. 107).

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.

Déplacer en quarantaine
Déplace les fichiers détectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 107).

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

15.1.3. 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 **Paramètres**.
3. Dans la fenêtre **Protection** cliquez sur le menu déroulant **Afficher les paramètres avancés**.

   Une fenêtre s'affiche.
4. Faites défiler la fenêtre jusqu'à voir l'option **Réinitialiser les réglages**. Sélectionnez cette option pour réinitialiser les réglages par défaut de l'antivirus.

15.2. Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre PC sans logiciel malveillant. Cela s'effectue en protégeant votre ordinateur 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 ordinateur après l'installation de Bitdefender. Et il encore plus prudent d'analyser régulièrement votre ordinateur 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'ordinateur quand vous le souhaitez en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

15.2.1. 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.

15.2.2. Exécuter une analyse rapide

L'analyse rapide utilise l'analyse "sur le nuage" 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 **Analyse rapide**.
3. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

15.2.3. Exécuter une analyse du système

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

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

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

- Vérifiez que la base de données d'information sur les menaces de Bitdefender est à jour. Analyser votre ordinateur 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 ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse

personnalisée. Pour plus d'informations, reportez-vous à « *Configurer une analyse personnalisée* » (p. 95).

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 **Analyse système**.
3. La fonctionnalité Analyse du système vous sera présentée lors de sa première exécution. Cliquez sur **OK, J'AI COMPRIS** pour continuer.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

15.2.4. Configurer une analyse personnalisée

Pour configurer une analyse personnalisée en détails puis l'exécuter :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Gérer analyses**.
3. Cliquez sur **NOUVELLE TÂCHE PERSONNALISÉE**. Saisissez un nom pour l'analyse dans la fenêtre **Standard** et sélectionnez les emplacements à analyser.
4. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**. Une nouvelle fenêtre apparaît. Suivez ces étapes :
   a. Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour choisir le niveau d'analyse souhaité. Reportez-vous à la description à droite de l'échelle pour identifier le niveau d'analyse le plus adapté à vos besoins.

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

   b. Vous pouvez aussi configurer ces options générales :

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

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

5. Si vous souhaitez paramétrer une heure pour votre tâche d'analyse, utilisez le bouton **Horaires** dans la fenêtre **Basique**. Sélectionnez l'une des options correspondantes pour définir une planification :
   - Au démarrage du système
   - Une fois
   - Périodiquement
6. Cliquez sur **DÉMARRER L'ANALYSE** et suivez l'Assistant d'analyse antivirus pour terminer l'analyse. En fonction des emplacements à analyser, l'analyse peut prendre quelque temps. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
7. Si vous le souhaitez, vous pouvez relancer rapidement une analyse personnalisée en cliquant sur le bouton correspondant dans la liste.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

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

  Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux menaces que les autres types de fichiers. Cette catégorie comprend les extensions de fichiers suivantes : 386; a6p; ac; accda; accdb; accdc;

accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Options d'analyse pour les archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Les 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.

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

- **Analyser les secteurs d'amorçage.** Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système. Quand une menace infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
- **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.
- **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.

- **Analyser les cookies.** Sélectionnez cette option pour analyser les temoins stockés par les navigateurs sur votre ordinateur.
- **Analyser uniquement les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Ignorer les enregistreurs de frappe commerciaux.** Sélectionnez cette option si vous avez installé et utilisez un keylogger commercial sur votre ordinateur. Les enregistreurs de frappe commerciaux sont des logiciels de surveillance légitimes dont la fonction principale consiste à enregistrer tout ce qui est tapé au clavier.
- **Rechercher les rootkits.** Sélectionnez cette option pour rechercher des rootkits et des objets cachés à l'aide de ce logiciel.
- **Analyser les applications potentiellement indésirables.** Sélectionnez cette option pour n'analyser que les applications indésirables. Une application potentiellement indésirable (PUA) ou programmes potentiellement indésirables (PIP) est un logiciel habituellement intégré à un logiciel gratuit qui provoque l'apparition de pop-up 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 Adware) ou sont inclus par défaut dans le kit d'installation rapide.

15.2.5. 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 leur 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. 107).

  ### 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. Le journal est fourni au format .xml et peut être enregistré en local en cliquant sur le bouton **Enregistrer le journal** puis en choisissant un emplacement.

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. 221).

15.2.6. 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**.

15.3. Analyse automatique de supports amovibles

Bitdefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre ordinateur et l'analyse en tâche de fond lorsque

l'analyse automatique est activée. Ceci est recommandé afin d'empêcher que des logiciels malveillants n'infectent votre ordinateur.

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

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

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

15.3.1. 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. 221).

15.3.2. Gérer l'analyse des supports amovibles

Pour gérer l'Analyse automatique de supports amovibles :

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

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Paramètres**.
3. Sélectionnez l'onglet **Disques et appareils**.

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.

15.4. Analyse du fichier hosts

Le fichier d'hôtes est livré par défaut avec l'installation de votre système d'exploitation et est utilisé pour la carte hostnames aux 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 agaçantes, ainsi que les bannières, les cookies tiers ou les pirates.

Pour configurer l'analyse du fichier d'hôtes :

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**.

15.5. 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 exceptions ne sont PAS appliquées pour les analyses contextuelle et du système. L'analyse du système est une analyse à la demande qui vous permet d'analyser l'intégralité du système en quête de menaces susceptibles de compromettre la sécurité de vos données. 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**.

15.5.1. 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 **Paramètres**.
3. Sélectionnez l'onglet **Exceptions**.
4. Cliquez sur le menu déroulant **Liste des fichiers et dossiers exclus de l'analyse**0 La fenêtre qui s'affiche vous permet de gérer les fichiers et dossiers exclus de l'analyse.

5. Ajoutez des exceptions en suivant ces étapes :
   a. Cliquez sur **Ajouter**.
   b. Cliquez sur **PARCOURIR**, sélectionnez le fichier ou le dossier à exclure de l'analyse, puis cliquez sur **AJOUTER**. Vous pouvez également taper (ou copier-coller) le chemin vers le fichier ou le dossier dans le champ de saisie.
   c. Par défaut, le fichier ou dossier sélectionné est exclu à la fois de l'analyse à l'accès et à la demande. Pour modifier les conditions d'application de l'exception, sélectionnez l'une des autres options.
   d. Cliquez sur **Ajouter**.

15.5.2. 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 ordinateur. 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 ordinateur 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 **Paramètres**.
3. Sélectionnez l'onglet **Exceptions**.
4. Cliquez sur le menu déroulant **Liste des extensions exclues de l'analyse**. La fenêtre qui s'affiche vous permet de gérer les extensions de fichiers exclues de l'analyse.
5. Ajoutez des exceptions en suivant ces étapes :
   a. Cliquez sur **Ajouter**.
   b. Saisissez les extensions que vous ne souhaitez pas analyser, en les séparant par des points-virgules (;). Voici un exemple :

txt;avi;jpg

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

d. Cliquez sur **AJOUTER**.

15.5.3. 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 **Paramètres**.
3. Sélectionnez l'onglet **Exceptions**.
4. Utilisez l'option dans le menu déroulant **Liste de fichiers et dossiers exclus de l'analyse** pour gérer les exceptions de l'analyse.
5. Pour supprimer ou éditer des exceptions d'analyse, cliquez sur l'un des liens. Procédez comme suit :
   - Pour supprimer une adresse de la liste, sélectionnez-la, puis cliquez sur **Supprimer**.
   - Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la et cliquez sur **Modifier**.) Une nouvelle fenêtre apparaît vous permettant de modifier l'extension ou le chemin à exclure et le type d'analyse dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **MODIFIER**.

15.6. 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 **Quarantaine**.

   Vous pouvez ici voir le nom des fichiers en quarantaine, leur emplacement d'origine et le nom des menaces détectées.
3. 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 sur les menaces
   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.
4. 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**.

16. 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'ordinateur, 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.

16.1. 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 **ADVANCED THREAT DEFENSE**, cliquez sur le bouton Activer/Désactiver.

> **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.

16.2. 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 **ADVANCED THREAT DEFENSE**, cliquez sur **Protection contre les menaces**.

3. La fonctionnalité Protection contre les ransomwares vous sera présentée lors de sa première exécution. Cliquez sur **OK, J'AI COMPRIS** pour continuer.

   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.

16.3. 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 **ADVANCED THREAT DEFENSE**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Exceptions**, cliquez sur **Ajouter des applications aux exceptions**.
4. Sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.

   Pour effacer une entrée de la liste, cliquez sur l'option **Supprimer** située à côté de celle-ci.

17. PRÉVENTION DES 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
- Mozilla 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 fenêtre **Protection web**, cliquez sur le bouton pour activer ou désactiver la fonctionnalité

- Web attack prevention bloque les menaces provenant d'internet, y compris les téléchargements intempestifs.
- Search Advisor, un composant qui évalue les résultats de vos requêtes sur les moteurs de recherche et les liens postés sur les sites Web de réseaux sociaux en plaçant une icône à côté de chaque résultat :

  Nous vous déconseillons de consulter cette page Web.

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

  Cette page peut être consultée en toute sécurité.

  Search Advisor évalue les résultats de recherche des moteurs de recherche Web suivants :
  - Google
  - Yahoo!

- Bing
- Baidu

Search Advisor évalue les liens postés 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 activée l'option Analyse web chiffrée.

- Protection contre les escroqueries.

- Protection Antiphishing.

L'option **Prévention des menaces en ligne** se trouve dans la fenêtre **Protection des menaces en ligne**. Pour protéger votre ordinateur des attaques de malwares complexes (comme les ransomwares) qui profitent de vulnérabilités, gardez cette option activée.

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

Pour configurer et gérer les sites Internet 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 **Exceptions**.
3. Saisissez le nom du site web que vous voulez ajouter à la liste blanche dans le champ correspondant, puis cliquez sur **AJOUTER**.

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

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

17.1. Alertes Bitdefender dans le navigateur

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

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

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

- Quittez la page Web en cliquant sur **RETOUR EN TOUTE SÉCURITÉ**.
- 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 la page web détectée est sûre, cliquez sur **VALIDER** pour l'ajouter à la liste blanche. Nous vous recommandons de n'ajouter que les sites auxquels vous vous fiez entièrement.

18. ANTISPAM

Le spam est un terme utilisé pour décrire les e-mails non sollicités. Le spam est un problème croissant, à la fois pour les particuliers et les entreprises. Vous ne voudriez pas que vos enfants tombent sur certains e-mails, vous pourriez perdre votre travail (pour une perte de temps trop grande ou parce que vous recevez trop de messages à caractère pornographique sur votre e-mail professionnel) et vous ne pouvez pas empêcher les gens d'en envoyer. L'idéal serait de pouvoir arrêter de les recevoir. Malheureusement, le spam revêt un large éventail de formes et de tailles, et il en existe beaucoup.

Bitdefender Antispam utilise des innovations technologiques de pointe et des filtres antispam répondant aux normes industrielles qui permettent d'éliminer les spams avant qu'ils n'atteignent la boîte aux lettres de l'utilisateur. Pour plus d'informations, reportez-vous à « *Aperçu de l'antispam* » (p. 115).

La protection Bitdefender Antispam est disponible seulement pour les clients de messagerie configurés pour recevoir des e-mails via le protocole POP3. POP3 est l'un des protocoles les plus utilisés pour télécharger des e-mails à partir d'un serveur de messagerie.

Note
Bitdefender ne fournit pas de protection antispam pour les comptes de messagerie auxquels vous accédez via un service de webmail.

Les messages de spam détectés par Bitdefender sont marqués avec le préfixe [spam] dans la ligne Objet. Bitdefender place automatiquement les messages de spam dans un dossier spécifique, comme indiqué :

- Dans Microsoft Outlook, les messages de spam sont placés dans le dossier **Spam**, situé dans le dossier **Éléments supprimés**. Le dossier **Spam** est créé lorsqu'un e-mail est marqué comme étant un spam.
- Dans Mozilla Thunderbird, les messages de spam sont placés dans le dossier **Spam**, situé dans le dossier **Corbeille**. Le dossier **Spam** est créé lorsqu'un e-mail est marqué comme étant un spam.

Si vous utilisez d'autres clients de messagerie, vous devez créer une règle pour déplacer les e-mails signalés comme étant du [spam] par Bitdefendervers un dossier de quarantaine personnalisé. Si les dossiers Éléments supprimés ou Corbeille sont supprimés, le dossier Spam sera également supprimé.

Néanmoins, un nouveau dossier Spam sera créé dès qu'un e-mail sera marqué comme spam.

18.1. Aperçu de l'antispam

18.1.1. Filtres AntiSpam

Le moteur antispam de Bitdefender intègre la protection cloud et plusieurs autres filtres qui garantissent que votre boîte de réception ne contient pas de spam, tels que la Liste d'amis, la Liste des spammeurs et le Filtre jeu de caractères.

Liste d'Amis / Liste des Spammeurs

La majorité des utilisateurs communiquent régulièrement avec un groupe de personnes ou reçoivent des messages de la part d'entreprises et d'organismes d'un même domaine. En utilisant **les listes amis/spammeurs**, vous pouvez déterminer aisément de quelles personnes vous voulez recevoir des e-mails quel que soit leur contenu (amis) et de quelles personnes vous ne voulez plus en recevoir (spammeurs).

> **Note**
> Nous vous suggérons d'ajouter les noms de vos amis et leurs adresses mail à la **Liste d'Amis**. Bitdefenderne bloquera aucun de leurs messages; l'ajout des amis à la liste assure la transmission des messages légitimes.

Filtre jeu de caractères

De nombreux messages de spam sont rédigés en caractères cyrilliques et/ou asiatiques. Le filtre de caractères détecte ce type de messages et les signale comme étant du SPAM.

18.1.2. Fonctionnement de l'Antispam

Le Moteur de Bitdefender Antispam utilise tous les filtres antispam combinés pour déterminer si un e-mail doit ou non accéder à votre **Boîte de réception**.

Chaque e-mail provenant du réseau Internet est d'abord vérifié à l'aide du filtre Liste d'amis/Liste des spammeurs. Si l'adresse de l'expéditeur est identifiée dans la Liste d'amis, alors l'e-mail est directement déplacé vers votre **boîte de réception**.

Sinon, le filtre Liste des spammeurs analysera à son tour l'e-mail pour vérifier si l'adresse de l'expéditeur figure dans sa liste. En cas de correspondance, l'e-mail sera étiqueté comme étant du SPAM et déplacé dans le dossier **Spam**.

Autrement, le filtre Jeu de caractères vérifiera si l'e-mail est rédigé en caractères cyrilliques ou asiatiques. Si tel est le cas, le message sera marqué comme étant du SPAM et déplacé vers le dossier **Spam**.

Note
Si l'e-mail est marqué comme SEXUALLY EXPLICIT dans sa ligne de sujet, Bitdefender le considérera comme du SPAM.

18.1.3. Clients et protocoles de messagerie pris en charge

La protection antispam fonctionne avec tous les clients de messagerie POP3/SMTP. La barre Antispam Bitdefender ne s'affiche cependant que dans :

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 ou version supérieure

18.2. Activer ou désactiver la protection antispam

La protection Antispam est activée par défaut.

Pour activer ou désactiver la fonction Antispam :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTISPAM**, activez ou désactivez le bouton.

18.3. Utilisation de la barre d'outils Antispam dans la fenêtre de votre client de messagerie

La barre d'outils Antispam se trouve dans la partie supérieure de votre client de messagerie. La barre d'outils Antispam vous aide à gérer la protection antispam directement à partir de votre client de messagerie. Vous pouvez facilement corriger Bitdefender s'il a indiqué comme SPAM un message légitime.

Important

Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 116).

Chaque bouton de la barre d'outils de Bitdefender sera expliqué ci-dessous:

Paramètres - ouvre une fenêtre qui vous permet de configurer les filtres antispam et les paramètres de la barre d'outils.
Spam - indique que le message sélectionné est un spam. L'e-mail sera immédiatement placé dans le dossier **Spam**. Si les services cloud antispam sont activés, le message est envoyé au Cloud Bitdefender pour une analyse plus approfondie.
Pas Spam - indique que l'e-mail sélectionné n'est pas du spam et que Bitdefender ne devrait pas l'avoir signalé comme tel. Cet email sera retiré du dossier **Spam** et placé dans la **Boîte de réception**. Si les services cloud antispam sont activés, le message est envoyé au Cloud Bitdefender pour une analyse plus approfondie.

Important

Le bouton **Pas Spam** devient actif quand vous choisissez un message marqué spam par Bitdefender (ces messages se trouvent d'habitude dans le répertoire **Spam**).

Ajouter Spammeur - ajoute l'expéditeur de l'e-mail sélectionné à la liste des Spammeurs. Il se peut que vous ayez besoin de cliquer sur **OK** pour valider. Les messages provenant d'adresses qui figurent dans la liste de Spammeurs seront automatiquement considérés comme étant du [spam].
Ajouter Ami - ajoute l'expéditeur de l'e-mail sélectionné à la liste d'Amis. Il se peut que vous ayez besoin de cliquer sur **OK** pour valider. Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.
Spammeurs - ouvre la liste des **Spammeurs**qui contient toutes les adresses e-mail dont vous ne voulez recevoir aucun message, quel que soit son contenu. Pour plus d'informations, reportez-vous à « *Configurer la liste des spammeurs* » (p. 120).
Amis - ouvre la **Liste d'amis** qui contient tous les emails que vous souhaitez recevoir quel qu'en soit le contenu. Pour plus d'informations, reportez-vous à « *Configurer la liste d'amis* » (p. 119).

18.3.1. Indiquer des erreurs de détection

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement corriger le filtre antispam (en indiquant quels e-mails n'auraient pas dû être signalés comme étant du [spam]). Cela contribue à améliorer considérablement l'efficacité du filtrage antispam. Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez le message légitime considéré à tort comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender pour ajouter l'expéditeur à la liste d'Amis. Il se peut que vous ayez besoin de cliquer sur **OK** pour valider. Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.
5. Cliquez sur le bouton **Pas Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Le message d'e-mail sera placé dans la boîte de réception.

18.3.2. Indiquer les messages de spam non détectés

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement indiquer quels e-mails auraient dû être détectés comme étant du spam. Cela contribue à améliorer considérablement l'efficacité du filtrage antispam. Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans la boîte de Réception.
3. Sélectionnez les messages de spam non détectés.
4. Cliquez sur le bouton **Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Ils sont immédiatement signalés comme étant du [spam] et déplacés vers le dossier du courrier indésirable.

18.3.3. Configurer les paramètres de la barre d'outils

Pour configurer les paramètres de la barre d'outils antispam de votre client de messagerie, cliquez sur le bouton **Paramètres** de la barre d'outils puis sur l'onglet **Paramètres de la barre d'outils**.

Vous disposez des options suivantes :

- **Signaler les messages spam comme 'lus'** - signale automatiquement les messages spam comme lus, de manière à éviter le dérangement que provoque leur arrivée.
- Vous pouvez choisir d'afficher ou non des fenêtres de confirmation lorsque vous cliquez sur les boutons **Ajouter spammeur** et **Ajouter ami** de la barre d'outils antispam.

  Les fenêtres de confirmation peuvent empêcher d'ajouter accidentellement des expéditeurs d'e-mails à la liste d'Amis / de Spammeurs.

18.4. Configurer la liste d'amis

La **liste d'amis** est une liste de toutes les adresses e-mail de la part desquelles vous voulez toujours recevoir les messages, quel que soit leur contenu. Les messages de vos amis ne seront jamais considérés comme étant du spam, même si leur contenu ressemble à du spam.

> **Note**
> Tout message provenant d'une adresse contenue dans la **liste d'amis** sera automatiquement déposé dans votre boîte de réception sans autre traitement.

Pour configurer et gérer la liste d'Amis :

- Si vous utilisez Microsoft Outlook ou Thunderbird, cliquez sur le bouton **Amis** de la barre d'outils antispam Bitdefender.
- Autre option :
  1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans le panneau **ANTISPAM**, cliquez sur **Gérer les amis**.

Pour ajouter une adresse e-mail, sélectionnez l'option **Adresse e-mail**, indiquez l'adresse puis cliquez sur **AJOUTER**. Syntaxe: name@domain.com.

Pour ajouter toutes les adresses e-mail d'un domaine particulier, sélectionnez l'option **Nom de domaine**, indiquez le nom de domaine puis cliquez sur **AJOUTER**. Syntaxe:

- @domain.com et domain.com - tous les messages en provenance de domain.com seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;
- domain - tous les messages de domain (quel que soit le suffixe) seront étiquetés comme SPAM;
- com - tous les messages provenant d'un domaine avec un suffixe com seront étiquetés comme SPAM;

Il est recommandé d'éviter d'ajouter des noms de domaines entiers, mais cela peut être utile dans certaines situations. Vous pouvez, par exemple, ajouter le domaine de messagerie électronique de la société pour laquelle vous travaillez ou les domaines de partenaires en qui vous avez confiance.

Pour retirer un élément de la liste, cliquez sur le lien correspondant **Supprimer**. Pour supprimer toutes les entrées de la liste, cliquez sur **NETTOYER**.

Vous pouvez enregistrer la liste d'amis dans un fichier afin de pouvoir l'utilisersur un autre ordinateur ou si vous réinstallez le produit. Pour enregistrer la liste d'Amis, cliquez sur le bouton **Enregistrer** et enregistrez-la à l'emplacement désiré. Le fichier aura l'extension .bwl.

Pour charger une liste d'Amis enregistrée préalablement, cliquez sur **CHARGER** et ouvrez le fichier .bwl correspondant. Pour supprimer le contenu de la liste en cours d'utilisation lorsque vous chargez une liste enregistrée auparavant, sélectionnez **Écraser la liste en cours**.

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

18.5. Configurer la liste des spammeurs

La **liste des spammeurs** est une liste de toutes les adresses e-mail de la part desquelles vous ne voulez recevoir aucun message, quel que soit leur contenu. Tout message en provenance d'une adresse de la **liste des spammeurs** sera automatiquement marqué SPAM sans autre traitement.

Pour configurer et gérer la liste des Spammeurs :

- Si vous utilisez Microsoft Outlook ou Thunderbird, cliquez sur le bouton **Spammeurs** de la barre d'outils antispam Bitdefender intégrée à votre client de messagerie.
- Autre option :
  1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans le panneau **ANTISPAM**, cliquez sur **Gérer les spammers**.

Pour ajouter une adresse e-mail, sélectionnez l'option **Adresse e-mail**, indiquez l'adresse puis cliquez sur **AJOUTER**. Syntaxe: name@domain.com.

Pour ajouter toutes les adresses e-mail d'un domaine particulier, sélectionnez l'option **Nom de domaine**, indiquez le nom de domaine puis cliquez sur **AJOUTER**. Syntaxe:

- @domain.com et domain.com - tous les messages en provenance de domain.com seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;
- domain - tous les messages de domain (quel que soit le suffixe) seront étiquetés comme SPAM;
- com - tous les messages provenant d'un domaine avec un suffixe com seront étiquetés comme SPAM.

Il est recommandé d'éviter d'ajouter des noms de domaines entiers, mais cela peut être utile dans certaines situations.

Avertissement

N'ajoutez pas de domaines de services webmail légitimes (tels que Yahoo, Gmail, Hotmail ou d'autres) à la liste des Spammeurs. Sinon, les e-mails envoyés par les utilisateurs de ces services seront identifiés comme étant du spam. Si par exemple, vous ajoutez yahoo.com à la liste des Spammeurs, tous les e-mails provenant d'adresses yahoo.com seront identifiés comme étant du [spam].

Pour retirer un élément de la liste, cliquez sur le lien correspondant **Supprimer**. Pour supprimer toutes les entrées de la liste, cliquez sur **NETTOYER**.

Vous pouvez enregistrer la liste des spammeurs dans un fichier afin de pouvoirl'utiliser sur un autre ordinateur ou si vous réinstallez le produit. Pour enregistrer la liste des Spammeurs, cliquez sur le bouton **Enregistrer** et enregistrez-la à l'emplacement désiré. Le fichier aura l'extension .bwl.

Pour charger une liste de Spammeurs enregistrée préalablement, cliquez sur **CHARGER** et ouvrez le fichier .bwl correspondant. Pour supprimer le contenu de la liste en cours d'utilisation lorsque vous chargez une liste enregistrée auparavant, sélectionnez **Écraser la liste en cours**.

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

18.6. Configurer les filtres antispam locaux

Comme cela est décrit dans « *Aperçu de l'antispam* » (p. 115), Bitdefender utilise une combinaison de divers filtres antispam pour identifier le spam. Les filtres antispam sont préconfigurés pour une protection efficace.

> **Important**
>
> Selon que vous recevez ou non des e-mails légitimes rédigés avec des caractères asiatiques ou cyrilliques, désactivez ou activez le paramètre bloquant automatiquement ces e-mails. Le paramètre correspondant est désactivé dans les versions localisées du programme utilisant ces jeux de caractères (par exemple, dans la version russe ou chinoise).

Pour configurer les filtres antispam locaux :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTISPAM**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton Activer/Désactiver correspondant.

Si vous utilisez Microsoft Outlook ou Thunderbird, vous pouvez configurer les filtres antispam locaux directement à partir de votre client de messagerie. Cliquez sur le bouton ⚙ **Paramètres** de la barre d'outils antispam de Bitdefender (généralement situé dans la partie supérieure de la fenêtre du client de messagerie) puis sur l'onglet **Filtres Antispam**.

18.7. Configurer les paramètres cloud

La détection « in the cloud » utilise les services Cloud de Bitdefender pour vous fournir une protection antispam efficace et toujours à jour.

La protection cloud fonctionne tant que vous maintenez Bitdefender Antispam activé.

Des échantillons d'e-mails de spam ou légitimes peuvent être envoyés au Cloud Bitdefender lorsque vous signalez des erreurs de détection ou des e-mails de spam non détectés. Cela contribue à améliorer la détection antispam de Bitdefender.

Pour configurer l'envoi d'échantillons d'e-mails au Cloud Bitdefender, sélectionnez les options souhaitées en procédant comme suit :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTISPAM**, cliquez sur **Paramètres**.
3. Cliquez sur le bouton Activer/Désactiver correspondant.

Si vous utilisez Microsoft Outlook ou Thunderbird, vous pouvez configurer la détection cloud directement à partir de votre client de messagerie. Cliquez sur le bouton ⚙ **Paramètres** de la barre d'outils antispam de Bitdefender (généralement situé dans la partie supérieure de la fenêtre du client de messagerie) puis sur l'onglet **Configuration du Cloud**.

19. PARE-FEU

Le pare-feu protège votre ordinateur contre les tentatives de connexion non autorisées entrantes et sortantes, à la fois sur les réseaux locaux et sur internet. Il fonctionne un peu comme un garde à votre porte - il surveille les tentatives de connexion et détermine celles à autoriser et à bloquer.

Le pare-feu Bitdefender utilise un ensemble de règles pour filtrer des données transmises vers et à partir de votre système.

Dans des conditions normales, Bitdefender crée automatiquement une règle lorsqu'une application essaie d'accéder à Internet. Vous pouvez également ajouter ou modifier manuellement des règles d'applications.

Vous recevrez une notification à chaque fois que l'accès d'une application potentiellement malveillante à Internet est bloqué.

Bitdefender attribue automatiquement un type de réseau à chaque connexion réseau qu'il détecte. En fonction du type de réseau, la protection pare-feu est définie pour le niveau approprié de chaque connexion.

Pour en savoir plus sur la configuration du pare-feu pour chaque type de réseau et sur comment modifier les paramètres réseau, veuillez vous reporter à « *Gérer les paramètres de connexion* » (p. 128).

19.1. Activer ou désactiver la protection pare-feu

Pour activer ou désactiver la protection pare-feu :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PARE-FEU**, activez ou désactivez le bouton.

Avertissement

La désactivation du pare-feu exposant votre ordinateur à des connexions non autorisées, il devrait s'agir d'une mesure temporaire. Réactivez le pare-feu dès que possible.

19.2. Gestion des règles des applications

Pour afficher et gérer les règles pare-feu contrôlant l'accès des applications aux ressources du réseau et à internet :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PARE-FEU**, cliquez sur **Accès des applications**.
3. La fonctionnalité Pare-Feu vous sera présentée lors de sa première exécution. Cliquez sur **OK, J'AI COMPRIS** pour continuer.

Vous pouvez ici connaitre les 15 derniers programmes (processus) à être passé par le Pare-Feu Bitdefender et le réseau auquel vous êtes connecté. Pour voir les règles créer pour une application en particulier, cliquez sur celle-ci, puis cliquez sur le lien **Voir les règles d'application**. La fenêtre **Règles** apparait.

Les informations suivantes s'affichent pour chaque règle :

- **RÉSEAU** - les processus et les types d'adaptateur réseau (Domicile / Bureau, Public ou Tous) auxquels la règle s'applique. Des règles sont créées automatiquement pour filtrer l'accès réseau ou internet via n'importe quel adaptateur. Les règles s'appliquent par défaut à tout réseau. Vous pouvez créer manuellement des règles ou éditer des règles existantes, afin de filtrer l'accès réseau ou Internet d'une application via un adaptateur spécifique (par exemple un adaptateur réseau sans fil).
- **Protocole** - le protocole IP auquel s'applique la règle. Les règles s'appliquent par défaut à tout protocole.
- **TRAFIC** - les règles s'appliquent dans le sens entrant comme sortant.
- **PORTS** - le protocole du port auquel s'applique la règle. Les règles s'appliquent par défaut à tous les ports.
- **IP** - le protocole IP auquel s'applique la règle. Les règles s'appliquent par défaut à toutes les adresses IP.
- **ACCÈS** - si l'application est autorisée ou non à se connecter au réseau ou à Internet selon les circonstances spécifiées.

Pour modifier ou supprimer les règles de l'application sélectionnée, cliquez sur l'icône ⋯.

- **Éditer une règle** - ouvre une fenêtre dans laquelle vous pouvez modifier une règle.
- **Supprimer la règle** - vous pouvez choisir de supprimer les règles actuelles de l'application sélectionnée.

Ajout de règles d'application

Pour ajouter une règle d'application :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PARE-FEU**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Règles**, cliquez sur **Ajouter une règle**.

Dans la fenêtre **PARAMÈTRES** vous pouvez appliquer les modifications suivantes :

- **Appliquer cette règle à toutes les applications.** Appuyez sur ce bouton pour appliquer les règles créées à toutes les applications.
- **Chemin du programme.** Cliquez sur **PARCOURIR** et sélectionnez l'application à laquelle s'applique la règle.
- **Permission.** Sélectionnez l'une des permissions disponibles :

Permission	Description
✔	L'application spécifiée se verra autoriser l'accès réseau/Internet dans les circonstances spécifiées.
✖	L'application spécifiée se verra refuser l'accès réseau/Internet dans les circonstances spécifiées.

- **Réseau.** Sélectionnez le type de réseau auquel s'applique la règle. Vous pouvez modifier le type de réseau en ouvrant le menu déroulant **Type de Réseau** et en sélectionnant l'un des types de réseau disponibles dans la liste.

Réseau	Description
Tous les réseaux	Autoriser tout le trafic entre votre ordinateur et les autres ordinateurs quel que soit le type de réseau.
Domicile/Bur.	Autoriser tout le trafic entre votre ordinateur et les ordinateurs du réseau local.
Public	Tout le trafic est filtré.

- **Protocole.** Sélectionnez dans le menu le protocole IP auquel s'applique la règle.
  - Si vous voulez que la règle s'applique à tous les protocoles, sélectionnez **Toutes**.
  - Si vous souhaitez que la règle s'applique au protocole TCP, sélectionnez **TCP**.
  - Si vous souhaitez que la règle s'applique au protocole UDP, sélectionnez **UDP**.
  - Si vous souhaitez que la règle s'applique au protocole ICMP, sélectionnez **ICMP**.
  - Si vous souhaitez que la règle s'applique au protocole IGMP, sélectionnez **IGMP**.
  - Si vous souhaitez que la règle s'applique à un protocole spécifique, saisissez le numéro affecté au protocole que vous souhaitez filtrer dans le champ vide.

    Note

    Les numéros des protocoles IP sont attribués par l'IANA (Internet Assigned Numbers Authority, l'organisation de gestion de l'adressage IP sur Internet). Vous pouvez obtenir la liste complète des numéros de protocoles IP attribués à l'adresse http://www.iana.org/assignments/protocol-numbers.

- **Direction.** Sélectionnez dans le menu la direction du trafic à laquelle s'applique la règle.

Direction	Description
Sortant	La règle s'applique seulement pour le trafic sortant.
Entrant	La règle s'applique seulement pour le trafic entrant.
Tous les deux	La règle s'applique dans les deux directions.

Dans la fenêtre **Avancé** vous pouvez personnaliser les paramètres suivants :

- **Adresse locale personnalisée.** Spécifiez l'adresse IP locale et le port auxquels s'applique la règle.

- **Adresse distante personnalisée.** Spécifiez l'adresse IP distante et le port auxquels s'applique la règle.

Pour supprimer les règles actuelles et restaurer celles par défaut, cliquez sur **Réinitialiser les règles** dans la fenêtre **Règles**.

19.3. Gérer les paramètres de connexion

Que vous vous connectiez à Internet via le WiFi ou un adaptateur Ethernet, vous pouvez configurer les réglages à appliquer pour assurer une navigation sûre. Les différentes options sont les suivantes :

- **Dynamique** – Le type de réseau sera automatiquement défini sur la base du profil du réseau auquel vous êtes connecté, Domicile / Bureau ou Public. Dans ce cas, seules les règles du Pare-feu pour le type de réseau ou celles définies pour tous les réseaux s'appliquent.
- **Domicile / Bureau** – Le type de réseau sera toujours Domicile / Bureau, quel que soit le profil du réseau auquel vous êtes connecté. Dans ce cas, seules les règles du Pare-feu pour le type de réseau Domicile / Bureau s'appliquent.
- **Public** – Le type de réseau sera toujours Public, quel que soit le profil du réseau auquel vous êtes connecté. Dans ce cas, seules les règles du Pare-feu pour le type de réseau Public s'appliquent.

Pour configurer vos adaptateurs réseau :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PARE-FEU**, cliquez sur **Paramètres**.
3. Cliquez sur l'onglet **Cartes réseau**.
4. Sélectionnez les options que vous voulez appliquer lors de la connexion aux adaptateurs suivants :
   - Wi-Fi
   - Ethernet

19.4. Configurer les paramètres avancés

Pour configurer les paramètres avancés du pare-feu :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PARE-FEU**, cliquez sur **Paramètres**.
3. Sélectionnez l'onglet **Paramètres**.

Les fonctionnalités suivantes peuvent être configurées :

- **Protection lors de l'analyse des ports** - détecte et bloque les démarches visant à détecter des ports ouverts sur un ordinateur.

  Les analyses de ports sont fréquemment utilisées par les pirates pour découvrir des ports ouverts sur votre ordinateur. Ils peuvent alors s'introduire dans votre ordinateur, s'ils découvrent un port vulnérable ou moins sécurisé.

- **Mode alerte** - une alerte est affichée à chaque fois qu'une application essaye de se connecter à Internet. Sélectionnez **Autoriser** ou **Bloquer**. Quand le mode Alerte est activé, la fonctionnalité Profils est automatiquement désactivée. Le Mode alerte peut être utilisé simultanément avec le **Mode Batterie**.

- **Mode Furtif** - détermine si vous pouvez être détecté par d'autres ordinateurs. Cliquez sur **Éditer les réglages de furtivité** pour sélectionner quand votre appareil doit ou ne doit pas être visible des autres ordinateurs.

- **Comportement par défaut des applications** - autorise Bitdefender à appliquer des réglages automatiques aux applications pour lesquelles aucune règle n'est définie. Cliquez sur **Éditer les règles par défaut** pour choisir si les réglages automatiques doivent ou non être appliqués.

  - Automatique - L'accès des applications sera autorisé ou bloqué en fonction des règles automatiques du pare-feu et de l'utilisateur.
  - Autoriser - Les applications n'ayant pas de règle de pare-feu seront automatiquement autorisées.
  - Bloquer - Les applications n'ayant pas de règle de pare-feu seront automatiquement bloquées.

20. VULNÉRABILITÉ

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

Bitdefender recherche automatiquement les vulnérabilités de votre système et vous les signale. Il analyse :

- la présence sur votre ordinateur d'applications non à jour.
- des mises à jour Windows manquantes
- des mots de passe non sécurisés de comptes utilisateurs Windows
- les réseaux et routeurs sans fils non protégés.

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.

20.1. Analyser votre système à la recherche de vulnérabilités

Pour corriger les vulnérabilités du système à l'aide de l'option Analyse de Vulnérabilité :

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

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

   - **Mises à jour critiques Windows**

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

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

   - **Mises à jour d'applications**

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

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

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

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

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

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

   - **Réseaux Wi-Fi**

     Cliquez sur **Voir détails** pour en savoir plus sur le réseau sans fil auquel vous êtes connecté. S'il est recommandé de définir un mot de passe plus fort pour votre réseau domestique, cliquez sur le lien correspondant.

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

Le coin supérieur droit de la fenêtre vous permet de filtrer les résultats en fonction de vos préférences.

20.2. 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 **Paramètres**.

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

3. 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 protégés, permettant ainsi aux pirates d'accéder à votre 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.

20.3. Wi-Fi Security Advisor

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 e-mails 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 e-mails, 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, cela peut être des réseaux malveillants ou honeypots, faisant d'eux une cible pour les cyber-criminels.

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.

Le Wifi Security Advisor Bitdefender donne des informations sur :

- Réseaux Wifi domestiques
- Réseaux Wifi publics

20.3.1. Activer ou désactiver les notifications Wifi Security Advisor

Pour activer ou désactiver les notifications Wifi Security Advisor :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **Vulnérabilité**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Paramètres**, activez ou désactivez l'option **Contrôle de sécurité des réseaux Wi-Fi**

20.3.2. Configuration du réseau Wifi 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 **Contrôle de sécurité des réseaux Wi-Fi**.
3. Dans l'onglet **WI-FI DOMESTIQUE**, cliquez sur le bouton **SÉLECTIONNER WI-FI DOMESTIQUE**.

   Une liste avec les réseaux sans fil auxquels vous vous êtes connectés jusqu'à ce jour s'affiche.
4. 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**.

20.3.3. 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 Internet Security est réglé pour accomplir automatiquement les paramètres de programme suivants :

- Advanced Threat Defense est activé
- Le pare-feu Bitdefender est activé et les paramètres suivants sont appliqués à votre adaptateur sans fil :
  - Mode furtif - ON
  - Type de réseau - public
- Les paramètres suivants de la Prévention des menaces en ligne sont activés :
  - Analyse web chiffrée
  - Protection contre les escroqueries
  - Protection contre le phishing
- Un bouton qui ouvre Bitdefender Safepay™ est disponible. Dans ce cas, la Protection hotspot pour les réseaux non sécurisés est activée par défaut.

20.3.4. 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 **Contrôle de sécurité des réseaux Wi-Fi**.
3. Selon les informations dont vous avez besoin, sélectionnez l'une des deux balises, **WI-FI DOMESTIQUE** ou **WI-FI PUBLIC**.
4. 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 activés.

Wifi dangereux - indique que le niveau de sécurité du réseau est moyenne. Cela signifie qu'il peut avoir des vulénrabilités 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 activés.
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 cryptés 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 qui ont mis des mots de passe faibles représentent une cible pour les cyber-criminels.
- **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.

Conservez l'option **Notifier** activée pour recevoir des notifications chaque fois que votre système se connecte à ce réseau.

21. PROTECTION DE WEBCAM

Le fait que les pirates soit en mesure d'exploiter votre webcam pour vous espionner n'a rien de nouveau, mais les solutions pour s'en prévenir, comme révoquer les privilèges de l'application, désactiver la caméra intégrée d'un appareil ou la couvrir n'ont rien de pratique. Pour empêcher les tentatives violation de votre vie privée, la Protection de Webcam Bitdefender surveille en permanence les applications qui essayent d'avoir accès à votre caméra et bloque celles n'étant pas considérées comme de confiance.

Vous recevrez une notification à chaque fois qu'une application non listée comme de confiance tentera d'avoir accès à votre caméra.

21.1. Activer ou désactiver la protection webcam

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PROTECTION WEBCAM**, cliquez sur le bouton Activer/Désactiver.

21.2. Configurer la protection webcam

Vous pouvez configurer les règles à appliquer lorsqu'une application tentera d'avoir accès à votre caméra en suivant ces instructions :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PROTECTION DE WEBCAM**, cliquez sur **Paramètres**.

Règles de blocage des applications

- **Bloquer tous les accès à la webcam** - aucune application n'aura l'autorisation d'accéder à votre webcam.
- **Bloquer l'accès des navigateurs à la webcam** - aucun navigateur Internet, sauf Internet Explorer et Microsoft Edge, n'aura l'autorisation d'accéder à votre webcam. Comme toutes les applications du Windows Store sont exécutées via un seul processus, Internet Explorer et Microsoft Edge ne peuvent pas être identifiés par Bitdefender en tant que navigateur Internet, et sont donc exclus de ce réglage.
- **Définir l'accès des applications à la webcam en fonction du choix des utilisateurs de Bitdefender** - si la majorité des utilisateurs de Bitdefender

considère l'application comme inoffensive, son accès à la webcam sera automatiquement autorisé. Si une application populaire est considérée comme dangereuse par la plupart d'entre eux, son accès sera automatiquement bloqué.

Vous serez informé à chaque fois qu'une de vos applications installées sera listée comme bloquée par la majorité des utilisateurs de Bitdefender.

Notifications

- **M'envoyer une notification quand une application autorisée se connecte à la webcam** - vous recevrez une notification à chaque fois qu'une application autorisée se connectera à la webcam.

21.3. Ajouter des applications à la liste de Protection de la Webcam

Les applications qui essayent de se connecter à votre webcam sont automatiquement détectées et leur accès est autorisé ou bloqué en fonction de leur comportement et du choix de la communauté. Néanmoins, vous pouvez configurer manuellement les mesures à prendre en suivant ces instructions :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PROTECTION WEBCAM**, cliquez sur **Accès à la Webcam**.
3. La fonctionnalité Protection de webcam vous sera présentée lors de sa première exécution.
4. Cliquez sur le lien désiré :
   - **Sélectionnez les applications Windows Store à ajouter à la liste des permissions** - une liste des applications Windows Store détectées apparait. Activez les boutons situés à côté des applications que vous voulez ajouter à la liste.
   - **Commencer à ajouter des applications à la liste d'accès à la webcam** - rendez-vous vers le fichier .exe que vous voulez ajouter à la liste, puis cliquez sur **OK**.

     Pour ajouter d'autres applications, cliquez sur le lient **Ajouter une nouvelle application à la liste**.

Cliquez sur le bouton **Accès autorisé / Accès bloqué**.

Pour savoir ce que les utilisateurs de Bitdefender ont décidé de faire de l'application sélectionnée, cliquez sur l'icône .

Cette fenêtre indiquera les applications qui ont demandé à avoir accès à votre webcam ainsi que la date de dernière activité.

Vous recevrez une notification à chaque fois qu'une des applications de la liste est autorisée par les utilisateurs de Bitdefender.

22. SAFE FILES

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

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

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

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

Avec Safe Files de Bitdefender, vous pouvez protéger vos fichiers personnels, tels que vos documents, photos ou films, des attaques par ransomware.

> **Note**
> Advanced Threat Defense et Safe Files sont deux couches de protection contre les ransomwares. Advanced Threat Defense est la fonctionnalité qui bloque les attaques de ransomware lorsqu'ils essayent d'accéder aux zones critiques de votre système, et Safe Files veille à ce qu'aucun fichier important de votre ordinateur ne soit chiffré.

22.1. Activer ou désactiver Safe Files

Pour activer ou désactiver la fonction Safe Files :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **SAFE FILES**, cliquez sur le bouton Activer/Désactiver.

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

Note
La fonctionnalité Safe Files n'est pas activée par défaut.

22.2. Protégez vos fichiers personnels contre les attaques de ransomwares

Si vous souhaitez mettre des fichiers personnels à l'abri :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **SAFE FILES**, cliquez sur **Dossiers protégés**.
3. La fonctionnalité Dossiers protégés vous sera présentée lors de sa première exécution. Cliquez sur **PROTÉGER PLUS DE DOSSIERS** pour continuer.
4. Sélectionnez le dossier que vous voulez protéger et cliquez sur **OK**.

   Pour ajouter d'autres dossiers, cliquez sur le lien **Protéger plus de dossiers**. Sinon, glissez-déposez les dossiers vers cette fenêtre.

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

Pour éviter les ralentissements du système, nous vous recommandons de ne pas ajouter plus de 30 dossiers, ou d'enregistrer de multiples fichiers dans un seul dossier.

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

22.3. Configuration des accès des applications

Ces applications qui tentent de modifier ou supprimer des fichiers protégés peuvent être signalées comme potentiellement dangereuses et ajoutées à la liste des applications bloquées. Si une telle application est bloquée et que vous êtes sûr que son comportement est normal, vous pouvez l'autoriser en procédant comme suit :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **SAFE FILES**, cliquez sur **Accès de l'application**.
3. Les applications qui essayent de modifier les fichiers de vos dossiers protégés sont présentées sous forme de liste. Activez le bouton situé à côté de l'application dont vous êtes certain qu'elle est fiable.

Sur cette même fenêtre, vous pouvez désactiver la protection contre les ransomwares pour certaines applications en désactivant sur le bouton correspondant.

Si vous voulez ajouter des applications à cette liste, cliquez sur le lien **Ajouter une nouvelle application à la liste**.

22.4. Protection au démarrage

Il est connu que plusieurs applications malveillantes sont configurées pour s'exécuter au démarrage, ce qui peut sérieusement abîmer une machine. La protection au démarrage Bitdefender analyse tous les zones systèmes critiques avant que tous les fichiers ne soient chargés, sans impact sur le système.

Pour désactiver la protection au démarrage :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **SAFE FILES**, cliquez sur **Paramètres**.
3. Désactivez la **Protection au démarrage**.

> **Note**
> Les applications ajoutées aux exceptions seront également analysées et traitées de la même manière.

23. REMÉDIATION DES RANSOMWARES

Le Nettoyage 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.

23.1. Activer ou désactiver le Nettoyage des ransomwares

Pour activer ou désactiver le Nettoyage des ransomwares :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **NETTOYAGE 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.

23.2. 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 **NETTOYAGE DES RANSOMWARES**, cliquez sur **Configurer**.
3. Activez ou désactivez le bouton **Restauration automatique**.

23.3. 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. De cette façon, vos fichiers 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.

23.4. 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 **RESTAURER 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 terminer la procédure 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;

23.5. 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 **REMÉDIATION DES RANSOMWARES**, cliquez sur **Exceptions**.
3. Pour ajouter des applications à la liste, cliquez sur **Ajouter une nouvelle application à la liste**.

24. CHIFFREMENT DE FICHIERS

Le Chiffrement de Fichiers Bitdefender vous permet de créer des disques (ou coffres) chiffrés, protégés par mot de passe, sur votre ordinateur, dans lesquels vous pouvez stocker vos documents confidentiels ou sensibles en toute sécurité. Les données stockées dans le coffre-fort ne sont accessibles qu'aux utilisateurs connaissant le mot de passe.

Le mot de passe vous permet d'ouvrir le coffre-fort pour y stocker vos données et de le refermer tout en préservant sa sécurité. Pendant qu'un coffre est ouvert, vous pouvez ajouter de nouveaux fichiers, accéder au fichiers courants ou les modifier.

Physiquement, le coffre-fort est un fichier stocké sur votre disque dur local avec l'extension .bvd. Même si les fichiers représentant les coffres peuvent être atteints depuis un système d'exploitation différent comme Linux, les informations stockées dedans ne peuvent être lues car elles sont chiffrées.

Les coffres-forts peuvent être gérés depuis la fenêtre de Bitdefender ou à l'aide du menu contextuel Windows et du disque logique associé au coffre-fort.

24.1. Gérer des coffres-forts

Pour gérer vos coffres-forts depuis Bitdefender

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **CHIFFREMENT DE FICHIERS**, cliquez sur **Paramètres**.

   Les coffres-forts existants apparaissent dans cette fenêtre.

24.2. Créer des coffres-forts

Pour créer un nouveau coffre-fort :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Sous le panneau **CHIFFREMENT DE FICHIERS**, cliquez sur **Créer un nouveau coffre-fort**.
3. Spécifiez l'emplacement et le nom du coffre-fort.
   - Saisissez le nom du fichier du coffre-fort dans le champ correspondant.

- Cliquez sur **PARCOURIR** pour sélectionner l'emplacement du coffre-fort et sauvegardez le coffre-fort sous le nom que vous souhaitez.

4. Sélectionnez une lettre de lecteur dans le menu correspondant. Quand vous ouvrez le coffre, un disque virtuel indexé avec la lettre choisie apparaît dans Poste de travail.
5. Si vous souhaitez modifier la taille par défaut du coffre-fort (100 Mo), utiliser les touches des flèches haut et bas dans le champ **Taille du coffre-fort (Mo)**.
6. Tapez le mot de passe souhaité pour le coffre-fort dans les champs **Mot de passe** et **Confirmer mot de passe**. Le mot de passe doit comporter au moins 8 caractères. Toutes personnes essayant d'ouvrir le coffre et d'utiliser les fichiers doit fournir le mot de passe.
7. Cliquez sur **CRÉER**.

Bitdefender vous informera immédiatement du résultat de l'opération. Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème.

Pour créer un nouveau coffre-fort plus rapidement, faites un clic droit sur votre bureau ou dans un dossier de votre ordinateur, pointez sur **Bitdefender** > **Coffre-fort Bitdefender** et sélectionnez **Créer un coffre-fort** .

Note
Il peut être pratique d'enregistrer tous les coffres-forts au même emplacement. De cette façon, vous les retrouverez plus vite.

24.3. Importer un coffre-fort

Pour importer un coffre-fort enregistré en local :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **CHIFFREMENT DE FICHIERS**, cliquez sur **Importer un coffre-fort**.
3. Recherchez l'emplacement de votre coffre-fort et sélectionnez-le (le fichier .bvd).
4. Cliquez sur **Ouvrir**.

24.4. Ouverture de coffres-forts

Pour accéder aux fichiers contenus dans un coffre et pouvoir travailler avec ces fichiers, il faut d'abord ouvrir le coffre. Quand vous ouvrez le coffre, un disque virtuel s'affiche dans le Poste de travail. Le disque se voit attribuer la lettre correspondant au coffre.

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **CHIFFREMENT DE FICHIERS**, cliquez sur **Paramètres**.
3. Sélectionnez le coffre-fort que vous voulez ouvrir et cliquez sur **DÉVERROUILLER**.
4. Entrez le mot de passe requis puis cliquez sur **OK**.
5. Cliquez sur **OUVRIR** pour ouvrir votre coffre-fort.

Bitdefender vous informera immédiatement du résultat de l'opération. Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème.

Pour ouvrir votre coffre-fort plus rapidement, localisez sur votre ordinateur le fichier .bvd correspondant au coffre-fort que vous voulez ouvrir. Faites un clic droit sur le fichier, allez sur **Bitdefender** > **Coffre-fort Bitdefender**et sélectionnez **Déverrouiller**. Entrez le mot de passe requis puis cliquez sur **OK**.

24.5. Ajouter des fichiers aux coffres-forts

Avant de pouvoir ajouter des fichiers ou des dossiers à un coffre-fort, vous devez ouvrir le coffre-fort.

Pour ajouter de nouveaux fichiers à votre coffre-fort :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **CHIFFREMENT DE FICHIERS**, cliquez sur **Paramètres**.
3. Sélectionnez le coffre-fort dans lequel vous voulez ajouter des fichiers et cliquez sur **DÉVERROUILLER**.
4. Entrez le mot de passe requis puis cliquez sur **OK**.
5. Cliquez sur **OUVRIR** pour ouvrir votre coffre-fort.

6. Ajoutez des fichiers ou des dossiers comme vous le faites habituellement sous Windows (par exemple, vous pouvez utiliser la méthode du copier-coller).

Pour ajouter plus rapidement des fichiers à votre coffre-fort, faites un clic droit sur le fichier ou le dossier que vous voulez copier dans un coffre-fort, allez sur **Bitdefender** > **Coffre-Fort Bitdefender** et sélectionner **Ajouter au coffre-fort**.

- Si un seul coffre-fort est ouvert, le fichier ou le dossier est copié directement dans ce coffre-fort.
- Si plusieurs coffres-forts sont ouverts, on vous demandera de choisir le coffre-fort où copier l'élément. Sélectionnez dans le menu la lettre de lecteur correspondant au coffre-fort souhaité et cliquez sur **OK** pour copier l'élément.

24.6. Verrouiller des coffres-forts

Quand vous avez fini de travailler avec les fichiers d'un coffre-fort, vous devez le verrouiller pour protéger vos données. En verrouillant le coffre-fort, le disque virtuel correspondant disparaît de Poste de Travail. L'accès aux données contenues dans le coffre est donc complètement bloqué.

Pour fermer un coffre-fort :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **CHIFFREMENT DE FICHIERS**, cliquez sur **Paramètres**.
3. Sélectionnez le coffre-fort que vous voulez verrouiller et cliquez sur **VERROUILLER**.

Bitdefender vous informera immédiatement du résultat de l'opération. Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème.

Pour verrouiller plus rapidement un coffre-fort, vous pouvez également faire un clic droit sur le fichier .bvd représentant le coffre-fort, aller dans **Bitdefender** > **Coffre-Fort Bitdefender** et sélectionner **Verrouiller**.

24.7. Supprimer des fichiers des coffres-forts

Pour pouvoir supprimer des fichiers ou des dossiers d'un coffre-fort, le coffre-fort doit être ouvert. Pour supprimer des fichiers ou des dossiers d'un coffre-fort :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **CHIFFREMENT DE FICHIERS**, cliquez sur **Paramètres**.
3. Sélectionnez le coffre-fort dans lequel vous voulez supprimer des fichiers et cliquez sur **DÉVERROUILLER** s'il est verrouillé.
4. Cliquez sur **OUVRIR**.

   Supprimez des fichiers ou des dossiers comme vous le faites habituellement avec Windows (par exemple, faites un clic droit sur un fichier que vous souhaitez supprimer et sélectionnez **Supprimer**).

24.8. Changer le mot de passe du coffre-fort

Le mot de passe protège le contenu d'un coffre-fort contre les accès non autorisés. Seuls les utilisateurs connaissant le mot de passe peuvent ouvrir le coffre-fort et accéder aux documents et aux données qu'il contient.

Le coffre-fort doit être verrouillé pour que vous puissiez modifier son mot de passe. Pour changer le mot de passe d'un coffre-fort :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **CHIFFREMENT DE FICHIERS**, cliquez sur **Paramètres**.
3. Sélectionnez le coffre-fort dont vous voulez modifier le mot de passe et cliquez sur **PARAMÈTRES**.
4. Entrez le mot de passe actuel du coffre-fort dans le champ **Ancien mot de Passe**.
5. Tapez le nouveau mot de passe souhaité pour le coffre-fort dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**.

> **Note**
> Le mot de passe doit comporter au moins 8 caractères. Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

Bitdefender vous informera immédiatement du résultat de l'opération. Si une erreur s'est produite, utilisez le message d'erreur pour essayer de régler le problème.

Pour changer plus rapidement le mot de passe d'un coffre-fort, localiser sur votre ordinateur le fichier .bvd qui représente le coffre-fort. Faites un clic droit sur le fichier, allez sur **Bitdefender** > **Coffre-fort des Bitdefender** et sélectionnez **Modifier le mot de passe du coffre-fort**.

25. PROTECTION PASSWORD MANAGER DE VOS IDENTIFIANTS

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

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

Et si nous ne sommes pas prudents sur Internet, nos informations confidentielles telles que notre adresse courriel, nos identifiants de messagerie instantanée ou les données de notre carte bancaire peuvent être compromises.

Noter vos mots de passe ou vos données confidentielles sur une feuille de papier ou dans votre ordinateur peut être dangereux car cela les rend accessibles à des personnes qui souhaitent les dérober et les utiliser. Et vous souvenir de tous les mots de passe que vous avez définis pour vos comptes en ligne ou pour vos sites Web préférés n'est pas une tâche facile.

Y a-t-il un moyen de nous garantir de trouver nos mots de passe au moment où nous en avons besoin ? Et pouvons-nous être sûrs que nos mots de passe confidentiels sont en sécurité ?

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

En utilisant un mot de passe principal unique pour accéder à vos identifiants, Password Manager vous permet de conserver facilement vos mots de passe en sécurité dans un Wallet.

Pour fournir la meilleure protection possible à vos activités en ligne, Password Manager est intégré à Bitdefender Safepay™ et offre une solution intégrée pour répondre aux différentes façons dont vos données confidentielles peuvent être compromises.

Password Manager protège les informations confidentielles suivantes :

- Des informations personnelles, telles que l'adresse courriel ou le numéro de téléphone
- Les identifiants de connexion aux sites Web
- Les informations bancaires sur les comptes et les numéros de carte

- Les données permettant d'accéder aux comptes de messagerie
- Mots de passe des applications
- Les mots de passe des réseaux Wi-Fi

25.1. Créer une nouvelle base de données Wallet

BitdefenderWallet est l'endroit où vous pouvez stocker vos données personnelles. Pour simplifier l'expérience de navigation, vous devez créer une base de données Wallet comme suit :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Créer un nouveau Wallet**.
3. Cliquez sur **Créer nouveau**.
4. Tapez les informations requises dans les champs correspondants.
   - Nom Wallet - saisissez un nom unique pour votre base de données Wallet.
   - Mot de passe principal - saisissez un mot de passe pour votre Wallet.
   - Saisissez le mot de passe à nouveau - saisissez à nouveau le mot de passe que vous avez configuré.
   - Indice - saisissez un indice pour vous souvenir du mot de passe.
5. Cliquez sur **CONTINUER**.
6. A cette étape, vous pouvez choisir de stocker vos informations dans le cloud. Si vous choisissez Oui, vos informations bancaires seront conservées localement sur votre appareil. Choisissez l'option souhaitée, puis cliquez sur **CONTINUER**.
7. Sélectionnez le navigateur web à partir duquel vous souhaitez importer vos identifiants.
8. Cliquez sur **TERMINER**.

25.2. Importer une base de données existante

Pour importer une base de données Wallet enregistrée en local :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PASSWORD MANAGER**, cliquez sur **Créer un nouveau Wallet**.
3. Cliquez sur **DEPUIS LA CIBLE**.
4. Rendez-vous à l'emplacement de votre appareil où vous voulez enregistrer la base de données du wallet, puis saisissez un nom.
5. Cliquez sur **Ouvrir**.
6. Donnez un nom à votre Wallet et saisissez le mot de passe attribué lors de sa création.
7. Cliquez sur **IMPORTER**.
8. Sélectionnez les programmes desquels le Wallet doit importer les identifiants, puis cliquez sur le bouton **TERMINER**.

25.3. 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 **Mes Wallets**.
3. Cliquez sur l'icône ⋮ du Wallet désiré, puis sélectionnez **Exporter**.
4. Recherchez l'emplacement de votre base de données Wallet et sélectionnez-la (le fichier .db).
5. Cliquez sur **Enregistrer**.

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

25.4. 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 **Mes Wallets**.
3. Cliquez sur l'icône ⋮ du Wallet désiré, puis sélectionnez **Configuration**.
4. 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 saisissez le mot de passe attribué lors de sa création.

25.5. 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 **Mes Wallets**.
3. Sélectionnez la base de données Wallet désirée, puis cliquez sur **ACTIVER LE WALLET**.
4. Entrez le mot de passe Master puis cliquez sur **OK**.

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

- Identité
- Sites Web
- Banques
- E-mails
- Accueil
- 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 un objet de la liste, sélectionnez le et cliquez sur le bouton **Editer**.
- Pour effacer une entrée, sélectionnez-la puis cliquez sur le bouton **Supprimer**.

25.6. Activer ou désactiver la protection du Password Manager

Pour activer ou désactiver la protection par Gestionnaire de mot de passe :

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.

25.7. Gestion des configurations du Password Manager

Pour configurer le mot de passe Master en détails :

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 l'onglet **Paramètres de sécurité**.

Voici les options proposées :

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

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

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

Améliorer votre expérience

Pour sélectionner les navigateurs ou les applications où vous souhaitez intégrer le Gestionnaire de mot 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. Sélectionnez l'onglet **Plugins**.

   Cochez une application pour utiliser le Password Manager et améliorer votre expérience :

   - Internet Explorer
   - Mozilla 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 saisissez vos informations d'identification et données personnelles dans votre navigateur Web pour la première fois, celles-ci sont automatiquement conservées en toute sécurité dans 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. Sélectionnez l'onglet **Paramètres saisie automatique**.
4. Configurez les options suivantes :
   - **Configurer la façon dont Password Manager sécurise vos identifiants**:
     - **Enregistrer automatiquement les identifiants dans 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 de Password Manager à partir de votre navigateur

Vous pouvez facilement gérer les détails de Password Manager directement à partir de votre navigateur afin d'avoir toutes vos données importantes à portée de main. L'extension Bitdefender Wallet est compatible avec les navigateurs suivants : Google Chrome, Internet Explorer et Mozilla Firefox et est également intégré à Safepay.

Pour accéder à l'extension Bitdefender Wallet, ouvrez votre navigateur web, autorisez l'installation de l'add-on et cliquez sur l'icône de la barre d'outils.

L'extension Bitdefender Wallet présente les options suivantes :

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

26. 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.

26.1. Installation du VPN

L'application VPN peut être installée depuis l'interface de Bitdefender, comme suit :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **VPN**, cliquez sur **Installer le VPN**.
3. Dans la fenêtre présentant l'application VPN, lisez les **Conditions d'utilisation de l'abonnement**, puis cliquez sur **INSTALLER LE VPN Bitdefender**.

   Attendez quelques instants pendant le téléchargement et l'installation des fichiers.
4. Cliquez sur **OUVRIR LE VPN BITDEFENDER** pour finir le processus d'installation.

Note
Le VPN Bitdefender nécessite que .Net Framework 4.5.2 ou supérieur soit installé. Si ce package n'est pas installé, une fenêtre de notification apparaitra. Cliquez sur **installer .Net Framework** pour être redirigé vers une page depuis laquelle vous pourrez télécharger la dernière version de ce logiciel.

26.2. 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**.

26.3. 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. 163).

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.

Lorsque vous êtes connecté, le temps passé et l'adresse IP qui vous a été attribuée sont affichés dans la partie inférieure de l'interface.

Pour accédez aux autres options, accédez au **Menu** en cliquant 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.

- **Paramètres** – vous pouvez personnaliser le produit en fonction de vos besoins :
  - recevoir des notifications lorsque le VPN se connecte ou se déconnecte automatiquement
  - exécuter automatiquement l'application VPN au démarrage de Windows
  - exécuter automatiquement l'application VPN lorsque votre appareil se connecte à un réseau sans fil non sécurisé
- **Passer à Premium** - si vous utilisez la version gratuite, vous pouvez ici passer à la version Premium.
- **Support** - vous serez redirigé vers notre plateforme d'assistance sur laquelle vous pourrez trouver des articles sur la manière d'utiliser le VPN Bitdefender.
- **À propos** - Informations sur la version installée de l'appli.

26.4. 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 **OBTENIR UN TRAFIC ILLIMITÉ** sur l'interface du produit.

L'abonnement de Bitdefender Premium VPN est indépendant de l'abonnement gratuit à Bitdefender Internet Security, 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 Internet Security 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.

27. LA SÉCURITÉ SAFEPAY POUR LES TRANSACTIONS EN LIGNE

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

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

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

Pour une meilleure protection de la vie privée, Bitdefender Password Manager est intégré à Bitdefender Safepay™ afin de protéger vos identifiants lorsque vous essayez d'accéder à des espaces en ligne confidentiels. Pour plus d'informations, reportez-vous à « *Protection Password Manager de vos identifiants* » (p. 153).

Bitdefender Safepay™ dispose des fonctions suivantes :

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

27.1. Utiliser Bitdefender Safepay™

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

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

- À partir de l'interface de Bitdefender :
  1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans le panneau **Safepay**, cliquez sur **Ouvrir 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.

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

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

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

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.

27.2. Configurer les paramètres

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

Liste des domaines

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

- Ouvrir automatiquement dans Bitdefender Safepay™.

- Faire en sorte que Bitdefender vous consulte pour l'action à chaque fois.
- Ne jamais utiliser Bitdefender Safepay™ lors de la consultation d'une page de ce domaine dans un navigateur standard.

Bloquer les 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.

Sélectionnez **Importez certificats** et suivez l'assistant pour utiliser des certificats dans Bitdefender Safepay™.

Lancer automatiquement le clavier virtuel dans les champs de saisie des mots de passe.

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

Utilisez le bouton correspondant pour activer ou désactiver la fonctionnalité.

Demander une confirmation avant d'imprimer

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

27.3. Gérer les marque-pages

Si vous avez désactivé la détection automatique de certains ou de tous les sites web, ou si Bitdefender ne détecte simplement pas certains sites web,

vous pouvez ajouter des marque-pages à Bitdefender Safepay™ afin de pouvoir lancer facilement vos sites web favoris à l'avenir.

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

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

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

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

27.4. Désactiver les notifications de Safepay

Le produit Bitdefender est configuré de sorte à vous avertir via une fenêtre pop-up lorsqu'un site de banque 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. Désactivez **Notifications Safepay**.

27.5. 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. Activez **Utilisez un VPN avec Safepay**.

28. PROTECTION DES DONNÉES

28.1. Supprimer définitivement des fichiers

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

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

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

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement.
2. Sélectionnez **Bitdefender** > **Destructeur de fichiers** dans le menu contextuel qui apparaît.
3. 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.
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 **Vie privée** 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 **AJOUT DE DOSSIERS** pour ajouter les fichiers ou dossiers que vous voulez 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. **Récapitulatif des résultats**

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

29. CONTRÔLE PARENTAL

La fonctionnalité Contrôle parental vous permet de contrôler l'accès à internet et à des applications spécifiques, pour chaque appareil sur lequel la fonctionnalité est installée. Une fois que vous avez configuré Contrôle parental, vous pouvez facilement savoir ce que votre enfant fait sur ses appareils et où il s'est rendu dans les dernières 24h. En outre, pour vous aider à mieux savoir ce que votre enfant fait, l'application vous donne des statistiques sur ses activtiés et ces intérêts.

Il vous suffit d'un ordinateur avec accès internet et d'un navigateur Web.

Vous pouvez configurer le Contrôle parental Bitdefender pour :

- Bloquer les pages Web inappropriées.
- Bloquer l'accès à Internet, pour des périodes bien définies (l'heure des devoirs, par exemple).
- Bloquer des applications comme les jeux, les logiciels de chat, les programmes de partage de fichiers et autres.
- Gérer les appels et les SMS depuis la liste des contacts. Cette fonctionnalité n'est disponible que sur Android.
- Bloquer les appels et SMS de certains contacts de la liste et de numéros inconnus.
- Définir des zones limitées.

Vérifiez les activités de vos enfants et modifiez les paramètres du Contrôle parental à l'aide de compte Bitdefender depuis tout ordinateur ou appareil mobile connecté à internet.

29.1. Allez dans Contrôle parental - Mes enfants

Une fois que vous êtes dans la rubrique Contrôle parental, la fenêtre **Mes enfants** est disponible. Ici vous pouvez voir et éditer tous les profils que vous avez créé pour vos enfants. Les profils sont affichés comme des cartes profils, vous permettant de les gérer et de vérifier leur état d'un coup d'oeil.

Une fois que vous avez créé un profil, vous pouvez commencer à personnaliser plus de paramètres détaillés, pour surveiller et contrôler l'accès à internet et à des applications spécifiques à vos enfants.

Vous pouvez accéder aux paramètres du Contrôle parental depuis Bitdefender Central sur tout ordinateur ou appareil mobile connecté à internet.

Accédez à votre compte Bitdefender.

- Sur tout appareil avec un accès à Internet :
  1. Accéder à Bitdefender Central.
  2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
  3. Sélectionnez le panneau **Contrôle parental**.
  4. Dans la fenêtre **Mes enfants** qui apparaît, vous pouvez gérer et configurer les profils du Contrôle parental pour chaque appareil.
- Depuis votre interface Bitdefender :
  1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
  2. Dans le panneau **CONTRÔLE PARENTAL**, cliquez sur **Configurer**.

     Vous êtes redirigé vers la page web compte Bitdefender. Assurez-vous que vous êtes connectés avec vos identifiants.
  3. Sélectionnez la fonctionnalité **Contrôle parental**.
  4. Dans la fenêtre **Mes enfants** qui apparaît, vous pouvez gérer et configurer les profils du Contrôle parental pour chaque appareil.

> **Note**
> Assurez-vous d'être connecté à l'ordinateur en utilisant un compte administrateur. Seuls les utilisateurs ayant des droits d'administrateur sur le système peuvent avoir accès et configurer le contrôle parental.

29.2. Ajouter le profil de votre enfant

Pour commencer à surveiller les activités de votre enfant, vous devez configurer un profil et installer une application Contrôle parental Bitdefender sur les appareils qu'il utilise.

Pour ajouter le profil de votre enfant au contrôle parental :

1. Accédez au panneau Contrôle parental depuis Bitdefender Central.
2. Cliquez sur **AJOUTER PROFIL** sur le côté droit de la fenêtre **Mes enfants**

3. Saisissez les informations demandées dans chaque champ, par exemple : nom et date de naissance. Pour ajouter une photo de profil, cliquez sur le lien **Choisir un fichier**. Cliquez sur **ÉTAPE SUIVANTE** pour continuer.

   Basée sur les standards de développement des enfants, la configuration de la date de naissance de l'enfant charge automatiquement les paramètres de recherche sur Internet considérés comme appropriés pour sa catégorie d'âge.

4. Si Bitdefender Internet Security est déjà installé sur l'appareil de votre enfant, sélectionnez le dans la liste puis sélectionnez le compte que vous souhaitez surveiller. Cliquez sur **Enregistrer**.

   Si votre enfant utilise un appareil Android ou iOS mais que l'application Contrôle parental Bitdefender n'est pas installée sur celui-ci, cliquez sur **AJOUTER UN APPAREIL**. Si votre enfant utilise un appareil Mac mais que l'application Antivirus for Mac Bitdefender n'est pas installée sur celui-ci, cliquez sur le même bouton. Sélectionnez le système d'exploitation sur lequel vous voulez installer l'application, puis cliquez sur **ÉTAPE SUIVANTE** pour continuer.

5. Saisissez l'adresse e-mail sur laquelle nous enverrons le lien de téléchargement du fichier d'installation de l'application Bitdefender, puis cliquez sur **ENVOYER UN LIEN D'INSTALLATION**.

> **Important**
> Sur les appareils Windows, le Bitdefender Internet Security que vous avez inclus dans votre abonnement doit être téléchargé et installé.
> Sur les appareils macOS, le produit Antivirus for Mac Bitdefender doit être téléchargé et installé.
> Sur les appareils Android et iOS, l'application Contrôle parental Bitdefender doit être téléchargée et installée.

29.2.1. Attribuer plusieurs appareils au même profil.

Vous pouvez attribuer plusieurs appareils au même profil pour que les mêmes restrictions soient appliquées à tous, comme suit :

1. Accéder à Bitdefender Central.
2. Sélectionnez le panneau Contrôle parental.
3. Cliquez sur l'icône ⋮ de la carte profil souhaitée, puis sélectionnez **Appareils**.

4. Sélectionnez dans la liste les appareils disponibles auxquels vous souhaitez assigner le profil.

   Si votre enfant utilise un appareil Android ou iOS mais que l'application Contrôle parental Bitdefender n'est pas installée sur celui-ci, cliquez sur **AJOUTER UN APPAREIL**. Si votre enfant utilise un appareil Mac mais que l'application Antivirus for Mac Bitdefender n'est pas installée sur celui-ci, cliquez sur le même bouton. Sélectionnez le système d'exploitation sur lequel vous voulez installer l'application, puis cliquez sur **ÉTAPE SUIVANTE** pour continuer.

   Saisissez l'adresse e-mail sur laquelle nous enverrons le lien de téléchargement du fichier d'installation de l'application Bitdefender, puis cliquez sur **ENVOYER UN LIEN D'INSTALLATION**.

5. Après avoir terminé le processus d'installation sur le nouvel appareil, sélectionnez-le dans la liste pour l'appliquer au profil.

6. Sélectionner **Enregistrer**.

Note
Si vous souhaitez bloquer temporairement l'accès de votre enfant aux appareils affectés, vous pouvez mettre son profil sur Pause. Pour cela, sélectionnez le profil désiré, puis cliquez sur ⏸ sur la photo de profil de votre enfant.

29.2.2. Lier le Contrôle Parental à Bitdefender Central

Pour surveiller l'activité en ligne de votre enfant sur Android et iOS, vous devez lier l'appareil de l'enfant à votre compte Bitdefender en vous connectant au compte à partir de l'application.

Pour lier un appareil à votre compte Bitdefender :

- Sous **Android** :

  1. Cliquez sur le bouton situé dans l'e-mail envoyé par notre serveur. Vous êtes redirigé vers Google Play Store.

     Si vous n'avez pas choisi dans votre compte Bitdefender d'envoyer un lien de téléchargement à l'adresse e-mail de votre enfant, allez dans Google Play et recherchez l'application Contrôle parental Bitdefender.

  2. Appuyez sur **INSTALLER** dans la fenêtre Contrôle parental Bitdefender, puis sur **ACCEPTER** si l'on vous demande d'approuver les permissions. Bitdefender a besoin de ces permissions pour vous informer des

activités de votre enfant. L'application ne fonctionnera pas si elles ne sont pas approuvées.

3. Ouvrez l'application Contrôle Parental.
4. Un assistant présentant les fonctions du produit s'affiche lors de la première ouverture de l'appli. Sélectionnez **SUIVANT** pour continuer à être guidé, ou **PASSER LA VISITE** pour fermer l'assistant.
5. Pour poursuivre la procédure d'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. Cochez la case correspondante puis cliquez sur **CONTINUER**.
6. Connectez-vous à votre compte déjà existant Bitdefender : Si vous n'avez pas de compte Bitdefender, vous pouvez en créer un en cliquant sur l'option correspondante. Vous pouvez aussi vous identifier par le biais d'un compte Facebook, Google ou Microsoft.
7. Appuyez sur **ACTIVER** pour être redirigé vers l'écran contenant l'option Accessibilité de l'application. Suivez les instructions à l'écran pour configurer correctement l'application.
8. Appuyez sur **AUTORISER** pour être redirigé vers la page contenant l'option Autoriser accès utilisation de l'application. Suivez les instructions à l'écran pour configurer correctement l'application.
9. Appuyez sur **ACTIVER** pour être redirigé vers l'écran contenant l'option Activer les droits administrateur de l'appareil pour l'application. Suivez les instructions à l'écran pour configurer correctement l'application.

   Cela empêchera votre enfant de désinstaller l'application Contrôle parental.
10. Appuyez sur **MODIFIER** pour utiliser l'application SMS du Contrôle parental au lieu de l'application par défaut, puis cliquez sur OK. Appuyé sur **PAS INTÉRESSÉ** pour continuer à utiliser l'application SMS par défaut et passer à l'étape suivante. Cette option apparait uniquement pour les versions 4.4 et supérieures d'Android.
11. Affectez l'appareil au profil de votre enfant.

- Sous **iOS** :

1. Cliquez sur le bouton qui apparaît dans l'e-mail envoyé par votre serveur, puis installez l'application.
2. Ouvrez l'application Contrôle Parental.
3. Pour poursuivre la procédure d'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 le Contrôle parental Bitdefender. Cochez la case correspondante puis cliquez sur **Continuer**.
4. Connectez-vous à votre compte déjà existant Bitdefender : Si vous n'avez pas de compte Bitdefender, vous pouvez en créer un en cliquant sur l'option correspondante. Vous pouvez aussi vous identifier par le biais d'un compte Facebook, Google ou Microsoft.
5. Un assistant de présentation des fonctionnalités du produit apparait. Appuyez sur **Suivant** pour continuer.
6. Il vous est demandé de donner accès à toutes les permissions requises par l'application. Appuyez sur **Autoriser**.
7. Autoriser l'accès à l'emplacement de l'appareil pour que Bitdefender puisse le localiser.
8. Autoriser l'application à envoyer des notifications.
9. Affectez l'appareil au profil de votre enfant.
10. La première fois que vous installez l'application Contrôle parental Bitdefender sur un appareil, vous devrez configurer un profil MDM (Mobile Device Management). Voici comment procéder :
    a. Appuyez sur **Autoriser** pour revenir sur l'écran Réglages.
    b. Appuyez sur **Autoriser** pour installer le profil MDM (Mobile Device Management) dont Bitdefender a besoin pour la suite de l'installation.

       Si un code PIN a été utilisé pour protéger votre smartphone, il vous sera demandé de le saisir.
    c. Lisez les informations concernant le certificat racine de l'AC et Mobile Device Management.
    d. Si vous acceptez les conditions présentées, appuyez sur **Installer**.

e. Appuyez sur **Faire confiance** dans la fenêtre d'alerte Gestion à distance, puis sur **Terminé** pour fermer la fenêtre.

Note
Si le message d'erreur **Échec de l'installation du profil**, vous devez supprimer le profil MDM actuellement installé, et le réinstaller. Pour supprimer le profil MDM actuel, rendez-vous dans Paramètres > Généraux > Gestion des appareils > Bitdefender. Sélectionnez le profil détecté, puis appuyez sur **Supprimer la gestion**. Si un code PIN a été utilisé pour protéger votre smartphone, il vous sera demandé de le saisir. Appuyez à nouveau sur **Supprimer la gestion** pour confirmer votre choix. Ouvrez l'application Contrôle parental Bitdefender, appuyez sur **Réinstaller**, et suivez les instructions. Si le problème persiste, vous pouvez envoyer un e-mail à notre équipe à l'adresse bdparental@bitdefender.com.

29.2.3. Surveiller les activités de l'enfant

Bitdefender vous aide à surveiller l'activité de vos enfants sur Internet.

Vous pouvez de cette façon toujours savoir exactement quels sites Web ils ont consultés, quelles applications ils ont utilisées et les activités bloquées par le Contrôle parental.

Selon les paramètres que vous souhaitez appliquer, les rapports peuvent contenir des informations détaillées pour chaque événement, comme :

- L'état de l'événement.
- La sévérité des notifications.
- Le nom de l'appareil.
- La date et l'heure auxquelles l'événement a eu lieu.

Pour surveiller le trafic Internet, les applications auxquelles a accédé votre enfant et ses activités en ligne :

1. Accédez au panneau Contrôle parental depuis Bitdefender Central.
2. Sélectionnez la carte appareil souhaitée.

   Dans la fenêtre **Activité** vous pouvez voir les informations qui vous intéressent. Autrement, sélectionnez le lien **Voir l'activité du jour** sur la carte de l'appareil surveillé pour être redirigé vers la fenêtre **Activité**.

29.2.4. Configurer les paramètres généraux

Lorsque le contrôle parental est activé, les activités de vos enfants sont enregistrées par défaut.

Pour recevoir des notifications par e-mail :

1. Accédez au panneau Contrôle parental depuis Bitdefender Central.
2. Sélectionnez l'onglet **Paramètres**.
3. Activez l'option correspondante pour recevoir les rapports d'activité.
4. Saisissez l'adresse e-mail pour recevoir les notifications par e-mail.
5. Recevez des notifications par courriel pour les éléments suivants :
   - Sites Web bloqués
   - Applications bloquées
   - Zones restreintes
   - Appel ou SMS reçu de numéros de téléphone bloqués/inconnus
6. Cliquez sur **Enregistrer**.

29.2.5. Modifier le profil

Pour modifier un profil existant :

1. Accéder à Bitdefender Central.
2. Sélectionnez le panneau **Contrôle parental**.
3. Cliquez sur l'icône ⋮ sur la carte profil souhaitée, puis sélectionnez **Éditer**.
4. Après avoir personnalisé les réglages, sélectionnez **SAUVEGARDER**.

29.2.6. Supprimer le profil

Pour modifier un profil existant :

1. Accéder à Bitdefender Central.
2. Sélectionnez le panneau **Contrôle parental**.
3. Cliquez sur l'icône ⋮ sur la carte profil souhaitée, puis sélectionnez **Supprimer**.

4. Confirmez votre choix.

29.3. Configurer les profils du Contrôle parental

Pour commencer à surveiller votre enfant, il vous faut assigner un profil à l'appareil sur lequel est installée l'application Contrôle parental Bitdefender.

Après avoir ajouté un profil à votre enfant, vous pouvez personnaliser des paramètres plus détaillés pour surveiller et contrôler l'accès à Internet et à des applications spécifiques.

Pour commencer à configurer un profil, sélectionnez le profil souhaité à partir de la fenêtre **Mes enfants**.

Cliquez sur un onglet pour configurer la fonction de Contrôle parental correspondante pour l'appareil :

- Activité - affiche toutes les activités, les intérêts, les lieux, et les interactions avec des amis pendant la journée.
- Applications - vous permet de bloquer l'accès à certaines applications, par exemple les jeux, les logiciels de messageries, les films, etc.
- Sites Web - vous permet d'appliquer des filtres à la navigation sur Internet.
- Contacts téléphone - vous pouvez ici indiquer quels sont les contacts autorisés à entrer en contact de votre enfant par téléphone parmi les contacts de celui-ci.
- Localisation de l'enfant - vous pouvez ici indiquer des lieux sûrs ou dangereux pour votre enfant.
- Temps passé devant l'écran - vous permet de bloquer l'accès des appareils que vous avez indiqués sur le profil de votre enfant.

29.3.1. Activité

La fenêtre Activité vous donne des informations détaillées sur les activités de votre enfant ces dernières 24 heures, à l'intérieur comme à l'extérieur du domicile. Pour voir les activités des jours précédents, cliquez sur l'icône calendrier dans le coin supérieur gauche de la fenêtre.

En fonction de l'activité, la fenêtre peut contenir des informations sur :

- **Lieux** - ici vous pouvez voir les endroits où votre enfant s'est rendu pendant la journée.

- **Intérêts** - ici vous pouvez voir des informations sur les catégories de sites web que votre enfant a visité. Cliquez sur le lien **Examiner le contenu inapproprié** pour autoriser ou refuser l'accès à des intérêts spécifiques.
- **Interactions sociales** - ici vous pouvez voir les contacts avec lesquels votre enfant communique. Cliquez sur le lien **Gérer contacts** pour sélectionner les contacts avec lesquels votre enfant peut communiquer ou non.
- **Applications** - ici vous pouvez voir les applications que votre enfant a utilisées. Cliquez sur le lien **Voir les restrictions d'applications** pour autoriser ou bloquer l'accès à certaines applications.
- **Activité de la journée** - ici vous pouvez voir le temps passé en ligne sur les appareils assignés à votre enfant, et les endroits où il a été actif. Les informations rassemblées sont celles de la journée en cours.

29.3.2. Applications

La fenêtre Applications vous permet de bloquer l'exécution de certaines applications sur les appareils Windows, macOS, Android et iOS. Les jeux, logiciels multimédias et services de messagerie, ainsi que d'autres catégories de logiciels peuvent être bloqués de cette manière.

Vous pourrez aussi y voir les applications les plus utilisées les 30 derniers jours ainsi que le temps passé sur chacune. Les informations relatives au temps passé sur les applications ne sont disponibles que sur les appareils Windows, macOS, et Android.

Pour configurer le contrôle des applications pour un compte utilisateur spécifique :

1. Une liste des appareils affectés apparaît.

   Sélectionnez la carte correspondant à l'appareil sur lequel vous voulez restreindre l'accès à des applications.

2. Cliquez sur **Gérer les applications utilisées par...**.

   Une liste des applications installées apparait.

3. Sélectionnez **Bloquée** à côté des applications que vous ne voulez plus que votre enfant utilise.

Vous pouvez arrêter de surveiller les applications installées en désactivant l'option **Surveiller les applications** dans le coin supérieur droit de la fenêtre.

29.3.3. Sites Web

La fenêtre Site Web vous permet de bloquer les sites Web au contenu inapproprié. Les sites web qui hébergent des vidéos, des jeux, des médias, et des logiciels de messagerie, ainsi que d'autres catégories de contenu négatif peuvent être bloqués de cette façon.

La fonctionnalité peut être activée ou désactivée à l'aide de l'interrupteur correspondant.

Selon l'âge que vous avez configuré pour votre enfant, la liste des Intérêts contient par défaut une sélection de catégories autorisées. Pour autoriser ou refuser l'accès à une catégorie spécifique, cliquez dessus.

Le symbole qui apparaît indique que votre enfant ne pourra pas accéder à du contenu lié à une catégorie spécifique.

Autoriser ou bloquer un site Web

Pour permettre ou restreindre l'accès à certaines pages web, vous devez les ajouter à la liste d'exceptions, comme suit :

1. Cliquez sur le bouton **GÉRER**.
2. Saisissez la page web que vous souhaitez bloquer ou autoriser dans le champ correspondant.
3. Sélectionnez **Autoriser** ou **Bloquer**.
4. Cliquez **FINISH** pour sauvegarder les changements.

> **Note**
> Les restrictions d'accès aux sites Internet ne peuvent être définies que pour les appareils Windows, Android et macOS ajoutés sur le profil de votre enfant.

29.3.4. Contacts téléphone

La fenêtre Contacts téléphone vous permet d'indiquer quels sont les contacts autorisés à entrer en contact de votre enfant par téléphone parmi les contacts de celui-ci.

Pour bloquer le numéro de téléphone d'un contact, vous devez d'abord ajouter l'appareil Android utilisé par votre enfant sur le profil de celui-ci, en procédant comme suit :

1. Sélectionnez l'onglet **Contrôle parental** dans Bitdefender Central.

2. Cliquez sur le lien **Installer le Contrôle parental sur un appareil** de la carte désirée.
3. Sélectionnez l'appareil Android que vous voulez affecter et cliquez sur **SAUVEGARDER**. Si l'appareil Android que vous voulez affecter au profil de votre enfant n'est pas dans la liste, suivez les instructions suivantes :
   a. Cliquez sur **AJOUTER UN APPAREIL**.
   b. Sélectionnez Android dans la liste, puis cliquez sur **ÉTAPE SUIVANTE** pour continuer.
   c. Saisissez l'adresse e-mail sur laquelle nous enverrons le lien de téléchargement du fichier d'installation de l'application Bitdefender, puis cliquez sur **ENVOYER UN LIEN D'INSTALLATION**.
   d. Installez l'application sur l'appareil désiré en suivant les instructions indiquées dans l'e-mail que vous avez reçu de notre part.
4. Sélectionnez l'onglet **Contacts téléphone** de Bitdefender Central.

   Une liste avec des cartes s'affiche. Les cartes représentent les contacts provenant du smartphone Android de votre enfant.
5. Sélectionnez la carte avec le numéro de téléphone que vous souhaitez bloquer.

   Le symbole qui apparaît indique que votre enfant ne pourra plus être contacté par ce numéro de téléphone.

   Les SMS seront bloqués uniquement si, lors de la configuration de l'application Contrôle parental Bitdefender sur l'appareil de votre enfant, vous avez choisir d'utiliser l'application SMS du Contrôle parental au lieu de l'application par défaut.

Les appels entrants et sortants depuis ou vers un numéro inconnu peuvent être bloqués en activant le bouton **Bloquer les appels des numéros privés inconnus sans identification de l'appelant**.

> **Note**
> Les restrictions d'appel ne peuvent être définies que pour les appareils Android ajoutés sur le profil de votre enfant, et s'appliquent aussi bien aux appels entrants que sortants.

29.3.5. Localisation

Afficher l'emplacement actuel de l'appareil sur Google Maps. Son emplacement est actualisé toutes les 5 secondes, afin que vous puissiez le suivre en cas de déplacement.

La précision de la localisation dépend de la façon dont Bitdefender est capable de la déterminer :

- Si le GPS est activé sur l'appareil, son emplacement peut être déterminé à quelques mètres près tant qu'il est à portée des satellites GPS (c'est-à-dire, à l'extérieur).
- Si l'appareil est à l'intérieur, il peut être localisé avec une précision d'une dizaine de mètres si le Wi-Fi est activé et si des réseaux sans fil sont à sa portée.
- Sinon, la localisation sera déterminée à l'aide des informations du réseau mobile, qui fournit une précision de pas plus de quelques centaines de mètres.

Configuration de la localisation et de la confirmation d'arrivée

Pour être certain que votre enfant se rend bien dans certains endroits, vous pouvez dresser une liste d'endroits sûrs ou non. Dès qu'il entre dans une zone prédéfinie, une notification apparait dans l'application Contrôle parental demandant de confirmer qu'il est en sécurité. En appuyant sur **JE SUIS BIEN ARRIVÉ** il vous avertit par une notification sur votre compte Bitdefender qu'il a bien atteint sa destination finale.

Si votre enfant n'envoie pas la confirmation, vous pouvez toujours consulter l'historique de ses déplacements de la journée depuis son profil sur votre compte Bitdefender.

Pour configurer un lieu :

1. Cliquez sur **Appareils** dans le cadre qui se trouve dans la fenêtre **Localisation de l'enfant**.
2. Cliquez sur **CHOISIR APPAREILS** puis sélectionnez l'appareil que vous souhaitez configurer.
3. Dans la fenêtre **Zones**, cliquez sur le bouton **AJOUTER ZONE**.
4. Choisissez le type de lieu, **Sécurisé** ou **Limité**.

5. Saisissez un nom valide pour la zone où vos enfants ont ou non la permission d'aller.
6. Configurez la portée qui devrait être appliquée pour la surveillance à partir du curseur **Rayon**.
7. Cliquez sur **AJOUTER ZONE** pour sauvegarder vos configurations. On vous demandera si votre enfant voyage ou non seul. Répondez par Oui ou par Non.

Note
La localisation peut être utilisée pour suivre les appareils Android et iOS sur lesquels est installée l'application Contrôle parental Bitdefender.

29.3.6. Temps devant l'écran

La section Temps passé devant l'écran vous informe du temps passé sur les appareils affectés pendant la journée, le temps restant par rapport à la limite définie, et le statut du profil sélectionné (actif ou en pause). Depuis cette fenêtre, vous pouvez également définir des restrictions pour différents moments de la journée, comme l'heure du coucher, des devoirs ou des cours particuliers.

Limites de temps

Pour commencer à configurer les limites de temps :

1. Cliquez sur **Voir les restrictions de temps**.
2. Dans la zone **Définir des limites de temps**, cliquez sur **Ajouter une nouvelle restriction**.
3. Donnez un nom à la restriction que vous souhaitez définir (par exemple sommeil, devoirs, cours de tennis, etc.).
4. Définissez la plage horaire à restreindre, puis cliquez sur **AJOUTER** pour enregistrer les réglages.

Pour modifier une limite existante, rendez-vous sur la fenêtre Temps passé devant l'écran, sélectionnez la limite que vous voulez modifier, et cliquez sur l'icône .

Pour supprimer une limite, rendez-vous sur la fenêtre Temps passé devant l'écran, sélectionnez la limite que vous voulez modifier, et cliquez sur l'icône .

Limite quotidienne

La limite d'utilisation quotidienne peut être appliquée aux appareils Android et Windows. Si vous choisissez de mettre en pause l'appareil une fois la limite atteinte, ce paramètre s'appliquera à tous les appareils affectés, qu'ils soient sur Windows, macOS, Android ou iOS.

Pour définir une limite quotidienne :

1. Cliquez sur **Voir les restrictions de temps**.
2. Dans la zone **Définir une limite quotidienne**, cliquez sur **Ajouter une nouvelle limite quotidienne**.
3. Définissez la plage horaire et les jours à restreindre, puis cliquez sur **SAUVEGARDER** pour enregistrer les réglages.

30. USB IMMUNIZER

La fonction AutoRun intégrée aux systèmes d'exploitation Windows est très utile car elle permet aux ordinateurs d'exécuter automatiquement un fichier depuis un support qui y est connecté. Par exemple, les installations de logiciels peuvent démarrer automatiquement lorsqu'un CD est inséré dans le lecteur optique.

Malheureusement, cette fonctionnalité peut également être utilisée par des menaces pour se lancer automatiquement et infiltrer votre ordinateur depuis des supports réinscriptibles tels que des lecteurs flash USB et des cartes mémoire connectés via des lecteurs de cartes. De nombreuses attaques exploitant la fonctionnalité AutoRun ont été créées ces dernières années.

Avec la protection USB, vous pouvez empêcher tout lecteur flash formaté en NTFS, FAT32 ou FAT d'exécuter des 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 ordinateur fonctionnant sous Windows.

Pour immuniser un appareil USB :

1. Connectez le lecteur flash à votre ordinateur.
2. Localisez sur votre ordinateur le périphérique de stockage amovible et faites un clic droit sur son icône.
3. Dans le menu contextuel, pointez sur **Bitdefender** et sélectionnez **Immuniser ce lecteur**.

> **Note**
> Si le lecteur a déjà été immunisé, le message **Le périphérique USB est protégé contre les menaces de type AutoRun** s'affichera au lieu de l'option Immuniser.

Pour empêcher que votre ordinateur 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. 132).

OPTIMISATION DU SYSTÈME

31. 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 pop-up de Bitdefender sont désactivées.
- La Mise à jour automatique est reportée.
- Les analyses planifiées sont reportées.
- Search Advisor 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 pop-up de Windows sont désactivées.
- Les programmes inutiles en arrière-plan sont interrompus.
- Les effets visuels sont ajustés pour de meilleures performances.
- Les tâches de maintenance sont reportées.

- Les paramètres du plan d'alimentation sont adaptés.

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

- Advanced Threat Defense est activé
- Le pare-feu Bitdefender est activé et les paramètres suivants sont appliqués à votre adaptateur sans fil :
  - Mode furtif - ON
  - Type de réseau - public
- Les paramètres suivants de la Prévention des menaces en ligne sont activés :
  - Analyse web chiffrée
  - Protection contre les escroqueries
  - Protection contre le phishing

31.1. 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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
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.

31.2. 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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.

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 en 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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
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.

31.3. 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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
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 en 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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
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.

31.4. Profil Wi-Fi public

Envoyer des e-mails, taper 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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
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**.

31.5. 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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone 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.
- Le Widget Windows est désactivé.

Bitdefender détecte le passage d'une alimentation secteur à une alimentation sur batterie et, en fonction du niveau de charge de la batterie, passe automatiquement en Mode Batterie. De la même manière, Bitdefender quitte automatiquement le Mode Batterie lorsqu'il détecte que l'ordinateur portable ne fonctionne plus sur batterie.

31.6. 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 **Paramètres** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Profils**.
3. Descendez jusqu'à voir l'option d'Optimisation en temps réel, puis utiliser le bouton Activer/Désactiver correspondant.

RÉSOLUTION DE PROBLÈMES

32. 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.

- « *Mon système semble lent* » (p. 198)
- « *L'analyse ne démarre pas* » (p. 200)
- « *Je ne peux plus utiliser une application* » (p. 202)
- « *Que faire lorsque Bitdefender bloque un site web ou une application sûre* » (p. 203)
- « *Que faire si Bitdefender détecte une appli fiable comme ransowmare* » (p. 204)
- « *Comment mettre à jour Bitdefender avec une connexion internet lente ?* » (p. 208)
- « *Le Services Bitdefender ne répondent pas* » (p. 209)
- « *Le filtre antispam ne fonctionne pas correctement* » (p. 210)
- « *La fonctionnalité saisie automatique de mon Wallet ne fonctionne pas* » (p. 215)
- « *La désinstallation de Bitdefender a échoué* » (p. 216)
- « *Mon système ne démarre pas après l'installation de Bitdefender* » (p. 217)

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du soutien technique Bitdefender comme indiqué dans le chapitre « *Assistance* » (p. 233).

32.1. 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. 83).

- **Vous ne disposez pas de la configuration système minimale pour l'exécution de Bitdefender.**

  Si votre machine ne dispose pas de la configuration système minimale, l'ordinateur deviendra lent, notamment lorsque plusieurs applications s'exécuteront simultanément. Pour plus d'informations, reportez-vous à « *Configuration système minimale* » (p. 3).

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

  Tous les ordinateurs ont des programmes ou des applications qui ne sont pas utilisés. Et de nombreux programmes indésirables s'exécutent en tâche de fond, utilisant de l'espace disque et de la mémoire. Si vous n'utilisez pas un programme, désinstallez-le. Cela s'applique également à tout autre logiciel préinstallé ou version d'évaluation d'une application que vous avez oublié de désinstaller.

  ! **Important**
  Si vous pensez qu'un programme ou qu'une application pourrait constituer un élément essentiel de votre système d'exploitation, ne les désinstallez pas et contactez le Service Client de Bitdefender pour obtenir de l'aide.

- **Votre système peut être infecté**.

  La vitesse de votre système et son comportement général peuvent également être affectés par des logiciels malveillants. Les logiciels espions, les malwares, les chevaux de Troie et les publiciels nuisent tous aux performances de votre ordinateur. Veillez à analyser votre système régulièrement, au moins une fois par semaine. Il est recommandé d'utiliser l'Analyse du système Bitdefender car elle recherche tous les types de logiciels malveillants menaçant la sécurité de votre système.

  Pour commencer l'Analyse système :

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

2. Dans le panneau **ANTIVIRUS**, cliquez sur **Analyse système**.
3. Suivez les étapes de l'assistant.

32.2. 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 Internet Security** 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 Internet Security** 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 Internet Security** 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. 83).
  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 Internet Security** 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 Internet Security** 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 Internet Security** 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. 233).

32.3. 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 **ADVANCED THREAT DEFENSE**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Exceptions**, cliquez sur **Ajouter des applications aux exceptions**.
4. Sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 233).

32.4. Que faire lorsque Bitdefender bloque un site web ou une application sûre

Bitdefender permet de naviguer sur Internet en toute sécurité en filtrant l'ensemble du trafic web et en bloquant tout contenu malveillant. Il est toutefois possible que Bitdefender considère à tort qu'un site web ou une application en ligne n'est pas sûr, et que l'analyse du trafic HTTP de Bitdefender les bloque par erreur.

Si une page ou une application est bloquée de façon répétée, elle peut être ajoutée à une liste 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 **Exceptions**.
3. Indiquez l'adresse du site Web ou d'une application en ligne bloquée dans le champ correspondant et cliquez sur **AJOUTER**.

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

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

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 233).

32.5. Que faire si Bitdefender détecte une appli fiable comme ransowmare

Le ransomware est un programme malveillant qui essaye de soutirer de l'argent aux utilisateurs en fermant leur système vulnérable. Pour protéger votre système des situations dangereuses, Bitdefender vous donne la possibilité d'indemniser des fichiers personnels.

Lorsqu'une application tente de modifier ou de supprimer un de vos fichiers protégés, elle sera considérée comme dangereuse et Bitdefender bloquera ses fonctionnalités.

Dans le cas où une telle demande est ajoutée à la liste des applications non fiables et vous êtes sûr qu'il est sûr de l'utiliser, procédez comme suit :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **SAFE FILES**, cliquez sur **Accès de l'application**.
3. Les applications qui essayent de modifier les fichiers de vos dossiers protégés sont présentées sous forme de liste. Cliquez sur le bouton **Autoriser** situé à côté de l'application dont vous êtes certain qu'elle est fiable.

32.6. Je ne peux pas me connecter à Internet

Vous remarquerez peut-être qu'un programme ou un navigateur Web ne peut plus se connecter à Internet ou accéder aux services réseau après avoir installé Bitdefender.

Dans ce cas, la meilleure solution est de configurer Bitdefender afin qu'il autorise automatiquement les connexions de et vers l'application logicielle en question :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PARE-FEU**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Règles**, cliquez sur **Ajouter une règle**.
4. Une nouvelle fenêtre apparaît dans laquelle vous pouvez ajouter les informations. Veillez à sélectionner tous les types de réseau disponibles et sélectionnez **Autoriser** dans la section **Permission**.

Fermez Bitdefender, ouvrez l'application logicielle et réessayez de vous connecter à Internet.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 233).

32.7. Je ne peux pas accéder à un périphérique de mon réseau

En fonction du réseau auquel vous êtes connecté, le pare-feu Bitdefender peut bloquer la connexion entre votre système et un autre périphérique (tel qu'un ordinateur ou une imprimante). Vous ne pouvez donc plus partager ou imprimer des fichiers.

Dans ce cas, la meilleure solution est de configurer Bitdefender afin qu'il autorise automatiquement les connexions de et vers le périphérique en question, comme suit :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PARE-FEU**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Règles**, cliquez sur **Ajouter une règle**.
4. Dans la fenêtre **Paramètres**, activez l'option **Appliquer cette règle à toutes les applications**.
5. Cliquez sur l'onglet **Avancé**.
6. Dans la case **Adresse à distance personnalisée** saisissez l'adresse IP de l'ordinateur ou de l'imprimante auquel vous voulez avoir un accès non restreint.

Si vous ne pouvez toujours pas vous connecter au périphérique, le problème n'est peut-être pas causé par Bitdefender.

Vérifiez d'autres causes possibles, telles que les suivantes :

- Le pare-feu de l'autre ordinateur peut bloquer le partage de fichiers et d'imprimantes avec celui-ci.
  - Si le pare-feu Windows est utilisé, il peut être configuré pour autoriser le partage de fichiers et d'imprimantes comme suit :
    - Dans **Windows 7** :
      1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et sélectionnez **Système et sécurité**.
      2. Allez dans **Pare-feu Windows** puis cliquez sur **Autoriser un programme via le Pare-feu Windows**.
      3. Cochez la case **Partage de fichiers et d'imprimantes**.
    - 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 **Système et sécurité**, allez dans **Pare-feu Windows** et sélectionnez **Autoriser une application via le pare-feu Windows**.
      3. Cochez la case **Partage de fichiers et d'imprimantes** puis cliquez sur **OK**.
    - Dans **Windows 10** :
      1. Tapez "Autoriser un programme via le Pare-feu Windows" dans le champ de recherche de la barre des tâches et cliquez sur son icône.
      2. Cliquez sur **Changer les paramètres**.
      3. Cochez la case **Partage de fichiers et d'imprimantes** dans la liste **Applications autorisées** puis cliquez sur **OK**.
  - Si un autre programme pare-feu est utilisé, veuillez vous reporter à sa documentation ou au fichier d'aide.
- Conditions générales pouvant empêcher d'utiliser ou de se connecter à une imprimante partagée :
  - Il se peut que vous ayez besoin de vous connecter à un compte Windows administrateur pour avoir accès à l'imprimante partagée.

- L'imprimante partagée est configurée pour autoriser l'accès uniquement à certains ordinateurs et utilisateurs. Si vous partagez votre imprimante, vérifiez que l'imprimante autorise l'accès à l'utilisateur de l'autre ordinateur. Si vous essayez de vous connecter à une imprimante partagée, vérifiez avec l'utilisateur de l'autre ordinateur que vous êtes autorisé(e) à vous connecter à l'imprimante.
- L'imprimante connectée à votre ordinateur ou à l'autre ordinateur n'est pas partagée.
- L'imprimante partagée n'a pas été ajoutée à l'ordinateur.

> **Note**
> Pour apprendre à gérer le partage d'imprimante (partager une imprimante, définir ou supprimer des permissions pour une imprimante, se connecter à l'imprimante d'un réseau ou à une imprimante partagée) consultez le Centre d'aide et de support de Windows (dans le menu Démarrer, cliquez sur **Aide et Support**).

- L'accès à une imprimante réseau peut être limité à des ordinateurs et des utilisateurs spécifiques uniquement. Consultez l'administrateur réseau pour savoir si vous avez l'autorisation de vous connecter à cette imprimante.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 233).

32.8. Ma connexion Internet est lente

Cette situation peut se produire après l'installation de Bitdefender. Le problème pourrait être causé par des erreurs dans la configuration du pare-feu de Bitdefender.

Pour régler ce problème :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **PARE-FEU**, placez le bouton en position Désactiver pour désactiver la fonctionnalité.
3. Vérifiez si votre connexion Internet s'est améliorée avec le pare-feu Bitdefender désactivé.

- Si votre connexion à Internet est toujours lente, le problème n'est peut-être pas causé par Bitdefender. Nous vous recommandons de contacter votre fournisseur d'accès à Internet afin de vérifier si la connexion est opérationnelle de son côté.

  Si vous recevez la confirmation de votre fournisseur d'accès à Internet que la connexion est opérationnelle de leur côté et que le problème persiste, contactez Bitdefender comme cela est décrit dans la section « *Assistance* » (p. 233).

- Si la connexion internet s'est améliorée après la désactivation du pare-feu Bitdefender :

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

  b. Dans le panneau **PARE-FEU**, cliquez sur **Paramètres**.

  c. Rendez-vous dans l'onglet **Adaptateurs réseau** et réglez votre connexion à Internet sur **Domicile / Bureau**.

  d. Dans l'onglet **Paramètres**, désactivez la **Protection lors de l'analyse des ports**.

     Dans la zone **Mode furtif**, cliquez sur **Éditer les réglages de furtivité**. Activez le mode furtif pour l'adaptateur réseau auquel vous êtes connecté.

  e. Fermez Bitdefender, redémarrez le système et vérifiez la vitesse de la connexion à Internet.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 233).

32.9. 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.

32.10. Le Services Bitdefender ne répondent pas

Cet article vous aide à régler l'erreur **Les Services Bitdefender ne répondent pas**. Vous pouvez rencontrer cette erreur de la façon suivante :

- L'icône Bitdefender de la zone de notification est grisée et vous informe que les services Bitdefender ne répondent pas.
- La fenêtre Bitdefender indique que les services Bitdefender ne répondent pas.

L'erreur peut être causée par :

- erreurs de communication temporaires entre les services Bitdefender.
- certains services Bitdefender sont interrompus.
- d'autres solutions de sécurité sont en cours d'exécution sur votre ordinateur en même temps que Bitdefender.

Pour régler cette erreur, essayez ces solutions :

1. Attendez quelques instants et voyez si quelque chose change. L'erreur peut être temporaire.
2. Redémarrez l'ordinateur et attendez quelques instants jusqu'à ce que Bitdefender soit chargé. Ouvrez Bitdefender pour voir si l'erreur persiste. Redémarrer l'ordinateur règle habituellement le problème.
3. Vérifiez que vous n'avez pas d'autre solution de sécurité installée car cela pourrait affecter le fonctionnement normal de Bitdefender. Si c'est le cas, nous vous recommandons de supprimer toutes les autres solutions de sécurité et de réinstaller ensuite Bitdefender.

   Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 83).

Si l'erreur persiste, veuillez contacter les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la section « *Assistance* » (p. 233).

32.11. Le filtre antispam ne fonctionne pas correctement

Cet article aide à régler les problèmes suivants avec le filtrage Antispam Bitdefender :

- Certains e-mails légitimes sont signalés comme étant du [spam].
- De nombreux messages de spam ne sont pas signalés comme tels par le filtre antispam.
- Le filtre antispam ne détecte aucun message de spam.

32.11.1. Des messages légitimes sont signalés comme étant du [spam]

Des messages légitimes sont signalés comme étant du [spam] car ils ressemblent à du spam pour le filtre antispam de Bitdefender. Vous pouvez normalement régler ce problème en configurant le filtre Antispam de façon adaptée.

Bitdefender ajoute automatiquement les destinataires de vos e-mails à une Liste d'Amis. Les e-mails que vous recevez des contacts de la Liste d'Amis sont considérés comme légitimes. Ils ne sont pas vérifiés par le filtre antispam et ne sont donc jamais signalés comme étant du [spam].

La configuration automatique de la liste d'Amis n'empêche pas les erreurs de détection pouvant se produire dans les situations suivantes :

- Vous recevez de nombreux e-mails commerciaux sollicités après vous être inscrit(e) sur plusieurs sites Internet. Dans ce cas, la solution est de ne pas ajouter les adresses e-mail des expéditeurs de ces messages à la liste d'Amis.
- Une part importante des e-mails légitimes que vous recevez provient de personnes auxquelles vous n'avez jamais envoyé d'e-mail auparavant, telles que des clients, des partenaires commerciaux potentiels etc. D'autres solutions sont requises dans ce cas.

Si vous utilisez l'un des clients de messagerie dans lesquels Bitdefender s'intègre, indiquez les erreurs de détection.

> **Note**
> Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 116).

Ajouter des contacts à la Liste d'amis

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement ajouter les expéditeurs d'e-mails légitimes à la liste d'Amis. Suivez ces étapes :

1. Dans votre client de messagerie, sélectionnez un e-mail provenant de l'expéditeur que vous voulez ajouter à la liste d'Amis.
2. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender.
3. Il se peut qu'on vous demande de valider les adresses ajoutées à la liste d'Amis. Sélectionnez **Ne plus afficher ce message** et cliquez sur **OK**.

Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.

Si vous utilisez un client de messagerie différent, vous pouvez ajouter des contacts à la liste d'Amis à partir de l'interface de Bitdefender. Suivez ces étapes :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTISPAM**, cliquez sur **Gérer les amis**.

   Une fenêtre de configuration s'affichera.
3. Tapez l'adresse e-mail dont vous souhaitez toujours recevoir les messages puis cliquez sur **AJOUTER**. Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
4. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Indiquer des erreurs de détection

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement corriger le filtre antispam (en indiquant quels e-mails n'auraient pas dû être signalés comme étant du [spam]). Cela contribue à améliorer considérablement l'efficacité du filtrage antispam. Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez le message légitime considéré à tort comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender pour ajouter l'expéditeur à la liste d'Amis. Il se peut que vous ayez besoin de cliquer sur **OK** pour valider. Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.
5. Cliquez sur le bouton **Pas Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Le message d'e-mail sera placé dans la boîte de réception.

32.11.2. De nombreux messages de spam ne sont pas détectés

Si vous recevez de nombreux messages de spam qui ne sont pas signalés comme étant du [spam], vous devez configurer le filtre antispam de Bitdefender pour améliorer son efficacité.

Essayez les solutions suivantes :

1. Si vous utilisez l'un des clients de messagerie dans lesquels Bitdefender s'intègre, indiquez les messages de spam non détectés.

> **Note**
>
> Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 116).

2. Ajouter des spammeurs à la liste des Spammeurs Les messages provenant d'adresses qui figurent dans la liste de Spammeurs seront automatiquement considérés comme étant du [spam].

Indiquer les messages de spam non détectés

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement indiquer quels e-mails auraient dû être détectés comme étant du spam. Cela contribue à améliorer considérablement l'efficacité du filtrage antispam. Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans la boîte de Réception.
3. Sélectionnez les messages de spam non détectés.
4. Cliquez sur le bouton **Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Ils sont immédiatement signalés comme étant du [spam] et déplacés vers le dossier du courrier indésirable.

Ajouter des spammeurs à la Liste des Spammeurs

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement ajouter les expéditeurs de spam à la liste de Spammeurs. Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez les messages signalés comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter Spammeur** de la barre d'outils antispam Bitdefender.
5. Il se peut qu'on vous demande de valider les adresses ajoutées à la liste de Spammeurs. Sélectionnez **Ne plus afficher ce message** et cliquez sur **OK**.

Si vous utilisez un autre client de messagerie, vous pouvez ajouter manuellement des spammeurs à la liste des Spammeurs à partir de l'interface de Bitdefender. Cela s'avère utile lorsque vous avez reçu plusieurs e-mails de spam provenant de la même adresse e-mail. Suivez ces étapes :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTISPAM**, cliquez sur **Gérer les spammers**.

   Une fenêtre de configuration s'affichera.
3. Tapez l'adresse e-mail du spammeur puis cliquez sur **AJOUTER**. Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
4. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

32.11.3. Le filtre antispam ne détecte aucun message de spam.

Si aucun message de spam n'est signalé comme étant du [spam], il se peut qu'il y ait un problème avec le filtre Antispam de Bitdefender. Avant d'essayer de régler ce problème, assurez-vous qu'il n'est pas causé par l'une des situations suivantes :

- La protection antispam pourrait être désactivée. Pour vérifier l'état de la protection antispam, cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender. Consultez le panneau **Antispam** pour vérifier que la fonctionnalité est activée.

  Si l'Antispam est désactivé, il s'agit de la cause de votre problème. Cliquez sur le bouton correspondant pour activer votre protection antispam.
- La protection Bitdefender Antispam est disponible seulement pour les clients de messagerie configurés pour recevoir des e-mails via le protocole POP3. Cela signifie que :
  - Les e-mails reçus via des services de webmail (tels que Yahoo, Gmail, Hotmail ou d'autres) ne font pas l'objet d'une analyse antispam de la part de Bitdefender.
  - Si votre client de messagerie est configuré pour recevoir des e-mails en utilisant un protocole autre que POP3 (par exemple IMAP4), vos e-mails ne seront pas analysés par Bitdefender Antispam.

  Note

  POP3 est l'un des protocoles les plus utilisés pour télécharger des e-mails à partir d'un serveur de messagerie. Si vous ne connaissez pas le protocole que votre client de messagerie utilise pour télécharger des e-mails, posez la question à la personne ayant configuré votre client de messagerie.

- Bitdefender Internet Security n'analyse pas le trafic POP3 de Lotus Notes.

Une solution possible consiste à réparer ou à réinstaller le produit. Il est toutefois recommandé de contacter Bitdefender pour obtenir de l'assistance, comme cela est décrit dans la section « *Assistance* » (p. 233).

32.12. La fonctionnalité saisie automatique de mon Wallet ne fonctionne pas

Vous avez enregistré vos identifiants en ligne dans votre Bitdefender le Gestionnaire de mots de passe 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 Outils.
  3. Cliquez sur Modules.
  4. Cliquez sur Extensions.
  5. Pointez sur **Bitdefender Wallet** et cliquez sur **Permettre**.
- 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. Pointez sur **Bitdefender Wallet** et cliquez sur **Permettre**.

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

Vérifiez maintenant que la fonctionnalité de saisie automatique de 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. 233).

32.13. 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 Internet Security** 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 Internet Security** 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 Internet Security** 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.

32.14. 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. 84).
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 Internet Security** 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 Internet Security** 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 Internet Security** 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. 84).
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. 84).
2. Utilisez l'option Restauration du système de Windows pour restaurer l'ordinateur à une date antérieure à l'installation du produit Bitdefender.
3. Redémarrez le système en mode normal et contactez les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la section « *Assistance* » (p. 233).

33. 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.

- « *Mode de Secours Bitdefender (Environnement de récupération sur Windows 10)* » (p. 221)
- « *Que faire lorsque Bitdefender détecte des menaces sur votre ordinateur ?* » (p. 225)
- « *Comment nettoyer un menace dans une archive ?* » (p. 227)
- « *Comment nettoyer une menace dans une archive de messagerie ?* » (p. 228)
- « *Que faire si je suspecte un fichier d'être dangereux ?* » (p. 229)
- « *Que sont les fichiers protégés par mot de passe du journal d'analyse ?* » (p. 230)
- « *Que sont les éléments ignorés du journal d'analyse ?* » (p. 230)
- « *Que sont les fichiers ultra-compressés du journal d'analyse ?* » (p. 230)
- « *Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?* » (p. 231)

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du soutien technique Bitdefender comme indiqué dans le chapitre « *Assistance* » (p. 233).

33.1. Mode de Secours Bitdefender (Environnement de récupération sur Windows 10)

Le **Mode de secours** est une fonctionnalité de Bitdefender qui vous permet d'analyser et de désinfecter toutes les partitions de disques durs gérées ou non par votre système d'exploitation.

Une fois Bitdefender Internet Security installé sur **Windows 7, Windows 8 ou Windows 8.1** et le fichier Mode de secours de Bitdefender téléchargé, le

Mode de secours peut être utilisé même si vous ne pouvez plus démarrer Windows.

Sous Windows 10, l'Environnement de secours de Bitdefender est intégré à Windows RE, ce qui signifie qu'il n'est pas nécessaire de télécharger une image du Mode de secours sur ce système d'exploitation et que la fonctionnalité ne peut pas être utilisées en cas de problème au démarrage. Pour nettoyer le système avant que les services de Windows ne soient chargés, nous recommandons d'utiliser le CD de secours Bitdefender.

Le CD de secours Bitdefender est un outil gratuit qui analyse et nettoie votre ordinateur lorsque vous suspectez qu'une menace en gêne le fonctionnement. Des articles utiles contenant des informations détaillées sur la manière de le créer et de l'utiliser sont disponibles sur la plateforme du centre de support Bitdefender : https://www.bitdefender.fr/support/consumer/.

Téléchargement de l'image du Mode de secours de Bitdefender

Pour pouvoir utiliser le Mode de secours sur **Windows 7, Windows 8 et Windows 8. 1** , vous devez d'abord télécharger son fichier image comme suit :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Mode de secours**.
3. Cliquez sur **Oui** dans la fenêtre de confirmation pour redémarrer votre ordinateur.

   Attendez que l'image du Mode de secours de Bitdefender se télécharge depuis les serveurs de Bitdefender. Votre ordinateur redémarre dès la fin du téléchargement.

   Un menu apparaît vous demandant de sélectionner un système d'exploitation. Lors de cette étape, vous pouvez choisir de démarrer votre système en Mode de secours ou en mode normal.

Note

Compte tenu de son intégration avec l'Environnement de secours Windows de **Windows 10** , il n'est pas nécessaire de télécharger une image du Mode de secours sur ce système d'exploitation.

Démarrer son système sur le Mode de secours sur Windows 7, Windows 8 et Windows 8. 1

Vous pouvez entrer en mode de secours de l'une des deux façons suivantes :

À partir de l'interface de Bitdefender

1. Cliquez sur **Protection** dans le menu de navigation de l'interface de Bitdefender.
2. Dans le panneau **ANTIVIRUS**, cliquez sur **Mode de secours**.
3. Cliquez sur **Oui** dans la fenêtre de confirmation pour redémarrer votre ordinateur.
4. Après le redémarrage de l'ordinateur, un menu apparaîtra vous demandant de sélectionner un système d'exploitation. Sélectionnez **Mode de secours de Bitdefender** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.
5. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.

   Le Mode de secours de Bitdefender se chargera dans quelques instants.

Démarrez votre ordinateur directement en mode de secours

Si Windows ne démarre plus, vous pouvez démarrer directement votre ordinateur en Mode de secours de Bitdefender en suivant les étapes ci-dessous:

- Dans **Windows 7** :
  1. Appuyez sur la touche **F8** jusqu'à ce que l'écran des **Options de démarrage avancées** apparaisse.
  2. Utilisez les flèches pour sélectionner le Mode de secours de Bitdefender, puis appuyez sur **Entrée** .

     Le Mode de secours de Bitdefender se chargera dans quelques instants.
- Dans **Windows 8 et Windows 8.1** :
  1. Appuyez sur la touche **Shift** jusqu'à ce que l'écran des **Options de démarrage avancées** apparaisse.

2. Sélectionnez l'option **Utiliser un autre système d'exploitation**, puis Mode de secours de Bitdefender.

   Le Mode de secours de Bitdefender se chargera dans quelques instants.

> **Note**
> Il n'est possible de démarrer votre ordinateur en Mode de secours que si vous avez téléchargé l'image du Mode de secours, comme expliqué dans « Téléchargement de l'image du Mode de secours de Bitdefender » (p. 222).

Démarrer son système sur l'Environnement de secours de Windows 10

Vous pouvez uniquement passer sur l'Environnement de secours 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 **Environnement de secours**.
3. Cliquez sur **Redémarrer** dans la fenêtre qui s'affiche.

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

Analyser son système depuis le Mode de secours (Environnement de secours de Windows 10)

Pour analyser votre système en Mode de Secours (Environnement de secours) :

- Dans **Windows 7, Windows 8 et Windows 8.1** :
  1. Entrez en mode de secours, comme indiqué dans « Démarrer son système sur le Mode de secours sur Windows 7, Windows 8 et Windows 8. 1 » (p. 223).
  2. Le logo de la Bitdefender apparaîtra et les moteurs de la solution de sécurité commenceront à être copiés.
  3. Une fenêtre d'accueil apparaîtra. Cliquez sur **Continuer**.

4. Une mise à jour de la base de données d'information sur les menaces a démarré.
5. Une fois la mise à jour terminée, la fenêtre du Scanner Antivirus à la demande Bitdefender s'affiche.
6. Cliquez sur **Analyser**, sélectionnez la cible de l'analyse dans la fenêtre qui s'affiche puis cliquez sur **Ouvrir** pour lancer l'analyse.

   Nous vous recommandons l'analyse de la totalité de votre partition Windows.

   > **Note**
   > En mode de secours, les noms de partitions sont de type Linux. Des partitions de disque apparaîtront, sda1 correspondant probablement à la partition de type Windows (C:), sda2 correspondant à (D:), etc.

7. Patientez jusqu'à la fin de l'analyse. Si une menace est détectée, suivez les instructions pour la supprimer.
8. Pour quitter le mode de secours, faites un clic droit sur une zone vide du bureau, sélectionnez **Quitter** dans le menu qui apparaît puis choisissez de redémarrer ou d'éteindre l'ordinateur.

- Dans **Windows 10** :

1. Entrez dans l'Environnement de secours, comme indiqué dans « Démarrer son système sur l'Environnement de secours de Windows 10 » (p. 224).
2. Le processus d'analyse de Bitdefender commence automatiquement quand le système charge l'Environnement de secours.
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** de la fenêtre contenant les résultats de l'analyse.

33.2. Que faire lorsque Bitdefender détecte des menaces sur votre ordinateur ?

Il est possible que vous découvriez qu'une menace se trouve sur votre ordinateur de l'une des manières suivantes :

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

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 **Paramètres**.
   c. Dans la fenêtre **Protection**, désactivez **Protection - Bitdefender**.
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 82).
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. 84).

2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 82).
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. 233).

33.3. 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 **Paramètres**.
   c. Dans la fenêtre **Protection**, désactivez **Protection - 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. 233).

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

Bitdefender permet également de repérer les menaces dans les bases de données d'e-mails et les archives d'e-mails stockées sur le disque.

Il est parfois nécessaire d'identifier le message infecté à l'aide des informations du rapport d'analyse, et de le supprimer manuellement.

Voici comment nettoyer 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 **Paramètres**.
   c. Dans la fenêtre **Protection**, désactivez **Protection - 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. 233).

33.5. Que faire si je suspecte un fichier d'être dangereux ?

Vous pouvez suspecter qu'un fichier de votre système est dangereux, même si votre produit Bitdefender ne l'a pas détecté.

Pour 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. 60).
2. Si le résultat de l'analyse n'indique pas d'infection, mais que vous avez encore des doutes et souhaitez vérifier le fichier, contactez les représentants de notre soutien technique afin que nous puissions vous aider.

   Pour savoir comment faire cela, consultez « *Assistance* » (p. 233).

33.6. Que sont les fichiers protégés par mot de passe du journal d'analyse ?

Il ne s'agit que d'une notification qui indique que Bitdefender a détecté que ces fichiers sont soit protégés par un mot de passe soit par une forme de chiffrement .

Les éléments protégés par un mot de passe sont généralement :

- Fichiers appartenant à une autre solution de sécurité.
- Fichiers appartenant au système d'exploitation.

Afin que le contenu soit analysé, ces fichiers auront besoin d'être extraits ou déchiffrés.

Si ce contenu était extrait, le moteur d'analyse en temps réel de Bitdefender l'analyserait automatiquement pour que votre ordinateur reste protégé. Si vous souhaitez analyser ces fichiers avec Bitdefender, vous devez contacter le fabricant du produit afin d'obtenir plus d'informations sur ces fichiers.

Nous vous recommandons d'ignorer ces fichiers car ils ne constituent pas une menace pour votre système.

33.7. 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.

33.8. Que sont les fichiers ultra-compressés du journal d'analyse ?

Les éléments ultra-compressés sont des éléments qui n'ont pas pu être extraits par le moteur d'analyse ou des éléments dont le temps de déchiffrement aurait été trop long et aurait rendu le système instable.

Surcompressé signifie que Bitdefender a ignoré l'analyse dans cette archive car sa décompression consommait trop de ressources système. Le contenu sera analysé à l'accès en temps réel si nécessaire.

33.9. 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

34. 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. 198) 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 Internet Security » (p. 233)
- « Contactez-nous via notre Centre de Support en ligne » (p. 234)

Contactez-nous directement depuis Bitdefender Internet Security

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 **Support** dans le menu de navigation de l'interface de Bitdefender.
2. Vous disposez des options suivantes :
   - **GUIDE D'UTILISATION**

     Accédez à notre base de données et recherchez les informations nécessaires.
   - **CENTRE DE SUPPORT**

     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.

34.1. 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 https://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.

35. 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.

35.1. 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/.

35.2. 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 certaines menaces de votre ordinateur ou si vous avez des questions sur son mode de fonctionnement, exposez votre problème ou posez vos questions sur le forum.

Les techniciens du support Bitdefender surveillent le forum à la recherche de nouvelles publications afin de vous aider. Vous pouvez également obtenir une réponse ou une solution d'un utilisateur Bitdefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de Bitdefender est disponible à 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.

35.3. Portail Bitdefender blog

Bitdefender blog comprend de nombreuses informations sur la sécurité informatique. Vous pouvez découvrir ici les différentes menaces auxquelles votre ordinateur est exposé lorsqu'il est connecté à internet (malwares, phishing, spam, cybercriminels).

De nouveaux articles sont régulièrement publiés pour vous tenir au courant des dernières menaces découvertes, des tendances actuelles en matière de sécurité et vous fournir encore d'autres informations sur le secteur de la sécurité informatique.

La page web de Bitdefender blog est https://www.bitdefender.fr/blog/.

36. CONTACT

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.

36.1. 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 Web : https://www.bitdefender.fr

36.2. 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.

36.3. 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 Web : https://www.bitdefender.es

Roumanie

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 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 Web : 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 Web : 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 Advanced persistent threat (APT) exploitent les vulnérabilités des systèmes pour voler des informations importantes et les livrer à la source. Les grands groupes tels que les entreprises, les sociétés ou les gouvernements sont ciblés par cette menace.

L'objectif d'une Advanced persistent threat est de passer inaperçue pendant le plus de temps possible, tout en surveillant et regroupant des informations importantes sans endommager les machines ciblées. La méthode utilisée pour injecter 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.

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.

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.

Cookie

Sur internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (le code barres se trouvant au dos des produits). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Dossier de démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage de l'ordinateur. Par exemple, un écran de démarrage, un fichier son pour le démarrage de l'ordinateur, un calendrier, des programmes, peuvent être placés dans ce dossier. C'est généralement un raccourci vers le fichier qui est placé dans le dossier, et pas le fichier.

E-mail

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Enregistreur de frappe

Un keylogger est une application qui enregistre tout ce qui est tapé.

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.

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.

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.

Honeypot

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.

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 hardware, destinée à remplacer une version antérieure du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, et si ce n'est pas le cas, la mise à jour ne se fait pas.

Bitdefender a 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 modules d'extension (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 e-mail 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 de l'e-mail. Cet e-mail 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.

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 collectées peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des termes de l'accord de licence.

Ransomwares

Le ransomware est un programme malveillant qui essaye de soutirer de l'argent aux utilisateurs en fermant leur système vulnérable. CryptoLocker, CryptoWall, et TeslaWall n'en sont que des variantes qui recherchent les systèmes personnels des utilisateurs.

L'infection peut se répandre via e-mail, le téléchargement de pièces jointes, ou l'installation d'applications, sans prévenir l'utilisateur de ce qui se passe dans son système. Les utilisateurs quotidiens et les entreprises sont ciblées par les pirates ransomwares.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant un accès de niveau administrateur à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs système.

Le principal rôle des rootkits est de masquer des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des menaces ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des menaces, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des logs et passer inaperçus.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur de boot :

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur 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 emails 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 spywares peuvent également récupérer des informations sur les adresses mail, 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 standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Télécharger

Copie des données (généralement un fichier entier) d'une source principale vers un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. 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.

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.

Virtual Private Network (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.

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.