GUIDE DE L'UTILISATEUR

Bitdefender CONSUMER SOLUTIONS

# Security for Creators

# Sécurité totale de Bitdefender

**Guide de l'utilisateur**

Date de parution 12/04/2023


## Mention légale



Bitdefender

# Table des matières

# À PROPOS DE CE GUIDE

## Objectifs et destinataires

Le présent guide fournit une assistance relative à la configuration et à l'utilisation des produits inclus dans votre abonnement à la solution Bitdefender Security for Creators, spécifiquement conçue pour les créateurs de contenu tels que vous.

Vous apprendrez comment configurer Bitdefender sur différents appareils afin de les protéger contre toutes sortes de menaces et, surtout, comment protéger votre compte YouTube contre les cyberattaques directes et les tentatives de piratage.

## Comment utiliser ce guide

Le présent guide s'articule autour des quatre produits inclus dans la suite **Bitdefender Security for Creators** :

- Security for Creators (page 4)
  Découvrez comment utiliser Security for Creators pour protéger et surveiller au mieux votre chaîne YouTube, afin d'éviter tout risque de piratage de votre compte et de sabotage de son contenu.
- Email Protection
  Découvrez comment protéger au mieux votre boîte de messagerie contre les spams, les e-mails malveillants et les tentatives de phishing grâce à la protection des e-mails.
- Sécurité totale pour PC (page 16)
  Découvrez comment utiliser le produit sur vos ordinateurs de bureau et ordinateurs portables Windows.
- Antivirus pour Mac (page 162)
  Découvrez comment utiliser le produit sur vos Mac.
- Sécurité mobile pour Android (page 196)
  Découvrez comment utiliser le produit sur vos smartphones et tablettes Android.
- Sécurité mobile pour iOS (page 230)

Découvrez comment utiliser le produit sur vos smartphones et tablettes iOS.

- VPN (page 245)
  Découvrez comment masquer votre identité en ligne grâce au VPN de Bitdefender sur n'importe lequel de vos appareils.
- Obtenir de l'aide (page 270)
  Découvrez où chercher de l'aide en cas d'imprévu.

# Conventions utilisées dans ce guide

## Normes typographiques

Plusieurs styles de texte sont utilisés dans ce guide pour une lisibilité améliorée. Leur aspect et signification sont présentés dans la liste ci-dessous.

| Style | Description |
|---|---|
| sample syntax | Les exemples de syntaxe sont écrits dans une police à espacement fixe. |
| https://www.bitdefender.com | Les liens URL renvoient vers un emplacement externe comme un serveur http ou ftp. |
| documentation@bitdefender.com | Les adresses email sont insérées dans le texte pour plus d'informations sur les contacts. |
| À propos de ce guide (page 1) | Ceci représente un lien interne vers un emplacement à l'intérieur de ce document. |
| Nom de fichier | Les noms de fichiers et de répertoires sont écrits dans une police à espacement fixe. |
| **Option** | Toutes les options du produit sont écrites en caractères **gras**. |
| **Mot-clé** | Les mots-clés et les expressions importantes sont mis en évidence à l'aide de caractères **gras**. |

## Avertissement

Les avertissements sont des notes mises en évidence pour attirer votre attention sur des informations complémentaires relatives au paragraphe dans lequel elles se trouvent.

### Note

Les notes sont de courtes observations. Vous pouvez les survoler, mais elles comportent des informations intéressantes, comme des précisions sur des fonctions spécifiques ou un lien vers un thème proche.

### Important

Le texte précédé de cette icône requiert votre attention et nous vous recommandons de ne pas l'ignorer. Il fournit habituellement des informations non essentielles mais utiles.

### Attention

Le texte précédé de cette icône contient des informations essentielles que vous devez lire attentivement. Si vous suivez les indications, tout se passera bien. Assurez-vous de bien les comprendre, car elles décrivent des procédures dangereuses.

## Commentaires

Aidez-nous à améliorer ce livret ! Nous avons testé et vérifié toutes les informations mais n'hésitez pas à nous écrire pour nous signaler d'éventuelles erreurs ou des améliorations que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Écrivez-nous à l'adresse documentation@bitdefender.com. Merci de bien vouloir rédiger en anglais vos e-mails concernant cette documentation afin que nous puissions les traiter efficacement.

# 1. SECURITY FOR CREATORS

## 1.1. Qu'est-ce que Bitdefender Security for Creators ?

Bitdefender Security for Creators est la solution de cybersécurité de Bitdefender spécifiquement conçue pour protéger tous les créateurs de contenu, quel que soit le contenu de leur chaîne et le nombre de leurs abonnés. Elle inclut les fonctionnalités suivantes :

- **Protection de la chaîne YouTube** : surveille votre chaîne YouTube 24 h/24, 7 j/7 pour détecter toute tentative de prise de contrôle et fournit un guide de récupération étape par étape en cas de piratage de votre compte.
- **Protection des appareils** : l'application de sécurité Bitdefender protège tous vos appareils, sécurise vos identifiants de connexion et votre utilisation des réseaux Wi-Fi publics, identifie les e-mails de parrainage frauduleux, et bien plus encore.

> **Attention**
> Actuellement, Security for Creators surveille et protège uniquement vos comptes YouTube, mais nous travaillons activement à étendre notre couverture à toutes les principales plateformes utilisées aujourd'hui par les créateurs de contenu.

Chaque jour, des chaînes YouTube sont piratées pour diffuser de fausses émissions en direct, promouvoir des escroqueries (par exemple, offres de cryptomonnaies) ou demander des rançons. Bitdefender Security for Creators apporte aux créateurs de contenu tout ce dont ils ont besoin pour protéger leur compte YouTube. La solution favorise la récupération rapide des comptes volés en cas de piratage et informe l'utilisateur de toute modification suspecte apportée à la chaîne, telle que la suppression de plusieurs vidéos en peu de temps ainsi que les modifications rapides des images du profil et de la bannière, des descriptions et d'autres éléments de la chaîne YouTube - autant de comportements typiques d'une situation de « compte volé ».

## 1.2. Configuration de Security for Creators

Pour commencer à configurer votre abonnement Bitdefender Security for Creators, vous devez d'abord activer le produit pour lancer le processus :

- **Activez la solution** : immédiatement après l'achat, vous devriez recevoir un e-mail de confirmation dans votre boîte de messagerie. Suivez les instructions qu'il contient pour activer votre abonnement Bitdefender Security for Creators.

Une fois cette étape franchie, configurez votre abonnement Bitdefender :

1. Sur l'écran confirmant l'activation de votre abonnement, cliquez sur le bouton **Commencer** pour démarrer la configuration.
   Sinon, si vous avez quitté cette fenêtre, cliquez sur **Security for Creators** dans le menu de gauche de votre compte Bitdefender.
2. Cliquez sur le bouton **Commençons** pour procéder à une configuration rapide.
3. Connectez votre chaîne YouTube en procédant comme suit :
   a. Cliquez sur le bouton **Se connecter avec Google**.
   b. Utilisez le compte Google associé à votre chaîne YouTube. Saisissez votre mot de passe et vérifiez votre numéro de téléphone si l'on vous y invite, puis cliquez sur **Suivant**.
   c. Cliquez sur **Continuer** pour accorder les autorisations nécessaires et autoriser Bitdefender à protéger votre chaîne YouTube.
4. Protégez votre appareil. Téléchargez et installez l'application Bitdefender pour bloquer toutes les menaces auxquelles votre appareil pourrait être exposé.
   a. Cliquez sur le bouton **Télécharger**.
   b. Suivez les instructions qui s'affichent à l'écran pour installer l'application Bitdefender sur votre appareil.
   c. Une fois l'installation terminée, cliquez sur **Suivant** pour continuer.
5. **Terminez la configuration** : cliquez sur le bouton**Passer à votre tableau de bord** pour ouvrir votre tableau de bord Bitdefender Central.

Le processus d'intégration est maintenant terminé !

## 1.3. Fonctionnalités & Capacités

Vous trouverez le tableau de bord Security for Creators dans le menu de gauche de votre compte Bitdefender.

De là, vous pouvez facilement sécuriser et récupérer votre chaîne YouTube, gérer les accès des membres de votre équipe et surveiller l'activité du compte, offrant ainsi à votre travail créatif un environnement plus sûr et plus productif. Nous détaillons ci-dessous les diverses caractéristiques et fonctionnalités de Bitdefender Security for Creators

## 1.3.1. Activité

**Détails de la chaîne** :

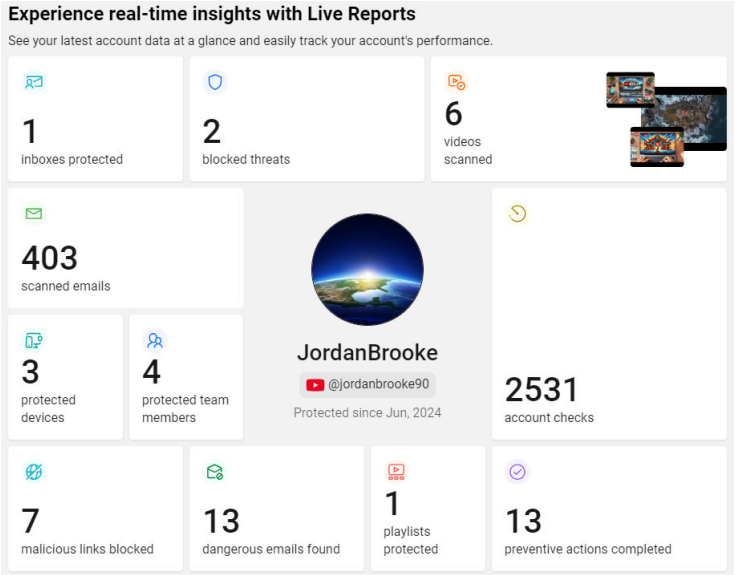
En haut de l'onglet « Activité », vous trouverez toutes les informations de base de votre chaîne YouTube.

- Photo de profil et nom de la chaîne.
- Nombre d'abonnés et nombre de vidéos actuellement téléchargées.

**Rapports en temps réel**:

Le bouton « Rapports en temps réel » vous permet d'obtenir des analyses et des informations en temps réel sur l'état de sécurité de votre chaîne :

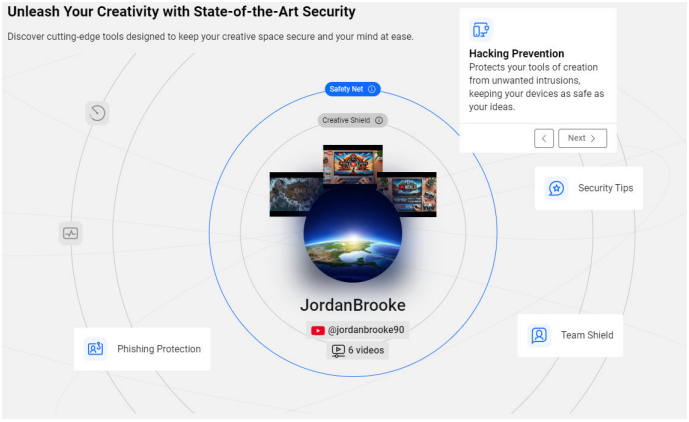
- Nombre d'appareils surveillés et protégés, membres de l'équipe, boîtes de messagerie surveillées.
- Nombre d'e-mails dangereux et d'URL malveillantes bloqués.
- Nombre d'e-mails et de vidéos analysés, ainsi que nombre de vérifications du compte effectuées par Bitdefender.




**Technologies** :

Les technologies facilitent l'exploration des différentes fonctionnalités de Bitdefender Security for Creators.

Appuyez sur le bouton **Suivant** ou cliquez sur une fonctionnalité spécifique pour en savoir plus :




**Informations de sécurité en temps réel** :

Lorsque vous faites défiler la page « Activité » vers le bas, vous voyez :

- **L'activité de la chaîne YouTube** : des informations actualisées sur l'activité récente de votre chaîne.
- **Des recommandations de sécurité** : des conseils de sécurité pour protéger votre compte contre les pirates. Pour chaque recommandation de sécurité (par exemple, « Vérifiez les applications tierces » ou « Vérifiez les options de récupération »), cliquez sur le bouton **Vérifier**. Vous accéderez alors à une page sur laquelle vous pourrez vérifier ou supprimer des éléments si nécessaire.
  Après avoir appliqué les actions recommandées, cliquez sur le bouton **Marquer comme terminé**.
- **Alertes critiques et conseils de récupération** : en cas de détection d'activités suspectes (par exemple, suppression de plusieurs vidéos ou modifications inhabituelles des diffusions ou du contenu), l'onglet **Activité** émettra des alertes critiques. Ces alertes vous guideront pas à pas dans les actions à entreprendre pour récupérer rapidement votre chaîne YouTube et la protéger contre de futurs piratages.

## 1.3.2. Sécurité

Dans l'onglet **Sécurité**, vous pouvez rapidement vérifier l'état de votre sécurité et visualiser les appareils protégés ainsi que les e-mails et les menaces bloqués par le passé. L'onglet **Sécurité** est divisé en deux sections : **Mes appareils** et **Protection des e-mails**.

- **Mon appareil**
  - Protection des nouveaux appareils Windows, macOS, Android et iOS.
  - Afficher un résumé des menaces cybersécuritaires récemment détectées.
  - Voir les appareils actuellement protégés par Bitdefender.
- **Protection des e-mails**
  - Visualiser tous les e-mails analysés par la protection des e-mails de Bitdefender au cours des 30 derniers jours, classés selon qu'ils ont été jugés sûrs ou dangereux.

- Visualiser toutes les boîtes de messagerie protégées et leur état actuel.

### 1.3.3. Membres de l'équipe

L'onglet **Membres de l'équipe** vous permet de gérer les membre de l'équipe de votre chaîne YouTube :

- Envoyer des invitations par e-mail pour protéger les nouveaux membres de l'équipe.
- Supprimer des membres de l'équipe.

## 1.4. Supprimer une chaîne YouTube et en ajouter une autre

Pour supprimer une chaîne YouTube surveillée et configurer Bitdefender Security for Creators pour un autre compte, procédez comme suit :

### 1.4.1. Supprimer une chaîne YouTube surveillée

1. Connectez-vous à votre compte Bitdefender Central.
2. Une fois connecté, cliquez sur votre nom d'utilisateur ou sur l'icône de votre profil dans le coin supérieur droit de la page.
3. Sélectionnez **Paramètres** dans le menu. La page des paramètres du compte Bitdefender s'affiche.
4. Dans la section **Gérer les comptes**, cliquez sur **Supprimer un compte**.
5. Une fenêtre pop-up s'affiche, vous demandant si vous souhaitez vraiment supprimer la chaîne.
   Cliquez sur **Supprimer le compte** pour confirmer l'action.

   **Important**
   Lorsque Bitdefender Security for Creators cesse de surveiller une chaîne YouTube, vous ne recevez plus d'alertes en cas de prise de contrôle de votre compte par des pirates.

### 1.4.2. Ajouter une autre chaîne YouTube

1. Accédez aux paramètres de votre compte :

- Si vous venez de supprimer un compte YouTube, vous verrez s'afficher le bouton **Connecter votre compte** dans la section **Gérer les comptes**.
- Si vous commencez de zéro, connectez-vous à votre compte Bitdefender Central, cliquez sur votre nom d'utilisateur ou sur l'icône de votre profil, puis sélectionnez **Paramètres** dans le menu.

2. Cliquez sur le bouton **Connecter votre compte** dans la section **Gérer les comptes**.
3. Vous serez redirigé vers le tableau de bord Bitdefender Security for Creators.
   Faites défiler vers le bas, puis cliquez sur le bouton **Reconnecter** dans le panneau de la **chaîne YouTube déconnectée**.
4. Une fenêtre pop-up vous invitera à connecter votre compte YouTube. Cliquez sur le bouton **Se connecter avec Google**.
5. Choisissez le compte Google lié à la chaîne YouTube que vous souhaitez surveiller.
   Saisissez votre mot de passe si l'on vous y invite, puis cliquez sur **Suivant**.
6. Cliquez sur **Continuer** pour autoriser Bitdefender Security for Creators à protéger votre compte YouTube.

Une fois la connexion réussie, le nom et la photo de profil de la chaîne YouTube connectée apparaîtront en haut du tableau de bord Bitdefender Security for Creators.

## 1.5. Récupérer un compte YouTube piraté

Il est essentiel d'agir sans délai pour reprendre le contrôle de votre compte et le protéger contre de nouvelles attaques similaires. Si vous utilisez Bitdefender Security for Creators, la récupération d'une chaîne YouTube piratée se fait au moyen d'un processus simple, durant lequel vous serez guidé étape par étape.

Voici comment procéder en cas de piratage de votre chaîne YouTube :

**Étape 1 : ouvrez l'e-mail Bitdefender que vous venez de recevoir**

En cas de piratage de votre chaîne YouTube, vous recevrez instantanément un e-mail de Bitdefender intitulé **Activité suspecte détectée**. Cet e-mail vous sera envoyé à l'adresse que vous avez

utilisée pour créer votre compte Bitdefender Central. Il contient diverses informations relatives aux activités suspectes et actions notables détectées sur la chaîne, telles que :

- Le pourcentage de vidéos supprimées (par exemple, 55 % de vidéos supprimées).
- Les modifications apportées à la bannière, aux miniatures des vidéos, à la photo de profil et à la description de la chaîne.

Cliquez sur le bouton **Sécuriser votre compte maintenant** qui se trouve dans l'e-mail.

**Étape 2 : que s'est-il passé ?**

Vous allez maintenant accéder à votre compte Bitdefender Central, où une fenêtre pop-up vous informe que votre chaîne YouTube est compromise.

Dans la section **Voir ce qui s'est passé**, vous trouverez - et pourrez ainsi vérifier - une liste détaillée de toutes les modifications apportées à votre compte YouTube.

**Étape 3 : récupérez votre chaîne YouTube piratée en quatre étapes**

1. **Accédez à votre compte** : suivez les liens du menu **Accéder à votre compte** pour récupérer rapidement votre compte. Si vous ne parvenez pas à vous connecter, contactez rapidement l'assistance YouTube à l'aide des liens fournis.
2. **Réinitialisez votre mot de passe** : cliquez sur le lien dans le menu **Réinitialiser votre mot de passe** pour définir un mot de passe unique et fort comprenant au moins huit caractères, dont des minuscules et des majuscules, des chiffres et des caractères spéciaux.
3. **Vérifiez vos paramètres** : suivez les liens pour supprimer les membres de votre équipe qui ne vous sont pas familiers, les appareils non autorisés et les applications tierces suspectes.
4. **Vérifiez vos informations de récupération** : assurez-vous que vos informations de récupération sont correctes afin de prévenir tout futur accès non autorisé.

N'oubliez pas de communiquer avec vos abonnés si votre compte a été utilisé pour poster du contenu inapproprié ou si des vidéos ont été supprimées. Postez une vidéo ou une mise à jour dans la section « Communauté » de votre chaîne YouTube pour expliquer la situation et les mesures que vous avez mises en place pour résoudre le problème. La

transparence peut contribuer à maintenir la confiance de vos abonnés et à vous assurer leur soutien.

## 1.6. Questions les Plus Fréquentes

**Comment la solution Bitdefender peut-elle m'aider en cas de piratage de ma chaîne YouTube ?**

En cas de piratage de votre chaîne YouTube, Bitdefender vous envoie une alerte e-mail contenant un guide étape par étape ainsi que des liens directs vers Google/YouTube afin de vous aider à reprendre rapidement le contrôle de votre compte.

**La solution Bitdefender peut-elle contribuer à empêcher le piratage de ma chaîne YouTube ?**

Oui. Pour empêcher le piratage de votre chaîne YouTube, Bitdefender vous fournit des conseils et des stratégies de sécurité personnalisés qui vont au-delà de ce que Google propose déjà.

**La solution Bitdefender Security for Creators assure-t-elle une protection contre les e-mails de parrainage frauduleux ?**

Oui, la fonctionnalité Scam Guard identifie les e-mails suspects contenant des pièces jointes ou des liens malveillants, vous protégeant ainsi contre les fraudes dissimulées dans de fausses offres de parrainage.

**L'authentification à deux facteurs (2FA) suffit-elle à protéger ma chaîne YouTube contre les pirates ?**

L'authentification à deux facteurs (2FA) ajoute une couche de sécurité supplémentaire, mais elle n'est pas infaillible. Les pirates ont toujours la possibilité de contourner l'authentification à deux facteurs en recourant à des méthodes telles que le phishing ou l'échange de cartes SIM.

**Puis-je modifier le compte YouTube connecté à Bitdefender Security for Creators ?**

Oui, vous pouvez modifier la chaîne YouTube surveillée à tout moment :

1. Connectez-vous à votre compte Bitdefender Central.
2. Cliquez sur votre nom d'utilisateur ou sur l'icône de votre profil dans le coin supérieur droit, puis sélectionnez **Paramètres**.
3. Cliquez sur **Supprimer le compte**.

4. Cliquez sur **Connecter votre compte** pour ajouter une autre chaîne YouTube.

**Comment puis-je restaurer des vidéos YouTube supprimées si je ne dispose pas de sauvegardes ?**

La suppression d'une vidéo YouTube est définitive et ne peut être annulée. Une fois que vos vidéos YouTube sont supprimées de votre compte, il peut être difficile de les restaurer si vous ne disposez pas de sauvegardes sur un dispositif de stockage externe ou sur des services cloud. Vous pouvez essayer de contacter l'assistance YouTube pour demander de l'aide. Toutefois, la restauration de vos vidéos n'est pas garantie.

**Que dois-je faire si je rencontre des problèmes lors de la connexion de mon compte YouTube ?**

Si vous rencontrez des problèmes pour connecter votre compte YouTube à Bitdefender Security for Creators, commencez par :

- Assurez-vous que votre connexion Internet est stable.
- Vérifiez que vous avez bien sélectionné le compte Google associé à votre chaîne YouTube.
- Vérifiez que vous avez saisi le bon mot de passe.
- Vérifiez que vous avez accordé toutes les autorisations requises.

# 2. PROTECTION DES E-MAILS

Votre courrier électronique constitue une partie importante de votre vie numérique et, compte tenu de ses multiples applications dans la vie réelle, il est devenu un vecteur d'attaque privilégié pour les acteurs malveillants et l'une des principales préoccupations en matière de cybersécurité de l'utilisateur quotidien.

Protection des e-mails est une fonctionnalité de sécurité qui vous permet d'analyser et d'identifier le contenu potentiellement dangereux dans les e-mails reçus dans votre boîte de réception. Cette fonctionnalité est un ensemble de diverses technologies réunies sous un même module de protection, telles que des logiciels anti-phishing, antimalware, antispam, anti-fraude et anti-arnaque.

En créant une connexion directe entre Bitdefender et votre fournisseur de services de messagerie, vous permettez à l'antivirus d'analyser directement vos e-mails et d'éliminer les limitations liées à l'utilisation de différents appareils ou clients de messagerie.

> **Note**
> Vous pouvez protéger jusqu'à 5 comptes de messagerie différents.

## 2.1. Configuration de votre compte

Cette fonctionnalité est parfaitement intégrée à l'interface utilisateur. Pour commencer à utiliser Protection des e-mails :

1. Sous **protection**, Cliquez sur **Ouvrir** dans le **Protection des e-mails** carte.
2. Choisissez votre fournisseur de messagerie pour le compte de messagerie que vous souhaitez protéger.

   > **Note**
   > Protection des e-mails est actuellement disponible pour les comptes Google, les comptes Outlook et sera bientôt également disponible pour Yahoo Mail.

3. Clique sur le **Se connecter** bouton.
   L'opération se poursuivra ensuite dans votre navigateur.

4. Entrez votre adresse email et cliquez sur le **Suivant** bouton
5. Pour continuer, entrez votre mot de passe et cliquez sur le **Suivant** bouton.
6. Vérifiez les autorisations demandées à l'écran et autorisez Bitdefender à protéger votre compte de messagerie.

Votre compte de messagerie est désormais protégé et tous vos nouveaux e-mails entrants seront analysés contre les menaces.

> **Note**
> Chaque e-mail numérisé sera marqué d'une étiquette pour indiquer ses niveaux de sécurité.

## 2.2. Tableau de bord

Le tableau de bord affichera vos emails protégés sous lesquels vous retrouverez :

- date de configuration (la date à laquelle le compte a été configuré pour Email Protection)
- statut (actif ou inactif)
- nombre d'e-mails filtrés au cours des 30 derniers jours.
  Ici, vous verrez un graphique présentant le nombre d'e-mails sûrs et d'e-mails dangereux reçus.

**Pour ajouter plusieurs comptes de messagerie** clique sur le **Ajouter un autre compte** et suivez le processus de configuration ci-dessus pour chacun d'eux.

**Pour suspendre l'analyse ou supprimer un compte** à partir de cette fonctionnalité, cliquez sur les trois points à côté du compte en question et cliquez sur **Gérer son compte**.

# 3. SÉCURITÉ TOTALE POUR PC

## 3.1. Installation

### 3.1.1. Préparer l'installation

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

- Vérifiez que l'appareil sur lequel vous prévoyez d'installer Bitdefender dispose de la configuration requise. Si l'appareil ne dispose pas de la configuration requise, Bitdefender ne pourra pas être installé, ou, une fois installé, il ne fonctionnera pas correctement, ralentira le système et le rendra instable. Pour des informations détaillées sur la configuration requise, veuillez consulter Configuration requise (page 16).
- Connectez-vous à l'appareil en utilisant un compte administrateur.
- Désinstallez tous les autres logiciels similaires sur l'appareil. Si un logiciel est détecté pendant le processus d'installation de Bitdefender, vous recevrez une notification pour le désinstaller. L'exécution de deux programmes de sécurité à la fois peut affecter leur fonctionnement et provoquer d'importants problèmes sur le système. Windows Defender sera désactivé pendant l'installation.
- Désactivez ou supprimez tout logiciel pare-feu s'exécutant sur l'appareil. 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 appareil soit connecté à Internet pendant l'installation, même pour une installation à partir d'un CD/DVD. Si des versions plus récentes des fichiers d'applications du logiciel d'installation sont disponibles, Bitdefender peut les télécharger et les installer.

### 3.1.2. Configuration requise

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

- Windows 7 avec Service Pack 1
- Windows 8.1
- Windows 10
- 2,5 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- 2 Go de mémoire (RAM)

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

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

- Sur **Windows 7**, faites un clic droit sur **Poste de travail** sur le bureau, puis sélectionnez **Propriétés** dans le menu.
- Sur **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. Sur **Windows 8.1**, localisez **Cet ordinateur**.
  Sélectionnez **Propriétés** dans le menu inférieur. Consultez la rubrique **Système** pour connaître le type du système.
- Sur **Windows 10**, tapez **Système** dans la zone de recherche de la barre des tâches et cliquez sur l'icône. Consultez la rubrique **Système** pour connaître le type du système.

## 3.1.3. Configuration logicielle requise

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

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

## 3.1.4. Installer votre produit Bitdefender

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

Si votre achat couvre plus d'un appareil, répétez le processus d'installation et activez votre produit avec le même compte sur chaque appareil. Le compte que vous devez utiliser est celui qui contient votre abonnement actif Bitdefender.

### 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 Total Security est activé.

Pour télécharger Bitdefender Total Security depuis Bitdefender Central :

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

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

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

## Valider l'installation

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

Si votre système ne dispose pas de la configuration minimale requise pour l'installation de Bitdefender, vous serez informé(e) des éléments devant être mis à niveau avant de pouvoir poursuivre.

Si une solution de sécurité incompatible ou une version antérieure de Bitdefender est détectée, il vous sera demandé de la désinstaller de votre système. Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite. Il est parfois nécessaire de redémarrer l'appareil pour terminer la désinstallation des solutions de sécurité détectées.

Le package d'installation de Bitdefender Total 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 d'installation s'ouvre. Suivez les instructions pour installer Bitdefender Total 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 Total 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.

## Étape 3 - Installation terminée

Votre produit Bitdefender a été installé avec succès.

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

## Étape 4 - Analyse de l'appareil

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

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

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

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

## Étape 5 - Pour commencer

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

Cliquez sur **TERMINER** pour accéder à l'interface Bitdefender Total Security.

## 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.

## Valider l'installation

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

Si votre système ne dispose pas de la configuration minimale requise pour l'installation de Bitdefender, vous serez informé(e) des éléments devant être mis à niveau avant de pouvoir poursuivre.

Si une solution de sécurité incompatible ou une version antérieure de Bitdefender est détectée, il vous sera demandé de la désinstaller de votre système. Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite. Il est parfois nécessaire de redémarrer l'appareil pour terminer la désinstallation des solutions de sécurité détectées.

Le package d'installation de Bitdefender Total 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 d'installation s'ouvre. Suivez les instructions pour installer Bitdefender Total Security.

## Étape 1 - Installation de Bitdefender

Avant de procéder à l'installation, vous devez accepter le contrat d'abonnement. Veuillez prendre le temps de lire le contrat d'abonnement car il contient les termes et conditions selon lesquels vous pouvez utiliser Bitdefender Total Security.

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

Deux tâches supplémentaires peuvent être effectuées à cette étape :

- Garder le **Envoyer des rapports sur les produits** option activée. En autorisant cette option, des rapports contenant des informations sur la façon dont vous utilisez le produit sont envoyés aux serveurs Bitdefender. Ces informations sont essentielles pour améliorer le produit et peuvent nous aider à offrir une meilleure expérience à l'avenir. Notez que ces rapports ne contiennent aucune donnée confidentielle, comme votre nom ou votre adresse IP, et qu'ils ne seront pas utilisés à des fins commerciales.
- Sélectionnez la langue dans laquelle vous souhaitez installer le produit.

Cliquez sur **INSTALLER** pour lancer le processus d'installation de votre produit Bitdefender.

## Étape 2 - Installation en cours

Attendez que l'installation soit terminée. Des informations détaillées sur la progression s'affichent.

## Étape 3 - Installation terminée

Un récapitulatif de l'installation s'affiche. Si une menace active a été détectée et supprimée lors de l'installation, un redémarrage du système peut être nécessaire.

## Étape 4 - Analyse de l'appareil

Il vous sera alors demandé si vous souhaitez effectuer une analyse de votre appareil, afin de vous assurer qu'il est sûr. Au cours de cette étape, Bitdefender analysera les zones critiques du système. Cliquez sur **Démarrer l'analyse de l'appareil** pour l'initier.

Vous pouvez masquer l'interface de numérisation en cliquant sur **Exécuter l'analyse en arrière-plan**. Après cela, choisissez si vous souhaitez être informé lorsque l'analyse est terminée ou non.

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

> **Note**
> Alternativement, si vous ne souhaitez pas effectuer le scan, vous pouvez simplement cliquer sur **Sauter**.

## Étape 5 - Compte Bitdefender

Une fois que vous avez fini le paramétrage initial, la fenêtre Bitdefender Account 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.

Procédez selon votre situation.

- **Je veux créer un compte Bitdefender**

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

     Vous pouvez également consulter notre Politique de confidentialité.
  3. Cliquez sur **CRÉER UN COMPTE**.

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

- **J'ai déjà un compte Bitdefender**

  1. Cliquez sur **Connexion**.
  2. Saisissez l'adresse e-mail dans le champ correspondant, puis cliquez sur **SUIVANT**.
  3. Saisissez votre mot de passe puis cliquez sur **CONNEXION**.
     Si vous avez oublié le mot de passe de votre compte ou que vous souhaitez simplement reconfigurer celui déjà existant :
     a. Cliquez sur **Mot de passe oublié**.
     b. Saisissez votre adresse e-mail, puis cliquez sur **SUIVANT**.
     c. Consultez votre boite e-mail, saisissez le code de sécurité que vous venez de recevoir, et cliquez sur **SUIVANT**.
     Vous pouvez aussi cliquer sur **Changer de mot de passe** dans l'e-mail que nous vous avons envoyé.
     d. Saisissez votre nouveau mot de passe, confirmez-le puis cliquez sur **ENREGISTRER**.

     > **Note**
     > Si vous avez déjà un compte MyBitdefender, vous pouvez l'utiliser pour vous connecter à votre compte Bitdefender. En cas d'oubli de votre mot de passe, vous devrez d'abord vous rendre sur https://my.bitdefender.com pour le réinitialiser. Vous pourrez ensuite utiliser le nouveau mot de passe pour vous connecter à votre compte Bitdefender.

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

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

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

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

## Étape 6 - Activer votre produit

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

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

Procédez selon votre situation :

- J'ai un code d'activation
  Dans ce cas, enregistrez le produit en procédant comme suit :

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

     > **Note**
     > Le code d'activation se trouve :
     >
     > - sur l'étiquette du CD ou DVD.
     > - sur le manuel du produit.
     > - sur l'e-mail de confirmation d'achat en ligne.

  2. **Je souhaite essayer Bitdefender**
     Dans ce cas, vous pouvez utiliser le produit pendant 30 jours. Pour commencer votre essai, sélectionnez **Je n'ai pas d'abonnement,**

**je souhaite essayer le produit gratuitement**, puis cliquez sur **CONTINUER**.

### Étape 7 - Pour commencer

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

Cliquez sur **FINIR** pour accéder à la Bitdefender Total Security interface.

## 3.2. Gérer votre sécurité

### 3.2.1. Protection antivirus

Bitdefender protège votre appareil contre tous les types de logiciels malveillants (programmes malveillants, chevaux de Troie, logiciels espions, trousses administrateur pirates, etc.). La protection offerte par Bitdefender est divisée en deux catégories:

- **Analyse à l'accès** - bloque les nouvelles menaces avant qu'elles infiltrent votre système. Par exemple, Bitdefender recherche les menaces connues dans un document Word quand vous l'ouvrez et dans un e-mail quand vous le recevez.
  L'analyse à l'accès assure une protection en temps réel contre les menaces, et constitue un composant essentiel de tout programme de sécurité informatique.

  > **Important**
  > Pour empêcher l'infection de votre appareil par des menaces, maintenez l'**analyse à l'accès** activée.

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

Bitdefender analyse automatiquement tout support amovible connecté à l'appareil afin de s'assurer que son accès ne pose pas de problème de sécurité. Pour plus d'informations, reportez-vous à Analyse automatique de supports amovibles (page 41).

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 (page 44).

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 (page 46).

Si votre appareil a été infecté par des logiciels malveillants, consultez-vous Suppression des menaces de votre système (page 154). 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 Environnement de sauvetage (page 155). Il s'agit d'un environnement approuvé, spécialement conçu pour la suppression de logiciels malveillants, qui vous permet de faire redémarrer votre appareil indépendamment de Windows. Lorsque l'appareil s'exécute en mode de secours, les menaces Windows sont inactives, rendant leur suppression facile.

## 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 e-mails auxquels vous accédez.

## 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 Bitdefender**.
2. Dans le volet **ANTIVIRUS**, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres avancés**, activez ou désactivez **Bitdefender Shield**.
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.

## 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 sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres avancés**, vous pouvez configurer les paramètres d'analyse en fonction de vos besoins.

## Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- **Analyse des applications uniquement.** Vous pouvez configurer Bitdefender pour que seules les applications utilisées soient analysées.
- **Analyse des applications potentiellement indésirables.** Sélectionnez cette option pour analyser les applications indésirables. Une application potentiellement indésirable (PUA), ou programme potentiellement indésirable (PUP), est un logiciel généralement fourni avec les logiciels libres, qui affiche des pop-ups ou installe une barre d'outils dans le navigateur par défaut. Certains changent la page d'accueil ou le moteur de recherche, d'autres exécutent divers processus en arrière-plan ou affichent de nombreuses publicités, ce qui ralentit l'appareil. Ces programmes peuvent être installés sans

votre autorisation (adwares) ou bien inclus par défaut dans le kit d'installation rapide (logiciels financés par la publicité).

- **Analyse des scripts.** La fonctionnalité Analyse des scripts permet à Bitdefender d'analyser des scripts PowerShell et des documents Office pouvant contenir des malwares basés sur des scripts.
- **Analyse des partages réseau.** Pour accéder en toute sécurité à un réseau à distance depuis votre appareil, nous vous recommandons de maintenir activée l'option Analyse des partages réseau.
- **Analyse de la mémoire des processus.** Cette option permet de rechercher des signes d'une activité malveillante dans la mémoire des processus en cours d'exécution.
- **Analyse des lignes de commande.** Cette option permet d'analyser les lignes de commande des applications nouvellement lancées pour empêcher les attaques sans fichier.
- **Analyse des archives.** L'analyse des archives est un processus long qui consomme beaucoup de ressources. Elle n'est donc pas recommandée dans le cadre de la protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Il y a un danger uniquement si le fichier infecté est extrait de l'archive et exécuté alors que la protection en temps réel n'est pas activée.
  Si vous décidez d'utiliser cette option, activez-la puis déplacez le curseur sur l'échelle pour exclure de l'analyse les archives dont le poids est supérieur à une valeur en Mo (Mégaoctets).
- **Analyse des secteurs de démarrage.** Vous pouvez configurer Bitdefender pour que les secteurs de démarrage de vos disques durs soient analysés. Le secteur de démarrage d'un disque dur contient le code informatique nécessaire pour initier le démarrage. Lorsqu'une menace touche le secteur de démarrage, le disque peut devenir inaccessible, ce qui empêche le démarrage du système et l'accès à vos données.
- **Analyse des nouveaux fichiers et des fichiers modifiés uniquement.** En analysant uniquement les nouveaux fichiers et les fichiers modifiés, vous pouvez améliorer considérablement la réactivité globale du système sans compromettre la sécurité.
- **Analyse des enregistreurs de frappe.** Sélectionnez cette option pour analyser votre système à la recherche d'enregistreurs de frappe. Il

s'agit d'applications qui enregistrent ce que vous tapez sur votre clavier et en envoient des rapports, par Internet, à une personne malveillante (pirate). Le pirate peut ensuite extraire de ces données volées des informations sensibles telles que des numéros de comptes bancaires ou des mots de passe et en tirer profit.

- **Analyse des composants d'amorçage.** Sélectionnez l'option **Analyse des composants d'amorçage** pour analyser votre système au démarrage, dès le chargement de tous les services critiques. L'objectif est à la fois d'améliorer la détection des menaces au démarrage et d'accélérer le démarrage 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 sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres avancés**, faites défiler vers le bas jusqu'à ce que vous voyiez l'option **Actions contre les menaces**.
4. Configurez les paramètres d'analyse selon vos besoins.

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

**Prendre la mesure appropriée**

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

- **Fichiers infectés.** Les fichiers marqués comme infectés contiennent un élément répertorié dans la base de données sur les menaces de Bitdefender. Bitdefender essaie automatiquement de supprimer le code malveillant du fichier infecté et de reconstituer le fichier d'origine. C'est ce qu'on appelle la 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 (page 46).

> **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.

- **Fichiers suspects.** Les fichiers marqués comme suspects par l'analyse heuristique ne peuvent pas être désinfectés car aucun processus de désinfection n'est disponible. Ils sont mis en quarantaine pour éviter une possible infection.
- **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.

**Mise 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 (page 46).

**Interdiction de l'accès**

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

## 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 sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.

3. Dans la fenêtre **Paramètres avancés**, faites défiler vers le bas jusqu'à ce que vous voyiez l'option **Restauration des paramètres avancés**. Sélectionnez cette option pour restaurer les paramètres par défaut de l'antivirus.

## Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre appareil sans logiciel malveillant. Cela s'effectue en protégeant votre appareil des nouvelles menaces par l'analyse des e-mails que vous recevez et des nouveaux fichiers que vous téléchargez ou copiez sur votre système.

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

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

## Rechercher des menaces dans un fichier ou un dossier

Il est recommandé d'analyser les fichiers et les dossiers dès que vous soupçonnez une infection. Faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser. Sélectionnez **Bitdefender** puis **Analyser avec Bitdefender**. L'**assistant d'analyse antivirus** s'affiche et vous guide tout au long de l'analyse. À l'issue du processus, il vous sera demandé de choisir les mesures à prendre pour traiter les fichiers détectés, le cas échéant.

## Exécuter une analyse rapide

L'analyse rapide utilise l'analyse cloud pour détecter les logiciels malveillants présents sur votre système. La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

Pour démarrer une analyse rapide :

1. Cliquez sur Protection dans le menu de navigation de l'interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Analyses**, cliquez sur le bouton **Exécuter l'analyse** à côté d'**Analyse rapide**.
4. Suivez les indications de l'**Assistant d'analyse antivirus** pour exécuter l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, il vous sera demandé de choisir les actions à appliquer.

## Exécuter une analyse du système

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

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

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

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

Si vous souhaitez analyser certains emplacements de votre appareil ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée. Pour plus d'informations, reportez-vous à Configurer une analyse personnalisée (page 34).

Pour exécuter une analyse du système :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Analyses**, cliquez sur le bouton **Exécuter l'analyse** à côté d'**Analyse du système**.
4. La fonctionnalité Analyse du système vous sera présentée lors de sa première exécution. Cliquez sur **OK, j'ai compris** pour continuer.
5. Suivre la Assistant d'analyse antivirus pour terminer l'analyse. Bitdefender prendra automatiquement les actions recommandées sur les fichiers détectés. S'il reste des menaces non résolues, vous serez invité à choisir les actions à entreprendre.

## Configurer une analyse personnalisée

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

Pour configurer une nouvelle analyse personnalisée en détails :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Analyses**, cliquez sur **+Créer une analyse**.
4. Dans le champ **Nom de la tâche**, saisissez un nom pour l'analyse, sélectionnez les emplacements que vous souhaitez analyser, puis cliquez sur **Suivant**.
5. Configurez les options générales suivantes :
   - **Analysez uniquement les applications.** Vous pouvez configurer Bitdefender pour analyser uniquement les applications auxquelles vous accédez.
   - **Priorité de l'analyse.** Vous pouvez choisir un impact qu'aura l'analyse sur les performances de votre système.
     - Auto - La priorité du processus d'analyse dépendra de l'activité de votre système. Pour veiller à ce que le processus d'analyse

ne nuise pas à l'activité du système, Bitdefender décidera si le processus d'analyse doit être exécuté avec une priorité haute ou basse.

- Haute - La priorité de la tâche d'analyse sera élevée. En choisissant cette option, vous permettez à d'autres programmes de fonctionner plus lentement, et diminuez le temps nécessaire pour que l'analyse soit finie.
- Basse - La priorité de la tâche d'analyse sera basse. En choisissant cette option, vous permettez à d'autres programmes de fonctionner plus rapidement, et augmentez le temps nécessaire pour que l'analyse soit finie.

- **Actions après l'analyse.** Choisissez ce que Bitdefender doit faire si aucune menace n'est détectée.
  - Afficher la fenêtre de résumé
  - Éteindre l'appareil
  - Fermer la fenêtre d'analyse

6. Si vous souhaitez configurer les options d'analyse en détail, cliquez sur **Afficher les options avancées**. Vous trouverez des informations sur les analyses listées à la fin de cette rubrique.
   Cliquez sur **Suivant**.
7. Si vous le souhaitez, vous pouvez activer l'option **Programmer la tâche d'analyse**, puis choisir le moment où l'analyse personnalisée que vous avez créée devra démarrer.
   - Au démarrage du système
   - Tous les jours
   - Tous les mois
   - Toutes les semaines

   Pour sélectionner Quotidien, Hebdomadaire ou Mensuel, bougez le curseur le long de l'échelle pour configurer la période durant laquelle l'analyse planifiée doit débuter.
8. Cliquez sur **Enregistrer** pour enregistrer les réglages et fermer la fenêtre de configuration.

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

## Informations sur les options de numérisation

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiers avec certains de ces termes, consultez le **glossaire**. Vous pouvez également rechercher des informations sur Internet.
- **Analysez les applications potentiellement indésirables.** Sélectionnez cette option pour rechercher les applications indésirables. Une application potentiellement indésirable (PUA) ou un programme potentiellement indésirable (PUP) est un logiciel qui est généralement fourni avec un logiciel gratuit et qui affiche des fenêtres contextuelles ou installe une barre d'outils dans le navigateur par défaut. Certains d'entre eux modifieront la page d'accueil ou le moteur de recherche, d'autres exécuteront plusieurs processus en arrière-plan ralentissant le PC ou afficheront de nombreuses publicités. Ces programmes peuvent être installés sans votre consentement (également appelés adwares) ou seront inclus par défaut dans le kit d'installation express (ad-supported).
- **Analyse des archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Il y a un danger uniquement si le fichier infecté est extrait de l'archive et exécuté alors que la protection en temps réel n'est pas activée. Il est toutefois recommandé d'activer cette option pour détecter et supprimer toute menace potentielle, même si elle n'est pas immédiate.

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

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

- **Analysez uniquement les fichiers nouveaux et modifiés.** En analysant uniquement les fichiers nouveaux et modifiés, vous pouvez

considérablement améliorer la réactivité globale du système avec un minimum de compromis en matière de sécurité.

- **Analysez les secteurs de démarrage.** Vous pouvez configurer Bitdefender pour analyser les secteurs de démarrage de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour démarrer le processus de démarrage. Lorsqu'une menace infecte le secteur de démarrage, le lecteur peut devenir inaccessible et vous ne pourrez peut-être pas démarrer votre système ni accéder à vos données.
- **Analyse de la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.
- **Analyse du 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 des systèmes d'exploitation Windows et des applications installées.
- **Analyse des cookies.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur votre appareil.
- **Scannez les enregistreurs de frappe.** Sélectionnez cette option pour analyser votre système à la recherche d'applications d'enregistreur de frappe. Les enregistreurs de frappe enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur Internet à une personne malveillante (hacker). Le pirate peut découvrir des informations sensibles à partir des données volées, telles que les numéros de compte bancaire et les mots de passe, et les utiliser pour obtenir des avantages personnels.

## Assistant d'analyse antivirus

À chaque fois que vous lancez une analyse à la demande (par exemple en faisant un clic droit sur un fichier et en sélectionnant Bitdefender puis **Analyser avec Bitdefender**), l'assistant d'analyse antivirus s'ouvre. Suivez ses instructions pour exécuter l'analyse.

### Note

Si l'assistant ne s'ouvre pas, c'est peut-être que l'analyse a été configurée pour s'exécuter silencieusement, en arrière-plan. Recherchez l'icône de progression de l'analyse dans la **zone de notification**. Vous pouvez cliquer sur cette icône pour afficher la fenêtre de l'analyse et suivre sa progression.

## 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, selon sa complexité.

**Arrêt ou interruption de l'analyse.** Vous pouvez arrêter l'analyse à tout moment en cliquant sur **ARRÊT**. Dans ce cas, vous passerez directement à la dernière étape de l'assistant d'analyse. Pour interrompre l'analyse, cliquez sur **PAUSE**. Cliquez sur **REPRISE** pour que l'analyse reprenne.

**Archives protégées par mot de passe.** Lorsqu'une archive protégée par mot de passe est détectée, en fonction des paramètres de l'analyse, vous devrez peut-être saisir le mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées si vous ne saisissez pas ce mot de passe. Les options suivantes sont proposées :

- **Mot de passe.** Si vous voulez que Bitdefender analyse cette archive, sélectionnez cette option et saisissez le mot de passe. Si vous ne connaissez pas le mot de passe, choisissez une autre option.
- **Ne pas demander le mot de passe et ignorer cet objet.** Sélectionnez cette option pour que l'archive ne soit pas analysée.
- **Exclure de l'analyse tous les éléments protégés par mot de passe.** Sélectionnez cette option si vous souhaitez laisser de côté les archives protégées par mot de passe. Bitdefender ne pourra pas les analyser, mais elles seront mentionnées dans le journal d'analyse.

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

## Étape 2 - Sélectionner des actions

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

> **Note**
> Si vous lancez une analyse rapide ou une analyse du système, Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés pendant l'analyse. Si des menaces non résolues sont toujours présentes, il vous sera demandé de choisir les actions à appliquer.

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

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

**Prendre les mesures appropriées**

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

- **Fichiers infectés.** Les fichiers détectés comme infectés correspondent à une information sur la menace trouvée dans la base de données d'informations sur les menaces de Bitdefender. Bitdefender tentera 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 pour contenir l'infection. Les fichiers en quarantaine ne peuvent pas être exécutés ou ouverts ; par conséquent, le risque d'être infecté disparaît. Pour plus d'informations, reportez-vous à Gérer les fichiers en quarantaine (page 46).

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

- **Documents suspects.** Les fichiers sont détectés comme 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 pour prévenir une éventuelle infection.

- **Archives contenant des fichiers infectés.**
  - Les archives qui ne contiennent que des fichiers infectés sont supprimées automatiquement.
  - Si une archive contient à la fois des fichiers infectés et sains, Bitdefender tentera de supprimer les fichiers infectés à condition qu'il puisse reconstruire l'archive avec les fichiers sains. Si la reconstruction de l'archive n'est pas possible, vous serez informé qu'aucune action ne peut être entreprise afin d'éviter de perdre des fichiers sains.

**Supprimer**

Supprime du disque les fichiers détectés.

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

**Ignorer**

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

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

## Étape 3 - Récapitulatif

Une fois les problèmes de sécurité résolus par BitDefender, les résultats de l'analyse apparaissent dans une nouvelle fenêtre. Si vous souhaitez consulter des informations complètes sur le processus d'analyse, cliquez sur **AFFICHER JOURNAL** pour afficher le journal d'analyse.

### Important

Dans la plupart des cas, BitDefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte. Il y a toutefois des problèmes qui ne peuvent pas être résolus automatiquement. Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation. Pour plus d'informations et d'instructions sur la méthode permettant de supprimer des logiciels malveillants manuellement, reportez-vous à Suppression des menaces de votre système (page 154).

## 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 **Avis** dans le menu de navigation sur le Interface Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant la dernière analyse.
   Cette rubrique 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**.

## Analyse automatique de supports amovibles

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

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

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

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

## 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 Bitdefender apparaît dans la **zone de notification**. Vous pouvez cliquer sur cette icône pour afficher la fenêtre de l'analyse et suivre sa progression.

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/DVD. Ni 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 (page 154).

## Gérer l'analyse des supports amovibles

Pour gérer l'analyse automatique de supports amovibles :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Paramètres**.

Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible. Si des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (supprimer le code malveillant) ou de les placer en quarantaine. Si ces actions échouent, l'assistant d'analyse antivirus vous permettra de spécifier d'autres actions à appliquer aux fichiers infectés. Les options d'analyse sont prédéterminées et vous ne pouvez pas les modifier.

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

## Analyse du fichier hôtes

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

Pour configurer l'analyse du fichier hôtes :

1. Cliquez sur **Paramètres** dans le menu de navigation sur le Interface Bitdefender.
2. Sélectionnez le **Avancé** languette.
3. Activez ou désactivez **Analyse du fichier hôtes**.

## Configurer des exceptions d’analyse

Bitdefender permet d'exclure des fichiers, des dossiers ou des extensions spécifiques de l'analyse. Cela permet d'éviter que l'analyse interfère avec votre travail, mais aussi d'améliorer les performances de votre système. Ces exceptions doivent être décidées par des utilisateurs ayant des compétences avancées en informatique, ou bien appliquées conformément aux recommandations d'un représentant de Bitdefender.

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

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

## 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 sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres**, cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez le chemin du dossier que vous souhaitez exclure de l'analyse dans le champ correspondant.
   Sinon, vous pouvez naviguer jusqu'au dossier en cliquant sur le bouton Parcourir situé sur la droite de l'interface, le sélectionner puis cliquer sur **OK**.
6. Activez l'interrupteur situé à côté de la fonctionnalité de protection qui ne devrait pas analyser le dossier. Il existe trois options :
   - Antivirus
   - Online Threat Prevention

- Advanced Threat Defense

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

## Exclure des extensions de fichier de l'analyse

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

> **Important**
> Soyez prudent lorsque vous excluez de l'analyse des extensions car celles-ci peuvent rendre votre appareil vulnérable aux menaces.

Pour exclure des extensions de fichiers de l'analyse :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans le **Paramètres** fenêtre, cliquez **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez les extensions que vous souhaitez exclure de l'analyse en les précédant d'un point et en les séparant par des points-virgules (;).
   txt;avi;jpg
6. Activez l'interrupteur situé à côté de la fonctionnalité de protection qui ne devrait pas analyser l'extension.
7. Cliquez sur **Enregistrer**.

## 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 sur le Interface Bitdefender.

2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Paramètres**, cliquez sur **Gérer les exception**. La liste de toutes vos exceptions s'affiche.
4. Pour supprimer ou éditer des exceptions d'analyse, cliquez sur l'un des boutons disponibles. Procédez comme suit :
   - Pour effacer une exception de la liste, cliquez sur le bouton situé à côté de celle-ci.
   - Pour modifier une entrée du tableau, cliquez sur le bouton **Éditer** situé à côté de celle-ci. Une nouvelle fenêtre apparaît dans laquelle vous pouvez modifier l'extension ou le chemin à exclure ainsi que la fonctionnalité de sécurité dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **MODIFIER**.

## 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.

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 sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Paramètres**.
   Vous pouvez ici voir le nom des fichiers en quarantaine, leur emplacement d'origine et le nom des menaces détectées.
4. Les fichiers en quarantaine sont gérés automatiquement par Bitdefender en fonction des paramètres de quarantaine par défaut.
   Bien que ce ne soit pas recommandé, vous pouvez régler les paramètres de quarantaine en fonction de vos préférences en cliquant sur **Voir les paramètres**.

Cliquez sur les boutons pour activer ou désactiver :

**Analyser la quarantaine après la mise à jour des informations 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.

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

## 3.2.2. Défense avancée contre les menaces

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

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

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

### Activer ou désactiver Advanced Threat Defense

Pour activer ou désactiver Advanced Threat Defense :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le volet **ADVANCED THREAT DEFENSE**, cliquez sur **Ouvrir**.

3. Ouvrez la fenêtre **Paramètres** et cliquez sur l'interrupteur situé à côté de **Bitdefender Advanced Threat Defense**.

> **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.

## 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 sur le Interface Bitdefender.
2. Dans le **DÉFENSE AVANCÉE CONTRE LES MENACES** volet, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Défense contre les menaces**.
   Les attaques détectées ces 90 derniers jours sont affichées. Pour en apprendre plus sur le type d'un ransomware détecté, le chemin du processus malveillant ou si la désinfection a été une réussite, cliquez sur celui-ci.

## Ajout de processus aux exceptions

Vous pouvez configurer des règles d'exceptions pour les applications approuvées 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 des exceptions d'Advanced Threat Defense :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **DÉFENSE AVANCÉE CONTRE LES MENACES** volet, cliquez sur **Ouvrir**.
3. Dans le **Paramètres** fenêtre, cliquez **Gérer les exceptions**.

4. Cliquez sur **+Ajouter une exception**.
5. Entrez le chemin du dossier que vous souhaitez exclure de l'analyse dans le champ correspondant.
   Sinon, vous pouvez naviguer jusqu'à l'exécutable en cliquant sur le bouton Parcourir situé sur la droite de l'interface, le sélectionner puis cliquer sur **OK**.
6. Activez l'interrupteur situé à côté de **Advanced Threat Defense**.
7. Cliquez sur **Sauvegarder**.

### Détection des exploits

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

### Activer ou désactiver la détection des exploits

Pour activer ou désactiver la détection des exploits :

- Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
- Dans le **DÉFENSE AVANCÉE CONTRE LES MENACES** volet, cliquez sur **Ouvrir**.
- Ouvrez la fenêtre **Paramètres** et cliquez sur l'interrupteur situé à côté de {3}Détection des exploits{4} pour activer ou désactiver cette fonctionnalité.

> **Note**
> L'option Détection des exploits est activée par défaut.

## 3.2.3. Prévention des menaces en ligne

Bitdefender Online Threat Prevention vous garantit une navigation sur Internet en toute sécurité, en vous signalant les pages web présentant un risque.

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

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

Pour configurer les paramètres d'Online Threat Prevention :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le volet **ONLINE THREAT PREVENTION**, cliquez sur **Paramètres**.

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

- La Prévention d'attaques réseaux bloque les menaces provenant d'Internet, y compris les téléchargements intempestifs.
- 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 :

  Vous ne devriez pas consulter cette page web.

  Cette page web peut contenir du contenu dangereux. Soyez prudent(e) si vous décidez de la consulter.

  Cette page ne présente pas de risque.

  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 l'option Analyse web chiffrée activée.
- Protection contre la fraude.
- Protection antiphishing.

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

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

Pour configurer et gérer les sites Internet, domaines et adresses IP en utilisant la fonctionnalité Online Threat Prevention fournie par Bitdefender :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PRÉVENTION DES MENACES EN LIGNE** volet, cliquez sur **Paramètres**.
3. Cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez dans le champ correspondant le nom du site Internet, le nom du domaine ou l'adresse IP que vous souhaitez ajouter aux exceptions.
6. Cliquez sur l'interrupteur situé à côté de **Online Threat Prevention**.
7. Pour supprimer une entrée de la liste, cliquez sur le bouton à côté.

Cliquez sur **Sauvegarder** pour enregistrer les modifications et fermer la fenêtre.

### Alertes de 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. Les options suivantes sont disponibles :

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

## 3.2.4. Antispam

Spam, ou pourriel, 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 dans votre boîte professionnelle) et vous ne pouvez pas empêcher les gens d'en envoyer. L'idéal serait de pouvoir arrêter de les recevoir. Malheureusement, les spams prennent des formes et des tailles variées, et il y en a 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 (page 53).

La protection antispam de Bitdefender est disponible uniquement pour les clients de messagerie configurés pour recevoir des messages via

le protocole POP3. POP3 est l'un des protocoles les plus utilisés pour télécharger des e-mails depuis un serveur de messagerie.

> **Note**
> Bitdefender ne fournit pas de protection antispam pour les comptes de messagerie auxquels vous accédez via un service sur le web.

Les spams détectés par Bitdefender portent le préfixe [Spam] dans leur ligne Objet. Bitdefender déplace automatiquement les spams dans un dossier spécifique :

- Dans Microsoft Outlook, les spams sont placés dans le sous-dossier **Courrier indésirable**, qui se trouve dans le dossier **Éléments supprimés**. Le sous-dossier **Courrier indésirable** est créé lorsqu'un e-mail est identifié comme spam.
- Dans Mozilla Thunderbird, les spams sont placés dans le sous-dossier **Courrier indésirable**, qui se trouve dans le dossier **Corbeille**. Le sous-dossier **Courrier indésirable** est créé lorsqu'un e-mail est identifié comme spam.

Si vous utilisez un autre client de messagerie, vous devez créer une règle pour déplacer les e-mails identifiés comme des [spams] par Bitdefender dans un dossier de quarantaine. Si les dossiers Éléments supprimés ou Corbeille sont supprimés, le dossier Courrier indésirable est également supprimé. Toutefois, un nouveau dossier est créé si un e-mail est identifié comme spam.

## Aperçu de l'antispam

L'antispam comprend les fonctionnalités et paramètres suivants :

## 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 des amis**, la **liste des spammeurs** et le **filtre Jeu de caractères**.

### Liste des 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 des 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 e-mail à la **liste des amis**. Bitdefender ne bloquera aucun de leurs messages; l'ajout d'amis à la liste assure la transmission des messages légitimes.

### Filtre Jeu de caractères

De nombreux spams sont écrits en caractères cyrilliques et/ou asiatiques. Le filtre Jeu de caractères détecte ce type de messages et les signale en tant que SPAM.

## Fonctionnement de l'antispam

Le moteur antispam de Bitdefender 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 d'Internet est d'abord vérifié à l'aide du filtre **Liste des amis**/**Liste des spammeurs**. Si l'adresse de l'expéditeur figure dans la **liste des 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 marqué comme un 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 un spam et déplacé vers le dossier **Spam**.

> **Note**
> Si l'e-mail a un objet À CARACTÈRE SEXUEL, Bitdefender le considérera comme du SPAM.

## Clients et protocoles de messagerie pris en charge

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

- Microsoft Outlook 2007 / 2010 / 2013 / 2016 / 2019
- Mozilla Thunderbird 14 ou versions supérieures

## Activer ou désactiver la protection antispam

La protection antispam est activée par défaut.

Pour activer ou désactiver la fonctionnalité Antispam :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le panneau **ANTISPAM**, activez ou désactivez le bouton.

## 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 marqué 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 (page 55).

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

**Paramètres** - ouvre une fenêtre permettant de configurer les filtres antispam et les paramètres de la barre d'outils.

**Est un spam** - indique que l'e-mail sélectionné est un spam. Il sera déplacé immédiatement vers le dossier **Spam**. Si les services antispam dans le cloud sont activés, il sera envoyé vers le cloud Bitdefender pour des analyses complémentaires.

**N'est pas un spam** - indique que l'e-mail sélectionné n'est pas un spam et que Bitdefender n'aurait pas dû l'identifier comme tel. Il sera déplacé immédiatement du dossier **Spam** à la **boîte de réception**. Si les services antispam dans le cloud sont activés, il sera envoyé vers le cloud Bitdefender pour des analyses complémentaires.

> **Important**
>
> Le bouton **Pas un spam** n'est actif que si vous sélectionnez un message marqué comme SPAM par Bitdefender (les messages de ce type se trouvent habituellement dans le dossier **Spam**).

**Ajouter un spammeur** - ajoute l'expéditeur de l'e-mail sélectionné à la liste des spammeurs. Il vous sera peut-être demandé de cliquer sur **OK** pour confirmer. Les e-mails provenant d'adresses figurant dans la liste des spammeurs sont automatiquement marqués comme [spam].

**Ajouter un ami** - ajoute l'expéditeur à la liste des amis. Il vous sera peut-être demandé de cliquer sur **OK** pour confirmer. 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 leur contenu. Pour plus d'informations, reportez-vous à Configurer la liste des spammeurs (page 59).

**Amis** - ouvre la **liste des spammeurs** qui contient toutes les adresses e-mail dont vous voulez toujours recevoir, quel que soit leur contenu. Pour plus d'informations, reportez-vous à Configurer la liste des amis (page 58).

## 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 des [spams] ). Cela contribue à améliorer l'efficacité du filtre antispam. Pour cela, procédez comme suit :

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 un [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils Bitdefender Antispam pour ajouter l'expéditeur à la liste des amis. Il vous sera peut-être demandé de cliquer sur **OK** pour confirmer. 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 un spam** de la barre d'outils Bitdefender Antispam (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Le message sera déplacé vers la boîte de réception.

## 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 considérés comme des spams. Cela contribue à améliorer considérablement l'efficacité du filtre antispam. Pour cela, procédez comme suit :

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 **Est un Spam** de la barre d'outils Bitdefender Antispam (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Les messages sont immédiatement marqués comme des [spams] et sont placés dans le dossier Courrier indésirable.

## 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 :

- **Marquer les spams comme lus** - marque automatiquement les spams comme lus, pour que leur réception ne vous perturbe pas.

- Vous pouvez choisir d'afficher ou non une fenêtre de confirmation lorsque vous cliquez sur le bouton **Ajouter un spammeur** et **Ajouter un ami** de la barre d'outils antispam.
  Les fenêtres de confirmation peuvent empêcher d'ajouter accidentellement des expéditeurs d'e-mails à la liste des amis/des spammeurs.

## Configurer la liste des amis

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

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

Pour configurer et gérer la liste des amis :

- Si vous utilisez Microsoft Outlook ou Thunderbird, cliquez sur le bouton Amis de la **barre d'outils Bitdefender Antispam**.
- Autre option :
  1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
  2. Dans le volet **ANTISPAM**, cliquez sur **Paramètres**.
  3. Ouvrez la fenêtre **Gérer les amis**.

Pour ajouter une e-mail, sélectionnez l'option **Adresse e-mail**, saisissez l'adresse puis cliquez sur **AJOUTER**. Syntaxe : nom@domaine.com.

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

- @domaine.com et domaine.com - tous les messages en provenance de domaine.com seront dirigés vers votre **boîte de réception** quel que soit leur contenu ;

- domaine - tous les messages de domaine (quel que soit le suffixe) seront marqués comme SPAM ;
- com - tous les messages provenant d'un domaine avec un suffixe com seront marqués 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 supprimer un élément de la liste, cliquez sur le bouton correspondant situé à côté de celui-ci. Pour supprimer l'intégralité de la liste, cliquez sur **Effacer la liste**.

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

Pour charger une liste préalablement enregistrée, cliquez sur **Charger**, puis ouvrez le fichier **.bwl** correspondant. Pour supprimer le contenu de la liste existante lorsque vous chargez une liste préalablement enregistrée, cochez la case située à côté de **Écraser la liste actuelle**.

## Configurer la liste des spammeurs

La **liste des spammeurs** est une liste de toutes les adresses e-mail dont vous ne voulez recevoir aucun message, quel que soit leur contenu. Tout message en provenance d'une adresse figurant dans la **liste des spammeurs** sera automatiquement marqué comme 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 Bitdefender Antispam** intégrée à votre client de messagerie.
- Alternativement :
  1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
  2. Dans le **ANTI-SPAM** volet, cliquez sur **Paramètres**.

3. Ouvrez la fenêtre **Gérer les spammeurs**.

Pour ajouter une adresse e-mail, sélectionnez le **Adresse e-mail** option, entrez l'adresse, puis cliquez sur **AJOUTER**. Syntaxe : nom@domaine.com.

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

- @domaine.com et domaine.com - tous les messages en provenance de domaine.com seront dirigés vers votre **boîte de réception** quel que soit leur contenu ;
- domaine - tous les e-mails reçus du domaine (quels que soient les suffixes du domaine) seront marqués 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 les noms de domaine de services de messagerie sur le web (Yahoo, Gmail, Hotmail, etc.) à la liste des spammeurs. Sinon, tous les messages provenant d'utilisateurs de ces services seront considérés comme des spams. Par exemple, si vous ajoutez yahoo.com à la liste des spammeurs, tous les e-mails envoyés depuis des adresses yahoo.com seront marqués comme [spams].

Pour supprimer un élément de la liste, cliquez sur le bouton à côté. Pour supprimer toutes les entrées de la liste, cliquez sur **Effacer la liste**.

Vous pouvez enregistrer la liste des spammeurs dans un fichier afin de pouvoir l'utiliser sur un autre appareil 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 des 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.

## Configurer les filtres antispam locaux

Comme cela est décrit dans Aperçu de l'antispam (page 53), Bitdefender utilise une combinaison de divers filtres antispam pour identifier les spams. 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 sur le Interface Bitdefender.
2. Dans le **ANTI-SPAM** volet, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Paramètres** et activez ou désactivez les interrupteurs correspondants.

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

## Configurer les paramètres cloud

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

La protection cloud fonctionne tant que Bitdefender Antispam est activé.

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

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

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.

2. Dans le **ANTI-SPAM** volet, cliquez sur **Paramètres**.
3. Allez à la **Paramètres** fenêtre et cliquez sur les commutateurs d'activation ou de désactivation correspondants.

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

## 3.2.5. Pare-feu

Le pare-feu protège votre appareil 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 (page 66).

### Activer ou désactiver la protection pare-feu

Pour activer ou désactiver la protection pare-feu :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le panneau **PARE-FEU**, activez ou désactivez le bouton.

Avertissement

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

## Gérer les 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 sur le Interface Bitdefender.
2. Dans le volet **PARE-FEU**, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Accès des applications**.

Vous pouvez voir les derniers programmes (processus) qui sont passés à travers le pare-feu Bitdefender et le réseau Internet auquel vous êtes connecté. Pour voir les règles associées à une application spécifique, cliquez sur celle-ci puis sur le lien **Voir les règles de l'application**. La fenêtre **Règles** s'ouvre.

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 ⋯ .

- **Modifier la règle** - ouvre une fenêtre dans laquelle vous pouvez modifier la règle actuelle.
- **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 sur le Interface Bitdefender.
2. Dans le **PARE-FEU** volet, cliquez sur **Paramètres**.
3. Dans la fenêtre **Règles**, cliquez sur **Ajouter une règle**.

Ici, vous pouvez apporter les modifications suivantes :

- **Appliquer cette règle à toutes les applications.** Activez cette option pour appliquer la règle créée à toutes les applications.
- **Chemin d'accès du programme.** Cliquez sur **PARCOURIR** et sélectionnez l'application à laquelle la règle s'applique
- **Autorisation.** Sélectionnez l'une des autorisations proposées :

| Autorisation | Description |
|---|---|
| **Autoriser** | L'application spécifiée se verra autoriser l'accès réseau/Internet dans les circonstances spécifiées. |
| **Refuser** | L'application spécifiée se verra refuser l'accès réseau/Internet dans les circonstances spécifiées. |

- **Type de réseau**. Sélectionnez le type de réseau auquel la règle s'applique. Vous pouvez le modifier en ouvrant le menu déroulant **Type de réseau** et en sélectionnant une des options proposées

| Réseau | Description |
|---|---|
| **Tout réseau** | Autoriser tout le trafic entre votre appareil et les autres appareils quel que soit le type de réseau. |

| Réseau | Description |
|---|---|
| **Domicile/Bureau** | Autoriser tout le trafic entre votre appareil et d'autres appareils présents sur le 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 au protocole GRE, sélectionnez **GRE**.
  - 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 de protocole IP sont attribués par l'IANA. La liste complète des numéros de protocole IP figure 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. |
| **Entrant et sortant** | La règle s'applique dans les deux directions. |

Cliquez sur le bouton **Paramètres avancés** situé dans la partie inférieure de la fenêtre pour 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**.

## Gérer les paramètres de connexion

Que vous vous connectez à Internet via le Wi-Fi 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 sur le Interface Bitdefender.
2. Dans le **PARE-FEU** volet, cliquez sur **Paramètres**.
3. Sélectionnez la fenêtre **Adaptateurs réseau**.
4. Sélectionnez les options que vous voulez appliquer lors de la connexion aux adaptateurs suivants :
   - Wi-Fi
   - Ethernet

## Configurer les paramètres avancés

Pour configurer les paramètres avancés du pare-feu :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PARE-FEU** volet, cliquez sur **Paramètres**.
3. Sélectionnez le **Paramètres** fenêtre.

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 appareil. Ils peuvent alors s'introduire dans votre appareil, s'ils découvrent un port vulnérable ou moins sécurisé.
- **Mode Alerte** - des alertes s'affichent à chaque fois qu'une application essaie de se connecter à Internet. Sélectionnez **Autoriser** or **Bloquer**. Lorsque le mode Alerte est activé, la fonctionnalité **Profils** est automatiquement désactivée. Le mode Alerte et le mode **Batterie** peuvent être utilisés en même temps.
- **Autoriser l'accès au réseau de domaine** - autoriser ou refuser l'accès à des ressources et fichiers partagés définis par vos contrôleurs de domaine.
- **Mode Furtif** - détermine si vous pouvez être détecté par d'autres appareil. Cliquez sur **Éditer les réglages de furtivité** pour sélectionner quand votre appareil doit ou ne doit pas être visible des autres appareils.
- **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.

## 3.2.6. Vulnérabilité

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

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

- Vous pouvez rechercher des vulnérabilités sur votre système et les corriger une à une à l'aide de l'option **Analyse des vulnérabilités**.
- 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.

### Analyser votre système à la recherche de vulnérabilités

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

Analyser votre système à la recherche de vulnérabilités

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

A modifié des réglages système pouvant compromettre votre appareil et vos données, par exemple en ne permettant pas l'affichage d'alertes lorsque des fichiers exécutés modifient votre système sans votre permission ou lorsque que des appareils MTP tels que des téléphones ou des appareils-photo se connectent et exécutent différentes opérations sans que vous le sachiez.

- **Mises à jour critiques de Windows**
  Une liste des mises à jour critiques de Windows qui ne sont pas installées sur votre ordinateur apparait. Un redémarrage du système peut être nécessaire pour permettre à Bitdefender de terminer l'installation du correctif. Attention, l'installation de ces mises à jour peut prendre du temps.
- **Comptes Windows faibles**
  Vous pouvez visualiser la liste des comptes utilisateur Windows configurés sur votre appareil ainsi que le niveau de protection que leur confèrent leurs mots de passe. Vous pouvez choisir entre demander à l'utilisateur de modifier le mot de passe lors de sa prochaine connexion ou modifier le mot de passe par vous-même immédiatement. Pour définir un nouveau mot de passe pour votre système, sélectionnez **Changer de mot de passe maintenant**.
  Pour créer un mot de passe sécurisé, nous vous recommandons d'utiliser un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

- **APPLICATIONS**
  - **Sécurité du navigateur**
    Modification des paramètres de votre appareil permettant l'exécution de fichiers et de programmes téléchargés via Internet Explorer sans que leur intégrité ait été validée, pouvant entraîner une compromission de votre appareil.
  - **Mises à jour des applications**
    Pour voir les informations sur une application devant être mise à jour, cliquez sur son nom dans la liste.
    Si une application n'est pas à jour, cliquez sur **Télécharger la nouvelle version** pour télécharger la dernière version.

- **RÉSEAU**
  - **Réseau et informations d'identification**
    A modifié les paramètres système afin de permettre la connexion automatique à des points d'accès de réseaux ouverts sans que vous le sachiez ou le non chiffrement du trafic sortant sur un canal sécurisé.
  - **Réseaux Wi-Fi et routeurs**
    Pour en apprendre plus sur le réseau sans fil et le routeur sur lesquels vous êtes connectés, cliquez sur son nom dans la liste. Il est recommandé de choisir un mot de passe complexe pour votre réseau domestique. Veuillez suivre nos instructions pour ne plus avoir à vous inquiéter pour votre vie privée quand vous êtes connecté.
    Lorsque d'autres recommandations sont disponibles, suivez les instructions fournies pour vous assurer que votre réseau domestique reste protégé des pirates informatiques.

## 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 **Avis** dans le menu de navigation sur le Interface 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 à jour maintenant** pour trouver un lien vers la page web du fournisseur d'où vous pourrez installer la dernière version de l'application.
- Si un compte utilisateur Windows a un mot de passe vulnérable, cliquez sur **Changer de mot de passe** pour obliger l'utilisateur à modifier son mot de passe lors de la prochaine connexion ou pour changer le mot de passe par vous-même. Pour avoir un mot de passe sécurisé, utilisez une combinaison 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 sur le Interface Bitdefender.
2. Dans le **VULNÉRABILITÉ** volet, cliquez sur **Ouvrir**.

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

3. Ouvrez l'onglet **Paramètres**.
4. Choisissez les vulnérabilités du système que vous souhaitez vérifier régulièrement à l'aide des boutons correspondants.
   **Mises à jour de Windows**
   Vérifiez que votre système d'exploitation Windows dispose des dernières mises à jour de sécurité critiques de Microsoft.
   **Mises à jour des 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 des utilisateurs**

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 @).

**Exécution automatique**

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.

**Wi-Fi Security Advisor**

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

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

Note

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

## 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, consulter 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.

On entend par données personnelles les mots de passe et noms d'utilisateur que vous utilisez pour accéder à vos comptes en ligne, tels que les messageries, comptes bancaires ou comptes de réseaux sociaux, mais aussi les messages que vous envoyez.

Habituellement, les réseaux sans fil publics sont plus susceptibles d'être dangereux car ils ne nécessitent pas de mot de passe lors de la connexion, et si c'est le cas, le mot de passe peuvent être mis à disposition de toute personne qui veut se connecter. De plus, il peut s'agir de réseaux malveillants ou de pots de miel, faisant d'eux une cible pour les cybercriminels.

Bitdefender Wi-Fi Security Advisor donne des informations sur :

- **Réseaux Wi-Fi domestiques**
- **Réseaux Wi-Fi professionnels**
- **Réseaux Wi-Fi publics**

## Activer ou désactiver les notifications de Wi-Fi Security Advisor

Pour activer ou désactiver les notifications de Wi-Fi Security Advisor :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **VULNÉRABILITÉ** volet, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Paramètres** et activez ou désactivez l'option **Wi-Fi Security Advisor**.

## Configuration du réseau Wi-Fi domestique

Pour commencer à configurer votre réseau domestique :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **VULNÉRABILITÉ** volet, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Wi-Fi Security Advisor** puis cliquez sur **Wi-Fi domestique**.
4. Dans l'onglet **WI-FI domestique**, cliquez sur **SÉLECTIONNER WI-FI DOMESTIQUE**.
   Une liste avec les réseaux sans fil auxquels vous vous êtes connectés jusqu'à ce jour s'affiche.

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

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

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

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

## Configuration du réseau Wi-Fi professionnel

Pour commencer à configurer votre réseau professionnel :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **VULNÉRABILITÉ** volet, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Wi-Fi Security Advisor** puis cliquez sur **Wi-Fi professionnel**.
4. Dans l'onglet **WI-FI domestique**, cliquez sur **SÉLECTIONNER WI-FI PROFESSIONNEL**.
   Une liste des réseaux sans fil auxquels vous vous êtes connecté jusqu'à présent s'affiche.
5. Cherchez votre réseau professionnel, puis cliquez sur **Sélectionner**.

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

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

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

## 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 Total Security est réglé pour accomplir automatiquement les paramètres de programme suivants :

- Advanced Threat Defense est activé

- Les paramètres suivants d'Online Threat Prevention sont activés :
  - Analyse web chiffrée
  - Protection contre la fraude
  - Protection contre le phishing
- Un bouton permet d'ouvrir Bitdefender Safepay™. Dans ce cas, la protection des hotspots pour les réseaux non sécurisés est activée par défaut.

## 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 sur le Interface Bitdefender.
2. Dans le **VULNÉRABILITÉ** volet, cliquez sur **Ouvrir**.
3. Ouvrez la fenêtre **Wi-Fi Security Advisor**.
4. Selon les informations dont vous avez besoin, sélectionnez l'un des trois onglets, **Wi-Fi domestique**, **Wi-Fi professionnel** ou **Wi-Fi public**.
5. Cliquez sur **Voir les détails** à côté du réseau à propos duquel vous souhaitez avoir plus d'informations.

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

**Ce réseau Wi-Fi n'est pas sûr** - indique que la sécurité sur ce réseau est faible. Il est risqué et n'est pas recommandé pour réaliser des transactions ou consulter des comptes bancaires sans protection supplémentaire. Dans ce cas, il est recommandé d'utiliser Bitdefender Safepay™ en activant la fonction de protection des hotspots pour les réseaux non sécurisés.

**Ce réseau Wi-Fi n'est pas sûr** - indique que la sécurité sur ce réseau n'est pas suffisante. Il peut comporter des vulnérabilités et n'est pas recommandé pour réaliser des transactions ou consulter des comptes bancaires sans protection supplémentaire. Dans ce cas, il est recommandé d'utiliser Bitdefender Safepay™ en activant la fonction de protection des hotspots pour les réseaux non sécurisés.

**Ce réseau Wi-Fi est sûr** - indique que le réseau que vous utilisez est sécurisé. Vous pouvez donc réaliser des opérations sensibles en ligne sans risque.

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

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

## 3.2.7. Video & Audio Protection

De plus en plus de menaces sont conçues pour pirater les webcams et les micros intégrés. Pour empêcher tout accès non autorisé à votre webcam et recevoir une alerte en cas de tentative d'accès à votre micro par une application non approuvée, Bitdefender Video & Audio comprend :

- **Webcam Protection**
- **Microphone Monitor**

### Webcam Protection

Ce n'est pas une nouveauté : les pirates peuvent prendre le contrôle de votre webcam pour vous espionner. La plupart des solutions permettant

d'éviter cela - révocation des privilèges des applications, désactivation de la caméra intégrée ou couverture de l'objectif - ne sont pas très pratiques. Pour prévenir toute tentative d'intrusion dans votre vie privée, Bitdefender Webcam Protection surveille en permanence les applications qui essaient d'accéder à votre caméra et bloque celles qui n'ont pas été approuvées.

Vous recevrez une notification à chaque fois qu'une application non approuvée tentera d'avoir accès à votre caméra.

## Activer ou désactiver Webcam Protection

1. Cliquez sur **Vie privée** dans le menu de navigation de l'**interface Bitdefender**.
2. Dans le panneau **VIDEO & AUDIO PROTECTION**, cliquez sur **Paramètres**.
3. Maintenant, ouvrez la fenêtre **Paramètres** et activez ou désactivez l'interrupteur correspondant.

## Configurer Webcam Protection

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

1. Cliquez sur **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PROTECTION VIDÉO & AUDIO** volet, cliquez sur **Paramètres**.
3. Allez à la **Paramètres** languette.

Voici les options proposées :

**Règles de blocage des applications**

- **Bloquer tous les accès à la webcam** - aucune application n'aura l'autorisation d'accéder à votre webcam.
- **Bloque l'accès du navigateur à la webcam** - aucun navigateur hormis Internet Explorer et Microsoft Edge ne pourra accéder à votre webcam. Dans la mesure où les applications du Windows Store s'exécutent comme un processus unique, Internet Explorer et Microsoft Edge ne sont pas reconnus par Bitdefender comme des navigateurs web et ne sont donc pas concernés par ce paramètre.
- **Définir les autorisations des applications en fonction des choix de la communauté** - si la majorité des utilisateurs de Bitdefender

considère qu'une application est inoffensive, alors son accès à la webcam sera automatiquement réglé sur Autorisé. Si une application populaire est considérée comme dangereuse par la plupart d'entre eux, son accès sera automatiquement bloqué.

**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.

## Ajouter des applications à la liste de Webcam Protection

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 **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PROTECTION VIDÉO & AUDIO** volet, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Webcam Protection**.
4. Cliquez sur la fenêtre **Ajouter une application**.
5. Cliquez sur le lien désiré :
   - **Depuis Windows Store** - une liste des applications Windows Store détectées est affichée. Activez les boutons situés à côté des applications que vous voulez ajouter à la liste.
   - **Depuis vos applications** - sélectionnez le fichier .exe que vous souhaitez ajouter à la liste, puis cliquez sur **OK**.

Pour voir ce que les utilisateurs de Bitdefender ont choisi de faire avec 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.

Pour empêcher l'accès d'une application ajoutée à votre webcam, cliquez sur l'icône .

L'icône devient , ce qui signifie que l'application n'a plus accès à votre webcam.

## Microphone Monitor

Des applications malveillantes peuvent discrètement accéder à votre micro sans votre consentement. Pour vous avertir de tout exploit malveillant, Bitdefender Microphone Monitor vous avertira en cas d'événement suspect. De cette manière, aucune application ne pourra accéder à votre micro sans que vous le sachiez.

## Activer ou désactiver Bitdefender Microphone Monitor

1. Cliquez sur **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PROTECTION VIDÉO & AUDIO** volet, cliquez sur **Paramètres**.
3. Sélectionnez le **Paramètres** fenêtre.
4. Dans la fenêtre **Paramètres**, activez ou désactivez l'interrupteur de **Microphone monitor**.

## Configurer les notifications de Microphone Monitor

Pour configurer les notifications à afficher lorsqu'une application tentera d'avoir accès à votre micro, suivez ces instructions :

1. Cliquez sur **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PROTECTION VIDÉO & AUDIO** volet, cliquez sur **Paramètres**.
3. Allez à la **Paramètres** fenêtre.

Avis

- **Recevoir une notification quand une application cherche à accéder au micro**
- **Recevoir une notification quand un navigateur accède au micro**
- **Recevoir une notification quand une application non approuvée accède au micro**
- **Afficher les notifications en fonction du choix des utilisateurs de Bitdefender**

### Ajouter des applications à la liste de Microphone Monitor

Les applications qui essayent de se connecter à votre micro seront automatiquement détectées et ajoutées à votre liste des notifications. Néanmoins, vous pouvez configurer manuellement si une notification doit apparaitre ou non en suivant les instructions suivantes :

1. Cliquez sur **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PROTECTION VIDÉO & AUDIO** volet, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Audio Protection**.
4. Cliquez sur **Ajouter une candidature** fenêtre.
5. Cliquez sur le lien souhaité :
   - **À partir du magasin Windows** - une liste avec les applications Windows Store détectées s'affiche. Activez les commutateurs à côté des applications que vous souhaitez ajouter à la liste.
   - **Depuis vos applications** - allez sur le fichier .exe que vous souhaitez ajouter à la liste, puis cliquez sur **D'ACCORD**.

Pour voir ce que les utilisateurs de Bitdefender ont choisi de faire avec l'application sélectionnée, cliquez sur le icône.

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

Pour ne plus recevoir de notification concernant l'activité d'une application ajoutée, cliquez sur l'icône .

L'icône devient , ce qui signifie que les notifications de Bitdefender seront affichées lorsque l'application sélectionnée essayera de se connecter à votre micro.

## 3.2.8. Remédiation des ransomwares

La fonctionnalité Bitdefender Ransomware Remediation sauvegarde vos fichiers (documents, photos, vidéos, musique, etc.) pour éviter qu'ils soient endommagés ou perdus en cas de chiffrement par un ransomware. Chaque fois qu'une attaque de ransomware est détectée, Bitdefender bloque l'ensemble des processus impliqués et entame un processus de nettoyage. Cela vous permet de récupérer le contenu de vos fichiers sans avoir à payer la rançon demandée.

## Activer ou désactiver le nettoyage des ransomwares

Pour activer ou désactiver le nettoyage des ransomwares:

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

## 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 sur le Interface Bitdefender.
2. Dans le volet **NETTOYAGE DES RANSOMWARES**, cliquez sur **Gérer**.
3. Dans la fenêtre Paramètres, activez ou désactivez l'interrupteur **Restauration automatique**.

## 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 ransomwares. Vos fichiers y sont en sécurité, quoi que vous fassiez.

Pour voir les fichiers qui ont été restaurés automatiquement :

1. Cliquez sur **Avis** dans le menu de navigation sur le Interface Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification relative au dernier ransomware traité, puis cliquez sur **Fichiers restaurés**.
   La liste des fichiers restaurés apparait. Vous pouvez également voir où les fichiers ont été restaurés.

## 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 **Avis** dans le menu de navigation sur le Interface Bitdefender.
2. Dans l'onglet **Tous**, sélectionnez la notification relative au dernier ransomware détecté, puis cliquez sur **Fichiers chiffrés**.
3. Une liste des fichiers chiffrés apparaît.
   Cliquez sur **Récupérer des fichiers** pour continuer.
4. Si tout ou une partie de la procédure de restauration échoue, vous devez choisir un emplacement où enregistrer les fichiers déchiffrés. Cliquez sur **Emplacement de restauration**, puis choisissez un emplacement sur votre ordinateur.
5. Une fenêtre de confirmation s'affiche.
   Cliquez sur **Terminer** pour achever le processus de restauration.

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

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

## Ajout d'applications aux exceptions

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

Pour ajouter des applications à la liste des exceptions de la fonctionnalité de nettoyage des ransomwares :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **CORRECTION DES RANSOMWARE** volet, cliquez sur **Gérer**.

3. Ouvrez la fenêtre **Exceptions** et cliquez sur **+Ajouter une exception**.

## 3.2.9. Cryptomining Protection

**Qu'est-ce que la protection contre le cryptominage ?**

Grâce au recours au cryptomining, les attaquants peuvent bénéficier financièrement sans supporter les coûts et les conséquences juridiques qui y sont associés.

La fonctionnalité Cryptomining Protection de Bitdefender défend les ordinateurs Windows contre la menace croissante des activités de crypto-mining non autorisées, une pratique malveillante qui exploite les ressources et l'électricité d'un utilisateur pour générer des revenus pour les attaquants.

Note

La protection contre le cryptomining repose sur :

- Bouclier Bitdefender
- Prévention des attaques Web

Pour que Cryptomining Protection puisse fonctionner, ces deux fonctionnalités doivent également être activées.

### Activation de la protection contre le cryptominage

La fonctionnalité de protection contre le cryptominage se trouve dans l'onglet Protection.

Pour l'activer, basculez simplement son interrupteur correspondant.

Note

La protection contre le cryptomining est désactivée par défaut, garantissant que les utilisateurs contrôlent son activation.

### Modes de fonctionnement

Une fois activée, la fonctionnalité Cryptomining Protection fonctionne dans 2 états distincts, chacun adapté aux préférences de l'utilisateur :

1. **Bloquez toutes les activités de cryptomining.** (bloque automatiquement toute activité de crypto-minage et prend les mesures nécessaires pour empêcher de nouvelles tentatives non autorisées)

Ce mode est idéal pour les utilisateurs qui n'ont pas l'intention de se lancer dans des activités de crypto-minage.

2. **Détectez les activités de cryptomining.** (émet des alertes chaque fois qu'une activité de crypto-minage est détectée et nécessite la saisie de l'utilisateur pour déterminer l'action appropriée)
   Ce mode convient aux utilisateurs activement impliqués dans leurs propres activités de crypto-minage mais souhaitant surveiller et contrôler toute tentative non autorisée.

### Gérer les exceptions

Des exceptions peuvent être spécifiées pour les applications, avec la possibilité supplémentaire de définir des lignes de commande spécifiques. Cependant, des exceptions peuvent également être établies sans qu'il soit nécessaire de fournir des paramètres aussi détaillés, offrant ainsi un équilibre entre personnalisation et simplicité.

Pour ajouter une exception :

1. Cliquez sur**protection**dans le menu de gauche de l'interface Bitdefender.
2. Dans le**Protection contre le cryptominage**volet, cliquez sur**Paramètres**.
3. Clique le**Gérer les exceptions**option.
4. Ensuite, cliquez sur le**Ajouter une exception**bouton.
5. Une nouvelle fenêtre s'ouvrira. Vous pouvez exclure manuellement des applications, des URL et des adresses IP.
6. Enfin, cliquez sur**Sauvegarder**. La nouvelle règle est ajoutée à la liste des exceptions de Cryptomining Protection.

> **Note**
> Pour supprimer une exception, cliquez simplement sur l'icône de la corbeille à côté d'elle.

## 3.2.10. Bloqueur de traceurs

De nombreux sites sur lesquels vous vous rendez utilisent des traceurs pour collecter des informations sur votre comportement, soit pour les communiquer à des tiers, soit pour vous proposer des publicités ciblées. Les propriétaires de sites web gagnent ainsi de l'argent, ce qui leur permet

de vous proposer gratuitement des contenus, ou même de continuer à exploiter leur site. En plus de collecter des informations, les traceurs peuvent également ralentir votre expérience de navigation et utiliser de la bande passante.

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

Cette extension de Bitdefender est compatible avec les navigateurs suivants :

- Internet Explorer
- Google Chrome
- MozillaFirefox

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

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

## Interface du Bloqueur de traceurs

Lorsque l'extension Bloqueur de traceurs est activée, l'icône apparaît à côté de la barre de recherche de votre navigateur. À chaque fois que vous visitez un site, un chiffre s'affiche sur cette icône. Il indique le nombre de traceurs détectés et bloqués. Si vous souhaitez en savoir plus sur les traceurs bloqués, cliquez sur l'icône pour ouvrir l'interface. Vous y verrez le nombre de traceurs bloqués, mais aussi le temps nécessaire au chargement de la page et les catégories auxquelles appartiennent les

traceurs détectés. Pour voir la liste des sites qui lancent ces traceurs, cliquez sur chaque catégorie.

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

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

## Désactiver le Bloqueur de traceurs Bitdefender

Pour désactiver le Bloqueur de traceurs Bitdefender :

- Depuis votre navigateur Web :
  1. Ouvrez votre navigateur web.
  2. Cliquez sur l'icône qui se trouve à côté de la barre d'adresse de votre navigateur.
  3. Cliquez sur l'icône dans le coin supérieur droit.
  4. Utilisez le bouton correspondant pour désactiver la fonctionnalité. L'icône Bitdefender devient grise.

- Depuis l'interface Bitdefender :
  1. Cliquez sur **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
  2. Dans le volet **BLOQUEUR DE TRACEURS**, cliquez sur **Paramètres**.
  3. Désactivez le bouton correspondant au navigateur pour lequel vous voulez désactiver l'extension.

## Autoriser le traçage d'un site web

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

1. Ouvrez votre navigateur Web.
2. Cliquez sur l'icône qui se trouve à côté de la barre de recherche.

3. Clique le icône dans le coin supérieur droit.
4. Si vous êtes sur le site web que vous voulez ajouter aux exceptions, cliquez sur **Ajouter le site web actuel à la liste**.
   Si vous voulez ajouter un autre site web, saisissez son adresse dans le champ correspondant, puis cliquez sur .

## 3.2.11. La sécurité Safepay pour les transactions en ligne

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

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

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

Bitdefender Safepay™ dispose des fonctions suivantes :

- Il bloque l'accès à votre bureau et toute tentative de prise d'instantanés de votre écran.
- Il est accompagné d'un clavier virtuel, qui, lorsqu'il est utilisé, empêche les pirates de lire vos frappes au clavier.
- Il est complètement indépendant de vos autres navigateurs.
- Il contient une protection hotspot intégrée à utiliser lorsque votre appareil est connecté à des réseaux Wi-Fi non sécurisés.
- Il supporte les marque-pages et vous permet de consulter vos sites bancaires et boutiques en ligne préférés.
- Il ne se limite pas aux sites bancaires et boutiques en ligne™. Tout site web peut être ouvert dans Bitdefender Safepay

## 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 :

- Depuis l'**interface Bitdefender** :
  1. Cliquez sur **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
  2. Dans le volet **SAFEPAY**, cliquez sur **Paramètres**.
  3. Dans la fenêtre **Safepay**, cliquez sur **Lancer Safepay**.
- À partir de Windows :
  - Sur **Windows 7** :
    1. Cliquez sur **Démarrer** puis sur **Tous les programmes**.
    2. Cliquez sur **Bitdefender**.
    3. Cliquez sur **Bitdefender Safepay™**.
  - Sur **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.
  - Sur **Windows 10** et **Windows 11** :
    Tapez "Bitdefender Safepay™" dans le champ de recherche de la barre des tâches et cliquez sur son icône.

Si vous avez l'habitude des navigateurs web, vous n'aurez aucun mal à utiliser Bitdefender Safepay™- il ressemble à un navigateur standard :

- saisissez les URL que vous souhaitez consulter dans la barre d'adresses.
- ajoutez des onglets pour consulter plusieurs sites en même temps dans la fenêtre Bitdefender Safepay™ en cliquant sur ⊞.

- reculez d'une page, avancez d'une page ou rafraîchissez la page en cliquant respectivement sur ←, → ou ↻.
- accédez aux **paramètres** de Bitdefender Safepay™ en cliquant sur **Paramètres**.
- gérez vos **marque-pages** en cliquant sur ☆ à côté de la barre d'outils.
- 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.
- consultez les informations relatives à votre produit Bitdefender en cliquant sur ⋯ puis sur **À propos**.
- imprimez les informations importantes en cliquant sur ⋯ puis sur **Imprimer**.

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

## Configurer les paramètres

Cliquez ⋯ sur puis sur **Paramètres** pour configurer Bitdefender Safepay™ :

**Appliquer les règles de Bitdefender Safepay aux domaines visités**

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

**Bloquer les pop-ups**

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

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

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

Pour retirer un site web de la liste, sélectionnez le X correspondant à l'entrée désirée.

**Gérer les plug-ins**

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

**Gérer les certificats**

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

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

**Utiliser le clavier virtuel**

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

Utilisez le bouton correspondant pour activer ou désactiver la fonctionnalité.

**Confirmer l'impression**

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

## 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 ⋯ puis sur **Marque-pages** pour ouvrir la page des marque-pages.

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

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

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

### Désactiver les notifications de Safepay

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

Pour désactiver les notifications de Safepay:

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

## 3.2.12. Antivol d'appareil

Le vol d'ordinateurs portables est un problème majeur qui touche autant les particuliers que les organisations. Plus encore que la perte du matériel lui-même, les données perdues avec lui peuvent causer des dommages importants, tant sur le plan financier qu'émotionnel.

Pourtant, peu de gens prennent les mesures appropriées pour sécuriser leurs données personnelles, professionnelles et financières importantes en cas de vol ou de perte.

Bitdefender Anti-Theft vous aide à mieux vous préparer à un tel événement en vous permettant de localiser ou de verrouiller à distance votre ordinateur portable et même d'effacer toutes les données qu'il contient, si jamais vous vous séparez de votre ordinateur portable contre votre volonté.

Pour utiliser les fonctionnalités Antivol, les conditions préalables suivantes doivent être remplies :

- Les commandes ne peuvent être envoyées qu'à partir du compte Bitdefender.
- L'ordinateur portable doit être connecté à Internet pour recevoir les commandes.

Les fonctions Antivol fonctionnent de la manière suivante :

**Localiser**

Affichez la position de votre appareil sur Google Maps.

La précision de l'emplacement dépend de la façon dont Bitdefender est capable de le déterminer. L'emplacement est déterminé à quelques dizaines de mètres près si le Wi-Fi est activé sur votre ordinateur portable et qu'il existe des réseaux sans fil à sa portée.

Si l'ordinateur portable est connecté à un réseau local câblé sans emplacement Wi-Fi disponible, l'emplacement sera déterminé en fonction de l'adresse IP, qui est considérablement moins précise.

**Alerte**

Envoyer une alerte à distance sur l'appareil.

La fonctionnalité n'est disponible que sur les appareils mobiles.

**Serrure**

Verrouillez votre ordinateur portable et définissez un code PIN à 4 chiffres pour le déverrouiller. Lorsque vous envoyez le **Serrure** commande, le système redémarre et la reconnexion à Windows n'est possible qu'après avoir entré le code PIN que vous avez défini.

Si vous souhaitez que Bitdefender prenne des photos de celui qui essaie d'accéder à votre ordinateur portable, cochez la case correspondante. Les photos prises sont prises à l'aide de la caméra frontale et affichées avec l'horodatage dans le tableau de bord Antivol. Seules les deux photos les plus récentes seront enregistrées.

Cette action n'est disponible que pour les ordinateurs portables équipés d'une caméra frontale.

**Essuyer**

Supprimez toutes les données de votre système. Lorsque vous envoyez le **Essuyer** commande, l'ordinateur portable redémarre et les données de toutes les partitions du disque dur sont effacées.

**Afficher l'IP**

Affiche la dernière adresse IP du périphérique sélectionné. Cliquez sur **AFFICHER IP** pour le rendre visible.

Antivol est activé après l'installation et est accessible exclusivement via votre compte Bitdefender depuis n'importe quel appareil connecté à Internet, n'importe où.

## Utilisation des fonctionnalités antivol

Pour accéder aux fonctionnalités de l'Antivol, utilisez l'une des possibilités suivantes :

- Depuis l'interface principale de Bitdefender :
  1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
  2. Cliquez sur **ALLER AU CENTRE**.
     Vous êtes redirigé vers la page Bitdefender Central. Assurez-vous que vous êtes connecté avec vos informations d'identification.
  3. Dans la fenêtre Bitdefender Central qui s'ouvre, cliquez sur la carte de l'appareil souhaité, puis sélectionnez **Antivol**.
- Sur n'importe quel appareil avec accès à Internet :
  1. Ouvrez un navigateur Web et accédez 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. Sélectionnez le **Mes appareils** panneau.
  4. Cliquez sur la carte d'appareil souhaitée, puis sélectionnez **Antivol**.
  5. Sélectionnez la fonctionnalité que vous souhaitez utiliser :
     **Localiser** - afficher la position de votre appareil sur Google Maps.
     **Afficher l'IP** - afficher la dernière adresse IP de votre appareil.
     **Alerte** - envoyer une alerte sur l'appareil.
     **Serrure** - verrouillez votre ordinateur portable et définissez un code PIN pour le déverrouiller.
     **Essuyer** - supprimer toutes les données de votre ordinateur portable.

**Important**
Une fois que vous avez effacé un appareil, toutes les fonctions Antivol cessent de fonctionner.

## 3.3. Utilitaires

### 3.3.1. 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 professionnel
- Profil du film
- Profil de jeu
- Profil Réseau Wi-FI public
- Profil du 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 pop-ups 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 contextuelles de Windows sont désactivées.
- Les programmes inutiles en arrière-plan sont interrompus.
- Les effets visuels sont ajustés pour de meilleures performances.
- Les tâches de maintenance sont reportées.
- Les paramètres du plan d'alimentation sont adaptés.

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

- Advanced Threat Defense est activé
- Les paramètres suivants de Online Threat Prevention sont activés :
  - Analyse Web cryptée
  - Protection contre la fraude
  - Protection contre le phishing

## Profil Travail

Effectuer plusieurs tâches au travail comme envoyer des e-mails, lancer une communication vidéo avec des collègues ou utiliser des applications de conception graphique peut affecter les performances de votre système. Le profil Travail est conçu pour vous aider à améliorer votre efficacité en désactivant certaines tâches de maintenance et services d'arrière-plan.

## Configurer le profil Travail

Pour configurer les actions à appliquer lorsque le profil Travail est activé :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Profils** onglet, cliquez **Paramètres**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone profil Travail.
4. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :
   - Améliorer les performances pour les applications de bureautique
   - Optimiser les paramètres du produit pour le profil Travail

- Reporter les tâches de maintenance et les programmes en arrière-plan
- Reporter les mises à jour automatiques de Windows

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

## Ajouter manuellement des applications à la liste du profil Travail

Si Bitdefender ne passe pas automatiquement en profil Travail lorsque vous lancez une application de travail spécifique, vous pouvez ajouter manuellement cette application à la **liste des applications professionnelles**.

Pour ajouter manuellement des applications à la liste des applications professionnelles dans le profil Travail :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Profils** onglet, cliquez **Paramètres**.
3. Clique le **CONFIGURER** dans la zone Profil professionnel.
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.

## Profil Film

Afficher du contenu vidéo de grande qualité comme des films haute définition nécessite d'importantes ressources système. Le profil Film ajuste la configuration du système et du logiciel afin que vous puissiez regarder des films sans interruptions.

## Configurer le profil Film

Pour configurer les actions à appliquer lorsque le profil Film est activé :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.

2. Dans le **Profils** onglet, cliquez **Paramètres**.
3. Cliquez sur le bouton **CONFIGURER** dans la zone profil Film.
4. Choisissez les ajustements 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
   - Différer les programmes en arrière-plan et les tâches de maintenance
   - Différer les mises à jour automatiques de Windows
   - Ajuster les paramètres du plan d'alimentation pour les films
5. Cliquez sur **SAUVEGARDER** pour enregistrer les modifications et fermer la fenêtre.

## Ajouter manuellement des lecteurs vidéo à la liste du profil Film

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

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

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Profils** onglet, cliquez **Paramètres**.
3. Clique le **CONFIGURER** dans la zone Movie Profile.
4. Dans la fenêtre **Paramètres du profil Film**, cliquez sur **Liste des lecteurs**.
5. Cliquez sur **AJOUTER**.
   Une nouvelle fenêtre apparaît. Accédez au fichier exécutable de l'application, sélectionnez-le et cliquez sur **D'ACCORD** pour l'ajouter à la liste.

## Profil Jeu

Pour une meilleure expérience de jeu, il suffit de réduire la charge du système et de diminuer les ralentissements. En associant des techniques

heuristiques comportementales à une liste de jeux connus, Bitdefender détecte automatiquement les jeux en cours d'exécution et optimise les ressources du système afin que vous puissiez profiter pleinement de vos pauses.

## Configurer le profil Jeu

Pour configurer les actions à appliquer lorsque le profil Jeu est activé :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Profils** onglet, cliquez **Paramètres**.
3. Cliquez sur le bouton **Configurer** dans la zone Profil Jeu.
4. Choisissez les ajustements 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
   - Différer les programmes en arrière-plan et les tâches de maintenance
   - Différer les mises à jour automatiques de Windows
   - Ajuster les paramètres du plan d'alimentation pour les jeux
5. Cliquez sur **SAUVEGARDER** pour enregistrer les modifications et fermer la fenêtre.

## Ajouter manuellement des jeux à la Liste des jeux.

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

Pour ajouter manuellement des jeux à la liste des applications de jeu dans le profil Jeu :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Profils** onglet, cliquez **Paramètres**.
3. Clique le **Configurer** dans la zone Profil de jeu.

4. Dans la fenêtre **Paramètres du profil Jeu**, cliquez sur **Liste des jeux**.
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.

## Profil Wi-Fi public

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

## Configurer le profil Wi-Fi public

Pour configurer Bitdefender afin qu'il applique les paramètres du produit en cas de connexion à un réseau sans fil non sécurisé :

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

## Profil Mode batterie

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

## Configurer le mode Batterie

Pour configurer le mode Batterie :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Profils** onglet, cliquez **Paramètres**.
3. Cliquez sur le bouton **Configurer** dans la zone Profil Mode Batterie.
4. Sélectionnez les réglages du système à appliquer en cochant les options suivantes :
   - ❍ Optimiser les paramètres du produit pour le mode Batterie.
   - ❍ Reporter les tâches des programmes en arrière-plan et de maintenance.
   - ❍ Reporter les mises à jour automatiques de Windows.
   - ❍ Ajuster les paramètres du plan d'alimentation pour le mode Batterie.
   - ❍ Désactiver les appareils externes et les ports du réseau.
5. Cliquez sur **SAUVEGARDER** pour enregistrer les modifications et fermer la fenêtre.

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

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

- ❍ La mise à jour automatique de Bitdefender est reportée.
- ❍ Les analyses planifiées sont reportées.

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

## Optimisation en temps réel

Bitdefender propose un plug-in d'optimisation en temps réel qui améliore les performances de votre système en arrière-plan, discrètement, pour ne pas risquer d'interruption lorsqu'un profil est activé. En fonction de la

charge du processeur, ce plug-in surveille l'ensemble des processus et ajuste ceux qui demandent une charge plus élevée, pour les adapter à vos besoins.

Pour activer ou désactiver l'Optimisation en temps réel :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Profils** onglet, cliquez **Paramètres**.
3. Descendez jusqu'à voir l'option d'Optimisation en temps réel, puis utiliser le bouton Activer/Désactiver correspondant.

## 3.3.2. Optimiseur OneClick

Des problèmes tels que les pannes de disque dur, les fichiers de registre restants et l'historique du navigateur peuvent ralentir votre travail, ce qui peut devenir lancinant pour vous. Tous ces problèmes peuvent désormais être résolus en un seul clic sur un bouton.

OneClick Optimizer vous permet d'identifier et de supprimer les fichiers inutiles en exécutant plusieurs tâches de nettoyage en même temps.

Pour démarrer le processus OneClick Optimizer :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Clique le **Optimiser** bouton.
   a. **en cours d'analyse**
   Attendez que Bitdefender ait fini de rechercher les problèmes système.
      - Nettoyage de disque - identifie les fichiers et dossiers inutiles.
      - Nettoyage du registre - identifie les références non valides ou obsolètes dans le registre Windows.
      - Nettoyage de la confidentialité - identifie les fichiers Internet temporaires et les cookies, le cache du navigateur et l'historique.

      Le nombre de problèmes trouvés s'affiche. Cliquez sur le lien Afficher les détails pour les examiner avant de poursuivre le processus de nettoyage. Cliquez sur Optimiser pour continuer.

b. **Optimisation**
Attendez que Bitdefender ait fini d'optimiser votre système.

c. **Questions**
C'est ici que vous pouvez voir le résultat de l'opération.
Si vous souhaitez des informations complètes sur le processus d'optimisation, cliquez sur le **Voir le rapport détaillé** bouton.

## 3.3.3. Protection des données

### 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.

Bitdefender File Shredder vous aide à supprimer définitivement des données en les supprimant physiquement de votre disque dur.

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

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement.
2. Sélectionnez **Bitdefender > File Shredder** dans le menu contextuel qui s'affiche.
3. Cliquez sur **Supprimer de façon permanente**, puis confirmez que vous souhaitez poursuivre cette procédure.
   Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
4. Les résultats sont affichés. Cliquez sur **Terminer** pour quitter l'assistant.

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

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le volet **Protection des données**, cliquez sur **File Shredder**.
3. Suivez les instructions de l'assistant de File Shredder :

a. Cliquez sur le bouton **Ajouter des dossiers** pour ajouter les fichiers ou dossiers que vous souhaitez supprimer définitivement.
   Sinon, glissez-déposez les fichiers ou dossiers vers cette fenêtre.

b. Cliquez sur **Supprimer de façon permanente**, puis confirmez que vous voulez poursuivre cette procédure.
   Attendez que Bitdefender ait fini de détruire les fichiers.

c. **Synthèse des résultats**
   Les résultats sont affichés. Cliquez sur **Finir** pour quitter l'assistant.

# 3.4. Comment faire pour

## 3.4.1. Installation

### Comment installer Bitdefender sur un deuxième appareil ?

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

Pour installer Bitdefender sur un deuxième appareil :

1. Cliquez sur **Installer sur un autre appareil** dans le coin inférieur gauche de l'**interface Bitdefender**.
   Une nouvelle fenêtre apparaît sur votre écran.
2. Cliquez sur **PARTAGER LE LIEN DE TÉLÉCHARGEMENT**.
3. Suivez les instructions qui s'affiche à l'écran pour installer BitDefender.

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

### Comment réinstaller Bitdefender ?

Quelques situations typiques pouvant exiger la réinstallation de 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.

Si vous êtes dans un des cas de figure mentionné, suivez les instructions suivantes :

- Dans **Windows 7**:
  1. Cliquez sur **Commencer** et allez à **Tous les programmes**.
  2. Trouvez *Bitdefender Total Security* et cliquez sur **Désinstaller**.
  3. Cliquez sur **RÉINSTALLER** dans la fenêtre qui s'affiche.
  4. Vous aurez besoin de redémarrer l'appareil pour terminer le processus.

- Dans **Windows 8** et **Windows 8.1**:
  1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
  2. Cliquez sur **Désinstaller** un programme ou **Programmes et fonctionnalités**.
  3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  4. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.
  5. Vous devez redémarrer l'appareil pour terminer le processus.

- Dans **Windows 10** et **Windows 11**:
  1. Cliquez sur **Démarrer**, puis sur **Paramètres**.
  2. Cliquez sur l'icône **Système** dans les paramètres, puis sélectionnez **Applications et fonctionnalités**.
  3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
  5. Cliquez sur **RÉINSTALLER**.
  6. Vous devez redémarrer l'appareil pour terminer le processus.

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

## D'où puis-je télécharger mon produit Bitdefender ?

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

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

Pour installer Bitdefender depuis Bitdefender Central :

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes appareils** panneau, puis cliquez sur **INSTALLER LA PROTECTION**.
3. Choisissez l'une des deux options disponibles :
   - **Protégez cet appareil**
     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
   - **Protégez d'autres appareils**
     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
     Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**. Saisissez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER UN COURRIEL**. Notez que le lien de téléchargement généré n'est valable que pour les prochaines 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes étapes.

Sur l'appareil sur lequel vous souhaitez installer votre produit Bitdefender, vérifiez le compte de messagerie que vous avez saisi, puis cliquez sur le bouton de téléchargement correspondant.

4. Exécutez le produit Bitdefender que vous avez installé.

## 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 ancienne version de Bitdefender, vous pouvez passer gratuitement à la dernière version en date :**

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

**Deux cas de figure sont possibles :**

- 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**, puis sur **Panneau de configuration** et deux fois sur **Programmes et fonctionnalités**.
    2. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
    3. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.
    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. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.
  2. Cliquez sur **Désinstaller un programme** ou **Programmes et fonctionnalités**.
  3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  4. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.
  5. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.
     Ouvrez l'interface de votre nouveau produit Bitdefender installé pour accéder à ses fonctionnalités.

- Dans **Windows 10** et **Windows 11**:
  1. Cliquez sur **Commencer**, puis clique **Paramètres**.
  2. Cliquez sur l'icône **Système** dans les paramètres, puis sélectionnez **Applications**.
  3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  4. Cliquez sur **Désinstaller** à nouveau pour confirmer votre choix.
  5. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.
  6. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.
     Ouvrez l'interface de votre nouveau produit Bitdefender installé pour accéder à ses fonctionnalités.

> **Note**
> En suivant cette procédure de réinstallation, les paramètres personnalisés sont enregistrés et disponibles dans le nouveau produit installé. D'autres paramètres peuvent être ramenés 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. Accès Centrale Bitdefender.
     b. Sélectionnez le **Mes appareils** panneau, puis cliquez sur **INSTALLER LA PROTECTION**.
     c. Choisissez l'une des deux options disponibles :
        - **Protégez cet appareil**
          Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
        - **Protéger un autre appareil**
          Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
          Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**. Saisissez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER UN COURRIEL**. Notez que le lien de téléchargement généré n'est valable que pour les prochaines 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes étapes.
          Sur l'appareil sur lequel vous souhaitez installer votre produit Bitdefender, vérifiez le compte de messagerie que vous avez saisi, puis cliquez sur le bouton de téléchargement correspondant.

  2. Exécutez le produit Bitdefender que vous avez téléchargé.

  Pour plus d'informations sur le processus d'installation de Bitdefender, reportez-vous à Installer votre produit Bitdefender (page 18).

## Comment passer à la dernière version de Bitdefender ?

La mise à jour vers la nouvelle version est désormais possible sans suivre la procédure de désinstallation et réinstallation. Plus exactement, le nouveau produit contenant de nouvelles fonctionnalités et des

améliorations majeures de produits sont diffusé via la mise à jour du produit, et si vous avez déjà un abonnement actif à Bitdefender, le produit s'active automatiquement.

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

1. Cliquez sur **REDÉMARRER MAINTENANT** dans la notification que vous avez reçue avec les informations de mise à jour. Si vous l'avez manqué, rendez-vous dans la fenêtre **Notifications**, sélectionnez la mise à jour la plus récente, puis cliquez sur le bouton **REDÉMARRER MAINTENANT**. Attendez que l'appareil redémarre.
   La fenêtre **Nouveautés** contenant des informations sur les améliorations et nouvelles fonctionnalités apparait.
2. Cliquez sur le lien **En apprendre plus** pour être redirigé vers notre page dédiée avec plus d'informations et d'articles sur le sujet.
3. Fermer la fenêtre **Nouveautés** pour accéder à l'interface de la nouvelle version.

Les utilisateurs qui souhaitent passer gratuitement de Bitdefender 2016 (ou une version antérieure) à 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 : https://www.bitdefender.com/Downloads/. L'activation de cette nouvelle version est possible uniquement avec un abonnement valide.

## 3.4.2. Centrale Bitdefender

### Comment se connecter à un compte Bitdefender depuis un autre compte ?

Vous avez créé un nouveau compte Bitdefender et c'est celui-ci que vous voulez utiliser à partir de maintenant.

Pour vous connecter avec un autre compte Bitdefender :

1. Cliquez sur le nom de votre compte dans la partie supérieure de **l'interface Bitdefender**.
2. Cliquez sur le bouton **Changer de compte** dans le coin supérieur droit pour changer le compte lié à l'appareil.

3. Saisissez l'adresse e-mail dans le champ correspondant, puis cliquez sur **SUIVANT**.
4. Saisissez votre mot de passe, puis cliquez sur **S'IDENTIFIER**.

> **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 Demander de l'aide (page 270).

## Comment désactiver les messages d'aide de 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. Accès Centrale Bitdefender.
2. Clique le icône dans le coin supérieur droit de l'écran.
3. Cliquez sur **Mon compte** dans le menu déroulant.
4. Cliquez sur **Paramètres** dans le menu coulissant.
5. Désactivez l'option **Activer/désactiver les messages d'aide**.

## 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 :

- Du Interface Bitdefender:
  1. Cliquez sur **Mon compte** dans le menu de navigation sur le Interface Bitdefender.
  2. Cliquez sur le bouton **Changer de compte** dans le coin supérieur droit.
     Une nouvelle fenêtre apparaît.
  3. Saisissez votre adresse e-mail puis cliquez sur **SUIVANT**.
     Une nouvelle fenêtre apparaît.

4. Cliquez sur **Mot de passe oublié?**.
5. Cliquez sur **SUIVANT**.
6. Vérifiez votre compte de messagerie, saisissez le code de sécurité que vous avez reçu, puis cliquez sur **SUIVANT**.
   Alternativement, vous pouvez cliquer sur **Changer le mot de passe** dans le mail que nous vous avons envoyé.
7. Saisissez le nouveau mot de passe que vous souhaitez définir, puis saisissez-le à nouveau. Cliquez sur **SAUVEGARDER**.

❍ Depuis votre navigateur Web :

1. Aller à: https://central.bitdefender.com.
2. Cliquez sur **CONNEXION**.
3. Saisissez votre adresse e-mail, puis cliquez sur **SUIVANT**.
4. Cliquez sur **Mot de passe oublié?**.
5. Cliquez sur **SUIVANT**.
6. Allez voir vos emails et suivez les instructions fournies pour configurer un nouveau mot de passe pour votre compte Bitdefender.

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

## 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. Accès Centrale Bitdefender.
2. Clique le icône dans le coin supérieur droit de l'écran.
3. Cliquez sur **Sessions** dans le menu coulissant.
4. Dans la zone **Sessions actives**, sélectionnez l'option **DÉCONNEXION** située à côté de l'appareil dont vous voulez fermer la session.

## 3.4.3. Analyser avec BitDefender

### Comment analyser un fichier ou un dossier ?

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

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

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

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

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

### Comment analyser mon système

Pour réaliser une analyse complète sur le système :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Cliquez sur le bouton **Exécuter l'analyse** à côté d'**Analyse du système**.
4. Suivez les indications de l'Assistant d'analyse du système pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés.
   Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à appliquer. Pour plus d'informations, reportez-vous à .

## Comment programmer une analyse ?

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

Pour programmer une analyse :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Cliquez sur ··· à côté du type d'analyse que vous souhaitez programmer, Analyse du système ou Analyse rapide, dans la partie inférieure de l'interface, puis sélectionnez **Modifier**.
   Vous pouvez aussi créer un type d'analyse qui correspond à vos besoins en cliquant sur **+Créer une analyse** à côté de **Gérer les analyses**.
4. Personnalisez l'analyse en fonction de vos besoins, puis cliquez sur **Suivant**.
5. Cochez la case à côté de **Choisir quand programmer cette tâche**.
   Sélectionnez l'une des options correspondantes pour définir une planification :
   - ❍ Au démarrage du système
   - ❍ Quotidien
   - ❍ Hebdomadaire
   - ❍ Mensuel

   Si vous choisissez Quotidien, Mensuel ou Hebdomadaire, faites glisser le curseur le long de l'échelle pour définir la période souhaitée à laquelle l'analyse planifiée doit démarrer.

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

## Comment créer une tâche d'analyse personnalisée ?

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

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

1. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
2. Cliquez sur **+Créer une analyse** à côté de **Gérer les analyses**.
3. Dans le champ correspondant au nom de la tâche, saisissez un nom pour l'analyse, sélectionnez les emplacements que vous souhaitez analyser, puis cliquez sur **SUIVANT**.
4. Configurez ces options générales :
   - **Analyse des applications uniquement**. Vous pouvez configurer Bitdefender pour que seules les applications utilisées soient analysées.
   - **Priorité de l'analyse**. Vous pouvez choisir un impact qu'aura l'analyse sur les performances de votre système.
     - Auto - La priorité du processus d'analyse dépendra de l'activité du système. Pour s'assurer que le processus d'analyse n'affectera pas l'activité du système, Bitdefender décidera si le processus d'analyse doit être exécuté avec une priorité élevée ou faible.
     - Élevé - La priorité du processus d'analyse sera élevée. En choisissant cette option, vous autorisez d'autres programmes à s'exécuter plus lentement et réduisez le temps nécessaire à la fin du processus d'analyse.
     - Faible - La priorité du processus d'analyse sera faible. En choisissant cette option, vous permettrez à d'autres programmes de s'exécuter plus rapidement et augmenterez le temps nécessaire à la fin du processus d'analyse.
   - **Actions après l'analyse**. Choisissez ce que Bitdefender doit faire si aucune menace n'est détectée.
     - Afficher la fenêtre Résumé
     - Dispositif d'arrêt
     - Fermer la fenêtre de numérisation
5. Si vous souhaitez configurer les options d'analyse en détail, cliquez sur **Afficher les options avancées**.

Cliquez sur **Suivant**.

6. Si vous le souhaitez, vous pouvez activer l'option **Programmer la tâche d'analyse**, puis choisir le moment où l'analyse personnalisée que vous avez créée devra démarrer.
   - ❍ Au démarrage du système
   - ❍ Quotidien
   - ❍ Mensuel
   - ❍ Hebdomadaire

   Si vous choisissez Quotidien, Mensuel ou Hebdomadaire, faites glisser le curseur le long de l'échelle pour définir la période souhaitée à laquelle l'analyse planifiée doit démarrer.
7. Cliquez sur **Sauvegarder** pour enregistrer les paramètres et fermer la fenêtre de configuration.
   Selon les emplacements à analyser, l'analyse peut prendre un certain temps. Si des menaces sont détectées pendant le processus d'analyse, vous serez invité à choisir les actions à entreprendre sur les fichiers détectés.

Si vous le souhaitez, vous pouvez relancer rapidement une analyse personnalisée en cliquant sur le bouton correspondant dans la liste.

## Comment exclure un dossier de l'analyse ?

Bitdefender permet d'exclure des fichiers, dossiers ou extensions de fichiers spécifiques de l'analyse.

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 des exceptions :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Cliquez sur l'onglet **Paramètres**.
4. Cliquez sur **Gérer les exceptions**.
5. Cliquez sur **+Ajouter une exception**.
6. Entrez le chemin du dossier que vous souhaitez exclure de l'analyse dans le champ correspondant.
   Alternativement, vous pouvez naviguer jusqu'au dossier en cliquant sur le bouton Parcourir sur le côté droit de l'interface, le sélectionner et cliquer sur **D'ACCORD**.
7. Activez le commutateur à côté de la fonction de protection qui ne doit pas analyser le dossier. Il y a trois options :
   - antivirus
   - Prévention des menaces en ligne
   - Défense avancée contre les menaces
8. Cliquez sur **Sauvegarder** pour enregistrer les modifications et fermer la fenêtre.

## Que faire lorsque Bitdefender a signalé qu'un fichier sain était infecté ?

Il peut arriver que Bitdefender identifie par erreur un fichier sain comme une menace (c'est ce qu'on appelle un faux positif). Pour corriger cette erreur, ajoutez ce fichier à la liste des exceptions Bitdefender.

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
   b. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
   c. Dans la fenêtre **Paramètres avancés**, désactivez **Bitdefender Shield**.
      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. Affichez les objets masqués dans Windows. Pour savoir comment procéder, reportez-vous à Comment afficher des objets cachés dans Windows ? (page 129).
3. Restaurez le fichier à partir de la zone de quarantaine :
   a. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
   b. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
   c. Dans la fenêtre **Paramètres**, cliquez sur **Gérer les exceptions**.
   d. Sélectionnez le fichier, puis cliquez sur **Restaurer**.
4. Ajoutez le fichier à la liste des exceptions. Pour savoir comment procéder, reportez-vous à Comment exclure un dossier de l'analyse ? (page 115).
5. Activez la protection antivirus en temps réel de Bitdefender.
6. Contactez notre service d'assistance technique afin que nous puissions supprimer détection de la mise à jour d'information sur les menaces. Pour savoir comment procéder, reportez-vous à Demander de l'aide (page 270).

## 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 ultérieurement un journal d'analyse ou toute infection détectée :

1. Cliquez sur **Avis** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Tous** , sélectionnez la notification concernant la dernière analyse.
   C'est là que vous pouvez trouver tous les événements d'analyse des menaces, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par l'utilisateur et les changements d'état pour les analyses automatiques.
3. Dans la liste des notifications, vous pouvez vérifier quelles analyses ont été effectuées récemment. Cliquez sur une notification pour afficher les détails la concernant.
4. Pour ouvrir un journal d'analyse, cliquez sur **Afficher le journal**.

## 3.4.4. Contrôle de la vie privée

### Comment vérifier si ma transaction en ligne est sécurisée ?

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

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

Pour garder vos activités en ligne privées et en sécurité :

1. Cliquez sur **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **SAFEPAY** volet, cliquez sur **Paramètres**.
3. Dans le **Safepay** fenêtre, cliquez **Lancer Safepay**.
4. Cliquez sur le bouton pour accéder au **clavier virtuel**.
   Utilisez le **clavier virtuel** lorsque vous tapez des informations confidentielles telles que des mots de passe.

## Que faire si mon périphérique a été volé ?

Le vol d'appareils mobiles, qu'il s'agisse de téléphones intelligents, de tablettes ou d'ordinateurs portables est l'un des principaux problèmes affectant actuellement les particuliers et les entreprises dans le monde.

L'Antivol Bitdefender vous permet de localiser et de verrouiller l'appareil volé mais également d'effacer toutes ses données afin d'empêcher que celles-ci ne soient utilisées par le voleur.

Pour accéder aux fonctionnalités antivol à partir de votre compte :

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes appareils** panneau.
3. Cliquez sur la carte appareil souhaitée, puis sélectionnez **Antivol**.
4. Sélectionnez la fonctionnalité que vous souhaitez utiliser :
   - **LOCALISER** - permet d'afficher la localisation de votre appareil sur Google Maps.
     **Afficher IP** - affiche la dernière adresse IP pour l'appareil sélectionné.
   - **Alerter** - envoie une alerte sur un appareil.
   - **Verrouiller** - verrouille votre appareil et définit un code PIN numérique permettant de le déverrouiller. Vous pouvez également activer l'option correspondante pour autoriser Bitdefender à prendre des photos de la personne qui essaie d'accéder à votre appareil.
   - **Effacer** - supprimez toutes les données de votre appareil.

     **Important**
     Une fois les données d'un appareil effacées, toutes les fonctionnalités d'Antivol cessent de fonctionner.

## 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.

Bitdefender File Shredder vous aide à détruire rapidement des fichiers ou des dossiers se trouvant sur votre appareil à l'aide du menu contextuel de Windows, en procédant comme suit :

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement, sélectionnez Bitdefender puis **File Shredder**.
2. Cliquez sur **supprimer définitivement**, puis confirmez que vous souhaitez poursuivre le processus.
   Attendez que Bitdefender ait fini de détruire les fichiers.
3. Les résultats sont affichés. Cliquez sur **TERMINER** pour quitter l'assistant.

## 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 **Confidentialité** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PROTECTION VIDÉO & AUDIO** volet, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Webcam Protection** pour voir la liste des applications ayant demandé à accéder à votre caméra.
4. Sélectionnez l'application à laquelle vous souhaitez autoriser ou interdire l'accès, puis cliquez sur l'interrupteur représenté par une caméra vidéo, situé à côté de celle-ci.
   Pour voir ce que les autres utilisateurs de Bitdefender ont choisi de faire avec l'application sélectionnée, cliquez sur l'icône . Vous recevez une notification à chaque fois qu'une des applications recensées est bloquée par les utilisateurs de Bitdefender.

Pour ajouter manuellement des applications à cette liste, cliquez sur le bouton **Ajouter une application** et sélectionnez l'une des deux options.

- Depuis Windows Store
- Depuis vos applications

### 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 **Avis** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **Tous** , sélectionnez la notification concernant le dernier comportement de rançongiciel détecté, puis cliquez sur **Fichiers cryptés**.
3. La liste des fichiers cryptés s'affiche.
   Cliquez sur **Récupérer des fichiers** pour continuer.
4. En cas d'échec de tout ou partie du processus de restauration, vous devez choisir l'emplacement où les fichiers décryptés doivent être enregistrés. Cliquez sur **Restaurer l'emplacement**, puis choisissez un emplacement sur votre PC.
5. Une fenêtre de confirmation apparaît.
   Cliquez sur **Finir** pour terminer le processus de restauration.

Les fichiers avec les extensions suivantes peuvent être restaurés au cas où ils seraient 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;

## 3.4.5. Outils d'optimisation

### Comment puis-je améliorer les performances de mon système ?

Les performances du système ne dépendent pas seulement de la configuration matérielle, telle que la charge du processeur, l'utilisation de la mémoire et l'espace disque. Il est également directement connecté à votre configuration logicielle et à la gestion de vos données.

Voici les principales actions que vous pouvez effectuer avec Bitdefender pour améliorer la vitesse et les performances de votre système :

- ❍ Optimisez les performances de votre système en un seul clic (page 122)
- ❍ Analysez votre système périodiquement (page 122)

## Optimisez les performances de votre système en un seul clic

L'option OneClick Optimizer vous fait gagner un temps précieux lorsque vous souhaitez améliorer rapidement les performances de votre système en analysant, détectant et nettoyant rapidement les fichiers inutiles.

Pour démarrer le processus OneClick Optimizer :

1. Cliquez sur **Utilitaires** dans le menu de navigation sur le Interface Bitdefender.
2. Clique le **Optimiser** bouton.
3. Laissez Bitdefender rechercher les fichiers pouvant être supprimés, puis cliquez sur le **Optimiser** bouton pour terminer le processus.

## Analysez votre système périodiquement

La vitesse de votre système et son comportement général peuvent également être affectés par des menaces.

Assurez-vous de scanner votre système périodiquement, au moins une fois par semaine.

Il est recommandé d'utiliser l'analyse du système car elle analyse tous les types de menaces mettant en danger la sécurité de votre système et analyse également l'intérieur des archives.

Pour démarrer l'analyse du système :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Cliquez sur **Exécuter l'analyse** près de **Analyse du système**.
4. Suivez les étapes de l'assistant.

## 3.4.6. Informations utiles

### 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 depuis la page officielle de l'organisation EICAR : http://www.eicar.org/.
2. Cliquez sur l'onglet **Fichier test antimalware**.
3. Cliquez sur **Télécharger** dans le menu de gauche.
4. Dans **zone de téléchargement utilisant le protocole HTTP standard** cliquez sur le fichier de test **eicar.com**.
5. Vous serez informé que la page à laquelle vous essayez d'accéder contient « EICAR-Test-File (not a threat) ».
   Si vous cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**, le téléchargement du test débutera et une fenêtre contextuelle de Bitdefender vous indiquera qu'une menace a été détectée.
   Cliquez sur **Plus de détails** pour obtenir plus d'informations sur cette action.

Si vous ne recevez pas d'alerte Bitdefender, nous vous recommandons de contacter Bitdefender pour obtenir de l'aide comme indiqué dans la rubrique Demander de l'aide (page 270).

### Comment supprimer Bitdefender ?

Si vous souhaitez supprimer {1}{2} :

❍ Dans **Windows 7**:

1. Cliquez sur **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.
2. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
3. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.

4. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

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

  1. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.
  2. Cliquez sur **Désinstaller un programme** ou **Programmes et fonctionnalités**.
  3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  4. Cliquez sur **RETIRER** dans la fenêtre qui apparaît.
  5. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

- Dans **Windows 10** et **Windows 11**:

  1. Cliquez sur **Démarrer**, puis sur Paramètres.
  2. Clique le **Système** icône dans la zone Paramètres, puis sélectionnez **applications**.
  3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  4. Cliquez sur **Désinstaller** à nouveau pour confirmer votre choix.
  5. Cliquez sur **RETIRER** dans la fenêtre qui apparaît.
  6. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

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

## Comment supprimer Bitdefender VPN ?

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

- Dans **Windows 7**:

1. Cliquez sur **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.
2. Trouvez **Bitdefender VPN** et sélectionnez **Désinstaller**.
   Patientez jusqu'à la fin du processus de désinstallation.

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

  1. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.
  2. Cliquez sur **Désinstaller** un programme ou **Programmes et fonctionnalités**.
  3. Trouver **VPN Bitdefender** et sélectionnez **Désinstaller**.
     Attendez que le processus de désinstallation soit terminé.

- Dans **Windows 10** et **Windows 11**:

  1. Cliquez sur **Commencer**, puis cliquez sur Paramètres.
  2. Cliquez sur l'icône **Système** dans les paramètres, puis sélectionnez **Applications installées**.
  3. Trouver **VPN Bitdefender** et sélectionnez **Désinstaller**.
  4. Cliquez sur **Désinstaller** à nouveau pour confirmer votre choix.
     Attendez que le processus de désinstallation soit terminé.

## Comment supprimer l'extension Bloqueur de traceurs de Bitdefender ?

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

- Internet Explorer

  1. Cliquez sur à côté de la barre de recherche, puis sur Gestion des modules complémentaires. Une liste des extensions installées s'affiche.
  2. Cliquez sur Bloqueur de traceurs Bitdefender.
  3. Cliquez sur **Désactiver** en bas à droite.

- Google Chrome

  1. Cliquez sur l'icône ⋮ à côté de la barre de recherche.
  2. Sélectionnez **Outils supplémentaires**, puis **Extensions**.
     Une liste des extensions installées apparait.
  3. Cliquez sur **Supprimer** sur la fiche du Bloqueur de traceurs Bitdefender.
  4. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.

- MozillaFirefox

  1. Cliquez sur ≡ à côté de la barre de recherche.
  2. Sélectionnez **Modules supplémentaires**, puis **Extensions**.
     Une liste avec les extensions installées apparaît.
  3. Cliquez sur ≡ puis sur **Supprimer**.

## Comment éteindre automatiquement l'appareil une fois l'analyse terminée ?

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

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

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

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

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Dans la fenêtre **Analyses**, cliquez sur ··· à côté d'Analyse rapide ou Analyse du système puis sur **Modifier**.

4. Personnalisez l'analyse en fonction de vos besoins puis cliquez sur **Suivant**.
5. Cochez la case située à côté de **Choisir quand programmer cette tâche**, puis choisissez quand la tâche devra démarrer.
   Si vous choisissez Quotidien, Mensuel ou Hebdomadaire, faites glisser le curseur le long de l'échelle pour définir la période souhaitée à laquelle l'analyse planifiée doit démarrer.
6. Cliquez sur **Sauvegarder**.

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

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

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

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à appliquer. Pour plus d'informations, reportez-vous à Assistant d'analyse antivirus (page 37).

## Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?

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

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

Pour gérer les paramètres du proxy :

1. Cliquez sur **Paramètres** dans le menu de navigation sur le Interface Bitdefender.

2. Sélectionnez le **Avancé** languette.
3. Activez **Serveur proxy**.
4. Cliquez sur **Modification du 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:
     - **Addresse** - 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.

## 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. Trouvez **Ordinateur** dans le menu **Démarrer**.
3. Faites un clic droit sur **Ordinateur** puis 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.
  2. Sélectionnez **Propriétés** dans le menu inférieur.
  3. Regardez sous Système pour connaître le type de système.
- Dans **Windows 10** et **Windows 11**:
  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.

## 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** puis ouvrez le **Panneau de configuration**.
   Sur **Windows 8** et **Windows 8.1** : sur 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. Ouvrez l'onglet **Affichage**.
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** et **Windows 11**:

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. Clair **Masquer les extensions des types de fichiers connus**.
4. Clair **Masquer les fichiers protégés du système**.
5. Cliquez sur **Appliquer**, puis clique **D'ACCORD**.

## Comment supprimer les autres solutions de sécurité ?

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

Lorsque vous utilisez plusieurs solutions de sécurité sur le même appareil, le système devient instable. Le programme de désinstallation de Bitdefender Total 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 **Commencer**, aller à **Panneau de commande** et double-cliquez **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 que le processus de désinstallation soit terminé, puis redémarrez votre système.

- Dans **Windows 8** et **Windows 8.1**:
  1. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer

à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.

2. Cliquez sur **Désinstaller un programme** ou **Programmes et fonctionnalités**.
3. Attendez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
4. Recherchez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
5. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

- Dans **Windows 10** et **Windows 11**:

1. Cliquez sur **Commencer**, puis cliquez sur Paramètres.
2. Clique le **Système** icône dans la zone Paramètres, puis sélectionnez **applications**.
3. Recherchez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
4. Cliquez sur **Désinstaller** à nouveau pour confirmer votre choix.
5. Attendez que le processus de désinstallation soit terminé, 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.

## Comment redémarrer en mode sans échec ?

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

Pour démarrer Windows en mode sans échec :

- Dans **Windows 7**:
  1. Redémarrez l'appareil.
  2. Appuyez plusieurs fois sur la touche **F8** avant que Windows ne démarre afin d'accéder au menu de démarrage.
  3. Sélectionnez **Mode sans échec** dans le menu de démarrage ou **Mode sans échec avec prise en charge réseau** si vous souhaitez avoir accès à internet.
  4. Cliquez sur **Entrée** et patientez pendant que Windows se charge en mode sans échec.
  5. Ce processus se termine avec un message de confirmation. Cliquez sur **OK** pour valider.
  6. Pour démarrer Windows normalement, il suffit de redémarrer le système.

- Sur **Windows 8**, **Windows 8.1**, **Windows 10** et **Windows 11**:
  1. Lancez **Configuration système** dans Windows en appuyant simultanément sur les touches **Windows et R** de votre clavier.
  2. Tapez **msconfig** dans la boîte de dialogue **Ouvrir** puis cliquez sur **OK**.
  3. Cliquez sur l'onglet **Démarrer**.
  4. Dans la zone **Options de démarrage**, cochez la case **Démarrage sécurisé**.
  5. Cliquez sur **Réseau** puis sur **OK**.
  6. Cliquez sur **OK** dans la fenêtre **Configuration système** qui vous informe que le système doit être redémarré pour que les changements soient appliqués.
     Votre système redémarre en mode sans échec avec prise en charge réseau.

Pour redémarrer en mode normal, modifiez les paramètres en lançant de nouveau **Configuration système** et en décochant la case **Démarrage sécurisé**. Cliquez sur **OK** puis sur **Redémarrer**. Patientez pendant l'application des nouveaux paramètres.

# 3.5. Résolution de problèmes

## 3.5.1. Résoudre les problèmes les plus fréquents

Ce chapitre présente certains problèmes que vous pouvez rencontrer en utilisant BitDefender et vous fournit des solutions possibles à ces problèmes. La plupart de ces problèmes peuvent être résolus par une configuration appropriée des paramètres du produit.


- Mon système semble lent (page 133)
- L'analyse ne démarre pas (page 135)
- Je ne peux plus utiliser une application (page 137)
- Que faire quand Bitdefender bloque un site web, un domaine, une adresse IP ou une application en ligne pourtant sûr ? (page 139)
- Comment mettre à jour Bitdefender avec une connexion internet lente ? (page 144)
- Les services Bitdefender ne répondent pas (page 144)
- La désinstallation de Bitdefender a échoué (page 150)
- Mon système ne démarre pas après l'installation de Bitdefender (page 151)


Si votre problème n'est pas évoqué ici, ou si les solutions proposées ne permettent pas de le régler, vous pouvez contacter le support technique BitDefender comme indiqué dans le chapitre {1}{2}.

### 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 ? (page 130).

- **Vous ne disposez pas de la configuration système minimale pour l'exécution de Bitdefender.**
  Si votre machine ne dispose pas de la configuration système minimale, l'appareil deviendra lent, notamment lorsque plusieurs applications s'exécuteront simultanément. Pour plus d'informations, reportez-vous à Configuration requise (page 16).

- **Vous avez installé des applications que vous n'utilisez pas.**
  Tout appareil possède des programmes ou des applications que vous n'utilisez pas. Et de nombreux programmes indésirables s'exécutent en tâche de fond, utilisant de l'espace disque et de la mémoire. Si vous n'utilisez pas un programme, désinstallez-le. Cela s'applique également à tout autre logiciel préinstallé ou version d'évaluation d'une application que vous avez oublié de désinstaller.

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

- **Votre système peut être infecté.**
  La rapidité et le comportement général de notre système peuvent également être modifiés par les menaces. Les spywares, les malwares, les chevaux de Troie et les adwares peuvent nuire aux performances de votre système. Réalisez régulièrement des analyses, au moins une fois par semaine. L'analyse du système Bitdefender est recommandée car elle recherche tous les types de menaces qui mettent en danger votre système.
  Pour commencer l'analyse du système :

  1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
  2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
  3. Dans la fenêtre **Analyses**, cliquez sur le bouton **Exécuter l'analyse** à côté d'**Analyse du système**.
  4. Suivez les étapes de l'assistant.

## 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 **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.
    2. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
    3. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.
    4. Attendez la fin du processus de réinstallation, puis redémarrez votre système.
  - Dans **Windows 8** et **Windows 8.1**:
    1. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.
    2. Cliquez sur **Désinstaller** un programme ou **Programmes et fonctionnalités**.
    3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
    4. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.
    5. Attendez que le processus de réinstallation soit terminé, puis redémarrez votre système.
  - Dans **Windows 10** et **Windows 11**:
    1. Cliquez sur **Commencer**, puis clique **Paramètres**.
    2. Clique le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.

3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
4. Cliquez sur **Désinstaller** à nouveau pour confirmer votre choix.
5. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.
6. Attendez que le processus de réinstallation soit terminé, puis redémarrez votre système.

> **Note**
> En suivant cette procédure de réinstallation, les paramètres personnalisés sont enregistrés et disponibles dans le nouveau produit installé. D'autres paramètres peuvent être ramenés 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 ? (page 130).
  2. Réinstallez Bitdefender :
     - Dans **Windows 7**:
       a. Cliquez sur **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.
       b. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
       c. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.
       d. Attendez que le processus de réinstallation soit terminé, puis redémarrez votre système.
     - Dans **Windows 8** et **Windows 8.1**:
       a. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.

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

c. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.

d. Cliquez sur **RÉINSTALLER** dans la fenêtre qui apparaît.

e. Attendez que le processus de réinstallation soit terminé, puis redémarrez votre système.

❍ Dans **Windows 10** et **Windows 11**:

a. Cliquez sur **Commencer**, puis clique **Paramètres**.

b. Clique le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.

c. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.

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

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

f. Attendez que le processus de réinstallation soit terminé, puis redémarrez votre système.

> **Note**
> En suivant cette procédure de réinstallation, les paramètres personnalisés sont enregistrés et disponibles dans le nouveau produit installé. D'autres paramètres peuvent être ramenés à leur configuration par défaut.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support BitDefender comme indiqué dans la rubrique Demander de l'aide (page 270).

## 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 cette fonctionnalité est basée sur un système heuristique, elle peut dans certains cas signaler des applications légitimes.

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 des exceptions :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **DÉFENSE AVANCÉE CONTRE LES MENACES** volet, cliquez sur **Ouvrir**.
3. Dans le **Paramètres** fenêtre, cliquez **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Saisissez le chemin de l'exécutable que vous souhaitez exclure de l'analyse dans le champ correspondant.
   Alternativement, vous pouvez accéder à l'exécutable en cliquant sur le bouton Parcourir sur le côté droit de l'interface, le sélectionner et cliquer sur **D'ACCORD**.
6. Allumez l'interrupteur à côté de **Défense avancée contre les menaces**.
7. Cliquez sur **Sauvegarder**.

Si ces informations ne vous ont pas été utiles, vous pouvez contacter Bitdefender pour obtenir de l'aide, comme décrit dans la section Demander de l'aide (page 270).

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

Bitdefender garantit une expérience de navigation sécurisée en filtrant l'intégralité du trafic web pour bloquer les contenus malveillants. Toutefois, il peut arriver Bitdefender considère à tort qu'un site, un domaine, une adresse IP ou une application en ligne présente un danger. Dans ce cas, l'analyse du trafic http de Bitdefender bloquera ces éléments par erreur.

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

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

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PRÉVENTION DES MENACES EN LIGNE** volet, cliquez sur **Paramètres**.
3. Cliquez sur **Gérer les exceptions**.
4. Cliquez sur **+Ajouter une exception**.
5. Tapez dans le champ correspondant le nom du site Web, le nom du domaine ou l'adresse IP que vous souhaitez ajouter aux exceptions.
6. Cliquez sur le commutateur à côté de **Prévention des menaces en ligne**.
7. Cliquez sur **Sauvegarder** pour enregistrer les modifications et fermer la fenêtre.

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

Si ces informations ne vous ont pas été utiles, vous pouvez contacter Bitdefender pour obtenir de l'aide, comme décrit dans la section Demander de l'aide (page 270).

## 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 sur le Interface Bitdefender.
2. Dans le **PARE-FEU** volet, cliquez sur **Paramètres**.
3. Dans le **Règles** fenêtre, cliquez **Ajouter une règle**.
4. Une nouvelle fenêtre s'ouvre, dans laquelle vous pouvez ajouter des détails. Sélectionnez tous les types de réseaux disponibles et dans la rubrique **Autorisation** cliquez sur **Autoriser**.

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

Si ces informations ne vous ont pas été utiles, vous pouvez contacter Bitdefender pour obtenir de l'aide, comme décrit dans la section Demander de l'aide (page 270).

## 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, en procédant comme suit :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **PARE-FEU** volet, cliquez sur **Paramètres**.
3. Dans le **Règles** fenêtre, cliquez **Ajouter une règle**.
4. Activez l'option **Appliquer cette règle à toutes les applications**.

5. Cliquez sur **Paramètres avancés**.
6. Dans la case **Adresse distante personnalisée**, saisissez l'adresse IP de l'ordinateur ou de l'imprimante auquel ou à laquelle vous souhaitez 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 présent sur l'autre appareil peut bloquer le partage de fichiers et d'imprimantes avec votre ordinateur.
  - 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**, ouvrez le **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. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.
      2. Cliquez sur **Système et sécurité**, allez dans **Pare-feu Windows** puis cliquez sur **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** et **Windows 11**:
      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 **Modifier les paramètres**.

3. Dans la liste des **Applications et fonctionnalités autorisées**, cochez la case **Partage de fichiers et d'imprimantes** 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 :
  - Vous devrez peut-être 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 appareils et utilisateurs. Si vous partagez votre imprimante, vérifiez que l'imprimante autorise l'accès à l'utilisateur de l'autre appareil. Si vous essayez de vous connecter à une imprimante partagée, vérifiez avec l'utilisateur de l'autre appareil que vous êtes autorisé(e) à vous connecter à l'imprimante.
  - L'imprimante connectée à votre appareil ou à l'autre appareil n'est pas partagée.
  - L'imprimante partagée n'a pas été ajoutée à l'appareil.

    **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 soutien de Windows (dans le menu Démarrer, cliquez sur **Aide et soutien**).

- L'accès à une imprimante réseau peut être limité à des appareils 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 été utiles, vous pouvez contacter Bitdefender pour obtenir de l'aide, comme décrit dans la section Demander de l'aide (page 270).

## Ma connexion Internet est lente

Cette situation peut se produire après l'installation de Bitdefender. Ce problème peut 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 sur le Interface 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 rubrique Demander de l'aide (page 270).
   - ❍ Si la connexion internet s'est améliorée après la désactivation du pare-feu Bitdefender :
     a. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
     b. Dans le **PARE-FEU** volet, cliquez sur **Paramètres**.
     c. Rendez-vous dans l'onglet **Adaptateurs réseau** et réglez votre connexion Internet sur **Domicile/Bureau**.
     d. Dans l'onglet **Paramètres**, désactivez **Protection lors de l'analyse des ports**.
        Dans la rubrique **Mode furtif**, cliquez sur **Modifier les paramètres du mode furtif**. 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 été utiles, vous pouvez contacter Bitdefender pour obtenir de l'aide, comme décrit dans la section Demander de l'aide (page 270).

## 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 sur le Interface Bitdefender.
2. Sélectionnez le **Mise à jour** languette.
3. Activez le bouton **Mise à jour silencieuse**.
4. Lorsqu'une nouvelle mise à jour sera disponible, il vous sera demandé d'indiquer quelle mise à jour vous souhaitez 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.

## Les 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 un message vous informe que les services Bitdefender ne répondent pas.
- La fenêtre BitDefender indique que les services BitDefender ne répondent pas.

L'erreur peut être causée par :

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

Pour réparer cette erreur, essayez ces solutions :

1. Attendez quelques instants et voyez si quelque chose change. L'erreur peut être temporaire.
2. Redémarrez l'appareil et attendez quelques instants jusqu'à ce que Bitdefender soit chargé. Ouvrez BitDefender pour voir si l'erreur persiste. Redémarrer l'appareil règle habituellement le problème.
3. Vérifiez que vous n'avez pas d'autre solution de sécurité installée car cela pourrait affecter le fonctionnement normal de BitDefender. Si c'est le cas, nous vous recommandons de supprimer toutes les autres solutions de sécurité et de réinstaller ensuite BitDefender.
   Pour plus d'informations, reportez-vous à Comment supprimer les autres solutions de sécurité ? (page 130).

Si l'erreur persiste, veuillez contacter les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la rubrique Demander de l'aide (page 270).

## 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 spams ne sont pas signalés comme tels par le filtre antispam.**
- **Le filtre antispam ne détecte aucun spam.**

## Des messages légitimes sont signalés comme étant du [spam]

Des messages légitimes peuvent être marqués comme [spam] par le filtre antispam de Bitdefender car ils ressemblent à des spams. Vous pouvez généralement résoudre ce problème en modifiant la configuration du filtre antispam.

Bitdefender ajoute automatiquement les destinataires de vos e-mails à votre liste d'amis. Les messages provenant de contacts figurant dans cette liste d'amis sont considérés comme légitimes. Ils ne sont pas traités par le filtre antispam et ne sont donc jamais marqués comme [spam].

La configuration automatique de la liste des 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

d'ajouter les adresses des expéditeurs de ces messages à la liste des amis.

- Une part importante des e-mails légitimes que vous recevez provient de personnes auxquelles vous n'avez jamais envoyé de messages auparavant, comme des clients, des partenaires commerciaux potentiels, etc. D'autres solutions sont requises dans ce cas.

Si vous utilisez l'un des clients de messagerie compatibles avec Bitdefender, **indiquez les erreurs de détection**.

> **Note**
> Bitdefender s'intègre aux clients de messagerie les plus couramment utilisés via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, reportez-vous à Clients et protocoles de messagerie pris en charge (page 55).

**Ajouter des contacts à la liste des amis**

Si vous utilisez un client de messagerie pris en charge vous pouvez facilement ajouter les expéditeurs d'e-mails légitimes à la liste des amis, en procédant comme suit :

1. Dans votre client de messagerie, sélectionnez un e-mail provenant de l'expéditeur que vous voulez ajouter à la liste des amis.
2. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils Bitdefender Antispam.
3. Il vous sera peut-être demandé de valider les adresses ajoutées à la liste des 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 des amis à partir de l'interface de Bitdefender. Pour cela, suivez les instructions ci-dessous :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le volet **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 que vous le souhaitez.
4. Cliquez sur **D'ACCORD** pour enregistrer les modifications et fermer la fenêtre.

**Indiquer les 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. Pour cela, suivez les étapes ci-dessous :

1. Ouvrez votre client de messagerie.
2. Accédez au dossier de courrier indésirable dans lequel les messages de spam sont déplacés.
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 des amis. Il vous sera peut-être demandé de cliquer sur **OK** pour confirmer. Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.
5. Clique le **Pas de spam** dans la barre d'outils antispam de Bitdefender (normalement situé dans la partie supérieure de la fenêtre du client de messagerie). Le message électronique sera déplacé vers le dossier Boîte de réception.

## De nombreux spams ne sont pas détectés

Si vous recevez de nombreux spams 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 compatibles avec Bitdefender, **indiquez les spams non détectés**.

> **Note**
> Bitdefender s'intègre aux clients de messagerie les plus couramment utilisés via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, reportez-vous à Clients et protocoles de messagerie pris en charge (page 55).

2. **Ajouter des spammeurs à la liste des spammeurs**. Les e-mails provenant de messages figurant dans cette liste sont automatiquement marqués comme [spam].

**Indiquer les spams non détectés**

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

1. Ouvrez votre client de messagerie.
2. Accédez au dossier Boîte de réception.
3. Sélectionnez les spams non détectés.
4. Cliquez sur le bouton **Est un spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Les messages sont immédiatement marqués comme des [spams] et sont placés dans le dossier 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 spams à la liste des spammeurs. Pour cela, suivez les étapes ci-dessous :

1. Ouvrez votre client de messagerie.
2. Accédez au dossier de courrier indésirable dans lequel les messages de spam sont déplacés.
3. Sélectionnez les messages signalés comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter un spammeur** de la barre d'outils Bitdefender Antispam.

5. Il vous sera peut-être demandé de valider les adresses ajoutées à la liste des amis. 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 spams provenant de la même adresse e-mail. Dans ce cas, suivez les étapes ci-dessous :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTI-SPAM** volet, cliquez sur **Paramètres**.
3. Ouvrez la fenêtre **Gérer les spammeurs**.
4. Tapez l'adresse e-mail du spammeur puis cliquez sur **Ajouter**. Vous pouvez ajouter autant d'adresses que vous le souhaitez.
5. Cliquez sur **D'ACCORD** pour enregistrer les modifications et fermer la fenêtre.

## 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 est peut-être désactivée. Pour vérifier l'état de la protection antispam, cliquez sur **Protection** dans le menu de navigation de **l'interface Bitdefender**. Consultez le volet **Antispam** pour vérifier que la fonctionnalité est activée.
  Si l'antispam est désactivé, c'est de là que vient votre problème. Cliquez sur le bouton correspondant pour activer votre protection antispam.
- La protection antispam de Bitdefender est disponible seulement pour les clients de messagerie configurés pour recevoir des e-mails via le protocole POP3. Voici ce que cela signifie :
  - Les e-mails reçus via des services web (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 le filtre antispam Bitdefender.

  **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 Total Security n'analyse pas le trafic POP3 de Lotus Notes.

Une solution possible consiste à réparer ou à réinstaller le produit. Cependant, si vous le souhaitez, vous pouvez contacter le support BitDefender, comme indiqué dans la rubrique Demander de l'aide (page 270).

## 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. Ces fichiers restants 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 **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.
  2. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  3. Cliquez sur **RETIRER** dans la fenêtre qui apparaît.
  4. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

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

1. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou **Programmes et fonctionnalités**.
3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
4. Cliquez sur **RETIRER** dans la fenêtre qui apparaît.
5. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

- Dans **Windows 10** et **Windows 11**:
  1. Cliquez sur **Commencer**, puis cliquez sur Paramètres.
  2. Clique le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.
  3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  4. Cliquez sur **Désinstaller** à nouveau pour confirmer votre choix.
  5. Cliquez sur **RETIRER** dans la fenêtre qui apparaît.
  6. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

## 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 utilisiez Bitdefender auparavant et vous ne l'avez pas supprimé correctement.**
  Pour résoudre ce problème :

1. Redémarrez votre système en mode sans échec. Pour savoir comment procéder, reportez-vous à Comment redémarrer en mode sans échec ? (page 131).
2. Désinstallez Bitdefender de votre système.
   - Dans **Windows 7**:
     a. Cliquez sur **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.
     b. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
     c. Cliquez sur **RETIRER** dans la fenêtre qui apparaît.
     d. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.
     e. Redémarrez votre système en mode normal.
   - Dans **Windows 8** et **Windows 8.1**:
     a. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.
     b. Cliquez sur **Désinstaller un programme** ou **Programmes et fonctionnalités**.
     c. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
     d. Cliquez sur **RETIRER** dans la fenêtre qui apparaît.
     e. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.
     f. Redémarrez votre système en mode normal.
   - Dans **Windows 10** et **Windows 11**:
     a. Cliquez sur **Commencer**, puis cliquez sur Paramètres.
     b. Clique le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.

c. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.

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

e. Cliquez sur **RETIRER** dans la fenêtre qui apparaît.

f. Attendez que le processus de désinstallation soit terminé, 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 résoudre ceci :

  1. Redémarrez votre système et entrez en mode sans échec. Pour savoir comment procéder, reportez-vous à Comment redémarrer en mode sans échec ? (page 131).
  2. Désinstallez l'autre solution de sécurité de votre système :
     - Dans **Windows 7**:

       a. Cliquez sur **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.

       b. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

       c. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

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

       a. À partir de l'écran de démarrage de Windows, localisez **Panneau de commande** (par exemple, vous pouvez commencer à taper "Panneau de configuration" directement dans l'écran de démarrage), puis cliquez sur son icône.

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

c. Recherchez le nom du programme que vous souhaitez supprimer et sélectionnez **Retirer**.

d. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

- Dans **Windows 10** et **Windows 11**:

  a. Cliquez sur **Commencer**, puis cliquez sur Paramètres.

  b. Clique le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.

  c. Recherchez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.

  d. Attendez que le processus de désinstallation soit terminé, puis redémarrez votre système.

Afin de désinstaller correctement les autres logiciels, allez sur leur site Internet et exécutez leur outil de désinstallation, ou contactez-les directement afin qu'ils vous indiquent la procédure de désinstallation.

3. Redémarrez votre système en mode normal et réinstallez Bitdefender.

**Vous avez déjà suivi les étapes ci-dessus et la situation n'est pas résolue.**

Pour résoudre ceci :

1. Redémarrez votre système et entrez en mode sans échec. Pour savoir comment procéder, reportez-vous à Comment redémarrer en mode sans échec ? (page 131).
2. Utilisez l'option Restauration du système de Windows pour restaurer l'appareil à une date antérieure à l'installation du produit Bitdefender.
3. Redémarrez le système en mode normal et contactez les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la rubrique Demander de l'aide (page 270).

## 3.5.2. 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.


- Environnement de sauvetage (page 155)
- Que faire quand Bitdefender détecte des menaces sur votre appareil ? (page 156)
- Comment nettoyer un menace dans une archive ? (page 158)
- Comment nettoyer une menace dans une archive de messagerie ? (page 159)
- Que faire si je soupçonne un fichier d'être dangereux ? (page 160)
- Que sont les fichiers protégés par mot de passe du journal d'analyse ? (page 160)
- Que sont les éléments ignorés du journal d'analyse ? (page 161)
- Que sont les fichiers ultra-compressés du journal d'analyse ? (page 161)
- Pourquoi Bitdefender a-t-il effacé automatiquement un fichier infecté ? (page 161)


Si vous ne trouvez pas votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du support technique de Bitdefender comme indiqué au chapitre Demander de l'aide (page 270).

## Environnement de sauvetage

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

Le mode de secours Bitdefender est compatible avec Windows RE.

## Démarrer votre système en mode de secours

Vous pouvez uniquement passer en mode de secours depuis votre produit Bitdefender, comme suit :

1. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
2. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
3. Cliquez sur **Ouvrir** à côté de **Mode de secours**.
4. Cliquez sur **REDÉMARRER** dans la fenêtre qui s'affiche.
   Le mode de secours de Bitdefender se charge en quelques instants.

## Analyser votre système en mode de secours

Pour analyser votre système en mode de secours :

1. Passez en mode de secours, comme indiqué dans Démarrer votre système en mode de secours (page 155).
2. Le processus d'analyse de Bitdefender commence automatiquement quand le système charge en mode 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 le mode de secours, cliquez sur le bouton Fermer situé dans la fenêtre contenant les résultats de l'analyse.

## Que faire quand Bitdefender détecte des menaces sur votre appareil ?

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

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

Dans de telles situations, mettez à jour Bitdefender pour vous assurer de disposer de la dernière base de données d'information sur les menaces puis exécutez une analyse du système.

Dès que l'analyse du système est terminée, sélectionnez l'action souhaitée à appliquer aux éléments infectés (Désinfecter, Supprimer, Quarantaine).

Avertissement

Si vous pensez que le fichier fait partie du système d'exploitation Windows ou qu'il ne s'agit pas d'un fichier infecté, ne suivez pas ces étapes et contactez le service client de Bitdefender dès que possible.

Si l'action sélectionnée ne peut être appliquée et que le journal d'analyse révèle une infection qui ne peut être supprimée, vous devez supprimer le(s) fichier(s) manuellement :

**La première méthode peut être utilisée en mode normal :**

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
   b. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
   c. Dans le **Avancé** fenêtre, éteignez **Bouclier Bitdefender**.
2. Afficher les objets cachés dans Windows. Pour savoir comment procéder, reportez-vous à Comment afficher des objets cachés dans Windows ? (page 129).
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 procéder, reportez-vous à Comment redémarrer en mode sans échec ? (page 131).
2. Afficher les objets cachés dans Windows. Pour savoir comment procéder, reportez-vous à Comment afficher des objets cachés dans Windows ? (page 129).
3. Accédez à l'emplacement du fichier infecté (vérifiez le journal d'analyse) et supprimez-le.
4. Redémarrez votre système et entrez en mode normal.

Si ces informations ne vous ont pas été utiles, vous pouvez contacter Bitdefender pour obtenir de l'aide, comme décrit dans la section Demander de l'aide (page 270).

## 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 d'appliquer 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 d'effectuer 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 sur le Interface Bitdefender.
   b. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
   c. Dans le **Avancé** fenêtre, éteignez **Bouclier Bitdefender**.
3. Rendez-vous à l'emplacement de l'archive et décompressez-la à l'aide d'une application d'archivage, comme WinZip.
4. Identifier le fichier infecté et le supprimer.
5. Supprimez l'archive d'origine afin de vous assurer que l'infection est totalement supprimée.
6. Recompressez les fichiers dans une nouvelle archive à l'aide d'une application d'archivage, comme WinZip.
7. Activez la protection antivirus en temps réel de Bitdefender et exécutez une analyse du système afin de vous assurer qu'aucune autre infection n'est présente sur le système.

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

Si ces informations ne vous ont pas été utiles, vous pouvez contacter Bitdefender pour obtenir de l'aide, comme décrit dans la section Demander de l'aide (page 270).

## Comment nettoyer une menace dans une archive de messagerie ?

Bitdefender permet également de repérer les menaces dans les bases de données des 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 e-mails avec Bitdefender.
2. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Cliquez sur **protection** dans le menu de navigation sur le Interface Bitdefender.
   b. Dans le **ANTIVIRUS** volet, cliquez sur **Ouvrir**.
   c. Dans le **Avancé** fenêtre, éteignez **Bouclier Bitdefender**.
3. Ouvrez le rapport d'analyse et utilisez les informations d'identification (Sujet, Expéditeur, Destinataire) des messages infectés pour les localiser dans le client de messagerie.
4. Supprimez les messages infectés. La plupart des clients de messagerie placent les messages supprimés dans un dossier de récupération permettant de les restaurer. Il est recommandé de vous assurer que le message a été supprimé également dans ce dossier de récupération.
5. Compressez le dossier contenant le message infecté.
   - Sur Microsoft Outlook 2007 : dans le menu Fichier, cliquez sur Gestion des fichiers de données. Sélectionnez les dossiers personnels (.pst) que vous souhaitez compresser et cliquez sur Paramètres. Cliquez sur Compresser maintenant.

- Sur Microsoft Outlook 2010 / 2013/ 2016 : dans le menu Fichier, cliquez sur Informations puis sur Paramètres du compte (Ajouter et supprimer des comptes ou modifier les paramètres de connexion existants). Cliquez sur Fichiers de données, sélectionnez les dossiers personnels que vous souhaitez compresser puis cliquer sur Paramètres. Cliquez sur Compresser.

6. Activez la protection antivirus en temps réel de Bitdefender.

Si ces informations ne vous ont pas été utiles, vous pouvez contacter Bitdefender pour obtenir de l'aide, comme décrit dans la section Demander de l'aide (page 270).

## Que faire si je soupçonne un fichier d'être dangereux ?

Vous pouvez soupçonner 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. Exécutez une **analyse du système** avec Bitdefender. Pour savoir comment procéder, reportez-vous à {3}{4}.
2. Si le résultat de l'analyse n'indique pas d'infection, mais que vous avez encore des doutes et souhaitez vérifier le fichier, contactez les représentants de notre service d'assistance afin que nous puissions vous aider.
   Pour savoir comment procéder, reportez-vous à Demander de l'aide (page 270).

## Que sont les fichiers protégés par mot de passe du journal d'analyse ?

Il ne s'agit que d'une notification qui indique que Bitdefender a détecté que ces fichiers sont soit protégés par un mot de passe soit par une forme de chiffrement .

Les éléments protégés par un mot de passe sont généralement :

- Fichiers appartenant à une autre solution de sécurité.
- Fichiers appartenant au système d'exploitation.

Afin que le contenu soit analysé, ces fichiers auront besoin d'être extraits ou déchiffrés.

Si ce contenu est extrait, le moteur d'analyse en temps réel de Bitdefender l'analyse automatiquement pour que votre appareil reste protégé. Si vous souhaitez analyser ces fichiers avec Bitdefender, vous devez contacter le fabricant du produit afin d'obtenir plus d'informations sur ces fichiers.

Nous vous recommandons d'ignorer ces fichiers car ils ne constituent pas une menace pour votre système.

## 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.

## 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. Son contenu sera analysé à l'accès en temps réel si nécessaire.

## Pourquoi Bitdefender a-t-il effacé 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 de tels 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 approuvés. 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.

# 4. ANTIVIRUS POUR MAC

## 4.1. Qu'est-ce que Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac est un scanner antivirus puissant, capable de détecter et de supprimer tous les types de logiciels malveillants (ou « menaces »), notamment :

- Ransomware
- les adwares
- les virus
- les spywares
- Chevaux de Troie
- les keyloggers
- les vers

Cette application détecte et supprime non seulement les menaces Mac mais également celles de Windows, vous empêchant ainsi d'envoyer accidentellement des fichiers infectés à votre famille, à vos amis ou à vos collègues utilisant des PC.

## 4.2. Installation et désinstallation

Ce chapitre traite des sujets suivants :


- Configuration requise (page 162)
- Installation de Bitdefender Antivirus for Mac (page 163)
- Supprimer Bitdefender Antivirus for Mac (page 167)


### 4.2.1. Configuration requise

Vous pouvez installer Bitdefender Antivirus for Mac sur les ordinateurs Macintosh sous OS X Yosemite (10.10) ou une version supérieure.

Vous Mac doit avoir au moins 1 Go d’espace disque disponible.

Une connexion Internet est requise pour enregistrer et mettre à jour Bitdefender Antivirus for Mac.

Note
Le bloqueur de traceurs Bitdefender et le VPN Bitdefender ne peuvent être installés que sur les systèmes sous macOS 10.12 ou une version supérieure.

**Comment connaître votre version de macOS et d'autres informations matérielles concernant votre Mac**
Dans le menu Pomme situé en haut à gauche de l'écran, choisissez **À propos de ce Mac**. Dans la fenêtre d'informations qui apparaît, vous trouverez entre autres la version de votre système d'exploitation. Cliquez sur **Informations système** pour obtenir des informations détaillées sur votre matériel.

## 4.2.2. Installation de Bitdefender Antivirus for Mac

Pour installer l'application Bitdefender Antivirus for Mac depuis votre compte Bitdefender, procédez comme suit :

1. Connectez-vous en tant qu'Administrateur
2. Rendez-vous sur : 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.
4. Sélectionnez le panneau **Mes appareils**, puis cliquez sur **INSTALLER LA PROTECTION**.
5. Sélectionnez l'une des deux actions disponibles :
   - **Protéger cet appareil**
     a. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
     b. Enregistrez le fichier d'installation.
   - **Protéger d'autres appareils**
     a. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
     b. Appuyez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**.
     c. Entrez une adresse électronique dans le champ correspondant, puis cliquez sur **ENVOYER PAR COURRIEL**.

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

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

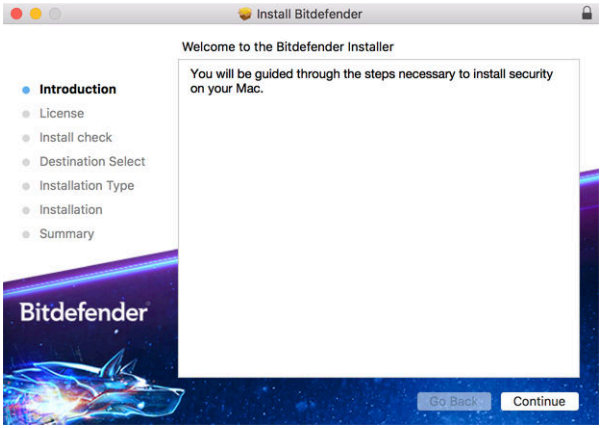
6. Exécutez le produit Bitdefender que vous avez installé.
7. Finissez les étapes de l'installation.

## Processus d'installation

Pour installer Bitdefender Antivirus for Mac :

1. Cliquez sur le fichier téléchargé. Cela lancera le programme d'installation, qui vous guidera au cours du processus d'installation.
2. Suivez les indications de l'assistant d'installation.

## Étape 1 - Fenêtre d'accueil




Cliquez sur **Continuer**.

## Étape 2 - Lire les Conditions d'abonnement

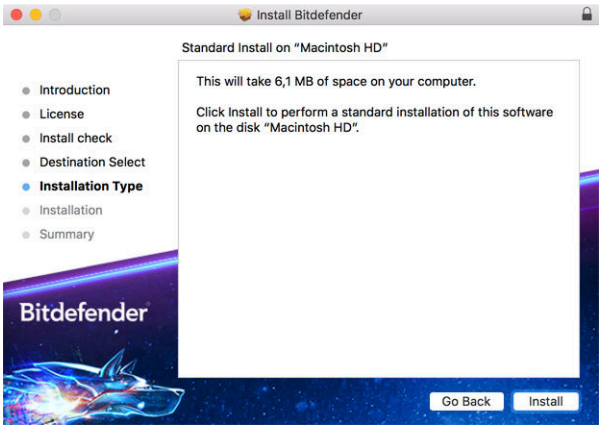

Pour poursuivre la procédure d'installation, vous devez accepter les Conditions d'utilisation de l'abonnement. Veuillez prendre le temps de lire les Conditions d'utilisation de l'abonnement, car elles contiennent les conditions dans le cadre desquelles vous pouvez utiliser Bitdefender Antivirus for Mac.

Depuis cette fenêtre, vous pourrez également sélectionner la langue dans laquelle vous voulez installer le produit.

Cliquez sur **Continuer** puis sur **J'accepte**.

> **Important**
> Si vous n'acceptez pas ces conditions, cliquez sur **Continuer** puis sur **Je refuse** pour annuler l'installation et quitter le programme d'installation.

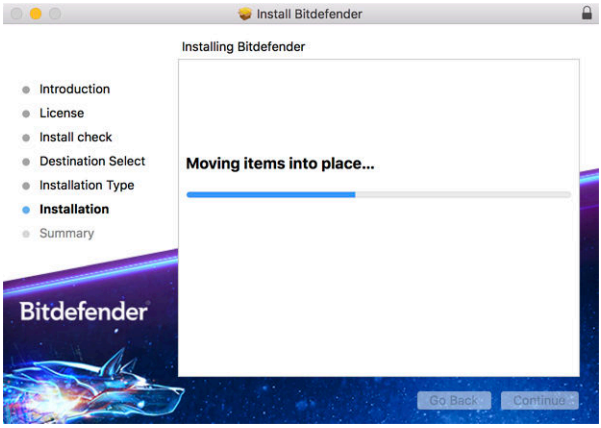
## Étape 3 - Démarrer l'Installation




Bitdefender Antivirus for Mac sera installé dans Macintosh HD/Library/Bitdefender. Vous ne pouvez pas modifier le chemin d'installation.

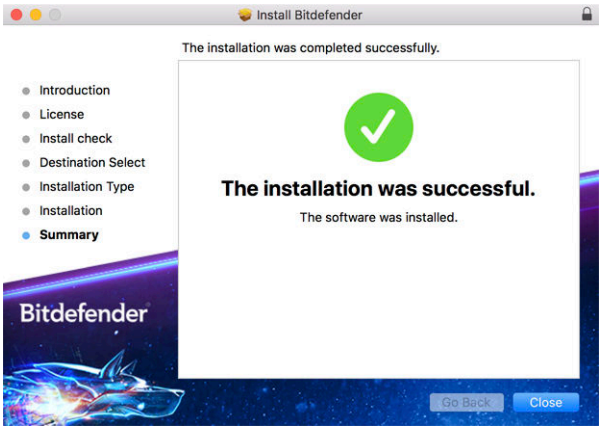
Cliquez sur **Installer** pour lancer l'installation.

## Étape 4 - Installer Bitdefender Antivirus for Mac




Patientez jusqu'à la fin de l'installation puis cliquez sur **Continuer**.

### Étape 5 - Terminer




Cliquez sur **Fermer** pour fermer la fenêtre du programme d'installation.

Le processus d'installation est terminé.

**Important**

- Si vous installez Bitdefender Antivirus sur un appareil équipé de macOS High Sierra 10.13.0 ou d'une version plus récente, la notification **Extension système bloquée** s'affiche. Elle indique que les extensions signées par Bitdefender ont été bloquées et doivent être activées manuellement. Cliquez sur OK pour continuer. Dans la fenêtre Bitdefender Antivirus for Mac qui s'ouvre, cliquez sur le lien **Sécurité et confidentialité**. Cliquez sur **Autoriser** en bas de la fenêtre ou sélectionnez Bitdefender SRL dans la liste et cliquez sur **OK**.
- Si vous installez Bitdefender Antivirus sur un appareil équipé de macOS Mojave 10.14 ou d'une version plus récente, une nouvelle fenêtre s'ouvre. Elle indique que vous devez **Accorder à Bitdefender l'accès complet au disque** et **Autoriser le chargement de Bitdefender**. Suivez les instructions qui s'affichent à l'écran pour configurer le produit.

## 4.2.3. Supprimer Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac étant une application complexe, elle ne peut pas être supprimée normalement, en faisant glisser l'icône de l'application du dossier **Applications** vers la corbeille.

Pour supprimer Bitdefender Antivirus for Mac, procédez comme suit :

1. Ouvrez une fenêtre **Finder** et allez dans le dossier **Applications**.
2. Dans **Applications**, ouvrez le dossier Bitdefender puis double-cliquez sur **BitdefenderUninstaller**.
3. Sélectionnez une méthode de désinstallation.

   **Note**
   Si vous souhaitez seulement désinstaller l'application Bitdefender VPN, sélectionnez **Désinstaller le VPN** seulement.

4. Cliquez sur **Désinstaller** et attendez la fin du processus.
5. Cliquez sur **Fermer** pour terminer.

   **Important**
   Si une erreur s'est produite, vous pouvez contacter le Service Client de Bitdefender comme indiqué dans Demander de l'aide (page 270).

## 4.3. Pour démarrer

Ce chapitre comprend les rubriques suivantes :



### 4.3.1. Ouvrir Bitdefender Antivirus for Mac

Vous pouvez ouvrir Bitdefender Antivirus for Mac de plusieurs façons :

- Cliquez sur l'icône de Bitdefender Antivirus for Mac dans le Launchpad.
- Cliquez sur l'icône dans la barre de menus et sélectionnez **Ouvrir l'interface de l'antivirus**.
- Ouvrez une fenêtre Finder, allez dans Applications et double-cliquez sur l'icône de **Bitdefender Antivirus for Mac**.

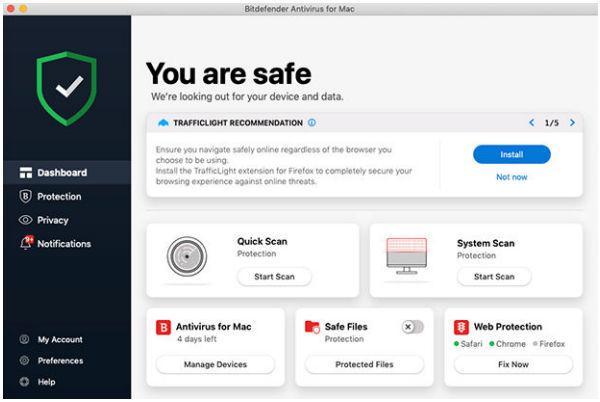
**Important**

La première fois que vous ouvrez Bitdefender Antivirus for Mac sur macOS Mojave 10.14 ou une version plus récente, une recommandation de protection apparait car nous avons besoin de certaines permissions pour analyser tout votre système en quête de menaces. Pour nous donner ces permissions, vous devez vous connecter en tant qu'administrateur et procéder comme suit :

1. Cliquez sur le lien **Préférences Système**.
2. Cliquez sur l'icône , puis saisissez vos informations d'identification administrateur.
3. Une nouvelle fenêtre s'ouvre. Déposez le fichier **BDLDaemon** dans la liste des applications autorisées.

## 4.3.2. Fenêtre principale

Bitdefender Antivirus for Mac 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.

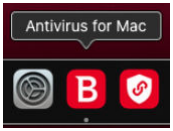
La barre d'état en haut de la fenêtre vous informe de l'état de la sécurité de l'appareil par le biais de messages et de couleurs explicites. Si aucune alerte n'est en cours dans Bitdefender Antivirus for Mac, la barre d'état est verte. Lorsqu'un problème de sécurité est détecté, la barre d'état devient rouge. Pour en savoir plus sur les problèmes et leur résolution, reportez-vous à Correction des problèmes (page 184).

Pour vous offrir une utilisation efficace et une meilleure protection pendant toutes vos activités, **Bitdefender Autopilot** jouera le rôle de conseiller de sécurité personnel. En fonction de votre activité - travail, opérations bancaires, etc. - Bitdefender Autopilot vous proposera des recommandations contextuelles basées sur votre utilisation de l'appareil et vos besoins. Vous pourrez ainsi découvrir et mettre à profit les avantages des différentes fonctionnalités de l'application Bitdefender Antivirus for Mac.

Depuis le menu de navigation à gauche, vous pouvez accéder aux sections Bitdefender permettant de configurer le produit et d'effectuer des tâches administratives avancées (onglets **Protection** et **Vie privée**), aux notifications, à votre **compte Bitdefender** et aux **préférences**. Par ailleurs, vous pouvez nous contacter via l'onglet **Aide** si vous avez des questions ou si vous rencontrez des difficultés.

## 4.3.3. Icône de l'application dans le Dock

L'icône Bitdefender Antivirus for Mac apparaît dans le Dock dès que vous ouvrez l'application. Elle vous permet de lancer facilement l'analyse de fichiers ou de dossiers. Il vous suffit de glisser-déposer le fichier ou le dossier que vous souhaitez analyser sur l'icône du Dock pour que l'analyse démarre immédiatement.



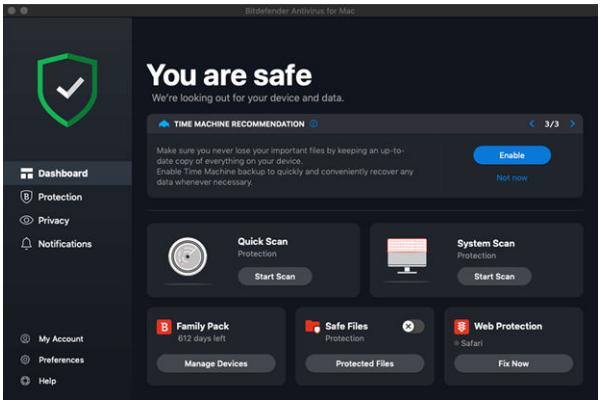

## 4.3.4. Menu de navigation

Le menu de navigation est situé à gauche de l'interface de Bitdefender, il vous permet d'accéder rapidement aux fonctionnalités de Bitdefender dont vous avez besoin pour utiliser le produit. Les onglets disponibles dans cet espace sont les suivants :

- **Tableau de bord**. Vous pouvez ici rapidement résoudre les problèmes de sécurité, voir les recommandations correspondant aux besoins de votre système, réaliser des actions rapides, et vous rendre sur votre compte Bitdefender pour gérer les appareils que vous avez ajoutés à votre abonnement Bitdefender.
- **Protection**. Vous pouvez ici lancer des analyses antivirus, ajouter des fichiers à la liste des exceptions, protéger vos fichiers et applications des attaques de ransomware, sécuriser vos sauvegardes Time Machine, et configurer votre protection lorsque vous surfez sur Internet.
- **Confidentialité**. Depuis cet onglet, vous pouvez ouvrir l'application Bitdefender VPN et installer l'extension Bloqueur de traceurs sur votre navigateur web.
- **Notifications**. Depuis cet onglet, vous pouvez obtenir des informations sur les actions déclenchées après l'analyse des fichiers.
- **Mon compte**. Depuis cet onglet, vous pouvez savoir quel est le compte ouvert sur cet appareil et quel est l'abonnement qui le protège, mais aussi changer de compte si nécessaire.
- **Préférences**. Depuis cet onglet, vous pouvez paramétrer Bitdefender.
- **Aide**. Si vous avez besoin d'assistance pour régler un problème avec votre produit Bitdefender, vous pouvez ici contacter le service de support technique. Vous pouvez également nous envoyer des commentaires pour nous aider à améliorer le produit.

## 4.3.5. Mode sombre

Pour protéger vos yeux des effets de la lumière lorsque vous travaillez la nuit ou dans un environnement peu éclairé. Bitdefender Antivirus for Mac est compatible avec le Mode sombre sur Mojave 10.14 et les versions ultérieures. Les couleurs de l'interface ont été optimisées pour que vous puissiez utiliser votre Mac sans vous fatiguer les yeux. L'interface Bitdefender Antivirus for Mac s'adapte en fonction des paramètres de votre appareil.




# 4.4. Protection contre les Logiciels Malveillants

Ce chapitre comprend les rubriques suivantes :



## 4.4.1. Utilisation optimale

Pour maintenir la protection de votre système contre les menaces et pour éviter l'infection accidentelle d'autres systèmes, suivez les conseils suivants :

- Faites en sorte que **Bitdefender Shield** soit toujours activé, pour que les fichiers système soient automatiquement analysés par Bitdefender Antivirus for Mac.
- Maintenez votre produit Bitdefender Antivirus for Mac à jour avec les dernières informations sur les menaces et mises à jour.
- Vérifiez et corrigez régulièrement les problèmes signalés par Bitdefender Antivirus for Mac. Pour plus d'informations, reportez-vous à Correction des problèmes (page 184).
- Vérifiez le détail des événements dans le journal d'activité de Bitdefender Antivirus for Mac sur votre ordinateur. À chaque fois qu'un événement lié à la sécurité de votre système ou de vos données se produit, un nouveau message apparaît dans la zone des notifications Bitdefender. Pour en savoir plus, reportez-vous à Notifications (page 185).
- Nous vous recommandons également d'adopter les pratiques suivantes :
  - Prenez l'habitude d'analyser les fichiers que vous téléchargez à partir d'un support de stockage externe (comme une clé USB ou un CD), en particulier lorsque vous ne connaissez pas la source.
  - Si vous avez un fichier DMG, montez-le puis analysez son contenu (les fichiers du volume/de l'image monté(e)).

  Pour analyser un fichier, un dossier ou un volume, la méthode la plus simple consiste à le glisser-déposer sur la fenêtre de Bitdefender Antivirus for Mac ou sur l'icône du Dock.

Aucune autre configuration ou action n'est requise. Cependant, si vous le souhaitez, vous pouvez ajuster les paramètres de l'application et les préférences en fonction de vos besoins. Pour plus d'informations, reportez-vous à Configuration des Préférences (page 188).

### 4.4.2. Analyse de Votre Mac

En plus de la fonctionnalité **Bitdefender Shield**, qui surveille régulièrement les applications installées à la recherche d'actions ressemblant à celles de menaces et empêche que de nouvelles menaces n'atteignent votre système, vous pouvez analyser votre Mac ou des fichiers spécifiques à tout moment.

Pour analyser un fichier, un dossier ou un volume, la méthode la plus simple consiste à le glisser-déposer sur la fenêtre de Bitdefender Antivirus for Mac ou sur l'icône du Dock. L'assistant d'analyse apparaîtra et vous guidera tout au long du processus d'analyse.

Vous pouvez également lancer une analyse comme suit :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface Bitdefender.
2. Sélectionnez l'onglet **Antivirus**.
3. Cliquez sur l'un des trois boutons d'analyse pour lancer l'analyse souhaitée.
   - **Quick Scan (Analyse rapide)** - recherche des menaces aux emplacements les plus vulnérables de votre système (par exemple, dans les dossiers contenant les documents, les téléchargements, les téléchargements de messagerie et les fichiers temporaires de chaque utilisateur).
   - **Analyse du système** - effectue une analyse complète des menaces sur l'ensemble du système. Tous les volumes montés connectés seront également analysés.

     Note

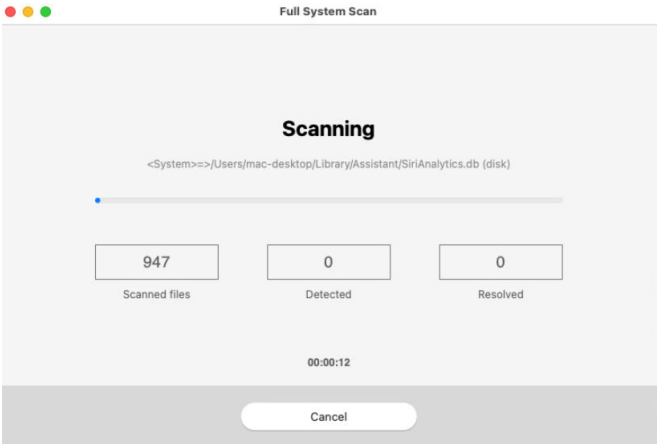
     En fonction de la taille de votre disque dur, l'analyse de l'ensemble du système peut être longue (une heure ou plus). Pour de meilleures performances, nous vous recommandons de ne pas exécuter cette tâche lorsque vous effectuez d'autres tâches consommant beaucoup de ressources (comme du montage vidéo).

     Vous pouvez, si vous le souhaitez, choisir de ne pas analyser certains volumes montés en les ajoutant à la liste d'**Exceptions** de la fenêtre Protection.
   - **Custom Scan (Analyser un emplacement spécifique)** - vous aide à rechercher des menaces dans certains fichiers, dossiers ou volumes.

Vous pouvez également lancer une analyse rapide ou une analyse du système depuis le tableau de bord.

### 4.4.3. Assistant d'analyse

Lorsque vous lancez une analyse, l'assistant d'analyse Bitdefender Antivirus for Mac apparaît.



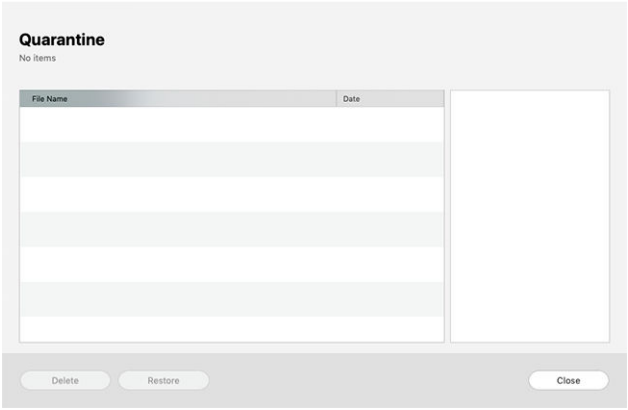

Des informations en temps réel sur les menaces détectées et résolues sont affichées pendant chaque analyse.

Patientez jusqu'à ce que Bitdefender Antivirus for Mac ait terminé l'analyse.

**Note**
L'analyse peut durer un certain temps, selon sa complexité.

### 4.4.4. Mise en quarantaine

Bitdefender Antivirus for Mac permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée appelée quarantaine. Quand une menace est en quarantaine, elle ne peut faire aucun dégât car elle ne peut ni être exécutée, ni être lue.




La partie Quarantaine affiche tous les fichiers actuellement isolés dans le dossier Quarantaine.

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

Pour consulter la liste de tous les éléments ajoutés en quarantaine :

1. Cliquez sur **protection** dans le menu de navigation de l'interface Bitdefender.
2. Cliquez sur **Ouvrir** dans le volet **Quarantaine**.

### 4.4.5. Bitdefender Shield (protection en temps réel)

Bitdefender assure la protection en temps réel contre un vaste éventail de menaces en analysant les applications installées, leurs mises à jour, ainsi que les nouveaux fichiers et les fichiers modifiés.

Pour désactiver la protection en temps réel :

1. Cliquez sur **Préférences** dans le menu de navigation de l'interface de Bitdefender.
2. Désactivez **Bitdefender Shield** dans la fenêtre **Protection**.

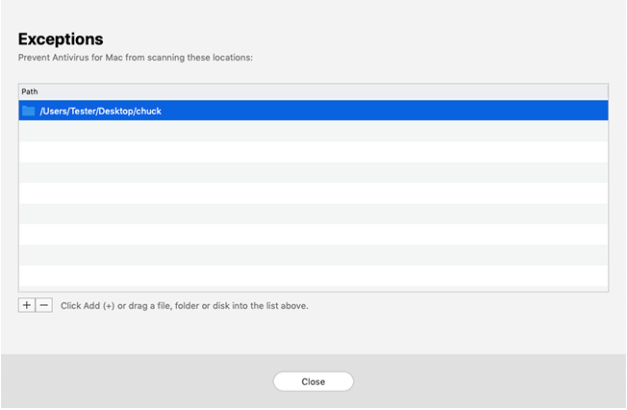
Avertissement

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.

## 4.4.6. Exceptions d'analyse

Si vous le souhaitez, vous pouvez configurer Bitdefender Antivirus for Mac afin qu'il n'analyse pas certains fichiers, dossiers, ou même, un volume entier. Vous pouvez par exemple souhaiter exclure de l'analyse :

- Les fichiers identifiés à tort comme étant infectés (connus comme étant de faux positifs)
- Les fichiers provoquant des erreurs d'analyse
- Les volumes de sauvegarde




La liste des exceptions contient les chemins ayant été exclus de l'analyse.

Pour accéder à la liste des exceptions :

1. Cliquez sur **protection** dans le menu de navigation de l'interface Bitdefender.
2. Cliquez sur **Ouvrir** dans le volet **Exceptions**.

Il y a deux manières de définir une exception d'analyse :

- Glissez-déposez un fichier, un dossier ou un volume dans la liste des exceptions.
- Cliquez sur le bouton avec le signe plus (+), situé sous la liste des exceptions. Sélectionnez ensuite le fichier, le dossier ou le volume à exclure de l'analyse.

Pour supprimer une exception d'analyse, sélectionnez-la dans la liste et cliquez sur le bouton avec le signe moins (-) situé sous la liste des exceptions.

## 4.4.7. Protection Web

Bitdefender Antivirus for Mac utilise les extensions TrafficLight pour protéger complètement votre expérience de navigation sur Internet. Les extensions TrafficLight interceptent, traitent et filtrent l'ensemble du trafic web, bloquant tout contenu malveillant.

Les extensions fonctionnent avec et s'intègrent aux navigateurs web suivants : Mozilla Firefox, Google Chrome et Safari.

### Activer les extensions Linkchecker

Pour activer les extensions TrafficLight :

1. Cliquez sur **Corriger** sur la carte **Protection web** du tableau de bord.
2. La fenêtre **Protection web** apparait.
   Le navigateur web que vous avez installé sur votre système apparait. Pour installer l'extension Linkchecker dans votre navigateur, cliquez sur **Obtenir l'extension**.
3. Vous êtes redirigé vers :
   https://bitdefender.fr/solutions/trafficlight.html
4. Sélectionnez **Téléchargement gratuit**.
5. Suivez ces étapes pour installer l'extension TrafficLight correspondant à votre navigateur web.

### Gérer les paramètres des extensions

Un vaste ensemble de fonctionnalités est disponible pour vous protéger contre toute sortes de menaces présentes sur Internet . Pour y accéder, cliquez sur l'icône de TrafficLight située à côté des paramètres de votre navigateur, puis sur le bouton ⚙ **Paramètres** :

- **Paramètres de BitDefender TrafficLight**
  - Web Protection - vous empêche d'accéder aux sites web utilisés pour perpétrer des attaques par malware, hameçonnage ou fraude.
  - Search Advisor - informe de la présence de sites Web à risque dans les résultats de recherche.

- **Exceptions**
  Si vous êtes sur le site web que vous voulez ajouter aux exceptions, cliquez sur **Ajouter le site web actuel à la liste**.
  Si vous voulez ajouter un autre site web, saisissez son adresse dans le champ correspondant, puis cliquez sur .
  Vous ne serez pas averti si des menaces sont présentes sur les pages exclues. Ainsi, nous vous recommandons de n'ajouter à cette liste que les sites web et les applications en lesquels vous avez pleinement confiance.

### Page des notes et alertes

En fonction de la façon dont Linkchecker classifie la page web que vous affichez, une des icônes suivantes s'affiche dans cette zone :

Cette page ne présente pas de risque. Vous pouvez poursuivre votre navigation.

Cette page web peut contenir du contenu dangereux. Soyez prudent(e) si vous décidez de la consulter.

Cette page contient un malware ou d'autres menaces, nous vous conseillons de la quitter immédiatement.

Sur Safari, le fond des icônes de TrafficLight est noir.

## 4.4.8. Bloqueur de traceurs

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

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

Cette extension de Bitdefender est compatible avec les navigateurs suivants :

- Google Chrome
- Mozilla Firefox
- Safari

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

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

## Activation du Bloqueur de traceurs Bitdefender

Pour activer cette extension sur votre navigateur :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Bloqueur de traceurs**.
3. Cliquez sur **Activer l'extension** à côté du navigateur sur lequel vous voulez activer l'extension.

## Interface du Bloqueur de traceurs

Lorsque l'extension Bloqueur de traceurs est activée, l'icône apparaît à côté de la barre de recherche de votre navigateur. À chaque fois que vous

visitez un site, un chiffre s'affiche sur cette icône. Il indique le nombre de traceurs détectés et bloqués. Si vous souhaitez en savoir plus sur les traceurs bloqués, cliquez sur l'icône pour ouvrir l'interface. Vous y verrez le nombre de traceurs bloqués, mais aussi le temps nécessaire au chargement de la page et les catégories auxquelles appartiennent les traceurs détectés. Pour voir la liste des sites qui lancent ces traceurs, cliquez sur chaque catégorie.

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

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

## Désactivation du Bloqueur de traceurs Bitdefender

Pour désactiver le Bloqueur de traceurs Bitdefender sur votre navigateur :

1. Ouvrez votre navigateur web.
2. Cliquez sur l'icône qui se trouve à côté de la barre d'adresse de votre navigateur.
3. Cliquez sur l'icône dans le coin supérieur droit.
4. Utilisez le bouton correspondant pour désactiver la fonctionnalité. L'icône Bitdefender devient grise.

## Autoriser le tracking d'un site web

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

1. Ouvrez votre navigateur Web.
2. Cliquez sur l'icône qui se trouve à côté de la barre de recherche.
3. Clique le icône dans le coin supérieur droit.
4. Si vous êtes sur le site Web que vous souhaitez ajouter aux exceptions, cliquez sur **Ajouter le site Web actuel à la liste**.

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

## 4.4.9. 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.

Grâce à ses technologies de pointe, Bitdefender veille à l'intégrité du système en protégeant les zones critiques contre les attaques par ransomware, sans répercussions sur le fonctionnement du système. Vous pouvez également souhaiter qu'aucune application suspecte n'accède à vos fichiers personnels (documents, photos ou vidéos). Avec Bitdefender Safe Files, vous pouvez mettre vos fichiers personnels à l'abri et sélectionner les applications autorisées à les modifier.

Pour ajouter dans un second temps des fichiers à l'environnement protégé :

1. Cliquez sur **protection** dans le menu de navigation de l'interface Bitdefender.
2. Sélectionnez l'onglet **Anti-Ransomware**.
3. Cliquez sur **Fichiers protégés** dans l'espace Safe Files.
4. Cliquez sur le bouton avec le signe plus (+), situé sous la liste des fichiers protégés. Choisissez ensuite le fichier, le dossier ou le volume à protéger en cas d'attaque de ransomware.

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.

Par défaut, les dossiers Images, Documents, Bureau et Téléchargement sont protégés des menaces.

> **Note**
> Les dossiers personnalisés ne peuvent être protégés que pour les utilisateurs actuels. Les disques externes ainsi que les fichiers du système et des applications ne peuvent pas être ajoutés à l'environnement de protection.

Vous recevrez une notification à chaque fois qu'une application inconnue avec un comportement inhabituel essayera de modifier les fichiers que vous avez ajoutés. Cliquez sur **Autoriser** ou **Bloquer** pour l'ajouter à la liste des **Applications gérées**.

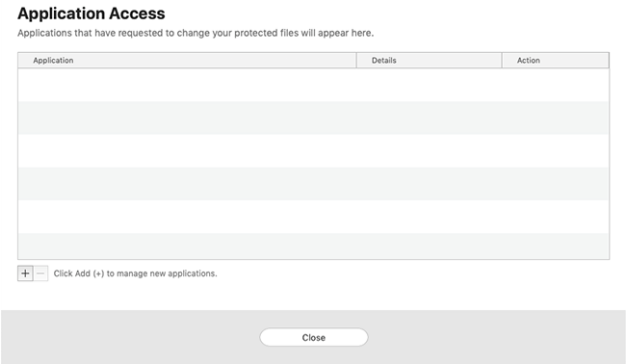
### Accès des applications

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 Bitdefender.
2. Sélectionnez le **Anti-ransomware** languette.
3. Cliquez sur **Accès de l'application** dans l'espace Safe Files.
4. Passez l'état de l'application bloquée sur Autoriser.

Les applications autorisées peuvent également être bloquées.

Ajoutez plus d'applications à la liste par glisser-déplacer ou en cliquant sur le signe plus (+).




## 4.4.10. Protection Time Machine

Bitdefender Time Machine Protection constitue une couche de sécurité supplémentaire pour votre disque dur externe, y compris tous les fichiers que vous avez décidé d'y stocker, en bloquant l'accès de toute source

externe. Si un jour les fichiers de votre lecteur Time Machine sont chiffrés par un ransomware, vous pourrez les récupérer sans payer la rançon demandée.

Si vous devez restaurer des éléments depuis une sauvegarde Time Machine, veuillez consulter le support Apple pour obtenir des instructions.

### Activer ou désactiver Protection Time Machine

Pour activer ou désactiver la Protection Time Machine :

1. Cliquez sur **Protection** dans le menu de navigation de l'**interface Bitdefender**.
2. Sélectionnez le **Anti-ransomware** languette.
3. Activez ou désactivez le bouton **Protection Time Machine**.

## 4.4.11. Correction des problèmes

Bitdefender Antivirus for Mac détecte automatiquement un ensemble de problèmes pouvant affecter la sécurité de votre système et de vos données et vous informe à leur sujet. Vous pouvez donc corriger les risques de sécurité facilement et rapidement.

Corriger les problèmes signalés par Bitdefender Antivirus for Mac est une façon simple et rapide d'assurer une protection optimale des données de votre système.

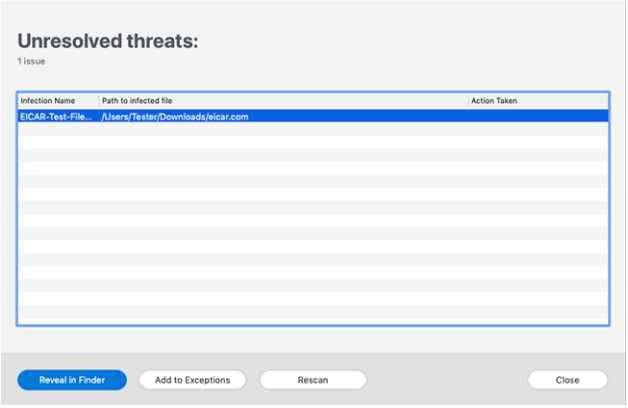
Les problèmes détectés comprennent :

- La mise à jour des informations sur les menaces n’a pas été téléchargée sur nos serveurs.
- Des menaces ont été détectées sur votre système et le produit ne peut pas automatiquement les désinfecter.
- La protection en temps réel est désactivée.

Pour consulter et corriger les problèmes détectés :

1. Si Bitdefender n'émet pas d'avertissement, la barre d'état est verte. Lorsqu'un problème de sécurité est détecté, la barre d'état change de couleur pour passer au rouge.
2. Consultez la description pour plus d'informations.

3. Quand un problème est détecté, cliquez sur le bouton adapté pour prendre une mesure.




La liste des menaces non résolues est mise à jour après chaque analyse du système, qu'elle soit réalisée automatiquement en tâche de fond ou à votre demande.

Vous pouvez choisir d'appliquer les actions suivantes aux menaces non résolues :

- **Suppression manuelle.** Choisissez cette option pour supprimer les infections manuellement.
- **Ajout aux exceptions.** Cette option n'est pas proposée pour les menaces qui sont détectées dans les archives.

## 4.4.12. 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 ce produit, un nouveau message apparaît dans la zone des notifications Bitdefender, comme lorsqu'un nouveau message 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** indiquent des problèmes critiques. Nous vous recommandons de les vérifier immédiatement.
- Les événements d'**avertissement** indiquent des problèmes non critiques. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
- Les événements **Informations** indiquent des opérations réussies.

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

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

## 4.4.13. Mises à jour

De nouvelles menaces sont détectées et identifiées tous les jours et il est donc important de veiller à ce que Bitdefender Antivirus for Mac soit à jour et bénéficie des dernières informations en matière de menaces.

Les mises à jour des informations sur les menaces sont exécutées à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, la mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

- Si Bitdefender Antivirus for Mac est à jour, il peut détecter les dernières menaces et nettoyer les fichiers infectés.
- Si Bitdefender Antivirus for Mac n'est pas à jour, les dernières menaces découvertes par les Bitdefender Labs ne pourront pas être détectées et supprimées.

## Demandes de mise à jour

Vous pouvez demander une mise à jour manuellement à tout moment.

Une connexion Internet active est nécessaire afin de rechercher les mises à jour disponibles et de les télécharger.

Comment lancer une mise à jour manuellement :

1. Cliquez sur le bouton **Actions** dans la barre de menus.
2. Choisissez **Mettre à jour la base de données d'information sur les menaces**.

Alternativement, vous pouvez demander une mise à jour manuellement en appuyant sur CMD + U.

Vous pouvez voir la progression de la mise à jour et les fichiers téléchargés.

## Obtenir des Mises à jour via un Serveur Proxy

Bitdefender Antivirus for Mac peut se mettre à jour uniquement via des serveurs proxy ne requérant pas d'authentification. Vous n'avez à configurer aucun paramètre du programme.

Si vous vous connectez à Internet via un serveur proxy exigeant une authentification, vous devez passer à une connexion Internet directe régulièrement afin d'obtenir les mises à jour des informations sur les menaces.

## Mise à niveau vers une nouvelle version

De façon occasionnelle, nous publions des mises à jour de produits pour ajouter de nouvelles fonctionnalités ou améliorations ou encore réparer des problèmes liés au produit. Ces mises à jour peuvent nécessiter un redémarrage du système pour lancer l'installation de nouveaux fichiers. Par défaut, si une mise à jour nécessite un redémarrage de l'ordinateur, Bitdefender Antivirus for Mac continuera à fonctionner avec les anciens fichiers jusqu'au redémarrage du système. Dans ce cas, le processus de mise à jour n'interférera pas avec le travail de l'utilisateur.

Lorsqu'une mise à jour du produit est terminée, une fenêtre contextuelle vous demande de redémarrer le système. Si vous ratez cette notification, vous pouvez cliquer sur **Redémarrer pour mettre à niveau** dans la barre de menus ou redémarrer manuellement le système.

### Trouver des informations sur votre version de Bitdefender Antivirus for Mac

Pour connaitre la version de Bitdefender Antivirus for Mac que vous utilisez, consultez la fenêtre **A propos**. Depuis cette même fenêtre, vous pouvez consulter les Conditions d'utilisation de l'abonnement, la Politique de confidentialité et les licences open-sources.

Pour ouvrir la fenêtre A propos :

1. Ouvrez Bitdefender Antivirus for Mac.
2. Cliquez sur Bitdefender Antivirus for Mac dans la barre de menus et sélectionnez **À propos d'Antivirus for Mac**.

## 4.5. Configuration des Préférences

Ce chapitre comprend les rubriques suivantes :



### 4.5.1. Accéder aux Préférences

Pour ouvrir la fenêtre des Préférences de Bitdefender Antivirus for Mac :

- Choisissez une des possibilités suivantes :
  - Cliquez sur **Préférences** dans le menu de navigation de l'interface Bitdefender.
  - Cliquez sur Bitdefender Antivirus for Mac dans la barre de menu et sélectionnez **Préférences**.

### 4.5.2. Préférences Protection

La fenêtre des préférences en matière de protection vous permet de configurer l'approche générale de l'analyse. Vous pouvez configurer les actions appliquées aux fichiers infectés et suspects détectés et d'autres paramètres généraux.

- **Bitdefender Shield.** Bitdefender Shield fournit une protection en temps réel contre un grand nombre de menaces en analysant

toutes les applications installées, leurs versions mises à jour et les fichiers nouveaux ou modifiés. Nous vous déconseillons de désactiver Bitdefender Shield, mais si c'est vraiment nécessaire, cette interruption doit être aussi courte que possible. Si Bitdefender Shield est désactivé, votre appareil ne sera plus protégé contre les menaces.

- **Analyser uniquement les fichiers nouveaux et modifiés.** Cochez cette case pour que Bitdefender Antivirus for Mac n'analyse que les fichiers n'ayant pas été analysés auparavant ou ayant été modifiés depuis leur dernière analyse.

  Vous pouvez choisir de ne pas appliquer ce paramètre à l'analyse personnalisée et par glisser-déposer en décochant la case correspondante.

- **Ne pas analyser le contenu des sauvegardes.** Cochez cette case pour que les fichiers de sauvegarde soient exclus de l'analyse. Si les fichiers infectés sont ultérieurement restaurés, Bitdefender Antivirus for Mac les détectera automatiquement et agira en conséquence.

### 4.5.3. Préférences avancées

Vous pouvez sélectionner une mesure générale à prendre pour tous les problèmes et éléments suspects détectés pendant une analyse.

**Action pour les éléments infectés**

- **Essayer de désinfecter ou déplacer en quarantaine** - Si des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (supprimer le code malveillant) ou de les placer en quarantaine.
- **Ignorer** - Aucune action ne sera appliquée aux fichiers détectés.

**Action pour les éléments suspects**

- **Déplacer les fichiers en quarantaine** - Si des fichiers suspects sont détectés, Bitdefender les déplacera en quarantaine.
- **Ne pas agir** - Aucune action ne sera entreprise sur les fichiers détectés.

### 4.5.4. Offres spéciales

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

Pour activer ou désactiver les notifications sur les promotions :

1. Cliquez sur **Préférences** dans le menu de navigation de l'interface Bitdefender.
2. Sélectionnez l'onglet **Autres**.
3. Activez ou désactivez le bouton **Mes offres**.

> **Note**
> L'option **Mes offres** est activée par défaut.

## 4.6. Questions les Plus Fréquentes

**Comment puis-je essayer Bitdefender Antivirus pour Mac avant de faire une demande d'abonnement ?**

Vous êtes un nouveau client de Bitdefender et vous souhaitez tester notre produit avant de l'acheter. La période d'essai est de 30 jours et vous pouvez continuer à utiliser le produit seulement si vous achetez un abonnement Bitdefender. Pour essayer Bitdefender Antivirus for Mac, vous devez :

1. Pour créer un compte Bitdefender, suivez ces étapes :
   a. Aller à: https://central.bitdefender.com.
   b. Tapez les informations requises dans les champs correspondants. Les informations fournies resteront confidentielles.
   c. 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.
   d. Cliquez sur **CRÉER UN COMPTE**.
2. Téléchargez Bitdefender Antivirus for Mac comme suit :
   a. Sélectionnez le **Mes appareils** panneau, puis cliquez sur **INSTALLER LA PROTECTION**.
   b. Choisissez l'une des deux options disponibles :

- **Protégez cet appareil**
  i. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
  ii. Enregistrez le fichier d'installation.

- **Protégez d'autres appareils**
  i. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
  ii. Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**.
  iii. Saisissez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER UN COURRIEL**.
  Notez que le lien de téléchargement généré n'est valable que pour les prochaines 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes étapes.
  iv. Sur l'appareil sur lequel vous souhaitez installer votre produit Bitdefender, vérifiez le compte de messagerie que vous avez saisi, puis cliquez sur le bouton de téléchargement correspondant.

c. Exécutez le produit Bitdefender que vous avez téléchargé.

**J'ai un code d'activation. Comment puis-je l'ajouter à mon abonnement ?**

Si vous avez acheté un code d'activation auprès de l'un de nos revendeurs ou si vous l'avez reçu en cadeau, vous pouvez ajouter sa disponibilité à votre abonnement Bitdefender.

Pour activer un abonnement à l'aide d'un code d'activation, procédez comme suit :

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes abonnements** panneau.
3. Clique le **CODE D'ACTIVATION** bouton, puis tapez le code dans le champ correspondant.
4. Cliquez sur **ACTIVER** continuer.

L'extension est désormais visible dans votre compte Bitdefender, et dans votre produit installé Bitdefender Antivirus for Mac, dans la partie en bas à droite de votre écran.

**Le journal d'analyse indique qu'il reste des éléments non résolus. Comment les supprimer ?**

Les éléments non résolus du journal d'analyse peuvent être :

- des archives dont l'accès est restreint (xar, rar, etc.)
  **Solution :** Utilisez l'option **Faire apparaître dans Finder** pour localiser le fichier et le supprimer manuellement. Veillez à vider la corbeille.
- des messageries dont l'accès est restreint (Thunderbird, etc.)
  **Solution :** Utilisez l'application pour supprimer l'entrée contenant le fichier infecté.
- Contenu des sauvegardes
  **Solution :** activez l'option **Ne pas analyser le contenu des sauvegardes** dans les Préférences de protection ou **ajoutez aux exceptions** les fichiers détectés.
  Si des fichiers éventuellement infectés étaient restaurés par la suite, Bitdefender Antivirus for Mac prendra automatiquement les mesures appropriées.

> **Note**
> Les fichiers ayant un accès restreint sont des fichiers que Bitdefender Antivirus for Mac peut ouvrir mais ne peut pas modifier.

**Où puis-je voir les détails de l'activité du produit ?**

Bitdefender tient un journal de toutes les actions importantes, des modifications d'état et d'autres messages critiques liés à son activité. Pour accéder à ces informations, cliquez sur **Notifications** dans le menu de navigation de l'interface Bitdefender.

**Puis-je mettre à jour Bitdefender Antivirus for Mac via un serveur proxy ?**

Bitdefender Antivirus for Mac ne peut se mettre à jour que via des serveurs proxy qui ne nécessitent pas d'authentification. Vous n'avez pas à configurer les paramètres du programme.

Si vous vous connectez à Internet via un serveur proxy nécessitant une authentification, vous devez passer régulièrement à une connexion

Internet directe pour obtenir des mises à jour des informations sur les menaces.

**Comment supprimer Bitdefender Antivirus for Mac ?**

Pour supprimer Bitdefender Antivirus for Mac, suivez ces étapes :

1. Ouvrez une fenêtre **Finder** et allez dans le dossier Applications.
2. Dans le dossier Bitdefender, double-cliquez sur BitdefenderUninstaller.
3. Cliquez sur **Désinstaller** et attendez que le processus soit terminé.
4. Cliquez sur **Fermer** pour finir.

> **Important**
> En cas d'erreur, vous pouvez contacter le service client de Bitdefender comme décrit dans Demander de l'aide (page 270).

**Comment retirer les extensions TrafficLight de mon navigateur web ?**

- Pour retirer les extensions TrafficLight de Mozilla Firefox, procédez comme suit :
  1. Allez dans **Outils** et sélectionnez **Modules complémentaires**.
  2. Sélectionnez **Extensions** dans la colonne de gauche.
  3. Sélectionnez l'extension et cliquez sur **Supprimer**.
  4. Redémarrez le navigateur pour que le processus de désinstallation se termine.

- Pour retirer les extensions TrafficLight de Google Chrome, procédez comme suit :
  1. En haut à droite, cliquez sur **Plus** ⋮ .
  2. Allez dans **Autres outils** et sélectionnez **Extensions**.
  3. Cliquez sur l'icône **Supprimer** 🗑 à côté de l'extension que vous voulez supprimer.
  4. Cliquez sur **Supprimer** pour confirmer la suppression.

- Pour désinstaller Bitdefender TrafficLight à partir de Safari, procédez comme suit :

1. Allez dans **Préférences** ou appuyez simultanément sur **Commande et Virgule(,)**.
2. Sélectionnez **Extensions**.
   Une liste des extensions installées apparait.
3. Sélectionnez l'extension Bitdefender TrafficLight puis cliquez sur **Désinstaller**.
4. Cliquez de nouveau sur **Désinstaller** pour confirmer le processus de désinstallation.

**Quand dois-je utiliser le VPN Bitdefender ?**

Vous devez être prudent lorsque vous accédez à des contenus, ou téléchargez/envoyez des données sur internet. Pour être certain de naviguer sur le web en toute sécurité, nous vous recommandons d'utiliser le VPN Bitdefender lorsque vous voulez :

- vous connecter à des réseaux sans-fil publics
- accéder à des contenus normalement disponibles uniquement depuis certaines régions, que vous soyez ou non chez vous
- assurer la confidentialité de vos données personnelles (identifiants, mots de passe, informations bancaires, etc.)
- masquer votre adresse IP

**Le VPN Bitdefender aura-t-il une incidence négative sur l'autonomie de mon appareil ?**

Le VPN Bitdefender a été conçu pour protéger vos données personnelles, masquer votre adresse IP quand vous êtes connecté à des réseaux sans-fil non sécurisés, et accéder à des contenus normalement indisponibles dans votre pays. Pour éviter d'utiliser pour rien la batterie de votre appareil, nous vous recommandons d'utiliser uniquement le VPN quand vous en avez besoin, et de le déconnecter quand vous êtes hors ligne.

**Pourquoi ma connexion à Internet ralentit-elle parfois lorsque je suis connecté(e) au VPN Bitdefender ?**

Bitdefender VPN a été pensé pour ne pas déranger votre navigation sur le web, mais votre connectivité à Internet ou la distance par rapport au serveur auquel vous êtes connecté peuvent provoquer des ralentissements. Dans ce cas, si vous n'êtes pas obligé d'être connecté à un serveur lointain (p.ex. en Chine) nous vous recommandons d'autoriser

le VPN Bitdefender à se connecter automatiquement au serveur le plus proche, ou de trouver un serveur plus proche de là où vous vous situez.

# 5. SÉCURITÉ MOBILE POUR ANDROID

## 5.1. Présentation de Bitdefender Mobile Security

Payer ses factures, réserver ses vacances, acheter des biens et des services... Il est pratique et très simple de faire ce type de choses en ligne. Mais un grand nombre de ces activités ayant évolué sur Internet, elles sont particulièrement risquées et si vous négligez les questions de sécurité, vos données personnelles pourraient être piratées. Et qu'y a-t-il de plus important que la protection des données stockées sur vos comptes en ligne ou votre smartphone ?

**Bitdefender Mobile Security** vous permet de :

- Bénéficiez de la meilleure protection pour votre smartphone et votre tablette Android, avec une incidence minimale sur l'autonomie de vos appareils
- Protégez-vous contre les arnaques mobiles basées sur des liens
- Accédez à notre VPN sécurisé pour une expérience rapide, anonyme et sûre de la navigation Internet
- Localisation, verrouillage et réinitialisation de votre appareil en cas de perte ou de vol.
- Vérifiez si votre compte de messagerie électronique a été impliqué dans des violations ou des fuites de données

## 5.2. Pour démarrer

### 5.2.1. Spécifications du produit

Bitdefender Mobile Security est compatible avec tout appareil fonctionnant sous Android 5.0 (ou version ultérieure du système d'exploitation). Une connexion Internet active est requise pour l'analyse des menaces dans le cloud.

### 5.2.2. Installer Bitdefender Mobile Security

- **Depuis Bitdefender Central**
  - Sous Android

1. Aller à : https://central.bitdefender.com.
2. Connectez-vous à votre compte Bitdefender.
3. Sélectionnez la section **Mes Appareils**.
4. Appuyez sur **INSTALLER LA PROTECTION**, puis appuyez sur **Protéger cet appareil**.
5. Sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
6. Vous serez alors redirigé vers **Google Play**. Sur l'écran de Google Play, appuyez sur Installer.

- Sur Windows, macOS et iOS
  1. Aller à: https://central.bitdefender.com.
  2. Connectez-vous à votre compte Bitdefender.
  3. Sélectionnez le **Mes appareils** panneau.
  4. Appuyez sur **INSTALLER LA PROTECTION**, puis appuyez sur **Protéger d'autres appareils**.
  5. Sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
  6. Appuyez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**.
  7. Entrez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER UN 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.
  8. 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.

- **Depuis Google Play**
  Recherchez l'application Bitdefender Mobile Security et installez-la. Vous pouvez également scanner le QR Code :

Avant de passer à l'étape de validation, 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 Mobile Security.

Appuyez sur **CONTINUER** pour passer à la fenêtre suivante.

### 5.2.3. Connectez-vous à votre compte Bitdefender

Pour utiliser Bitdefender Mobile Security, vous devez associer votre appareil à un compte Bitdefender, Facebook, Google, Microsoft ou Apple en vous connectant au compte à partir de l'application. Lorsque vous ouvrirez l'application pour la première fois, vous serez invité à vous connecter à un compte.

Si vous avez installé Bitdefender Mobile Security depuis votre compte Bitdefender, l'application tentera de se connecter automatiquement à ce compte.

Pour rattacher votre appareil à un compte Bitdefender :

1. Saisissez l'adresse e-mail de votre compte Bitdefender et le mot de passe correspondant dans les champs prévus à cet effet. Si vous n'avez pas de compte Bitdefender et souhaitez en créer un, cliquez sur le lien correspondant.
2. Appuyez sur **CONNEXION**.

Pour vous connecter en utilisant un compte Facebook, Google, ou Microsoft, sélectionnez le service que vous voulez utilisez dans la partie Ou s'inscrire via. Vous serez redirigé vers la page de connexion du service sélectionné. Suivez les instructions pour associer votre compte à Bitdefender Mobile Security.

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.

## 5.2.4. Configurer la protection

Une fois connecté à l'application, la fenêtre Configurer la protection apparait. Pour sécuriser votre appareil, nous vous recommandons de suivre les étapes suivantes :

- **Statut de l'abonnement** Afin d'être protégé par Bitdefender Mobile Security, vous devez activer votre produit avec une clé de licence ou un abonnement, qui indiquent pendant combien de temps vous pouvez utiliser le produit. Dès qu'elle expire, l'application cesse de fonctionner et de protéger votre appareil.
  Si vous avez un code d'activation, appuyez sur **J'AI UN CODE**, puis sur **ACTIVER**.
  Si vous vous êtes connecté avec un nouveau compte Bitdefender et n'avez pas de code d'activation, vous pouvez utiliser gratuitement le produit pendant 14 jours.
- **Protection web**. si votre appareil vous demande l'Accessibilité pour activer la Protection Web, appuyez sur **ACTIVER**. Vous serez alors redirigé vers le menu Accessibilité. Tapez Bitdefender Mobile Security, et activez l'option correspondante.
- **Scanner Antimalware**. Réalise une analyse ponctuelle pour garantir que votre appareil ne contient aucune menace. Pour démarrer la procédure d'analyse, appuyez sur **ANALYSER MAINTENANT**.
  Dès que la procédure d'analyse commence, le tableau de bord apparait. Vous pouvez voir ici l'état de la sécurité de votre appareil.

## 5.2.5. Tableau de bord

Cliquez sur l'icône de Bitdefender Mobile Security dans la liste des applications de votre appareil pour ouvrir l'interface de l'application.

Le tableau de bord vous donne des informations sur l'état de la sécurité de votre appareil et, par le biais d'Autopilot, vous aide à améliorer la sécurité de votre appareil en vous recommandant des fonctionnalités.

La carte d'état en haut de la fenêtre vous informe de l'état de la sécurité de l'appareil par le biais de messages et de couleurs explicites. Si aucune

alerte n’est en cours dans Bitdefender Mobile Security, la carte d'état est verte. Lorsqu’un problème de sécurité est détecté, la carte d'état devient rouge.

Pour vous offrir une utilisation efficace et une meilleure protection lorsque vous menez à bien diverses activités, **Bitdefender Autopilot** jouera le rôle de conseiller de sécurité personnel. En fonction de votre activité, Bitdefender Autopilot vous proposera des recommandations contextuelles basées sur votre utilisation de l’appareil et vos besoins. Vous pourrez ainsi découvrir et profiter des avantages apportés par les fonctionnalités de l’application Bitdefender Mobile Security.

A chaque fois qu'un processus est en cours ou qu'une fonctionnalité nécessite votre avis, une carte avec plusieurs informations et actions possibles est affichée dans le tableau de bord.

Depuis la barre de navigation inférieure, vous pouvez accéder aux fonctionnalités de Bitdefender Mobile Security et naviguer facilement :

**Scanner Antimalware**

Vous permet de lancer une analyse à la demande et d'activer l'analyse de la mémoire. Pour plus d'informations, reportez-vous à Analyse Antimalware (page 202).

**Protection web**

Vous garantit une navigation sur Internet en toute sécurité en vous signalant les pages web présentant un risque. Pour plus d'informations, reportez-vous à Protection Web (page 205).

**VPN**

Chiffre la communication à Internet, vous permettant d'assurer votre confidentialité, quel que soit le réseau auquel vous êtes connecté. Pour plus d'informations, reportez-vous à VPN (page 206).

**Scam Alert**

Vous protège en vous alertant lorsque des liens malveillants vous parviennent via SMS, via des applications de messagerie ou via tout type de notification. Pour plus d'informations, référez-vous à Scam Alert (page 209).

**Antivol**

Vous permet d'activer ou de désactiver les fonctionnalités de l'Antivol et de le configurer. Pour plus d'informations, reportez-vous à Fonctionnalités Antivol (page 211).

**Confidentialité des comptes**

Vérifie que vos comptes en ligne n'ont pas été victimes d'une brèche de données. Pour plus d'informations, reportez-vous à Confidentialité des comptes (page 215).

**Blocage des applications**

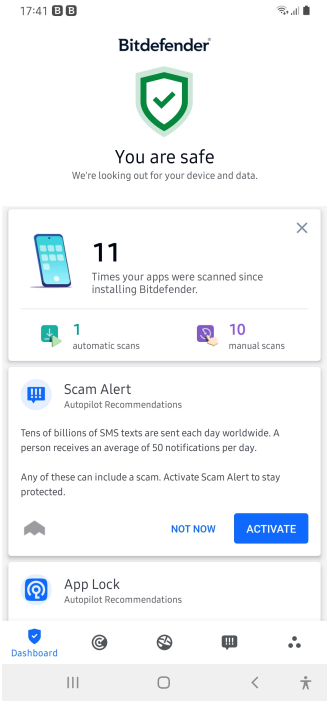
Vous permet de protéger votre apps en configurant un code PIN d'accès. Pour plus d'informations, reportez-vous à App Lock (page 217).

**Reports**

Conserve un journal de l'ensemble des actions importantes, changements d'état et autres messages critiques en lien avec l'activité de votre appareil. Pour plus d'informations, référez-vous à Rapports (page 221).

**WearON**

Communique avec votre montre connectée pour vous aider à localiser votre téléphone en cas de perte. Pour plus d'informations, reportez-vous à WearON (page 222).




## 5.3. Caractéristiques et fonctionnalités

### 5.3.1. Analyse Antimalware

Bitdefender protège votre appareil et vos données contre les apps malveillantes à l'aide des analyses à l'installation et à la demande.

L'interface de Malware Scanner fournit une liste de tous les types de menaces recherchés par Bitdefender. Il suffit d'appuyer sur une menace pour consulter sa définition.

> **Note**
> Vérifiez que votre appareil est connecté à internet. Si il n'est pas connecté, l'analyse ne pourra pas être lancée.

- **Analyse à l'installation**
  Lorsque vous installez une app, Bitdefender Mobile Security l'analyse automatiquement en utilisant sa technologie dans le cloud. La même

procédure d'analyse est réalisée à chaque mise à jour des applications installées.

Si l'application est détectée comme étant malveillante, une alerte s'affichera vous demandant de la désinstaller. Tapez sur **Désinstaller** pour accéder à l'écran de désinstallation de cette app.

- **Analyse à la demande**

  Si vous voulez vous assurer que les applications installées sur votre appareil sont sûres, vous pouvez lancer une analyse à la demande.

  Pour débuter une analyse à la demande :

  1. Dans la barre de navigation inférieure, appuyez sur **Analyse antimalware**.
  2. Appuyez sur **COMMENCER L'ANALYSE**.

  > **Note**
  > Des permissions supplémentaires sont requises sur Android 6 pour la fonctionnalité d'analyse antimalware. Après avoir appuyé sur **COMMENCER L'ANALYSE**, sélectionnez **Autoriser** pour ce qui suit :
  >
  > - Autoriser **Antivirus** à passer et gérer les appels ?
  > - Autoriser **Antivirus** à accéder aux photos, médias, et fichiers sur votre périphérique ?

  La progression de l'analyse s'affiche et vous pouvez arrêter le processus à tout moment.

Par défaut, Bitdefender Mobile Security analysera le stockage interne de votre appareil, dont toute carte SD. De cette façon, toute les applications dangereuses se trouvant sur la carte pourront être détectées avant qu'elles ne causent des dommages.

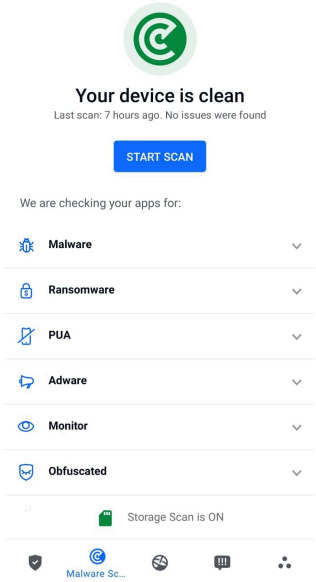
Pour désactiver les paramètres d'analyse stockage :

1. Dans la barre de navigation inférieure, appuyez sur **Plus**.
2. Appuyez sur **Paramètres**.
3. Désactivez **Analyse du stockage** dans la zone Malware Scanner.

Si des applications malveillantes sont détectées, des informations à leur sujet s'afficheront et vous pourrez les supprimer en appuyant sur **DÉSINSTALLER**.

La carte Analyse Malware affiche l'état de votre appareil. Lorsque celui-ci est protégé, la carte est de couleur verte. Lorsque l'appareil nécessite une analyse, ou si une action nécessite votre avis, la carte deviendra rouge.

Si vous possédez la version 7.1 d'Android ou une version plus récente, vous pouvez accéder à un raccourci vers Malware Scanner afin d'effectuer plus rapidement des analyses, sans avoir à ouvrir l'interface Bitdefender Mobile Security. Pour ce faire, appuyez et maintenez une pression sur l'icône Bitdefender de votre écran d'accueil ou de l'App Drawer, puis sélectionnez l'icône .




## Détection des anomalies dans les applications

Bitdefender App Anomaly Detection est une nouvelle technologie intégrée au Bitdefender Malware Scanner pour fournir une couche de protection supplémentaire en surveillant et en détectant en permanence tout comportement malveillant et en alertant l'utilisateur si des activités suspectes sont identifiées.

Bitdefender App Anomaly Detection protège les utilisateurs même lorsqu'ils ont installé sans le savoir une application dangereuse qui reste

inactive pendant un certain temps ou une application apparemment fiable qui interrompt ses fonctionnalités et devient malveillante.

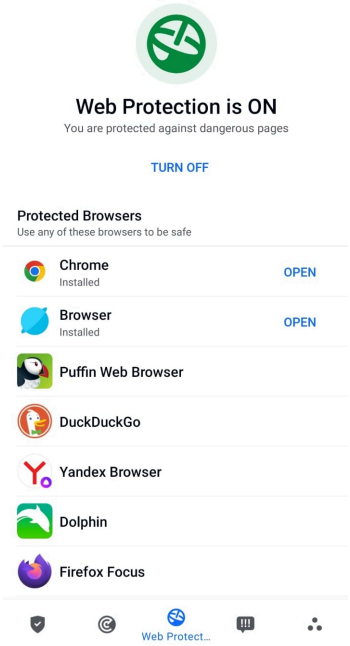
## 5.3.2. Protection Web

La protection Web vérifie, à l'aide des services cloud de Bitdefender, les pages Internet auxquelles vous accédez via le navigateur Android par défaut, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser et Dolphin.

### Note

Des permissions supplémentaires sont nécessaires sur Android 6 pour la fonctionnalité Sécurité Web.

Autoriser l'enregistrement comme service Accessibilité et appuyez sur **ACTIVER** lorsque c'est nécessaire. Appuyez sur **Antivirus** et activez le commutateur, puis confirmez que vous acceptez la permission d'accès à votre périphérique.



À chaque fois que vous accédez à un site bancaire, Bitdefender Web Protection vous propose d'utiliser le VPN Bitdefender. La notification apparaît dans la barre d'état. Nous vous recommandons d'utiliser le VPN Bitdefender lorsque vous vous connectez à votre compte bancaire afin de protéger vos données contre d'éventuelles brèches de sécurité.

Pour désactiver les notifications de la Protection Web :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Désactivez le bouton correspondant dans la zone Protection Web.

## 5.3.3. VPN

Avec le VPN Bitdefender vous pouvez assurer la confidentialité de vos données lorsque vous vous connectez à des réseaux sans-fil non sécurisés dans les aéroports, les commerces, les cafés ou les hôtels. Vous pouvez de cette manière éviter le vol de données personnelles ou les tentatives d'accès des pirates à l'adresse IP de votre appareil.

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 , 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 de Bitdefender VPN. 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.

Il existe deux manières d'activer ou de désactiver le VPN Bitdefender :

- Appuyez sur **CONNECTER** depuis la carte VPN du tableau de bord. L'état du VPN Bitdefender s'affiche.
- Dans la barre de navigation inférieure, appuyez sur **VPN**, puis appuyez sur **CONNEXION**.

Appuyez sur **SE CONNECTER** à chaque fois que vous voulez être protégé quand vous vous connectez à des réseaux sans-fil non sécurisés.

Appuyez sur **SE DÉCONNECTER** quand vous voulez mettre un terme à la connexion.

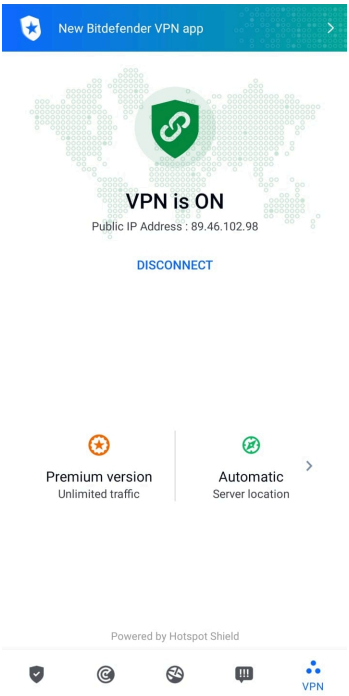
> **Note**
> La première fois que vous activerez le VPN, il vous sera demandé d'autoriser Bitdefender à créer une connexion VPN pour surveiller votre trafic réseau. Appuyez sur **OK** pour continuer.

Si vous possédez la version 7.1 ou une version plus récente d'Android, vous pouvez accéder directement au VPN Bitdefender via un raccourci, sans avoir à ouvrir l'interface Bitdefender Mobile Security.

Pour ce faire, appuyez et maintenez une pression sur l'icône Bitdefender de votre écran d'accueil ou de l'App Drawer, puis sélectionnez l'icône .

Pour économiser de la batterie, nous vous recommandons de désactiver la fonctionnalité VPN quand vous n'en avez pas besoin.

Si vous avez un abonnement Premium, vous pouvez choisir votre serveur en appuyant sur Emplacement du serveur depuis la fonctionnalité VPN, puis en sélectionnant le pays de votre choix. Pour en apprendre plus sur les abonnements VPN, rendez-vous sur




## Paramètres du VPN

Pour accéder aux paramètres avancés de votre VPN :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.

Depuis la zone VPN, vous pouvez configurer les options suivantes :

- Accès rapide au VPN - une notification apparaitra dans la barre d'état de votre appareil pour vous permettre d'activer rapidement le VPN.
- Avertissement réseau Wi-Fi ouvert - à chaque fois que vous vous connecterez à un réseau Wi-Fi ouvert, une notification apparaitra dans la barre d'état pour vous proposer d’activer le VPN.

## Abonnements

Le VPN Bitdefender vous offre gratuitement 200 Mo de trafic par jour et par appareil afin de sécuriser vos connexions chaque fois que c'est

nécessaire, 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 Premium du VPN Bitdefender à tout moment en appuyant sur **Activer Premium** dans la fenêtre du VPN.

L'abonnement à la version Premium du VPN Bitdefender est indépendant de l'abonnement à Bitdefender Mobile Security ; cela signifie que vous pourrez l'utiliser pendant toute la durée de votre abonnement au VPN, quel que soit l'état de votre abonnement à la solution de sécurité. Dans le cas où votre abonnement à la version Premium du VPN Bitdefender expirerait alors que votre abonnement à Bitdefender Mobile Security serait encore actif, vous seriez automatiquement rebasculé(e) sur la version gratuite du VPN.

Bitdefender VPN 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.

> **Note**
> Le VPN Bitdefender fonctionne également en tant qu'application autonome sur tous les systèmes d'exploitation pris en charge (à savoir, Windows, macOS, Android et iOS).

### 5.3.4. Scam Alert

La fonctionnalité Scam Alert prend des mesures préventives en amont, traitant les situations potentiellement dangereuses (y compris les menaces liées à des malwares) avant même qu'elles aient eu l'occasion de devenir problématiques. Scam Alert contrôle tous les messages SMS et toutes les notifications Android en temps réel.

Lorsqu'un lien dangereux vous parvient via un message sur votre téléphone, une pop-up d'avertissement s'affiche sur votre écran. Bitdefender vous proposera deux options. La première option vous permettra d'ignorer l'information. La seconde option vous permettra d'**AFFICHER LES DÉTAILS**. Ces détails vous fourniront plus

d'informations sur l'incident, ainsi que quelques conseils essentiels, tels que :

- Si un lien dangereux est détecté, ne l'ouvrez pas et ne le transférez pas.
- Dans la mesure du possible, supprimez le message concerné.
- Bloquez l'expéditeur si ce n'est pas un contact digne de confiance.
- Désinstaller l'application qui envoie des liens dangereux via des notifications.

> **Note**
> En raison de limitations inhérentes au système d'exploitation Android, Bitdefender n'est pas en mesure de supprimer les messages texte ni de prendre de mesures directes en lien avec des messages SMS ou toute autre source de notifications malveillantes. Si vous ignorez un avertissement émis par Scam Alert et essayez d'ouvrir un lien dangereux, la fonctionnalité Protection Web de Bitdefender l'interceptera automatiquement, empêchant ainsi la compromission de votre appareil.

## Activer Scam Alert

Pour activer Scam Alert, vous devez autoriser l'application Bitdefender Mobile Security à accéder aux messages SMS et au système de notification :

1. Ouvrez l'application Bitdefender Mobile Security installée sur votre téléphone ou votre tablette Android.
2. Sur l'écran d'accueil de l'application Bitdefender, appuyez sur l'option **Scam Alert** située dans la barre de navigation inférieure, puis appuyez sur **ACTIVER**.
3. Appuyez sur le bouton **AUTORISER**.
4. Dans la liste Accès aux notifications, faites basculer Bitdefender Security sur la position **active**.
5. Confirmez l'action en appuyant sur **AUTORISER**.
6. Revenez à l'écran Scam Alert et appuyez sur **AUTORISER** pour autoriser Bitdefender à analyser les messages SMS entrants.

## Protection des conversations en direct (chats) en temps réel

Les messageries instantanées (chats) offrent un moyen simple de garder le contact, mais elles permettent également aux liens dangereux de vous atteindre facilement.

Lorsque vous activez la fonctionnalité de protection des messageries instantanées (Chat Protection), le module Scam Alert, qui protège déjà vos messages texte et vos notifications, protège aussi vos messageries instantanées contre les attaques basées sur des liens, en détectant les liens dangereux que vous recevez ou que vous envoyez lors de vos discussions.

Pour activer la protection des conversations instantanées :

1. Ouvrez l'application Bitdefender Mobile Security installée sur votre téléphone ou tablette Android.
2. Sur l'écran d'accueil de l'application Bitdefender, appuyez sur l'option **Scam Alert** située dans la barre de navigation inférieure.
3. La fonctionnalité Chat Protection s'affichera en haut de l'onglet Scam Alert. Faites basculer l'interrupteur correspondant sur la position **active**.

> **Note**
> Actuellement, la protection des conversations instantanées est compatible avec les applications suivantes :
>
> - WhatsApp
> - Facebook Messenger
> - Telegram
> - Discord

## 5.3.5. Fonctionnalités Antivol

Bitdefender peut vous aider à localiser votre appareil et empêche que vos données personnelles finissent entre de mauvaises mains.

Il vous suffit d'activer Antivol à partir de l'appareil et, en cas de besoin, d'accéder à **Bitdefender Central** à partir de n'importe quel navigateur Web, partout.

Note

Un lien situé sur l'interface d'Antivol vous permettra de télécharger l'application Bitdefender Central sur Google Play si ce n'est pas déjà fait.

Bitdefender Mobile Security propose les fonctionnalités antivol suivantes :

**Localisation à distance**

Afficher l'endroit où se trouve votre 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.

**Verrouillage à distance**

Verrouillez l'écran de votre appareil et choisissez un code PIN numérique pour le déverrouiller.

**Effacement du contenu de l'appareil à distance**

Supprimer à distance toutes les données personnelles de votre appareil.

**Envoyer une alerte à l'appareil (alarme)**

Envoyer un message à distance à afficher à l'écran de l'appareil, ou faites émettre un son à l'appareil.

Si vous perdez votre appareil, vous pouvez indiquer à la personne qui le trouve comment vous le rapporter en affichant un message sur l'écran de l'appareil.

Si vous avez égaré votre appareil et qu'il est possible qu'il ne soit pas loin (par exemple, chez vous ou au bureau), quoi de mieux pour le trouver que

de lui faire émettre un son fort ? Le son sera émis même si l'appareil est en mode silencieux.

## Activer l'Antivol

Pour activer les fonctionnalités Antivol, veuillez simplement terminer le processus de configuration à partir de la carte Antivol disponible sur le tableau de bord.

Alternativement, vous pouvez activer Antivol en suivant les étapes suivantes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Appuyez sur **Antivol**.
3. Appuyez sur **ACTIVER**.
4. La procédure suivante vous aidera à activer cette fonctionnalité :

> **Note**
> Les permissions supplémentaires sont nécessaires sous Android 6 pour la fonctionnalité Antivol.
>
> Pour l'activer, suivez ces étapes :
>
> a. Appuyez sur **Activer l'antivol**, puis appuyez sur **ACTIVER**.
>
> b. Autoriser les permissions pour **Antivirus** à avoir accès à l'emplacement du votre périphérique.

a. **Octroyer des privilèges d'administrateur**
Ces privilèges sont essentiels au fonctionnement d'Antivol et doivent donc être accordés afin de poursuivre.

b. **Définir le code PIN de l'application**
Un code PIN doit être défini pour éviter tout accès non autorisé à votre appareil. Le code PIN devra être saisi avant toute utilisation de votre appareil. Sur les appareils compatibles avec l'authentification par empreintes digitales, cette méthode peut être utilisée à la place du code PIN.
Le même code PIN est utilisé par Blocage des applications pour protéger les applications que vous avez installées.

c. **Activer Snap Photo**

Lorsque Snap Photo est activé, à chaque fois qu'une personne essayera de déverrouiller votre appareil sans succès, Bitdefender prendra une photo d'elle.

Plus précisément, à chaque fois que la confirmation par code PIN, mot de passe ou empreinte digitale que vous avez défini pour protéger votre appareil est saisi de manière incorrecte trois fois de suite, une photo est prise par la caméra frontale. a photo est ensuite enregistrée en indiquant l'heure et la raison, et celle-ci peut être consultée en accédant à la fenêtre Antivol de Bitdefender Mobile Security.

Vous pouvez également consulter les photos prises depuis votre compte Bitdefender :

i. Aller à: https://central.bitdefender.com.

ii. Connectez-vous à votre compte.

iii. Sélectionnez le **Mes appareils** panneau.

iv. Sélectionnez votre appareil Android, puis rendez-vous dans l'onglet **Antivol**.

v. Appuyez sur ⋮ à côté de l'option **Afficher les instantanés** pour visualiser les dernières photos prises.
Seules les deux dernières photos sont sauvegardées.

Une fois la fonction antivol est activée, vous pouvez activer ou désactiver les commandes de contrôle Web individuellement à partir de la fenêtre Antivol en appuyant sur les options correspondantes.

## Utiliser les fonctionnalités Antivol depuis Bitdefender Central

> **Note**
> Toutes les fonctions Antivol requièrent que l'option **Données en arrière plan** soit activée dans les paramètres Utilisation des données de votre appareil.

Pour accéder aux fonctionnalités antivol à partir de votre compte Bitdefender :

1. Accédez à **Bitdefender Central**.
2. Sélectionnez le **Mes appareils** panneau.

3. Dans la fenêtre **MES APPAREILS**, sélectionnez la carte de l'appareil que vous souhaitez consulter en appuyant sur le bouton **Afficher les détails** qui lui est associé.
4. Sélectionnez l'onglet **Antivol**.
5. Appuyez sur le bouton correspondant à la fonctionnalité que vous souhaitez utiliser :
   **Localiser** - permet d'afficher la localisation de votre appareil sur Google Maps.
   **Afficher IP** - affiche la dernière adresse IP pour l'appareil sélectionné.
   **Alerter** - saisissez un message à afficher sur l'écran de votre appareil et/ou faites émettre un son à votre appareil.
   **Verrouiller** - verrouillez votre appareil et définissez un code PIN permettant de le déverrouiller.
   **Effacer** - supprimez toutes les données de votre appareil.

   > **Important**
   > Une fois les données d'un appareil effacées, toutes les fonctionnalités Antivol cessent de fonctionner.

### Paramètres d'Antivol

Pour activer ou désactiver les commandes à distance :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Antivol**.
3. Activez ou désactivez les options souhaitées.

## 5.3.6. Confidentialité des comptes

Bitdefender Account Privacy détecte si des fuites de données se sont produites sur les comptes que vous utilisez pour effectuer des paiements en ligne et des achats ou pour vous connecter à différents sites Internet ou applications. Parmi les données pouvant être stockées dans un compte figurent les mots de passe, les informations de carte de crédit et les informations bancaires et, si le compte n'est pas correctement sécurisé, une usurpation d'identité ou une violation de la vie privée peuvent survenir.

Le statut de confidentialité d'un compte est affiché juste après la validation.

De nouvelles vérifications automatiques sont programmées pour s'exécuter en arrière-plan, mais des analyses manuelles peuvent également être lancées quotidiennement.

Des notifications seront affichées chaque fois que de nouvelles brèches impliquant l'un des comptes de messagerie validés seront découvertes.

Pour commencer à protéger des informations personnelles :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Appuyez sur **Confidentialité du compte**.
3. Appuyez sur **COMMENCER**.
4. L'adresse e-mail utilisée pour créer votre compte Bitdefender apparait et est automatiquement ajoutée à la liste des comptes pris en charge.
5. Pour ajouter un autre compte, appuyez sur **AJOUTER UN COMPTE** dans la fenêtre Confidentialité des comptes, puis saisissez l'adresse e-mail.
   Appuyez sur **AJOUTER** pour continuer.
   Bitdefender doit valider ce compte avant d'afficher des informations privées. Par conséquent, un e-mail contenant un code de validation est envoyé à l'adresse e-mail fournie.
   Consultez votre boîte de réception, puis saisissez le code reçu dans la section **Confidentialité du compte** de votre application. Si vous ne trouvez pas l'e-mail de validation dans le dossier Boîte de réception, vérifiez le dossier Spam.
   Le statut de confidentialité du compte validé est affiché.

Si des brèches sont détectées sur l'un de vos comptes, nous vous conseillons d'en modifier le mot de passe dès que possible. Voici quelques astuces pour créer un mot de passe fiable et sécurisé :

- Choisissez un mot de passe comportant au moins huit caractères.
- Incluez des minuscules et des majuscules.
- Intégrez au moins un chiffre ou un symbole, tel que #, @, % ou !.

Après avoir sécurisé un compte victime d'une atteinte à la vie privée, vous pouvez confirmer les changements en marquant la ou les brèches identifiées comme Résolues. Pour cela :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Confidentialité du compte**.
3. Sélectionnez le compte que vous venez de sécuriser.
4. Appuyez sur la brèche pour laquelle vous avez sécurisé votre compte.
5. Appuyez sur **RÉSOLU** pour valider le fait que le compte est sécurisé.

Lorsque toutes les brèches détectées sont marquées comme **Résolues**, le compte n'apparaît plus comme victime de brèche, du moins tant qu'une nouvelle brèche n'est pas détectée.

Pour ne plus recevoir de notification à chaque fois qu'une analyse automatique est terminée :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Désactivez le bouton correspondant dans la zone Confidentialité des comptes.

## 5.3.7. App Lock

Les applications installées comme les e-mails, photos ou messages peuvent contenir des données personnelles que vous souhaiteriez conserver privées en limitant de façon sélective leur accès.

App Lock vous aide à bloquer les accès indésirables aux applications en configurant un code PIN d'accès. Ce code PIN doit contenir au moins 4 chiffres, mais pas plus de 8, et est requis à chaque fois que vous souhaitez accéder aux applications sélectionnées à l'accès restreint.

L'authentification biométrique (telle que la confirmation par empreinte digital ou par reconnaissance faciale) peut être utilisée à la place du code PIN configuré.

### Activer Blocage des applications

Pour limiter l'accès aux applications sélectionnées, configurez App Lock à partir de la carte affichée sur le tableau de bord après avoir activé Antivol.

Alternativement, vous pouvez activer App Lock en suivant les étapes suivantes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Appuyez sur **Blocage des applications**.
3. Robinet **ALLUMER**.
4. Autoriser Bitdefender Security à accéder aux données d'utilisation.
5. Autoriser la **superposition d'écrans**.
6. Retournez dans l'application et appuyez sur **CONFIGURER CODE PIN** pour confirmer le code d'accès.

> **Note**
> Cette étape n'est disponible que si vous n'avez pas précédemment configuré de PIN dans Antivol.

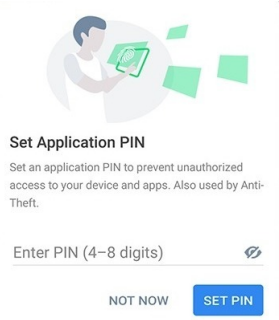
7. Activez l'option Snap Photo pour prendre en flagrant délit tout intrus essayant d'accéder à vos données personnelles.

> **Note**
> Des permissions supplémentaires sont nécessaires sur Android 6 pour la fonctionnalité Snap Photo. Pour l'activer, autorisez**Antivirus** à prendre des photos et des vidéos.

8. Sélectionnez les applications que vous souhaitez protéger.

Après 5 erreurs de code PIN ou empreintes digitales incorrectes, l'application marque une pause de 30 secondes. De cette manière, toute tentative d'utilisation des applications protégées sera bloquée.

> **Note**
> Le même code PIN est utilisé par l'Antivol pour vous aider à localiser votre appareil.



## Mode de verrouillage

La première fois que vous ajoutez une application à App Lock, l'écran Mode de verrouillage des applications apparait. Vous pouvez ici choisir quand la fonctionnalité App Lock doit protéger les applications installées sur votre appareil.

Vous pouvez sélectionner l'une des options suivantes :

- **Nécessite un déverrouillage à chaque utilisation** - le code PIN ou l'empreinte digitale définie devra être utilisé à chaque fois que vous accédez à l'application verrouillée.
- **Laisser déverrouillé jusqu'à extinction de l'écran** - l'accès à vos applications sera possible jusqu'à ce que votre écran s'éteigne.
- **Verrouiller après 30 secondes** -vous avez 30 secondes pour revenir sur une application déverrouillée.

Si vous voulez modifier le réglage sélectionné :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Appuyez sur **Nécessite un déverrouillage à chaque utilisation** dans la zone App Lock.
4. Choisissez l'option désirée.

## Paramètres de Blocage des applications

Pour accéder aux paramètres avancés de App Lock :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.

Depuis la zone App Lock, vous pouvez configurer les options suivantes :

- **Suggestion d'applications sensibles** - recevez une notification de verrouillage à chaque fois que vous installez une application sensible.
- **Nécessite un déverrouillage à chaque utilisation** - choisissez l'une des options de verrouillage et de déverrouillage disponibles.
- **Smart Unlock** - les applications restent déverrouillées quand vous êtes connecté à un réseau Wi-Fi de confiance.

- **Clavier aléatoire** - empêche la lecture du code PIN en plaçant les chiffre de manière aléatoire sur le clavier.

## Snap photo

L'option Snap Photo de Bitdefender vous permet de prendre vos amis et vos proches la main dans le sac et de leur donner une bonne leçon en matière de vie privée : ils ne sont pas censés consulter vos fichiers personnels ni les applications que vous utilisez.

La fonction est simple à chaque fois que la confirmation par code PIN ou empreinte digitale que vous avez défini pour protéger vos applications est saisi de manière incorrecte trois fois de suite, une photo est prise par la caméra frontale. La photo est ensuite enregistrée en indiquant l'heure et la raison, et celle-ci peut être consultée en dans la section App Lock de Bitdefender Mobile Security.

> **Note**
> Cette fonctionnalité est disponible seulement sur les téléphones qui ont une caméra frontale.

Pour configurer la fonctionnalité Snap Photo de App Lock :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Activez le bouton correspondant dans la zone Snap Photo.

Les photos prises lorsque le code PIN saisi n'est pas correct sont affichées dans la fenêtre App Lock et peuvent être vues en plein écran.

Alternativement, vous pouvez les voir dans votre compte Bitdefender :

1. Aller à: https://central.bitdefender.com.
2. Connectez-vous à votre compte.
3. Sélectionnez la section **Mes Appareils**.
4. Sélectionnez votre appareil Android, puis le **Antivol** languette.
5. Robinet près de **Vérifiez vos instantanés** pour voir les dernières photos prises.

Seules les deux photos les plus récentes sont enregistrées.

Pour ne plus envoyer les photos sur votre compte Bitdefender :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Désactiver **Envoyer les photos** dans la zone Snap Photo.

### Smart Unlock

Pour ne plus avoir à vous authentifier par code PIN ou empreinte digitale sur vos applications protégées à chaque fois que vous les ouvrez, le plus simple est d'activer Smart Unlock.

Avec Smart Unlock vous pouvez définir des réseaux Wi-Fi de confiance auxquels vous vous connectez fréquemment, et désactiver le blocage de App Lock lorsque vous êtes connecté à ceux-ci.

Pour configurer la fonctionnalité Smart Unlock :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Verrou d'application**.
3. Appuyez sur le bouton .
4. Appuyez sur le bouton situé à côté de **Smart Unlock**, si la fonctionnalité n'est pas encore activée.
   Validez à l'aide de votre empreinte digitale ou de votre code PIN.
   Lorsque vous activerez cette fonctionnalité pour la première fois, vous devrez autoriser la localisation. Appuyez sur le bouton **AUTORISER**, puis appuyez de nouveau sur **AUTORISER**.
5. Appuyez sur **AJOUTER** pour définir le réseau Wi-Fi sur lequel vous êtes connecté comme étant de confiance.

Chaque fois que vous changez d'avis, désactivez la fonctionnalité et les réseaux Wi-Fi que vous avez configuré comme fiables seront traités comme non fiables.

## 5.3.8. Rapports

La fonctionnalité Rapports tient un journal détaillé des événements liés à l'activité d'analyse de votre appareil.

Lorsqu'un événement lié à la sécurité de votre appareil a lieu, un nouveau message est ajouté aux Rapports.

Pour accéder à la rubrique Rapports :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Appuyez sur **Rapports**.

Les onglets suivants sont disponibles sur la fenêtre de rapport :

- **RAPPORTS HEBDOMADAIRES** - vous avez ici accès à l'état de sécurité et aux tâches réalisées pendant cette semaine et la semaine dernière. Le rapport de la semaine est généré tous les dimanches et vous recevrez une notification vous informant de sa disponibilité.
  Chaque semaine un nouveau conseil sera affiché dans cette rubrique, alors n'oubliez pas de regarder régulièrement pour utiliser l'application au mieux.
  Pour ne plus recevoir de notification à chaque fois qu'un rapport est généré :
  1. Robinet **Plus** dans la barre de navigation inférieure.
  2. Robinet **Paramètres**.
  3. Désactivez le bouton **Notification de nouveau rapport** dans la zone Rapports.
- **JOURNAL D'ACTIVITÉ** - vous pouvez ici consulter les informations détaillées sur l'activité de votre application Bitdefender Mobile Security depuis son installation sur votre appareil Android.
  Pour supprimer un journal d'activité disponible :
  1. Robinet **Plus** dans la barre de navigation inférieure.
  2. Robinet **Paramètres**.
  3. Appuyez sur **Effacer le journal d'activité**, puis appuyez sur **EFFACER**.

## 5.3.9. WearON

Bitdefender WearON vous permet de retrouver facilement votre smartphone, que vous l'ayez oublié au bureau dans une salle de conférence ou sous l'un des coussins de votre canapé. L'appareil peut être retrouvé même s'il est en mode silencieux.

Conservez cette fonctionnalité activée pour vous assurer que votre smartphone est toujours à votre portée.

Note
La fonctionnalité fonctionne avec Android 4.3 et Android Wear.

### Activer WearON

Pour utiliser WearON, connectez simplement votre montre connectée à l'application Bitdefender Mobile Security et activez la fonctionnalité à l'aide de la commande vocale suivante :

Commencer : <Où est mon téléphone>

**Bitdefender WearON** dispose de deux commandes :

1. **Alerte téléphone**
   La fonctionnalité Alerte Téléphone vous permet de retrouver facilement votre smartphone lorsque vous vous en éloignez trop.
   Si vous avez une montre connectée, celle-ci détectera automatiquement l'application sur votre téléphone et celui-ci vibrera quand il ne sera pas à portée de votre montre et que la connectivité Bluetooth est perdue.
   Pour activer cette fonctionnalité, ouvrez Bitdefender Mobile Security, sélectionnez **Paramètres globaux** dans le menu puis le bouton correspondant sous la section WearON.
2. **Alarme**
   Retrouver votre téléphone n'a jamais été aussi simple. Lorsque vous oubliez où vous avez laissé votre téléphone, appuyez sur la commande Faire émettre un son de votre montre afin de faire émettre un son à votre téléphone.

## 5.3.10. À propos de

Pour connaitre la version de Bitdefender Mobile Security que vous utilisez, et consulter les Conditions d'utilisation de l'abonnement, la Politique de confidentialité et les licences open-sources :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Appuyez sur l'option souhaitée dans la zone À propos.

## 5.4. Questions les Plus Fréquentes

**Pourquoi la solution Bitdefender Mobile Security nécessite-t-elle une connexion à Internet ?**

L'application a besoin de communiquer avec les serveurs de Bitdefender afin de déterminer l'état de sécurité des applications qu'elle analyse et des pages web que vous consultez et pour recevoir des commandes de votre compte Bitdefender, lorsque vous utilisez les fonctionnalités de l'Antivol.

**Pourquoi Bitdefender Mobile Security a-t-il besoin de chaque permission ?**

- Accès Internet -> utilisé pour les communications cloud.
- Consulter l'état et l'identité du téléphone -> utilisé pour déterminer si l'appareil est connecté à Internet et pour extraire certaines informations de l'appareil nécessaires à la création d'un identifiant unique aux fins de la communication avec le cloud Bitdefender.
- Lire et écrire les favoris du navigateur -> le module de protection Web supprime les sites malveillants de votre historique de navigation.
- Lire les données du journal -> Bitdefender Mobile Security détecte les traces d'activités malveillantes dans les journaux Android.
- Localisation -> requise pour la localisation à distance.
- Appareil photo -> requis pour l'utilisation du module Snap Photo.
- Stockage -> utilisé pour autoriser l'analyse antimalware à vérifier la carte SD.

**Comment ne plus envoyer d'informations à Bitdefender au sujet des applications suspectes ?**

Par défaut, Bitdefender Mobile Security envoie des rapports aux serveurs Bitdefender sur les applications suspectes que vous installez. Ces informations sont essentielles pour améliorer la détection des menaces et peuvent nous aider à vous offrir une meilleure expérience à l'avenir. Si vous souhaitez cesser de nous envoyer les informations relatives aux applications suspectes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.

3. Désactivez la **Détection dans le cloud** dans la zone Malware Scanner.

**Où puis-je trouver des informations sur l'activité de l'application ?**

Bitdefender Mobile Security tient un journal de toutes les actions importantes, des modifications d'état et d'autres messages critiques liés à son activité. Pour accéder aux activités de l'application :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Rapports**.
   La fenêtre RAPPORTS HEBDOMADAIRES vous donne accès aux rapports générés chaque semaine et la fenêtre JOURNAL D'ACTIVITÉ vous donne des informations sur l'activité de votre application Bitdefender.

**J'ai oublié le code PIN que j'avais choisi pour protéger mon app. Que puis-je faire ?**

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes appareils** panneau.
3. Appuyez sur la carte de l'appareil qui vous intéresse, puis sur dans le coin supérieur droit de l'écran.
4. Sélectionner **Paramètres**.
5. Récupérez le code PIN à partir du champ **Application PIN**.

**Comment modifier le code PIN que j'ai défini pour App Lock et Antivol ?**

Pour modifier le code PIN que vous avez défini pour App Lock et Antivol :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Appuyez sur **CODE PIN** de sécurité dans la zone Antivol.
4. Saisissez le code PIN actuel.
5. Saisissez le code PIN que vous voulez utiliser.

**Comment désactiver la fonction App Lock ?**

La fonction App Lock ne peut pas être éteinte, mais vous pouvez la désactiver en effaçant les cases à cocher situées à côté des applications sélectionnées après vous être authentifié par code PIN ou empreinte digitale.

**Comment définir un autre réseau sans fil comme étant de confiance ?**

Vous devez d'abord connecter votre appareil au réseau sans-fil que vous voulez définir comme étant de confiance. Ensuite, suivez les instructions suivantes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Verrou d'application**.
3. Appuyez sur dans le coin supérieur droit.
4. Appuyez sur **AJOUTER** à côté du réseau que vous voulez définir comme de confiance.

**Comment faire pour ne plus voir les photos prises avec mes appareils ?**

Pour ne plus voir les photos prises sur vos appareils :

1. Accès Centrale Bitdefender.
2. Appuyez sur dans le coin supérieur droit de l'écran.
3. Appuyez sur **Paramètres** dans le menu coulissant.
4. Désactivez l'option **Afficher/Ne pas afficher les instantanés pris sur vos appareils**.

**Comment puis-je sécuriser mes achats en ligne ?**

Les achats en ligne comportent des risques élevés lorsque certains aspects sont ignorés. Pour éviter d'être victime d'une fraude, nous vous recommandons de procéder comme suit :

- Veillez à ce que votre application de sécurité soit à jour.
- Ne soumettez de paiements en ligne qu'avec une protection de l'acheteur.
- Utilisez un VPN lorsque vous vous connectez à internet depuis des réseaux sans fil publics et non sécurisés.
- Prêtez attention aux mots de passe que vous attribuez à vos comptes en ligne. Ils doivent être fiables et comporter des majuscules et des minuscules, des chiffres et des symboles (@, !, %, #, etc.).
- Veillez à ce que les informations que vous envoyez le soient sur des connexions sécurisées. L'extension du site Internet doit être HTTPS:// et non HTTP://.

**Quand dois-je utiliser le VPN Bitdefender ?**

Vous devez être prudent lorsque vous accédez à des contenus, ou téléchargez/envoyez des données sur internet. Pour être certain de naviguer sur le web en toute sécurité, nous vous recommandons d'utiliser le VPN Bitdefender lorsque vous voulez :

- vous connecter à des réseaux sans-fil publics
- accéder à des contenus normalement disponibles uniquement depuis certaines régions, que vous soyez ou non chez vous
- assurer la confidentialité de vos données personnelles (identifiants, mots de passe, informations bancaires, etc.)
- masquer votre adresse IP

**Le VPN Bitdefender aura-t-il une incidence négative sur l'autonomie de mon appareil ?**

Le VPN Bitdefender a été conçu pour protéger vos données personnelles, masquer votre adresse IP quand vous êtes connecté à des réseaux sans-fil non sécurisés, et accéder à des contenus normalement indisponibles dans votre pays. Pour éviter d'utiliser pour rien la batterie de votre appareil, nous vous recommandons d'utiliser uniquement le VPN quand vous en avez besoin, et de le déconnecter quand vous êtes hors ligne.

**Pourquoi ma connexion à Internet ralentit-elle parfois lorsque je suis connecté(e) au VPN Bitdefender ?**

Bitdefender VPN a été pensé pour ne pas déranger votre navigation sur le web, mais votre connectivité à Internet ou la distance par rapport au serveur auquel vous êtes connecté peuvent provoquer des ralentissements. Dans ce cas, si vous n'êtes pas obligé d'être connecté à un serveur lointain (p.ex. en Chine) nous vous recommandons d'autoriser le VPN Bitdefender à se connecter automatiquement au serveur le plus proche, ou de trouver un serveur plus proche de là où vous vous situez.

**Puis-je modifier le compte Bitdefender associé à mon appareil ?**

Oui, vous pouvez facilement changer le compte Bitdefender lié à votre appareil en suivant les étapes suivantes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Saisissez votre adresse e-mail.
3. Appuyez sur **Se déconnecter de votre compte**. Si un code PIN a été défini, il vous est demandé de le saisir.

4. Confirmez votre choix.
5. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants, et appuyez sur **CONNEXION**.

**Quel est l'impact de Bitdefender Mobile Security sur les performances et l'autonomie de la batterie de mon appareil ?**

L'impact est très faible. L'application s'exécute uniquement lorsque c'est essentiel - après l'installation d'une application, lorsque vous accédez à l'interface de l'application ou lorsque vous souhaitez un contrôle de sécurité. Bitdefender Mobile Security ne s'exécute pas en arrière-plan lorsque vous appelez vos amis, tapez un message ou jouez.

**Qu'est-ce que la fonctionnalité Administrateur de l'appareil ?**

La fonctionnalité Administrateur de l'appareil est une fonctionnalité Android qui octroie à Bitdefender Mobile Security les permissions nécessaires pour effectuer certaines tâches à distance. Sans ces privilèges, le verrouillage à distance ne fonctionnerait pas et la fonctionnalité d'effacement des données de l'appareil ne serait pas capable de supprimer complètement vos données. Si vous souhaitez supprimer l'application, veillez à supprimer ces privilèges dans **Paramètres > Sécurité > Administrateurs de l'appareil** avant d'essayer de la désinstaller.

**Comment résoudre l'erreur "Aucun jeton Google" qui apparaît lorsque vous vous connectez à Bitdefender Mobile Security.**

Cette erreur apparaît quand l'appareil n'est associé à aucun compte Google, ou si l'appareil est associé avec un compte mais qu'il existe un problème temporaire de connexion avec Google. Essayez l'un des solutions suivantes :

- Allez dans Paramètres Android > Applications > Gérer les applications > Bitdefender Mobile Security, puis appuyez sur **Supprimer les données**. Réessayez ensuite de vous connecter.
- Soyez certain que votre appareil est associé à un compte Google.
  Pour le vérifier, allez dans Paramètres > Comptes et vérifiez si un compte Google est listé sous **Gérer les comptes**. Ajoutez un compte si aucun n'est listé, redémarrez votre appareil, puis essayez de vous connecter.

- Redémarrez votre appareil, puis essayez de nouveau de vous connecter.

**Dans quelles langues Bitdefender Mobile Security est-il disponible ?**

Bitdefender Mobile Security est actuellement disponible dans les langues suivantes :

- Brésilien
- Tchèque
- Néerlandais
- Anglais
- Français
- Allemand
- Grec
- Hongrois
- Italien
- Japonais
- Coréen
- Polonais
- Portugais
- Roumain
- Russe
- Espagnol
- Suédois
- Thaï
- Turc
- Vietnamien

D'autres langues seront ajoutées avec les prochaines versions. Pour modifier la langue de l'interface de Bitdefender Mobile Security, allez dans les paramètres **Langue & clavier** de votre appareil et sélectionnez la langue que vous souhaitez utiliser sur votre appareil.

# 6. SÉCURITÉ MOBILE POUR IOS

## 6.1. Qu'est-ce que Bitdefender Mobile Security pour iOS

Les activités en ligne telles que le paiement de factures, la réservation de vacances ou l'achat de biens et de services sont pratiques et sans tracas. Mais comme de nombreuses activités ont évolué sur Internet, celles-ci comportent des risques élevés et, si les détails de sécurité sont ignorés, des données personnelles peuvent être piratées. Et quoi de plus important que de protéger les données stockées dans les comptes en ligne et sur le smartphone personnel ?

Bitdefender Mobile Security pour iOS vous permet de :

- Bénéficiez de la protection la plus puissante contre les menaces avec le moins d'impact sur la batterie
- Protégez vos données personnelles : mots de passe, adresse, informations sociales et financières
- Vérifiez facilement la sécurité de votre téléphone pour détecter et corriger les erreurs de configuration qui pourraient l'exposer
- Évitez l'exposition accidentelle des données et l'utilisation abusive de toutes les applications installées
- Analysez votre appareil pour obtenir des paramètres de sécurité et de confidentialité optimaux
- Obtenez des informations sur l'utilisation de votre activité en ligne et l'historique des incidents évités
- Vérifiez vos comptes en ligne contre les violations de données ou les fuites de données
- Crypter le trafic Internet avec le VPN inclus

Bitdefender Mobile Security pour iOS est fourni gratuitement et nécessite une activation avec un Compte Bitdefender. Cependant, certaines fonctionnalités importantes de Bitdefender, telles que notre module 'Web Protection', nécessitent un abonnement payant pour être accessibles à nos utilisateurs.

# 6.2. Commencer

## 6.2.1. Configuration requise pour l'appareil

Bitdefender Mobile Security pour iOS fonctionne sur tout appareil exécutant iOS 12 ou des versions ultérieures du système d'exploitation et a besoin d'une connexion Internet active pour être activé et pour détecter si une fuite de données s'est produite dans vos comptes en ligne.

## 6.2.2. Installation de Bitdefender Mobile Security pour iOS

- **De Bitdefender Central**
  - Sur iOS
    1. Accès Centrale Bitdefender.
    2. Sélectionnez le **Mes appareils** panneau.
    3. Robinet **INSTALLER LA PROTECTION**, puis appuyez sur **Protégez cet appareil**.
    4. Sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
    5. Vous êtes redirigé vers le **Magasin d'applications** application. Dans l'écran App Store, appuyez sur l'option d'installation.
  - Sur Windows, macOS, Androïd
    1. Accès Centrale Bitdefender.
    2. Sélectionnez le **Mes appareils** panneau.
    3. Presse **INSTALLER LA PROTECTION**, puis appuyez sur **Protégez d'autres appareils**.
    4. Sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
    5. Presse **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**.
    6. Saisissez une adresse e-mail dans le champ correspondant et appuyez sur **ENVOYER UN COURRIEL**. Notez que le lien de téléchargement généré n'est valable que pour les prochaines 24

heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes étapes.

7. Sur l'appareil que vous souhaitez installer Bitdefender, vérifiez le compte de messagerie que vous avez saisi, puis appuyez sur le bouton de téléchargement correspondant.

- **À partir de l'App Store**
  Recherchez Bitdefender Mobile Security pour iOS pour localiser et installer l'application.

Une fenêtre d'introduction contenant des détails sur les fonctionnalités du produit s'affiche la première fois que vous ouvrez l'application. Appuyez sur Commencer pour passer à la fenêtre suivante.

Avant de passer par les étapes de validation, vous devez accepter le contrat d'abonnement. Veuillez prendre le temps de lire le Contrat d'abonnement car il contient les termes et conditions selon lesquels vous pouvez utiliser Bitdefender Mobile Security pour iOS.

Robinet **Continuer** pour passer à la fenêtre suivante.

### 6.2.3. Connectez-vous à votre compte Bitdefender

Pour utiliser Bitdefender Mobile Security pour iOS, vous devez lier votre appareil à un compte Bitdefender, Facebook, Google, Apple ou Microsoft en vous connectant au compte depuis l'application. La première fois que vous ouvrez l'application, vous êtes invité à vous connecter à un compte.

Pour lier votre appareil à un compte Bitdefender :

1. Saisissez l'adresse e-mail de votre compte Bitdefender dans le champ correspondant, puis appuyez sur **SUIVANT**. Si vous n'avez pas de compte Bitdefender et que vous souhaitez en créer un, sélectionnez le lien correspondant, puis suivez les instructions à l'écran jusqu'à ce que le compte soit activé.
   Pour vous connecter à l'aide d'un compte Facebook, Google, Apple ou Microsoft, appuyez sur le service que vous souhaitez utiliser à partir du **Ou connectez-vous** avec zone. Vous êtes redirigé vers la page de connexion du service sélectionné. Suivez les instructions pour lier votre compte à Bitdefender Mobile Security pour iOS.

> **Note**
> Bitdefender n'a accès 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.

2. Tapez votre mot de passe, puis appuyez sur **S'IDENTIFIER**.

De là, vous pouvez également accéder à la politique de confidentialité de Bitdefender.

### 6.2.4. Tableau de bord

Appuyez sur l'icône Bitdefender Mobile Security pour iOS dans le tiroir d'applications de votre appareil pour ouvrir l'interface de l'application.

La première fois que vous accédez à l'application, vous êtes invité à autoriser Bitdefender à vous envoyer des notifications. Robinet **Permettre** pour rester informé chaque fois que Bitdefender doit vous communiquer quelque chose concernant votre application. Pour gérer les notifications de Bitdefender, accédez à Paramètres > Notifications > Mobile Security.

Pour accéder à la section dont vous avez besoin, appuyez sur l'icône correspondante en bas de l'écran.

**Protection Internet**

Restez en sécurité lorsque vous naviguez sur le Web et chaque fois que des applications moins sécurisées tentent d'accéder à des domaines non approuvés. Pour plus d'informations, reportez-vous à Protection Internet (page 237).

**VPN**

Préservez votre confidentialité quel que soit le réseau auquel vous êtes connecté en cryptant vos communications Internet. Pour plus d'informations, reportez-vous à VPN (page 239).

**Confidentialité du compte**

Découvrez si vos comptes de messagerie ont été divulgués ou non. Pour plus d'informations, reportez-vous à Confidentialité du compte (page 242).

Pour voir des options supplémentaires, appuyez sur le ••• icône sur votre appareil lorsque vous êtes dans l'écran d'accueil de l'application. Les options suivantes s'affichent :

- **Restaurer les achats** - à partir de là, vous pouvez restaurer les abonnements précédents que vous avez achetés via votre compte iTunes.
- **Paramètres** - à partir d'ici vous avez accès à :
  - **Paramètres VPN**
    - **Accord** - vous pouvez lire les conditions d'utilisation du service VPN Bitdefender. Si vous touchez **je ne suis plus d'accord**, vous ne pourrez pas utiliser Bitdefender VPN au moins tant que vous n'aurez pas appuyé sur **Je suis d'accord**.
    - **Ouvrir l'avertissement Wi-Fi** - vous pouvez activer ou désactiver la notification du produit qui s'affiche chaque fois que vous vous connectez à un réseau Wi-Fi non sécurisé.
      Le but de cette notification est de vous aider à garder vos données privées et sécurisées en utilisant Bitdefender VPN.
  - **Paramètres de protection Web**
    - **Accord** - vous pouvez lire les conditions d'utilisation du service Bitdefender Web Protection. Si vous touchez **je ne suis plus d'accord**, vous ne pourrez pas utiliser Bitdefender VPN au moins tant que vous n'aurez pas appuyé sur **Je suis d'accord**.
    - **Activer la notification de protection Web** - Vous avertit que la protection Web peut être activée après avoir terminé une session VPN.
  - **Rapports sur les produits**
- **Retour** - à partir de là, vous pouvez lancer le client de messagerie par défaut pour nous envoyer vos commentaires sur l'application.
- **Informations sur l'application** - à partir d'ici, vous avez accès aux informations sur la version installée et aux conformités du contrat d'abonnement, de la politique de confidentialité et des licences open-source.

## 6.3. Analyse

Bitdefender Mobile Security pour iOS vous permet d'analyser votre appareil à la recherche de vulnérabilités de sécurité et de menaces potentielles sur votre appareil. L'exécution de l'analyse vérifiera :

- **Version du système d'exploitation :** Vérification de votre version iOS pour les dernières mises à jour.
- **Code d'accès/Biométrie :** Vérification du niveau de sécurité en ce qui concerne l'accès à votre appareil.
- **Protection Internet :** Vérification de l'état du module Web Protection
- **Confidentialité du compte :** Vérification de la présence de comptes surveillés répertoriés dans le module Confidentialité des comptes.
- **Scan Wi-Fi :** Vérification de l'état de sécurité du réseau actuellement connecté.

L'état de la protection est déterminé après l'exécution d'une analyse manuelle.

Après avoir exécuté la première analyse, vous rencontrerez les informations de Bitdefender Recommandations du pilote automatique. Il s'agit de votre conseiller en sécurité personnel, fournissant des recommandations contextuelles basées sur l'utilisation et les besoins de votre appareil. De cette façon, vous bénéficierez de tout ce que votre application a à offrir.

> **Note**
> Lors de la première entrée dans l'application, vous serez invité à exécuter une analyse.

## 6.4. Alerte aux arnaques

La fonctionnalité Scam Alert disponible dans Bitdefender Mobile Security pour iOS protège de manière proactive les utilisateurs Apple contre les escroqueries par phishing. Scam Alert pour iOS comprend deux niveaux de protection qui surveillent les escroqueries transmises via des messages SMS/MMS et des invitations d'agenda :

- **Filtre de messages texte (SMS, MMS)**
  Cette fonctionnalité identifie et filtre les messages SMS et MMS indésirables.
  Un SMS/MMS (Short Message Service/Multimedia Messaging Service) malveillant fait référence à un type de message envoyé à des appareils mobiles dans un but nuisible. Ces messages sont conçus pour exploiter les vulnérabilités, tromper les destinataires ou nuire à l'appareil, aux informations personnelles ou à la sécurité de la cible.

- **Scanner de liens d'invitation de calendrier**
  Cette fonctionnalité détecte les calendriers de spam et les événements contenant des liens dangereux. Le virus du calendrier est un type de spam qui affecte l'application Calendrier de votre iPhone, ce qui peut être ennuyeux et potentiellement dangereux :
  - Vous recevez des invitations de calendrier ou des notifications d'événements indésirables lorsque vous acceptez accidentellement une fausse invitation de calendrier envoyée à votre adresse e-mail par des pirates ou des spammeurs.
  - Lorsque vous cliquez sur le lien dans l'invitation, vous vous abonnez sans le savoir au calendrier de l'expéditeur, ce qui lui permet de vous envoyer davantage d'événements de spam.
  - Les événements de spam peuvent contenir des liens ou des pièces jointes qui pourraient vous conduire vers des pages de phishing ou d'autres cybermenaces si vous les ouvrez.

### 6.4.1. Comment configurer une alerte d'arnaque

Pour activer l'alerte d'arnaque, vous devez accorder à l'application Bitdefender Mobile Security l'accès aux notifications du calendrier et aux messages SMS :

**Comment activer le filtrage SMS :**

Pour que Bitdefender commence à filtrer les messages, vous devez activer manuellement l'option Filtrer les expéditeurs inconnus dans les paramètres de l'application Messages :

1. Ouvrez le **Paramètres** application sur votre iPhone ou iPad.
2. Faites défiler vers le bas et sélectionnez **messages** dans la liste.
3. Appuyez sur le **Inconnu et spam** section.
4. Basculer **Filtrer les expéditeurs inconnus** en position marche.
5. Sélectionner **Sécurité mobile** dans la section Filtrage SMS puis choisissez **Activer**.

Bitdefender sera désormais capable de filtrer les messages indésirables sur votre iPhone/iPad.

> **Note**
> En raison des restrictions iOS, le filtrage SMS de Bitdefender ne peut être utilisé que pour les messages SMS et MMS provenant de personnes que vous n'avez pas enregistrées dans vos contacts. Cela signifie qu'il ne filtrera pas les messages des personnes déjà présentes dans votre liste de contacts ni les messages iMessage de quiconque.

**Comment activer l'analyse du calendrier :**

1. Ouvrez le **Sécurité mobile Bitdefender** application installée sur votre iPhone ou iPad.
2. Allez au **Alerte aux arnaques** option dans la barre de navigation inférieure et appuyez sur **Configurer maintenant**.
3. Robinet **Continuer**, puis appuyez sur **Activer**.
4. Choisir **D'ACCORD** pour accorder à Bitdefender l'accès à votre calendrier. Une analyse du calendrier commencera immédiatement.

## 6.5. Protection Internet

Bitdefender Web Protection garantit une expérience de navigation sécurisée en vous alertant sur les pages Web malveillantes potentielles et lorsque des applications installées moins sécurisées tenteront d'accéder à des domaines non approuvés.

Lorsqu'une URL pointe vers un site Web de phishing ou frauduleux connu, ou vers un contenu malveillant tel qu'un logiciel espion ou un virus, la page Web est bloquée et une alerte s'affiche. La même chose se produit lorsque des applications installées tentent d'accéder à des domaines malveillants.

> **Important**
> Si vous vous trouvez dans une zone où l'utilisation d'un service VPN est restreinte par la loi, la fonctionnalité de la protection Web ne sera pas disponible.

Pour activer la protection Web :

1. Appuyez sur le icône en bas de l'écran.
2. Robinet **Je suis d'accord**.
3. Activez le commutateur de protection Web.

**Note**

La première fois que vous activez la protection Web, vous serez peut-être invité à autoriser Bitdefender à configurer des configurations VPN qui surveilleront le trafic réseau. Robinet **Permettre**, continuer. Si une méthode d'authentification (empreinte digitale ou code PIN) a été définie pour protéger votre smartphone, vous devez l'utiliser. Pour pouvoir détecter l'accès à des domaines non approuvés, Web Protection travaille en collaboration avec les services VPN.

**Important**

La fonction de protection Web et le VPN ne peuvent pas fonctionner en même temps. Chaque fois que l'un d'eux est activé, l'autre (s'il est actif à ce moment-là) sera désactivé.

### 6.5.1. Alertes Bitdefender

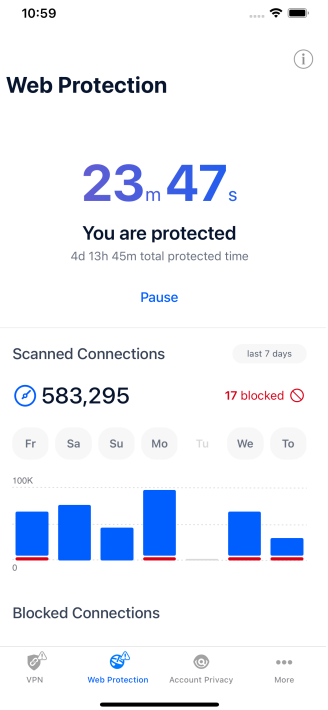
Chaque fois que vous essayez de visiter un site Web classé comme dangereux, le site Web est bloqué. Pour vous informer de l'événement, vous êtes averti par Bitdefender dans le centre de notification et dans votre navigateur. La page d'avertissement contient des informations telles que l'URL du site Web et la menace détectée. Vous devez décider quoi faire ensuite.

De plus, vous êtes averti dans le centre de notification chaque fois qu'une application moins sécurisée tente d'accéder à des domaines non approuvés. Appuyez sur la notification affichée pour être redirigé vers la fenêtre où vous pouvez décider quoi faire ensuite.

Les options suivantes sont disponibles dans les deux cas :

- Quittez le site Web en appuyant sur **RAMENEZ-MOI EN SÉCURITÉ**.
- Accédez au site Web, malgré l'avertissement, en appuyant sur la notification affichée, puis **Je veux accéder à la page**.

Confirmez votre choix.




## 6.6. VPN

Avec le VPN Bitdefender vous pouvez assurer la confidentialité de vos données lorsque vous vous connectez à des réseaux sans-fil non sécurisés dans les aéroports, les commerces, les cafés ou les hôtels. Vous pouvez de cette manière éviter le vol de données personnelles ou les tentatives d'accès des pirates à l'adresse IP de votre appareil.

Le VPN sert de tunnel entre votre appareil et le réseau auquel vous vous connectez pour sécuriser votre connexion, crypter les données à l'aide d'un cryptage de niveau militaire et masquer votre adresse IP où que vous soyez. Votre trafic est redirigé via un serveur séparé ; rendant ainsi votre appareil impossible à identifier par votre FAI, à travers la myriade d'autres appareils qui utilisent nos services. De plus, lorsqu'il est connecté à Internet via Bitdefender VPN, vous pouvez accéder à du contenu normalement limité à des zones spécifiques.

> **Note**
> Certains pays pratiquent la censure sur Internet et, par conséquent, l'utilisation de VPN sur leur territoire a été interdite par la loi. Pour éviter des conséquences juridiques, un message d'avertissement peut apparaître lorsque vous essayez d'utiliser l'application Bitdefender VPN pour la première fois. En continuant à utiliser l'application, vous confirmez avoir pris connaissance des réglementations nationales applicables et des risques auxquels vous pourriez être exposé.

Pour activer Bitdefender VPN :

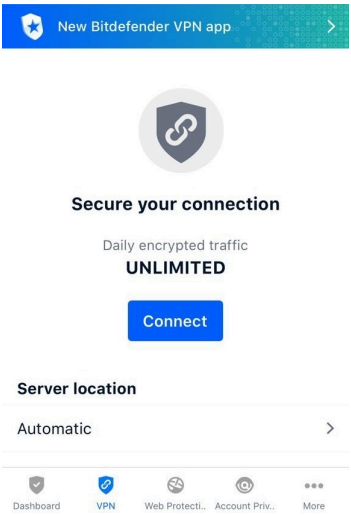
1. Appuyez sur le icône en bas de l'écran.
2. Robinet **Connecter** chaque fois que vous souhaitez rester protégé lorsque vous êtes connecté à des réseaux sans fil non sécurisés.
   Robinet **Déconnecter** chaque fois que vous souhaitez désactiver la connexion.

> **Note**
> La première fois que vous activez le VPN, vous êtes invité à autoriser Bitdefender à configurer les configurations VPN qui surveilleront le trafic réseau. Robinet **Permettre**, continuer. Si une méthode d'authentification (empreinte digitale ou code PIN) a été définie pour protéger votre smartphone, vous devez l'utiliser.

Le VPN L'icône apparaît dans la barre d'état lorsque le VPN est actif.

Pour économiser la batterie, nous vous recommandons de désactiver le VPN lorsque vous n'en avez pas besoin.

Si vous avez un abonnement premium et que vous souhaitez vous connecter à un serveur à votre guise, appuyez sur Automatique dans l'interface VPN, puis sélectionnez l'emplacement souhaité. Pour plus de détails sur les abonnements VPN, reportez-vous à Abonnements (page 241).




## 6.6.1. Abonnements

Bitdefender VPN offre gratuitement un quota de trafic quotidien de 200 Mo par appareil pour sécuriser votre connexion à chaque fois que vous en avez besoin et vous connecte automatiquement à l'emplacement optimal du serveur.

Pour obtenir un trafic illimité et un accès illimité au contenu dans le monde entier en choisissant un emplacement de serveur à votre guise, passez à la version premium.

Vous pouvez mettre à niveau vers la version Bitdefender Premium VPN à tout moment en appuyant sur le bouton **Activer le VPN Premium** bouton disponible dans la fenêtre VPN. Vous avez le choix entre deux types d'abonnements : annuel et mensuel.

L'abonnement Bitdefender Premium VPN est indépendant de l'abonnement gratuit Bitdefender Mobile Security pour iOS, ce qui signifie que vous pourrez l'utiliser pendant toute sa disponibilité. En cas d'expiration de l'abonnement Bitdefender Premium VPN, vous reviendrez automatiquement au forfait gratuit.

Bitdefender VPN est un produit multiplateforme, disponible dans les produits Bitdefender compatibles avec Windows, macOS, Android et iOS. Une fois que vous aurez mis à niveau vers le plan premium, vous pourrez

utiliser votre abonnement sur tous les produits, à condition que vous vous connectiez avec le même compte Bitdefender.

> **Note**
> Bitdefender VPN fonctionne également comme une application autonome sur tous les systèmes d'exploitation pris en charge, à savoir Windows, macOS, Android et iOS.

## 6.7. Confidentialité du compte

Bitdefender Account Privacy détecte si une fuite de données s'est produite dans les comptes que vous utilisez pour effectuer des paiements en ligne, faire des achats ou vous connecter à différentes applications ou sites Web. Les données qui peuvent être stockées dans un compte peuvent être des mots de passe, des informations de carte de crédit ou des informations de compte bancaire et, si elles ne sont pas correctement sécurisées, un vol d'identité ou une atteinte à la vie privée peut se produire.

Le statut de confidentialité d'un compte s'affiche juste après la validation.

Pour vérifier si l'un des comptes a été divulgué, appuyez sur **Rechercher les fuites**.

Pour commencer à protéger les informations personnelles :

1. Appuyez sur le icône en bas de l'écran.
2. Robinet **Ajouter un compte**.
3. Saisissez votre adresse e-mail dans le champ correspondant, puis appuyez sur **Suivant**.
   Bitdefender doit valider ce compte avant d'afficher des informations privées. Par conséquent, un e-mail avec un code de validation est envoyé à l'adresse e-mail fournie.
4. Vérifiez votre boîte de réception, puis tapez le code reçu dans le **Confidentialité du compte** zone de votre application. Si vous ne trouvez pas l'e-mail de validation dans le dossier Boîte de réception, vérifiez également le dossier Spam.
   L'état de confidentialité du compte validé s'affiche.

Si des fuites sont constatées dans l'un de vos comptes, nous vous recommandons de changer son mot de passe dès que possible. Pour créer un mot de passe fort et sécurisé, tenez compte de ces conseils :

- Faites-en au moins huit caractères.
- Inclure les caractères minuscules et majuscules.
- Ajoutez au moins un chiffre ou un symbole, tel que #, @, % ou !.

Une fois que vous avez sécurisé un compte qui faisait partie d'une violation de la vie privée, vous pouvez confirmer les modifications en marquant la ou les fuites identifiées comme **Résolu**. Pour faire ça:

1. Robinet ··· à côté de la brèche que vous avez résolue.
2. Robinet **Marquer comme résolu**.

Lorsque toutes les fuites détectées sont marquées comme résolues, le compte n'apparaîtra plus comme ayant fui, du moins jusqu'à ce qu'une nouvelle fuite soit détectée.

## 6.8. Questions fréquemment posées

**Comment Bitdefender Mobile Security pour iOS me protège-t-il contre les virus et les cybermenaces ?**

Bitdefender Mobile Security pour iOS offre une protection absolue contre toutes les cybermenaces et est spécialement conçu pour protéger vos données sensibles des regards indiscrets.

Vous bénéficiez d'une multitude de fonctionnalités avancées de sécurité et de confidentialité pour votre iPhone et iPad, ainsi que de nombreuses fonctionnalités bonus, notamment le VPN et la protection Web.

Bitdefender Mobile Security pour iOS réagit instantanément aux virus et malwares sans compromettre les performances de votre système.

**Quels types d'appareils et de systèmes d'exploitation sont couverts par Bitdefender Mobile Security pour iOS ?**

Bitdefender Mobile Security pour iOS protégera vos smartphones et tablettes exécutant iOS contre toutes les cybermenaces.

**Pourquoi ai-je besoin de Bitdefender Mobile Security pour iOS sur Apple OS ?**

Certaines de vos données les plus personnelles sont stockées sur votre iPhone ou iPad - et vous devez savoir qu'elles sont en sécurité à tout moment. Bitdefender Mobile Security pour iOS offre une protection absolue contre les cybermenaces et prend soin de votre vie privée en

ligne et de vos informations privées sans interférer avec vos activités quotidiennes.

**Est-ce que j'obtiens un VPN avec mon abonnement Bitdefender Mobile Security pour iOS ?**

Bitdefender Mobile Security pour iOS est livré avec une version de base de Bitdefender VPN qui inclut une quantité généreuse de trafic (200 Mo/jour, un total de 6 Go/mois) gratuitement.

# 7. VPN

## 7.1. Qu'est-ce que Bitdefender Total Security

Le VPN sert de tunnel entre votre appareil et le réseau auquel vous vous connectez pour sécuriser votre connexion, crypter les données à l'aide d'un cryptage de niveau militaire et masquer votre adresse IP où que vous soyez. Votre trafic est redirigé via un serveur distinct ; rendant ainsi votre appareil impossible à identifier par votre FAI, à travers la myriade d'autres appareils qui utilisent nos services. De plus, lorsque vous êtes connecté à Internet via Bitdefender VPN, vous pouvez accéder à du contenu normalement restreint dans des zones spécifiques.

> **Note**
> Certains pays pratiquent la censure de l'Internet et la loi interdit donc l'utilisation de VPN. Pour éviter les conséquences juridiques, un message d'avertissement peut apparaitre lors de votre première utilisation de la fonctionnalité de Bitdefender Total Security. En continuant à utiliser cette fonctionnalité, vous confirmez avoir connaissance des réglementations applicables dans le pays et des risques auxquels vous êtes susceptibles d'être exposé.

### 7.1.1. Protocoles de chiffrement

Les ensembles de suites cryptographiques activés sur le serveur et le client Hydra sont indiqués ci-dessous. Toutes les autres suites cryptographiques sont désactivées.

Suites cryptographiques du client Hydra:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

> **Note**
> L'ensemble côté serveur est bien plus restrictif et le client comme le serveur Hydra rejetteront tout mode différent de GCM avec AES. Le serveur Hydra force une priorité côté serveur des suites cryptographiques les plus robustes et rejettera un handshake TLS si une suite plus faible est demandée par un client. Cette liste peut également être configurée à la volée côté serveur.

## 7.2. Abonnements au VPN

Avec Bitdefender Total Security, vous avez le choix entre deux types d'abonnement :

- L'abonnement Basic
- L'abonnement Premium

### 7.2.1. Abonnement Basic

Bitdefender Total Security vous offre gratuitement 200 Mo de trafic par appareil pour sécuriser votre connexion quand vous le souhaitez et vous permet de vous connecter à un emplacement qui ne peut être changé.

L'abonnement Basic est disponible pour tous les utilisateurs qui téléchargent Bitdefender Total Security.

### 7.2.2. Abonnement Premium

Passez à la version Premium pour bénéficier d'un accès illimité à toutes les fonctionnalités de Bitdefender Total Security. Les utilisateurs disposant d'un abonnement Premium VPN actif bénéficient d'un trafic protégé illimité et peuvent se connecter à tous nos serveurs du monde.

Deux offres sont disponibles pour l'abonnement Premium : l'offre mensuelle et l'offre annuelle.

- Offre mensuelle : avec cette offre, vous serez facturé chaque mois pour l'utilisation des services Premium VPN. Vous pouvez arrêter l'abonnement quand vous le souhaitez.
- Offre annuelle : nécessite un paiement en une fois qui vous donne un accès aux services de notre VPN Premium pendant toute une année.

## 7.2.3. Comment passer à la version Premium du VPN

La manière la plus simple de passer à la version Premium de Bitdefender Total Security est de cliquer sur le bouton **Mettre à niveau** situé en bas de l'interface principale. Choisissez le modèle d'abonnement souhaité puis suivez les instructions à l'écran.

Si vous avez déjà un code d'activation, suivez les instructions ci-dessous :

- **Pour les utilisateurs de Windows**
  1. Cliquez sur l'icône Mon compte située à gauche de l'interface du VPN.
  2. Cliquez sur **L'ajouter ici**.
  3. Saisissez le code reçu par e-mail, puis cliquez sur le bouton **Activer le code**.

- **Pour les utilisateurs d'appareils macOS**
  1. Cliquez sur la roue dentée en haut à droite de l'interface du VPN et sélectionnez **Mon compte**.
  2. Cliquez sur **Ajoutez-le ici**.
  3. Tapez le code reçu par e-mail, puis cliquez sur le **Code d'activation** bouton.

- **Pour les utilisateurs d'appareils Android**
  1. Appuyez sur la roue dentée en haut à droite de l'interface du VPN et sélectionnez **Mon compte**.
  2. Appuyez sur **Ajouter le code**.
  3. Tapez le code reçu par e-mail, puis cliquez sur le **Code d'activation** bouton.

- **Pour les utilisateurs d'appareils iOS**
  1. Appuyez sur la roue dentée dans le coin supérieur droit de l'interface VPN et sélectionnez **Mon compte**.
  2. Robinet **Ajouter un code**.
  3. Tapez le code reçu par e-mail, puis cliquez sur le **Code d'activation** bouton.

# 7.3. Installation

## 7.3.1. Préparation de l'installation

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

- Vérifiez que l'appareil sur lequel vous prévoyez d'installer Bitdefender dispose de la configuration requise. Si l'appareil ne dispose pas de la configuration requise, Bitdefender ne pourra pas être installé, ou, une fois installé, il ne fonctionnera pas correctement, ralentira le système et le rendra instable.

  Pour des informations détaillées sur la configuration requise, veuillez consulter Configuration requise (page 248).

- Connectez-vous à l'appareil en utilisant un compte administrateur.

- Il est recommandé que votre appareil soit connecté à Internet pendant l'installation, même pour une installation à partir d'un CD/DVD. Si des versions plus récentes des fichiers d'applications du logiciel d'installation sont disponibles, Bitdefender peut les télécharger et les installer.

## 7.3.2. Configuration requise

- **Pour les utilisateurs Windows**
  - **Système d'exploitation** : Windows 7 avec Service Pack 1, Windows 8, Windows 8.1 Windows 10 et Windows 11
  - **Mémoire (RAM):** 1 Go
  - **Espace disponible sur le disque dur :** 500 Mo d'espace libre
  - **Net Framework:** min version 4.5.2

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

- **Pour les utilisateurs de macOS**
  - **Système d'exploitation :** macOS Sierra (10.12) et versions supérieures

- **Espace disponible sur le disque dur :** 100 Mo d'espace libre

- **Pour les utilisateurs d'Android**
  - **Système d'exploitation :** Android 5.0 ou versions supérieures
  - **Stockage :** 100 Mo
  - Une connexion Internet active

- **Pour les utilisateurs iOS**
  - **Système d'exploitation :** iOS 12 et versions supérieures
  - **Stockage sur iPhone :** 50 Mo
  - **Stockage sur iPad :** 100 Mo
  - Une connexion Internet active

### 7.3.3. Installation de Bitdefender Total Security

Pour débuter l'installation, suivez les instructions correspondant au système d'exploitation que vous utilisez :

- **Pour les utilisateurs Windows**

  1. Pour commencer l'installation de Bitdefender Total Security sur un PC Windows, téléchargez le kit d'installation depuis https://www.bitdefender.com/solutions/vpn/download ou depuis l'e-mail que vous avez reçu suite à votre achat.
  2. Double-cliquez sur le programme d'installation que vous avez téléchargé pour l'exécuter.
  3. Choisissez Oui si une boite de dialogue du Contrôle de compte d'utilisateur apparait.
  4. Attendez la fin du téléchargement.
  5. Sélectionnez la langue du produit dans le menu déroulant de l'assistant d'installation.
  6. Cochez la case « Je confirme avoir lu et accepter les Conditions d'utilisation de l'abonnement et la Politique de confidentialité », puis cliquez sur **COMMENCER L'INSTALLATION**.
  7. Attendez que l'installation se termine.

8. **CONNECTEZ-VOUS** avec votre compte Bitdefender Central. Si vous n'avez pas de compte Central, vous pouvez en créer un en cliquant sur le bouton **CRÉER UN COMPTE**.
9. Sélectionnez **J'ai un code d'activation** si vous avez déjà acheté un abonnement Premium VPN.
   Sinon, vous pouvez choisir **COMMENCER L'ÉVALUATION** pour tester gratuitement le produit pendant 7 jours avant de vous engager à l'utiliser.
10. Saisissez le code reçu par e-mail, puis cliquez sur le bouton **ACTIVER PREMIUM**.
11. Au bout de quelques instants, Bitdefender Total Security sera installé sur votre ordinateur et prêt à être utilisé.

❍ **Pour les utilisateurs de macOS**

1. Pour commencer l'installation de Bitdefender Total Security sur macOS, téléchargez le kit d'installation depuis https://www.bitdefender.com/solutions/vpn/download ou depuis l'e-mail que vous avez reçu suite à votre achat.
2. L'assistant d'installation sera enregistré sur votre Mac. Dans le dossier Téléchargements, double-cliquez sur le package .
3. Suivez les instructions à l'écran. Sélectionnez **Continuer**.
4. Vous serez guidé(e) dans toutes les étapes de l'installation de Bitdefender Total Security sur votre Mac. Cliquez deux fois sur le bouton **Continuer**.
5. Cliquez sur **J'accepte**, après avoir lu et compris les conditions du Contrat de licence du logiciel.
6. Cliquez sur **Installer**.
7. Saisissez un nom d'utilisateur et un mot de passe pour l'administrateur, puis cliquez sur **Installer le logiciel**.
8. Un message vous informe qu'une extension système signée par Bitdefender a été bloquée. Il ne s'agit pas d'une erreur, mais uniquement d'un contrôle de sécurité. Cliquez sur **Ouvrir les préférences de sécurité**.
9. Cliquez sur l'icône du verrou pour le déverrouiller.

Saisissez le nom et le mot de passe administrateur puis cliquez sur **Déverrouiller**.

10. Cliquez sur **Autoriser** pour charger l'extension système Bitdefender Bitdefender. Fermez ensuite la fenêtre Sécurité et confidentialité ainsi que l'assistant d'installation.

11. Cliquez sur l'icône en forme de boucler de la barre des menus puis **connectez-vous** à l'aide de votre compte Bitdefender Central. Si vous n'avez pas de compte Central, vous devez en créer un.

12. Choisissez J'ai un **Code d'activation** si vous avez déjà acheté un abonnement Premium VPN.
    Sinon, vous pouvez choisir **COMMENCER PROCÈS** de tester gratuitement le produit pendant 7 jours avant de s'engager à le payer.

13. Tapez le code reçu par e-mail, puis cliquez sur le **Code d'activation** bouton.

14. Au bout de quelques instants, Bitdefender Total Security sera installé sur votre Mac et prêt à être utilisé.

❍ **Pour les utilisateurs d'Android**

1. Pour installer Bitdefender Total Security sur Android, commencez par ouvrir l'application **Google Play Store** sur votre smartphone ou votre tablette.
2. Recherchez Bitdefender Total Security et sélectionnez l'application correspondante.
3. Appuyez sur le bouton **Installer** et patientez jusqu'à la fin du téléchargement.
4. Appuyez sur **Ouvrir** pour exécuter l'application.
5. Cochez la case « J'accepte les Conditions d'utilisation de l'abonnement et la Politique de confidentialité », puis appuyez sur **Continuer**.
6. **Connectez-vous** avec votre compte Bitdefender Central. Si vous n'avez pas de compte Central, vous devez en créer un en appuyant sur **Créer un compte**.
7. Sélectionnez **J'ai un code d'activation** si vous avez déjà acheté un abonnement Premium VPN.

Sinon, vous pouvez choisir de commencer l'évaluation de 7 jours pour tester gratuitement le produit pendant 7 jours avant de vous engager à l'utiliser.

8. Saisissez le code reçu par e-mail puis appuyez sur **Code d'activation**.

❍ **Pour les utilisateurs iOS**

1. Pour installer Bitdefender Total Security sur iOS, commencez par ouvrir l'**App Store** sur votre iPhone ou votre iPad.
2. Rechercher Bitdefender Total Security et sélectionnez cette application.
3. Appuyez sur l'icône **Obtenir** et patientez jusqu'à la fin du téléchargement.
4. Robinet **Ouvrir** pour exécuter l'application.
5. Cochez la case **J'accepte les Conditions d'utilisation de l'abonnement et la Politique de confidentialité**, puis appuyez sur **Continuer**.
6. **Connectez-vous** avec votre compte Bitdefender Central. Si vous n'avez pas de compte, vous devez en créer un en appuyant sur **Créer un compte**.
7. Appuyez sur **Autoriser** si vous souhaitez recevoir des notifications de Bitdefender Total Security.
8. Choisir **J'ai un code d'activation** si vous avez acheté un abonnement VPN Premium.
   Sinon, vous pouvez choisir Démarrer l'essai de 7 jours pour tester le produit gratuitement pendant 7 jours avant de vous engager à le payer.
9. Tapez le code reçu par e-mail, puis appuyez sur **Code d'activation**.

## 7.4. Utilisation du VPN de Bitdefender

### 7.4.1. Ouverture de Bitdefender VPN

❍ **Pour Windows**

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

- **Depuis la zone de notification**
  Faites un clic droit sur l'icône représentant un bouclier rouge dans la zone de notification, puis sélectionnez **Afficher** dans le menu.
- **Depuis l'interface Bitdefender**
  Si un produit de sécurité Bitdefender tel que Bitdefender Total Security ou Bitdefender Antivirus Plus (etc.) est déjà installé sur votre ordinateur Windows, vous pouvez ouvrir le VPN de Bitdefender en procédant comme suit :
  1. Cliquez sur l'icône **Vie privée** située dans le volet latéral gauche de l'interface Bitdefender.
  2. Cliquez sur **Ouvrir le VPN** dans le panneau du VPN.
- **Depuis votre bureau**
  Double-cliquez sur l'icône Bitdefender VPN située sur votre bureau.

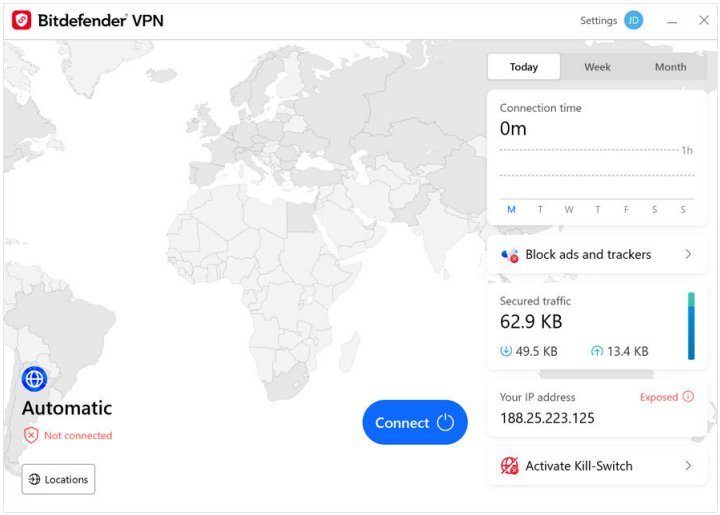
- **Pour macOS**
  Vous pouvez ouvrir l'application Bitdefender VPN en cliquant sur l'icône située dans la barre de menu en haut à droite de l'écran.
  Si vous ne trouvez pas le bouclier Bitdefender dans la barre de menu, utilisez la barre de lancement ou le Finder de votre Mac pour retrouver l'icône :
  - **Depuis la barre de lancement**
    1. Appuyez sur la touche **F4** de votre clavier pour accéder à la barre de lancement de votre Mac.
    2. Cliquez sur Parcourir puis allez à l'emplacement de l'application Bitdefender VPN. Vous pouvez également saisir **Bitdefender VPN** dans la barre de lancement pour commencer à filtrer les résultats.
    3. Une fois que vous voyez l'application Bitdefender VPN, cliquez sur son icône pour l'épingler à la barre de menu.
  - **Depuis le Finder**
    1. Cliquez sur **Finder** en bas à gauche du bureau (l'icône de Finder est celle qui ressemble à un carré bleu avec un visage souriant).
    2. Ensuite, cliquez sur **Aller** en haut à gauche de l'écran, dans la barre de menu.

3. Sélectionnez **Applications** dans le menu pour accéder au dossier Applications de votre Mac.
4. Dans le dossier Applications, ouvrez le dossier **Bitdefender** puis double-cliquez sur l'application **Bitdefender VPN**.

> **Note**
> Pour accéder au VPN de Bitdefender sur vos appareils mobiles Android ou iOS, il vous suffit d'ouvrir l'application Bitdefender VPN après l'avoir installée.

## 7.4.2. Comment se connecter à Bitdefender Total Security

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 en le sélectionnant dans la liste des emplacements virtuels. Pour vous connecter ou vous déconnecter, il vous suffit de cliquer sur le bouton marche situé dans l'interface du VPN.




- **Pour Windows :** la zone de notification affiche une coche verte lorsque le VPN est connecté, et une coche noire lorsque le VPN est déconnecté. Lorsque vous vous connectez manuellement à un

emplacement sélectionné, l'adresse IP s'affiche dans l'interface principale.

- **Pour macOS :** l'icône  située dans la barre de menu s'affiche en noir lorsque le VPN est connecté, et  en blanc lorsque le VPN est déconnecté. Cliquez sur le bouton rond situé au centre de l'interface et patientez le temps que la connexion soit établie.
- **Pour Android et iOS :** pour connecter le VPN de Bitdefender sur Android, iOS et iPadOS :
  - **Dans l'application Bitdefender VPN :** pour vous connecter ou vous déconnecter, appuyez simplement sur le bouton marche dans l'interface du VPN. L'état du VPN de Bitdefender s'affiche.
  - **Dans l'application Bitdefender Mobile Security :**
    1. Accédez à l'icône  VPN située dans la barre de navigation inférieure de Bitdefender Mobile Security.
    2. Appuyez sur **CONNECTER** à chaque fois que vous souhaitez sécuriser une connexion à un réseau sans fil non sécurisé.Appuyez sur **DÉCONNECTER** lorsque vous souhaitez désactiver la connexion VPN.

## 7.4.3. Comment se connecter à un autre serveur

Avec un abonnement Premium, Bitdefender Total Security vous permet de vous connecter à n'importe lequel de nos serveurs dans le monde, à tout moment. Pour ce faire, vous devez :

1. Ouvrir l'application Bitdefender Total Security.
2. Appuyez sur le bouton **Emplacement virtuel** situé en bas de l'interface.
3. Sélectionnez le pays de votre choix.
4. Cliquez sur le bouton **Se connecter à [pays sélectionné]** situé en bas de l'interface.

- L'icône de la barre d'état système affiche une coche verte lorsque le VPN est connecté.
- L'adresse IP du serveur virtuel est affichée sur l'écran d'accueil lors de la connexion au VPN Bitdefender.

- Un résumé de votre temps de connexion, de la quantité de trafic sécurisé et des 5 derniers emplacements auxquels vous vous êtes connecté sont également affichés sur le tableau de bord principal.

## 7.5. Bitdefender Total Security Paramètres & Fonctionnalités

### 7.5.1. Accéder aux paramètres

Pour accéder aux paramètres de Bitdefender Total Security, suivez les instructions suivantes :

- {1}Sur Windows{2}
  1. Ouvrez l'application Bitdefender Total Security en double-cliquant sur son icône dans le système ou par un clic droit puis en sélectionnant Afficher.
  2. Cliquez sur le bouton **Paramètres** (représenté par une roue dentée) situé à gauche de l'interface.

- **Sur macOS**
  1. Ouvrez l'application Bitdefender Total Security sur votre appareil macOS en cliquant sur son icône dans la barre des menus.
  2. Cliquez sur la roue dentée en haut à droite de l'interface de Bitdefender Total Security et sélectionnez Paramètres.

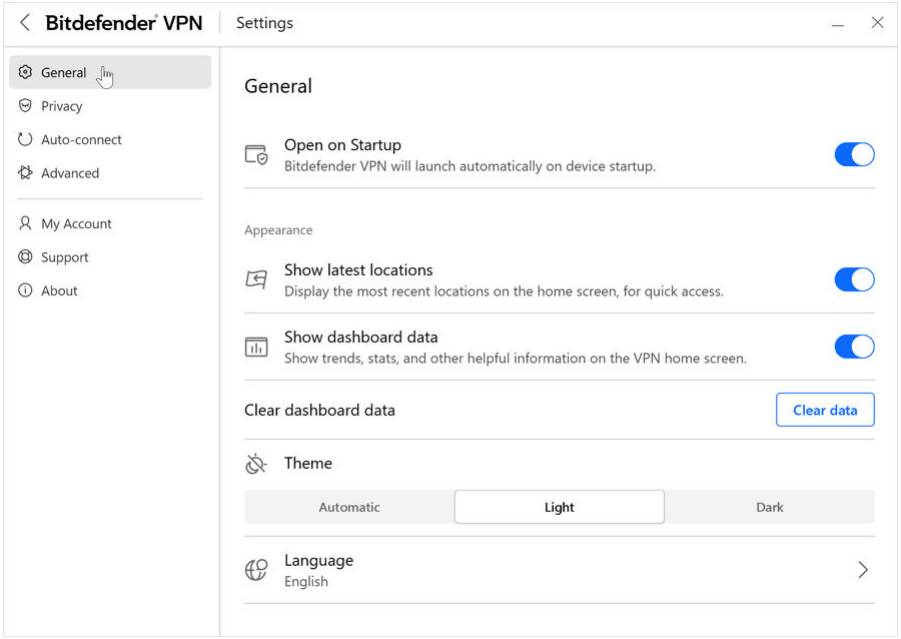
- **Sur Android**
  1. Ouvrez l'application Bitdefender Total Security sur votre appareil.
  2. Cliquez sur l'icône en forme de roue dentée située en haut à droite de l'interface de Bitdefender Total Security.

- **Sur iOS**
  1. Ouvrez le Bitdefender Total Security application sur votre appareil.
  2. Cliquez sur le bouton de la roue dentée dans le coin supérieur droit de la Bitdefender Total Security interface.

### 7.5.2. Général

Ici, vous pouvez modifier les éléments suivants :

- **Ouvrir au démarrage**– Bitdefender VPN se lancera automatiquement au démarrage de l'appareil.
- **Afficher les derniers emplacements**– Affichez les emplacements les plus récents sur l'écran d'accueil, pour un accès rapide.
- **Afficher les données du tableau de bord** – Affichez les tendances, les statistiques et d'autres informations utiles sur l'écran d'accueil du VPN.
- **Effacer les données du tableau de bord**– Toutes les données de votre tableau de bord seront effacées et tous les compteurs réinitialisés.
- **Thème**– Thème clair/obscur
- **Langue**– Changez la langue du VPN Bitdefender.
- **Notifications**– Gérez vos préférences de notifications.
- **Aidez-nous à améliorer le VPN Bitdefender**– Soumettez des rapports de produits anonymes pour nous aider à améliorer votre expérience.
- **Réinitialiser tous les réglages**– Réinitialisez le VPN à ses paramètres d'origine sans le réinstaller.



## 7.5.3. Fonctionnalités

### Confidentialité

### Fonction Kill Switch

Le Kill-Switch est une nouvelle fonctionnalité de Bitdefender Total Security. Lorsqu'elle est activée, cette fonctionnalité suspend temporairement tout le trafic Internet si la connexion au VPN est perdue par accident. Dès que vous êtes de retour en ligne, la connexion VPN est rétablie.

Pour activer le Kill-Switch, suivez les instructions suivantes :

- **Sous Windows**

  1. Ouvrez l'application Bitdefender Total Security sur votre appareil en double-cliquant sur son icône dans la zone de notification ou en faisant un clic droit sur l'icône et en sélectionnant **Afficher**.
  2. Clique sur le **Paramètres** bouton (représenté par une roue dentée) sur le côté gauche de l'interface.
  3. Sélectionnez **Avancé**.
  4. Activez l'option **Fonction Kill Switch**.

- **Sur Androïd**

  1. Ouvrez le Bitdefender Total Security application sur votre appareil.
  2. Cliquez sur le bouton de la roue dentée dans le coin supérieur droit de la Bitdefender Total Security interface.
  3. Dans **Paramètres**, activez l'option **Kill Switch** (arrêt d'urgence).

- **Sur iOS**

  1. Ouvrez le Bitdefender Total Security application sur votre appareil.
  2. Cliquez sur le bouton de la roue dentée dans le coin supérieur droit de la Bitdefender Total Security interface.
  3. Sous **Paramètres**, activez le **Antidémarreur** option.

> **Note**
> Cette fonctionnalité est également disponible pour les appareils macOS fonctionnant avec la version 10.15.4 du système (ou versions ultérieures).

## Bloqueur de publicités et Bloqueur de traceurs

Ces fonctionnalités sont conçues pour vous aider à protéger votre vie privée et à profiter d'Internet sans que des publicités agaçantes ou des entreprises trop curieuses perturbent votre expérience. Elles contribuent à bloquer les publicités et les traceurs en ligne.

### Bloqueur de publicités

Le **bloqueur de publicités** est utilisé pour bloquer les publicités, les pop-ups, les vidéos envahissantes et les bannières publicitaires pendant votre navigation. Les sites Internet se chargeront plus rapidement, seront plus agréables à consulter et seront plus sûrs.

Pour activer la fonctionnalité Ad Blocker :

1. Localisez la fonctionnalité **Bloqueur de publicités & Bloqueur de traceurs** dans les **Paramètres**.
2. Faites basculer l'interrupteur sur la position **MARCHE**.

### Bloqueur de traceurs

Le **bloqueur de traceurs** permet de bloquer les traceurs utilisés par les annonceurs pour vous suivre et établir votre profil en ligne. Certains sites Internet peuvent mal fonctionner une fois les traceurs bloqués, mais il suffit d'ajouter l'URL sur la liste blanche pour corriger le problème.

Pour activer le bloqueur de traceurs :

1. Localisez le **Bloqueur de publicités et Antitracker** fonctionnalité dans **Paramètres**.
2. Basculez le commutateur sur **SUR** position.

### Liste blanche

Certains sites ne fonctionnent pas correctement quand les traceurs et les publicités sont bloqués, Vous pouvez résoudre ce problème en ajoutant les URL des domaines concernés à la liste blanche, mais n'oubliez pas que dans ce cas vous verrez des publicités et les traceurs seront activés.

Ajoutez les sites Internet pour lesquels vous souhaitez autoriser l'affichage de publicités et l'utilisation de traceurs :

1. Localisez le **Bloqueur de publicités et Antitracker** fonctionnalité dans **Paramètres**.
2. en cliquant sur le lien **Gérer**, puis en vous rendant dans la section Liste blanche de la fenêtre et en cliquant sur le lien **Gérer** correspondant.
3. en cliquant sur **Ajouter un site Internet** et en insérant l'URL souhaitée.

## Connexion automatique

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

Pour vous éviter de vous mettre en danger lorsque vous vous connectez à un réseau Wi-Fi public non sécurisé, Bitdefender Total Security comprend une fonctionnalité de connexion automatique. Elle permet à Bitdefender Total Security de s'activer automatiquement dans certaines situations, en fonction de vos préférences et de votre système d'exploitation.

- Sur **Windows**, la fonctionnalité de connexion automatique peut être activée dans les situations suivantes :
  - **Démarrage :** pour connecter le VPN au démarrage de Windows.
  - **Wi-Fi non sécurisé :** pour utiliser le VPN à chaque fois que vous vous connectez à un réseau Wi-Fi public ou non sécurisé.
  - **Applications de pair-à-pair :** pour vous connecter au VPN lorsque vous lancez une application de partage de fichiers en pair-à-pair.
  - **Applications et domaines :** pour utiliser systématiquement le VPN avec certaines applications et certains sites Internet.

Note

1. Cliquez sur le lien **Gérer**.
2. Cliquez sur Parcourir, allez à l'emplacement de l'application avec laquelle vous souhaitez utiliser le VPN, sélectionnez le nom de l'application, puis cliquez sur **Ajouter**.

- **Catégories de sites Internet :** pour connecter le VPN lorsque vous visitez certaines catégories de sites Internet. Le VPN de Bitdefender peut se connecter automatiquement pour les catégories de sites Internet suivantes :
  - Finance
  - Paiements en ligne
  - Santé
  - Partage de fichiers
  - Rencontres en ligne
  - Contenu réservé aux adultes

Note

Vous pouvez sélectionner un serveur différent pour l'établissement de la connexion VPN pour chaque catégorie.

- Sur **macOS**, la fonctionnalité de connexion automatique peut être activée dans les situations suivantes :
  - **Démarrage :** pour connecter le VPN au démarrage de macOS.
  - **Wi-Fi non sécurisé :** Utilisez le VPN chaque fois que vous vous connectez à des réseaux Wi-Fi publics ou non sécurisés.
  - **Applications peer-to-peer :** Connectez-vous au VPN lorsque vous démarrez une application de partage de fichiers peer-to-peer.
  - **Applications:** pour utiliser systématiquement le VPN avec certaines applications.
- Sur **Android** et **iOS**, Bitdefender Total Security peut être configuré pour se connecter automatiquement uniquement lorsque vous vous connectez à un réseau Wi-Fi public ou non sécurisé.

# Avancé

## Segmentation du tunnel

La segmentation de tunnel opérée par un réseau privé virtuel (VPN) vous permet de chiffrer le trafic lié à certaines de vos applications ou à certains de vos appareils en l'acheminant via un VPN, tandis que les autres applications et appareils conservent un accès direct à Internet. Cette fonctionnalité est particulièrement utile si vous souhaitez bénéficier de services qui fonctionnent mieux lorsqu'ils connaissent votre localisation tout en profitant d'un accès sécurisé à des communications et données potentiellement sensibles.

Lorsque vous activez la fonctionnalité **Segmentation de tunnel**, les applications et sites Internet sélectionnés contourneront le VPN et accèderont directement à Internet.

Pour gérer les applications et sites Internet qui contournent le VPN :

1. Cliquez sur le lien **Gérer** une fois la fonctionnalité activée.
2. Cliquez sur le bouton **Ajouter**.
3. Cliquez sur Parcourir, allez à l'emplacement de l'application en question ou insérez l'URL du site Internet souhaité, puis cliquez sur **Ajouter**.

> **Note**
> Lorsque vous ajoutez un site Internet, tout le domaine, y compris l'ensemble des sous-domaines, sera contourné.

> **Important**
> Sur les appareils **macOS**, la fonctionnalité de segmentation de tunnel n'est disponible que pour les sites Internet.

## App Traffic Optimizer

La fonctionnalité App Traffic Optimizer de Bitdefender Total Security vous permet de de donner la priorité au trafic des applications les plus importantes sur votre appareil sans exposer votre connexion aux risques de confidentialité. Les VPN redirigent le trafic Internet à travers un tunnel sécurisé tout en utilisant des algorithmes de cryptage puissants pour le protéger.

Cependant, cette combinaison de techniques peut présenter quelques inconvénients, particulièrement en ce qui concerne la vitesse de la connexion. Plusieurs facteurs peuvent ralentir la connexion, les plus courants étant la distance qui vous sépare du serveur auquel vous vous connectez, la congestion du réseau et l'utilisation élevée de la bande passante. Si vous remarquez que Bitdefender Total Security ralentit parfois votre connexion Internet, il y a peut-être une meilleure solution que de désactiver le VPN.

**Comment fonctionne App Traffic Optimizer ?**

Certaines applications et services tels que les plateformes de streaming, les clients torrent et les jeux nécessitent plus de bande passante. Leur utilisation constante pourrait affecter la vitesse de votre connexion Internet. L'acheminement de votre trafic par un tunnel VPN soumet déjà votre connexion à un ralentissement relatif. Une pression supplémentaire sur votre connexion peut sérieusement dégrader votre expérience en ligne.

La fonctionnalité App Traffic Optimizer de Bitdefender Total Security peut vous aider à faire face aux ralentissements de la connexion VPN en donnant la priorité à l'application de votre choix. Cette fonction vous permet de décider quelles applications doivent recevoir la majeure partie de votre trafic, puis d'allouer les ressources en conséquence. Par exemple, si vous êtes en réunion et que vous remarquez que la qualité de votre appel est médiocre, App Traffic Optimizer vous permet de donner la priorité au trafic vers l'application de vidéoconférence pour améliorer les résultats.

En général, les utilisateurs de VPN ferment tous les processus qui interfèrent sur leur appareil, voire désactivent leur connexion VPN pour obtenir une vitesse Internet plus rapide. App Traffic Optimizer vous permet de bénéficier d'une protection ininterrompue de votre vie privée sans compromettre votre vitesse de connexion.

## Utiliser App Traffic Optimizer

Actuellement, la fonctionnalité est uniquement disponible sur les appareils Windows et vous permet de donner la priorité au trafic de 3 applications maximum.

Suivez ces étapes pour activer et configurer facilement App Traffic Optimizer :

1. Lancez l'application Bitdefender VPN sur votre ordinateur Windows.
2. Cliquez sur la petite roue dentée dans le volet latéral pour accéder aux paramètres du VPN.
3. Accédez à l'onglet **Généraux** et activez la fonctionnalité **App Traffic Optimizer**. La couleur de l'interrupteur passera du gris au bleu.

Pour gérer les applications priorisées par cette fonctionnalité :

1. Clique le**Gérer**lien.
2. Cliquez sur Parcourir, allez à l'emplacement de l'application que vous voulez accélérer, sélectionnez-la, puis cliquez sur **Ajouter**. L'application apparaît dans la section **Prioritaire**.

> **Note**
> Sinon, si vous avez récemment ouvert l'application que vous souhaitez prioriser, appuyez sur le bouton + situé dans la fenêtre de l'optimiseur de trafic.

3. Déconnectez et reconnectez le VPN de Bitdefender après avoir ajouté ou supprimé des applications de la liste.

Pour supprimer une application de l'optimiseur de trafic, il vous suffit de cliquer sur l'icône à côté du nom de l'application.

> **Note**
> L'App Traffic Optimizer n'est pas disponible sur macOS.

## Protocole

Ici, vous pouvez choisir le type de protocole que vous souhaitez utiliser pour le transfert de données. Les options suivantes sont disponibles :

- **Automatique** - Bitdefender VPN sélectionnera le protocole optimal pour votre appareil et votre réseau spécifiques.
- **Catapulte d'Hydre** - Rapide et sécurisé, idéal pour le streaming et les jeux.
- **OpenVPN UDP** - Optimisé pour des vitesses rapides. Cependant, ce protocole n'est pas aussi fiable en termes de perte de données que les autres protocoles de la liste.

- **OpenVPN TCP** - Conçu pour la fiabilité. Garantit que vos données sont entièrement livrées, mais ce n'est pas aussi rapide qu'OpenVPN UDP.
- **Fil de protection** - Protocole plus récent, offrant une sécurité renforcée et un haut niveau de performances.

### Double saut

Avec cette fonctionnalité, vous pouvez gérer les serveurs via lesquels envoyer et double-crypter votre trafic Internet. Vos données transiteront par deux serveurs VPN au lieu d'un, ce qui rendra plus difficile le suivi de votre activité Internet.

**Note**
Vous ne pouvez ajouter qu'un total de 5 emplacements à double saut. Cependant, vous pouvez supprimer les doubles sauts personnalisés de votre liste et en créer d'autres à tout moment.

**Important**
L'utilisation de serveurs situés sur différents continents dans le même double saut peut ralentir votre vitesse de connexion.

## 7.6. Désinstallation de Bitdefender Total Security

La procédure de suppression de Bitdefender Total Security est similaire à celle que vous utilisez pour les autres programmes de votre ordinateur :

- **Désinstallation de Bitdefender Total Security sur les appareils Windows**
  - Sur **Windows 7** :
    1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration** et deux fois sur **Programmes et fonctionnalités**.
    2. Trouvez **Bitdefender Total Security** et cliquez sur **Désinstaller**. Patientez jusqu'à la fin du processus de désinstallation.
  - Sur **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 **Programmes et fonctionnalités**.
3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
   Attendez que le processus de désinstallation soit terminé.

- Sur **Windows 10** et **Windows 11** :
  1. Cliquez sur **Démarrer**, puis sur **Paramètres**.
  2. Cliquez sur l'icône **Système** dans les paramètres, puis sélectionnez **Applications installées**.
  3. Trouver **Bitdefender Total Security** et sélectionnez **Désinstaller**.
  4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
     Attendez que le processus de désinstallation soit terminé.

- **Désinstallation sur des appareils macOS**
  1. Cliquez sur **Aller** dans la barre de menu et sélectionnez **Applications**.
  2. Double-cliquez sur le dossier **Bitdefender**.
  3. Lancez **l'assistant de désinstallation de Bitdefender**.
  4. Dans la nouvelle fenêtre, cochez la case située à côté de **Bitdefender Total Security**, puis cliquez sur **Désinstaller**.
  5. Saisissez un nom de compte administrateur et un mot de passe valide, puis cliquez sur **OK**.
  6. Vous serez ensuite averti que Bitdefender Total Security a bien été désinstallé. Cliquez sur **Fermer**.

- **Désinstallation sur des appareils Android**
  1. Ouvrez l'application **Play Store**.
  2. Cherchez **Bitdefender Total Security**.
  3. Sur la page Bitdefender Total Security du magasin d'applications, sélectionnez **Désinstaller**.
  4. Confirmez en appuyant sur **OK**.

- **Désinstallation sur des appareils iOS**
  1. Maintenez votre doigt appuyé sur l'application Bitdefender Total Security.
  2. Sélectionnez **Supprimer l'application**.
  3. Appuyez sur **Supprimer**.

## 7.7. Questions les Plus Fréquentes

**Quand dois-je utiliser le VPN Bitdefender ?**

Vous devez faire preuve de prudence lorsque vous accédez à des contenus ou que vous téléchargez/envoyez des données sur Internet. Pour être certain(e) de rester en sécurité pendant que vous naviguez sur le Web, nous vous recommandons d'utiliser le VPN lorsque vous voulez :

- vous connecter à des réseaux sans-fil publics
- accéder à des contenus normalement disponibles uniquement depuis certaines régions, que vous soyez ou non chez vous
- assurer la confidentialité de vos données personnelles (identifiants, mots de passe, adresses e-mail, informations bancaires, etc.)
- masquer votre adresse IP

**Puis-je choisir une ville avec le VPN de Bitdefender ?**

Oui. Actuellement, le VPN de Bitdefender pour Windows, macOS, Android et iOS peut être utilisé pour sélectionner une ville spécifique. Voici la liste des villes présentement disponibles :

- **États-Unis :** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada :** Montréal, Toronto, Vancouver
- **Royaume-Uni :** Londres, Manchester

**Le VPN de Bitdefender peut-il être installé en tant qu'application indépendante ?**

L'application VPN est installée automatiquement en même temps que votre solution de sécurité Bitdefender. Elle peut également être installée en tant qu'application indépendante depuis la page du produit (Google Play Store et App Store).

**Est-ce que Bitdefender partagera mon adresse IP et mes données personnelles avec des tiers ?**

Non, avec le VPN de Bitdefender, votre vie privée est protégée à 100 %. Personne n'aura accès aux journaux de vos activités en ligne (qu'il s'agisse d'agences publicitaires, de FAI, de compagnies d'assurance, etc.).

**Quels algorithmes de chiffrement le VPN utilise-t-il ?**

Le VPN de Bitdefender utilise le protocole Hydra sur toutes les plateformes, un chiffrement AES 256 bits ou le plus haut chiffre disponible pris en charge par le client et le serveur, avec Perfect Forward Secrecy. Cela signifie que les clés de chiffrement sont générées pour chaque nouvelle session VPN et effacées de la mémoire lorsque la session est terminée.

**Puis-je avoir accès à des contenus normalement indisponibles dans ma région ?**

Avec le VPN Premium vous avez accès à un vaste réseau d'emplacements virtuels dans le monde entier.

**Le VPN aura-t-il une incidence négative sur l'autonomie de mon appareil ?**

Le VPN de Bitdefender a été conçu pour protéger vos données personnelles, masquer votre adresse IP quand vous êtes connecté à des réseaux sans-fil non sécurisés, et accéder à des contenus normalement indisponibles dans votre pays. Pour éviter d'utiliser pour rien la batterie de votre appareil, nous vous recommandons d'utiliser uniquement le VPN quand vous en avez besoin, et de le déconnecter quand vous êtes hors ligne.

**Pourquoi le VPN ralentit-il ma connexion Internet ?**

Le VPN de Bitdefender a été pensé pour ne pas perturber votre navigation Web, mais la distance entre votre emplacement réel et le serveur auquel vous choisissez de vous connecter peut provoquer des ralentissements. Toutefois, ces ralentissements sont presque toujours suffisamment minimes pour que vous ne les remarquiez pas lors de vos activités en ligne habituelles. De plus, nous nous appuyons sur l'une des infrastructures VPN les plus rapides du monde. Si vous n'avez pas l'obligation de vous connecter à un serveur lointain (par exemple, des États-Unis à la France), nous vous recommandons d'autoriser le VPN à se

connecter automatiquement au serveur le plus proche, ou de trouver un serveur plus proche de votre emplacement actuel.

# 8. OBTENIR DE L'AIDE

## 8.1. Demander de l'aide

Bitdefender offre à ses clients une assistance sans égale, rapide et précise. Si vous rencontrez des difficultés ou si vous avez la moindre question au sujet de votre produit Bitdefender, nous mettons à votre disposition plusieurs ressources en ligne dans lesquelles vous trouverez sûrement une solution ou une réponse. Vous pouvez également contacter le service client Bitdefender. Nos représentants vous répondront dans les plus brefs délais et vous fourniront toute l'aide dont vous avez besoin.

## 8.2. Ressources En Ligne

De nombreuses ressources en ligne sont disponibles pour vous aider à trouver des réponses à vos questions et résoudre les problèmes liés à Bitdefender.

- Centre de Support Bitdefender :
  https://www.bitdefender.fr/consumer/support/
- Communauté des experts Bitdefender :
  https://community.bitdefender.com/fr/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Vous pouvez également utiliser le moteur de recherche de votre choix pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

### 8.2.1. Centre de support 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, ainsi que les bugs constatés, par le support technique de Bitdefender. Vous y découvrirez également des articles généraux sur la prévention contre les menaces, sur la gestion, en détail, des solutions Bitdefender et beaucoup d'autres articles.

La base de connaissances de Bitdefender est ouverte au public et consultable gratuitement. Cet ensemble d'information est une autre

manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'information ou les rapports de bug venant de clients de Bitdefender trouvent une réponse en cherchant dans la base de donnés de Bitdefender, comme les rapports de bugs, travaux associés, feuillet ou article d'information venant compléter les fichiers d'aide des produits.

Le centre de support Bitdefender est accessible à tout moment à l'adresse suivante : https://www.bitdefender.fr/consumer/support/.

### 8.2.2. Communauté des experts Bitdefender

La communauté des experts est un espace dans lequel des utilisateurs et des amateurs des produits Bitdefender peuvent échanger, s'entraider et partager leurs connaissances et leurs solutions. C'est aussi un espace propice à l'émergence d'idées et de commentaires précieux pour nos développeurs. Les membres de la communauté sont des utilisateurs expérimentés heureux de donner un peu de leur temps pour aider les autres. Grâce à leurs généreux efforts, nous avons créé une base de connaissances dans laquelle tous les utilisateurs peuvent une aide et un peu de convivialité.

Vous pourrez avoir des conversations riches avec des personnes qui utilisent vraiment les produits Bitdefender. Cette communauté permet aux membres d'établir des liens et de faire entendre leurs voix. Ils sont encouragés à y participer en sachant que leurs opinions et leurs contributions sont respectées et appréciées. En tant que fournisseur reconnu, nous nous efforçons d'offrir à nos clients une assistance rapide et précise et nous voulons nous rapprocher d'eux. C'est dans cette optique nous avons créé cette communauté.

Vous pouvez rejoindre la communauté des experts ici :

https://community.bitdefender.com/fr/

### 8.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia regroupe toutes les dernières informations sur les cybermenaces. c'est là que les experts Bitdefender partagent deq conseils et des astuces sur la protection contre les pirates, les violations de données et l'usurpation d'identité, notamment sur les réseaux sociaux.

La page Bitdefender Cyberpedia se trouve ici :

https://www.bitdefender.com/cyberpedia.

## 8.3. Pour nous joindre

Une communication efficace est la clé d'une relation professionnelle réussie. Depuis 2001, BITDEFENDER s'est bâti une réputation irréprochable en cherchant sans cesse à améliorer sa communication pour dépasser les attentes de ses clients et de ses partenaires. Si vous avez la moindre question, n'hésitez pas à nous contacter directement via **Bitdefender Support Center**.

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

### 8.3.1. 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. Rendez-vous sur https://www.bitdefender.com/partners/partner-locator.html.
2. Choisissez vos pays et ville à l'aide des options correspondantes.

# GLOSSAIRE

**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.

**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. ActiveX est connu pour son manque total de contrôles de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

**Menaces persistantes avancées**

Les Menaces persistantes avancées exploitent les vulnérabilités des systèmes pour voler des informations importantes et les livrer à la source. Les grands groupes tels que les entreprises, les sociétés ou les gouvernements sont ciblés par cette menace. L'objectif d'une menace persistante avancée est de passer inaperçue pendant le plus de temps possible, tout en surveillant et regroupant des informations importantes sans endommager les machines ciblées. La méthode utilisée pour injecter la menace dans le réseau consiste à faire ouvrir un fichier PDF ou un document Office qui a l'air inoffensif, pour que chaque utilisateur puisse exécuter les fichiers.

**Adware**

Les publiciels sont souvent associés à des applications gratuites qui exigent leur acceptation par l'utilisateur. Ces publiciels étant généralement installés une fois que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux. Cependant, les fenêtres publicitaires peuvent devenir

contrariantes et, dans certains cas, nuire aux performances du système. De plus, les informations recueillies peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des conditions de l’accord de licence.

**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.

**Porte dérobée**

Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative ; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

**Secteur de démarrage**

Un secteur au début de chaque disque qui identifie l’architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.

**Virus de démarrage**

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.

**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 pourriels, voler des données, contrôler à distance les appareils vulnérables ou diffuser des logiciels espions, rançongiciels, ou tout autre type de menace. Leur objectif est d'infecter autant d'appareils connectés que possible, comme les PC, serveurs, mobiles ou autres objets connectés appartenant à des grandes entreprises.

**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 (plugiciels) pour certains formats.

**Attaque par force brute**

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

**Ligne de commande**

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

**Cookies**

Sur Internet, les témoins sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des témoins est encore en développement. Son but est de cibler directement les intérêts que vous avez exprimés. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "code SKU" (ce code barres se trouvant au dos des produits de consommation). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

**Cyberharcèlement**

Lorsque des camarades ou des inconnus mènent des actions abusives envers des enfants dans le but de les blesser physiquement. Pour leur nuire sur le plan émotionnel, les assaillants envoient des messages malveillants ou des photos peu flatteuses, provoquant l’isolation de leurs victimes ou un sentiment de frustration.

**Attaque par dictionnaire**

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

**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).

**Télécharger**

Copier des données (généralement un fichier entier) d'une source principale à 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.

**E-mail**

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

**Événements**

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire.

**Exploits**

Une manière de tirer profit des bugs et vulnérabilités (logicielles ou matérielles) qui sont présents sur un ordinateur. Les pirates peuvent ainsi prendre le contrôle des ordinateurs ou réseaux.

**Faux positif**

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

**Extension du nom 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 systèmes plus anciens n'en supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

**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.

**Pot de miel**

Un faux système informatique est créé pour attirer les pirates informatiques afin d'étudier la façon dont ils agissent et identifient les méthodes hérétiques utilisées pour collecter des informations sur le système. Les sociétés et les entreprises sont plus intéressées par la mise en place et l'utilisation de pots de miel 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.

**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.

**Enregistreur de frappe**

Un enregistreur de frappe est une application qui enregistre tout ce qui est saisi avec le clavier. Les enregistreurs de frappe ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros d'assurance sociale).

**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.

**Client de messagerie**

Un client de messagerie est une application qui vous permet d'envoyer et recevoir des e-mails.

**Mémoire**

Zone de stockage interne dans votre ordinateur. Le terme mémoire regarde le stockage des données dans les "chips" (composants), et le terme stockage regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

**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.

**Prédateurs en ligne**

Individus cherchant à discuter avec des mineurs et des adolescents dans le but de les impliquer dans des activités sexuelles illégales. Les réseaux sociaux sont l'endroit idéal pour traquer les enfants vulnérables et les séduire dans le but de les faire se livrer à des activités sexuelles, en ligne ou en face à face.

**Programmes compressés**

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 comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

**Chemin**

Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas.

La connexion entre deux points, comme le canal de communication entre deux ordinateurs.

**Phishing**

Action d'envoyer un courriel à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du courriel. Cet courriel oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

**Photon**

Photon est une technologie Bitdefender innovante et discrète, conçue pour limiter l'impact de la solution de sécurité sur les performances. En surveillant l'activité de votre PC en tâche de fond, elle crée des modèles d'utilisation qui aident à optimiser les processus de démarrage et d'analyse.

**Virus polymorphe**

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.

**Port**

Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les PCs 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.

**Ransomware**

Les ransomwares sont des programmes malveillants qui tentent de soutirer de l'argent aux utilisateurs en bloquant leurs systèmes vulnérables. CryptoLocker, CryptoWall, et TeslaWall ne sont que des variantes qui traquent les systèmes personnels des utilisateurs.

L'infection peut se répandre via courriel, le téléchargement de pièces jointes, ou l'installation d'applications, sans prévenir l'utilisateur de ce qui se passe dans son système. Les utilisateurs quotidiens et les entreprises sont ciblés par les pirates derrière les rançongiciels.

**Fichier de rapport**

Un fichier qui enregistre les actions qui surviennent. 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.

**Rootkit**

Un rootkit est un ensemble d'outils logiciels permettant aux administrateurs d'accéder à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs systèmes.

Le principal rôle des rootkits est de cacher des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau, s'ils incluent les logiciels appropriés.

Les trousses administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des trousses administrateur. Cependant, ils sont principalement utilisés pour camoufler des menaces

ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des menaces, les trousses administrateur pirates sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des journaux et passer inaperçus.

**Script**

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

**Spam**

Message électronique ou envoi de messages souvent répertoriés comme des e-mails « non sollicités ».

**Spyware**

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.

**Éléments 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.

**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.

**Barre d'état**

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.

**TCP/IP**

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des normes pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

**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 des informations sur les menaces**

La signature binaire de la menace, utilisée par la solution de sécurité pour détecter et éliminer la menace.

**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 Trojans, 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.

**Mise à jour**

Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas.

BitDefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

**Réseau privé virtuel (VPN)**

C'est une technologie qui permet une connexion temporaire et chiffrée à un certain réseau plutôt qu'à un autre moins sécurisé. De cette façon, l'envoi et la réception de données sont protégés et chiffrés et plus difficiles à intercepter pour les pirates. Une preuve de sécurité est l'identification, qui ne peut se faire que via un identifiant et un mot de passe.

**Ver**

Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.