

Bitdefender[®] ANTIVIRUS FREE



**GUIDE DE
L'UTILISATEUR**





Bitdefender Antivirus Gratuit

Guide de l'utilisateur

Date de parution 04/12/2023
Copyright © 2023 Bitdefender

Mention légale

Tous les droits sont réservés. Aucune partie de ce livre ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris la photocopie, l'enregistrement ou par tout système de stockage et de récupération d'informations, sans l'autorisation écrite d'un représentant autorisé de Bitdefender. L'inclusion de brèves citations dans les critiques n'est possible qu'avec la mention de la source citée. Le contenu ne peut en aucun cas être modifié.

Avertissement et clause de non-responsabilité. Ce produit et sa documentation sont protégés par copyright. Les informations contenues dans ce document sont fournies « telles quelles », sans garantie. Bien que toutes les précautions aient été prises lors de la préparation de ce document, les auteurs n'assumeront aucune responsabilité envers toute personne ou entité en ce qui concerne toute perte ou dommage causé ou prétendument causé directement ou indirectement par les informations contenues dans ce travail.

Ce livre contient des liens vers des sites Web tiers qui ne sont pas sous le contrôle de Bitdefender. Par conséquent, Bitdefender n'est pas responsable du contenu de tout site lié. Si vous accédez à un site Web tiers répertorié dans ce document, vous le ferez à vos risques et périls. Bitdefender fournit ces liens uniquement à titre de commodité, et l'inclusion du lien n'implique pas que Bitdefender approuve ou accepte toute responsabilité quant au contenu du site tiers.

Marques de commerce. Des noms de marque peuvent apparaître dans ce livre. Toutes les marques déposées et non déposées dans ce document sont la propriété exclusive de leurs propriétaires respectifs et sont respectueusement reconnues.

Bitdefender®



Table des matières

À propos de ce guide	1
Objectifs et destinataires	1
Comment utiliser ce guide	1
Conventions utilisées dans ce guide	1
Normes typographiques	1
Avertissement	2
Commentaires	2
1. Installation	4
1.1. Préparer l'installation	4
1.2. Configuration requise	4
1.3. Configuration logicielle requise	5
1.4. Installer votre produit Bitdefender	6
1.4.1. Installation depuis Bitdefender Central	6
1.4.2. Installer à partir du disque d'installation	9
2. Pour démarrer	15
2.1. Fonctions de base	15
2.1.1. Notifications	16
2.1.2. Profils	17
2.1.3. Paramètres de la protection par mot de passe	19
2.1.4. Rapports sur les produits	20
2.1.5. Notifications sur les promotions	20
2.2. Interface Bitdefender	20
2.2.1. Icône de la zone de notification	21
2.2.2. Menu de navigation	23
2.2.3. Tableau de bord	24
2.2.4. Rubriques Bitdefender	27
2.2.5. Changer la langue du produit	32
2.3. Bitdefender Central	32
2.3.1. À propos de Bitdefender Central	32
2.3.2. Accéder à Bitdefender Central	33
2.3.3. Authentification à deux facteurs	34
2.3.4. Ajouter des appareils approuvés	36
2.3.5. Activité	36
2.3.6. Mes abonnements	37
2.3.7. Mes appareils	38
2.3.8. Avis	42
2.4. Maintenir Bitdefender à jour	42
2.4.1. Vérifier si Bitdefender est à jour	42
2.4.2. Mise à jour en cours	43



2.4.3. Activer ou désactiver la mise à jour automatique	43
2.4.4. Réglage des paramètres de mise à jour	44
2.4.5. Mises à jour continues	45
3. Gérer votre sécurité	46
3.1. Protection antivirus	46
3.1.1. Analyse à l'accès (protection en temps réel)	47
3.1.2. Analyse à la demande	52
3.1.3. Consulter les journaux d'analyse	61
3.1.4. Analyse automatique de supports amovibles	61
3.1.5. Configurer des exceptions d'analyse	63
3.1.6. Gérer les fichiers en quarantaine	66
3.2. Défense avancée contre les menaces	67
3.2.1. Activer ou désactiver Advanced Threat Defense	67
3.2.2. Vérification des attaques malveillantes détectées	68
3.2.3. Ajout de processus aux exceptions	68
3.2.4. Détection des exploits	69
3.2.5. Activer ou désactiver la détection des exploits	69
3.3. Prévention des menaces en ligne	69
3.3.1. Alertes de Bitdefender dans le navigateur	71
4. Comment faire pour	73
4.1. Installation	73
4.1.1. Comment installer Bitdefender sur un deuxième appareil ?	73
4.1.2. Comment réinstaller Bitdefender ?	73
4.1.3. D'où puis-je télécharger mon produit Bitdefender ?	74
4.1.4. Comment passer à la dernière version de Bitdefender ? ..	75
4.2. Centrale Bitdefender	76
4.2.1. Comment se connecter à un compte Bitdefender depuis un autre compte ?	76
4.2.2. Comment désactiver les messages d'aide de Bitdefender Central ?	77
4.2.3. J'ai oublié le mot de passe de mon compte Bitdefender. Comment le réinitialiser ?	77
4.2.4. Comment gérer les sessions de connexion de mon compte Bitdefender ?	78
4.3. Analyser avec BitDefender	79
4.3.1. Comment analyser un fichier ou un dossier ?	79
4.3.2. Comment analyser mon système	79
4.3.3. Comment programmer une analyse ?	80
4.3.4. Comment créer une tâche d'analyse personnalisée ?	80
4.3.5. Comment exclure un dossier de l'analyse ?	82



4.3.6. Que faire lorsque Bitdefender a signalé qu'un fichier sain était infecté ?	83
4.3.7. Comment connaître les menaces détectées par Bitdefender ?	84
4.4. Informations utiles	85
4.4.1. Comment tester ma solution de sécurité ?	85
4.4.2. Comment supprimer Bitdefender ?	86
4.4.3. Comment éteindre automatiquement l'appareil une fois l'analyse terminée ?	87
4.4.4. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?	88
4.4.5. Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?	89
4.4.6. Comment afficher des objets cachés dans Windows ?	90
4.4.7. Comment supprimer les autres solutions de sécurité ?	91
4.4.8. Comment redémarrer en mode sans échec ?	92
5. Résolution de problèmes	94
5.1. Résoudre les problèmes les plus fréquents	94
5.1.1. Mon système semble lent	94
5.1.2. L'analyse ne démarre pas	96
5.1.3. Je ne peux plus utiliser une application	98
5.1.4. Que faire quand Bitdefender bloque un site web, un domaine, une adresse IP ou une application en ligne pourtant sûr ?	100
5.1.5. Comment mettre à jour Bitdefender avec une connexion internet lente ?	101
5.1.6. Les services Bitdefender ne répondent pas	101
5.1.7. La désinstallation de Bitdefender a échoué	102
5.1.8. Mon système ne démarre pas après l'installation de Bitdefender	103
5.2. Suppression des menaces de votre système	106
5.2.1. Que faire quand Bitdefender détecte des menaces sur votre appareil ?	107
5.2.2. Comment nettoyer un menace dans une archive ?	109
5.2.3. Comment nettoyer une menace dans une archive de messagerie ?	110
5.2.4. Que faire si je soupçonne un fichier d'être dangereux ? ...	111
5.2.5. Que sont les fichiers protégés par mot de passe du journal d'analyse ?	111
5.2.6. Que sont les éléments ignorés du journal d'analyse ?	112
5.2.7. Que sont les fichiers ultra-compressés du journal d'analyse ?	112



5.2.8. Pourquoi Bitdefender a-t-il effacé automatiquement un fichier infecté ?	112
6. Obtenir de l'aide	114
6.1. Demander de l'aide	114
6.2. Ressources En Ligne	114
6.2.1. Centre de support Bitdefender	114
6.2.2. Communauté des experts Bitdefender	115
6.2.3. Bitdefender Cyberpedia	115
6.3. Pour nous joindre	116
6.3.1. Distributeurs locaux	116
Glossaire	117



À PROPOS DE CE GUIDE

Objectifs et destinataires

Ce manuel d'utilisation est destiné à tous les utilisateurs qui ont choisi Bitdefender Antivirus Free comme solution de sécurité pour leur ordinateur personnel. Les informations présentées dans ce livret sont destinées aussi bien aux utilisateurs expérimentés en informatique qu'à toute personne sachant utiliser Windows.

Vous découvrirez comment configurer et utiliser Bitdefender Antivirus Free pour vous protéger contre les menaces et les autres logiciels malveillants. Vous saurez comment tirer le meilleur parti de votre Bitdefender.

Nous vous souhaitons un apprentissage agréable et utile.

Comment utiliser ce guide

Ce guide est organisé autour de plusieurs grands thèmes :

[Pour démarrer \(page 15\)](#)

Démarrez avec Bitdefender Free et son interface utilisateur.

[Gérer votre sécurité \(page 46\)](#)

Apprenez à utiliser Bitdefender Free pour vous protéger contre les logiciels malveillants.

[Comment faire pour \(page 73\)](#)

En savoir plus sur Bitdefender Gratuit.

[Obtenir de l'aide \(page 114\)](#)

Où chercher et où demander de l'aide si quelque chose d'inattendu apparaît.

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. INSTALLATION

1.1. Préparer l'installation

Avant d'installer Bitdefender Antivirus Free, 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 \(page 4\)](#).
- 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.

1.2. Configuration requise

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

- Windows 7 avec Service Pack 1
- Windows 8



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



Important

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



Note

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

- 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.

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



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.

1.4.1. Installation depuis Bitdefender Central

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

Pour télécharger Bitdefender Antivirus Free 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 boîte 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 Antivirus Free.

Étape 1 - Installation de Bitdefender

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

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 Antivirus Free.

1.4.2. Installer à partir du disque d'installation

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

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

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

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

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 Antivirus Free.

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 Antivirus Free.

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 \(page 32\)](#).

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 boîte 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 Antivirus Free interface.



2. POUR DÉMARRER

2.1. Fonctions de base

Une fois Bitdefender Antivirus Free installé, votre appareil est protégé contre toutes sortes de menaces (comme les programmes malveillants, les logiciels espion, les ransomwares, les exploits, les botnets et les chevaux de Troie) et les menaces Internet (comme les pirates, le phishing et le spam).

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

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

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

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

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



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

Bitdefender peut vous permettre de travailler, jouer ou regarder des films sans être dérangé en reportant les tâches de maintenance, en supprimant les interruptions et en ajustant les effets visuels du système. Vous pouvez bénéficier de tout ceci en activant et en configurant les [Profils \(page 17\)](#).

Bitdefender prendra pour vous la plupart des décisions de sécurité et affichera rarement des alertes contextuelles. Des détails sur les actions prises et des informations sur le fonctionnement du programme sont disponibles dans la fenêtre Notifications. Pour plus d'informations, reportez-vous à [Avis \(page 42\)](#).

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

Pour utiliser les fonctionnalités en ligne de Bitdefender Antivirus Free et gérez vos abonnements et appareils, accédez à votre compte Bitdefender. Pour plus d'informations, reportez-vous à [Bitdefender Central \(page 32\)](#).

Vous trouverez dans la rubrique [Comment faire pour \(page 73\)](#) des instructions étape par étape pour les tâches courantes. Si vous rencontrez des difficultés, consultez la rubrique [Résoudre les problèmes les plus fréquents \(page 94\)](#) qui indique comment résoudre les problèmes les plus courants.

2.1.1. Notifications

Bitdefender tient un journal détaillé des événements concernant son activité sur votre appareil. Lorsqu'un événement relatif à la sécurité de votre système ou de vos données se 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 appareil, etc.



Vous pouvez également adopter d'autres actions si nécessaire ou modifier les actions appliquées par Bitdefender.

Pour accéder au journal des **notifications**, cliquez sur Notifications dans le menu de navigation de l'**interface 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 à 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 rubrique.

2.1.2. Profils

Certaines utilisations de l'ordinateur comme les jeux en ligne ou les présentations vidéo nécessitent plus de performance et de réactivité du système et aucune interruption. Lorsque votre ordinateur portable est alimenté par sa batterie, il vaut mieux que les opérations non indispensables, qui consomment de l'énergie supplémentaire, soient reportées jusqu'au moment où l'ordinateur portable sera branché sur secteur.

Les profils Bitdefender permettent d'attribuer davantage de ressources du système aux applications en cours d'exécution en modifiant les paramètres de la protection et en adaptant la configuration du système. Par conséquent, l'impact sur votre activité est réduit.

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



Profil Travail

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

Profil Films

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

Profil Jeux

Améliore les effets visuels et supprime les interruptions lorsque vous jouez.

Profil Réseau Wi-Fi public

Applique les paramètres du produit afin de bénéficier de la protection complète lorsque vous êtes connecté à un réseau sans fil non sécurisé.

Profil Économie de batterie

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

Configurer l'activation automatique des profils

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

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

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

Pour permettre à Bitdefender d'activer les profils automatiquement :

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

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



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

Pour plus d'informations sur les profils, reportez-vous à [Profils \(page 17\)](#).

2.1.3. Paramètres de la protection par mot de passe

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

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

1. Cliquez sur **Paramètres** dans le menu de navigation de l'**interface Bitdefender**.
2. Dans la fenêtre **Paramètres généraux**, activez **Protection par mot de passe**.
3. Saisissez le mot de passe dans les deux champs puis cliquez sur OK. (8 caractères minimum)

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



Important

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

Pour supprimer la protection par mot de passe :

1. Cliquez sur **Paramètres** dans le menu de navigation sur le [Interface Bitdefender](#).
2. Dans la fenêtre **Paramètres généraux**, désactivez **Protection par mot de passe**.
3. Saisissez le mot de passe puis cliquez sur **OK**.



Note

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



2.1.4. Rapports sur les produits

Les rapports sur les produits contiennent des informations sur la manière d'utiliser le produit Bitdefender que vous avez installé. Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir un meilleur service à l'avenir.

Veuillez noter que ces rapports ne comportent aucune donnée confidentielle, comme votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

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

1. Cliquez sur **Paramètres** dans le menu de navigation sur le [Interface Bitdefender](#).
2. Cliquez sur l'onglet **Paramètres avancés**.
3. Désactivez **Rapports sur les produits**.

2.1.5. Notifications sur les promotions

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

Pour activer ou désactiver les notifications sur les promotions :

1. Cliquez sur **Paramètres** dans le menu de navigation sur le [Interface Bitdefender](#).
2. Dans la fenêtre **Généraux**, activez ou désactivez le bouton correspondant.

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

2.2. Interface Bitdefender

Bitdefender Antivirus Free 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 Bitdefender, un assistant d'introduction présentant des informations sur la manière d'interagir et de configurer le



produit est affiché dans la partie supérieure gauche. Cliquez sur la flèche pour continuer à être guidé, ou sur **Passer le tour** pour fermer l'assistant.

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

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

Depuis le menu de navigation situé à gauche, vous pouvez accéder aux paramètres, aux notifications et aux **rubriques Bitdefender** qui contiennent des informations détaillées sur la configuration et les tâches administratives avancées.

Depuis la partie supérieure de l'interface principale, vous pouvez accéder à votre **compte Bitdefender**. Vous pouvez également communiquer avec nous pour obtenir des réponses à vos questions ou de l'aide face à une situation normale.

2.2.1. Icône de la zone de notification

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



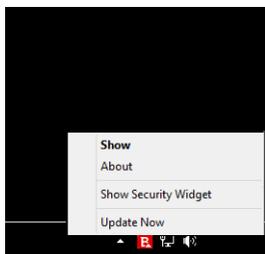
Note

L'icône Bitdefender n'est pas toujours visible. Pour qu'elle s'affiche en permanence :

- Sur **Windows 7, Windows 8 et Windows 8.1**
 1. Cliquez sur la flèche  en bas à droite de l'écran.
 2. Cliquez sur **Personnaliser...** pour ouvrir la fenêtre Icônes de la zone de notification.
 3. Sélectionnez l'option **Afficher les icônes et les notifications** pour l'icône **Agent Bitdefender**.
- Sur **Windows 10**
 1. Faites un clic droit sur la barre des tâches et sélectionnez **Paramètres de la barre des tâches**.
 2. Faites défiler le menu déroulant et cliquez sur le lien **Sélectionner les icônes à afficher dans la barre des tâches** dans la rubrique **Zone de notification**.
 3. Activez le bouton à côté de **Agent Bitdefender**.

Double-cliquez sur cette icône pour ouvrir BitDefender. Si vous effectuez un clic droit sur cette icône, le menu contextuel qui apparaît vous permettra de gérer le produit BitDefender plus rapidement.

- **Afficher** - ouvre la fenêtre principale de Bitdefender.
- **À propos** - ouvre une fenêtre sur laquelle vous trouverez des informations sur Bitdefender, où trouver de l'aide en cas d'imprévu, où consulter les Conditions d'utilisation de l'abonnement, les composants de tiers et la Politique de confidentialité.
- **Mettre à jour** - lance immédiatement une mise à jour. Vous pouvez connaître l'état de mise à jour dans le panneau Mise à jour de la **fenêtre principale de Bitdefender**.





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

A. Aucun problème de sécurité n'affecte votre système.

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

Si Bitdefender ne fonctionne pas, l'icône de la zone de notification apparaît sur fond gris : **B.** C'est généralement le cas lorsque l'abonnement a expiré. Cela peut aussi se produire lorsque les services Bitdefender ne répondent pas ou lorsque d'autres erreurs empêchent le fonctionnement normal de Bitdefender.

2.2.2. Menu de navigation

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

-  **Tableau de bord.** D'ici, vous pouvez rapidement corriger les problèmes de sécurité, voir des recommandations adaptées aux besoins de votre système et à vos habitudes d'utilisation, exécuter des actions rapides et installer Bitdefender sur d'autres appareils.
-  **Protection.** D'ici, vous pouvez lancer et configurer des analyses antivirus, accéder aux réglages du pare-feu, récupérer des données qui auraient été chiffrées par un ransomware et configurer une protection tout en naviguant sur Internet.
-  **Vie privée.** D'ici, vous pouvez créer des gestionnaires de mots de passe pour vos comptes en ligne, empêcher les accès indésirables à votre webcam, procéder à des paiements en ligne dans un environnement sécurisé, ouvrir l'application VPN et protéger vos enfants en consultant et en limitant leurs activités en ligne.
-  **Utilitaires.** D'ici, vous pouvez optimiser la vitesse de votre système et configurer la fonctionnalité Antivol de vos appareils.
-  **Notifications.** D'ici, vous pouvez accéder aux notifications générées.



-  **Paramètres.** D'ici, vous pouvez accéder aux paramètres généraux.
-  **Support.** D'ici, vous pouvez contacter le support technique Bitdefender si vous avez besoin d'aide pour utiliser Bitdefender Antivirus Free.
-  **Mon compte.** D'ici, vous pouvez accéder à votre compte Bitdefender pour vérifier votre abonnement et effectuer des tâches de sécurité sur les appareils que vous gérez. Les détails à propos du compte Bitdefender et les abonnements en cours sont également disponibles.

2.2.3. Tableau de bord

Le tableau de bord permet d'effectuer des tâches courantes, de corriger rapidement des problèmes de sécurité, d'afficher des informations sur le fonctionnement du produit et accéder aux panneaux à partir desquels vous configurez le produit.

Tout se trouve à quelques clics.

La fenêtre est organisée en trois catégories :

Zone État de la sécurité

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

Autopilot

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

Actions rapides

Ici, vous pouvez exécuter différentes tâches pour protéger votre système et maintenir une vitesse optimale. Vous pouvez également facilement installer Bitdefender sur d'autres appareils, si votre abonnement peut les couvrir.

Zone de l'état de sécurité

Bitdefender utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre appareil et de vos données et vous en informer. Les problèmes détectés comprennent la désactivation d'importants paramètres de protection et d'autres conditions pouvant constituer un risque pour la sécurité.

Lorsque des problèmes affectent la sécurité de votre appareil, l'état affiché en haut de l'**interface Bitdefender** devient rouge. L'état affiché indique la



nature des problèmes affectant votre système. En outre, l'icône de la **zone de notification** devient , et si vous faites glisser le curseur de la souris sur l'icône, une fenêtre de notification confirmera la présence de problèmes en attente.

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

Autopilot

Pour garantir un fonctionnement 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, visionnage de films, jeux - Bitdefender Autopilot vous proposera des recommandations contextuelles basées sur votre utilisation de l'appareil et vos besoins.

Les recommandations peuvent également concerner des mesures que vous devez prendre pour assurer le bon fonctionnement de votre produit.

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

Désactivation des notifications d'Autopilot

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

Pour désactiver les notifications d'Autopilot :

1. Cliquez sur **Paramètres** dans le menu de navigation sur le [Interface Bitdefender](#).
2. Dans la fenêtre **Paramètres généraux**, désactivez **Notification des recommandations**.

Actions rapides

Grâce aux actions rapides, vous pouvez rapidement exécuter des tâches jugées importantes pour maintenir la protection de votre système tout en lui assurant des performances optimales.



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

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

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

- **Analyse rapide.** Exécuter une analyse rapide pour détecter rapidement les menaces potentiellement présentes sur votre appareil.
- **Analyse du système.** Exécuter une analyse du système pour vérifier qu'aucune menace se trouve sur votre appareil.
- **Analyse des vulnérabilités.** Rechercher des vulnérabilités sur votre appareil pour vérifier que toutes les applications, ainsi que le système d'exploitation, sont à jour et fonctionnent correctement.
- **Wifi Security Advisor.** Ouvrir la fenêtre de Wi-Fi Security Advisor dans le module Vulnérabilité.
- **Wallets.** Visualiser et gérer vos wallets.
- **Safepay.** Ouvrir Bitdefender Safepay™ pour protéger vos données sensibles lorsque vous effectuez des transactions en ligne.
- **VPN.** Ouvrir Bitdefender VPN pour bénéficier d'une couche supplémentaire de protection pendant nos activités sur Internet.
- **File Shredder.** Lancer l'outil File Shredder pour supprimer toute trace de données sensibles sur votre appareil.
- **OneClick Optimizer.** Libérer de l'espace sur le disque, corriger les erreurs du registre et protéger votre vie privée en supprimant les fichiers qui ne sont plus utiles d'un simple clic.

Pour commencer à protéger d'autres appareils avec Bitdefender :

1. Cliquez sur **Installer sur un autre appareil**.
Une nouvelle fenêtre s'affiche à l'écran.
2. Cliquez sur **PARTAGER LE LIEN DE TÉLÉCHARGEMENT**.
3. Suivez les étapes figurant à l'écran pour installer Bitdefender.



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

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

2.2.4. Rubriques Bitdefender

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

Pour accéder aux fonctionnalités d'une rubrique spécifique ou pour commencer à configurer votre produit, accédez aux icônes suivantes situées dans le menu de navigation de l'**interface Bitdefender** :

-  **Protection**
-  **Vie privée**
-  **Utilitaires**

Protection

Dans la rubrique Protection, vous pouvez configurer vos réglages de sécurité avancés, gérer vos amis et les spammeurs, afficher et modifier les paramètres de connexion réseau, configurer les fonctionnalités de protection contre les menaces en ligne, vérifier et corriger les vulnérabilités potentielles du système et évaluer la sécurité des réseaux sans fil auxquels vous vous connectez.

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

ANTIVIRUS

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



La fonctionnalité Antivirus vous permet d'accéder facilement aux tâches d'analyse suivantes :

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

Pour plus d'informations sur les tâches d'analyse et sur comment configurer la protection antivirus, consultez [Protection antivirus \(page 46\)](#).

ONLINE THREAT PREVENTION

Online Threat Prevention en ligne vous protège contre les attaques de phishing, les tentatives de fraude et les fuites de données personnelles lorsque vous naviguez sur internet.

Pour plus d'informations sur comment configurer Bitdefender pour protéger vos activités en ligne, consultez [Prévention des menaces en ligne \(page 69\)](#).

PARE-FEU

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

Pour plus d'informations sur la configuration du pare-feu, consultez [Pare-feu](#).

ADVANCED THREAT DEFENSE

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

Pour plus d'informations sur la manière de protéger votre système des menaces, veuillez vous référer à [Défense avancée contre les menaces \(page 67\)](#).

ANTISPAM

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



Pour plus d'informations sur la protection antispam, reportez-vous à [Antispam](#).

VULNÉRABILITÉ

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

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

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

Pour plus d'informations sur la configuration de la protection contre les vulnérabilités, reportez-vous à [Vulnérabilité](#).

TRAITEMENT DES RANSOMWARES

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

Pour en savoir plus sur la manière de récupérer vos fichiers chiffrés, reportez-vous à [Remédiation des ransomwares](#).

Vie privée

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

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

VPN

Le VPN sécurise vos activités en ligne et masque votre adresse IP lorsque vous vous connectez à des réseaux sans-fil non sécurisés dans les



aéroports, les commerces, les cafés ou les hôtels. Il vous permet en outre d'accéder à des contenus qui ne seraient normalement pas disponibles dans votre région.

Pour plus d'informations sur cette fonctionnalité, reportez-vous à [VPN](#).

PROTECTION VIDÉO & AUDIO

La protection vidéo & audio protège votre webcam en bloquant son accès aux applications non approuvées et vous informe lorsque des applications tentent d'accéder à votre micro.

Pour plus d'informations sur la façon dont vous pouvez protéger votre webcam des accès non désirés et sur comment configurer Bitdefender afin qu'il vous informe des activités de votre micro, veuillez vous référer à [Video & Audio Protection](#).

PASSWORD MANAGER

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

Pour plus d'informations sur la configuration de Password Manager, consultez [Password Manager protège vos identifiants](#).

SAFEPAY

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

Pour en savoir plus sur Bitdefender Safepay™, reportez-vous à [La sécurité Safepay pour les transactions en ligne](#).

PARENTAL CONTROL

Bitdefender Parental Control vous permet de contrôler les activités de vos enfants sur leurs appareils. S'ils consultent des contenus appropriés, vous pouvez décider de restreindre leur accès à Internet ou à des applications spécifiques.

Cliquez sur **Configurer** dans le volet Parental Control afin de commencer à configurer les appareils de vos enfants et ainsi suivre leurs activités en ligne.

Pour plus d'informations sur la configuration de Parental Control, consultez [Contrôle parental](#).



BLOQUEUR DE TRACEURS

Le bloqueur de traceurs vous aide à éviter les traceurs afin que vos données restent privées lorsque vous naviguez en ligne, tout en réduisant le temps de chargement des sites Internet.

Pour plus d'informations sur le bloqueur de traceurs, référez-vous à [Bloqueur de traceurs](#).

Utilitaires

Dans la rubrique Outils, vous pouvez améliorer la vitesse système et gérer vos appareils.

OneClick Optimizer

Bitdefender Total Security n'assure pas que la sécurité. La solution préserve aussi les performances de vos appareils.

Our OneClick Optimizer vous aidera à identifier et à supprimer les fichiers inutiles de votre appareil en une étape simple.

Pour plus d'informations à ce sujet, reportez-vous à [Optimiseur OneClick](#).

Antivol

L'antivol Bitdefender protège votre appareil et vos données contre la perte ou le vol. Cette fonctionnalité permet de localiser ou de verrouiller à distance votre appareil, ainsi que d'en effacer toutes les données.

L'antivol Bitdefender comprend les fonctionnalités suivantes :

- Localisation à distance
- Verrouillage à distance
- Effacement des données à distance
- Alerte à distance

Pour savoir comment maintenir votre système hors de portée des personnes malintentionnées, reportez-vous à [Antivol d'appareil](#).

Protection des données

La fonctionnalité Bitdefender File Shredder vous permet de supprimer définitivement des données en les effaçant de votre disque dur.

Pour plus d'informations à ce sujet, reportez-vous à [Protection des données](#).



Profils

Effectuer des activités professionnelles quotidiennes, regarder des films ou jouer peut ralentir le système, en particulier si des processus de mise à jour Windows et des tâches de maintenance ont lieu simultanément.

Bitdefender vous permet désormais de choisir et d'appliquer le profil de votre choix, qui fait les réglages nécessaires pour améliorer les performances de certaines applications installées sur le système.

Pour plus d'informations sur cette fonctionnalité, reportez-vous à [Profils](#).

2.2.5. Changer la langue du produit

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

1. Cliquez sur **Paramètres** dans le menu de navigation sur le [Interface Bitdefender](#).
2. Dans la fenêtre **Paramètres généraux**, cliquez sur **Modifier la langue**.
3. Sélectionnez la langue souhaitée dans la liste puis cliquez sur **ENREGISTRER**.
4. Attendez quelques instants que les paramètres soient appliqués.

2.3. Bitdefender Central

2.3.1. À propos de Bitdefender Central

La plateforme Bitdefender Central vous permet d'accéder aux fonctionnalités et aux services en ligne du produit et d'effectuer des tâches importantes sur les appareils sur lesquels Bitdefender est installé. Vous pouvez vous connecter à votre compte Bitdefender depuis n'importe quel ordinateur ou appareil mobile connecté à Internet en suivant ce lien <https://central.bitdefender.com> ou directement depuis l'application Bitdefender Central pour les appareils Android et iOS.

Pour installer l'application Bitdefender Central sur vos appareils :

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



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

Une fois la connexion effectuée, vous pouvez commencer à :

- Télécharger et installer Bitdefender sur les systèmes d'exploitation Windows, macOS, iOS et Android. Les produits disponibles au téléchargement sont :
 - Gamme de produits Bitdefender pour Windows
 - Bitdefender Antivirus for Mac
 - Bitdefender Mobile Security for Android
 - Bitdefender Mobile Security for iOS
- Gérer et renouveler vos abonnement Bitdefender.
- Ajouter de nouveaux appareils à votre réseau et les gérer où que vous soyez.
- Protéger les appareils de votre réseau et leurs données contre le vol et la perte avec **Antivol**.
- Configurer **Parental Control** pour les appareils de vos enfants et surveiller leurs activités d'où que vous soyez.

2.3.2. Accéder à Bitdefender Central

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

- Depuis l'interface principale de Bitdefender :
 1. Cliquez sur **Mon compte** dans le menu de navigation de l'**interface Bitdefender**.
 2. Cliquez sur **Accéder à Bitdefender Central**.
 3. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
- A partir de votre navigateur web :



1. Ouvrir un navigateur web sur chaque appareil ayant accès à internet.
 2. Aller à : <https://central.bitdefender.com>.
 3. Connectez-vous à votre compte à l'aide de votre adresse e-mail et de votre mot de passe.
- Depuis votre appareil Android ou iOS :
1. Ouvrez l'application Bitdefender Central que vous avez installée.



Note

Ce document reprend les options que vous pourrez trouver sur l'interface web.

2.3.3. Authentification à deux facteurs

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

Activer l'authentification à deux facteurs

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

Pour activer l'authentification à deux facteurs :

1. Accès [Centrale Bitdefender](#).
2. Cliquez sur l'icône  située dans le coin supérieur droit de l'écran.
3. Cliquez sur **Compte Bitdefender** dans le menu coulissant.
4. Sélectionnez l'onglet **Mot de passe et sécurité**.
5. Cliquez sur **Authentification à 2 facteurs**.
6. Cliquez sur **COMMENCER**.

Choisissez l'une des deux méthodes suivantes :



- **Application d'authentification** - utilise une application d'authentification pour générer un code chaque fois que vous souhaitez vous connecter à votre compte Bitdefender.
Si vous souhaitez utiliser une application d'authentification, mais que vous ne savez pas laquelle choisir, nous mettons à votre disposition une liste des applications d'authentification que nous recommandons.
 - a. Cliquez sur **UTILISER UNE APPLICATION D'AUTHENTIFICATION** pour commencer.
 - b. Pour vous connecter sur un appareil Android ou iOS, utilisez votre appareil pour scanner le QR code.
Pour vous connecter sur un ordinateur portable ou sur un ordinateur de bureau, vous pouvez saisir manuellement le code qui s'affiche.
Cliquez sur **CONTINUER**.
 - c. Saisissez le code fourni par l'application ou celui affiché lors de l'étape précédente, puis cliquez sur **ACTIVER**.
- **E-mail** - chaque fois que vous vous connecterez à votre compte Bitdefender, un code de vérification vous sera envoyé par e-mail. Validez votre adresse e-mail puis utilisez le code que vous avez reçu.
 - a. Cliquez sur **UTILISER UNE ADRESSE E-MAIL** pour commencer.
 - b. Consultez votre messagerie et saisissez le code fourni.
 - c. Cliquez sur **ACTIVER**.
 - d. 10 codes d'activation vous sont fournis. Vous pouvez copier, télécharger ou imprimer la liste et l'utiliser en cas d'oubli de votre adresse e-mail ou d'impossibilité de vous connecter à votre messagerie. Chaque code peut être utilisé une seule fois.
 - e. Cliquez sur **TERMINER**.

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

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



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

3. Confirmez votre choix.

2.3.4. Ajouter des appareils approuvés

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

Pour ajouter des appareils aux appareils approuvés :

1. Accès [Centrale Bitdefender](#).
2. Cliquez le  icône dans le coin supérieur droit de l'écran.
3. Cliquez sur **Compte Bitdefender** dans le menu des diapositives.
4. Sélectionnez le **Mot de passe et sécurité** languette.
5. Cliquez sur **Appareils approuvés**.
6. La liste des appareils sur lesquels Bitdefender est installé s'affiche. Cliquez sur l'appareil de votre choix.

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

2.3.5. Activité

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

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

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



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

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

- **Menaces bloquées.** Vous pouvez ici voir un graphique présentant une statistique générale avec des informations sur les menaces bloquées ces dernières 24 heures et au cours des sept derniers jours. Les informations affichées sont récupérées en fonction du comportement malveillant détecté sur les fichiers, applications et URL.
- **Utilisateurs avec le plus de menaces bloquées.** Ici, vous pouvez visualiser un classement indiquant quels utilisateurs ont été le plus confrontés à des menaces.
- **Appareils avec le plus de menaces bloquées.** Vous pouvez voir ici un classement des appareils sur lesquels le plus de menaces ont été détectés.

2.3.6. Mes abonnements

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

Vérifier les abonnements disponibles

Pour vérifier vos abonnements disponibles :

1. Accès [Centrale Bitdefender](#).
2. Sélectionner le panneau **Mes Abonnements**.

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

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



Note

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



Activer abonnement

Un abonnement peut être activé pendant le processus d'installation grâce à votre compte Bitdefender. Avec le processus d'activation, la validité de l'abonnement commence le décompte.

Si vous avez acheté un code d'activation chez l'un de nos revendeurs ou que vous l'avez reçu en cadeau, vous pouvez ajouter sa disponibilité à votre abonnement Bitdefender.

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

1. Accès [Centrale Bitdefender](#).
2. Sélectionnez le **Mes abonnements** panneau.
3. Cliquez sur le bouton **CODE D'ACTIVATION**, puis saisissez le code dans le champs correspondant.
4. Cliquez sur **ACTIVER** pour continuer.

L'abonnement est désormais activé.

Renouveler abonnement

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

1. Accès [Centrale Bitdefender](#).
2. Sélectionnez le **Mes abonnements** panneau.
3. Sélectionnez la carte d'abonnement souhaitée.
4. Cliquez sur **RENOUVELER** pour continuer.

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

2.3.7. Mes appareils

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



Ajouter un nouvel appareil

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

1. Accès [Centrale Bitdefender](#).
2. Sélectionnez le **Mes appareils** panneau, puis appuyez 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, appuyez 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, appuyez sur le bouton correspondant.
Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**. Saisissez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER PAR E-MAIL**. Attention, le lien de téléchargement généré sera valide pendant 24 heures seulement. Si le lien expire, il vous faudra 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 appuyez sur le bouton de téléchargement correspondant.
4. Attendez que le téléchargement soit terminé, puis lancez l'installation.

Personnalisez votre appareil

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

1. Accès [Centrale Bitdefender](#).
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur la carte de l'appareil désiré, puis sur l'icône  dans l'angle supérieur droit de l'écran.
4. Sélectionnez **Paramètres**.



5. Saisissez un nouveau nom dans le champ **Nom de l'appareil**, puis cliquez sur **ENREGISTRER**.

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

1. Accès [Centrale Bitdefender](#).
2. Sélectionnez le **Mes appareils** panneau.
3. Appuyez sur la carte d'appareil souhaitée, puis sur la ☰ icône dans le coin supérieur droit de l'écran.
4. Sélectionnez **Profil**.
5. Cliquez sur **Ajouter un propriétaire**, puis remplissez les champs correspondants. Vous pouvez personnaliser le profil en ajoutant une photo, une date de naissance et une adresse e-mail ou un numéro de téléphone.
6. Cliquez sur **AJOUTER** pour sauvegarder le profil.
7. Sélectionnez le propriétaire souhaité dans la liste des **propriétaires d'appareils**, puis cliquez sur **ASSIGNER**.

Actions à distance

Pour mettre à jour Bitdefender à distance sur un appareil :

1. Accès [Centrale Bitdefender](#).
2. Sélectionnez le **Mes appareils** panneau.
3. Appuyez sur la carte d'appareil souhaitée, puis sur la ☰ icône dans le coin supérieur droit de l'écran.
4. Sélectionnez **Mise à jour**.

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

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

- **Tableau de bord.** Dans cette fenêtre, vous pouvez consulter des informations relatives à l'appareil sélectionné, vérifier l'état de sa protection, l'état du VPN Bitdefender et le nombre de menaces bloquées au cours des sept derniers jours. L'état de la protection peut



s'afficher en vert (aucun problème n'affecte votre appareil), en jaune (un sujet mérite votre attention) ou en rouge (l'appareil est en danger). Si votre appareil présente des problèmes, cliquez sur la flèche située dans la zone d'état supérieure pour en savoir plus. D'ici, vous

- **Protection.** Depuis cette fenêtre, vous pouvez exécuter à distance une analyse rapide ou une analyse système de vos appareils. Cliquez sur le bouton **ANALYSER** pour lancer le processus. Vous pouvez également vérifier à quand remonte les dernières analyses sur vos appareils et obtenir les rapports correspondants, contenant les informations les plus importantes.
- **Optimizer.** Ici, vous pouvez améliorer à distance les performances d'un appareil en analysant, en détectant et en effaçant rapidement les fichiers inutiles. Cliquez sur le bouton **COMMENCER**, puis sélectionnez les zones que vous souhaitez optimiser. Cliquez de nouveau sur le bouton **COMMENCER** pour lancer le processus d'optimisation. Cliquez sur **Plus d'informations** pour accéder à un rapport détaillé sur les problèmes résolus.
- **Antivol.** En cas de perte ou de vol de votre appareil, la fonctionnalité antivol vous permet de le localiser et de prendre des mesures à distance. Cliquez sur **LOCALISER** pour découvrir l'emplacement de l'appareil. Sa dernière position connue sera affichée, ainsi que la date et l'heure correspondantes.
- **Vulnérabilité.** Pour vérifier la présence de vulnérabilités (telles que des mises à jour Windows manquantes, des applications obsolètes ou des mots de passe faibles) sur un appareil, cliquez sur le bouton **ANALYSER** dans l'onglet Vulnérabilité. Il n'est pas possible de corriger les vulnérabilité à distance. Si une vulnérabilité est découverte, vous devez lancer une nouvelle analyse sur l'appareil concerné puis appliquer les actions recommandées. Cliquez sur **Plus d'informations** pour accéder à un rapport détaillé sur les problèmes détectés.



2.3.8. Avis

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

2.4. Maintenir Bitdefender à jour

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

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

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



Important

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

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

- Si votre appareil se connecte à internet via un serveur proxy, vous devez configurer les paramètres du proxy comme indiqué dans .
- Si vous êtes connecté à Internet via une connexion à distance, nous vous conseillons de régulièrement mettre à jour Bitdefender en utilisant la fonctionnalité de mise à jour à la demande.

2.4.1. Vérifier si Bitdefender est à jour

Pour savoir à quand remonte la dernière mise à jour de Bitdefender :



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

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

2.4.2. Mise à jour en cours

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

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

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



Important

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

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

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

1. Accès [Centrale Bitdefender](#).
2. Sélectionnez le **Mes appareils** panneau.
3. Cliquez sur la carte de périphérique souhaitée, puis sur le  icône dans le coin supérieur droit de l'écran.
4. Sélectionner **Mise à jour**.

2.4.3. Activer ou désactiver la mise à jour automatique

Activer ou désactiver la mise à jour automatique :

1. Cliquez sur **Paramètres** dans le menu de navigation sur le [Interface Bitdefender](#).



2. Cliquez sur l'onglet **Mettre à jour**.
3. Activez ou désactivez le bouton correspondant.
4. Une fenêtre d'avertissement s'affiche. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactiver la mise à jour automatique.
Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, ou jusqu'au redémarrage du système.



Avertissement

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

2.4.4. Réglage des paramètres de mise à jour

Les mises à jour peuvent être effectuées depuis le réseau local, sur Internet, directement ou via un serveur proxy. Par défaut, Bitdefender vérifie la disponibilité de nouvelles mises à jour toutes les heures, sur Internet, et les installe sans vous en avertir.

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

Pour ajuster les paramètres de mise à jour :

1. Cliquez sur **Paramètres** dans le menu de navigation sur le [Interface Bitdefender](#).
2. Sélectionnez l'onglet **Mise à jour**, ajustez les paramètres en fonction de vos préférences.

Fréquence de la mise à jour

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

Règles de traitement des mises à jour

À chaque fois qu'une mise à jour est disponible, Bitdefender téléchargera et installera automatiquement la mise à jour, sans aucune notification.



Désactivez l'option **Mise à jour silencieuse** si vous voulez être averti à chaque fois qu'une nouvelle mise à jour est disponible.

Certaines mises à jour nécessitent un redémarrage pour terminer l'installation.

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

Si vous souhaitez être averti lorsqu'une mise à jour nécessite un redémarrage, activez l'option **Notification de redémarrage**.

2.4.5. Mises à jour continues

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

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



Note

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



3. GÉRER VOTRE SÉCURITÉ

3.1. Protection antivirus

Bitdefender protège votre appareil contre tous les types de logiciels malveillants (programmes malveillants, chevaux de Troie, logiciels espions, trousseaux 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 \(page 61\)](#).

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 \(page 63\)](#).

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 \(page 66\)](#).

Si votre appareil a été infecté par des logiciels malveillants, consultez-vous [Suppression des menaces de votre système \(page 106\)](#). 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](#). 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.

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

Bitdefender fournit une protection en temps réel contre une large gamme de logiciels malveillants en analysant tous les fichiers et 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 désactiver 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 \(page 66\)](#).



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.

Par défaut, les fichiers mis en quarantaine sont automatiquement envoyés aux Bitdefender Labs pour être analysés par les chercheurs de Bitdefender. Si la présence d'une menacée est confirmée, les informations sur cette menace seront mises à jour pour permettre son élimination.

- **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 \(page 66\)](#).

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.

3.1.2. Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre appareil sans logiciel malveillant. Cela s'effectue en protégeant votre appareil des nouvelles menaces par l'analyse des 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 est 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 identifiés depuis la mise à jour précédente. Pour plus d'informations, reportez-vous à [Maintenir Bitdefender à jour \(page 42\)](#).
- 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 \(page 54\)](#).

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 débiter.

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 dont 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 **B** 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).

Patiencez 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 \(page 66\)](#).



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.

Par défaut, les fichiers mis en quarantaine sont automatiquement envoyés aux Bitdefender Labs pour être analysés par les chercheurs de Bitdefender. Si la présence d'une menacée est confirmée, les informations sur cette menace seront mises à jour pour permettre son élimination.

○ 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 \(page 106\)](#).

3.1.3. 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**.

3.1.4. 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 **B** 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

Veillez 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 recrée correctement). Pour savoir comment traiter les menaces, reportez-vous à [Suppression des menaces de votre système \(page 106\)](#).

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.

3.1.5. 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 accédez.



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**.

3.1.6. Gérer les fichiers en quarantaine

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

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

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. 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.

3.2.1. 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.



3.2.2. Vérification des attaques malveillantes détectées

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

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

3.2.3. 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**.

3.2.4. Détection des exploits

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

3.2.5. 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.

3.3. 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.

3.3.1. 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.



4. COMMENT FAIRE POUR

4.1. Installation

4.1.1. 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.

4.1.2. 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 Antivirus Free* 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 Antivirus Free** 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 Antivirus Free** 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.

4.1.3. 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.

4.1.4. 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 apparaît.
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.

4.2. Centrale Bitdefender

4.2.1. 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 \(page 114\)](#).

4.2.2. 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. Cliquez 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**.

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

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

○ 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.

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

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

1. Accès [Centrale Bitdefender](#).
2. Cliquez 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.



4.3. Analyser avec BitDefender

4.3.1. Comment analyser un fichier ou un dossier ?

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

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

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

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

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

4.3.2. 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 .



4.3.3. Comment programmer une analyse ?

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

Pour programmer une analyse :

1. Cliquez sur **protection** dans le menu de navigation 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** apparaît. D'ici, vous pouvez choisir les emplacements que vous souhaitez analyser.

4.3.4. Comment créer une tâche d'analyse personnalisée ?

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



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

1. Dans le **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.

4.3.5. 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.

4.3.6. 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 désactiver 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 ? \(page 90\)](#).
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 ? \(page 82\)](#).

Par défaut, Bitdefender est programmé pour ajouter automatiquement les fichiers restaurés à la liste des exceptions.
5. Activez la protection antivirus en temps réel de Bitdefender.
6. Contactez 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 \(page 114\)](#).

4.3.7. Comment connaître les menaces détectées par Bitdefender ?

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

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

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

Pour vérifier 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**.

4.4. Informations utiles

4.4.1. Comment tester ma solution de sécurité ?

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

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

Pour tester votre solution de sécurité :

1. Téléchargez le test 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 \(page 114\)](#).

4.4.2. 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 Antivirus Free** 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 Antivirus Free** 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. Cliquez le **Système** icône dans la zone Paramètres, puis sélectionnez **applications**.
3. Trouver **Bitdefender Antivirus Free** 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.

4.4.3. 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 \(page 57\)](#).

4.4.4. 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:
 - **Adresse** - saisissez l'adresse IP du serveur proxy.
 - **Port** - saisissez le port utilisé par Bitdefender pour se connecter au serveur proxy.
 - **Nom d'utilisateur** - entrez le nom d'utilisateur reconnu par le serveur proxy.
 - **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.

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

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

4.4.5. 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.
Sur **Windows 8.1**, trouvez **Ce PC**.
 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.

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

4.4.7. Comment supprimer les autres solutions de sécurité ?

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

Lorsque vous utilisez plusieurs solutions de sécurité sur le même appareil, le système devient instable. Le programme de désinstallation de Bitdefender Antivirus Free 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**, allez à **Panneau de commande** et double-cliquez sur **Programmes et fonctionnalités**.
2. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
3. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
4. Attendez 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. Cliquez 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.

4.4.8. Comment redémarrer en mode sans échec ?

Le mode sans échec est un mode de fonctionnement de diagnostic, utilisé principalement pour résoudre des problèmes affectant le fonctionnement normal de Windows. Ce type de problèmes peut intervenir lors de conflits de pilotes et de 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.



5. RÉOLUTION DE PROBLÈMES

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 \(page 94\)](#)
- [L'analyse ne démarre pas \(page 96\)](#)
- [Je ne peux plus utiliser une application \(page 98\)](#)
- [Que faire quand Bitdefender bloque un site web, un domaine, une adresse IP ou une application en ligne pourtant sûr ? \(page 100\)](#)
- [Comment mettre à jour Bitdefender avec une connexion internet lente ? \(page 101\)](#)
- [Les services Bitdefender ne répondent pas \(page 101\)](#)
- [Le filtre antispam ne fonctionne pas correctement](#)
- [La fonctionnalité Saisie automatique de mon Wallet ne fonctionne pas](#)
- [La désinstallation de Bitdefender a échoué \(page 102\)](#)
- [Mon système ne démarre pas après l'installation de Bitdefender \(page 103\)](#)

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}.

5.1.1. Mon système semble lent

Généralement, après l'installation d'un logiciel de sécurité, on assiste à un léger ralentissement du système, qui est normal dans une certaine mesure.

Si vous remarquez un ralentissement important, ce problème peut apparaître pour les raisons suivantes :

- **Bitdefender n'est pas le seul logiciel de sécurité installé sur le système.**



Bien que Bitdefender recherche et supprime les programmes de sécurité trouvés pendant l'installation, il est recommandé de supprimer toute solution de sécurité que vous utilisiez avant d'installer Bitdefender. Pour plus d'informations, reportez-vous à [Comment supprimer les autres solutions de sécurité ? \(page 91\)](#).

- **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 \(page 4\)](#).

- **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.

5.1.2. L'analyse ne démarre pas

Ce type de problème peut avoir deux causes principales :

- **Une installation précédente de Bitdefender qui n'a pas été complètement supprimée ou une installation défectueuse de Bitdefender.**

Dans ce cas, réinstallez Bitdefender :

- Dans **Windows 7**:
 1. Cliquez sur **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.
 2. Trouver **Bitdefender Antivirus Free** 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 Antivirus Free** 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 cliquer **Paramètres**.



2. Cliquez le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.
3. Trouver **Bitdefender Antivirus Free** 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 ? \(page 91\)](#).

2. Réinstallez Bitdefender :

○ Dans **Windows 7**:

- a. Cliquez sur **Commencer**, aller à **Panneau de commande** et double-cliquez **Programmes et fonctionnalités**.
- b. Trouver **Bitdefender Antivirus Free** 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 Antivirus Free** 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 cliquer **Paramètres**.
 - b. Cliquez le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.
 - c. Trouver **Bitdefender Antivirus Free** 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 \(page 114\)](#).

5.1.3. Je ne peux plus utiliser une application

Ce problème se produit lorsque vous essayez d'utiliser un programme qui fonctionnait normalement avant d'installer Bitdefender.

Après l'installation de Bitdefender vous pouvez vous trouver dans l'une des situations suivantes :



- Vous pourriez recevoir un message de Bitdefender indiquant que le programme essaie d'apporter une modification au système.
- Il est possible que vous receviez un message d'erreur du programme que vous tentez d'utiliser.

Ce type de situation se produit quand Advanced Threat Defense détecte à tort certaines applications comme étant malveillantes.

Advanced Threat Defense est une fonctionnalité de Bitdefender qui surveille en permanence les applications s'exécutant sur votre système et signale celles au comportement potentiellement malveillant. Étant donné que 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 \(page 114\)](#).



5.1.4. 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 que 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 \(page 114\)](#).



5.1.5. Comment mettre à jour Bitdefender avec une connexion internet lente ?

Si votre connexion internet est lente (RTC ou RNIS, par exemple), des erreurs peuvent se produire pendant le processus de mise à jour.

Pour maintenir votre système à jour avec la dernière base de données d'information sur les menaces de Bitdefender :

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

5.1.6. 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 ? \(page 91\)](#).

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 \(page 114\)](#).

5.1.7. 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 Antivirus Free** 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 Antivirus Free** 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. Cliquez le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.
 3. Trouver **Bitdefender Antivirus Free** 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.

5.1.8. 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 ? \(page 92\)](#).
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 Antivirus Free** 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 Antivirus Free** 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. Cliquez le **Système** icône dans la zone Paramètres, puis sélectionnez **Applications installées**.
 - c. Trouver **Bitdefender Antivirus Free** 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 ? \(page 92\)](#).
 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. Cliquez 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 ? \(page 92\)](#).
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 \(page 114\)](#).

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](#)



- Que faire quand Bitdefender détecte des menaces sur votre appareil ? (page 107)
- Comment nettoyer un menace dans une archive ? (page 109)
- Comment nettoyer une menace dans une archive de messagerie ? (page 110)
- Que faire si je soupçonne un fichier d'être dangereux ? (page 111)
- Que sont les fichiers protégés par mot de passe du journal d'analyse ? (page 111)
- Que sont les éléments ignorés du journal d'analyse ? (page 112)
- Que sont les fichiers ultra-compressés du journal d'analyse ? (page 112)
- Pourquoi Bitdefender a-t-il effacé automatiquement un fichier infecté ? (page 112)

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 114).

5.2.1. 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 ? \(page 90\)](#).
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 ? \(page 92\)](#).
2. Afficher les objets cachés dans Windows. Pour savoir comment procéder, reportez-vous à [Comment afficher des objets cachés dans Windows ? \(page 90\)](#).
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 \(page 114\)](#).



5.2.2. 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. Recompresser 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 114).

5.2.3. 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. Comprimez 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 cliquez 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 \(page 114\)](#).

5.2.4. 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 \(page 114\)](#).

5.2.5. 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.

5.2.6. 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.

5.2.7. 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.

5.2.8. 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.



6. OBTENIR DE L'AIDE

6.1. 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.

6.2. 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.

6.2.1. 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 données 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/>.

6.2.2. 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>

6.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia regroupe toutes les dernières informations sur les cybermenaces. c'est là que les experts Bitdefender partagent des 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>.



6.3. 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/>

6.3.1. 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 troussees administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des troussees 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 troussees 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 pernicioeux 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'Illiade 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.

VPN (réseau virtuel privé)

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.