

Bitdefender[®] **ANTIVIRUS FOR MAC**



**GUIDE
D'UTILISATION**





Bitdefender Antivirus for Mac

Guide de l'utilisateur

Date de publication : 24/11/2022
Copyright © 2022 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	2
Normes typographiques	2
Avertissement	2
Commentaires	3
1. Qu'est-ce que Bitdefender Antivirus for Mac	4
2. Installation et désinstallation	5
2.1. Configuration requise	5
2.2. Installation de Bitdefender Antivirus for Mac	5
2.2.1. Processus d'installation	6
2.3. Supprimer Bitdefender Antivirus for Mac	10
3. Pour démarrer	11
3.1. Ouvrir Bitdefender Antivirus for Mac	11
3.2. Fenêtre principale	11
3.3. Icône de l'application dans le Dock	13
3.4. Menu de navigation	13
3.5. Mode sombre	14
4. Protection contre les Logiciels Malveillants	15
4.1. Utilisation optimale	15
4.2. Analyse de Votre Mac	16
4.3. Assistant d'analyse	17
4.4. Mise en quarantaine	18
4.5. Bitdefender Shield (protection en temps réel)	19
4.6. Exceptions d'analyse	20
4.7. Protection Web	21
4.7.1. Activer les extensions Linkchecker	21
4.7.2. Gérer les paramètres des extensions	21
4.7.3. Page des notes et alertes	22
4.8. Bloqueur de traceurs	22
4.8.1. Activation du Bloqueur de traceurs Bitdefender	23
4.8.2. Interface du Bloqueur de traceurs	23
4.8.3. Désactivation du Bloqueur de traceurs Bitdefender	24
4.8.4. Autoriser le tracking d'un site web	24
4.9. Safe Files	25
4.9.1. Accès des applications	26
4.10. Protection Time Machine	26
4.10.1. Activer ou désactiver Protection Time Machine	27



4.11. Correction des problèmes	27
4.12. Notifications	28
4.13. Mises à jour	29
4.13.1. Demandes de mise à jour	30
4.13.2. Obtenir des Mises à jour via un Serveur Proxy	30
4.13.3. Mise à niveau vers une nouvelle version	30
4.13.4. Trouver des informations sur votre version de Bitdefender Antivirus for Mac	31
5. VPN	32
5.1. À propos du VPN	32
5.2. Ouvrir l'application VPN	32
5.3. Interface	33
5.4. Abonnements	35
6. Configuration des Préférences	37
6.1. Accéder aux Préférences	37
6.2. Préférences Protection	37
6.3. Préférences avancées	38
6.4. Offres spéciales	38
7. À propos de Bitdefender Central	40
7.1. Accéder à Bitdefender Central	40
7.2. Authentification à 2 facteurs	41
7.2.1. Activer l'authentification à deux facteurs	41
7.3. Ajouter des appareils approuvés	43
7.4. Mes appareils	43
7.4.1. Ajouter un nouvel appareil	44
7.4.2. Personnalisez votre appareil	44
7.4.3. Actions à distance	45
7.5. Activité	46
7.6. Mes abonnements	47
7.6.1. Vérifier les abonnements disponibles	47
7.6.2. Activer abonnement	48
7.6.3. Renouveler abonnement	48
7.7. Avis	49
8. Questions les Plus Fréquentes	50
9. Obtenir de l'aide	55
9.1. Demander de l'aide	55
9.2. Ressources En Ligne	55
9.2.1. Centre de support Bitdefender	55
9.2.2. Communauté des experts Bitdefender	56
9.2.3. Bitdefender Cyberpedia	56
9.3. Pour nous joindre	57
9.3.1. Distributeurs locaux	57



Glossaire 58



À PROPOS DE CE GUIDE

Objectifs et destinataires

Ce manuel d'utilisation est destiné à tous les Bitdefender Antivirus for Mac utilisateurs qui ont choisi 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 Macintosh.

Vous découvrirez comment configurer et utiliser Bitdefender Antivirus for Mac 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 thèmes essentiels :

[Pour démarrer \(page 11\)](#)

Commencez à utiliser Bitdefender Antivirus for Mac et son interface utilisateur.

[Protection contre les Logiciels Malveillants \(page 15\)](#)

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

[Configuration des Préférences \(page 37\)](#)

Découvrez les préférences disponibles dans Bitdefender Antivirus for Mac.

[Obtenir de l'aide \(page 55\)](#)

Sachez où regarder et à qui 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. QU'EST-CE QUE BITDEFENDER ANTIVIRUS FOR MAC

Bitdefender Antivirus for Mac est un scanner antivirus puissant, capable de détecter et de supprimer tous les types de logiciels malveillants (ou « menaces »), notamment :

- ☐ Ransomware
- ☐ les adwares
- ☐ les virus
- ☐ les spywares
- ☐ Chevaux de Troie
- ☐ les keyloggers
- ☐ les vers

Cette application détecte et supprime non seulement les menaces Mac mais également celles de Windows, vous empêchant ainsi d'envoyer accidentellement des fichiers infectés à votre famille, à vos amis ou à vos collègues utilisant des PC.



2. INSTALLATION ET DÉSINSTALLATION

Ce chapitre traite des sujets suivants :

- Configuration requise (page 5)
- Installation de Bitdefender Antivirus for Mac (page 5)
- Supprimer Bitdefender Antivirus for Mac (page 10)

2.1. Configuration requise

Vous pouvez installer Bitdefender Antivirus for Mac sur les ordinateurs Macintosh sous OS X Yosemite (10.10) ou une version supérieure.

Votre Mac doit avoir au moins 1 Go d'espace disque disponible.

Une connexion Internet est requise pour enregistrer et mettre à jour Bitdefender Antivirus for Mac.



Note

Le bloqueur de traceurs Bitdefender et le VPN Bitdefender ne peuvent être installés que sur les systèmes sous macOS 10.12 ou une version supérieure.



Comment connaître votre version de macOS et d'autres informations matérielles concernant votre Mac

Dans le menu Pomme situé en haut à gauche de l'écran, choisissez **À propos de ce Mac**. Dans la fenêtre d'informations qui apparaît, vous trouverez entre autres la version de votre système d'exploitation. Cliquez sur **Informations système** pour obtenir des informations détaillées sur votre matériel.

2.2. Installation de Bitdefender Antivirus for Mac

Pour installer l'application Bitdefender Antivirus for Mac depuis votre compte Bitdefender, procédez comme suit :

1. Connectez-vous en tant qu'Administrateur
2. Rendez-vous sur : <https://central.bitdefender.com>.
3. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.



4. Sélectionnez le panneau **Mes appareils**, puis cliquez sur **INSTALLER LA PROTECTION**.
5. Sélectionnez l'une des deux actions disponibles :
 - **Protéger cet appareil**
 - a. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
 - b. Enregistrez le fichier d'installation.
 - **Protéger d'autres appareils**
 - a. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
 - b. Appuyez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**.
 - c. Entrez une adresse électronique dans le champ correspondant, puis cliquez sur **ENVOYER PAR COURRIEL**.
Attention, le lien de téléchargement généré ne sera valide que pendant 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes instructions.
 - d. Depuis l'appareil sur lequel vous voulez installer votre produit Bitdefender, consultez la boîte de messagerie que vous avez précédemment saisie, et cliquez sur le bouton de téléchargement.
6. Exécutez le produit Bitdefender que vous avez installé.
7. Finissez les étapes de l'installation.

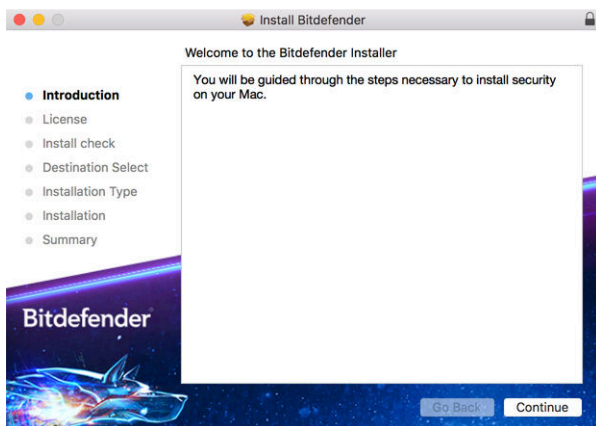
2.2.1. Processus d'installation

Pour installer Bitdefender Antivirus for Mac :

1. Cliquez sur le fichier téléchargé. Cela lancera le programme d'installation, qui vous guidera au cours du processus d'installation.
2. Suivez les indications de l'assistant d'installation.

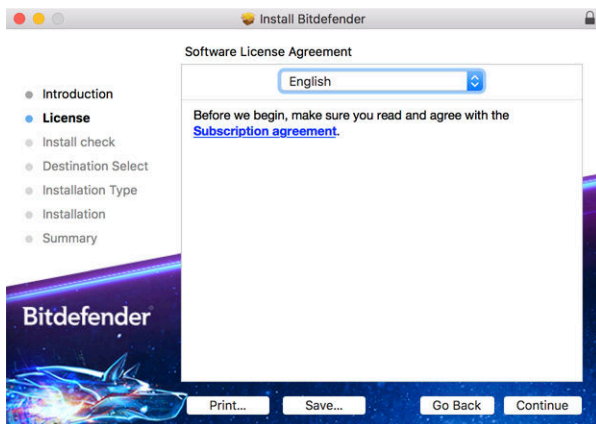


Étape 1 - Fenêtre d'accueil



Cliquez sur **Continuer**.

Étape 2 - Lire les Conditions d'abonnement



Pour poursuivre la procédure d'installation, vous devez accepter les Conditions d'utilisation de l'abonnement. Veuillez prendre le temps de lire les Conditions d'utilisation de l'abonnement, car elles contiennent les conditions dans le cadre desquelles vous pouvez utiliser Bitdefender Antivirus for Mac.

Depuis cette fenêtre, vous pourrez également sélectionner la langue dans laquelle vous voulez installer le produit.



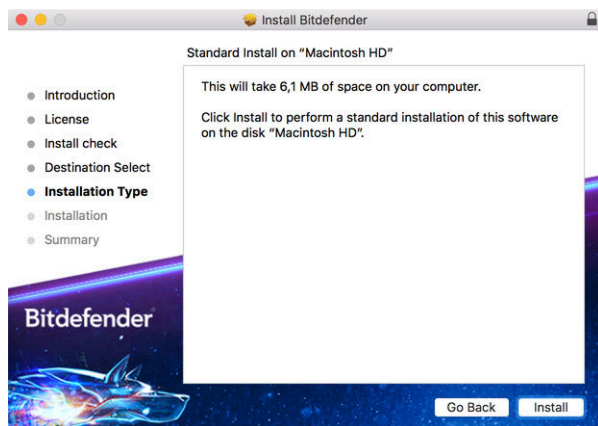
Cliquez sur **Continuer** puis sur **J'accepte**.



Important

Si vous n'acceptez pas ces conditions, cliquez sur **Continuer** puis sur **Je refuse** pour annuler l'installation et quitter le programme d'installation.

Étape 3 - Démarrer l'Installation

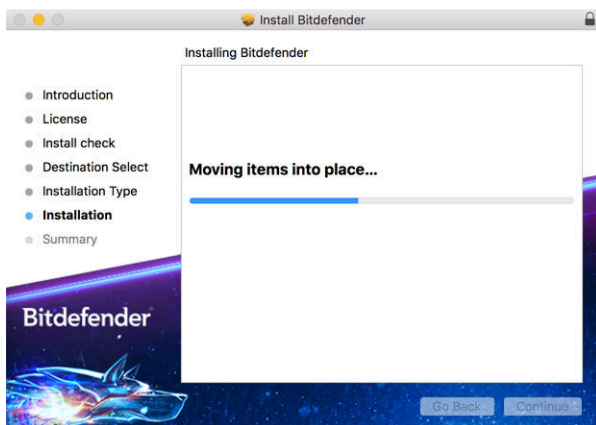


Bitdefender Antivirus for Mac sera installé dans `Macintosh HD/Library/Bitdefender`. Vous ne pouvez pas modifier le chemin d'installation.

Cliquez sur **Installer** pour lancer l'installation.

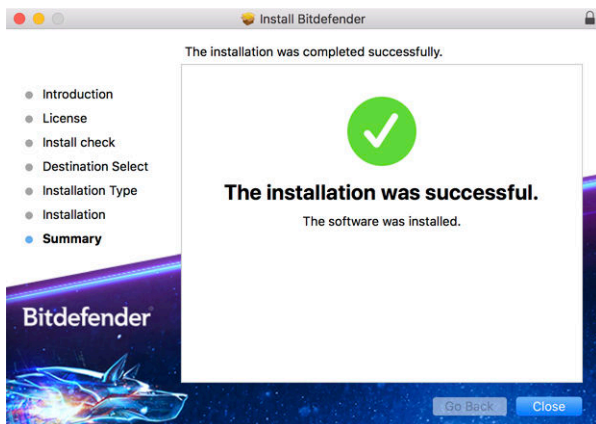


Étape 4 - Installer Bitdefender Antivirus for Mac



Patientez jusqu'à la fin de l'installation puis cliquez sur **Continuer**.

Étape 5 - Terminer



Cliquez sur **Fermer** pour fermer la fenêtre du programme d'installation.
Le processus d'installation est terminé.



Important

- Si vous installez Bitdefender Antivirus sur un appareil équipé de macOS High Sierra 10.13.0 ou d'une version plus récente, la notification **Extension système bloquée** s'affiche. Elle indique que les extensions signées par Bitdefender ont été bloquées et doivent être activées manuellement. Cliquez sur OK pour continuer. Dans la fenêtre Bitdefender Antivirus for Mac qui s'ouvre, cliquez sur le lien **Sécurité et confidentialité**. Cliquez sur **Autoriser** en bas de la fenêtre ou sélectionnez Bitdefender SRL dans la liste et cliquez sur **OK**.
- Si vous installez Bitdefender Antivirus sur un appareil équipé de macOS Mojave 10.14 ou d'une version plus récente, une nouvelle fenêtre s'ouvre. Elle indique que vous devez **Accorder à Bitdefender l'accès complet au disque et Autoriser le chargement de Bitdefender**. Suivez les instructions qui s'affichent à l'écran pour configurer le produit.

2.3. Supprimer Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac étant une application complexe, elle ne peut pas être supprimée normalement, en faisant glisser l'icône de l'application du dossier **Applications** vers la corbeille.

Pour supprimer Bitdefender Antivirus for Mac, procédez comme suit :

1. Ouvrez une fenêtre **Finder** et allez dans le dossier **Applications**.
2. Dans **Applications**, ouvrez le dossier Bitdefender puis double-cliquez sur **BitdefenderUninstaller**.
3. Sélectionnez une méthode de désinstallation.



Note

Si vous souhaitez seulement désinstaller l'application Bitdefender VPN, sélectionnez **Désinstaller le VPN** seulement.

4. Cliquez sur **Désinstaller** et attendez la fin du processus.
5. Cliquez sur **Fermer** pour terminer.



Important

Si une erreur s'est produite, vous pouvez contacter le Service Client de Bitdefender comme indiqué dans [Demander de l'aide \(page 55\)](#).




3. POUR DÉMARRER

Ce chapitre comprend les rubriques suivantes :

- Ouvrir Bitdefender Antivirus for Mac (page 11)
- Fenêtre principale (page 11)
- Icône de l'application dans le Dock (page 13)
- Menu de navigation (page 13)
- Mode sombre (page 14)

3.1. Ouvrir Bitdefender Antivirus for Mac


Vous pouvez ouvrir Bitdefender Antivirus for Mac de plusieurs façons :

- Cliquez sur l'icône de Bitdefender Antivirus for Mac dans le Launchpad.
- Cliquez sur l'icône  dans la barre de menus et sélectionnez **Ouvrir l'interface de l'antivirus**.
- Ouvrez une fenêtre Finder, allez dans Applications et double-cliquez sur l'icône de **Bitdefender Antivirus for Mac**.



Important

La première fois que vous ouvrez Bitdefender Antivirus for Mac sur macOS Mojave 10.14 ou une version plus récente, une recommandation de protection apparaît car nous avons besoin de certaines permissions pour analyser tout votre système en quête de menaces. Pour nous donner ces permissions, vous devez vous connecter en tant qu'administrateur et procéder comme suit :

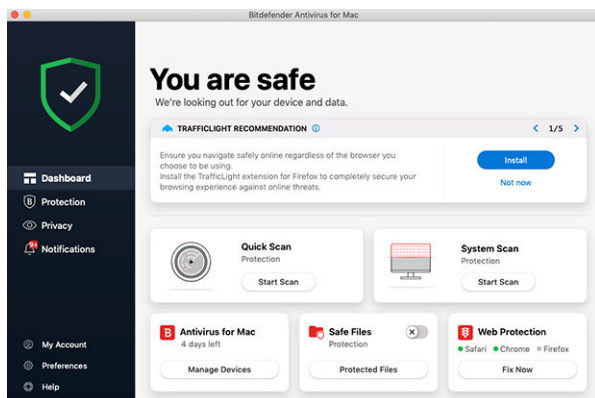
1. Cliquez sur le lien **Préférences Système**.
2. Cliquez sur l'icône , puis saisissez vos informations d'identification administrateur.
3. Une nouvelle fenêtre s'ouvre. Déposez le fichier **BDLDaemon** dans la liste des applications autorisées.

3.2. Fenêtre principale

Bitdefender Antivirus for Mac répond aux besoins de tous les utilisateurs, qu'ils soient débutants ou armés de solides connaissances techniques.



Son interface utilisateur graphique est conçue pour s'adapter à chaque catégorie d'utilisateurs.



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

La barre d'état en haut de la fenêtre vous informe de l'état de la sécurité de l'appareil par le biais de messages et de couleurs explicites. Si aucune alerte n'est en cours dans Bitdefender Antivirus for Mac, la barre d'état est verte. Lorsqu'un problème de sécurité est détecté, la barre d'état devient rouge. Pour en savoir plus sur les problèmes et leur résolution, reportez-vous à [Correction des problèmes \(page 27\)](#).

Pour vous offrir une utilisation efficace et une meilleure protection pendant toutes vos activités, **Bitdefender Autopilot** jouera le rôle de conseiller de sécurité personnel. En fonction de votre activité - travail, opérations bancaires, etc. - Bitdefender Autopilot vous proposera des recommandations contextuelles basées sur votre utilisation de l'appareil et vos besoins. Vous pourrez ainsi découvrir et mettre à profit les avantages des différentes fonctionnalités de l'application Bitdefender Antivirus for Mac.

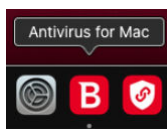
Depuis le menu de navigation à gauche, vous pouvez accéder aux sections Bitdefender permettant de configurer le produit et d'effectuer des tâches administratives avancées (onglets **Protection** et **Vie privée**), aux notifications, à votre **compte Bitdefender** et aux **préférences**. Par ailleurs,



vous pouvez nous contacter via l'onglet **Aide** si vous avez des questions ou si vous rencontrez des difficultés.





3.3. Icône de l'application dans le Dock

L'icône Bitdefender Antivirus for Mac apparaît dans le Dock dès que vous ouvrez l'application. Elle vous permet de lancer facilement l'analyse de fichiers ou de dossiers. Il vous suffit de glisser-déposer le fichier ou le dossier que vous souhaitez analyser sur l'icône du Dock pour que l'analyse démarre immédiatement.



3.4. Menu de navigation

Le menu de navigation est situé à gauche de l'interface de Bitdefender, il vous permet d'accéder rapidement aux fonctionnalités de Bitdefender dont vous avez besoin pour utiliser le produit. Les onglets disponibles dans cet espace sont les suivants :

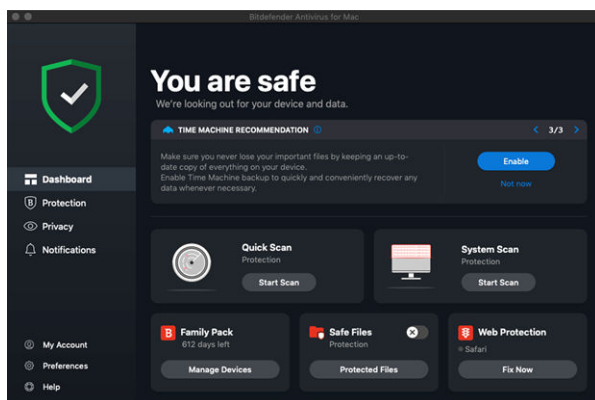
-  **Tableau de bord.** Vous pouvez ici rapidement résoudre les problèmes de sécurité, voir les recommandations correspondant aux besoins de votre système, réaliser des actions rapides, et vous rendre sur votre compte Bitdefender pour gérer les appareils que vous avez ajoutés à votre abonnement Bitdefender.
-  **Protection.** Vous pouvez ici lancer des analyses antivirus, ajouter des fichiers à la liste des exceptions, protéger vos fichiers et applications des attaques de ransomware, sécuriser vos sauvegardes Time Machine, et configurer votre protection lorsque vous surfez sur Internet.
-  **Confidentialité.** Depuis cet onglet, vous pouvez ouvrir l'application Bitdefender VPN et installer l'extension Bloqueur de traceurs sur votre navigateur web.
-  **Notifications.** Depuis cet onglet, vous pouvez obtenir des informations sur les actions déclenchées après l'analyse des fichiers.



- ⓘ **Mon compte.** Depuis cet onglet, vous pouvez savoir quel est le compte ouvert sur cet appareil et quel est l'abonnement qui le protège, mais aussi changer de compte si nécessaire.
- ⚙️ **Préférences.** Depuis cet onglet, vous pouvez paramétrer Bitdefender.
- ⓘ **Aide.** Si vous avez besoin d'assistance pour régler un problème avec votre produit Bitdefender, vous pouvez ici contacter le service de support technique. Vous pouvez également nous envoyer des commentaires pour nous aider à améliorer le produit.

3.5. Mode sombre

Pour protéger vos yeux des effets de la lumière lorsque vous travaillez la nuit ou dans un environnement peu éclairé. Bitdefender Antivirus for Mac est compatible avec le Mode sombre sur Mojave 10.14 et les versions ultérieures. Les couleurs de l'interface ont été optimisées pour que vous puissiez utiliser votre Mac sans vous fatiguer les yeux. L'interface Bitdefender Antivirus for Mac s'adapte en fonction des paramètres de votre appareil.





4. PROTECTION CONTRE LES LOGICIELS MALVEILLANTS

Ce chapitre comprend les rubriques suivantes :

- Utilisation optimale (page 15)
- Analyse de Votre Mac (page 16)
- Assistant d'analyse (page 17)
- Mise en quarantaine (page 18)
- Bitdefender Shield (protection en temps réel) (page 19)
- Exceptions d'analyse (page 20)
- Protection Web (page 21)
- Bloqueur de traceurs (page 22)
- Safe Files (page 25)
- Protection Time Machine (page 26)
- Correction des problèmes (page 27)
- Notifications (page 28)
- Mises à jour (page 29)

4.1. Utilisation optimale

Pour maintenir la protection de votre système contre les menaces et pour éviter l'infection accidentelle d'autres systèmes, suivez les conseils suivants :

- Faites en sorte que **Bitdefender Shield** soit toujours activé, pour que les fichiers système soient automatiquement analysés par Bitdefender Antivirus for Mac.
- Maintenez votre produit Bitdefender Antivirus for Mac à jour avec les dernières informations sur les menaces et mises à jour.
- Vérifiez et corrigez régulièrement les problèmes signalés par Bitdefender Antivirus for Mac. Pour plus d'informations, reportez-vous à [Correction des problèmes \(page 27\)](#).



- Vérifiez le détail des événements dans le journal d'activité de Bitdefender Antivirus for Mac sur votre ordinateur. À chaque fois qu'un événement lié à la sécurité de votre système ou de vos données se produit, un nouveau message apparaît dans la zone des notifications Bitdefender. Pour en savoir plus, reportez-vous à [Notifications \(page 28\)](#).
- Nous vous recommandons également d'adopter les pratiques suivantes :
 - Prenez l'habitude d'analyser les fichiers que vous téléchargez à partir d'un support de stockage externe (comme une clé USB ou un CD), en particulier lorsque vous ne connaissez pas la source.
 - Si vous avez un fichier DMG, montez-le puis analysez son contenu (les fichiers du volume/de l'image monté(e)).

Pour analyser un fichier, un dossier ou un volume, la méthode la plus simple consiste à le glisser-déposer sur la fenêtre de Bitdefender Antivirus for Mac ou sur l'icône du Dock.

Aucune autre configuration ou action n'est requise. Cependant, si vous le souhaitez, vous pouvez ajuster les paramètres de l'application et les préférences en fonction de vos besoins. Pour plus d'informations, reportez-vous à [Configuration des Préférences \(page 37\)](#).

4.2. Analyse de Votre Mac

En plus de la fonctionnalité **Bitdefender Shield**, qui surveille régulièrement les applications installées à la recherche d'actions ressemblant à celles de menaces et empêche que de nouvelles menaces n'atteignent votre système, vous pouvez analyser votre Mac ou des fichiers spécifiques à tout moment.

Pour analyser un fichier, un dossier ou un volume, la méthode la plus simple consiste à le glisser-déposer sur la fenêtre de Bitdefender Antivirus for Mac ou sur l'icône du Dock. L'assistant d'analyse apparaîtra et vous guidera tout au long du processus d'analyse.

Vous pouvez également lancer une analyse comme suit :

1. Cliquez sur **Protection** dans le menu de navigation de l'interface Bitdefender.
2. Sélectionnez l'onglet **Antivirus**.



3. Cliquez sur l'un des trois boutons d'analyse pour lancer l'analyse souhaitée.

- **Quick Scan (Analyse rapide)** - recherche des menaces aux emplacements les plus vulnérables de votre système (par exemple, dans les dossiers contenant les documents, les téléchargements, les téléchargements de messagerie et les fichiers temporaires de chaque utilisateur).
- **Analyse du système** - effectue une analyse complète des menaces sur l'ensemble du système. Tous les volumes montés connectés seront également analysés.



Note

En fonction de la taille de votre disque dur, l'analyse de l'ensemble du système peut être longue (une heure ou plus). Pour de meilleures performances, nous vous recommandons de ne pas exécuter cette tâche lorsque vous effectuez d'autres tâches consommant beaucoup de ressources (comme du montage vidéo).

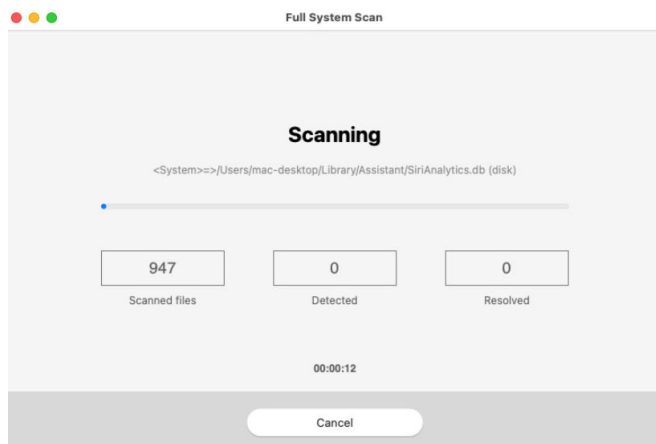
Vous pouvez, si vous le souhaitez, choisir de ne pas analyser certains volumes montés en les ajoutant à la liste d'**Exceptions** de la fenêtre Protection.

- **Custom Scan (Analyser un emplacement spécifique)** - vous aide à rechercher des menaces dans certains fichiers, dossiers ou volumes.

Vous pouvez également lancer une analyse rapide ou une analyse du système depuis le tableau de bord.

4.3. Assistant d'analyse

Lorsque vous lancez une analyse, l'assistant d'analyse Bitdefender Antivirus for Mac apparaît.



Des informations en temps réel sur les menaces détectées et résolues sont affichées pendant chaque analyse.

Patientez jusqu'à ce que Bitdefender Antivirus for Mac ait terminé l'analyse.

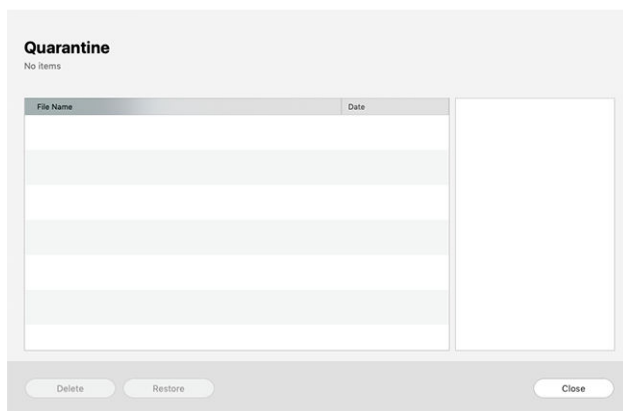


Note

L'analyse peut durer un certain temps, selon sa complexité.

4.4. Mise en quarantaine

Bitdefender Antivirus for Mac permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée appelée quarantaine. Quand une menace est en quarantaine, elle ne peut faire aucun dégât car elle ne peut ni être exécutée, ni être lue.



La partie Quarantaine affiche tous les fichiers actuellement isolés dans le dossier Quarantaine.

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

Pour consulter la liste de tous les éléments ajoutés en quarantaine :

1. Cliquez sur **protection** dans le menu de navigation de l'interface Bitdefender.
2. Cliquez sur **Ouvrir** dans le volet **Quarantaine**.

4.5. Bitdefender Shield (protection en temps réel)

Bitdefender assure la protection en temps réel contre un vaste éventail de menaces en analysant les applications installées, leurs mises à jour, ainsi que les nouveaux fichiers et les fichiers modifiés.

Pour désactiver la protection en temps réel :

1. Cliquez sur **Préférences** dans le menu de navigation de l'interface de Bitdefender.
2. Désactivez **Bitdefender Shield** dans la fenêtre **Protection**.



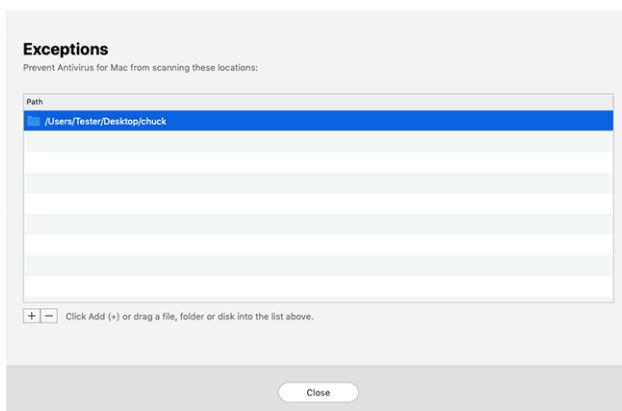
Avertissement

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

4.6. Exceptions d'analyse

Si vous le souhaitez, vous pouvez configurer Bitdefender Antivirus for Mac afin qu'il n'analyse pas certains fichiers, dossiers, ou même, un volume entier. Vous pouvez par exemple souhaiter exclure de l'analyse :

- ☐ Les fichiers identifiés à tort comme étant infectés (connus comme étant de faux positifs)
- ☐ Les fichiers provoquant des erreurs d'analyse
- ☐ Les volumes de sauvegarde



La liste des exceptions contient les chemins ayant été exclus de l'analyse.

Pour accéder à la liste des exceptions :

1. Cliquez sur **protection** dans le menu de navigation de l'interface Bitdefender.
2. Cliquez sur **Ouvrir** dans le volet **Exceptions**.

Il y a deux manières de définir une exception d'analyse :



- Glissez-déposez un fichier, un dossier ou un volume dans la liste des exceptions.
- Cliquez sur le bouton avec le signe plus (+), situé sous la liste des exceptions. Sélectionnez ensuite le fichier, le dossier ou le volume à exclure de l'analyse.

Pour supprimer une exception d'analyse, sélectionnez-la dans la liste et cliquez sur le bouton avec le signe moins (-) situé sous la liste des exceptions.

4.7. Protection Web

Bitdefender Antivirus for Mac utilise les extensions TrafficLight pour protéger complètement votre expérience de navigation sur Internet. Les extensions TrafficLight interceptent, traitent et filtrent l'ensemble du trafic web, bloquant tout contenu malveillant.


Les extensions fonctionnent avec et s'intègrent aux navigateurs web suivants : Mozilla Firefox, Google Chrome et Safari.

4.7.1. Activer les extensions Linkchecker

Pour activer les extensions TrafficLight :

1. Cliquez sur **Corriger** sur la carte **Protection web** du tableau de bord.
2. La fenêtre **Protection web** apparaît.
Le navigateur web que vous avez installé sur votre système apparaît. Pour installer l'extension Linkchecker dans votre navigateur, cliquez sur **Obtenir l'extension**.
3. Vous êtes redirigé vers :
<https://bitdefender.fr/solutions/trafficlight.html>
4. Sélectionnez **Téléchargement gratuit**.
5. Suivez ces étapes pour installer l'extension TrafficLight correspondant à votre navigateur web.

4.7.2. Gérer les paramètres des extensions

Un vaste ensemble de fonctionnalités est disponible pour vous protéger contre toute sortes de menaces présentes sur Internet . Pour y accéder, cliquez sur l'icône de TrafficLight située à côté des paramètres de votre navigateur, puis sur le bouton  **Paramètres** :




○ Paramètres de BitDefender TrafficLight

- Web Protection - vous empêche d'accéder aux sites web utilisés pour perpétrer des attaques par malware, hameçonnage ou fraude.
- Search Advisor - informe de la présence de sites Web à risque dans les résultats de recherche.

○ Exceptions


Si vous êtes sur le site web que vous voulez ajouter aux exceptions, cliquez sur **Ajouter le site web actuel à la liste**.


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


Vous ne serez pas averti si des menaces sont présentes sur les pages exclues. Ainsi, nous vous recommandons de n'ajouter à cette liste que les sites web et les applications en lesquels vous avez pleinement confiance.

4.7.3. Page des notes et alertes

En fonction de la façon dont Linkchecker classifie la page web que vous affichez, une des icônes suivantes s'affiche dans cette zone :

 Cette page ne présente pas de risque. Vous pouvez poursuivre votre navigation.

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

 Cette page contient un malware ou d'autres menaces, nous vous conseillons de la quitter immédiatement.

Sur Safari, le fond des icônes de TrafficLight est noir.

4.8. Bloqueur de traceurs

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



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

Cette extension de Bitdefender est compatible avec les navigateurs suivants :

- Google Chrome
- Mozilla Firefox
- Safari

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


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

4.8.1. Activation du Bloqueur de traceurs Bitdefender

Pour activer cette extension sur votre navigateur :

1. Cliquez sur **Vie privée** dans le menu de navigation de l'interface de Bitdefender.
2. Sélectionnez l'onglet **Bloqueur de traceurs**.
3. Cliquez sur **Activer l'extension** à côté du navigateur sur lequel vous voulez activer l'extension.

4.8.2. Interface du Bloqueur de traceurs

Lorsque l'extension Bloqueur de traceurs est activée, l'icône  apparaît à côté de la barre de recherche de votre navigateur. À chaque fois que vous





visitez un site, un chiffre s'affiche sur cette icône. Il indique le nombre de traceurs détectés et bloqués. Si vous souhaitez en savoir plus sur les traceurs bloqués, cliquez sur l'icône pour ouvrir l'interface. Vous y verrez le nombre de traceurs bloqués, mais aussi le temps nécessaire au chargement de la page et les catégories auxquelles appartiennent les traceurs détectés. Pour voir la liste des sites qui lancent ces traceurs, cliquez sur chaque catégorie.

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

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




4.8.3. Désactivation du Bloqueur de traceurs Bitdefender

Pour désactiver le Bloqueur de traceurs Bitdefender sur votre navigateur :

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

4.8.4. Autoriser le tracking d'un site web

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

1. Ouvrez votre navigateur Web.
2. Cliquez sur l'icône  qui se trouve à côté de la barre de recherche.
3. Cliquez le  icône dans le coin supérieur droit.
4. Si vous êtes sur le site Web que vous souhaitez ajouter aux exceptions, cliquez sur **Ajouter le site Web actuel à la liste**.
Si vous souhaitez ajouter un autre site Web, saisissez son adresse dans le champ correspondant, puis cliquez sur .



4.9. Safe Files

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

Grâce à ses technologies de pointe, Bitdefender veille à l'intégrité du système en protégeant les zones critiques contre les attaques par ransomware, sans répercussions sur le fonctionnement du système. Vous pouvez également souhaiter qu'aucune application suspecte n'accède à vos fichiers personnels (documents, photos ou vidéos). Avec Bitdefender Safe Files, vous pouvez mettre vos fichiers personnels à l'abri et sélectionner les applications autorisées à les modifier.

Pour ajouter dans un second temps des fichiers à l'environnement protégé :

1. Cliquez sur **protection** dans le menu de navigation de l'interface Bitdefender.
2. Sélectionnez l'onglet **Anti-Ransomware**.
3. Cliquez sur **Fichiers protégés** dans l'espace Safe Files.
4. Cliquez sur le bouton avec le signe plus (+), situé sous la liste des fichiers protégés. Choisissez ensuite le fichier, le dossier ou le volume à protéger en cas d'attaque de ransomware.

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

Par défaut, les dossiers Images, Documents, Bureau et Téléchargement sont protégés des menaces.



Note

Les dossiers personnalisés ne peuvent être protégés que pour les utilisateurs actuels. Les disques externes ainsi que les fichiers du système et des applications ne peuvent pas être ajoutés à l'environnement de protection.

Vous recevrez une notification à chaque fois qu'une application inconnue avec un comportement inhabituel essaiera de modifier les fichiers que



vous avez ajoutés. Cliquez sur **Autoriser** ou **Bloquer** pour l'ajouter à la liste des **Applications gérées**.

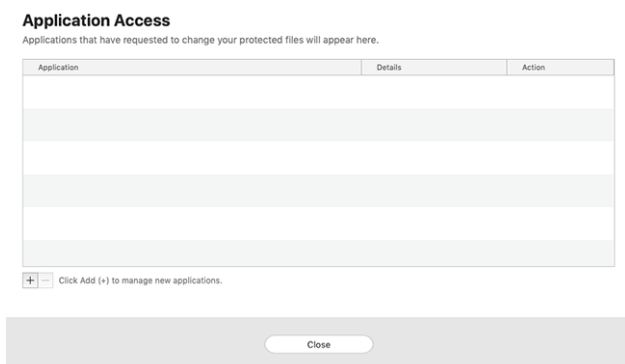
4.9.1. Accès des applications

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

1. Cliquez sur **protection** dans le menu de navigation de l'interface Bitdefender.
2. Sélectionnez le **Anti-ransomware** languette.
3. Cliquez sur **Accès de l'application** dans l'espace Safe Files.
4. Passez l'état de l'application bloquée sur Autoriser.

Les applications autorisées peuvent également être bloquées.

Ajoutez plus d'applications à la liste par glisser-déplacer ou en cliquant sur le signe plus (+).



4.10. Protection Time Machine

Bitdefender Time Machine Protection constitue une couche de sécurité supplémentaire pour votre disque dur externe, y compris tous les fichiers que vous avez décidé d'y stocker, en bloquant l'accès de toute source externe. Si un jour les fichiers de votre lecteur Time Machine sont chiffrés



par un ransomware, vous pourrez les récupérer sans payer la rançon demandée.

Si vous devez restaurer des éléments depuis une sauvegarde Time Machine, veuillez consulter le support Apple pour obtenir des instructions.

4.10.1. Activer ou désactiver Protection Time Machine

Pour activer ou désactiver la Protection Time Machine :

1. Cliquez sur **Protection** dans le menu de navigation de l'**interface Bitdefender**.
2. Sélectionnez le **Anti-ransomware** languette.
3. Activez ou désactivez le bouton **Protection Time Machine**.

4.11. Correction des problèmes

Bitdefender Antivirus for Mac détecte automatiquement un ensemble de problèmes pouvant affecter la sécurité de votre système et de vos données et vous informe à leur sujet. Vous pouvez donc corriger les risques de sécurité facilement et rapidement.

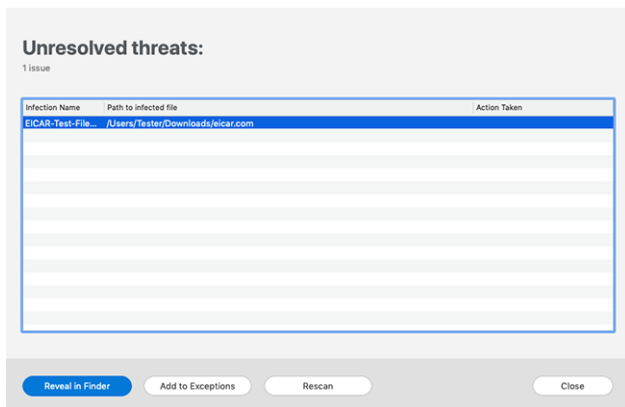
Corriger les problèmes signalés par Bitdefender Antivirus for Mac est une façon simple et rapide d'assurer une protection optimale des données de votre système.

Les problèmes détectés comprennent :

- La mise à jour des informations sur les menaces n'a pas été téléchargée sur nos serveurs.
- Des menaces ont été détectées sur votre système et le produit ne peut pas automatiquement les désinfecter.
- La protection en temps réel est désactivée.

Pour consulter et corriger les problèmes détectés :

1. Si Bitdefender n'émet pas d'avertissement, la barre d'état est verte. Lorsqu'un problème de sécurité est détecté, la barre d'état change de couleur pour passer au rouge.
2. Consultez la description pour plus d'informations.
3. Quand un problème est détecté, cliquez sur le bouton adapté pour prendre une mesure.



La liste des menaces non résolues est mise à jour après chaque analyse du système, qu'elle soit réalisée automatiquement en tâche de fond ou à votre demande.

Vous pouvez choisir d'appliquer les actions suivantes aux menaces non résolues :

- ☐ **Suppression manuelle.** Choisissez cette option pour supprimer les infections manuellement.
- ☐ **Ajout aux exceptions.** Cette option n'est pas proposée pour les menaces qui sont détectées dans les archives.

4.12. Notifications

Bitdefender tient un journal détaillé des événements concernant son activité sur votre ordinateur. Lorsqu'un événement concernant la sécurité de votre système ou de vos données ce produit, un nouveau message apparaît dans la zone des notifications Bitdefender, comme lorsqu'un nouveau message arrive dans votre boîte de réception.

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



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

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

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

Cliquez sur chaque onglet pour obtenir plus de détails sur les événements générés. De brefs détails sont affichés en un clic sur chaque titre d'événement, à savoir : une courte description, l'action effectuée par Bitdefender lorsqu'il s'est produit, et la date et l'heure 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 section.

4.13. Mises à jour

De nouvelles menaces sont détectées et identifiées tous les jours et il est donc important de veiller à ce que Bitdefender Antivirus for Mac soit à jour et bénéficie des dernières informations en matière de menaces.

Les mises à jour des informations sur les menaces sont exécutées à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, la mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

- Si Bitdefender Antivirus for Mac est à jour, il peut détecter les dernières menaces et nettoyer les fichiers infectés.
- Si Bitdefender Antivirus for Mac n'est pas à jour, les dernières menaces découvertes par les Bitdefender Labs ne pourront pas être détectées et supprimées.



4.13.1. Demandes de mise à jour

Vous pouvez demander une mise à jour manuellement à tout moment.

Une connexion Internet active est nécessaire afin de rechercher les mises à jour disponibles et de les télécharger.

Comment lancer une mise à jour manuellement :

1. Cliquez sur le bouton **Actions** dans la barre de menus.
2. Choisissez **Mettre à jour la base de données d'information sur les menaces**.

Alternativement, vous pouvez demander une mise à jour manuellement en appuyant sur CMD + U.

Vous pouvez voir la progression de la mise à jour et les fichiers téléchargés.

4.13.2. Obtenir des Mises à jour via un Serveur Proxy

Bitdefender Antivirus for Mac peut se mettre à jour uniquement via des serveurs proxy ne requérant pas d'authentification. Vous n'avez à configurer aucun paramètre du programme.

Si vous vous connectez à Internet via un serveur proxy exigeant une authentification, vous devez passer à une connexion Internet directe régulièrement afin d'obtenir les mises à jour des informations sur les menaces.

4.13.3. Mise à niveau vers une nouvelle version

De façon occasionnelle, nous publions des mises à jour de produits pour ajouter de nouvelles fonctionnalités ou améliorations ou encore réparer des problèmes liés au produit. Ces mises à jour peuvent nécessiter un redémarrage du système pour lancer l'installation de nouveaux fichiers. Par défaut, si une mise à jour nécessite un redémarrage de l'ordinateur, Bitdefender Antivirus for Mac continuera à fonctionner avec les anciens fichiers jusqu'au redémarrage du système. Dans ce cas, le processus de mise à jour n'interférera pas avec le travail de l'utilisateur.

Lorsqu'une mise à jour du produit est terminée, une fenêtre contextuelle vous demande de redémarrer le système. Si vous ratez cette notification, vous pouvez cliquer sur **Redémarrer pour mettre à niveau** dans la barre de menus ou redémarrer manuellement le système.



4.13.4. Trouver des informations sur votre version de Bitdefender Antivirus for Mac

Pour connaître la version de Bitdefender Antivirus for Mac que vous utilisez, consultez la fenêtre **A propos**. Depuis cette même fenêtre, vous pouvez consulter les Conditions d'utilisation de l'abonnement, la Politique de confidentialité et les licences open-sources.

Pour ouvrir la fenêtre A propos :

1. Ouvrez Bitdefender Antivirus for Mac.
2. Cliquez sur Bitdefender Antivirus for Mac dans la barre de menus et sélectionnez **À propos d'Antivirus for Mac**.



5. VPN

Ce chapitre comprend les rubriques suivantes :

- À propos du VPN (page 32)
- Ouvrir l'application VPN (page 32)
- Interface (page 33)
- Abonnements (page 35)

5.1. À propos du VPN

Avec le VPN Bitdefender vous pouvez assurer la confidentialité de vos données lorsque vous vous connectez à des réseaux sans-fil non sécurisés dans les aéroports, les commerces, les cafés ou les hôtels. Vous pouvez de cette manière éviter le vol de données personnelles ou les tentatives d'accès des pirates à l'adresse IP de votre appareil.

L'application VPN peut être installée depuis votre produit Bitdefender et utilisée à chaque fois que vous souhaitez ajouter une couche de protection supplémentaire à votre connexion. Le VPN forme un tunnel entre votre appareil et le réseau sur lequel vous vous connectez pour sécuriser votre connexion en chiffrant vos données à l'aide d'algorithmes de pointe et en masquant votre adresse IP, où que vous soyez. Votre trafic est intégralement redirigé à travers un serveur distinct. Votre appareil est donc presque impossible à identifier parmi les milliers d'autres qui utilisent nos services. Par ailleurs, si vous vous connectez à Internet avec Bitdefender VPN, vous pouvez contourner les restrictions géographiques pour accéder à tous les contenus que vous souhaitez.




Note

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

5.2. Ouvrir l'application VPN

Il existe trois manières d'ouvrir l'application Bitdefender VPN :



- Cliquez sur **Vie privée** dans le menu de navigation de l'**interface de Bitdefender**.
Cliquez sur **Ouvrir** dans la fenêtre Bitdefender VPN.
- Cliquez sur l'icône  dans la barre de menus.
- Allez dans le dossier Applications, ouvrez le dossier Bitdefender, puis double-cliquez sur l'icône Bitdefender VPN.

La première fois que vous ouvrez l'application, il vous est demandé d'autoriser Bitdefender à ajouter des configurations. En autorisant Bitdefender à ajouter des configurations, vous acceptez que toutes les activités réseau de votre appareil soient filtrées ou surveillées lorsque vous utilisez l'application VPN.



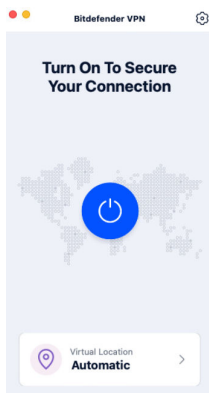
Note

L'application Bitdefender VPN peut uniquement être installée sur macOS Sierra (10.12.6), macOS High Sierra (10.13.6), macOS Mojave (10.14) ou une version plus récente du système d'exploitation.

5.3. Interface

L'interface du VPN affiche l'état de l'application, connectée ou déconnectée. Pour les utilisateurs de la version gratuite, l'emplacement du serveur le plus approprié est automatiquement défini par Bitdefender, tandis que les utilisateurs de la version Premium peuvent changer l'emplacement du serveur en le sélectionnant dans la liste Emplacements virtuels. Pour en apprendre plus sur les abonnements VPN, rendez-vous sur [Abonnements \(page 35\)](#).

Pour vous connecter ou vous déconnecter, cliquez simplement sur l'état affiché en haut de l'écran. L'icône de la barre de menu est noire quand le VPN est connecté et blanche quand il est déconnecté.



La durée de connexion est affichée dans la partie inférieure de l'interface. Pour accéder à plus d'options, cliquez sur l'icône ⚙️ située dans la partie supérieure droite :

- **Mon compte** - affiche des informations sur votre compte Bitdefender et sur votre abonnement au VPN. Cliquez sur **Changer de compte** si vous voulez vous connecter avec un autre compte.
- **Paramètres** - vous pouvez personnaliser le produit en fonction de vos besoins :
 - **General**
 - Notifications - affiche les notifications du produit.
 - Exécution au démarrage - lance automatiquement Bitdefender VPN à l'ouverture de la session.
 - Rapport sur les produits - envoie des rapports anonymes sur les produits pour nous aider à en améliorer les performances et les capacités de protection.
 - **Paramètres avancés**
 - Kill Switch Internet - suspend temporairement tout le trafic Internet si la connexion VPN s'interrompt accidentellement.
 - Bloqueur de publicités et Bloqueur de traceurs - Bloquent les publicités et les traceurs pour vous offrir une expérience de navigation plus fluide et plus rapide.
 - Segmentation de tunnel - les sites Internet sélectionnés contourneront le VPN et accéderont directement à Internet.



Note

Cliquez sur **Gérer** puis sur **Ajouter un site** pour ajouter des pages web à cette liste.

- ☐ Connexion automatique - connecte automatiquement le VPN en cas de :
 - ☐ Connexion à un Wi-Fi public ou non sécurisé.
 - ☐ Démarrage d'une application de partage de fichiers en peer-to-peer.
- ☐ **Support** - vous redirige vers notre plateforme d'assistance sur laquelle vous trouverez des articles sur l'utilisation de Bitdefender VPN.
- ☐ **À propos** - affiche des informations sur la version installée.
- ☐ **Quitter** - ferme l'application.

5.4. Abonnements

Le VPN Bitdefender vous offre gratuitement 200 Mo de trafic par jour et par appareil afin de sécuriser vos connexions chaque fois que c'est nécessaire, et vous connecte automatiquement au meilleur serveur disponible.

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

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

L'abonnement à Bitdefender Premium VPN est indépendant de l'abonnement à Bitdefender Antivirus for Mac : cela signifie que vous pourrez l'utiliser pendant toute la durée de votre abonnement au VPN, quel que soit l'état de votre abonnement à la solution de sécurité. Dans le cas où votre abonnement à Bitdefender Premium VPN expirerait alors que votre abonnement à Bitdefender Antivirus for Mac est encore actif, vous seriez automatiquement rebasculé(e) sur la version gratuite du VPN.

Bitdefender VPN est un produit multiplateforme disponible dans les produits Bitdefender compatibles avec Windows, macOS, Android, et iOS. Avec un abonnement Premium, vous pourrez utiliser votre abonnement



sur tous les produits, si vous vous connectez avec le même compte Bitdefender.



6. CONFIGURATION DES PRÉFÉRENCES

Ce chapitre comprend les rubriques suivantes :

- [Accéder aux Préférences \(page 37\)](#)
- [Préférences Protection \(page 37\)](#)
- [Préférences avancées \(page 38\)](#)
- [Offres spéciales \(page 38\)](#)

6.1. Accéder aux Préférences

Pour ouvrir la fenêtre des Préférences de Bitdefender Antivirus for Mac :

- Choisissez une des possibilités suivantes :
 - Cliquez sur **Préférences** dans le menu de navigation de l'interface Bitdefender.
 - Cliquez sur Bitdefender Antivirus for Mac dans la barre de menu et sélectionnez **Préférences**.

6.2. Préférences Protection

La fenêtre des préférences en matière de protection vous permet de configurer l'approche générale de l'analyse. Vous pouvez configurer les actions appliquées aux fichiers infectés et suspects détectés et d'autres paramètres généraux.

- **Bitdefender Shield.** Bitdefender Shield fournit une protection en temps réel contre un grand nombre de menaces en analysant toutes les applications installées, leurs versions mises à jour et les fichiers nouveaux ou modifiés. Nous vous déconseillons de désactiver Bitdefender Shield, mais si c'est vraiment nécessaire, cette interruption doit être aussi courte que possible. Si Bitdefender Shield est désactivé, votre appareil ne sera plus protégé contre les menaces.
- **Analyser uniquement les fichiers nouveaux et modifiés.** Cochez cette case pour que Bitdefender Antivirus for Mac n'analyse que les fichiers n'ayant pas été analysés auparavant ou ayant été modifiés depuis leur dernière analyse.



Vous pouvez choisir de ne pas appliquer ce paramètre à l'analyse personnalisée et par glisser-déposer en décochant la case correspondante.

- ☐ **Ne pas analyser le contenu des sauvegardes.** Cochez cette case pour que les fichiers de sauvegarde soient exclus de l'analyse. Si les fichiers infectés sont ultérieurement restaurés, Bitdefender Antivirus for Mac les détectera automatiquement et agira en conséquence.

6.3. Préférences avancées

Vous pouvez sélectionner une mesure générale à prendre pour tous les problèmes et éléments suspects détectés pendant une analyse.

Action pour les éléments infectés

- ☐ **Essayer de désinfecter ou déplacer en quarantaine** - Si des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (supprimer le code malveillant) ou de les placer en quarantaine.
- ☐ **Ignorer** - Aucune action ne sera appliquée aux fichiers détectés.

Action pour les éléments suspects

- ☐ **Déplacer les fichiers en quarantaine** - Si des fichiers suspects sont détectés, Bitdefender les déplacera en quarantaine.
- ☐ **Ne pas agir** - Aucune action ne sera entreprise sur les fichiers détectés.

6.4. Offres spéciales

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

Pour activer ou désactiver les notifications sur les promotions :

1. Cliquez sur **Préférences** dans le menu de navigation de l'interface Bitdefender.
2. Sélectionnez l'onglet **Autres**.
3. Activez ou désactivez le bouton **Mes offres**.



Note

L'option **Mes offres** est activée par défaut.



7. 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 que vous êtes connectés, vous pouvez commencer à faire ce qui suit :

- Télécharger et installer Bitdefender sur les systèmes d'exploitation Windows, macOS, iOS et Android. Les produits disponibles au téléchargement sont :
 - Bitdefender Antivirus pour Mac
 - Gamme de produits Bitdefender pour Windows
 - 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.

7.1. 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 Antivirus for Mac :
 1. Cliquez sur le lien **Aller dans votre compte** de la partie inférieure droite de l'écran.
- 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.

7.2. Authentification à 2 facteurs

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


7.2.1. 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. Accédez à **Bitdefender Central**.



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 **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**.

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.

7.3. 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.

7.4. 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.



7.4.1. Ajouter un nouvel appareil

Si votre abonnement couvre plus d'un appareil, vous pouvez ajouter un nouvel appareil et y installer votre Bitdefender Antivirus for Mac, 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.

7.4.2. 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**.

7.4.3. 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.

7.5. 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.

7.6. Mes abonnements

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

7.6.1. 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).

7.6.2. 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.

7.6.3. 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.



7.7. 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.



8. QUESTIONS LES PLUS FRÉQUENTES

Comment puis-je essayer Bitdefender Antivirus pour Mac avant de faire une demande d'abonnement ?

Vous êtes un nouveau client de Bitdefender et vous souhaitez tester notre produit avant de l'acheter. La période d'essai est de 30 jours et vous pouvez continuer à utiliser le produit seulement si vous achetez un abonnement Bitdefender. Pour essayer Bitdefender Antivirus for Mac, vous devez :

1. Pour créer un compte Bitdefender, suivez ces étapes :
 - a. Aller à : <https://central.bitdefender.com>.
 - b. Tapez les informations requises dans les champs correspondants. Les informations fournies resteront confidentielles.
 - c. Pour continuer, vous devez accepter les Conditions d'utilisation. Lisez attentivement nos Conditions d'utilisation car elles contiennent les termes et conditions selon lesquels vous pouvez utiliser Bitdefender.
Vous pouvez également consulter notre Politique de confidentialité.
 - d. Cliquez sur **CRÉER UN COMPTE**.
2. Téléchargez Bitdefender Antivirus for Mac comme suit :
 - a. Sélectionnez le **Mes appareils** panneau, puis cliquez sur **INSTALLER LA PROTECTION**.
 - b. Choisissez l'une des deux options disponibles :
 - **Protégez cet appareil**
 - i. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
 - ii. Enregistrez le fichier d'installation.
 - **Protégez d'autres appareils**



- i. Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, cliquez sur le bouton correspondant.
- ii. Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**.
- iii. Saisissez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER UN COURRIEL**.
Notez que le lien de téléchargement généré n'est valable que pour les prochaines 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes étapes.
- iv. Sur l'appareil sur lequel vous souhaitez installer votre produit Bitdefender, vérifiez le compte de messagerie que vous avez saisi, puis cliquez sur le bouton de téléchargement correspondant.

c. Exécutez le produit Bitdefender que vous avez téléchargé.

J'ai un code d'activation. Comment puis-je l'ajouter à mon abonnement ?

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

Pour activer un abonnement à l'aide d'un code d'activation, procédez comme suit :

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

L'extension est désormais visible dans votre compte Bitdefender, et dans votre produit installé Bitdefender Antivirus for Mac, dans la partie en bas à droite de votre écran.

Le journal d'analyse indique qu'il reste des éléments non résolus. Comment les supprimer ?

Les éléments non résolus du journal d'analyse peuvent être :



- des archives dont l'accès est restreint (xar, rar, etc.)

Solution : Utilisez l'option **Faire apparaître dans Finder** pour localiser le fichier et le supprimer manuellement. Veillez à vider la corbeille.

- des messageries dont l'accès est restreint (Thunderbird, etc.)

Solution : Utilisez l'application pour supprimer l'entrée contenant le fichier infecté.

- Contenu des sauvegardes

Solution : activez l'option **Ne pas analyser le contenu des sauvegardes** dans les Préférences de protection ou **ajoutez aux exceptions** les fichiers détectés.

Si des fichiers éventuellement infectés étaient restaurés par la suite, Bitdefender Antivirus for Mac prendra automatiquement les mesures appropriées.



Note

Les fichiers ayant un accès restreint sont des fichiers que Bitdefender Antivirus for Mac peut ouvrir mais ne peut pas modifier.

Où puis-je voir les détails de l'activité du produit ?

Bitdefender tient un journal de toutes les actions importantes, des modifications d'état et d'autres messages critiques liés à son activité. Pour accéder à ces informations, cliquez sur **Notifications** dans le menu de navigation de l'interface Bitdefender.

Puis-je mettre à jour Bitdefender Antivirus for Mac via un serveur proxy ?

Bitdefender Antivirus for Mac ne peut se mettre à jour que via des serveurs proxy qui ne nécessitent pas d'authentification. Vous n'avez pas à configurer les paramètres du programme.

Si vous vous connectez à Internet via un serveur proxy nécessitant une authentification, vous devez passer régulièrement à une connexion Internet directe pour obtenir des mises à jour des informations sur les menaces.

Comment supprimer Bitdefender Antivirus for Mac ?

Pour supprimer Bitdefender Antivirus for Mac, suivez ces étapes :

1. Ouvrez une fenêtre **Finder** et allez dans le dossier Applications.
2. Dans le dossier Bitdefender, double-cliquez sur BitdefenderUninstaller.



3. Cliquez sur **Désinstaller** et attendez que le processus soit terminé.
4. Cliquez sur **Fermer** pour finir.



Important

En cas d'erreur, vous pouvez contacter le service client de Bitdefender comme décrit dans [Demander de l'aide \(page 55\)](#).

Comment retirer les extensions TrafficLight de mon navigateur web ?

- Pour retirer les extensions TrafficLight de Mozilla Firefox, procédez comme suit :
 1. Allez dans **Outils** et sélectionnez **Modules complémentaires**.
 2. Sélectionnez **Extensions** dans la colonne de gauche.
 3. Sélectionnez l'extension et cliquez sur **Supprimer**.
 4. Redémarrez le navigateur pour que le processus de désinstallation se termine.
- Pour retirer les extensions TrafficLight de Google Chrome, procédez comme suit :
 1. En haut à droite, cliquez sur **Plus** ⋮.
 2. Allez dans **Autres outils** et sélectionnez **Extensions**.
 3. Cliquez sur l'icône **Supprimer** 🗑️ à côté de l'extension que vous voulez supprimer.
 4. Cliquez sur **Supprimer** pour confirmer la suppression.
- Pour désinstaller Bitdefender TrafficLight à partir de Safari, procédez comme suit :
 1. Allez dans **Préférences** ou appuyez simultanément sur **Commande et Virgule(,)**.
 2. Sélectionnez **Extensions**.
Une liste des extensions installées apparaît.
 3. Sélectionnez l'extension Bitdefender TrafficLight puis cliquez sur **Désinstaller**.
 4. Cliquez de nouveau sur **Désinstaller** pour confirmer le processus de désinstallation.



Quand dois-je utiliser le VPN Bitdefender ?

Vous devez être prudent lorsque vous accédez à des contenus, ou téléchargez/envoyez des données sur internet. Pour être certain de naviguer sur le web en toute sécurité, nous vous recommandons d'utiliser le VPN Bitdefender lorsque vous voulez :

- ☐ vous connecter à des réseaux sans-fil publics
- ☐ accéder à des contenus normalement disponibles uniquement depuis certaines régions, que vous soyez ou non chez vous
- ☐ assurer la confidentialité de vos données personnelles (identifiants, mots de passe, informations bancaires, etc.)
- ☐ masquer votre adresse IP

Le VPN Bitdefender aura-t-il une incidence négative sur l'autonomie de mon appareil ?

Le VPN Bitdefender a été conçu pour protéger vos données personnelles, masquer votre adresse IP quand vous êtes connecté à des réseaux sans-fil non sécurisés, et accéder à des contenus normalement indisponibles dans votre pays. Pour éviter d'utiliser pour rien la batterie de votre appareil, nous vous recommandons d'utiliser uniquement le VPN quand vous en avez besoin, et de le déconnecter quand vous êtes hors ligne.

Pourquoi ma connexion à Internet ralentit-elle parfois lorsque je suis connecté(e) au VPN Bitdefender ?

Bitdefender VPN a été pensé pour ne pas déranger votre navigation sur le web, mais votre connectivité à Internet ou la distance par rapport au serveur auquel vous êtes connecté peuvent provoquer des ralentissements. Dans ce cas, si vous n'êtes pas obligé d'être connecté à un serveur lointain (p.ex. en Chine) nous vous recommandons d'autoriser le VPN Bitdefender à se connecter automatiquement au serveur le plus proche, ou de trouver un serveur plus proche de là où vous vous situez.



9. OBTENIR DE L'AIDE

9.1. 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.

9.2. 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.

9.2.1. 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/>.

9.2.2. 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>

9.2.3. 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>.



9.3. 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/>

9.3.1. 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 essaient 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 ransoms 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 trousseaux administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des trousseaux 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 trousseaux 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 Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

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.