

Bitdefender®
**TOTAL
SECURITY
2017**



MANUEL D'UTILISATION



Bitdefender Total Security 2017 Manuel d'utilisation

Date de publication 21/09/2016

Copyright© 2016 Bitdefender

Mentions légales

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduite ou transmise, sous aucune forme et d'aucune façon, électronique ou physique, y compris photocopies, enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de Bitdefender. Il est permis d'inclure de courtes citations dans la rédaction de textes sur le produit, à condition d'en mentionner la source. Le contenu ne peut en aucun cas être modifié.

Avertissement. Ce produit et ses textes sont protégés par copyright. Les informations contenues dans ce document sont données « à titre indicatif », sans garantie. Bien que toutes les précautions aient été prises lors de l'élaboration de ce document, ses auteurs ne sauraient être tenus pour responsables envers toute personne ou entité, des pertes ou dommages directs ou indirects consécutifs à l'utilisation des informations qu'il contient.

Ce manuel contient des liens vers des sites Web tiers qui ne sont pas sous le contrôle de Bitdefender, et Bitdefender n'est pas responsable du contenu de ces sites. Si vous accédez à l'un des sites web d'une tierce partie fourni dans ce document, vous le ferez à vos propres risques. Bitdefender indique ces liens uniquement à titre informatif, et l'inclusion d'un lien n'implique pas que Bitdefender assume ou accepte la responsabilité du contenu de ce site Web.

Marques commerciales. Des noms de marques peuvent apparaître dans ce manuel. Toutes les marques, enregistrées ou non, citées dans ce document, sont la propriété exclusive de leurs propriétaires respectifs.



Table des matières

Installation	1
1. Préparation de l'installation	2
2. Configuration requise	3
2.1. Configuration système minimale	3
2.2. Configuration système recommandée	3
2.3. Configuration logicielle requise	4
3. Installer Bitdefender	5
3.1. Installation depuis Bitdefender Central	5
3.2. Installer à partir du disque d'installation	8
Commencer	14
4. Fonctions de base	15
4.1. Ouverture de la fenêtre de Bitdefender	16
4.2. Correction des problèmes	16
4.2.1. Assistant de Problèmes de Sécurité	17
4.2.2. Configurer les alertes d'état	18
4.3. Notifications	19
4.4. Autopilot	20
4.5. Profils	20
4.5.1. Configurer l'activation automatique des profils	21
4.6. Paramètres de Bitdefender de la protection par mot de passe	22
4.7. Rapports d'utilisation anonymes	23
4.8. Offres spéciales et notifications du produit	23
5. Interface de Bitdefender	24
5.1. Icône de la zone de notification	24
5.2. Fenêtre principale	26
5.2.1. Zone d'état	26
5.2.2. Barre gauche	27
5.2.3. Actionnez les boutons et accédez à la zone des modules	28
5.3. Les rubriques Bitdefender	29
5.3.1. Protection	29
5.3.2. Vie privée	31
5.3.3. Outils	33
5.4. Widget de sécurité	33
5.4.1. Analyse des fichiers et des dossiers	35
5.4.2. Masquer / afficher le Widget Windows	35
5.5. Activité	36
5.5.1. Consulter le rapport de sécurité	38
5.5.2. Activer ou désactiver la notification Rapport de Sécurité	39
6. Bitdefender Central	40
6.1. Accéder à Bitdefender Central	40
6.2. Mes abonnements	41



6.2.1. Vérifier les abonnements disponibles	41
6.2.2. nouvel appareil	41
6.2.3. Renouveler abonnement	42
6.2.4. Activer abonnement	42
6.3. Mes appareils	43
7. Maintenir Bitdefender à jour	46
7.1. Vérifier que Bitdefender est à jour	46
7.2. Mise à jour en cours	47
7.3. Activer ou désactiver la mise à jour automatique	48
7.4. Réglage des paramètres de mise à jour	48

Comment faire pour 50

8. Installation	51
8.1. Comment installer Bitdefender sur un deuxième ordinateur ?	51
8.2. Quand devrais-je réinstaller Bitdefender ?	51
8.3. Où est-ce que je peux télécharger mon produit Bitdefender ?	52
8.4. Comment changer la langue de mon produit Bitdefender ?	52
8.5. Comment utiliser mon abonnement Bitdefender après une mise à niveau Windows ?	55
8.6. Comment réparer Bitdefender ?	58
9. Licence(s)	60
9.1. Comment activer l'abonnement Bitdefender à l'aide d'une clé de licence ?	60
10. Bitdefender Central	62
10.1. Comment me connecter à Bitdefender Central à l'aide d'un autre compte en ligne ?	62
10.2. Comment désactiver les messages d'aide Bitdefender Central ?	62
10.3. Comment faire pour ne plus voir les photos prises avec mes appareils ?	63
10.4. J'ai oublié le mot de passe que j'avais configuré pour mon compte Bitdefender. Comment le reconfigurer ?	63
10.5. Comment redéfinir le mot de passe du compte Bitdefender ?	64
10.6. Comment supprimer compte Bitdefender ?	64
11. Analyser avec Bitdefender	66
11.1. Comment analyser un fichier ou un dossier ?	66
11.2. Comment analyser mon système ?	66
11.3. Comment programmer une analyse ?	67
11.4. Comment créer une tâche d'analyse personnalisée ?	67
11.5. Comment exclure un dossier de l'analyse ?	68
11.6. Que faire lorsque Bitdefender a détecté un fichier sain comme infecté ?	69
11.7. Comment connaître les virus détectés par Bitdefender ?	70
12. Parental Advisor	72
12.1. Comment protéger mes enfants des menaces sur Internet ?	72
12.2. Comment empêcher mon enfant d'accéder à un site Web ?	73
12.3. Comment empêcher mon enfant de jouer à un jeu ?	73
12.4. Comment empêcher mon enfant d'être en contact avec des personnes malveillantes ?	74



12.5. Comment puis-je configurer une localisation aussi sécurisée ou limitée pour mon enfant ?	75
12.6. Comment supprimer un profil enfant	76
13. Protection de la vie privée	77
13.1. Comment vérifier que ma transaction en ligne est sécurisée ?	77
13.2. Que faire si mon périphérique a été volé ?	77
13.3. Comment utiliser les coffres-forts ?	78
13.4. Comment supprimer définitivement un fichier avec Bitdefender ?	80
14. Outils d'optimisation	81
14.1. Comment améliorer les performances de mon système ?	81
14.1.1. Optimisez les performances de votre système d'un simple clic	81
14.1.2. Analysez votre système régulièrement	81
14.2. Comment puis-je améliorer le temps de démarrage de mon système ?	82
15. Informations utiles	83
15.1. Comment tester ma solution antivirus ?	83
15.2. Comment désinstaller Bitdefender ?	83
15.3. Comment éteindre automatiquement l'ordinateur une fois l'analyse terminée ?	85
15.4. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?	86
15.5. Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?	87
15.6. Comment afficher des objets cachés dans Windows ?	88
15.7. Comment supprimer les autres solutions de sécurité ?	88
15.8. Comment redémarrer en mode sans échec ?	90

Gérer votre sécurité 92

16. Protection antivirus	93
16.1. Analyse à l'accès (protection en temps réel)	94
16.1.1. Activer ou désactiver la protection en temps réel	94
16.1.2. Régler le niveau de protection en temps réel	95
16.1.3. Configurer les paramètres de protection en temps réel	96
16.1.4. Restauration des paramètres par défaut	100
16.2. Analyse à la demande	100
16.2.1. Rechercher des logiciels malveillants dans un fichier ou un dossier ...	101
16.2.2. Exécuter une analyse rapide	101
16.2.3. Exécuter une analyse du système	102
16.2.4. Configurer une analyse personnalisée	103
16.2.5. Assistant d'analyse antivirus	106
16.2.6. Consulter les journaux d'analyse	109
16.3. Analyse automatique de supports amovibles	110
16.3.1. Comment cela fonctionne-t-il ?	110
16.3.2. Gérer l'analyse des supports amovibles	111
16.4. Analyse du fichier hosts	112
16.5. Configurer des exceptions d'analyse	112
16.5.1. Exclure des fichiers et des dossiers de l'Analyse	113
16.5.2. Exclure de l'analyse des extensions de fichiers	113
16.5.3. Gérer les exceptions d'analyse	114



16.6. Gérer les fichiers en quarantaine	115
16.7. Active Threat Control	116
16.7.1. Vérifier des applications détectées	117
16.7.2. Activer ou désactiver Active Threat Control	117
16.7.3. Régler la protection Active Threat Control	117
16.7.4. Gérer les processus exclus	118
17. Antispam	120
17.1. Aperçu de l'antispam	121
17.1.1. Filtres AntiSpam	121
17.1.2. Fonctionnement de l'Antispam	121
17.1.3. Clients et protocoles de messagerie pris en charge	122
17.2. Activer ou désactiver la protection antispam	122
17.3. Utilisation de la barre d'outils Antispam dans la fenêtre de votre client de messagerie	122
17.3.1. Indiquer des erreurs de détection	124
17.3.2. Indiquer les messages de spam non détectés	124
17.3.3. Configurer les paramètres de la barre d'outils	125
17.4. Configurer la liste d'amis	125
17.5. Configurer la liste des spammeurs	126
17.6. Configurer les filtres antispam locaux	128
17.7. Configurer les paramètres cloud	128
18. Protection Web	130
18.1. Alertes Bitdefender dans le navigateur	131
19. Protection des données	132
19.1. Supprimer définitivement des fichiers	132
20. Chiffrement de fichiers	134
20.1. Gérer des coffres-forts	134
20.2. Créer des coffres-forts	134
20.3. Ouverture de coffres-forts	135
20.4. Ajouter des fichiers aux coffres-forts	136
20.5. Verrouiller des coffres-forts	137
20.6. Supprimer des fichiers des coffres-forts	137
20.7. Changer le mot de passe du coffre-fort	138
21. Vulnérabilité	140
21.1. Analyser votre système à la recherche de vulnérabilités	140
21.2. Utiliser la surveillance des vulnérabilités automatique	142
21.3. Wi-fi Security Advisor	144
21.3.1. Activer ou désactiver les notifications Wifi Security Advisor	145
21.3.2. Configuration du réseau Wifi domestique	145
21.3.3. Wi-Fi Public	146
21.3.4. Vérifier les informations à propos des réseaux Wifi	146
22. Pare-feu	149
22.1. Activer ou désactiver la protection pare-feu	149
22.2. Gérer les règles de pare-feu	150
22.2.1. Règles générales	150
22.2.2. Règles d'applications	151



22.3. Gérer les paramètres de connexion	154
22.4. Configurer les paramètres avancés	156
22.5. Configurer l'intensité de l'alerte	156
23. Protection ransomware	158
23.1. Activer ou désactiver la protection contre les ransomwares	158
23.2. Protégez vos fichiers personnels contre les attaques de ransomwares	159
23.3. Configuration des applications fiables	159
23.4. Configuration des applications bloquées	160
23.5. Protection au démarrage	160
24. La sécurité SafePay pour les transactions en ligne	162
24.1. Utiliser Bitdefender Safepay™	163
24.2. Configurer les paramètres	164
24.3. Gérer les marque-pages	166
24.4. Protection zones d'accès sans fil pour les réseaux non sécurisés	166
25. Protection Password Manager de vos identifiants	168
25.1. Configurer Password Manager	169
25.2. Activer ou désactiver la protection du Password Manager	172
25.3. Gestion des configurations du Password Manager	172
26. Parental Advisor	177
26.1. Allez dans le Contrôle parental - Mes enfants	177
26.2. Ajouter le profil de votre enfant	178
26.2.1. Assigner le même profil à plusieurs appareils	179
26.2.2. Lier le Contrôle parental à Bitdefender Central	180
26.2.3. Surveiller les activités de l'enfant	180
26.2.4. Configurer les paramètres généraux	181
26.2.5. Modifier le profil	181
26.2.6. Supprimer le profil	182
26.3. Configurer les profils Contrôle parental	182
26.3.1. Tableau de bord	183
26.3.2. Activités	183
26.3.3. Intérêts	184
26.3.4. Amis	185
26.3.5. Lieux	185
26.3.6. Réseaux sociaux	186
27. Antivol de l'appareil	188
28. Protection USB	191
Optimisation du système	192
29. Outils	193
29.1. Optimisation de la vitesse de votre système d'un simple clic	193
29.2. Optimisation du temps de démarrage de votre PC	194
29.3. Optimisation de votre disque	195
30. Profils	198
30.1. Profil Travail	199



30.2. Profil Film	200
30.3. Profil Jeu	202
30.4. Profil Wifi public	203
30.5. Profil Mode batterie	204
30.6. Optimisation en temps réel	205

Résolution des problèmes 206

31. Résoudre les problèmes les plus fréquents	207
31.1. Mon système semble lent	207
31.2. L'analyse ne démarre pas	209
31.3. Je ne peux plus utiliser une application	212
31.4. Que faire lorsque Bitdefender bloque un site web ou une application en ligne sûre	214
31.5. Que faire si Bitdefender détecte une application fiable comme ransomware	214
31.6. Je ne peux pas me connecter à Internet	215
31.7. Je ne peux pas accéder à un périphérique de mon réseau	216
31.8. Mon Internet est lent	218
31.9. Comment mettre à jour Bitdefender avec une connexion Internet lente ?	220
31.10. Les Services Bitdefender ne répondent pas	220
31.11. Le filtre antispam ne fonctionne pas correctement	221
31.11.1. Des messages légitimes sont signalés comme étant du [spam]	221
31.11.2. De nombreux messages de spam ne sont pas détectés	224
31.11.3. Le filtre antispam ne détecte aucun message de spam.	225
31.12. La fonctionnalité saisie automatique de mon Wallet ne fonctionne pas	226
31.13. La désinstallation de Bitdefender a échoué	227
31.14. Mon système ne démarre pas après l'installation de Bitdefender	229
32. Suppression des malwares de votre système	234
32.1. Mode de Secours de Bitdefender	234
32.2. Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?	236
32.3. Comment nettoyer un virus dans une archive ?	238
32.4. Comment nettoyer un virus dans une archive de messagerie ?	239
32.5. Que faire si je suspecte un fichier d'être dangereux ?	240
32.6. Que sont les fichiers protégés par mot de passe du journal d'analyse ?	241
32.7. Que sont les éléments ignorés du journal d'analyse ?	241
32.8. Que sont les fichiers ultra-compressés du journal d'analyse ?	242
32.9. Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?	242

Contact 243

33. Assistance	244
33.1. Assistance téléphonique :	246
34. Ressources en ligne	248
34.1. Centre de Support de Bitdefender	248
34.2. Forum du Support Bitdefender	249
34.3. Portail Bitdefender blog	249
35. Pour nous joindre	250



35.1. Adresses Web	250
35.2. Distributeurs locaux	250
35.3. Bureaux de Bitdefender	251
Glossaire	253



INSTALLATION



1. PRÉPARATION DE L'INSTALLATION

Avant d'installer Bitdefender Total Security 2017, procédez comme suit pour faciliter l'installation :

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



2. CONFIGURATION REQUISE

Vous pouvez installer Bitdefender Total Security 2017 uniquement sur les ordinateurs fonctionnant avec les systèmes d'exploitation suivants :

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

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



Note

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

- Dans **Windows 7**, faites un clic droit sur **Poste de travail** sur le bureau, puis sélectionnez **Propriétés** dans le menu.
- Dans **Windows 8**, sur l'écran d'accueil Windows, localisez **Ordinateur** (vous pouvez, par exemple, taper « Ordinateur » directement sur l'écran d'accueil), puis faites un clic droit sur son icône. Dans **Windows 8.1**, localisez **Ce PC**. Sélectionnez **Propriétés** dans le menu inférieur. Regardez sous **Système** pour connaître le type de système.
- Dans **Windows 10**, tapez **Système** dans le champ de recherche de la barre des tâches cliquez sur son icône. Regardez sous **Système** pour connaître le type de système.

2.1. Configuration système minimale

- 1.5 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- Processeur 1,6 GHz
- 1 Go de mémoire (RAM)

2.2. Configuration système recommandée

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



2.3. Configuration logicielle requise

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

- Internet Explorer 10 ou version supérieure
- Mozilla Firefox 30 ou version supérieure
- Google Chrome version 34 ou supérieure
- Skype 6.3 ou version supérieure
- Microsoft Outlook 2007 / 2010 / 2013
- Mozilla Thunderbird 14 ou version supérieure



3. INSTALLER BITDEFENDER

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

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

3.1. Installation depuis Bitdefender Central

A partir de Bitdefender Central vous pouvez télécharger le kit d'installation correspondant à l'abonnement auquel vous avez souscrit. Une fois le processus d'installation terminé, Bitdefender Total Security 2017 est activé.

Pour télécharger Bitdefender Total Security 2017 depuis Bitdefender Central:

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
4. Sélectionnez l'une des deux actions disponibles :

- **TÉLÉCHARGER**

Cliquez sur le bouton pour sauvegarder le fichier d'installation.

- **Sur un autre appareil**

Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrez une adresse électronique dans le champ correspondant, puis cliquez sur **ENVOYER**.

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

Validation de l'installation

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

Si votre système ne dispose pas de la configuration minimale requise pour l'installation de Bitdefender, vous serez informé des zones devant être améliorées avant de pouvoir poursuivre.

Si un programme antivirus incompatible ou une version antérieure de Bitdefender est détecté, on vous demandera de le désinstaller de votre



système. Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite. Il est parfois nécessaire de redémarrer l'ordinateur pour terminer la désinstallation des programmes antivirus détectés.

Le paquet d'installation de Bitdefender Total Security 2017 est constamment mis à jour.



Note

Le téléchargement des fichiers d'installation peut être long, en particulier sur des connexions Internet plus lentes.

Une fois l'installation validée, l'assistant de configuration s'affiche. Suivez les étapes pour installer Bitdefender Total Security 2017.

Étape 1 - Installation de Bitdefender

L'écran d'installation de Bitdefender vous permet de choisir le type d'installation que vous souhaitez effectuer.

Pour une installation simplifiée, cliquez simplement sur le bouton **Installer**. Bitdefender sera installé dans l'emplacement par défaut avec les paramètres par défaut et vous passerez directement à l'**Étape 3** de l'assistant.

Si vous souhaitez configurer les paramètres d'installation, cliquez sur **INSTALLATION PERSONNALISÉE**.

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

- Veuillez lire l'Accord de licence de l'utilisateur final avant de procéder à l'installation. L'Accord de licence contient les conditions d'utilisation de Bitdefender Total Security 2017.

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

- Gardez l'option **Envoyer rapports anonymes** activée. Si vous activez cette option, les rapports contenant des informations sur votre utilisation du produit seront envoyés aux serveurs de Bitdefender. Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir la meilleure expérience possible. Veuillez noter que ces rapports ne comportent aucune donnée confidentielle, comme votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

- Sélectionnez la langue dans laquelle vous souhaitez installer le produit.



Étape 2 - Personnaliser les paramètres d'installation



Note

Cette étape apparaît uniquement si vous avez choisi de personnaliser l'installation lors de l'étape précédente.

Voici les options proposées :

Chemin d'installation

Par défaut, Bitdefender Total Security 2017 sera installé dans C:\Program Files\Bitdefender\Bitdefender 2017. Si vous souhaitez choisir un autre répertoire, cliquez sur **Modifier** et choisissez le répertoire d'installation de Bitdefender.

Configurer les paramètres du proxy

Bitdefender Total Security 2017 nécessite un accès à Internet pour l'activation du produit, le téléchargement de mises à jour du produit et de sécurité, les composants de détection "in the cloud", etc. Si vous utilisez une connexion via un proxy au lieu d'une connexion Internet directe, activez le bouton correspondant et configurez les paramètres du proxy.

Les paramètres peuvent être importés à partir du navigateur par défaut ou vous pouvez les indiquer manuellement.

Scan du PC pendant l'installation

Désactivez cette option si vous ne souhaitez pas que votre système soit analysé pendant l'installation du produit Bitdefender.

Cliquez sur **Installer** pour confirmer vos préférences et commencer l'installation. Si vous changez d'avis, cliquez sur le bouton **RETOUR**.

Étape 3 - Installation en cours

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

Les zones critiques de votre système font l'objet d'une analyse antivirus, les dernières versions des fichiers d'applications sont téléchargées et installées et les services de Bitdefender sont lancés. Cette étape peut prendre quelques minutes.



Étape 4 - Installation terminée

Votre produit Bitdefender a été installé avec succès.

Un résumé de l'installation s'affiche. Si des logiciels malveillants actifs ont été détectés et supprimés pendant l'installation, un redémarrage du système peut être nécessaire. Cliquez sur **COMMENCER À UTILISER Bitdefender** pour continuer.

Étape 5 - Formule d'abonnement

Dans la fenêtre **Formule d'abonnement**, vous pouvez accéder aux informations relatives à votre abonnement actif.

Cliquez sur **Terminer** pour accéder à l'interface de Bitdefender Total Security 2017.

3.2. Installer à partir du disque d'installation

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

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

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

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

Validation de l'installation

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

Si votre système ne dispose pas de la configuration minimale requise pour l'installation de Bitdefender, vous serez informé des zones devant être améliorées avant de pouvoir poursuivre.

Si un programme antivirus incompatible ou une version antérieure de Bitdefender est détecté, on vous demandera de le désinstaller de votre



système. Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite. Il est parfois nécessaire de redémarrer l'ordinateur pour terminer la désinstallation des programmes antivirus détectés.



Note

Le téléchargement des fichiers d'installation peut être long, en particulier sur des connexions Internet plus lentes.

Une fois l'installation validée, l'assistant de configuration s'affiche. Suivez les étapes pour installer Bitdefender Total Security 2017.

Étape 1 - Installation de Bitdefender

L'écran d'installation de Bitdefender vous permet de choisir le type d'installation que vous souhaitez effectuer.

Pour une installation simplifiée, cliquez simplement sur le bouton **Installer**. Bitdefender sera installé dans l'emplacement par défaut avec les paramètres par défaut et vous passerez directement à l'**Étape 3** de l'assistant.

Si vous souhaitez configurer les paramètres d'installation, cliquez sur **INSTALLATION PERSONNALISÉE**.

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

- Veuillez lire l'Accord de licence de l'utilisateur final avant de procéder à l'installation. L'Accord de licence contient les conditions d'utilisation de Bitdefender Total Security 2017.

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

- Gardez l'option **Envoyer rapports anonymes** activée. Si vous activez cette option, les rapports contenant des informations sur votre utilisation du produit seront envoyés aux serveurs de Bitdefender. Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir la meilleure expérience possible. Veuillez noter que ces rapports ne comportent aucune donnée confidentielle, comme votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.
- Sélectionnez la langue dans laquelle vous souhaitez installer le produit.



Étape 2 - Personnaliser les paramètres d'installation



Note

Cette étape apparaît uniquement si vous avez choisi de personnaliser l'installation lors de l'étape précédente.

Voici les options proposées :

Chemin d'installation

Par défaut, la Bitdefender Total Security 2017 sera installé dans C:\Program Files\Bitdefender\Bitdefender2017\. Si vous souhaitez choisir un autre répertoire, cliquez sur **Modifier** et choisissez le répertoire d'installation de Bitdefender.

Configurer les paramètres du proxy

Bitdefender Total Security 2017 nécessite un accès à Internet pour l'activation du produit, le téléchargement de mises à jour du produit et de sécurité, les composants de détection "in the cloud", etc. Si vous utilisez une connexion via un proxy au lieu d'une connexion Internet directe, activez le bouton correspondant et configurez les paramètres du proxy.

Les paramètres peuvent être importés à partir du navigateur par défaut ou vous pouvez les indiquer manuellement.

Scan du PC pendant l'installation

Désactivez cette option si vous ne souhaitez pas que votre système soit analysé pendant l'installation du produit Bitdefender.

Cliquez sur **Installer** pour confirmer vos préférences et commencer l'installation. Si vous changez d'avis, cliquez sur le bouton **RETOUR**.

Étape 3 - Installation en cours

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

Les zones critiques de votre système sont analysées et les services Bitdefender sont lancés. Cette étape peut prendre quelques minutes.

Étape 4 - Installation terminée

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



peut être nécessaire. Cliquez sur **COMMENCER À UTILISER Bitdefender** pour continuer.

Étape 5 - compte Bitdefender

Une fois que vous avez fini le paramétrage initial, la fenêtre compte Bitdefender apparaît. Un compte Bitdefender est nécessaire pour activer le produit et utiliser ses fonctionnalités en ligne. Pour plus d'informations, reportez-vous à « *Bitdefender Central* » (p. 40).

Procédez selon votre situation.

Je souhaite créer un compte Bitdefender

Saisissez les informations nécessaires dans les champs correspondants, puis cliquez sur **CRÉER COMPTE**.

Les informations fournies resteront confidentielles.

Le mot de passe doit contenir au moins 8 caractères et contenir un chiffre.

Veillez lire les Termes et conditions générales de Bitdefender avant de poursuivre.



Note

Une fois le compte créé, vous pouvez utiliser l'adresse courriel et le mot de passe indiqués pour vous connecter à votre compte sur <https://central.bitdefender.com>.

J'ai déjà un compte Bitdefender

Cliquez sur le lien **Se Connecter** puis tapez l'adresse e-mail et le mot de passe de votre compte Bitdefender.

Cliquez sur **Se connecter** pour poursuivre.

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



Note

Si vous possédez déjà un compte MyBitdefender, vous pouvez l'utiliser afin de vous connecter à votre compte Bitdefender. Si vous avez oublié



vosre mot de passe, cliquez tout d'abord sur le lien <https://my.bitdefender.com> afin de le réinitialiser. Ensuite, utilisez les nouveaux identifiants pour vous connecter à votre compte Bitdefender.

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

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

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



Note

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

Étape 6 - Activer votre produit



Note

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

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

Procédez selon votre situation :

● J'ai un code d'activation

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

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



Note

Pour trouver votre code d'activation :

- sur l'étiquette du CD ou DVD.
- sur le manuel du produit.
- sur le courriel de confirmation d'achat en ligne.



2. Je veux évaluer la Bitdefender

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

Étape 7 - Formule d'abonnement

Dans la fenêtre **Formule d'abonnement**, vous pouvez accéder aux informations relatives à votre abonnement actif.

Cliquez sur **Terminer** pour accéder à l'interface de Bitdefender Total Security 2017.



COMMENCER



4. FONCTIONS DE BASE

Une fois Bitdefender Total Security 2017 installé, votre ordinateur est protégé contre toutes sortes de logiciels malveillants (comme les virus, les logiciels espions et les chevaux de Troie) et les menaces Internet (comme les pirates, le hameçonnage et les pourriels).

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

Vous pouvez activer la fonction **Autopilot** pour bénéficier d'une protection complètement silencieuse. Vous n'aurez ainsi aucun paramètre à configurer. Cependant, vous pouvez souhaiter profiter des paramètres de Bitdefender pour ajuster et améliorer votre protection.

Lorsque votre appareil est connecté à un réseau sans fil non sécurisé, Bitdefender l'identifie et aide la protection à vous préserver de potentiels espions. Pour des instructions sur comment protéger vos données personnelles, veuillez vous référer à votre **Wi-Fi Security Advisor**.

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

Bitdefender prendra pour vous la plupart des décisions de sécurité et affichera rarement des alertes contextuelles. Des détails sur les actions prises et des informations sur le fonctionnement du programme sont disponibles dans la fenêtre Notifications. Pour plus d'informations, reportez-vous à « **Notifications** » (p. 19).

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

Pour utiliser les fonctionnalités en ligne de Bitdefender Total Security 2017 et gérer vos abonnements et appareils, accédez à votre compte Bitdefender. Pour plus d'informations, reportez-vous à « **Bitdefender Central** » (p. 40).



La section « **Comment faire pour** » (p. 50) vous fournit des instructions détaillées pour utiliser les fonctionnalités les plus courantes. Si vous rencontrez des problèmes lors de l'utilisation de Bitdefender, recherchez dans la section « **Résoudre les problèmes les plus fréquents** » (p. 207) des solutions possibles aux problèmes les plus courants.

4.1. Ouverture de la fenêtre de Bitdefender

Pour accéder à l'interface principale de Bitdefender Total Security 2017, suivez les étapes ci-dessous :

● Dans **Windows 7** :

1. Cliquez sur **Démarrer** et allez dans **Programmes**.
2. Cliquez sur **Bitdefender 2017**.
3. Cliquez sur **Bitdefender Total Security 2017** ou faites un double clic sur Bitdefender **B** dans la zone de notification.

● Dans **Windows 8 et Windows 8.1** :

Localisez Bitdefender Total Security 2017 dans l'écran d'accueil Windows (vous pouvez par exemple taper "Bitdefender" directement dans l'écran d'accueil) puis cliquez sur son icône. Vous pouvez également ouvrir le Bureau puis double-cliquer sur Bitdefender **B** de la zone de notification.

● Dans **Windows 10** :

Tapez "Bitdefender" dans le champ de recherche de la barre des tâches puis cliquez sur son icône. Vous pouvez également double-cliquer sur l'icône Bitdefender **B** dans la zone de notification.

Pour plus d'informations sur la fenêtre de Bitdefender et l'icône de la zone de notification, reportez-vous à « **Interface de Bitdefender** » (p. 24).

4.2. Correction des problèmes



Bitdefender utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous en informer. Par défaut, il surveille uniquement un ensemble de problèmes considérés comme très importants. Cependant, vous pouvez le configurer selon vos besoins en sélectionnant les problèmes spécifiques que vous souhaitez surveiller.



Les problèmes détectés comprennent la désactivation d'importants paramètres de protection et d'autres conditions pouvant constituer un risque pour la sécurité. Ils sont regroupés en deux catégories :

- **Problèmes critiques** - ils empêchent Bitdefender de vous protéger contre les malwares ou constituent un risque majeur pour la sécurité.
- **Problèmes mineurs (non critiques)** - ces problèmes pourraient éventuellement affecter votre protection.

L'icône de Bitdefender de la **zone de notification** signale les problèmes en attente en changeant de couleur comme suit :

-  Des problèmes critiques affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.
-  Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.

Si vous faites glisser le curseur de la souris sur l'icône, une fenêtre de notification confirmera la présence de problèmes en attente.

Lorsque vous ouvrez l'**interface de Bitdefender**, la zone d'état de Sécurité de la barre d'outils supérieure indique la nature des problèmes affectant votre système.

4.2.1. Assistant de Problèmes de Sécurité

Pour corriger les problèmes détectés, suivez l'assistant de **Problèmes de sécurité**.

1. Pour ouvrir l'assistant, procédez comme suit :

- Faites un clic droit sur l'icône de Bitdefender dans la **zone de notification** et sélectionnez **Voir les problèmes de sécurité**.
- Ouvrez l'**interface de Bitdefender** et cliquez à l'intérieur de la zone d'état de Sécurité de la barre d'outils supérieure.

2. Vous pouvez voir les problèmes affectant la sécurité de votre ordinateur et de vos données. Tous les problèmes présents sont sélectionnés pour être corrigés.

Si vous ne souhaitez pas corriger un problème spécifique immédiatement, décochez la case correspondante. On vous demandera de spécifier pendant combien de temps vous souhaitez reporter la correction du



problème. Sélectionnez l'option souhaitée dans le menu et cliquez sur **OK**. Pour cesser de surveiller cette catégorie de problème, sélectionnez **En permanence**.

L'état du problème deviendra **Reporté** et aucune action ne sera adoptée pour corriger le problème.

3. Pour corriger les problèmes sélectionnés, cliquez sur **Corriger**. Certains problèmes sont corrigés immédiatement. Pour d'autres, un assistant vous aide à les corriger.

Les problèmes que cet assistant vous aide à corriger peuvent être regroupés dans les catégories suivantes :


- **Paramètres de sécurité désactivés.** Ces problèmes sont corrigés immédiatement en activant les paramètres de sécurité correspondants.
- **Tâches de sécurité préventives devant être réalisées.** Un assistant vous aide à corriger ces problèmes.

4.2.2. Configurer les alertes d'état

Bitdefender peut vous avertir lorsque des problèmes sont détectés lors du fonctionnement des composants de programmes suivants :

- Antivirus
- Pare-feu
- Mettre à jour
- Sécurité du navigateur

Vous pouvez configurer le système d'alertes afin de répondre à vos besoins spécifiques en choisissant les problèmes à propos desquels vous souhaitez être informé. Suivez ces étapes :



1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Avancé**.
3. Cliquez sur le lien **Configurer les alertes d'état**.
4. Cliquez sur les boutons pour activer ou désactiver les alertes d'état en fonction de vos préférences.



4.3. Notifications

Bitdefender tient un journal détaillé des événements concernant son activité sur votre ordinateur. Lorsqu'un événement concernant la sécurité de votre système ou de vos données a lieu, un nouveau message est ajouté aux Événements de Bitdefender, comme lorsqu'un nouvel e-mail 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 qu'une mise à jour s'est effectuée correctement, s'il y a eu des logiciels malveillants ou des vulnérabilités détectés sur votre ordinateur, etc. Vous pouvez également adopter d'autres actions si nécessaire ou modifier les actions appliquées par Bitdefender.

Pour accéder au journal de Notifications, cliquez sur l'icône  dans la barre de gauche dans l'interface Bitdefender. Chaque fois qu'un événement critique se produit, un compteur apparaît dans l'icône .

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

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

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

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



4.4. Autopilot


Pour les utilisateurs qui souhaitent que leur solution de sécurité les protège sans les interrompre, Bitdefender Total Security 2017 dispose d'un mode Autopilote intégré.

En Autopilot, Bitdefender applique une configuration de sécurité optimale et prend pour vous toutes les décisions de sécurité. Cela signifie qu'aucune fenêtre contextuelle ni alerte ne s'affichera et que vous n'aurez aucun paramètre à configurer.

En mode Autopilote, Bitdefender corrige automatiquement les problèmes critiques, active et gère silencieusement :

- La protection antivirus, fournie par l'analyse à l'accès et l'analyse en continu.
- La protection pare-feu.
- Protection Web.
- Les mises à jour automatiques.

Pour activer ou désactiver **Autopilote**, cliquez sur le bouton dans la barre d'outils de **l'interface Bitdefender**.

Tant que l'Autopilote est activé, l'icône de Bitdefender de la zone de notification est .

Important

Lorsque l'Autopilote est activé, modifier l'un des paramètres qu'il gère conduit à sa désactivation.

Pour afficher un historique des actions réalisées par Bitdefender alors que l'Autopilote était en cours, ouvrez la fenêtre **Notifications**.

4.5. Profils

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



Les profils de Bitdefender allouent davantage de ressources système aux applications en cours d'exécution en modifiant momentanément les paramètres de protection et en adaptant la configuration du système. L'impact du système sur vos activités est donc réduit.

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

Profil Travail

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

Profil Film

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

Profil Jeu

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

Profil Wifi public

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


Profil Mode batterie

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

4.5.1. Configurer l'activation automatique des profils

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

Pour autoriser Bitdefender à activer les profils :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Profils**.
3. Utilisez le bouton correspondant pour activer **Activer automatiquement les profils**.




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

Pour plus d'informations sur les profils, consultez « *Profils* » (p. 198)

4.6. Paramètres de Bitdefender de la protection par mot de passe

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

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Général** :
3. Activez la protection mot de passe en cliquant sur le bouton correspondant.
4. Entrez le mot de passe dans les deux champs puis cliquez sur **OK**. (8 caractères minimum)


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



Important

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

Pour supprimer la protection par mot de passe :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Général** :
3. Désactivez la protection mot de passe en cliquant sur le bouton correspondant. Entrez le mot de passe puis cliquez sur **OK**.




Note

Pour modifier le mot de passe de votre produit, cliquez sur le lien **Changer de mot de passe**.

4.7. Rapports d'utilisation anonymes

Par défaut, Bitdefender envoie des rapports contenant des informations sur votre utilisation aux serveurs Bitdefender. Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir un meilleur service à l'avenir. Veuillez noter que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Si vous souhaitez ne plus envoyer de rapports d'utilisation Anonymes :


1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Avancé**.
3. Cliquez sur le bouton correspondant pour désactiver les rapports d'utilisation anonymes.

4.8. Offres spéciales et notifications du produit

Le produit Bitdefender est configuré pour vous signaler via une fenêtre pop-up les offres promotionnelles disponibles. Cela vous donne la possibilité de bénéficier de tarifs avantageux et de protéger vos appareils plus longtemps.

Des notifications du produit peuvent apparaître également lorsque vous effectuez des modifications dans le produit.

Pour activer ou désactiver les notifications produit :

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Général** :
3. Activez ou désactivez les offres spéciales et les notifications du produit en cliquant sur le bouton correspondant.

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



5. INTERFACE DE BITDEFENDER

Bitdefender Total Security 2017 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 afficher l'état du produit et effectuer des tâches essentielles, l'**icône de la zone de notification** de Bitdefender est disponible à tout moment.

La **fenêtre principale** vous permet de gérer le comportement du produit à l'aide d'**Autopilote**, vous donne accès à d'importantes informations produit et vous permet d'effectuer des tâches quotidiennes. Dans la barre gauche, vous pouvez accéder à **compte Bitdefender** et aux rubriques **Bitdefender** pour une configuration détaillée et des tâches administratives avancées.

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

5.1. Icône de la zone de notification


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



Note

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

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

1. Cliquez sur la flèche  dans l'angle inférieur droit de l'écran.
2. Cliquez sur **Personnaliser...** pour ouvrir la fenêtre Icônes de la Zone de Notification.
3. Sélectionnez l'option **Afficher les icônes et les notifications** pour l'icône **Agent Bitdefender**.

● Dans **Windows 10** :

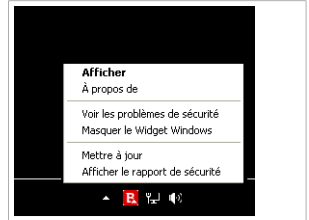
1. Faites un clic droit sur la barre des tâches et sélectionnez **Propriétés**.
2. Cliquez sur **Personnaliser...** dans la fenêtre de la barre des tâches.
3. Cliquez sur le lien **Choisir quelles icônes apparaissent dans la barre des tâches** dans la fenêtre **Notifications & actions**.



4. Activez le bouton à côté de **BitdefenderAgent**.




Double-cliquez sur cette icône pour ouvrir Bitdefender. Un clic droit sur l'icône donne également accès à un menu contextuel qui vous permettra de rapidement administrer le produit Bitdefender.


- **Afficher** - ouvre la fenêtre principale de Bitdefender.
- **À propos de** - Affichage d'une fenêtre contenant des informations relatives à Bitdefender, ainsi que des éléments d'aide si vous rencontrez une situation anormale.
- **Voir les problèmes de sécurité** - vous aide à résoudre les problèmes de vulnérabilité en matière de sécurité. Si l'option n'est pas disponible, c'est qu'il n'y a pas de problème à corriger. Pour plus d'information, consultez « *Correction des problèmes* » (p. 16).
- **Afficher / Masquer le Widget Windows** - permet d'activer / de désactiver le **Widget Windows**.
- **Mettre à jour** - lance immédiatement une mise à jour. Vous pouvez suivre l'état de mise à jour dans le panneau Mise à jour de la **fenêtre principale de Bitdefender**.
- **Afficher le rapport de sécurité** - ouvre une fenêtre où vous pouvez voir un rapport hebdomadaire et des recommandations pour votre système. Vous pouvez suivre les recommandations pour améliorer la sécurité de votre système.



Icône de la barre d'état

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

-  D'importants problèmes affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.
-  Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
-  L'**Autopilote** de Bitdefender est activé.

Si Bitdefender ne fonctionne pas, l'icône de la zone de notification apparaît sur un fond gris : . Cela se produit généralement lorsque l'abonnement est



expiré. Cela peut également avoir lieu lorsque les services Bitdefender ne répondent pas ou lorsque d'autres erreurs affectent le fonctionnement normal de Bitdefender.

5.2. Fenêtre principale

La fenêtre principale de Bitdefender permet d'effectuer des tâches courantes, de corriger rapidement des problèmes de sécurité, d'afficher des informations sur le fonctionnement du produit et accéder aux panneaux à partir desquels vous configurez le produit. Tout se trouve à quelques clics.

La fenêtre est organisée en trois catégories :

Zone d'état

Là, vous pouvez vérifier l'état de sécurité de votre ordinateur, effectuer une mise à jour et configurer l'**Autopilote**.

Barre gauche

Ce menu vous permet d'accéder et de gérer votre **compte Bitdefender** ainsi que les fonctionnalités en ligne de votre produit, ou passer d'une rubrique à l'autre. A partir de là, vous pouvez également accéder aux **Notifications**, au **Rapport de sécurité** hebdomadaire, aux Paramètres généraux et aux zones d'**Aide & Support**.

Actionnez les boutons et accédez à la zone des modules

Là, vous pouvez exécuter différentes tâches pour garder votre système protégé et fonctionnant à une vitesse optimale. De plus, vous pouvez également accéder aux modules Bitdefender pour configurer le produit que vous possédez.

5.2.1. Zone d'état

La zone barre d'états supérieure contient les éléments suivants :

- **État de sécurité** à gauche de la zone vous indique si des problèmes affectent la sécurité de votre ordinateur et vous aide à les corriger.

La couleur de la zone d'état de la sécurité change en fonction des problèmes détectés et différents messages s'affichent :

- **La zone est en vert.** Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.



- **La zone est en jaune.** Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
- **La zone est en rouge.** Des problèmes critiques affectent la sécurité de votre système. Nous vous recommandons de vous occuper de ces problèmes immédiatement.



En cliquant sur la zone d'état de la sécurité, vous pouvez accéder à un assistant qui vous aidera à supprimer facilement toutes les menaces de votre ordinateur. Pour plus d'information, consultez « *Correction des problèmes* » (p. 16).

- **Autopilote** vous permet de profiter d'une protection optimale et d'une sécurité totalement silencieuse. Pour plus d'informations, consultez « *Autopilot* » (p. 20).
- **Mettre à jour** vous permet de lancer une mise à jour produit quand vous le souhaitez pour vous assurer que vous avez les dernières signatures malwares. Pour plus d'informations, consultez « *Maintenir Bitdefender à jour* » (p. 46).
- **Profil actif** affiche le profil actuellement activé dans votre produit Bitdefender. Pour plus d'informations, consultez « *Profils* » (p. 198).

5.2.2. Barre gauche

Les icônes de suggestion sont disponibles dans la barre de gauche pour vous donner accès à compte Bitdefender, aux rubriques produit, aux rapports d'activités, aux notifications, aux paramètres généraux et au support.

Les noms des icônes sont visibles en cliquant sur l'icône ≡, comme suit :

-  **Protection.** Les boutons d'action **Analyse rapide** and **Analyse vulnérabilités** deviennent visibles dans coin en bas à gauche de l'interface Bitdefender. De plus, des informations à propos d'applications bloquées, des menaces détectées et des attaques deviennent visibles. Cliquez sur le lien **VOIR MODULES** pour accéder à la zone de configuration.
-  **Vie privée.** Les boutons d'action **Safepay** et **Contrôle parental** deviennent visibles dans le coin en bas à gauche de l'interface Bitdefender. De plus, des informations à propos des wallets et des coffres-forts sont affichées. Cliquez sur le lien **VOIR MODULES** pour accéder à la zone de configuration.



- **Outils.** Les boutons d'action **OneClick Optimizer** et **Startup Optimizer** deviennent visibles dans le coin en bas à gauche de l'interface Bitdefender. En outre, des informations sur l'espace optimisé sont affichées et la fonctionnalité **Nettoyage de disque** peut être lancée pour faire de la place à de nouvelles données en effaçant des fichiers et dossiers volumineux que vous n'utilisez plus. De plus, la fonctionnalité Antivol est présente.
- **Activité.** Ici, vous pouvez suivre l'activité du produit au cours des 30 derniers jours et accéder au rapport de sécurité généré tous les sept jours.
- **Informations compte.** Les détails à propos de compte Bitdefender et les abonnements en cours sont disponibles. Accéder à votre compte Bitdefender pour vérifier votre abonnement et effectuer des tâches de sécurité sur les appareils que vous gérez.
- **Notifications.** Là, vous pouvez accéder aux notifications générées.
- **Configuration.** Là, vous pouvez accéder aux Paramètres généraux.
- **Support.** Là, quand vous avez besoin d'assistance pour régler un problème avec votre Bitdefender Total Security 2017, vous pouvez contacter le service de support technique de Bitdefender.

5.2.3. Actionnez les boutons et accédez à la zone des modules

Avec les boutons d'action, vous pouvez exécuter rapidement des tâches importantes. Les boutons d'action apparaîtront dans le coin en bas à gauche de l'interface Bitdefender lorsque vous sélectionnez l'une des trois rubriques : **Protection**, **Vie privée** or **Outils** dans la barre de gauche.

Selon la section que vous choisissez, les boutons d'action visibles dans cette zone seront :

- **Analyse rapide.** Exécutez une analyse rapide pour vérifier qu'aucun malware n'est présent sur votre ordinateur.
- **Analyse de vulnérabilités.** Analysez votre ordinateur à la recherche de vulnérabilités pour vous assurer que toutes les applications, ainsi que le système d'exploitation, sont mis à jour et fonctionnent correctement.
- **Safepay.** Ouvrez Bitdefender Safepay™ pour protéger vos données sensibles lorsque vous effectuez des transactions en ligne.



- **Contrôle Parental.** Accédez au Contrôle parental de Bitdefender pour rester informé des activités de vos enfants.
- **Optimisation du démarrage.** Réduisez votre temps de démarrage en empêchant les applications superflues de s'exécuter au démarrage.
- **Optimisation en 1 clic.** Libérez de l'espace sur le disque, corrigez les erreurs du registre et protégez votre vie privée en supprimant les fichiers qui ne sont plus utiles d'un simple clic sur un bouton.

5.3. Les rubriques Bitdefender

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

Chaque fois que vous souhaitez accéder aux modules pour une raison spécifique ou pour commencer à configurer votre produit, accédez aux icônes suivantes localisées dans la barre de gauche de l'**interface Bitdefender**:

-  **Protection**
-  **Vie privée**
-  **Outils**

5.3.1. Protection

Dans la rubrique Protection, vous pouvez configurer le niveau de sécurité, gérer vos amis et les spammeurs, afficher et modifier les paramètres de connexion réseau, configurer les fonctions de protection ransomware et Web, vérifier et corriger les vulnérabilités potentielles du système et évaluer la sécurité du réseau sans fil auquel vous êtes connecté.

Les modules que vous pouvez gérer dans la rubrique Protection sont les suivants :

ANTIVIRUS

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

Le module Antivirus vous permet d'accéder facilement aux tâches d'analyse suivantes :



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

Pour plus d'informations sur les tâches d'analyse et sur comment configurer la protection antivirus, consultez « *Protection antivirus* » (p. 93).

PROTECTION WEB

La protection web vous aide à être protégé contre les attaques de phishing, les tentatives de fraude et les fuites de données personnelles lorsque vous naviguez sur Internet.

Pour plus d'informations sur comment configurer Bitdefender pour protéger vos activités en ligne, consultez « *Protection Web* » (p. 130).

VULNÉRABILITÉ

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

Cliquez sur **Analyse de Vulnérabilité** dans le module Vulnérabilité pour commencer à identifier les mises à jour critiques de Windows, les mises à jour d'applications, les mots de passe vulnérables appartenant à des comptes Windows et les réseaux sans fil qui ne sont pas sûrs.

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

Pour plus d'informations sur la configuration de la protection contre les vulnérabilités, reportez-vous à « *Vulnérabilité* » (p. 140).

Pare-feu bidirectionnel

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

Pour plus d'informations sur la configuration du pare-feu, consultez « *Pare-feu* » (p. 149).



ANTIPOURRIEL

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

Pour plus d'informations sur la protection antispam, reportez-vous à « *Antispam* » (p. 120).

PROTECTION RANSOMWARE

Le module Ransomware Protection garantit que vos fichiers personnels restent protégés contre l'extorsion en ligne.

Pour plus d'informations sur comment configurer la Ransomware Protection pour protéger les activités du système contre les attaques de ransomwares, reportez-vous à « *Protection ransomware* » (p. 158).

5.3.2. Vie privée

La rubrique Vie privée vous permet de chiffrer vos données confidentielles, de protéger vos transactions en ligne, de sécuriser votre navigation sur Internet et de protéger vos enfants en vous offrant la possibilité de voir et de limiter leurs activités en ligne.

Les modules que vous pouvez gérer dans la rubrique Vie privée sont les suivants :

PROTECTION DES DONNÉES

Le module Protection des données vous permet de supprimer des fichiers de façon permanente.

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

Pour plus d'informations sur la configuration de la protection des données, reportez-vous à « *Protection des données* » (p. 132).

WALLET

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

Le module Password Manager vous permet de sélectionner les tâches suivantes :

- **Ouvrir Wallet** - ouvre la base de données d'un Wallet existant.
- **Verrouiller Wallet** - verrouille la base de données d'un Wallet existant.



- **Exporter Wallet** - sauvegarde la base de données existante sur votre système.
- **Créer un Wallet** - lance un assistant qui vous permet de créer une nouvelle base de données Wallet.
- **Supprimer** - vous permet de supprimer une base de données Wallet.
- **Paramètres** - ici, vous pouvez modifier le nom de votre base de données Wallet et configurer de façon à ce que la synchronisation soit faite entre les informations existantes et tous vos appareils, ou non.

Pour plus d'informations sur la configuration du Gestionnaire de mots de passe, consultez « *Protection Password Manager de vos identifiants* » (p. 168).

SAFEPAY

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

Cliquez sur le bouton d'action **Safepay** dans l'interface Bitdefender pour commencer à effectuer des transactions en ligne dans un environnement sécurisé.

Pour plus d'informations sur Bitdefender Safepay™, reportez-vous à « *La sécurité SafePay pour les transactions en ligne* » (p. 162).

Parental Advisor

Le Contrôle parental de Bitdefender vous permet de surveiller ce que votre enfant fait sur l'ordinateur. En cas de contenu inapproprié vous pouvez décider de limiter son accès à Internet ou à certaines applications.

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

Pour plus d'informations sur la configuration du Contrôle parental, consultez « *Parental Advisor* » (p. 177).

CHIFFREMENT

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



Pour plus d'informations sur comment créer des disques logiques (ou des coffres-forts) chiffrés, protégés par mot de passe sur votre ordinateur, veuillez vous reporter à « *Chiffrement de fichiers* » (p. 134).

5.3.3. Outils

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

Optimisations

Bitdefender Total Security 2017 offre plus que de la sécurité, et contribue également aux bonnes performances de votre ordinateur.

Le module Optimisation vous permet d'accéder à des outils utiles :

- Optimisation en un clic
- Optimisation du démarrage
- Nettoyage du disque

Pour plus d'informations sur les outils d'optimisation des performances, veuillez vous référer à « *Outils* » (p. 193).

Antivol

Bitdefender Antivol protège votre ordinateur et vos données contre la perte et le vol. Dans ce cas, cela vous permet de localiser ou de verrouiller votre ordinateur à distance. Vous pouvez également effacer toutes les données présentes sur votre système.

Bitdefender Anti-Theft dispose des fonctionnalités suivantes :

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

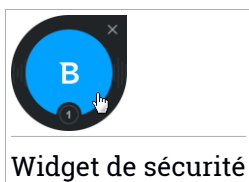
Pour plus d'informations sur comment maintenir votre système hors de portée des personnes malintentionnées veuillez vous référer à « *Antivol de l'appareil* » (p. 188).

5.4. Widget de sécurité

Le **Widget Windows** est une façon simple et rapide de surveiller et de contrôler Bitdefender Total Security 2017. Ajouter ce petit widget discret à votre bureau vous permet de voir des informations critiques et d'effectuer des tâches essentielles à tout moment :



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



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



Des problèmes critiques affectent la sécurité de votre système.

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



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



Votre système est protégé.



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

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



La **partie inférieure** du widget affiche le compteur d'événements non lus (le nombre d'événements importants signalés par Bitdefender, s'il y en a). Cliquez sur le compteur d'événements, par exemple **1** pour un événement non lu, pour ouvrir la fenêtre Notifications. Pour plus d'informations, reportez-vous à « **Notifications** » (p. 19).

5.4.1. Analyse des fichiers et des dossiers

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

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

5.4.2. Masquer / afficher le Widget Windows

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

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

● Dans la zone de notification :

1. Faites un clic droit sur l'icône de Bitdefender dans la **zone de notification**.
2. Cliquez sur **Afficher le Widget Windows** dans le menu contextuel qui apparaît.

● À partir de l'interface de Bitdefender :

1. Cliquez sur **⚙** l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Général** :
3. Activez Afficher le Widget Windows en cliquant sur le bouton correspondant.



5.5. Activité

La fenêtre Activité affiche les informations relatives aux actions entreprises par Bitdefender sur votre appareil au cours des 30 derniers jours. Ici, vous pouvez vérifier quelles applications, menaces et attaques ont été bloquées au cours de cette période, et si des tentatives d'attaques par ransomware ont été faites.

Le Rapport de sécurité, qui fournit un suivi hebdomadaire pour votre produit et plusieurs conseils pour améliorer la protection du système, est également accessible en cliquant sur le lien correspondant. Ces conseils sont importants pour gérer la protection globale et vous pouvez voir facilement les actions que vous pouvez appliquer sur votre système.

Le rapport est généré une fois par semaine et résume les principales informations sur l'activité de votre produit afin que vous puissiez comprendre facilement ce qui s'est passé pendant cette période.

Les informations fournies par le rapport de sécurité sont divisées en trois catégories :

- **Zone Protection** - permet d'afficher des informations liées à la protection de votre système.

- **Fichiers analysés**

Vous permet de voir les fichiers analysés par Bitdefender pour la semaine. Vous pouvez afficher des informations comme le nombre de fichiers analysés et le nombre de fichiers nettoyés par Bitdefender.

Pour plus d'informations sur la protection antivirus, reportez-vous à « *Protection antivirus* » (p. 93).

- **Pages Web analysées**

Vous permet de consulter le nombre de pages Web analysées et bloquées par Bitdefender. Pour vous protéger contre la divulgation d'informations personnelles lorsque vous êtes sur Internet, Bitdefender sécurise votre trafic Web.

Pour plus d'informations sur la protection Web, reportez-vous à « *Protection Web* » (p. 130).

- **Vulnérabilités**



Vous permet d'identifier et de corriger facilement les vulnérabilités du système afin de renforcer la protection de votre ordinateur contre les malwares et les pirates informatiques.

Pour plus d'informations sur l'analyse de vulnérabilité, consultez « *Vulnérabilité* » (p. 140).

● **Chronologie des événements**

Vous permet d'avoir une image globale des processus d'analyse et des problèmes corrigés par Bitdefender au cours de la semaine. Les événements sont séparés par jours.

Pour plus d'informations sur un journal détaillé d'événements concernant l'activité sur votre ordinateur, consultez « *Notifications* » (p. 19).

- **Zone Vie privée** - permet d'afficher des informations liées à la confidentialité de votre système.

● **Fichiers dans le coffre-fort**

Vous permet de voir combien de fichiers sont protégés contre l'accès non autorisé.

Pour plus d'informations sur comment créer des disques logiques (ou des coffres-forts) chiffrés, protégés par mot de passe sur votre ordinateur, veuillez vous reporter à « *Chiffrement de fichiers* » (p. 134).

- **La zone Optimisation** - affiche des informations au sujet de l'espace libéré, des applications optimisées et de la quantité de batterie économisée avec le Mode Batterie.

● **Espace libéré**

Vous permet de connaître la quantité d'espace libéré lors du processus d'optimisation du système. Bitdefender utilise l'Optimisation pour vous aider à améliorer la vitesse de votre système.

Pour plus d'informations sur l'Optimisation, reportez-vous à « *Outils* » (p. 193).

● **Batterie économisée**

Vous permet de voir la quantité de batterie économisée lorsque le système fonctionnait en Mode Batterie.

Pour plus d'informations sur le Mode Batterie, reportez-vous à « *Profil Mode batterie* » (p. 204).



● Application(s) optimisée(s)

Vous permet de voir le nombre d'applications que vous avez utilisées sous les Profils.


Pour plus d'informations sur les Profils, reportez-vous à « *Profils* » (p. 198).

5.5.1. Consulter le rapport de sécurité

Le Rapport de sécurité utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous en informer. Les problèmes détectés comprennent la désactivation d'importants paramètres de protection et d'autres conditions pouvant constituer un risque pour la sécurité. Utiliser le rapport vous permet de configurer des composants de Bitdefender spécifiques ou d'appliquer des actions préventives afin de protéger votre ordinateur et vos données confidentielles.

Pour consulter le Rapport de sécurité :

1. Accédez au rapport :

- Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.

Cliquez sur le lien **Rapport de sécurité** situé dans le coin inférieur droit de la fenêtre Rapport d'activité.

- Faites un clic droit sur l'icône de Bitdefender dans la zone de notification et sélectionnez **Afficher le rapport de sécurité**.

- Lorsqu'un rapport est terminé, vous serez averti par une fenêtre contextuelle. Cliquez sur **Afficher** pour accéder au rapport d'activité.

Une page Web s'ouvrira dans votre navigateur Web où vous pourrez voir le rapport généré.

2. Consultez la partie supérieure de la fenêtre pour voir l'état de sécurité global.

3. Consultez nos recommandations en bas de la page.


La couleur de la zone d'état de la sécurité change en fonction des problèmes détectés et différents messages s'affichent :



- **La zone est en vert.** Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.
- **La zone est en orange.** Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
- **La zone est en rouge.** Des problèmes critiques affectent la sécurité de votre système. Nous vous recommandons de vous occuper de ces problèmes immédiatement.

5.5.2. Activer ou désactiver la notification Rapport de Sécurité

Pour activer ou désactiver la notification Rapport de sécurité :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Général** :
3. Cliquez sur le bouton correspondant pour activer ou désactiver la notification Rapport de sécurité.

La notification Rapport de sécurité est activée par défaut.




6. BITDEFENDER CENTRAL

Bitdefender Central est la plateforme web à partir de laquelle vous avez accès aux fonctionnalités et services en ligne du produit, et peut effectuer d'importantes tâches sur les appareils sur lesquels Bitdefender est installé. Vous pouvez vous connecter à votre compte Bitdefender à partir de n'importe quel ordinateur ou appareil mobile connecté à Internet en allant dans <https://central.bitdefender.com>. Une fois que vous êtes connectés, vous pouvez commencer à faire ce qui suit :

- Télécharger et installer Bitdefender sur les systèmes d'exploitation OS X, Windows et Android. Les produits disponibles au téléchargement sont :
 - Bitdefender Total Security 2017
 - Antivirus Bitdefender pour Mac
 - Bitdefender Mobile Security
- Gérer et renouveler vos abonnement Bitdefender.
- Ajouter de nouveaux appareils à votre réseau et les gérer où que vous soyez.
- Protégez les appareils de votre réseau et leurs données contre le vol et la perte avec **Antivol**.

6.1. 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 :

- À partir de l'interface principale de Bitdefender :
 1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
 2. Sélectionnez le lien **Aller dans le Central de Bitdefender**.
 3. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
- A partir de votre navigateur web :
 1. Ouvrir un navigateur web sur chaque appareil ayant accès à Internet.



2. Allez à : <https://central.bitdefender.com>.
3. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.

6.2. Mes abonnements

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

6.2.1. Vérifier les abonnements disponibles

Pour vérifier vos abonnements disponibles :

1. Accéder à **Bitdefender Central**.
2. Sélectionner le panneau **Mes Abonnements**.

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

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



Note

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

6.2.2. nouvel appareil

Si votre abonnement couvre plus d'un appareil, vous pouvez ajouter un nouvel appareil et y installer votre Bitdefender Total Security 2017, comme suit :

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
4. Sélectionnez l'une des deux actions disponibles :

- **TÉLÉCHARGER**

Cliquez sur le bouton pour sauvegarder le fichier d'installation.

- **Sur un autre appareil**



Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrez une adresse électronique dans le champ correspondant, puis cliquez sur **ENVOYER**.

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

6.2.3. Renouveler abonnement

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

1. Accéder à **Bitdefender Central**.
2. Sélectionner le panneau **Mes Abonnements**.
3. Sélectionnez la carte d'abonnement souhaitée.
4. Cliquez sur **Renouveler** pour poursuivre.

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

6.2.4. Activer abonnement

Un abonnement peut être activé pendant le processus d'installation à l'aide de votre compte Bitdefender. En même temps que le processus d'activation, sa validité commence le compte à rebours.

Si vous avez acheté un code d'activation chez l'un de nos revendeurs ou que vous l'avez reçu en cadeau, vous pouvez ajouter sa disponibilité à tout abonnement Bitdefender existant disponible sur le compte, s'ils sont pour le même produit.

Pour activer un abonnement avec un code d'activation :

1. Accéder à **Bitdefender Central**.
2. Sélectionner le panneau **Mes Abonnements**.
3. Cliquez sur le bouton **CODE D'ACTIVATION**, puis saisissez le code dans le champs correspondant.
4. Cliquez à nouveau sur le bouton **CODE D'ACTIVATION**.

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



6.3. Mes appareils

La zone **Mes Appareils** dans Bitdefender Central vous donne la possibilité d'installer, gérer et exécuter des actions à distance sur votre Bitdefender sur n'importe quel appareil, pourvu qu'il soit allumé et connecté à Internet. Les cartes appareils affichent le nom de l'appareil, le statut de protection et la disponibilité restante de votre abonnement.

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

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur l'icône  sur la carte appareil souhaitée, puis sélectionnez **Paramètres**.
4. Changez le nom de l'appareil dans le champs correspondant, puis sélectionnez **Sauvegarder**.

Si Autopilot est désactivé, vous pouvez l'activer en cliquant sur le bouton. Cliquez sur **Enregistrer** pour appliquer les configurations.


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

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur l'icône  sur la carte appareil souhaitée, puis sélectionnez **Profil**.
4. Cliquez sur **Ajouter propriétaire**, puis remplissez les champs correspondants, configurer le sexe, la date de naissance, et ajoutez une photo de profil si vous le souhaitez.
5. Cliquez sur **AJOUTER** pour sauvegarder le profil.
6. Sélectionnez le propriétaire souhaité à partir de la liste **Propriétaire appareil**, puis cliquez sur **ASSIGNER**.

Pour mettre à jour Bitdefender à distance sur un appareil :

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.



3. Cliquez sur l'icône  sur la carte appareil souhaitée, puis 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 vérifier le statut de protection de vos produits Bitdefender et le nombre de jours restants pour votre abonnement. Le statut de protection peut être vert lorsque aucun problème n'affecte votre produit, ou rouge si le produit est en danger. Quand des problèmes affectent votre produit, cliquez sur **Voir problèmes** pour en savoir plus. A partir de là, vous pouvez réparer manuellement les problèmes qui affectent la sécurité de vos appareils.

- **Protection.** A partir de cette fenêtre, vous pouvez lancer à distance une Analyse rapide ou une Analyse système sur vos appareils. Cliquez sur le bouton **ANALYSE** pour commencer le processus. Vous pouvez également vérifier à quelle date la dernière analyse a été faite sur l'appareil, et un rapport de l'analyse la plus récente contenant les informations importantes est à votre disposition. Pour plus d'informations sur les deux processus d'analyse, reportez-vous à « *Exécuter une analyse du système* » (p. 102) et à « *Exécuter une analyse rapide* » (p. 101) .

- **Optimisation.** Ici, vous pouvez améliorer à distance la performance d'un appareil en analysant, détectant et nettoyant rapidement les fichiers inutiles. Cliquez sur le bouton **DÉMARRER**, puis sélectionnez les zones que vous souhaitez optimiser. Cliquez à nouveau sur le bouton **DÉMARRER** pour lancer le processus d'optimisation. Cliquez sur **Plus de détails** pour accéder à un rapport détaillé sur les problèmes réparés.

En outre, vous pouvez améliorer le démarrage de votre appareil en identifiant les applications consommant beaucoup de ressources. Cliquez sur le bouton **DÉMARRER** puis choisissez ce que vous voulez faire avec les applications détectées. Pour plus de détails sur ces fonctionnalités, reportez-vous à « *Optimisation de la vitesse de votre système d'un simple clic* » (p. 193) et à « *Optimisation du temps de démarrage de votre PC* » (p. 194).

- **Antivol.** En cas d'égarement, de vol ou de perte, vous pouvez avec la fonctionnalité Antivol localiser votre appareil et agir à distance. Cliquez sur **LOCALISER** pour déterminer la position de votre appareil. La dernière



position connue s'affichera, ainsi que la date et l'heure. Pour plus de détails sur cette fonctionnalité, reportez-vous à « *Antivol de l'appareil* » (p. 188).

- **Vulnérabilité.** Pour vérifier les vulnérabilités sur un appareil (comme les mises à jour Windows manquantes, les applications obsolètes, ou les mots de passe faibles) cliquez sur le bouton **ANALYSE** dans l'onglet Vulnérabilité. Les vulnérabilités ne peuvent pas être réparées à distance. Dans le cas où une vulnérabilité est trouvée, vous devez exécuter une nouvelle analyse sur l'appareil puis effectuer les actions recommandées. Cliquez sur **Plus de détails** pour accéder à un rapport détaillé sur les problèmes trouvés. Pour plus de détails sur cette fonctionnalité, reportez-vous à « *Vulnérabilité* » (p. 140).



7. MAINTENIR BITDEFENDER À JOUR

De nouveaux virus sont trouvés et identifiés chaque jour. C'est pourquoi il est très important que Bitdefender soit à jour dans les signatures de codes malveillants.

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

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



Important

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

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


- Si votre ordinateur se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy comme indiqué dans « *Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?* » (p. 86).
- Des erreurs peuvent se produire lors du téléchargement de mises à jour avec une connexion à Internet lente. Pour savoir comment éviter ces erreurs, veuillez consulter « *Comment mettre à jour Bitdefender avec une connexion Internet lente ?* » (p. 220).
- Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour manuelles de Bitdefender. Pour plus d'informations, reportez-vous à « *Mise à jour en cours* » (p. 47).

7.1. Vérifier que Bitdefender est à jour

Pour vérifier l'heure de la dernière mise à jour de votre Bitdefender, regardez la **Zone état sécurité**, sur le côté gauche de la Zone d'états.



Pour des informations détaillées sur les dernières mises à jour, vérifiez les événements de mise à jour :

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant la dernière mise à jour.

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

7.2. Mise à jour en cours

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

Pour lancer une mise à jour, choisissez l'une des options suivantes :

- Ouvrez **l'interface Bitdefender** et cliquez sur le lien **Mettre à jour maintenant** sous l'état de votre programme.
- Faites un clic droit sur l'icône de Bitdefender **B** de la **zone de notification** et sélectionnez **Mettre à jour maintenant**.


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

Important

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

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


Pour mettre à jour Bitdefender à distance sur un appareil :

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur l'icône  sur la carte appareil souhaitée, puis sélectionnez **Mise à jour**.



7.3. Activer ou désactiver la mise à jour automatique

Activer ou désactiver la mise à jour automatique :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Mise à jour**.
3. Cliquez sur le bouton correspondant pour activer ou désactiver la mise à jour automatique.
4. Une fenêtre d'avertissement s'affiche. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactiver la mise à jour automatique. Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.



Avertissement


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

7.4. Réglage des paramètres de mise à jour

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

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

Pour ajuster les paramètres de mise à jour :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Mise à jour**, ajustez les paramètres en fonction de vos préférences.



Fréquence de la mise à jour

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

Emplacement de mise à jour

Bitdefender est configuré pour se mettre à jour à partir des serveurs de mise à jour de Bitdefender sur Internet. L'emplacement de mise à jour est une adresse Internet générique qui est automatiquement redirigée vers le serveur de mise à jour Bitdefender le plus proche de votre région.

Ne modifiez pas l'emplacement de mise à jour sauf sur demande d'un représentant de Bitdefender ou de votre administrateur réseau (si vous êtes connecté à un réseau d'entreprise).

Vous pouvez revenir à l'emplacement de mise à jour Internet générique en cliquant sur **Par défaut**.

Règles de traitement des mises à jour

Vous disposez de trois façons de télécharger et d'installer des mises à jour :

- **Mise à jour silencieuse** - Bitdefender télécharge et implémente automatiquement la mise à jour.
- **Demander avant de télécharger les mises à jour** - à chaque fois qu'une mise à jour sera disponible, le système demandera votre autorisation avant de la télécharger.
- **Demander avant l'installation** - à chaque fois qu'une mise à jour est téléchargée, le système demande votre autorisation avant de l'installer.

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

Si vous souhaitez être averti lorsqu'une mise à jour nécessite un redémarrage, désactivez l'option **Reporter le redémarrage** en cliquant sur le bouton correspondant.



COMMENT FAIRE POUR



8. INSTALLATION

8.1. Comment installer Bitdefender sur un deuxième ordinateur ?

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

installer Bitdefender sur un deuxième ordinateur :

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
4. Sélectionnez l'une des deux actions disponibles :

● **TÉLÉCHARGER**

Cliquez sur le bouton pour sauvegarder le fichier d'installation.

● **Sur un autre appareil**

Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrer une adresse électronique dans le champ correspondant, puis cliquer sur **ENVOYER**.

5. Exécutez le produit Bitdefender que vous avez installé. Attendez la fin du processus d'installation et fermez la fenêtre.

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

8.2. Quand devrais-je réinstaller Bitdefender ?

Dans certains cas, vous pouvez avoir besoin de réinstaller votre produit Bitdefender.

Quelques situations typiques nécessitant de réinstaller Bitdefender :

- vous avez réinstallé le système d'exploitation.
- vous avez acheté un nouvel ordinateur.
- vous souhaitez modifier la langue d'affichage de l'interface de Bitdefender



Pour réinstaller Bitdefender, vous pouvez utiliser le disque d'installation que vous avez acheté ou télécharger une nouvelle version à partir de Bitdefender Central.

Pour plus d'informations sur le processus d'installation de Bitdefender, reportez-vous à « *Installer Bitdefender* » (p. 5).

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

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



Note

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

Pour installer Bitdefender à partir de Bitdefender Central :

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
4. Sélectionnez l'une des deux actions disponibles :

● TÉLÉCHARGER

Cliquez sur le bouton pour sauvegarder le fichier d'installation.

● Sur un autre appareil

Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrez une adresse électronique dans le champ correspondant, puis cliquez sur **ENVOYER**.

5. Exécutez le produit Bitdefender que vous avez installé.

8.4. Comment changer la langue de mon produit Bitdefender ?

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



Pour utiliser Bitdefender dans une autre langue :

1. Supprimez Bitdefender en procédant comme suit :

● Dans **Windows 7** :

- a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
- b. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
- c. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
- d. Cliquez sur **CONTINUER**.
- e. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

● Dans **Windows 8 et Windows 8.1** :

- a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
- b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
- c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
- d. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
- e. Cliquez sur **CONTINUER**.



- f. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Dans **Windows 10** :
 - a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
 - b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
 - c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
 - e. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - f. Cliquez sur **CONTINUER**.
 - g. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
2. Modifier la langue de Bitdefender Central :
 - a. Accéder à **Bitdefender Central**.
 - b. Cliquez sur l'icône **Q** dans l'angle supérieur droit de l'écran.
 - c. Cliquez sur **Mon compte** dans le menu déroulant.
 - d. Sélectionnez l'onglet **Profil**.
 - e. Sélectionnez une langue à partir de la liste déroulante **Langue**, puis cliquez sur **ENREGISTRER**.
3. Téléchargez le fichier d'installation :
 - a. Sélectionnez la section **Mes Appareils**.
 - b. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
 - c. Sélectionnez l'une des deux actions disponibles :
 - **TÉLÉCHARGER**



Cliquez sur le bouton pour sauvegarder le fichier d'installation.

- **Sur un autre appareil**

Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrez une adresse électronique dans le champ correspondant, puis cliquez sur **ENVOYER**.

4. Exécutez le produit Bitdefender que vous avez installé.

8.5. Comment utiliser mon abonnement Bitdefender après une mise à niveau Windows ?

Cette situation se produit lorsque vous mettez à niveau votre système d'exploitation et souhaitez continuer à utiliser votre abonnement Bitdefender.

Si vous utilisez une version antérieure de Bitdefender vous pouvez la mettre à niveau, gratuitement, vers la dernière version de Bitdefender en procédant comme suit :

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

Deux situations peuvent se produire :

- Vous avez mis à niveau le système d'exploitation à l'aide de Windows Update et vous remarquez que Bitdefender ne fonctionne plus.

Dans ce cas, vous avez besoin de réinstaller le produit avec la dernière version disponible.

Pour résoudre cette situation :

1. Supprimez Bitdefender en procédant comme suit :

- Dans **Windows 7** :

- a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
- b. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.



- c. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
- d. Cliquez sur **CONTINUER**.
- e. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Dans **Windows 8 et Windows 8.1** :
 - a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
 - b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
 - c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - d. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - e. Cliquez sur **CONTINUER**.
 - f. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Dans **Windows 10** :
 - a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
 - b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.



- c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
 - e. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - f. Cliquez sur **CONTINUER**.
 - g. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
2. Téléchargez le fichier d'installation :
- a. Accéder à **Bitdefender Central**.
 - b. Sélectionnez la section **Mes Appareils**.
 - c. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
 - d. Sélectionnez l'une des deux actions disponibles :
 - **TÉLÉCHARGER**
Cliquez sur le bouton pour sauvegarder le fichier d'installation.
 - **Sur un autre appareil**
Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrez une adresse électronique dans le champ correspondant, puis cliquez sur **ENVOYER**.
3. Exécutez le produit Bitdefender que vous avez installé.
- Vous avez changé de système et souhaitez continuer à utiliser la protection Bitdefender.
Vous avez donc besoin de réinstaller le produit avec la dernière version.
Pour résoudre cette situation :
1. Téléchargez le fichier d'installation :
 - a. Accéder à **Bitdefender Central**.



- b. Sélectionnez la section **Mes Appareils**.
- c. Dans la fenêtre **Mes Appareils**, cliquez sur **INSTALLER Bitdefender**.
- d. Sélectionnez l'une des deux actions disponibles :

- **TÉLÉCHARGER**

Cliquez sur le bouton pour sauvegarder le fichier d'installation.

- **Sur un autre appareil**

Sélectionnez **Windows** pour télécharger votre produit Bitdefender puis cliquez sur **CONTINUER**. Entrez une adresse électronique dans le champ correspondant, puis cliquez sur **ENVOYER**.

2. Exécutez le produit Bitdefender que vous avez installé.

Pour plus d'informations sur le processus d'installation de Bitdefender, reportez-vous à « *Installer Bitdefender* » (p. 5).

8.6. Comment réparer Bitdefender ?

Si vous souhaitez réparer votre produit Bitdefender Total Security 2017 à partir du menu Démarrer de Windows :

- Dans **Windows 7** :

1. Cliquez sur **Démarrer** et allez dans **Programmes**.
2. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
3. Cliquez sur **Réparer** dans la fenêtre qui s'affiche.
Cela peut prendre quelques minutes.
4. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.

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

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
4. Cliquez sur **Réparer** dans la fenêtre qui s'affiche.
Cela peut prendre quelques minutes.



5. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.

● Dans **Windows 10** :

1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **& Fonctionnalités Applications**.
3. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Cliquez sur **Réparer**.

Cela peut prendre quelques minutes.

6. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.



9. LICENCE(S)

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


Si vous avez une clé de licence valide et que vous souhaitez l'utiliser pour activer votre abonnement pour Bitdefender Total Security 2017, il y a deux cas possibles :

- Vous avez fait une mise à niveau à partir d'une version précédente de Bitdefender vers la nouvelle :

1. Une fois que la mise à niveau vers Bitdefender Total Security 2017 est terminée, vous devez vous connecter à votre compte Bitdefender.
2. Cliquez sur le lien **Se Connecter** puis tapez l'adresse e-mail et le mot de passe de votre compte Bitdefender.
3. Cliquez sur **Se connecter** pour poursuivre.
4. Une notification vous informant qu'un abonnement a été créé apparaît sur l'écran de votre compte. L'abonnement créé sera valide pour la période restante sur votre clé de licence et pour le même nombre d'utilisateurs.

Les appareils qui utilisent les versions précédentes de Bitdefender et sont enregistrés avec la clé de licence que vous avez convertie en abonnement doivent activer le produit avec le même compte Bitdefender.

- Bitdefender n'était pas précédemment installé sur le système :

1. Dès que le processus d'installation est terminé, vous devez vous connecter à votre compte Bitdefender.
2. Cliquez sur le lien **Se Connecter** puis tapez l'adresse e-mail et le mot de passe de votre compte Bitdefender.
3. Cliquez sur **CONNEXION** pour continuer, puis sur le bouton **TERMINER** pour accéder à l'interface Bitdefender Total Security 2017.
4. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
5. Sélectionnez le lien **Code d'activation**.



Une nouvelle fenêtre apparaît.

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




10. BITDEFENDER CENTRAL

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

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

Pour ajouter un nouveau compte :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface Bitdefender.
2. Cliquez sur le bouton **Changer de compte** pour changer le compte lié à l'ordinateur.
3. Tapez l'adresse courriel et le mot de passe de votre compte dans les champs correspondants, puis cliquez sur **CONNEXION**.



Note


Le produit Bitdefender de votre appareil change automatiquement selon l'abonnement associé au nouveau compte Bitdefender.

S'il n'y a pas d'abonnement disponible associé au nouveau compte Bitdefender, ou que vous souhaitez le transférer à partir du compte précédent, vous pouvez contacter le support Bitdefender comme décrit dans la rubrique « *Assistance* » (p. 244).

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

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


Si vous souhaitez ne plus voir ces messages :

1. Accéder à **Bitdefender Central**.
2. Cliquez sur l'icône  dans l'angle supérieur droit de l'écran.
3. Cliquez sur **Mon compte** dans le menu déroulant.
4. Sélectionnez l'onglet **Paramètres**.
5. Désactivez l'option **Activez/désactivez les messages d'aide**.




10.3. Comment faire pour ne plus voir les photos prises avec mes appareils ?

Pour ne plus voir les photos prises sur vos appareils :

1. Accéder à **Bitdefender Central**.
2. Cliquez sur l'icône  dans l'angle supérieur droit de l'écran.
3. Cliquez sur **Mon compte** dans le menu déroulant.
4. Sélectionnez l'onglet **Paramètres**.
5. Désactivez l'option **Montrer/ne pas montrer de photos prises depuis vos appareils**

10.4. J'ai oublié le mot de passe que j'avais configuré pour mon compte Bitdefender. Comment le reconfigurer ?

Pour créer un nouveau mot de passe pour votre compte Bitdefender :


1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le bouton **CRÉER COMPTE**.
Une nouvelle fenêtre apparaît.
3. Cliquez sur le lien **J'ai oublié mon mot de passe**.
4. Saisissez l'adresse courriel utilisée pour créer votre compte Bitdefender puis cliquez sur le bouton **Mot de passe oublié**.
5. Consultez votre courriel et cliquez sur le bouton indiqué.
6. Saisissez votre adresse e-mail dans le champ correspondant.
7. Saisissez le nouveau mot de passe. Le mot de passe doit contenir au moins 8 caractères et contenir des chiffres.
8. Cliquez sur le bouton **Reconfigurer mot de passe**.

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



10.5. Comment redéfinir le mot de passe du compte Bitdefender ?


Pour changer votre mot de passe actuel compte Bitdefender avec un nouveau :

1. Accéder à **Bitdefender Central**.
2. Cliquez sur l'icône  dans l'angle supérieur droit de l'écran.
3. Cliquez sur **Mon compte** dans le menu déroulant.
4. Sélectionnez l'onglet **Changer de mot de passe**.
5. Entrez l'ancien mot de passe dans le champ **Ancien mot de Passe**.
6. Saisissez le nouveau mot de passe que vous souhaitez configurer pour votre compte dans le champ **Nouveau mot de passe**.
7. Cliquez sur le bouton **Changer mot de passe**.

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

10.6. Comment supprimer compte Bitdefender ?

Pour supprimer votre compte Bitdefender :

1. Accéder à **Bitdefender Central**.
2. Cliquez sur l'icône  dans l'angle supérieur droit de l'écran.
3. Cliquez sur **Mon compte** dans le menu déroulant.
4. Sélectionnez l'onglet **Supprimer compte**.
5. Cliquez sur **SUPPRIMER COMPTE**, puis sur le bouton **ENVOYER E-MAIL** pour recevoir un e-mail de confirmation.
6. Cliquez sur le bouton **SUPPRIMER COMPTE** dans l'e-mail que nous vous avons envoyé.

Une nouvelle fenêtre apparaît.

7. Confirmez votre choix.



Note

Une fois que compte Bitdefender est supprimé, tous les abonnements actifs qui s'y rattachent seront automatiquement annulés et les produits en utilisant ses pouvoirs cesseront de fonctionner.



11. ANALYSER AVEC BITDEFENDER

11.1. Comment analyser un fichier ou un dossier ?

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

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


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

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

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

11.2. Comment analyser mon système ?

Pour réaliser une analyse complète sur le système :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **ANTIVIRUS**, sélectionnez **Analyse système**.
4. Suivez les indications de l'Assistant d'analyse système pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés.


Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 106).



11.3. Comment programmer une analyse ?

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

Pour programmer une analyse :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **ANTIVIRUS**, sélectionnez **Gérer analyses**.
4. Choisissez le type d'analyse que vous souhaitez programmer, Analyse système ou Analyse rapide, puis cliquez sur **Options Analyse**.

Alternativement, vous pouvez créer un type d'analyse qui correspond à vos besoins en cliquant sur **Nouvelle tâche personnalisée**.

5. Activer le bouton **Programme**.

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


- Au démarrage du système
- Une fois
- Périodiquement

Dans la fenêtre **Cibles analyse** vous pouvez choisir les localisations que vous souhaitez analyser.

11.4. Comment créer une tâche d'analyse personnalisée ?

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

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.



3. Sous le module **ANTIVIRUS**, sélectionnez **Gérer analyses**.
4. Cliquez sur **Nouvelle tâche personnalisée**. Saisissez un nom pour l'analyse dans l'onglet **Standard** et sélectionnez les emplacements à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**.

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

Vous pouvez également choisir d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée. N'oubliez pas qu'il s'agira du comportement par défaut à chaque fois que vous exécuterez cette tâche.

6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
7. Utilisez le bouton correspondant si vous souhaitez définir une planification pour cette tâche d'analyse.
8. Cliquez sur **Démarrer l'analyse** et suivez l'**Assistant d'analyse** pour terminer l'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
9. Si vous le souhaitez, vous pouvez relancer rapidement une analyse personnalisée en cliquant sur le bouton correspondant dans la liste.

11.5. Comment exclure un dossier de l'analyse ?



Bitdefender vous permet d'exclure de l'analyse certains fichiers, dossiers ou extensions de fichiers.

Les exclusions doivent être employées par des utilisateurs ayant un niveau avancé en informatique et uniquement dans les situations suivantes :

- Vous avez un dossier important sur votre système où se trouvent des films et de la musique.
- Vous avez une archive importante sur votre système où se trouvent différentes données.
- Vous gardez un dossier où vous installez différents types de logiciels et applications à des fins de test. L'analyse du dossier peut conduire à la perte de certaines données.



Pour ajouter un dossier à la liste d'exclusions :



1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Sélectionnez l'onglet **Exclusions**.
5. Cliquez sur le menu déroulant **Liste des fichiers et dossiers exclus de l'Analyse**.
6. Cliquez sur le bouton **AJOUTER**.
7. Cliquez sur **Parcourir**, sélectionnez le dossier à exclure de l'analyse, puis cliquez sur **OK**.
8. Cliquez sur **Ajouter** pour sauvegarder les modifications et fermez la fenêtre.



11.6. Que faire lorsque Bitdefender a détecté un fichier sain comme infecté ?

Il arrive parfois que Bitdefender indique par erreur qu'un fichier légitime est une menace (une fausse alerte). Pour corriger cette erreur, ajoutez le fichier à la zone des exclusions de Bitdefender :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
 - a. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
 - b. Sélectionnez le lien **VOIR MODULES**.
 - c. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
 - d. Dans l'onglet **Bouclier**, cliquez sur le bouton correspondant pour activer ou désactiver l'Analyse à l'accès.

Une fenêtre d'avertissement s'affiche. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactiver la protection en temps-réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.



2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 88).
3. Restaurer le fichier à partir de la zone de quarantaine :
 - a. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
 - b. Sélectionnez le lien **VOIR MODULES**.
 - c. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
 - d. Sélectionnez l'onglet **Quarantaine**.
 - e. Sélectionnez le fichier puis cliquez sur **Restaurer**.
4. Ajouter le fichier à la liste d'exceptions. Pour savoir comment faire cela, consultez « *Comment exclure un dossier de l'analyse ?* » (p. 68).
5. Activez la protection antivirus en temps réel de Bitdefender.
6. Contactez les représentants de notre soutien technique afin que nous puissions supprimer la signature de détection. Pour savoir comment faire cela, consultez « *Assistance* » (p. 244).


11.7. Comment connaître les virus détectés par Bitdefender ?

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

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

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

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.



2. Dans l'onglet **Tous**, sélectionnez la notification concernant la dernière analyse.

Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.

3. Dans la liste des notifications, vous pouvez consulter les analyses ayant été réalisées récemment. Cliquez sur une notification pour afficher des informations à son sujet.
4. Pour ouvrir un journal d'analyse, cliquez sur **Afficher le journal**.




12. PARENTAL ADVISOR

12.1. Comment protéger mes enfants des menaces sur Internet ?

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

Pour configurer Contrôle parental :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.

2. Cliquez sur le bouton d'action **Contrôle parental**.

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

3. Le tableau de bord du Contrôle parental s'ouvre. Vous pouvez consulter et configurer ici les paramètres du Contrôle parental.

4. Cliquez sur **AJOUTER PROFIL** sur le côté droit de la fenêtre **Mes enfants**

5. Configurez des informations spécifiques dans les champs correspondants, telles que : nom, sexe et date de naissance, puis cliquez sur **CONTINUER**.

Basée sur les standards de développement des enfants, la configuration de la date de naissance de l'enfant charge automatiquement les spécificités considérées comme appropriées pour sa catégorie d'âge.

6. Si l'appareil de votre enfant contient déjà Bitdefender Total Security 2017, sélectionnez son appareil à partir de la liste disponible, puis cliquez sur **CONTINUER**.

Si l'appareil de votre enfant n'a pas de produit Bitdefender contenant les fonctionnalités de Contrôle parental, cliquez sur **Ajouter un nouvel appareil**. Sélectionnez le système d'exploitation de son appareil, puis cliquez sur **CONTINUER**.

Saisissez l'adresse e-mail sur laquelle nous devons envoyer le lien d'installation de l'application Bitdefender Contrôle parental.

Sur les appareils Windows, le Bitdefender Total Security 2017 que vous avez inclus dans votre abonnement doit être téléchargé et installé. Sur



les appareils Android, l'agent Contrôle parental de Bitdefender doit être téléchargé et installé.

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

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

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

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

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

12.3. Comment empêcher mon enfant de jouer à un jeu ?

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

Pour bloquer l'accès à un jeu :

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



2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle parental** pour accéder au tableau de bord.
4. Sélectionnez le profil de votre enfant à partir de la fenêtre **Mes enfants**.
5. Sélectionnez l'onglet **Activités**.

Une liste avec des cartes s'affiche. Les cartes représentent les applications utilisées par votre enfant.


6. Sélectionnez la carte avec l'application que vous ne voulez plus que votre enfant utilise.

Le symbole qui apparaît indique que votre enfant ne pourra plus utiliser cette application.

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

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

Pour bloquer un contact spécifique :

1. Allez à : <https://central.bitdefender.com>.
2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle parental** pour accéder au tableau de bord.
4. Cliquez sur l'icône  sur la carte profil souhaitée, puis sélectionnez **Éditer**.
5. Saisissez le numéro de votre enfant dans le champ correspondant, puis cliquez sur **SAUVEGARDER**.
6. Sélectionnez le profil de l'enfant que vous souhaitez limiter.
7. Sélectionnez l'onglet **Amis**.

Une liste avec des cartes s'affiche. Les cartes représentent les contacts provenant du téléphone de votre enfant.



8. Sélectionnez la carte avec le numéro de téléphone que vous souhaitez bloquer.

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

Pour bloquer les numéros de téléphone inconnus, activez l'interrupteur **Ne bloquer aucune interaction avec ID appelant**.

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

Le Contrôle parental de Bitdefender vous permet de configurer une localisation aussi sécurisée ou limitée pour votre enfant.

Pour configurer un emplacement :


1. Allez à : <https://central.bitdefender.com>.
2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Cliquez sur **Contrôle parental** pour accéder au tableau de bord.
4. Sélectionnez le profil de votre enfant à partir de la fenêtre **Mes enfants**.
5. Sélectionnez l'onglet **Lieux**.
6. Cliquez sur **Appareils** dans le cadre qui se trouve dans la fenêtre **Lieux**.
7. Cliquez sur **CHOISIR APPAREILS** puis sélectionnez l'appareil que vous souhaitez configurer.
8. Dans la fenêtre **Zones**, cliquez sur le bouton **AJOUTER ZONE**.
9. Choisissez le type de lieu, **Sécurisé** ou **Limité**.
10. Saisissez un nom valide pour la zone où votre enfant a la permission d'aller ou non.
11. Configurez la portée qui devrait être appliquée pour la surveillance à partir du curseur **Rayon**.
- 12 Cliquez sur **AJOUTER ZONE** pour sauvegarder vos configurations.

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



12.6. Comment supprimer un profil enfant

Si vous souhaitez supprimer un profil enfant existant :

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





13. PROTECTION DE LA VIE PRIVÉE

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

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

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

Pour garder vos activités en ligne privées et en sécurité :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface Bitdefender.
2. Cliquez sur le bouton d'action **Safepay**.
3. Cliquez sur le bouton  pour accéder au **Clavier virtuel**.

Utilisez le **Clavier virtuel** lorsque vous tapez des informations confidentielles telles que des mots de passe.

13.2. Que faire si mon périphérique a été volé ?

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




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

Pour accéder aux fonctionnalités antivol à partir de votre compte :

1. Accéder à **Bitdefender Central**.
2. Sélectionnez la section **Mes Appareils**.
3. Dans la fenêtre **Mes Appareils**, sélectionnez l'appareil qui pose problème.
4. Cliquez sur **Antivol**.



5. Sélectionnez la fonctionnalité que vous souhaitez utiliser :

- **LOCALISER** - permet d'afficher la localisation de votre appareil sur Google Maps.
-  **Alerte** - envoyer une alerte sur l'appareil.
-  **Verrouiller** - permet de verrouiller votre ordinateur et de spécifier un code NIP numérique pour le déverrouiller. Vous pouvez également activer l'option correspondante pour permettre à Bitdefender pour prendre des clichés de la personne qui tente d'accéder à votre appareil.
-  **Effacer** - permet d'effacer toutes les données de votre ordinateur.



Important

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

- **Afficher IP** - affiche la dernière adresse IP pour l'appareil sélectionné.

13.3. Comment utiliser les coffres-forts ?

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

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

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

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

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



Une nouvelle fenêtre apparaît. Procédez comme suit :

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



Note

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

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

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

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

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

● Maintenez toujours le coffre-fort verrouillé.

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



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

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

Pour plus d'informations sur l'utilisation des coffres-forts, consultez « *Chiffrement de fichiers* » (p. 134).

13.4. Comment supprimer définitivement un fichier avec Bitdefender ?

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

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

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement, pointez sur Bitdefender et sélectionnez **Destructeur de fichiers**.
2. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour lancer l'assistant du destructeur de fichiers.
3. Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
4. Les résultats sont affichés. Cliquez sur **Fermer** pour quitter l'assistant.



14. OUTILS D'OPTIMISATION

14.1. Comment améliorer les performances de mon système ?

Les performances système dépendent entre autres de la configuration matérielle, comme la charge du processeur, l'utilisation de la mémoire et l'espace sur le disque dur. Il est aussi lié directement à votre configuration logicielle et à la gestion de vos données.


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

- « *Optimisez les performances de votre système d'un simple clic* » (p. 81)
- « *Analysez votre système régulièrement* » (p. 81)

14.1.1. Optimisez les performances de votre système d'un simple clic

L'option Optimisation en 1 clic vous permet d'améliorer rapidement les performances de votre système en analysant, détectant et supprimant les fichiers inutiles.

Pour commencer le processus d'Optimisation en 1 clic :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le bouton d'action **Optimisation en 1 clic**.
3. Laissez Bitdefender rechercher les fichiers qui peuvent être supprimés puis cliquez sur le bouton **Optimiser** pour terminer le processus.

Pour plus d'informations sur comment améliorer la vitesse de votre ordinateur d'un simple clic, veuillez vous reporter à « *Optimisation de la vitesse de votre système d'un simple clic* » (p. 193).

14.1.2. Analysez votre système régulièrement


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



Veillez à analyser votre système régulièrement, au moins une fois par semaine.

Il est recommandé d'utiliser l'analyse du système car elle recherche tous les types de malwares menaçant la sécurité de votre système et analyse également l'intérieur des archives.


Pour commencer l'Analyse système :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **ANTIVIRUS**, sélectionnez **Analyse système**.
4. Suivez les étapes de l'assistant.

14.2. Comment puis-je améliorer le temps de démarrage de mon système ?

Les applications inutiles qui ralentissent le démarrage du système lorsque vous allumez votre PC peuvent être désactivées ou ouvertes ultérieurement avec l'Optimisation du démarrage ce qui vous fait gagner un temps précieux.

Pour utiliser l'Optimisation démarrage :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le bouton d'action **Optimisation démarrage**.
3. Sélectionnez les applications dont vous souhaitez reporter le lancement au démarrage du système.

Pour plus d'informations sur la manière d'optimiser le temps de démarrage de votre PC, reportez-vous à « *Optimisation du temps de démarrage de votre PC* » (p. 194).



15. INFORMATIONS UTILES

15.1. Comment tester ma solution antivirus ?

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

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

Pour tester votre solution antivirus :

1. Téléchargez le test à partir de la page Web officielle de l'organisme EICAR <http://www.eicar.org/>.
2. Cliquez sur l'onglet **Anti-Malware Testfile**.
3. Cliquez sur **Télécharger** dans le menu de gauche.
4. Dans **zone de téléchargement utilisant le protocole HTTP standard** cliquez sur le fichier de test **eicar.com**.
5. Vous serez informé que la page à laquelle vous essayez d'accéder contient « EICAR-Test-File (not a virus) ».

Si vous cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**, le téléchargement du test débutera et une fenêtre pop-up de Bitdefender vous indiquera qu'un virus a été détecté.

Cliquez sur **Plus de détails** pour obtenir plus d'informations sur cette action.

Si vous ne recevez pas d'alerte Bitdefender, nous vous recommandons de contacter Bitdefender pour obtenir de l'aide comme indiqué dans la section « *Assistance* » (p. 244).

15.2. Comment désinstaller Bitdefender ?

Si vous souhaitez supprimer votre Bitdefender Total Security 2017 :

● Dans **Windows 7** :

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
2. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.



3. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
4. Cliquez sur **CONTINUER**.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Dans **Windows 8 et Windows 8.1** :
 1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
 2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
 3. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 4. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 5. Cliquez sur **CONTINUER**.
 6. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Dans **Windows 10** :
 1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
 2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
 3. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
 5. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :



- Fichiers en quarantaine
- Wallets
- Coffres-forts

6. Cliquez sur **CONTINUER**.

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


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

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

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

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

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **ANTIVIRUS**, sélectionnez **Gérer analyses**.
4. Dans la fenêtre **Gérer les tâches d'analyse**, cliquez sur **Nouvelle tâche personnalisée** pour saisir un nom pour l'analyse et sélectionnez les emplacements à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**.
6. Choisissez d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.



8. Cliquez sur le bouton **Démarrer analyse** pour analyser votre système.

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

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, reportez-vous à « *Assistant d'analyse antivirus* » (p. 106).


15.4. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?

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

Important

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

Pour gérer les paramètres du proxy :

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Avancé**.
3. Activez l'utilisation du proxy en cliquant sur le bouton.
4. Cliquez sur le lien **Gérer proxy**.
5. Deux options permettent de définir les paramètres du proxy :
 - **Importer les paramètres proxy à partir du navigateur par défaut** - paramètres du proxy de l'utilisateur actuel provenant du navigateur par défaut. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.

Note

Bitdefender peut importer les paramètres proxy des principaux navigateurs, y compris des dernières versions d'Internet Explorer, de Mozilla Firefox et de Google Chrome.



- **Paramètres proxy personnalisés** - paramètres proxy que vous pouvez configurer vous-même. Voici les paramètres à spécifier:
 - **Adresse** - saisissez l'adresse IP du serveur proxy.
 - **Port** - saisissez le port utilisé par Bitdefender pour se connecter au serveur proxy.
 - **Nom d'utilisateur** - entrez le nom d'utilisateur reconnu par le serveur proxy.
 - **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.

6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre. Bitdefender utilisera les paramètres proxy disponibles jusqu'à ce qu'il parvienne à se connecter à Internet.

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

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

- Dans **Windows 7** :
 1. Cliquez sur **Démarrer**.
 2. Repérez **Ordinateur** dans le menu **Démarrer**.
 3. Faites un clic droit sur **Ordinateur** et sélectionnez **Propriétés**.
 4. Consultez ce qui est indiqué sous **Système** afin de vérifier les informations concernant votre système.
- Dans **Windows 8** :
 1. Dans l'écran d'accueil Windows, localisez l'**Ordinateur** (vous pouvez, par exemple, taper « Ordinateur » directement dans l'écran d'accueil), puis faites un clic droit sur son icône.
Dans **Windows 8.1**, localisez **Ce PC**.
 2. Sélectionnez **Propriétés** dans le menu inférieur.
 3. Regardez sous **Système** pour connaître le type de système.
- Dans **Windows 10** :
 1. Tapez "Système" dans le champ de recherche de la barre des tâches et cliquez sur son icône.



2. Regardez sous **Système** pour connaître le type de système.

15.6. Comment afficher des objets cachés dans Windows ?

Ces étapes sont utiles en cas de malwares, si vous avez besoin de détecter et de supprimer les fichiers infectés, qui peuvent être cachés.

Suivez ces étapes pour afficher les objets cachés dans Windows :

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration**.

Dans **Windows 8 et Windows 8.1** : Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil), puis cliquez sur son icône.

2. Sélectionnez **Options des dossiers**.
3. Allez dans l'onglet **Afficher**.
4. Sélectionnez **Afficher les fichiers et les dossiers cachés**.
5. Décochez **Masquer les extensions des fichiers dont le type est connu**.
6. Décochez **Masquer les fichiers protégés du système d'exploitation**.
7. Cliquez sur **Appliquer** puis sur **OK**.

Dans **Windows 10** :

1. Tapez "Afficher les fichiers et les dossiers cachés" dans le champ de recherche de la barre des tâches puis cliquez sur son icône.
2. Sélectionnez **Afficher les fichiers et les dossiers cachés**.
3. Décochez **Masquer les extensions des fichiers dont le type est connu**.
4. Décochez **Masquer les fichiers protégés du système d'exploitation**.
5. Cliquez sur **Appliquer** puis sur **OK**.

15.7. Comment supprimer les autres solutions de sécurité ?

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



Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, le système devient instable. Le programme de désinstallation de Bitdefender Total Security 2017 détecte d'autres programmes de sécurité et vous permet de les désinstaller.

Si vous n'avez pas supprimé les autres solutions de sécurité au cours de l'installation initiale :

● Dans **Windows 7** :

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
2. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
3. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
4. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

● Dans **Windows 8 et Windows 8.1** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
4. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

● Dans **Windows 10** :

1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
3. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.



4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

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

15.8. Comment redémarrer en mode sans échec ?

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

Pour démarrer Windows en mode sans échec :

● Dans **Windows 7** :

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

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

1. Exécutez **Configuration système** dans Windows en appuyant simultanément sur les touches **Windows + R** de votre clavier.
2. Tapez **msconfig** dans la boîte de dialogue **Ouvrir** puis cliquez sur **OK**.



3. Sélectionnez l'onglet **Démarrage**.
4. Dans la zone **Options de démarrage**, cochez la case **Démarrage sécurisé**
5. Cliquez sur **Réseau** puis **OK**.
6. Cliquez sur **OK** dans la fenêtre **Configuration système** qui vous informe que le système doit être redémarré pour pouvoir faire les changements que vous souhaitez.

Votre système redémarre en mode sécurisé avec le réseau.

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



GÉRER VOTRE SÉCURITÉ



16. PROTECTION ANTIVIRUS

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

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

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



Important

Pour empêcher l'infection de votre ordinateur par des virus, maintenez l'**analyse à l'accès** activée.

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

Bitdefender analyse automatiquement tout support amovible connecté à l'ordinateur afin de s'assurer que son accès ne pose pas de problème de sécurité. Pour plus d'informations, reportez-vous à « **Analyse automatique de supports amovibles** » (p. 110).

Les utilisateurs avancés peuvent configurer des exceptions d'analyse s'ils ne souhaitent pas que certains fichiers ou types de fichiers soient analysés. Pour plus d'informations, reportez-vous à « **Configurer des exceptions d'analyse** » (p. 112).

Lorsqu'il détecte un virus ou un autre logiciel malveillant, Bitdefender tente automatiquement de supprimer le code malveillant du fichier infecté et de reconstruire le fichier d'origine. Cette opération est appelée désinfection. Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Pour plus d'informations, reportez-vous à « **Gérer les fichiers en quarantaine** » (p. 115).

Si votre ordinateur a été infecté par des logiciels malveillants, veuillez consulter « **Suppression des malwares de votre système** » (p. 234). Pour vous aider à supprimer les logiciels malveillants qui ne peuvent pas l'être à partir



du système d'exploitation Windows, Bitdefender vous fournit le **Mode de secours**. Il s'agit d'un environnement de confiance, spécialement conçu pour la suppression de logiciels malveillants, qui vous permet de faire redémarrer votre ordinateur indépendamment de Windows. Lorsque l'ordinateur s'exécute en Mode de secours, les logiciels malveillants Windows sont inactifs, ce qui rend leur suppression facile.

Pour vous protéger contre les ransomwares et les applications malveillantes inconnues, Bitdefender utilise Active Threat Control, une technologie heuristique avancée, qui surveille en permanence les applications en cours d'exécution sur votre système. Active Threat Control bloque automatiquement les applications ayant un comportement similaire à celui des malwares afin de les empêcher d'endommager votre ordinateur. Des applications légitimes sont parfois bloquées. Vous pouvez dans ce cas configurer Active Threat Control afin qu'il ne bloque plus ces applications en créant des règles d'exclusion. Pour en savoir plus, consultez « *Active Threat Control* » (p. 116).



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

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

Le réglage par défaut de la protection en temps réel assure un bon niveau de protection contre les logiciels malveillants, avec un impact minimal sur les performances système. Vous pouvez facilement modifier les paramètres de la protection en temps réel selon vos besoins en choisissant un des niveaux de protection prédéfinis. Si vous êtes un utilisateur avancé, vous pouvez également configurer les paramètres d'analyse en détail en créant un niveau de protection personnalisé.

16.1.1. Activer ou désactiver la protection en temps réel

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.



4. Dans la fenêtre **Bouclier**, cliquez sur le bouton correspondant pour activer ou désactiver l'Analyse à l'accès.
5. Si vous tentez de désactiver la protection en temps réel, une fenêtre d'avertissement apparaît. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactiver la protection en temps- réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système. La protection en temps réel sera automatiquement activée lorsque la durée sélectionnée expirera.





Avertissement

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

16.1.2. Régler le niveau de protection en temps réel

Le niveau de protection en temps réel détermine les paramètres d'analyse pour la protection en temps réel. Vous pouvez facilement modifier les paramètres de la protection en temps réel selon vos besoins en choisissant un des niveaux de protection prédéfinis.

Pour régler le niveau de protection en temps réel :



1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Dans la fenêtre **Bouclier** déplacez le curseur sur l'échelle pour choisir le niveau de protection souhaité. Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.



16.1.3. Configurer les paramètres de protection en temps réel

Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Bitdefender. Vous pouvez configurer les paramètres de protection en temps réel en détail en créant un niveau de protection personnalisé.

Pour configurer les paramètres de protection en temps réel :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Faites glisser **Analyse à l'accès** au niveau **PERSONNALISÉ**.
Une nouvelle fenêtre apparaît.
5. Configurez les paramètres d'analyse selon vos besoins.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiarisé avec certains des termes, consultez le **glossaire**. Vous pouvez également rechercher des informations sur Internet.
- **Options d'analyse à l'accès des fichiers**. Vous pouvez régler Bitdefender pour analyser tous les types de fichiers auxquels vous accédez ou uniquement les applications (fichiers programmes). L'analyse de tous les fichiers accédés offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour obtenir de meilleures performances du système.

Par défaut, les dossiers locaux et les partages réseau sont sujets à l'analyse à l'accès. Pour de meilleures performances du système, vous pouvez exclure certains emplacements du réseau de l'analyse à l'accès.

Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques que les autres types de fichiers. Cette catégorie comprend les extensions de fichiers suivantes :



386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analyser le contenu compressé.** L'analyse des fichiers compressés est un processus lent et consommant beaucoup de ressources, qui n'est donc pas recommandé pour une protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée.

Si vous décidez d'utiliser cette option, vous pouvez définir une limite de taille pour les archives à analyser à l'accès. Cochez la case correspondante et tapez la taille maximale des archives (en Mo).

- **Options d'analyse pour les trafics e-mails et HTTP.** Afin d'éviter que des malwares soient téléchargés sur votre ordinateur, Bitdefender analyse automatiquement les points d'entrée des logiciels malveillants suivants :

- courriels entrants et sortants
- Trafic HTTP

L'analyse du trafic Web peut ralentir un peu la navigation sur Internet, mais elle bloquera les logiciels malveillants provenant d'Internet, y compris les téléchargements de type "drive-by".

Bien que ce ne soit pas recommandé, vous pouvez désactiver l'analyse antivirus de messagerie ou web pour améliorer les performances du système. Si vous désactivez les options d'analyse correspondantes, les courriels et les fichiers reçus ou téléchargés sur Internet ne seront pas analysés, ce qui permettra aux fichiers infectés d'être enregistrés sur votre ordinateur. Il ne s'agit pas d'une menace critique, car la protection en





temps réel bloquera le malware lorsque vous tenterez d'accéder (ouvrir, déplacer, copier ou exécuter) aux fichiers infectés.

- **Analyser les secteurs d'amorçage.** Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
- **Analyser que les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Analyse des enregistreurs de frappe.** Sélectionnez cette option pour analyser la présence d'enregistreurs de frappe sur votre système. Les enregistreurs de frappe enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur Internet à une personne malveillante (un pirate informatique). Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.
- **Analyser au redémarrage.** Sélectionnez l'option d'analyse **Early boot** pour analyser votre système au démarrage dès que tous ses services critiques ont été téléchargés. La mission de cette fonctionnalité est d'améliorer la détection des virus au démarrage et redémarrage de votre système.

Actions appliquées à l'encontre des logiciels malveillants détectés

Vous pouvez configurer les actions appliquées par la protection en temps réel.

Pour configurer les actions :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Faites glisser **Analyse à l'accès** au niveau **PERSONNALISÉ**.

Une nouvelle fenêtre apparaît.



5. Sélectionnez l'onglet **Actions** et configurez les options d'analyse comme souhaité.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

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

Action automatique

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

- **Fichier(s) infecté(s)**. Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la base de données de signatures de codes malveillants Bitdefender. Bitdefender tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer le fichier d'origine. Cette opération est appelée désinfection.

Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 115).



Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Fichier(s) suspect(s)**. Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter une infection potentielle.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Archives contenant des fichiers infectés.**



- Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.
- Si une archive contient à la fois des fichiers infectés et des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Déplacer en quarantaine

Déplace les fichiers détectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 115).



Refuser l'accès

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

16.1.4. Restauration des paramètres par défaut

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

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Faites glisser **Analyse à l'accès** au niveau **NORMAL**.

16.2. Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre PC sans virus. Cela s'effectue en protégeant votre ordinateur des nouveaux virus par l'analyse des courriels que vous recevez et des nouveaux fichiers que vous téléchargez ou copiez sur votre système.

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de Bitdefender. C'est pourquoi il est prudent



d'analyser votre ordinateur après l'installation de Bitdefender. Et il est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

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


16.2.1. Rechercher des logiciels malveillants dans un fichier ou un dossier

Il est conseillé d'analyser les fichiers et les dossiers chaque fois que vous soupçonnez qu'ils peuvent être infectés. Faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser, pointez sur **Bitdefender** et sélectionnez **Analyser avec Bitdefender**. L'**Assistant d'analyse antivirus** s'affichera et vous guidera au cours du processus d'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.


16.2.2. Exécuter une analyse rapide

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

Pour démarrer une analyse rapide :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'**interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **ANTIVIRUS**, sélectionnez **Analyse Rapide**.
4. Suivez les indications de l'**Assistant d'analyse antivirus** pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.



Ou plus rapide, cliquez sur l'icône  dans la barre de gauche de l'**interface Bitdefender**, puis cliquez sur le bouton d'action **Analyse rapide**.

16.2.3. Exécuter une analyse du système

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



Note


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

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

- Vérifiez que Bitdefender dispose de signatures à jour. Analyser votre ordinateur en utilisant une base de données de signatures non à jour peut empêcher Bitdefender de détecter les logiciels malveillants identifiés depuis la mise à jour précédente. Pour plus d'informations, reportez-vous à « *Maintenir Bitdefender à jour* » (p. 46).
- Fermez tous les programmes ouverts.

Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée. Pour plus d'informations, reportez-vous à « *Configurer une analyse personnalisée* » (p. 103).


Pour exécuter une analyse système :

1. Cliquez sur  l'icône dans le coin en bas à gauche de l'**interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **ANTIVIRUS**, sélectionnez **Analyse système**.
4. Suivez les indications de l'**Assistant d'analyse antivirus** pour terminer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.



16.2.4. Configurer une analyse personnalisée

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **ANTIVIRUS**, sélectionnez **Gérer analyses**.
4. Cliquez sur le bouton **Nouvelle tâche personnalisée**. Saisissez un nom pour l'analyse dans l'onglet **Standard** et sélectionnez les emplacements à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**. Une nouvelle fenêtre apparaît. Suivez ces étapes :

- a. Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour choisir le niveau d'analyse souhaité. Reportez-vous à la description à droite de l'échelle pour identifier le niveau d'analyse le plus adapté à vos besoins.

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

- b. Vous pouvez aussi configurer ces options générales :

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

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

6. Si vous souhaitez paramétrer une heure pour votre tâche d'analyse, utilisez le bouton **Horaires** dans la fenêtre **Basique**. Sélectionnez l'une des options correspondantes pour définir une planification :

- Au démarrage du système



- Une fois
 - Périodiquement
7. Cliquez sur **Démarrer l'analyse** et suivez l'**Assistant d'analyse antivirus** pour terminer l'analyse. En fonction des emplacements à analyser, l'analyse peut prendre quelque temps. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
 8. Si vous le souhaitez, vous pouvez relancer rapidement une analyse personnalisée en cliquant sur le bouton correspondant dans la liste.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

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

Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques que les autres types de fichiers. Cette catégorie comprend les extensions de fichiers suivantes : 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fpx; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

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



votre système. Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.



Note

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

- **Analyser les secteurs d'amorçage.** Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
- **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.
- **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.
- **Analyser les témoins.** Sélectionnez cette option pour analyser les témoins stockés par les navigateurs sur votre ordinateur.
- **Analyser que les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Ignorer les enregistreurs de frappe commerciaux.** Sélectionnez cette option si vous avez installé et utilisez un keylogger commercial sur votre ordinateur. Les enregistreurs de frappe commerciaux sont des logiciels de surveillance légitimes dont la fonction principale consiste à enregistrer tout ce qui est tapé au clavier.
- **Rechercher les rootkits.** Sélectionnez cette option pour rechercher des **rootkits** et des objets cachés à l'aide de ce logiciel.



16.2.5. Assistant d'analyse antivirus

À chaque fois que vous lancerez une analyse à la demande (par exemple en faisant un clic droit sur un dossier, en pointant sur Bitdefender et en sélectionnant **Analyser avec Bitdefender**), l'assistant de l'analyse antivirus Bitdefender s'affichera. Suivez l'assistant pour terminer le processus d'analyse.



Note

Si l'assistant d'analyse ne s'affiche pas, il est possible que l'analyse soit paramétrée pour s'exécuter invisiblement, en tâche de fond. Recherchez l'icône de l'avancement de l'analyse **B** dans la **zone de notification**. Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Étape 1 - Effectuer l'analyse

Bitdefender commence à analyser les objets sélectionnés. Vous pouvez voir des informations en temps réel sur l'état et les statistiques de l'analyse (y compris le temps écoulé, une estimation du temps restant et le nombre de menaces détectées).

Patientez jusqu'à ce que Bitdefender ait terminé l'analyse. L'analyse peut durer un certain temps, suivant sa complexité.

Arrêt ou pause de l'analyse. Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Arrêter**. Vous vous retrouverez alors à la dernière étape de l'assistant. Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

Archives protégées par mot de passe. Lorsqu'une archive protégée par mot de passe est détectée, en fonction des paramètres de l'analyse, on peut vous demander d'indiquer son mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe. Voici les options proposées :

- **Mot de passe.** Si vous souhaitez que Bitdefender analyse l'archive, sélectionnez cette option et entrez le mot de passe. Si vous ne connaissez pas le mot de passe, choisissez l'une des autres options.
- **Ne pas demander le mot de passe et ne pas analyser cet objet.** Sélectionnez cette option pour ne pas analyser cette archive.



- **Ne pas analyser les éléments protégés par mot de passe.** Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe. Bitdefender ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

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

Étape 2 - Sélectionner des actions

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

Note

Si vous lancez une analyse rapide ou une analyse système, Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés pendant l'analyse. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

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

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

Action automatique

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

- **Fichier(s) infecté(s).** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la base de données de signatures de codes malveillants Bitdefender. Bitdefender tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer le fichier d'origine. Cette opération est appelée désinfection.

Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Pour plus d'informations, reportez-vous à « *Gérer les fichiers en quarantaine* » (p. 115).



Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Fichier(s) suspect(s).** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter une infection potentielle.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Archives contenant des fichiers infectés.**

- Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.
- Si une archive contient à la fois des fichiers infectés et des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Supprimer

Supprime du disque les fichiers détectés.

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

Ne rien faire

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

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



Étape 3 - Récapitulatif

Une fois que les problèmes de sécurité auront été corrigés par Bitdefender, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre. Si vous souhaitez consulter des informations complètes sur le processus d'analyse, cliquez sur **Afficher journal** pour afficher le journal d'analyse.

Cliquez sur **Fermer** pour fermer la fenêtre.



Important


Dans la plupart des cas, Bitdefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte. Il y a toutefois des problèmes qui ne peuvent pas être résolus automatiquement. Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation. Pour plus d'informations et d'instructions sur la méthode permettant de supprimer des malwares manuellement, reportez-vous à « *Suppression des malwares de votre système* » (p. 234).

16.2.6. Consulter les journaux d'analyse

À chaque fois qu'une analyse est effectuée, un journal d'analyse est créé et Bitdefender enregistre les problèmes détectés dans la fenêtre Antivirus. Le rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises à l'encontre de ces menaces.

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

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant la dernière analyse.

Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.



3. Dans la liste des notifications, vous pouvez consulter les analyses ayant été réalisées récemment. Cliquez sur une notification pour afficher des informations à son sujet.
4. Pour ouvrir le journal d'analyse, cliquez sur **VOIR JOURNAL**.

16.3. Analyse automatique de supports amovibles

Bitdefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre ordinateur et l'analyse en tâche de fond. Ceci est recommandé afin d'empêcher que des virus ou autres malwares n'infectent votre ordinateur.

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

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

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

16.3.1. Comment cela fonctionne-t-il ?

Lorsqu'il détecte un périphérique de stockage amovible, Bitdefender commence à l'analyser en tâche de fond à la recherche de malwares (à condition que l'analyse automatique soit activée pour ce type de périphérique). Une icône d'analyse de Bitdefender **B** apparaîtra dans la **zone de notification**. Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Si la fonction Autopilot est activée, vous n'aurez pas à vous soucier de l'analyse. L'analyse sera seulement enregistrée et des informations à son sujet seront disponibles dans la fenêtre **Notifications**.

Si Autopilot est désactivé :

1. Vous serez averti via une fenêtre contextuelle qu'un nouveau périphérique a été détecté et est en cours d'analyse.
2. Dans la plupart des cas, Bitdefender supprime automatiquement les malwares détectés ou isole les fichiers infectés en quarantaine. S'il y a



des menaces non résolues après l'analyse, on vous demandera de choisir les actions à appliquer.



Note

Veillez prendre en compte le fait qu'aucune mesure ne sera prise à l'encontre des fichiers infectés ou suspects détectés sur des CD ou DVD. De plus, aucune action ne sera appliquée à l'encontre des fichiers suspects détectés sur des lecteurs mappés du réseau si vous ne disposez pas des privilèges appropriés.

3. Lorsque l'analyse est terminée, la fenêtre des résultats de l'analyse s'affiche afin de vous informer si vous pouvez accéder aux fichiers en toute sécurité sur le support amovible.



Ces informations peuvent vous être utiles :

- Soyez prudent lorsque vous utilisez un CD ou DVD infecté par des malwares, car ces malwares ne peuvent pas être supprimés du disque (le support est en lecture seule). Vérifiez que la protection en temps réel est activée pour empêcher la diffusion de malwares sur votre système. Il est recommandé de copier toutes les données essentielles du disque sur le système avant de se séparer du disque.
- Bitdefender n'est parfois pas en mesure de supprimer les malwares de certains fichiers en raison de contraintes légales ou techniques. C'est le cas par exemple des fichiers archivés à l'aide d'une technologie propriétaire (car l'archive ne peut pas être recréée correctement).

Pour savoir comment traiter les malwares, reportez-vous à « *Suppression des malwares de votre système* » (p. 234).

16.3.2. Gérer l'analyse des supports amovibles

Pour gérer l'Analyse automatique de supports amovibles :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Sélectionnez l'onglet **Pilotes et Appareils**.




Pour une meilleure protection, nous vous recommandons d'activer l'analyse automatique de tous les types de périphériques de stockage amovibles.

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

16.4. Analyse du fichier hosts

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

Pour configurer l'analyse du fichier d'hôtes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Avancé**.
3. Cliquez sur le bouton correspondant pour activer ou désactiver l'analyse de fichiers d'hôtes.

16.5. Configurer des exceptions d'analyse

Bitdefender vous permet d'exclure de l'analyse certains fichiers, dossiers ou extensions de fichiers. Cette fonctionnalité est conçue pour éviter d'interférer avec votre travail et peut également contribuer à améliorer les performances du système. Les exclusions doivent être employées par des utilisateurs ayant un niveau avancé en informatique ou, sinon, selon les recommandations d'un représentant de Bitdefender.

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





Note

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

16.5.1. Exclure des fichiers et des dossiers de l'Analyse

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Sélectionnez l'onglet **Exclusions**.
5. Cliquez sur le menu déroulant **Liste des fichiers et dossiers exclus de l'Analyse**. La fenêtre qui s'affiche vous permet de gérer les fichiers et dossiers exclus de l'analyse.
6. Ajoutez des exclusions en suivant ces étapes :
 - a. Cliquez sur le bouton **AJOUTER**.
 - b. Cliquez sur **Parcourir**, sélectionnez le fichier ou le dossier à exclure de l'analyse, puis cliquez sur **OK**. Vous pouvez également taper (ou copier-coller) le chemin vers le fichier ou le dossier dans le champ de saisie.
 - c. Par défaut, le fichier ou dossier sélectionné est exclu à la fois de l'analyse à l'accès et à la demande. Pour modifier les conditions d'application de l'exclusion, sélectionnez l'une des autres options.
 - d. Cliquez sur **Ajouter**.

16.5.2. Exclure de l'analyse des extensions de fichiers



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



Important

Soyez prudent lorsque vous excluez de l'analyse des extensions car celles-ci peuvent rendre votre ordinateur vulnérable aux logiciels malveillants.


Pour exclure des extensions de fichier de l'analyse :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Sélectionnez l'onglet **Exclusions**.
5. Cliquez sur le menu déroulant **Liste des extensions exclus de l'Analyse**. La fenêtre qui s'affiche vous permet de gérer les extensions de fichiers exclues de l'analyse.
6. Ajoutez des exclusions en suivant ces étapes :
 - a. Cliquez sur le bouton **AJOUTER**.
 - b. Indiquez les extensions que vous ne souhaitez pas analyser, en les séparant par des points-virgules (;). Voici un exemple :
txt;avi;jpg
 - c. Par défaut, tous les fichiers ayant les extensions indiquées sont exclus à la fois de l'analyse à l'accès et à la demande. Pour modifier les conditions d'application de l'exclusion, sélectionnez l'une des autres options.
 - d. Cliquez sur **Ajouter**.


16.5.3. Gérer les exceptions d'analyse

Si les exceptions d'analyse configurées ne sont plus nécessaires, il est recommandé de les supprimer ou de les désactiver.

Pour gérer des exclusions d'analyse :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.



3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Sélectionnez l'onglet **Exclusions**.
5. Utilisez l'option dans le menu déroulant **Liste de fichiers et dossiers exclus de l'Analyse** pour gérer les exclusions de l'analyse.
6. Pour supprimer ou éditer des exceptions d'analyse, cliquez sur l'un des liens. Procédez comme suit :
 - Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **SUPPRIMER**.
 - Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la et cliquez sur le bouton **MODIFIER**.) Une nouvelle fenêtre apparaît vous permettant de modifier l'extension ou le chemin à exclure et le type d'analyse dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **Modifier**.



16.6. Gérer les fichiers en quarantaine

Bitdefender isole les fichiers infectés par des malwares qu'il ne peut pas désinfecter et les fichiers suspects dans une zone sécurisée nommée quarantaine. Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté, ni être lu.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

Bitdefender analyse également les fichiers en quarantaine après chaque mise à jour de signatures de malware. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Pour consulter et gérer les fichiers en quarantaine :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.



4. Sélectionnez l'onglet **Quarantaine**.
5. Les fichiers en quarantaine sont gérés automatiquement par Bitdefender en fonction des paramètres de quarantaine par défaut. Bien que ce ne soit pas recommandé, vous pouvez régler les paramètres de quarantaine en fonction de vos préférences.

Analyser la quarantaine après la mise à jour des définitions de virus

Maintenez cette option activée pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour des définitions de virus. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Envoyer les fichiers suspects de la quarantaine pour analyse

Maintenez cette option activée pour envoyer automatiquement les fichiers de la quarantaine aux laboratoires de Bitdefender. Les échantillons seront analysés par les spécialistes malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

Supprimer le contenu datant de plus de {30} jours

Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés. Si vous souhaitez modifier ce délai, entrez une nouvelle valeur dans le champ correspondant. Pour désactiver la suppression automatique des fichiers de la quarantaine selon la date, tapez 0.

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

16.7. Active Threat Control

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

Active Threat Control surveille en permanence les applications en cours d'exécution sur l'ordinateur, à la recherche d'actions ressemblant à celles des malwares. Chacune de ces actions est notée et un score global est calculé pour chaque processus. Lorsque la note globale d'un processus




atteint un seuil donné, le processus est considéré comme malveillant et est automatiquement bloqué.

Si la fonction Autopilot est désactivée, vous serez averti via une fenêtre contextuelle sur les ransomwares détectés ou l'application bloquée. Sinon, l'application sera bloquée sans notification. Vous pouvez vérifier les applications détectées par Active Threat Control dans la fenêtre **Notifications**.



16.7.1. Vérifier des applications détectées

Pour vérifier les applications détectées par Active Threat Control :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant l'analyse Active Threat Control.
3. Si vous considérez que l'application est fiable, vous pouvez configurer Active Threat Control afin qu'il ne la bloque plus en cliquant sur **AUTORISER ET SURVEILLER**. Active Threat Control continuera à surveiller les applications exclues. Si les activités suspectes d'une application exclue sont détectées, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

16.7.2. Activer ou désactiver Active Threat Control

Activer ou désactiver Active Threat Control :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Dans la fenêtre **Bouclier**, cliquez sur le bouton correspondant pour activer ou désactiver Active Threat Control.

16.7.3. Régler la protection Active Threat Control

Si vous remarquez qu'Active Threat Control détecte souvent des applications légitimes, optez pour un niveau de protection moins strict.



Pour ajuster la protection Active Threat Control, faites monter ou descendre le curseur sur l'échelle afin de déterminer le niveau de protection désiré.

Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.





Note

Si vous élevez le niveau de protection, Active Threat Control aura besoin de moins de signes de comportements similaires à ceux des malwares pour signaler un processus. Cela conduira au signalement d'un nombre plus important d'applications et, en même temps, à un risque plus élevé de faux positifs (des applications saines détectées comme étant malveillantes).

16.7.4. Gérer les processus exclus

Vous pouvez configurer des règles d'exceptions pour les applications de confiance afin qu'Active Threat Control ne les bloque pas si elles effectuent des actions ressemblant à celles de malwares. Active Threat Control continuera à surveiller les applications exclues. Si les activités suspectes d'une application exclue sont détectées, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

Pour gérer les exclusions du processus Active Threat Control :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Sélectionnez l'onglet **Exclusions**.
5. Cliquez sur le menu déroulant **Liste des processus exclus de l'Analyse**.
Là, vous pouvez gérer les exclusions du processus Active Threat Control.
6. Ajoutez des exclusions en suivant ces étapes :
 - a. Cliquez sur le bouton **AJOUTER**.
 - b. Cliquez sur **Parcourir**, sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.
 - c. Gardez l'option **Autoriser** sélectionnée pour empêcher Active Threat Control de bloquer l'application.



- d. Cliquez sur **Ajouter**.
7. Pour supprimer ou éditer des exclusions, procédez comme suit :
 - Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **EFFACER**.
 - Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la) et cliquez sur le bouton **MODIFIER**. Effectuez les modifications nécessaires, puis cliquez sur **Modifier**.



17. ANTISPAM

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

Bitdefender Antispam utilise des innovations technologiques de pointe et des filtres antispam répondant aux normes industrielles qui permettent d'éliminer les spams avant qu'ils n'atteignent la boîte aux lettres de l'utilisateur. Pour plus d'informations, reportez-vous à « *Aperçu de l'antispam* » (p. 121).

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



Note

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

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

- Dans Microsoft Outlook, les messages de spam sont placés dans le dossier **Spam**, situé dans le dossier **Éléments supprimés**. Le dossier **Spam** est créé lors de l'installation de Bitdefender.
- Dans Mozilla Thunderbird, les messages de spam sont placés dans le dossier **Spam**, situé dans le dossier **Corbeille**. Le dossier **Spam** est créé lors de l'installation de Bitdefender.

Si vous utilisez d'autres clients de messagerie, vous devez créer une règle pour déplacer les e-mails signalés comme étant du [spam] par Bitdefendervers un dossier de quarantaine personnalisé.



17.1. Aperçu de l'antispam

17.1.1. Filtres AntiSpam

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

Liste d'Amis / Liste des Spammeurs

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



Note

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

Filtre jeu de caractères

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

17.1.2. Fonctionnement de l'Antispam

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

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

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



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



Note

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

17.1.3. Clients et protocoles de messagerie pris en charge



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

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

17.2. Activer ou désactiver la protection antispam

La protection Antispam est activée par défaut.

Pour désactiver le module Antispam :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTISPAM**.
4. Cliquez sur le bouton correspondant pour activer ou désactiver **Antispam**.

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

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



! Important

Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 122).

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

⚙️ **Paramètres** - ouvre une fenêtre qui vous permet de configurer les filtres antispam et les paramètres de la barre d'outils.

🗑️ **Spam** - indique que le message sélectionné est un spam. L'e-mail sera immédiatement placé dans le dossier **Spam**. Si les services cloud antispam sont activés, le message est envoyé au Cloud Bitdefender pour une analyse plus approfondie.

📧 **Pas Spam** - indique que l'e-mail sélectionné n'est pas du spam et que Bitdefender ne devrait pas l'avoir signalé comme tel. Cet email sera retiré du dossier **Spam** et placé dans la **Boîte de réception**. Si les services cloud antispam sont activés, le message est envoyé au Cloud Bitdefender pour une analyse plus approfondie.

! Important

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

➕ **Ajouter Spammueur** - ajoute l'expéditeur de l'e-mail sélectionné à la liste des Spammeurs. Il se peut que vous ayez besoin de cliquer sur **OK** pour valider. Les messages provenant d'adresses qui figurent dans la liste de Spammeurs seront automatiquement considérés comme étant du [spam].

➕ **Ajouter Ami** - ajoute l'expéditeur de l'e-mail sélectionné à la liste d'Amis. Il se peut que vous ayez besoin de cliquer sur **OK** pour valider. Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.

➕ **Spammeurs** - ouvre la liste des **Spammeurs** qui contient toutes les adresses e-mail dont vous ne voulez recevoir aucun message, quel que soit son contenu. Pour plus d'informations, reportez-vous à « *Configurer la liste des spammeurs* » (p. 126).

➕ **Amis** - ouvre la **Liste d'amis** qui contient tous les emails que vous souhaitez recevoir quel qu'en soit le contenu. Pour plus d'informations, reportez-vous à « *Configurer la liste d'amis* » (p. 125).




17.3.1. Indiquer des erreurs de détection

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

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

17.3.2. Indiquer les messages de spam non détectés

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



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



17.3.3. Configurer les paramètres de la barre d'outils

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

Vous disposez des options suivantes :

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

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

17.4. Configurer la liste d'amis



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



Note

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

Pour configurer et gérer la liste d'Amis :

- Si vous utilisez Microsoft Outlook ou Thunderbird, cliquez sur le bouton  **Amis** de la **barre d'outils antispam Bitdefender**.
- Autre option :
 1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
 2. Cliquez sur le lien **VOIR MODULES**.
 3. Dans le module **ANTISPAM**, sélectionnez **Gérer les amis**.

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



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

- @domain.com, *domain.com et domain.com - tous les messages en provenance de domain.com seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;
- *domain* - tous les messages provenant de domain (quel que soit le suffixe) seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;
- *com - tous les messages ayant comme suffixe du domaine com seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;

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

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

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


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

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

17.5. Configurer la liste des spammeurs


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

Pour configurer et gérer la liste des Spammeurs :

- Si vous utilisez Microsoft Outlook ou Thunderbird, cliquez sur le bouton  **Spammeurs** de la **barre d'outils antispam Bitdefender** intégrée à votre client de messagerie.



● Autre option :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'**interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **ANTISPAM**, sélectionnez **Gérer les spammers**.

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

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

- @domain.com, *domain.com et domain.com - tous les messages provenant de domain.com seront étiquetés comme SPAM;
- *domain* - tous les messages de domain (quel que soit le suffixe) seront étiquetés comme SPAM;
- *com - tous les messages provenant d'un domaine avec un suffixe com seront étiquetés comme SPAM.

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

Avertissement

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

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

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

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



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

17.6. Configurer les filtres antispam locaux



Comme cela est décrit dans « *Aperçu de l'antispam* » (p. 121), Bitdefender utilise une combinaison de divers filtres antispam pour identifier le spam. Les filtres antispam sont préconfigurés pour une protection efficace.




Important

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

Pour configurer les filtres antispam locaux :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTISPAM**.
4. Cliquez sur les boutons pour activer ou désactiver les filtres antispam locaux.

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

17.7. Configurer les paramètres cloud

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



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


Des échantillons d'e-mails de spam ou légitimes peuvent être envoyés au Cloud Bitdefender lorsque vous signalez des erreurs de détection ou des



e-mails de spam non détectés. Cela contribue à améliorer la détection antispam de Bitdefender.

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTISPAM**.
4. Sélectionnez les options souhaitées dans l'onglet **Configuration**.

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





18. PROTECTION WEB

La protection Web de Bitdefender vous garantit une navigation sur Internet en toute sécurité en vous signalant les pages web présentant un risque.




Bitdefender fournit une protection web en temps réel pour :

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Pour configurer les paramètres de protection Web :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **WEBPROTECTION**.

Cliquez sur les boutons pour activer ou désactiver :

- Search Advisor, un composant qui évalue les résultats de vos requêtes sur les moteurs de recherche et les liens postés sur les sites Web de réseaux sociaux en plaçant une icône à côté de chaque résultat :
 -  Nous vous déconseillons de consulter cette page Web.
 -  Cette page Web peut contenir du contenu dangereux. Soyez prudent si vous décidez de le consulter.
 -  Cette page peut être consultée en toute sécurité.

Search Advisor évalue les résultats de recherche des moteurs de recherche Web suivants :

- Google
- Yahoo!
- Bing
- Baidu

Search Advisor évalue les liens postés sur les sites de réseaux sociaux suivants :

- Facebook
- Twitter



- Analyse SSL.

Des attaques plus sophistiquées peuvent utiliser le trafic Web sécurisé pour induire en erreur leurs victimes. Nous vous recommandons donc d'activer l'analyse SSL.

- Protection contre les escroqueries.

- Protection contre l'hameçonnage.

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

Pour configurer et administrer les sites web à l'aide de la protection web fournie par Bitdefender, cliquez sur le lien **Liste blanche**. Une nouvelle fenêtre apparaît.

Pour ajouter un site à la liste blanche, entrez son adresse dans le champ correspond et cliquez sur **Ajouter**.

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

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

18.1. Alertes Bitdefender dans le navigateur

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

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

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

- Quittez la page Web en cliquant sur **Retour en toute sécurité**.
- Pour vous rendre sur le site Web, malgré l'avertissement, cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**.



19. PROTECTION DES DONNÉES

19.1. Supprimer définitivement des fichiers


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

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

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

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement.
2. Sélectionnez **Bitdefender** > **Destructeur de fichiers** dans le menu contextuel qui apparaît.
3. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour lancer l'assistant du destructeur de fichiers.
4. Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
5. Les résultats sont affichés. Cliquez sur **Fermer** pour quitter l'assistant.

Vous pouvez également détruire des fichiers à partir de l'interface de Bitdefender.

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **PROTECTION DES DONNÉES**, sélectionnez **Destructeur de fichiers**.
4. Suivez l'assistant du destructeur de fichiers :
 - a. **Ajouter**
Ajoutez les fichiers ou les dossiers que vous souhaitez supprimer définitivement.
 - b. Cliquez sur **Suivant** et confirmez que vous souhaitez continuer le processus.



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

c. Résultats

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



20. CHIFFREMENT DE FICHIERS

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

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

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

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


20.1. Gérer des coffres-forts

Pour gérer votre fichier coffres-forts dans Bitdefender, cliquez sur l'icône  du côté gauche de l'**interface Bitdefender**.

Les coffres-forts existants apparaissent dans le module **Coffres-forts**.

20.2. Créer des coffres-forts

Pour créer un nouveau coffre-fort :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'**interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **CHIFFREMENT DE FICHIERS**, sélectionnez **Créer fichier coffre-fort**.
4. Spécifiez l'emplacement et le nom du coffre-fort.
 - Saisissez le nom du fichier du coffre-fort dans le champ correspondant.



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

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

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




Note

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

20.3. Ouverture de coffres-forts

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

Pour ouvrir un coffre-fort :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.

Les coffres-forts existants apparaissent dans le module **Coffres-forts**.

2. Cliquez sur le lien **Voir Coffres-forts**, puis sélectionnez le coffre-fort que vous souhaitez ouvrir.



3. Cliquez sur le bouton **Déverrouiller**, puis saisissez le mot de passe requis.
4. Cliquez sur **OK**, puis sur le bouton **Ouvrir** pour ouvrir votre coffre-fort.



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

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

20.4. Ajouter des fichiers aux coffres-forts

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

Pour ajouter de nouveaux fichiers à votre coffre-fort :

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **CHIFFREMENT DE FICHIER**.
4. Dans la fenêtre **Mes Coffres-forts**, sélectionnez le coffre-fort que vous souhaitez ouvrir.
5. Cliquez sur le bouton **Déverrouiller**, puis saisissez le mot de passe requis.
6. Cliquez sur le bouton **Ouvrir** pour ouvrir votre coffre-fort.
7. Ajoutez des fichiers ou des dossiers comme vous le faites habituellement sous Windows (par exemple, vous pouvez utiliser la méthode du copier-coller).

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

- Si un seul coffre-fort est ouvert, le fichier ou le dossier est copié directement dans ce coffre-fort.
- Si plusieurs coffres-forts sont ouverts, on vous demandera de choisir le coffre-fort où copier l'élément. Sélectionnez dans le menu la lettre de




lecteur correspondant au coffre-fort souhaité et cliquez sur **OK** pour copier l'élément.

20.5. Verrouiller des coffres-forts

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

Pour fermer un coffre-fort :



1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Dans le module **Fichier coffre-forts** sélectionnez **Voir coffres-forts**.
3. Dans la fenêtre **Mes Coffres-forts**, sélectionnez le coffre-fort que vous souhaitez verrouiller.
4. Cliquez sur le bouton **Verrouiller**.

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

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

20.6. Supprimer des fichiers des coffres-forts

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **CHIFFREMENT DE FICHIER**.
4. Dans la fenêtre **Mes Coffres-forts**, sélectionnez le coffre-fort dans lequel vous souhaitez supprimer des fichiers.





5. Cliquez sur le bouton **Déverrouiller**, dans le cas où il est verrouillé.
6. Cliquez sur le bouton **Ouvrir**.

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

20.7. Changer le mot de passe du coffre-fort

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

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

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **CHIFFREMENT DE FICHIER**.
4. Dans la fenêtre **Mes Coffres-forts**, sélectionnez le coffre-fort dont vous souhaitez modifier le mot de passe.
5. Cliquez sur le bouton **Paramètres**.
6. Entrez le mot de passe actuel du coffre-fort dans le champ **Ancien mot de Passe**.
7. Tapez le nouveau mot de passe souhaité pour le coffre-fort dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**.

Note

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

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



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



21. VULNÉRABILITÉ

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

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

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


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

- Vous pouvez rechercher des vulnérabilités sur votre système et les corriger pas à pas à l'aide de l'option **Analyse de vulnérabilité**.
- La surveillance des vulnérabilités automatique vous permet de vérifier et de corriger les vulnérabilités détectées dans la fenêtre **Notifications**.

Nous vous recommandons de vérifier et de corriger les vulnérabilités du système toutes les semaines, ou une fois toutes les deux semaines.

21.1. Analyser votre système à la recherche de vulnérabilités

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'**interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **VULNÉRABILITÉS**, sélectionnez **Analyse de Vulnérabilité**.



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

● **Mises à jour critiques Windows**

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

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

● **Mises à jour d'applications**

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

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

● **Mots de passe de comptes Windows vulnérables**

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

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

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

● **Réseaux Wifi faibles**

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




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

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

21.2. Utiliser la surveillance des vulnérabilités automatique

Bitdefender analyse régulièrement votre système à la recherche de vulnérabilités, en tâche de fond, et enregistre les problèmes détectés dans la fenêtre **Notifications**.



Pour consulter et corriger les problèmes détectés :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Dans l'onglet **Tous**, sélectionnez la notification concernant la vulnérabilité.
3. Vous pouvez consulter des informations détaillées au sujet des vulnérabilités du système détectées. En fonction du problème, procédez comme suit pour corriger une vulnérabilité spécifique :
 - Si des mises à jour Windows sont disponibles, cliquez sur **INSTALLER**.
 - Si la mise à jour Windows automatique est désactivée, cliquez sur **ACTIVER**.
 - Si une application n'est pas à jour, cliquez sur **METTRE A JOUR MAINTENANT** pour trouver un lien vers la page Web du fournisseur d'où vous pourrez installer la dernière version de l'application.
 - Si un compte utilisateur Windows a un mot de passe vulnérable, cliquez sur **CHANGER DE MOT DE PASSE** pour obliger l'utilisateur à modifier son mot de passe lors de la prochaine connexion ou pour changer le mot de passe par vous-même. Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, \$ ou @).
 - Si la fonctionnalité AutoRun de Windows est activée, cliquez sur **CORRIGER** pour la désactiver.



- Si le routeur que vous avez configuré a défini un mot de passe faible, cliquez sur **CHANGER MOT DE PASSE** pour accéder à son interface à partir de laquelle vous pouvez en définir un plus fort.
- Si le réseau auquel vous êtes connecté a des vulnérabilités qui peuvent exposer votre système à des risques, cliquez sur **Modifier les paramètres WIFI**.

Pour configurer les paramètres de surveillance de la vulnérabilité :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **VULNÉRABILITÉ**.
4. Cliquez sur le bouton correspondant pour activer ou désactiver l'analyse de vulnérabilité.



Important

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

5. Choisissez les vulnérabilités du système que vous souhaitez vérifier régulièrement à l'aide des boutons correspondants.

Mises à jour critiques Windows

Vérifiez que votre système d'exploitation Windows dispose des dernières mises à jour de sécurité critiques de Microsoft.

Mises à jour d'applications

Vérifiez que les applications installées sur votre système sont à jour. Des applications non à jour peuvent être exploitées par des logiciels malveillants, rendant votre PC vulnérable aux attaques extérieures.

Mots de passe vulnérables

Vérifiez si les mots de passe des comptes Windows et des routeurs configurés sur le système sont faciles à deviner. Choisir des mots de passe difficiles à deviner rend difficile l'introduction dans votre système de pirates informatiques. Un mot de passe sécurisé est constitué d'une association de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, \$ ou @).



Exécution automatique des supports amovibles

Vérifiez l'état de la fonctionnalité AutoRun de Windows. Cette fonctionnalité permet aux applications d'être automatiquement lancées à partir de CD, DVD, lecteurs USB ou autres périphériques externes.

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

Notifications Wi-Fi Security Advisor

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

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



Note

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

21.3. Wi-fi Security Advisor

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

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

Habituellement, les réseaux sans fil publics sont plus susceptibles d'être dangereux car ils ne nécessitent pas de mot de passe lors de la connexion, et si c'est le cas, le mot de passe peuvent être mis à disposition de toute



personne qui veut se connecter. De plus, cela peut être des réseaux malveillants ou honeypots, faisant d'eux une cible pour les cyber-criminels.



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

Le Wifi Security Advisor Bitdefender donne des informations sur :

- Réseaux Wifi domestiques
- Réseaux Wifi publics


21.3.1. Activer ou désactiver les notifications Wifi Security Advisor

Pour activer ou désactiver les notifications Wifi Security Advisor :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **VULNÉRABILITÉ**.
4. Cliquez sur le bouton correspondant pour activer ou désactiver les **notifications Wifi Security Advisor**.

21.3.2. Configuration du réseau Wifi domestique

Pour commencer à configurer votre réseau domestique :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **VULNÉRABILITÉ**, sélectionnez **Wi-Fi Security Advisor**.
4. Dans l'onglet **Wifi domestique**, cliquez sur le bouton **Sélectionner Wifi domestique**.

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

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



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

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


21.3.3. Wi-Fi Public

Lorsque vous êtes connecté à un réseau sans fil non sécurisé ou dangereux, le Profil Wifi public est activé. Lorsque vous êtes sous ce profil, Bitdefender Total Security 2017 est réglé pour accomplir automatiquement les paramètres de programme suivants :

- Active Threat Control est activé
- Le pare-feu Bitdefender est activé et les paramètres suivants sont appliqués à votre adaptateur sans fil :
 - Mode furtif - ON
 - Générique - OFF
 - Type de réseau - public
- Les paramètres suivants de la protection Web sont activés :
 - Analyse SSL
 - Protection contre les escroqueries
 - Protection contre le phishing
- Un bouton qui ouvre Bitdefender Safepay™ est disponible. Dans ce cas, la Protection hotspot pour les réseaux non sécurisés est activée par défaut.

21.3.4. Vérifier les informations à propos des réseaux Wifi

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **VULNÉRABILITÉ**, sélectionnez **Wi-Fi Security Advisor**.
4. Selon les informations dont vous avez besoin, sélectionnez l'une des deux balises, **Wifi domestique** ou **Wifi public**.



5. Cliquez sur **Voir les détails** à côté du réseau à propos duquel vous souhaitez avoir plus d'informations.

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

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

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

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

En cliquant sur le lien de la **Plus de détails** dans la zone de chaque réseau, les détails suivants sont affichés :

- **Chiffré** - ici vous pouvez voir si le réseau sélectionné est chiffré ou non. Les réseaux non cryptés peuvent exposer vos données.
- **Type de chiffrement** - ici vous pouvez voir le type de chiffrement utilisé par le réseau sélectionné. Certains types de chiffrement peuvent ne pas être sécurisés. Par conséquent, nous vous recommandons vivement de vérifier les informations sur le type de chiffrement affiché pour être sûr que vous êtes protégé en naviguant sur le web.
- **Canal/fréquence** - ici vous pouvez voir la fréquence du canal utilisé par le réseau sélectionné.
- **Force du mot de passe** - ici vous pouvez voir la force du mot de passe. Notez que les réseaux qui ont mis des mots de passe faibles représentent une cible pour les cyber-criminels.
- **Type de connexion** - ici vous pouvez voir si le réseau sélectionné est protégé par un mot de passe ou non. Il est fortement recommandé de se



connecter uniquement aux réseaux qui ont mis en place des mots de passe forts.

- **Type d'authentification** - ici vous pouvez voir le type d'authentification utilisé par le réseau sélectionné.

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



22. PARE-FEU

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

Le pare-feu Bitdefender utilise un ensemble de règles pour filtrer des données transmises vers et à partir de votre système. Les règles sont regroupées en 2 catégories :

Règles générales

Règles qui déterminent les protocoles sur lesquels la communication est autorisée.

Un ensemble de règles par défaut fournissant une protection optimale est utilisé. Vous pouvez éditer les règles en autorisant ou refusant des connexions sur certains protocoles.

Règles d'applications

Règles déterminant comment chaque application peut accéder aux ressources réseau et à Internet.


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

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


Pour en savoir plus sur la configuration du pare-feu pour chaque type de réseau et sur comment modifier les paramètres réseau, veuillez vous reporter à « *Gérer les paramètres de connexion* » (p. 154).

22.1. Activer ou désactiver la protection pare-feu

Pour activer ou désactiver la protection pare-feu :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface Bitdefender.
2. Cliquez sur le lien **VOIR MODULES**.



3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
4. Activez et désactivez le Pare-feu en cliquant sur le bouton correspondant.

Avertissement



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

22.2. Gérer les règles de pare-feu

22.2.1. Règles générales

Quand des données sont transmises sur Internet, certains protocoles sont utilisés.

Les règles générales vous permettent de configurer les protocoles sur lesquels le trafic est autorisé. Par défaut, les règles générales ne s'affichent pas lorsque vous ouvrez le Pare-feu. Pour modifier les règles :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
4. Sélectionnez l'onglet **Règles**.
5. Sélectionnez la case **Afficher les règles générales** dans l'angle inférieur gauche de la fenêtre.

Les règles par défaut s'affichent. Pour éditer la priorité d'une règle, cliquez sur la flèche correspondante dans la colonne **Permission** et sélectionnez **Autoriser** ou **Refuser**.

DNS sur UDP / TCP

Autoriser ou refuser DNS sur UDP et TCP.

Par défaut, ce type de connexion est autorisé.

Envoi d'e-mails

Autoriser ou refuser l'envoi de courriels sur SMTP.



Par défaut, ce type de connexion est autorisé.

HTTP navigation Web

Autoriser ou refuser la navigation Web HTTP.

Par défaut, ce type de connexion est autorisé.

ICMP / ICMPv6 entrants

Autoriser ou refuser les messages ICMP / ICMPv6.

Les messages ICMP sont souvent utilisés par des pirates pour perpétrer des attaques contre les réseaux informatiques. Par défaut, ce type de connexion est refusé.

Connexions bureau à distance entrantes

Autoriser ou refuser l'accès à d'autres ordinateurs sur des connexions bureau à distance.

Par défaut, ce type de connexion est autorisé.



Trafic Windows Explorer sur HTTP / FTP

Autoriser ou refuser le trafic HTTP et FTP de Windows Explorer.

Par défaut, ce type de connexion est refusé.

22.2.2. Règles d'applications

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
4. Sélectionnez l'onglet **Règles**.

Vous pouvez consulter dans le tableau les programmes (c'est-à-dire les processus) pour lesquels des règles pare-feu ont été créées. Pour voir les règles créées pour une application spécifique, double-cliquez simplement dessus.

Les informations suivantes s'affichent pour chaque règle :

- **Nom** - le nom du processus auquel les règles s'appliquent.



- **Types de Réseau** - les types de processus et d'adaptateur réseau auxquels la règle s'applique. Des règles sont créées automatiquement pour filtrer l'accès réseau ou Internet via n'importe quel adaptateur. Les règles s'appliquent par défaut à tout réseau. Vous pouvez créer manuellement des règles ou éditer des règles existantes, afin de filtrer l'accès réseau ou Internet d'une application via un adaptateur spécifique (par exemple un adaptateur réseau sans fil).
- **Protocole** - le protocole IP auquel s'applique la règle. Les règles s'appliquent par défaut à tout protocole.
- **Permission** - si l'application est autorisée ou non à se connecter au réseau ou à Internet dans certaines circonstances.

Pour gérer les règles, utilisez les boutons au-dessus du tableau :

- **AJOUTER UNE RÈGLE** - ouvre une fenêtre dans laquelle vous pouvez créer une nouvelle règle.
- **SUPPRIMER LA RÈGLE** - supprime la règle sélectionnée.
- **RÉINITIALISER LES REGLES** - ouvre une fenêtre où vous pouvez choisir de supprimer l'ensemble des règles existantes et de restaurer celles par défaut.

Ajouter / modifier des règles d'application

Pour ajouter ou modifier une règle d'application, cliquez sur le bouton **AJOUTER UNE RÈGLE** au-dessus du tableau ou cliquez sur une règle existante. Une nouvelle fenêtre apparaît. Procédez comme suit :

Dans l'onglet **Paramètres** vous pouvez appliquer les modifications suivantes :

- **Chemin du programme.** Cliquez sur **Parcourir** et sélectionnez l'application à laquelle s'applique la règle.
- **Réseau.** Sélectionnez le type de réseau auquel s'applique la règle. Vous pouvez modifier le type de réseau en ouvrant le menu déroulant **Type de Réseau** et en sélectionnant l'un des types de réseau disponibles dans la liste.

Réseau	Description
De confiance	Désactiver le pare-feu pour l'adaptateur concerné.



Réseau	Description
Domicile/Bur.	Autoriser tout le trafic entre votre ordinateur et les ordinateurs du réseau local.
Public	Tout le trafic est filtré.
Non fiable	Bloquer complètement le trafic réseau et Internet via l'adaptateur respectif.

- **Permission.** Sélectionnez l'une des permissions disponibles :

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

Dans l'onglet **Avancé** vous pouvez personnaliser les paramètres suivants :

- **Adresse locale personnalisée.** Spécifiez l'adresse IP locale et le port auxquels s'applique la règle.
- **Adresse distance personnalisée.** Spécifiez l'adresse IP distante et le port auxquels s'applique la règle.
- **Direction.** Sélectionnez dans le menu la direction du trafic à laquelle s'applique la règle.

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

- **Protocole.** Sélectionnez dans le menu le protocole IP auquel s'applique la règle.
 - Si vous voulez que la règle s'applique à tous les protocoles, sélectionnez **Toutes**.



- Si vous souhaitez que la règle s'applique au protocole TCP, sélectionnez **TCP**.
- Si vous souhaitez que la règle s'applique au protocole UDP, sélectionnez **UDP**.
- Si vous souhaitez que la règle s'applique à un protocole spécifique, saisissez le numéro affecté au protocole que vous souhaitez filtrer dans le champ vide.



Note

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



22.3. Gérer les paramètres de connexion

Pour chaque connexion réseau vous pouvez configurer des zones de confiance et des zones non fiables.

Une zone de confiance est un périphérique en lequel vous avez entièrement confiance, comme un ordinateur ou une imprimante. Tout le trafic entre votre ordinateur et un périphérique de confiance est autorisé. Pour partager des ressources avec des ordinateurs en particulier dans une réseau Wi-Fi non sécurisé, ajoutez les comme étant des ordinateurs autorisés.

Une zone non fiable est un périphérique avec lequel vous n'autorisez aucune communication avec votre ordinateur.

Pour voir et gérer les zones sur vos adaptateurs réseaux :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
4. Sélectionnez l'onglet **Adaptateurs**.

Les périphériques réseau avec connexions actives et les zones actuelles, s'il y en a, sont affichés dans cet onglet.



Les informations suivantes s'affichent pour chaque zone :

- **Type de Réseau** - le type de réseau auquel votre ordinateur est connecté.
- **Mode Furtif** - détermine si vous pouvez être détecté par d'autres ordinateurs.

Pour configurer le mode furtif, sélectionnez l'option souhaitée dans le menu déroulant correspondant.

Option furtif	Description
Oui	Le mode Furtif est activé. Votre ordinateur n'est pas visible depuis le réseau local et Internet.
Non	Le mode Furtif est désactivé. N'importe qui sur le réseau local ou sur Internet peut détecter votre ordinateur (via la commande ping).

- **Générique** - si des règles génériques sont appliquées à cette connexion.

Si l'adresse IP d'un adaptateur réseau est modifiée, Bitdefender modifie le type de réseau en conséquence. Si vous souhaitez conserver le même type de réseau, sélectionnez **Oui** dans le menu déroulant correspondant.

Ajouter / modifier des exceptions

Pour ajouter ou modifier une exception, cliquez sur le lien **Exceptions Réseau** au-dessus du tableau. Une nouvelle fenêtre affichant les périphériques disponibles connectés au réseau s'affichera. Procédez comme suit :



1. Sélectionnez l'adresse IP de l'ordinateur que vous souhaitez ajouter, ou tapez une adresse ou une plage d'adresses dans la zone de texte prévue à cet effet.
2. Sélectionnez la permission :
 - **Autoriser** - pour autoriser tout le trafic entre votre ordinateur et l'ordinateur sélectionné.
 - **Bloquer** - permet de bloquer tout le trafic entre votre ordinateur et l'ordinateur sélectionné.
3. Cliquez sur le bouton + pour ajouter l'exception et fermez la fenêtre.



Si vous souhaitez supprimer une IP, cliquez sur le bouton correspondant et fermez la fenêtre.

22.4. Configurer les paramètres avancés

Pour configurer les paramètres avancés du pare-feu :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
4. Sélectionnez l'onglet **Paramètres**.

Les fonctionnalités suivantes peuvent être activées ou désactivées :


- **Bloquer les analyses de port dans le réseau** - détecte et bloque les démarches visant à détecter les ports ouverts.

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

22.5. Configurer l'intensité de l'alerte

Bitdefender Total Security 2017 est conçu pour être aussi discrète que possible. Dans des conditions normales, vous n'avez pas à prendre de décisions pour autoriser ou non des connexions ou des actions tentées par des applications en cours d'exécution sur votre système.

Si vous souhaitez être en total contrôle de la prise de décisions :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Dans la fenêtre **Général**, activez le **Mode Paranoïa** en cliquant sur le bouton correspondant.



Note

Quand le mode Paranoïaque est activé, les fonctionnalités **Autopilot** et **Profils** sont automatiquement désactivées.

Le **Mode Paranoïaque** peut être utilisé simultanément avec le **Mode Batterie**.



Tant que le mode Paranoïaque sera activé, une alerte vous demandera de sélectionner l'action à appliquer à chaque fois que l'une des situations suivantes se produira :

- Une application essaie de se connecter à Internet.
- Une application tente d'effectuer une action considérée comme suspecte par **Active Threat Control**.

L'alerte contient des informations détaillées au sujet de l'application et du comportement détecté. Sélectionnez l'action **Autoriser** ou **Refuser** à l'aide du bouton correspondant.



23. PROTECTION RANSOMWARE

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

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



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

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

Grâce aux dernières technologies, la Protection Bitdefender contre les ransomwares garantit l'intégrité du système en protégeant les zones critiques du système contre les dommages, sans répercussions sur le système. Vous pouvez également souhaiter protéger vos fichiers personnels tels que les documents, photos, films, ou les fichiers que vous conservez dans le cloud.

23.1. Activer ou désactiver la protection contre les ransomwares

Pour désactiver le module de Protection ransomware :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **RANSOMWARE PROTECTION**.





4. Cliquez sur le bouton correspondant pour activer ou désactiver la **Protection contre les ransomwares**.

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

23.2. Protégez vos fichiers personnels contre les attaques de ransomwares

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

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **RANSOMWARE PROTECTION**.
4. Cliquez sur le bouton **AJOUTER**.
5. Allez dans le dossier que vous souhaitez protéger, puis cliquez sur **OK** pour ajouter le dossier sélectionné à l'environnement de protection.

Par défaut, les dossiers Mes Documents, Mes images, Documents publics, et Images publiques sont protégés contre les attaques de malwares.




Note

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

23.3. Configuration des applications fiables

Désactiver la protection contre les ransomwares pour certaines applications spécifiques, mais seulement celles que vous jugez fiables peuvent être ajoutées à la liste.

Pour ajouter des applications fiables aux exclusions :


1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.



3. Dans le module **Protection contre les ransomwares**, sélectionnez **Applications fiables**.
4. Cliquez sur **Ajouter** pour sélectionner les applications que vous voulez protéger.
5. Cliquez sur **OK** pour ajouter l'application sélectionnée à l'environnement de protection.

23.4. Configuration des applications bloquées

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'exclure en procédant comme suit :



1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **Protection contre les ransomwares**, sélectionnez **Applications bloquées**.
4. Cliquez sur **Autoriser** pour sélectionner l'application dont vous êtes certain qu'elle est fiable.
5. Cliquez sur **OK** pour ajouter l'application sélectionnée à la liste de confiance.

23.5. Protection au démarrage

Il est connu que plusieurs applications malwares sont configurées pour s'exécuter au démarrage, ce qui peut sérieusement abîmer une machine. La protection au démarrage Bitdefender analyse tous les zones systèmes critiques avant que tous les fichiers ne soient chargés, sans impact sur le système. Dans le même temps, la protection est assurée contre certaines attaques se basant sur l'exécution de code au niveau de la pile ou du tas, les injections de code ou les hooks à l'intérieur de certaines bibliothèques logicielles dynamiques.

Pour désactiver la protection au démarrage :



1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface **Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **RANSOMWARE PROTECTION**.
4. Cliquez sur le bouton correspondant pour activer ou désactiver la **Protection du démarrage**.



24. LA SÉCURITÉ SAFEPAY POUR LES TRANSACTIONS EN LIGNE

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

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

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

Pour une meilleure protection de la vie privée, Bitdefender Password Manager est intégré à Bitdefender Safepay™ afin de protéger vos identifiants lorsque vous essayez d'accéder à des espaces en ligne confidentiels. Pour plus d'informations, reportez-vous à « *Protection Password Manager de vos identifiants* » (p. 168).

Bitdefender Safepay™ dispose des fonctions suivantes :

- Il bloque l'accès à votre bureau et toute tentative de prise d'instantanés de votre écran.
- Il protège vos mots de passe confidentiels lorsque vous naviguez sur Internet avec Password Manager.
- Il est accompagné d'un clavier virtuel, qui, lorsqu'il est utilisé, empêche les pirates de lire vos frappes au clavier.
- Il est complètement indépendant de vos autres navigateurs.
- Il contient une protection hotspot intégrée à utiliser lorsque votre ordinateur est connecté à des réseaux Wi-Fi non sécurisés.
- Il supporte les marque-pages et vous permet de consulter vos sites bancaires et boutiques en ligne préférés.




- Il ne se limite pas aux sites bancaires et boutiques en ligne. Tout site web peut être ouvert dans Bitdefender Safepay™.

24.1. Utiliser Bitdefender Safepay™

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

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

- À partir de **l'interface de Bitdefender** :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le bouton d'action **Safepay**.

- À partir de Windows :

- Dans **Windows 7** :

1. Cliquez sur **Démarrer** et allez dans **Programmes**.
2. Cliquez sur **Bitdefender**.
3. Cliquez sur **Bitdefender Safepay™**.

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

Localisez Bitdefender Safepay™ dans l'écran d'accueil Windows (vous pouvez, par exemple, taper « Bitdefender Safepay™ » directement dans l'écran d'accueil) puis cliquez sur l'icône.

- Dans **Windows 10** :

Tapez "Bitdefender Safepay™" dans le champ de recherche de la barre des tâches et cliquez sur son icône.













Note

Si le plugin Adobe Flash Player n'est pas installé ou n'est pas à jour, un message Bitdefender apparaîtra. Cliquez sur le bouton correspondant pour poursuivre.

Une fois le processus d'installation terminé, vous pourrez rouvrir manuellement le navigateur Bitdefender Safepay™ pour poursuivre votre travail.



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

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



Note

Pour basculer entre Bitdefender Safepay™ et le bureau de Windows, appuyez sur les touches **Alt + Tab**, ou cliquez sur le bouton **Minimiser**.

24.2. Configurer les paramètres

Cliquer sur  puis sélectionnez **Paramètres** pour configurer Bitdefender Safepay™ :

- Dans les **Paramètres Généraux**, vous pouvez configurer ce qui suit :

Comportement de Bitdefender Safepay™

Choisissez ce qui se passera lorsque vous accéderez à une boutique ou à un site bancaire en ligne dans un navigateur Web standard :

- Ouvrir automatiquement les sites Web dans Safepay.
- Me recommander d'utiliser Safepay.
- Ne pas me recommander d'utiliser Safepay.



Liste des domaines

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

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

Bloquer les fenêtres publicitaires

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

Vous pouvez également créer une liste de sites Web dont vous autorisez les fenêtres publicitaires. La liste ne doit contenir que des sites Web de confiance.

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

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

Activer la protection Hotspot

Vous pouvez activer une couche de sécurité supplémentaire pour quand vous êtes connectés à des réseaux Wifi non sécurisés en activant cette fonctionnalité.

Accéder à « *Protection zones d'accès sans fil pour les réseaux non sécurisés* » (p. 166) pour plus d'informations.

- Dans la zone **Paramètres avancés**, les options suivantes sont disponibles :

Gérer les plugins

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

Gérer les certificats

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



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

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


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

Utilisez le bouton correspondant pour activer ou désactiver la fonctionnalité.

24.3. Gérer les marque-pages

Si vous avez désactivé la détection automatique de certains ou de tous les sites web, ou si Bitdefender ne détecte simplement pas certains sites web, vous pouvez ajouter des marque-pages à Bitdefender Safepay™ afin de pouvoir lancer facilement vos sites web favoris à l'avenir.

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

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



Note

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

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


24.4. Protection zones d'accès sans fil pour les réseaux non sécurisés

Lorsque vous utilisez Bitdefender Safepay™ en étant connecté à des réseaux Wifi non sécurisés (par exemple, à un point d'accès public), un niveau de sécurité supplémentaire est fourni par la fonctionnalité Protection Hotspot. Ce service chiffre la communication Internet sur des connexions non



sécurisées, vous aidant à assurer la protection de votre vie privée quel que soit le réseau auquel vous êtes connecté.

La protection Hotspot ne fonctionne que si votre ordinateur est connecté à un réseau non sécurisé.

La connexion sécurisée sera initialisée et un message s'affichera dans la fenêtre Bitdefender Safepay™ lorsque la connexion sera établie. Le symbole  apparaît en face de l'URL dans la barre d'adresses pour vous aider à identifier facilement les connexions sécurisées.

Vous aurez peut-être besoin de confirmer l'action.



25. PROTECTION PASSWORD MANAGER DE VOS IDENTIFIANTS

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

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

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

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

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

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

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

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

Password Manager protège les informations confidentielles suivantes :

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



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

25.1. Configurer Password Manager

Une fois l'installation terminée, lorsque vous ouvrirez votre navigateur, une fenêtre contextuelle vous indiquera que vous pouvez utiliser Wallet pour faciliter votre navigation sur Internet.

BitdefenderWallet est l'endroit où vous pouvez stocker vos données personnelles.

Cliquez sur **Explorer** pour lancer l'assistant de configuration de Wallet. Suivez l'assistant pour terminer le processus de configuration.

Deux tâches peuvent être réalisées au cours de cette étape :

- **Créer une nouvelle base de données Wallet pour protéger vos mots de passe.**

Lors de la configuration, vous serez invité à protéger votre Wallet avec un mot de passe principal. Le mot de passe doit être sécurisé et contenir au moins 7 caractères.

Pour créer un mot de passe sécurisé, utilisez au moins un chiffre ou un symbole et une majuscule. Une fois que vous aurez défini un mot de passe, toute personne essayant d'accéder au Wallet devra indiquer ce mot de passe.

Après avoir configuré le mot de passe principal, vous pouvez synchroniser les informations du Wallet dans le cloud pour l'utiliser sur tous vos appareils.

À la fin de la configuration, les paramètres suivants de Wallet sont activés par défaut :


- **Enregistrer automatiquement les identifiants dans Wallet.**
- **Me demander mon mot de passe principal lorsque je me connecte à mon PC.**
- **Saisir automatiquement les identifiants de connexion.**
- **Me demander mes options de saisie lorsque je consulte une page contenant des formulaires.**



- Importez une base de données existante si vous avez déjà utilisé Wallet sur votre système.

Exporter la base de données du Wallet

Pour exporter votre base de données du Wallet :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface Bitdefender.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **GESTIONNAIRE DE MOT DE PASSE**, sélectionnez **Exporter Wallet**.
4. Suivez ces étapes pour exporter la base de données du Wallet vers votre système.




Note

Le wallet doit être ouvert pour que le lien **Exporter Wallet** soit disponible.

Créer une nouvelle base de données Wallet

Pour créer une nouvelle base de données Wallet :



1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface Bitdefender.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **GESTIONNAIRE DE MOT DE PASSE**, sélectionnez **Créer nouveau Wallet**.
4. Dans la zone **Partir de zéro**, cliquez sur **Créer nouveau**.
5. Tapez les informations requises dans les champs correspondants.
 - Nom Wallet - saisissez un nom unique pour votre base de données Wallet.
 - Mot de passe principal - saisissez un mot de passe pour votre Wallet.
 - Saisissez le mot de passe à nouveau - saisissez à nouveau le mot de passe que vous avez configuré.
 - Indice - saisissez un indice pour vous souvenir du mot de passe.
6. Cliquez sur **Continuer**.



7. A cette étape, vous pouvez choisir de stocker vos informations dans le cloud. Si vous choisissez Oui, vos informations bancaires seront conservées localement sur votre appareil. Choisissez les options souhaitées, puis cliquez sur **Continuer**.
8. Sélectionnez le navigateur web à partir duquel vous souhaitez importer vos identifiants.
9. Cliquez sur **Terminer**.

Synchroniser vos Wallets dans le cloud.

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **GESTIONNAIRE DE MOT DE PASSE**.
4. Sélectionnez la base de données Wallet souhaitée à partir de la section **Mes Wallets**, puis cliquez sur le bouton **PARAMÈTRES**
5. Choisissez l'option désirée dans la fenêtre qui apparaît, puis cliquez sur **Sauvegarder**.




Note

Le wallet doit être ouvert pour que le bouton **PARAMÈTRES** soit disponible.

Gérer les identifiants de votre Wallet

Pour gérer vos mots de passe :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **GESTIONNAIRE DE MOT DE PASSE**, sélectionnez **Ouvrir Wallet**.
4. Sélectionnez la base de données Wallet souhaitée à partir de l'onglet **Mes Wallets**, puis cliquez sur le bouton **OUVRIR**.
5. Entrez le mot de passe Master puis cliquez sur **OK**.



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



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

Ajouter/ modifier les identifiants

- Pour ajouter un nouveau mot de passe, choisissez la catégorie souhaitée en haut, cliquez sur **+ Ajouter un élément**, insérez les informations dans les champs correspondants et cliquez sur le bouton Enregistrer.
- Pour éditer un objet de la liste, sélectionnez le et cliquez sur le bouton **Editer**.
- Pour supprimer une entrée, sélectionnez-la, cliquez sur le bouton **Modifier** et sélectionnez **Supprimer**.

25.2. Activer ou désactiver la protection du Password Manager



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

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface Bitdefender.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **GESTIONNAIRE DE MOT DE PASSE**.
4. Utilisez le bouton correspondant pour activer ou désactiver le Gestionnaire de mot de passe.

25.3. Gestion des configurations du Password Manager

Pour configurer le mot de passe Master en détails :



1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **GESTIONNAIRE DE MOT DE PASSE**.
4. Sélectionnez l'onglet **Paramètres de sécurité**.

Voici les options proposées :

- **Me demander mon mot de passe principal lorsque je me connecte à mon PC** - vous devrez indiquer votre mot de passe principal lorsque vous accéderez à l'ordinateur.
- **Me demander mon mot de passe principal lorsque j'ouvre mes navigateurs et applications** - vous devrez indiquer votre mot de passe principal lorsque vous accéderez à un navigateur ou à une application.
- **Verrouiller automatiquement Wallet lorsque mon PC n'est pas utilisé** - vous devrez saisir votre mot de passe principal lorsque vous utiliserez votre ordinateur après 15 minutes d'inactivité.





Important

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

Améliorer votre expérience

Pour sélectionner les navigateurs ou les applications où vous souhaitez intégrer le Gestionnaire de mot de passe :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **GESTIONNAIRE DE MOT DE PASSE**.
4. Sélectionnez l'onglet **Plugins**.

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





- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safepay
- Skype

Configurer la saisie automatique

La fonctionnalité Saisie automatique vous permet d'accéder facilement à vos sites web préférés ou de vous connecter à vos comptes en ligne. Lorsque vous saisissez vos informations d'identification et données personnelles dans votre navigateur Web pour la première fois, celles-ci sont automatiquement conservées en toute sécurité dans Wallet.

Pour configurer les paramètres **Saisie automatique** :


1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **GESTIONNAIRE DE MOT DE PASSE**.
4. Sélectionnez l'onglet **Paramètres saisie automatique**.
5. Configurez les options suivantes :
 - **Saisir automatiquement les identifiants de connexion**:
 - **Saisir automatiquement les identifiants de connexion à chaque fois** - les identifiants de connexion sont insérés automatiquement dans le navigateur.
 - **Me laisser choisir quand je souhaite que mes identifiants de connexion soient saisis automatiquement** - vous pouvez choisir quand les identifiants seront saisis automatiquement dans le navigateur.
 - **Configurer la façon dont Wallet sécurise vos identifiants**:
 - **Enregistrer automatiquement les identifiants dans Wallet** - les identifiants de connexion et autres informations identifiables telles que vos données personnelles et bancaires sont automatiquement enregistrées et mises à jour dans le Wallet.



- **Me demander à chaque fois** - on vous demandera à chaque fois si vous souhaitez ajouter vos identifiants au Wallet.
- **Ne pas enregistrer, je mettrai les informations à jour manuellement** - les identifiants peuvent être ajoutés uniquement manuellement dans le Wallet.
- **Compléter automatiquement les formulaires:**
 - **Me demander mes options de saisie lorsque je consulte une page contenant des formulaires** - une fenêtre avec les options de remplissage apparaîtra à chaque fois que Bitdefender détectera que vous souhaitez effectuer un paiement en ligne ou vous connecter.

Gérer les informations de Password Manager à partir de votre navigateur

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

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

L'extension Bitdefender Wallet présente les options suivantes :

- Ouvrir Wallet - ouvre le Wallet.
- Verrouiller Wallet - verrouille le Wallet.
- Sites Web - ouvre un sous-menu avec tous les identifiants de sites Web contenus dans Wallet. Cliquez sur **Ajouter un site Web** pour ajouter de nouveaux sites Web à la liste.
- Remplir les formulaires - ouvre un sous-menu contenant les informations que vous avez ajoutées pour une catégorie spécifique. Vous pouvez ajouter ici de nouvelles données à votre Wallet.
- Générateur de mot de passe - vous permet de générer des mots de passe au hasard que vous pourrez utiliser pour des comptes existants. Cliquez sur **Afficher configurations avancées** pour personnaliser la complexité du mot de passe.



- Configuration - ouvre la fenêtre des paramètres de Password Manager.
- Signaler un problème - permet de signaler tout problème rencontré avec Bitdefender Password Manager.



26. PARENTAL ADVISOR

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

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

Vous pouvez configurer le Contrôle parental pour bloquer :

- aux pages Web indésirables.
- les applications comme les jeux, les logiciels de clavardage, les programmes de partage de fichiers et autres.
- les contacts spécifiques qui ne sont pas autorisés à entrer en contact avec votre enfant par téléphone.

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

26.1. Allez dans le Contrôle parental - Mes enfants

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

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


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

Accédez à votre compte Bitdefender.

- Sur tout appareil avec un accès à Internet :

1. Accéder à **Bitdefender Central**.



2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
 3. Sélectionnez le module **Contrôle parental**.
 4. Dans la fenêtre **Mes enfants** qui apparaît, vous pouvez gérer et configurer les profils Contrôle parental pour chaque appareil.
- Depuis votre interface Bitdefender :
1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
 2. Cliquez sur le lien **VOIR MODULES**.
 3. Sous le module **Contrôle parental**, sélectionnez **Configurer**.
Vous êtes redirigé vers la page web compte Bitdefender. Assurez-vous que vous êtes connectés avec vos identifiants.
 4. Sélectionnez le module **Contrôle parental**.
 5. Dans la fenêtre **Mes enfants** qui apparaît, vous pouvez gérer et configurer les profils Contrôle parental pour chaque appareil.



Note

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

26.2. Ajouter le profil de votre enfant

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

Pour ajouter le profil de votre enfant au Contrôle parental :

1. Accédez au panneau **Contrôle parental** depuis Bitdefender Central.
2. Cliquez sur **AJOUTER PROFIL** sur le côté droit de la fenêtre **Mes enfants**
3. Configurez des informations spécifiques dans les champs correspondants, telles que : nom, sexe et date de naissance, puis cliquez sur **CONTINUER**.

Basée sur les standards de développement des enfants, la configuration de la date de naissance de l'enfant charge automatiquement les spécificités considérées comme appropriées pour sa catégorie d'âge.



4. Si l'appareil de votre enfant contient déjà Bitdefender Total Security 2017, sélectionnez son appareil à partir de la liste disponible, puis cliquez sur **CONTINUER**.

Si l'appareil de votre enfant n'a pas de produit Bitdefender contenant les fonctionnalités de Contrôle parental, cliquez sur **Ajouter un nouvel appareil**. Sélectionnez le système d'exploitation de son appareil, puis cliquez sur **CONTINUER**.


Saisissez l'adresse e-mail sur laquelle nous devons envoyer le lien d'installation de l'application Bitdefender Contrôle parental.

Sur les appareils Windows, le Bitdefender Total Security 2017 que vous avez inclus dans votre abonnement doit être téléchargé et installé. Sur les appareils Android, l'agent Contrôle parental de Bitdefender doit être téléchargé et installé.

26.2.1. Assigner le même profil à plusieurs appareils

Vous pouvez assigner le même profil à plusieurs appareils appartenant au même enfant, pour que les mêmes restrictions soient appliquées.

Pour affecter un profil à plusieurs appareils :

1. Accéder à **Bitdefender Central**.
2. Sélectionnez le module **Contrôle parental**.
3. Cliquez sur l'icône  sur la carte profil souhaitée, puis sélectionnez **Éditer**.
4. Cliquez sur le signe + sur chacun des appareils disponibles auquel vous souhaitez assigner le profil.

Si l'appareil de votre enfant n'a pas de produit Bitdefender contenant les fonctionnalités de Contrôle parental, cliquez sur **Ajouter un nouvel appareil**. Sélectionnez le système d'exploitation de son appareil, puis cliquez sur **CONTINUER**.

Saisissez l'adresse e-mail sur laquelle nous devons envoyer le lien d'installation de l'application Bitdefender Contrôle parental. Allez dans l'e-mail et cliquez sur le lien fourni pour installer l'agent.

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



5. Sélectionner **Enregistrer**.

26.2.2. Lier le Contrôle parental à Bitdefender Central

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

Pour lier l'appareil à votre compte Bitdefender :

1. Cliquez sur le bouton **Google Play** qui apparaît dans l'e-mail envoyé par votre serveur, puis installez l'application.

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

2. Ouvrir l'application Contrôle parental.

3. Lire le **contrat de licence utilisateur final** puis appuyez sur **CONTINUER**.

4. Connectez-vous à votre compte déjà existant Bitdefender :

Si vous n'avez pas de compte, choisissez de créer un nouveau compte à l'aide de l'option correspondante.

5. Activez les droits administrateur de l'appareil pour l'application en appuyant sur **Activer**.

Cela empêchera votre enfant de désinstaller l'agent Contrôle parental.

6. Appuyez sur **Autoriser accès utilisation** et cochez la case correspondante.

26.2.3. Surveiller les activités de l'enfant

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

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

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

- L'état de l'événement.
- La sévérité des notifications.
- Le nom de l'appareil.



- La date et l'heure auxquelles l'événement a eu lieu.

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


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

Dans la fenêtre **Tableau de bord** vous pouvez voir les informations qui vous intéressent.

26.2.4. Configurer les paramètres généraux

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

Pour recevoir des notifications par e-mail :


1. Accédez au panneau **Contrôle parental** depuis Bitdefender Central.
2. Cliquez sur l'icône  dans le coin en haut à droite.
3. Activez l'option correspondante pour recevoir les rapports d'activité.
4. Saisissez l'adresse courriel pour recevoir les notifications par courriel.
5. Ajustez la fréquence en sélectionnant : quotidienne, hebdomadaire ou mensuelle.
6. Recevez des notifications par courriel pour les éléments suivants :
 - Sites Web bloqués
 - Applications bloquées
 - Zones restreintes
 - SMS d'un contact bloqué
 - Appel reçu d'un numéro de téléphone bloqué
 - Désinstallation de l'application Contrôle parental pour Facebook
7. Cliquez sur **Enregistrer**.

26.2.5. Modifier le profil

Pour modifier un profil existant :


1. Accéder à **Bitdefender Central**.



2. Sélectionnez la section **Contrôle parental**.
3. Cliquez sur l'icône  sur la carte profil souhaitée, puis sélectionnez **Éditer**.
4. Après avoir personnalisé les paramètres souhaités, sélectionnez **Sauvegarder**.

26.2.6. Supprimer le profil

Pour modifier un profil existant :

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

26.3. Configurer les profils Contrôle parental

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

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

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

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

- **Tableau de bord** - affiche toutes les activités, intérêts, localisations, et interactions avec les amis, à partir du jour même.
- **Activités** - vous permet de bloquer l'accès à certaines applications, telles que les jeux, les logiciels de messagerie, les films, etc.
- **Intérêts** - vous permet de filtrer la navigation sur le Web
- **Amis** - ici vous pouvez spécifier quels contacts de la liste de votre enfant sont autorisés à entrer en contact avec lui via son téléphone.
- **Lieux** - ici vous pouvez configurer les lieux qui sont sûrs ou non pour votre enfant.



- **Social** - vous permet de bloquer l'accès aux réseaux sociaux.

26.3.1. Tableau de bord

La fenêtre Tableau de bord vous donne des informations détaillées sur les activités de vos enfants sur les dernières 24h, à l'intérieur comme à l'extérieur de la maison.

Selon l'activité, la fenêtre Tableau de bord peut inclure les informations suivantes :

- **Lieux** - ici vous pouvez voir les endroits où votre enfant s'est rendu pendant la journée.
- **Intérêts** - ici vous pouvez voir des informations sur les catégories de sites web que votre enfant a visité. Cliquez sur le lien **Examiner le contenu inapproprié** pour autoriser ou refuser l'accès à des intérêts spécifiques.
- **Interactions sociales** - ici vous pouvez voir les contacts avec lesquels votre enfant communique. Cliquez sur le lien **Amis** pour sélectionner les contacts avec lesquels votre enfant peut communiquer ou non.
- **Applications** - ici vous pouvez voir les applications que votre enfant a utilisé. Cliquez sur le lien **Voir les restrictions d'applications** pour autoriser ou bloquer l'accès à certaines applications.
- **Activité de la journée** - ici vous pouvez voir le temps passé en ligne sur les appareils assignés à votre enfant, et les endroits où il a été actif. Les informations rassemblées sont celles de la journée en cours. Cliquez sur le lien **Configurer une heure de coucher** pour configurer une heure à partir de laquelle les activités de surveillance seront automatiquement passées en mode veille.



Note

Pour des informations détaillées, cliquez sur l'option souhaitée qui se trouve dans le coin droit de chaque rubrique.

26.3.2. Activités

La fenêtre des Activités vous aide à bloquer l'exécution des applications. Les jeux, logiciels multimédias et services de messagerie, ainsi que d'autres catégories de logiciels peuvent être bloqués de cette manière.

Le module peut être activé ou désactivé à l'aide de l'interrupteur correspondant.



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

1. Une liste avec des cartes s'affiche. Les cartes représentent les applications utilisées par votre enfant.
2. Sélectionnez la carte avec l'application que vous ne voulez plus que votre enfant utilise.

Le symbole qui apparaît indique que votre enfant ne pourra plus utiliser cette application.

26.3.3. Intérêts

La fenêtre des Intérêts vous aide à bloquer les sites web avec du contenu inapproprié. Les sites web qui hébergent des vidéos, des jeux, des médias, et des logiciels de messagerie, ainsi que d'autres catégories de contenu négatif peuvent être bloqués de cette façon.

Le module peut être activé ou désactivé à l'aide de l'interrupteur correspondant.

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

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

Autoriser ou bloquer un site Web

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


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



26.3.4. Amis

La fenêtre Amis vous offre la possibilité de spécifier quels amis de la liste de votre enfant sont autorisés ou non à entrer en contact avec lui via son téléphone.

Pour restreindre le numéro de téléphone d'un ami spécifique, vous devez d'abord ajouter le numéro de téléphone de votre enfant à son profil :

1. Sélectionnez l'onglet **Contrôle parental** dans Bitdefender Central.
2. Cliquez sur l'icône  sur la carte profil souhaitée, puis sélectionnez **Éditer**.
3. Saisissez le numéro de votre enfant dans le champ correspondant, puis cliquez sur **SAUVEGARDER**.
4. Sélectionnez le profil de l'enfant que vous souhaitez limiter.
5. Sélectionnez l'onglet **Amis**.

Une liste avec des cartes s'affiche. Les cartes représentent les contacts provenant du téléphone de votre enfant.

6. Sélectionnez la carte avec le numéro de téléphone que vous souhaitez bloquer.

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

Pour bloquer les numéros de téléphone inconnus, activez l'interrupteur **Ne bloquer aucune interaction avec ID appelant**.

26.3.5. Lieux

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

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

- Si le GPS est activé sur l'appareil, son emplacement peut être déterminé à quelques mètres près tant qu'il est à portée des satellites GPS (c'est-à-dire, à l'extérieur).



- Si l'appareil est à l'intérieur, il peut être localisé avec une précision d'une dizaine de mètres si le Wi-Fi est activé et si des réseaux sans fil sont à sa portée.
- Sinon, la localisation sera déterminée à l'aide des informations du réseau mobile, qui fournit une précision de pas plus de quelques centaines de mètres.

Configurer une localisation

Pour être certain que votre enfant se rend bien dans certains endroits, vous pouvez dresser une liste d'endroits sûrs ou non.

Pour configurer un lieu :

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

26.3.6. Réseaux sociaux

Contrôle parental surveille le compte Facebook de votre enfant et signale ses principales activités.

Ces activités en ligne sont vérifiées et vous êtes averti si elles constituent une menace pour la confidentialité de votre enfant.

Les éléments surveillés du compte en ligne comprennent :

- Informations sur le compte
- Aimer les pages
- Photos téléchargées



Pour configurer la protection Facebook pour un compte spécifique, saisissez l'e-mail du compte de votre enfant, puis cliquez sur **ENVOYER**.

Informez votre enfant de vos intentions, et demandez-lui de cliquer sur le bouton **Protéger compte** qu'il a reçu par e-mail.

Pour accéder au compte Facebook surveillé, cliquez sur le lien **Voir sur Facebook**.

Pour cesser de surveiller le compte, utilisez le bouton **Dissocier le compte** en haut.

Pour être prévenu par e-mail lorsque votre enfant supprime le Contrôle parental de son appareil, cochez la case correspondante.



27. ANTIVOL DE L'APPAREIL

Le vol d'ordinateurs portables est un problème important qui touche à la fois les particuliers et les entreprises. Plus que la perte du matériel en lui-même, la perte des données qui l'accompagne peut causer d'importants dommages, à la fois financiers et émotionnels.

Pourtant, peu de personnes prennent les mesures adaptées pour protéger leurs données personnelles, commerciales et financières importantes en cas de perte ou de vol.

Bitdefender Antivol vous aide à mieux vous préparer à un tel événement en vous permettant de localiser ou de verrouiller à distance votre ordinateur portable, et même, d'effacer toutes ses données, si jamais vous en étiez séparé contre votre gré.

Pour utiliser les fonctionnalités Antivol, les configurations requises suivantes doivent être remplies :

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

Les fonctionnalités Antivol fonctionnent de la manière suivante :

Localiser

Afficher l'endroit où se trouve votre appareil sur Google Maps.

La précision de la localisation dépend de la façon dont Bitdefender est capable de la déterminer. L'emplacement est déterminé avec une précision de dix mètres si le Wi-Fi est activé sur votre ordinateur portable et s'il y a des réseaux sans fil à sa portée.

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

Alerter

Envoyer une alerte à distance sur l'appareil.

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



Verrouiller

Verrouillez votre ordinateur portable et spécifiez un code PIN à 4 chiffres pour le déverrouiller. Lorsque vous envoyez la commande **Verrouiller**, l'ordinateur redémarre et se reconnecter à Windows est possible uniquement après avoir saisi le code PIN que vous avez défini.

Si vous souhaitez que Bitdefender prenne des photos de celui qui tente d'accéder à votre ordinateur portable, cochez la case correspondante. Les photos sont prises en utilisant la caméra frontale et affichées avec la date et l'heure dans le tableau de bord d'Antivol. Seules les 2 dernières photos sont sauvegardées.

Cette fonctionnalité est disponible seulement sur les ordinateurs portables qui ont une caméra frontale.

Supprimer

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


Afficher IP

Affiche la dernière adresse IP pour l'appareil sélectionné. Cliquez sur **AFFICHER IP** pour la rendre visible.

Antivol est activé après l'installation et est accessible uniquement via votre compte Bitdefender à partir de tout appareil connecté à Internet, où que vous soyez.

Utiliser des fonctionnalités Antivol

Pour accéder aux fonctionnalités Antivol, utilisez les possibilités suivantes :

- À partir de l'interface principale de Bitdefender :
 1. Cliquer sur  l'icône dans le coin en bas à gauche de l'**interface Bitdefender**.
 2. Cliquez sur le bouton d'action **Antivol**.
 3. Dans la fenêtre Bitdefender Central qui s'ouvre, cliquez sur la carte appareil souhaitée, puis sélectionnez **Antivol**.
- Sur tout appareil avec un accès à Internet :



1. Ouvrez la fenêtre d'un navigateur web et allez à <https://central.bitdefender.com>.
2. Connectez-vous à votre compte Bitdefender à l'aide de votre adresse e-mail et de votre mot de passe.
3. Sélectionnez la section **Mes Appareils**.
4. Cliquez sur la carte appareil souhaitée, puis sélectionnez **Antivol**.
5. Sélectionnez la fonctionnalité que vous souhaitez utiliser :

Afficher IP - afficher la dernière adresse IP de votre appareil.

Localiser - permet d'afficher la localisation de votre appareil sur Google Maps.



Alerte - envoyer une alerte sur l'appareil.



Verrouiller - permet de verrouiller votre ordinateur portable et de spécifier un code PIN pour le déverrouiller.



Effacer - permet d'effacer toutes les données de votre ordinateur portable.



Important

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



28. PROTECTION USB

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

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

Avec la protection USB, vous pouvez empêcher tout lecteur flash formaté en NTFS, FAT32 ou FAT d'exécuter des logiciels malveillants. Lorsqu'un périphérique USB est immunisé, les logiciels malveillants ne peuvent plus le configurer pour qu'il exécute une application spécifique lorsqu'il est connecté à un ordinateur fonctionnant sous Windows.

Pour immuniser un appareil USB :

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



Note

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

Pour empêcher que votre ordinateur ne lance des logiciels malveillants depuis des lecteurs USB non immunisés, désactivez la fonction Exécution automatique des médias. Pour plus d'informations, reportez-vous à « *Utiliser la surveillance des vulnérabilités automatique* » (p. 142).



OPTIMISATION DU SYSTÈME



29. OUTILS

Bitdefender comporte une rubrique Outils qui vous permet de préserver l'intégrité de votre système. Les outils de maintenance proposés sont essentiels pour améliorer la réactivité de votre système et pour gérer efficacement l'espace sur le disque dur.

Bitdefender vous propose les outils d'optimisation de PC suivants :


- **L'Optimisation en 1 clic** analyse et améliore la vitesse de votre système en exécutant plusieurs tâches d'un simple clic sur un bouton.
- **L'Optimisation du démarrage** réduit le temps de démarrage de votre système en empêchant le téléchargement d'applications inutiles lorsque le PC démarre.
- **Nettoyage disque** identifie les plus gros fichiers et dossiers qui n'ont pas été utilisés depuis un certain temps.

29.1. Optimisation de la vitesse de votre système d'un simple clic

Des problèmes tels que des défaillances de disque dur, des fichiers de registre et un historique de navigateur restants peuvent ralentir le fonctionnement de votre ordinateur, ce qui peut devenir agaçant. Tout cela peut désormais être corrigé d'un simple clic sur un bouton.

L'Optimisation en 1 clic permet d'identifier et de supprimer les fichiers inutiles en exécutant plusieurs tâches de nettoyage à la fois.

Pour commencer le processus d'Optimisation en 1 clic :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le bouton d'action **Optimisation en 1 clic**.
 - a. **Analyse**

Patientez jusqu'à ce que Bitdefender ait terminé la recherche de problèmes associés au système.

- **Nettoyage disque** - identifie les gros fichiers et dossiers que vous n'utilisez plus.



- Nettoyage du registre - identifie les références non valides ou ayant expiré dans le registre Windows.
- Le Nettoyage des Données - identifie les fichiers Internet temporaires et les témoins, le cache et l'historique du navigateur.

Le nombre de problèmes détectés s'affiche. Cliquez sur le lien **Voir détails** pour les examiner avant de procéder au nettoyage. Cliquez sur **Optimisation** pour poursuivre.

b. Optimisation

Attendez que Bitdefender termine d'optimiser votre système.

c. Problèmes

Cette étape vous permet d'afficher le résultat de l'opération.


Pour des informations complètes sur le processus d'optimisation, cliquez sur le bouton **Afficher le rapport détaillé**.

29.2. Optimisation du temps de démarrage de votre PC

Un long démarrage du système est un véritable problème dû à des applications configurées pour s'exécuter alors qu'elles ne sont pas nécessaires. Attendre le démarrage du système pendant plusieurs minutes vous fait perdre un temps précieux et a un impact sur la productivité.

La fenêtre de l'optimisation du démarrage affiche les applications en cours d'exécution au démarrage du système et vous permet de gérer leur comportement à cette étape.

Pour commencer le processus d'Optimisation démarrage :

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le bouton d'action **Optimisation démarrage**.
 - a. **Sélectionnez les applications**

Vous pouvez voir une liste des applications qui s'exécutent au démarrage du système. Sélectionnez celles que vous souhaitez désactiver ou différer au démarrage.

b. Choix de la communauté



Découvrez ce que les autres utilisateurs de Bitdefender ont décidé de faire avec l'application que vous avez sélectionnée.

c. Temps de démarrage du système

Le curseur en haut de la fenêtre indique le temps nécessaire à la fois à votre système et aux applications sélectionnées pour s'exécuter au démarrage.

Un redémarrage du système est nécessaire pour obtenir des informations sur le temps de démarrage du système et des applications.

d. État du démarrage

- **Permettre.** Sélectionnez cette option lorsque vous souhaitez qu'une application commence à s'exécuter au démarrage du système. Cette option est activée par défaut.
- **Différer.** Sélectionnez cette option pour reporter l'exécution d'un programme au démarrage du système. Cela signifie que les applications sélectionnées démarreront cinq minutes après la connexion de l'utilisateur au système. La fonctionnalité **Différer** est prédéfinie et ne peut pas être configurée par l'utilisateur.
- **Désactiver.** Sélectionnez cette option pour désactiver l'exécution d'un programme au démarrage du système.

e. Résultats

Des informations telles que l'estimation du temps de démarrage du système après le report ou la désactivation de l'exécution de programmes s'affichent.

Un redémarrage du système peut être requis pour voir toutes ces informations.

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



Note

Si votre abonnement expire ou si vous décidez de désinstaller Bitdefender, les paramètres par défaut des programmes dont vous avez décidé de bloquer l'exécution au démarrage seront restaurés.

29.3. Optimisation de votre disque


Les fichiers et dossiers inutiles qui utilisent de l'espace sur votre disque dur peuvent provoquer des ralentissements du système. Par conséquent, il est



recommandé d'améliorer votre vitesse de système en le nettoyant à intervalles réguliers.

Le Nettoyage de disque Bitdefender vous permet de libérer de l'espace disque en identifiant de gros fichiers et dossiers que vous n'utilisez plus.

Pour commencer à nettoyer votre système :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le bouton d'action **Nettoyage de disque**.
3. Une fenêtre affichant des informations sur ce que le Nettoyage de disque peut faire pour votre système pour faire de la place à de nouvelles données devient visible. Cliquez sur **CONTINUER**.

a. Appareils et lecteurs

Vous pouvez voir une liste des disques disponibles. A côté des disques Windows, les disques durs externes et les périphériques USB sont analysés et affichés dans la liste. Cliquez sur **VOIR** pour avoir accès aux dossiers appartenant à l'emplacement sélectionné. Cliquez sur **Analyser** dans la zone du disque que vous voulez nettoyer.

b. Analyser le lecteur

Le disque sélectionné est analysé. Patientez jusqu'à ce que Bitdefender ait terminé la recherche de fichiers et dossiers volumineux.

c. Problèmes

Ceci est l'endroit où vous pouvez voir les résultats de l'opération divisés en dossiers. Dans la partie gauche de la fenêtre, un diagramme circulaire montrant la quantité d'espace disque utilisée est affiché. Survolez-le à l'aide de votre souris pour voir le nom de ses fichiers et la place qu'ils occupent.

Pour naviguer entre les dossiers de la localisation système sélectionnée, sélectionnez-les à partir de la partie droite de la fenêtre. Pour voir le contenu d'un dossier dans une fenêtre distincte, sélectionnez **Afficher dans l'explorateur de fichiers**.

Faites glisser les fichiers que vous souhaitez supprimer vers la partie inférieure de la fenêtre. Cliquez sur **VOIR** si vous souhaitez examiner de nouveau les fichiers que vous avez sélectionnés pour suppression.



Cliquez sur **SUPPRIMER DÉFINITIVEMENT** pour lancer le processus d'effacement.

Confirmez votre choix.



30. PROFILS

Effectuer des activités professionnelles quotidiennes, regarder des films ou jouer peut ralentir le système, en particulier si des processus de mise à jour Windows et des tâches de maintenance ont lieu simultanément. Bitdefender vous permet désormais de choisir et d'appliquer le profil de votre choix, qui fait les réglages nécessaires pour améliorer les performances de certaines applications installées sur le système.

Bitdefender propose les profils suivants :

- Profil Travail
- Profil Film
- Profil Jeu
- Profil Wifi public
- Profil Mode batterie

Si vous décidez de ne pas utiliser les **Profils**, un profil par défaut nommé **Standard** est activé et n'apporte aucune optimisation à votre système.

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

- Toutes les alertes et fenêtres pop-up de Bitdefender sont désactivées.
- La Mise à jour automatique est reportée.
- Les analyses planifiées sont reportées.
- **Search Advisor** est désactivé.
- Les offres spéciales et notifications du produit sont désactivées.

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

- Les mises à jour automatiques de Windows sont reportées.
- Les alertes et fenêtres pop-up de Windows sont désactivées.
- Les programmes inutiles en arrière-plan sont interrompus.
- Les effets visuels sont ajustés pour de meilleures performances.
- Les tâches de maintenance sont reportées.



- Les paramètres du plan d'alimentation sont adaptés.

Lorsqu'il fonctionne sous le profil Wi-Fi public, Bitdefender Total Security 2017 est configuré pour exécuter les paramètres de programme suivants :


- Active Threat Control est activé
- Le pare-feu Bitdefender est activé et les paramètres suivants sont appliqués à votre adaptateur sans fil :
 - Mode furtif - ON
 - Générique - OFF
 - Type de réseau - public
- Les paramètres suivants de la protection Web sont activés :
 - Analyse SSL
 - Protection contre les escroqueries
 - Protection contre le phishing

30.1. Profil Travail

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

Configurer le Profil Travail

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Profils**.
3. Assurez-vous que l'option **Profils** est activée.
4. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Travail.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :
 - Améliorer les performances pour les applications de bureautique




- Optimiser les paramètres du produit pour le profil Travail
 - Reporter les tâches de maintenance et les programmes en arrière-plan
 - Reporter les mises à jour automatiques de Windows
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des applications à la liste du Profil Travail

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

Pour ajouter manuellement des applications à la Liste des applications dans le Profil Travail :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Profils**.
3. Assurez-vous que l'option **Profils** est activée.
4. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Travail.
5. Dans la fenêtre **PROFIL TRAVAIL**, cliquez sur le lien **Liste des applications**.
6. Cliquez sur **Ajouter** pour ajouter une nouvelle application à la **Liste des applications**.

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


30.2. Profil Film

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

Configurer le Profil Film

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




1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Profils**.
3. Assurez-vous que l'option **Profils** est activée.
4. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Film.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :
 - Améliorer les performances pour les lecteurs vidéo
 - Optimiser les paramètres du produit pour le profil Film
 - Reporter les tâches de maintenance et les programmes en arrière-plan
 - Reporter les mises à jour automatiques de Windows
 - Ajuster les paramètres du plan d'alimentation pour les films
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des lecteurs vidéo à la liste du Profil Film

Si Bitdefender ne passe pas automatiquement en Profil Film lorsque vous lancez un lecteur vidéo spécifique, vous pouvez ajouter manuellement cette application à la **Liste des lecteurs vidéo**.

Pour ajouter manuellement des lecteurs vidéo à la Liste des lecteurs vidéo dans le Profil Film :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Profils**.
3. Assurez-vous que l'option **Profils** est activée.
4. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Film.
5. Dans la fenêtre **PROFIL FILM**, cliquez sur le lien **Liste des lecteurs vidéo**.
6. Cliquez sur **Ajouter** pour ajouter une nouvelle application à la **Liste des lecteurs vidéo**.




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

30.3. Profil Jeu

Pour une meilleure expérience de jeu, il suffit de réduire la charge du système et de diminuer les ralentissements. En associant des techniques heuristiques comportementales à une liste de jeux connus, Bitdefender détecte automatiquement les jeux en cours d'exécution et optimise les ressources du système afin que vous puissiez profiter pleinement de vos pauses.

Configurer le Profil Jeu

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


1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Profils**.
3. Assurez-vous que l'option **Profils** est activée.
4. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Jeu.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :
 - Améliorer les performances pour les jeux
 - Optimiser les paramètres du produit pour le profil Jeu
 - Reporter les tâches de maintenance et les programmes en arrière-plan
 - Reporter les mises à jour automatiques de Windows
 - Ajuster les paramètres du plan d'alimentation pour les jeux
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des jeux à la Liste des jeux.

Si Bitdefender ne passe pas automatiquement en Profil Jeu lorsque vous lancez un jeu ou une application spécifique, vous pouvez ajouter manuellement cette application à la **Liste des Jeux**.

Pour ajouter manuellement des jeux à la liste des Jeux dans le Profil Jeu :




1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface Bitdefender.
2. Sélectionnez l'onglet **Profils**.
3. Assurez-vous que l'option **Profils** est activée.
4. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Jeu.
5. Dans la fenêtre **PROFIL JEU**, cliquez sur le lien **Liste des Jeux**.
6. Cliquez sur **Ajouter** pour ajouter un nouveau jeu à la **Liste des Jeux**.
Une nouvelle fenêtre apparaît. Localisez le fichier exécutable du jeu, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

30.4. Profil Wifi public

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

Configurer le profil Wi-Fi public

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'interface Bitdefender.
2. Sélectionnez l'onglet **Profils**.
3. Assurez-vous que l'option **Profils** est activée.
4. Cliquez sur le bouton **CONFIGURER** dans la zone Profil Wi-Fi Public.
5. Laissez cochée la case **Ajuster les paramètres du produit pour renforcer la protection en cas de connexion à un réseau Wi-Fi public non sécurisé**.
6. Cliquez sur **Enregistrer**.




30.5. Profil Mode batterie

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

Configurer le Mode Batterie

Pour configurer le Mode Batterie :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Profils**.
3. Assurez-vous que l'option **Profils** est activée.
4. Cliquez sur le bouton **CONFIGURER** dans la zone Mode Batterie.
5. Sélectionnez les réglages du système à appliquer en cochant les options suivantes :
 - Optimiser les paramètres du produit pour le mode Batterie.
 - Reporter les tâches des programmes en arrière-plan et de maintenance.
 - Reporter les mises à jour automatiques de Windows.
 - Ajuster les paramètres du plan d'alimentation pour le mode Batterie.
 - Désactiver les appareils externes et les ports du réseau.
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

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

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

- La mise à jour automatique de Bitdefender est reportée.
- Les analyses planifiées sont reportées.
- Le **Widget Windows** est désactivé.




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

30.6. Optimisation en temps réel

L'Optimisation en temps réel de Bitdefender est un plugin qui améliore les performances de votre système discrètement, en arrière-plan, en veillant à ce que vous ne soyez pas interrompu lorsque vous êtes en mode profil. En fonction de la charge du processeur, le plugin surveille tous les processus, en particulier ceux qui ont une charge plus élevée, afin de les adapter à vos besoins.

Pour activer ou désactiver l'Optimisation en temps réel :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Profils**.
3. Utilisez le bouton correspondant pour activer ou désactiver l'Optimisation en temps réel.



RÉSOLUTION DES PROBLÈMES



31. RÉSOUDRE LES PROBLÈMES LES PLUS FRÉQUENTS

Ce chapitre présente certains problèmes que vous pouvez rencontrer lorsque vous utilisez Bitdefender et vous fournit des solutions possibles à ces problèmes. La plupart de ces problèmes peuvent être résolus via la configuration appropriée des paramètres du produit.

- « *Mon système semble lent* » (p. 207)
- « *L'analyse ne démarre pas* » (p. 209)
- « *Je ne peux plus utiliser une application* » (p. 212)
- « *Que faire lorsque Bitdefender bloque un site web ou une application en ligne sûre* » (p. 214)
- « *Que faire si Bitdefender détecte une application fiable comme ransomware* » (p. 214)
- « *Comment mettre à jour Bitdefender avec une connexion Internet lente ?* » (p. 220)
- « *Le Services Bitdefender ne répondent pas* » (p. 220)
- « *Le filtre antispam ne fonctionne pas correctement* » (p. 221)
- « *La fonctionnalité saisie automatique de mon Wallet ne fonctionne pas* » (p. 226)
- « *La désinstallation de Bitdefender a échoué* » (p. 227)
- « *Mon système ne démarre pas après l'installation de Bitdefender* » (p. 229)

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du soutien technique Bitdefender comme indiqué dans le chapitre « *Assistance* » (p. 244).

31.1. Mon système semble lent

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

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



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

Bien que Bitdefender recherche et supprime les programmes de sécurité trouvés pendant l'installation, il est recommandé de supprimer tout programme antivirus que vous utilisiez avant d'installer Bitdefender. Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 88).

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

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

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

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




Important

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

- **Votre système peut être infecté.**

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

Pour commencer l'Analyse système :

1. Cliquer sur  l'icône dans le coin en bas à gauche de l'**interface Bitdefender**.



2. Cliquez sur le lien **VOIR MODULES**.
3. Sous le module **ANTIVIRUS**, sélectionnez **Analyse système**.
4. Suivez les étapes de l'assistant.

31.2. L'analyse ne démarre pas

Ce type de problème peut avoir deux causes principales :

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

Dans ce cas :

1. Désinstaller complètement Bitdefender du système :

- Dans **Windows 7** :

- a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
- b. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
- c. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
- d. Cliquez sur **CONTINUER**.
- e. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

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

- a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
- b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.



- c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - d. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - e. Cliquez sur **CONTINUER**.
 - f. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
 - Dans **Windows 10** :
 - a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
 - b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
 - c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
 - e. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - f. Cliquez sur **CONTINUER**.
 - g. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
2. Réinstallez votre produit Bitdefender.
- **Bitdefender n'est pas la seule solution de sécurité installée sur votre système.**

Dans ce cas :



1. Supprimer l'autre solution de sécurité. Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 88).
2. Désinstaller complètement Bitdefender du système :
 - Dans **Windows 7** :
 - a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
 - b. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - c. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - d. Cliquez sur **CONTINUER**.
 - e. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
 - Dans **Windows 8 et Windows 8.1** :
 - a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
 - b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
 - c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - d. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets



- Coffres-forts
 - e. Cliquez sur **CONTINUER**.
 - f. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
 - Dans **Windows 10** :
 - a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
 - b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
 - c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
 - e. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - f. Cliquez sur **CONTINUER**.
 - g. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
3. Réinstallez votre produit Bitdefender.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).

31.3. Je ne peux plus utiliser une application

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

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

- Vous pourriez recevoir un message de Bitdefender indiquant que le programme essaie d'apporter une modification au système.





- Il est possible que vous receviez un message d'erreur du programme que vous tentez d'utiliser.

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

Active Threat Control est un module Bitdefender qui surveille en permanence les applications s'exécutant sur votre système et signale celles au comportement potentiellement malveillant. Étant donné que la fonction est basée sur un système heuristique, des applications légitimes peuvent, dans certains cas, être signalées par Active Threat Control.

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

Pour ajouter un programme à la liste d'exclusions :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
4. Sélectionnez l'onglet **Exclusions**.
5. Cliquez sur le menu déroulant **Liste des processus exclus de l'Analyse**. Dans la fenêtre qui apparaît, vous pouvez gérer les exclusions de processus Active Threat Control.
6. Ajoutez des exclusions en suivant ces étapes :
 - a. Cliquez sur le bouton **AJOUTER**.
 - b. Cliquez sur **Parcourir**, sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.
 - c. Gardez l'option **Autoriser** sélectionnée pour empêcher Active Threat Control de bloquer l'application.
 - d. Cliquez sur **Ajouter**.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « **Assistance** » (p. 244).





31.4. Que faire lorsque Bitdefender bloque un site web ou une application en ligne sûre

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

Si une page ou une application est bloquée de façon répétée, elle peut être ajoutée à une liste blanche afin de ne pas être analysée par les moteurs de Bitdefender et de permettre une navigation sans interruptions.

Pour ajouter un site Web à la **Liste blanche** :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **WEBPROTECTION**.
4. Cliquez sur le lien **Liste blanche**.
5. Indiquez l'adresse du site Web ou d'une application en ligne bloquée dans le champ correspondant et cliquez sur **Ajouter**.
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

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

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).

31.5. Que faire si Bitdefender détecte une application fiable comme ransomware


Le ransomware est un programme malveillant qui essaye de soutirer de l'argent aux utilisateurs en fermant leur système vulnérable. Pour protéger



vosre système des situations dangereuses, Bitdefender vous donne la possibilité d'indemniser des fichiers personnels.

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



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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **Protection contre les ransomwares**, sélectionnez **Applications bloquées**.
4. Cliquez sur **Autoriser** pour sélectionner l'application dont vous êtes certain qu'elle est fiable.
5. Cliquez sur **OK** pour ajouter l'application sélectionnée à la liste de confiance.

31.6. Je ne peux pas me connecter à Internet

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

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

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
4. Sélectionnez l'onglet **Règles**.
5. Pour ajouter une règle d'application, cliquez sur le bouton **Ajouter une règle**.



6. Une nouvelle fenêtre apparaît dans laquelle vous pouvez ajouter les informations. Veillez à sélectionner tous les types de réseau disponibles et sélectionnez **Autoriser** dans la section **Permission**.

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

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).



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

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

Dans ce cas, la meilleure solution est de configurer Bitdefender afin qu'il autorise automatiquement les connexions de et vers le périphérique en question. Pour chaque connexion réseau vous pouvez configurer une zone spéciale de confiance.

Une zone de confiance est un périphérique auquel vous faites entièrement confiance. Tout le trafic entre votre ordinateur et le périphérique de confiance est autorisé. Pour partager des ressources avec des périphériques spécifiques, tels que des ordinateurs ou des imprimantes, ajoutez-les comme zones de confiance.

Pour ajouter une zone fiable sur vos adaptateurs réseaux :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
4. Sélectionnez l'onglet **Adaptateurs**.
5. Pour ajouter une zone, cliquez sur le lien **Exceptions réseau**.
6. Tapez l'adresse IP de l'ordinateur ou l'imprimante à ajouter dans le champ correspondant.



7. Dans la colonne **Adaptateur** sélectionnez **Fiable**.
8. Dans la colonne **Permission** sélectionnez **Autoriser**.
9. Cliquez sur le bouton + pour ajouter l'exception et fermez la fenêtre.

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

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

- Le pare-feu de l'autre ordinateur peut bloquer le partage de fichiers et d'imprimantes avec celui-ci.
- Si le pare-feu Windows est utilisé, il peut être configuré pour autoriser le partage de fichiers et d'imprimantes comme suit :
 - Dans **Windows 7** :
 1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et sélectionnez **Système et sécurité**.
 2. Allez dans **Pare-feu Windows** puis cliquez sur **Autoriser un programme via le Pare-feu Windows**.
 3. Cochez la case **Partage de fichiers et d'imprimantes**.
 - Dans **Windows 8 et Windows 8.1** :
 1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
 2. Cliquez sur **Système et sécurité**, allez dans **Pare-feu Windows** et sélectionnez **Autoriser une application via le pare-feu Windows**.
 3. Cochez la case **Partage de fichiers et d'imprimantes** puis cliquez sur **OK**.
 - Dans **Windows 10** :
 1. Tapez "Autoriser un programme via le Pare-feu Windows" dans le champ de recherche de la barre des tâches et cliquez sur son icône.
 2. Cliquez sur **Changer les paramètres**.
 3. Cochez la case **Partage de fichiers et d'imprimantes** dans la liste **Applications autorisées** puis cliquez sur **OK**.



- Si un autre programme pare-feu est utilisé, veuillez vous reporter à sa documentation ou au fichier d'aide.
- Conditions générales pouvant empêcher d'utiliser ou de se connecter à une imprimante partagée :
 - Il se peut que vous ayez besoin de vous connecter à un compte Windows administrateur pour avoir accès à l'imprimante partagée.
 - L'imprimante partagée est configurée pour autoriser l'accès uniquement à certains ordinateurs et utilisateurs. Si vous partagez votre imprimante, vérifiez que l'imprimante autorise l'accès à l'utilisateur de l'autre ordinateur. Si vous essayez de vous connecter à une imprimante partagée, vérifiez avec l'utilisateur de l'autre ordinateur que vous êtes autorisé(e) à vous connecter à l'imprimante.
 - L'imprimante connectée à votre ordinateur ou à l'autre ordinateur n'est pas partagée.
 - L'imprimante partagée n'a pas été ajoutée à l'ordinateur.



Note

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

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



Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).

31.8. Mon Internet est lent

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



Pour régler ce problème :



1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
4. Cliquez sur le bouton correspondant pour activer ou désactiver **Pare-feu**.
5. Vérifiez si votre connexion Internet s'est améliorée avec le pare-feu Bitdefender désactivé.

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

Si vous recevez la confirmation de votre fournisseur d'accès à Internet que la connexion est opérationnelle de leur côté et que le problème persiste, contactez Bitdefender comme cela est décrit dans la section « *Assistance* » (p. 244).

- Si la connexion Internet s'est améliorée après la désactivation du pare-feu Bitdefender :
 - a. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
 - b. Cliquez sur le lien **VOIR MODULES**.
 - c. Sélectionnez l'  icône dans le coin en haut à droite dans le module **FIREWALL**.
 - d. Dans l'onglet **Paramètres** cliquez sur le bouton pour désactiver **Bloquer analyse des ports dans le réseau**.
 - e. Allez dans l'onglet **Adaptateurs** et sélectionnez votre connexion Internet.
 - f. Dans la colonne **Type de Réseau**, sélectionnez **Domicile/Bureau**.
 - g. Dans la colonne **Mode Furtif** sélectionnez **Activé**. Réglez la colonne **Générique** sur **Activé**.
 - h. Fermez Bitdefender, redémarrez le système et vérifiez la vitesse de la connexion à Internet.




Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).

31.9. Comment mettre à jour Bitdefender avec une connexion Internet lente ?

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

Pour maintenir votre système à jour avec les dernières signatures de malwares Bitdefender :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Sélectionnez l'onglet **Mise à jour**.
3. À côté de **Règles de traitement**, sélectionnez **Demander avant le téléchargement** dans le menu déroulant.
4. Retournez dans la fenêtre principale et cliquez sur le bouton d'action **Mise à jour** dans l'interface Bitdefender.
5. Sélectionnez uniquement **Mises à jour de signatures**, puis cliquez sur **OK**.
6. Bitdefender ne téléchargera et n'installera que les mises à jour des signatures de malwares.

31.10. Le Services Bitdefender ne répondent pas

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

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

L'erreur peut être causée par :

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



Pour régler cette erreur, essayez ces solutions :

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

Pour plus d'informations, reportez-vous à « *Comment supprimer les autres solutions de sécurité ?* » (p. 88).

Si l'erreur persiste, veuillez contacter les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la section « *Assistance* » (p. 244).

31.11. Le filtre antispam ne fonctionne pas correctement

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

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

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

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

Bitdefender ajoute automatiquement les destinataires de vos e-mails à une Liste d'Amis. Les e-mails que vous recevez des contacts de la Liste d'Amis



sont considérés comme légitimes. Ils ne sont pas vérifiés par le filtre antispam et ne sont donc jamais signalés comme étant du [spam].

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

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

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




Note

Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 122).

Ajouter des contacts à la Liste d'amis


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

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

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



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

1. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **ANTISPAM**, sélectionnez **Gérer les amis**.
Une fenêtre de configuration s'affichera.
4. Tapez l'adresse e-mail à partir de laquelle vous souhaitez toujours recevoir les messages d'e-mail puis cliquez sur **Ajouter**. Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Indiquer des erreurs de détection

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

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



31.11.2. De nombreux messages de spam ne sont pas détectés

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

Essayez les solutions suivantes :

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




Note

Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à « *Clients et protocoles de messagerie pris en charge* » (p. 122).

2. **Ajouter des spammeurs à la liste des Spammeurs** Les messages provenant d'adresses qui figurent dans la liste de Spammeurs seront automatiquement considérés comme étant du [spam].

Indiquer les messages de spam non détectés


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

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




Ajouter des spammeurs à la Liste des Spammeurs

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement ajouter les expéditeurs de spam à la liste de Spammeurs. Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez les messages signalés comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton  **Ajouter Spammeur** de la barre d'outils antispam Bitdefender.
5. Il se peut qu'on vous demande de valider les adresses ajoutées à la liste de Spammeurs. Sélectionnez **Ne plus afficher ce message** et cliquez sur **OK**.


Si vous utilisez un autre client de messagerie, vous pouvez ajouter manuellement des spammeurs à la liste des Spammeurs à partir de l'interface de Bitdefender. Cela s'avère utile lorsque vous avez reçu plusieurs e-mails de spam provenant de la même adresse e-mail. Suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **ANTISPAM**, sélectionnez **Gérer les spammers**.
Une fenêtre de configuration s'affichera.
4. Tapez l'adresse e-mail du spammeur puis cliquez sur **Ajouter**. Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

31.11.3. Le filtre antispam ne détecte aucun message de spam.

Si aucun message de spam n'est signalé comme étant du [spam], il se peut qu'il y ait un problème avec le filtre Antispam de Bitdefender. Avant d'essayer de régler ce problème, assurez-vous qu'il n'est pas causé par l'une des situations suivantes :



- La protection antispam pourrait être désactivée. Pour vérifier l'état de la protection anti-spam, cliquez sur l'icône  sur la barre latérale gauche de l'**Interface Bitdefender** puis sélectionnez le lien **Voir modules**. Cliquez sur la roue dentée dans le panneau **ANTISPAM**, puis regardez dans la partie supérieure de la fenêtre pour vérifier si le module est activé.
Si l'Antispam est désactivé, il s'agit de la cause de votre problème. Cliquez sur le bouton correspondant pour activer votre protection antispam.
- La protection Bitdefender Antispam est disponible seulement pour les clients de messagerie configurés pour recevoir des e-mails via le protocole POP3. Cela signifie que :
 - Les e-mails reçus via des services de webmail (tels que Yahoo, Gmail, Hotmail ou d'autres) ne font pas l'objet d'une analyse antispam de la part de Bitdefender.
 - Si votre client de messagerie est configuré pour recevoir des e-mails en utilisant un protocole autre que POP3 (par exemple IMAP4), vos e-mails ne seront pas analysés par Bitdefender Antispam.



Note

POP3 est l'un des protocoles les plus utilisés pour télécharger des e-mails à partir d'un serveur de messagerie. Si vous ne connaissez pas le protocole que votre client de messagerie utilise pour télécharger des e-mails, posez la question à la personne ayant configuré votre client de messagerie.

- Bitdefender Total Security 2017 n'analyse pas le trafic POP3 de Lotus Notes.

Une solution possible consiste à réparer ou à réinstaller le produit. Il est toutefois recommandé de contacter Bitdefender pour obtenir de l'assistance, comme cela est décrit dans la section « *Assistance* » (p. 244).

31.12. La fonctionnalité saisie automatique de mon Wallet ne fonctionne pas

Vous avez enregistré vos identifiants en ligne dans votre Bitdefender le Gestionnaire de mots de passe et avez remarqué que la saisie automatique ne fonctionne pas. Ce problème se produit généralement lorsque l'extension de Bitdefender Wallet n'est pas installée dans votre navigateur.

Pour résoudre cette situation, suivez ces étapes :



● Dans **Internet Explorer** :

1. Ouvrez Internet Explorer.
2. Cliquez sur Outils.
3. Cliquez sur Gérer les modules.
4. Cliquez sur Barres d'outils et Extensions.
5. Pointez sur **Bitdefender Wallet** et cliquez sur **Permettre**.

● Dans **Mozilla Firefox** :

1. Ouvrez Mozilla Firefox.
2. Cliquez sur Outils.
3. Cliquez sur Modules.
4. Cliquez sur Extensions.
5. Pointez sur **Bitdefender Wallet** et cliquez sur **Permettre**.

● Dans **Google Chrome** :

1. Ouvrez Google Chrome.
2. Allez sur l'icône du Menu.
3. Cliquez sur Paramètres.
4. Cliquez sur Extensions.
5. Pointez sur **Bitdefender Wallet** et cliquez sur **Permettre**.



Note

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

Vérifiez maintenant que la fonctionnalité de saisie automatique de Wallet fonctionne pour vos comptes en ligne.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).

31.13. La désinstallation de Bitdefender a échoué

Si vous souhaitez supprimer votre produit Bitdefender et remarquez que le processus se bloque ou que le système se fige, cliquez sur **Annuler** pour annuler l'action. Si cela ne fonctionne pas, redémarrez le système.



Lorsque la désinstallation échoue, certaines clés de registre et fichiers de Bitdefender peuvent demeurer sur votre système. De tels restes peuvent empêcher une nouvelle installation de Bitdefender. Ils peuvent aussi affecter la performance du système et sa stabilité.

Afin de supprimer complètement Bitdefender de votre système :

● Dans **Windows 7** :

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
2. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
3. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
4. Cliquez sur **CONTINUER**.
5. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

● Dans **Windows 8 et Windows 8.1** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
4. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
5. Cliquez sur **CONTINUER**.



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

● Dans **Windows 10** :

1. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
2. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
3. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
4. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
5. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
6. Cliquez sur **CONTINUER**.
7. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

31.14. Mon système ne démarre pas après l'installation de Bitdefender

Si vous venez d'installer Bitdefender et ne pouvez plus redémarrer votre système en mode normal, il peut y avoir plusieurs raisons à ce problème.

Cela est sans doute dû à une installation précédente de Bitdefender qui n'a pas été désinstallée correctement ou à une autre solution de sécurité toujours présente sur le système.

Voici comment faire face à chaque situation :

● **Vous aviez Bitdefender et vous ne l'avez pas désinstallé correctement.**

Pour le résoudre :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 90).
2. Désinstallez Bitdefender de votre système :



- Dans **Windows 7** :
 - a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
 - b. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - c. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - d. Cliquez sur **CONTINUER**.
 - e. Patientez jusqu'à la fin du processus de désinstallation.
 - f. Redémarrez votre système en mode normal.
- Dans **Windows 8 et Windows 8.1** :
 - a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
 - b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
 - c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
 - d. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
 - e. Cliquez sur **CONTINUER**.
 - f. Patientez jusqu'à la fin du processus de désinstallation.



g. Redémarrez votre système en mode normal.

● Dans **Windows 10** :

- a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
- b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
- c. Localisez **Bitdefender Total Security 2017** et sélectionnez **Désinstaller**.
- d. Cliquez à nouveau sur **Désinstaller** pour confirmer votre choix.
- e. Cliquez sur **SUPPRIMER** dans la fenêtre qui apparaît, puis choisissez quelle donnée doit être sauvegardée pour une installation ultérieure :
 - Fichiers en quarantaine
 - Wallets
 - Coffres-forts
- f. Cliquez sur **CONTINUER**.
- g. Patientez jusqu'à la fin du processus de désinstallation.
- h. Redémarrez votre système en mode normal.

3. Réinstallez votre produit Bitdefender.

● **Vous aviez une autre solution de sécurité auparavant et vous ne l'avez pas désinstallée correctement.**

Pour le résoudre :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 90).
2. Désinstallez l'autre solution de sécurité de votre système :

● Dans **Windows 7** :

- a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
- b. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.



- c. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Dans **Windows 8 et Windows 8.1** :
 - a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
 - b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
 - c. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.
 - d. Attendez la fin du processus de désinstallation, puis redémarrez votre système.
- Dans **Windows 10** :
 - a. Cliquez sur **Démarrer**, puis cliquez sur "Paramètres".
 - b. Cliquez sur l'icône **System** dans les paramètres, puis sélectionnez **Applications installées**.
 - c. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
 - d. Attendez la fin du processus de désinstallation, puis redémarrez votre système.

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

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

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

Pour le résoudre :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 90).
2. Utilisez l'option Restauration du système de Windows pour restaurer l'ordinateur à une date antérieure à l'installation du produit Bitdefender.



3. Redémarrez le système en mode normal et contactez les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la section « *Assistance* » (p. 244).



32. SUPPRESSION DES MALWARES DE VOTRE SYSTÈME

Les logiciels malveillants peuvent affecter votre système de nombreuses manières et l'approche de Bitdefender dépend du type d'attaque. Les virus changeant souvent de comportement, il est difficile de définir leur comportement et leurs actions.

Il s'agit des situations où Bitdefender ne peut supprimer automatiquement l'infection de malwares de votre système. Dans ce cas, votre intervention est nécessaire.

- « *Mode de Secours de Bitdefender* » (p. 234)
- « *Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?* » (p. 236)
- « *Comment nettoyer un virus dans une archive ?* » (p. 238)
- « *Comment nettoyer un virus dans une archive de messagerie ?* » (p. 239)
- « *Que faire si je suspecte un fichier d'être dangereux ?* » (p. 240)
- « *Que sont les fichiers protégés par mot de passe du journal d'analyse ?* » (p. 241)
- « *Que sont les éléments ignorés du journal d'analyse ?* » (p. 241)
- « *Que sont les fichiers ultra-compressés du journal d'analyse ?* » (p. 242)
- « *Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?* » (p. 242)

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du soutien technique Bitdefender comme indiqué dans le chapitre « *Assistance* » (p. 244).

32.1. Mode de Secours de Bitdefender

Le **Mode de secours** est une fonctionnalité de Bitdefender qui vous permet d'analyser et de désinfecter toutes les partitions de votre disque dur hors de votre système d'exploitation.

Une fois Bitdefender Total Security 2017 installé, le Mode de secours peut être utilisé même si vous ne pouvez plus démarrer sous Windows.




Démarrer votre système en mode de secours

Vous pouvez entrer en mode de secours de l'une des deux façons suivantes :

À partir de **l'interface de Bitdefender**

Pour passer en Mode secours directement dans Bitdefender :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Cliquez sur le lien **VOIR MODULES**.
3. Dans le module **Antivirus**, sélectionnez **Mode de secours**.
Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour redémarrer votre ordinateur.
4. Après le redémarrage de l'ordinateur, un menu apparaîtra vous demandant de sélectionner un système d'exploitation. Sélectionnez **Mode de secours de Bitdefender** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.
5. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.

Le Mode de secours de Bitdefender se chargera dans quelques instants.

Démarrez votre ordinateur directement en mode de secours

Si Windows ne démarre plus, vous pouvez démarrer directement votre ordinateur en Mode de secours de Bitdefender en suivant les étapes ci-dessous:

1. Démarrez / redémarrez votre ordinateur et appuyez sur la touche **espace** de votre clavier avant que n'apparaisse le logo Windows.
2. Un menu apparaîtra vous demandant de sélectionner un système d'exploitation à démarrer. Cliquez sur **ONGLET** pour vous rendre dans la zone d'outils. Sélectionnez **Image de secours de Bitdefender** et appuyez sur la touche **Entrée** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.
3. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.



Le Mode de secours de Bitdefender se chargera dans quelques instants.

Analyser votre système en mode de secours

Pour analyser votre système en Mode de Secours :

1. Entrez en mode de secours, comme indiqué dans « **Démarrer votre système en mode de secours** » (p. 235).
2. Le logo Bitdefender apparaîtra et les moteurs antivirus commenceront à être copiés.
3. Une fenêtre d'accueil apparaîtra. Cliquez sur **Continuer**.
4. Une mise à jour des signatures antivirus a démarré.
5. Une fois la mise à jour terminée, la fenêtre du Scanner Antivirus à la demande Bitdefender s'affiche.
6. Cliquez sur **Analyser**, sélectionnez la cible de l'analyse dans la fenêtre qui s'affiche puis cliquez sur **Ouvrir** pour lancer l'analyse.

Nous vous recommandons l'analyse de la totalité de votre partition Windows.

Note

En mode de secours, les noms de partitions sont de type Linux. Des partitions de disque apparaîtront, sda1 correspondant probablement à la partition de type Windows (C:), sda2 correspondant à (D:), etc.

7. Patientez jusqu'à la fin de l'analyse. Si un malware est détecté, suivez les instructions pour supprimer la menace.
8. Pour quitter le mode de secours, faites un clic droit sur une zone vide du bureau, sélectionnez **Quitter** dans le menu qui apparaît puis choisissez de redémarrer ou d'éteindre l'ordinateur.

32.2. Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?

Il est possible que vous découvriez qu'un virus se trouve sur votre ordinateur de l'une des manières suivantes :



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

Dans de telles situations, mettez à jour Bitdefender pour vous assurer de disposer des dernières signatures de malwares puis exécutez une analyse du système.



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

Avertissement

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

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

La première méthode peut être utilisée en mode normal :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
 - a. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
 - b. Sélectionnez le lien **VOIR MODULES**.
 - c. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
 - d. Cliquez sur le bouton correspondant pour désactiver l'**Analyse à l'accès**.
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 88).
3. Accédez à l'emplacement du fichier infecté (consultez le journal d'analyse), puis supprimez-le.
4. Activez la protection antivirus en temps réel de Bitdefender.

Si la première méthode n'a pas réussi à supprimer l'infection :



1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez « *Comment redémarrer en mode sans échec ?* » (p. 90).
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez « *Comment afficher des objets cachés dans Windows ?* » (p. 88).
3. Accédez à l'emplacement du fichier infecté (consultez le journal d'analyse), puis supprimez-le.
4. Redémarrez votre système et entrez en mode normal.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).

32.3. Comment nettoyer un virus dans une archive ?


Une archive est un fichier ou un ensemble de fichiers compressés sous un format spécial pour réduire l'espace nécessaire sur le disque pour stocker les fichiers.

Certains de ces formats sont des formats ouverts, permettant ainsi à Bitdefender de les analyser, puis de mener les actions appropriées pour les supprimer.


D'autres formats d'archive sont fermés partiellement ou totalement, et Bitdefender peut uniquement détecter la présence de virus dans ceux-ci, mais n'est pas capable de mener d'autres actions.

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

Voici comment nettoyer un virus stocké dans une archive :

1. Identifiez l'archive où se trouve le virus en réalisant une analyse du système.
2. Désactivez la protection antivirus en temps réel de Bitdefender :
 - a. Cliquez sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
 - b. Sélectionnez le lien **VOIR MODULES**.



- c. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
- d. Dans la fenêtre **Bouclier**, cliquez sur le bouton correspondant pour activer ou désactiver **l'Analyse à l'accès**.
3. Rendez-vous à l'emplacement de l'archive et décompressez-la à l'aide d'une application d'archivage, comme WinZip.
4. Identifier le fichier infecté et le supprimer.
5. Supprimez l'archive d'origine afin de vous assurer que l'infection est totalement supprimée.
6. Recompresses les fichiers dans une nouvelle archive à l'aide d'une application d'archivage, comme WinZip.
7. Activez la protection antivirus en temps réel de Bitdefender et exécutez une analyse du système afin de vous assurer qu'aucune autre infection n'est présente sur le système.



Note

Il est important de noter qu'un virus contenu dans une archive ne représente pas de menace immédiate pour votre système, puisque, pour infecter votre système, le virus doit être décompressé et exécuté.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).

32.4. Comment nettoyer un virus dans une archive de messagerie ?



Bitdefender permet également de repérer les virus dans les bases de données d'e-mails et les archives d'e-mails stockées sur le disque.

Il est parfois nécessaire d'identifier le message infecté à l'aide des informations du rapport d'analyse, et de le supprimer manuellement.

Voici comment nettoyer un virus stocké dans une archive de messagerie électronique :

1. Analysez la base de données des courriels avec Bitdefender.
2. Désactivez la protection antivirus en temps réel de Bitdefender :



- a. Cliquez sur  l'icône dans le coin en bas à gauche de l'interface **Bitdefender**.
 - b. Sélectionnez le lien **VOIR MODULES**.
 - c. Sélectionnez l'  icône dans le coin en haut à droite dans le module **ANTIVIRUS**.
 - d. Cliquez sur le bouton correspondant pour désactiver l'**Analyse à l'accès**.
3. Ouvrez le rapport d'analyse et utilisez les informations d'identification (Sujet, Expéditeur, Destinataire) des messages infectés pour les localiser dans le client de messagerie.
 4. Supprimez les messages infectés. La plupart des clients de messagerie placent les messages supprimés dans un dossier de récupération permettant de les restaurer. Il est recommandé de vous assurer que le message a été supprimé également dans ce dossier de récupération.
 5. Comprimez le dossier contenant le message infecté.
 - Dans Microsoft Outlook 2007 : Dans le menu Fichier, cliquez sur Gestion des fichiers de données. Sélectionnez les dossiers de fichiers personnels (.pst) que vous souhaitez compresser, puis cliquez sur Configuration. Cliquez sur Compresser.
 - Dans Microsoft Outlook 2010 / 2013 : Dans le menu Fichier, cliquez sur Infos puis sur Paramètres du compte (Ajouter et supprimer des comptes ou modifier les paramètres de connexion existants). Cliquez ensuite sur Fichier de données, sélectionnez les fichiers des dossiers personnels (.pst) que vous souhaitez compacter puis cliquez sur Paramètres. Cliquez sur Compresser.
 6. Activez la protection antivirus en temps réel de Bitdefender.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Assistance* » (p. 244).

32.5. Que faire si je suspecte un fichier d'être dangereux ?

Vous pouvez suspecter qu'un fichier de votre système est dangereux, même si votre produit Bitdefender ne l'a pas détecté.

Pour vous assurer que votre système est protégé :



1. Exécuter une **Analyse du système** avec Bitdefender. Pour savoir comment faire cela, reportez-vous à « *Comment analyser mon système ?* » (p. 66).
2. Si le résultat de l'analyse n'indique pas d'infection, mais que vous avez encore des doutes et souhaitez vérifier le fichier, contactez les représentants de notre soutien technique afin que nous puissions vous aider.
Pour savoir comment faire cela, consultez « *Assistance* » (p. 244).

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

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

Les éléments protégés par un mot de passe sont généralement :

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

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

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

Nous vous recommandons d'ignorer ces fichiers car ils ne constituent pas une menace pour votre système.

32.7. Que sont les éléments ignorés du journal d'analyse ?

Tous les fichiers apparaissant comme ignorés dans le rapport d'analyse sont sains.

Pour de meilleures performances, Bitdefender n'analyse pas les fichiers n'ayant pas été modifiés depuis la dernière analyse.



32.8. Que sont les fichiers ultra-compressés du journal d'analyse ?

Les éléments ultra-compressés sont des éléments qui n'ont pas pu être extraits par le moteur d'analyse ou des éléments dont le temps de déchiffrement aurait été trop long et aurait rendu le système instable.

Surcompressé signifie que Bitdefender a ignoré l'analyse dans cette archive car sa décompression consommait trop de ressources système. Le contenu sera analysé à l'accès en temps réel si nécessaire.

32.9. Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?

Si un fichier infecté est détecté, Bitdefender tente automatiquement de le désinfecter. Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection.

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

C'est généralement le cas avec les fichiers d'installation qui sont téléchargés depuis des sites non fiables. Si vous vous trouvez dans une telle situation, téléchargez le fichier d'installation sur le site Web du fabricant ou sur un autre site de confiance.



CONTACT



33. ASSISTANCE

Bitdefender fournit à ses clients une aide hors pair, rapide et efficace. Si vous rencontrez le moindre problème ou si vous avez des questions sur votre produit Bitdefender, vous pouvez utiliser plusieurs ressources en ligne pour trouver rapidement une solution ou une réponse. Vous pouvez également contacter l'équipe du Service Client de Bitdefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.

La section « *Résoudre les problèmes les plus fréquents* » (p. 207) fournit les informations nécessaires concernant les problèmes les plus fréquents que vous pouvez rencontrer lors de l'utilisation de ce produit.


Si vous ne trouvez pas de réponse à votre question dans les ressources fournies, vous pouvez nous contacter directement :

- « **Contactez-nous directement à partir de votre produit Bitdefender** » (p. 244)
- « **Contactez-nous via notre Centre de Support en ligne** » (p. 245)

Contactez-nous directement à partir de votre produit Bitdefender

Si vous disposez d'une connexion Internet, vous pouvez contacter l'assistance de Bitdefender directement à partir de l'interface du produit.

Suivez ces étapes :

1. Cliquer sur  l'icône dans le coin en bas à gauche de **l'interface Bitdefender**.
2. Vous disposez des options suivantes :
 - **Documentation du produit**
Accédez à notre base de données et recherchez les informations nécessaires.
 - **Support Technique**
Utilisez le bouton **Contactez le Support** pour lancer l'Outil Support de Bitdefender et contacter le Support Client. Vous pouvez naviguer dans



l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

- a. Cochez la case d'accord et cliquez sur **Suivant**.
- b. Compléter le formulaire de soumission avec les données nécessaires :
 - i. Saisissez votre adresse e-mail.
 - ii. Indiquez votre nom complet.
 - iii. Décrivez le problème que vous avez rencontré.
 - iv. Sélectionnez l'option **Essayer de reproduire le problème avant la soumission** si vous rencontrez un problème avec le produit. Poursuivez avec les étapes requises.
- c. Veuillez patienter pendant quelques minutes pendant que Bitdefender recueille les informations sur le produit. Ces informations aideront nos ingénieurs à trouver une solution à votre problème.
- d. Cliquez sur **Terminer** pour envoyer les informations au Service Client de Bitdefender. Nous vous contacterons dès que possible.

● Trouver de l'aide en ligne

Accédez à nos articles en ligne.

Contactez-nous via notre Centre de Support en ligne

Si vous ne parvenez pas à accéder aux informations nécessaires à l'aide du produit Bitdefender, consultez notre Centre de Support en ligne :

1. Allez à <http://www.bitdefender.fr/support/consumer.html>.

Le Centre de Support de Bitdefender contient de nombreux articles apportant des solutions aux problèmes liés à Bitdefender.

2. Utilisez la barre de recherche en haut de la fenêtre pour trouver des articles susceptibles d'apporter une solution à votre problème. Pour effectuer une recherche, saisissez simplement un terme dans la barre de recherche et cliquez sur **Rechercher**.
3. Consultez les articles et les documents pertinents et essayez les solutions proposées.
4. Si la solution ne règle pas votre problème, allez dans



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

33.1. Assistance téléphonique :

Les Laboratoires Bitdefender mettent en oeuvre tous les efforts commercialement envisageables pour maintenir l'accès à l'assistance téléphonique de ce service, pendant les heures ouvrées locales du lundi au vendredi, sauf pendant les jours fériés.

Accès téléphoniques aux Laboratoires Bitdefender :

- **Pour la France et les DOM-TOM** : 0892 561 161 (0.40 euros / minute)
- **Pour la Belgique** : 070 35 83 04
- **Pour la Suisse** : 0900 000 118 (0,60 FS / minute)

Avant de nous appeler, munissez-vous :

- du numéro de licence du produit Bitdefender. Communiquez le à un de nos analystes afin qu'il vérifie votre niveau d'assistance.
- de la version actuelle du système d'exploitation.
- des informations sur les marques et modèles de tous les périphériques et des logiciels chargés en mémoire ou utilisés.

En cas d'infection, l'analyste pourra demander une liste d'informations techniques à fournir ainsi que certains fichiers, qui pourront être nécessaires à son diagnostic.

Lorsqu'un analyste vous le demande, précisez les messages d'erreurs reçus et le moment où ils apparaissent, les activités qui ont précédées le message d'erreur et les démarches déjà entreprises pour résoudre le problème.

L'analyste suivra une procédure de dépannage stricte afin de tenter de diagnostiquer le problème.

Le Service n'inclut pas les éléments suivants :

- Ce service d'assistance ne comprend pas les applications, les installations, la désinstallation, le transfert, la maintenance préventive, la formation, l'administration à distance ou configurations logicielles autres que celles spécifiquement notifiées par l'analyste des Laboratoires Bitdefender lors de l'intervention.



- L'installation, le paramétrage, l'optimisation et la configuration en réseau ou à distance d'applications n'entrant pas dans le cadre de l'assistance actuelle.
- Sauvegarde des logiciels/données. Il incombe au Client d'effectuer une sauvegarde de toutes les données, des logiciels et des programmes existants sur les systèmes d'information pris en charge avant toute prestation de service par Bitdefender.

Bitdefender NE PEUT ÊTRE TENUS RESPONSABLE DE LA PERTE OU DE LA RÉCUPÉRATION DE DONNÉES, DE PROGRAMMES, OU DE LA PRIVATION DE JOUISSANCE DES SYSTÈME(S) OU DU RÉSEAU.

Les conseils sont strictement limités aux questions demandées et basées sur les informations fournies par le client. Les problèmes et les solutions peuvent dépendre de la nature de l'environnement du système et d'une variété d'autres paramètres qui sont inconnus à Bitdefender. Par conséquent, Bitdefender ne peut en aucun cas être tenu responsable de dommages résultant de l'utilisation de ces informations.

Il est possible que l'état du système sur lequel les produits Bitdefender doivent être installés soit instable (infection préalable, installation d'antivirus ou solutions de sécurité multiples, etc.). Dans ces cas précis, il est possible que l'analyste vous propose une prestation de maintenance auprès de votre revendeur avant de pouvoir régler votre problème.

Les informations techniques peuvent changer lorsque des nouvelles données deviennent disponibles, par conséquent, Bitdefender recommande que vous consultiez régulièrement notre site "Produits" à l'adresse suivante : <http://www.bitdefender.fr> pour des mises à jour, ou notre site internet de F A Q à l'adresse <http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/>.

Tout dommage direct, indirect, spécial, accidentel ou conséquent en relation avec l'usage des informations fournies ne peuvent pas être imputés à Bitdefender.

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



34. RESSOURCES EN LIGNE

De nombreuses ressources en ligne sont disponibles pour vous aider à résoudre vos questions et problèmes liés à Bitdefender.

- Centre de Support de Bitdefender :

<http://www.bitdefender.fr/support/consumer.html>

- Forum du Support Bitdefender :

<http://forum.bitdefender.com/index.php?showforum=59>

- Le portail de sécurité informatique Bitdefender blog :

<http://www.bitdefender.fr/blog/>

Vous pouvez également utiliser votre moteur de recherche favori pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

34.1. Centre de Support de Bitdefender

Le Centre de Support de Bitdefender est une base en ligne d'informations concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus et constatés par le support technique, les équipes de réparation des bugs de Bitdefender. Ainsi que des articles généraux sur la prévention antivirus, la gestion des solutions Bitdefender, des informations détaillées et beaucoup d'autres articles.

Le Centre de Support de Bitdefender est accessible au public et consultable gratuitement. Cet ensemble d'informations est une autre manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'informations ou de rapports de bugs provenant de clients Bitdefender trouvent une réponse dans le Centre de Support Bitdefender, comme les rapports de corrections de bugs, les solutions de rechange, ou les articles d'informations venant compléter les fichiers d'aide des produits.

Le Centre de Support de Bitdefender est disponible en permanence sur

<http://www.bitdefender.fr/support/consumer.html>.



34.2. Forum du Support Bitdefender

Le Forum du Support Bitdefender fournit aux utilisateurs de Bitdefender une manière simple d'obtenir de l'aide et d'aider les autres.

Si votre produit Bitdefender ne fonctionne pas correctement, s'il ne peut pas supprimer certains virus de votre ordinateur ou si vous avez des questions sur son mode de fonctionnement, exposez votre problème ou posez vos questions sur le forum.

Les techniciens du support Bitdefender surveillent le forum à la recherche de nouvelles publications afin de vous aider. Vous pouvez également obtenir une réponse ou une solution d'un utilisateur Bitdefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de Bitdefender est disponible à <http://forum.bitdefender.com/index.php?showforum=59>, dans 5 langues différentes : français, anglais, allemand, espagnol et roumain. Cliquez sur le lien **Protection des indépendants & des petites entreprises** pour accéder à la section dédiée aux produits de consommation.

34.3. Portail Bitdefender blog

Bitdefender blog comprend de nombreuses informations sur la sécurité informatique. Vous pouvez découvrir ici les différentes menaces auxquelles votre ordinateur est exposé lorsqu'il est connecté à Internet (malwares, phishing, spam, cybercriminels).

De nouveaux articles sont régulièrement publiés pour vous tenir au courant des dernières menaces découvertes, des tendances actuelles en matière de sécurité et vous fournir encore d'autres informations sur le secteur de la sécurité informatique.

La page web de Bitdefender blog est <http://www.bitdefender.fr/blog/>.



35. POUR NOUS JOINDRE

Une communication efficace est la clé d'une relation réussie. Au cours des dix dernières années, BITDEFENDER s'est bâti une réputation incontestable dans sa recherche constante d'amélioration de la communication pour dépasser les attentes de ses clients et de ses partenaires. N'hésitez pas à nous contacter pour toute question.

35.1. Adresses Web

Ventes : bitdefender@profiltechnology.com

Centre de support : <http://www.bitdefender.fr/support/consumer.html>

Documentation : documentation@bitdefender.com

D i s t r i b u t e u r s l o c a u x :

<http://www.bitdefender.fr/partenaires/trouver-un-partenaire.html>

Programme de partenariat : partners@bitdefender.com

Relations médias : pr@bitdefender.com

Emplois : jobs@bitdefender.com

Soumissions de virus : virus_submission@bitdefender.com

Envoi de spams : spam_submission@bitdefender.com

Signaler un abus : abuse@bitdefender.com

Site web : <http://www.bitdefender.fr>

35.2. Distributeurs locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Allez à <http://www.bitdefender.fr/partenaires/trouver-un-partenaire.html>.
2. Choisissez vos pays et ville à l'aide des options correspondantes.
3. Si vous ne trouvez pas de distributeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse sales@bitdefender.com. Merci de nous contacter par email pour optimiser le traitement de votre demande.



35.3. Bureaux de Bitdefender

Les bureaux de Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux. Leur adresse respective et contacts sont listés ci-dessous.

France

Profil Technology

49, Rue de la Vanne

92120 Montrouge

Téléphone : +33 (0)1 47 35 72 73

Ventes : bitdefender@profiltechnology.com

Support technique : <http://www.bitdefender.fr/site/Main/nousContacter>

Site Web : <http://www.bitdefender.fr>

U.S.A

Bitdefender, LLC

6301 NW 5th Way, Suite 4300

Fort Lauderdale, Florida 33309

Téléphone (services administratif et commercial) : 1-954-776-6262

Ventes : sales@bitdefender.com

Support technique : <http://www.bitdefender.com/support/consumer.html>

Site Web : <http://www.bitdefender.com>

Allemagne

Bitdefender GmbH

TechnoPark Schwerte

Lohbachstrasse 12

D - 58239 Schwerte

Service administratif : +49 2304 9 45 - 162

Fax : +49 2304 9 45 - 169

Ventes : vertrieb@bitdefender.de

Support technique : <http://www.bitdefender.de/support/consumer.html>

Site Web : <http://www.bitdefender.de>

Espagne

Bitdefender España, S.L.U.



C/Bailén, 7, 3-D
08010 Barcelona
Fax : +34 93 217 91 28
Téléphone : +34 902 19 07 65
Ventes : comercial@bitdefender.es
Support technique : <http://www.bitdefender.es/support/consumer.html>
Site Web : <http://www.bitdefender.es>

Roumanie

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax : +40 21 2641799
Téléphone du service commercial : +40 21 2063470
Email du service commercial : sales@bitdefender.ro
Support technique : <http://www.bitdefender.ro/support/consumer.html>
Site Web : <http://www.bitdefender.ro>

Émirats arabes unis

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Téléphone du service commercial : 00971-4-4588935 / 00971-4-4589186
Email du service commercial : mena-sales@bitdefender.com
Support technique : <http://www.bitdefender.com/support/consumer.html>
Site Web : <http://www.bitdefender.com>



Glossaire

Abonnement

Achetez une licence qui donne à l'utilisateur le droit d'utiliser un produit ou service particulier sur un nombre spécifique d'appareils et pour un certain laps de temps. Un abonnement expiré peut être renouvelé automatiquement en utilisant les informations données par l'utilisateur lors du premier achat.

ActiveX

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour créer des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent poser ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est connu pour son manque total de commandes de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Advanced Persistent Threats (menaces persistantes avancées)

Les Advanced persistent threat (APT) exploitent les vulnérabilités des systèmes pour voler des informations importantes et les livrer à la source. Les grands groupes tels que les entreprises, les sociétés ou les gouvernements sont ciblés par ce malware.

L'objectif d'une Advanced persistent threat est de passer inaperçue pendant le plus de temps possible, tout en surveillant et regroupant des informations importantes sans endommager les machines ciblées. La méthode utilisée pour injecter le virus dans le réseau consiste à faire ouvrir un fichier PDF ou un document Office qui a l'air inoffensif, pour que chaque utilisateur puisse exécuter les fichiers.

Applet Java

Il s'agit d'un programme Java conçu pour s'exécuter uniquement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels)



qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Chemin

Directions exactes vers un fichier d'un ordinateur. Ces directions sont généralement décrites par arborescence, de haut en bas.

La connexion entre deux points, comme le canal de communication entre deux ordinateurs.

Client de messagerie

Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (courriels).

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.

Dossier de démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage de l'ordinateur. Par exemple, un écran de démarrage, un fichier son pour le démarrage de l'ordinateur, un calendrier, des programmes, peuvent être placés dans ce dossier. C'est généralement un raccourci vers le fichier qui est placé dans le dossier, et pas le fichier.



E-mail

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Enregistreur de frappe

Application qui enregistre tout ce qui est tapé.

Les enregistreurs de frappe ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros d'assurance sociale).

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme le manque de mémoire.

Extension de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS-DOS. Elles comportent communément une à trois lettres (certains anciens OS n'en supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Fausse alerte

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Fichier journal (Log)

Fichier qui enregistre les actions ayant eu lieu. Bitdefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.



Heuristique

Méthode basée sur des règles permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

Honeypot

Un faux système d'ordinateur est créé pour attirer des pirates afin d'étudier la façon dont ils agissent et identifient les méthodes hérétiques qu'ils utilisent pour collecter des informations sur le système. Les sociétés et les entreprises sont plus intéressées par la mise en place et l'utilisation de honeypots pour améliorer leur état de sécurité global.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Lecteur de disque

C'est un appareil qui lit et écrit des données sur un disque.

Une unité de disque dur lit et écrit sur un disque dur.

Un lecteur de disquette accède à des disquettes.

Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestion.

Malwares

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des virus peuvent également se répliquer. Tous les virus informatiques sont créés par des personnes. Un virus simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.



Mettre à jour

Nouvelle version d'un logiciel ou d'un produit hardware, destinée à remplacer une version antérieure du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, et si ce n'est pas le cas, la mise à jour ne se fait pas.

Bitdefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

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 (plug-ins) pour certains formats.

Non-heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être un virus et ne génère donc pas de fausses alertes.

Phishing

Action d'envoyer un courriel à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du courriel. Cet courriel oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Photon

Photon est une technologie Bitdefender innovante et discrète, conçue pour limiter l'impact de la protection antivirus sur les performances. En surveillant l'activité de votre PC en tâche de fond, elle crée des modèles



d'utilisation qui aident à optimiser les processus de démarrage et d'analyse.

Port

Une interface sur un ordinateur auquel vous pouvez connecter un appareil. Les ordinateurs comportent plusieurs sortes de ports. Il existe plusieurs ports internes permettant de connecter des lecteurs de disques, des écrans et des claviers. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Portes dérobées

Il s'agit d'une faille dans la sécurité d'un système délibérément laissée en place par des développeurs ou des personnes chargées de la maintenance. Les intentions ne sont pas toujours malveillantes ; quelques systèmes d'exploitation, par exemple, permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Programmes empaquetés

Fichier dans un format compressé. Beaucoup de systèmes d'exploitation et d'applications contiennent des commandes vous permettant de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide" à la suite. Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui compresse des fichiers remplace la série d'espaces par un caractère spécial pour les séries d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. Il s'agit d'une technique de compression - il en existe plusieurs autres.

Publiciels

Les publiciels sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces publiciels étant généralement installés une fois que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.



Cependant, les fenêtres publicitaires peuvent devenir contrariantes et, dans certains cas, nuire aux performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des termes de l'accord de licence.

Ransomwares

Le ransomware est un programme malveillant qui essaye de soutirer de l'argent aux utilisateurs en fermant leur système vulnérable. CryptoLocker, CryptoWall, et TeslaWall n'en sont que des variantes qui recherchent les systèmes personnels des utilisateurs.

L'infection peut se répandre via e-mail, le téléchargement de pièces jointes, ou l'installation d'applications, sans prévenir l'utilisateur de ce qui se passe dans son système. Les utilisateurs quotidiens et les entreprises sont ciblées par les pirates ransomwares.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant un accès de niveau administrateur à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs système.

Le principal rôle des rootkits est de masquer des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des logs et passer inaperçus.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.



Secteur de boot :

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur d'amorçage contient aussi un programme qui charge le système d'exploitation.

Signature de virus

La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.

Spam

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des courriels non sollicités.

Spywares

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les logiciels espions sont généralement cachés dans des logiciels gratuits et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des logiciels gratuits ne contiennent pas de logiciels espions. Une fois installé, le logiciel espion surveille l'activité de l'utilisateur sur Internet et transmet discrètement ces informations à une tierce personne. Les logiciels espions peuvent également récupérer des informations sur les adresses courriel, les mots de passe ou même, les numéros de cartes de crédit.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'être victime de logiciels espions est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les logiciels espions volent les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.



TCP/IP

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Télécharger

Copie des données (généralement un fichier entier) d'une source principale vers un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Témoins

Sur Internet, les témoins sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des témoins est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (le code barres se trouvant au dos des produits). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. Contrairement aux virus, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout aussi destructeurs. Un des types de chevaux de Troie les plus insidieux est un logiciel qui prétend désinfecter votre PC mais qui au lieu de cela l'infecte.

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.

Utilisation de la Mémoire

Zones de stockage internes dans l'ordinateur. Le terme mémoire définit le stockage de données sous la forme de composants électroniques, le mot stockage étant utilisé pour définir le stockage de données sur bande magnétique ou disques amovibles. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Ver

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure de sa propagation. Il ne peut pas se joindre à d'autres programmes.

Virtual Private Network (VPN)

C'est une technologie qui permet une connexion temporaire et chiffrée à un certain réseau plutôt qu'à un autre moins sécurisé. De cette façon, l'envoi et la réception de données sont protégés et chiffrés et plus difficiles à intercepter pour les pirates. Une preuve de sécurité est l'identification, qui ne peut se faire que via un identifiant et un mot de passe.

Virus d'amorçage

Virus 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 le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Virus Macro

Type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.



Virus polymorphique

Virus qui change de forme avec chaque fichier qu'il infecte. Ces virus n'ayant pas de forme unique bien définie, ils sont plus difficiles à identifier.

Zone de notification

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : télécopieur, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.