GUIDE D'UTILISATION

Bitdefender CONSUMER SOLUTIONS

Mobile Security

Bitdefender Mobile Security

Guide de l'utilisateur

Date de publication : 02/10/2023

Mention légale

Bitdefender

Table des matières

À PROPOS DE CE GUIDE

Objectifs et destinataires

Le présent guide est destiné à tous les utilisateurs d'Android qui ont choisi Bitdefender Mobile Security comme solution de sécurité pour leurs appareils mobiles. Les informations qui y sont présentées ne sont pas réservées aux personnes ayant un bagage technique ; elles sont accessibles à toute personne capable de se servir d'un appareil fonctionnant sous Android.

Vous découvrirez comment configurer et utiliser Bitdefender Mobile Security pour vous protéger contre les menaces et autres applications malveillantes. Vous découvrirez également comment tirer le meilleur parti de Bitdefender.

Nous vous souhaitons un apprentissage agréable et utile.

Comment utiliser ce guide

Ce guide couvre plusieurs thèmes essentiels :

Pour démarrer (page 5)

Commencez à utiliser Bitdefender Mobile Security et son interface utilisateur.

Caractéristiques et fonctionnalités (page 11)

Apprenez à utiliser Bitdefender Mobile Security pour vous protéger contre les menaces et les applications malveillantes en vous familiarisant avec ses capacités et ses fonctionnalités.

Obtenir de l’aide (page 52)

Où chercher et à qui demander de l'aide en cas d'imprévu

Conventions utilisées dans ce guide

Normes typographiques

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

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

Avertissement

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

Note

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

Important

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

Attention

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

Commentaires

Aidez-nous à améliorer ce livret ! Nous avons testé et vérifié toutes les informations mais n'hésitez pas à nous écrire pour nous signaler

d'éventuelles erreurs ou des améliorations que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

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

1. PRÉSENTATION DE BITDEFENDER MOBILE SECURITY

Payer ses factures, réserver ses vacances, acheter des biens et des services... Il est pratique et très simple de faire ce type de choses en ligne. Mais un grand nombre de ces activités ayant évolué sur Internet, elles sont particulièrement risquées et si vous négligez les questions de sécurité, vos données personnelles pourraient être piratées. Et qu'y a-t-il de plus important que la protection des données stockées sur vos comptes en ligne ou votre smartphone ?

Bitdefender Mobile Security vous permet de :

- Bénéficiez de la meilleure protection pour votre smartphone et votre tablette Android, avec une incidence minimale sur l'autonomie de vos appareils
- Protégez-vous contre les arnaques mobiles basées sur des liens
- Accédez à notre VPN sécurisé pour une expérience rapide, anonyme et sûre de la navigation Internet
- Localisation, verrouillage et réinitialisation de votre appareil en cas de perte ou de vol.
- Vérifiez si votre compte de messagerie électronique a été impliqué dans des violations ou des fuites de données

2. POUR DÉMARRER

2.1. Spécifications du produit

Bitdefender Mobile Security est compatible avec tout appareil fonctionnant sous Android 5.0 (ou version ultérieure du système d'exploitation). Une connexion Internet active est requise pour l'analyse des menaces dans le cloud.

2.2. Installer Bitdefender Mobile Security

- **Depuis Bitdefender Central**
  - Sous Android
    1. Aller à : https://central.bitdefender.com.
    2. Connectez-vous à votre compte Bitdefender.
    3. Sélectionnez la section **Mes Appareils**.
    4. Appuyez sur **INSTALLER LA PROTECTION**, puis appuyez sur **Protéger cet appareil**.
    5. Sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
    6. Vous serez alors redirigé vers **Google Play**. Sur l'écran de Google Play, appuyez sur Installer.
  - Sur Windows, macOS et iOS
    1. Aller à: https://central.bitdefender.com.
    2. Connectez-vous à votre compte Bitdefender.
    3. Sélectionnez le **Mes appareils** panneau.
    4. Appuyez sur **INSTALLER LA PROTECTION**, puis appuyez sur **Protéger d'autres appareils**.
    5. Sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.

6. Appuyez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**.
7. Entrez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER UN E-MAIL**. Attention, le lien de téléchargement généré ne sera valide que pendant 24 heures. Si le lien expire, vous devrez en générer un nouveau en suivant les mêmes instructions.
8. Depuis l'appareil sur lequel vous voulez installer Bitdefender, consultez la boite de messagerie que vous avez précédemment saisie, et appuyez sur le bouton de téléchargement.

- **Depuis Google Play**
  Recherchez l'application Bitdefender Mobile Security et installez-la.
  Vous pouvez également scanner le QR Code :

  Avant de passer à l'étape de validation, vous devez accepter les Conditions d'utilisation de l'abonnement. Veuillez prendre le temps de lire les Conditions d'utilisation de l'abonnement, car elles contiennent les termes et conditions dans le cadre desquels vous pouvez utiliser Bitdefender Mobile Security.
  Appuyez sur **CONTINUER** pour passer à la fenêtre suivante.

2.3. Connectez-vous à votre compte Bitdefender

Pour utiliser Bitdefender Mobile Security, vous devez associer votre appareil à un compte Bitdefender, Facebook, Google, Microsoft ou Apple en vous connectant au compte à partir de l'application. Lorsque vous ouvrirez l'application pour la première fois, vous serez invité à vous connecter à un compte.

Si vous avez installé Bitdefender Mobile Security depuis votre compte Bitdefender, l'application tentera de se connecter automatiquement à ce compte.

Pour rattacher votre appareil à un compte Bitdefender :

1. Saisissez l'adresse e-mail de votre compte Bitdefender et le mot de passe correspondant dans les champs prévus à cet effet. Si vous n'avez pas de compte Bitdefender et souhaitez en créer un, cliquez sur le lien correspondant.
2. Appuyez sur **CONNEXION**.

Pour vous connecter en utilisant un compte Facebook, Google, ou Microsoft, sélectionnez le service que vous voulez utilisez dans la partie Ou s'inscrire via. Vous serez redirigé vers la page de connexion du service sélectionné. Suivez les instructions pour associer votre compte à Bitdefender Mobile Security.

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

2.4. Configurer la protection

Une fois connecté à l'application, la fenêtre Configurer la protection apparait. Pour sécuriser votre appareil, nous vous recommandons de suivre les étapes suivantes :

- **Statut de l'abonnement** Afin d'être protégé par Bitdefender Mobile Security, vous devez activer votre produit avec une clé de licence ou un abonnement, qui indiquent pendant combien de temps vous pouvez utiliser le produit. Dès qu'elle expire, l'application cesse de fonctionner et de protéger votre appareil.
  Si vous avez un code d'activation, appuyez sur **J'AI UN CODE**, puis sur **ACTIVER**.
  Si vous vous êtes connecté avec un nouveau compte Bitdefender et n'avez pas de code d'activation, vous pouvez utiliser gratuitement le produit pendant 14 jours.
- **Protection web**. si votre appareil vous demande l'Accessibilité pour activer la Protection Web, appuyez sur **ACTIVER**. Vous serez alors redirigé vers le menu Accessibilité. Tapez Bitdefender Mobile Security, et activez l'option correspondante.
- **Scanner Antimalware**. Réalise une analyse ponctuelle pour garantir que votre appareil ne contient aucune menace. Pour démarrer la procédure d'analyse, appuyez sur **ANALYSER MAINTENANT**.

Dès que la procédure d'analyse commence, le tableau de bord apparait. Vous pouvez voir ici l'état de la sécurité de votre appareil.

2.5. Tableau de bord

Cliquez sur l'icône de Bitdefender Mobile Security dans la liste des applications de votre appareil pour ouvrir l'interface de l'application.

Le tableau de bord vous donne des informations sur l'état de la sécurité de votre appareil et, par le biais d'Autopilot, vous aide à améliorer la sécurité de votre appareil en vous recommandant des fonctionnalités.

La carte d'état en haut de la fenêtre vous informe de l'état de la sécurité de l'appareil par le biais de messages et de couleurs explicites. Si aucune alerte n'est en cours dans Bitdefender Mobile Security, la carte d'état est verte. Lorsqu'un problème de sécurité est détecté, la carte d'état devient rouge.

Pour vous offrir une utilisation efficace et une meilleure protection lorsque vous menez à bien diverses activités, **Bitdefender Autopilot** jouera le rôle de conseiller de sécurité personnel. En fonction de votre activité, Bitdefender Autopilot vous proposera des recommandations contextuelles basées sur votre utilisation de l'appareil et vos besoins. Vous pourrez ainsi découvrir et profiter des avantages apportés par les fonctionnalités de l'application Bitdefender Mobile Security.

A chaque fois qu'un processus est en cours ou qu'une fonctionnalité nécessite votre avis, une carte avec plusieurs informations et actions possibles est affichée dans le tableau de bord.

Depuis la barre de navigation inférieure, vous pouvez accéder aux fonctionnalités de Bitdefender Mobile Security et naviguer facilement :

Scanner Antimalware

Vous permet de lancer une analyse à la demande et d'activer l'analyse de la mémoire. Pour plus d'informations, reportez-vous à Analyse Antimalware (page 11).

Protection web

Vous garantit une navigation sur Internet en toute sécurité en vous signalant les pages web présentant un risque. Pour plus d'informations, reportez-vous à Protection Web (page 13).

VPN

Chiffre la communication à Internet, vous permettant d'assurer votre confidentialité, quel que soit le réseau auquel vous êtes connecté. Pour plus d'informations, reportez-vous à VPN (page 15).

Scam Alert

Vous protège en vous alertant lorsque des liens malveillants vous parviennent via SMS, via des applications de messagerie ou via tout type de notification. Pour plus d'informations, référez-vous à Scam Alert (page 18).

Antivol

Vous permet d'activer ou de désactiver les fonctionnalités de l'Antivol et de le configurer. Pour plus d'informations, reportez-vous à Fonctionnalités Antivol (page 21).

Confidentialité des comptes

Vérifie que vos comptes en ligne n'ont pas été victimes d'une brèche de données. Pour plus d'informations, reportez-vous à Confidentialité des comptes (page 25).

Blocage des applications

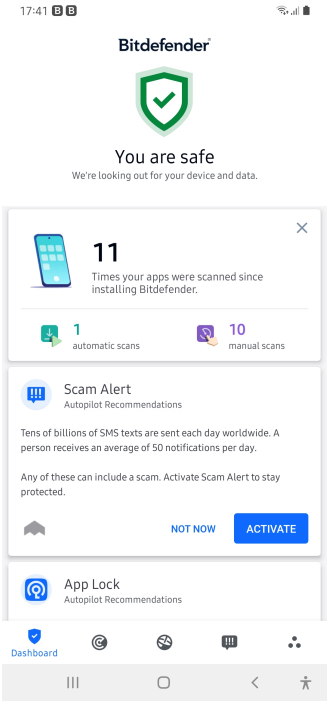
Vous permet de protéger votre apps en configurant un code PIN d'accès. Pour plus d'informations, reportez-vous à App Lock (page 27).

Reports

Conserve un journal de l'ensemble des actions importantes, changements d'état et autres messages critiques en lien avec l'activité de votre appareil. Pour plus d'informations, référez-vous à Rapports (page 31).

WearON

Communique avec votre montre connectée pour vous aider à localiser votre téléphone en cas de perte. Pour plus d'informations, reportez-vous à WearON (page 32).


17:41
Bitdefender
You are safe
We're looking out for your device and data.
11
Times your apps were scanned since installing Bitdefender.
1
automatic scans
10
manual scans
Scam Alert
Autopilot Recommendations
Tens of billions of SMS texts are sent each day worldwide. A person receives an average of 50 notifications per day.
Any of these can include a scam. Activate Scam Alert to stay protected.
NOT NOW
ACTIVATE
App Lock
Autopilot Recommendations
Dashboard

3. CARACTÉRISTIQUES ET FONCTIONNALITÉS

3.1. Analyse Antimalware

Bitdefender protège votre appareil et vos données contre les apps malveillantes à l'aide des analyses à l'installation et à la demande.

L'interface de Malware Scanner fournit une liste de tous les types de menaces recherchés par Bitdefender. Il suffit d'appuyer sur une menace pour consulter sa définition.

> **Note**
> Vérifiez que votre appareil est connecté à internet. Si il n'est pas connecté, l'analyse ne pourra pas être lancée.

- **Analyse à l'installation**
  Lorsque vous installez une app, Bitdefender Mobile Security l'analyse automatiquement en utilisant sa technologie dans le cloud. La même procédure d'analyse est réalisée à chaque mise à jour des applications installées.
  Si l'application est détectée comme étant malveillante, une alerte s'affichera vous demandant de la désinstaller. Tapez sur **Désinstaller** pour accéder à l'écran de désinstallation de cette app.
- **Analyse à la demande**
  Si vous voulez vous assurer que les applications installées sur votre appareil sont sûres, vous pouvez lancer une analyse à la demande.
  Pour débuter une analyse à la demande :

  1. Dans la barre de navigation inférieure, appuyez sur **Analyse antimalware**.
  2. Appuyez sur **COMMENCER L'ANALYSE**.

> **Note**
> Des permissions supplémentaires sont requises sur Android 6 pour la fonctionnalité d'analyse antimalware. Après avoir appuyé sur **COMMENCER L'ANALYSE**, sélectionnez **Autoriser** pour ce qui suit :
>
> - Autoriser **Antivirus** à passer et gérer les appels ?
> - Autoriser **Antivirus** à accéder aux photos, médias, et fichiers sur votre périphérique ?

La progression de l'analyse s'affiche et vous pouvez arrêter le processus à tout moment.

Par défaut, Bitdefender Mobile Security analysera le stockage interne de votre appareil, dont toute carte SD. De cette façon, toute les applications dangereuses se trouvant sur la carte pourront être détectées avant qu'elles ne causent des dommages.

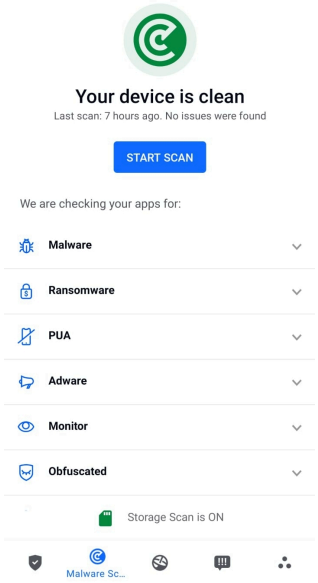
Pour désactiver les paramètres d'analyse stockage :

1. Dans la barre de navigation inférieure, appuyez sur **Plus**.
2. Appuyez sur **Paramètres**.
3. Désactivez **Analyse du stockage** dans la zone Malware Scanner.

Si des applications malveillantes sont détectées, des informations à leur sujet s'afficheront et vous pourrez les supprimer en appuyant sur **DÉSINSTALLER**.

La carte Analyse Malware affiche l'état de votre appareil. Lorsque celui-ci est protégé, la carte est de couleur verte. Lorsque l'appareil nécessite une analyse, ou si une action nécessite votre avis, la carte deviendra rouge.

Si vous possédez la version 7.1 d'Android ou une version plus récente, vous pouvez accéder à un raccourci vers Malware Scanner afin d'effectuer plus rapidement des analyses, sans avoir à ouvrir l'interface Bitdefender Mobile Security. Pour ce faire, appuyez et maintenez une pression sur l'icône Bitdefender de votre écran d'accueil ou de l'App Drawer, puis sélectionnez l'icône .



3.1.1. Détection des anomalies dans les applications

Bitdefender App Anomaly Detection est une nouvelle technologie intégrée au Bitdefender Malware Scanner pour fournir une couche de protection supplémentaire en surveillant et en détectant en permanence tout comportement malveillant et en alertant l'utilisateur si des activités suspectes sont identifiées.

Bitdefender App Anomaly Detection protège les utilisateurs même lorsqu'ils ont installé sans le savoir une application dangereuse qui reste inactive pendant un certain temps ou une application apparemment fiable qui interrompt ses fonctionnalités et devient malveillante.

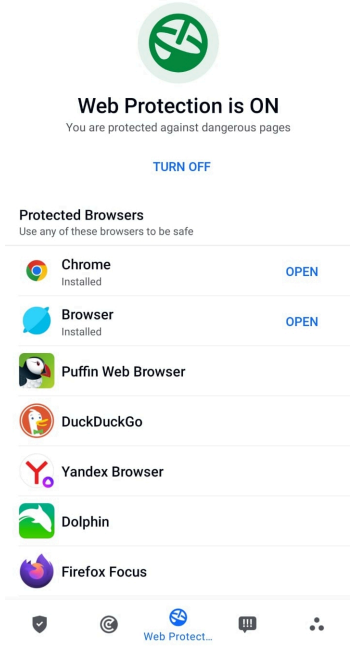
3.2. Protection Web

La protection Web vérifie, à l'aide des services cloud de Bitdefender, les pages Internet auxquelles vous accédez via le navigateur Android par défaut, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser et Dolphin.

Note

Des permissions supplémentaires sont nécessaires sur Android 6 pour la fonctionnalité Sécurité Web.

Autoriser l'enregistrement comme service Accessibilité et appuyez sur **ACTIVER** lorsque c'est nécessaire. Appuyez sur **Antivirus** et activez le commutateur, puis confirmez que vous acceptez la permission d'accès à votre périphérique.



À chaque fois que vous accédez à un site bancaire, Bitdefender Web Protection vous propose d'utiliser le VPN Bitdefender. La notification apparaît dans la barre d'état. Nous vous recommandons d'utiliser le VPN Bitdefender lorsque vous vous connectez à votre compte bancaire afin de protéger vos données contre d'éventuelles brèches de sécurité.

Pour désactiver les notifications de la Protection Web :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.

3. Désactivez le bouton correspondant dans la zone Protection Web.

3.3. VPN

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

Le VPN fait office de tunnel entre votre appareil et le réseau que vous utilisez pour sécuriser votre connexion, chiffrer vos données à l'aide d'une technologie comparable à celle utilisée par les banques et masquer votre adresse IP. L'intégralité du trafic est redirigée vers un serveur séparé, rendant ainsi votre appareil presque impossible à identifier par la multitude d'autres appareils qui utilise nos serveurs. En outre, quand vous êtes connecté à Internet via le VPN , vous pouvez accéder à des contenus qui ne seraient normalement pas disponibles dans votre région.

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

Il existe deux manières d'activer ou de désactiver le VPN Bitdefender :

- Appuyez sur **CONNECTER** depuis la carte VPN du tableau de bord.
  L'état du VPN Bitdefender s'affiche.
- Dans la barre de navigation inférieure, appuyez sur **VPN**, puis appuyez sur **CONNEXION**.
  Appuyez sur **SE CONNECTER** à chaque fois que vous voulez être protégé quand vous vous connectez à des réseaux sans-fil non sécurisés.
  Appuyez sur **SE DÉCONNECTER** quand vous voulez mettre un terme à la connexion.

Note

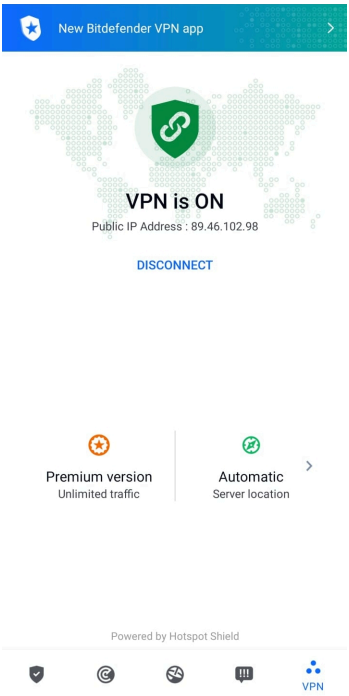
La première fois que vous activerez le VPN, il vous sera demandé d'autoriser Bitdefender à créer une connexion VPN pour surveiller votre trafic réseau. Appuyez sur **OK** pour continuer.

Si vous possédez la version 7.1 ou une version plus récente d'Android, vous pouvez accéder directement au VPN Bitdefender via un raccourci, sans avoir à ouvrir l'interface Bitdefender Mobile Security.

Pour ce faire, appuyez et maintenez une pression sur l'icône Bitdefender de votre écran d'accueil ou de l'App Drawer, puis sélectionnez l'icône .

Pour économiser de la batterie, nous vous recommandons de désactiver la fonctionnalité VPN quand vous n'en avez pas besoin.

Si vous avez un abonnement Premium, vous pouvez choisir votre serveur en appuyant sur Emplacement du serveur depuis la fonctionnalité VPN, puis en sélectionnant le pays de votre choix. Pour en apprendre plus sur les abonnements VPN, rendez-vous sur



3.3.1. Paramètres du VPN

Pour accéder aux paramètres avancés de votre VPN :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.

Depuis la zone VPN, vous pouvez configurer les options suivantes :

- Accès rapide au VPN - une notification apparaitra dans la barre d'état de votre appareil pour vous permettre d'activer rapidement le VPN.
- Avertissement réseau Wi-Fi ouvert - à chaque fois que vous vous connecterez à un réseau Wi-Fi ouvert, une notification apparaitra dans la barre d'état pour vous proposer d’activer le VPN.

3.3.2. Abonnements

Le VPN Bitdefender vous offre gratuitement 200 Mo de trafic par jour et par appareil afin de sécuriser vos connexions chaque fois que c'est

nécessaire, et vous connecte automatiquement au meilleur serveur disponible.

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

Vous pouvez passer à la version Premium du VPN Bitdefender à tout moment en appuyant sur **Activer Premium** dans la fenêtre du VPN.

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

Bitdefender VPN est un produit multiplateforme disponible dans les produits Bitdefender compatibles avec Windows, macOS, Android, et iOS. Avec un abonnement Premium, vous pourrez utiliser votre abonnement sur tous les produits, si vous vous vous connectez avec le même compte Bitdefender.

> **Note**
> Le VPN Bitdefender fonctionne également en tant qu'application autonome sur tous les systèmes d'exploitation pris en charge (à savoir, Windows, macOS, Android et iOS).

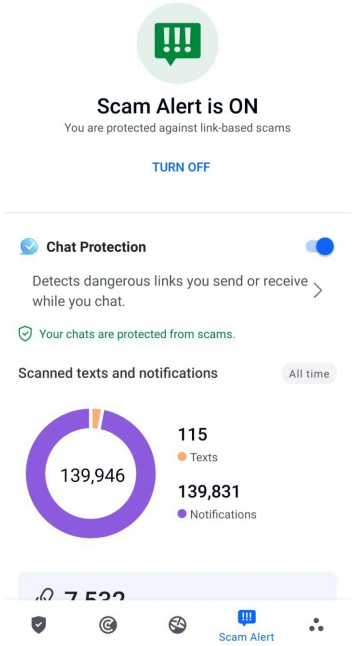
3.4. Scam Alert

La fonctionnalité Scam Alert prend des mesures préventives en amont, traitant les situations potentiellement dangereuses (y compris les menaces liées à des malwares) avant même qu'elles aient eu l'occasion de devenir problématiques. Scam Alert contrôle tous les messages SMS et toutes les notifications Android en temps réel.

Lorsqu'un lien dangereux vous parvient via un message sur votre téléphone, une pop-up d'avertissement s'affiche sur votre écran. Bitdefender vous proposera deux options. La première option vous permettra d'ignorer l'information. La seconde option vous permettra d'**AFFICHER LES DÉTAILS**. Ces détails vous fourniront plus

d'informations sur l'incident, ainsi que quelques conseils essentiels, tels que :

- Si un lien dangereux est détecté, ne l'ouvrez pas et ne le transférez pas.
- Dans la mesure du possible, supprimez le message concerné.
- Bloquez l'expéditeur si ce n'est pas un contact digne de confiance.
- Désinstaller l'application qui envoie des liens dangereux via des notifications.



Note

En raison de limitations inhérentes au système d'exploitation Android, Bitdefender n'est pas en mesure de supprimer les messages texte ni de prendre de mesures directes en lien avec des messages SMS ou toute autre source de notifications malveillantes. Si vous ignorez un avertissement émis par Scam Alert et essayez d'ouvrir un lien dangereux, la fonctionnalité Protection Web de Bitdefender l'interceptera automatiquement, empêchant ainsi la compromission de votre appareil.

3.4.1. Activer Scam Alert

Pour activer Scam Alert, vous devez autoriser l'application Bitdefender Mobile Security à accéder aux messages SMS et au système de notification :

1. Ouvrez l'application Bitdefender Mobile Security installée sur votre téléphone ou votre tablette Android.
2. Sur l'écran d'accueil de l'application Bitdefender, appuyez sur l'option **Scam Alert** située dans la barre de navigation inférieure, puis appuyez sur **ACTIVER**.
3. Appuyez sur le bouton **AUTORISER**.
4. Dans la liste Accès aux notifications, faites basculer Bitdefender Security sur la position **active**.
5. Confirmez l'action en appuyant sur **AUTORISER**.
6. Revenez à l'écran Scam Alert et appuyez sur **AUTORISER** pour autoriser Bitdefender à analyser les messages SMS entrants.

3.4.2. Protection des conversations en direct (chats) en temps réel

Les messageries instantanées (chats) offrent un moyen simple de garder le contact, mais elles permettent également aux liens dangereux de vous atteindre facilement.

Lorsque vous activez la fonctionnalité de protection des messageries instantanées (Chat Protection), le module Scam Alert, qui protège déjà vos messages texte et vos notifications, protège aussi vos messageries instantanées contre les attaques basées sur des liens, en détectant les liens dangereux que vous recevez ou que vous envoyez lors de vos discussions.

Pour activer la protection des conversations instantanées :

1. Ouvrez l'application Bitdefender Mobile Security installée sur votre téléphone ou tablette Android.
2. Sur l'écran d'accueil de l'application Bitdefender, appuyez sur l'option **Scam Alert** située dans la barre de navigation inférieure.

3. La fonctionnalité Chat Protection s'affichera en haut de l'onglet Scam Alert. Faites basculer l'interrupteur correspondant sur la position **active**.

> **Note**
> Actuellement, la protection des conversations instantanées est compatible avec les applications suivantes :
>
> - WhatsApp
> - Facebook Messenger
> - Telegram
> - Discord

3.5. Fonctionnalités Antivol

Bitdefender peut vous aider à localiser votre appareil et empêche que vos données personnelles finissent entre de mauvaises mains.

Il vous suffit d'activer Antivol à partir de l'appareil et, en cas de besoin, d'accéder à **Bitdefender Central** à partir de n'importe quel navigateur Web, partout.

> **Note**
> Un lien situé sur l'interface d'Antivol vous permettra de télécharger l'application Bitdefender Central sur Google Play si ce n'est pas déjà fait.

Bitdefender Mobile Security propose les fonctionnalités antivol suivantes :

Localisation à distance

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

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

- Si le GPS est activé sur l'appareil, son emplacement peut être déterminé à quelques mètres près tant qu'il est à portée des satellites GPS (c'est-à-dire, à l'extérieur).

- Si l'appareil est à l'intérieur, il peut être localisé avec une précision d'une dizaine de mètres si le Wi-Fi est activé et si des réseaux sans fil sont à sa portée.
- Sinon, la localisation sera déterminée à l'aide des informations du réseau mobile, qui fournit une précision de pas plus de quelques centaines de mètres.

Verrouillage à distance

Verrouillez l'écran de votre appareil et choisissez un code PIN numérique pour le déverrouiller.

Effacement du contenu de l'appareil à distance

Supprimer à distance toutes les données personnelles de votre appareil.

Envoyer une alerte à l'appareil (alarme)

Envoyer un message à distance à afficher à l'écran de l'appareil, ou faites émettre un son à l'appareil.

Si vous perdez votre appareil, vous pouvez indiquer à la personne qui le trouve comment vous le rapporter en affichant un message sur l'écran de l'appareil.

Si vous avez égaré votre appareil et qu'il est possible qu'il ne soit pas loin (par exemple, chez vous ou au bureau), quoi de mieux pour le trouver que de lui faire émettre un son fort ? Le son sera émis même si l'appareil est en mode silencieux.

3.5.1. Activer l'Antivol

Pour activer les fonctionnalités Antivol, veuillez simplement terminer le processus de configuration à partir de la carte Antivol disponible sur le tableau de bord.

Alternativement, vous pouvez activer Antivol en suivant les étapes suivantes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Appuyez sur **Antivol**.
3. Appuyez sur **ACTIVER**.
4. La procédure suivante vous aidera à activer cette fonctionnalité :

Note

Les permissions supplémentaires sont nécessaires sous Android 6 pour la fonctionnalité Antivol.

Pour l'activer, suivez ces étapes :

a. Appuyez sur **Activer l'antivol**, puis appuyez sur **ACTIVER**.

b. Autoriser les permissions pour **Antivirus** à avoir accès à l'emplacement du votre périphérique.

a. **Octroyer des privilèges d'administrateur**
Ces privilèges sont essentiels au fonctionnement d'Antivol et doivent donc être accordés afin de poursuivre.

b. **Définir le code PIN de l'application**
Un code PIN doit être défini pour éviter tout accès non autorisé à votre appareil. Le code PIN devra être saisi avant toute utilisation de votre appareil. Sur les appareils compatibles avec l'authentification par empreintes digitales, cette méthode peut être utilisée à la place du code PIN.
Le même code PIN est utilisé par Blocage des applications pour protéger les applications que vous avez installées.

c. **Activer Snap Photo**
Lorsque Snap Photo est activé, à chaque fois qu'une personne essayera de déverrouiller votre appareil sans succès, Bitdefender prendra une photo d'elle.
Plus précisément, à chaque fois que la confirmation par code PIN, mot de passe ou empreinte digitale que vous avez défini pour protéger votre appareil est saisi de manière incorrecte trois fois de suite, une photo est prise par la caméra frontale. a photo est ensuite enregistrée en indiquant l'heure et la raison, et celle-ci peut être consultée en accédant à la fenêtre Antivol de Bitdefender Mobile Security.
Vous pouvez également consulter les photos prises depuis votre compte Bitdefender :

i. Aller à: https://central.bitdefender.com.

ii. Connectez-vous à votre compte.

iii. Sélectionnez le **Mes appareils** panneau.

iv. Sélectionnez votre appareil Android, puis rendez-vous dans l'onglet **Antivol**.

v. Appuyez sur ⋮ à côté de l'option **Afficher les instantanés** pour visualiser les dernières photos prises.
Seules les deux dernières photos sont sauvegardées.

Une fois la fonction antivol est activée, vous pouvez activer ou désactiver les commandes de contrôle Web individuellement à partir de la fenêtre Antivol en appuyant sur les options correspondantes.

3.5.2. Utiliser les fonctionnalités Antivol depuis Bitdefender Central

> **Note**
> Toutes les fonctions Antivol requièrent que l'option **Données en arrière plan** soit activée dans les paramètres Utilisation des données de votre appareil.

Pour accéder aux fonctionnalités antivol à partir de votre compte Bitdefender :

1. Accédez à **Bitdefender Central**.
2. Sélectionnez le **Mes appareils** panneau.
3. Dans la fenêtre **MES APPAREILS**, sélectionnez la carte de l'appareil que vous souhaitez consulter en appuyant sur le bouton **Afficher les détails** qui lui est associé.
4. Sélectionnez l'onglet **Antivol**.
5. Appuyez sur le bouton correspondant à la fonctionnalité que vous souhaitez utiliser :
   Localiser - permet d'afficher la localisation de votre appareil sur Google Maps.
   Afficher IP - affiche la dernière adresse IP pour l'appareil sélectionné.
   Alerter - saisissez un message à afficher sur l'écran de votre appareil et/ou faites émettre un son à votre appareil.
   Verrouiller - verrouillez votre appareil et définissez un code PIN permettant de le déverrouiller.
   Effacer - supprimez toutes les données de votre appareil.

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

3.5.3. Paramètres d'Antivol

Pour activer ou désactiver les commandes à distance :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Antivol**.
3. Activez ou désactivez les options souhaitées.

3.6. Confidentialité des comptes

Bitdefender Account Privacy détecte si des fuites de données se sont produites sur les comptes que vous utilisez pour effectuer des paiements en ligne et des achats ou pour vous connecter à différents sites Internet ou applications. Parmi les données pouvant être stockées dans un compte figurent les mots de passe, les informations de carte de crédit et les informations bancaires et, si le compte n'est pas correctement sécurisé, une usurpation d'identité ou une violation de la vie privée peuvent survenir.

Le statut de confidentialité d'un compte est affiché juste après la validation.

De nouvelles vérifications automatiques sont programmées pour s'exécuter en arrière-plan, mais des analyses manuelles peuvent également être lancées quotidiennement.

Des notifications seront affichées chaque fois que de nouvelles brèches impliquant l'un des comptes de messagerie validés seront découvertes.

Pour commencer à protéger des informations personnelles :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Appuyez sur **Confidentialité du compte**.
3. Appuyez sur **COMMENCER**.
4. L'adresse e-mail utilisée pour créer votre compte Bitdefender apparait et est automatiquement ajoutée à la liste des comptes pris en charge.

5. Pour ajouter un autre compte, appuyez sur **AJOUTER UN COMPTE** dans la fenêtre Confidentialité des comptes, puis saisissez l'adresse e-mail.
   Appuyez sur **AJOUTER** pour continuer.
   Bitdefender doit valider ce compte avant d'afficher des informations privées. Par conséquent, un e-mail contenant un code de validation est envoyé à l'adresse e-mail fournie.
   Consultez votre boîte de réception, puis saisissez le code reçu dans la section **Confidentialité du compte** de votre application. Si vous ne trouvez pas l'e-mail de validation dans le dossier Boîte de réception, vérifiez le dossier Spam.
   Le statut de confidentialité du compte validé est affiché.

Si des brèches sont détectées sur l'un de vos comptes, nous vous conseillons d'en modifier le mot de passe dès que possible. Voici quelques astuces pour créer un mot de passe fiable et sécurisé :

- Choisissez un mot de passe comportant au moins huit caractères.
- Incluez des minuscules et des majuscules.
- Intégrez au moins un chiffre ou un symbole, tel que #, @, % ou !.

Après avoir sécurisé un compte victime d'une atteinte à la vie privée, vous pouvez confirmer les changements en marquant la ou les brèches identifiées comme Résolues. Pour cela :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Confidentialité du compte**.
3. Sélectionnez le compte que vous venez de sécuriser.
4. Appuyez sur la brèche pour laquelle vous avez sécurisé votre compte.
5. Appuyez sur **RÉSOLU** pour valider le fait que le compte est sécurisé.

Lorsque toutes les brèches détectées sont marquées comme **Résolues**, le compte n'apparaît plus comme victime de brèche, du moins tant qu'une nouvelle brèche n'est pas détectée.

Pour ne plus recevoir de notification à chaque fois qu'une analyse automatique est terminée :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.

3. Désactivez le bouton correspondant dans la zone Confidentialité des comptes.

3.7. App Lock

Les applications installées comme les e-mails, photos ou messages peuvent contenir des données personnelles que vous souhaiteriez conserver privées en limitant de façon sélective leur accès.

App Lock vous aide à bloquer les accès indésirables aux applications en configurant un code PIN d'accès. Ce code PIN doit contenir au moins 4 chiffres, mais pas plus de 8, et est requis à chaque fois que vous souhaitez accéder aux applications sélectionnées à l'accès restreint.

L'authentification biométrique (telle que la confirmation par empreinte digital ou par reconnaissance faciale) peut être utilisée à la place du code PIN configuré.

3.7.1. Activer Blocage des applications

Pour limiter l'accès aux applications sélectionnées, configurez App Lock à partir de la carte affichée sur le tableau de bord après avoir activé Antivol.

Alternativement, vous pouvez activer App Lock en suivant les étapes suivantes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Appuyez sur **Blocage des applications**.
3. Robinet **ALLUMER**.
4. Autoriser Bitdefender Security à accéder aux données d'utilisation.
5. Autoriser la **superposition d'écrans**.
6. Retournez dans l'application et appuyez sur **CONFIGURER CODE PIN** pour confirmer le code d'accès.

   > **Note**
   > Cette étape n'est disponible que si vous n'avez pas précédemment configuré de PIN dans Antivol.

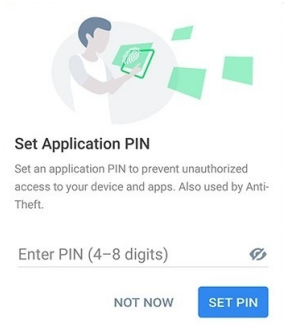
7. Activez l'option Snap Photo pour prendre en flagrant délit tout intrus essayant d'accéder à vos données personnelles.

> **Note**
> Des permissions supplémentaires sont nécessaires sur Android 6 pour la fonctionnalité Snap Photo. Pour l'activer, autorisez**Antivirus** à prendre des photos et des vidéos.

8. Sélectionnez les applications que vous souhaitez protéger.

Après 5 erreurs de code PIN ou empreintes digitales incorrectes, l'application marque une pause de 30 secondes. De cette manière, toute tentative d'utilisation des applications protégées sera bloquée.

> **Note**
> Le même code PIN est utilisé par l'Antivol pour vous aider à localiser votre appareil.



3.7.2. Mode de verrouillage

La première fois que vous ajoutez une application à App Lock, l'écran Mode de verrouillage des applications apparait. Vous pouvez ici choisir quand la fonctionnalité App Lock doit protéger les applications installées sur votre appareil.

Vous pouvez sélectionner l'une des options suivantes :

- **Nécessite un déverrouillage à chaque utilisation** - le code PIN ou l'empreinte digitale définie devra être utilisé à chaque fois que vous accédez à l'application verrouillée.
- **Laisser déverrouillé jusqu'à extinction de l'écran** - l'accès à vos applications sera possible jusqu'à ce que votre écran s'éteigne.
- **Verrouiller après 30 secondes** -vous avez 30 secondes pour revenir sur une application déverrouillée.

Si vous voulez modifier le réglage sélectionné :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Appuyez sur **Nécessite un déverrouillage à chaque utilisation** dans la zone App Lock.
4. Choisissez l'option désirée.

3.7.3. Paramètres de Blocage des applications

Pour accéder aux paramètres avancés de App Lock :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.

Depuis la zone App Lock, vous pouvez configurer les options suivantes :

- **Suggestion d'applications sensibles** - recevez une notification de verrouillage à chaque fois que vous installez une application sensible.
- **Nécessite un déverrouillage à chaque utilisation** - choisissez l'une des options de verrouillage et de déverrouillage disponibles.
- **Smart Unlock** - les applications restent déverrouillées quand vous êtes connecté à un réseau Wi-Fi de confiance.
- **Clavier aléatoire** - empêche la lecture du code PIN en plaçant les chiffre de manière aléatoire sur le clavier.

3.7.4. Snap photo

L'option Snap Photo de Bitdefender vous permet de prendre vos amis et vos proches la main dans le sac et de leur donner une bonne leçon en matière de vie privée : ils ne sont pas censés consulter vos fichiers personnels ni les applications que vous utilisez.

La fonction est simple à chaque fois que la confirmation par code PIN ou empreinte digitale que vous avez défini pour protéger vos applications est saisi de manière incorrecte trois fois de suite, une photo est prise par la caméra frontale. La photo est ensuite enregistrée en indiquant l'heure et la raison, et celle-ci peut être consultée en dans la section App Lock de Bitdefender Mobile Security.

Note
Cette fonctionnalité est disponible seulement sur les téléphones qui ont une caméra frontale.

Pour configurer la fonctionnalité Snap Photo de App Lock :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Activez le bouton correspondant dans la zone Snap Photo.

Les photos prises lorsque le code PIN saisi n'est pas correct sont affichées dans la fenêtre App Lock et peuvent être vues en plein écran.

Alternativement, vous pouvez les voir dans votre compte Bitdefender :

1. Aller à: https://central.bitdefender.com.
2. Connectez-vous à votre compte.
3. Sélectionnez la section **Mes Appareils**.
4. Sélectionnez votre appareil Android, puis le **Antivol** languette.
5. Robinet près de **Vérifiez vos instantanés** pour voir les dernières photos prises.

Seules les deux photos les plus récentes sont enregistrées.

Pour ne plus envoyer les photos sur votre compte Bitdefender :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Désactiver **Envoyer les photos** dans la zone Snap Photo.

3.7.5. Smart Unlock

Pour ne plus avoir à vous authentifier par code PIN ou empreinte digitale sur vos applications protégées à chaque fois que vous les ouvrez, le plus simple est d'activer Smart Unlock.

Avec Smart Unlock vous pouvez définir des réseaux Wi-Fi de confiance auxquels vous vous connectez fréquemment, et désactiver le blocage de App Lock lorsque vous êtes connecté à ceux-ci.

Pour configurer la fonctionnalité Smart Unlock :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Verrou d'application**.
3. Appuyez sur le bouton .
4. Appuyez sur le bouton situé à côté de **Smart Unlock**, si la fonctionnalité n'est pas encore activée.
   Validez à l'aide de votre empreinte digitale ou de votre code PIN.
   Lorsque vous activerez cette fonctionnalité pour la première fois, vous devrez autoriser la localisation. Appuyez sur le bouton **AUTORISER**, puis appuyez de nouveau sur **AUTORISER**.
5. Appuyez sur **AJOUTER** pour définir le réseau Wi-Fi sur lequel vous êtes connecté comme étant de confiance.

Chaque fois que vous changez d'avis, désactivez la fonctionnalité et les réseaux Wi-Fi que vous avez configuré comme fiables seront traités comme non fiables.

3.8. Rapports

La fonctionnalité Rapports tient un journal détaillé des événements liés à l'activité d'analyse de votre appareil.

Lorsqu'un événement lié à la sécurité de votre appareil a lieu, un nouveau message est ajouté aux Rapports.

Pour accéder à la rubrique Rapports :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Appuyez sur **Rapports**.

Les onglets suivants sont disponibles sur la fenêtre de rapport :

- **RAPPORTS HEBDOMADAIRES** - vous avez ici accès à l'état de sécurité et aux tâches réalisées pendant cette semaine et la semaine dernière. Le rapport de la semaine est généré tous les dimanches et vous recevrez une notification vous informant de sa disponibilité.
  Chaque semaine un nouveau conseil sera affiché dans cette rubrique, alors n'oubliez pas de regarder régulièrement pour utiliser l'application au mieux.
  Pour ne plus recevoir de notification à chaque fois qu'un rapport est généré :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Désactivez le bouton **Notification de nouveau rapport** dans la zone Rapports.

- **JOURNAL D'ACTIVITÉ** - vous pouvez ici consulter les informations détaillées sur l'activité de votre application Bitdefender Mobile Security depuis son installation sur votre appareil Android.
  Pour supprimer un journal d'activité disponible :
  1. Robinet **Plus** dans la barre de navigation inférieure.
  2. Robinet **Paramètres**.
  3. Appuyez sur **Effacer le journal d'activité**, puis appuyez sur **EFFACER**.

3.9. WearON

Bitdefender WearON vous permet de retrouver facilement votre smartphone, que vous l'ayez oublié au bureau dans une salle de conférence ou sous l'un des coussins de votre canapé. L'appareil peut être retrouvé même s'il est en mode silencieux.

Conservez cette fonctionnalité activée pour vous assurer que votre smartphone est toujours à votre portée.

Note
La fonctionnalité fonctionne avec Android 4.3 et Android Wear.

3.9.1. Activer WearON

Pour utiliser WearON, connectez simplement votre montre connectée à l'application Bitdefender Mobile Security et activez la fonctionnalité à l'aide de la commande vocale suivante :

Commencer : <Où est mon téléphone>

Bitdefender WearON dispose de deux commandes :

1. **Alerte téléphone**
   La fonctionnalité Alerte Téléphone vous permet de retrouver facilement votre smartphone lorsque vous vous en éloignez trop.

Si vous avez une montre connectée, celle-ci détectera automatiquement l'application sur votre téléphone et celui-ci vibrera quand il ne sera pas à portée de votre montre et que la connectivité Bluetooth est perdue.

Pour activer cette fonctionnalité, ouvrez Bitdefender Mobile Security, sélectionnez **Paramètres globaux** dans le menu puis le bouton correspondant sous la section WearON.

2. **Alarme**

   Retrouver votre téléphone n'a jamais été aussi simple. Lorsque vous oubliez où vous avez laissé votre téléphone, appuyez sur la commande Faire émettre un son de votre montre afin de faire émettre un son à votre téléphone.

3.10. À propos de

Pour connaitre la version de Bitdefender Mobile Security que vous utilisez, et consulter les Conditions d'utilisation de l'abonnement, la Politique de confidentialité et les licences open-sources :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Appuyez sur l'option souhaitée dans la zone À propos.

4. À PROPOS DE BITDEFENDER CENTRAL

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

Pour installer l'application Bitdefender Central sur vos appareils :

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

Une fois que vous êtes connectés, vous pouvez commencer à faire ce qui suit :

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

4.1. Accéder à Bitdefender Central

Il y a deux manières d'accéder à Bitdefender Central

- A partir de votre navigateur web :
  1. Ouvrir un navigateur web sur chaque appareil ayant accès à internet.
  2. Aller à: https://central.bitdefender.com.
  3. Connectez-vous à votre compte à l'aide de votre adresse e-mail et de votre mot de passe.

- Depuis votre appareil Android ou iOS :
  Ouvrez l'application Bitdefender Central que vous avez installée.

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

4.2. Authentification à 2 facteurs

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

4.2.1. Activer l'authentification à deux facteurs

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

Pour activer l'authentification à deux facteurs :

1. Accès Centrale Bitdefender.
2. Appuyez sur l'icône située dans le coin supérieur droit de l'écran.
3. Appuyez sur **Compte Bitdefender** dans le menu coulissant.
4. Sélectionnez l'onglet **Mot de passe et sécurité**.

5. Robinet **COMMENCER**.
   Choisissez l'une des deux méthodes suivantes :

   - **Application d'authentification** - utilise une application d'authentification pour générer un code chaque fois que vous souhaitez vous connecter à votre compte Bitdefender.
     Si vous souhaitez utiliser une application d'authentification, mais que vous ne savez pas laquelle choisir, nous mettons à votre disposition une liste des applications d'authentification que nous recommandons.

     a. Appuyez sur **UTILISER UNE APPLICATION D'AUTHENTIFICATION** pour commencer.

     b. Pour vous connecter sur un appareil Android ou iOS, utilisez votre appareil pour scanner le QR code.
     Pour vous connecter sur un ordinateur portable ou sur un ordinateur de bureau, vous pouvez saisir manuellement le code qui s'affiche.
     Appuyez sur **CONTINUER**.

     c. Saisissez le code fourni par l'application ou celui affiché lors de l'étape précédente, puis appuyez sur **ACTIVER**.

   - **E-mail** - chaque fois que vous vous connecterez à votre compte Bitdefender, un code de vérification vous sera envoyé par e-mail. Validez votre adresse e-mail puis utilisez le code que vous avez reçu.

     a. Appuyez sur **UTILISER UNE ADRESSE E-MAIL**pour commencer.

     b. Consultez votre messagerie et saisissez le code fourni.
     Notez que vous disposez de cinq minutes pour consulter votre boîte de réception et saisir le code généré. Passé ce délai, il vous faudra générer un nouveau code en suivant les mêmes étapes.

     c. Appuyez sur **ACTIVER**.

     d. 10 codes d'activation vous sont fournis. Vous pouvez copier, télécharger ou imprimer la liste et l'utiliser en cas d'oubli de votre adresse e-mail ou d'impossibilité de vous connecter à votre messagerie. Chaque code peut être utilisé une seule fois.

e. Appuyez sur **TERMINÉ**.

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

1. Appuyez sur **DÉSACTIVER L'AUTHENTIFICATION À 2 FACTEURS**.
2. Consultez votre application ou votre compte de messagerie et saisissez le code que vous avez reçu.
   Dans le cas où vous auriez choisi de recevoir le code d'authentification par e-mail, vous disposez de cinq minutes pour consulter votre boîte de réception et saisir le code généré. Passé ce délai, il vous faudra générer un nouveau code en suivant les mêmes étapes.
3. Confirmez votre choix.

4.3. Ajouter des appareils approuvés

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

Pour ajouter des appareils aux appareils approuvés :

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

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

4.4. Mes appareils

La zone **Mes Appareils** de votre compte Bitdefender vous donne la possibilité d'installer, de gérer et d'exécuter des actions à distance sur

votre produits Bitdefender sur n'importe quel appareil, pourvu qu'il soit allumé et connecté à Internet. Les cartes des appareils présentent le nom de l'appareil, l'état de sa protection et s'il court un risque potentiel de sécurité.

4.4.1. Ajouter un nouvel appareil

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

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes appareils** panneau, puis appuyez sur **INSTALLER LA PROTECTION**.
3. Choisissez l'une des deux options disponibles :
   - **Protégez cet appareil**
     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
   - **Protégez d'autres appareils**
     Sélectionnez cette option, puis sélectionnez le propriétaire de l'appareil. Si l'appareil appartient à quelqu'un d'autre, appuyez sur le bouton correspondant.
     Cliquez sur **ENVOYER LE LIEN DE TÉLÉCHARGEMENT**. Saisissez une adresse e-mail dans le champ correspondant, puis cliquez sur **ENVOYER PAR E-MAIL**. Attention, le lien de téléchargement généré sera valide pendant 24 heures seulement. Si le lien expire, il vous faudra en générer un nouveau en suivant les mêmes étapes.
     Sur l'appareil sur lequel vous souhaitez installer votre produit Bitdefender, vérifiez le compte de messagerie que vous avez saisi, puis appuyez sur le bouton de téléchargement correspondant.
4. Attendez que le téléchargement soit terminé, puis lancez l'installation.

4.4.2. Personnalisez votre appareil

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

1. Accès Centrale Bitdefender.

2. Sélectionnez la section **Mes Appareils**.
3. Cliquez sur la carte de l'appareil désiré, puis sur l'icône ⋮ dans l'angle supérieur droit de l'écran.
4. Sélectionnez **Paramètres**.
5. Saisissez un nouveau nom dans le champ **Nom de l'appareil**, puis cliquez sur **ENREGISTRER**.

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

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

4.4.3. Actions à distance

Pour mettre à jour Bitdefender à distance sur un appareil :

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

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

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

- **Tableau de bord.** Dans cette fenêtre, vous pouvez consulter des informations relatives à l'appareil sélectionné, vérifier l'état de sa protection, l'état du VPN Bitdefender et le nombre de menaces bloquées au cours des sept derniers jours. L'état de la protection peut s'afficher en vert (aucun problème n'affecte votre appareil), en jaune (un sujet mérite votre attention) ou en rouge (l'appareil est en danger). Si votre appareil présente des problèmes, cliquez sur la flèche située dans la zone d'état supérieure pour en savoir plus. D'ici, vous
- **Protection.** Depuis cette fenêtre, vous pouvez exécuter à distance une analyse rapide ou une analyse système de vos appareils. Cliquez sur le bouton **ANALYSER** pour lancer le processus. Vous pouvez également vérifier à quand remonte les dernières analyses sur vos appareils et obtenir les rapports correspondants, contenant les informations les plus importantes.
- **Optimizer.** Ici, vous pouvez améliorer à distance les performances d'un appareil en analysant, en détectant et en effaçant rapidement les fichiers inutiles. Cliquez sur le bouton **COMMENCER**, puis sélectionnez les zones que vous souhaiter optimiser. Cliquez de nouveau sur le bouton **COMMENCER** pour lancer le processus d'optimisation. Cliquez sur **Plus d'informations** pour accéder à un rapport détaillé sur les problèmes résolus.
- **Antivol.** En cas de perte ou de vol de votre appareil, la fonctionnalité antivol vous permet de le localiser et de prendre des mesures à distance. Cliquez sur **LOCALISER** pour découvrir l'emplacement de l'appareil. Sa dernière position connue sera affichée, ainsi que la date et l'heure correspondantes.
- **Vulnérabilité.** Pour vérifier la présence de vulnérabilités (telles que des mises à jour Windows manquantes, des applications obsolètes ou des mots de passe faibles) sur un appareil, cliquez sur le bouton **ANALYSER** dans l'onglet Vulnérabilité. Il n'est pas possible de corriger les vulnérabilité à distance. Si une vulnérabilité est découverte, vous devez lancer une nouvelle analyse sur l'appareil concerné puis appliquer les actions recommandées. Cliquez sur **Plus d'informations** pour accéder à un rapport détaillé sur les problèmes détectés.

4.5. Activité

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

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

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

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

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

- **Menaces bloquées.** Vous pouvez ici voir un graphique présentant une statistique générale avec des informations sur les menaces bloquées ces dernières 24 heures et au cours des sept derniers jours. Les informations affichées sont récupérées en fonction du comportement malveillant détecté sur les fichiers, applications et URL.

- **Utilisateurs avec le plus de menaces bloquées.** Ici, vous pouvez visualiser un classement indiquant quels utilisateurs ont été le plus confrontés à des menaces.

- **Appareils avec le plus de menaces bloquées.** Vous pouvez voir ici un classement des appareils sur lesquels le plus de menaces ont été détectés.

4.6. Mes abonnements

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

4.6.1. Vérifier les abonnements disponibles

Pour vérifier vos abonnements disponibles :

1. Accès Centrale Bitdefender.
2. Sélectionner le panneau **Mes Abonnements**.

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

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

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

4.6.2. Activer abonnement

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

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

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

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

L'abonnement est désormais activé.

4.6.3. Renouveler abonnement

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

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

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

4.7. Avis

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

5. QUESTIONS LES PLUS FRÉQUENTES

Pourquoi la solution Bitdefender Mobile Security nécessite-t-elle une connexion à Internet ?

L'application a besoin de communiquer avec les serveurs de Bitdefender afin de déterminer l'état de sécurité des applications qu'elle analyse et des pages web que vous consultez et pour recevoir des commandes de votre compte Bitdefender, lorsque vous utilisez les fonctionnalités de l'Antivol.

Pourquoi Bitdefender Mobile Security a-t-il besoin de chaque permission ?

- Accès Internet -> utilisé pour les communications cloud.
- Consulter l'état et l'identité du téléphone -> utilisé pour déterminer si l'appareil est connecté à Internet et pour extraire certaines informations de l'appareil nécessaires à la création d'un identifiant unique aux fins de la communication avec le cloud Bitdefender.
- Lire et écrire les favoris du navigateur -> le module de protection Web supprime les sites malveillants de votre historique de navigation.
- Lire les données du journal -> Bitdefender Mobile Security détecte les traces d'activités malveillantes dans les journaux Android.
- Localisation -> requise pour la localisation à distance.
- Appareil photo -> requis pour l'utilisation du module Snap Photo.
- Stockage -> utilisé pour autoriser l'analyse antimalware à vérifier la carte SD.

Comment ne plus envoyer d'informations à Bitdefender au sujet des applications suspectes ?

Par défaut, Bitdefender Mobile Security envoie des rapports aux serveurs Bitdefender sur les applications suspectes que vous installez. Ces informations sont essentielles pour améliorer la détection des menaces et peuvent nous aider à vous offrir une meilleure expérience à l'avenir. Si vous souhaitez cesser de nous envoyer les informations relatives aux applications suspectes :

1. Robinet **Plus** dans la barre de navigation inférieure.

2. Robinet **Paramètres**.
3. Désactivez la **Détection dans le cloud** dans la zone Malware Scanner.

Où puis-je trouver des informations sur l'activité de l'application ?

Bitdefender Mobile Security tient un journal de toutes les actions importantes, des modifications d'état et d'autres messages critiques liés à son activité. Pour accéder aux activités de l'application :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Rapports**.
   La fenêtre RAPPORTS HEBDOMADAIRES vous donne accès aux rapports générés chaque semaine et la fenêtre JOURNAL D'ACTIVITÉ vous donne des informations sur l'activité de votre application Bitdefender.

J'ai oublié le code PIN que j'avais choisi pour protéger mon app. Que puis-je faire ?

1. Accès Centrale Bitdefender.
2. Sélectionnez le **Mes appareils** panneau.
3. Appuyez sur la carte de l'appareil qui vous intéresse, puis sur ⋮ dans le coin supérieur droit de l'écran.
4. Sélectionner **Paramètres**.
5. Récupérez le code PIN à partir du champ **Application PIN**.

Comment modifier le code PIN que j'ai défini pour App Lock et Antivol ?

Pour modifier le code PIN que vous avez défini pour App Lock et Antivol :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Paramètres**.
3. Appuyez sur **CODE PIN** de sécurité dans la zone Antivol.
4. Saisissez le code PIN actuel.
5. Saisissez le code PIN que vous voulez utiliser.

Comment désactiver la fonction App Lock ?

La fonction App Lock ne peut pas être éteinte, mais vous pouvez la désactiver en effaçant les cases à cocher situées à côté des applications

sélectionnées après vous être authentifié par code PIN ou empreinte digitale.

Comment définir un autre réseau sans fil comme étant de confiance ?

Vous devez d'abord connecter votre appareil au réseau sans-fil que vous voulez définir comme étant de confiance. Ensuite, suivez les instructions suivantes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Robinet **Verrou d'application**.
3. Appuyez sur dans le coin supérieur droit.
4. Appuyez sur **AJOUTER** à côté du réseau que vous voulez définir comme de confiance.

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

Pour ne plus voir les photos prises sur vos appareils :

1. Accès Centrale Bitdefender.
2. Appuyez sur dans le coin supérieur droit de l'écran.
3. Appuyez sur **Paramètres** dans le menu coulissant.
4. Désactivez l'option **Afficher/Ne pas afficher les instantanés pris sur vos appareils**.

Comment puis-je sécuriser mes achats en ligne ?

Les achats en ligne comportent des risques élevés lorsque certains aspects sont ignorés. Pour éviter d'être victime d'une fraude, nous vous recommandons de procéder comme suit :

- Veillez à ce que votre application de sécurité soit à jour.
- Ne soumettez de paiements en ligne qu'avec une protection de l'acheteur.
- Utilisez un VPN lorsque vous vous connectez à internet depuis des réseaux sans fil publics et non sécurisés.
- Prêtez attention aux mots de passe que vous attribuez à vos comptes en ligne. Ils doivent être fiables et comporter des majuscules et des minuscules, des chiffres et des symboles (@, !, %, #, etc.).

- Veillez à ce que les informations que vous envoyez le soient sur des connexions sécurisées. L'extension du site Internet doit être HTTPS:// et non HTTP://.

Quand dois-je utiliser le VPN Bitdefender ?

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

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

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

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

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

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

Puis-je modifier le compte Bitdefender associé à mon appareil ?

Oui, vous pouvez facilement changer le compte Bitdefender lié à votre appareil en suivant les étapes suivantes :

1. Robinet **Plus** dans la barre de navigation inférieure.
2. Saisissez votre adresse e-mail.
3. Appuyez sur **Se déconnecter de votre compte**. Si un code PIN a été défini, il vous est demandé de le saisir.
4. Confirmez votre choix.
5. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants, et appuyez sur **CONNEXION**.

Quel est l'impact de Bitdefender Mobile Security sur les performances et l'autonomie de la batterie de mon appareil ?

L'impact est très faible. L'application s'exécute uniquement lorsque c'est essentiel - après l'installation d'une application, lorsque vous accédez à l'interface de l'application ou lorsque vous souhaitez un contrôle de sécurité. Bitdefender Mobile Security ne s'exécute pas en arrière-plan lorsque vous appelez vos amis, tapez un message ou jouez.

Qu'est-ce que la fonctionnalité Administrateur de l'appareil ?

La fonctionnalité Administrateur de l'appareil est une fonctionnalité Android qui octroie à Bitdefender Mobile Security les permissions nécessaires pour effectuer certaines tâches à distance. Sans ces privilèges, le verrouillage à distance ne fonctionnerait pas et la fonctionnalité d'effacement des données de l'appareil ne serait pas capable de supprimer complètement vos données. Si vous souhaitez supprimer l'application, veillez à supprimer ces privilèges dans **Paramètres > Sécurité > Administrateurs de l'appareil** avant d'essayer de la désinstaller.

Comment résoudre l'erreur "Aucun jeton Google" qui apparaît lorsque vous vous connectez à Bitdefender Mobile Security.

Cette erreur apparaît quand l'appareil n'est associé à aucun compte Google, ou si l'appareil est associé avec un compte mais qu'il existe un problème temporaire de connexion avec Google. Essayez l'un des solutions suivantes :

- Allez dans Paramètres Android > Applications > Gérer les applications > Bitdefender Mobile Security, puis appuyez sur **Supprimer les données**. Réessayez ensuite de vous connecter.
- Soyez certain que votre appareil est associé à un compte Google.

Pour le vérifier, allez dans Paramètres > Comptes et vérifiez si un compte Google est listé sous **Gérer les comptes**. Ajoutez un compte si aucun n'est listé, redémarrez votre appareil, puis essayez de vous connecter.

- Redémarrez votre appareil, puis essayez de nouveau de vous connecter.

Dans quelles langues Bitdefender Mobile Security est-il disponible ?

Bitdefender Mobile Security est actuellement disponible dans les langues suivantes :

- Brésilien
- Tchèque
- Néerlandais
- Anglais
- Français
- Allemand
- Grec
- Hongrois
- Italien
- Japonais
- Coréen
- Polonais
- Portugais
- Roumain
- Russe
- Espagnol
- Suédois
- Thaï
- Turc
- Vietnamien

D'autres langues seront ajoutées avec les prochaines versions. Pour modifier la langue de l'interface de Bitdefender Mobile Security, allez

dans les paramètres **Langue & clavier** de votre appareil et sélectionnez la langue que vous souhaitez utiliser sur votre appareil.

6. OBTENIR DE L'AIDE

6.1. Demander de l'aide

Bitdefender offre à ses clients une assistance sans égale, rapide et précise. Si vous rencontrez des difficultés ou si vous avez la moindre question au sujet de votre produit Bitdefender, nous mettons à votre disposition plusieurs ressources en ligne dans lesquelles vous trouverez sûrement une solution ou une réponse. Vous pouvez également contacter le service client Bitdefender. Nos représentants vous répondront dans les plus brefs délais et vous fourniront toute l'aide dont vous avez besoin.

6.2. Ressources En Ligne

De nombreuses ressources en ligne sont disponibles pour vous aider à trouver des réponses à vos questions et résoudre les problèmes liés à Bitdefender.

- Centre de Support Bitdefender :
  https://www.bitdefender.fr/consumer/support/
- Communauté des experts Bitdefender :
  https://community.bitdefender.com/fr
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Vous pouvez également utiliser le moteur de recherche de votre choix pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

6.2.1. Centre de support Bitdefender

Le Centre de Support de Bitdefender est une base en ligne d'informations concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus, ainsi que les bugs constatés, par le support technique de Bitdefender. Vous y découvrirez également des articles généraux sur la prévention contre les menaces, sur la gestion, en détail, des solutions Bitdefender et beaucoup d'autres articles.

La base de connaissances de Bitdefender est ouverte au public et consultable gratuitement. Cet ensemble d'information est une autre

manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'information ou les rapports de bug venant de clients de Bitdefender trouvent une réponse en cherchant dans la base de donnés de Bitdefender, comme les rapports de bugs, travaux associés, feuillet ou article d'information venant compléter les fichiers d'aide des produits.

Le centre de support Bitdefender est accessible à tout moment à l'adresse suivante : https://www.bitdefender.fr/consumer/support/.

6.2.2. Communauté des experts Bitdefender

La communauté des experts est un espace dans lequel des utilisateurs et des amateurs des produits Bitdefender peuvent échanger, s'entraider et partager leurs connaissances et leurs solutions. C'est aussi un espace propice à l'émergence d'idées et de commentaires précieux pour nos développeurs. Les membres de la communauté sont des utilisateurs expérimentés heureux de donner un peu de leur temps pour aider les autres. Grâce à leurs généreux efforts, nous avons créé une base de connaissances dans laquelle tous les utilisateurs peuvent une aide et un peu de convivialité.

Vous pourrez avoir des conversations riches avec des personnes qui utilisent vraiment les produits Bitdefender. Cette communauté permet aux membres d'établir des liens et de faire entendre leurs voix. Ils sont encouragés à y participer en sachant que leurs opinions et leurs contributions sont respectées et appréciées. En tant que fournisseur reconnu, nous nous efforçons d'offrir à nos clients une assistance rapide et précise et nous voulons nous rapprocher d'eux. C'est dans cette optique nous avons créé cette communauté.

Vous pouvez rejoindre la communauté des experts ici :

https://community.bitdefender.com/fr

6.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia regroupe toutes les dernières informations sur les cybermenaces. c'est là que les experts Bitdefender partagent deq conseils et des astuces sur la protection contre les pirates, les violations de données et l'usurpation d'identité, notamment sur les réseaux sociaux.

La page Bitdefender Cyberpedia se trouve ici :

https://www.bitdefender.com/cyberpedia.

6.3. Pour nous joindre

Une communication efficace est la clé d'une relation professionnelle réussie. Depuis 2001, BITDEFENDER s'est bâti une réputation irréprochable en cherchant sans cesse à améliorer sa communication pour dépasser les attentes de ses clients et de ses partenaires. Si vous avez la moindre question, n'hésitez pas à nous contacter directement via **Bitdefender Support Center**.

https://www.bitdefender.fr/consumer/support/

6.3.1. Distributeurs locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Rendez-vous sur https://www.bitdefender.com/partners/partner-locator.html.
2. Choisissez vos pays et ville à l'aide des options correspondantes.

GLOSSAIRE

Code d'activation

Clé unique qui peut être achetée chez un revendeur et utilisée pour activer un produit ou service spécifique. Un code d'activation permet l'activation de l'abonnement valide pour un certain laps de temps et pour certains appareils, et peut également être utilisé pour prolonger un abonnement avec pour seule condition d'être utilisé pour le même produit ou service.

ActiveX

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour créer des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent poser ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic. ActiveX est connu pour son manque total de contrôles de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Menaces persistantes avancées

Les Menaces persistantes avancées exploitent les vulnérabilités des systèmes pour voler des informations importantes et les livrer à la source. Les grands groupes tels que les entreprises, les sociétés ou les gouvernements sont ciblés par cette menace. L'objectif d'une menace persistante avancée est de passer inaperçue pendant le plus de temps possible, tout en surveillant et regroupant des informations importantes sans endommager les machines ciblées. La méthode utilisée pour injecter la menace dans le réseau consiste à faire ouvrir un fichier PDF ou un document Office qui a l'air inoffensif, pour que chaque utilisateur puisse exécuter les fichiers.

Adware

Les publiciels sont souvent associés à des applications gratuites qui exigent leur acceptation par l'utilisateur. Ces publiciels étant généralement installés une fois que l'utilisateur en a accepté le

principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux. Cependant, les fenêtres publicitaires peuvent devenir contrariantes et, dans certains cas, nuire aux performances du système. De plus, les informations recueillies peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des conditions de l'accord de licence.

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Porte dérobée

Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative ; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Secteur de démarrage

Un secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.

Virus de démarrage

Menace qui infecte le secteur d'amorçage d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus d'amorçage rendra la menace active en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez la menace active en mémoire.

Botnet

Le terme « botnet » est un mot composé de robot et de network (réseau). Les botnets sont des appareils connectés à Internet infectés par une menace et pouvant servir à envoyer des pourriels, voler des données, contrôler à distance les appareils vulnérables ou diffuser des logiciels espions, rançongiciels, ou tout autre type de menace. Leur objectif est d'infecter autant d'appareils connectés que possible, comme les PC, serveurs, mobiles ou autres objets connectés appartenant à des grandes entreprises.

Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les principaux navigateurs comprennent Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Ce sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugiciels) pour certains formats.

Attaque par force brute

Les attaques qui essayent de pénétrer un système informatique en saisissant toutes les combinaisons de mots de passe possible, ce en commençant par les mots de passe les plus faciles à deviner.

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Cookies

Sur Internet, les témoins sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des témoins est encore en développement. Son but est de cibler directement les intérêts que vous avez exprimés. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "code SKU" (ce code barres se trouvant au dos des produits de consommation). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Cyberharcèlement

Lorsque des camarades ou des inconnus mènent des actions abusives envers des enfants dans le but de les blesser physiquement. Pour leur nuire sur le plan émotionnel, les assaillants envoient des messages malveillants ou des photos peu flatteuses, provoquant l’isolation de leurs victimes ou un sentiment de frustration.

Attaque par dictionnaire

Les attaques qui essayent de pénétrer un système informatique en saisissant une combinaison de mots communs pour générer des mots de passe potentiels. La même méthode est utilisée pour deviner les clés de chiffrements des messages ou documents chiffrés. Les attaques par dictionnaire fonctionnent car de nombreuses personnes ont tendance à choisir des mots de passe simples à deviner et ne contenant qu'un seul mot.

Lecteur de disque

C'est un appareil qui lit et écrit des données sur un disque. Une unité de disque dur lit et écrit sur un disque dur. Un lecteur de disquette accède à des disquettes. Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

Télécharger

Copier des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

E-mail

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire.

Exploits

Une manière de tirer profit des bugs et vulnérabilités (logicielles ou matérielles) qui sont présents sur un ordinateur. Les pirates peuvent ainsi prendre le contrôle des ordinateurs ou réseaux.

Faux positif

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Extension du nom de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier. De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS-DOS. Elles comportent communément une à trois lettres (certains systèmes plus anciens n'en supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Heuristique

Méthode basée sur des règles permettant d'identifier de nouvelles menaces. Cette méthode d'analyse ne s'appuie pas sur une base de données d'information sur les menaces spécifique. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'une menace existante. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

Pot de miel

Un faux système informatique est créé pour attirer les pirates informatiques afin d'étudier la façon dont ils agissent et identifient les méthodes hérétiques utilisées pour collecter des informations sur le système. Les sociétés et les entreprises sont plus intéressées par la mise en place et l'utilisation de pots de miel pour améliorer leur état de sécurité global.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Applet Java

Il s'agit d'un programme Java conçu pour s'exécuter uniquement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les

applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Enregistreur de frappe

Un enregistreur de frappe est une application qui enregistre tout ce qui est saisi avec le clavier. Les enregistreurs de frappe ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros d'assurance sociale).

Virus macro

Type de menace codée sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants langages macro. Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Client de messagerie

Un client de messagerie est une application qui vous permet d'envoyer et recevoir des e-mails.

Mémoire

Zone de stockage interne dans votre ordinateur. Le terme mémoire regarde le stockage des données dans les "chips" (composants), et le terme stockage regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Non-heuristique

Cette méthode d'analyse s'appuie sur une base de données d'information sur les menaces spécifique. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être une menace et ne génère donc pas de fausses alertes.

Prédateurs en ligne

Individus cherchant à discuter avec des mineurs et des adolescents dans le but de les impliquer dans des activités sexuelles illégales. Les réseaux sociaux sont l’endroit idéal pour traquer les enfants vulnérables et les séduire dans le but de les faire se livrer à des activités sexuelles, en ligne ou en face à face.

Programmes compressés

Fichier dans un format compressé. Beaucoup de systèmes d'exploitation et d'applications contiennent des commandes vous permettant de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide" à la suite. Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

Chemin

Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas.

La connexion entre deux points, comme le canal de communication entre deux ordinateurs.

Phishing

Action d'envoyer un courriel à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du courriel. Cet courriel oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Photon

Photon est une technologie Bitdefender innovante et discrète, conçue pour limiter l'impact de la solution de sécurité sur les performances. En surveillant l'activité de votre PC en tâche de fond, elle crée des modèles d'utilisation qui aident à optimiser les processus de démarrage et d'analyse.

Virus polymorphe

Menace qui change de forme avec chaque fichier qu'elle infecte. Ces menaces n'ayant pas de forme unique bien définie, elles sont plus difficiles à identifier.

Port

Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les PCs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Ransomware

Les ransomwares sont des programmes malveillants qui tentent de soutirer de l'argent aux utilisateurs en bloquant leurs systèmes vulnérables. CryptoLocker, CryptoWall, et TeslaWall ne sont que des variantes qui traquent les systèmes personnels des utilisateurs.

L'infection peut se répandre via courriel, le téléchargement de pièces jointes, ou l'installation d'applications, sans prévenir l'utilisateur de ce qui se passe dans son système. Les utilisateurs quotidiens et les entreprises sont ciblés par les pirates derrière les rançongiciels.

Fichier de rapport

Un fichier qui enregistre les actions qui surviennent. BitDefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant aux administrateurs d'accéder à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs systèmes.

Le principal rôle des rootkits est de cacher des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau, s'ils incluent les logiciels appropriés.

Les trousses administrateur ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications

cachent des fichiers sensibles en utilisant des trousses administrateur. Cependant, ils sont principalement utilisés pour camoufler des menaces ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des menaces, les trousses administrateur pirates sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des journaux et passer inaperçus.

Script

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Spam

Message électronique ou envoi de messages souvent répertoriés comme des e-mails « non sollicités ».

Spyware

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les logiciels espions sont généralement cachés dans des partagiciels et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des partagiciels et logiciels gratuits ne contiennent pas de logiciels espions. Une fois installé, le logiciel espion surveille l'activité de l'utilisateur sur internet et transmet discrètement ces informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même, les numéros de cartes bancaires.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'être victime de logiciels espions est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les logiciels espions volent les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

Éléments de démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage de l'ordinateur. Par exemple, un écran de démarrage, un fichier son pour le démarrage de l'ordinateur, un calendrier, des programmes, peuvent être placés dans ce dossier. C'est généralement un raccourci vers le fichier qui est placé dans le dossier, et pas le fichier.

Abonnement

Achetez une licence qui donne à l'utilisateur le droit d'utiliser un produit ou service particulier sur un nombre spécifique d'appareils et pour un certain laps de temps. Un abonnement expiré peut être renouvelé automatiquement en utilisant les informations données par l'utilisateur lors du premier achat.

Barre d'état

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.

TCP/IP

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des normes pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Menace

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des menaces peuvent également se répliquer. Toutes les menaces informatiques sont créées par des personnes. Une menace simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même une menace simple comme celle décrite est dangereuse puisqu'elle remplit vite la mémoire et bloque le système. Une menace plus dangereuse encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Mise à jour des informations sur les menaces

La signature binaire de la menace, utilisée par la solution de sécurité pour détecter et éliminer la menace.

Cheval de Troie

Programme destructeur qui prétend être une application normale. À la différence des programmes malveillants comme les vers, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout autant destructeurs. L'un des types les plus pernicieux de chevaux de Troie est un programme qui, sous couvert de supprimer les menaces de votre ordinateur, en installe en fait de nouvelles.

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Mise à jour

Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas.

BitDefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

VPN (réseau virtuel privé)

C'est une technologie qui permet une connexion temporaire et chiffrée à un certain réseau plutôt qu'à un autre moins sécurisé. De cette façon, l'envoi et la réception de données sont protégés et chiffrés et plus difficiles à intercepter pour les pirates. Une preuve de sécurité est l'identification, qui ne peut se faire que via un identifiant et un mot de passe.

Ver

Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.