



**Bitdefender®**

**Endpoint Security for  
Mac**

**MANUEL D'UTILISATION**

## Endpoint Security for Mac Manuel d'utilisation

Date de publication 2020.08.31

Copyright© 2020 Bitdefender

### Mentions Légales

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduite ou transmise, sous aucune forme et d'aucune façon, électronique ou physique, y compris photocopies, enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de Bitdefender. L'inclusion de courtes citations dans des textes n'est possible qu'avec la mention de la source. Le contenu ne peut en aucun cas être modifié.

**Avertissement.** Ce produit et sa documentation sont protégés par copyright. Les informations de ce document sont données « à titre indicatif », sans garantie. Bien que toutes les précautions aient été prises lors de la préparation de ce document, les auteurs ne pourront être tenus responsables envers quiconque de toute perte ou dommage occasionné, ou supposé occasionné, directement ou indirectement par les informations contenues dans ce document.

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

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

## Table des matières

Utilisation de ce guide .....	v
1. Objectifs et destinataires .....	v
2. Comment utiliser ce guide .....	v
3. Conventions utilisées dans ce guide .....	vi
3.1. Normes Typographiques .....	vi
3.2. Avertissements .....	vi
4. Commentaires .....	vii
1. Pour démarrer .....	1
1.1. À propos de Endpoint Security for Mac .....	1
1.2. Ouvrir Endpoint Security for Mac .....	1
1.3. Fenêtre Principale de l'Application .....	2
1.4. Icône Dock de l'Application .....	4
2. Protection contre les malwares .....	5
2.1. Utilisation optimale .....	5
2.2. Analyse de Votre Mac .....	5
2.3. Assistant d'analyse .....	6
2.4. Correction des problèmes .....	7
2.5. Quarantaine .....	9
2.6. Contrôle de contenu .....	10
2.7. Contrôle des appareils .....	11
2.8. Protection Web .....	12
2.9. Mises à jour .....	13
2.9.1. Demandes de mise à jour .....	14
2.9.2. Obtenir des Mises à jour via un Serveur Proxy .....	14
2.9.3. Mise à jour vers une nouvelle version .....	14
3. Utilisation du module Chiffrement .....	15
3.1. Chiffrer des volumes .....	15
3.2. Déchiffrer des volumes .....	17
3.3. Modifier la clé de récupération .....	18
3.4. Modifier le mot de passe de chiffrement .....	19
4. Configuration des Préférences .....	21
4.1. Accéder aux Préférences .....	21
4.2. Quarantaine .....	21
4.3. Historique .....	21
4.4. Préférences d'analyse .....	22
5. Utiliser l'outil de Ligne de commande .....	23
5.1. Commandes prises en charge .....	24
5.2. Le paramètre authToken .....	26
5.3. Codes d'erreur .....	26
6. Questions les Plus Fréquentes .....	28
7. Obtenir de l'aide .....	30



Types de Logiciels Malveillants ..... 31

## Utilisation de ce guide

### 1. Objectifs et destinataires

Cette documentation est destinée aux utilisateurs finaux d'**Endpoint Security for Mac**, le logiciel client de Security for Endpoints installé sur les ordinateurs afin de les protéger contre les malwares et les autres menaces d'Internet. Les informations présentées ici devraient être faciles à comprendre par toute personne capable de travailler sous Macintosh.

Vous découvrirez comment configurer et utiliser Endpoint Security for Mac pour protéger votre ordinateur contre les virus et les autres logiciels malveillants. Vous saurez comment tirer le meilleur parti de Bitdefender.

Nous vous souhaitons un apprentissage agréable et utile.

### 2. Comment utiliser ce guide

Ce guide est organisé autour de plusieurs thèmes essentiels :

[Pour démarrer \(p. 1\)](#)

Commencez à utiliser Endpoint Security for Mac et son interface utilisateur.

[Protection contre les malwares \(p. 5\)](#)

Apprenez à utiliser Endpoint Security for Mac pour protéger votre ordinateur contre les logiciels malveillants.

[Configuration des Préférences \(p. 21\)](#)

Découvrez les préférences disponibles dans Endpoint Security for Mac.

[Obtenir de l'aide \(p. 30\)](#)

Sachez où regarder et à qui demander de l'aide si quelque chose d'inattendu apparaît.

## 3. Conventions utilisées dans ce guide

### 3.1. 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.

Apparence	Description
exemple de syntaxe	Les exemples de syntaxe sont imprimés avec des caractères séparés d'un espace.
<a href="http://www.bitdefender.fr">http://www.bitdefender.fr</a>	Les liens URL pointent vers un emplacement externe comme un serveur http ou ftp.
<a href="mailto:documentation@bitdefender.com">documentation@bitdefender.com</a>	Les adresses e-mail sont insérées dans le texte pour plus d'informations sur les contacts.
<a href="#">Utilisation de ce guide (p. v)</a>	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
nom de fichier	Les fichiers et répertoires sont imprimés en utilisant des caractères séparés d'un espace.
<b>option</b>	Toutes les options du produit sont imprimées à l'aide de caractères <b>gras</b> .
<b>mot clé</b>	Les mots-clés et les expressions importantes sont mises en évidence à l'aide de caractères <b>gras</b> .

### 3.2. Avertissements

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.



#### Note

La note est une courte observation. Bien que vous puissiez l'omettre, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien à un thème proche.



#### Important

Cette icône requiert votre attention et nous vous recommandons de ne pas l'ignorer. Elle fournit habituellement des informations non critiques mais significatives.

**Avertissement**

Marque une information critique que vous devrez lire attentivement. Rien de négatif ne se passera si vous suivez les indications. Vous devriez le lire et le comprendre car cette marqué décrit une opération risquée.

## 4. Commentaires

Nous vous invitons à nous aider à améliorer ce livret. Nous avons testé et vérifié toutes les informations mais vous pouvez trouver que certaines fonctions ont changé. N'hésitez pas à nous écrire pour nous dire si vous avez trouvé des erreurs dans ce livret ou concernant toute amélioration que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Faites le nous savoir en nous écrivant à cette adresse [documentation@bitdefender.com](mailto:documentation@bitdefender.com). Merci de bien vouloir rédiger en anglais vos e-mails concernant cette documentation afin que nous puissions les traiter efficacement.

## 1. POUR DÉMARRER

Ce chapitre traite des sujets suivants :

- À propos de Endpoint Security for Mac
- Ouvrir Endpoint Security for Mac
- Fenêtre Principale de l'Application
- Icône Dock de l'Application

### 1.1. À propos de Endpoint Security for Mac

Endpoint Security for Mac est un programme de sécurité informatique entièrement automatisé, géré à distance par votre administrateur réseau. Une fois installé, il vous protège contre tous les types de malwares y compris contre les virus, spywares, chevaux de Troie, keyloggers, vers et adwares. Il peut également être utilisé pour appliquer les politiques d'utilisation des ordinateurs et d'Internet de votre entreprise.

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

### 1.2. Ouvrir Endpoint Security for Mac

Vous pouvez ouvrir Endpoint Security for Mac de différentes façons.

- Cliquez sur l'icône de Endpoint Security for Mac dans le Launchpad.
- Ouvrez une fenêtre Finder, allez dans **Applications** et double-cliquez sur l'icône de **Endpoint Security for Mac**.
- Vous pouvez également utiliser Spotlight pour trouver et ouvrir l'application.

Quand l'application s'ouvre, elle détecte automatiquement la langue de votre système et affichera l'interface utilisateur dans votre langue.



#### Note

Si la langue du système ne fait pas partie des langues supportées par Endpoint Security for Mac, l'application va charger l'interface en anglais par défaut.



## 1.3. Fenêtre Principale de l'Application

La fenêtre principale de l'application vous permet d'appliquer des actions importantes pour améliorer la protection de votre système. Vous pouvez connaître l'état de sécurité de votre ordinateur et de sécuriser votre navigation sur Internet.



Fenêtre Principale de l'Application

La barre d'état en haut de la fenêtre vous informe de l'état de sécurité de votre système à l'aide de messages clairs et de couleurs évocatrices :

- Vert - Si Endpoint Security for Mac n'a aucun avertissement.
- Jaune - Si un problème de sécurité a été détecté.
- Rouge - Si la licence a expiré.

Sous la barre d'état, trois boutons d'analyse sont disponibles pour vous aider à analyser votre Mac :

- **Quick Scan (Analyse rapide)** - recherche des malwares aux emplacements les plus vulnérables de votre système (par exemple, dans les dossiers contenant

les documents, les téléchargements, les téléchargements de messagerie et les fichiers temporaires de chaque utilisateur).

- **Full Scan (Analyse complète)** - effectue une analyse antimalware complète de l'ensemble du système. Tous les volumes montés connectés seront également analysés.
- **Custom Scan (Analyser un emplacement spécifique)** - vous aide à rechercher des malwares dans certains fichiers, dossiers ou volumes.

Pour plus d'informations, reportez-vous à [Analyse de Votre Mac \(p. 5\)](#).

À côté des boutons d'analyse, la section Modules vous informe sur :

- **L'antimalware** - vous permet de savoir si l'analyse à l'accès est activée (On) ou désactivée (Off).
- **Contrôle du contenu** - vous permet de savoir si les composants suivants sont activés (On) ou désactivés (Off) :
  - Analyse du trafic
  - Liste noire des applications
  - Contrôle de l'accès à Internet
  - Antiphishing
- **Contrôle des appareils** - vous indique si le module est activé (On) ou désactivé (Off).



### Note

Les modules Contrôle du contenu et Contrôle des appareils sont disponibles à partir de l'OS X El Capitan (10.11). Ces fonctionnalités reposent sur une extension du noyau macOS. Votre autorisation vous sera demandée pour l'installation de ces extensions sur macOS High Sierra (10.13) et supérieur.

- **Chiffrement** – indique le statut de chaque disque (Chiffré, Chiffrement en cours, Déchiffrement en cours, Non chiffré, Verrouillé ou En pause) si une politique de chiffrement GravityZone est appliquée à votre ordinateur.
- **EDR Sensor** - informs you if the EDR module is enabled (On) or disabled (Off).

Sous les boutons d'analyse, une autre option est disponible :

- **Protection Web** - filtre l'ensemble du trafic web et bloque tout contenu malveillant pour sécuriser votre navigation sur Internet. Pour plus d'informations, reportez-vous à [Protection Web \(p. 12\)](#).

**Note**

La Protection Web est disponible sur OS X Mavericks (10.9) et OS X Yosemite (10.10). À partir de l'OS X El Capitan (10.11), cette fonction est remplacée par le Contrôle du contenu.

En bas de la fenêtre, en cliquant sur le bouton **Afficher l'historique**, vous ouvrez un journal des événements détaillé en rapport avec l'activité d'Endpoint Security for Mac sur votre ordinateur. Pour plus d'informations, référez-vous à [Historique \(p. 21\)](#).

## 1.4. Icône Dock de l'Application

L'icône de Endpoint Security for Mac apparaît dans le Dock dès que vous ouvrez l'application. L'icône du Dock vous permet d'analyser facilement des fichiers et des dossiers à la recherche de malwares. Glissez-déposez simplement le fichier ou le dossier sur l'icône du Dock et l'analyse démarrera immédiatement.



Icône du Dock

## 2. PROTECTION CONTRE LES MALWARES

Ce chapitre traite des sujets suivants :

- Utilisation optimale
- Analyse de Votre Mac
- Assistant d'analyse
- Correction des problèmes
- Quarantaine
- Contrôle de contenu
- Contrôle des appareils
- Protection Web
- Mises à jour

### 2.1. Utilisation optimale

Pour maintenir votre système sans malwares et pour éviter l'infection accidentelle d'autres systèmes, adoptez ces meilleures pratiques :

- Vérifiez et corrigez régulièrement les problèmes signalés par Endpoint Security for Mac. Pour plus d'informations, reportez-vous à [Correction des problèmes](#) (p. 7).
- Nous vous recommandons également d'adopter les pratiques suivantes :
  - Prenez l'habitude d'analyser les fichiers que vous téléchargez à partir d'un support de stockage externe (comme une clé USB ou un CD), en particulier lorsque vous ne connaissez pas la source.
  - Si vous avez un fichier DMG, montez-le puis analysez son contenu (les fichiers du volume/de l'image monté(e)).

### 2.2. Analyse de Votre Mac

Le module d'Analyse à l'accès surveille votre ordinateur en continu, à la recherche d'actions de malwares et empêchant les nouvelles menaces malwares de pénétrer votre système. L'Analyse à l'accès est contrôlée par votre administrateur réseau via les politiques de sécurité.

Vous pouvez également analyser votre Mac ou des fichiers spécifiques chaque fois que vous le souhaitez.

La façon la plus facile d'analyser un fichier, un dossier ou un volume est d'amener & vers l'icône Station. L'assistant d'analyse apparaîtra et vous aidera dans le processus d'analyse.

Vous pouvez également lancer une analyse comme suit :

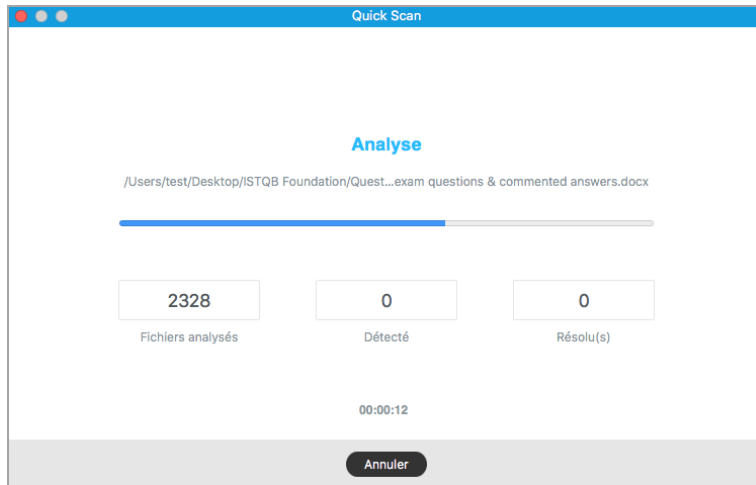
1. Ouvrez Endpoint Security for Mac.
2. Cliquez sur l'un des trois boutons d'analyse pour lancer l'analyse souhaitée.
  - **Quick Scan (Analyse rapide)** - recherche des malwares aux emplacements les plus vulnérables de votre système (par exemple, dans les dossiers contenant les documents, les téléchargements, les téléchargements de messagerie et les fichiers temporaires de chaque utilisateur).
  - **Full Scan (Analyse complète)** - effectue une analyse antimalware complète de l'ensemble du système. Tous les volumes montés connectés seront également analysés.

### Note

- En fonction de la taille de votre disque dur, l'analyse de l'ensemble du système peut être longue (une heure ou plus). Pour de meilleures performances, nous vous recommandons de ne pas exécuter cette tâche lorsque vous effectuez d'autres tâches consommant beaucoup de ressources (comme du montage vidéo).
  - You can also run a quick scan or a full scan by using the **productConfigurationTool** [Utiliser l'outil de Ligne de commande \(p. 23\)](#).
- **Custom Scan (Analyser un emplacement spécifique)** - vous aide à rechercher des malwares dans certains fichiers, dossiers ou volumes.

## 2.3. Assistant d'analyse

Lorsque vous lancez une analyse, l'assistant d'analyse Endpoint Security for Mac apparaît.



Analyse en Cours...

Vous pouvez voir les informations en temps réel sur l'analyse, comme le nombre de menaces détectées et le nombre de problèmes résolus.

Attendez qu'Endpoint Security for Mac termine l'analyse.



### Note

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

## 2.4. Correction des problèmes

Endpoint Security for Mac détecte automatiquement un ensemble de problèmes pouvant affecter la sécurité de votre système et de vos données et vous informe à leur sujet.

Les problèmes détectés peuvent se référer à :

- Les nouvelles signatures malwares et mises à jour produit n'ont pas été téléchargées à partir des serveurs Bitdefender.
- Des menaces de sécurité ont été détectées sur votre système.
- Le module d'Analyse à l'accès est désactivé.
- La licence a expiré.

La réparation des problèmes indiqués par Endpoint Security for Mac est un processus simple et rapide. Ainsi vous pouvez réparer les risques de sécurité en temps voulu.

Pour consulter et corriger les problèmes détectés :

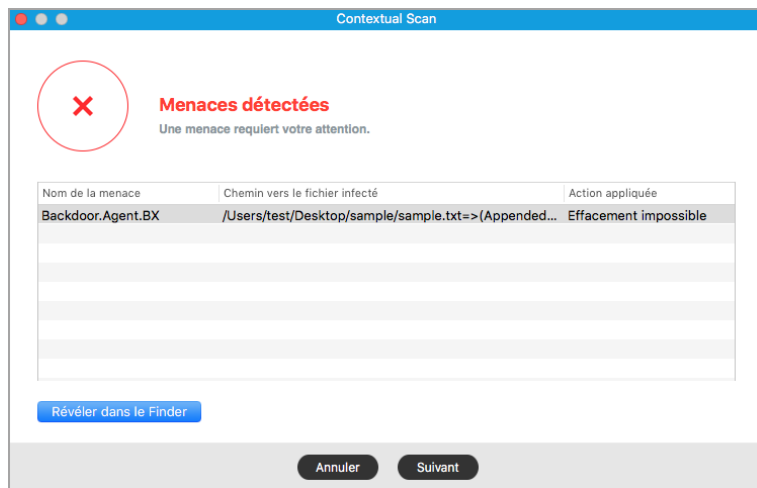
1. Ouvrez Endpoint Security for Mac.
2. Vérifier la couleur de la zone d'état :
  - Vert - votre Mac est protégé.
  - Jaune ou rouge - Votre Mac a des problèmes. Pour enquêter plus avant, veuillez suivre les étapes suivantes.
3. Consultez la description pour plus d'informations.
4. Selon le nombre et type de problèmes détectés, un bouton peut être disponible dans la barre d'états :
  - **Réparer problème**, si un seul problème a été trouvé. Cliquez sur le bouton pour réparer rapidement le risque de sécurité.
  - **Afficher les problèmes**, si plus d'un problème ont été trouvés. Cliquez sur le bouton pour afficher les problèmes. Une nouvelle fenêtre apparaît et ensuite réparer les problèmes.

Si des malwares ont été détecté, l'application va automatiquement tenter de les supprimer et de reconstruire le fichier d'origine. Cette opération est appelée la désinfection. Les fichiers qui ne peuvent pas être désinfectés sont déplacés en quarantaine pour contenir l'infection.

Si le fichier ne peut être ni désinfecté ni placé en quarantaine, Endpoint Security for Mac vous informe du problème et vous pouvez le supprimer manuellement.

Pour supprimer les infections manuellement :

- Cliquez sur le bouton **Révéler dans Recherche**.
- Sélectionnez le fichier et supprimez-le de votre système.  
Si le fichier venait d'une application installée, assurez-vous de bien avoir réparer l'installation pour que le programme puisse fonctionner correctement.



Fenêtre Menaces non résolues

Certains problèmes nécessiteront peut être que votre administrateur réseau les répare à partir de la console d'administration, par exemple :

- Activation du module A l'accès via la politique de sécurité.
- Renouvellement de la licence expirée.

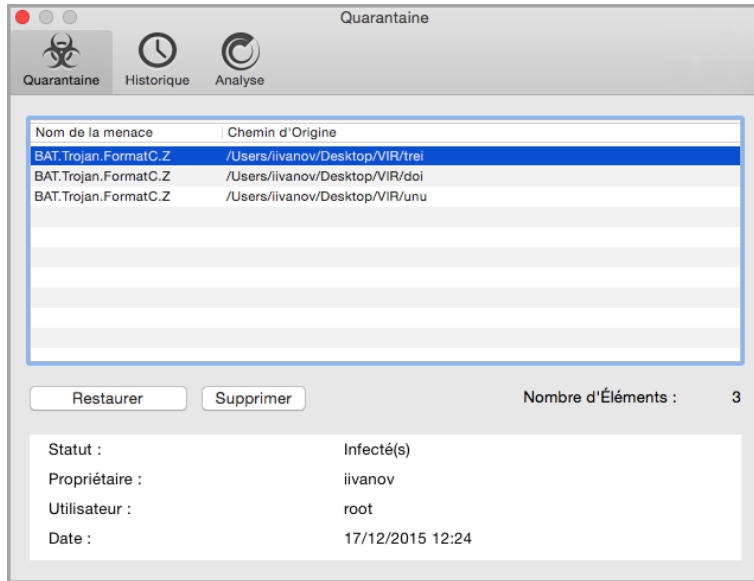
## 2.5. Quarantaine

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

Pour voir et gérer les fichiers mis en quarantaine, ouvrez la fenêtre **Quarantaine** :

1. Faites un clic droit sur l'icône Bitdefender dans la barre de menu.
2. Choisissez **Préférences** dans la liste des options. Une fenêtre va apparaître.
3. Choisissez l'onglet **Voir Quarantaine**.





Fichiers placés en quarantaine

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

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

## 2.6. Contrôle de contenu

Le module Contrôle du contenu vous protège contre les tentatives de phishing et de fraude pendant que vous naviguez sur Internet ; tout en vous signalant les contenus inappropriés. Il inclut également une gamme complète de commandes qui permettent à l'administrateur réseau de définir des politiques d'utilisation des ordinateurs et des navigateurs Internet. Ce module fonctionne avec Chrome, Firefox et Safari.

- **Analyse du trafic.** Ce composant empêche le téléchargement de malwares sur l'endpoint en analysant le trafic web en temps réel.

- **Liste noire des applications.** Ce composant empêche l'accès à des applications non autorisées dans votre entreprise. L'administrateur est responsable de la création de règles pour les applications autorisées dans l'entreprise.
- **Contrôle de l'accès à Internet.** Ce composant vous protège contre l'accès à des sites web dangereux grâce aux règles définies par l'administrateur.
- **Antiphishing.** Ce composant bloque automatiquement les pages connues pour abriter des mécanismes de phishing ; afin que les utilisateurs ne risquent pas de dévoiler par inadvertance des informations personnelles ou confidentielles à des escrocs.

### **Note**

Le module Contrôle du contenu est disponible à partir d'OS X El Capitan (10.11). Cette fonctionnalité repose sur une extension du noyau macOS. Votre autorisation vous sera demandée pour l'installation de ces extensions sur macOS High Sierra (10.13). Le système nous informe qu'une extension Bitdefender a été bloquée et que vous devez l'autoriser (en allant dans **Sécurité & Confidentialité**). Tant que cette extension Bitdefender n'a pas été autorisée, ce module ne fonctionne pas et un message à ce sujet apparaît dans l'interface utilisateur d'Endpoint Security for Mac.

## 2.7. Contrôle des appareils

Le module **Contrôle des appareils** permet de lutter contre les fuites de données sensibles et les infections transmises par des périphériques externes connectés aux endpoints, en appliquant des règles de blocage à une grande variété de périphériques. L'administrateur est chargé de la gestion des permissions pour les appareils suivants :

- Périphériques Bluetooth
- Périphériques CD-ROM
- Périphériques de traitement d'images
- Modems
- Mobile Windows
- Imprimantes
- Adaptateurs réseau
- Adaptateurs réseau sans fil
- Périphériques de stockage externe

### **Note**

Le module Contrôle des appareils est disponible à partir d'OS X El Capitan (10.11). Cette fonctionnalité repose sur une extension du noyau macOS. Votre autorisation

vous sera demandée pour l'installation de ces extensions sur le macOS High Sierra (10.13). Le système nous informe qu'une extension Bitdefender a été bloquée et que vous devez l'autoriser (en allant dans **Sécurité & Confidentialité**). Tant que cette extension Bitdefender n'a pas été autorisée, ce module ne fonctionne pas et un message à ce sujet apparaît dans l'interface utilisateur d'Endpoint Security for Mac.

## 2.8. Protection Web

Endpoint Security for Mac utilise les extensions TrafficLight pour protéger complètement votre navigation sur Internet. Les extensions TrafficLight interceptent, traitent et filtrent l'ensemble du trafic web en bloquant tous les contenus malveillants.

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



### Note

Cette fonction est disponible sur OS X Mavericks (10.9) et OS X Yosemite (10.10). À partir de l'OS X El Capitan (10.11), la Protection Web est remplacée par le Contrôle du contenu.

Un vaste ensemble de fonctionnalités est disponible pour vous protéger contre toutes sortes de menaces présentes sur Internet :

- Filtre antiphishing de pointe - il vous empêche d'accéder aux sites web utilisés pour perpétrer des attaques de phishing.
- Filtre antimalware - bloque tout malware rencontré en naviguant sur Internet.
- Analyseur des résultats de recherche - informe de la présence de sites Web à risque dans les résultats de recherche.
- Filtre Antifraude - fournit une protection contre les sites web frauduleux sur Internet.
- Signalement de trackers - détecte les trackers présents sur les pages web consultées protégeant ainsi votre vie privée sur Internet.

## Activer les extensions Linkchecker




Pour activer les extensions TrafficLight, procédez comme suit :

1. Ouvrez Endpoint Security for Mac.
2. Cliquez sur **Réparer maintenant** pour ouvrir la fenêtre Web Protection.

3. Endpoint Security for Mac va détecter le navigateur Web que vous avez installé sur votre système. Pour installer l'extension TrafficLight que vous souhaitez, cliquez sur **Obtenir extension** dans le panneau correspondant.
4. Vous serez redirigé vers cet emplacement en ligne :  
<http://bitdefender.fr/solutions/trafficlight.html>
5. Sélectionnez **Téléchargement gratuit**.
6. Suivez ces étapes pour installer l'extension TrafficLight pour le navigateur Web sélectionné.

## Page des notes et alertes

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

-  C'est une page sûre. Vous pouvez continuer votre travail.
-  Cette page web peut contenir du contenu dangereux. Soyez prudent si vous décidez de la consulter.
-  Vous devez quitter cette page Web tout de suite. Sinon, veuillez choisir l'une des options disponibles :
  - Quittez le site web en cliquant sur **Retour en toute sécurité**.
  - Pour vous rendre sur le site web, malgré l'avertissement, cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**.

## 2.9. Mises à jour

Chaque jour, de nouveaux codes malveillants sont détectés et identifiés. C'est pourquoi il est très important de maintenir Endpoint Security for Mac à jour avec les dernières signatures de codes malveillants.

Quand **l'Analyse à l'accès** est activée, les signatures malwares et les mises à jour produites sont téléchargées automatiquement sur votre système. Si votre administrateur réseau désactive le module A l'accès via une politique, vous devrez demander une mise à jour manuellement pour votre application Endpoint Security for Mac.

La mise à jour des signatures de malwares est exécutée à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi,

la mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

### 2.9.1. Demandes de mise à jour

Vous pouvez demander une mise à jour manuellement à tout moment. Une mise à jour à la demande de l'utilisateur est recommandée avant que vous ne lanciez une analyse complète.

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

Comment lancer une mise à jour manuellement :

1. Ouvrez Endpoint Security for Mac.
2. Cliquez sur **Actions** dans la barre de menus.
3. Sélectionnez **Mettre à jour la base de données des virus**.

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

### 2.9.2. Obtenir des Mises à jour via un Serveur Proxy

Endpoint Security for Mac peut se mettre à jour uniquement via des serveurs proxy n'exigeant pas d'authentification. Vous n'avez aucun paramètre à configurer dans le programme.

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

### 2.9.3. Mise à jour vers une nouvelle version

Nous publions parfois des mises à jour du produit pour améliorer ses fonctionnalités. Ces mises à jour peuvent nécessiter un redémarrage du système pour lancer l'installation de nouveaux fichiers. Par défaut, si une mise à jour nécessite un redémarrage de l'ordinateur, Endpoint Security for Mac continuera à fonctionner avec les anciens fichiers jusqu'au redémarrage du système. Dans ce cas, le processus de mise à jour n'interférera pas avec votre travail.

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

## 3. UTILISATION DU MODULE CHIFFREMENT

Le module de chiffrement permet le chiffrement complet de disques sur votre Mac par le biais de politiques appliquées par votre administrateur de la sécurité. L'agent de sécurité exécute FileVault pour chiffrer le disque de démarrage du Mac et l'utilitaire de ligne de commande diskutil pour chiffrer tout autre disque. Les disques amovibles ne sont pas chiffrés.

Ce chapitre traite des sujets suivants :

- [Chiffrer des volumes](#)
- [Déchiffrer des volumes](#)
- [Modifier la clé de récupération](#)
- [Modifier le mot de passe de chiffrement](#)

### 3.1. Chiffrer des volumes

Lorsqu'une politique de chiffrement est appliquée sur votre Mac :

- Pour les disques de démarrage :
  1. Une fenêtre vous invite à saisir votre nom d'utilisateur et votre mot de passe système.



The screenshot shows a dialog box titled "Chiffrer avec FileVault" from "Endpoint Security for Mac". The text inside reads: "Saisissez vos identifiants système pour chiffrer le disque suivant : Macintosh HD". Below this, there are two input fields: "User:" and "Password:". At the bottom, there are two buttons: "Pas maintenant" and "OK".

2. Cliquez sur le bouton **OK** pour débiter le processus de chiffrement.

Si vous cliquez sur l'option **Pas maintenant**, le processus de chiffrement sera repoussé, mais la fenêtre réapparaîtra au bout d'un certain temps. La fenêtre continuera d'apparaître aussi longtemps que la politique de chiffrement sera active sur le Mac.

3. Voici ce qu'il se passe une fois que la fenêtre **Chiffrer avec FileVault** se ferme :
  - Si le système d'exploitation de votre Mac est antérieur à macOS Catalina (10.15), le processus de chiffrement débute immédiatement.
  - Si votre Mac est sous macOS Catalina (10.15), Endpoint Security for Mac ("fdesetup") demandera, dans une nouvelle fenêtre, votre accord pour activer FileVault. Cliquez sur le bouton **OK** pour débiter le chiffrement. En cliquant sur **Ne pas autoriser**, Endpoint Security for Mac ne débutera pas le chiffrement et vous demandera de nouveau votre autorisation après quelques minutes.

**Note**

En cas de système dual-boot, l'autre volume de démarrage ne sera pas chiffré.

- Pour les autres disques :
  1. Une fenêtre vous invite à configurer un mot de passe dédié au chiffrement de chaque disque. Ce mot de passe est nécessaire uniquement pour déverrouiller un disque spécifique (autre que le disque de démarrage).
  2. Cliquez sur **Enregistrer**. Le processus de chiffrement démarre immédiatement.

Si vous cliquez sur l'option **Ignorer**, le processus de chiffrement sera repoussé. La boîte de dialogue réapparaîtra au bout d'un certain temps et continuera d'apparaître aussi longtemps que la politique de chiffrement sera active sur le Mac.

Endpoint Security for Mac

## Définir MdP de chiffrement

NonBoot

Choisissez un mot de passe

Retaper mot de passe

Prérequis du mot de passe :

- ✘ Contient entre 8 et 30 caractères
- ✘ Doit contenir une minuscule et une majuscule
- ✘ Doit contenir un chiffre

Dismiss

Si le Mac possède plus d'un disque, les boîtes de dialogue pour le chiffrement de tous les disques apparaîtront au même moment.

## 3.2. Déchiffrer des volumes

Lorsqu'une politique de déchiffrement est appliquée sur votre Mac :

- Pour les disques de démarrage :
  1. Une boîte de dialogue vous invite à saisir votre nom d'utilisateur et votre mot de passe système.
  2. Cliquez sur **OK**. Le processus de déchiffrement démarre immédiatement.
- Pour les autres disques :
  1. Une boîte de dialogue vous invite à saisir le mot de passe utilisé pour le chiffrement.
  2. Cliquez sur **Enregistrer**. Le processus de déchiffrement démarre immédiatement.

Si vous cliquez sur l'option **Ignorer**, le processus de déchiffrement sera repoussé. La boîte de dialogue réapparaîtra au bout d'un certain temps et



continuera d'apparaître aussi longtemps que la politique de chiffrement sera active sur le Mac.

Si le Mac possède plus d'un disque, les boîtes de dialogue pour le déchiffrement de tous les disques apparaîtront au même moment.

### 3.3. Modifier la clé de récupération

Après le démarrage du processus de chiffrement, Endpoint Security for Mac envoie une clé de récupération à la console de gestion de l'administrateur de la sécurité. Votre administrateur de la sécurité pourra se servir de cette clé de récupération si vous oubliez vos identifiants de connexion ou les mots de passe de chiffrement et que vous vous trouvez dans l'impossibilité de déverrouiller les disques, ou si le Mac est utilisé par un autre utilisateur et que celui-ci ne peut pas accéder à l'un des disques.

Vous pouvez modifier la clé de récupération associée au disque de démarrage sans avoir besoin de modifier vos identifiants de connexion.

Pour modifier la clé de récupération associée au chiffrement du disque de démarrage :

1. Cliquez sur le disque de démarrage chiffré dans la fenêtre principale d'Endpoint Security for Mac.
2. Cliquez sur l'option **Modifier la clé de récupération**.
3. Saisissez votre nom d'utilisateur et votre mot de passe système.
4. Cliquez sur le bouton **Sauvegarder**.



Endpoint Security for Mac

### Modifier la clé de récupération

Saisissez vos identifiants système pour modifier la clé de récupération du disque chiffré suivant: Macintosh HD

User:

Password:

Annuler

L'option permettant de modifier la clé de récupération n'est disponible que si une politique de chiffrement est appliquée sur votre Mac.

Lorsque vous modifiez le mot de passe système, le disque de démarrage chiffré reste tel qu'il est et aucune action n'est requise de votre part.

### 3.4. Modifier le mot de passe de chiffrement

Vous pouvez modifier le mot de passe de chiffrement pour les autres disques à partir de l'interface utilisateur d'Endpoint Security for Mac. Une fois le mot de passe modifié, Endpoint Security for Mac enverra une nouvelle clé de récupération à la console de gestion de l'administrateur de la sécurité.

Comment modifier le mot de passe de chiffrement d'un disque (autre que le disque de démarrage) :

1. Cliquez sur le nom du disque chiffré dans la fenêtre principale d'Endpoint Security for Mac.
2. Cliquez sur le bouton **Changer mot de passe**.
3. Dans la fenêtre **Modification du mot de passe de chiffrement**, configurez le nouveau mot de passe.
4. Cliquez sur **Enregistrer**.

Endpoint Security for Mac

## Modifier le mot de passe de chiffrement

NonBoot

Ancien mot de passe

Choisissez un mot de passe

Retaper mot de passe

---

Prérequis du mot de passe :

- ✘ Contient entre 8 et 30 caractères
- ✘ Doit contenir une minuscule et une majuscule
- ✘ Doit contenir un chiffre

Dismiss
Enregistrer

L'option permettant de modifier le mot de passe de chiffrement n'est disponible que si une politique de chiffrement est appliquée sur votre Mac.

## 4. CONFIGURATION DES PRÉFÉRENCES

Endpoint Security for Mac offre une gamme minimum d'options à configurer pour l'utilisateur, puisqu'il est géré par l'administrateur réseau via la politique assignée.

Ce chapitre traite des sujets suivants :

- [Accéder aux Préférences](#)
- [Quarantaine](#)
- [Historique](#)
- [Préférences d'analyse](#)

### 4.1. Accéder aux Préférences

Pour ouvrir la fenêtre des **Préférences** :

1. Ouvrez Endpoint Security for Mac.
2. Choisissez une des possibilités suivantes :
  - Cliquez sur Endpoint Security for Mac dans le menu Applications et choisissez **Préférences**.
  - Faites un clic du droit sur l'icône Bitdefender dans le menu États et choisissez **Préférences**.
  - Appuyez sur la touche Commande puis sur la virgule(,).
3. Cliquez sur l'onglet de la fonctionnalité que vous souhaitez configurer. Veuillez les trouver décrits ci-après.

### 4.2. Quarantaine

La partie Quarantaine affiche tous les fichiers actuellement isolés dans le dossier Quarantaine sur votre ordinateur local.

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

### 4.3. Historique

Endpoint Security for Mac vous donne le détail des événements dans le journal d'activité sur votre ordinateur. A chaque fois qu'un événement lié à la sécurité de votre Mac ou de vos données a lieu, un nouveau message est ajouté à l'historique

Endpoint Security for Mac. Les Événements sont un outil important dans la surveillance et la gestion de la protection de votre ordinateur. Par exemple, vous pouvez vérifier facilement si la mise à jour a bien été faite, si des malwares ont été trouvés sur votre ordinateur, etc.

Chaque fois que vous souhaitez supprimer l'historique, cliquez sur le bouton **Effacer Historique**. Le bouton **Copier** vous donne la possibilité de copier cette information dans le presse-papiers.

## 4.4. Préférences d'analyse

Cette fenêtre vous permet de choisir si Endpoint Security for Mac analyse les fichiers sauvegardés ou non. L'application vous informera uniquement d'une menace existante, puisque OS X protège votre disque Time Machine et empêche Endpoint Security for Mac de supprimer des fichiers. Si jamais il restaure des fichiers infectés plus tard, Endpoint Security for Mac les détectera automatiquement et prendra les dispositions nécessaires.

Par défaut, les fichiers sauvegardés sont exclus de l'analyse. Désélectionnez la case **Ne pas analyser le disque Time Machine** pour analyser cet emplacement également.

## 5. UTILISER L'OUTIL DE LIGNE DE COMMANDE

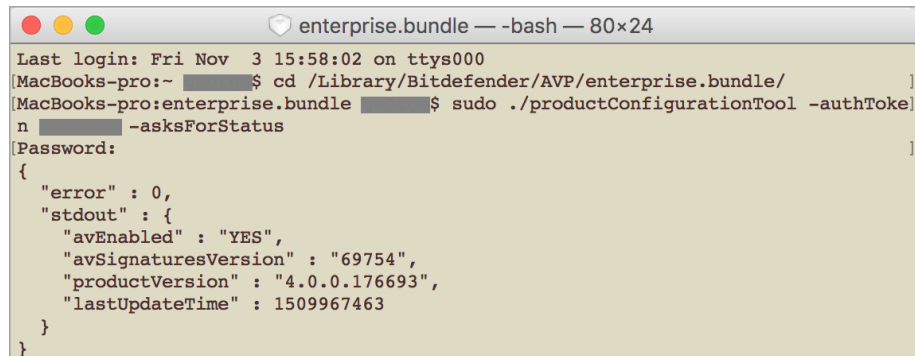
Endpoint Security for Mac vous permet d'exécuter certaines tâches en utilisant un outil de ligne de commande appelé **productConfigurationTool**. En particulier, vous pouvez récupérer des informations relatives au statut du produit et lancer des analyses système rapides et complètes.

Pour utiliser **productConfigurationTool** :

1. Ouvrez **Terminal** sur votre ordinateur.
2. Modifiez le répertoire de travail en utilisant la commande suivante :

```
cd /Library/Bitdefender/AVP/enterprise.bundle/
```

3. Exécutez les commandes prises en charge avec les privilèges administrateur (commande `sudo`).



```
enterprise.bundle — -bash — 80x24
Last login: Fri Nov  3 15:58:02 on ttys000
MacBooks-pro:~ ██████$ cd /Library/Bitdefender/AVP/enterprise.bundle/
MacBooks-pro:enterprise.bundle ██████$ sudo ./productConfigurationTool -authToken ██████ -asksForStatus
Password:
{
  "error" : 0,
  "stdout" : {
    "avEnabled" : "YES",
    "avSignaturesVersion" : "69754",
    "productVersion" : "4.0.0.176693",
    "lastUpdateTime" : 1509967463
  }
}
```

Utiliser `productConfigurationTool` dans le Terminal

Ce chapitre inclut les sujets suivants en relation avec **productConfigurationTool** :

- [Commandes prises en charge](#)
- [Le paramètre `authToken`](#)
- [Codes d'erreur](#)

## 5.1. Commandes prises en charge

L'interface **productConfigurationTool** prend en charge les commandes suivantes :

### **asksForStatus**

Récupère des informations concernant :

- Le statut du module antimalware (activé ou désactivé).
- La version des signatures antimalware.
- La version du produit.
- La date de la dernière mise à jour.

Comment l'utiliser :

```
sudo ./productConfigurationTool -authToken [password]
-asksForStatus
```

Exemple de résultat en cas de succès :

```
{
  "error" : 0,
  "stdout" : {
    "avEnabled" : "YES",
    "avSignaturesVersion" : "69440",
    "productVersion" : "4.0.0.175873",
    "lastUpdateTime" : 1507185205
  }
}
```

Exemple de résultat en cas d'échec :

```
"error" : 100
```

### **asksForAScanToRun**

Démarre une tâche d'analyse et fournit, une fois la tâche achevée, des informations relatives au processus : nombre total d'éléments analysés, durée de l'analyse, chemin du journal et nombre d'infections détectées, le cas échéant.

Cette commande est suivie d'un identifiant prédéfini pour chaque type de tâche d'analyse :

- **Analyse rapide** (ID : da29f7c8-23b1-4974-8d11-209959ac694b - cette tâche est configurée pour une sécurité de base et une faible utilisation des ressources. Les principales cibles de l'analyse sont les processus en cours d'exécution et certains emplacements vulnérables. Il n'est possible d'exécuter qu'une seule tâche de ce type à la fois.

Comment effectuer une analyse rapide :

```
sudo ./productConfigurationTool -authToken  
[password] -asksForAScanToRun  
da29f7c8-23b1-4974-8d11-209959ac694b
```

- **Analyse complète** (ID : dcf483c4-26d0-4e6f-ba28-6a53a00adae1) - cette tâche est configurée pour une protection maximale contre tout type de malware. Il n'est possible d'effectuer qu'une tâche de ce type à la fois.

Comment effectuer une analyse complète :

```
sudo ./productConfigurationTool -authToken  
[password] -asksForAScanToRun  
dcf483c4-26d0-4e6f-ba28-6a53a00adae1
```

Exemple de résultat en cas de succès après l'exécution de la commande asksForAScanToRun :

```
{  
  "error" : 0,  
  "stdout" : {  
    "scanDuration" : 13,  
    "logfilepath" : "\\Library\\Application Support\  
      /Antivirus for Mac\\Logs\  
      /da29f7c8-23b1-4974-8d11-209959ac694b.xml",  
    "totalScanned" : 6158,  
    "infection" : "NO"  
  }  
}
```

Exemple de résultat en cas d'échec :




```
"error" : 95
```

### Note

- Vous ne pouvez pas lancer une analyse personnalisée en utilisant **productConfigurationTool**.
- Certaines tâches d'analyse nécessitent beaucoup de temps. Par exemple, une analyse complète peut durer plus de 20 minutes.

## 5.2. Le paramètre authToken

Ce paramètre vous aide à prévenir l'utilisation non autorisée de **productConfigurationTool**. Il doit être inclus chaque fois que vous exécutez une commande.

 **Note** En tant que mesure temporaire, le paramètre `authToken` nécessite un mot de passe que vous pouvez obtenir en contactant l'Assistance commerciale Bitdefender.

## 5.3. Codes d'erreur

L'interface **productConfigurationTool** peut renvoyer l'un des codes d'erreur suivants :

Erreur	Description
100	Les paramètres de <b>productConfigurationTool</b> sont <b>incorrects</b> .
99	L'outil n'est pas exécuté avec les privilèges administrateur.
98	"/Library/Bitdefender/AVP/enterprise.bundle/epsdk.dylib" n'a pas été trouvé. Mettez à jour le produit.
97	Échec du chargement des fonctions de type <code>f_EPSDK_GetInstance</code> et <code>f_EPSDK_ReleaseInstance</code> à partir de la bibliothèque. Mettez à jour le produit.
96	Il manque certains champs attendus à la réponse <code>.json</code> ou son format est différent du format attendu. Mettez à jour le produit.
95	Une certaine requête requiert des événements afin d'obtenir toutes les données pertinentes, mais tous les événements ne sont pas capturés. Mettez

Erreur	Description
	à jour le produit. Si cette erreur persiste, contactez l'Assistance commerciale Bitdefender.
94	"/Library/Bitdefender/AVP/EndpointSecurityforMac.app/Contents/Info.plist" n'a pas été trouvé ou "CFBundleVersion" n'a pas été trouvé dans le fichier .plist. Mettez à jour le produit.
93	<b>productConfigurationTool</b> n'est pas pris en charge sur cette version d'Endpoint Security for Mac. Mettez à jour le produit.
92	Le mot de passe <code>authToken</code> fourni ne correspond pas à la valeur attendue.
0	La commande a été exécutée avec succès.

## 6. QUESTIONS LES PLUS FRÉQUENTES

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

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

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

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

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

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

- fichiers appartenant à un autre utilisateur

**Solution :** Utilisez l'option **Faire apparaître dans le Finder** pour trouver le fichier et contactez son propriétaire afin de savoir si le fichier peut être supprimé sans danger. Si c'est le cas, supprimez-le manuellement. Pensez à vider la Corbeille.



### Note

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



**Puis-je mettre à jour Endpoint Security for Mac via un serveur proxy ?**

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

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

**Comment retirer les extensions TrafficLight de mon navigateur web ?**

- Pour retirer les extensions TrafficLight de Mozilla Firefox, procédez comme suit :
  1. Ouvrez votre navigateur Mozilla Firefox.
  2. Allez dans **Outils** et sélectionnez **Add-ons**.
  3. Sélectionnez **Extensions** dans la colonne de gauche.

4. Sélectionnez l'extension et cliquez sur **Supprimer**.
  5. Redémarrez le navigateur pour que le processus de désinstallation se termine.
- Pour retirer les extensions TrafficLight de Google Chrome, procédez comme suit :
    1. Ouvrez votre navigateur Google Chrome.
    2. Cliquez sur  sur la barre d'outils du navigateur.
    3. Allez dans **Outils** et sélectionnez **Extensions**.
    4. Sélectionnez l'extension et cliquez sur **Supprimer**.
    5. Cliquez sur **Désinstaller** pour confirmer le processus de désinstallation.
  - Pour désinstaller Bitdefender TrafficLight à partir de Safari, procédez comme suit :
    1. Ouvrez votre navigateur Safari.
    2. Cliquez sur  sur la barre d'outils du navigateur et cliquez sur **Préférences**.
    3. Sélectionnez l'onglet **Extensions** et recherchez l'extension **Bitdefender TrafficLight sur Safari** dans la liste.
    4. Sélectionnez l'extension et cliquez sur **Désinstaller**.
    5. Cliquez sur **Désinstaller** pour confirmer le processus de désinstallation.



## 7. OBTENIR DE L'AIDE

Pour tout problème ou toute question relative à Endpoint Security for Mac, veuillez contacter votre administrateur réseau.

Ouvrez la fenêtre **À propos d'Endpoint Security for Mac** pour des informations sur le produit et des coordonnées :

1. Ouvrez Endpoint Security for Mac.
2. Cliquez sur **Endpoint Security for Mac** dans la barre de menus.
3. Choisissez **À propos de Endpoint Security for Mac**.

## Types de Logiciels Malveillants

### Adware

Les adwares sont souvent associés à des applications gratuites ce qui implique leur acceptation par l'utilisateur. Ces adwares étant généralement installés après que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant les « pop up » publicitaires peuvent devenir contrariant et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

### Keylogger

Application qui enregistre tout ce qui est tapé.

Les keyloggers 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 des cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion et des numéros de sécurité sociale).

### 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 Rootkits ne sont pas malveillants par nature. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils

peuvent analyser le trafic, créer des portes dérobées sur le système, corrompre des fichiers et des logs et éviter leur détection.

## Spywares

Tout type de logiciel qui récupère secrètement les informations des utilisateurs au travers de leur connexion Internet sans les avertir, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels shareware ou freeware qui peuvent être téléchargés sur Internet. Cependant, la majorité des applications shareware ou freeware ne comportent pas de spyware. Après son installation, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement des 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 de crédit.

Leur point commun avec les Chevaux de Troie est que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une de manière les plus classique pour être victime de spywares 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 spywares volent aussi les ressources de l'ordinateur de l'utilisateur en utilisant de la bande passante lors de l'envoi d'information au travers de sa connexion Internet. A cause 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.

## Trojan (Cheval de Troie)

Un programme destructif qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se répliquent pas, mais peuvent être tout aussi destructifs. Un des types les plus répandu de Trojans est un logiciel prétendant désinfecter votre PC (mais au lieu de faire cela il l'infecte).

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.

## 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.

## **Virus**

Programme ou morceau de code qui est chargé dans votre ordinateur sans que vous le sachiez et fonctionne contre votre gré. La plupart des virus peuvent se répliquer. Tous les virus sont créés par des personnes. Un virus simple capable de se copier continuellement est relativement facile à créer. Même un virus simple de ce type est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau et d'échapper aux systèmes de sécurité.

## **Virus polymorphique**

Un virus qui change de forme avec chaque fichier qu'il infecte. Comme ils n'ont pas une forme unique bien définie, ces virus sont plus difficiles à identifier.