Dr.WEB

Server Security Suite (macOS)

Manuel Utilisateur

Dr.Web Server Security Suite (macOS)
Version 12.6
Manuel Utilisateur
1/31/2025

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125124 Moscou, Russie

Site web : https://www.drweb.com/

Téléphone : +7 (495) 789-45-87

Vous pouvez trouver les informations sur les bureaux régionaux sur le site officiel de la société.

Doctor Web

Doctor Web — éditeur russe de solutions de sécurité informatique.

Doctor Web propose des solutions antivirus et antispam efficaces pour les institutions publiques, les entreprises, ainsi que pour les particuliers.

Les solutions antivirus Dr.Web sont connues depuis 1992 pour leur excellence en matière de détection des programmes malveillants et leur conformité aux standards internationaux de sécurité.

Les certificats et les prix attribués, ainsi que l'utilisation de nos produits dans le monde entier sont les meilleurs témoins de la confiance qui leur est accordée.

Nous remercions tous nos clients pour leur soutien !

Contenu

1. Dr.Web Server Security Suite (macOS)

1.1. Conventions

Les styles utilisés dans ce manuel :

Style	Commentaire
⚠	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
Réseau antivirus	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<IP-address>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.
`/Volumes/Macintosh HD/`	Noms de fichiers/dossiers ou fragments de programme.
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

1.2. À propos de l'application

Dr.Web protège votre Mac de façon fiable contre les menaces de tout type : virus, rootkits, Trojans, spywares, adwares, hacktools et d'autres objets malveillants en utilisant les plus récentes technologies de détection et de neutralisation de virus.

Les composants de Dr.Web sont mis à jour régulièrement, les bases virales et les bases des catégories de ressources Web sont complétées par de nouvelles signatures. Les mises à jour assurent un haut niveau de sécurité. Pour la protection contre des virus inconnus un analyseur heuristique est utilisé.

Fonctionnalités principales

- analyse permanent de tous les fichiers sur Mac ;
- analyse du système à la demande de l'utilisateur ;
- analyse des données transmises par le protocole HTTP non sécurisé ;
- contrôle des connexions des applications au réseau et blocage de connexions suspectes ;
- protection de la webcam et du microphone contre un accès non autorisé (uniquement sur les appareils tournant sous macOS 10.13 ou une version antérieure).

Informations sur l'application

Pour ouvrir la fenêtre contenant les informations sur l'application, cliquez sur l'icône en haut à gauche de la fenêtre d'accueil de l'application.

Les informations sur l'application sont reparties en cinq onglets :

- **A propos de Dr.Web** : version de l'application, version du moteur antivirus, date de la dernière mise jour, identifiant de l'appareil, option de génération du rapport pour le support technique si ce paramètre est activé dans la section Paramètres généraux.
- **Aide** : aide Dr.Web.
- **Actualités** : actualités publiées sur le site de la société Doctor Web.
- **Offres** : offres de la société Doctor Web.
- **A propos de virus** : actualités sur les virus détectés par les analystes de Doctor Web.

1.3. Pré-requis système

Paramètre	Configuration requise
Appareil	Mac tournant sous le système d'exploitation macOS
Espace disque	2 Go
Système d'exploitation	• OS X 10.11 El Capitan ; • macOS 10.12 Sierra ; • macOS 10.13 High Sierra ; • macOS 10.14 Mojave ; • macOS 10.15 Catalina ; • macOS 11 Big Sur ; • macOS 12 Monterey ; • macOS 13 Ventura ; • macOS 14 Sonoma ; • macOS 15 Sequoia.

Pour un fonctionnement correct de Dr.Web, les ports suivants doivent être ouverts :

Usage	Direction	Numéros de ports
Pour l'activation et le renouvellement de la licence	sortant	443
Pour la mise à jour	sortant	80
Pour la connexion au service cloud Dr.Web Cloud	sortant	UDP : • 2075

Usage	Direction	Numéros de ports
		TCP : • 3010, • 3020, • 3030, • 3040

Comment connaitre la version du système d'exploitation de Mac

1. Ouvrez le menu Apple .
2. Cliquez sur **À propos de ce Mac**.
3. (Uniquement pour les appareils tournant sous macOS 12 ou une version antérieure) Sélectionnez l'onglet **Aperçu**.

Comment savoir combien d'espace libre il reste sur Mac

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **À propos de ce Mac**.
3. Cliquez sur **Stockage**. Vous verrez l'espace disponible sur Mac.

Si vous voulez voir les recommandation d'optimisation du stockage, cliquez sur **Gérer**.

Sous macOS 13.0 et les versions antérieures

1. Sélectionnez le menu Apple > **Réglages système**.
2. Cliquez sur **<%GENERAL_MAC%>** dans la barre latérale à gauche.
3. À droite, sélectionnez **Stockage**. Vous verrez l'espace disponible sur Mac.

De plus, dans la section **<%RECOMMENDATIONS_MAC%>**, vous trouverez les conseils pour optimiser le stockage.

2. Installation et désinstallation

Installation de Dr.Web

Pour installer Dr.Web

1. Téléchargez le fichier d'installation du site https://download.drweb.com/mac/.
2. Lancez ce fichier.
3. Cliquez sur **Installer Dr.Web**.
4. Cliquez sur **Suivant**. L'installation de l'application commence.
5. Entrez le mot de passe du compte et cliquez sur **Installer un logiciel complémentaire**.
6. Une fois l'avertissement **L'extension système est bloquée** affiché, autorisez le téléchargement des extensions système.
7. Dr.Web se copie dans le dossier **Applications** et se lance.
8. Accordez à Dr.Web le droit de l'accès complet au disque.

Pour autoriser le téléchargement d'extensions système

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Préférences système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur **Autoriser** à côté du message de blocage du logiciel système de Doctor Web Ltd.

Sous macOS 11.0 et 12.0, cliquez sur **Avancé** et cochez les composants de Dr.Web.

Sous macOS 13.0 et 14.0

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Dans cette section trouvez la ligne **Certains logiciels système requièrent votre attention**

avant de pouvoir être utilisés et cliquez sur **Détails** ci-dessous.

5. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
6. Basculez le commutateur contre les composants de Dr.Web sur la position Activé et cliquez sur **OK**.

Sous macOS 15.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Général** et sélectionnez **Ouverture et extensions**.
4. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions de sécurité de point de terminaison** et cliquez sur l'icône ⓘ qui se trouve à droite.
5. Basculez le commutateur **Dr.Web Spider** sur la position Activé et cliquez sur **Terminé**.
6. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions du réseau** et cliquez sur l'icône ⓘ qui se trouve à droite.
7. Basculez le commutateur **Dr.Web Firewall** sur la position Activé et cliquez sur **Terminé**.

Pour autoriser l'accès complet au disque

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Préférences système**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Accédez à la section **Sécurité et confidentialité**.
5. Accédez à la section **Confidentialité**.
6. Cliquez sur **Accès complet au disque**.
7. Ajoutez les modules de Dr.Web dans la liste d'applications autorisées.
8. Cliquez sur **Redémarrer**.

Sous macOS 13.0 et les versions antérieures

1. Dans la fenêtre principale de Dr.Web, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Cliquez sur **Autoriser**.
4. Cliquez sur **Ouvrir les Préférences système** dans le Gestionnaire d'accès au disque.
5. Dans la fenêtre d'instruction du Gestionnaire, cliquez sur la flèche jusqu'à ce que vous voy-

iez l'icône de Dr.Web.

6. Faites-glisser l'icône de Dr.Web du Gestionnaire d'accès au disque vers la section de préférences système indiquée dans le Gestionnaire.
7. Pour confirmer, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
8. Cliquez sur **Redémarrer** pour enregistrer les modifications.

Si le bouton **Autoriser** n'est pas actif, l'accès au disque est déjà autorisé.

Après la fin de l'installation, l'icône  s'affichera en haut du panneau macOS. Elle ouvre la fenêtre principale de Dr.Web.

Au premier lancement Dr.Web mettra à jour les bases virales jusqu'à l'état actuel. Ensuite Dr.Web met à jour les bases virales toutes les 30 minutes. Vous pouvez modifier la fréquence de mises à jour.

Erreurs d'installation

Le système d'exploitation n'est pas supporté

Dr.Web peut être installé uniquement sur Mac tournant sous une version supportée du système d'exploitation macOS. Veuillez mettre à niveau votre système d'exploitation.

Comment connaitre la version du système d'exploitation de Mac

1. Ouvrez le menu Apple .
2. Cliquez sur **À propos de ce Mac**.
3. (Uniquement pour les appareils tournant sous macOS 12 ou une version antérieure) Sélectionnez l'onglet **Aperçu**.

Pas assez de mémoire sur le disque

Pour installer Dr.Web, il faut avoir environ 2 Go d'espace libre sur le disque.

Comment savoir combien d'espace libre il reste sur Mac

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **À propos de ce Mac**.
3. Cliquez sur **Stockage**. Vous verrez l'espace disponible sur Mac.

Si vous voulez voir les recommandation d'optimisation du stockage, cliquez sur **Gérer**.

Sous macOS 13.0 et les versions antérieures

1. Sélectionnez le menu Apple > **Réglages système**.
2. Cliquez sur **<%GENERAL_MAC%>** dans la barre latérale à gauche.
3. À droite, sélectionnez **Stockage**. Vous verrez l'espace disponible sur Mac.

De plus, dans la section **<%RECOMMENDATIONS_MAC%>**, vous trouverez les conseils pour optimiser le stockage.

Un autre antivirus est installé

Dr.Web n'est pas compatible avec d'autres applications antivirus. Il est également impossible d'installer deux versions de Dr.Web sur un Mac.

L'installation de deux antivirus sur un ordinateur peut provoquer des erreurs et la perte de données importantes. C'est pourquoi avant d'installer Dr.Web, il est nécessaire de supprimer sa version précédente ou un autre antivirus installé sur votre ordinateur.

Vous pouvez trouver les informations sur la suppression d'un antivirus dans les documents de référence ou sur le site officiel de l'application en question.

Erreur n°

Contactez le support technique de la société Doctor Web. Veuillez joindre à votre requête le journal d'installation qui se trouve dans le dossier `\Library\DrWeb`.

Liste d'erreurs

Désinstallation de Dr.Web

1. Dans **Finder**, trouvez l'application **Désinstaller Dr.Web** et lancez-la.

2. Entrez le nom et le mot de passe de l'utilisateur.
3. Dr.Web sera supprimé du dossier **Applications**.

> Après la suppression de Dr.Web sur Mac, le fichier clé, le fichier de configuration et le fichier contenant les paramètres de l'application restent.
>
> N'utilisez pas de tierces applications pour supprimer Dr.Web. Cela peut entrainer une suppression incomplète de l'application.

Si l'application n'est pas complètement supprimée, vous pouvez la désinstaller manuellement.

Pour supprimer manuellement Dr.Web

Entrez les commandes suivantes à tour de rôle dans **Terminal** :

```
sudo /usr/bin/killall 'Dr.Web for macOS'

sudo /bin/launchctl remove com.drweb.pro.configd

sudo /bin/launchctl remove com.drweb.LoginLauncher

sudo rm -f /Library/PrivilegedHelperTools/com.drweb.agent

sudo rm -f /Library/LaunchDaemons/com.drweb.agent.plist

sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove '/Library/Application Support/DrWeb/bin/drweb-gated'

sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove '/Library/Application Support/DrWeb/bin/drweb-firewall'

sudo /sbin/kextunload -m com.drweb.kext.DrWebNetMonitor

sudo /sbin/kextunload -m com.drweb.kext.DrWebMonitor

sudo /bin/launchctl remove com.drweb.agent

sudo "/Applications/Dr.Web/Dr.Web for macOS.app/Contents/Resources/Extensions/Dr.Web Firewall.app/Contents/MacOS/Dr.Web Firewall" --deactivate

sudo "/Applications/Dr.Web/Dr.Web for macOS.app/Contents/Resources/Extensions/Dr.Web Spider.app/Contents/MacOS/Dr.Web Spider" --deactivate

sudo rm -Rf /usr/local/bin/drweb-ctl

sudo rm -Rf "/Library/LaunchDaemons/com.drweb.pro.configd.plist"

sudo rm -Rf "/Library/LaunchAgents/com.drweb.LoginLauncher.plist"

sudo rm -Rf "/Library/Application Support/DrWeb/mail"
```

```
sudo rm -Rf "/Library/Application Support/DrWeb/html"

sudo rm -Rf "/Library/Application Support/DrWeb/dws"

sudo rm -Rf "/Library/Application Support/DrWeb/var/drl"

sudo rm -Rf "/Library/Application Support/DrWeb/bases"

sudo rm -Rf "/Library/Application Support/DrWeb/lib"

sudo rm -Rf "/Library/Application Support/DrWeb/bin"

sudo rm -Rf "/Library/Application Support/DrWeb/version"

sudo rm -Rf "/Library/Application Support/DrWeb/var"

sudo rm -Rf "/Library/Application Support/DrWeb/www"

sudo rm -Rf "/Library/Application Support/DrWeb/update/Library/Application
Support/DrWeb/cache/esagent"

sudo rm -Rf "/Library/Application Support/DrWeb/cache/cloud"

sudo rm -Rf "/Library/Application Support/DrWeb/cache"

sudo rm -Rf "/Library/Application Support/DrWeb/install.plist"

sudo rm -Rf "/Applications/Dr.Web/Dr.Web for macOS.app"

sudo rm -Rf "/Applications/Dr.Web/Uninstall Dr.Web.app"

sudo rm -Rf /Applications/Dr.Web
```

3. Accès complet au disque

Pour que les composants de Dr.Web puissent effectuer leurs fonctions et protéger votre Mac, il faut accorder à l'application *l'accès complet au disque*.

Vous pouvez le faire

- lors du passage des notifications vous informant de la nécessité de l'autorisation de l'accès,
- dans les paramètres de Dr.Web, la section **Général**.

> Lors de la mise à niveau du système d'exploitation vers macOS 13 Ventura, il vous faudra autoriser l'accès au disque encore une fois.

Si l'accès au disque n'est pas autorisé, une fenêtre pop-up s'affichera après chaque redémarrage de Mac vous signalant que l'application demande l'accès.

Configuration de l'accès complet au disque

Dans les paramètres

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Cliquez sur **Autoriser**.
4. Cliquez sur **Ouvrir les Préférences système** dans le Gestionnaire d'accès au disque.
5. Dans la fenêtre d'instruction du Gestionnaire, cliquez sur la flèche jusqu'à ce que vous voyiez l'icône de Dr.Web.
6. Faites-glisser l'icône de Dr.Web du Gestionnaire d'accès au disque vers la section de préférences système indiquée dans le Gestionnaire.
7. Pour confirmer, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
8. Cliquez sur **Redémarrer** pour enregistrer les modifications.

> Si le bouton **Autoriser** n'est pas actif, l'accès au disque est déjà autorisé.

Lors du passage de la notification

1. Cliquez sur **Autoriser**.
2. Cliquez sur **Ouvrir les Préférences système** dans le Gestionnaire d'accès au disque.

3. Dans la fenêtre d'instruction du Gestionnaire, cliquez sur la flèche jusqu'à ce que vous voyiez l'icône de Dr.Web.
4. Faites-glisser l'icône de Dr.Web du Gestionnaire d'accès au disque vers la section de préférences système indiquée dans le Gestionnaire.
5. Pour confirmer, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
6. Cliquez sur **Redémarrer** pour enregistrer les modifications.

Pour ouvrir l'accès complet au disque via les réglages système de votre Mac sans aide du Gestionnaire d'accès au disque, il fous faudra déplacer manuellement tous les composants de Dr.Web dans la fenêtre de réglages. Pour éviter les erreurs, nous vous recommandons d'utiliser le Gestionnaire.

4. Gestion des licences

Le fonctionnement de Dr.Web est assuré par une licence que l'on peut acheter sur le site de la société Doctor Web ou chez les partenaires. La licence permet d'utiliser toutes les fonctionnalités de l'application pendant toute la durée de validité. La licence régit les droits d'utilisateur définis conformément au Contrat de licence que l'utilisateur accepte lors de l'installation de l'application.

Chaque licence possède un numéro de série unique et un fichier spécifique contenant les paramètres de la licence est sauvegardé sur l'ordinateur de l'utilisateur. Ce fichier s'appelle le fichier clé de licence.

Si avant d'acheter une licence, vous voulez tester Dr.Web, vous pouvez activer la version d'essai. Toutes les fonctionnalités et les composants de protection sont disponibles dans la version d'essai.

4.1. Version d'essai

Si avant d'acheter une licence, vous voulez tester Dr.Web, vous pouvez activer la version d'essai. Vous bénéficierez de tous les composants essentiels mais pendant une période limitée.

Vous pouvez activer une version d'essai sur le même ordinateur une seule fois par an.

Vous pouvez activer la version d'essai :

- D'un mois. Dans ce cas, aucun numéro de série, ni données d'enregistrement ne sont requis. La licence sera activée automatiquement.

Pour activer la version d'essai

1. Dans la fenêtre principale de Dr.Web  , sélectionnez l'élément **Licence**.
2. Dans la section**Activation de licence**, cloquez sur le lien **Obtenir une version d'essai de 30 jours**.

4.2. Achat d'une licence

Si vous n'avez pas de licence valide de Dr.Web, vous pouvez acheter une nouvelle licence sur la page de la boutique en ligne de Doctor Web.

Pour acheter une nouvelle licence

1. Dans la fenêtre principale de Dr.Web, sélectionnez l'élément **Licence**.
2. Cliquez sur le bouton **Acheter**. La page du site de la société Doctor Web va s'ouvrir. Sur cette page, vous pouvez continuer l'achat.

Une fois l'achat terminé, vous recevrez un message contenant le numéro de série et le fichier clé (en pièce jointe) à l'adresse e-mail indiquée lors de l'enregistrement.

4.3. Activation de la licence

Pour utiliser toutes les fonctionnalités et les composants de l'application, il faut activer la licence. Nous recommandons d'activer la licence juste après l'installation de l'application Cela est nécessaire pour la mise à jour des bases virales et le fonctionnement des composants de l'application, par exemple pour une protection permanente du système de fichiers, la protection contre les menaces réseau et l'analyse du trafic Web.

La fenêtre d'activation s'affiche automatiquement, lorsque vous lancez Dr.Web pour la première fois. Vous pouvez également lancer l'activation plus tard dans la section **Licence** de la fenêtre principale de l'application. L'activation de la licence se fait avec un fichier clé, un numéro de série ou un fichier de configuration (.cfg).

Comment activer la licence avec le numéro de série

1. Dans la fenêtre principale de Dr.Web, sélectionnez l'élément **Licence**.
2. Cliquez sur le bouton **Activer**.
3. Dans la fenêtre **Activation de licence**, entrez le numéro de série.
4. Cliquez sur le bouton **Activer**.
5. Dans le formulaire d'enregistrement, entrez le nom, la région et l'adresse e-mail. Ces informations sont nécessaires pour la récupération de la licence en cas de nécessite. Cliquez sur le bouton **Inscription**.

Comment activer la licence avec le fichier clé

1. Dans la fenêtre principale de Dr.Web, sélectionnez l'élément **Licence**.
2. Cliquez sur le bouton **Activer**.
3. Dans la fenêtre **Activation de licence**, ouvrez l'onglet **Fichiers d'activation**.
4. Faites glisser le fichier clé au format `.key` dans la zone pointillée ou cliquez pour sélectionner le fichier sur Mac.
5. Dans le formulaire d'enregistrement, entrez le nom, la région et l'adresse e-mail. Ces informations sont nécessaires pour la récupération de la licence en cas de nécessite. Cliquez sur le bouton **Inscription**.

Questions fréquentes

Comment puis-je transférer la licence sur un autre ordinateur ?

Vous pouvez transférer votre licence commerciale sur un autre ordinateur à l'aide du fichier clé ou le numéro de série.

Pour transférer la licence sur un autre ordinateur

- avec le numéro de série :
  1. Supprimez Dr.Web de l'ordinateur duquel vous voulez transférer la licence ou activez une autre licence sur cet ordinateur.
  2. Activez la licence actuelle sur l'ordinateur sur lequel vous voulez transférer la licence avec le numéro de série. Vous pouvez activer la licence lors de l'installation ou lors du fonctionnement de l'application.
- avec le fichier clé :
  1. Copiez le fichier clé de l'ordinateur duquel vous voulez transférer la licence. Par défaut, le fichier clé se trouve dans le dossier d'installation de Dr.Web et il a l'extension `.key`.
  2. Supprimez Dr.Web de l'ordinateur duquel vous voulez transférer la licence ou activez une autre licence sur cet ordinateur.
  3. Activez la licence actuelle sur l'ordinateur sur lequel vous voulez transférer la licence avec le fichier clé. Vous pouvez activer la licence lors de l'installation ou lors du fonctionnement de l'application.

Il est impossible de transférer sur un autre ordinateur la licence que vous avez reçue pour l'activation de la version d'essai de l'application.

J'ai oublié l'e-mail d'enregistrement. Comment puis-je le récupérer ?

Si vous avez oublié l'adresse e-mail que vous aviez indiquée lors de l'enregistrement, contactez le support technique de la société Doctor Web.

Si vous envoyez une demande depuis une adresse différente de celle que vous avez indiquée lors de l'enregistrement, le spécialiste du support technique peut vous demander de fournir une photo ou un scan du certificat de licence, le ticket de paiement de la licence, la lettre de la boutique en ligne et d'autres justificatifs.

Comment puis-je changer l'e-mail d'enregistrement ?

Si vous voulez changer l'adresse e-mail que vous avez indiquée lors de l'enregistrement, utilisez le service spécial sur le site de la société Doctor Web.

4.4. Renouvellement de la licence

Vous pouvez renouveler la licence actuelle dans la section **Activation de licence**.

Comment renouveler la licence qui n'a pas encore expiré

1. Dans la fenêtre principale de Dr.Web, sélectionnez l'élément **Licence**.
2. Cliquez sur le bouton **Acheter**. La page du site de la société Doctor Web va s'ouvrir. Sur cette page, vous pouvez continuer l'achat.

Comment renouveler la licence qui a déjà expiré

1. Dans la fenêtre principale de Dr.Web, sélectionnez l'élément **Licence**.
2. Cliquez sur le bouton **Acheter**. La page du site de la société Doctor Web va s'ouvrir. Sur cette page, vous pouvez continuer l'achat.

Dr.Web prend en charge la mise à jour à la volée. Vous n'avez pas à réinstaller l'application ou l'arrêter. Pour mettre à jour la licence de Dr.Web, activez la nouvelle licence.

Pour enregistrer la licence

1. Dans la fenêtre principale de Dr.Web, sélectionnez l'élément **Licence**.
2. Cliquez sur le bouton **Activer**.
3. Dans la fenêtre **Activation de licence** :
   - Entrez le numéro de série et cliquez sur le bouton **Activer**.
   - Si vous avez un fichier clé, ouvrez l'onglet **Fichiers d'activation**. Faites glisser le fichier dans la zone pointillée ou cliquez pour sélectionner un fichier sur Mac.

Les instructions détaillées sur l'activation de la licence sont disponibles dans la rubrique Activation de la licence.

Si la licence que vous voulez renouveler a expiré, Dr.Web commencera à utiliser la nouvelle licence.

Si la licence que vous voulez renouveler n'a pas encore expiré, les jours restants seront automatiquement ajoutés à la nouvelle licence. Dans ce cas, l'ancienne licence sera bloquée et vous recevrez un avertissement correspondant sur l'e-mail que vous avez indiqué lors de l'enregistrement.

4.5. Restauration de la licence

Si le fichier clé est perdu ou endommagé, le fonctionnement de tous les composants de Dr.Web est bloqué et la sécurité de votre Mac peut être menacée. Pour activer la licence encore une fois, restaurez le fichier clé à l'aide du numéro de série.

Comment restaurer le fichier clé

1. Dans la fenêtre principale de Dr.Web, sélectionnez l'élément **Licence**.
2. Cliquez sur le bouton **Activer**.
3. Dans la fenêtre **Activation de licence**, entrez le numéro de série et cliquez sur le bouton **Activer**.

En cas de nouvelle activation, le même fichier clé que vous avez déjà reçu est délivré.

Comment récupérer le numéro de série

Si vous n'avez pas trouvé le numéro de série, vous pouvez le restaurer des façons suivantes :

- Contactez le vendeur de la licence (s'il ne s'agit pas d'une version en boîte).
- Utilisez le formulaire de restauration sur le site de la société Doctor Web.
- Contactez le support technique de la société Doctor Web. Veuillez joindre à votre demande un justificatif de l'achat de la licence conformément à ces règles.

Vous pouvez activer la licence encore une fois si elle n'a pas expiré.

Vous pouvez obtenir le fichier clé de licence via l'application un nombre de fois limité. Si ce nombre est dépassé, vous pouvez obtenir le fichier clé en confirmant l'enregistrement de votre numéro de série sur le site https://products.drweb.com/register/. Le fichier clé sera envoyé à l'adresse e-mail que vous avez indiquée au premier enregistrement.

4.6. Numéro de série

Chaque licence possède un *numéro de série* unique. Avec ce numéro de série vous pouvez activer la licence de Dr.Web.

Comment puis-je connaitre mon numéro de série

Si le numéro de série n'est pas enregistré

- Si vous avez acheté la licence dans une boutique en ligne, vous pouvez trouver le numéro de série dans le message de la boutique en ligne portant sur l'achat de la licence.

  - Si vous avez acheté la licence dans la boutique en ligne Dr.Web, vous pouvez trouver le numéro de série dans l'Espace personnel sur le site Allsoft.ru, dans les informations sur la commande.
  - Si vous avez acheté la licence dans la boutique en ligne de Doctor Web, depuis votre compte sur le site et que vous avez inscrit votre licence dans le programme de fidélité, vous pouvez trouver le numéro de série dans le service Mes achats.
- Si vous avez acheté une version en boîte, vous pouvez trouver le numéro de série dans le certificat de Licence mis dans la boîte.
- Si vous avez acheté la licence dans une chaîne de magasins, vous pouvez trouver le numéro de série dans le ticket de paiement.

Si le numéro de série est enregistré

- Si Dr.Web est installé sur Mac, téléchargez ce fichier et ouvrez-le. Double-cliquez sur le fichier `YSN.cmd`. Le fichier texte `YourSerialNumber.txt` sera créé et automatiquement ouvert dans un éditeur de texte. Tous les numéros de série seront précédés par le préfixe « SN= ».
- Si Dr.Web n'est pas installé, récupérez le numéro de série à l'aide du formulaire sur le site de la société Doctor Web.

Si vous utilisez l'abonnement de Dr.Web

Dans ce cas, vous n'avez pas besoin de numéro de série ni de fichier clé.

- Si vous avez acheté l'abonnement sur le site de la société Doctor Web, vous pouvez trouvez l'identificateur (ID) de l'abonnement dans la section Mes abonnements.
- Si vous avez acheté l'abonnement chez un fournisseur tiers, vous pouvez trouver l'ID de l'abonnement dans votre compte sur le site de votre fournisseur IT.

Comment récupérer le numéro de série

Si vous n'avez pas trouvé le numéro de série, vous pouvez le restaurer des façons suivantes :

- Contactez le vendeur de la licence (s'il ne s'agit pas d'une version en boîte).
- Utilisez le formulaire de restauration sur le site de la société Doctor Web.
- Contactez le support technique de la société Doctor Web. Veuillez joindre à votre demande un justificatif de l'achat de la licence conformément à ces règles.

4.7. Fichier clé

Le fichier clé détermine le type de la licence et le droit de l'utilisateur d'utiliser Dr.Web.

Le fichier clé de licence possède l'extension `.key`. Vous pouvez le recevoir pendant l'activation de la licence.

Le fichier clé contient les informations sur :

- la liste des composants antivirus que l'utilisateur a le droit d'utiliser ;
- la durée d'utilisation de Dr.Web ;
- la disponibilité du support technique ;
- d'autres restrictions (notamment, le nombre d'ordinateurs sur lesquels vous êtes autorisé à utiliser Dr.Web).

Le fichier clé doit être placé dans le dossier d'installation de Dr.Web. L'application vérifie régulièrement la présence et la validité du fichier clé. Ne modifiez pas le fichier clé et ne l'ouvrez pas dans des éditeurs de texte pour ne pas compromettre son intégrité.

Si aucun fichier clé valide n'est trouvé, les composants de Dr.Web sont bloqués.

Un fichier clé de Dr.Web est *valide* s'il satisfait aux critères suivants :

- la licence n'a pas expiré,
- l'intégrité du fichier clé n'a pas été violée.

Si l'une des conditions n'est pas respectée, le fichier clé devient *invalide* et Dr.Web arrête de neutraliser les logiciels malveillants.

Il est recommandé de conserver le fichier clé pendant toute la durée de validité de la licence ou de la version d'essai. Si vous installez Dr.Web sur plusieurs ordinateurs ou réinstallez le logiciel, vous pouvez avoir besoin du fichier clé de licence obtenu lors de la première activation.

Le fichier clé obtenu lors de l'activation de la version d'essai peut être utilisé seulement sur l'ordinateur sur lequel a eu lieu la procédure d'enregistrement.

5. Panneau de gestion

Dans l'onglet **Panneau de gestion** de la fenêtre principale de l'application, vous pouvez :

- configurer le fonctionnement des composants de protection,
- lancer l'analyse de Mac pour la présence de virus,
- spécifier les paramètres d'accès à la webcam et au microphone (uniquement sur les appareils tournant sous macOS 10.13 ou une version antérieure),
- mettre à jour manuellement les bases virales,
- obtenir les informations sur la licence actuelle,
- voir les informations sur les menaces détectées.

Composants de protection

- SpIDer Guard : moniteur du système de fichiers. Il analyse en temps réel tous les fichiers auxquels accèdent les utilisateurs et contrôle les applications et les processus lancés sur Mac.
- SpIDer Gate : moniteur Internet. Il analyse le trafic HTTP et contrôle l'accès aux ressources Internet.
- Pare-feu : pare-feu qui protège Mac d'un accès non autorisé et prévient la perte de données vitales via le réseau.

Analyser Mac

Scanner : c'est le principal composant de détection des virus, qui permet d'effectuer :

- l'analyse rapide, complète ou personnalisée du système à la demande de l'utilisateur ;
- la neutralisation des menaces détectées (désinfection, suppression, déplacement en quarantaine). Vous pouvez sélectionner l'action nécessaire manuellement ou configurer dans les paramètres les actions automatiques pour chaque type de menaces.

Protection de la confidentialité

- **Webcam** : contrôle de l'accès d'applications à la webcam.
- **Microphone** : contrôle de l'accès d'applications au microphone.

> Les paramètres de contrôle de l'accès à la webcam et au microphone ne sont pas disponibles dans la version macOS 10.14 ou une version supérieure.

Mise à jour

Sélectionnez l'élément **Aucune mise à jour n'est requise**/**Une mise à jour est requise** pour mettre à jour manuellement les bases virales. Les bases virales contiennent les informations sur tous les logiciels malveillants connus.

Licence

La section **Licence** contient les informations sur la licence actuelle :

- statut de la licence,
- numéro,
- nom du titulaire,
- date d'activation,
- date d'expiration,
- nombre de jours restants.

Vous pouvez activer la licence si vous avez le numéro de série, le fichier clé ou le fichier de configuration, ou bien vous pouvez acheter une nouvelle licence.

Menaces

- Menaces : liste des menaces détectées. Vous pouvez supprimer ces menaces, les mettre en quarantaine ou ignorer.
- Quarantaine : c'est un dossier spécial pour isoler des fichiers infectés et autres menaces de sécurité afin qu'ils ne puissent pas endommager le système.

6. Notifications

L'onglet **Notifications** de la fenêtre principale de l'application affiche les informations suivantes sur Dr.Web et son fonctionnement :

- le statut de la licence ;
- les informations sur la détection de menaces et leur neutralisation ;
- la statut des bases virales ;
- les informations sur les erreurs des composants de protection ;
- le statut de la connexion au serveur de protection centralisée ;
- les informations sur les tentatives de connexion au microphone et à la webcam ;
- les messages de l'administrateur du serveur de protection centralisée.

> Les informations portant sur les tentatives de connexion au microphone et à la webcam s'affichent uniquement sous macOS 10.13 ou une version antérieure.

Dr.Web utilise les notifications système de macOS pour afficher les messages sur la détection de menaces et leur neutralisation et les erreurs de fonctionnement des composants. Vous pouvez désactiver ou configurer les notifications système de Dr.Web.

Pour désactiver les notifications

1. Ouvrez le menu Apple > **Préférences système**.
2. Cliquez sur **Notifications et mode de concentration**.
3. À gauche, dans la liste des applications, sélectionnez Dr.Web pour macOS et désactivez les notifications avec l'interrupteur .

> Dans la version macOS 10.14 ou une version antérieure, cet interrupteur n'est pas présent. Pour désactiver les notifications, décochez toutes les cases.

Pour configurer les notifications système

1. Ouvrez le menu Apple > **Préférences système**.
2. Cliquez sur **Notifications et mode de concentration**.
3. À gauche, dans la liste des applications sélectionnez Dr.Web pour macOS. Configurez le style de notifications de l'application et les options correspondantes.

7. Mise à jour des bases virales

Dans la section **Module de mise à jour**, vous pouvez configurer la fréquence de mise à jour des bases virales. Les bases virales contiennent les informations sur tous les logiciels malveillants connus.

Chaque jour, de nouveaux types de menaces informatiques émergent avec des fonctions de camouflage plus avancées. La mise à jour de Dr.Web permet de détecter de nouveaux virus inconnus, de bloquer leur diffusion et, parfois, de désinfecter les fichiers infectés qui étaient incurables auparavant. Mettez à jour régulièrement les bases virales : elles deviennent obsolètes dans 24 heures après la dernière mise à jour réussie.

Pour que Dr.Web puisse mettre à jour les bases virales, une connexion Internet est requise.

Au premier lancement Dr.Web met à jour les bases virales jusqu'à l'état actuel. Ensuite, Dr.Web met à jour les bases virales toutes les 30 minutes. Vous pouvez modifier la fréquence de mise à jour.

Pour modifier la fréquence de mises à jour des bases virales

1. Dans la fenêtre principale, cliquez sur  .
2. Dans la fenêtre **Préférences** sélectionnez la section **Module de mise à jour**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur  et entrez le nom d'utilisateur et le mot de passe.
4. Dans la liste déroulante **Mettre à jour les bases virales**, sélectionnez la fréquence de mises à jour.

Dr.Web sera mis à jour automatiquement conformément à la fréquence sélectionnée du téléchargement des mises à jour.

Vous pouvez lancer manuellement le processus de mise à jour.

Pour mettre à jour manuellement les bases virales

- Dans la fenêtre principale, sélectionnez l'élément **Aucune mise à jour n'est requise/Une mise à jour est requise**.

Dr.Web analysera et mettra à jour les bases virales.

Configuration du serveur proxy

Si vous ne voulez pas installer les mises à jour directement sur votre Mac, vous pouvez configurer l'installation de mises à jour via le serveur proxy.

Pour configurer l'installation de mises à jour via le serveur proxy

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Module de mise à jour**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur et entrez le nom d'utilisateur et le mot de passe.
4. Cochez la case **Utiliser le serveur proxy**.
5. Cliquez sur **Configurer le proxy**.
6. Indiquez l'adresse et le port du serveur proxy.
7. S'il faut un mot de passe pour le serveur proxy, cochez la case **Protéger le serveur proxy par un mot de passe**.
8. Indiquez le nom d'utilisateur et le mot de passe.
9. Cliquez sur **Enregistrer**.

8. Protection permanente du système de fichiers

Le moniteur du système de fichiers SpIDer Guard analyse en temps réel tous les fichiers auxquels les utilisateurs accèdent et contrôle les applications et les processus lancés sur Mac.

Vous pouvez exclure certains dossiers et fichiers de l'analyse permanente.

SpIDer Guard se lance automatiquement après l'installation et l'activation de la licence de Dr.Web. Le moniteur fonctionne en permanence et se lance au démarrage de Mac.

Une fois une menace détectée, SpIDer Guard affiche sur l'écran un message et applique l'action spécifiée dans les paramètres. Vous pouvez modifier les actions qui s'appliquent automatiquement aux différents types de menaces ou appliquer les actions manuellement.

Activation et désactivation de SpIDer Guard

Seuls les utilisateurs ayant les privilèges d'administrateur peuvent désactiver SpIDer Guard.

Si la protection antivirus permanente est désactivée, il ne faut pas se connecter à Internet et ouvrir les fichiers depuis les supports amovibles non analysés par le Scanner.

Pour suspendre ou reprendre la protection permanente du système de fichiers

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, sélectionnez **Composants de protection**.
2. Activez ou désactivez le moniteur du système de fichiers SpIDer Guard avec l'interrupteur  .

SpIDer Guard ne marche pas / L'extension système est bloquée

Dans macOS 10.13 ou des versions supérieures le téléchargement des extensions système (modules de noyau) est bloqué. Dans ce cas, SpIDer Guard ne marche pas et le message sur le blocage de l'extension système s'affiche sur l'écran. Pour un fonctionnement correct de l'analyse du système de fichiers sur votre Mac, autorisez le téléchargement des logiciels de Doctor Web Ltd.

Pour autoriser le téléchargement d'extensions système

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .

2. Cliquez sur **Préférences système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur **Autoriser** à côté du message de blocage du logiciel système de Doctor Web Ltd.

> Sous macOS 11.0 et 12.0, cliquez sur **Avancé** et cochez les composants de Dr.Web.

Sous macOS 13.0 et 14.0

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Dans cette section trouvez la ligne **Certains logiciels système requièrent votre attention avant de pouvoir être utilisés** et cliquez sur **Détails** ci-dessous.
5. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
6. Basculez le commutateur contre les composants de Dr.Web sur la position Activé et cliquez sur **OK**.

Sous macOS 15.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Général** et sélectionnez **Ouverture et extensions**.
4. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions de sécurité de point de terminaison** et cliquez sur l'icône ⓘ qui se trouve à droite.
5. Basculez le commutateur **Dr.Web Spider** sur la position Activé et cliquez sur **Terminé**.
6. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions du réseau** et cliquez sur l'icône ⓘ qui se trouve à droite.
7. Basculez le commutateur **Dr.Web Firewall** sur la position Activé et cliquez sur **Terminé**.

8.1. Configuration du moniteur de fichiers SpIDer Guard

Dans la section de paramètres **SpIDer Guard**, vous pouvez configurer les actions que Dr.Web appliquera automatiquement aux menaces en fonction de leur type.

SpIDer Guard essaie de désinfecter les fichiers infectés : les objets infectés par un virus connu et potentiellement curable, tandis que les objets suspects et les différents types des programmes malveillants sont placés en Quarantaine.

Vous pouvez modifier séparément la réaction de SpIDer Guard vis-à-vis de chaque type d'objets malveillants. Les actions disponibles dépendent du type de menace :

Action	Description
Désinfecter, mettre les incurables en quarantaine	Restaure l'objet dans son état original avant infection. Si le virus est incurable, ou qu'une tentative de désinfection a échoué, l'objet sera mis en quarantaine. Cette action est possible uniquement pour les virus connus, sauf les trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
Désinfecter, supprimer les incurables	Restaure l'objet dans son état original avant infection. Si le virus est incurable, ou qu'une tentative de désinfection a échoué, l'objet sera supprimé. Cette action est possible uniquement pour les virus connus, sauf les trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
Supprimer	Supprime l'objet. Aucune action n'est appliquée aux secteurs d'amorçage.
Mettre en quarantaine	Isole l'objet dans le dossier spécial Quarantaine. Permet de prévenir une perte de données vitales. Aucune action n'est appliquée aux secteurs d'amorçage.
Ignorer	Ignore l'objet sans appliquer aucune action ni afficher d'alerte. Cette action est disponible uniquement pour les programmes malveillants dont adwares, dialers, canulars, hacktools et riskwares.

Il ne faut pas modifier les paramètres prédéfinis des actions automatiques si vous n'êtes pas sûr que c'est vraiment nécessaire.

Actions de SpIDer Guard qui s'appliquent aux objets malveillants

Type d'objet	Action				
	Désinfecter, mettre les incurables en quarantaine	Désinfecter, supprimer les incurables	Mettre en quarantaine	Supprimer	Ignorer
Infectés	+/*	+	+	+	
Suspects			+/*	+	+
Adwares			+/*	+	+
Dialers			+/*	+	+
Canulars			+	+	+/*
Riskwares			+	+	+/*
Hacktools			+	+	+/*
Archives infectées	+	+	+	+	+
Fichiers de messagerie infectés	+	+	+	+	+

Conventions

+	action possible
+/*	action spécifiée par défaut

Il n'est pas possible de spécifier une action par défaut à appliquer aux archives et aux fichiers de messagerie infectés car les actions s'y appliquent en fonction de la menace détectée. S'il y a plusieurs menaces, l'action de la menace plus importante sera appliquée.

Pour configurer les actions automatiques

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Guard**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. En cas de besoin, modifiez les actions automatiques pour les types de menaces listés.

Paramètres avancés

Vous pouvez configurer les paramètres avancés de SpIDer Guard et activer l'analyse d'archives et de fichiers de messagerie, ainsi que spécifier la durée maximale de l'analyse d'un seul objet.

> La modification de ces paramètres peut ralentir votre Mac et augmenter la durée totale de l'analyse.

Pour activer l'analyse d'archives et de fichiers de messagerie

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Guard**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Cliquez sur le bouton **Avancé**.
5. Activez les options **Archives**, **Fichiers de messagerie**.
6. Cliquez sur **Enregistrer**.

Pour spécifier la durée maximale de l'analyse d'un objet

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Guard**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Cliquez sur le bouton **Avancé**.
5. Activez l'option **Durée maximale de l'analyse d'un objet**.
6. Spécifiez la durée maximale de l'analyse d'un objet en secondes.
7. Cliquez sur **Enregistrer**.

8.2. Exclusion des fichiers et des dossiers de l'analyse

Vous pouvez exclure certains dossiers et fichiers de l'analyse permanente.

Pour exclure les fichiers et les dossiers de l'analyse

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Exclusions**.

3. Accédez à l'onglet **Fichiers et dossiers**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur le bouton et indiquez le dossier ou le fichier nécessaire ou faites-le glisser dans la liste.
6. Cliquez sur **Enregistrer**. SpIDer Guard n'analysera plus ce fichier.

Si vous voulez annuler temporairement l'exclusion de l'objet de l'analyse, mais vous voulez le garder dans la liste, désactivez l'option **SpIDer Guard** à droite de l'objet.

- Pour supprimer un objet de la liste d'exclusions, sélectionnez-le dans la liste et cliquez sur ou faites glisser en dehors de la fenêtre de l'application.
- Pour vider la liste d'exclusions, sélectionnez tous les éléments dans la liste (COMMANDE + A) et cliquez sur .

Les paramètres par défaut des réactions automatiques sont optimaux, il n'est pas recommandé de les modifier sans une nécessité réelle.

Tous les dossiers de la quarantaine sont ajoutés dans les deux listes des exclusions par défaut. La quarantaine est destinée à isoler des objets malveillants détectés, et comme l'accès à ces objets est bloqué, il n'est pas nécessaire de les scanner.

9. Analyse du trafic web

Lors de chaque connexion à Internet les navigateurs, les gestionnaires de téléchargements et d'autres applications échangent les données avec le serveur du site particulier. Les données sont transmises par le protocole non sécurisé HTTP. Le moniteur Internet SpIDer Gate analyse le trafic et bloque la transmission des objets qui peuvent compromettre la sécurité de Mac.

SpIDer Gate supporte également l'analyse des données transmises par le protocole sécurisé HTTPS. Pour configurer l'analyse du trafic chiffré, il faut activer l'option correspondante dans la section Réseau.

SpIDer Gate se lance automatiquement après l'installation et l'activation de la licence de Dr.Web. Le composant fonctionne en permanence et se lance au démarrage de Mac.

SpIDer Gate restreint l'accès aux sites non recommandés et aux pages qui contiennent les éléments violant le droit d'auteur. Vous pouvez modifier ces options et spécifier les paramètres d'accès aux sites spécifiques et aux catégories de ressources Internet.

Vous pouvez exclure certains sites et les connexions réseau des applications indiquées de l'analyse du trafic Web.

Activation et désactivation de SpIDer Gate

D'autres applications de contrôle du trafic web et de contrôle d'accès aux ressources Web installées sur Mac peuvent ne pas fonctionner correctement si SpIDer Gate est activé.

Pour suspendre ou reprendre l'analyse du trafic Web

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, sélectionnez **Composants de protection**.
2. Activez ou désactivez le SpIDer Gate avec l'interrupteur  .

SpIDer Gate ne marche pas / L'extension système est bloquée

Dans macOS 10.13 ou les versions supérieures le téléchargement des extensions système (modules de noyau) est bloqué. Dans ce cas, SpIDer Gate ne marche pas et le message sur le blocage de l'extension système s'affiche sur l'écran. Pour un fonctionnement correct de l'analyse du trafic Web sur votre Mac, autorisez le téléchargement des logiciels de Doctor Web Ltd.

Pour autoriser le téléchargement d'extensions système

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Préférences système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur **Autoriser** à côté du message de blocage du logiciel système de Doctor Web Ltd.

Sous macOS 11.0 et 12.0, cliquez sur **Avancé** et cochez les composants de Dr.Web.

Sous macOS 13.0 et 14.0

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Dans cette section trouvez la ligne **Certains logiciels système requièrent votre attention avant de pouvoir être utilisés** et cliquez sur **Détails** ci-dessous.
5. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
6. Basculez le commutateur contre les composants de Dr.Web sur la position Activé et cliquez sur **OK**.

Sous macOS 15.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Général** et sélectionnez **Ouverture et extensions**.
4. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions de sécurité de point de terminaison** et cliquez sur l'icône ⓘ qui se trouve à droite.
5. Basculez le commutateur **Dr.Web Spider** sur la position Activé et cliquez sur **Terminé**.
6. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions du réseau** et cliquez sur l'icône ⓘ qui se trouve à droite.
7. Basculez le commutateur **Dr.Web Firewall** sur la position Activé et cliquez sur **Terminé**.

9.1. Configuration du moniteur Internet SpIDer Gate

Dans la section de paramètres de **SpIDer Gate**, vous pouvez configurer l'analyse de menaces réseau et l'accès aux ressources Internet.

SpIDer Gate restreint l'accès aux sites non recommandés et aux pages qui contiennent les éléments violant le droit d'auteur. De plus, SpIDer Gate bloque des programmes suspects, des adwares et des dialers.

Vous pouvez configurer l'analyse de menaces web, créer les règles d'accès aux pages particuliers et sélectionner les catégories de sites supplémentaires auxquelles l'accès sera restreint.

> ⚠ Il n'est pas recommandé de modifier les paramètres par défaut si vous n'êtes pas sûr que c'est vraiment nécessaire.

Analyse de menaces

Dans l'onglet **Analyse des menaces**, vous pouvez spécifier les paramètres de l'analyse de menaces web, configurer le blocage des programmes malveillants par types et indiquer la durée maximale de l'analyse d'un objet.

SpIDer Gate restreint l'accès à des sites non recommandés et aux URL ajoutées sur la demande du détenteur de droits. Quels sites sont-ils considérés comme non recommandés selon Dr.Web ?

Vous pouvez enlever les restrictions d'accès à ces sites.

Pour enlever les restrictions

1. Dans la fenêtre principale, cliquez sur ⚙.
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Gate**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur 🔒 en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Dans l'onglet **Analyse des menaces**, désactivez les options **Bloquer les URL ajoutées à la demande du titulaire des droits**, **Bloquer les sites non recommandés**, **Bloquer les objets non analysés**.

Par défaut, Dr.Web saute les objets dont l'analyse n'a pas réussi. Vous pouvez activer le blocage des objets non analysés.

Pour activer le blocage des objets non analysés

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Gate**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Dans l'onglet **Analyse des menaces**, activez l'option **Bloquer les objets non analysés**.

Par défaut, SpIDer Gate bloque des logiciels suspects, des adwares et des dialers. Vous pouvez configurer le blocage des types de logiciels malveillants.

Pour configurer le blocage des logiciels malveillants

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Gate**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Dans l'onglet **Analyse des menaces** sélectionnez les types des logiciels malveillants à bloquer.

Vous pouvez spécifier la durée maximale de l'analyse d'un objet.

L'augmentation de la durée maximale de l'analyse d'un seul objet peut ralentir votre Mac.

Pour spécifier la durée maximale de l'analyse d'un objet

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Gate**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Dans l'onglet **Analyse des menaces** de l'option **Durée maximale de l'analyse d'un objet**, spécifiez la durée maximale de l'analyse d'un objet en secondes.

Filtre URL

Dans l'onglet **Accès aux sites**, vous pouvez créer les règles d'accès aux pages particulières et sélectionner les catégories des sites auxquels l'accès sera temporairement restreint.

Vous pouvez sélectionner les catégories des sites auxquels l'accès sera temporairement restreint quels que soient les autres configurations de SpIDer Gate.

Pour restreindre l'accès aux catégories de sites

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Gate**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Dans l'onglet **Accès aux sites**, sélectionnez les catégories des sites auxquels l'accès sera restreint :

Catégorie	Description
Sites pour adultes	Sites au contenu pornographique ou érotique, sites de rencontres, etc.
Violence	Sites appelant à la violence, sites contenant les informations sur les accidents avec des victimes humaines, etc.
Armes	Sites consacrés aux armes et aux explosifs, sites contenant la description de fabrication d'explosifs, etc.
Jeux d'argent	Sites de jeux en ligne, casinos en ligne, sites d'enchères en ligne, sites de paris, etc.
Drogues	Sites faisant l'apologie de la production, distribution et consommation de drogues, etc.
Jeux en ligne	Sites de jeux nécessitant la connexion Internet permanente.
Terrorisme	Sites contenant de la propagande agressive, sites contenant les descriptions des attentats, etc.
Langage ordurier	Sites contenant du langage obscène (dans des titres de sections, articles, etc.).
Tchats	Sites d'échange de messages en temps réel.
Boîtes mail	Sites permettant de créer gratuitement une boîte e-mail.
Réseaux sociaux	Réseaux sociaux d'ordre général, réseaux d'entreprise, réseaux sociaux thématiques et des sites de rencontres thématiques.
Anonymiseurs	Sites permettant aux utilisateurs de masquer leurs informations personnelles et donnant accès à des sites bloqués.
<% CRYPTOCURRENCY POOLS%>	Sites donnant accès aux services rassemblant les utilisateurs pour le minage de cryptomonnaies.

Catégorie	Description
<%JOBS%>	Site de recherche d'emploi.

Vous pouvez sélectionner les sites auxquels l'accès sera temporairement restreint quels que soient les autres configurations de SpIDer Gate.

Pour restreindre l'accès à un site spécifique

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **SpIDer Gate**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Dans l'onglet **Accès aux sites**, cliquez sur en bas du tableau et entrez l'adresse du site.

9.2. Exclusion des sites de l'analyse

Vous pouvez exclure certains sites de l'analyse du trafic Web. L'accès à ces sites sera autorisé quels que soient les paramètres du moniteur Internet SpIDer Gate.

Pour autoriser l'accès à un site particulier

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Exclusions**.
3. Accédez à l'onglet **Sites**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur en bas du tableau et entrez l'adresse du site.

- Pour supprimer un objet de la liste d'exclusions, sélectionnez-le dans la liste et cliquez sur ou faites glisser en dehors de la fenêtre de l'application.
- Pour vider la liste d'exclusions, sélectionnez tous les éléments dans la liste (COMMANDE + A) et cliquez sur .

9.3. Analyse du trafic chiffré

A chaque connexion à Internet, Mac échange les données avec le serveur du site particulier. De plus en plus de services Web utilisent les connexions sécurisées : l'échange des informations est effectué par le protocole HTTPS. La sécurité dans ce cas est assurée par le protocole cryptographique SSL/TLS qui supporte le chiffrement des données.

Par défaut Dr.Web n'analyse pas le trafic chiffré.

Pour activer l'analyse du trafic chiffré

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Réseau**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Sélectionnez **Analyser le trafic chiffré**.

Pour que Dr.Web puisse analyser le trafic chiffré, le certificat numérique du site auquel la connexion est établie est remplacé par le certificat de sécurité de la société Doctor Web.

Qu'est-ce qu'un certificat de sécurité

Le certificat de sécurité est un document électronique confirmant que le programme certifié a été vérifié dans une autorité de certification.

Le certificat de sécurité garantit que la communication sera effectuée en mode sécurisé avec la vérification de l'authenticité du titulaire de certificat.

Lors de l'installation de Dr.Web, le certificat de sécurité de la société Doctor Web est importé automatiquement dans la liste de certificats système. Pourtant certaines applications, par exemple les navigateurs (Opera, Firefox) et les clients de messagerie (Mozilla Thunderbird, The Bat!) n'accède pas au stockage système de certificats.

Pour ces applications, vous pouvez exporter le certificat de la société Doctor Web manuellement et ensuite installer (importer) dans l'application nécessaire.

Pour exporter le certificat de Doctor Web

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Réseau**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur et entrez le nom d'utilisateur et le mot de passe.
4. Cliquez sur le bouton **Exporter**.
5. Sélectionnez le dossier dans lequel vous voulez enregistrer le certificat. Cliquez sur **Enregistrer**.
6. Importez le certificat dans l'application nécessaire. Pour en savoir plus sur l'importation du certificat, consultez les documents de référence de cette application.

Si après l'activation de l'option **Analyser le trafic chiffré** vous rencontrez des problèmes de fonctionnement des clients de stockages cloud (tels que Google Drive, Dropbox, Yandex.Disk, etc.), il faut exclure ces applications de l'analyse.

9.4. Exclusion des applications de l'analyse

Vous pouvez exclure les connexions réseau de certaines applications de l'analyse du trafic Web. Les connexions de ces applications seront autorisées quels que soient les paramètres du moniteur Internet SpIDer Gate.

Pour exclure de l'analyse les connexions réseau d'applications

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Exclusions**.
3. Accédez à l'onglet **Applications**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur et indiquez l'application nécessaire ou faites-la glisser dans la liste.

- Pour supprimer un objet de la liste d'exclusions, sélectionnez-le dans la liste et cliquez sur ou faites glisser en dehors de la fenêtre de l'application.
- Pour vider la liste d'exclusions, sélectionnez tous les éléments dans la liste (COMMANDE + A) et cliquez sur .

10. Protection contre des menaces réseau

Le Pare-feu protège Mac d'un accès non autorisé et prévient la perte de données vitales. Il permet de contrôler les connexions Internet des applications et le transfert de données dans le réseau. Il bloque également des connexions suspectes.

Le Pare-feu se lance automatiquement après l'installation et l'activation de la licence de Dr.Web. Le composant fonctionne en permanence et se lance au démarrage de Mac.

Le Pare-feu contrôle tout le trafic entrant et sortant et décide s'il faut bloquer ou autoriser l'accès des applications aux ressources réseau conformément au mode de fonctionnement sélectionné et aux règles de filtrage individuelles.

Activation et désactivation du Pare-feu

Si le Pare-feu est activé, cela peut affecter le fonctionnement des applications tierces de contrôle du trafic Web et de contrôle de l'accès aux ressources Web installées sur votre Mac.

Pour suspendre ou reprendre la protection contre les menaces réseau

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, sélectionnez **Composants de protection**.
2. Activez ou désactivez le Pare-feu avec l'interrupteur  .

Le pare-feu ne marche pas / L'extension système est bloquée

Dans macOS 10.13 ou une version supérieure, le téléchargement des extensions système (modules de noyau) est bloqué. Dans ce cas, le Pare-feu ne marchera pas et le message de blocage de l'extension système s'affichera sur l'écran. Pour que la protection contre des menaces réseau fonctionne correctement sur votre Mac, autorisez le téléchargement des logiciels de Doctor Web Ltd.

Pour autoriser le téléchargement d'extensions système

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Préférences système**.
3. Accédez à la section **Sécurité et confidentialité**.

4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur **Autoriser** à côté du message de blocage du logiciel système de Doctor Web Ltd.

> Sous macOS 11.0 et 12.0, cliquez sur **Avancé** et cochez les composants de Dr.Web.

Sous macOS 13.0 et 14.0

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Dans cette section trouvez la ligne **Certains logiciels système requièrent votre attention avant de pouvoir être utilisés** et cliquez sur **Détails** ci-dessous.
5. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
6. Basculez le commutateur contre les composants de Dr.Web sur la position Activé et cliquez sur **OK**.

Sous macOS 15.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Général** et sélectionnez **Ouverture et extensions**.
4. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions de sécurité de point de terminaison** et cliquez sur l'icône ⓘ qui se trouve à droite.
5. Basculez le commutateur **Dr.Web Spider** sur la position Activé et cliquez sur **Terminé**.
6. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions du réseau** et cliquez sur l'icône ⓘ qui se trouve à droite.
7. Basculez le commutateur **Dr.Web Firewall** sur la position Activé et cliquez sur **Terminé**.

Le Pare-feu a bloqué l'accès à Internet

Si une application, par exemple le Pare-feu, ne peut pas obtenir l'accès à Internet, créez une règle d'autorisation dans les paramètres du Pare-feu.

10.1. Configuration du Pare-feu

Dans la section de paramètres du **Pare-feu**, vous pouvez spécifier les paramètres de l'analyse du trafic entrant et sortant et configurer l'accès d'applications individuelles aux ressources Web.

Le Pare-feu autorise l'accès aux ressources réseau pour toutes les applications de confiances. Si l'application ne figure pas dans la liste d'applications de confiance, Dr.Web affiche une notification et demande quelle action appliquer.

Quelles applications sont-elles considérées comme celles de confiance selon Dr.Web

Les applications de confiance comprennent les applications système de macOS, les applications ayant le certificat de sécurité ou une signature numérique valide. Les règles pour ces applications s'affichent dans la liste de règles de filtrage.

Vous pouvez modifier le mode de fonctionnement du Pare-feu et spécifier les règles de filtrage pour les applications individuelles qui ne concernent pas le mode sélectionné.

Mode de fonctionnement

Sélectionnez un des modes suivants :

- **Autoriser les applications de confiance** : toutes les applications de confiance sont autorisées à accéder aux ressources réseau. Pour les autres applications, Dr.Web affiche une notification et demande quelle action appliquer.
- **Autoriser toutes les connexions** : toutes les applications inconnues sont autorisées à accéder aux ressources réseau. Les connexions connues sont traitées par le Pare-feu conformément aux règles de filtrage.
- **Bloquer toutes les connexions** : aucune application inconnue n'est autorisée à accéder aux ressources réseau. Les connexions connues sont traitées par le Pare-feu conformément aux règles de filtrage.

Toutes les connexions sont autorisées par défaut.

Pour modifier le mode de fonctionnement du Pare-feu

1. Dans la fenêtre principale, cliquez sur  .
2. Dans la fenêtre **Préférences** sélectionnez la section **Pare-feu**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur  en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.

4. Sélectionnez le mode de fonctionnement dans la liste déroulante **Mode**, dans la partie supérieure de la fenêtre.

Règles de filtrage

Vous pouvez spécifier les règles de filtrage pour les applications individuelles. Les règles spécifiées s'appliquent quel que soit le mode de fonctionnement du Pare-feu.

Une règle de filtrage comporte :

- un fichier de l'application au format `.app` ;
- les actions : autoriser ou bloquer la connexion ;
- le numéro de port par lequel la connexion est établie ;
- l'adresse IP, le nom d'hôte du site ou du serveur l'accès auquel sera contrôlé par le Pare-feu.

Pour créer une nouvelle règle

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Pare-feu**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Cliquez sur en bas du tableau. La fenêtre de création d'une nouvelle règle va s'ouvrir.
5. Dans le champ **<%ADD APP%>**, cliquez sur .
6. Choisissez si la règle concerne toutes les applications ou sélectionnez une application sur Mac.
7. Sélectionnez une action dans la liste déroulante : **Bloquer** ou **Autoriser**.
8. Indiquez le numéro du port par lequel la connexion est établie.

> Si vous laissez le champ **Port** vide, la règle concernera tous les ports.
>
> Exclusion : si vous voulez créer une règle pour toutes les applications, il faut obligatoirement indiquer le numéro de port.

9. Dans la liste déroulante **Connexion**, sélectionnez :
   - **Tout serveur**, si vous voulez configurer l'accès à tous les serveurs et par toutes les adresses IP.

> Si vous voulez créer une règle pour tous les ports, il faut obligatoirement indiquer l'adresse IP ou l'hôte.

- **Adresse IP**, si vous voulez configurer l'accès à une adresse IP particulière. Entrez l'adresse au format IPv4 : `192.0.2.235`.
- **Hôte**, si vous voulez configurer l'accès à un hôte particulier. Entrez l'hôte du site ou du serveur au format `example.com`.

10. Cliquez sur le bouton **Créer**.

Pour éditer une règle

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Pare-feu**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Dans le tableau de règles de filtrage, double-cliquez sur la règle nécessaire. La fenêtre d'édition de la règle va s'ouvrir.

   Si plusieurs règles sont créées pour une application, cliquez sur l'icône pour ouvrir la liste.

5. Modifiez les paramètres nécessaires de la règle.
6. Cliquez sur **Enregistrer**.

11. Analyse de Mac à la demande

Le Scanner Dr.Web analyse les objets du système de fichiers à la demande de l'utilisateur et détecte les menaces qui dissimulent leur présence dans le système. Pour assurer une protection fiable de votre Mac, il est recommandé de lancer de temps en temps l'analyse du système par Dr.Web.

Vous pouvez exclure certains dossiers et fichiers de l'analyse à la demande.

> Quand votre Mac passe en fonctionnement sur batterie, l'analyse est mise en pause pour ralentir la décharge de la batterie. Dans ce cas, Dr.Web vous propose de décider si vous voulez continuer l'analyse ou non. Une fois l'ordinateur branché, l'analyse reprend automatiquement.

Pour analyser rapidement les parties les plus vulnérables du système, lancez l'**Analyse rapide**, pour analyser tout le système de fichiers, lancez l'**Analyse complète**, ou spécifiez les fichiers et les dossiers à analyser.

Types de l'analyse

Mode d'analyse	Description
Analyse rapide	Ce mode prévoit l'analyse des objets suivants : • secteurs d'amorçage de tous les disques ; • mémoire vive ; • dossier racine du disque de démarrage ; • dossier système ; • répertoire de l'utilisateur actuel ; • fichiers temporaires ; • points de restauration du système ; • présence de rootkits (si le scan a été lancé en mode administrateur). Dans ce mode les archives et les fichiers de messagerie ne sont pas analysés.
Analyse complète	Ce mode assure l'analyse complète de la mémoire vive et de tous les disques durs (y compris les secteurs d'amorçage). La recherche des rootkit est également effectuée.
Analyse personnalisée	L'analyse de tous les fichiers et dossiers indiqués par l'utilisateur.

Pour lancer une analyse rapide

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, sélectionnez **Analyser Mac**.
2. Cliquez sur **Analyse rapide**.

Pour lancer une analyse complète

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, sélectionnez **Analyser Mac**.
2. Cliquez sur **Analyse complète**.

Pour lancer une analyse des fichiers et des dossiers individuels

Vous pouvez analyser certains fichiers et dossiers en utilisant l'un des moyens suivants.

Via la section Analyser Mac

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, sélectionnez **Analyser Mac**.
2. Faites glisser les fichiers et les dossiers que vous voulez analyser dans la zone pointillée ou cliquez sur cette zone et sélectionnez les objets à analyser.

En faisant glisser sur l'icône de l'application

1. Faites glisser le fichier ou le dossier à analyser sur l'icône Dr.Web dans la ligne du menu (elle se trouve le long du bord supérieur de l'écran de Mac).

Depuis le menu contextuel

1. Sélectionnez le fichier ou le dossier nécessaire sur le Bureau ou dans Finder.
2. Ouvrez le menu contextuel et cliquez sur **Analyser avec Dr.Web**.

Résultats de l'analyse

La fenêtre contenant les résultats de l'analyse devient disponible si

- vous avez interrompu l'analyse (vous avez cliqué sur **Stop**),
- Dr.Web a terminé l'analyse de Mac.

La fenêtre de résultats de l'analyse contient :

- le nombre d'objets analysés,
- le nombre d'objets sautés,
- le nombre de menaces détectées,
- le nombre de menaces neutralisées.

Une fois une menace détectée, le Scanner applique l'action spécifiée dans les paramètres. Vous pouvez modifier les actions qui s'appliquent automatiquement aux différents types de menaces ou appliquer les actions manuellement.

Pour voir les informations détaillées sur les menaces

- Dans la fenêtre de résultats de l'analyse cliquez sur le bouton **En savoir plus**. L'onglet **Détails de l'analyse** va s'ouvrir.

Dans l'onglet **Détails de l'analyse**, vous pouvez voir les informations détaillées sur les menaces que Dr.Web a détecté lors de la dernière analyse.

Pourquoi certains objets sont-ils sautés

Cause	Résolution
Droits insuffisants pour l'appliquer une action à l'objet.	Lancez l'analyse avec les droits d'administrateur.
Fichier trop volumineux.	Augmentez la durée maximale de l'analyse d'un objet dans les paramètres du Scanner. Lancer l'analyse encore une fois.
Fichier endommagé ou protégé par un mot de passe.	S'il s'agit d'une archive, décompressez-la. Lancer l'analyse encore une fois.
Il y a des archives dans la liste d'objets sautés.	Dans les paramètres du Scanner, activez l'option **Archives** ou décompressez les archives. Lancer l'analyse encore une fois.
Il y a des fichiers de messagerie dans la liste d'objets sautés.	Dans les paramètres du Scanner, activez l'option **Fichiers de messagerie**. Lancer l'analyse encore une fois.

Analyse avec les droits d'administrateur

L'application Dr.Web peut demander les droits d'administrateur pour appliquer des actions à certains objets malveillants.

Pour lancer l'analyse avec les droits d'administrateur

1. Dans la fenêtre principale, cliquez sur .

2. Dans la fenêtre **Préférences** sélectionnez la section **Scanner**.
3. Cliquez sur le bouton **Avancé**.
4. Sélectionnez **Lancer l'analyse au nom de l'administrateur**.
5. Lancer l'analyse encore une fois.

11.1. Configuration du Scanner

Dans la section de paramètres **Scanner**, vous pouvez configurer les actions que Dr.Web appliquera aux menaces en fonction de leur type.

Le Scanner essaie de désinfecter les fichiers infectés : les objets infectés par des virus connus et potentiellement curables, tandis que les objets suspects et les différents types de logiciels malveillants sont placés en Quarantaine.

Vous pouvez modifier séparément la réaction du Scanner vis-à-vis d'objets malveillants. Les actions disponibles dépendent du type de menace :

Action	Description
Désinfecter, mettre les incurables en quarantaine	Restaure l'objet dans son état original avant infection. Si le virus est incurable, ou qu'une tentative de désinfection a échoué, l'objet sera mis en quarantaine. Cette action est possible uniquement pour les virus connus, sauf les trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
Désinfecter, supprimer les incurables	Restaure l'objet dans son état original avant infection. Si le virus est incurable, ou qu'une tentative de désinfection a échoué, l'objet sera supprimé. Cette action est possible uniquement pour les virus connus, sauf les trojans et les fichiers infectés au sein des objets complexes (les archives, les fichiers de messagerie ou les conteneurs de fichiers).
Supprimer	Supprime l'objet. Aucune action n'est appliquée aux secteurs d'amorçage.
Mettre en quarantaine	Isole l'objet dans le dossier spécial Quarantaine. Permet de prévenir une perte de données vitales. Aucune action n'est appliquée aux secteurs d'amorçage.
Ignorer	Ignore l'objet sans appliquer aucune action ni afficher d'alerte. Cette action est disponible uniquement pour les programmes malveillants dont adwares, dialers, canulars, hacktools et riskwares.

Pour modifier les paramètres du Scanner. il ne faut pas entrer le nom d'utilisateur et le mot de passe. Les paramètres seront automatiquement modifiés pour tous les utilisateurs de Mac.

Il ne faut pas modifier les paramètres prédéfinis des actions automatiques si vous n'êtes pas sûr que c'est vraiment nécessaire.

Actions du Scanner qui s'appliquent aux objets malveillants

Type d'objet	Action				
	Désinfecter, mettre les incurables en quarantaine	**Désinfecter, supprimer les incurables**	**Mettre en quarantaine**	**Supprimer**	**Ignorer**
Infectés	+/*	+	+	+	
Suspects			+/*	+	+
Adwares			+/*	+	+
Dialers			+/*	+	+
Canulars			+	+	+/*
Riskwares			+	+	+/*
Hacktools			+	+	+/*
Archives infectées	+	+	+	+	+
Fichiers de messagerie infectés	+	+	+	+	+

Conventions

+	action possible
+/*	action spécifiée par défaut

Il n'est pas possible de spécifier une action par défaut à appliquer aux archives et aux fichiers de messagerie infectés car les actions s'y appliquent en fonction de la menace détectée. S'il y a plusieurs menaces, l'action de la menace plus importante sera appliquée.

Pour configurer les actions automatiques

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Scanner**.
3. Activez l'option **Appliquer les actions aux menaces automatiquement**.
4. En cas de besoin, modifiez les actions automatiques pour les types de menaces listés.

Paramètres avancés

Analyse avec les droits d'administrateur

L'application Dr.Web peut demander les droits d'administrateur pour appliquer des actions à certains objets malveillants.

Pour lancer l'analyse avec les droits d'administrateur

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Scanner**.
3. Cliquez sur le bouton **Avancé**.
4. Sélectionnez **Lancer l'analyse au nom de l'administrateur**.

Maintenant avant chaque analyse, Mac demandera le nom d'utilisateur et le mot de passe.

De plus, vous pouvez configurer l'analyse de fichiers à la demande, c'est-à-dire, activer l'analyse d'archives et de fichiers de messagerie, ainsi que spécifier la durée maximale de l'analyse d'un seul objet.

La modification de ces paramètres peut ralentir votre Mac et augmenter la durée totale de l'analyse.

Pour activer l'analyse d'archives et de fichiers de messagerie

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Scanner**.
3. Cliquez sur le bouton **Avancé**.
4. Cochez les cases **Archives** et **Fichiers de messagerie**.
5. Cliquez sur **Enregistrer**.

Les archives et les fichiers de messagerie ne sont pas analysés en mode **Analyse rapide**.

Pour spécifier la durée maximale de l'analyse d'un objet

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Scanner**.
3. Cliquez sur le bouton **Avancé**.
4. Cochez la case **Durée maximale de l'analyse d'un objet**.
5. Spécifiez la durée maximale de l'analyse d'un objet en secondes.
6. Cliquez sur **Enregistrer**.

Économie de la batterie

Quand votre Mac passe en fonctionnement sur batterie, l'analyse est mise en pause pour ralentir la décharge de la batterie. Dans ce cas, Dr.Web vous propose de décider si vous voulez continuer l'analyse ou non. Une fois l'ordinateur branché, l'analyse reprend automatiquement.

Vous pouvez désactiver l'option de la mise en pause de l'analyse en cas de passage sur batterie.

Pour configurer l'analyse lors du fonctionnement sur batterie

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Scanner**.
3. Cliquez sur le bouton **Avancé**.
4. Activez (ou désactivez) l'option **Mettre l'analyse en pause en cas de passage au mode d'alimentation sur batterie**.
5. Cliquez sur **Enregistrer**.

11.2. Exclusion des fichiers et des dossiers de l'analyse

Vous pouvez exclure certains dossiers et fichiers de l'analyse à la demande.

Pour exclure les fichiers et les dossiers de l'analyse

1. Dans la fenêtre principale, cliquez sur .

2. Dans la fenêtre **Préférences** sélectionnez la section **Exclusions**.
3. Accédez à l'onglet **Fichiers et dossiers**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur  en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur le bouton  et indiquez le dossier ou le fichier à ajouter aux exclusions, ou bien, faites glisser l'objet directement dans la liste des exclusions.
6. Cliquez sur **Enregistrer**. Le Scanner n'analysera plus ce dossier ou fichier lors de l'analyse à la demande.

Si vous voulez annuler temporairement l'exclusion de l'objet de l'analyse, mais que vous voulez le garder dans la liste, décochez la case de cet objet dans la colonne **Scanner**.

- Pour supprimer un objet de la liste des exclusions, sélectionnez-le dans la liste et cliquez sur ou faites glisser l'objet en dehors de la fenêtre de l'application.
- Pour vider la liste d'exclusions, sélectionnez tous les éléments dans la liste (COMMANDE + A) et cliquez sur .

Les paramètres par défaut des réactions automatiques sont optimaux, il n'est pas recommandé de les modifier sans une nécessité réelle.

Tous les dossiers de la quarantaine sont ajoutés dans les deux listes des exclusions par défaut. La quarantaine est destinée à isoler des objets malveillants détectés, et comme l'accès à ces objets est bloqué, il n'est pas nécessaire de les scanner.

12. Protection de la confidentialité

Dr.Web protège la confidentialité de votre vie privée, en surveillant l'accès des applications à la webcam et au microphone connectés à votre ordinateur.

Par défaut, l'accès à la webcam et au microphone est autorisé pour toutes les applications. Vous pouvez activer le contrôle de l'accès à la webcam et au microphone.

> Les paramètres de contrôle de l'accès à la webcam et au microphone ne sont pas disponibles dans la version macOS 10.14 ou une version supérieure.

Pour activer le contrôle de l'accès à la webcam et au microphone

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, sélectionnez **Protection de la confidentialité**.
2. Activez la protection de l'accès à la webcam et au microphone avec l'interrupteur .

Chaque fois qu'une application tente d'avoir l'accès à la webcam et au microphone, Dr.Web affiche une notification et demande quelle action appliquer :

- **Bloquer** : bloquer l'accès de l'application à la webcam ou au microphone. Dans ce cas, l'accès est bloqué une fois. Si l'application est fermée et qu'elle tente de nouveau d'avoir l'accès, Dr.Web affichera la notification encore une fois.
- **Autoriser** : autoriser l'application à accéder à la webcam ou au microphone.

  Les options supplémentaires de contrôle de l'accès sont disponibles pour les utilisateurs du groupe Administrateurs :

  - **Autoriser une seule fois** : autoriser l'application à accéder à la webcam ou au microphone une seule fois.
  - **Autoriser toujours** : toujours autoriser l'application à accéder à la webcam ou au microphone.

  Si vous sélectionnez l'option **Autoriser toujours**, Dr.Web créera une règle séparée pour cette application dans la liste d'exclusions.

  > Pour créer une règle dans la liste d'exclusions, les droits d'administrateur sont requis.

12.1. Autoriser l'accès à la webcam et au microphone

Vous pouvez configurer l'accès de certaines applications à la webcam et au microphone.

Les paramètres d'accès à la webcam et au microphone ne sont pas disponibles dans la version macOS 10.14 ou une version supérieure.

Pour autoriser l'accès à la webcam et au microphone

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Exclusions**.
3. Accédez à l'onglet **Webcam et microphone**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur en bas de la liste **Webcam** ou **Microphone** et indiquez l'application nécessaire ou faites-la glisser dans la liste correspondante.

- Pour supprimer un objet de la liste des exclusions, sélectionnez-le dans la liste et cliquez sur ou faites glisser l'objet en dehors de la fenêtre de l'application.
- Pour vider la liste d'exclusions, sélectionnez tous les éléments dans la liste (COMMANDE + A) et cliquez sur .

13. Neutralisation des menaces

13.1. Menaces

Dans la section **Menaces**, vous pouvez voir la liste complète de menaces et y appliquer les actions nécessaires. Pour neutraliser les menaces, configurez des actions automatiques ou appliquez des actions aux menaces détectées manuellement.

Pour voir les informations sur les menaces

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, cliquez sur **Menaces**.

   L'onglet **Menaces** contient toutes les menaces détectées.

   La barre d'état en bas de la fenêtre contient le nombre total des menaces et leur taille totale, ainsi que le nombre et la taille des objets sélectionnés.
2. Pour voir les informations sur une menace, cliquez sur le champ correspondant.
3. Si nécessaire, vous pouvez appliquer une action à la menace. Pour ce faire, dans la liste déroulante en bas de la fenêtre sélectionnez :
   - **Supprimer** : supprimer définitivement l'objet du système de fichiers ;
   - **Mettre en quarantaine** : déplacer l'objet en quarantaine ;
   - **Ignorer** : n'appliquer aucune action.

Pour appliquer une actions à la menace

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, cliquez sur **Menaces**.
2. Dans la liste déroulante, sélectionnez une action pour la menace correspondante :
   - **Supprimer** : supprimer définitivement l'objet du système de fichiers ;
   - **Mettre en quarantaine** : déplacer l'objet en quarantaine ;
   - **Ignorer** : n'appliquer aucune action.
3. Pour neutraliser toutes le menaces détectées, cliquez sur **Neutraliser tout**. Les actions spécifiées dans les paramètres de l'application pour les types de menaces correspondants seront appliquées.

S'il y a des archives dans la liste de menaces, l'action sera appliquée à l'archive entière.

Si vous voulez appliquer l'action à un fichier séparé, décompressez l'archive et lancez l'analyse encore une fois.

Pour appliquer une action à plusieurs menaces

1. Sélectionnez plusieurs menaces avec la touche MAJ.
2. Utilisez les raccourcis clavier :
   - pour supprimer les menaces, appuyez sur Commande + Maj +D ;
   - pour mettre les menaces en quarantaine, appuyez sur Commande + Maj + M.

13.2. Quarantaine

Dans la section **Quarantaine**, vous pouvez consulter les informations sur les objets mis en quarantaine et y appliquer une action. La Quarantaine est un dossier spécial dans lequel vous pouvez isoler les menaces détectées du reste du système au cas ou vous auriez besoin d'un objet qui ne peut pas être désinfecté.

Pour des raisons de confidentialité, un dossier séparé de la quarantaine est créé pour chaque utilisateur du système. De ce fait, si vous passez en mode Administrateur, les menaces détectées sont déplacées vers la quarantaine de l'administrateur et ne seront pas accessibles dans la quarantaine d'utilisateurs.

Pour voir les informations sur les objets en quarantaine

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, cliquez sur **Menaces**.
2. Ouvrez l'onglet **Quarantaine**.
3. Pour afficher les informations sur l'objet en quarantaine, double-cliquez sur l'objet correspondant.

Pour appliquer l'action à l'objet en quarantaine

1. Dans l'onglet **Panneau de gestion** de la fenêtre principale, cliquez sur **Menaces**.
2. Ouvrez l'onglet **Quarantaine**.
3. Dans la liste déroulante, sélectionnez l'action nécessaire pour l'objet correspondant :
   - **Supprimer** : supprimer définitivement l'objet du système de fichiers ;
   - **Restaurer** : restaurer l'objet dans son emplacement original ;
   - **Restaurer vers** : spécifier le chemin de restauration de l'objet.

Il est impossible de désinfecter les objets en quarantaine. Vous pouvez analyser l'objet encore une fois si vous doutez que le fichier soit malveillant.

Vous pouvez également restaurer l'objet. Les algorithmes de désinfection sont toujours améliorés. Il est possible qu'après une mise à jour de l'application vous parveniez à désinfecter l'objet.

S'il y a des archives dans la liste de menaces, l'action sera appliquée à l'archive entière.

Si vous voulez appliquer l'action à un fichier séparé, décompressez l'archive et lancez l'analyse encore une fois.

Pour appliquer une action à plusieurs menaces

1. Sélectionnez plusieurs menaces avec la touche MAJ.
2. Utilisez les raccourcis clavier :
   - pour supprimer la menace, appuyez sur Commande + Maj + D ;
   - pour restaurer l'objet dans son emplacement original, appuyez sur Commande + Maj + R ;
   - pour spécifier le chemin de restauration de l'objet, appuyez sur Commande + Maj + P.

14. Support

14.1. Aide

Pour ouvrir l'aide de Dr.Web

1. Dans la fenêtre principale, cliquez sur .
2. Sélectionnez l'onglet **Aide**.

Si vous n'avez pas trouvé les informations nécessaires dans l'Aide, consultez la liste de questions et de réponses. Si vous n'arrivez pas à trouver une solution à votre problème ou une réponse à votre question, veuillez contacter le support technique de la société Doctor Web.

14.2. Questions et réponses

Voici une liste de problèmes qui peuvent survenir lors de la gestion de Dr.Web et de différentes solutions pour les résoudre. Merci de prendre connaissance de ces informations avant de vous adresser au support technique.

Problèmes d'ordre général

Comment changer la langue

Le changement de langue est disponible sous macOS 10.15 ou une version supérieure.

Pour changer la langue de l'application

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Sélectionnez **Général**.
4. Cliquez sur **Langue et région**.
5. Cliquez sur **Apps**.
6. Sélectionnez Dr.Web pour macOS et choisissez une langue d'application.

Les composants SpIDer Gate, SpIDer Guard et le Pare-feu ne se lancent pas

macOS bloque le téléchargement des extensions système (modules de noyau). Pour un fonctionnement correct de SpIDer Gate et SpIDer Guard, autorisez le téléchargement des logiciels

de Doctor Web dans le panneau **Sécurité et confidentialité**, dans la section **Réglages système**.

Pour autoriser le téléchargement d'extensions système

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Préférences système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur **Autoriser** à côté du message de blocage du logiciel système de Doctor Web Ltd.

Sous macOS 11.0 et 12.0, cliquez sur **Avancé** et cochez les composants de Dr.Web.

Sous macOS 13.0 et 14.0

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Dans cette section trouvez la ligne **Certains logiciels système requièrent votre attention avant de pouvoir être utilisés** et cliquez sur **Détails** ci-dessous.
5. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
6. Basculez le commutateur contre les composants de Dr.Web sur la position Activé et cliquez sur **OK**.

Sous macOS 15.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Général** et sélectionnez **Ouverture et extensions**.
4. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions de sécurité de point de terminaison** et cliquez sur l'icône ⓘ qui se trouve à droite.
5. Basculez le commutateur **Dr.Web Spider** sur la position Activé et cliquez sur **Terminé**.

6. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions du réseau** et cliquez sur l'icône ⓘ qui se trouve à droite.
7. Basculez le commutateur **Dr.Web Firewall** sur la position Activé et cliquez sur **Terminé**.

La licence est activée, mais Dr.Web ne fonctionne pas

- Il est possible que la licence ait expiré. Les informations sur la durée de validité de la licence se trouvent dans la section **Licence** de la fenêtre principale de Dr.Web .Si la licence a expiré, achetez une nouvelle licence.
- Il est probable que vous avez mis à niveau le système d'exploitation et la version installée de Dr.Web ne prend pas en charge la nouvelle version de macOS. Désinstallez la version actuelle de Dr.Web et installez l'application de nouveau.

Le fonctionnement de Dr.Web est instable (il plante ou il ralentit)

Cela peut être causé par une activité élevée des processus système exigeant de grands volumes de mémoire vive. Il est recommandé de fermer les applications dont vous n'avez plus besoin pour libérer une partie de la mémoire. Vous pouvez prendre connaissance des processus activés ainsi que les gérer via l'utilitaire standard de macOS Moniteur d'activité.

Si le problème persiste, réinstallez l'application.

Le Pare-feu a bloqué l'accès à Internet

Créez une règle d'autorisation dans les paramètres du Pare-feu pour l'application qui ne peut pas obtenir l'accès à Internet.

Les alertes sonores sont paramétrées, mais ne fonctionnent pas

Vérifiez le niveau du son dans la section Préférences système et sur les haut-parleurs.

Les paramètres sont bloqués

Les paramètres de certains composants sont bloqués. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.

Le VPN dans l'application AdGuard ne marche pas

Si vous rencontrez des problèmes avec le VPN AdGuard, effectuez les actions suivantes :

1. Ouvrez les préférences de AdGuard.
2. Cliquez sur **Réseau**.
3. Assurez-vous que la case **Filtrage automatique des applications** est cochée.
4. Cliquez sur **Apps**.
5. Ajoutez Dr.Web pour macOS à la liste d'applications filtrées.

Si vous ne pouvez pas trouver Dr.Web pour macOS pour l'ajouter à la liste d'applications filtrées, redémarrez votre Mac et réessayez.

Problèmes de l'analyse

L'analyse du système de fichiers ne s'effectue pas (impossible de lancer le Scanner et/ou SpIDer Guard)

Il est possible que la licence ait expiré. Les informations sur la durée de validité de la licence se trouvent dans la section **Licence** de la fenêtre principale de Dr.Web .Si la licence a expiré, achetez une nouvelle licence.

Les bases virales mettent beaucoup de temps à être téléchargées ou l'analyse s'effectue trop lentement

- Dr.Web télécharge les bases virales lors du lancement de l'analyse et avant chaque tentative de désinfecter un objet malveillant. C'est pourquoi cela peut demander un certain temps.
- Le fonctionnement instable de l'antivirus peut être causé par une activité élevée des processus système exigeant un grand volume de mémoire vive. Il est recommandé de fermer les applications dont vous n'avez plus besoin pour libérer une partie de la mémoire. Vous pouvez prendre connaissance des processus activés aussi bien que les gérer via l'utilitaire macOS Moniteur d'activité.

Certains fichiers sont sautés lors du scan (ne sont pas analysés)

- Il est probable que les fichiers (ou les dossiers où ils se trouvent) sont exclus de l'analyse.
- Certains fichiers peuvent être sautés lors de l'analyse parce qu'ils sont corrompus, protégés par mot de passe ou les droits d'administrateurs sont requis pour y avoir accès. Si la liste des objets exclus contient des archives, décompressez-les avant de lancer l'analyse.

Le Scanner plante

Si le Scanner a planté, arrêtez-le et ensuite redémarrez. Si le problème persiste, réinstallez l'application.

Erreur de lecture

Cette erreur peut survenir si Dr.Web n'a pas l'accès complet au disque.

Pour autoriser l'accès complet au disque

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Préférences système**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Accédez à la section **Sécurité et confidentialité**.
5. Accédez à la section **Confidentialité**.
6. Cliquez sur **Accès complet au disque**.
7. Ajoutez les modules de Dr.Web dans la liste d'applications autorisées.
8. Cliquez sur **Redémarrer**.

Sous macOS 13.0 et les versions antérieures

1. Dans la fenêtre principale de Dr.Web, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Cliquez sur **Autoriser**.
4. Cliquez sur **Ouvrir les Préférences système** dans le Gestionnaire d'accès au disque.
5. Dans la fenêtre d'instruction du Gestionnaire, cliquez sur la flèche jusqu'à ce que vous voyiez l'icône de Dr.Web.
6. Faites-glisser l'icône de Dr.Web du Gestionnaire d'accès au disque vers la section de préférences système indiquée dans le Gestionnaire.
7. Pour confirmer, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
8. Cliquez sur **Redémarrer** pour enregistrer les modifications.

> ⚠ Si le bouton **Autoriser** n'est pas actif, l'accès au disque est déjà autorisé.

Problèmes de fonctionnement de SpIDer Gate

SpIDer Gate ne bloque pas les sites par catégories sélectionnées

- Assurez-vous que la case contre la catégorie de sites correspondante est cochée dans l'onglet SpIDer Gate.
- Si la connexion avec le site a été établie avant le lancement de SpIDer Gate, désactivez et activez SpIDer Gate et redémarrez le navigateur.
- Vérifiez si le site utilise une connexion sécurisée (en cas de connexion sécurisée, normalement un cadenas est affiché dans la ligne d'adresse du navigateur). Si une connexion sécurisée est utilisée, activez l'option **Analyser le trafic chiffré** dans l'onglet Réseau et redémarrerez le navigateur.
- SpIDer Gate ne bloque pas les sites utilisant la connexion via les protocoles FTP/SPDY ou HTTP/2.0.

Lors de l'ouverture du site un message apparaît signalant une erreur de certificat

- Une erreur peut survenir car certains navigateurs et les clients de messagerie ne s'adressent pas au stockage des certificats système lors de la réception et la transmission du trafic chiffré. Dans ce cas, installez le certificat de la société Doctor Web que vous pouvez obtenir en cliquant sur le bouton Exporter dans l'onglet Réseau.
- Si le navigateur ou le client de messagerie a été lancé juste après l'installation, il pouvait ne pas obtenir le certificat de sécurité. Dans ce cas, redémarrez le navigateur ou le client de messagerie.
- Il est probable que le certificat original du serveur n'est pas fiable. Pour le vérifier, désactivez SpIDer Gate et redémarrez le navigateur ou le client de messagerie. Si l'erreur persiste, le certificat n'est pas fiable. Dans ce cas il est recommandé de ne pas visiter ce site.

SpIDer Gate a bloqué un site nécessaire

Il est probable que ce site fait partie de la catégorie des sites auxquels l'accès est bloqué. Pour obtenir l'accès au site, ajoutez-le aux exclusions.

Mise à jour

Les mises à jour ne se téléchargent pas

- Assurez-vous que Mac est connecté à Internet.

- Si vous utilisez un serveur proxy, essayez de le désactiver et lancez la mise à jour encore une fois. Pour lancer la mise à jour manuellement, sélectionnez l'élément **Une mise à jour est requise** dans la fenêtre principale de Dr.Web .
- Si le routeur fonctionne en mode Connexion à la demande, assurez-vous que la connexion est toujours active (c'est-à-dire, la durée d'inactivité maximale est de 0 minutes).
- Il est possible que la licence ait expiré. Les informations sur la durée de validité de la licence se trouvent dans la section **Licence** de la fenêtre principale de Dr.Web .Si la licence a expiré, achetez une nouvelle licence.

Licence

La durée de validité de la version d'essai n'a pas expiré, mais la licence est devenue invalide

- La licence de la version d'essai est liée à la somme de contrôle du système d'exploitation. Il est probable que vous avez mis à niveau le système d'exploitation ou un autre logiciel ou bien, vous avez remplacé un composant de l'ordinateur et, par conséquent, la somme de contrôle a changé.
- La licence de la version d'essai est liée à l'adresse MAC de l'appareil. Il est probable que vous avez changé l'adresse MAC et, par conséquent, la licence est devenue invalide.

Contactez le support technique de la société Doctor Web ou activez une nouvelle version d'essai à l'aide d'une autre adresse e-mail.

Impossible d'activer la licence

- Assurez-vous que Mac est connecté à Internet.
- Si vous utilisez un serveur proxy, essayez de le désactiver et lancez la mise à jour encore une fois. Pour lancer la mise à jour manuellement, sélectionnez l'élément **Une mise à jour est requise** dans la fenêtre principale de Dr.Web .
- Si le routeur fonctionne en mode Connexion à la demande, assurez-vous que la connexion est toujours active (c'est-à-dire, la durée d'inactivité maximale est de 0 minutes).

Si lors de l'utilisation de Dr.Web, vous rencontrez un problème dont la résolution n'est pas décrite ci-dessus, contactez le support technique de la société Doctor Web. Pour que les spécialistes de Doctor Web puissent vous aider le plus vite possible, veuillez fournir le maximum d'informations sur le problème.

14.3. Codes d'erreurs

Code	Erreur	Description
1	Erreur de connexion à l'écran	Erreur de connexion d'un composant au démon de gestion de la configuration Dr.Web ConfigD.
2	L'opération est déjà en cours d'exécution	L'opération demandée par l'utilisateur est en cours d'exécution.
3	L'opération attend l'exécution	L'opération demandée par l'utilisateur attend l'exécution (il est possible que la connexion réseau s'établisse ou qu'un composant du produit soit en train de télécharger ou de s'initialiser. Cela peut prendre un certain temps).
4	Interrompu par l'utilisateur	L'action exécutée a été interrompue par l'utilisateur (peut-être, elle a été exécutée pendant trop longtemps).
5	L'opération est annulée	L'action exécutée a été annulée (peut-être, elle a été exécutée pendant trop longtemps).
6	La connexion IPC est interrompue	La connexion IPC à un certain composant du produit est interrompue (le composant s'est arrêté à cause de l'inactivité ou suite à une commande de l'utilisateur).
7	Taille de message IPC invalide	Lors de l'échange de données entre les composants, un message de taille inacceptable est reçu.
8	Format de message IPC invalide	Lors de l'échange de données entre les composants, un message au format inacceptable est reçu.
9	Non prêt	L'action nécessaire ne peut pas être effectuée car le composant ou l'appareil requis n'est pas encore initialisé.
10	Le composant n'est pas installé	La fonction nécessaire de Dr.Web n'est pas disponible, car le composant qui la réalise n'est pas installé.
11	Message IPC inattendu	Lors de l'échange de données entre les composants, un message inacceptable est reçu.
12	Violation du protocole IPC	Lors de l'échange de données entre les composants, le protocole d'échange de données a été violée.
13	Statut de sous-système inconnu	Il est déterminé qu'un sous-système de logiciel, nécessaire pour l'exécution de l'opération, est en état inconnu.
20	Le chemin doit être absolu	Le chemin absolu (commençant par la racine du système de fichiers) vers un fichier ou un répertoire est requis, tandis que le chemin indiqué est relatif.
21	Pas assez de mémoire pour terminer l'opération	Pas assez de mémoire pour exécuter l'opération nécessaire (par exemple, tentative d'extraire un fichier trop grand).

Code	Erreur	Description
22	Erreur d'entrée-sortie	Une erreur d'entrée/sortie s'est produite (par exemple, le lecteur n'est pas encore initialisé ou que la section du système de fichiers n'est plus disponible).
23	Fichier ou répertoire inexistant	L'objet indiqué du système de fichier (un fichier ou un répertoire) est manquant. Il est probable qu'il a été supprimé.
24	Accès interdit	Pas assez de droits pour accéder à l'objet indiqué du système de fichiers (fichier ou répertoire).
25	N'est pas un répertoire	Le chemin vers le répertoire a été prévu, pourtant l'objet indiqué du système de fichiers n'est pas un répertoire.
26	Le fichier de données est endommagé	Les données accédées sont endommagées.
27	Un tel fichier existe déjà	Lors de la tentative de créer un fichier, il est déterminé qu'un objet avec ce nom existe déjà.
28	Le système de fichiers est accessible seulement en lecture	Lors de la tentative de créer ou de modifier un objet du système de fichiers (un répertoire, un fichier ou un socket), il est déterminé que le système de fichiers est accessible seulement en lecture.
29	Erreur de réseau	Une erreur de réseau s'est produite (il est probable que l'hôte distant a cessé de répondre ou qu'il est impossible d'établir la connexion nécessaire).
30	N'est pas un lecteur	Tentative d'accès à un appareil d'entrée/sortie qui n'est pas un lecteur.
31	Fin de fichier inattendue	La fin de fichier inattendue a été atteinte lors de la lecture de données.
32	Le fichier a été modifié	Lors du scan du fichier, il est déterminé qu'il a été modifié.
33	Fichier spécial	Lors de l'accès à un objet du système de fichiers, il est déterminé que ce n'est pas un fichier régulier (c'est-à-dire, un répertoire, un socket ou un autre objet du système de fichiers).
34	Ce nom est déjà utilisé	Lors de la tentative de créer un objet du système de fichiers (un répertoire, un fichier ou un socket), il est déterminé qu'un objet avec ce nom existe déjà.
35	L'hôte est désactivé	Il est déterminé que l'hôte distant n'est pas accessible par le réseau.
36	La limite d'utilisation de la ressource est atteinte	La limite d'utilisation d'une certaine ressource est atteinte.

Code	Erreur	Description
37	Différents points de montage	Tentative de récupérer un fichier qui nécessite son déplacement entre les répertoires du système de fichiers appartenant au points de montage différents.
38	Erreur de décompression	Impossible de décompresser l'archive (il est possible qu'elle soit protégée par un mot de passe ou endommagée).
40	La base virale est endommagée	Il est déterminé que les bases virales sont endommagées.
41	Version des bases virales non supportée	Il est déterminé que les bases virales existantes s'appliquent à l'ancienne version de l'application.
42	La base virale est vide	Il est déterminé que les bases virales sont vides.
43	L'objet ne peut pas être désinfecté	Tentative d'appliquer l'action **Désinfecter** à un objet incurable lors du traitement d'une menace.
44	Combinaison des bases virales non supportée	Il est déterminé que l'ensemble de bases virales est incompatible.
45	La limite de l'analyse est atteinte	Les limitations spécifiées sont dépassées lors du scan de l'objet (par exemple, la limitation de la taille du fichier décompressé, la limitation du niveau d'imbrication, etc.).
47	Identifiants d'utilisateur incorrects	Tentative d'authentification avec les identifiants d'utilisateur incorrects.
48	L'utilisateur ne possède pas les droits requis	Tentative d'authentification avec les identifiants de l'utilisateur ne possédant pas les droits requis.
49	Jeton d'accès invalide	Un composant du produit a présenté un jeton d'authentification incorrect lors d'une tentative d'accès à l'opération requérant des privilèges élevés.
60	Argument invalide	Un argument invalide a été indiqué lors de la tentative d'exécuter une commande.
61	Opération invalide	Tentative d'exécuter une commande invalide.
62	Les privilèges de super-utilisateur sont requis	Seul l'utilisateur possédant les privilèges de super-utilisateur peut effectuer l'action nécessaire.
63	N'est pas autorisé en mode de protection centralisée	L'action nécessaire peut être exécutée uniquement en mode de fonctionnement standalone.
64	OS non supporté	Le système d'exploitation installé sur l'hôte n'est pas supporté par le produit.
65	La fonctionnalité n'est pas implémentée	Tentatives d'utiliser des fonctions d'un composant qui ne sont pas implémentées dans la version actuelle.

Code	Erreur	Description
66	Paramètre inconnu	Le fichier de configuration contient les paramètres qui sont inconnus ou non supportés dans la version actuelle du produit.
67	Section inconnue	Le fichier de configuration contient les sections qui sont inconnues ou non supportées dans la version actuelle du produit.
68	Valeur de paramètre invalide	Un paramètre dans le fichier de configuration a une valeur invalide pour ce paramètre.
69	Statut invalide	Un composant ou tout le logiciel sont en état non valide pour l'exécution de l'opération demandée.
70	Une seule valeur est autorisée	Un paramètre dans le fichier de configuration a une liste de valeurs ce qui n'est pas autorisé pour ce paramètre.
71	Nom de balise invalide	Une section dans le fichier de configuration, dont le nom comporte l'identificateur-balise unique, a une valeur invalide de la balise.
80	Entrée introuvable	Lors de la tentative de consulter les informations sur la menace détectée, il est déterminé que les informations sont manquantes (il est probable que la menace a été déjà traitée par un autre composant du produit).
81	L'enregistrement est traité en ce moment	Lors de la tentative de consulter les informations sur la menace détectée, il est déterminé qu'elle est déjà traitée par un autre composant du produit.
82	Le fichier est déjà mis en quarantaine	Lors de la tentative de placer le fichier contenant la menace détectée en quarantaine, il est déterminé qu'il est déjà mis en quarantaine (il est fort probable que la menace a été déjà traitée par un autre composant du produit).
89	Impossible d'enregistrer la copie de sauvegarde avant la mise à jour	Impossible d'enregistrer la copie de sauvegarde des fichiers mis à jour avant le téléchargement des mises à jour depuis le serveur de mises à jour.
90	Fichier DRL invalide	Il est détecté que la structure d'un fichier de listes des serveurs de mises à jour est endommagée.
91	Fichier LST invalide	Il est détecté que la structure d'un fichier contenant la liste des bases virales mises à jour est endommagée.
92	Fichier compressé invalide	Il est déterminé que la structure du fichier téléchargé contenant des mises à jour est endommagée.
93	Erreur d'authentification sur le serveur proxy	Impossible de se connecter au serveur de mises à jour via le serveur proxy spécifié dans les paramètres.

Code	Erreur	Description
94	Aucun serveur de mise à jour disponible	Impossible de se connecter à aucun serveur de mises à jour.
95	Format de fichier clé invalide	Format de fichier clé corrompu.
96	La licence a expiré	Votre licence a expiré.
97	Le délai de l'opération réseau a expiré	Le délai de l'opération réseau a expiré.
98	Somme de contrôle incorrecte	Il est déterminé que la somme de contrôle du fichier téléchargé contenant des mises à jour est invalide.
99	Le fichier clé de démonstration est invalide	Le fichier clé de démonstration est invalide (par exemple, il a été obtenu pour un autre ordinateur).
100	Le fichier clé de licence est bloqué	La licence utilisée a été bloquée (il est probable que les termes du Contrat de licence d'utilisation du logiciel Dr.Web avaient été violés).
101	Licence invalide	La licence que vous utilisez est destinée à un autre produit ou elle ne contient pas d'autorisations nécessaires pour le fonctionnement des composants du produit installé.
102	Configuration incorrecte	Un des composants du produit ne peut pas fonctionner à cause des paramètres de configuration incorrects.
104	Fichier exécutable invalide	Un des composants du produit n'est pas lancé car le chemin d'accès a son fichier exécutable est incorrect ou le contenu du fichier est corrompu.
105	Le moteur Virus-Finding Engine n'est pas disponible	Le fichier du moteur antivirus Dr.Web Virus-Finding Engine (requis pour la recherche de menaces) est manquant ou indisponible.
106	Les bases virales n'existent pas	Il est déterminé que les bases virales sont manquantes.
107	Le processus est terminé à réception d'un signal	Le composant s'est arrêté (peut-être, à cause de l'inactivité ou suite à une commande de l'utilisateur).
108	Fin de processus inattendue	Le composant s'est arrêté brusquement suite à une panne.
109	Logiciel incompatible détecté	Le composant du produit ne peut pas fonctionner car un logiciel incompatible a été détecté.
112	Les bases des catégories de ressources web sont introuvables	Il est déterminé que les bases des catégories de ressources web sont introuvables.
113	Le module noyau Linux pour SpIDer Guard n'est pas	Le module noyau absent Linux est requis pour le fonctionnement de SpIDer Guard.

Code	Erreur	Description
	disponible	
117	SpIDer Gater n'est pas disponible	Le composant SpIDer Gate est manquant (nécessaire pour l'analyse de connexions réseau).
118	Le composant MailD n'est pas disponible	Le composant SpIDer Mail est manquant (nécessaire pour l'analyse de messagerie).
119	Scanning Engine n'est pas disponible	Impossible d'analyser les fichiers car le composant Scanning Engine est manquant ou qu'il a échoué à démarrer. Ce module est utilisé pour la recherche du contenu malveillant.
120	Le Scanner n'est pas disponible	Impossible d'analyser les fichiers car le composant Scanner, nécessaire pour l'analyse de fichiers, est manquant.
121	ES Agent n'est pas disponible	Le composant ESAgent est manquant (nécessaire pour la connexion au serveur de protection centralisée).
122	Le composant Firewall n'est pas disponible	Impossible de contrôler les connexions réseau car le composant Firewalll est manquant ou a échoué à démarrer. Le composant est utilisé pour le détournement des connexions.
123	Network Checker n'est pas disponible	Impossible de contrôler les connexions réseau car le module Network Checker est manquant ou a échoué à démarrer. Le module est utilisé pour la analyser des fichiers téléchargés via le réseau.
124	Le composant CloudD n'est pas disponible	Le composant CloudD est manquant (nécessaire pour accéder à Dr.Web Cloud).
125	Erreur inattendue	Une erreur imprévue s'est produite lors du fonctionnement d'un certain composant.

14.4. Support technique

En cas de problèmes liés à l'installation ou au fonctionnement des produits de la société, avant de contacter le support technique, essayez de trouver la solution par un des moyens suivants :

1. Consultez les dernières versions des descriptions et des manuels à l'adresse https://download.drweb.com/doc/.
2. Lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/.
3. Visitez des forums de Doctor Web à l'adresse https://forum.drweb.com/.

Si après avoir tout essayé, vous n'avez pas résolu le problème, utilisez un des moyens suivants pour contacter le support technique de Doctor Web :

1. Remplissez le formulaire de question dans la section correspondante de la rubrique https://support.drweb.com/.

2. Appelez le numéro de l'assistance technique française 0 825 300 230 ou le numéro de l'assistance internationale +7 (495) 789 45 86. Les utilisateurs en Russie peuvent nous contacter en appelant le numéro vert 8 800 333 7932.

Vous pouvez trouver les informations sur les bureaux régionaux de Doctor Web sur le site officiel à l'adresse https://company.drweb.com/contacts/offices/.

15. Paramètres généraux

Dans la section **Général**, vous pouvez configurer les notifications sonores, les notifications d'écran, rétablir les paramètres par défaut et configurer la journalisation pour générer le rapport pour le support technique.

Pour modifier les paramètres généraux, il ne faut pas entrer le nom d'utilisateur et le mot de passe. Les paramètres seront automatiquement modifiés pour tous les utilisateurs de Mac.

La configuration des notifications dans cette section est disponible uniquement sous macOS 10.14 et les versions antérieures. Dans les versions supérieures, elle se fait dans le menu **Préférences système** de votre Mac.

Notifications

Dr.Web utilise les notifications système de macOS pour afficher les messages sur la détection de menaces et leur neutralisation et les erreurs de fonctionnement des composants.

Pour désactiver les notifications

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Décochez la case **Activer les notifications**.

Notifications sonores

Dr.Web utilisent les notifications sonores pour signaler la détection de menaces, leur neutralisation et leur suppression.

Pour désactiver les notifications sonores

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Décochez la case **Utiliser les notifications sonores**.

Réinitialisation des paramètres par défaut

Si vous rencontrez des problèmes de fonctionnement de Dr.Web après la modification des paramètres, réinitialisez les paramètres par défaut. Dans ce cas, toutes les modifications de paramètres seront perdues.

Pour réinitialiser les paramètres par défaut

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Cliquez sur le bouton **Paramètres par défaut**.
5. Cliquez sur le bouton **Restaurer** pour confirmer la réinitialisation des paramètres initiaux de l'application.

Configuration de la journalisation

Activez la journalisation d'événements pour pouvoir générer le rapport d'événements pour le support technique.

Pour activer la journalisation

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Cochez la case **Activer l'enregistrement d'événements**.

Cette option permet d'attribuer aux événements des modules de Dr.Web une classification qui influencera les informations qui s'afficheront dans le rapport.

Pour configurer la classification d'événements des modules de Dr.Web dans le journal

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Cochez la case **Activer l'enregistrement d'événements**.
5. Cliquez sur le bouton **Configuration**.

6. Sélectionnez la classification nécessaire pour les événements de chaque module.
7. Cliquez sur **Enregistrer**.

Les événements des modules et des produits suivants sont disponibles dans la liste pour la configuration :

- ConfigD
- SpIDer Guard
- ScanningEngine
- FileCheck
- Firewall
- GateD
- NetCheck
- UrlCheck
- Dr.Web pour MacOS
- Module de mise à jour
- Agent Dr.Web

Le tableau ci-dessous contient les variantes possibles de classification des événements et leur descriptions.

Classification	Description
DEBUG	Description la plus détaillée des événements de débogage. Le rapport contient tous les messages possibles qui peuvent aider à résoudre le problème.
INFO	Le rapport contient tous les messages, y compris les messages informant du fonctionnement normal du système, du lancement de tâches planifiées, du lancement et de l'arrêt de services, des processus et des actions effectuées par l'utilisateur.
NOTICE	Tous les messages d'erreurs, les avertissement et les notifications s'affichent.
WARNING	Tous les avertissement et les messages d'erreur s'affichent.
ERROR	Seuls les messages d'erreurs sont affichés.

Configuration de l'accès au disque

Pour autoriser l'accès complet au disque

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .

2. Cliquez sur **Préférences système**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur  en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Accédez à la section **Sécurité et confidentialité**.
5. Accédez à la section **Confidentialité**.
6. Cliquez sur **Accès complet au disque**.
7. Ajoutez les modules de Dr.Web dans la liste d'applications autorisées.
8. Cliquez sur **Redémarrer**.

Sous macOS 13.0 et les versions antérieures

1. Dans la fenêtre principale de Dr.Web, cliquez sur  .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Cliquez sur **Autoriser**.
4. Cliquez sur **Ouvrir les Préférences système** dans le Gestionnaire d'accès au disque.
5. Dans la fenêtre d'instruction du Gestionnaire, cliquez sur la flèche jusqu'à ce que vous voyiez l'icône de Dr.Web.
6. Faites-glisser l'icône de Dr.Web du Gestionnaire d'accès au disque vers la section de préférences système indiquée dans le Gestionnaire.
7. Pour confirmer, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
8. Cliquez sur **Redémarrer** pour enregistrer les modifications.

Si le bouton **Autoriser** n'est pas actif, l'accès au disque est déjà autorisé.

16. Connexion aux services cloud

Dr.Web se connecte aux services cloud de la société Doctor Web pour protéger Mac contre les menaces récentes et améliorer le fonctionnement des composants de l'application. Les services cloud permettent de protéger les utilisateurs contre les fichiers infectés et les sites indésirables.

En fonction des paramètres de mise à jour des bases virales, les informations sur les menaces utilisées par votre Mac peuvent ne pas être à jour. Le traitement de données dans le service cloud se fait plus vite que la mise à jour des bases virales locales sur l'ordinateur.

De plus, les données anonymisées sur le fonctionnement des composants de Dr.Web sont automatiquement envoyées sur les serveurs de la société Doctor Web. Vous pouvez consulter la politique de confidentialité sur le site officiel de la société Doctor Web.

Pour se déconnecter des services cloud

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Dr.Web Cloud**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Désactivez l'option **Je veux me connecter aux services (recommandé)**.

17. Mode de protection centralisée

La protection centralisée de Mac est effectuée par l'administrateur du serveur Dr.Web Enterprise Security Suite ou le fournisseur IT à l'aide du service antivirus Dr.Web AV-Desk. Votre licence personnelle n'est pas utilisée en ce mode.

Préférences et composants

Les préférences et le fonctionnement des composants de Dr.Web peuvent être modifiés ou bloqués conformément à la politique de sécurité de l'entreprise ou à la liste des services payés. Le serveur de protection centralisée peut contrôler :

- Mise à jour de bases virales. Les mises à jour sont téléchargées automatiquement depuis le serveur de protection centralisée. En cas d'absence de connexion au serveur les mises à jour seront téléchargées par Internet depuis les serveurs de mises à jour Dr.Web.
- Protection permanente du système de fichiers.
- Analyse du trafic Web.
- Analyse antivirus de Mac. L'administrateur du réseau antivirus peut lancer une analyse distante de Mac manuellement depuis le serveur ou selon la planification.

Connexion de Mac

Chaque Mac avec Dr.Web installé est un poste à part. En fonction des paramètres d'authentification des postes sur le serveur de protection centralisée, vous pouvez vous connecter au réseau antivirus :

- Automatiquement, si le poste est déjà créé sur le serveur, c'est-à-dire, un identificateur et un mot de passe y sont attribués.
- En tant qu'un nouveau poste (novice). Dr.Web créera un nouvel identificateur du poste et un mot de passe. Dans ce cas, l'approbation du poste sur le serveur peut être nécessaire, ou bien le poste sera authentifié automatiquement si les paramètres d'accès au serveur le permettent.

Pour plus d'informations sur la connexion des postes au serveur de protection antivirus, referez-vous au **Manuel Administrateur de Dr.Web Enterprise Security Suite** et au **Manuel Administrateur de Dr.Web AV-Desk**.

Connexion automatique

Si vous avez acheté un abonnement pour le service antivirus Dr.Web AV-Desk, vous pouvez installer Dr.Web avec le fichier au format `.run` qui contient les paramètres de connexion au serveur. Contactez votre fournisseur IT pour obtenir le fichier `.run`.

Pour installer Dr.Web avec le fichier .run

1. Rendez le fichier obtenu `.run` exécutable.
2. Lancez le fichier `.run`.
3. Cliquez sur **Installer Dr.Web**.
4. Acceptez les termes du Contrat de licence. L'installation de l'application commence.
5. Entrez le mot de passe de l'administrateur et cliquez sur le bouton **Installer un logiciel complémentaire**.
6. Une fois l'avertissement **L'extension système est bloquée** affiché, autorisez le téléchargement des extensions système.
7. Dr.Web se copie dans le dossier **Applications** et se lance.
8. Accordez à Dr.Web le droit de l'accès complet au disque.

Pour rendre le fichier .run exécutable

1. Ouvrez **Terminal**.
2. Accédez au répertoire contenant le fichier .run :

```
cd <votre-répertoire>
```

3. Saisissez la commande suivante :

```
chmod 0755 <nom-de-fichier>.run
```

Exemple :

```
cd Desktop
chmod 0755 drweb-12.5.0-av-macosx.run
```

Pour autoriser le téléchargement d'extensions système

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Préférences système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur  en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
5. Cliquez sur **Autoriser** à côté du message de blocage du logiciel système de Doctor Web Ltd.

Sous macOS 11.0 et 12.0, cliquez sur **Avancé** et cochez les composants de Dr.Web.

Sous macOS 13.0 et 14.0

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Sécurité et confidentialité**.
4. Dans cette section trouvez la ligne **Certains logiciels système requièrent votre attention avant de pouvoir être utilisés** et cliquez sur **Détails** ci-dessous.
5. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
6. Basculez le commutateur contre les composants de Dr.Web sur la position Activé et cliquez sur **OK**.

Sous macOS 15.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Réglages système**.
3. Accédez à la section **Général** et sélectionnez **Ouverture et extensions**.
4. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions de sécurité de point de terminaison** et cliquez sur l'icône ⓘ qui se trouve à droite.
5. Basculez le commutateur **Dr.Web Spider** sur la position Activé et cliquez sur **Terminé**.
6. Dans la sous-section **Extensions**, trouvez la catégorie **Extensions du réseau** et cliquez sur l'icône ⓘ qui se trouve à droite.
7. Basculez le commutateur **Dr.Web Firewall** sur la position Activé et cliquez sur **Terminé**.

Pour autoriser l'accès complet au disque

Sous macOS 12.0 et les versions antérieures

1. Ouvrez le menu Apple .
2. Cliquez sur **Préférences système**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Accédez à la section **Sécurité et confidentialité**.
5. Accédez à la section **Confidentialité**.
6. Cliquez sur **Accès complet au disque**.

7. Ajoutez les modules de Dr.Web dans la liste d'applications autorisées.
8. Cliquez sur **Redémarrer**.

Sous macOS 13.0 et les versions antérieures

1. Dans la fenêtre principale de Dr.Web, cliquez sur  .
2. Dans la fenêtre **Préférences** sélectionnez la section **Général**.
3. Cliquez sur **Autoriser**.
4. Cliquez sur **Ouvrir les Préférences système** dans le Gestionnaire d'accès au disque.
5. Dans la fenêtre d'instruction du Gestionnaire, cliquez sur la flèche jusqu'à ce que vous voyiez l'icône de Dr.Web.
6. Faites-glisser l'icône de Dr.Web du Gestionnaire d'accès au disque vers la section de préférences système indiquée dans le Gestionnaire.
7. Pour confirmer, entrez le nom d'utilisateur et le mot de passe dans la fenêtre pop-up.
8. Cliquez sur **Redémarrer** pour enregistrer les modifications.

Si le bouton **Autoriser** n'est pas actif, l'accès au disque est déjà autorisé.

Si l'administrateur du réseau antivirus de votre entreprise ou le fournisseur IT a fourni le fichier de configuration au format `.cfg`, vous pouvez connecter Dr.Web dans la section **Activation de licence**. Les paramètres de connexion au serveur de protection centralisée seront configurés automatiquement.

Pour connecter un poste avec le fichier .cfg

1. Dans la fenêtre principale de Dr.Web, sélectionnez l'élément **Licence**.
2. Cliquez sur **Activer**.
3. Dans la fenêtre **Activation de licence**, ouvrez l'onglet **Fichiers d'activation**.
4. Faites glisser le fichier au format `.cfg` dans la zone pointillée ou cliquez pour sélectionner le fichier sur Mac.
5. Une fois l'activation terminée, les paramètres de connexion au Serveur seront configurés automatiquement.

Si l'administrateur du réseau antivirus de votre entreprise a fourni la clé de chiffrement publique au format `.pub` ou le certificat, vous pouvez configurer les paramètres de connexion manuellement.

Pour configurer manuellement les paramètres de connexion au serveur

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Mode**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Activez l'option **Activer le mode de protection centralisée**. En cas d'activation du mode de protection centralisée, les paramètres de la dernière connexion sont rétablis.
5. Indiquez l'adresse IP du serveur et le numéro du port qui est utilisé pour la connexion au serveur.
6. Faites glisser la clé de chiffrement publique au format `.pub` ou le certificat dans la zone pointillée ou double-cliquez pour sélectionner le fichier.
7. Ouvrez la sous-rubrique **Identification**.
8. Désactivez l'option **Se connecter en tant que novice**. Configurez les paramètres avancés pour l'authentification du poste :
   - identificateur du poste ;
   - mot de passe (attribué à votre ordinateur pour l'enregistrement sur le serveur) ;
   - mode de compression du trafic ;
   - mode de chiffrement du trafic.

   Les valeurs spécifiées sont enregistrées par la fonction Keychain. De ce fait, lors de la re-connexion au serveur vous n'aurez pas besoin de les ressaisir.
9. Cliquez sur **Se connecter**.

Connexion en tant que novice

Si l'administrateur n'a pas encore créé le poste sur le serveur, vous pouvez le connecter en tant que novice. Adressez-vous à l'administrateur du réseau antivirus de votre entreprise ou au fournisseur IT pour obtenir la clé de chiffrement publique ou le certificat et les paramètres de connexion au serveur de la protection centralisée.

Pour connecter un poste en tant que novice

1. Dans la fenêtre principale, cliquez sur .
2. Dans la fenêtre **Préférences** sélectionnez la section **Mode**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Activez l'option **Activer le mode de protection centralisée**.

5. Indiquez l'adresse IP du serveur et le numéro du port qui est utilisé pour la connexion au serveur.
6. Faites glisser la clé de chiffrement publique `.pub` ou le certificat dans la zone pointillée ou double-cliquez pour sélectionner le fichier.
7. Assurez-vous que l'option **Se connecter en tant que novice** est activée dans la sous-rubrique **Identification**.
8. Cliquez sur **Se connecter**.

Mode autonome

Vous pouvez désactiver le mode de protection centralisée et restaurer le fonctionnement autonome de Dr.Web.

Lorsque le mode autonome est activé, tous les paramètres de l'application sont restaurés à leur configuration précédente avant le passage en mode centralisé ou réinitialisés par défaut. L'accès à tous les composants de Dr.Web est également restauré.

Pour le fonctionnement en mode autonome, un fichier clé valide est requis. En ce mode, il est impossible d'utiliser la licence obtenue automatiquement depuis le serveur de protection centralisée. Si cela est nécessaire, activez la licence personnelle.

Pour rétablir le mode autonome

1. Dans la fenêtre principale, cliquez sur  .
2. Dans la fenêtre **Préférences** sélectionnez la section **Mode**.
3. Si les paramètres ne sont pas disponibles, débloquez-les. Pour ce faire, cliquez sur  en bas de la fenêtre et entrez le nom d'utilisateur et le mot de passe.
4. Désactivez l'option **Activer le mode de protection centralisée**.
5. Confirmez l'action en cliquant sur le bouton **Désactiver**.

18. Informations de référence

18.1. Protection centralisée et réseau antivirus

Les solutions de la société Doctor Web pour la protection antivirus centralisée permettent d'automatiser et de simplifier la configuration et la gestion de la sécurité informatique des ordinateurs organisés dans une structure logique (par exemple, des ordinateurs d'entreprise dans un réseau local, ainsi qu'en dehors). Les ordinateurs protégés sont réunis dans un *réseau antivirus* dont la sécurité est gérée par des administrateurs depuis le serveur central. La connexion aux systèmes de protection centralisée assure un haut niveau de la protection de l'ordinateur avec des efforts minimaux du côté des utilisateurs finaux.

Interaction des composants du réseau antivirus

Les solutions de Doctor Web pour la protection centralisée sont basées sur l'architecture *client-serveur* (voir la figure ci-dessous).

Les ordinateurs d'entreprise ou des utilisateurs des services IT sont protégés des menaces et du spam par les *composants* antivirus locaux (les clients ; ici – Dr.Web) qui assurent la protection antivirus et fournissent une connexion au serveur de protection centralisée.

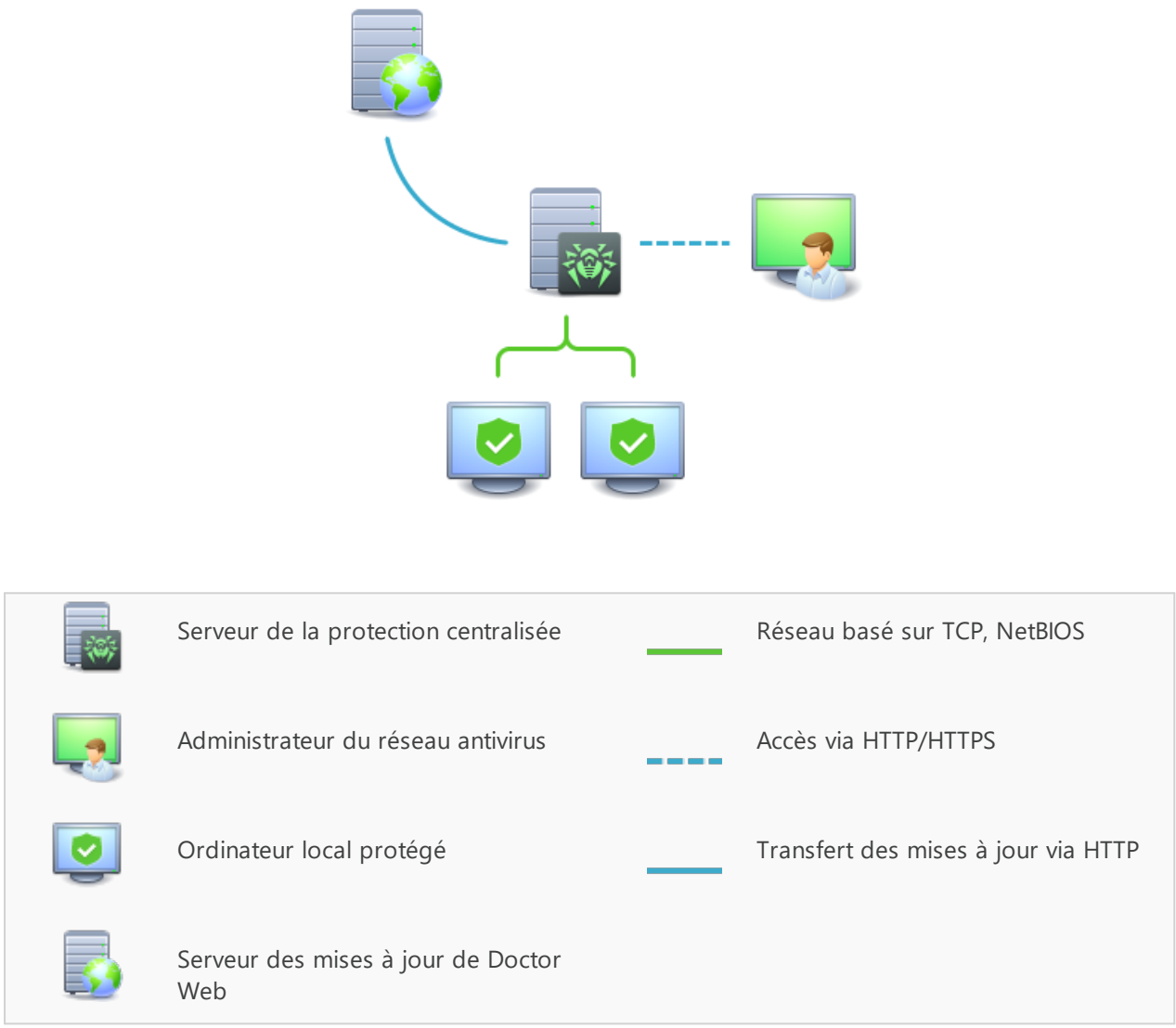

Figure 1. Structure logique du réseau antivirus

Les ordinateurs locaux sont mis à jour et configurés depuis le *serveur central*. Le flux de commandes, de données et des statistiques dans le réseau antivirus passe par le serveur de protection centralisée. Le trafic entre les ordinateurs protégés et le serveur antivirus peut être considérable, c'est pourquoi le réseau antivirus permet de le compresser. Le chiffrement de données est utilisé afin d'éviter une fuite de données importantes et une substitution des logiciels installés sur les ordinateurs protégés.

Toutes les mises à jour nécessaires sont téléchargées sur le serveur de protection centralisée du serveur de mises à jour de la société Doctor Web.

Les composants antivirus locaux sont configurés et gérés depuis le serveur antivirus selon les commandes des *administrateurs du réseaux antivirus*. Les administrateurs gèrent la configuration du serveur de protection centralisée et la formation du réseau antivirus (notamment, ils ap-

prouvent la validité des connexions des postes locaux au réseau) et, si nécessaire, ils spécifient les paramètres des composants antivirus locaux.

Les composants antivirus locaux ne sont pas compatibles avec d'autres logiciels antivirus, y compris les produits Dr.Web qui ne supportent pas le mode de protection centralisée. L'installation de deux logiciels antivirus sur le même ordinateur peut entraîner un crash système et une perte de données importantes.

Solutions pour la protection centralisée

Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite est une solution antivirus pour des réseaux d'entreprise de toute taille qui assure une protection fiable des postes de travail, ainsi que des serveurs de fichiers et de messagerie contre tous les types des menaces dans des entreprises de toute taille. Ce produit fournit aux administrateurs des réseaux d'entreprise un ensemble des outils permettant de contrôler et de gérer les composants antivirus installés, y compris le déploiement, les mises à jour des bases virales de Dr.Web et de composants du logiciel, le suivi du réseau, les notifications sur les événements viraux et la collecte des statistiques.

Service Internet Dr.Web AV-Desk

Dr.Web AV-Desk est un service de sécurité novateur de Doctor Web destiné aux prestataires de services Internet. Avec ce service Internet, les prestataires peuvent fournir à ses utilisateurs (les particuliers ou les entreprises) des services de protection informatique contre les virus, le spam et les autres menaces. Pour bénéficier de ces services le client doit souscrire à un abonnement pour une période nécessaire. Les services sont fournis en ligne.

Pour en savoir plus sur le service Internet Dr.Web AV-Desk, consultez le site de Doctor Web à l'adresse suivante : https://www.av-desk.com/.

18.2. Types de menaces

Par le terme *« menace »*, il faut entendre, selon notre classification, un logiciel qui peut porter atteinte soit directement soit indirectement à l'ordinateur, au réseau, aux informations ou aux droits de l'utilisateur (logiciels malveillants ou indésirables). Dans le sens plus large du terme, une « menace » peut signifier un danger potentiel pour l'ordinateur ou pour le réseau (vulnérabilités et possibilités d'attaques).

Tous les types de logiciels décrits ci-dessous peuvent présenter un danger pour les données de l'utilisateur et pour son droit à la confidentialité. Les logiciels qui ne dissimulent pas leur présence dans le système (par exemple, certains logiciels pour diffusion du spam ou analyseurs

du trafic), ne sont pas d'ordinaire classés comme menaces, mais sous certaines conditions, ils peuvent aussi causer des dommages à l'utilisateur.

Virus informatiques

Ce type de menaces informatiques est capable d'introduire son code dans le code d'exécution d'autres logiciels. Cette pénétration porte le nom d'*infection*. Dans la plupart des cas, le fichier infecté devient lui-même porteur de virus et le code introduit n'est pas obligatoirement conforme à l'original. La grande partie des virus est conçue pour détériorer ou détruire les données.

En fonction du type de fichiers infectés, Doctor Web classifie les virus selon les types suivants :

- *Virus de fichier* infectent les fichiers de système d'exploitation (fichiers exécutables, fichiers dll). Ces virus sont activés lors de l'accès au fichier infecté.
- Les *macrovirus* infectent les documents utilisés par les logiciels de Microsoft® Office et d'autres programmes utilisant des commandes macros généralement écrits en Visual Basic. Les *macros*, ce sont des logiciels internes, écrits en langage de programmation totalement fonctionnel qui sont automatiquement lancés sous les conditions déterminées (par exemple, dans Microsoft® Word, quand vous ouvrez, fermez ou enregistrez un document).
- Les *virus script* sont écrits en langages de script (langages des scénarios). Ils infectent, dans la plupart des cas, les autres fichiers script (par exemple, les fichiers du système d'exploitation). Ils peuvent infecter aussi d'autres types de fichiers qui supportent l'exécution des scripts, tout en se servant des scripts vulnérables des applications Web.
- Les *virus de téléchargement* infectent les secteurs d'amorçage des disques et des partitions aussi bien que les principaux secteurs d'amorçage des disques durs. Ils occupent peu de mémoire et restent prêts à remplir leurs fonctions jusqu'à ce qu'un déchargement, un redémarrage ou un arrêt du système ne soit effectué.

La plupart des virus possèdent des mécanismes spécifiques pour se dissimuler dans le système. Leurs méthodes de protection contre la détection s'améliorent sans cesse. Cependant, dans le même temps, de nouveaux moyens d'élimination de cette protection apparaissent. On peut également subdiviser les virus d'après leur protection contre la détection :

- Les *virus cryptés* chiffrent leur code à chaque infection pour éviter leur détection dans un fichier, dans la mémoire ou un secteur d'amorçage. Chaque exemplaire d'un tel virus contient un ensemble commun de caractères (la procédure de déchiffrement) qui constitue la signature du virus.
- *Les virus polymorphes* cryptent également leur code, mais ils génèrent en plus une procédure de décryptage spéciale différente dans chaque copie de virus. Ceci signifie que de tels virus n'ont pas de signatures.
- Les *virus furtifs* agissent de telle façon qu'ils masquent leur activité et cachent leur présence dans les objets infectés. Ces virus captent les caractéristiques d'un objet avant de l'infecter et présentent ensuite ces anciennes caractéristiques au système d'exploitation ou à un programme cherchant à dépister des fichiers modifiés.

Les virus peuvent également être classifiés selon le langage de programmation en lequel ils sont écrits (dans la plupart des cas, il sont écrits en assembleur, mais il existe des virus qui sont écrits en langages de programmation de haut niveau, en langages de script, etc.) ou selon les systèmes d'exploitation qu'ils ciblent.

Vers d'ordinateurs

Ce dernier temps, les logiciels malveillants de type « ver informatique » sont devenus beaucoup plus répandus que les virus et les autres logiciels malveillants. Comme les virus, ils sont capables de créer leurs copies mais ils n'infectent pas d'autres objets. Un ver infiltre un ordinateur via le réseau (généralement sous forme d'une pièce jointe dans les messages e-mail ou via Internet) et distribue ses copies fonctionnelles sur d'autres ordinateurs. Pour se propager, les vers peuvent profiter des actions de l'utilisateur ou choisir un poste à attaquer de manière automatique.

Les vers ne consistent pas forcément en un seul fichier (le corps du ver). La plupart d'entre eux comportent une partie infectieuse (le shellcode) qui se charge dans la mémoire vive de l'ordinateur, puis télécharge le corps du ver via le réseau sous forme d'un fichier exécutable. Tant que le système n'est pas encore infecté par le corps du ver, vous pouvez régler le problème en redémarrant l'ordinateur (et la mémoire vive est déchargée et remise à zéro). Mais aussitôt que le corps du ver entre dans le système, seul l'antivirus peut le désinfecter.

A cause de leur propagation intense, les vers peuvent mettre hors service des réseaux entiers, même s'ils n'endommagent pas directement le système.

Doctor Web divise les vers d'après leur mode de propagation :

- Les *vers de réseau* se propagent à l'aide de différents protocoles réseau ou protocoles d'échanges de fichiers.
- Les *vers de courrier* se propagent via les protocoles de courrier (POP3, SMTP, etc.).
- Les *vers de tchats* se propagent à l'aide de logiciels de messagerie instantanée (ICQ, IM, IRC, etc.).

Chevaux de Troie

Ce type de logiciels malveillants ne peut pas se répliquer. Un trojan remplace un programme souvent lancé et exécute ses fonctions (ou imite l'exécution de ces fonctions). En même temps, un Trojan effectue des actions malveillantes (endommage ou supprime des données, envoie des informations confidentielles, etc.) ou rend possible l'accès d'un cybercriminel à l'ordinateur afin de nuire à de tierces personnes.

Le masquage de trojans et les fonctions malveillantes sont similaires à ceux d'un virus et peuvent même être un composant de virus. Cependant, la plupart des trojans sont diffusés comme des fichiers exécutables séparés (via des serveurs d'échanges de fichiers, des supports amovibles ou des pièces jointes), qui sont lancés par l'utilisateur ou par une tâche système.

Il est difficile de classifier les trojans car ils sont souvent diffusés par des virus ou des vers mais également parce que beaucoup d'actions malveillantes pouvant être effectuées par d'autres types de menaces sont imputées aux trojans uniquement. Vous trouverez ci-dessous une liste de certains types de trojans qui sont classés à part par les spécialistes de Doctor Web :

- *Backdoors* : ce sont des programmes de Troie qui offrent un accès privilégié au système, contournant le mécanisme existant d'accès et de protection. Les backdoors n'infectent pas les fichiers, mais ils s'inscrivent dans le registre, en modifiant les clés.
- *Rootkits* : ils sont destinés à intercepter les fonctions du système d'exploitation pour dissimuler leur présence dans le système. En outre, le rootkit peut masquer les processus des autres logiciels, des clés de registre, des fichiers et des dossiers. Le rootkit se propage comme un logiciel indépendant ou comme un composant supplémentaire d'un autre logiciel malveillant. Selon le principe de leur fonctionnement, les rootkits sont divisés en deux groupes : les rootkits qui fonctionnent en mode utilisateur (interception des fonctions des bibliothèques du mode utilisateur) *(User Mode Rootkits – UMR)*, et les rootkits qui fonctionnent en mode noyau (interception des fonctions au niveau du noyau système, ce qui rend toute détection et toute désinfection très difficile) *(Kernel Mode Rootkits – KMR)*.
- *Enregistreurs de frappe (keyloggers)* : ils sont utilisés pour collecter les données que l'utilisateur entre avec son clavier. Le but de ces actions est le vol de toute information personnelle (mots de passe, logins, numéros de cartes bancaires etc.).
- *Clickers* : ils redirigent les liens quand on clique dessus. D'ordinaire, l'utilisateur est redirigé vers des sites déterminés (probablement malveillants) avec le but d'augmenter le trafic publicitaire des sites web ou pour organiser des attaques par déni de service (attaques DDoS).
- *Trojans proxy* : ils offrent au cybercriminel l'accès anonyme à Internet via l'ordinateur de la victime.

Outre les actions listées ci-dessus, les programmes de Troie peuvent exécuter d'autres actions malveillantes, par exemple, changer la page d'accueil dans le navigateur web ou bien supprimer certains fichiers. Mais ces actions peuvent être aussi exécutées par les menaces d'autres types (par exemple, virus et vers).

Hacktools

Les hacktools sont créés pour aider les hackers. Les logiciels de ce type les plus répandus sont des scanners de ports qui permettent de détecter les vulnérabilités des pare-feux (firewalls) et des autres composants qui assurent la sécurité informatique de l'ordinateur. Ces instruments peuvent également être utilisés par les administrateurs pour vérifier la solidité de leurs réseaux. Parfois, les logiciels utilisant les méthodes de l'ingénierie sociale sont aussi considérés comme hacktools.

Adwares

Sous ce terme, on désigne le plus souvent un code interne des logiciels gratuits qui impose l'affichage d'une publicité sur l'ordinateur de l'utilisateur. Mais parfois, ce code peut être diffusé par d'autres logiciels malveillants et afficher la publicité, par exemple, sur des navigateurs In-

ternet. Très souvent, ces logiciels publicitaires fonctionnent en utilisant la base de données collectées par des logiciels espions.

Canulars

Comme les adwares, ce type de programme malveillant ne provoque pas de dommage direct au système. Habituellement, les canulars génèrent des alertes sur des erreurs qui n'ont jamais eu lieu et effraient l'utilisateur afin qu'il effectue des actions qui conduiront à la perte de données. Leur objectif est d'effrayer ou de déranger l'utilisateur.

Dialers

Ce sont de petites applications installées sur les ordinateurs, élaborées spécialement pour scanner un certain spectre de numéros de téléphone. Par la suite, les cybercriminels utiliseront les numéros trouvés pour prélever de l'argent à leur victime ou pour connecter l'utilisateur à des services téléphoniques surtaxés et coûteux.

Riskwares

Ces logiciels ne sont pas créés pour endommager le système, mais à cause de leurs particularités, ils peuvent présenter une menace pour la sécurité du système. Ces logiciels peuvent non seulement endommager les données ou les supprimer par hasard, mais ils peuvent également être utilisés par des hackers ou par d'autres logiciels pirates pour nuire au système. Les logiciels de communication ou d'administration à distance, les serveurs FTP etc. peuvent être considérés comme potentiellement dangereux.

Objets suspects

Ce sont des menaces potentielles détectées à l'aide de l'analyse heuristique. Ces objets peuvent appartenir à un des types de menaces informatiques (même inconnues pour les spécialistes de la sécurité informatique) ou être absolument inoffensifs, en cas de faux positif. En tous cas, il est recommandé de placer les fichiers contenant des objets suspects en quarantaine et envoyer pour analyse aux spécialistes du laboratoire antivirus de l'entreprise Doctor Web.

18.3. Méthodes de détection des menaces

Tous les produits antivirus créés par Doctor Web utilisent l'ensemble de méthodes de détection de menaces, ce qui permet d'analyser les objets suspects de manière approfondie.

Analyse par signatures

Cette méthode de détection est appliquée en première. Elle est basée sur la recherche des signatures des menaces connues dans le contenu de l'objet analysé. Une signature est une

séquence continue et finie d'octets qui est nécessaire et suffisante pour identifier une menace. Pour réduire la taille de la base de signatures, les solutions antivirus Dr.Web utilisent des sommes de contrôle de signatures au lieu de séquences complètes de signatures. Les sommes de contrôle identifient les signatures de manière unique, ce qui garantit l'exactitude de la détection de virus et leur neutralisation. Les bases de données virales Dr.Web sont faites de telle sorte que certaines entrées peuvent être utilisées pour détecter non seulement un virus, mais des classes entières ou des familles de menaces.

Origins Tracing

C'est un algorithme unique de Dr.Web permettant de détecter un comportement malveillant et de nouvelles menaces, ainsi que des menaces modifiées utilisant des mécanismes connus et décrits dans les bases virales. Cette technologie intervient à la fin de la recherche par signatures et assure la protection des utilisateurs utilisant les solutions antivirus Dr.Web contre des menaces telles que Trojan.Encoder.18 (également connu sous le nom « gpcode »). En outre, l'utilisation de la technologie Origins Tracing peut réduire considérablement le nombre de faux positifs de l'analyseur heuristique. Le postfix `.Origin` est ajouté aux noms des menaces détectées à l'aide de la technologie Origins Tracing.

Émulation d'exécution

La méthode d'émulation du code logiciel est utilisée pour la détection des virus polymorphes et chiffrés, lorsque l'utilisation de l'analyse par signatures est impossible ou bien, elle devient compliquée, car la création de signatures fiables devient impossible. La méthode consiste en une imitation du code, analysé à l'aide de l'*émulateur* (logiciel qui reproduit le modèle du processeur et de l'environnement d'exécution de programmes). L'émulateur opère avec la partie protégée de la mémoire *(tampon d'émulation)*. Les instructions ne sont alors pas transmises au processeur central pour leur réelle exécution. Si le code traité par l'émulateur est infecté par un virus, le corps de virus sera déchiffré. Ensuite, ce corps de virus sera détecté sans problèmes par la méthode de l'analyse par signatures.

Analyse heuristique

Le fonctionnement de l'analyseur heuristique est fondé sur un ensemble d'*heuristiques* (hypothèses, dont la signification statistique est confirmée par l'expérience) des signes caractéristiques de logiciels malveillants et, inversement, le code exécutable sécurisé. Chaque attribut ou caractéristique du code possède un score (le nombre indiquant l'importance et la validité de cette caractéristique). Le score peut être positif si l'attribut indique la présence d'un comportement de code malveillant, et négatif si l'attribut ne correspond pas à une menace informatique. En fonction du score total du contenu du fichier, l'analyseur heuristique calcule la probabilité de la présence d'un objet malveillant inconnu. Si cette probabilité dépasse une certaine valeur de seuil, l'objet analysé est considéré comme malveillant.

L'analyseur heuristique utilise également la technologie FLY-CODE – un algorithme universel pour l'extraction des fichiers. Ce mécanisme permet de construire des hypothèses heuristiques

sur la présence d'objets malveillants dans les objets compressés par des outils de compression (packers), non seulement par des outils connus des développeurs des produits Dr.Web, mais également par des outils de compression nouveaux et inexplorés. Lors de l'analyse des objets emballés, une technologie d'analyse de leur entropie structurelle est également utilisée, cette technologie permet de détecter les menaces grâce aux spécificités de la localisation des fragments de leur code. Cette technologie permet avec une seule entrée de la base virale de détecter un ensemble de différents types de menaces qui sont emballées par le même packer polymorphe.

Comme tout système basé sur des hypothèses, l'analyseur heuristique peut commettre des erreurs de type I (omettre une menace inconnue) ou II (faire un faux positif). Par conséquent, les objets marqués par l'analyseur heuristique comme « malveillants » reçoivent le statut « suspects ».

Méthode de l'apprentissage machine

Elle est utilisée pour rechercher et neutraliser les objets malveillant qui ne sont pas encore inclus dans les bases virales. L'avantage de cette méthode est que le code malveillant est détecté en fonction de ses caractéristiques, sans être exécuté.

La détection de menaces est basée sur la classification des objets malveillants par les caractéristiques particulières. La technologie de l'apprentissage machine est basée sur les machines à vecteurs de support et elle permet d'effectuer la classification et l'enregistrement des fragments du code de langages de script dans la base. Ensuite, les objets détectés sont analysés pour leur conformité aux caractéristiques du code malveillant. La technologie de l'apprentissage machine met à jour automatiquement la liste des caractéristiques et les bases virales. Grâce à la connexion au service cloud, de grands volumes de données sont traités plus vite et l'apprentissage constant du système assure la protection préventive contre les menaces les plus récentes. De plus, la technologie peut fonctionner sans la connexion permanente au cloud.

La méthode de l'apprentissage machine économise les ressources du système d'exploitation car elle ne nécessite pas l'exécution du code pour détecter des menaces et l'apprentissage machine dynamique peut s'effectuer sans la mise à jour permanente de bases virales comme c'est le cas de l'analyse de signatures.

Technologies cloud de détection de menaces

Les méthodes cloud de détection permettent d'analyser n'importe quel objet (fichier, application, extension pour le navigateur, etc.) par la somme de contrôle. La somme de contrôle est une séquence de lettres et chiffres de la longueur spécifiée. Lors de l'analyse par la somme de contrôle les objets sont vérifiés dans la base existante et puis, ils sont classés en catégories : sains, suspects, malveillants, etc.

Une telle technologie réduit le temps de l'analyse des fichiers et économise les ressources de l'appareil. Vu que c'est la somme de contrôle unique qui est analysée et non pas l'objet, la dé-

cision est prise tout de suite. S'il n'y a pas de connexion aux serveurs Dr.Web, les fichiers sont analysés de manière locale et l'analyse cloud est reprise après la restauration de la connexion.

Ainsi, le service cloud de la société Doctor Web collecte les informations sur de multiples utilisateurs et met à jour rapidement les données sur les menaces inconnues auparavant ce qui augmente l'efficacité de la protection des appareils.

18.4. Raccourcis clavier

Vous pouvez utiliser les raccourcis clavier pour lancer une analyse, appliquer les actions aux menaces détectées et configurer les paramètres de Dr.Web :

Raccourci clavier		**Action**
Actions appliquées aux menaces	COMMANDE + MAJ + C	Désinfecter la menace
	COMMANDE + MAJ + M	Mettre la menace en quarantaine
	COMMANDE + MAJ + I	Ignorer la menace
	COMMANDE + MAJ + D	Supprimer la menace
	COMMANDE + MAJ + R	Restaurer la menace
	COMMANDE + MAJ + P	Sélectionnez le dossier dans lequel il faut restaurer la menace
Général	COMMANDE + A	Sélectionner tout
	COMMANDE + W	Fermer