Dr.WEB

Antivirus pour Windows

Manuel Utilisateur

Antivirus Dr.Web pour Windows
Version 12.0
Manuel Utilisateur
23/09/2021

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. Introduction

Ce manuel décrit l'installation du produit Antivirus Dr.Web pour Windows et contient des conseils sur son utilisation et sur la résolution des problèmes les plus courants causés par les menaces virales. Il décrit principalement les modes de fonctionnement standard des composants de Dr.Web (avec les paramètres par défaut).

Les Annexes contiennent des informations de référence générales ainsi que les paramètres avancés pour la configuration du logiciel Dr.Web, destinés aux utilisateurs expérimentés.

1.1. Conventions et abréviations

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.
`C:\Windows\`	Noms de fichiers/dossiers ou fragments de programme.
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

Abréviations

Dans ce Manuel les abréviations suivantes sont utilisées sans définition du terme :

- Dr.Web : Antivirus Dr.Web pour Windows ;
- FTP (File Transfer Protocol) : protocole de transfert de fichiers ;
- HTTP (Hypertext Transfer Protocol) : protocole de transfert hypertexte ;

- IMAP (Internet Message Access Protocol) : protocole permettant l'accès direct aux messages sur un serveur de messagerie ;
- IMAPS (Internet Message Access Protocol Secure) : protocole sécurisé permettant l'accès direct aux messages sur un serveur de messagerie ;
- MTU (Maximum Transmission Unit) : unité de transmission maximale ;
- NNTP (Network News Transfer Protocol) : protocole réseau de transfert de nouvelles ;
- OS : système d'exploitation ;
- POP3 (Post Office Protocol Version 3) : protocole sécurisé de bureau de poste, version 3 ;
- POP3S (Post Office Protocol Version 3 Secure) : protocole sécurisé de bureau de poste, version 3 ;
- SIP (Session Initiation Protocol) : protocole d'ouverture de session ;
- SMTPS (Simple Mail Transfer Protocol Secure) : protocole simple et sécurisé de transfert de courrier ;
- SSL (Secure Sockets Layer) : couche des sockets sécurisés ;
- TCP (Transmission Control Protocol) : protocole de contrôle de transmission ;
- TLS (Transport Layer Security) : protocole de sécurité de la couche de transport ;
- UAC (User Account Control) : contrôle des comptes des utilisateurs ;
- UNC (Uniform Naming Convention) : convention de dénomination uniforme ;
- URL (Uniform Resource Locator) : localisateur uniforme de ressource.

2. A propos de

Antivirus Dr.Web pour Windows est destiné à protéger la mémoire système, les disques durs et les supports amovibles tournant sous les OS de la famille Windows contre les menaces de tout type : virus, rootkits, Trojans, spywares, adwares, hacktools et d'autres objets malveillants provenant de sources externes.

Antivirus Dr.Web pour Windows est composé de plusieurs modules responsables des fonctions différentes. Le moteur antivirus et les bases virales sont communs pour tous les composants et les plateformes différentes.

Les composants du produit sont constamment mis à jour, les bases virales, les bases des catégories de ressources web et les bases des règles de filtrage antispam de messages e-mail sont régulièrement complétées par les signatures de virus. La mise à jour permanente assure un niveau pertinent de la protection des appareil de l'utilisateur, ainsi que des applications et des données. Pour une protection supplémentaire contre des logiciels malveillants, on utilise les méthodes d'analyse heuristique réalisées dans le moteur antivirus.

Antivirus Dr.Web pour Windows peut détecter et supprimer les programmes indésirables (adwares, dialers, canulars, riskwares et hacktools) de votre ordinateur. Dr.Web utilise ses composants antivirus standard pour détecter ces programmes et appliquer des actions aux fichiers qui les contiennent.

Sur la page **Support** de la section A propos du logiciel, vous pouvez trouver les informations sur la version du produit, l'ensemble de composants, la date de la dernière mise à jour.

2.1. Composants de protection et modules de gestion

Antivirus Dr.Web pour Windows comprend les composants de protection et les modules de gestion suivants :

Composant/module	Description
SpIDer Guard	Composant qui réside toujours en mémoire vive. Il analyse les processus lancés et les fichiers créés et détecte toute activité malveillante.
SpIDer Mail	Composant qui intercepte toutes les requêtes de clients de messagerie aux serveurs de messagerie via les protocoles POP3/SMTP/IMAP4/NNTP (sous IMAP4 on comprend le protocole IMAPv4rev1). Il détecte et neutralise les menaces avant que les messages soient reçus par le client de messagerie depuis le serveur ou avant qu'ils soient envoyés sur le serveur de messagerie.
Pare-feu Dr.Web	Pare-feu personnel qui protège l'ordinateur d'un accès non autorisé et prévient la perte de données vitales via le réseau.

Composant/module	Description
Analyse de comportement	Composant contrôlant l'accès aux objets importants du système et assurant l'intégrité des applications lancées.
Protection contre les exploits	Composant bloquant les objets malveillants qui utilisent des vulnérabilités d'applications.
Protection contre les ransomwares	Composant assurant la protection contre les ransomwares.
Scanner	Scanner avec une interface graphique, lancé sur demande de l'utilisateur ou selon la planification. Il effectue une analyse antivirus de l'ordinateur.
Scanner en ligne de commande Dr.Web	Version du Scanner avec l'interface de la ligne de commande.
Dr.Web pour Microsoft Outlook	Plug-in qui analyse les boîtes mail Microsoft Outlook pour la présence de menaces.
Module de mise à jour	Il permet aux utilisateurs enregistrés de recevoir et d'installer automatiquement des mises à jour des bases virales et des modules Dr.Web.
SpIDer Agent	Module qui vous aide à configurer et à gérer les composants du produit antivirus.

2.2. Méthode de détection des menaces

Toutes les solutions antivirus créées par Doctor Web utilisent un ensemble de méthodes de détection, ce qui leur permet d'effectuer des analyses en profondeur des fichiers suspects.

Analyse de signature

Cette méthode de détection est appliquée en premier lieu. Elle est basée sur la recherche des signatures de 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. La comparaison du contenu de l'objet avec les signatures n'est pas effectuée directement, mais par leur sommes de contrôle ce qui permet de réduire considérablement la taille des entrées dans les bases de données virales tout en préservant le caractère unique de la conformité et par conséquent, l'exactitude de la détection des menaces et du traitement des objets infectés. Les entrées dans les bases virales Dr.Web sont rédigées de sorte que la même entrée peut détecter des classes entières ou des familles de menaces.

Origins Tracing

Cette une technologie unique Dr.Web permettant de détecter les nouvelles menaces ou les menaces modifiées et utilisant des mécanismes de contamination ou un comportement malveillant qui sont déjà connus de la base de données virale. Cette technologie intervient à la fin de l'analyse par signature et assure une protection des utilisateurs utilisant des solutions antivirus Dr.Web contre les 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. Les noms des menaces détectées à l'aide d'Origins Tracing sont complétés par `.Origin`.

Émulation de l'exécution

La méthode d'émulation d'exécution de code est utilisée pour détecter les virus polymorphes et cryptés si la recherche à l'aide des sommes de contrôle des signatures est inapplicable ou très compliquée en raison de l'impossibilité de construire des signatures fiables. La méthode consiste à simuler l'exécution du code en utilisant l'*émulateur* — un modèle du processeur et de l'environnement du programme. L'Émulateur fonctionne avec un espace mémoire protégé (*tampon d'émulation*). Dans ce cas, les instructions ne sont pas transmises au processeur central pour exécution réelle. Si le code traité par l'émulateur est infecté, alors le résultat de son émulation est un rétablissement du code malveillant d'origine disponible pour une analyse de signature.

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 code malveillant et, inversement, de 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 le signe indique la présence d'un comportement de code malveillant, et négatif si le signe 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 (emballeurs). De plus il ne s'agit pas seulement des outils connus par les développeurs des produits Dr.Web, mais également 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 par les spécificités de la localisation des fragments de leur code. Grâce à une seule entrée de la base de données, la technologie permet 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 de type II (faire un faux positif). Par conséquent, les objets marqués par l'analyseur heuristique comme « malveillants » reçoivent le statut « suspects ».

Analyse de comportement

Les techniques de l'analyse de comportement permettent d'analyser la cohérence des actions de tous les processus du système. Si une application se comporte comme un programme malveillant, ses actions seront bloquées.

Dr.Web Process Heuristic

La technologie de l'analyse de comportement Dr.Web Process Heuristic protège contre les nouveaux programmes les plus dangereux qui sont capables d'éviter la détection par les moyens traditionnels : le mécanisme de signatures et le mécanisme heuristique.

Dr.Web Process Heuristic analyse le comportement de chaque programme lancé en consultant le service cloud Dr.Web qui est mis à jour constamment. Dr.Web Process Heuristic se base sur les connaissances actuelles de comportement des programmes malveillants, il évalue le niveau de danger et prend les mesures nécessaires afin de neutraliser la menace. Le préfixe `DPH` est ajouté aux noms des menaces détectées grâce à Dr.Web Process Heuristic.

Cette technologie permet de minimiser les pertes dues à l'action d'un virus inconnu — en cas de consommation minimum des ressources du système à protéger.

Dr.Web Process Heuristic contrôle toutes les tentatives de modifier le système :

- il identifie les processus de programmes malveillants qui modifient des fichiers utilisateur d'une manière indésirable (par exemple, les tentatives de chiffrements de la part des Trojans-encodeurs), y compris les fichiers se trouvant dans des répertoires accessibles par le réseau ;
- il empêche les tentatives de programmes malveillants de s'infiltrer dans des processus d'autres applications ;
- il protège les zones critiques du système contre les modifications par les programmes malveillants ;
- il détecte et arrête des scripts et des processus malveillants, suspects et peu fiables ;
- il bloque la possibilité de modifier les zones d'amorçage du disque par les programmes malveillants afin d'éviter le lancement (par exemple, d'un bootkit) sur l'ordinateur ;
- il prévient la désactivation de la mode sécurisée Windows en bloquant les modification du registre ;
- il n'autorise pas aux programmes malveillants de modifier les règles de lancement de programmes ;
- il bloque les téléchargements de nouveaux pilotes ou de pilotes inconnus qui sont lancés sans avertissement de l'utilisateur ;

- il bloque l'autodémarrage de programmes malveillants et des applications particulières, par exemple des anti-antivirus en les empêchant de s'enregistrer dans le registre pour un lancement ultérieur ;
- il bloque les branches du registre qui sont responsables des pilotes des dispositifs virtuels ce qui rend impossible l'installation du cheval de Troie sous forme d'un nouveau dispositif virtuel ;
- il ne permet pas au logiciel malveillant de perturber le fonctionnement normal des services système.

Dr.Web Process Dumper

L'analyseur complexe des menaces compressées Dr.Web Process Dumper augmente considérablement le niveau de détection des menaces supposées « nouvelles » (ce sont des menaces connues dans la base virale de Dr.Web, mais qui sont masquées sous de nouveaux packers) et exclut la nécessité d'ajouter dans les bases de nouvelles entrées portant sur les menaces. Vu que les bases virales Dr.Web gardent leur taille réduite, les pré-requis système n'augmentent pas et les mises à jour restent légères pendant que la détection et la désinfection de menaces est de haut niveau. Le préfixe `DPD` est ajouté aux noms des menaces détectées grâce à Dr.Web Process Dumper.

Dr.Web ShellGuard

La technologie Dr.Web ShellGuard protège l'ordinateur contre les *exploits* — les objets malveillants qui essaient d'exploiter les vulnérabilités afin d'obtenir le contrôle sur les applications attaquées et sur le système entier. Le préfixe `DPH:Trojan.Exploit` est ajouté aux noms des menaces détectées grâce à Dr.Web ShellGuard.

Dr.Web ShellGuard protège les applications les plus utilisées installées sur les ordinateurs tournant sous Windows :

- les navigateurs web (Internet Explorer, Mozilla Firefox, Google Chrome, etc.) ;
- les applications MS Office ;
- les applications système ;
- les applications utilisant les technologies java, flash et pdf ;
- les lecteurs média.

En analysant des actions potentiellement dangereuses, le système de protection grâce à la technologie Dr.Web ShellGuard se base non seulement sur les règles établies qui sont sauvegardées sur l'ordinateur mais aussi sur les connaissances du service cloud Dr.Web dans lequel sont collectées :

- les données sur les algorithmes des programmes aux intentions malveillantes ;
- les informations sur les fichiers sains ;
- les informations sur les signatures numériques compromises des développeurs de logiciels célèbres ;
- les informations sur les signatures numériques des logiciels publicitaires ou potentiellement dangereux ;

- les informations sur les sites indésirables ;
- les algorithmes de protection de telles ou telles applications.

Protection contre l'injection de code

Injection de code : une technique qui consiste à injecter un code malveillant dans les processus lancés sur l'appareil. Dr.Web surveille en permanence le comportement de tous les processus dans le système et prévient les tentatives d'injection s'il les considère comme malveillantes. Le préfixe `DPH:Trojan.Inject` est ajouté aux noms des menaces détectées grâce à la Protection contre les injections de code.

Dr.Web vérifie les caractéristiques suivantes de l'application qui a lancé le processus :

- si l'application est nouvelle ;
- comment elle a pénétré dans le système ;
- où l'application se trouve ;
- comment elle s'appelle ;
- si l'application est incluse dans la liste de confiance ;
- si elle porte une signature numérique du centre de certification fiable ;
- si elle est ajoutée dans la liste noire ou blanche d'applications qui se trouve dans le service cloud de Dr.Web.

Dr.Web suit le statut du processus lancé : vérifie si les flux distants sont créés dans l'espace du processus, si un code s'infiltre dans le processus actif.

L'Antivirus contrôle les modifications qu'apportent les applications, interdit de modifier les processus système et privilégiés. Dr.Web veille à ce que le code malveillant ne puisse pas modifier la mémoire des navigateurs populaires, par exemple, quand vous achetez ou effectuez des virements en ligne.

Protection contre les ransomwares

Protection contre les ransomwares : un des composants de la Protection préventive assurant la protection des fichiers d'utilisateurs contre les Trojans-encodeurs. Ces programmes malveillants pénètrent dans l'ordinateur de l'utilisateur, bloquent l'accès aux données en les chiffrant et, ensuite, réclament une rançon. Le préfixe `DPH:Trojan.Encoder` est ajouté aux noms des menaces détectées grâce à la Protection contre les ransomwares.

Le composant analyse le comportement d'un processus suspect, en prêtant attention à la recherche des fichiers, à la lecture et aux tentatives de leur modification.

Les caractéristiques suivantes de l'application sont également vérifiées :

- si l'application est nouvelle ;
- comment elle a pénétré dans le système ;

- où l'application se trouve ;
- comment elle s'appelle ;
- si l'application est une application de confiance ;
- si elle porte une signature numérique du centre de certification fiable ;
- si elle est ajoutée dans la liste noire ou blanche d'applications qui se trouve dans le service cloud de Dr.Web.

La nature de la modification du fichier est aussi analysée. Si une application se comporte comme un programme malveillant, ses actions seront bloquées et les tentatives de modification de fichiers seront rejetées.

Méthode de l'apprentissage machine

Elle est utilisée pour rechercher et neutraliser les objets malveillants 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 une 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 de détection cloud 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. Le préfixe `CLOUD` est ajouté aux noms des menaces détectées grâce aux Technologies cloud.

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 décision 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 l'entreprise Doctor Web collecte les informations sur de multiples utilisateurs et met rapidement à jour les données sur les menaces inconnues auparavant ce qui augmente l'efficacité de la protection des appareils.

2.3. Pré-requis système

Dr.Web peut être installé et fonctionner sur un ordinateur possédant au minimum ces pré-requis :

Paramètre	**Pré-requis**
Processeur	Processeur i686.
Système d'exploitation	Pour les plateformes 32-bits : • Windows XP avec Service Pack 2 ou supérieur ; • Windows Vista avec Service Pack 2 ou supérieur ; • Windows 7 avec Service Pack 1 ou supérieur ; • Windows 8 ; • Windows 8.1 ; • Windows 10 21H1 ou une version antérieure. Pour les plateformes 64-bits : • Windows Vista avec Service Pack 2 ou supérieur ; • Windows 7 avec Service Pack 1 ou supérieur ; • Windows 8 ; • Windows 8.1 ; • Windows 10 21H1 ou une version antérieure ; • Windows 11.
RAM disponible	512 Mo et plus.
Résolution d'écran	Au moins 1024x768.
Support d'environnements virtuels et cloud	Le programme fonctionne dans les environnement suivants : • VMware ; • Hyper-V ; • Xen ; • KVM.
Autre	Le plug-in Dr.Web pour Microsoft Outlook nécessite l'installation du client Microsoft Outlook intégré dans Microsoft Office : • Outlook 2000 ; • Outlook 2002 ;

Paramètre	Pré-requis
	• Outlook 2003 ; • Outlook 2007 ; • Outlook 2010 avec Service Pack 2 ; • Outlook 2013 ; • Outlook 2016 ; • Outlook 2019.

Vu que la société Microsoft ne supporte plus l'algorithme de hachage SHA-1, assurez-vous que votre système d'exploitation supporte l'algorithme de hachage SHA-256 avant d'installer Antivirus Dr.Web pour Windows sous Windows Vista ou Windows 7. Pour ce faire, installez toutes les mises à jour recommandées depuis le Centre de mise à jour Windows. Pour en savoir plus sur les paquets de mises à jour nécessaires, visitez le site officiel de la société Doctor Web.

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

Destination	Direction	Numéros de ports
Pour activer et renouveler une licence	sortant	443
Pour mettre à jour (si l'option de mise à jour par https est activée)	sortant	443
Pour mettre à jour	sortant	80
Pour envoyer les notifications e-mail		25 ou 465 (ou en fonction des paramètres des notifications par e-mail)
Pour se connecter au service Dr.Web Cloud	sortant	2075 (y compris les ports UDP)

2.4. Tester l'antivirus

Test avec le fichier EICAR

Le fichier de test EICAR (European Institute for Computer Anti-Virus Research) permet de tester les performances des programmes antivirus utilisant la méthode de détection par signatures.

Dans ce but, la plupart des éditeurs d'antivirus utilisent généralement le programme standard `test.com`. Ce programme a été spécialement conçu pour que l'utilisateur puisse tester la réaction de l'antivirus installé à la détection de virus sans compromettre la sécurité de son ordinateur. Bien que le programme test.com ne soit pas un virus, il est traité par la plupart des antivirus comme tel.

Dr.Web appelle ce « virus » de manière suivante : `EICAR Test File (Not a Virus!)`. D'autres logiciels antivirus alertent les utilisateurs de la même façon.

Le programme `test.com` est un fichier-COM 68-bits qui affiche la ligne suivante dans la console lorsqu'il est exécuté : `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!`

Le fichier `test.com` ne contient que des caractères de texte qui forment la chaîne suivante :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Pour créer votre propre fichier test avec le « virus », vous devez créer un nouveau fichier contenant cette ligne et le sauvegarder comme `test.com`.

> Lancé dans le mode optimal, SpIDer Guard n'interrompt pas le lancement du fichier de test EICAR et ne classe pas telle situation comme dangereuse puisque ce fichier ne représente aucun danger pour l'ordinateur. Cependant, lors de la copie ou de la création de ce fichier, SpIDer Guard le traite automatiquement comme un programme malveillant et par défaut le déplace en Quarantaine.

Test avec le fichier CloudCar

Pour vérifier le fonctionnement du service Dr.Web Cloud, utilisez le fichier de test CloudCar créé par l'organisation AMTSO (Anti-Malware Testing Standards Organization). Ce fichier est créé spécialement pour vérifier le fonctionnement de services antivirus cloud et il n'est pas malveillant.

Vérification du fonctionnement de Dr.Web Cloud

1. Assurez-vous que l'utilisation du service Dr.Web Cloud est activée.
2. Téléchargez le fichier de test. Pour ce faire, suivez le lien https://www.amtso.org/feature-settings-check-cloud-lookups/ et cliquez sur **Launch the Test**.
3. Une fois sur l'ordinateur, le fichier sera automatiquement déplacé en quarantaine si le composant SpIDer Guard est installé et activé. Si le composant SpIDer Guard n'est pas installé ou qu'il est désactivé, scannez le fichier téléchargé. Pour ce faire , ouvrez le menu contextuel en cliquant droit sur le nom du fichier et sélectionnez l'élément **Analyser par Dr.Web**.
4. Assurez-vous que le fichier de test est traité par Dr.Web comme `CLOUD:AMTSO.Test.Virus`. Le préfixe `CLOUD` dans le nom de la menace signifie le fonctionnement correct de Dr.Web Cloud.

3. Installation, modification et suppression du logiciel

Avant d'installer Antivirus Dr.Web pour Windows, consultez les pré-requis système. Il est également recommandé d'effectuer les actions suivantes :

- installer toutes les mises à jour critiques de Microsoft pour la version de l'OS utilisée sur votre ordinateur (pour en savoir plus sur la mise à jour Windows) ; si le producteur ne supporte plus le système d'exploitation, il est recommandé de migrer vers une version plus récente du système d'exploitation ;
- analyser le système de fichiers en utilisant les outils système, et, en cas d'erreurs détectées, résoudre le problème ;
- supprimer tout autre antivirus installé sur l'ordinateur afin d'éviter une possible incompatibilité de ses composants avec les composants de Dr.Web ;
- si le Pare-feu Dr.Web est installé, vous devrez supprimer tout autre pare-feu installé sur votre ordinateur ;
- fermer toutes les applications en cours.

Il est nécessaire d'avoir les droits d'administrateur de l'ordinateur pour installer Dr.Web.

Dr.Web est incompatible avec les produits de la protection proactive d'autres développeurs.

L'installation de Dr.Web se fait dans l'un des modes suivants :

- en mode de la ligne de commande ;
- en mode de l'assistant d'installation.

3.1. Installation du logiciel

Il est nécessaire d'avoir les droits d'administrateur de l'ordinateur pour installer Dr.Web.

Installation en mode de l'assistant d'installation

Pour lancer l'installation en mode standard, suivez l'une des instructions ci-dessous :

- si vous avez le fichier d'installation (`drweb-12.0-av-win.exe`), lancez-le ;
- si vous possédez un package d'installation enregistré sur le disque Dr.Web, insérez le disque dans le lecteur. Si le démarrage automatique est activé pour ce lecteur, l'installation va démarrer automatiquement. Si le démarrage automatique n'est pas activé, lancez le fichier `autorun.exe`

se trouvant sur le disque. Une fenêtre affichant le menu d'autorun sera ouverte. Cliquez sur le bouton **Installer**.

Suivez les instructions de l'assistant d'installation. A chaque étape avant la copie de fichier sur l'ordinateur, vous pouvez réaliser les fonctions suivantes :

- pour revenir vers l'étape précédente de l'installation, cliquez sur **Précédent** ;
- pour passer à l'étape suivante, cliquez sur **Suivant** ;
- pour interrompre l'installation, cliquez sur **Annuler**.

Pour installer le programme

1. Si un autre antivirus est déjà installé sur votre ordinateur, l'Assistant d'installation va vous avertir de l'incompatibilité de Dr.Web avec d'autres solutions antivirus, et il vous sera proposé de les supprimer.

   

   Avant l'installation, le statut du fichier d'installation est vérifié. S'il existe une version plus récente du fichier d'installation, vous serez invité à la télécharger.

2. A la première étape, vous pouvez vous connecter aux services cloud Dr.Web qui permettent d'effectuer une analyse antivirus en utilisant les données virales les plus récentes. Ces données sont stockées et mises à jour en temps réel sur les serveurs de Doctor Web. L'option est activée par défaut. Vous pouvez également indiquer si vous souhaitez d'installer le Pare-feu Dr.Web.

Figure 1. Assistant d'installation

3. Si vous voulez effectuer une installation avec les paramètres par défaut, allez à l'étape 4. Pour sélectionner les composants à installer, spécifier le chemin d'installation et certains paramètres supplémentaires, cliquez sur le lien **Paramètres d'installation**.

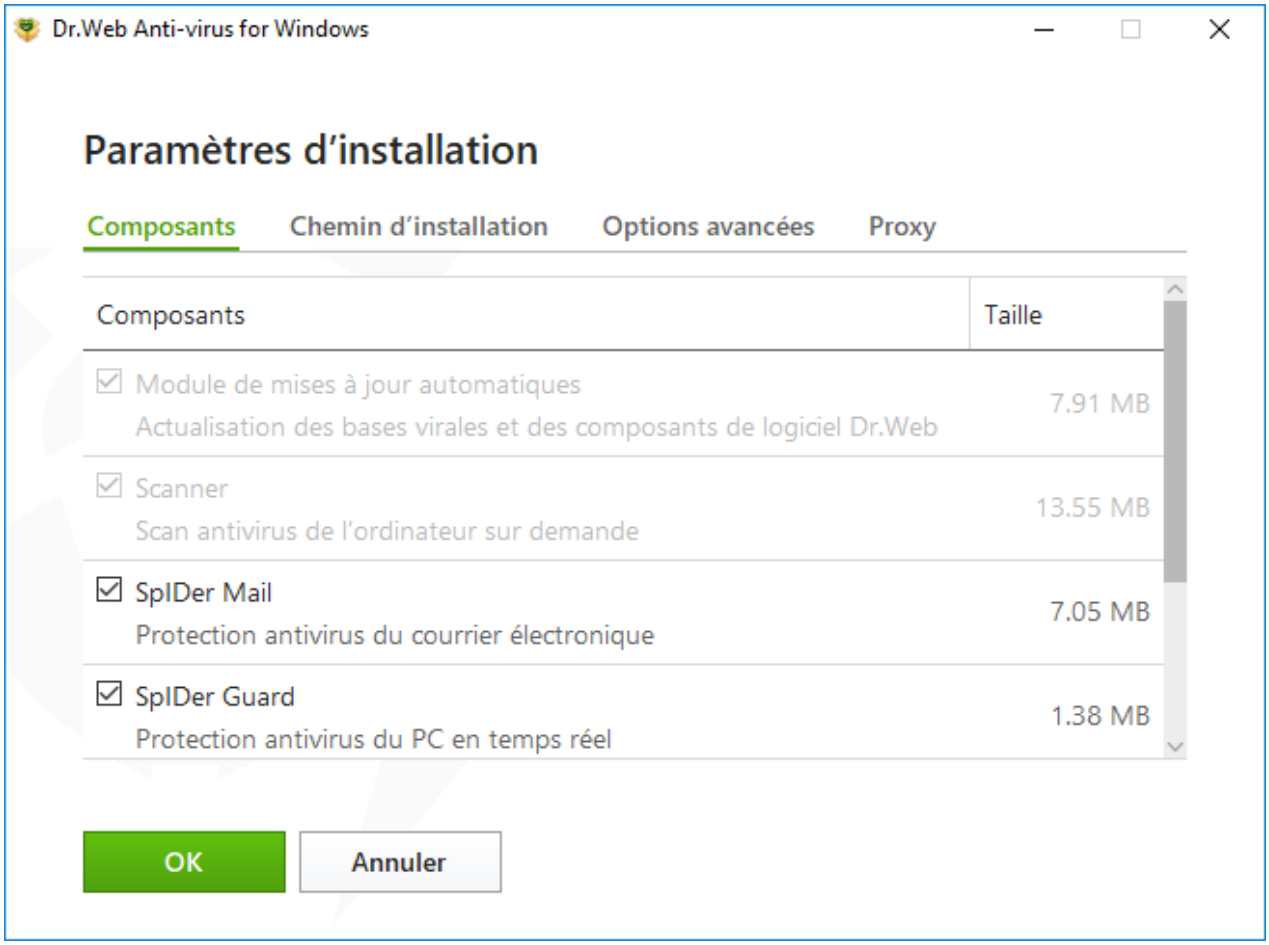

Figure 2. Paramètres d'installation

Cette option est réservée aux utilisateurs expérimentés.

- Sur le premier onglet, vous pouvez modifier l'ensemble de composants à installer. Cochez les cases contre les composants que vous souhaitez installer sur votre ordinateur.
- Sur le deuxième onglet, vous pouvez modifier le chemin d'installation. Par défaut, c'est le dossier DrWeb se trouvant dans le répertoire `Program Files` sur le disque système. Pour modifier le chemin d'installation, cliquez sur **Parcourir** et spécifiez le chemin nécessaire.
- Sur le troisième onglet de la fenêtre, vous pouvez cocher la case **Télécharger des mises à jour pendant l'installation** afin de télécharger les bases virales les plus récentes et d'autres composants de l'antivirus lors de l'installation. Cette fenêtre vous permet également de créer des raccourcis pour le lancement de Dr.Web. Vous pouvez cocher la case **Activer le support de compatibilité avec les outils de lecture d'écran** pour utiliser les lecteurs d'écran tels que JAWS et NVDA pour énoncer les éléments de l'interface de Dr.Web. Cette fonction rend l'interface du logiciel accessible pour les personnes malvoyantes. Vous pourrez également de créer des raccourcis pour le lancement de Dr.Web.
- Si nécessaire, indiquez les paramètres du serveur proxy.

Pour sauvegarder les modifications apportées, cliquez sur **OK**. Pour quitter sans enregistrer les modifications, cliquez sur **Annuler**.

4. Cliquez sur **Suivant**. Ainsi vous acceptez les termes du contrat de licence.
5. Dans la fenêtre **Assistant d'enregistrement**, il faut sélectionner l'une des options suivantes :

- si vous possédez un fichier clé sur le disque dur ou sur un support amovible, sélectionnez **Spécifiez le chemin vers le fichier clé valide**. Cliquez sur **Parcourir** et sélectionnez le fichier nécessaire dans la fenêtre qui s'affiche. Pour en savoir plus, consultez le manuel Activation de la licence avec le fichier clé ;
- si vous n'avez pas de fichier clé, mais vous voulez en recevoir un durant l'installation, sélectionnez **Obtenir le fichier clé lors de l'installation**. Pour en savoir plus, consultez le manuel Activation de la licence avec le numéro de série ;
- pour continuer l'installation sans licence, sélectionnez **Obtenir le fichier clé plus tard**. La mise à jour n'est pas disponible tant que vous n'avez pas obtenu de fichier clé.

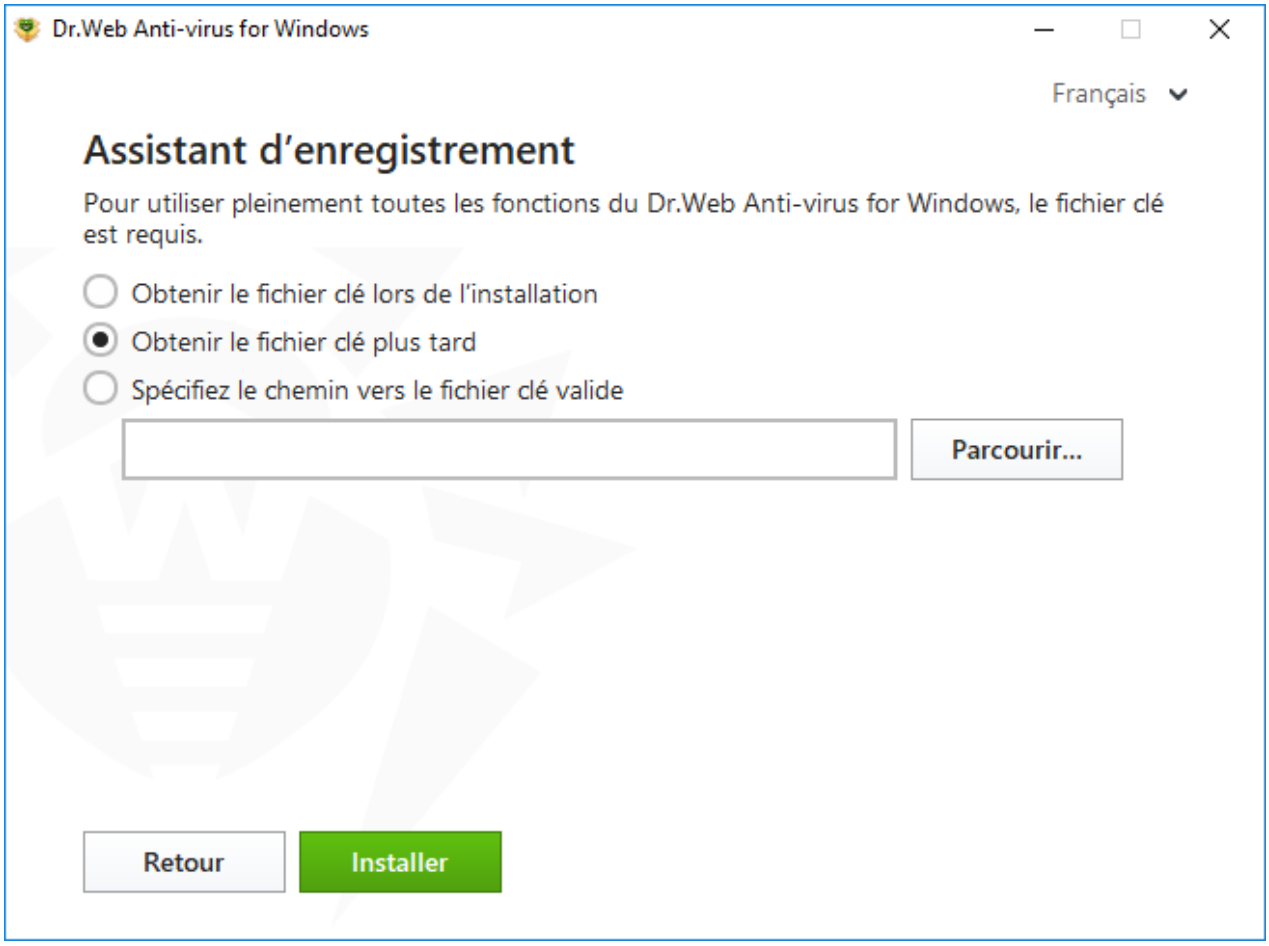

Figure 3. Assistant d'enregistrement

Cliquez sur **Installer**.

6. Si lors de l'installation vous avez spécifié ou reçu un fichier clé valide et que vous n'avez pas décoché la case **Télécharger des mises à jour pendant l'installation**, les bases virales et d'autres composants de Dr.Web seront mis à jour. La mise à jour démarre automatiquement et ne requiert aucune action supplémentaire.
7. Pour terminer l'installation, redémarrez l'ordinateur.

Installation en mode de la ligne de commande

Pour lancer l'installation de Dr.Web en tâche de fond, entrez dans la ligne de commande le nom du fichier exécutable avec les paramètres nécessaires :

Paramètre	Valeur
`installFirewall`	Le Pare-feu Dr.Web sera installé.
`lang`	Langue du produit. La valeur de ce paramètre est le code de la langue au format ISO 639-1, par exemple, `/lang fr`.
`reboot`	Redémarrage automatique de l'ordinateur après l'installation complète. Il peut prendre les valeurs `yes` et `no`.
`silent`	Redémarrage en tâche de fond. Il peut prendre les valeurs `yes` et `no`.
`blockEmulateUserActions`	Activation de l'option **Bloquer l'émulation des actions d'utilisateur** lors de l'installation. Elle peut prendre les valeurs `yes` et `no`.
`allowUiAccessibility`	Activation de la compatibilité avec les outils de lecture d'écran. Elle peut prendre les valeurs `yes` et `no`.
`importSettings`	Importation des paramètres depuis un fichier (taille maximale du fichier - 20 Mo). Il faut indiquer le chemin d'accès au fichier.
`enableDebugLogs`	Journalisation de débogage. Elle peut prendre les valeurs `yes` et `no`. La journalisation s'effectue pour les composants SpIDer Guard, SpIDer Mail, SpIDer Gate et le Scanner, le Module de mise à jour et le service de Dr.Web. La journalisation est désactivée lors du redémarrage de l'ordinateur après la fin de l'installation.

Par exemple, pour lancer une installation de Dr.Web en tâche de fond avec un redémarrage après l'installation, exécutez la commande suivante :

```
drweb-12.0-av-win.exe /silent yes /reboot yes
```

Erreur du service BFE lors de l'installation du logiciel Dr.Web

Pour le fonctionnement de certains composants de Dr.Web, il faut que le service du moteur de filtrage de base (BFE) soit lancé. Si ce service est manquant ou endommagé, l'installation de Dr.Web est impossible. L'endommagement ou l'absence du service BFE peut signaler la présence des menaces de sécurité sur votre ordinateur.

Si une tentative d'installer Dr.Web a échoué avec l'erreur du service BFE, faites le suivant :

1. Scannez le système avec l'utilitaire de désinfection CureIt! de Doctor Web. Vous pouvez télécharger l'utilitaire sur le site : https://free.drweb.com/download+cureit+free/.
2. Restaurez le service BFE. Pour cela, vous pouvez utiliser l'utilitaire de résolution de problèmes du Pare-feu conçu par Microsoft (pour les systèmes d'exploitation Windows 7 ou les versions supérieures).
3. Lancez l'Assistant d'installation Dr.Web et effectuez l'installation selon la procédure standard décrite ci-dessus.

Si le problème persiste, contactez le support technique de Doctor Web.

3.2. Modification des composants du logiciel

La modification des composants du logiciel se fait via l'Assistant de suppression/modification des composants. Vous pouvez ouvrir l'Assistant de suppression/modification des composants de deux façons :

- si vous avez le fichier d'installation, lancez-le ;
- depuis le Panneau de gestion de Windows :
  1. Sélectionnez (en fonction du système d'exploitation) :

Système d'exploitation	**Suite des actions**			
Windows XP	Menu Démarrer	**Démarrer** → **Panneau de configuration** → **Ajout/suppression de programmes**		
	Menu Démarrer classique	**Démarrer** → **Paramètres** → **Panneau de configuration** → **Ajout/suppression de programmes**		
Windows Vista	Menu Démarrer	**Démarrer** → **Panneau de configuration**	Affichage classique	**Programmes et fonctionnalités**
			Page d'accueil	**Programmes** → **Programmes et fonctionnalités**

Système d'exploitation	Suite des actions			
	Menu Démarrer classique	**Démarrer** → **Paramètres** → **Panneau de configuration** → **Programmes et fonctionnalités**		
Windows 7	**Démarrer** → **Panneau de configuration**	Petites/grandes icônes : **Programmes et fonctionnalités**		
		Catégorie : **Programmes** → **Suppression de programmes**		
Windows 8, Windows 8.1, Windows 10	**Panneau de configuration**	Petites/grandes icônes : **Programmes et fonctionnalités**		
		Catégorie : **Programmes** → **Suppression de programmes**		

2. Dans la liste des logiciels installés, sélectionnez la ligne **Dr.Web Anti-virus for Windows**.
3. Cliquez sur **Modifier**.

Pour supprimer ou ajouter des composants

1. Dans la fenêtre de l'Assistant de suppression/modification des composants, cliquez sur **Modifier les composants** :

Figure 4. Assistant de suppression/modification des composants

2. Dans la fenêtre qui s'ouvre, cochez les cases contre les composants à ajouter et décochez les cases contre les composants à supprimer.
3. Cliquez sur **Appliquer**.
4. Dans la fenêtre **Désactivation de l'Autoprotection** qui s'ouvre, entrez le code de confirmation affiché.
5. Cliquez sur le bouton **Appliquer**.

Dans la fenêtre de l'Assistant de suppression/modification des composants du logiciel, les options suivantes sont également disponibles :

- **Récupérer le programme**, s'il faut restaurer la protection antivirus sur votre ordinateur. Cette fonction est appliquée au cas où certains composants de Dr.Web seraient endommagés.
- **Supprimer le programme**, pour supprimer tous les composants installés.

3.3. Suppression et réinstallation du logiciel

Suppression de Dr.Web

Après la suppression de Dr.Web, votre ordinateur ne sera plus protégé contre les virus et d'autres programmes malveillants.

Si vous avez le fichier d'installation, vous pouvez sauter les étapes 1-3. Lancez le fichier d'installation et allez à l'étape 4.

1. Pour supprimer le logiciel Antivirus Dr.Web pour Windows depuis le Panneau de gestion de Windows, sélectionnez (en fonction du système d'exploitation) :

Système d'exploitation	**Suite des actions**			
Windows XP	Menu Démarrer	**Démarrer → Panneau de configuration → Ajout/suppression de programmes**		
	Menu Démarrer classique	**Démarrer → Paramètres → Panneau de configuration → Ajout/suppression de programmes**		
Windows Vista	Menu Démarrer	**Démarrer → Panneau de configuration**	Affichage classique	**Programmes et fonctionnalités**
			Page d'accueil	**Programmes → Programmes et fonctionnalités**
	Menu Démarrer classique	**Démarrer → Paramètres → Panneau de configuration → Programmes et fonctionnalités**		

Système d'exploitation	Suite des actions			
Windows 7	**Démarrer** → **Panneau de configuration**	Petites/grandes icônes : **Programmes et fonctionnalités**		
		Catégorie : **Programmes** → **Suppression de programmes**		
Windows 8, Windows 8.1, Windows 10	**Panneau de configuration**	Petites/grandes icônes : **Programmes et fonctionnalités**		
		Catégorie : **Programmes** → **Suppression de programmes**		

2. Dans la liste qui apparaît, sélectionnez la ligne portant le nom du programme.
3. Cliquez sur **Supprimer**.
4. Dans la fenêtre **Paramètres sauvegardés**, cochez les cases contre les éléments à conserver après la suppression du logiciel. Les objets et les paramètres conservés peuvent être utilisés par le logiciel en cas de réinstallation. Par défaut, toutes les options sont activées : **Quarantaine**, **Paramètres Dr.Web Anti-virus for Windows** et **Copies de fichiers protégées**. Cliquez sur le bouton **Suivant**.
5. La fenêtre **Désactivation de l'Autoprotection** va s'ouvrir. Dans cette fenêtre, saisissez le code de confirmation, puis cliquez sur **Supprimer le programme**.
6. Les modifications entrent en vigueur après le redémarrage de l'ordinateur. Vous pouvez reporter le redémarrage en cliquant sur **Redémarrer plus tard**. Cliquez sur **Redémarrer maintenant** pour terminer la désinstallation et modifier l'ensemble des composants Dr.Web tout de suite.

Réinstallation de Dr.Web

1. Téléchargez la distribution actuelle du logiciel depuis le site officiel de l'entreprise Doctor Web. Pour cela, il faut saisir le numéro de série valide dans le champ approprié.
2. Supprimez le produit, comme cela est décrit ci-dessus.
3. Redémarrez l'ordinateur.

4. Réinstallez le logiciel en utilisant la distribution téléchargée (`drweb-12.0-av-win.exe`) . À cette étape de l'installation, saisissez le numéro de série valide ou indiquez le chemin d'accès au fichier clé.
5. Redémarrez l'ordinateur.

4. Licence

Les droits de l'utilisateur d'utiliser Dr.Web sont régis par une licence achetée sur le site de Doctor Web ou chez les partenaires. La licence accorde le droit d'utiliser toutes les fonctionnalités du produit durant 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 du logiciel.

Chaque licence possède un *numéro de série* unique et un fichier spécifique est lié à la licence sur l'ordinateur de l'utilisateur. Ce fichier s'appelle le *fichier clé* de licence et il régule le fonctionnement de Dr.Web conformément aux paramètres de la licence. Pour plus d'infos sur le fichier clé de licence, voir la rubrique Fichier clé.

Méthodes d'activation de la licence

Vous pouvez activer la licence commerciale par l'une des méthodes suivants :

- lors de l'installation du produit à l'aide de l'Assistant d'enregistrement ;
- à n'importe quel moment à l'aide de l'Assistant d'enregistrement inclus dans le Gestionnaire de licences ;
- sur le site officiel de Doctor Web à l'adresse https://products.drweb.com/register/.

L'activation de la licence dans l'Assistant d'enregistrement se fait avec le numéro de série ou le fichier clé. Les utilisateurs de Windows XP peuvent activer la licence uniquement avec le fichier clé.

Pour plus d'infos sur l'activation de la licence, consultez la rubrique Comment activer la licence.

Si vous avez des questions sur la licence, consultez la liste des questions les plus fréquentes sur le site de Doctor Web.

Questions possibles

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. Si vous voulez transférer la licence sur un ordinateur tournant sous Windows XP, vous pouvez le faire en utilisant le fichier clé seulement.

Pour transférer la licence sur un autre ordinateur

- avec le numéro de série :
  1. Copiez le numéro de série de l'ordinateur depuis lequel vous voulez transférer la licence.
  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. Pour ce faire, utilisez l'Assistant d'enregistrement lors de l'enregistrement du produit ou après l'installation lors du fonctionnement du produit (voir Activation avec le numéro de série).

- 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. Pour ce faire, utilisez l'Assistant d'enregistrement lors de l'installation du produit ou après l'installation lors du fonctionnement du produit (voir Activation avec le fichier clé).

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

Si vous avez oublié l'adresse e-mail que vous aviez indiquée lors de l'enregistrement, vous devez contacter le support technique de l'entreprise Doctor Web à l'adresse https://support.drweb.com.

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 de changement d'e-mail se trouvant à l'adresse https://products.drweb.com/register/change_email.

Pourquoi n'y a-t-il pas certains composants dans mon produit ?

- Lors de l'installation du produit, pas tous les composants inclus dans la licence ont été installés.

Pour inclure les composants manquants

1. Allez dans la section consacrée à l'installation et la suppression de programmes du Panneau de gestion Windows.
2. Dans la liste des programmes installés, sélectionnez la ligne portant le nom du programme.
3. Cliquez sur le bouton **Modifier**. Dans ce cas, l'Assistant de suppression/modification des composants du programme va s'afficher.
4. Sélectionnez l'option **Modifier les composants**.
5. Sélectionnez dans la liste les composants que vous voulez inclure et cliquez sur le bouton

Appliquer.

Lancez le fichier d'installation `drweb-12.0-av-win.exe` et, dans la fenêtre qui s'affiche, sélectionnez l'option **Modifier les composants**. Allez à l'étape 5.

Vous avez installé un produit qui ne correspond pas à la licence achetée.

Pour installer un autre produit Dr.Web correspondant à la licence activée

1. Téléchargez la version actuelle Dr.Web depuis le site officiel : https://download.drweb.com/.
2. Indiquez le numéro de série et l'e-mail d'enregistrement. Ensuite, cliquez sur **Télécharger**.
3. Sélectionnez la version nécessaire du produit. Ensuite, téléchargez le package avec la distribution.
4. Supprimez le produit installé, en suivant les instructions de suppression dans la rubrique Suppression et réinstallation du logiciel.
5. Installez le produit téléchargée en utilisant la distribution téléchargée.

4.1. Comment activer la licence

Pour utiliser toutes les fonctionnalités et les composants du logiciel, il faut activer la licence. L'activation de la licence se fait avec le fichier clé ou le numéro de série. Les utilisateurs de Windows XP peuvent activer la licence uniquement avec le fichier clé.

Si vous n'avez pas de fichier clé, mais vous possédez un numéro de série, il faudra l'enregistrer sur le site de l'entreprise Doctor Web. Après l'enregistrement, vous recevrez un lien de téléchargement du fichier clé. Utilisez ce fichier clé pour activer la licence.

> Si vous êtes déjà un utilisateur de Dr.Web, vous pouvez bénéficier d'une extension de votre licence de 150 jours. Pour activer le bonus, entrez votre numéro de série ou indiquez le chemin vers l'ancienne licence dans la fenêtre qui s'ouvre avant l'entrée des données d'enregistrement.

Activation de la licence avec le numéro de série

Si vous avez un numéro de série, vous pouvez :

- activer la licence lors de l'installation du produit à l'aide de l'Assistant d'enregistrement :
  1. Lancez l'installation du produit. A l'étape 5 de l'installation, sélectionnez l'élément **Obtenir le fichier clé lors de l'installation**. Cliquez sur **Installer**.

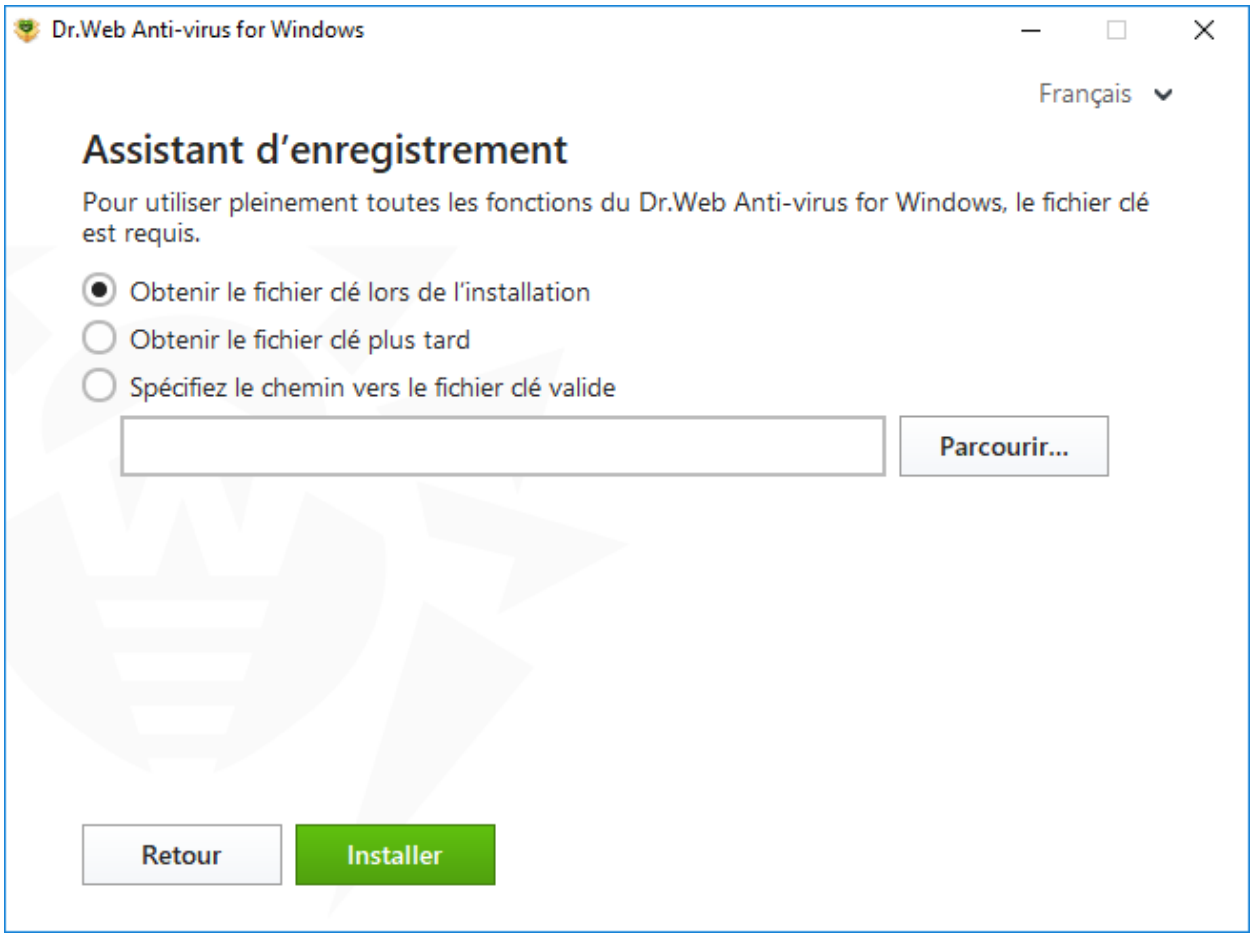

Figure 5. Installation. Assistant d'enregistrement

2. L'installation du produit commencera. A la fin de l'étape Obtention de licence, la fenêtre de l'Assistant d'enregistrement s'ouvrira. Entrez le numéro de série et cliquez sur **Activer**. Si le numéro de série n'a pas été enregistré, une fenêtre s'ouvrira dans laquelle vous devrez indiquer les données d'enregistrement.

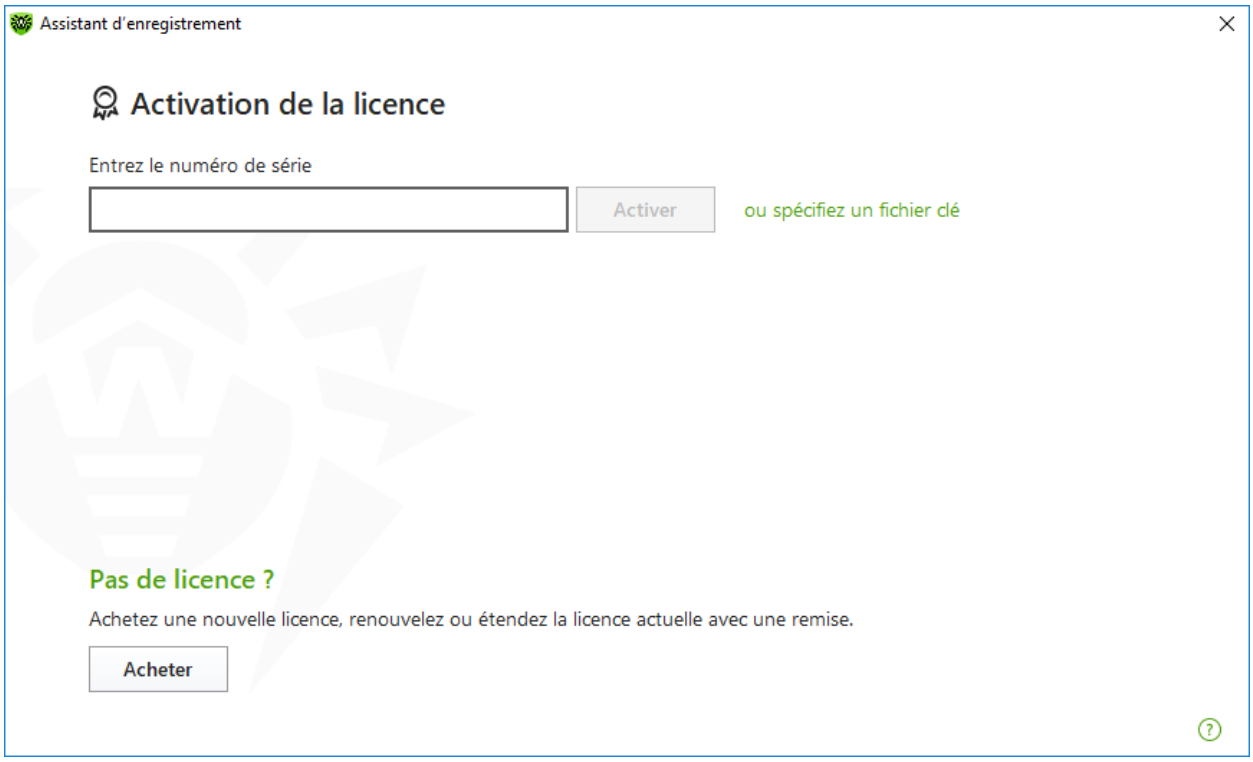

Figure 6. Assistant d'enregistrement. Activation de la licence

3. Continuez l'installation du produit en suivant les instructions de l'Assistant d'installation.

Si l'activation de la licence a échoué, un message d'erreur s'affiche. Vérifiez la connexion Internet ou cliquez sur **Réessayer** pour corriger les données erronées.

- activer la licence à n'importe quel moment à l'aide de l'Assistant d'enregistrement inclus dans le Gestionnaire de licences :

1. Dans le menu de Dr.Web, sélectionnez l'élément **Licence**. La fenêtre du Gestionnaire de licences va s'afficher. Cliquez sur **Activer ou acheter une nouvelle licence**.

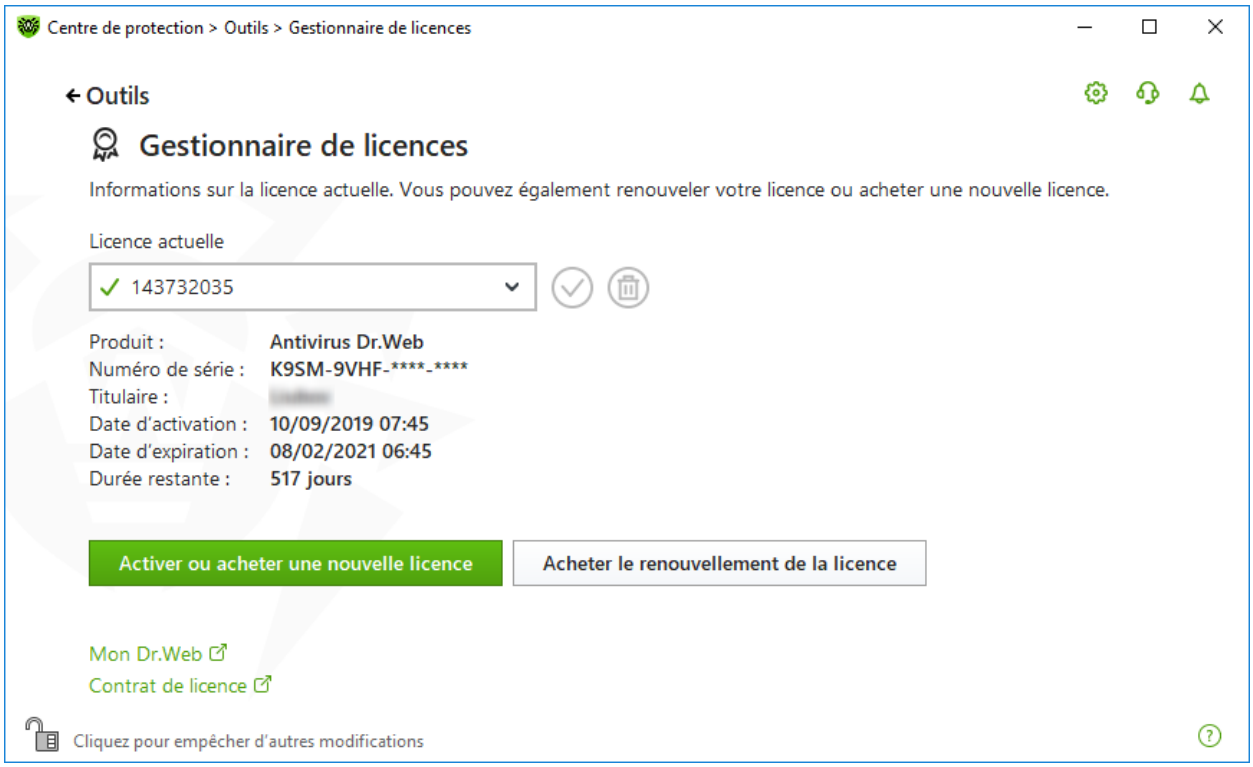

Figure 7. Gestionnaire de licences

2. La fenêtre de l'Assistant d'enregistrement s'ouvrira. Entrez le numéro de série et cliquez sur **Activer**. Si le numéro de série n'a pas été enregistré, une fenêtre s'ouvrira dans laquelle vous devrez indiquer les données d'enregistrement.

Figure 8. Assistant d'enregistrement. Activation de la licence

Si l'activation de la licence a échoué, un message d'erreur s'affiche. Vérifiez la connexion Internet ou cliquez sur **Réessayer** pour corriger les données erronées.

- enregistrer le numéro de série sur le site de l'entreprise Doctor Web et obtenir le fichier clé à l'aide duquel vous pouvez activer la licence.

Activation de la licence avec le fichier clé

Si vous avez un fichier clé, vous pouvez activer la licence :

- lors de l'installation du produit à l'aide de l'Assistant d'enregistrement :

  1. Lancez l'installation du produit. A l'étape 5 de l'installation, sélectionnez l'élément **Spécifiez le chemin vers le fichier clé valide**. Cliquez sur **Installer**.

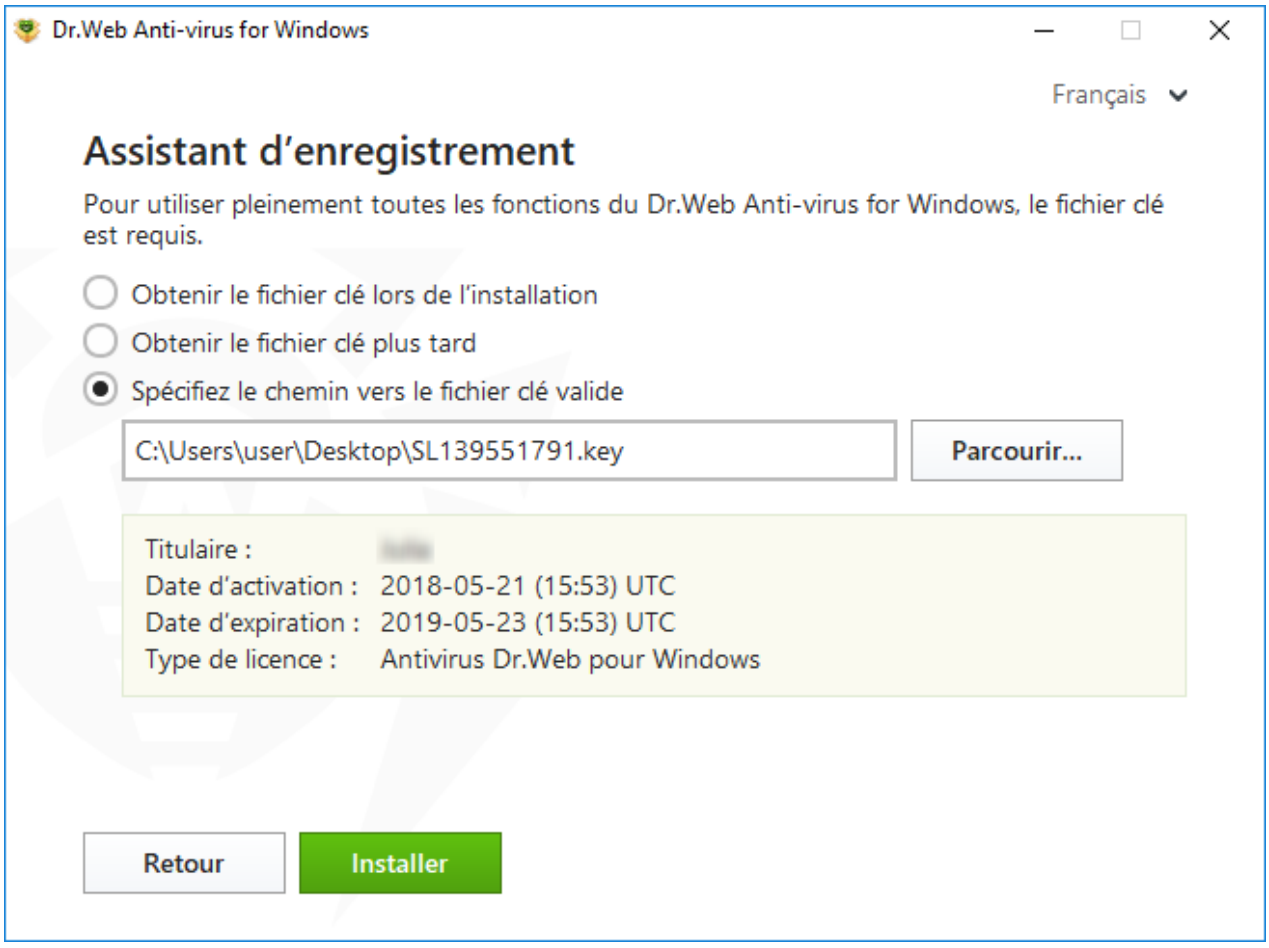

Figure 9. Installation. Assistant d'enregistrement

  2. Continuez l'installation du produit en suivant les instructions de l'Assistant d'installation.

- à n'importe quel moment à l'aide de l'Assistant d'enregistrement inclus dans le Gestionnaire de licences :

  1. Dans le menu de Dr.Web, sélectionnez l'élément **Licence**. La fenêtre du Gestionnaire de licences va s'afficher. Cliquez sur **Activer ou acheter une nouvelle licence**.

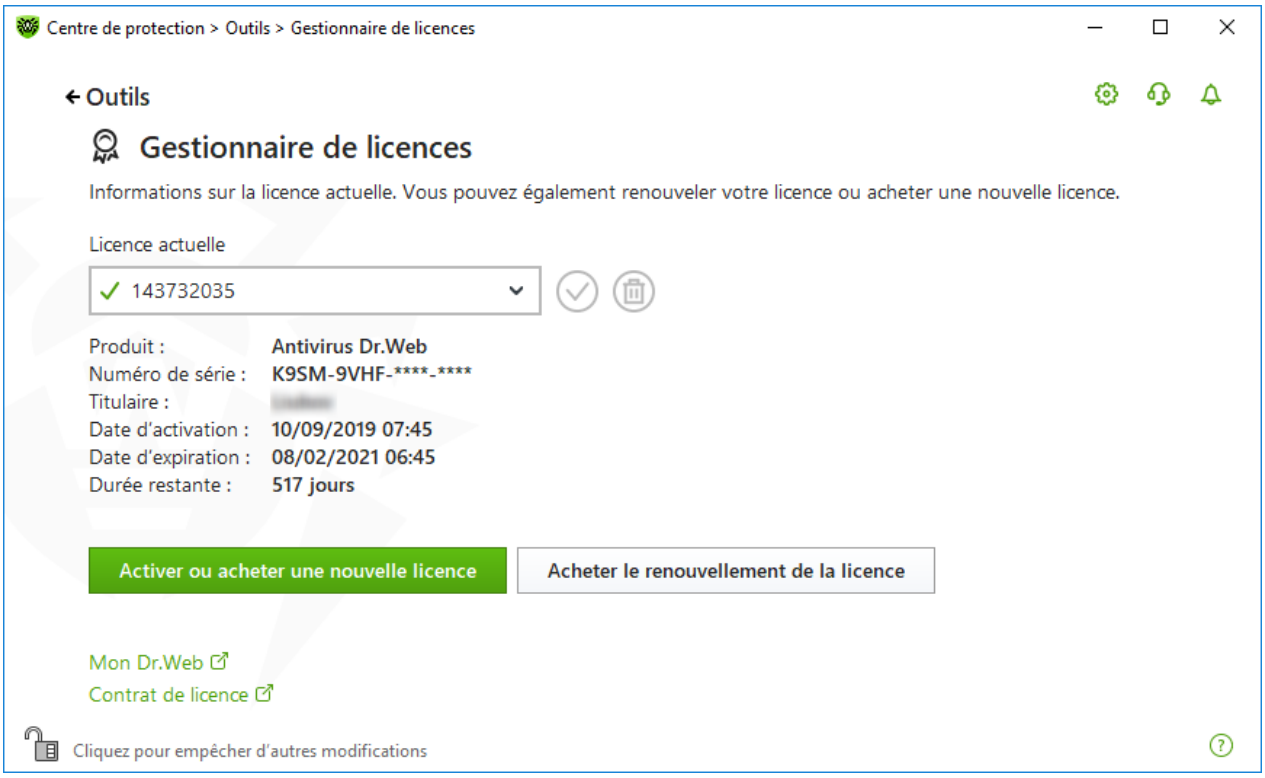

Figure 10. Gestionnaire de licences

2. La fenêtre de l'Assistant d'enregistrement s'ouvrira. Dans la fenêtre qui s'ouvre, spécifiez le chemin vers le fichier clé. Cliquez sur le lien **ou spécifiez un fichier clé**.

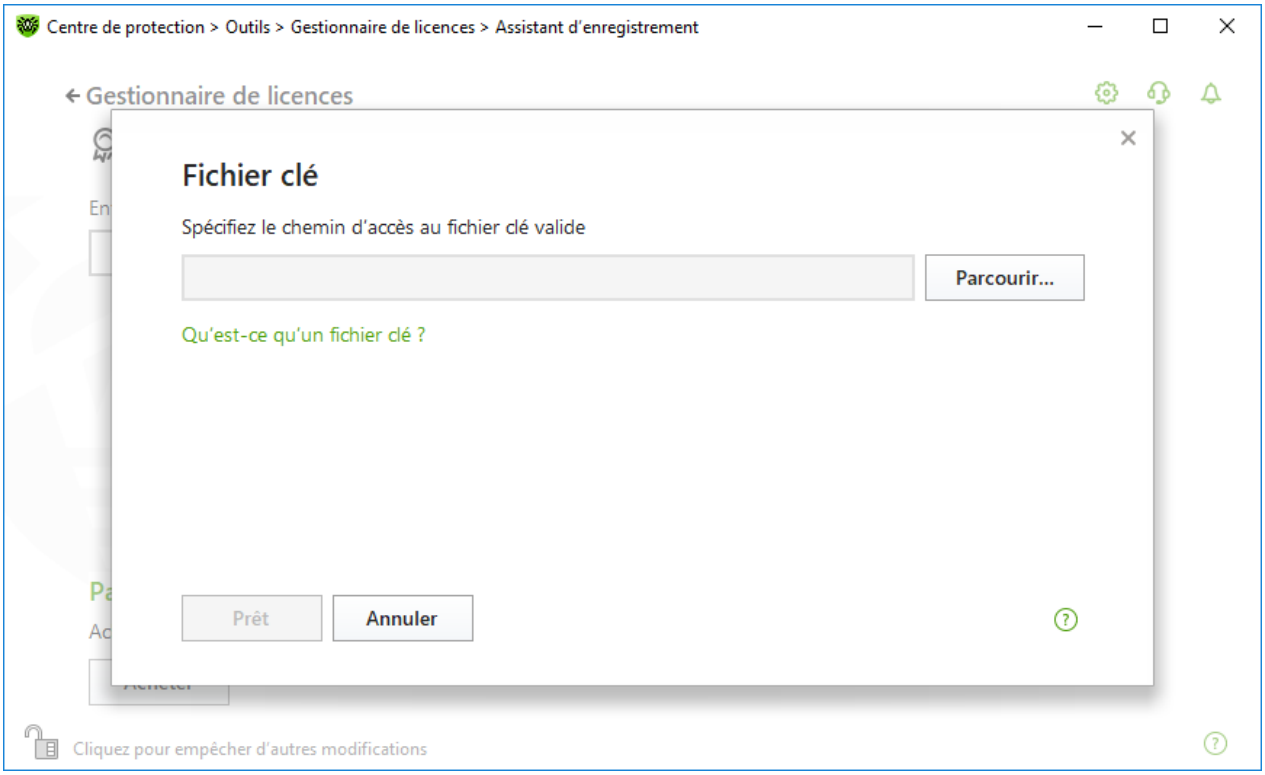

Figure 11. Assistant d'enregistrement. Activation de la licence

Activations de la licence sous Windows XP

Les utilisateurs de Windows XP peuvent activer la licence uniquement avec le fichier clé. Si vous n'avez pas de fichier clé, mais vous possédez un numéro de série, il faudra l'enregistrer sur le site de l'entreprise Doctor Web. Après l'enregistrement, vous recevrez un lien de téléchargement du fichier clé. Utilisez ce fichier clé pour activer la licence.

Réactivation

Vous pourriez avoir à réactiver votre licence si vous avez perdu le fichier clé.

> Lors de la réactivation de la licence, vous recevez le même fichier clé que durant l'enregistrement antérieur à condition que la licence n'ait pas expiré.

Si vous réinstallez le produit ou que la licence vous donne le droit d'installer le produit sur plusieurs ordinateurs, la réactivation du numéro de série n'est pas requise. Vous pouvez utiliser le fichier clé obtenu lors du premier enregistrement.

Le nombre de demandes de fichiers clés est limité. Un numéro de série ne peut pas être enregistré plus de 25 fois. Si ce nombre est dépassé, aucun fichier clé ne vous sera pas envoyé. Dans ce cas, pour recevoir un fichier clé perdu, contactez le Support technique en décrivant votre problème en détails, en fournissant les données personnelles que vous avez indiquées lors de votre enregistrement, ainsi que le numéro de série. Le fichier clé vous sera envoyé par le service support technique à votre adresse e-mail.

Questions possibles

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. Si vous voulez transférer la licence sur un ordinateur tournant sous Windows XP, vous pouvez le faire en utilisant le fichier clé seulement.

Pour transférer la licence sur un autre ordinateur

- avec le numéro de série :
  1. Copiez le numéro de série de l'ordinateur depuis lequel vous voulez transférer la licence.
  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. Pour ce faire, utilisez l'Assistant d'enregistrement lors de l'enregistrement du produit ou après l'installation lors du fonctionnement du produit (voir Activation avec le numéro de série).

- 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. Pour ce faire, utilisez l'Assistant d'enregistrement lors de l'installation du produit ou après l'installation lors du fonctionnement du produit (voir Activation avec le fichier clé).

4.2. Renouveler la licence

Pour renouveler la licence actuelle à l'aide du Gestionnaire de licences

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Licence**.
2. Dans la fenêtre du Gestionnaire de licences, cliquez sur **Acheter le renouvellement de la licence**. Une page du site de Doctor Web s'ouvrira et vous pourrez renouveler la licence avec la possibilité de remise.

Dr.Web supporte la mise à jour à la volée. Dans ce cas, vous n'avez pas à réinstaller Dr.Web ou interrompre son fonctionnement. Pour renouveler la licence de Dr.Web, il vous faudra activer une nouvelle licence.

Pour activer la licence

1. Ouvrez la fenêtre du Gestionnaire de licences en sélectionnant l'élément **Licence** dans le menu de Dr.Web. Cliquez sur **Activer ou acheter une nouvelle licence**.
2. Dans la fenêtre qui s'affiche entrez le numéro de série ou cliquez sur le lien **ou spécifiez un fichier clé** et indiquez le chemin vers le fichier clé. Les utilisateurs de Windows XP peuvent activer la licence uniquement à l'aide du fichier clé.

Les instructions détaillées sur l'activation de la licence sont disponibles dans la rubrique Comment activer 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. Il est également recommandé de supprimer l'ancienne licence à l'aide du Gestionnaire de licences.

Si vous avez des questions sur le renouvellement de la licence, consultez la liste des questions les plus fréquentes sur le site de Doctor Web.

Questions possibles

Après le renouvellement de la licence, j'ai reçu un message informant que mon fichier clé sera bloquée dans 30 jours.

Si la licence renouvelée n'a pas encore expiré, les jours restants s'ajoutent automatiquement à la nouvelle licence. Dans ce cas, la licence servant de base pour le renouvellement sera bloquée. Si vous utilisez une licence bloquée, les composants de Dr.Web ne marchent pas et la mise à jour ne se fait pas.

Il est recommandé de supprimer l'ancienne licence du produit. Pour ce faire :

1. Ouvrez le menu de Dr.Web en mode administrateur et sélectionnez l'élément **Licence**. La fenêtre du Gestionnaire de licences va s'afficher.
2. Dans la liste déroulante, sélectionnez la licence servant de base pour le renouvellement et cliquez sur le bouton .

4.3. Fichier clé

Les droits d'utilisation de Dr.Web sont spécifiés dans le fichier spécial dit le *fichier clé*. Les fichiers clés reçus lors de l'installation ou dans le kit de distribution du produit sont installés automatiquement et ne requièrent aucune action supplémentaire.

Le fichier clé possède l'extension `.key` et contient les informations suivantes :

- liste des composants antivirus fournis dans la licence ;
- durée de la licence pour le produit ;
- disponibilité du Support Technique pour l'utilisateur ;
- autres restrictions (notamment, le nombre d'ordinateurs sur lesquels vous êtes autorisé à utiliser l'antivirus).

Par défaut, le fichier clé est placé dans le dossier d'installation de Dr.Web. Le logiciel vérifie régulièrement la présence et la validité du fichier clé. Ne modifiez pas le fichier clé pour éviter de compromettre la licence.

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

Un fichier clé de Dr.Web valide 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 détecter et de neutraliser les programmes malveillants et laisse passer les messages sans les analyser.

Si durant l'installation de Dr.Web, vous n'avez pas reçu le fichier clé et que vous n'avez pas spécifié le chemin d'accès à ce fichier, un fichier clé temporaire sera utilisé. Ce fichier clé fournit les fonctionnalités complètes des composants de Dr.Web. Cependant, dans le menu de Dr.Web  , l'élément **Mise à jour** ne sera pas présent. Les mises à jour ne seront pas téléchargées jusqu'à ce que vous activiez une licence ou une version d'essai ou jusqu'à ce que vous indiquez le chemin d'accès au fichier clé valide via l'Assistant d'enregistrement.

Il est recommandé de conserver le fichier clé durant toute la durée de validité de la licence.

5. Menu du logiciel

Lorsque Dr.Web est installé, l'icône s'ajoute dans la zone de notification Windows. Cette icône indique le statut du logiciel. Pour ouvrir le menu de Dr.Web. cliquez sur l'icône. Si le logiciel n'est pas lancé, ouvrez le groupe **Dr.Web** dans le menu **Démarrer** et sélectionnez **Centre de protection**.

Dans le menu de Dr.Web vous pouvez voir le statut de protection ainsi qu'obtenir l'accès aux outils principaux de gestion et aux paramètres du logiciel.

Pour accéder aux paramètres des composants et ouvrir le service en ligne Mon Dr.Web, vous devez entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par un mot de passe** dans les paramètres.

Si vous avez oublié votre mot de passe pour accéder aux paramètres de produit, veuillez contacter le support technique.

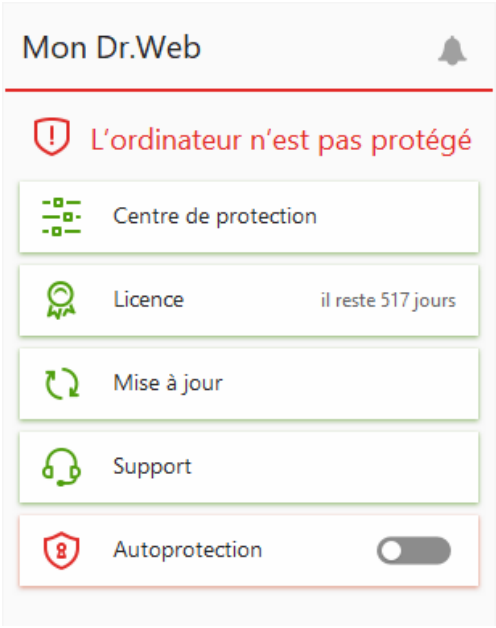

Figure 12. Menu du logiciel

Éléments du menu du logiciel

Mon Dr.Web. Ouvre votre espace personnel sur le site officiel de Doctor Web. Cette page vous fournit des informations sur vos licences (durée, numéro de série), vous permet de renouveler les licences, de contacter le support technique et plus encore.

Statut de protection de l'ordinateur. Si tous les composants du programmes fonctionnent, le statut **L'ordinateur est protégé** est affiché. Si un ou plusieurs composants sont désactivés, le statut change en **L'ordinateur n'est pas protégé**.

Centre de protection. Ouvre la fenêtre d'accès aux paramètres généraux, aux paramètres des composants de la protection et aux exclusions.

Licence. Informations sur le nombre de jours restants jusqu'à l'expiration de la licence. Ouvre le Gestionnaire de licences.

Mise à jour. Informations sur le statut des bases virales et l'heure de la dernière mise à jour. Lance une mise à jour du programme et des bases virales.

Support. Ouvre la fenêtre de support.

Autoprotection (s'affiche si l'Autoprotection est désactivée). Vous pouvez réactiver l'Autoprotection avec un interrupteur.

Le bouton **Flux de notifications** . Ouvre la fenêtre du Flux de notifications.

Statuts possibles du programmes

L'icône Dr.Web indique l'état actuel du logiciel :

Icône de Dr.Web	Description
	Tous les composants nécessaires sont activés et fonctionnent correctement.
	L'Autoprotection ou un des composants est désactivé ou les bases virales sont obsolètes, ce qui compromet la sécurité de l'antivirus et de votre ordinateur. Activez l'Autoprotection ou le composant désactivé.
	Le lancement des composants est attendue après le démarrage du système d'exploitation, attendez le lancement des composants ; ou bien, une erreur est survenue lors du démarrage d'un composant important de Dr.Web, votre ordinateur risque d'être infecté. Veuillez vérifier la présence d'un fichier clé valide, et si nécessaire, installez le fichier clé.
	Le Scanner Dr.Web est en cours d'exécution.

6. Centre de protection

La fenêtre **Centre de protection** fournit l'accès à tous les composants, les outils, les statistiques et les paramètres du logiciel.

Pour accéder à la fenêtre Centre de protection

1. Ouvrez le menu de Dr.Web .
2. Sélectionnez l'élément **Centre de protection**.

Pour accéder à la fenêtre Centre de protection depuis le menu Démarrer

1. Ouvrez le groupe **Dr.Web** dans le menu **Démarrer**.
2. Cliquez sur **Centre de protection**.

Figure 13. Fenêtre Centre de protection

Groupes de paramètres

La fenêtre principale fournit l'accès aux groupes de paramètres suivants :

- Onglet principal **Centre de protection**. Accès à tous les composants de protection et aux outils :
  - Fichiers et réseau ;
  - Protection préventive ;
  - Outils ;

    - Exclusions ;
- Onglet Statistiques : statistiques des événements essentiels du logiciel ;
- Bouton  en haut de la fenêtre : accès aux paramètres du logiciel ;
- Bouton  en haut de la fenêtre : accès à la fenêtre **Support** où vous pouvez créer un rapport pour le support technique et consulter les informations sur la version du produit et la date de la dernière mise à jour des composants et des bases virales ;
- Bouton  en haut de la fenêtre : accès à la fenêtre **Flux de notifications** où vous pouvez consulter les notifications importantes sur les événements du logiciel.

Mode administrateur

Pour accéder à tous les groupes de paramètres, il faut activer le mode administrateur de Dr.Web en cliquant sur le cadenas  en bas de la fenêtre. Quand Dr.Web fonctionne en mode administrateur, le cadenas est ouvert  .

Dans tous les modes, vous disposez d'un accès complet au groupe de paramètres **Outils**. Vous pouvez également activer un composant de sécurité et lancer le Scanner sans passer en mode administrateur. La désactivation des composants de sécurité, l'accès aux paramètres des composants et aux paramètres du logiciel sont possibles uniquement en mode administrateur.

Statuts de protection

Le statut de sécurité est affiché en haut de la fenêtre.

- **L'ordinateur est protégé** : tous les composants sont activés et marchent bien. L'Autoprotection est activée, la licence est valide. Ce statut est marqué en vert.
- **L'ordinateur n'est pas protégé** : ce statut s'affiche quand un composant de protection est désactivé. Il est marqué en rouge. La vignette du composant désactivé est aussi marquée en rouge.
- **La licence va expirer** : ce statut commence à s'afficher 7 jours avant l'expiration de la licence. Le statut est marqué en jaune. Pour renouveler la licence, il faut aller dans Gestionnaire de licences.

7. Mise à jour des bases et des modules de programme

Les produits Dr.Web utilisent les bases virales pour détecter des objets malveillants. Ces bases contiennent les informations sur tous les programmes malveillants connus. Les mises à jour régulières permettent de détecter de nouveaux virus, de bloquer leur diffusion et, parfois, de désinfecter les fichiers infectés qui n'étaient pas curables auparavant. Outre les bases virales, les modules de programme Dr.Web et l'aide du produit sont mis à jour.

Pour la mise à jour de Dr.Web, une connexion à Internet ou au miroir de mise à jour (dossier local ou réseau), ou au réseau antivirus avec le miroir de mises à jour configuré sur au moins un des ordinateurs est requise. La source de mises à jour et les autres paramètres sont configurés dans le groupe de paramètres **Général** → **Mise à jour**. Pour plus d'infos sur la configuration des paramètres de la mise à jour de Dr.Web, consultez la section Paramètres de la mise à jour.

Vérification du statut des mises à jour

Pour vérifier le statut des bases virales et des composants, ouvrez le menu de Dr.Web . S'ils sont à jour, l'élément **Mise à jour** du menu sera marqué en vert :

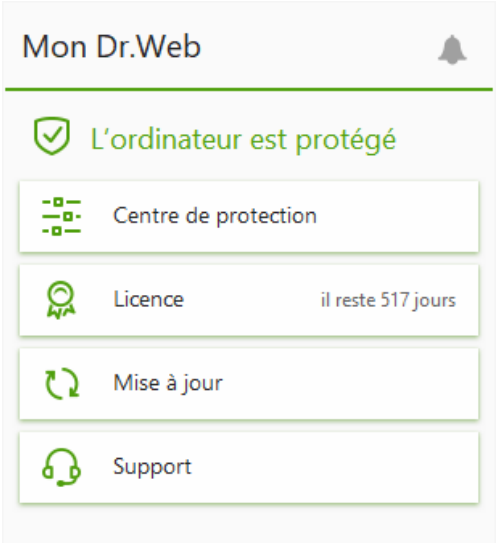

Figure 14. Menu Dr.Web

Si une mise à jour est requise, l'élément **La mise à jour est requise** marqué en rouge apparait dans le menu :

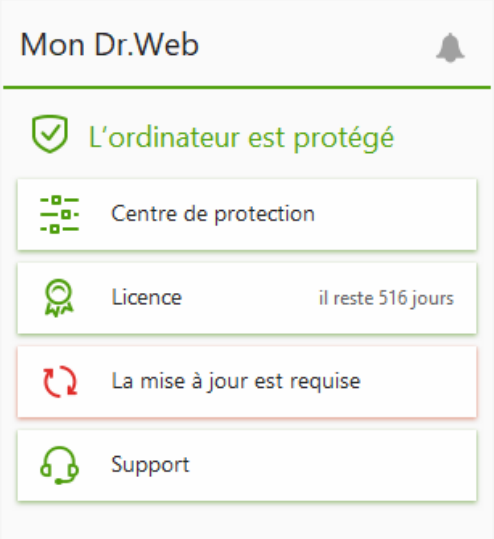

Figure 15. Nécessite de mise à jour

Lancement d'une mise à jour

Lors d'une mise à jour Dr.Web télécharge et installe automatiquement tous les fichiers mis à jour en fonction de votre version de Dr.Web, ainsi qu'une nouvelle version de Dr.Web si elle est disponible.

> Après une mise à jour des fichiers exécutables, des pilotes ou des bibliothèques, un redémarrage de l'ordinateur peut être requis. Dans ce cas, un avertissement correspondant sera affiché. Vous pouvez spécifier l'heure de redémarrage qui vous convient le mieux ou choisir l'heure du futur avertissement.

Pour lancer une mise à jour depuis le menu de Dr.Web

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Mise à jour**. En fonction du statut des bases et des composants, la couleur de cet élément peut varier.
2. Une fenêtre apparaît et affiche les informations sur les bases virales et les composants ainsi que la date de la dernière mise à jour. Pour lancer une mise à jour cliquez sur **Mettre à jour**.

Pour lancer une mise à jour depuis la ligne de commande

1. Ouvrez le dossier d'installation de Dr.Web (`%PROGRAMFILES%\Common Files\Doctor Web\Updater`).
2. Lancez `drwupsrv.exe`. La liste des paramètres de lancement se trouve dans l'Annexe A.

Rapports et journal de statistiques

Pour voir l'historique des mises à jour dans l'onglet Statistiques

1. Ouvrez le menu de Dr.Web.

2. Sélectionnez l'élément **Centre de protection**.
3. Accédez à l'onglet **Statistiques**.
4. Cliquez sur la vignette **Rapport détaillé**.

Les rapports de la mise à jour sont également enregistrés dans le fichier `dwupdater.log` situé dans le dossier `%allusersprofile%\Doctor Web\Logs\`.

Comment configurer la mise à jour des bases virales et des composants sans accès à Internet ?

Si l'ordinateur est connecté au réseau local, vous pouvez configurer la mise à jour des bases virales et des composants depuis le miroir de mise à jour créé sur un autre ordinateur avec un produit Dr.Web installé (Security Space, Antivirus pour Windows ou Antivirus pour les serveurs Windows). L'ordinateur sur lequel le miroir de mise à jour est créé doit être connecté à Internet. Les versions des produits doivent correspondre.

En savoir plus sur la configuration du miroir de mise à jour

Vous pouvez configurer la mise à jour depuis le miroir de mise à jour de deux façons :

Pour configurer la réception des mises à jour en cas de connexion au réseau antivirus

1. Autorisez la gestion à distance du produit Dr.Web dans la section de paramètres Réseau antivirus.

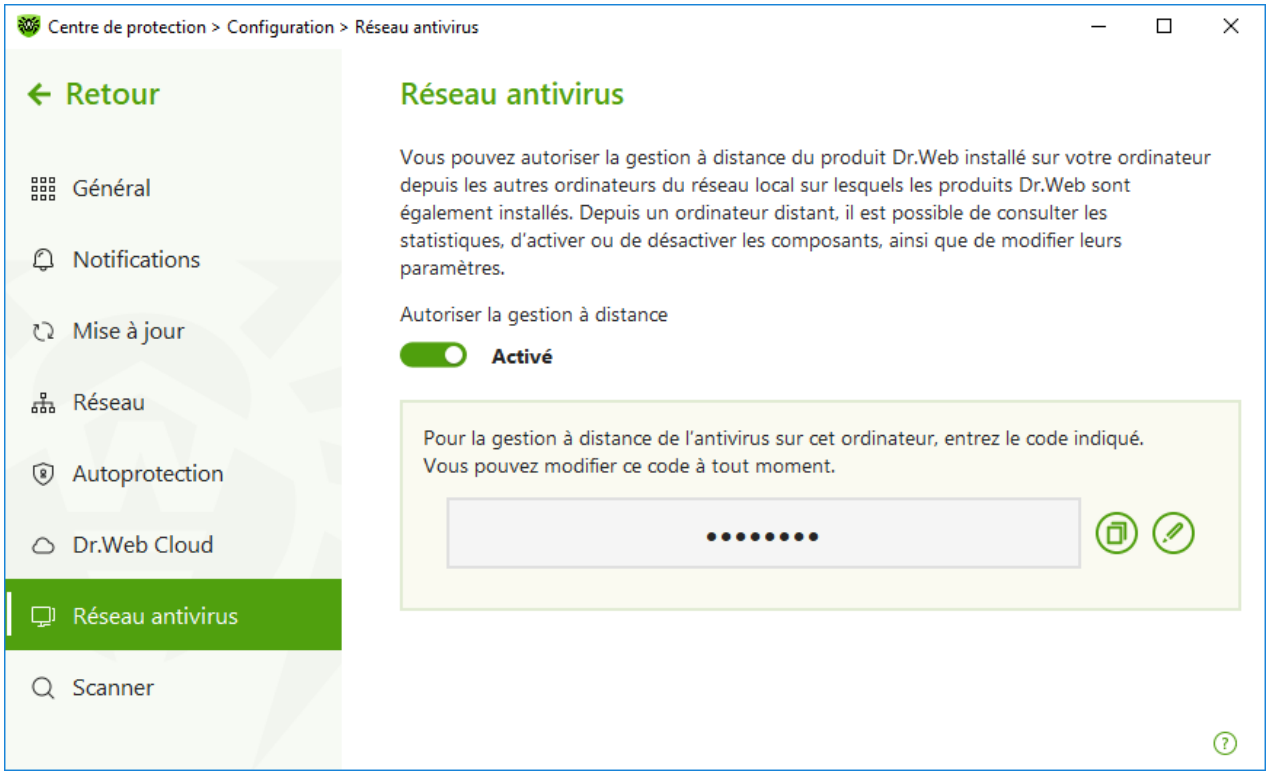

Figure 16. Activation de l'accès à distance

2. Ouvrez la fenêtre **Configuration** → **Mise à jour**.
3. Dans l'élément **Source de mises à jour**, cliquez sur **Modifier** et sélectionnez **Réseau antivirus** dans la liste déroulante.

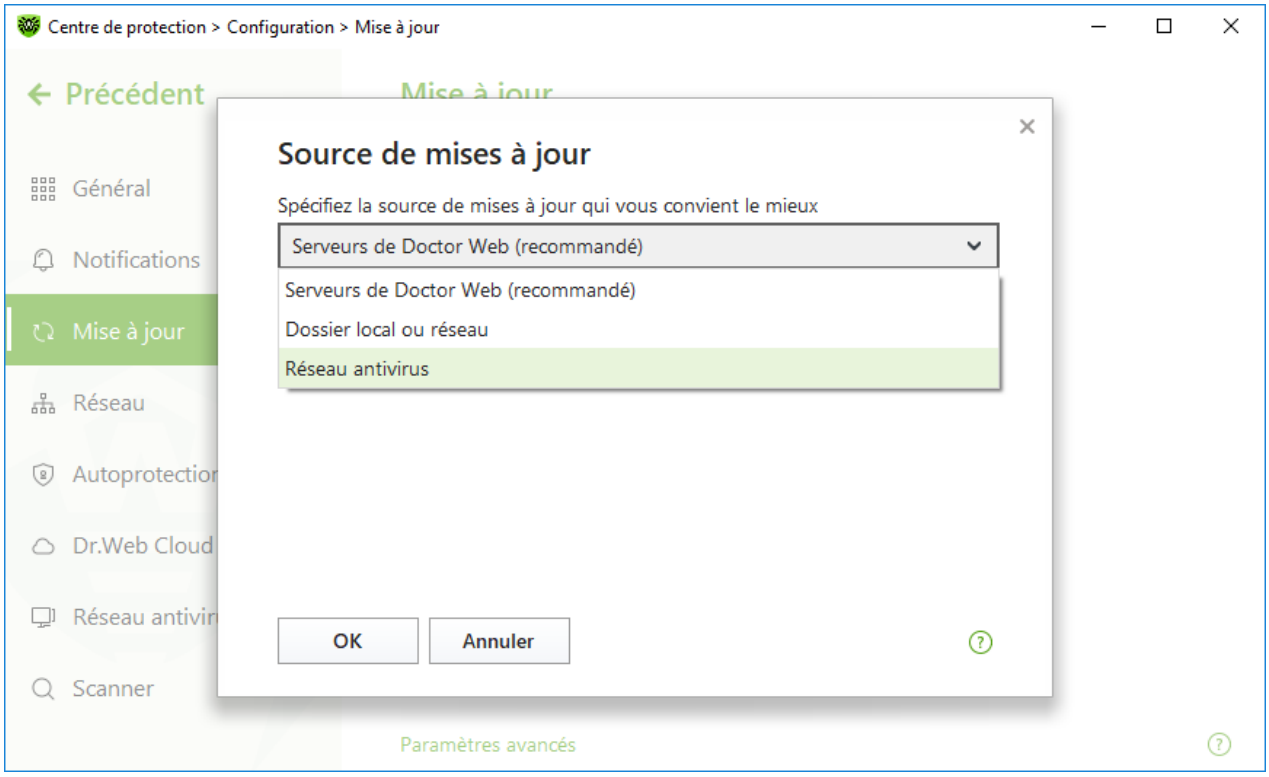

Figure 17. Sélection d'une source de mises à jour

4. Sélectionnez l'ordinateur nécessaire depuis lequel sera effectuée la mise à jour des bases virales et des composants du logiciel.
5. Cliquez sur **OK**.

Pour configurer la réception des mises à jour depuis un dossier local ou réseau

1. Ouvrez la fenêtre **Configuration** → **Mise à jour**.
2. Dans l'élément **Source de mises à jour**, cliquez sur **Modifier** et sélectionnez **Dossier local ou réseau** dans la liste déroulante.

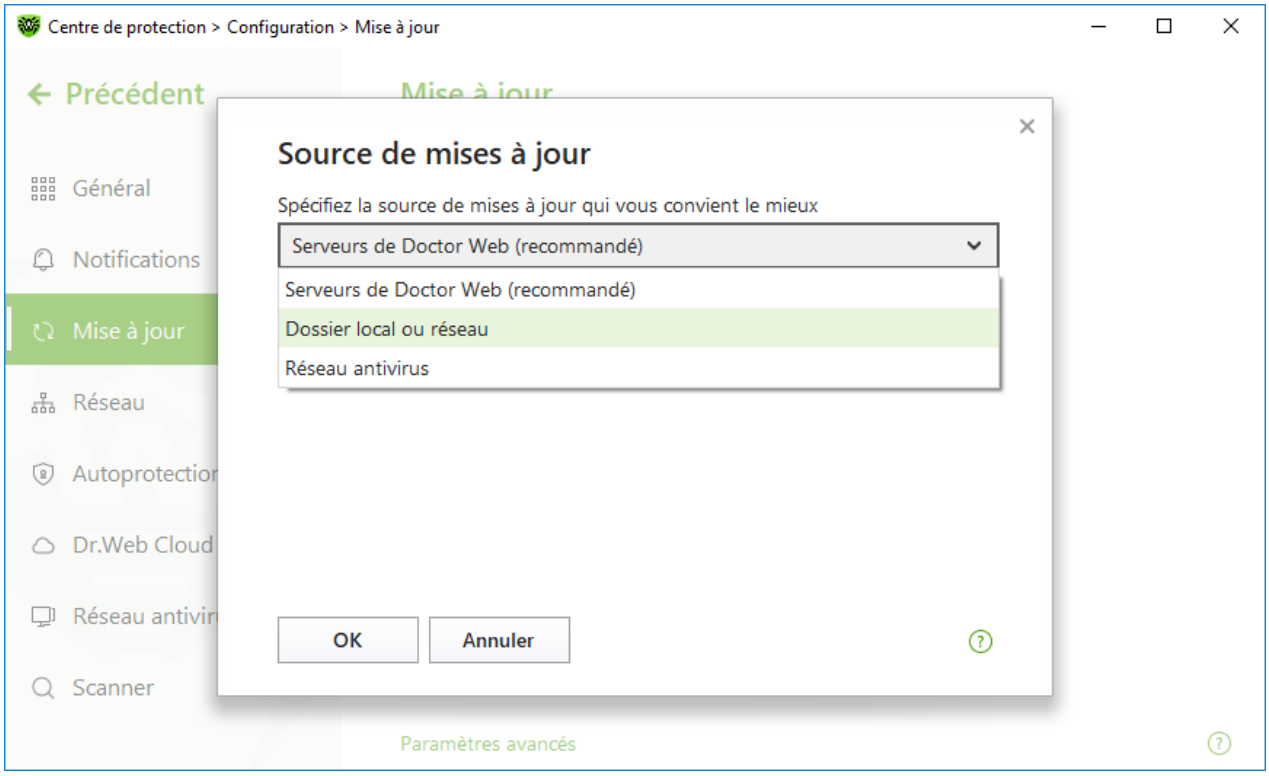

Figure 18. Sélection d'une source de mises à jour

3. Dans la ligne **Chemin vers le miroir de mise à jour**, indiquez le dossier contenant les fichiers du miroir de mise à jour créé. Pour ce faire, cliquez sur **Parcourir** et sélectionnez le dossier nécessaire ou entrez le chemin manuellement au format UNC.
4. Si nécessaire, indiquez le **Login** et le **Mot de passe** du dossier auquel vous voulez vous connecter. **Login** est le nom d'utilisateur du compte de l'ordinateur où se trouve le dossier réseau. Le login doit inclure le nom de l'ordinateur sur le réseau local et le chemin complet vers le dossier. **Mot de passe** est le mot de passe de ce compte.
5. Cliquez sur **OK**.

8. Flux de notifications

Cette fenêtre contient les notifications importantes sur le fonctionnement du logiciel. Les notifications de cette section dupliquent certains pop-ups.

Pour aller au flux de notifications depuis le Menu du logiciel

1. Ouvrez le menu de Dr.Web .
2. Cliquez sur le bouton . Le nombre de notifications sauvegardées est affiché au dessus de l'icône .
3. La fenêtre de notifications des événements va s'ouvrir.

Pour accéder au flux de notifications depuis le Centre de sécurité

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Cliquez sur en haut de la fenêtre du programme.
3. La fenêtre de notifications des événements va s'ouvrir.

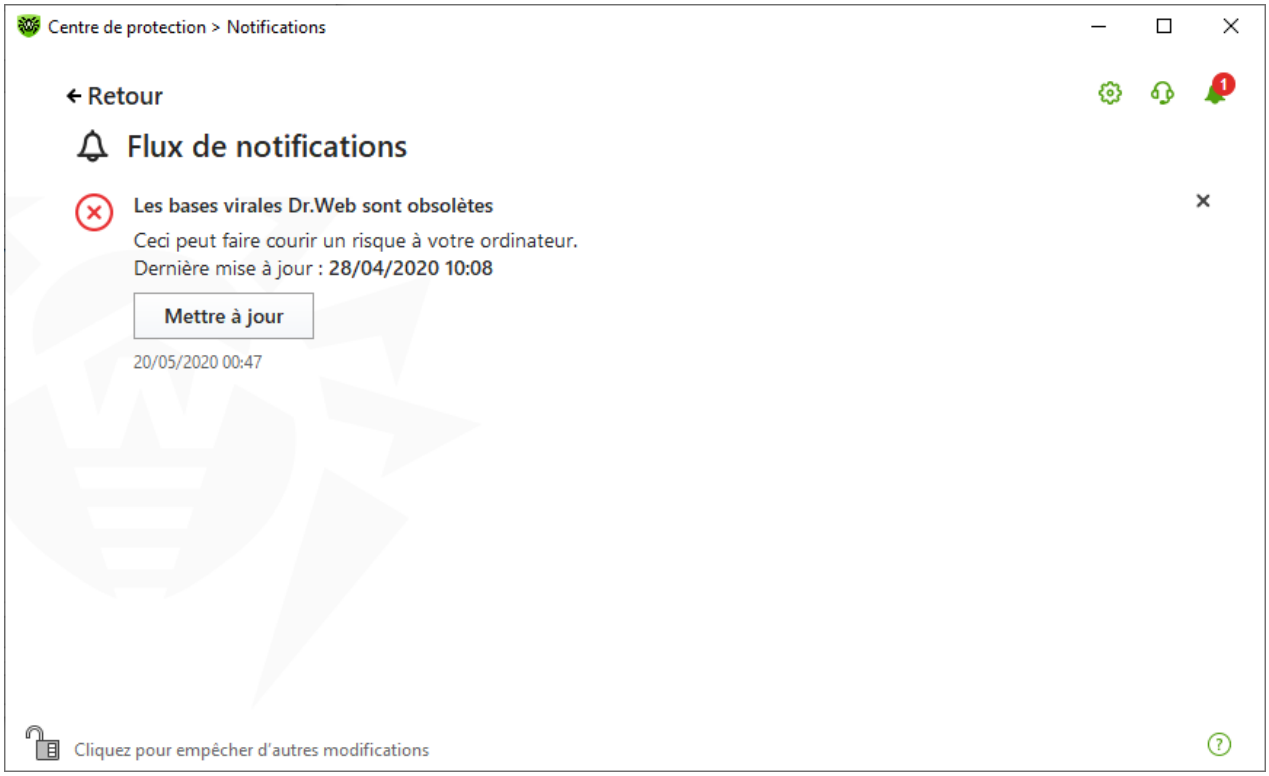

Figure 19. Fenêtre du flux de notifications

Délai de stockage des notifications

Le délai de stockage de notifications est de deux semaines. En cas de résolution de problèmes, les notification sont également supprimées.

Types de notifications

Notifications critiques	
Licence	• La licence actuelle est introuvable. • La licence actuelle est bloquée.
Menaces	• Une menace est détectée. • Vous devez redémarrer l'ordinateur pour neutraliser les menaces. • Les bases virales sont obsolètes.
Notifications majeures	
Licence	• La licence va bientôt expirer. • La licence actuelle est bloquée.
Mise à jour	• Vous devez redémarrer l'ordinateur pour que les mises à jour soient prises en compte.
Notifications mineures	
Nouvelle version	• Une nouvelle version du produit est disponible.

Paramètres d'affichage

Les paramètres d'affichage de notifications dupliquent les paramètres de pop-ups. Si vous voulez modifier les paramètres d'affichage pour que certaines notifications ne s'affichent pas dans le flux, il faut décocher la case contre l'élément nécessaire dans la colonne **Écran** de la fenêtre **Paramètres des notifications** (voir la rubrique Paramètres de notifications).

9. Paramètres du logiciel

Pour modifier les paramètres du programme

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas.
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de configuration va s'ouvrir.

> Si vous avez coché la case **Protéger les paramètres de Dr.Web par un mot de passe** dans les paramètres généraux, vous êtes invité à entrer le mot de passe pour accéder aux paramètres généraux de Dr.Web.

Dans cette section :

- Général : protection des paramètres par un mot de passe, sélection de la langue du programme, importation et exportation des paramètres.
- Notifications : configuration de l'affichage de notifications sur l'écran et la réception de notifications par e-mail.
- Mise à jour : modification de la source et de la périodicité des mises à jour, création d'un miroir de mise à jour.
- Réseau : configuration de l'utilisation du serveur proxy et de l'analyse des données transmises via des protocoles sécurisés.
- Autoprotection : configuration des paramètres avancés de la sécurité.
- Dr.Web Cloud : configuration de l'accès au services Cloud de Doctor Web.
- Réseau antivirus : configuration de l'accès distant à Dr.Web installé sur votre ordinateur.
- Paramètres de l'analyse de fichiers : configuration des paramètres de fonctionnement du Scanner.

9.1. Paramètres généraux

Les paramètres généraux comprennent les paramètres suivants :

- protection des paramètres par un mot de passe ;
- sélection de la langue du logiciel ;
- gestion des paramètres du logiciel (importation, exportation, réinitialisation des paramètres par défaut) ;
- configuration de journalisation ;
- paramètres de quarantaine ;
- paramètres de suppression automatique des entrées statistiques.

Pour ouvrir les paramètres généraux

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas.
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de paramètres généraux va s'ouvrir. Sélectionnez l'élément **Général** dans la partie gauche de la fenêtre.

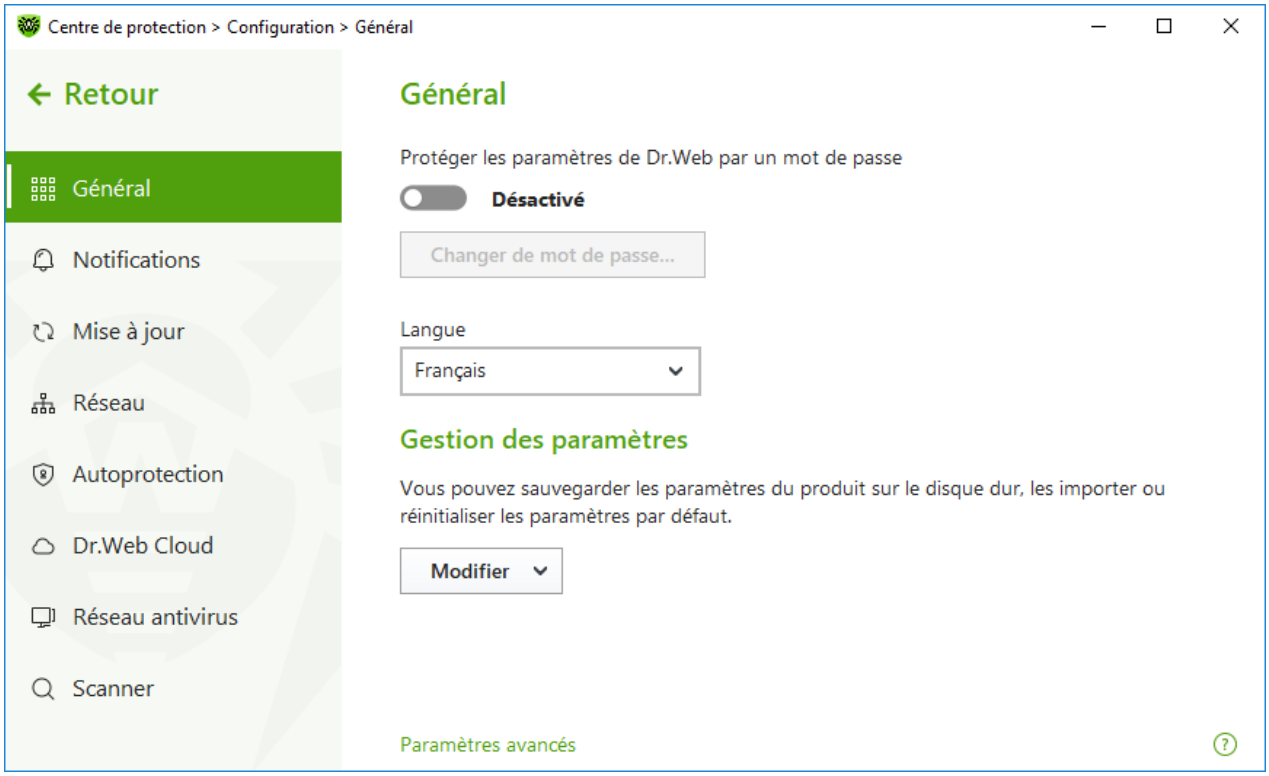

Figure 20. Paramètres généraux

9.1.1. Protection des paramètres par un mot de passe

Vous pouvez restreindre l'accès aux paramètres de Dr.Web sur votre ordinateur à l'aide d'un mot de passe. Le mot de passe sera demandé à chaque recours aux paramètres de Dr.Web.

Pour spécifier un mot de passe

1. Dans la fenêtre de modification des paramètres généraux, activez l'option **Protéger les paramètres de Dr.Web par un mot de passe** avec l'interrupteur correspondant.

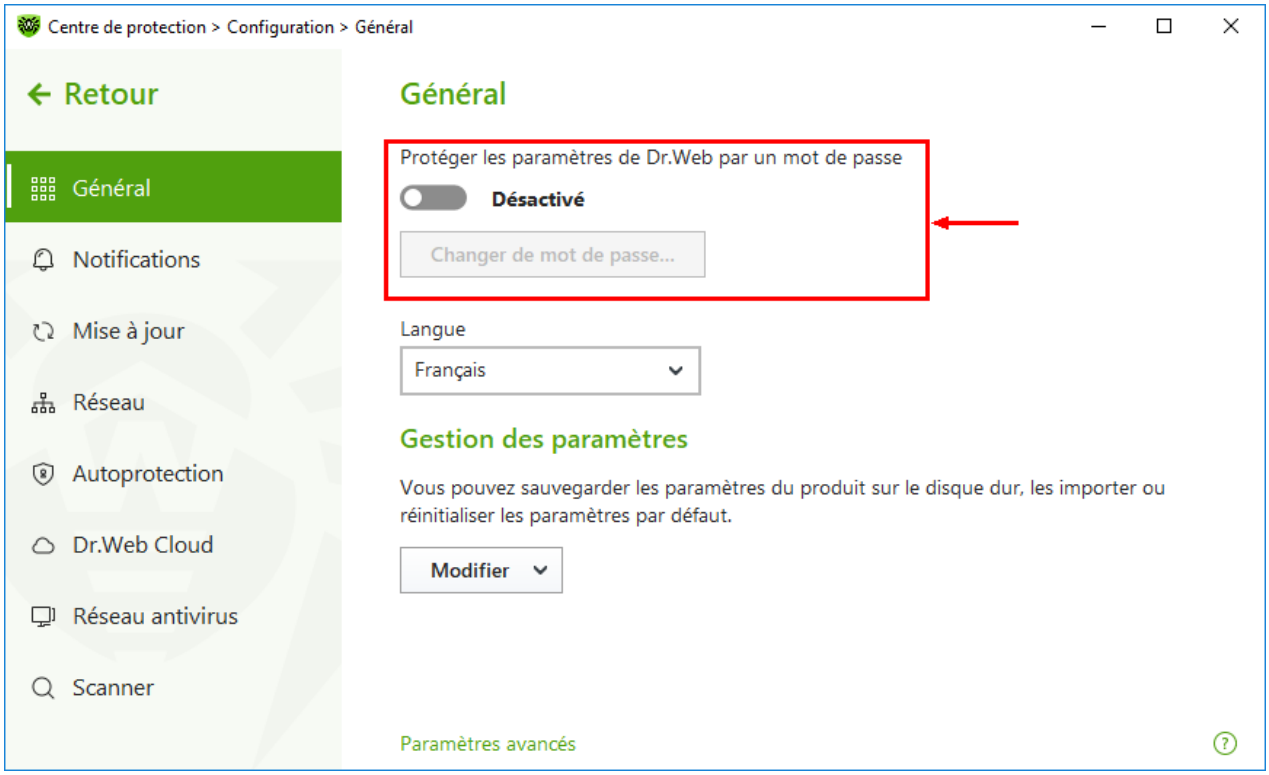

Figure 21. Protection des paramètres par un mot de passe

2. Dans la fenêtre qui s'ouvre, spécifiez un mot de passe et confirmez-le.
3. Cliquez sur le bouton **OK**.

Si vous avez oublié le mot de passe, il faut réinstaller Dr.Web sans sauvegarder les paramètres actuels.

9.1.2. Sélection de la langue du logiciel

Si nécessaire, vous pouvez changer la langue d'interface du logiciel. La liste de langues se complète automatiquement et elle contient toutes les localisations disponibles pour le moment de l'interface graphique de Dr.Web. Pour ce faire, sélectionnez la langue nécessaire dans la liste déroulante **Langue**.

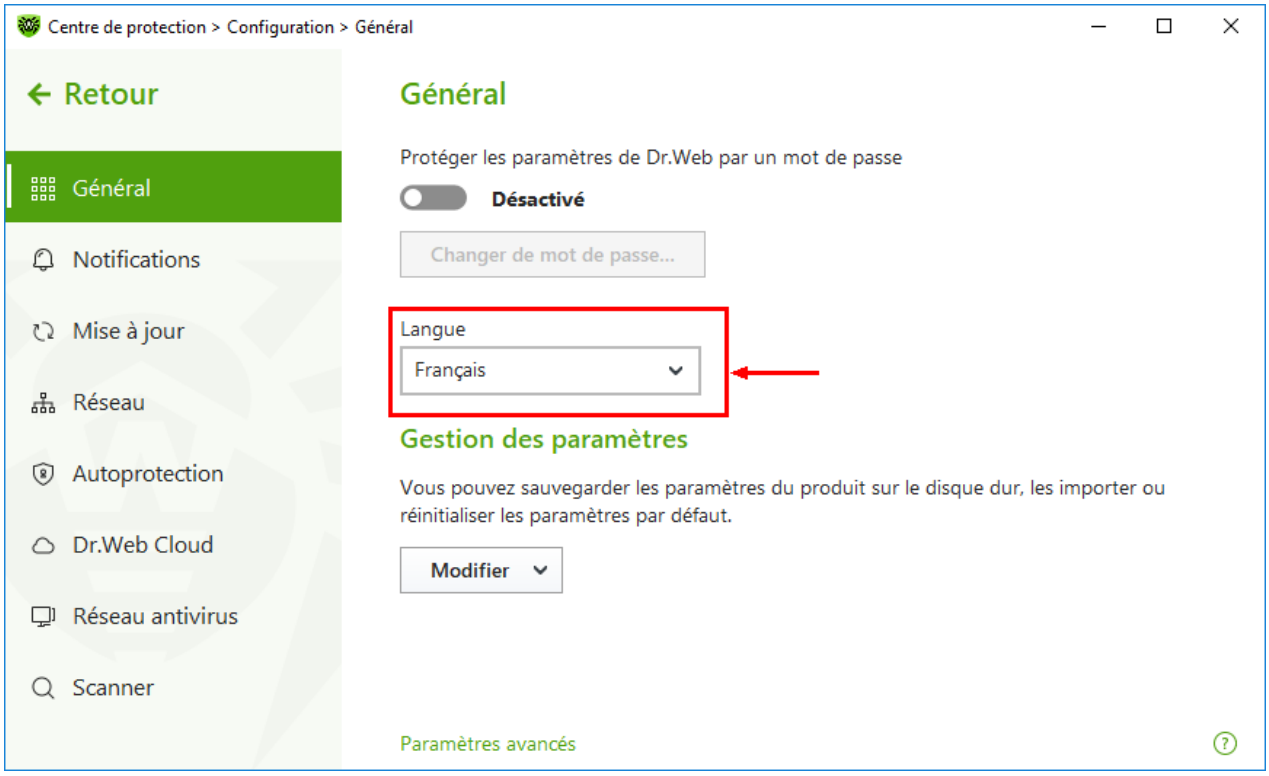

Figure 22. Sélection de la langue du logiciel

9.1.3. Gestion des paramètres de Dr.Web

Pour la gestion des paramètres, sélectionnez une des valeurs suivantes dans la liste déroulante du groupe de paramètres **Gestion des paramètres** :

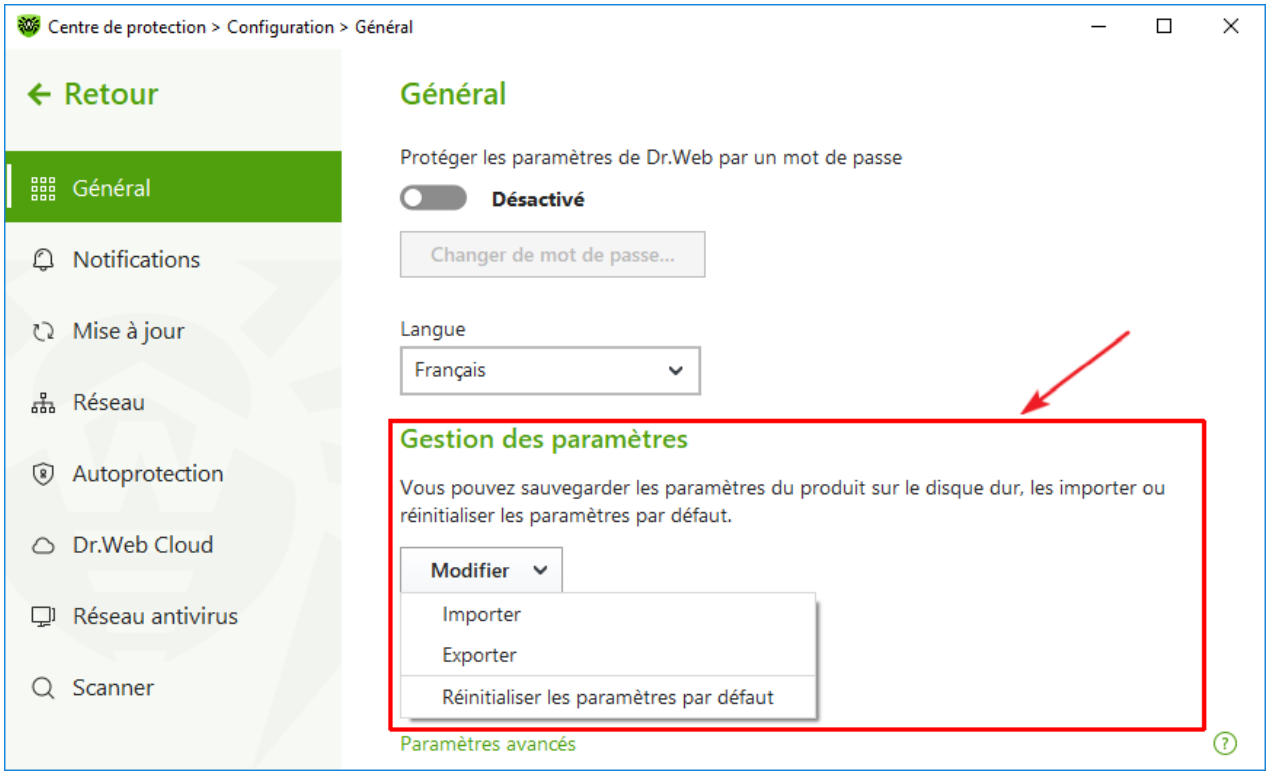

Figure 23. Gestion des paramètres

- **Réinitialiser les paramètres par défaut** pour réinitialiser les paramètres par défaut.
- **Importer**, si vous souhaitez utiliser les paramètres de Dr.Web que vous avez déjà configurés sur un autre ordinateur.
- **Exporter**, si vous souhaitez utiliser vos paramètres sur d'autres ordinateurs. Ensuite, utilisez la fonction d'importation des paramètres sur l'autre ordinateur.

9.1.4. Journalisation de Dr.Web

Vous pouvez activer la journalisation détaillée d'un ou de plusieurs composants ou services Dr.Web.

Pour modifier les paramètres de journalisation

1. Cliquez sur le lien **Paramètres avancés**.
2. Dans la section de configuration de **Journal**, cliquez sur le bouton **Modifier**.

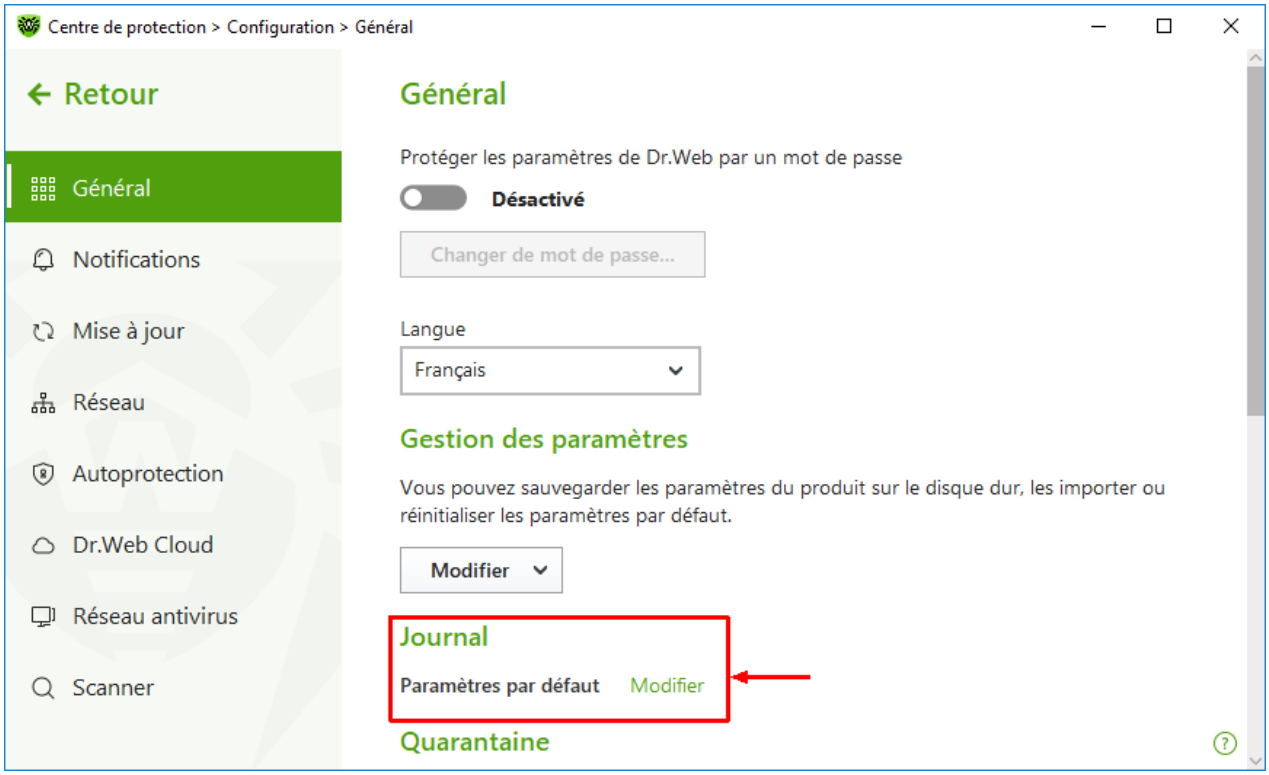

Figure 24. Paramètres généraux. Journal

La fenêtre de configuration de journalisation détaillée va s'ouvrir :

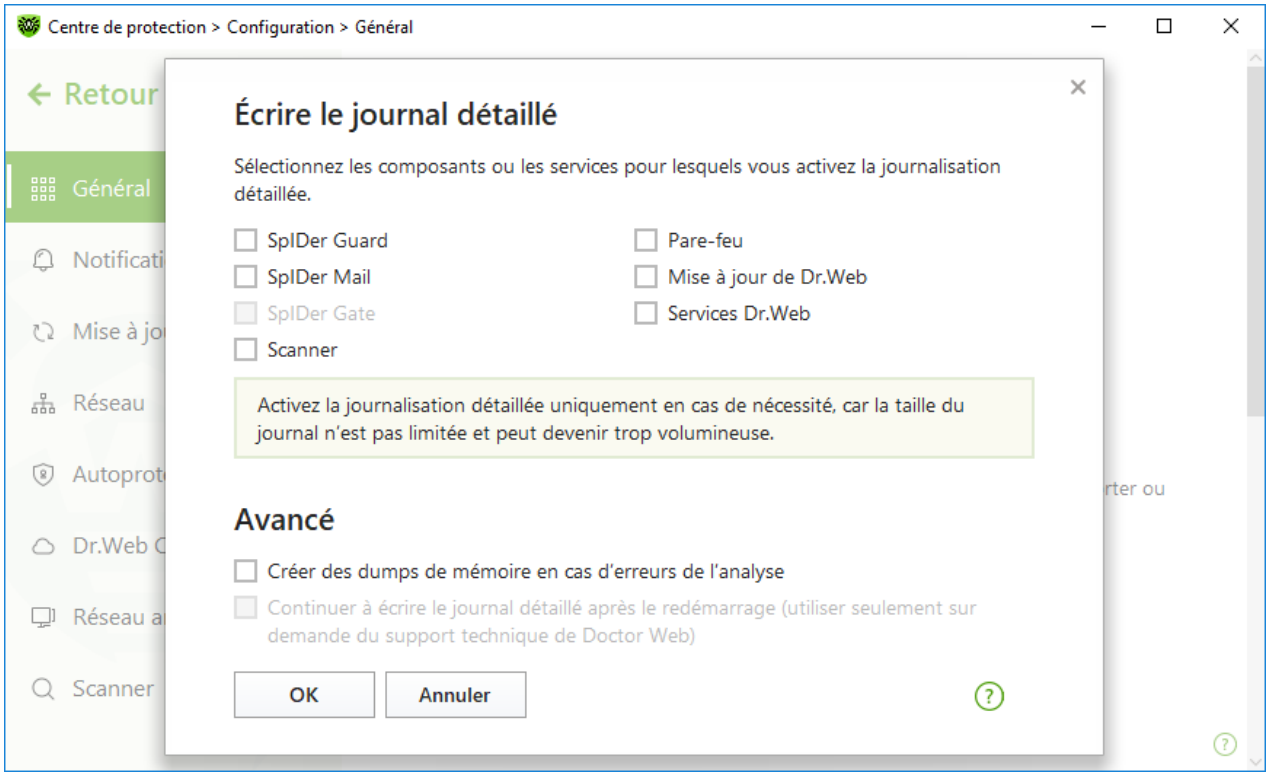

Figure 25. Configuration de journalisation

3. Sélectionnez les composants pour lesquels la journalisation détaillée sera activée. Par défaut pour tous les composants de Dr.Web le journal est enregistré en mode standard et les informations suivantes sont enregistrées :

Composant	Information
SpIDer Guard	Les heures des mises à jour et des démarrages/arrêts de SpIDer Guard, les événements viraux, les noms des fichiers scannés, les noms des packers et le contenu des objets complexes scannés (archives, pièces jointes d'e-mail, conteneurs de fichiers). Il est recommandé d'utiliser ce mode pour déterminer les objets les plus fréquemment scannés par le moniteur du système de fichiers SpIDer Guard. Si nécessaire, vous pouvez ajouter ces objets dans la liste des exclusions pour réduire la charge sur l'ordinateur.
SpIDer Mail	Les heures des mises à jour et des démarrages/arrêts de l'antivirus de messagerie SpIDer Mail, les événements viraux, les paramètres d'interception des connexions, les informations sur les fichiers scannés, les noms des packers et le contenu des archives scannées. Il est recommandé d'utiliser ce mode lors du test des paramètres d'interception des connexions avec les serveurs de messagerie.
Scanner	Les mises à jour des modules de scan, les informations sur les bases virales, le démarrage et l'arrêt du Scanner, les menaces détectées, ainsi que les informations sur les noms des packers et sur le contenu des archives analysées.
Pare-feu	Les informations sur les requêtes reçues par le service et les décisions les concernant, les informations sur des connexions inconnues avec la raison de requête, les informations sur des erreurs. Si vous activez les journaux détaillés, le Pare-feu collecte des données sur les paquets réseau (pcap logs).
Mise à jour de Dr.Web	Liste des fichiers Dr.Web mis à jour et état de leur téléchargement, détails sur l'exécution de scripts auxiliaires, date et heure des mises à jour, détails sur le redémarrage des composants Dr.Web après la mise à jour.
Services Dr.Web	Informations sur les composants Dr.Web, modification de paramètres des composants, activation ou désactivation des composants, événements relatifs à la protection préventive, connexion au réseau antivirus.

Créer des dumps de mémoire

L'option **Créer des dumps de mémoire en cas d'erreurs de l'analyse** permet de sauvegarder les informations utiles sur le fonctionnement de certains composants de Dr.Web ce qui aide les spécialistes du support technique de Doctor Web à analyser un problème en détails et à trouver une solution. Il est recommandé d'activer cette option sur demande du support technique de Doctor Web ou lorsque des erreurs de scan ou de neutralisation surviennent. Le dump de mémoire est sauvegardé dans un fichier `.dmp` situé dans le dossier `%PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\`.

Pour activer les journaux détaillés

En cas de journalisation détaillée le maximum d'informations sur le fonctionnement des composants Dr.Web est fixé. Cela va désactiver la restriction de la taille de fichiers du journal et augmenter la charge de Dr.Web et du système d'exploitation. Il est recommandé d'utiliser ce mode uniquement lorsque des erreurs de composants surviennent ou sur demande du support technique de Doctor Web.

1. Pour activer les journaux détaillés pour un composant Dr.Web, cochez la case correspondante.
2. Par défaut, le mode de journal détaillé est utilisé avant le premier redémarrage de l'OS. S'il est nécessaire d'enregistrer le comportement d'un composant avant et après le redémarrage, cochez la case **Continuer à écrire le journal détaillé après le redémarrage (utiliser seulement sur demande du support technique de Doctor Web)**.
3. Enregistrez les modifications, en cliquant **OK**.

Par défaut, la taille des fichiers de journal est limitée à 10 Mo (pour le composant SpIDer Guard — 100 Mo). Si la taille du fichier de journal excède la limite, le contenu du fichier est réduit à :

- la taille spécifiée si le fichier de journal obtenu après le scan de la session en cours n'excède pas cette limite ;
- la taille du fichier de journal obtenu après le scan de la session en cours, si le fichier de journal global excède la limite.

9.1.5. Paramètres de quarantaine

Pour ne pas surcharger le disque, vous pouvez spécifier les paramètres de stockage d'objets en quarantaine tels que le délai de conservation des objets et la création du dossier de la quarantaine sur un support amovible.

Pour modifier les paramètres de stockage des menaces détectées

1. Dans la fenêtre de modification des paramètres généraux, cliquez sur le lien **Paramètres avancés**.
2. Dans la section des paramètres **Quarantaine**, activez ou désactivez l'option nécessaire avec l'interrupteur .

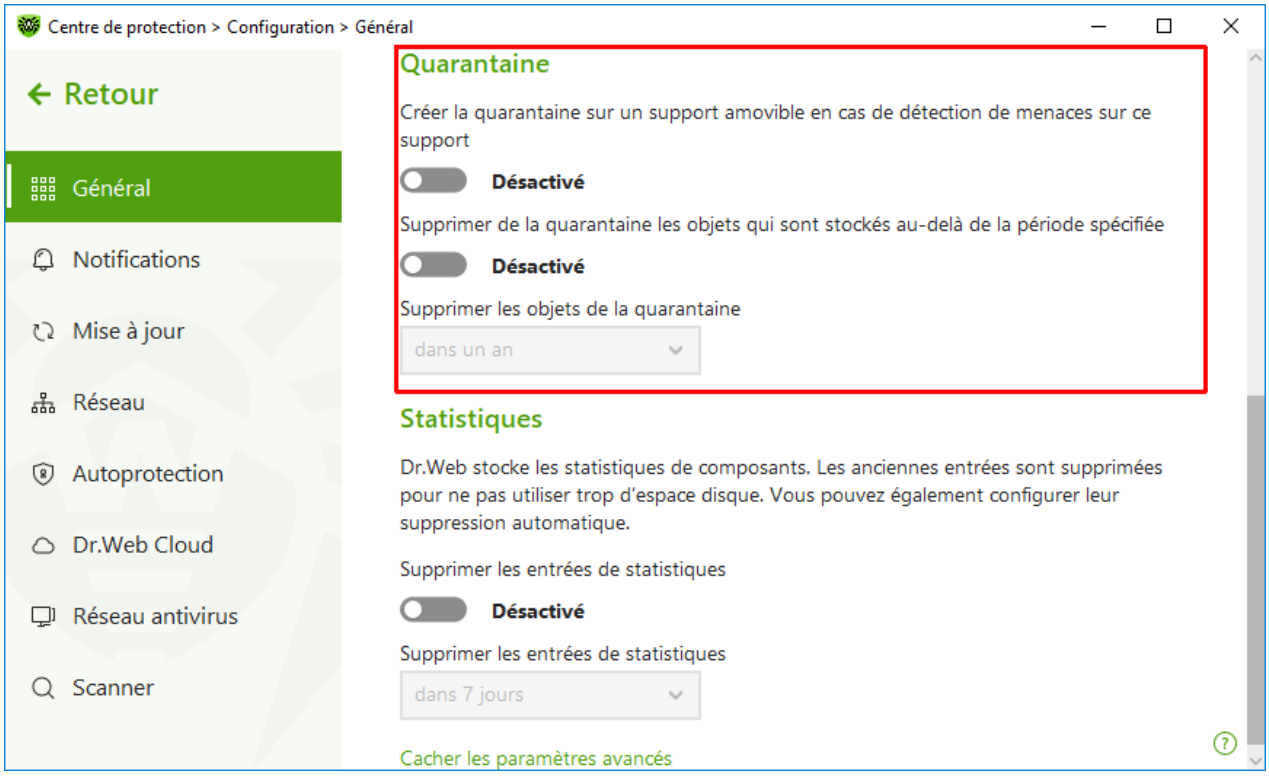

Figure 26. Configuration de la quarantaine

3. Si la suppression automatique des objets de la quarantaine est activée, sélectionnez le délai dans le menu déroulant. Les objets stockés au-delà de ce délai seront supprimés.

Création d'une quarantaine sur un support amovible

En cas de détection d'une menace sur un support amovible, l'option **Créer la quarantaine sur un support amovible en cas de détection de menaces sur ce support** vous permettra de créer un dossier de quarantaine sur le même support et déplacer les menaces dans ce dossier sans chiffrement préalable. Le dossier de quarantaine est créé sur le support amovible uniquement lorsqu'il est accessible en écriture. L'utilisation de dossiers séparés et le non chiffrement sur les supports amovibles prévient la perte de données.

Si l'option est désactivée, les menaces détectées sur des supports amovibles sont déplacées en quarantaine se trouvant sur un disque local.

Suppression automatique des objets de la quarantaine

Pour ne pas utiliser trop d'espace disque, activez la suppression automatique des objets de la quarantaine.

9.1.6. Suppression automatique des entrées statistiques

Par défaut, Dr.Web stocke un nombre optimal d'entrées statistiques pour ne pas utiliser trop d'espace disque. De plus, vous pouvez activer la suppression automatiques des entrées conservées au-delà du délai spécifié.

Pour activer ou désactiver la suppression automatique des entrées statistiques

1. Dans la fenêtre de modification des paramètres généraux, cliquez sur le lien **Paramètres avancés**.
2. Dans la section des paramètres **Statistiques**, activez ou désactivez la suppression automatique des entrées statistiques à l'aide de l'interrupteur .

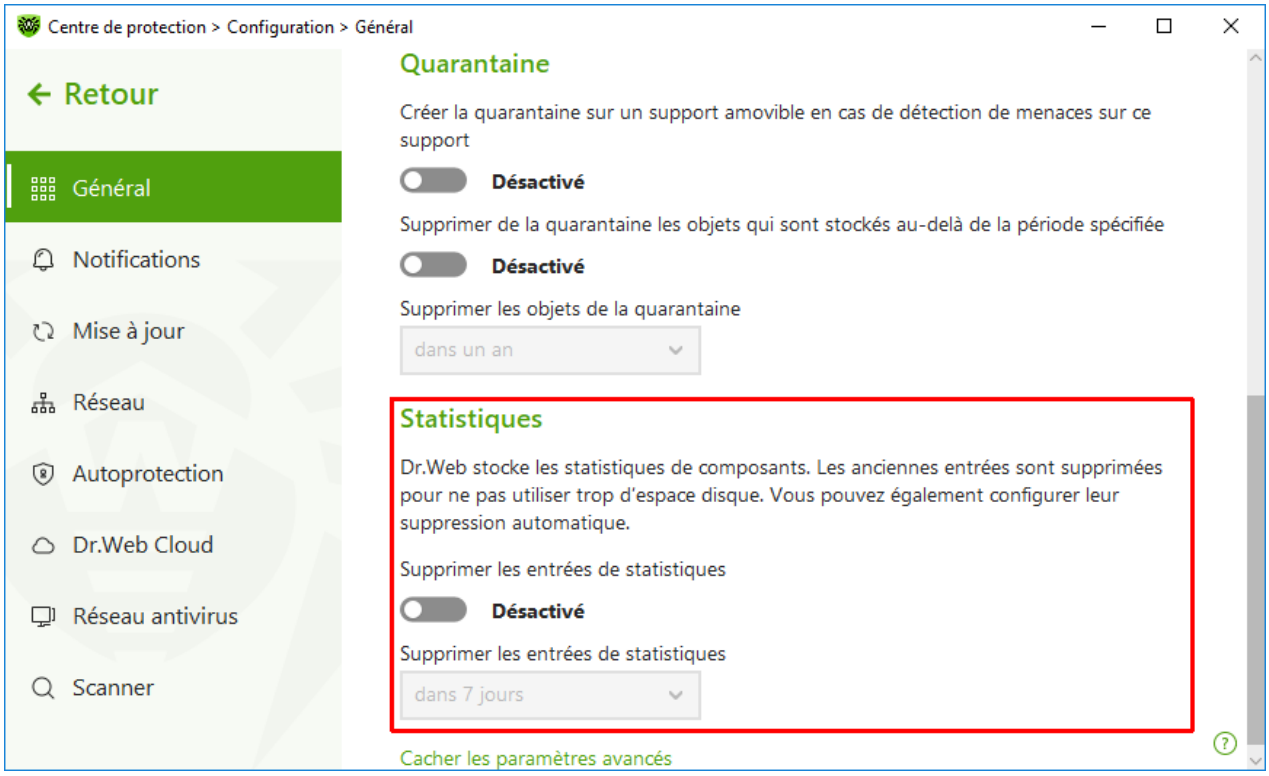

Figure 27. Paramètres des statistiques

3. Si la suppression automatique des entrées statistiques est activée, sélectionnez le délai dans le menu déroulant. Les entrées stockées au-delà de ce délai seront supprimés.

9.2. Paramètres de notifications

Vous pouvez configurer les paramètres de réception des notifications des événements critiques et majeurs de fonctionnement de Dr.Web.

Dans cette section :

- Configuration des paramètres de notifications
- Configuration de l'affichage de notifications sur l'écran

- Configuration de l'envoi de notifications par e-mail

Si nécessaire, configurez les paramètres de réception des notifications des événements critiques et majeurs de fonctionnement de Dr.Web.

Pour ouvrir les paramètres de notifications

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de paramètres généraux va s'ouvrir. Sélectionnez l'élément **Notifications** dans la partie gauche de la fenêtre.

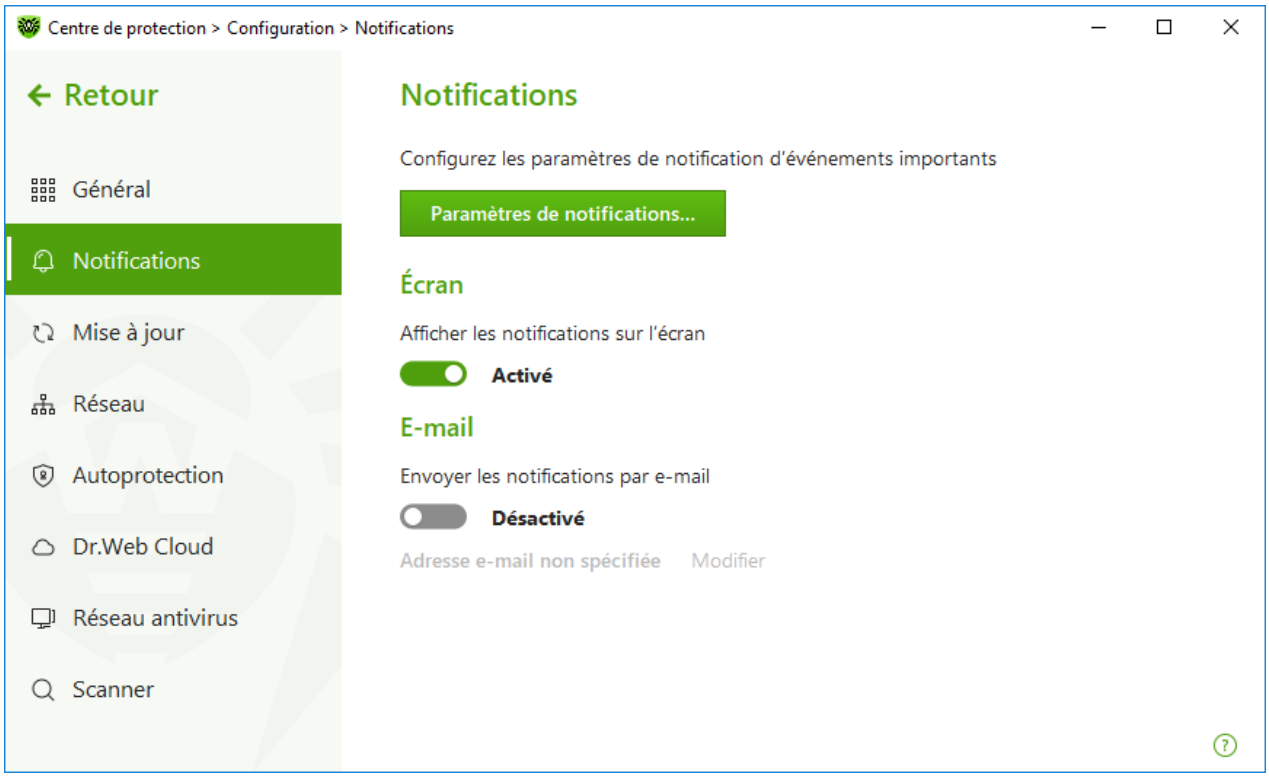

Figure 28. Paramètres de notifications

Pour configurer les paramètres de notifications

1. Cliquez sur **Paramètres des notifications**.
2. Choisissez les notifications que vous souhaitez recevoir.
   - Pour que les notifications s'affichent sur l'écran, cochez la case correspondante dans la colonne **Écran**.
   - Pour recevoir les notifications par e-mail, cochez la case dans la colonne **E-mail**.

   Si vous ne voulez pas recevoir les notifications sur les événements, décochez les cases.

Type de notification	Description
Menace détectée	Notifications des menaces détectées par SpIDer Guard. Ces notifications sont activées par défaut.
Notifications critiques	Notifications critiques des événements suivants : • Des connexions en attente de réponse du Pare-feu sont détectées. Ces notifications sont activées par défaut.
Notifications majeures	Notifications importantes des événements suivants : • Les bases virales Dr.Web sont obsolètes. • Une tentative de modifier la date et l'heure système a été bloquée. • L'accès à l'objet protégé est bloqué par l'Analyse de comportement. • L'accès à l'objet protégé est bloqué par la Protection contre les exploits. • L'accès à l'objet protégé est bloqué par la Protection contre les ransomwares. • Informations sur les mises à jour et support du produit. Les notifications sont activés par défaut.
Notifications mineurs	Notifications mineures des événements suivants : • Mise à jour réussie. • Erreur de la mise à jour. Les notifications sont désactivées par défaut.
Licence	Notifications des événements suivants : • La licence va bientôt expirer. • La licence actuelle est introuvable. • La licence actuelle est bloquée.

3. Si nécessaire, configurez les paramètres avancés d'affichage des notifications :

Option	Description
Ne pas afficher les notifications en mode plein écran	Affichage des notifications lorsque vous utilisez les applications en mode plein écran (affichage des filmes, graphiques etc.). Décochez la case pour recevoir toujours de telles notifications.
Afficher les notifications du Pare-feu dans une fenêtre séparée en	Affichage des notifications du Pare-feu sur un bureau séparée lorsque les applications tournent en mode plein écran (jeux,

Option	Description
mode plein écran	vidéo). Décochez la case pour afficher les notifications sur le même bureau que celui où l'application est lancée en mode plein écran.

4. Si vous avez choisi une ou plusieurs notifications e-mail, configurez l'envoi d'e-mails depuis votre ordinateur.

> ⚠ Les notifications de certains événements ne sont pas inclues dans les groupes listés et s'affichent toujours à l'utilisateur :
>
> - installation des mises à jour prioritaires exigeant un redémarrage ;
> - redémarrage pour achever la neutralisation des menaces ;
> - redémarrage automatique ;
> - demande d'autorisation de modification de l'objet par le processus
> - un nouveau clavier est connecté.

Notifications pop-up

Dans la fenêtre de notifications, activez l'option correspondante pour recevoir des notifications pop-up au-dessus de l'icône de Dr.Web dans la zone de notification Windows.

Notifications e-mail

Pour recevoir des notifications sur les événements par e-mai

1. Dans la fenêtre de paramètres, activez l'option **Envoyer les notifications par e-mail**.
2. Dans la fenêtre qui s'affiche, spécifiez l'adresse e-mail que vous souhaitez utiliser pour recevoir les notifications. Il est nécessaire de confirmer l'utilisation de cette adresse à l'étape 7.

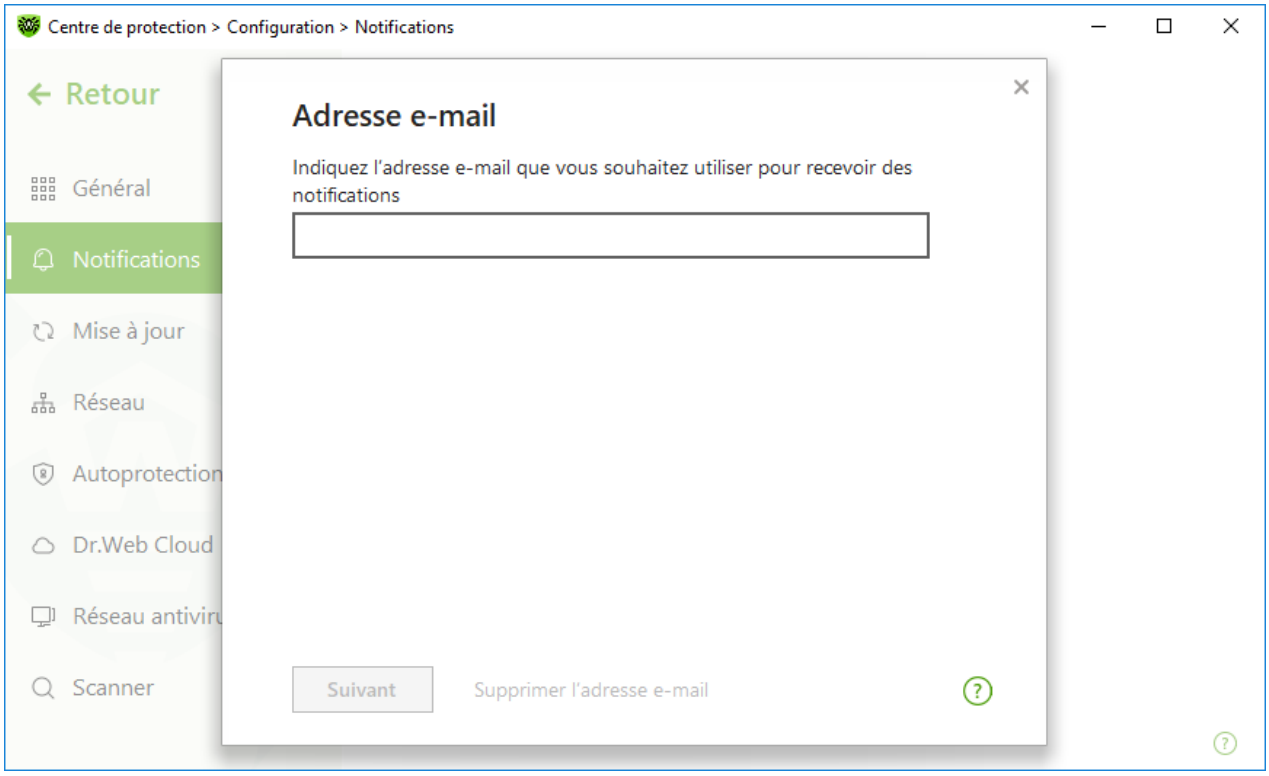

Figure 29. Indication de l'adresse pour les notifications e-mail

3. Cliquez sur **Suivant**.
4. Dans la fenêtre qui s'ouvre, indiquez les données du compte depuis lequel les notifications seront envoyées.
   - Si la liste des serveurs de messagerie contient le serveur nécessaire, sélectionnez-le et indiquez le login et le mot de passe de votre compte.
   - Si la liste des serveurs de messagerie ne contient pas le serveur nécessaire, cliquez sur **Spécifiez manuellement** et remplissez les champs nécessaires dans la fenêtre qui s'affiche :

Paramètre	Description
Serveur SMTP	Entrez l'adresse du serveur de messagerie qui sera utilisé par Dr.Web pour envoyer les notifications e-mail.
Port	Entrez le port du serveur de messagerie auquel Dr.Web va se connecter pour envoyer des notifications e-mail.
Login	Entrez le login pour se connecter au serveur de messagerie.
Mot de passe	Entrez le mot de passe à utiliser pour se connecter au serveur de messagerie.
Utiliser SSL/TLS	Cochez cette case pour utiliser le chiffrement SSL/TLS lors de la transmission de messages.
Authentification NTLM	Cochez cette case pour effectuer l'authentification via le protocole NTLM.

5. Cliquez sur le lien **Envoyer un message de test** si vous voulez vérifier si le compte est indiqué correctement. Le message sera envoyé à l'adresse depuis laquelle les notifications doivent être envoyées (configurée à l'étape 4).
6. Cliquez sur **Suivant**.
7. Entrez le code de confirmation qui sera envoyée à l'adresse e-mail que vous avez indiquée à l'étape 2 pour recevoir les notifications. Si vous n'avez pas reçu le code pendant 10 minutes, cliquez sur **Envoyer le code encore une fois**. Si vous n'entrez pas le code de confirmation, les notifications ne seront pas envoyées à cette adresse.

Pour modifier l'adresse e-mail et les autres paramètres, cliquez sur **Modifier** dans la fenêtre de configuration des notifications (voir la figure Configuration des notifications) et répétez toutes les actions à commencer par l'étape 2.

9.3. Paramètres de mise à jour

Configurez la période de réception de mises à jour et la source de mises à jour des bases virales et des composants. Vous pouvez également créer un miroir de mise à jour pour recevoir des mises à jour sur un autre ordinateur.

Vous pouvez configurer les paramètres suivants de la mise à jour de Dr.Web :

- périodicité des mises à jour ;
- source de mises à jour ;
- composants à mettre à jour ;
- miroir de mise à jour.

Pour ouvrir les paramètres des mises à jour

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de paramètres généraux va s'ouvrir. Sélectionnez l'élément **Mise à jour** dans la partie gauche de la fenêtre.

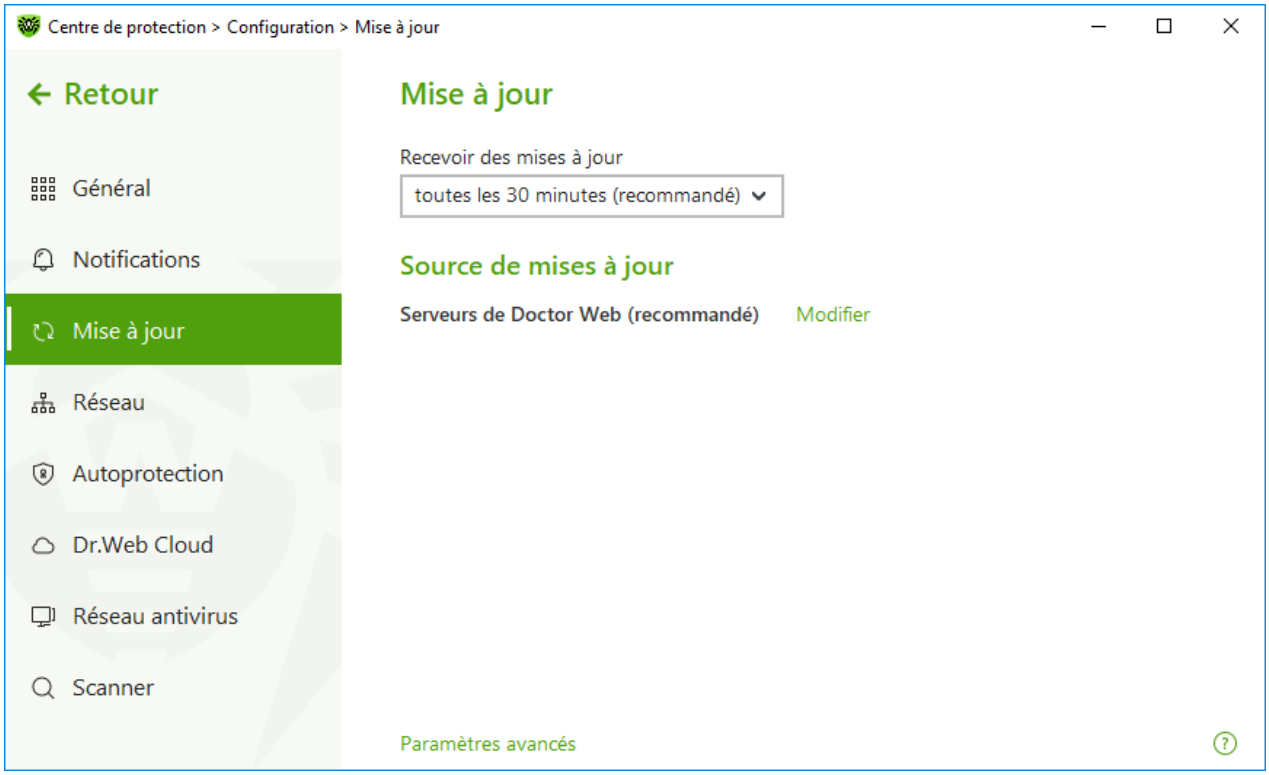

Figure 30. Paramètres de la mise à jour

Périodicité des mises à jour

La valeur par défaut (30 minutes) est optimale pour maintenir les informations sur les menaces à jour. Pour changer la périodicité de mises à jour, sélectionnez la valeur nécessaire dans le menu déroulant.

La mise à jour automatique se fait en tâche de fond. Vous pouvez également sélectionner la valeur **Manuellement** dans la liste déroulante. Dans ce cas, il vous faudra lancer la mise à jour de Dr.Web manuellement.

Configuration de la source de mises à jour

La valeur **Serveurs de Doctor Web (recommandé)** est spécifiée par défaut en tant que source de mises à jour.

Pour configurer la source de mises à jour qui vous convient le mieux

1. Dans la fenêtre de configuration de la mise à jour (voir la figure Paramètres de la mise à jour) dans la section **Source de mises à jour**, cliquez sur le lien **Modifier**. La fenêtre de configuration de la source de mises à jour va s'ouvrir.

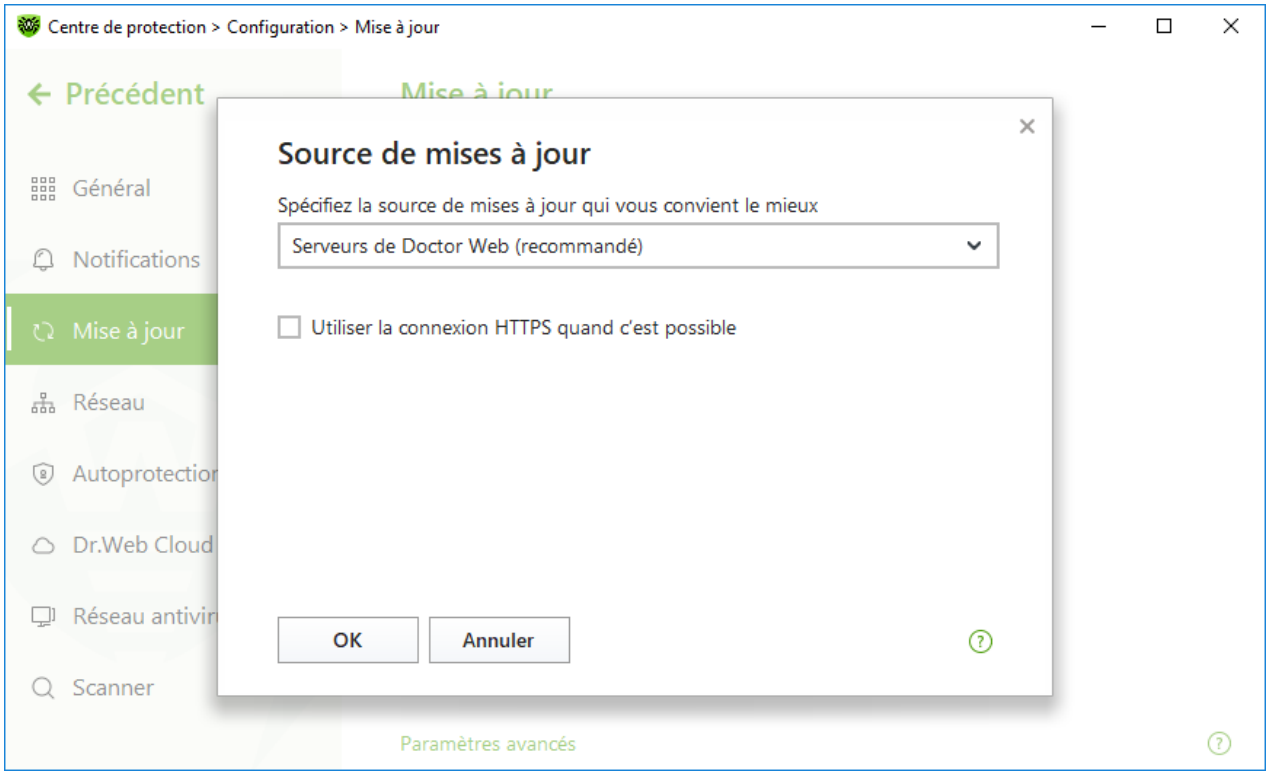

Figure 31. Configuration de la source de mises à jour

2. Sélectionnez la source de mises à jour qui vous convient le mieux dans la liste déroulante.
   - **Serveurs de Doctor Web (recommandé)**. La mise à jour s'effectue depuis les serveurs de Doctor Web via Internet. Si vous voulez télécharger les mises à jour via le protocole sécurisé et que cela est possible, activez l'option **Utiliser la connexion HTTPS quand c'est possible**.
   - **Dossier local ou réseau**. La mise à jour se fait depuis le dossier local ou le dossier réseau dans lequel ont été copiées les mises à jour. Spécifiez le chemin d'accès au dossier (en cliquant sur **Parcourir** ou en entrant le chemin au format UNC manuellement), ainsi que le nom de l'utilisateur et le mot de passe si nécessaire.
   - **Réseau antivirus**. La mise à jour sera effectuée via le réseau local depuis l'ordinateur sur lequel le produit Dr.Web est installé et un miroir de mise à jour a été créé. Sélectionnez l'ordinateur qui sera utilisé en tant que source de mises à jour.
3. Cliquez sur **OK** pour enregistrer les modifications.

Si un autre produit Dr.Web en version 12.0 est installé sur votre ordinateur, il est interdit d'indiquer en tant que source de mise à jour un ordinateur sur lequel une version antérieure du produit est installée. Cela peut provoquer des erreurs critiques et des échecs du système.

Paramètres avancés

Pour accéder aux paramètres avancés, cliquez sur le lien **Paramètres avancés** dans la fenêtre **Mise à jour** (voir la figure Paramètres de la mise à jour).

Configuration des composants mis à jour

Vous pouvez choisir l'un des moyens suivants pour télécharger les mises à jour des composants de Dr.Web :

- **Tout (recommandé)**. Les mises à jour des bases virales Dr.Web ainsi que les mises à jour du moteur antivirus et d'autres composants de Dr.Web sont téléchargées ;
- **Uniquement les bases virales**. Seules les mises à jour des bases virales Dr.Web et du moteur antivirus sont téléchargées ; les autres composants de Dr.Web ne sont pas mis à jour.

Création d'un miroir de mise à jour

Le miroir de mise à jour est un dossier dans lequel sont copiées des mises à jour. Le miroir de mise à jour peut être utilisé en tant que source de mises à jour Dr.Web pour les ordinateurs du réseau local qui ne sont pas connectés à Internet.

Pour configurer votre ordinateur en tant que miroir de mise à jour

1. Dans la fenêtre de configuration de la mise à jour (voir la figure Paramètres de la mise à jour), cliquez sur le lien **Paramètres avancés** et activez l'utilisation du miroir de mise à jour à l'aide de l'interrupteur . La fenêtre de configuration du miroir de mise à jour va s'ouvrir.

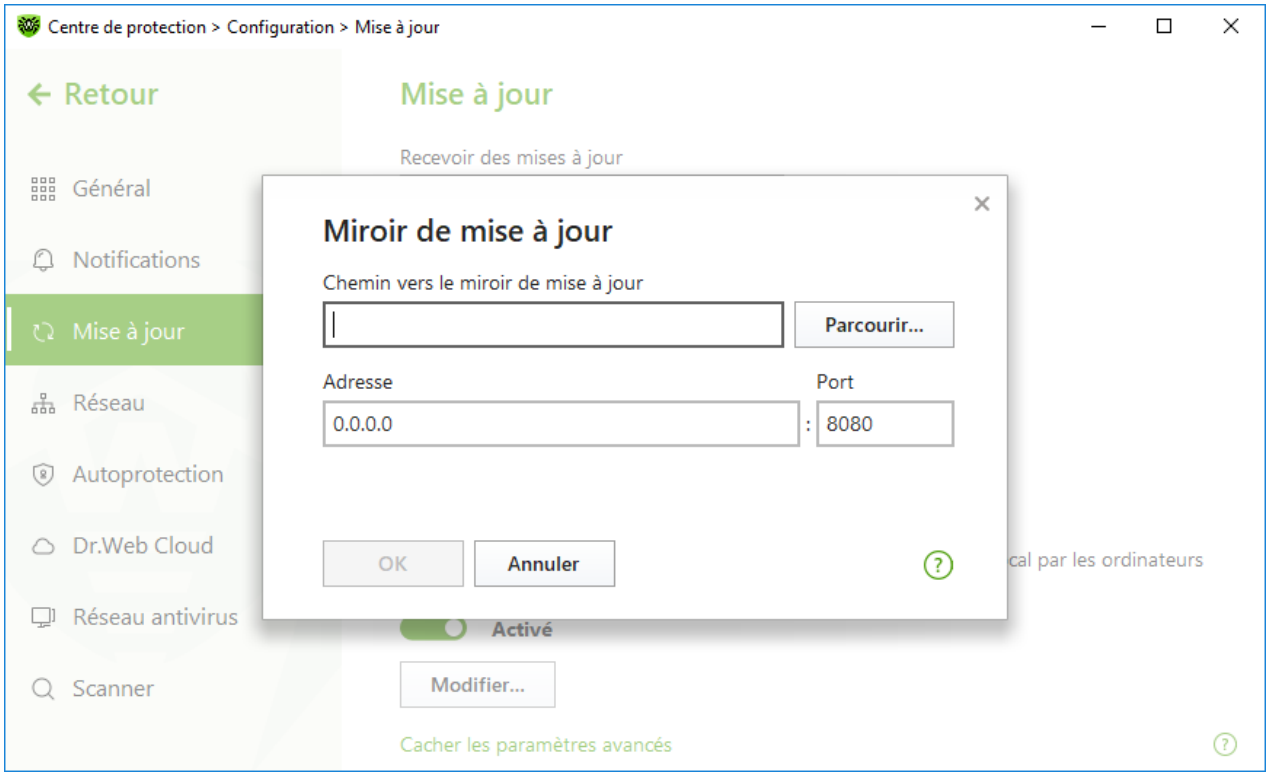

Figure 32. Configuration du miroir de mise à jour

2. Cliquez sur **Parcourir** et sélectionnez le dossier dans lequel les mises à jour seront copiées. Il est recommandé de sélectionner un dossier vide ou créer un nouveau dossier. Si un dossier pas vide

est indiqué, son contenu sera supprimé. Vous pouvez également indiquer manuellement le chemin vers le dossier au format UNC.

3. Si votre ordinateur comprend plusieurs sous-réseaux, vous pouvez indiquer l'adresse qui sera disponible pour un réseau seulement. Vous pouvez également indiquer le port sur lequel le serveur HTTP recevra des requêtes de connexion.
   - Dans le champ **Adresse** est indiqué le nom d'hôte ou l'adresse IP au format IPv4 ou IPv6.
   - Dans le champ **Port** est indiqué un port libre.
4. Cliquez sur **OK** pour enregistrer les modifications.

La périodicité de téléchargement des mises à jour sur le miroir va correspondre à la valeur sélectionnée du menu déroulant **Recevoir des mises à jour**.

9.4. Réseau

Vous pouvez configurer les paramètres de connexion au serveur proxy, activer l'analyse des données transmises par les protocoles cryptographiques et exporter le certificat Dr.Web pour sa future importation dans d'autres programmes.

Dans cette section :

- Configuration de la connexion au serveur proxy
- Analyse des données transmises par les protocoles cryptographiques
- Exportation du certificat Dr.Web

Pour ouvrir les paramètres du réseau

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas.
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de paramètres généraux va s'ouvrir. Sélectionnez l'élément **Réseau** dans la partie gauche de la fenêtre.

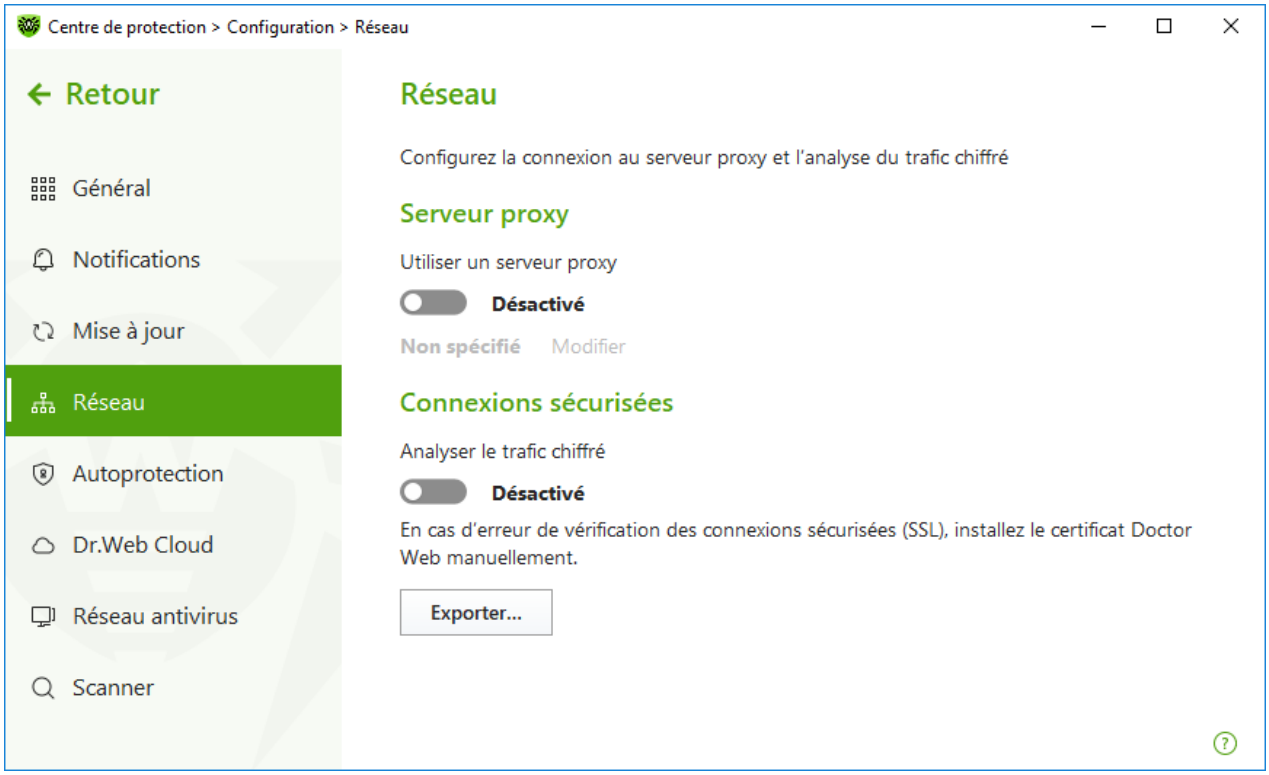

Figure 33. Connexion au serveur proxy et analyse du trafic chiffré

Utiliser le serveur proxy

Vous pouvez activer le mode d'utilisation du serveur proxy et configurer les paramètres de connexion au serveur proxy. Pour ce faire :

1. Activez l'option **Utiliser un serveur proxy** avec l'interrupteur .
2. Cliquez sur **Modifier** pour configurer les paramètres de connexion au serveur proxy :

Paramètre	Description
Adresse	Spécifiez l'adresse du serveur proxy.
Port	Spécifiez le port du serveur proxy.
Login	Spécifiez le nom du compte pour la connexion au serveur proxy.
Mot de passe	Spécifiez le mot de passe du compte utilisé pour se connecter au serveur proxy.
Type d'authentification	Sélectionnez un type d'authentification nécessaire pour se connecter au serveur proxy.

Connexions sécurisées

Pour que Dr.Web analyse les données transmises via les protocoles cryptographiques SSL, TLS ou STARTTLS, activez l'option **Analyser le trafic chiffré**. SpIDer Mail va analyser les données transmises via les protocoles POP3S, SMTPS, IMAPS

Si l'application utilisant les connexions chiffrées ne se connecte pas au stockage de certificats système Windows, il faut exporter le certificat de sécurité de Doctor Web et l'importer manuellement dans chaque application.

Durée de validité du certificat de sécurité — 1 an. Si cela est nécessaire, importez le certificat de nouveau chaque année.

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. Les certificats de sécurité s'appellent également les certificats SSL car le protocole SSL (Secure Socket Layer — couche de sockets sécurisés) est utilisé pour leur fonctionnement. Il assure l'interaction protégé par le chiffrement entre les hôtes du réseau Internet, par exemple entre l'utilisateur et le serveur web.

L'installation (l'importation) du certificat de sécurité d'un hôte web dans le programme utilisant Internet garantit que la communication sera effectuée en mode sécurisé avec la vérification de l'authenticité. Dans ce cas, les cybercriminels auront du mal à intercepter les données.

L'importation du certificat Dr.Web peut être requis pour les logiciels suivants :

- navigateur Opera ;
- navigateur Firefox ;
- client de messagerie Mozilla Thunderbird ;
- client de messagerie The Bat!, etc.

Pour exporter et importer le certificat de sécurité Dr.Web

1. Activez l'option **Analyser le trafic chiffré** avec l'interrupteur  , si le bouton **Exporter** n'est pas actif. Dans ce cas, un certificat de sécurité Dr.Web sera généré.
2. Cliquez sur le bouton **Exporter**.
3. Sélectionnez le dossier dans lequel vous voulez sauvegarder le certificat. Cliquez sur **OK**.
4. Importez le certificat dans l'application nécessaire. Pour en savoir plus sur l'importation du certificat, consultez les documents de référence de l'application nécessaire.

9.5. Autoprotection

Vous pouvez configurer les paramètres de l'autoprotection de Dr.Web contre l'influence non autorisée des programmes attaquant les antivirus ou contre les dommages accidentels.

Dans cette section :

- Activation et désactivation de l'autoprotection
- Interdire de modifier la date et l'heure système

Pour accéder aux paramètres de l'Autoprotection

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de paramètres généraux va s'ouvrir. Sélectionnez l'élément **Autoprotection** dans la partie gauche de la fenêtre.

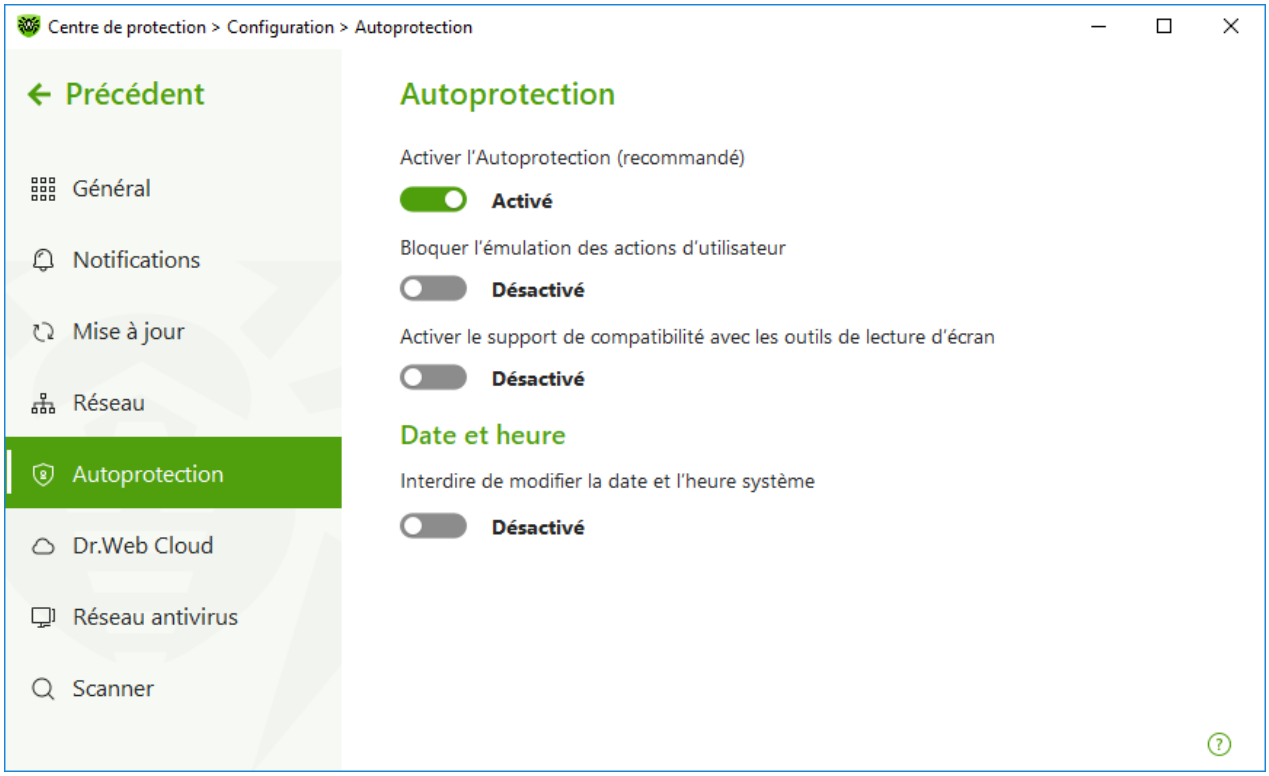

Figure 34. Paramètres de la protection Dr.Web

Paramètres de l'Autoprotection

L'option **Activer l'Autoprotection (recommandé)** permet de protéger les fichiers et les processus de Dr.Web contre l'accès non autorisé. L'Autoprotection est activée par défaut. Il n'est pas recommandé de désactiver l'Autoprotection.

En cas de problèmes survenus lors de l'utilisation d'outils de défragmentation, il est recommandé de désactiver temporairement l'Autoprotection.

Pour réaliser un rollback vers un point de restauration du système, il est nécessaire de désactiver le module de l'Autoprotection.

L'option **Bloquer l'émulation des actions d'utilisateur** permet de prévenir les modifications automatiques dans les paramètres de Dr.Web, y compris l'exécution de scripts qui imitent l'interaction de l'utilisateur avec Dr.Web et qui sont lancés par l'utilisateur (par exemple, des scripts de modification des paramètres de Dr.Web, de suppression de la licence et d'autres actions visant la modification du fonctionnement de Dr.Web).

L'option **Activer le support de compatibilité avec les outils de lecture d'écran** permet d'utiliser les lecteurs d'écran tels que JAWS et NVDA pour énoncer les éléments de l'interface de Dr.Web. Cette fonction rend l'interface du logiciel accessible pour les personnes malvoyantes.

Date et heure

Certains programmes malveillants modifient la date et l'heure système. Dans ce cas, les mises à jour des bases virales ne se font pas selon la planification, la licence peut être considérée comme obsolète et les composants de protection peuvent être désactivés.

L'option **Interdire de modifier la date et l'heure système** permet d'empêcher les modifications manuelles ou automatiques de l'heure et de la date système ainsi que du fuseau horaire. Cette restriction s'applique à tous les utilisateurs. Vous pouvez configurer la réception des notifications afin d'être informé d'une tentative de modification de l'heure système.

9.6. Dr.Web Cloud

Vous pouvez vous connecter au service cloud de Doctor Web et participer au programme d'amélioration de la qualité des produits Dr.Web. Le service cloud collecte les informations sur les dernières menaces sur les postes d'utilisateurs. Grâce à cela, les bases virales sont constamment mises à jour et de nouvelles menaces sont vite supprimées. De plus, les données sont traitées plus vite dans le service cloud que sur l'ordinateur de l'utilisateur.

Dans cette section :

- Service Cloud

- Programme d'amélioration de la qualité du logiciel

Pour activer ou désactiver le composant Dr.Web Cloud

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de paramètres généraux va s'ouvrir. Sélectionnez l'élément **Dr.Web Cloud** dans la partie gauche de la fenêtre.
5. Activez ou désactivez Dr.Web Cloud avec l'interrupteur .

Figure 35. Connexion à Dr.Web Cloud

Service Cloud

Dr.Web Cloud permet à la protection antivirus d'utiliser les informations actuelles sur les menaces, ces informations sont mises à jour sur les serveurs de Doctor Web en temps réel.

En fonction des paramètres de mises à jour, les informations sur les menaces utilisées par les composants de la protection antivirus peuvent être obsolètes. Les services Cloud peuvent, de façon fiable, restreindre l'accès des utilisateurs de votre ordinateur aux sites au contenu indésirable ainsi que restreindre l'accès aux fichiers infectés.

Programme d'amélioration de la qualité du logiciel

Si vous participez au programme d'amélioration de la qualité du logiciel, les données non personnelles sur le fonctionnement de Dr.Web sur votre ordinateur seront périodiquement envoyées sur les serveurs de la société. Les données reçues ne sont pas utilisées pour vous identifier ni vous contacter.

Cliquez sur le lien **Politique de confidentialité de Doctor Web** pour consulter cette politique sur le site officiel de Doctor Web.

9.7. Accès distant à Dr.Web

Pour autoriser ou interdire la gestion à distance du produit Dr.Web

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas.
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de paramètres généraux va s'ouvrir. Sélectionnez l'élément **Réseau antivirus** dans la partie gauche de la fenêtre.
5. Autorisez ou interdisez la gestion à distance du produit Dr.Web avec l'interrupteur.

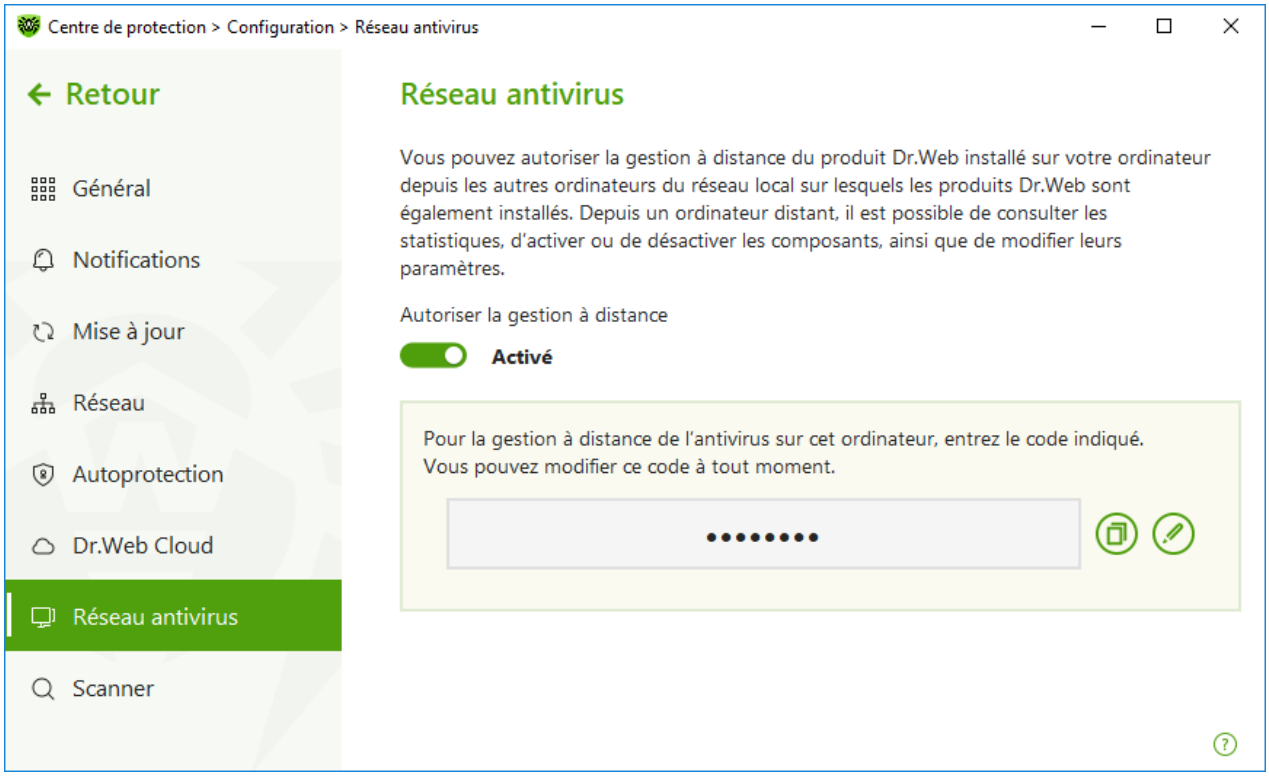

Figure 36. Activation de la gestion distante de l'antivirus

Vous pouvez autoriser l'accès à l'Antivirus Dr.Web sur votre ordinateur. Pour ce faire, activez l'option **Autoriser la gestion à distance** et spécifiez le code qu'il faudra saisir pour la gestion de votre antivirus à distance.

> ⚠ Si vous utilisez la clé pour Dr.Web Security Space vous pouvez télécharger la documentation correspondante sur le site https://download.drweb.com/doc et prendre connaissance du composant Réseau antivirus.

La gestion à distance permet de consulter des statistiques, activer ou désactiver les modules et modifier leurs paramètres. Les composants Quarantaine et Scanner sont indisponibles.

9.8. Paramètres de l'analyse de fichiers

Vous pouvez configurer les paramètres du scanner et modifier les actions par défaut effectuées en cas de détection d'objets malveillants. Les paramètres par défaut permettent une utilisation optimale du produit. Ne les modifiez pas si ce n'est pas nécessaire.

Pour ouvrir les paramètres de l'analyse de fichiers

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
3. Cliquez sur en haut de la fenêtre du programme.
4. La fenêtre de paramètres généraux va s'ouvrir. Sélectionnez l'élément **Scanner** dans la partie gauche de la fenêtre.

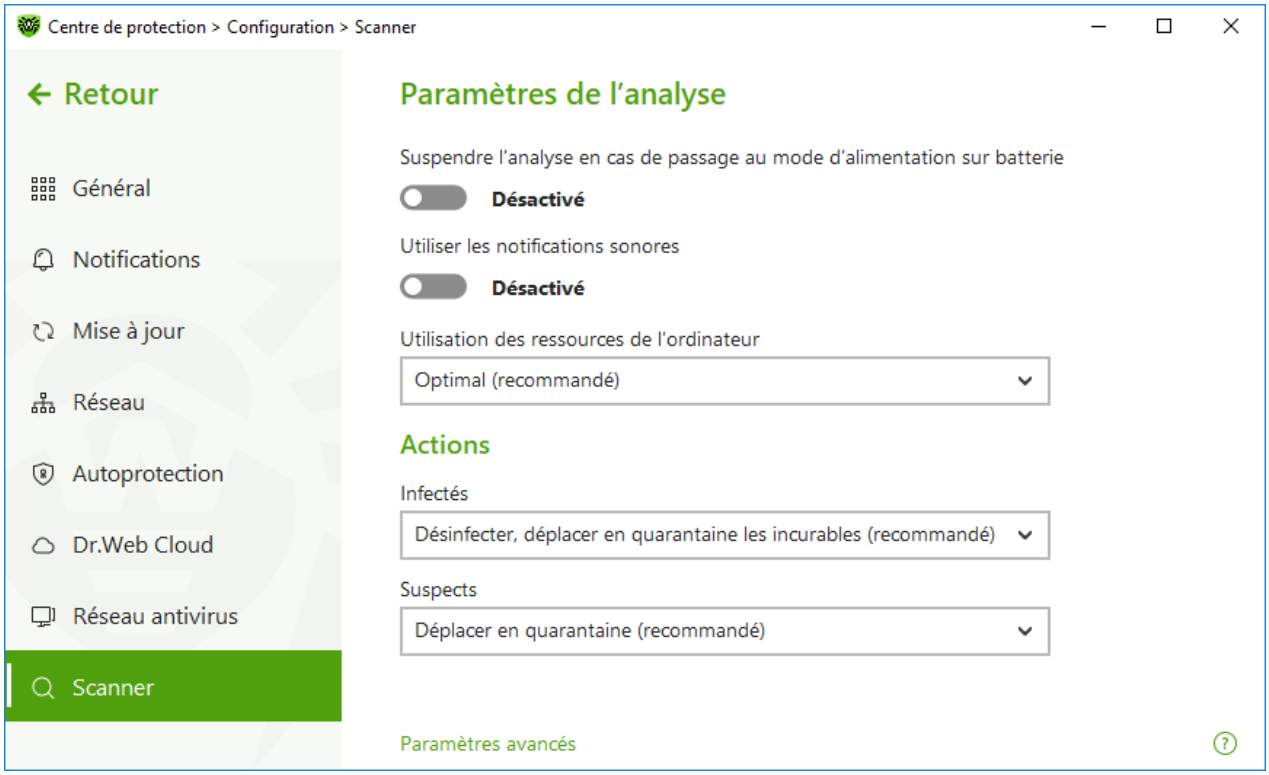

Figure 37. Configuration du Scanner

Paramètres de l'analyse

Dans cette rubrique, vous pouvez configurer les paramètres généraux du Scanner Dr.Web :

- **Suspendre l'analyse en cas de passage au mode d'alimentation sur batterie**. Activez cette option pour suspendre l'analyse en cas de passage en mode d'alimentation sur la batterie. Cette option est désactivée par défaut.
- **Utiliser les notifications sonores**. Activez cette option pour commander au Scanner Dr.Web d'accompagner chaque détection et neutralisation d'un signal sonore. Cette option est désactivée par défaut.
- **Utilisation des ressources de l'ordinateur**. Cette option limite l'utilisation des ressources de l'ordinateur par le Scanner Dr.Web. La valeur optimale est utilisée par défaut.

Actions

Dans ce groupe, vous pouvez configurer la réaction de Scanner à la détection des fichiers infectés, suspects ou des programmes malveillants.

La réaction est spécifiée séparément pour chaque catégorie des objets :

- **Infectés** : objets infectés par un virus connu et (supposé) curable ;
- **Suspects** : objets suspectés d'être infectés par des virus ou de contenir un objet malveillant ;
- objets potentiellement dangereux.

Par défaut, le Scanner essaie de désinfecter les fichiers qui sont infectés par un virus connu et potentiellement curable, tandis que les autres objets qui sont considérés comme les plus dangereux sont placés en Quarantaine. Vous pouvez modifier la réaction du Scanner vis-à-vis de chaque type d'objets. Les actions spécifiés par défaut sont optimales et marquées comme recommandés.

Les actions suivantes sont disponibles pour être appliquées aux objets détectés :

Action	Description
Désinfecter, déplacer en quarantaine les incurables	Indique de restaurer l'objet dans son état initial avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, cet objet est déplacé en quarantaine. Cette action s'applique uniquement aux 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	Indique de restaurer l'objet dans son état initial avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, l'objet sera supprimé. Cette action s'applique uniquement aux 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	Supprimer l'objet. Aucune action n'est appliquée aux secteurs d'amorçage.
Déplacer en quarantaine	Déplacer l'objet dans le dossier spécial de Quarantaine. Aucune action n'est appliquée aux secteurs d'amorçage.
Ignorer	Ignorer l'objet sans lui appliquer aucune action ni afficher d'alerte. Cette action est disponible uniquement pour les programmes malveillants dont adwares, dialers, canulars, hacktools et riskwares.

Si un virus ou un code suspect est détecté au sein des objets complexes comme les archives, les boîtes e-mail ou les conteneurs de fichiers, les actions appliquées aux menaces contenues dans tels objets sont appliquées à l'objet entier et non seulement à sa partie infectée.

Options supplémentaires

Pour accéder aux paramètres avancés, cliquez sur le lien **Paramètres avancés** dans la fenêtre **Paramètres de l'analyse** (voir la figure Paramètres du scanner).

Vous pouvez désactiver le scan des packages d'installation, des archives et des fichiers de messagerie. Le scan de ces objets est activé par défaut.

Vous pouvez configurer le comportement du Scanner après le scan :

- **N'appliquer aucune action**. Scanner va afficher le tableau contenant la liste des menaces détectées.
- **Neutraliser les menaces détectées**. Scanner va appliquer automatiquement les actions aux menaces détectées.
- **Neutraliser les menaces détectées et arrêter l'ordinateur**. Scanner va appliquer automatiquement les actions aux menaces détectées et après, l'ordinateur sera arrêté.

10. Fichiers et réseau

Ce groupe de paramètres fournit l'accès aux paramètres des composants de protection principaux et au Scanner.

Pour accéder au groupe de paramètres Fichiers et réseau

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Fichiers et réseau**.

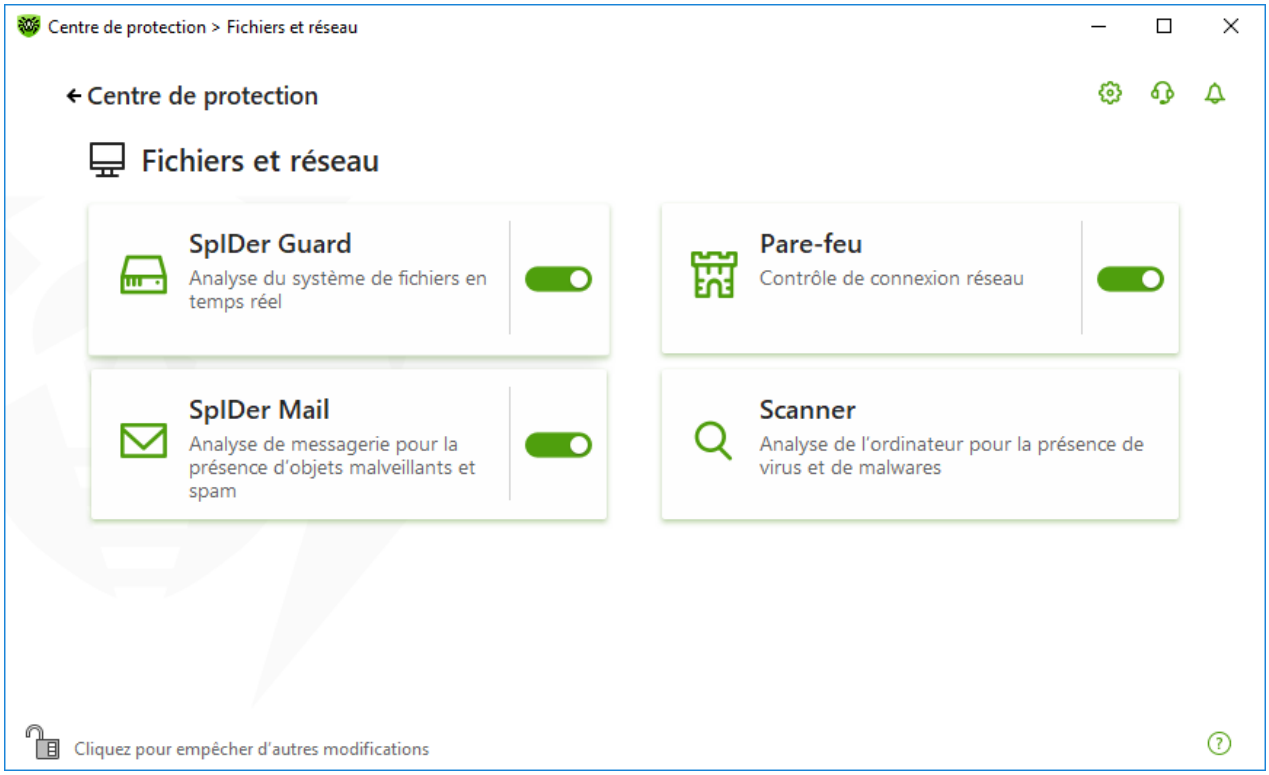

Figure 38. Fenêtre Fichiers et réseau

Activation et désactivation des composants de protection

Activez ou désactivez le composant nécessaire avec l'interrupteur .

Pour accéder aux paramètres des composants

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
2. Cliquez sur la vignette du composant nécessaire.

Dans cette section :

- Moniteur du système de fichiers SpIDer Guard : composant analysant les fichiers lors de leur ouverture, lancement ou modification ainsi que les processus lancés en temps réel.

- Antivirus de messagerie SpIDer Mail : composant analysant les messages e-mail pour la présence d'objets malveillants et du spam.
- Pare-feu : composant contrôlant les connexions et le transfert de données via le réseau et bloquant les connexions suspectes au niveau des paquets et des applications.
- Scanner : composant analysant les objets sur demande ou selon la planification.
- Dr.Web pour Microsoft Outlook : plag-in Dr.Web pour Microsoft Outlook.

> ⚠ Pour *désactiver* un composant, Dr.Web doit fonctionner en mode administrateur. Pour cela, cliquez sur le cadenas en bas de la fenêtre du programme.

10.1. Protection permanente du système de fichiers

Le moniteur du système de fichiers SpIDer Guard protège l'ordinateur en mode réel et prévient l'infection. SpIDer Guard est lancé au démarrage du système d'exploitation et analyse les fichiers lors de leur ouverture, lancement ou modification. Il suit également les actions des processus lancés.

Pour activer ou désactiver le moniteur du système de fichiers

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Fichiers et réseau**.
3. Activez ou désactivez le moniteur du système de fichiers SpIDer Guard avec l'interrupteur.

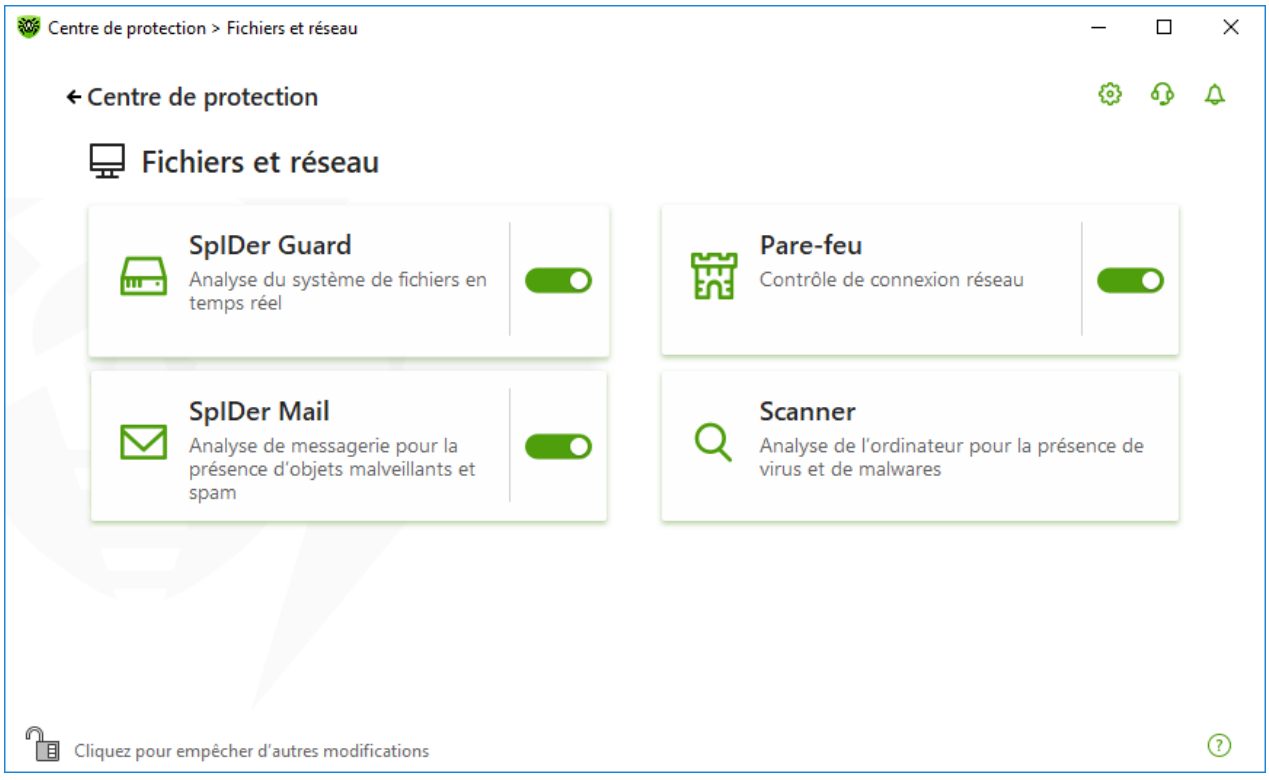

Figure 39. Activation/désactivation de SpIDer Guard

Dans cette section :

Voir aussi :

Particularités de fonctionnement de SpIDer Guard

Avec les paramètres par défaut, SpIDer Guard analyse à la volée les fichiers créés ou modifiés sur le disque dur ainsi que tous les fichiers ouverts sur des supports amovibles. De plus, SpIDer Guard suit constamment les processus lancés propres aux virus et, s'il en détecte un, il le bloque.

> ⚠ Les fichiers en archives, les archives de messagerie et les conteneurs de fichiers ne sont pas analysés par le composant SpIDer Guard. Si un fichier en archive ou en pièce jointe d'un e-mail est infecté, la menace sera détectée au moment de l'extraction du fichier avant que l'ordinateur soit infecté.

Par défaut SpIDer Guard se lance automatiquement à chaque démarrage du système d'exploitation. De plus, le moniteur du système d'exploitation lancé SpIDer Guard ne peut pas être déchargé durant la session du système d'exploitation en cours.

Paramètres du moniteur du système de fichiers SpIDer Guard

En cas de détection d'objets infectés, SpIDer Guard y applique les actions conforment aux paramètres prédéfinis. Les paramètres par défaut sont optimaux dans la plupart des cas. Ne les modifiez pas si ce n'est pas nécessaire.

Pour accéder aux paramètres du composant SpIDer Guard

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert ). Sinon, cliquez sur le cadenas  .
2. Cliquez sur la vignette **SpIDer Guard**. La fenêtre de paramètres du composant va s'ouvrir.

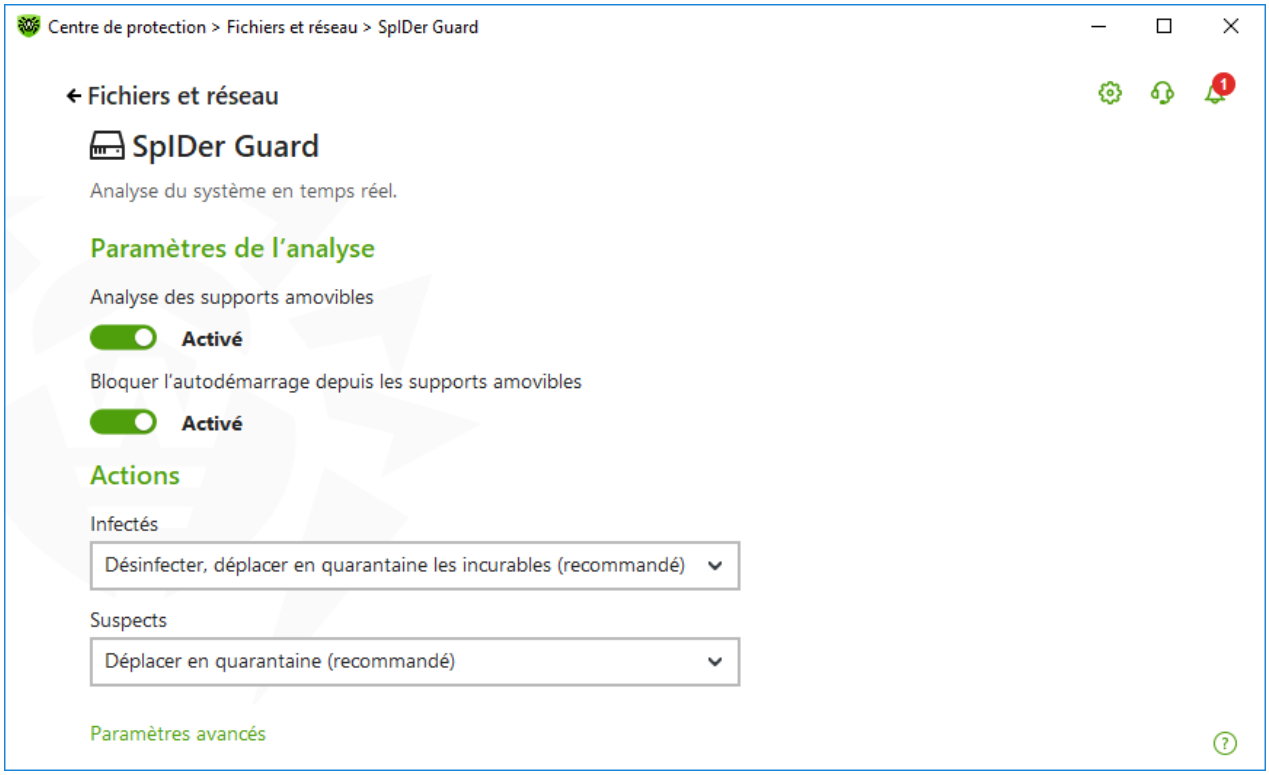

Figure 40. Paramètres du moniteur du système de fichiers

Analyse de supports amovibles

SpIDer Guard analyse par défaut les fichiers ouverts, modifiés et lancés sur des supports amovibles (disques CD/DVD, mémoires flash, etc) et bloque le lancement automatique de leur contenu actif. L'utilisation de ces paramètres permet de prévenir l'infection de votre ordinateur via les supports amovibles.

> ⚠ Le système d'exploitation peut reconnaitre certains supports amovibles comme des disques durs (notamment les disques durs externes à l'interface USB). Veuillez utiliser ces dispositifs avec beaucoup de précautions et analysez-les avec le Scanner Dr.Web lorsqu'ils sont connectés à l'ordinateur.

Vous pouvez activer ou désactiver les options **Analyse des supports amovibles** et **Bloquer l'autodémarrage depuis les supports amovibles** avec l'interrupteur dans le groupe de paramètres **Paramètres de l'analyse**.

> ⚠ En cas de problèmes lors de l'installation des programmes utilisant le fichier `autorun.inf`, désactivez temporairement l'option **Bloquer l'autodémarrage depuis les supports amovibles**.

Actions à appliquer aux menaces détectées

Dans ce groupe de paramètres, vous pouvez configurer les actions que Dr.Web doit appliquer aux menaces en cas de leur détection par le moniteur du système de fichiers SpIDer Guard.

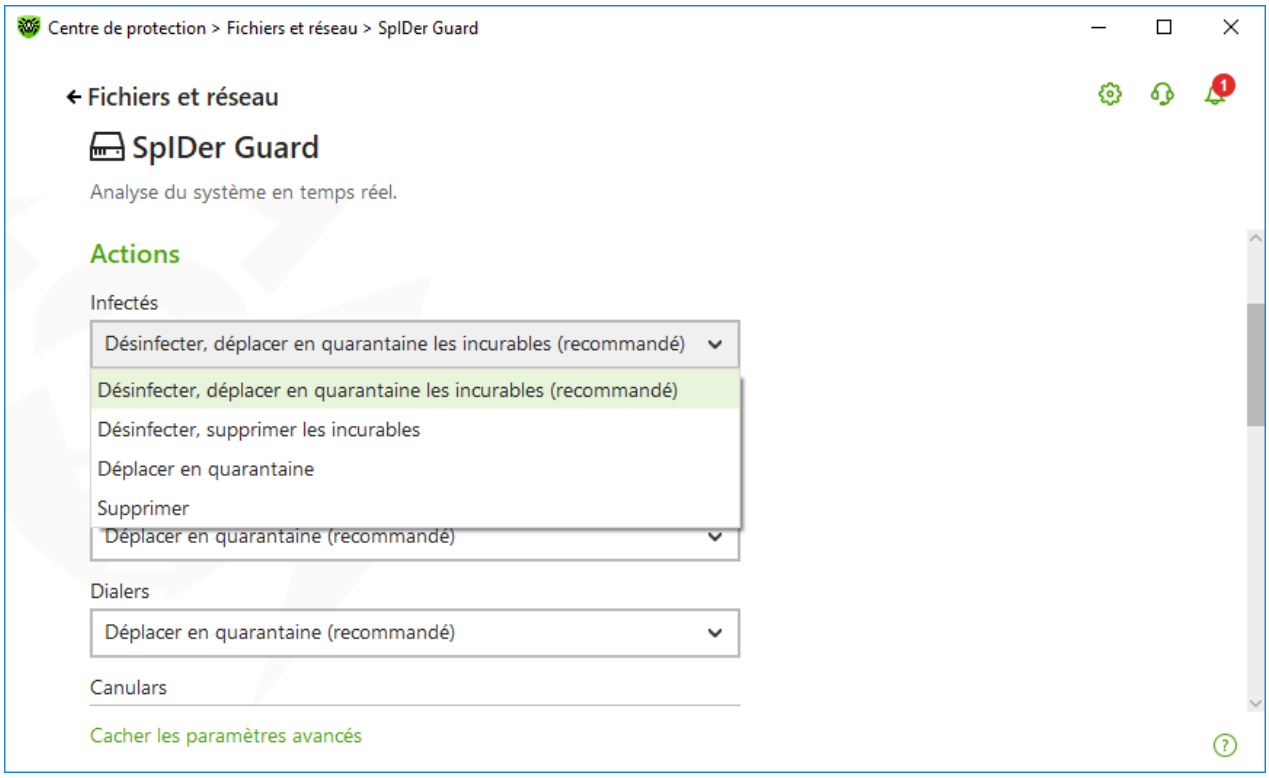

Figure 41. Configuration des actions appliqués aux menaces

Les actions sont spécifiées séparément pour chaque type d'objets suspects. L'ensemble d'actions disponibles dépend du type d'objets. Les actions recommandées sont spécifiées pour chaque type d'objet. Les copies d'objets traités sont sauvegardées dans la Quarantaine.

Actions possibles

Les actions suivantes peuvent être appliquées aux menaces :

Action	Description
Désinfecter, déplacer en quarantaine les incurables	Indique de restaurer l'objet dans son état initial avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, cet objet est déplacé en quarantaine. Cette action s'applique uniquement aux 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).

Action	Description
Désinfecter, supprimer les incurables	Indique de restaurer l'objet dans son état initial avant infection. Si l'objet est incurable, ou que la tentative de désinfection a échoué, l'objet sera supprimé. Cette action s'applique uniquement aux 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	Supprimer l'objet. Aucune action n'est appliquée aux secteurs d'amorçage.
Déplacer en quarantaine	Déplacer l'objet dans le dossier spécial de Quarantaine. Aucune action n'est appliquée aux secteurs d'amorçage.
Ignorer	Ignorer l'objet sans lui appliquer aucune action ni afficher d'alerte. Cette action est disponible uniquement pour les programmes malveillants dont adwares, dialers, canulars, riskwares et hacktools.

Mode de l'analyse par le composant SpIDer Guard

Pour accéder à cette section et la section suivante, cliquez sur le lien **Paramètres avancés**.

Dans ce groupe de paramètres, vous pouvez sélectionner le mode de l'analyse de fichiers par le moniteur SpIDer Guard.

Mode	Description
Optimal, utilisé par défaut	Dans ce mode, SpIDer Guard analyse les objets dans les cas suivants : • pour les objets sur les disques durs, lorsqu'il y a une tentative d'exécuter un fichier, de créer un nouveau fichier ou d'écrire sur un fichier existant ou sur le secteur d'amorçage ; • pour les objets sur les supports amovibles : à chaque tentative d'accéder à un fichier ou aux secteurs d'amorçage (lecture, écriture, lancement). Il est recommandé de l'utiliser après l'analyse de tous les disques durs effectuée par le Scanner Dr.Web. Dans ce cas, de nouveaux virus et d'autres programmes malveillants ne pourront pas pénétrer dans votre ordinateur via les supports amovibles. Les objets déjà analysés et inoffensifs ne seront pas scannés de nouveau.

Mode	Description
Paranoïde	Dans ce mode, SpIDer Guard analyse tous les fichiers et les secteurs d'amorçage sur les disques durs ou réseau et sur les supports amovibles en cas de tentative d'y accéder (création, lecture, écriture, lancement). Ce mode assure une protection maximum mais consomme beaucoup plus de ressources de l'ordinateur.

Options supplémentaires

Dans ce groupe de paramètres, vous pouvez configurer les paramètres de l'analyse à la volée qui seront appliqués en fonction du mode de fonctionnement du moniteur du système de fichiers SpIDer Guard. Vous pouvez activer :

- l'utilisation de l'analyseur heuristique ;
- l'analyse des programmes et modules en cours de démarrage ;
- l'analyse des fichiers d'installation ;
- l'analyse des fichiers en réseau local (non recommandé) ;
- l'analyse de l'ordinateur pour la présence des rootkits (recommandé) ;
- l'analyse des scripts exécutés par Windows Script Host et PowerShell (pour Windows 10).

Analyse heuristique

Par défaut, SpIDer Guard effectue l'analyse en utilisant l'analyseur heuristique. Si l'option est désactivée, il effectue l'analyse uniquement par signatures de virus connus.

Scan Anti-rootkit en tâche de fond

Le composant Anti-rootkit intégré à Dr.Web offre des fonctions de scan en tâche de fond du système d'exploitation à la recherche de menaces complexes ainsi que des fonctionnalités de traitement des infections actives lorsque c'est nécessaire.

Si cette option est activée, Antirootkit Dr.Web réside de manière permanente en mémoire. A la différence de l'analyse à la volée des fichiers effectué par le composant SpIDer Guard, la recherche de rootkits se fait dans le BIOS de l'ordinateur, les zones critiques de Windows, telles que les objets autorun, les processus et les modules en cours, la mémoire vive (RAM), des disques MBR/VBR, etc.

Une des fonctionnalités principales de Anti-rootkit Dr.Web est sa faible consommation des ressources système ainsi que sa prise en considération des capacités hardware.

Lorsque Antirootkit Dr.Web détecte une menace, il notifie l'utilisateur et neutralise l'activité malveillante.

Durant l'analyse en tâche de fond pour la présence de rootkits, les fichiers et dossiers indiqués dans l'onglet correspondant sont exclus du scan.

Le scan Anti-rootkit en tâche de fond est activé par défaut.

La désactivation de SpIDer Guard n'a pas d'impact sur l'analyse en tâche de fond. Si le paramètre est activé, l'analyse en tâche de fond est effectuée indépendamment du statut de SpIDer Guard.

10.2. Analyse e-mail

L'analyse e-mail est effectué par le composant SpIDer Mail. L'antivirus de messagerie SpIDer Mail est installé par défaut, il réside dans la mémoire et il se lance au démarrage du système d'exploitation.

SpIDer Mail supporte l'analyse du trafic e-mail chiffré par les protocoles POP3S, SMTPS, IMAPS. Pour cela, il faut activer l'option **Analyser le trafic chiffré** dans la section Réseau.

Pour activer et désactiver l'analyse d'e-mail

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Fichiers et réseau**.
3. Activez ou désactivez l'antivirus de messagerie SpIDer Mail avec l'interrupteur .

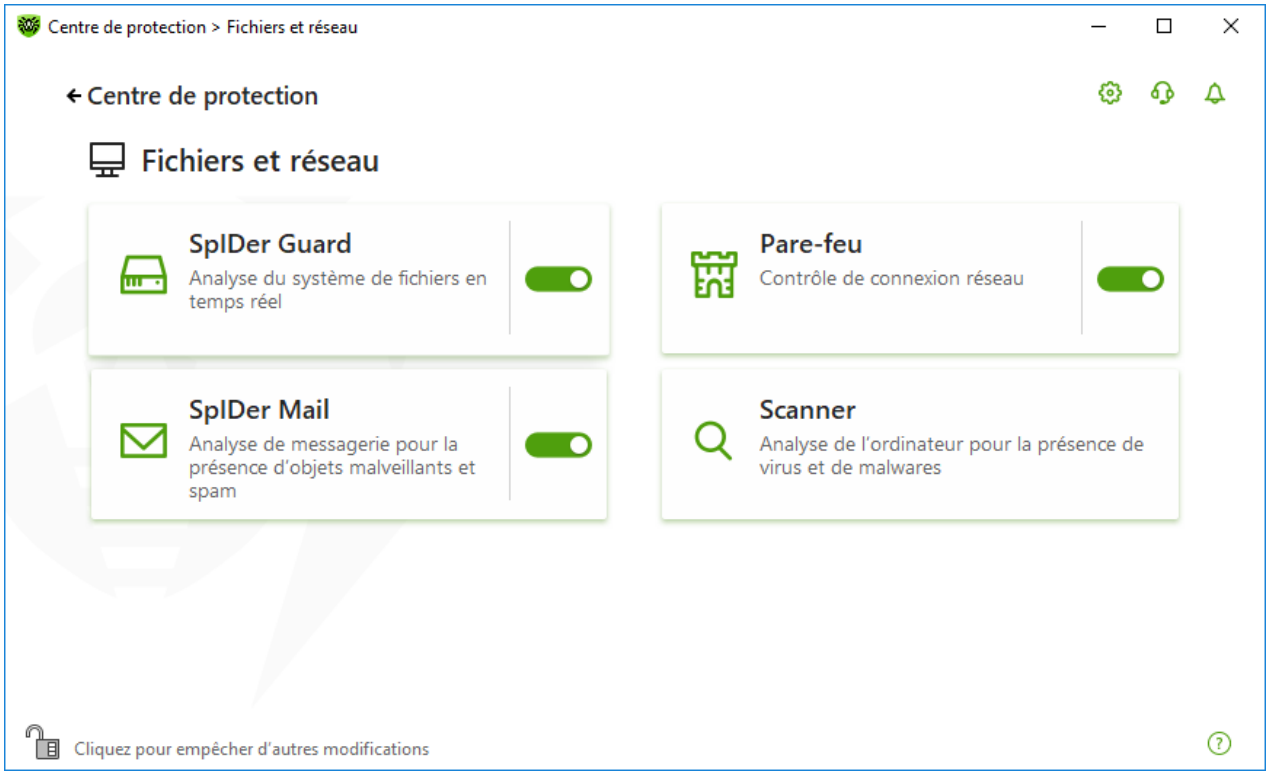

Figure 42. Activation/désactivation de SpIDer Mail

Dans cette section :

- Particularités de traitement des e-mails
- Analyse des e-mails par d'autres outils

Voir aussi :

- Paramètres de l'analyse de messages

Particularités de traitement des e-mails

SpIDer Mail reçoit tous les messages à la place du client de messagerie et les analyse. S'il n y a aucune menace, le message est transmis au client de messagerie comme s'il était reçu directement du serveur. La même procédure est appliquée aux messages sortants avant leur envoi au serveur.

Par défaut, l'antivirus de messagerie SpIDer Mail réagit aux messages entrants infectés et suspects aussi bien qu'aux messages qui n'ont pas été analysés (à cause de leur structure compliquée, par exemple) de la manière suivante :

Type de messages	Action
Messages infectés	Le contenu malveillant est supprimé de tels messages, puis les messages sont délivrés. Cette action est appelée *désinfection* du message.

Type de messages	Action
Messages aux objets suspects	Ils sont déplacés en Quarantaine dans des fichiers séparés ; le client de messagerie reçoit alors une alerte. Cette action est appelée *déplacement* du message. Les messages déplacés sont également supprimés du serveur POP3 ou IMAP4.
Messages sains et messages non analysés	Ils sont transmis sans modifications (*sautés*).

Les *messages sortants* infectés ou suspects ne sont pas envoyés au serveur, l'utilisateur est informé que le message ne sera pas envoyé (généralement, le client messagerie sauvegarde les messages).

Analyse des e-mails par d'autres outils

Le Scanner peut également détecter des virus dans les messageries de différents formats, mais SpIDer Mail comporte plusieurs avantages :

- tous les formats de messageries ne sont pas supportés par le Scanner Dr.Web. Si vous utilisez SpIDer Mail, les messages infectés ne sont même pas délivrés dans la boîte de réception ;
- Scanner n'analyse pas les boîtes de réception au moment de la réception des e-mails, mais à la demande de l'utilisateur ou selon la planification. Cette analyse consomme des ressources et peut prendre beaucoup de temps.

10.2.1. Paramètres de l'analyse de messages

Par défaut, SpIDer Mail tente de désinfecter les messages infectés par un virus connu et supposé curable. Les messages incurables et suspects, tout comme les dialers et les adwares, sont mis en Quarantaine. Les autres messages sont délivrés par le moniteur de messagerie sans modification (*ignorés*). Les paramètres de l'analyse de messages par défaut sont optimaux dans la plupart de cas, il ne faut pas les modifier sans nécessité.

Dans cette section :

- Actions à appliquer aux menaces détectées
- Configuration de paramètres de l'analyse de messages
- Analyse d'archives
- Analyse des messages transmis par les protocoles cryptographiques

Paramètres de l'analyse de messages

Les paramètres par défaut de SpIDer Mail sont optimaux pour les utilisateurs novices. Ils fournissent une protection maximum tout en sollicitant au minimum l'intervention de l'utilisateur. Cependant, SpIDer Mail peut bloquer certaines options des outils de messagerie (par exemple, l'envoi d'un

message à plusieurs destinataires peut être considéré comme un envoi massif, ou bien le spam reçu n'est pas détecté), de plus, en cas de suppression automatique, vous ne pouvez plus obtenir des informations utiles (contenue dans une partie saine du message).

Pour commencer à modifier les paramètres de l'analyse de messages

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Fichiers et réseau**.
3. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
4. Cliquez sur la vignette **SpIDer Mail**. La fenêtre de paramètres du composant va s'ouvrir.

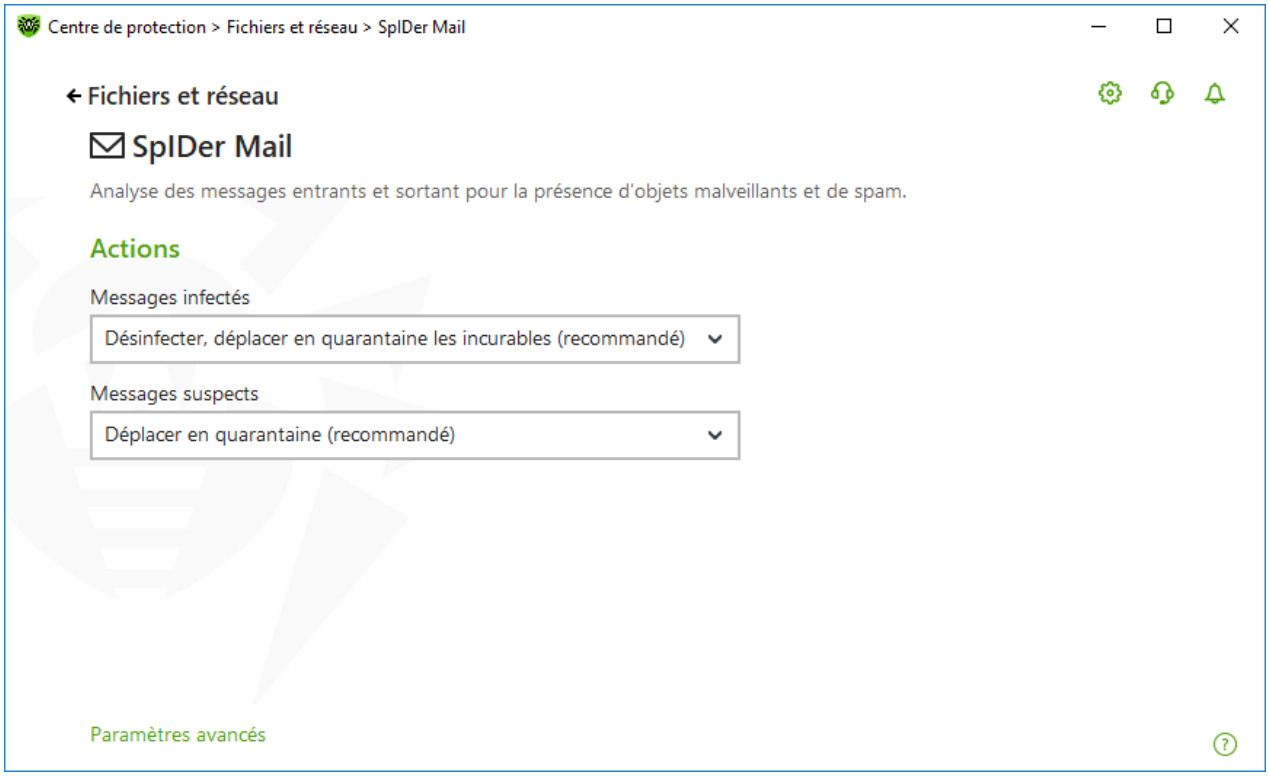

Figure 43. Paramètres de l'analyse de messages

Actions à appliquer aux menaces détectées

Dans ce groupe de paramètres, vous pouvez configurer les actions que Dr.Web doit appliquer aux messages en cas de détection de menaces dans ce messages.

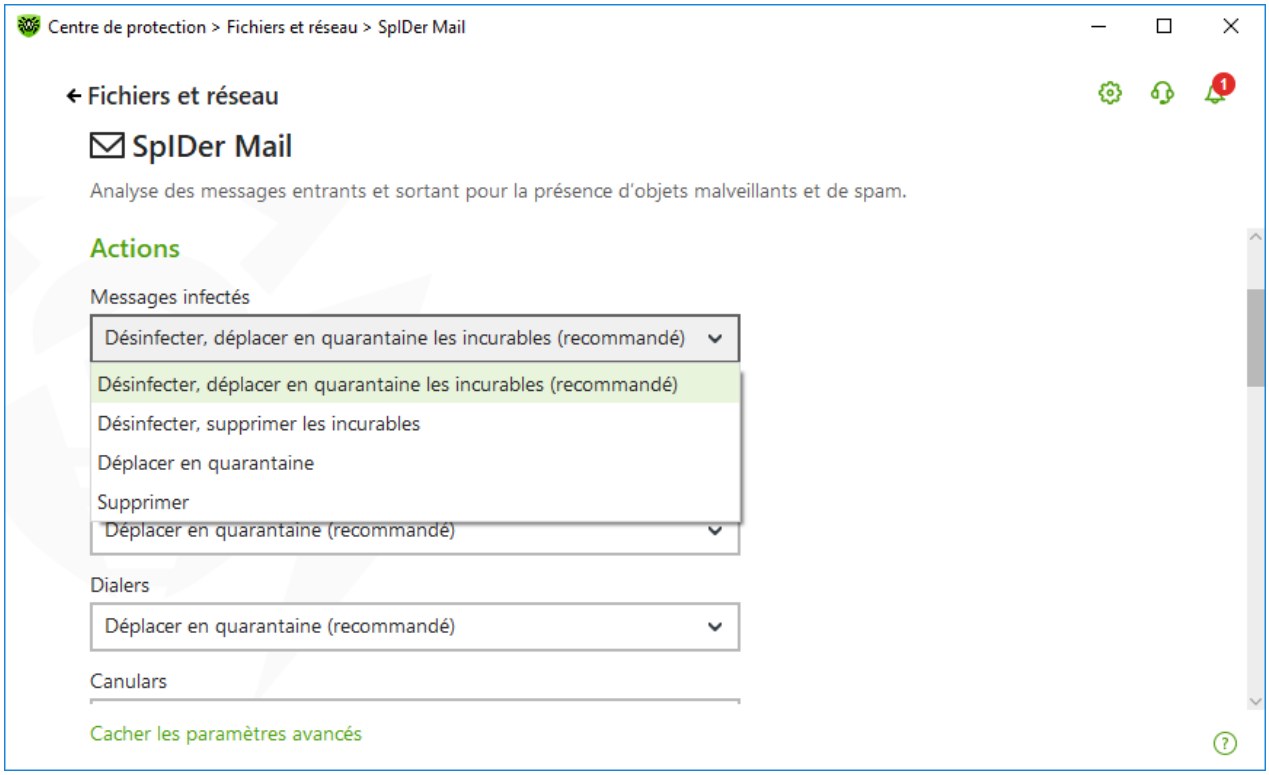

Figure 44. Configuration des actions appliqués aux messages

Actions possibles

Les actions suivantes peuvent être appliquées aux menaces :

Action	Description
Désinfecter, déplacer en quarantaine les incurables	Restaurer le message dans son état initial avant infection. Si le message est incurable, ou que la tentative de désinfection a échoué, le message est placé en quarantaine. Cette action est disponible uniquement pour les messages infectés par des virus connus et « curables », exceptés les Trojans qui sont supprimés au moment de leur détection. Cette action n'est pas applicable aux messages contenus dans des archives, quel que soit le type de virus. Entraine le refus d'envoyer le message.
Désinfecter, supprimer les incurables	Restaurer le message dans son état initial avant infection. Si le virus est incurable, ou que la tentative de désinfection a échoué, le message sera supprimé. Entraine le refus d'envoyer le message.
Supprimer	Supprimer le message. Dans ce cas, le message n'est pas envoyé au destinataire, le client de messagerie reçoit une notification de l'opération

Action	Description
	effectuée. Entraine le refus d'envoyer le message.
Déplacer en quarantaine	Déplacer le message dans la Quarantaine. Dans ce cas, le message n'est pas envoyé au destinataire, le client de messagerie reçoit une notification de l'opération effectuée. Entraine le refus d'envoyer le message.
Ignorer	Commande d'adresser le message à la boîte de réception comme d'habitude, c'est-à-dire sans entreprendre aucune action.

Vous pouvez augmenter la sécurité de la protection antivirus par rapport au niveau par défaut. Pour ce faire, cliquez sur le lien **Paramètres avancés** et sélectionnez dans la liste **Non analysés** l'élément **Déplacer en quarantaine**. Il est recommandé de scanner les fichiers contenant les messages déplacés plus tard avec le Scanner Dr.Web.

Si vous souhaitez désactiver la protection contre les e-mails suspects, assurez-vous que le moniteur de fichiers SpIDer Guard contrôle constamment votre ordinateur.

Configuration de paramètres de l'analyse de messages

Pour accéder aux paramètres d'analyse des messages, cliquez sur le lien **Paramètres avancés**.

Actions réalisées sur les messages

Dans ce groupe de paramètres, vous pouvez configurer des actions supplémentaires à appliquer aux messages traités par SpIDer Mail.

Paramètre	Description
Ajouter l'en-tête 'X-Antivirus' dans les messages	Activé par défaut. Commande d'ajouter les informations sur l'analyse du message et la version de Dr.Web à l'en-tête de tous les messages traités par le moniteur de messagerie SpIDer Mail. Vous ne pouvez pas éditer le format de l'en-tête ajouté.
Supprimer les messages modifiés sur le serveur	Commande de supprimer depuis le serveur de messagerie les messages supprimés ou déplacés en Quarantaine par le moniteur de messagerie SpIDer Mail quels que soient les paramètres de votre client messagerie.

Optimisation de l'analyse

Vous pouvez configurer SpIDer Mail pour qu'il reconnaisse les messages trop compliqués et dont le scan est trop consommateur de temps, comme non analysés. Pour cela, activez l'option **Délai d'attente lors de l'analyse de message** et indiquez la durée maximum de scan d'un message. Après l'expiration de ce délai, le moniteur de messagerie SpIDer Mail arrête d'analyser le message. La valeur 250 secondes est utilisée par défaut.

Analyse d'archives

Activez l'option **Analyse des archives** si vous souhaitez que SpIDer Mail analyse le contenu des archives transmises par e-mail. Si cela est nécessaire, vous pouvez activer les options suivantes et configurer les paramètres de l'analyse des archives :

- **Taille maximum des fichiers à décompresser**. Si la taille de l'archive décompressée dépasse la limite, SpIDer Mail ne décompresse l'archive ni ne l'analyse. La valeur 30720 Ko est utilisée par défaut ;
- **Niveau maximum d'imbrication**. Si le taux d'imbrication dépasse la valeur spécifiée SpIDer Mail analyse l'archive jusqu'à ce que cette limite soit atteinte. La valeur 64 est utilisée par défaut.

Il n'y a pas de restrictions pour un paramètre si la valeur est égale à 0.

Options supplémentaires

Dans ce groupe, vous pouvez spécifier les options supplémentaires d'analyse des e-mails :

- utilisation de l'analyse heuristique – dans ce mode, des mécanismes spécialisés sont utilisés de sorte qu'ils permettent de détecter, dans le courrier électronique, des objets suspects, avec une forte probabilité, contaminés par des virus inconnus. Pour désactiver l'analyse heuristique, utilisez l'interrupteur **Utiliser l'analyse heuristique (recommandé)** ;
- analyse de packages d'installation. Cette option est désactivée par défaut.

Configuration des notifications

Après avoir exécuté l'action spécifiée par défaut, SpIDer Mail affiche une notification appropriée dans la zone de notification Windows. Si nécessaire, vous pouvez configurer les notifications s'affichant sur le bureau ou les notifications envoyées par e-mail.

Analyse des messages par les protocoles POP3S, SMTPS, IMAPS

Pour que SpIDer Mail analyse les données transmises via les protocoles cryptographiques, activez l'option **Analyser le trafic chiffré** dans la fenêtre Réseau.

10.3. Pare-feu

Le Pare-feu Dr.Web protège votre ordinateur de l'accès non autorisé et prévient les fuites de données importantes via les réseaux. Il gère les tentatives de connexion et le transfert de données et vous aide à bloquer les connexions suspectes au niveau des paquets et des applications.

Le Pare-feu fournit les fonctionnalités suivantes :

- contrôle et filtrage de tout le trafic entrant et sortant ;
- contrôle d'accès au niveau des applications ;
- filtrage des paquets au niveau du réseau ;
- sélection rapide des règles ;
- journal des événements.

Pour activer ou désactiver le Pare-feu

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Fichiers et réseau**.
3. Activez ou désactivez le Pare-feu avec l'interrupteur .

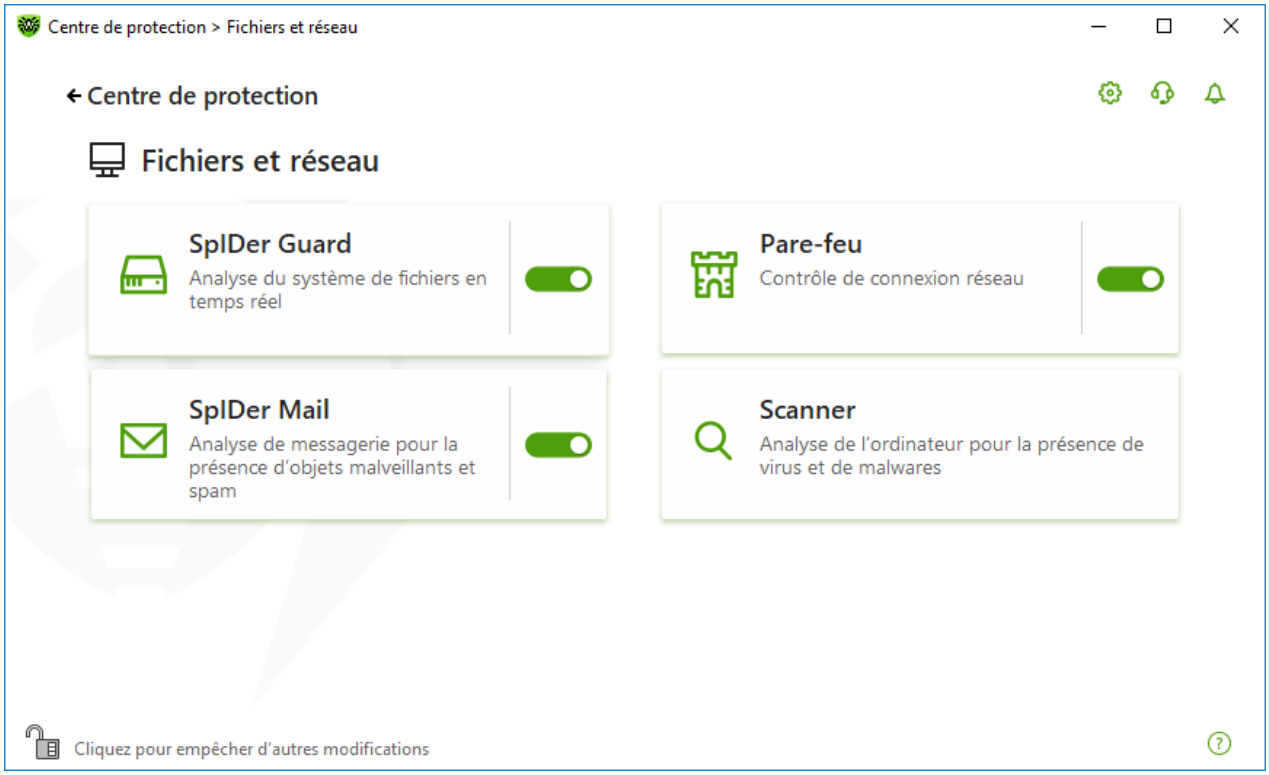

Figure 45. Activation/désactivation du Pare-feu

Dans cette section :

- Configuration du Pare-feu
- Page Applications

- Règles pour les applications
- Configuration des paramètres de règles pour les applications
- Paramètres des réseaux
- Filtre de paquets
- Ensemble de règles de filtrage de paquets
- Création d'une règle de filtrage

10.3.1. Paramètres de fonctionnement du Pare-feu

Dans cette section, vous pouvez configurer les paramètres suivants du Pare-feu :

- sélectionner le mode opératoire ;
- configurer la liste des applications autorisées ;
- configurer les paramètres des réseaux connus.

> ⚠ Pour accéder aux paramètres du Pare-feu, vous êtes invité à entrer le mot de passe si vous avez activé l'option **Protéger les paramètres de Dr.Web par un mot de passe** dans la section Configuration.

Par défaut, le Pare-feu ne crée pas de règles pour les applications connues. Quel que soit le mode opératoire, les événements sont journalisés.

Les paramètres par défaut permettent une utilisation optimale du produit. Ne les modifiez pas si ce n'est pas nécessaire.

Pour accéder à la sélection du mode de fonctionnement et aux paramètres du composant Pare-feu

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert ). Sinon, cliquez sur le cadenas  .
2. Cliquez sur la vignette **Pare-feu**. La fenêtre de configuration du composant va s'ouvrir.

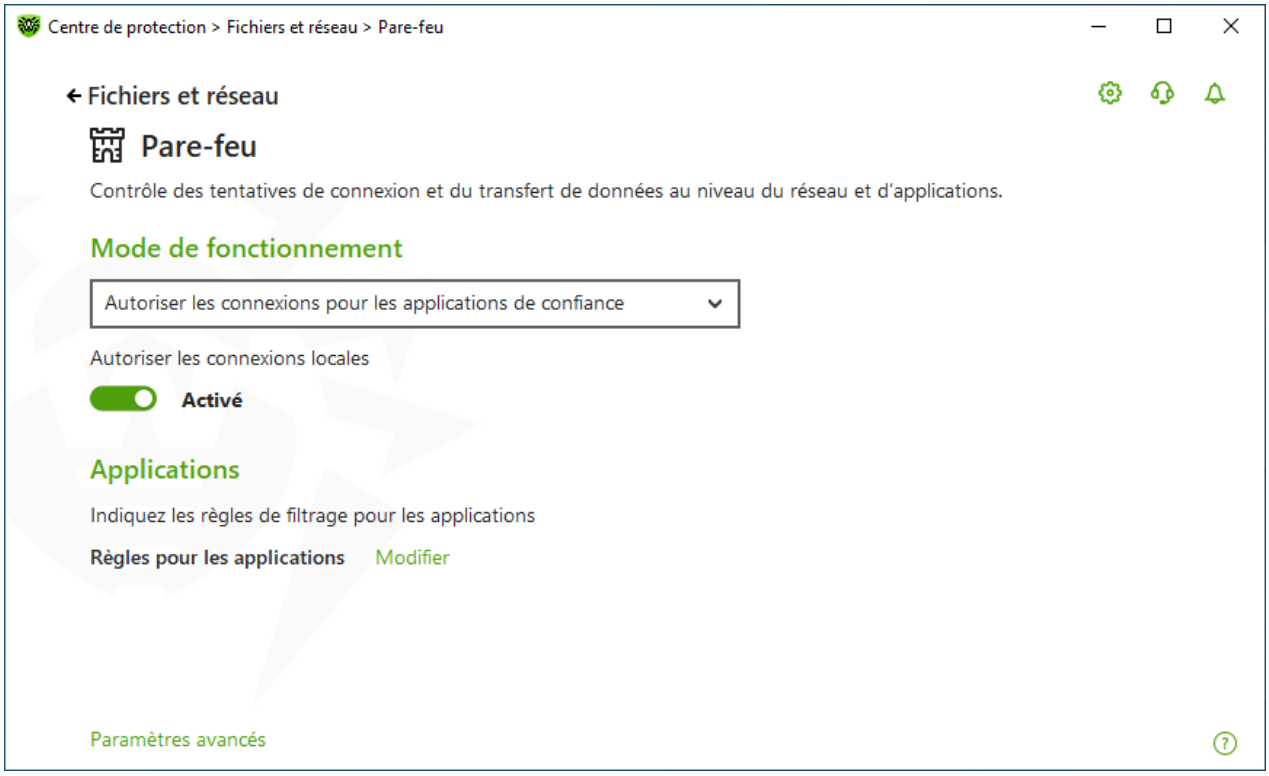

Figure 46. Paramètres du Pare-feu

Le paramètre **Autoriser les connexions locales** permet à toutes les applications d'établir des connexions locales sur votre ordinateur (depuis l'interface ou à l'interface 127.0.0.1 (localhost)). Cette option s'applique après la vérification de conformité des connexions aux règles spécifiées. Désactivez cette option pour appliquer des règles de filtrage indépendamment du fait que la connexion se fait via le réseau ou au sein de votre ordinateur.

Sélection du mode opératoire

Sélectionnez un des modes suivants :

Mode de fonctionnement	Description
Autoriser les connexions pour les applications de confiance	Ce mode est utilisé par défaut. Dans ce mode, toutes les applications de confiance sont autorisées à accéder aux ressources réseau, y compris Internet. Les applications de confiance comprennent les applications système, les applications ayant le certificat Microsoft et les applications avec une signature numérique valide. Les règles pour ces applications ne sont pas affichées dans la liste de règles. Pour d'autres applications, le Pare-feu offre une possibilité de bloquer ou d'autoriser une connexion inconnue ainsi que de créer une règle pour cette connexion.

Mode de fonctionnement	Description
	En cas de tentative d'accès aux ressources réseau de la part du système d'exploitation ou d'une application d'utilisateur, le Pare-feu vérifie s'il existe un ensemble de règles de filtrage pour ces programmes. S'il n'y en a pas, un avertissement est affiché et vous invite à choisir une solution temporaire ou à créer une règle qui sera appliquée à chaque fois lors du traitement des connexions pareilles.
Autoriser les connexions inconnues	Dans ce mode, l'accès aux ressources réseau, y compris Internet, est fourni à toutes les applications inconnues pour lesquelles les règles de filtrage ne sont pas spécifiées. Aucune notification sur les tentatives d'accès ne sont affichées par le Pare-feu.
Mode interactif	Dans ce mode, vous avez un contrôle total sur les réactions du Pare-feu à la détection d'une connexion inconnue. En cas de tentative d'accès aux ressources réseau de la part du système d'exploitation ou d'une application d'utilisateur, le Pare-feu vérifie s'il existe un ensemble de règles de filtrage pour ces programmes. S'il n'y en a pas, un avertissement est affiché et vous invite à choisir une solution temporaire ou à créer une règle qui sera appliquée à chaque fois lors du traitement des connexions pareilles.
Bloquer les connexions inconnues	Dans ce mode, toutes les connexions inconnues aux ressources réseau y compris la connexion à Internet sont bloquées de manière automatique. En cas de tentative d'accès aux ressources réseau de la part du système d'exploitation ou d'une application d'utilisateur, le Pare-feu vérifie s'il existe des règles de filtrage pour ces programmes. S'il n'y en a pas, le Pare-feu bloque automatiquement l'accès au réseau sans afficher aucune notification. S'il y a des règles de filtrage spécifiées pour la connexion en question, les actions déterminées seront effectuées.

Page Applications

Le filtrage au niveau des applications vous aide à contrôler l'accès de diverses applications et processus aux ressources réseaux, et vous permet d'interdire ou d'autoriser aux applications de lancer d'autres processus. Vous pouvez créer des règles pour les applications système et utilisateur.

Dans cette rubrique, vous pouvez établir des ensembles de règles de filtrage. Pour cela, vous pouvez créer de nouvelles règles, éditer les règles existantes ou supprimer les règles dont vous n'avez plus besoin. Chaque application est explicitement identifiée par le chemin vers son fichier

exécutable. Le Pare-feu utilise le nom `SYSTEM` pour indiquer le noyau du système d'exploitation (le processus system pour lequel il n'y a pas de fichier exécutable correspondant).

Vous ne pouvez pas créer plus d'un ensemble de règles par application.

Si vous avez créé une règle de blocage pour un processus ou que vous avez spécifié le mode Bloquer les connexions inconnues, et après, vous avez désactivé la règle de blocage ou modifié le mode de fonctionnement, le blocage reste activé jusqu'à la deuxième tentative d'établir une connexion après le redémarrage du processus.

Règles pour les applications

Pour accéder à la fenêtre Règles pour les applications

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Fichiers et réseau**.
3. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas.
4. Cliquez sur la vignette **Pare-feu**. La fenêtre de configuration du composant va s'ouvrir.
5. Dans la section de paramètres **Règles pour les applications**, cliquez sur **Modifier**. La fenêtre qui s'ouvre contient la liste des applications pour lesquelles les règles sont spécifiées.

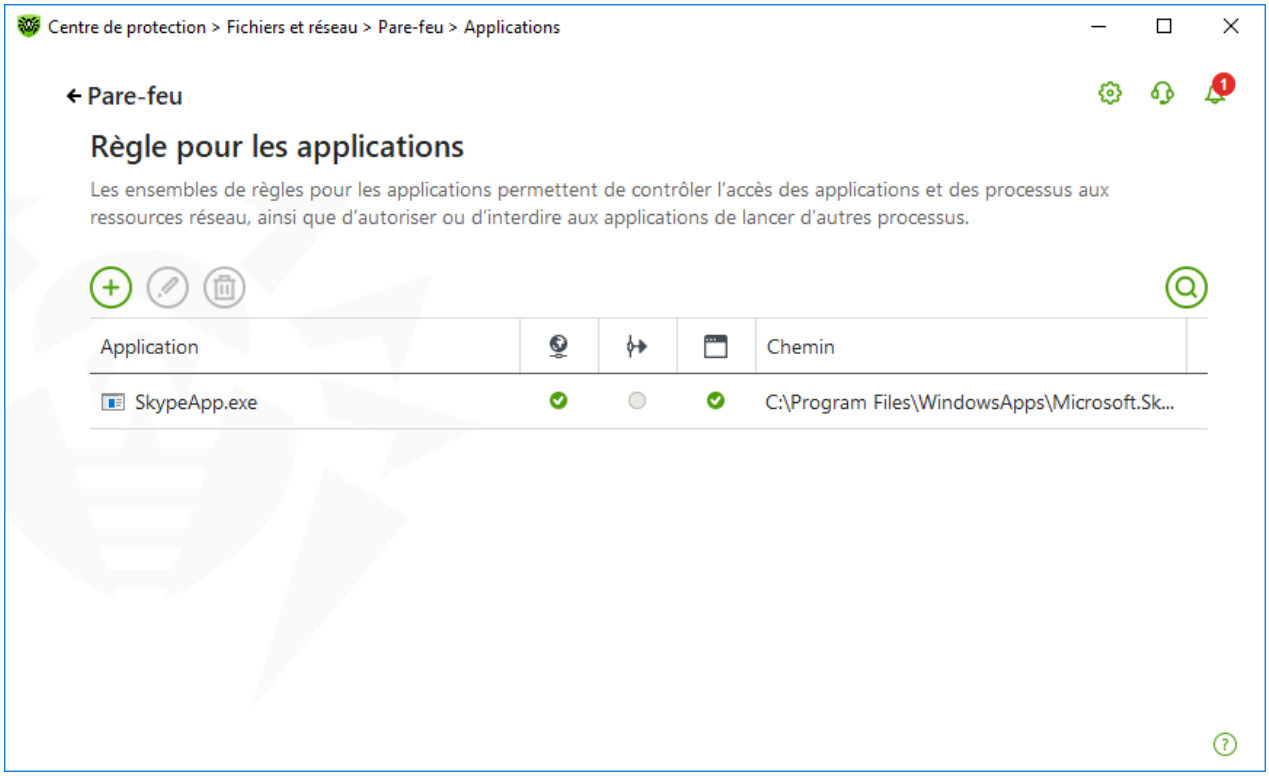

Figure 47. Règles pour les applications

6. Pour créer un nouvel ensemble de règles ou éditer un ensemble existant, cliquez sur le bouton ⊕ ou sélectionnez une application dans la liste et cliquez sur ✎. Pour chercher la règle nécessaire, cliquez sur le bouton 🔍.

Les règles pour les applications supprimées de votre ordinateur ne sont pas supprimées automatiquement. Pour supprimer de telles règles, sélectionnez l'élément **Suppression de règles non utilisées** dans le menu contextuel de la liste.

Édition d'une règle existante ou création d'un nouvel ensemble de règles

Dans la fenêtre **Création d'un nouvel ensemble de règles pour l'application** (ou **Éditer l'ensemble de règles pour <*nom de l'application*>**), vous pouvez configurer l'accès de l'application aux ressources réseau ainsi qu'interdire ou autoriser le lancement d'autres applications.

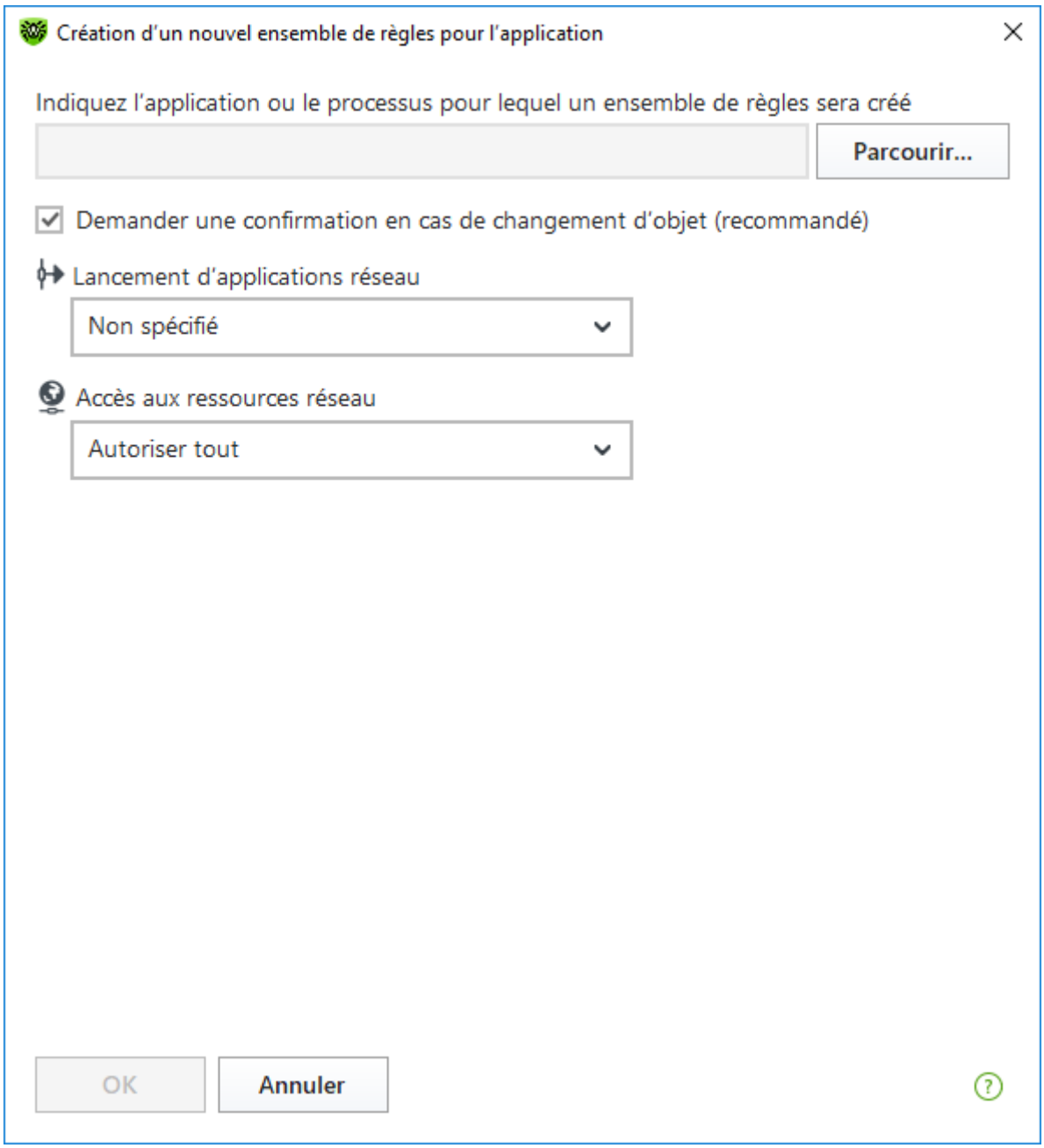

Figure 48. Création d'un nouvel ensemble de règles

Lancer d'autres applications

Pour interdire ou autoriser à une application de lancer d'autres application, dans la liste déroulante **Lancement des application réseau**, sélectionnez :

- **Autoriser**, pour autoriser l'application à lancer des processus ;
- **Bloquer**, pour interdire à l'application de lancer des processus ;
- **Non spécifié**. Dans ce cas, l'application va fonctionner avec les paramètres spécifiés correspondant au mode de fonctionnement du Pare-feu.

Accès aux ressources réseau

1. Spécifiez le type d'accès aux ressources réseau :
   - **Autoriser tout** : toutes les connexions seront autorisées ;
   - **Bloquer tout** : toutes les connexions seront bloquées ;
   - **Non spécifié**. Dans ce cas, l'application fonctionnera avec les paramètres du mode de fonctionnement sélectionné du Pare-feu ;
   - **Personnalisé** : dans ce mode, vous pouvez créer un ensemble de règles qui autorisera ou bloquera les différentes connexions.
2. Si vous avez sélectionné le mode **Personnalisé** de l'accès aux ressources réseau, un tableau contenant les informations sur l'ensemble de règles pour l'application correspondante sera affiché ci-dessous.

Paramètre	Description
Activé	État de l'exécution de la règle.
Action	L'action que le Pare-feu doit accomplir lorsque une tentative de connexion à Internet est détectée : • **Bloquer les paquets** : bloquer la tentative de connexion ; • **Autoriser les paquets** : autoriser la connexion.
Nom de règle	Nom de la règle.
Type de connexion	Direction de la connexion : • **Entrant** : la règle s'applique lorsque quelqu'un tente de se connecter à l'application sur votre machine, depuis le réseau ; • **Sortant** : la règle s'applique lorsqu'une application sur votre machine tente de se connecter au réseau ; • **Toute** : la règle s'applique sans tenir compte de la direction de la connexion.
Description	Description de la règle.

3. Si nécessaire, éditez l'ensemble de règle pré-installé ou créez un nouvel ensemble de règles pour l'application.
4. Si vous avez choisi de créer ou d'éditer une règle, configurez les paramètres de la règle dans la fenêtre ouverte.
5. Après avoir édité l'ensemble de règles, cliquez sur **OK** pour enregistrer les modifications apportées ou sur **Annuler** pour annuler les modifications. Les modifications apportées dans l'ensemble de règles sont conservées en cas de passage en autre mode.

Cochez la case **Demander confirmation en cas de changement d'objet (recommandé)** si vous voulez que l'application demande l'accès aux ressources réseau en cas de modification ou mise à jour des applications.

Création de règles pour les applications depuis la fenêtre de notification du Pare-feu

Lors du fonctionnement du Pare-feu en mode interactif ou en mode Autoriser les connexions pour les applications de confiance, vous pouvez créer un ensemble de règles directement depuis la fenêtre de notification de tentative de connexion non autorisée.

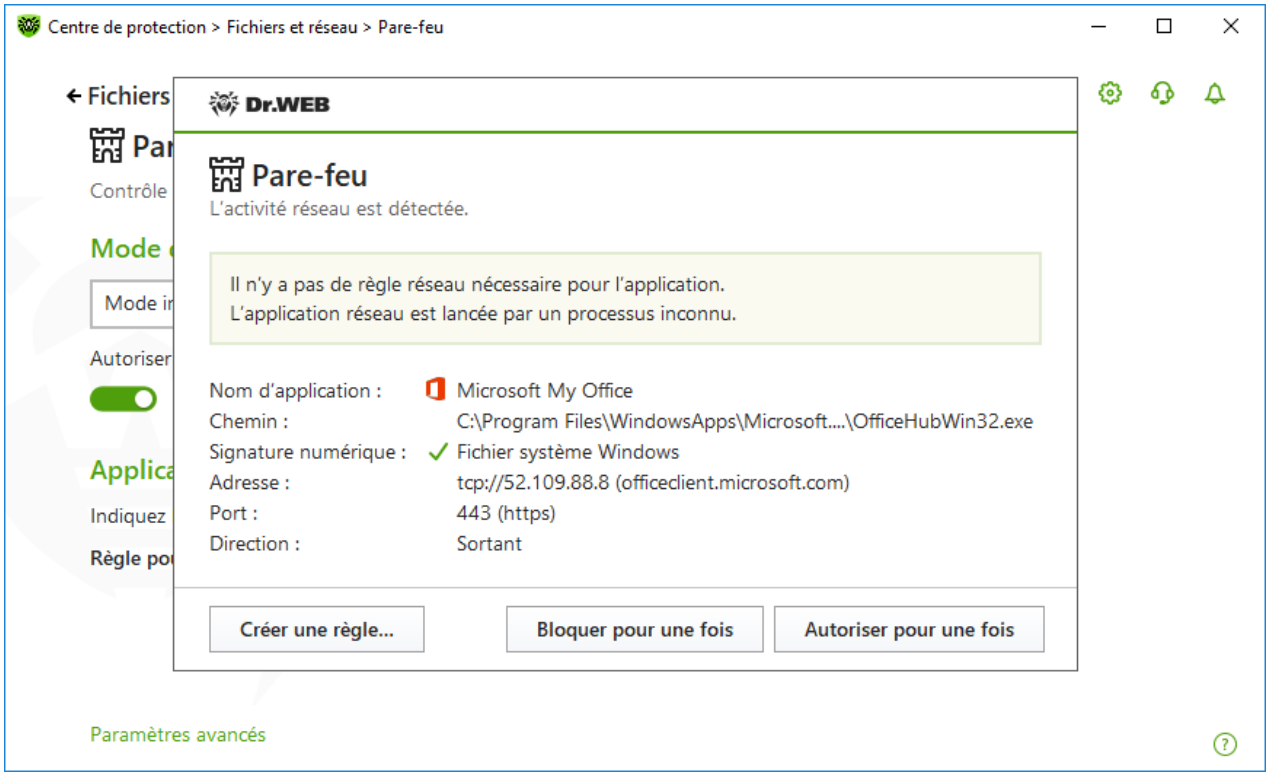

Figure 49. Exemple d'alerte en cas de tentative d'accès au réseau

Lors du fonctionnement sous un compte limité (Invité), le Pare-feu Dr.Web n'affiche pas d'alertes à l'utilisateur en cas de tentatives d'accès au réseau. Les alertes de ce type seront affichées en mode administrateur seulement si cette session est active en même temps que la session de l'invité.

Pour définir les règles des applications

1. En cas de détection d'une tentative de se connecter au réseau du côté de l'application, prenez connaissance des informations suivantes :

Champ	Description
Application	Nom du programme. Assurez-vous que le chemin vers le fichier exécutable spécifié dans le champ **Chemin** correspond à sa localisation habituelle.
Chemin	Le chemin complet vers le fichier exécutable de l'application et son nom.

Champ	Description
Signature numérique	Signature numérique de l'application.
Adresse	Protocole et adresse de l'hôte auquel on tente de se connecter.
Port	Le port utilisé lors de la tentative de connexion.
Direction	Direction de connexion.

2. Après avoir pris une décision, sélectionnez l'action appropriée en bas de la fenêtre :
   - pour bloquer une fois la connexion de l'application via le port spécifiée, sélectionnez l'action **Bloquer pour une fois** ;
   - pour autoriser une fois la connexion de l'application via le port spécifiée, sélectionnez l'action **Autoriser pour une fois** ;
   - pour ouvrir une fenêtre où vous pouvez créer une nouvelle règle de filtrage, sélectionnez **Créer une règle**. Dans la fenêtre qui s'ouvre, vous pouvez soit choisir une des règles prédéfinies, soit créer une règle pour cette application.
3. Cliquez sur **OK**. Le Pare-feu exécute l'action sélectionnée et ferme la fenêtre de notification.

Dans certains cas, le système d'exploitation Windows ne permet pas l'identification explicite d'un service qui est lancé comme un processus système. Lorsqu'une tentative de connexion d'un service système est détectée, notez le port utilisé pour la connexion indiqué dans les informations sur la connexion. Si vous utilisez l'application qui peut s'adresser à ce port, autorisez la connexion.

Lorsque la connexion a été initiée par une application connue par le Pare-feu (possédant déjà des règles) mais que cette application a été lancée par un processus parent inconnu, une notification sera affichée par le Pare-feu.

Pour définir les règles des processus parents

1. En cas de détection d'une tentative de se connecter au réseau depuis une application lancée par un programme inconnu pour le Pare-feu, prenez connaissance des informations sur le fichier exécutable du programme parent.
2. Dès que vous avez pris une décision concernant l'opération à réaliser, sélectionnez l'une des actions suivantes :
   - pour bloquer la connexion de l'application au réseau une fois, cliquez sur **Bloquer** ;
   - pour autoriser la connexion de l'application au réseau une fois, cliquez sur **Autoriser** ;
   - pour créer une nouvelle règle de filtrage, cliquez sur **Créer une règle**. Dans la fenêtre ouverte, configurez les paramètres du processus parent.
3. Cliquez sur **OK**. Le Pare-feu exécute l'action sélectionnée et ferme la fenêtre de notification.

Lorsqu'une application inconnue est lancée par une autre application inconnue, une alerte s'affiche. Cette alerte contient toutes les informations nécessaires. Si vous cliquez sur **Créer une règle**, une nouvelle fenêtre s'ouvrira, vous permettant de configurer les règles pour les applications et les processus parents.

Configuration des paramètres de règles

Les règles de filtrage des applications contrôlent l'interaction entre une application en particulier et un certain hôte réseau.

Pour créer ou éditer une règle

1. Dans l'élément **Accès aux ressources réseau**, sélectionnez le mode **Personnalisé**.
2. Dans la fenêtre **Éditer l'ensemble de règles pour**, cliquez sur le bouton ⊕ pour ajouter une nouvelle règle ou bien, sélectionnez une règle dans la liste et cliquez sur ✎ pour modifier la règle.
3. Configurez les paramètres suivants :

Paramètre	Description
Général	
Nom de règle	Le nom de la règle en cours de création/édition.
Description	La description abrégée de la règle.
Action	L'action que le Pare-feu doit accomplir lorsque une tentative de connexion à Internet est détectée : • **Bloquer les paquets** : bloquer la tentative de connexion ; • **Autoriser les paquets** : autoriser la connexion.
Statut	État de la règle : • **Activé** : la règle est appliquée ; • **Désactivé** : la règle n'est pas appliquée temporairement.
Type de connexion	Direction de la connexion : • **Entrant** : la règle s'applique lorsque quelqu'un tente de se connecter à l'application sur votre machine, depuis le réseau ; • **Sortant** : la règle s'applique lorsqu'une application sur votre machine tente de se connecter au réseau ; • **Toute** : la règle s'applique sans tenir compte de la direction de la connexion.

Paramètre	Description
Journalisation	Mode de journalisation : • **Activé** : enregistrer les événements ; • **Désactivé** : ne pas enregistrer les informations sur la règle.
Configuration de la règle	
Protocole	Les protocoles réseaux et transport utilisés lors de la tentative de connexion. Les protocoles réseaux suivants sont supportés : • IPv4 ; • IPv6 ; • IP all : toute version de protocole IP. Les protocoles de transport suivants sont supportés : • TCP ; • UDP ; • TCP & UDP – protocole TCP et UDP ; • RAW.
Adresse locale/ Adresse distante	L'adresse IP du hôte distant pour la connexion. Vous pouvez spécifier soit une adresse spécifique (**Égal**), soit plusieurs adresses IP en utilisant une plage (**Dans la plage**), vous pouvez également utiliser le masque du sous-réseau (**Masque**) ou les masques de tous les sous-réseaux dans lesquels votre ordinateur a l'adresse réseau (**MY_NETWORK**). Pour appliquer la règle à tous les hôtes distants, sélectionnez **Toute**.
Port local/Port distant	Le port utilisé pour la connexion. Vous pouvez spécifier soit un port spécifique (**Égal**), soit une plage de ports (**Dans la plage**). Pour appliquer la règle à tous les ports, sélectionnez **Toute**.

4. Cliquez sur le bouton **OK**.

Paramètres des réseaux

Le filtrage des paquets vous permet de contrôler l'accès au réseau quel que soit le programme qui initie la connexion. Le Pare-feu applique ces règles aux paquets réseaux d'un certain type transmis via les interfaces réseaux de votre ordinateur.

Ce type de filtrage vous fournit des mécanismes généraux de contrôle à la différence du filtrage au niveau des applications.

Filtre de paquets

Dans la fenêtre **Réseau**, vous pouvez configurer l'ensemble de règles de filtrage des paquets transmis via une interface particulière.

Pour accéder à la fenêtre Réseau

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la section **Fichiers et réseau**.
3. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas.
4. Cliquez sur la vignette **Pare-feu**. La fenêtre de configuration du composant va s'ouvrir.
5. Ouvrez le groupe **Paramètres avancés**.
6. Dans la section de paramètres **Paramètres de fonctionnement pour les réseaux connus**, cliquez sur **Modifier**. La fenêtre qui s'ouvre contient la liste des interfaces réseau pour lesquelles les règles sont spécifiées.

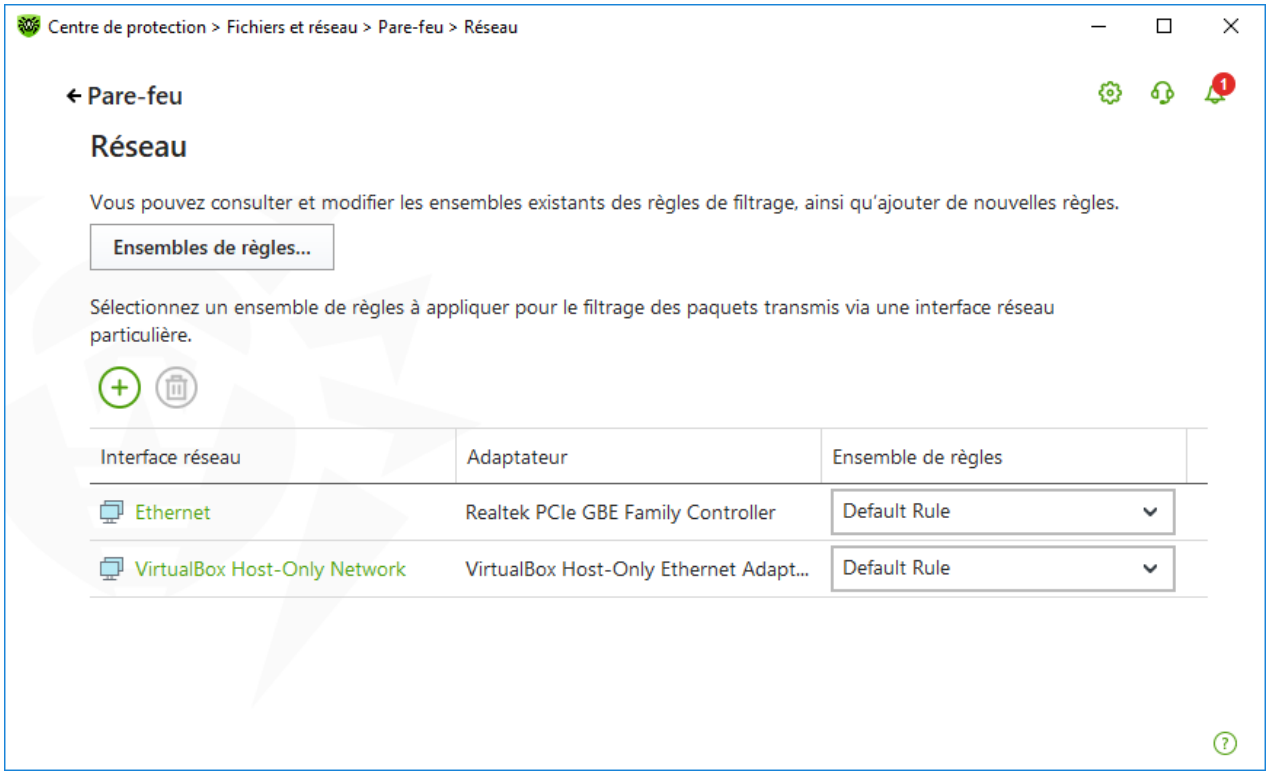

Figure 50. Ensembles de règles pour les interfaces réseau

7. Sélectionnez dans la liste l'interface de votre choix et l'ensemble de règles correspondant. Si l'ensemble de règles nécessaire n'est pas présent dans la liste, vous pouvez le créer.

Le Pare-feu est fourni avec les ensembles de règles suivants :

- **Default Rule** : cet ensemble inclut des règles décrivant les configurations systèmes les plus fréquentes et prévenant contre les attaques réseaux communes. Cet ensemble de règles est utilisé par défaut pour les nouvelles interfaces réseaux ;
- **Allow All** : laisser passer tous les paquets ;
- **Block All** : bloquer tous les paquets.

Pour passer rapidement d'un mode de filtrage à un autre, vous pouvez créer des ensembles de règles de filtrage.

Pour afficher toutes les interfaces disponibles ou ajouter une nouvelle interface dans le tableau, cliquez sur le bouton ⊕. Dans la fenêtre qui apparaît, vous pouvez spécifier les interfaces à toujours afficher dans le tableau. Les interfaces actives seront affichées automatiquement dans le tableau.

Vous pouvez supprimer les interfaces réseau inactives du tableau affiché en cliquant sur 🗑.

Pour consulter les paramètres d'une interface réseau, cliquez sur son nom.

Configuration du filtre de paquets

Pour gérer les ensembles de règles existants et ajouter de nouveaux ensembles, ouvrez la fenêtre **Configuration du filtre de paquets** en cliquant sur **Ensembles de règles**.

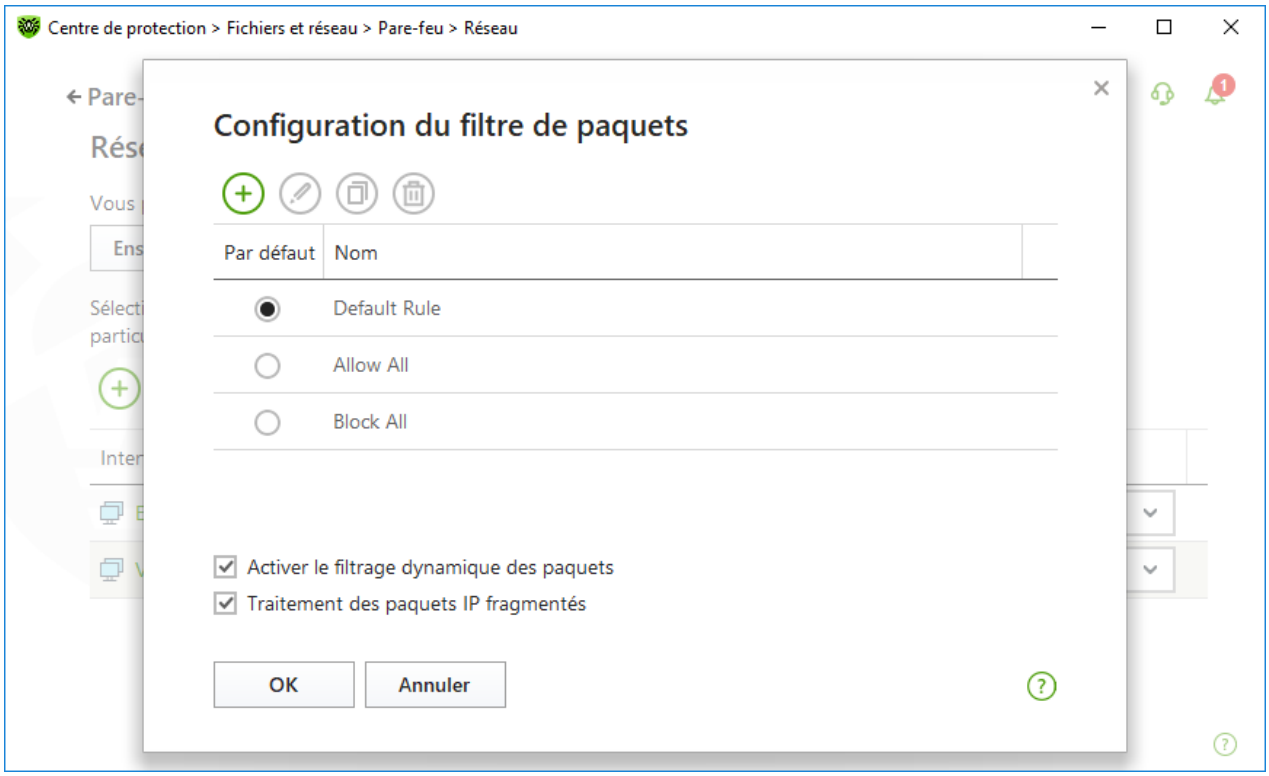

Figure 51. Fenêtre Configuration du filtre de paquets

Sur cette page, vous pouvez :

- configurer les ensembles de règles de filtrage en ajoutant de nouvelles règles, en modifiant ou en supprimant les règles existantes ;
- configurer les paramètres avancés du filtrage.

Création d'un ensemble de règles

Pour créer un ensemble de règles, effectuez l'une des actions suivantes :

- pour créer un ensemble de règles d'une interface réseau, cliquez sur ⊕ ;
- pour éditer un ensemble de règles, sélectionnez-le dans la liste et cliquez sur ✎ ;
- pour ajouter une copie de l'ensemble de règles existant, cliquez sur ⧉. La copie sera ajoutée sous l'ensemble sélectionné ;
- pour supprimer un ensemble de règles, sélectionnez-le et cliquez sur 🗑.

Paramètres avancés

Pour spécifier les paramètres avancés du filtrage de paquets, dans la fenêtre **Configuration du filtre de paquets**, cochez les cases suivantes :

Option	Description
Activer le filtrage dynamique des paquets	Cochez cette case pour filtrer les paquets selon l'état des connexions TCP existantes. Le Pare-feu bloquera les paquets qui ne correspondent pas aux connexions actives selon les spécifications des protocoles TCP. Cette option protège votre ordinateur contre les attaques DoS (par déni de service), scan des ressources, vol de données et autres opérations malveillantes. Il est également recommandé d'activer le filtrage dynamique des paquets si vous utilisez des protocoles de transfert de données complexes tels que FTP, SIP, etc. Décochez cette case pour filtrer les paquets sans tenir compte des sessions TCP.
Traitement des paquets IP fragmentés	Cochez cette case pour garantir le traitement correct de larges volumes de données. La taille de MTU (Maximum Transmission Unit) peut varier en fonction de différents réseaux, ainsi les paquets IP importants peuvent arriver fragmentés. Lorsque cette option est activée, le Pare-feu applique la règle sélectionnée pour le premier fragment du paquet IP important à tous les autres fragments. Décochez cette case pour traiter tous les paquets indépendamment.

Cliquez sur **OK** pour sauvegarder les modifications apportées ou **Annuler** pour quitter sans enregistrer les modifications apportées.

Ensemble de règles de filtrage de paquets

La fenêtre **Éditer l'ensemble de règles** donne la liste des règles de filtrage de paquets pour l'ensemble sélectionné. Vous pouvez configurer la liste en ajoutant de nouvelles règles pour une application ou modifier les règles existantes et l'ordre de leur exécution. Les règles sont appliquées selon leur ordre dans la liste.

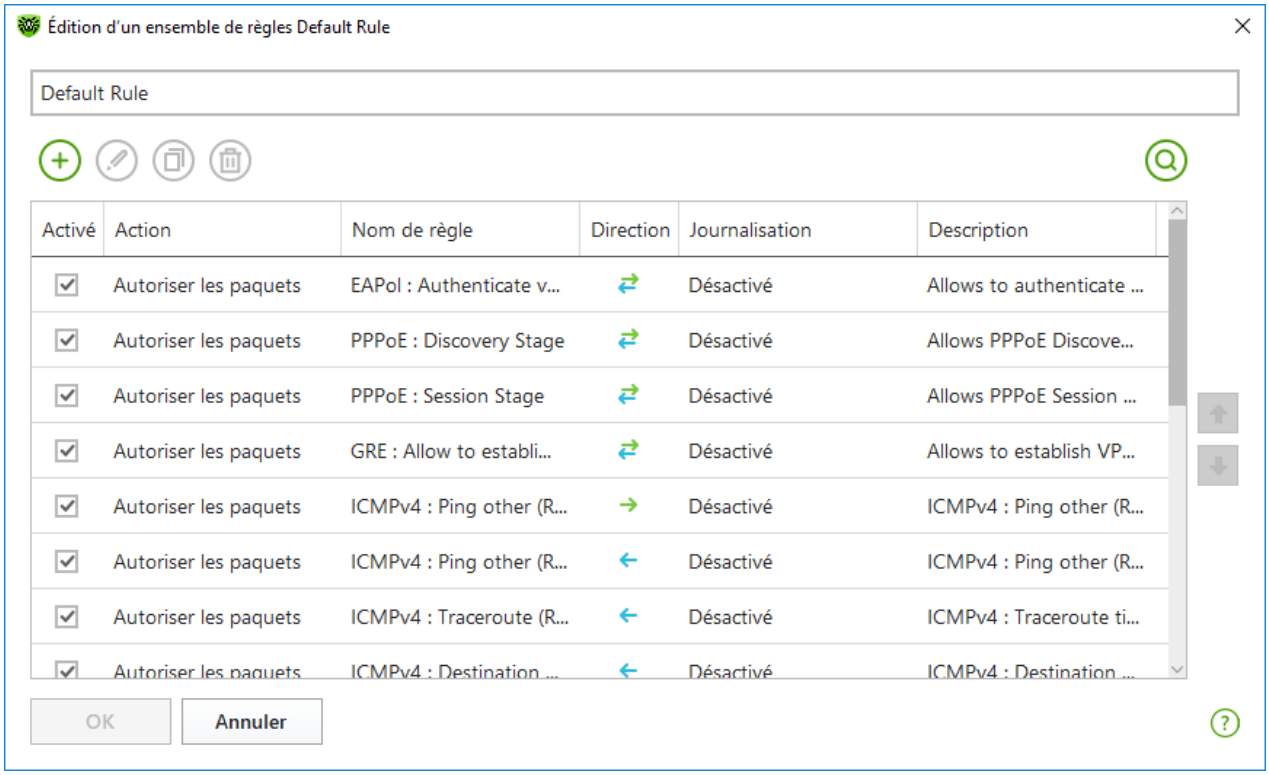

Figure 52. Ensemble de règles de filtrage de paquets

Pour chaque règle dans un ensemble, les informations suivantes s'affichent :

Paramètre	Description
Activé	État de l'exécution de la règle.
Action	L'action du Pare-feu lorsqu'un paquet est intercepté : • **Bloquer les paquets** : bloquer le paquet ; • **Autoriser les paquets** : transmettre le paquet.
Nom de règle	Le nom de la règle.
Direction	Direction de la connexion : • ← : la règle s'applique lorsque le paquet provient du réseau ;

Paramètre	Description
	• : la règle s'applique lorsque le paquet est envoyé dans le réseau depuis votre machine ; • : la règle s'applique sans tenir compte de la direction de la connexion.
Journalisation	Mode de journalisation des événements. Il spécifie les informations à enregistrer dans le journal : • **En-têtes seulement** : enregistrer uniquement les en-têtes de paquets ; • **Paquet entier** : enregistrer les paquets entiers ; • **Désactivé** : ne pas enregistrer les informations sur le paquet.
Description	La description abrégée de la règle.

Pour éditer ou créer un ensemble de règles

1. Si nécessaire, spécifiez le nom ou changez le nom de l'ensemble de règles.
2. Utilisez les options suivantes pour créer des règles de filtrage :
   - pour ajouter une nouvelle règle, cliquez sur . La nouvelle règle est ajoutée au début de la liste ;
   - pour modifier la règle sélectionnée, cliquez sur ;
   - pour ajouter une copie de la règle sélectionnée, cliquez sur . La copie est ajoutée devant la règle sélectionnée ;
   - pour supprimer la règle sélectionnée, cliquez sur ;
   - pour trouver la règle nécessaire, cliquez sur .
3. Si vous avez choisi de créer une nouvelle règle ou d'éditer une règle existante, configurez ses paramètres.
4. Utilisez la flèche près de la liste pour changer l'ordre des règles. Les règles sont appliquées en fonction de l'ordre dans lequel elles apparaissent dans l'ensemble.
5. A la fin de l'édition, cliquez sur le bouton **OK** pour sauvegarder les modifications apportées ou sur le bouton **Annuler** pour refuser les modifications.

> Les paquets pour lesquels il n'y a pas de règles dans l'ensemble de règles sont automatiquement bloqués, sauf les paquets autorisés dans les règles du Filtre d'applications.

Configuration des paramètres de règles de filtrage

Pour ajouter ou éditer une règle de filtrage

1. Dans la fenêtre de modification de l'ensemble de règles du filtre de paquets, cliquez sur ⊕ ou sur ✎. Ceci ouvre la fenêtre de création ou de modification de règle de filtrage de paquets.

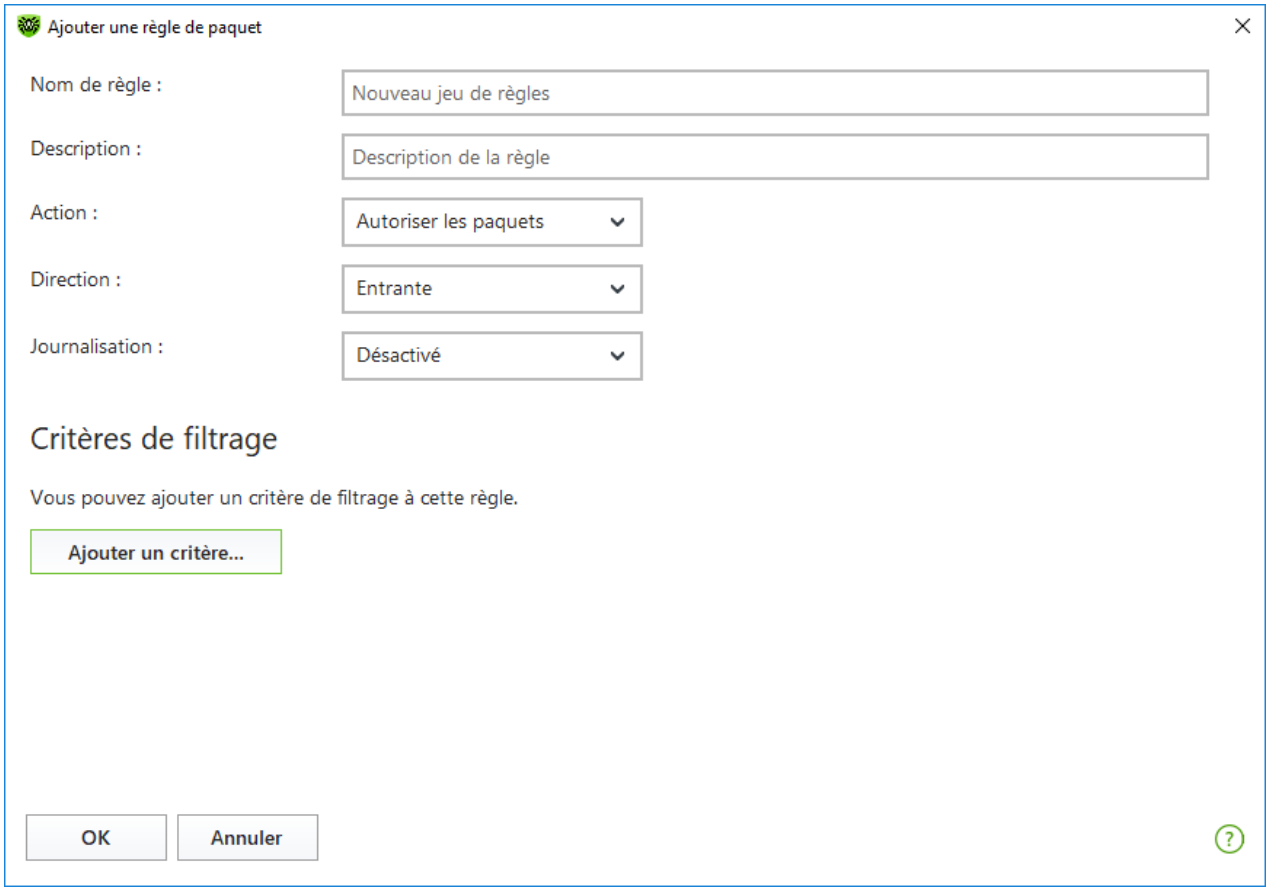

Figure 53. Ajout d'une règle de filtrage

2. Configurez les paramètres suivants :

Paramètre	Description
Nom de règle	Le nom de la règle en cours de création/édition.
Description	La description abrégée de la règle.
Action	L'action du Pare-feu lorsqu'un paquet est intercepté : • **Bloquer les paquets** : bloquer le paquet ; • **Autoriser les paquets** : transmettre le paquet.
Direction	Direction de la connexion : • **Entrant** : la règle s'applique lorsque le paquet provient du réseau ;

Paramètre	Description
	• **Sortant** : la règle s'applique lorsque le paquet est envoyé dans le réseau depuis votre machine ; • **Toute** : la règle s'applique sans tenir compte de la direction de la connexion.
Journalisation	Mode de journalisation des événements. Il spécifie les informations à enregistrer dans le journal : • **Paquet entier** : enregistrer les paquets entiers ; • **En-têtes seulement** : enregistrer uniquement les en-têtes de paquets ; • **Désactivé** : ne pas enregistrer les informations sur le paquet.

3. Si nécessaire, ajoutez un critère de filtrage, par exemple le protocole de transport ou le protocole réseau en cliquant sur **Ajouter un critère**. La fenêtre **Ajouter un critère de filtrage** va s'ouvrir :

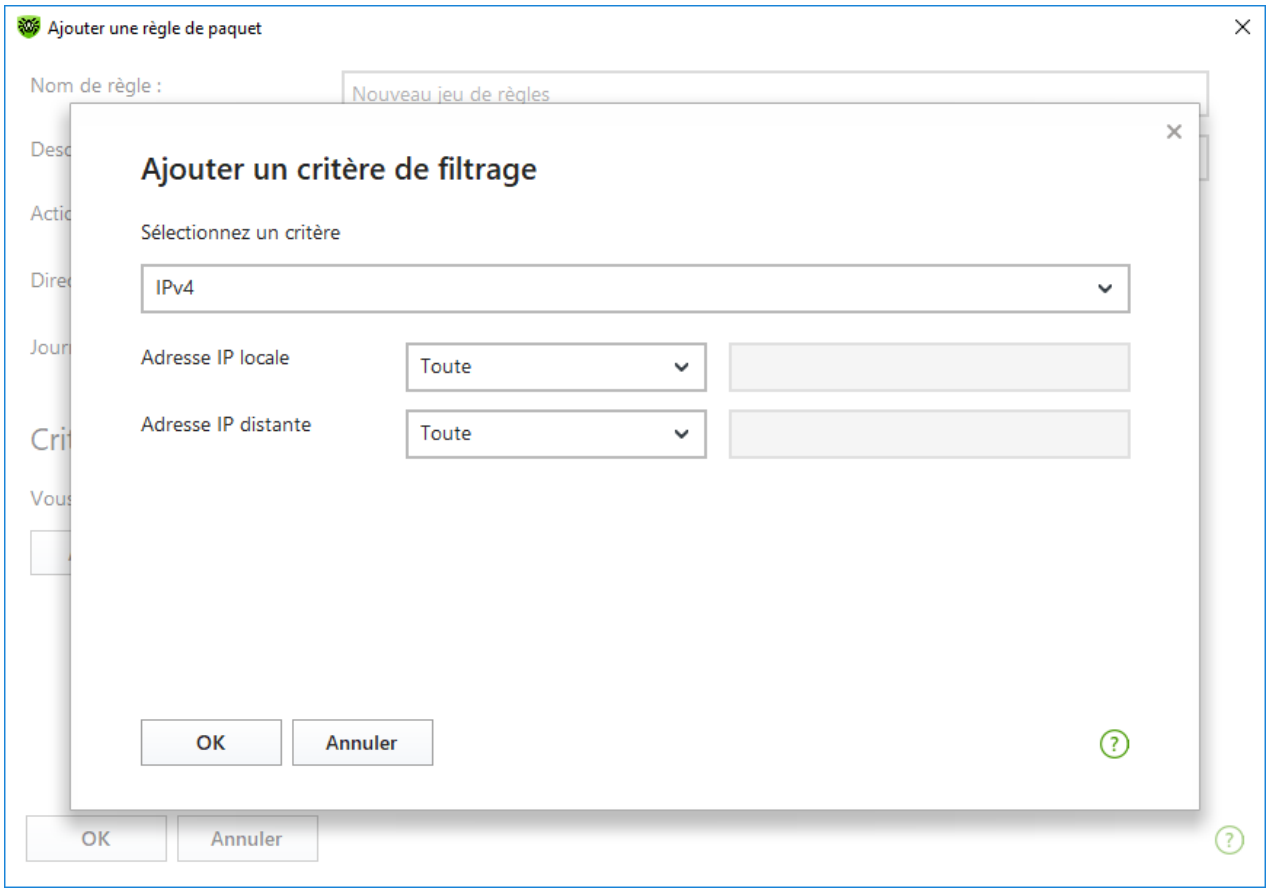

Figure 54. Ajout d'un critère de filtrage

Sélectionnez le critère nécessaire dans la liste déroulante. Dans cette fenêtre, vous pouvez configurer les paramètres pour le critère sélectionné. Vous pouvez ajouter autant de critères que vous le souhaitez. Pour que l'action de la règle soit appliquée au paquet, il faut que le paquet réponde à tous les critères de la règle.

Des critères complémentaires sont disponibles pour certains en-têtes. Tous les critères ajoutés sont affichés dans la fenêtre d'édition de la règle de paquet et ils sont disponibles pour l'édition.

4. Cliquez ensuite sur **OK** pour enregistrer les modifications ou sur **Annuler** pour les annuler.

> ⚠ Si vous n'ajoutez aucun critère de filtrage, alors cette règle autorisera ou bloquera tous les paquets (en fonction de la configuration du champ **Action**).

Si dans cette règle, dans l'en-tête IPv4, vous sélectionnez la valeur **Toute** pour les paramètres **Adresse IP locale** et **Adresse IP distante**, la règle sera appliquée à tout paquet contenant l'en-tête IPv4 et envoyé depuis l'adresse physique d'un ordinateur local.

10.4. Analyse de l'ordinateur

L'analyse antivirus de l'ordinateur est effectuée par le composant Scanner. Scanner analyse les secteurs d'amorçage, la mémoire vive, des fichiers particuliers et des objets contenus dans des structures complexes telles que les archives, les conteneurs et les e-mails avec des pièces jointes. Toutes les méthodes de détection des menaces sont utilisées pour l'analyse.

En cas de détection d'un objet malveillant, le Scanner signale uniquement la menace détectée. Le rapport sur les résultats de l'analyse s'affiche dans un tableau où vous pouvez choisir l'action nécessaire pour traiter un objet malveillant ou suspect. Vous pouvez appliquer les actions définies par défaut à toutes les menaces détectées ou sélectionner une méthode appropriée pour traiter des objets particuliers.

Les actions par défaut sont optimales dans la plupart des cas, mais si besoin est, vous pouvez les modifier dans la fenêtre de configuration du Scanner. Les actions à appliquer à objet particulier peuvent être choisies après la fin de l'analyse, tandis que les paramètres généraux relatifs à la neutralisation des types différents de menaces doivent être spécifiés avant de procéder à l'analyse.

Voir aussi :

- Paramètres de l'analyse de fichiers
- Lancement et modes de l'analyse
- Neutralisation des menaces détectées

10.4.1. Lancement et modes de l'analyse

Pour lancer l'analyse de fichiers

> ⚠ Si vous utilisez Windows Vista ou un système d'exploitation ultérieur, il est recommandé de lancer le Scanner avec les droits d'administrateur. Sinon, les fichiers et les dossiers auxquels l'utilisateur sans droits n'a pas accès (y compris les dossiers système) ne seront pas analysés.

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.

2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Fichiers et réseau**, ensuite sur la vignette **Scanner**.

> Vous pouvez également lancer l'analyse des fichiers en ouvrant le menu **Démarrage**, le groupe **Dr.Web** et en sélectionnant l'élément **Scanner Dr.Web**.

3. Sélectionnez le mode d'analyse nécessaire :
   - l'élément **Rapide** pour analyser uniquement les zones critiques de Windows ;
   - l'élément **Complète**, pour analyser tous les fichiers sur les disques logiques et les supports amovibles ;
   - l'élément **Personnalisée** pour scanner uniquement les objets que vous avez désignés. La fenêtre de sélection de fichiers pour l'analyse de Scanner va s'ouvrir.

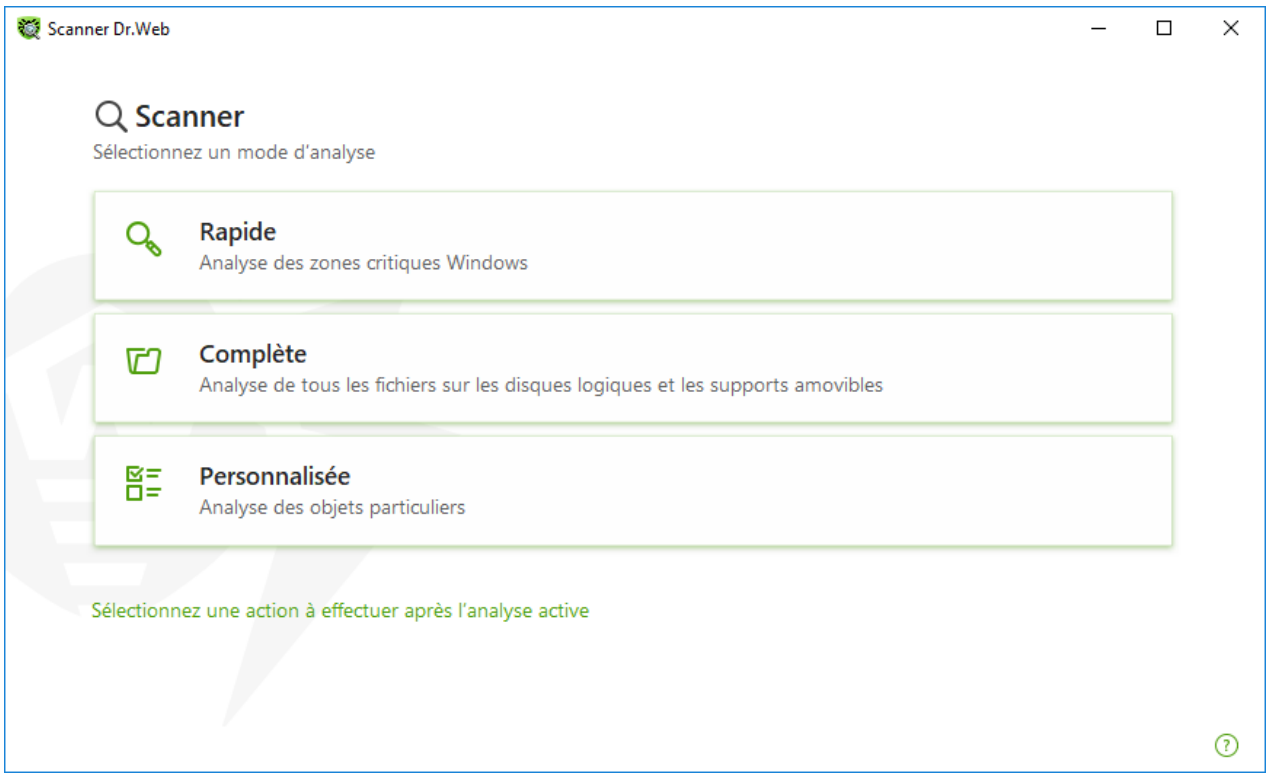

Figure 55. Sélection d'un mode de l'analyse

Vous pouvez également sélectionner une action après le scan en cliquant sur le lien correspondant dans la partie inférieure de la fenêtre. Cette action ne dépend pas des paramètres sélectionnés du Scanner en n'influence pas les paramètres généraux.

4. L'analyse va commencer. Pour suspendre l'analyse, cliquez sur **Pause**. Pour arrêter l'analyse définitivement, cliquez sur **Stop**.

> Le bouton **Pause** est indisponible lors de l'analyse de la mémoire vive et des processus.

A la fin de l'analyse, le Scanner vous informe des menaces détectées et propose de les neutraliser.

Pour analyser un fichier ou un dossier particulier

1. Ouvrez le menu contextuel en cliquant droit sur le nom du fichier ou du répertoire (sur le bureau ou dans l'explorateur de Windows).
2. Sélectionnez l'élément **Analyser par Dr.Web**. L'analyse sera effectuée conformément aux paramètres par défaut.

Description des modes d'analyse

Mode d'analyse	Description
Rapide	Dans ce mode sont analysés : • secteurs d'amorçage de tous les disques ; • mémoire vive ; • dossier racine du disque de démarrage ; • dossier système Windows ; • dossier « Mes documents » ; • 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 e-mail ne sont pas scannés.
Complète	Dans ce mode, la mémoire vive et tous les disques durs (y compris les secteurs d'amorçage) sont scannés. La recherche des rootkit est également effectuée.
Personnalisée	Dans ce mode, vous pouvez analyser des fichiers et des dossiers, ainsi que la mémoire vive, les secteurs d'amorçage, etc. Pour ajouter un objet dans la liste d'analyse, cliquez sur le bouton ⊕.

10.4.2. Neutralisation des menaces détectées

A la fin de l'analyse, le Scanner vous informe des menaces détectées et propose de les neutraliser.

⚠ Si dans les paramètres du Scanner Dr.Web, vous avez sélectionné l'élément **Neutraliser les menaces détectées** ou **Neutraliser les menaces détectées et arrêter l'ordinateur** pour le paramètre **Après la fin de l'analyse**, les menaces seront neutralisées automatiquement.

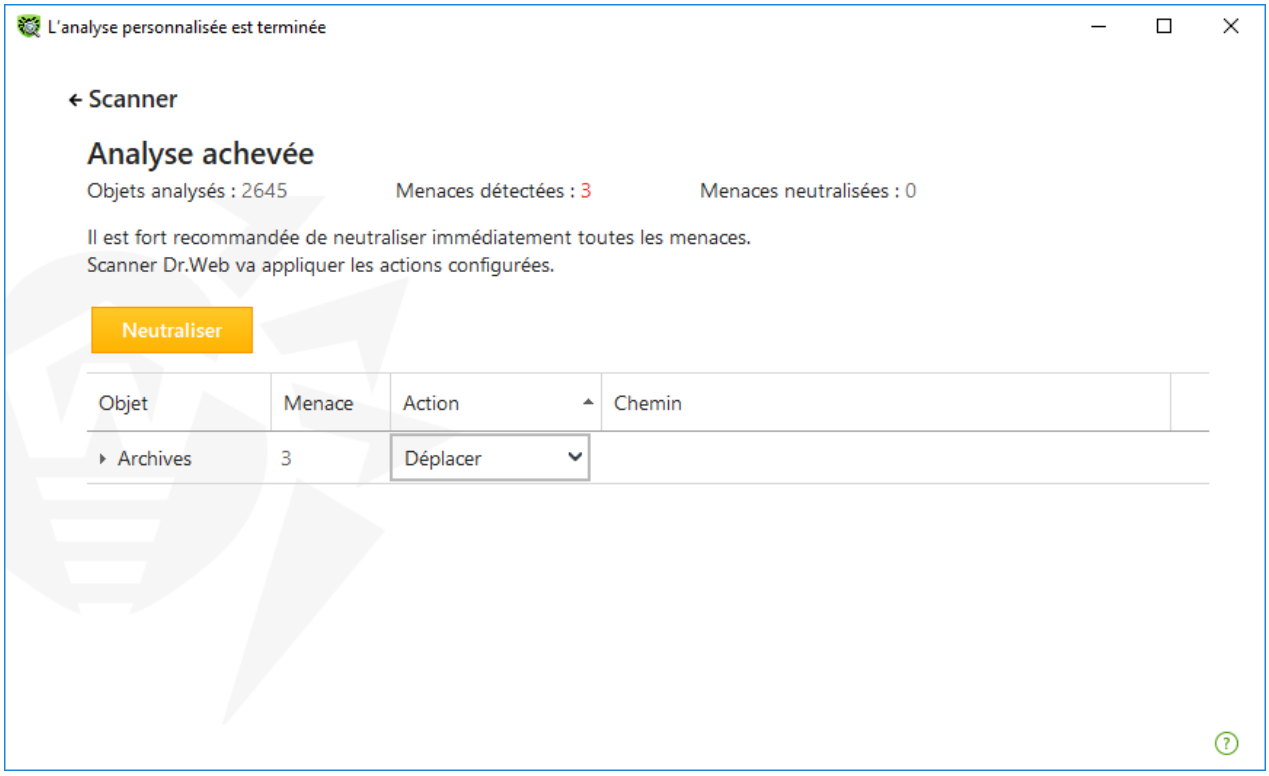

Figure 56. Sélection de l'action à la fin de l'analyse

Le tableau de résultats de l'analyse contient les informations suivantes :

Colonne	Description
Objet	Cette colonne comporte le nom de l'objet suspect ou contaminé (nom du fichier en cas de contamination d'un fichier, **Boot sector** si un secteur d'amorçage est contaminé, **Master Boot Record** si le MBR du disque dur est infecté).
Menace	Ici vous trouverez le nom du virus ou d'une modification de virus selon la classification interne de l'entreprise Doctor Web. Pour les objets suspects détectés, il est indiqué que l'objet est « probablement infecté » et le type du virus supposé selon la classification de l'analyseur heuristique est également affiché.
Action	Cette colonne contient l'action pour la menace détectée conformément aux paramètres du Scanner. À l'aide de la liste déroulante, vous pouvez définir l'action pour la menace sélectionnée.
Chemin	Ce colonne affiche le chemin complet vers le fichier correspondant.

Neutralisation de toutes les menaces dans le tableau

Pour chaque menace, l'action est spécifiée conformément aux paramètres du Scanner. Pour neutraliser toutes les menaces en appliquant les actions indiquées dans le tableau, cliquez sur **Neutraliser**.

Pour modifier l'action appliquée à la menace indiquée dans le tableau

1. Sélectionnez un objet ou un groupe d'objets.
2. Dans la colonne **Action** de la liste déroulante, sélectionnez l'action nécessaire.
3. Cliquez sur le bouton **Neutraliser**. Dans ce cas, le Scanner commence à neutraliser toutes les menaces dans le tableau.

Neutralisation des menaces sélectionnées

Vous pouvez neutraliser les menaces sélectionnées séparément. Pour ce faire :

1. Sélectionnez un objet, plusieurs objets (en maintenant la touche CTRL enfoncée) ou un groupe d'objets.
2. Cliquez droit pour ouvrir le menu contextuel et sélectionnez l'action nécessaire. Le Scanner commencera à neutraliser la menace (les menaces) sélectionnée uniquement.

Limitations lors de la neutralisation des menaces

Restrictions existantes :

- il est impossible de désinfecter les objets suspects ;
- il est impossible de déplacer ou supprimer les objets qui ne sont pas des fichiers (par exemple, les secteurs d'amorçage) ;
- il est impossible d'effectuer action quelconque pour des fichiers particuliers au sein des archives, des packages d'installation ou dans des e-mails. Dans ce cas, l'action sera appliquée à l'objet entier.

Rapport sur le fonctionnement du Scanner

Le journal détaillé sur le fonctionnement du composant est enregistré dans le fichier journal `dwscanner.log` se trouvant dans le dossier `%USERPROFILE%\Doctor Web`.

10.4.3. Options supplémentaires

Cette section contient les informations sur les fonctionnalités supplémentaires du Scanner :

- Lancement du Scanner avec les paramètres de la ligne de commande
- Scanner en ligne de commande
- Lancement de l'analyse selon la planification

Lancement du Scanner avec les paramètres de la ligne de commande

Vous pouvez lancer le Scanner en mode de ligne de commande. Ce mode vous permet de configurer les paramètres avancés pour la session courante de l'analyse ainsi qu'une liste des objets à scanner en tant que paramètres de lancement. C'est en mode de ligne de commande que vous pouvez réaliser le lancement automatique du Scanner selon la planification.

Syntaxe de la commande de lancement :

`[<chemin_vers_le_programme>]dwscanner [<clés>] [<objets>]`

Clés : paramètres de la ligne de commande déterminant la configuration du logiciel. Si aucune clé n'est présente, le scan sera réalisé avec les paramètres enregistrés précédemment (ou avec les paramètres définis par défaut s'ils n'ont pas été modifiés). Les clés commencent par le symbole slash (/) et sont séparées par des espaces comme les autres paramètres de ligne de commande.

La liste des objets à scanner peut être vide ou contenir plusieurs éléments séparés par des blancs. Si le chemin vers les objets à analyser n'est pas spécifié, la recherche sera effectuée dans le dossier d'installation Dr.Web.

Les variantes suivantes d'indication des objets d'analyse sont fréquemment utilisées :

- `/FAST` : commande d'effectuer une analyse rapide du système.
- `/FULL` : commande d'effectuer une analyse complète de tous les disques durs et de tous les supports amovibles (y compris les secteurs d'amorçage).
- `/LITE` : commande d'effectuer un scan du système en analysant la mémoire vive, les secteurs d'amorçage de tous les disques, une recherche des rootkit sera également réalisée.

Scanner en ligne de commande

Le jeu de composants Dr.Web inclut également le Scanner en ligne de commande qui permet de réaliser l'analyse en mode ligne de commande et offre à l'utilisateur les possibilités avancées de configuration.

Le Scanner en ligne de commande place des objets suspects en Quarantaine.

Afin de lancer le Scanner en ligne de commande, utilisez la commande suivante :

`[<chemin_vers_le_programme>]dwscancl [<clés>] [<objets>]`

Une clé commence par le symbole « / », plusieurs clés sont séparées par des espaces. La liste des objets à scanner peut être vide ou peut contenir plusieurs éléments séparés par des espaces.

Pour la liste des clés du Scanner en ligne de commande, consulter l'Annexe A.

Codes de retour :

0 : l'analyse est achevée avec succès, aucun objet infecté n'est trouvé

1 : l'analyse est achevée avec succès, des objets infectés ont été détectés

10 : les clés non valides sont spécifiées

11 : le fichier clé est introuvable ou ne supporte pas le Scanner en ligne de commande

12 : Scanning Engine n'est pas lancé

255 : l'analyse est interrompue par l'utilisateur

Lancement de l'analyse dans le Planificateur de tâches Windows

Lors de l'installation de Dr.Web, une tâche d'analyse antivirus est automatiquement créée dans le Planificateur de tâche Windows (par défaut, la tâche est désactivée).

Pour consulter les paramètres de tâche, ouvrez le **Panneau de configuration** (affichage détaillé) → **Outils d'administration** → **Planificateur de tâches**.

Dans la liste de tâches, sélectionnez la tâche d'analyse antivirus. Vous pouvez activer la tâche ainsi que configurer l'heure du démarrage et spécifier les paramètres nécessaires.

Sur l'onglet **Général** en bas de la fenêtre, les informations générales sur la tâche et les options de sécurité sont affichées. Sur les onglets **Déclencheurs** et **Conditions** vous pouvez spécifier les conditions qui déclenchent l'exécution de la tâche. Pour consulter l'historique des évènements, allez sur l'onglet **Journal**.

Vous pouvez également créer vos propres tâches d'analyse antivirus. Pour en savoir plus, consultez la rubrique d'aide et la documentation de l'OS Windows.

Si le Pare-feu est installé, il bloquera le planificateur de tâches après l'installation de Dr.Web et le premier redémarrage du système. Les **tâches planifiées** seront effectuées uniquement après le second redémarrage si une nouvelle règle a déjà été créée.

10.5. Dr.Web pour Microsoft Outlook

Les fonctions clés du composant

Le plug-in Dr.Web pour Microsoft Outlook exécute les fonctions suivantes :

- l'analyse antivirus des fichiers contenus dans les pièces jointes des messages entrants ;
- l'analyse de messages entrant via la connexion sécurisée SSL ;
- la détection et neutralisation de programmes malveillants ;
- l'analyse heuristique pour une protection plus fiable contre les virus inconnus.

Configuration du plag-in Dr.Web pour Microsoft Outlook

Vous pouvez configurer les paramètres et consulter les statistiques du programme dans le client de messagerie Microsoft Outlook. Pour cela, allez dans la rubrique **Outils** → **Options** → onglet **Antivirus Dr.Web** (dans Microsoft Outlook 2010 — rubrique **Fichiers** → **Options** → **Compléments**, puis sélectionnez le module Dr.Web pour Microsoft Outlook et cliquez sur **Options du complément**).

L'onglet **Antivirus Dr.Web** dans les paramètres de Microsoft Outlook n'est disponible que si l'utilisateur dispose des droits permettant de modifier les paramètres.

L'onglet **Antivirus Dr.Web** affiche le statut actuel de la protection (active/inactive) et permet d'accéder aux fonctions suivantes :

- Journal permet de configurer l'écriture des événements dans le fichier de journal ;
- Contrôle des pièces jointes permet de configurer le contrôle du courrier électronique et de spécifier des réactions en cas de détection d'objets malveillants ;
- Statistiques affiche des informations sur les objets analysés et traités par l'application.

10.5.1. Analyse antivirus

Dr.Web pour Microsoft Outlook utilise les diverses méthodes de détection des virus. L'utilisateur peut spécifier les réactions à appliquer aux objets malveillants détectés : le programme peut réparer les objets infectés, ainsi que les supprimer ou les déplacer en Quarantaine pour les isoler et les conserver de manière sécurisée.

L'application Dr.Web pour Microsoft Outlook détecte les objets malveillants suivants :

- objets infectés ;
- bombes de décompression ou bombes d'archive ;
- adwares ;
- hacktools ;
- dialers ;
- canulars ;
- riskwares ;
- spywares ;
- chevaux de Troie ;
- vers et virus.

Actions

Dr.Web pour Microsoft Outlook peut être configuré pour réagir en cas de détection de fichiers infectés ou suspects et de programmes malveillants lors de l'analyse des pièces jointes du courrier électronique.

Pour configurer l'analyse des pièces jointes et déterminer les actions, dans l'application Microsoft Outlook, allez à **Outils** → **Options** → onglet **Antivirus Dr.Web** (sous Microsoft Outlook 2010, dans la section **Fichier** → **Options** → **Compléments** choisissez Dr.Web pour Microsoft Outlook et cliquez sur le bouton **Options du complément**) et cliquez sur **Analyse de pièces jointes**.

La fenêtre **Analyse de pièces jointes** est disponible à condition que l'utilisateur dispose des droits administrateur.

Sous l'OS Windows Vista ou supérieur, si vous cliquez sur le bouton **Analyse de pièces jointes** :

- Lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas des droits administrateur sera invité à saisir les informations d'authentification de l'administrateur système ;
- Lorsque UAC est désactivé : l'administrateur peut modifier les paramètres de l'application, l'utilisateur ne pourra pas accéder à la modification des paramètres.

La fenêtre **Contrôle de pièces jointes** vous permet de configurer les réactions de l'application face à différentes catégories d'objets analysés ainsi qu'en cas d'erreurs survenues lors de l'analyse. Il existe également une possibilité de configurer l'analyse des archives.

Utilisez les paramètres listés ci-dessous pour configurer les réactions face aux objets malveillants détectés :

- la liste déroulante **Infectés** définit la réaction en cas de détection d'objets infectés par des virus connus et probablement curables ;
- la liste déroulante **Non désinfectés** définit la réaction en cas de détection d'objets infectés par un virus connu et incurable ainsi qu'en cas d'échec de la tentative de désinfection ;
- la liste déroulante **Suspects** définit la réaction face aux objets probablement infectés par un virus (réaction du moteur heuristique) ;
- la section **Programmes malveillants** définit la réaction en cas de détection des programmes malveillants suivants :
  - adwares ;
  - dialers ;
  - canulars ;
  - hacktools ;
  - riskware ;

- la liste déroulante **En cas d'échec de l'analyse** permet de configurer les réactions dans le cas où l'analyse de la pièce jointe serait impossible, par exemple en cas de pièce jointe contenant un fichier endommagé ou protégé par un mot de passe ;
- la case **Analyse des archives** permet d'activer ou de désactiver l'analyse des fichiers archivés en pièce jointe. Cochez cette case pour activer l'analyse, décochez-la pour la désactiver.

Le jeu de réactions applicables est fonction de l'événement viral.

Les réactions ci-dessous sont applicables aux objets détectés :

- **Désinfecter** : l'application va tenter de désinfecter l'objet infecté (cette action est disponible uniquement pour les objets infectés) ;
- **Supprimer** : supprimer l'objet du système ;
- **Déplacer vers la quarantaine** : isoler l'objet dans le dossier de Quarantaine ;
- **Ignorer** : laisser passer l'objet sans modifications.

10.5.2. Journal des événements

Dr.Web pour Microsoft Outlook enregistre les erreurs survenues et les événements dans les journaux suivants :

- journal d'événements système (Event Log) ;
- journal texte de débogage.

Journal d'événements système

Le journal d'événement système (Event Log) collecte les informations suivantes :

- messages sur l'arrêt ou le démarrage de l'application ;
- paramètres du fichier clé : validité ou non validité de la licence, la durée de validité de la licence (ces informations sont écrites au démarrage, lors du fonctionnement ou lors du remplacement du fichier clé) ;
- paramètres des modules : scanner, moteur, bases virales (ces informations sont écrites au démarrage ou lors de la mise à jour des modules) ;
- message sur la non validité de la licence : fichier clé absent, autorisation manquante sur l'utilisation des modules dans le fichier clé, licence bloquée, violation d'intégrité du fichier clé (ces informations sont écrites au démarrage et lors du fonctionnement de l'application) ;
- messages sur la détection des virus ;
- notifications sur l'expiration de la licence (ces informations sont enregistrées 30, 15, 7, 3, 2 ou 1 jour(s) avant la date d'expiration).

Pour afficher le journal d'événements système

1. Allez au **Panneau de configuration du système d'exploitation**.

2. Sélectionnez la section **Outils d'administration** → **Observateur d'événements**.
3. Dans la partie gauche de la fenêtre **Observateur d'événements**, sélectionnez l'élément **Application**. La liste des événements enregistrés dans le journal par des applications utilisateurs va s'afficher. La source des messages pour Dr.Web pour Microsoft Outlook est l'application Dr.Web pour Microsoft Outlook.

Journal texte de débogage

Le journal texte de débogage collecte les informations listées ci-dessous :

- messages sur la validité ou non validité de la licence ;
- messages sur la détection des virus ;
- messages sur des erreurs survenues lors de l'écriture dans des fichiers ou lors de la lecture depuis des fichiers ainsi que sur des erreurs d'analyse des archives ou des fichiers protégés par mot de passe ;
- paramètres des modules : scanner, moteur, bases virales ;
- messages sur les arrêts urgents du moteur ;
- notifications sur l'expiration de la licence (ces informations sont enregistrées 30, 15, 7, 3, 2 ou 1 jour(s) avant la date d'expiration).

Pur configurer l'enregistrement des événements

1. Dans l'onglet **Antivirus Dr.Web**, cliquez sur le bouton **Journal**. La fenêtre de paramètres du journal s'ouvre.
2. Pour obtenir le niveau maximum de détails du fichier de journal, cochez la case **Écrire le journal détaillé**. Par défaut, la journalisation est paramétrée en mode standard.

La journalisation détaillée du programme ralentit les performances du serveur ; ainsi, il est recommandé d'activer le niveau maximum de détail uniquement en cas d'erreur de Dr.Web pour Microsoft Outlook.

3. Cliquez sur **OK** pour sauvegarder les modifications apportées.

La fenêtre **Journal** est disponible à condition que l'utilisateur dispose des droits administrateur.

Sous Windows Vista ou une version supérieure, si vous cliquez sur le bouton **Journal** :

- lorsque UAC est activé : l'administrateur sera invité à confirmer l'action de l'application, l'utilisateur qui ne dispose pas des droits administrateur sera invité à saisir les informations d'authentification de l'administrateur système ;
- lorsque UAC est désactivé : l'administrateur peut modifier les paramètres de l'application, l'utilisateur ne pourra pas accéder à la modification des paramètres.

Pour voir le journal des événements du logiciel

1. Dans l'onglet **Antivirus Dr.Web**, cliquez sur le bouton **Journal**. La fenêtre de paramètres du journal s'ouvre.
2. Cliquez sur le bouton **Afficher dans le dossier**. Le dossier dans lequel est sauvegardé le journal sera ouvert.

10.5.3. Statistiques de l'analyse

Dans l'application Microsoft Outlook, la section **Outils** → **Options** → l'onglet **Antivirus Dr.Web** (en cas de Microsoft Outlook 2010, allez dans la section **Fichier** → **Options** → **Compléments**, sélectionnez le module **Dr.Web pour Microsoft Outlook** et cliquez sur **Options de complément**) offre des informations statistiques sur le total d'objets analysés et traités par l'application.

Les objets sont divisés en catégories suivantes :

- **Analysés** : le total des objets et des messages analysés ;
- **Infectés** : le total des objets infectés dans les pièces jointes de messages ;
- **Suspects** : le total des messages probablement infectés par des virus (réaction du moteur heuristique) ;
- **Désinfectés** : le total des objets désinfectés par l'application ;
- **Non analysés** : le total des objets dont l'analyse est impossible ou entraîne des erreurs d'analyse ;
- **Sains** : le total des objets et des messages qui ne contiennent aucun objet malveillant.

Les informations suivantes seront également affichées :

- **Déplacés** : le total des objets déplacés en Quarantaine ;
- **Supprimés** : le total des objets supprimés du système ;
- **Ignorés** : le total des objets sautés sans modifications ;
- **Messages spam** : le total des messages classés comme spam.

Par défaut, les statistiques sont sauvegardées dans le fichier `drwebforoutlook.log` se trouvant dans le dossier `%USERPROFILE%\Doctor Web`.

Les informations statistiques sont accumulées pendant une session. Après le redémarrage de l'ordinateur ou lors d'un nouveau lancement de Antivirus Dr.Web pour Windows, les statistiques sont remises à zéro.

11. Protection préventive

Dans ce groupe de paramètres, vous pouvez configurer la réaction de Dr.Web à des actions d'autres applications qui pourraient compromettre la sécurité de votre ordinateur et choisir le niveau de la protection contre les exploits.

Pour accéder au groupe de paramètres Protection préventive

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Protection préventive**.

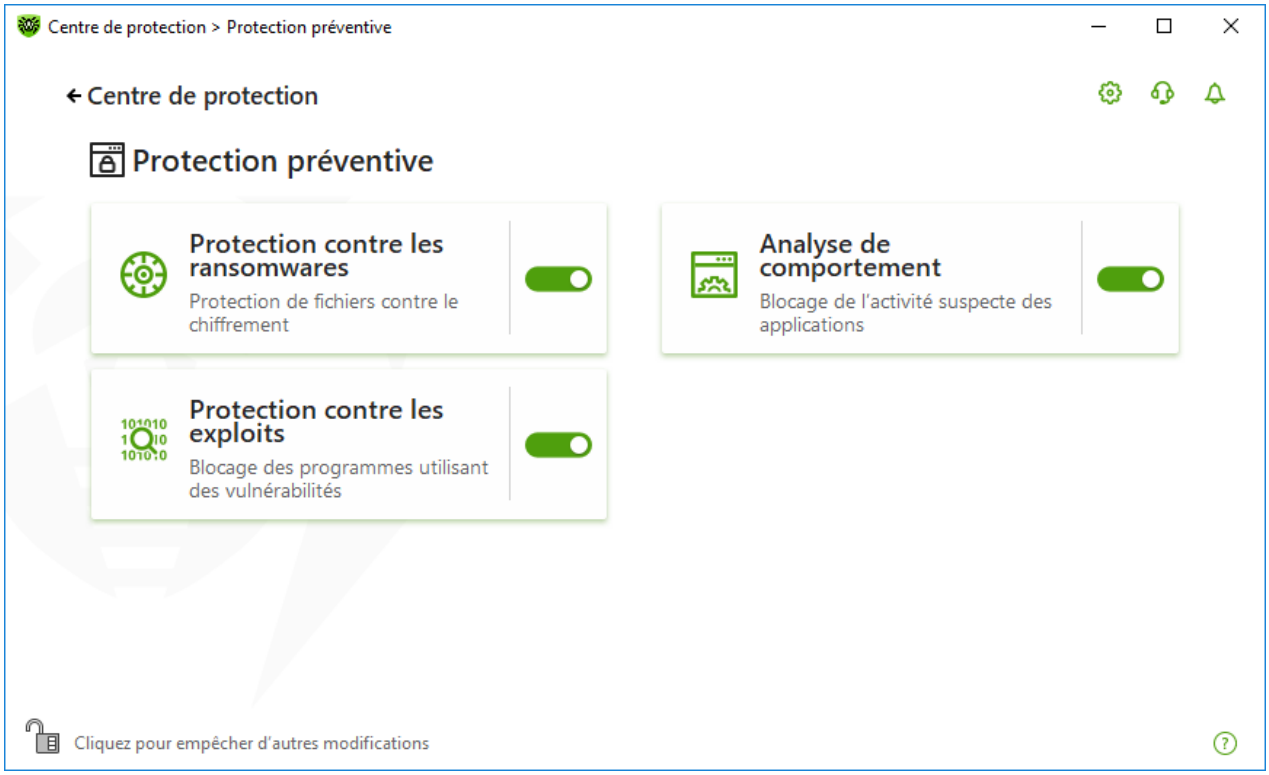

Figure 57. Fenêtre Protection préventive

Activation et désactivation des composants de protection

Activez ou désactivez le composant nécessaire avec l'interrupteur .

Pour accéder aux paramètres des composants

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
2. Cliquez sur la vignette du composant nécessaire.

Dans cette section :

- Analyse de comportement : paramètres d'interdiction d'accès d'applications aux objets système.

- Protection contre les ransomwares : paramètres d'interdiction de chiffrer les fichiers d'utilisateurs.
- Protection contre les exploits : paramètres d'interdiction d'utiliser les vulnérabilités dans des applications.

> ⚠ Pour *désactiver* un composant, Dr.Web doit fonctionner en mode administrateur. Pour cela, cliquez sur le cadenas en bas de la fenêtre du logiciel.

11.1. Protection contre les ransomwares

Le composant Protection contre les ransomwares permet de détecter les processus qui essaient de chiffrer les fichiers d'utilisateur avec un algorithme connu qui indique que le processus peut compromettre la sécurité de l'ordinateur. Les *Trojans-encodeurs* font parties de tels processus. Ces programmes malveillants s'introduisent dans l'ordinateur de l'utilisateur, bloquent l'accès aux données et demandent de l'argent pour le déblocage. Ce virus est l'un des programmes malveillants les plus répandus et entraîne des pertes considérables aux entreprises et aux utilisateurs. La voie principale de propagation du virus est l'envoi de messages contenant un fichier malveillant ou un lien vers le virus.

Selon les statistiques de Doctor Web, le déchiffrement des fichiers endommagés par un Trojan n'est possible que dans 10 % des cas. C'est pourquoi, il est plus efficace de prévenir l'infection. Ces derniers temps, le nombre d'utilisateurs touchés par ce virus diminue. Pourtant le nombre de requêtes de déchiffrement de données envoyées au support technique de Doctor Web atteint 1000 par mois.

Pour activer ou désactiver le composant Protection contre les ransomwares

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Protection préventive**.
3. Activez ou désactivez le composant Protection contre les ransomwares avec l'interrupteur .

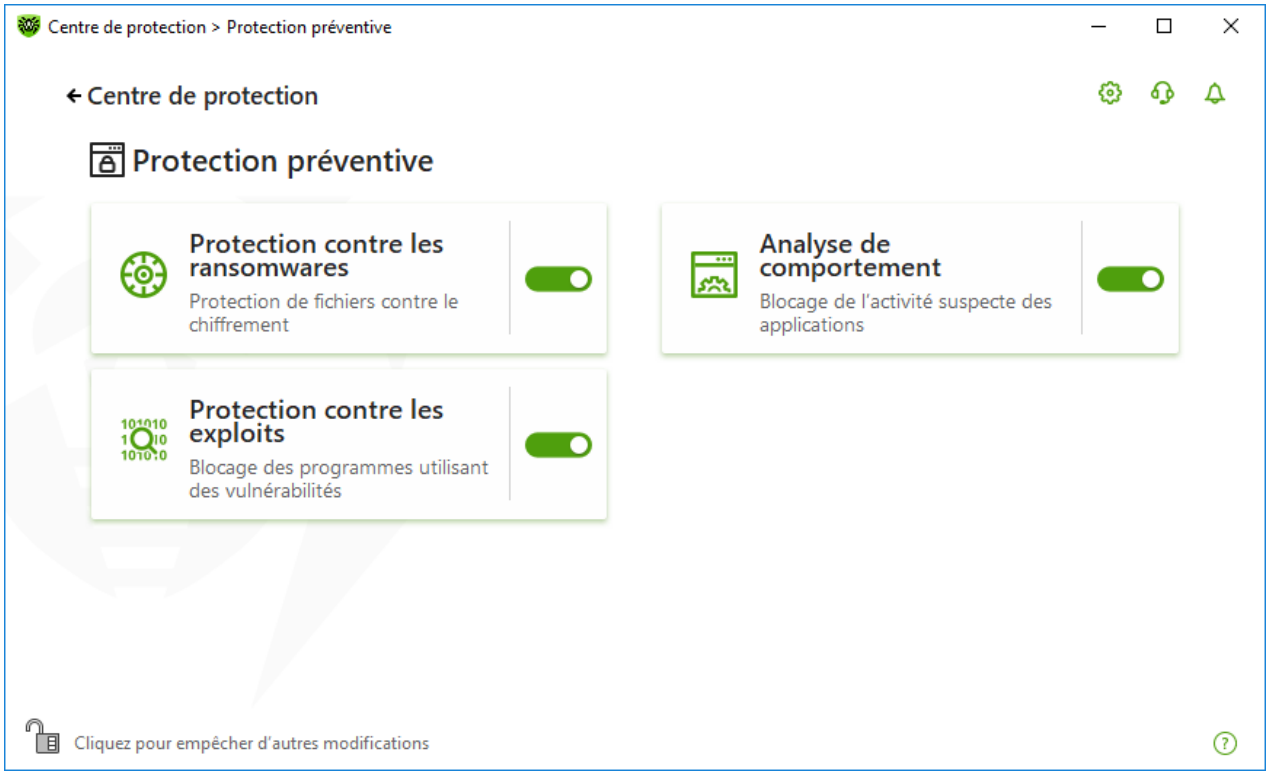

Figure 58. Activation/désactivation du composant Protection contre les ransomwares

Dans cette section :

- Configuration de la réaction à une tentative de chiffrer les fichiers
- Exclusions de l'analyse

Réaction de Dr.Web aux tentatives d'applications de chiffrer un fichier

Pour configurer les paramètres du composant Protection contre les ransomwares

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
2. Cliquez sur la vignette **Protection contre les ransomwares**. La fenêtre de paramètres du composant va s'ouvrir.
3. Dans le menu déroulant, sélectionnez une action qui sera appliquée à toutes les applications.

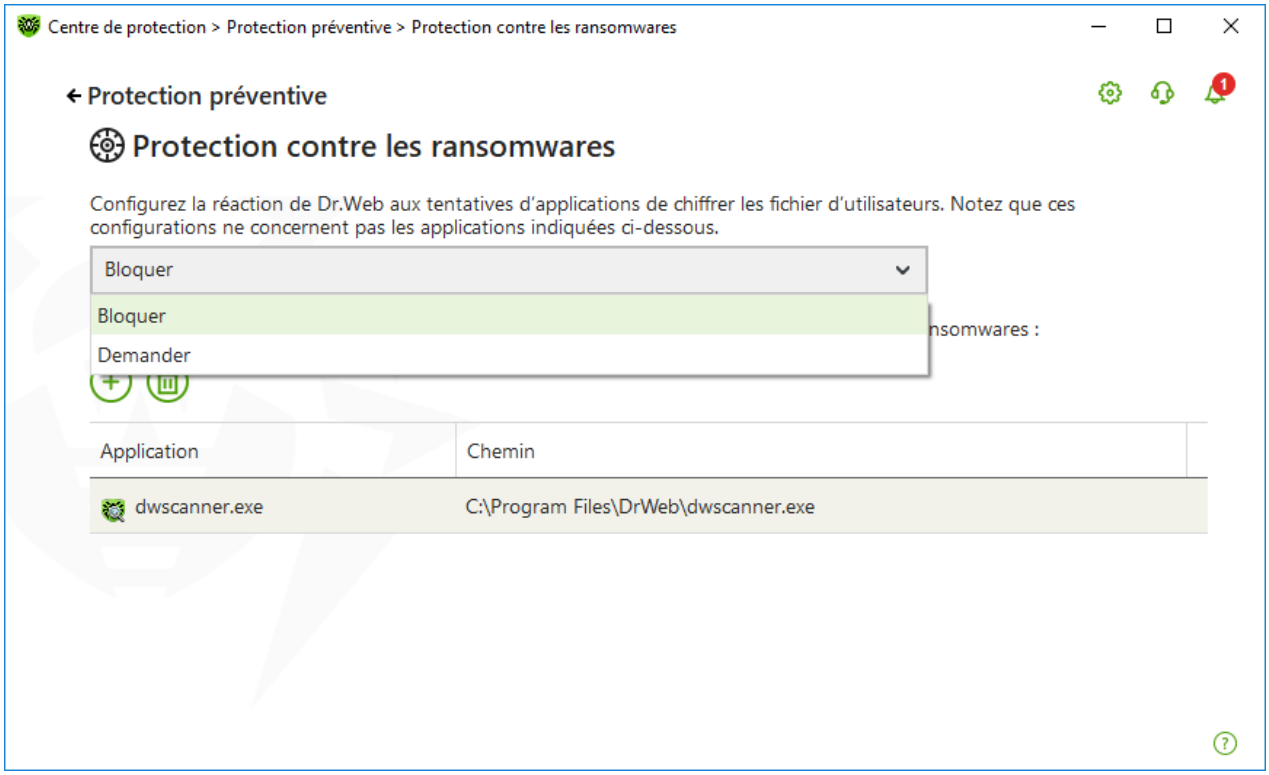

Figure 59. Sélection de réaction de Dr.Web

- **Bloquer** : aucune application ne sera autorisée de chiffrer les fichiers d'utilisateur. Ce mode est spécifié par défaut. Si une application tente de chiffrer les fichiers de l'utilisateur, une notification s'affichera :

Figure 60. Exemple d'une notification contenant l'interdiction de modification des fichiers d'utilisateur

- **Demander** : en cas de tentative de chiffrement d'un fichier d'utilisateur, une notification s'affichera et vous pourrez interdire à l'application d'effectuer cette action ou l'ignorer :

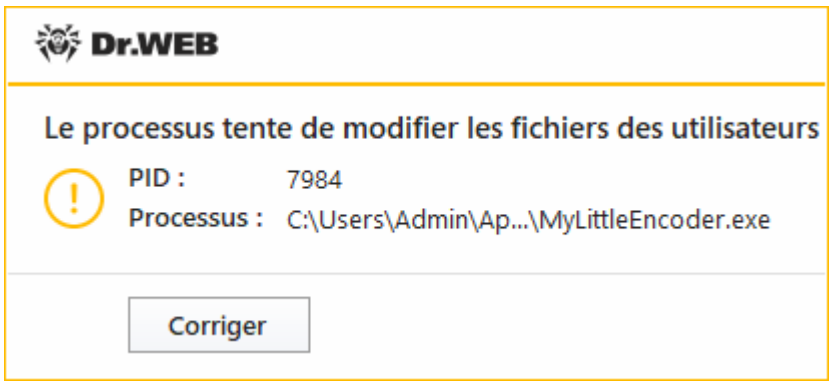

Figure 61. Exemple de notification informant d'une tentative de modifier les fichiers d'utilisateur

- Si vous cliquez sur le bouton **Corriger**, le processus sera bloqué et mis en quarantaine. Même en cas de restauration de l'application de la quarantaine, elle ne sera pas lancée avant le redémarrage de l'ordinateur.
- Si vous fermez la fenêtre de notification, l'application ne sera pas désinfectée.

Réception de notifications

Vous pouvez configurer l'affichage des notifications des actions du composant Protection contre les ransomwares sur l'écran ou l'envoi des notifications par e-mail.

Voir aussi :

- Notifications

Liste des applications exclues de l'analyse

Vous pouvez créer une liste des applications à exclure de l'analyse effectuée par le composant Protection contre les ransomwares. Pour gérer les objets dans la liste, les éléments de gestion suivants sont disponibles :

- Bouton ⊕ : ajout d'une application aux exclusions de l'analyse.
- Bouton 🗑 : suppression d'une application de la liste des exclusions.

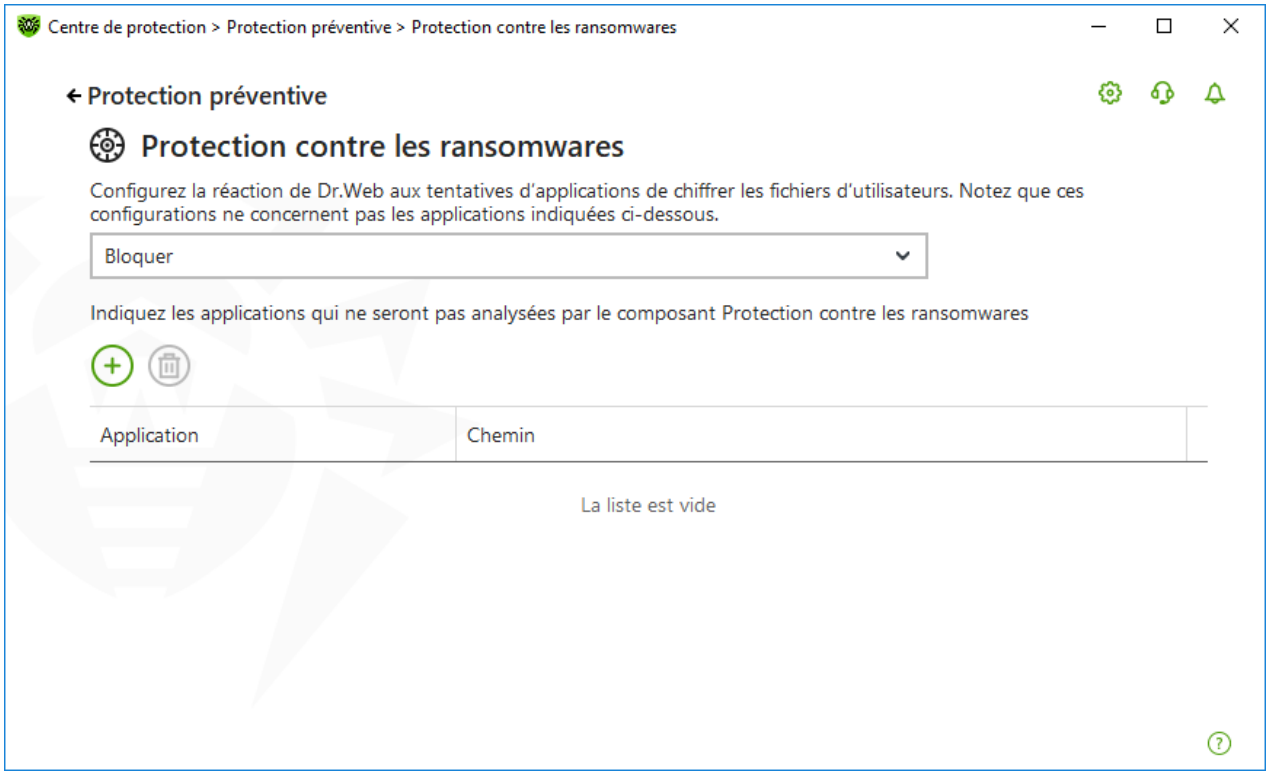

Figure 62. Exclusions de l'analyse effectuée par la Protection contre les ransomwares

Pour ajouter une application à la liste

1. Cliquez sur ⊕ et, dans la fenêtre qui s'affiche, sélectionnez l'application nécessaire.
2. Cliquez sur **OK**.

11.2. Analyse de comportement

Le composant Analyse de comportement permet de configurer la réaction de Dr.Web aux actions d'applications tierces qui peuvent infecter votre ordinateur, par exemple, aux tentatives de modifier le fichier HOSTS ou de modifier les branches critiques du registre. En cas d'activation du composant Analyse de comportement, le programme interdit une modification automatique des objets système dont la modification indique clairement une tentative d'affecter le système d'exploitation. L'analyse de comportement protège le système contre les programmes malveillants inconnus qui ne sont pas détectés par l'analyse de signature et les mécanismes heuristique traditionnels. Les données les plus récentes du service cloud Dr.Web sont utilisées pour déterminer la nocivité des applications.

Pour activer ou désactiver le composant Analyse de comportement

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Protection préventive**.
3. Activez ou désactivez le composant Analyse de comportement avec l'interrupteur.

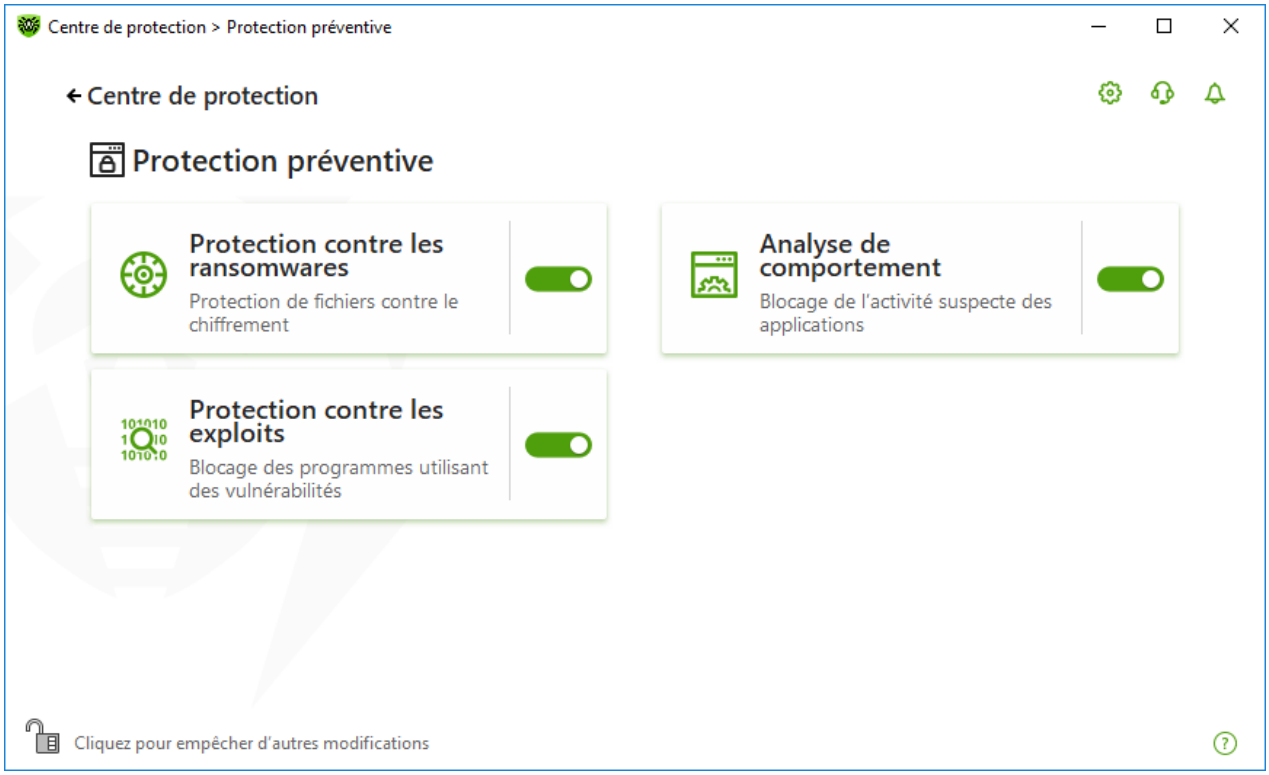

Figure 63. Activation/désactivation du composant Analyse de comportement

Dans cette section :

- Modes de fonctionnement du composant
- Création et modification de règles particulières pour les applications
- Description des objets protégés

Paramètres de l'Analyse de comportement

Les paramètres par défaut sont optimaux dans la plupart des cas. Ne les modifiez pas si ce n'est pas nécessaire.

Pour accéder aux paramètres du composant Analyse de comportement

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
2. Cliquez sur la vignette **Analyse de comportement**. La fenêtre de paramètres du composant va s'ouvrir.

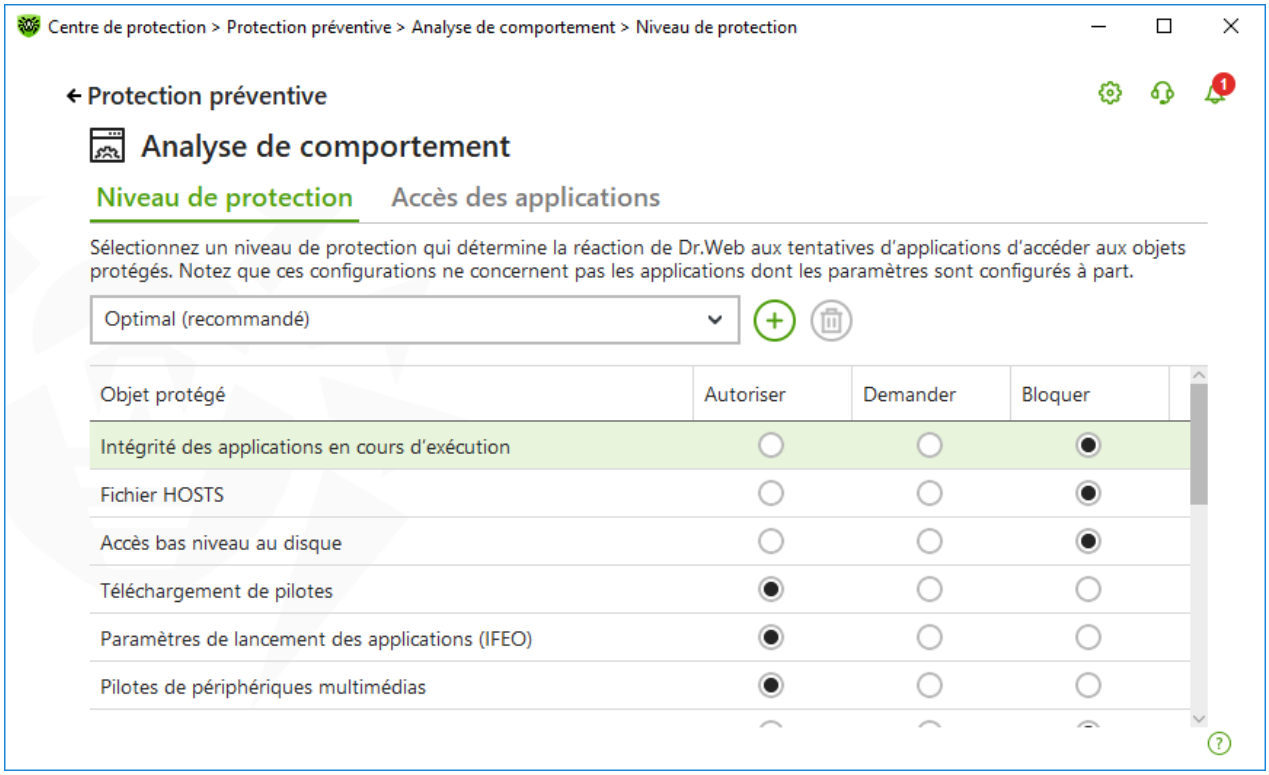

Figure 64. Paramètres de l'Analyse de comportement

Vous pouvez spécifier un niveau de protection à part pour les objets et les processus particuliers et le niveau général dont les configurations seront appliquées à tous les autres processus. Pour spécifier le niveau général de protection, dans l'onglet **Niveau de protection**, sélectionnez le niveau nécessaire dans la liste déroulante.

Niveaux de protection

Niveau de protection	Description
Optimal (recommandé)	Utilisé par défaut. Dr.Web interdit la modification automatique des objets système, la modification qui indiquerait clairement une tentative malveillante d'endommager le système d'exploitation. L'accès bas niveau au disque est interdit également, ainsi que toute modification du fichier HOSTS par les applications dont les actions sont considérées comme tentative d'endommager le système d'exploitation. ⚠ Seules les actions des applications qui ne sont pas de confiance sont bloquées.
Moyen	Vous pouvez choisir ce niveau de protection, s'il existe un risque élevé d'infection. Dans ce mode, l'accès aux objets critiques qui peuvent être potentiellement utilisés par des programmes malveillants est bloqué.

	⚠ L'utilisation de ce mode peut entraîner des problèmes de compatibilité avec des logiciels légitimes qui utilisent les branches du registre protégées.
Paranoïde	Ce niveau de protection est nécessaire pour avoir un contrôle total de l'accès aux objets critiques de Windows. Dans ce mode, vous aurez également un contrôle interactif du chargement de pilotes et du démarrage automatique de programmes.
Personnalisé	Dans ce mode, vous pouvez choisir vous-même les niveaux de protection pour chaque objet.

Mode utilisateur

Toutes les modifications des paramètres sont enregistrées en mode Personnalisé. Dans cette fenêtre, vous pouvez également créer un nouveau profil pour sauvegarder les paramètres nécessaires. Quels que soient les paramètres du composants, les objets protégés seront accessibles en lecture.

Vous pouvez choisir une réaction de Dr.Web aux tentatives d'applications de modifier les objets protégés :

- **Autoriser** : l'accès à l'objet protégé est autorisée pour toutes les applications.
- **Demander** : une notification sera affichée si une application tente de modifier l'objet protégée :

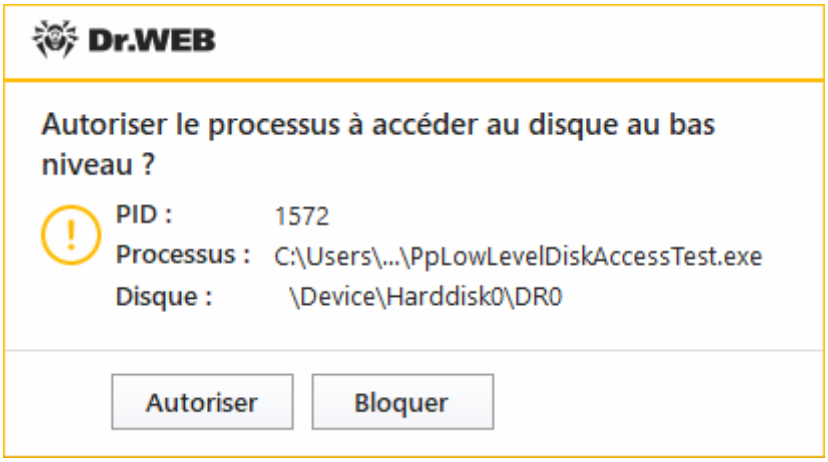

Figure 65. Exemple de notification contenant une demande d'accès à l'objet protégé

- **Demander** : si une application tente de modifier l'objet protégé, l'accès de l'application sera refusé. Une notification correspondante sera affichée :

Figure 66. Exemple de notification contenant l'interdiction d'accès à l'objet protégé

Pour créer un nouveau niveau de protection

1. Consultez les paramètres de protection spécifiés par défaut. Modifiez-les, si cela est nécessaire.
2. Cliquez sur ⊕.
3. Dans la fenêtre qui s'affiche, indiquez le nom du nouveau profil.
4. Cliquez sur **OK**.

Pour supprimer un niveau de protection

1. Dans la liste déroulante, sélectionnez le niveau de protection que vous voulez supprimer.
2. Cliquez sur le bouton 🗑. Il est impossible de supprimer les profils prédéfinis.
3. Cliquez sur **OK** pour confirmer la suppression.

Réception de notifications

Vous pouvez configurer l'affichage de notifications des actions du composant Analyse de comportement sur l'écran ou l'envoi des notifications par e-mail.

Voir aussi :

- Notifications

Accès des applications

Pour configurer certains paramètres d'accès pour les applications concrètes, ouvrez l'onglet **Accès des applications**. Dans la fenêtre qui s'affiche, vous pouvez ajouter une nouvelle règle pour l'application, modifier une règle déjà créée ou supprimer une règle inutile.

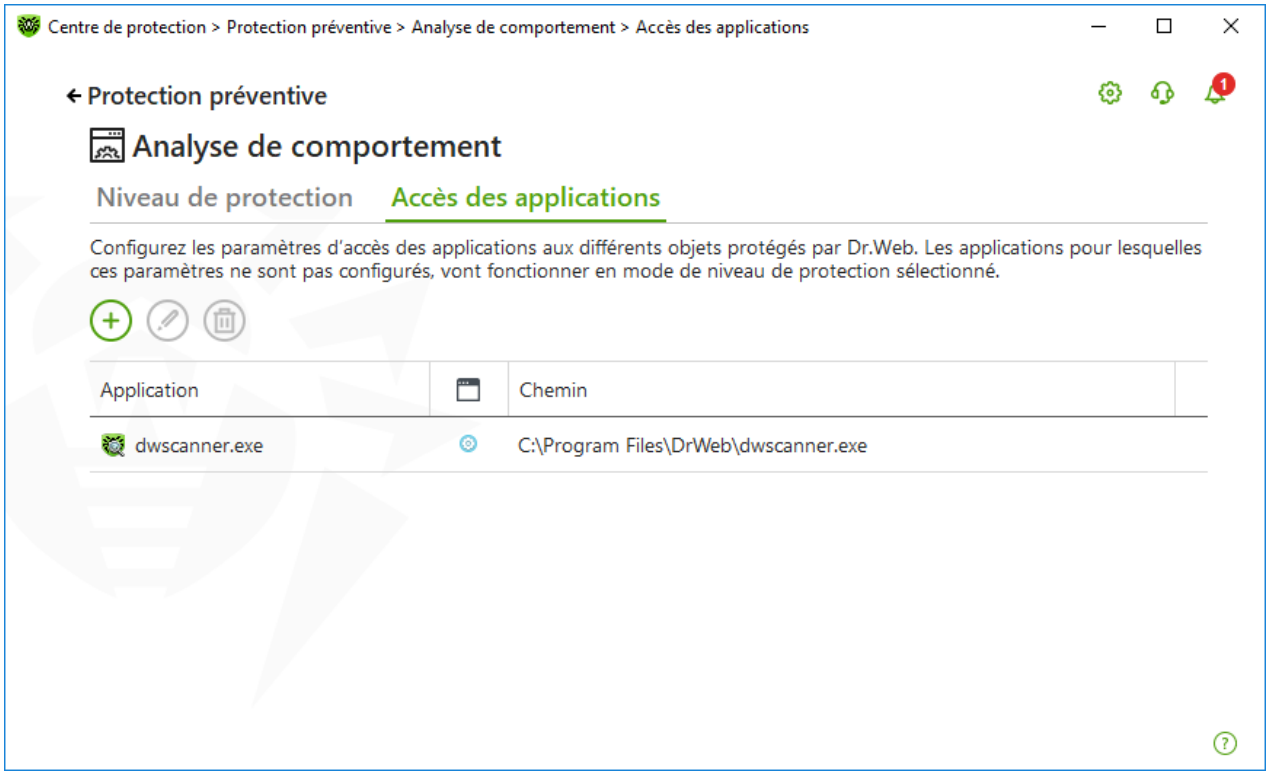

Figure 67. Paramètres d'accès pour les applications

Pour gérer les objets dans le tableau, les éléments de gestion suivants sont fournis :

- Bouton : ajout d'un ensemble de règles pour l'application.
- Bouton : édition d'un ensemble de règles existants.
- Bouton : suppression d'un ensemble de règles.

Dans la colonne (**Type de règle**), trois types de règles peuvent s'afficher :

- : la règle **Autoriser tout** est spécifiée pour tous les objets protégés.
- : des règles différentes sont spécifiées pour les objets protégés.
- : la règle **Bloquer tout** est spécifiée pour tous les objets protégés.

Pour ajouter une règle pour l'application

1. Cliquez sur .
2. Dans la fenêtre qui s'affiche, cliquez sur **Parcourir** et spécifiez le chemin d'accès au fichier exécutable de l'application.

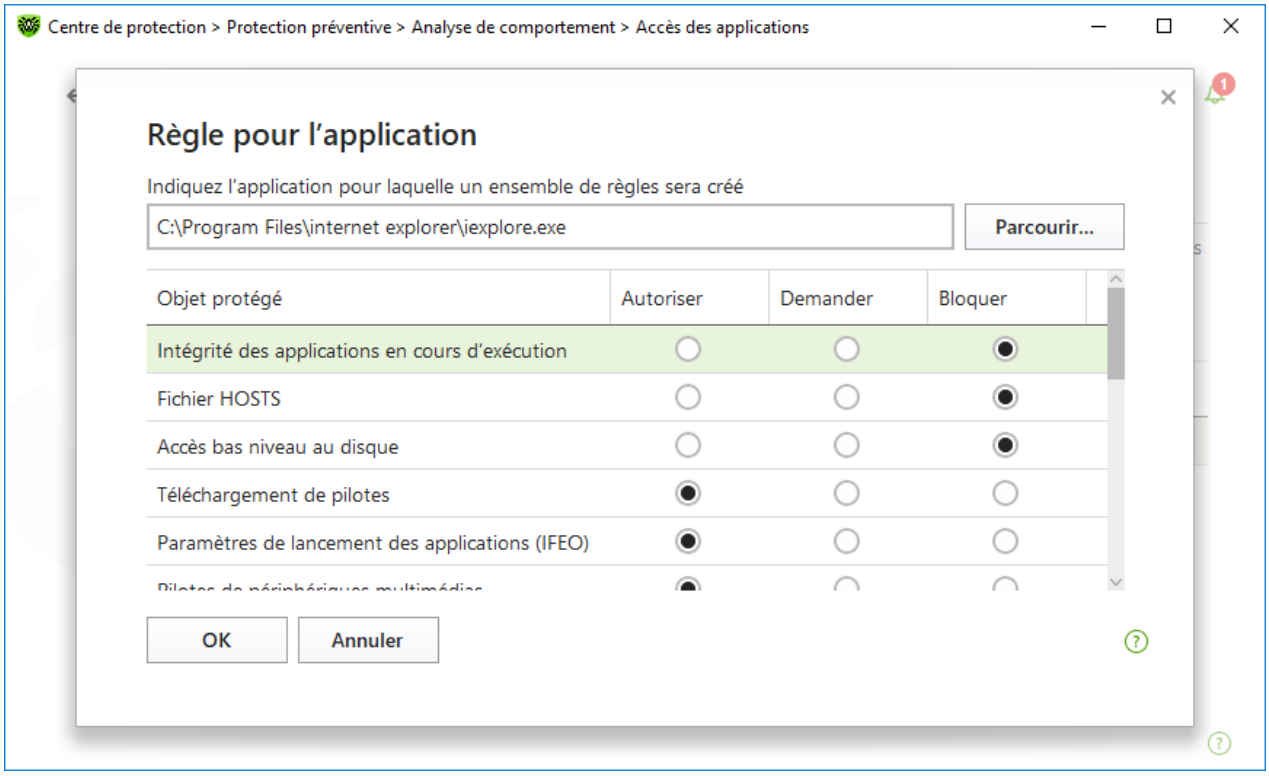

Figure 68. Ajout de l'ensemble de règles pour l'application

3. Consultez les paramètres de protection spécifiés par défaut. Modifiez-les, si cela est nécessaire.
4. Cliquez sur **OK**.

Objets protégés

Objet protégé	Description
Intégrité des applications en cours d'exécution	Cette option permet la détection des processus qui injectent leur code dans les applications en cours d'exécution ce qui représente une menace pour la sécurité de l'ordinateur.
Fichier HOSTS	Le système d'exploitation utilise le fichier HOSTS pour faciliter la connexion à Internet. La modification de ce fichier peut indiquer une infection virale.
Accès bas niveau au disque	Empêche les applications d'écrire sur les disques par secteurs évitant le système de fichiers.
Téléchargement de pilotes	Empêche les applications de charger des pilotes nouveaux ou inconnus.
Objets critiques Windows	D'autres options permettent la protection des branches de registre suivantes contre la modification (dans le profil système ainsi que dans les profils de tous les utilisateurs). Accès aux paramètres de lancement des applications (IFEO) :

Objet protégé	Description
	• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Pilotes des périphériques multimédia : • Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Paramètres de Winlogon : • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Notificateurs Winlogon : • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify Autodémarrage de Windows : • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Associations de fichiers exécutables : • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (clés) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (clés) Politiques de restriction du démarrage des programmes (SRP) : • Software\Policies\Microsoft\Windows\Safer Plugin Internet Explorer (objet application d'assistance du navigateur) : • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Autodémarrage de programmes : • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup • Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Autodémarrage de politiques : • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Configuration du mode sans échec : • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network

Objet protégé	Description
	Paramètres du Gestionnaire de sessions : • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows Services système : • System\CurrentControlXXX\Services

Si un problème survient durant l'installation d'une mise à jour importante de Microsoft ou durant l'installation et le fonctionnement de programmes (y compris des programmes de défragmentation), désactivez Analyse de comportement pour le moment.

11.3. Protection contre les exploits

Le composant Protection contre les exploits permet de bloquer les objets malveillants qui utilisent des vulnérabilités des applications connues. Les données du service cloud Dr.Web sont également utilisées pour déterminer la nocivité de l'objet.

Pour activer ou désactiver le composant Protection contre les exploits

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Protection préventive**.
3. Activez ou désactivez le composant Protection contre les exploits avec l'interrupteur .

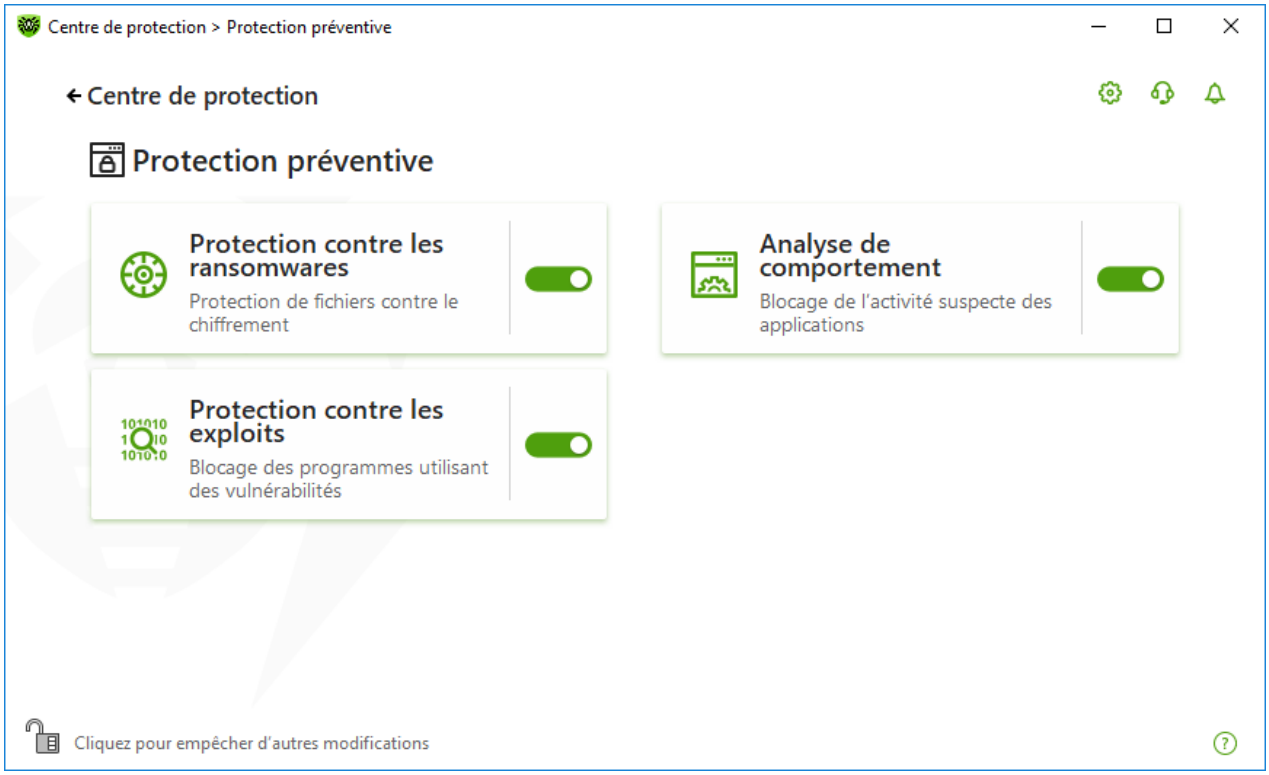

Figure 69. Activation/désactivation du composant Protection contre les exploits

Pour accéder aux paramètres des composants Protection contre les exploits

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
2. Cliquez sur la vignette **Protection contre les exploits**. La fenêtre de paramètres du composant va s'ouvrir.

Sélectionnez le niveau nécessaire de la protection contre les exploits dans la liste déroulante correspondante de la fenêtre de paramètres du composant.

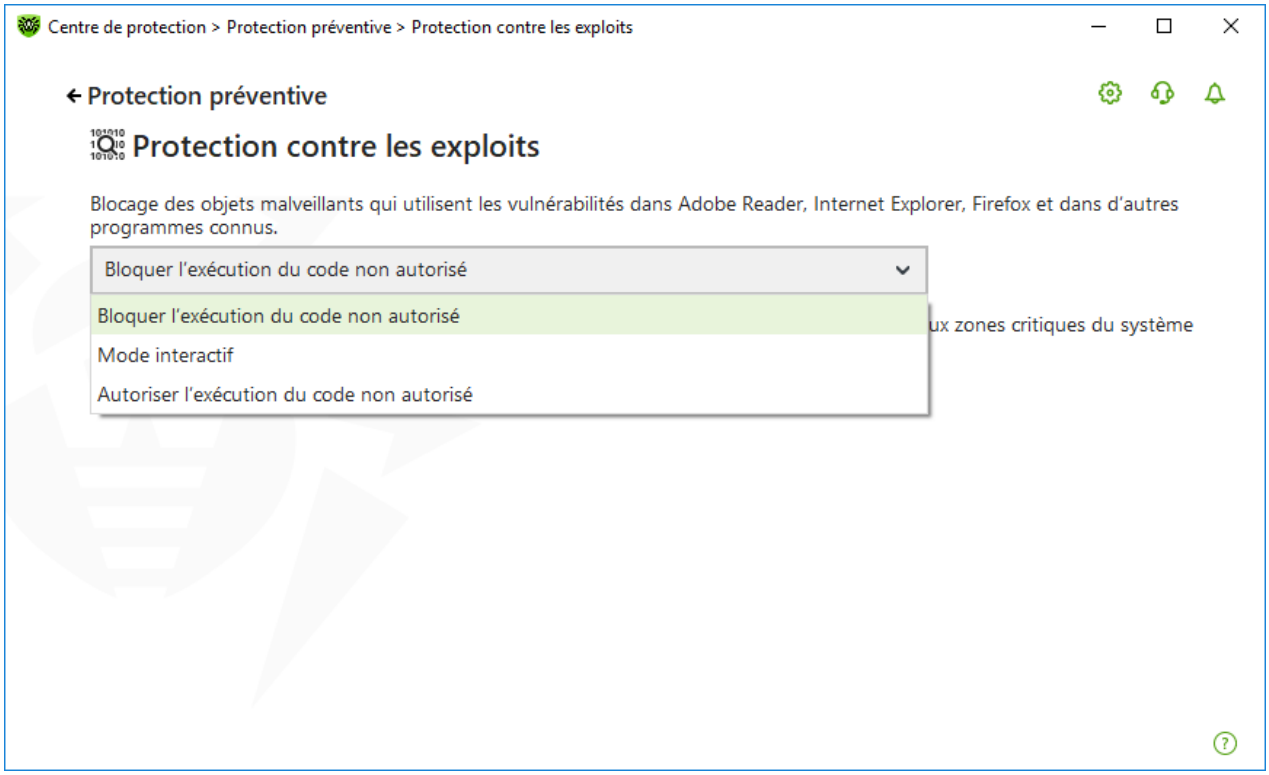

Figure 70. Sélection de niveau de protection

Niveaux de protection

Niveau de protection	Description
Bloquer l'exécution du code non autorisé	Une tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation sera bloquée automatiquement.
Mode interactif	En cas de tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation, Dr.Web affichera le message correspondant. Lisez les informations et sélectionnez l'action nécessaire.
Autoriser l'exécution du code non autorisé	Une tentative d'un objet malveillant d'utiliser les vulnérabilités du logiciel pour obtenir l'accès aux zones critiques du système d'exploitation sera autorisée automatiquement.

Réception de notifications

Vous pouvez configurer l'affichage des notifications des actions du composant Protection contre les exploits sur l'écran ou l'envoi des notifications par e-mail.

Voir aussi :

- Notifications

12. Outils

Dans cette fenêtre, l'accès aux outils avancés de gestion du produit Dr.Web est fourni.

Pour accéder au groupe de paramètres Outils

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Outils**.

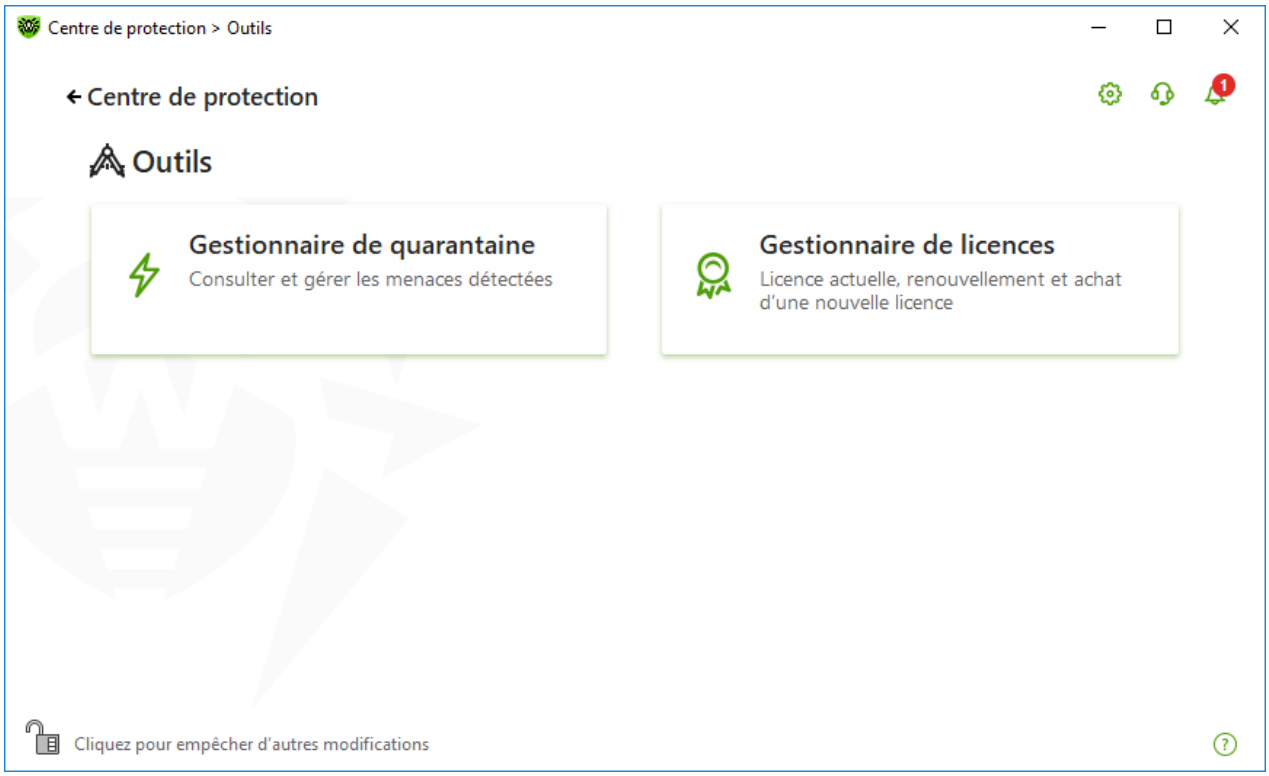

Figure 71. Fenêtre Outils

Pour passer à l'outil nécessaire, cliquez sur la vignette correspondante.

Dans cette section :

- Gestionnaire de quarantaine : liste des fichiers isolés et possibilité de leur restauration.
- Gestionnaire de licences : informations sur la licence et obtention d'une nouvelle licence.

12.1. Gestionnaire de quarantaine

Gestionnaire de quarantaine : outil qui permet de gérer les fichiers isolés. Dans la quarantaine se trouvent les fichiers contenant des objets malveillants. Les copies de sauvegarde des fichiers traités par Dr.Web sont également mises en quarantaine. Le Gestionnaire de quarantaine fournit la possibilité de supprimer, rescanner et restaurer les fichiers isolés.

Pour accéder à la fenêtre Gestionnaire de quarantaine

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Outils**.
3. Cliquez sur la vignette **Gestionnaire de quarantaine**.

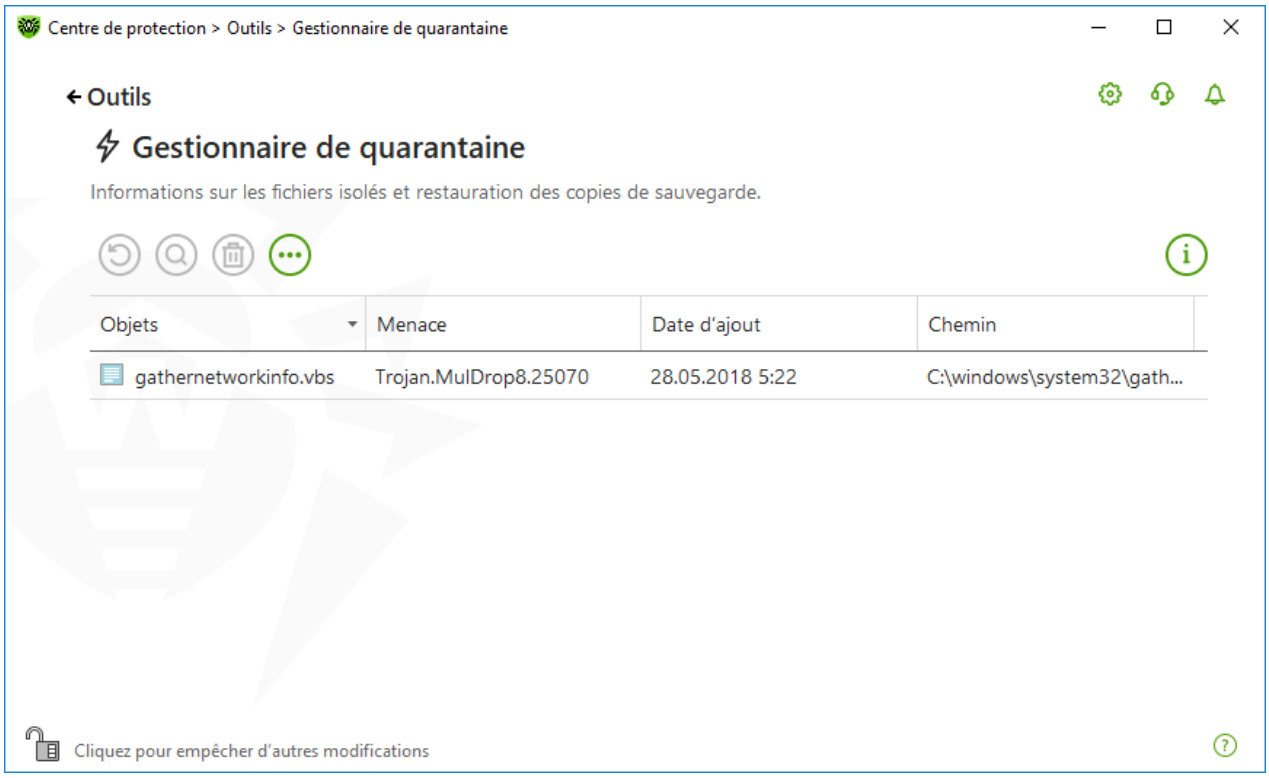

Figure 72. Objets en quarantaine

Le tableau central liste les informations suivantes sur les objets placés en quarantaine auxquels vous avez accès :

- **Objets** : nom de l'objet placé en quarantaine ;
- **Menace** : type du programme malveillant déterminé automatiquement par Dr.Web lorsque l'objet est placé en quarantaine ;
- **Date d'ajout** : date à laquelle l'objet a été déplacé en quarantaine ;
- **Chemin** : chemin complet du fichier avant qu'il ne soit placé en quarantaine.

> Dans la fenêtre du Gestionnaire de quarantaine les fichiers sont visibles uniquement pour les utilisateurs qui ont l'accès à ces fichiers. Pour afficher les objets caches, il faut posséder les droits d'administrateur.

Les copies de sauvegarde déplacées en quarantaine sont affichées dans le tableau par défaut. Pour les voir dans la liste des objets, cliquez sur et dans la liste déroulante, sélectionnez l'élément **Afficher les copies de sauvegarde**.

Gestion des objets en quarantaine

En mode administrateur, les boutons suivants sont disponibles pour chaque objet :

- Bouton (**Restaurer**) : déplacer un ou plusieurs objets sélectionnés dans le dossier nécessaire ;

  > Utilisez cette option uniquement si vous êtes sûr que les objets sélectionnés ne sont pas nocifs.

- Bouton (**Rescanner**) : scanner l'objet déplacé en quarantaine encore une fois.
- Bouton (**Supprimer**) : supprimer un ou plusieurs objets sélectionnés de la quarantaine et du système.

Ces actions sont également disponibles dans le menu contextuel qui s'ouvre si vous cliquez droit sur un ou plusieurs objets.

Pour supprimer tous les objets de la quarantaine en même temps, cliquez sur le bouton et sélectionnez **Tout supprimer** dans la liste déroulante.

Avancé

Pour configurer l'option de sauvegarde et l'option de suppression automatique des entrées en quarantaine, ouvrez les paramètres du Gestionnaire de quarantaine.

12.2. Gestionnaire de licences

Cet outil vous permet de consulter les informations sur toutes les licences de Dr.Web sauvegardées sur votre ordinateur ainsi que de modifier la licence actuelle, de la renouveler ou d'acheter une nouvelle licence et de l'activer.

Pour passer à la fenêtre Gestionnaire de licences depuis le Centre de sécurité

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Outils**.
3. Cliquez sur la vignette **Gestionnaire de licences**.

Pour acceder à la fenêtre Gestionnaire de licences depuis le Menu du programme

1. Ouvrez le menu de Dr.Web .
2. Sélectionnez l'élément **Gestionnaire de licences**.

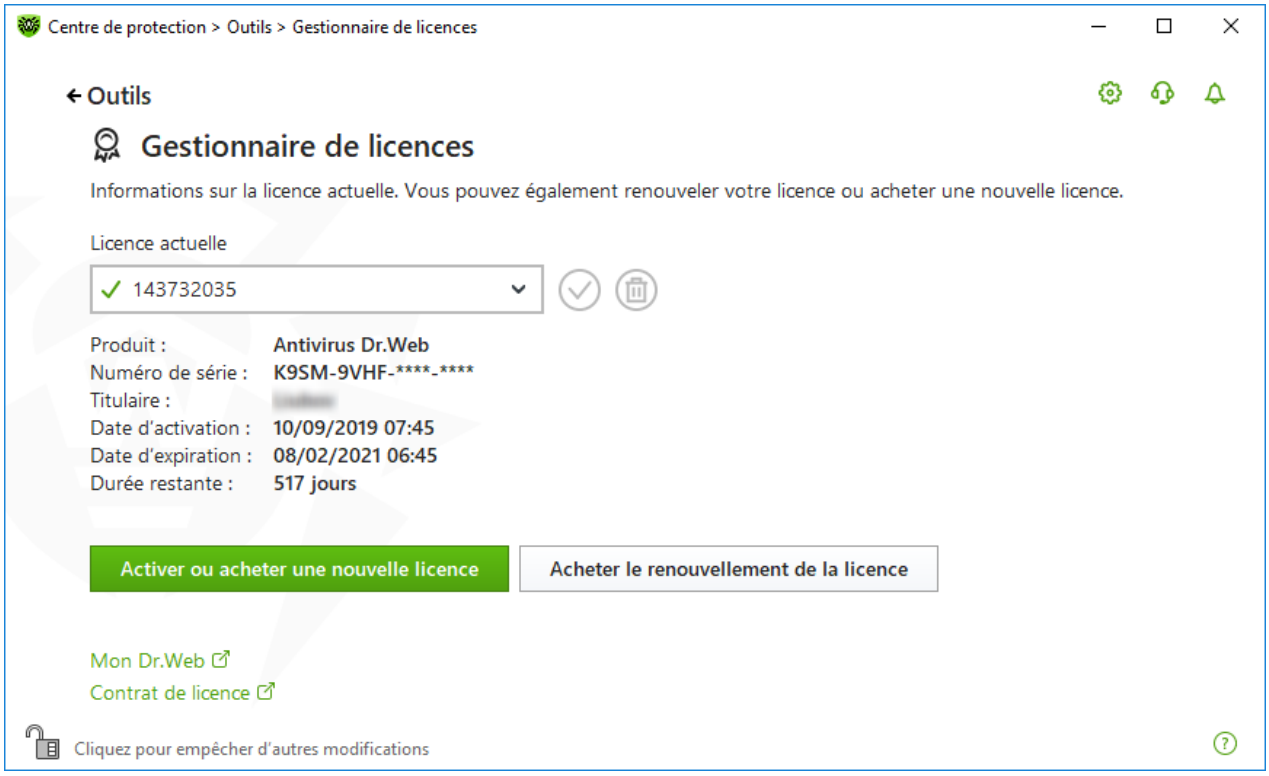

Figure 73. Informations sur la licence actuelle

Pour voir les informations sur la licence qui n'est pas actuelle, sélectionnez la licence nécessaire dans la liste déroulante.

Si la licence couvre plusieurs produits, la liste de produits est disponible dans la liste déroulante par le lien **Plus d'infos**.

> ⚠ Si plusieurs licences valides ont été activées en même temps, le délai de validité de chaque licence va s'écouler. Afin de l'éviter, lors de l'activation d'une nouvelle licence, indiquez les numéros de série de licences activées précédemment. Dans ce cas, les durées de validité sont additionnées.

Pour supprimer la licence

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas.
2. Sélectionnez dans la liste déroulante la licence à supprimer et cliquez sur le bouton. Notez qu'il est impossible de supprimer la dernière licence valide.

Pour assigner la licence actuelle

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas.

2. Sélectionnez dans la liste déroulante la licence que vous voulez designer comme actuelle et cliquez sur ✓.

Si vous cliquez sur **Activer ou acheter une nouvelle licence**, le programme ouvre la fenêtre dans laquelle vous pouvez acheter ou activer la nouvelle licence.

Si vous cliquez sur **Acheter le renouvellement de la licence**, le programme va ouvrir la page de renouvèlement de la licence sur le site de Doctor Web sur laquelle tous les paramètres de la licence utilisée seront affichés.

Avancé

Le lien Mon Dr.Web ouvre votre espace personnel sur le site officiel de l'entreprise Doctor Web. Cette page vous fournit les informations sur votre licence y compris sa durée et son numéro de série, et permet de renouveler la licence, contacter le support technique et plus encore.

Le lien Contrat de licence ouvre le texte du contrat de licence sur le site de Doctor Web.

13. Exclusions

Dans ce groupe de paramètres, vous pouvez configurer les exclusions des analyses effectuées par les composants SpIDer Guard, SpIDer Mail et Scanner.

Pour accéder au groupe de paramètres Exclusions

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Exclusions**.

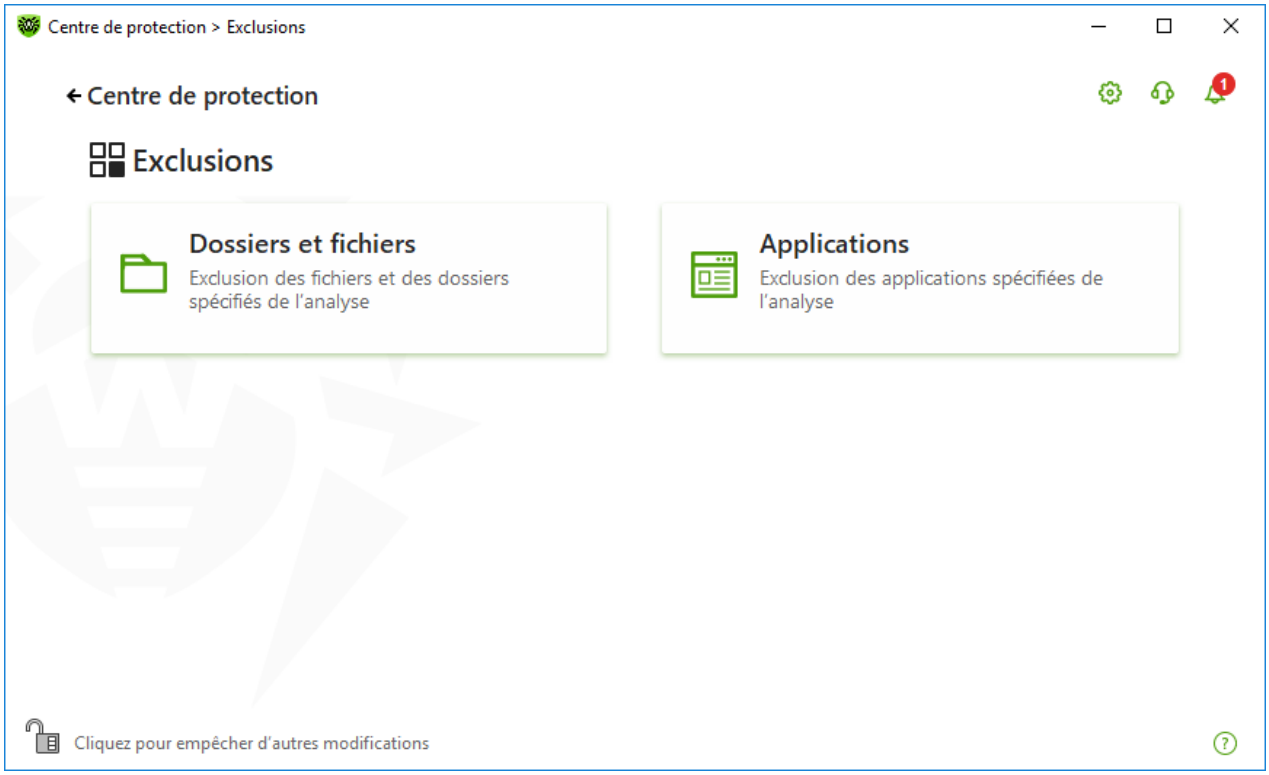

Figure 74. Fenêtre Exclusions

Pour accéder aux paramètres d'exclusions

1. Assurez-vous que Dr.Web fonctionne en mode administrateur (le cadenas en bas du logiciel est ouvert). Sinon, cliquez sur le cadenas .
2. Cliquez sur la vignette de la section correspondante.

Dans cette section :

- Fichiers et dossiers : exclusion de certains fichiers et dossiers de l'analyse effectuée par les composants SpIDer Guard et Scanner.
- Applications : exclusion de certains processus de l'analyse effectuée par les composants SpIDer Guard et SpIDer Mail.

13.1. Fichiers et dossiers

Vous pouvez spécifier la liste des fichiers et des dossiers qui sont exclus du scan de SpIDer Guard et du Scanner. Vous pouvez exclure les dossiers de quarantaine, les dossiers de travail de certains logiciels, les fichiers temporaires (fichiers swap), etc.

Pour configurer la liste des fichiers et dossiers à exclure

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Exclusions**.
3. Cliquez sur la vignette **Fichiers et dossiers**.

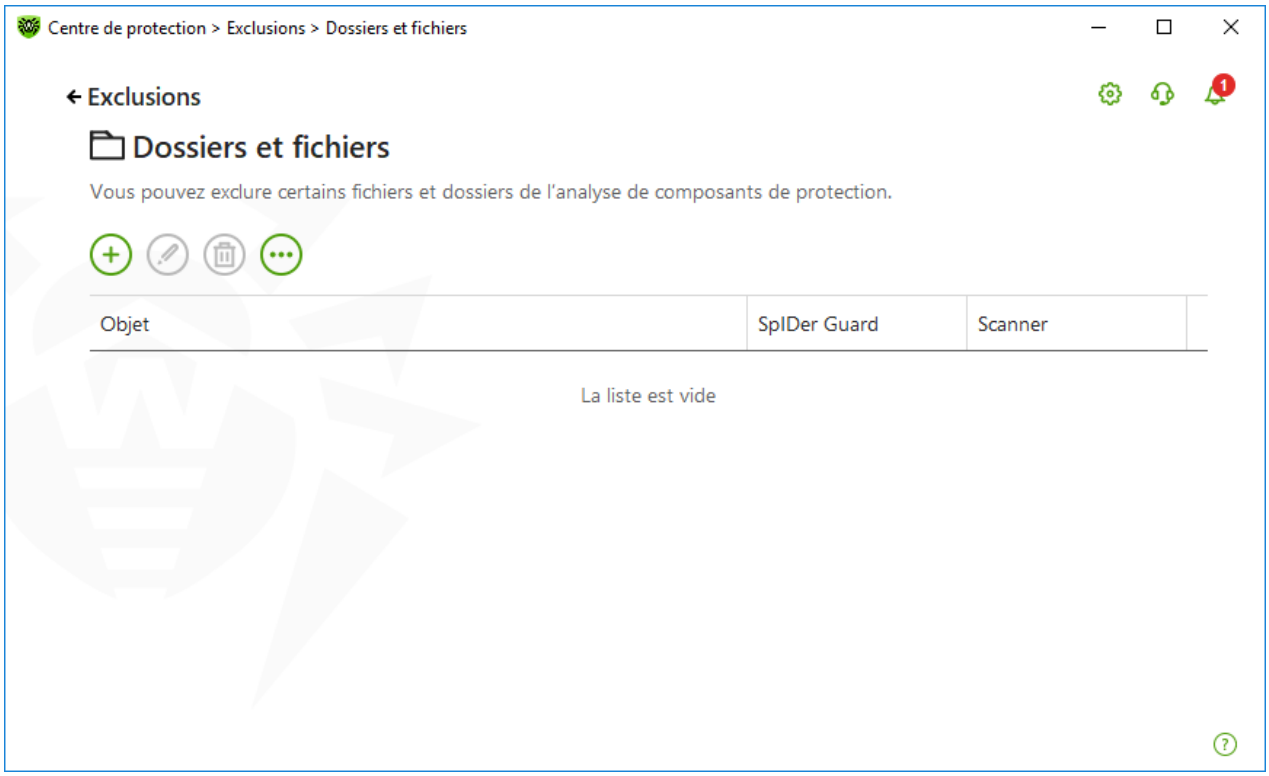

Figure 75. Liste des fichiers et dossiers à exclure

La liste est vide par défaut. Ajoutez des fichiers et dossiers aux exclusions ou utilisez des masques pour désactiver le scan de certains groupes de fichiers. Tout objet ajouté peut être exclu du scan des deux composants ou du scan de chaque composant séparément.

Pour ajouter les fichiers et les dossiers dans la liste d'exclusions

1. Faites une des actions suivantes pour ajouter un dossier ou un fichier à la liste :
   - pour ajouter un fichier ou dossier existant, cliquez sur ⊕. Dans la fenêtre qui s'ouvre, cliquez sur **Parcourir** et choisissez un fichier ou un dossier. Vous pouvez entrer manuellement le chemin complet vers le fichier ou le dossier, ou modifier le chemin dans le champ réservé à cet effet avant de l'ajouter à la liste . Par exemple :
     - `C:\folder\file.txt` : exclut de l'analyse le fichier `file.txt` se trouvant dans le dossier `C:\folder`.
     - `C:\folder` : exclut de l'analyse tous les sous-dossiers et les fichiers se trouvant dans le dossier `C:\folder`.
   - pour exclure de l'analyse un fichier avec un nom particulier, entrez dans le champ de saisie le nom du fichier y compris l'extension. Il n'est pas nécessaire de spécifier le chemin d'accès au fichier . Par exemple :
     - `file.txt` : exclut de l'analyse tous les fichiers avec le nom `file` et l'extension `.txt` dans tous les dossiers.
     - `file` : exclut de l'analyse tous les fichiers avec le nom `file` sans extension dans tous les dossiers.
   - pour exclure du scan des fichiers ou des dossiers du type particulier, entrez le masque qui les détermine dans le champ de saisie.

   Un masque désigne les éléments communs aux noms des objets, ainsi :
     - le caractère « `*` » remplace toute séquence (potentiellement vide) de caractères ;
     - le caractère « `?` » remplace n'importe quel caractère (un seul caractère) ;

   Exemples :
     - `rapport*.doc` : un masque qui désigne tous les documents Microsoft Word dont les noms commencent par le mot « rapport », par exemple, les fichiers `rapport-fevrier.doc`, `rapport121209.doc` etc. ;
     - `*.exe` : un masque qui désigne tous les fichiers exécutable ayant l'extension EXE, par exemple, `setup.exe`, `iTunes.exe` etc. ;
     - `photo????09.jpg` : un masque qui désigne tous les fichiers des images au format JPG dont le nom commence par « photo » et se termine par « 09 », dans ce cas entre ces deux fragments, dans le nom de fichier, il y a quatre n'importe quels symboles, par exemple `photo121209.jpg`, `photopapa09.jpg` ou `photo----09.jpg`.
     - `file*` : exclut de l'analyse tous les fichiers, dont les noms commencent pas `file`, avec n'importe quelle extension dans tous les dossiers.
     - `file.*` : exclut de l'analyse tous les fichiers avec le nom `file` et n'importe quelle extension dans tous les dossiers.
     - `C:\folder\**` : exclut de l'analyse tous les sous-dossiers et les fichiers se trouvant dans le dossier `C:\folder`. Cependant les fichiers dans les sous-dossiers seront scannés.

- `C:\folder\*` : exclut de l'analyse tous les fichiers se trouvant dans le dossier `C:\folder` ainsi que dans tous les sous-dossiers à tout niveau d'emboîtement.
- `C:\folder\*.txt` : exclut de l'analyse les fichiers de type `*.txt` se trouvant dans le dossier `C:\folder`. Les fichiers `*.txt` se trouvant dans les sous-dossiers seront scannés.
- `C:\folder\*\*.txt` : exclut de l'analyse les fichiers de type `*.txt` uniquement dans les sous-dossier du premier niveau d'emboîtement dans le dossier `C:\folder`.
- `C:\folder\**\*.txt` : exclut de l'analyse les fichiers de type `*.txt` dans les sous-dossiers de tout niveau d'emboîtement dans le dossier `C:\folder`. Les fichiers `*.txt` se trouvant dans le dossier `C:\folder` seront scannés.

2. Dans la fenêtre d'ajout d'un fichier ou d'un dossier, indiquez les composants qui ne doivent pas scanner l'objet sélectionné.
3. Cliquez sur **OK**. Le fichier ou dossier apparaît dans la liste.
4. Si nécessaire, répétez les étapes 1–3 pour ajouter d'autres fichiers et dossiers.

Gestion des objets dans la liste

Pour gérer les objets dans le tableau, les éléments de gestion suivants sont fournis :

- Bouton ⊕ : ajout d'un objet dans la liste des exclusions.
- Bouton ✎ : édition de l'objet sélectionné dans la liste des exclusions.
- Bouton 🗑 : suppression de l'objet sélectionné de la liste des exclusions.

  Ces actions sont également disponibles dans le menu contextuel qui s'ouvre si vous cliquez droit sur un ou plusieurs objets.
- Si vous cliquez sur ⋯, les actions suivantes seront disponibles :
  - **Exporter** : cette option permet de sauvegarder la liste créée des exclusions pour l'utiliser sur un autre ordinateur sur lequel Dr.Web est installé.
  - **Importer** : cette option permet d'utiliser la liste des exclusions créée sur un autre ordinateur.
  - **Désélectionner tout** : cette option permet de supprimer tous les objets de la liste des exclusions.

13.2. Applications

Vous pouvez spécifier la liste des programmes et des processus à exclure de l'analyse du moniteur de fichiers SpIDer Guard et de l'antivirus de messagerie SpIDer Mail. Les objets modifiés en conséquence de fonctionnement de ces applications seront exclus de l'analyse.

Pour configurer la liste des applications à exclure

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'affiche, cliquez sur la vignette **Exclusions**.

3. Cliquez sur la vignette **Applications**.

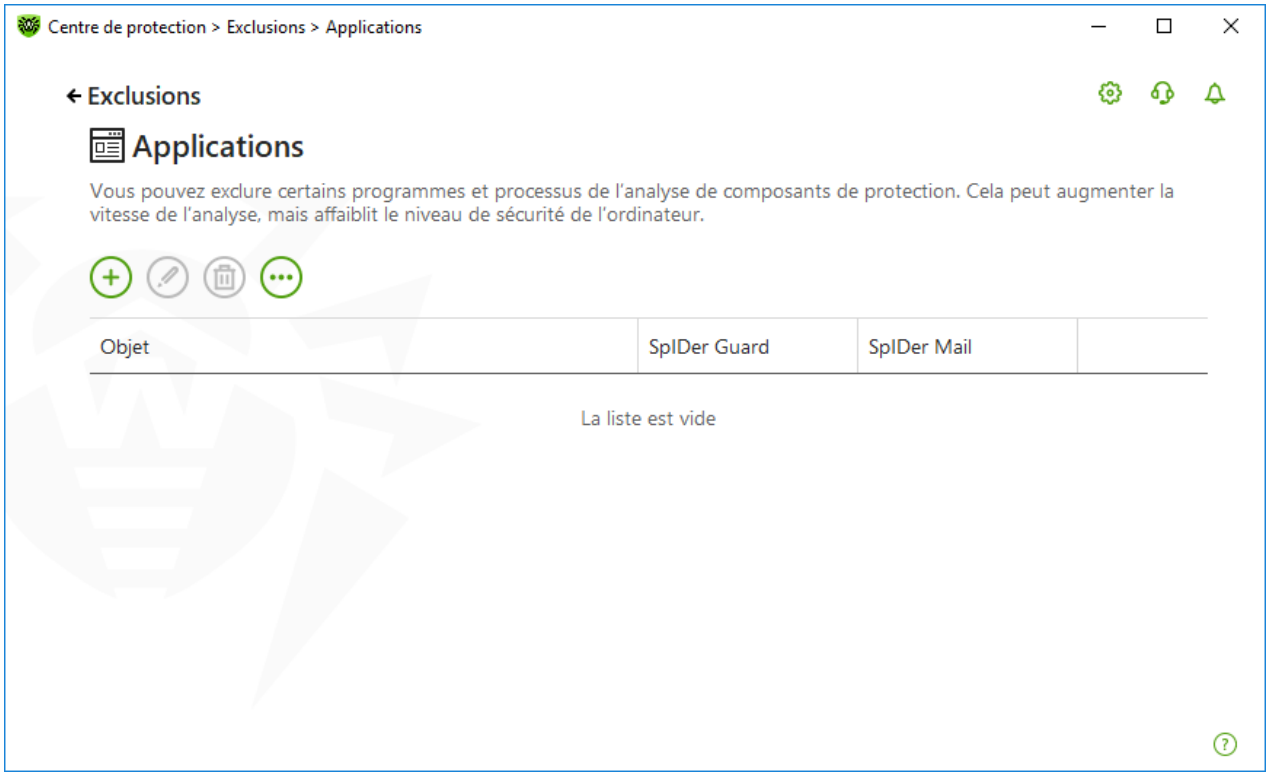

Figure 76. Liste des applications à exclure

Par défaut, la liste est vide.

Pour ajouter une application aux exclusions

1. Pour ajouter un programme ou un processus à la liste des exclusions, cliquez sur ⊕. Exécutez une des actions suivantes :
   - dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir** pour sélectionner l'application. Vous pouvez entrer manuellement le chemin complet vers l'application dans le champ de saisie. Par exemple :

     `C:\Program Files\folder\example.exe`
   - pour exclure une application de l'analyse, entrez son nom dans le champ de saisie. Dans ce cas, il n'est pas nécessaire de spécifier le chemin complet vers l'application. Par exemple :

     `example.exe`
   - pour exclure de l'analyse des applications du type particulier, entrez le masque qui les détermine dans le champ de saisie.

     Un masque désigne les éléments communs aux noms des objets, ainsi :
     - le caractère « * » remplace toute séquence (potentiellement vide) de caractères ;
     - le caractère « ? » remplace n'importe quel caractère (un seul caractère) ;

Exemples de configuration des exclusions :

- `C:\Program Files\folder\*.exe` : exclut de l'analyse les applications dans le dossier `C:\Program Files\folder`. Les applications dans les sous-dossiers seront analysées.
- `C:\Program Files\*\*.exe` : exclut de l'analyse uniquement les applications dans les sous-dossiers du premier niveau d'emboîtement du dossier `C:\Program Files`.
- `C:\Program Files\**\*.exe` : exclut de l'analyse les applications dans les sous-dossiers de tout niveau d'emboîtement du dossier `C:\Program Files`. Dans le dossier `C:\Program Files`, les applications seront analysées.
- `C:\Program Files\folder\exam*.exe` : exclut de l'analyse toutes les applications du dossier `C:\Program Files\folder` dont les noms commencent par exam. Dans les sous-dossiers, ces applications seront analysées.
- `example.exe` : exclut de l'analyse toutes les applications avec le nom `example` et l'extension `.exe` dans tous les dossiers.
- `example*` : exclut de l'analyse dans tous les dossiers les applications de tout type dont les noms commencent par `example`.
- `example.*` : exclut de l'analyse toutes les applications avec le nom `example` et n'importe quelle extension dans tous les dossiers.

- vous pouvez exclure une application de l'analyse par le nom de variable, si dans les paramètres des variables système, le nom et la valeur de cette variable sont spécifiés. Par exemple :

`%EXAMPLE_PATH%\example.exe` : exclut de l'analyse l'application selon le nom de la variable système. Vous pouvez spécifier le nom et la valeur de la variable système dans les paramètres du système d'exploitation.

Sous Windows 7 et supérieur : **Panneau de configuration** → **Système** → **Paramètres système avancés** → **Avancé** → **Variables d'environnement** → **Variables système**.

Nom de la variable dans l'exemple : `EXAMPLE_PATH`.

Valeur de la variable dans l'exemple : `C:\Program Files\folder`.

2. Dans la fenêtre de configuration, indiquez les composants qui ne doivent pas analyser l'application sélectionnée.

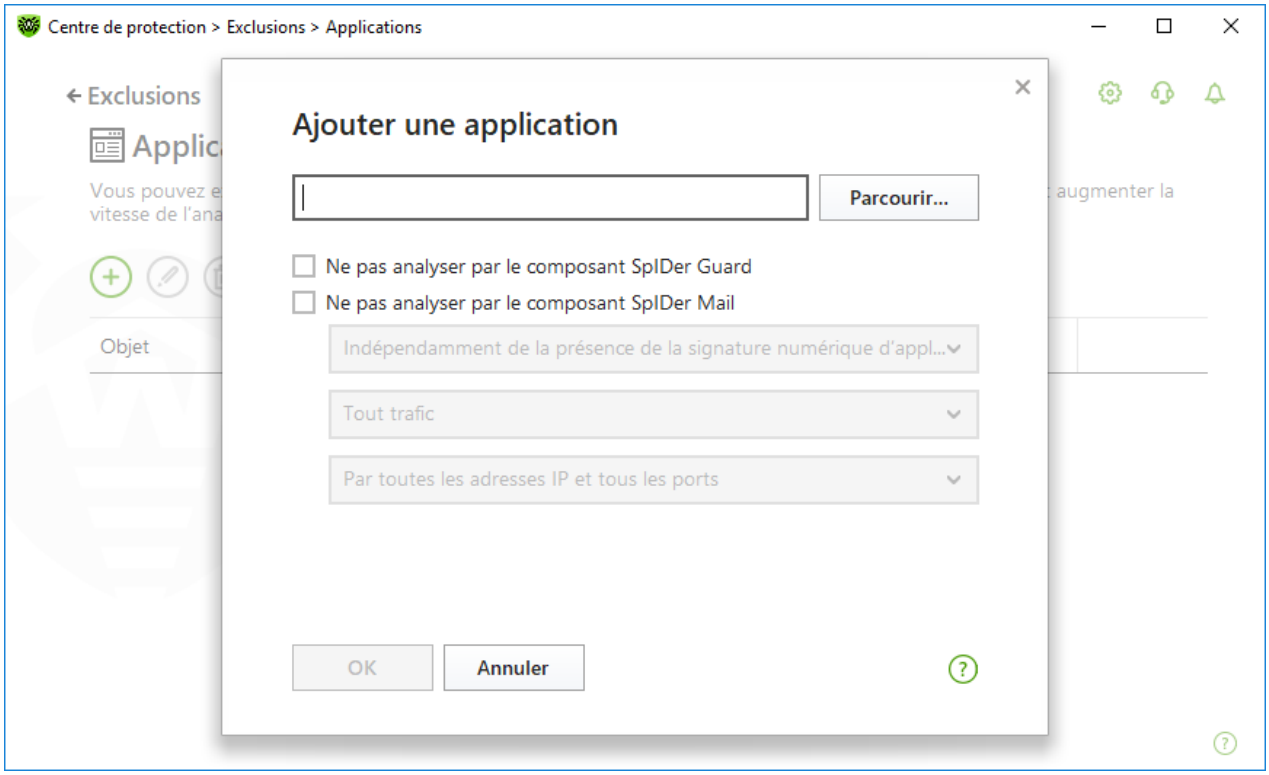

Figure 77. Ajout des applications aux exclusions

3. Pour les objets exclus de l'analyse par le composant SpIDer Mail, indiquez les conditions supplémentaires.

Paramètre	Description
Indépendamment de la présence de la signature numérique d'application	Sélectionnez ce paramètre si l'application doit être exclue du scan indépendamment de la présence de la signature numérique.
En cas de présence de la signature numérique d'application	Sélectionnez ce paramètre si l'application doit être exclue du scan uniquement en cas de présence de la signature numérique d'application. Sinon l'application sera scannée par les composants.
Tout trafic	Sélectionnez ce paramètre pour exclure du scan le trafic chiffré et non chiffré de l'application.
Trafic chiffré	Sélectionnez ce paramètre pour exclure du scan seulement le trafic chiffré de l'application.
Via toutes les adresses IP et tous les ports	Sélectionnez ce paramètre pour exclure du scan le trafic acheminé vers toutes les adresses IP et tous les ports.

Paramètre	Description
Via les adresses IP et les ports indiqués	Sélectionnez ce paramètre pour indiquer les adresses IP et les ports dont le trafic sera exclu du scan. Le trafic acheminé des autres adresses IP et des ports sera scanné (s'il n'est pas exclu par un autre paramètre).
Spécifier les adresses et les ports	Pour configurer les exclusions de manière précise, utilisez les recommandations suivantes : • pour exclure de l'analyse un domaine particulier par un port particulier, indiquez, par exemple, `site.com:80` ; • pour exclure de l'analyse le trafic par un port non standard (par exemple, 1111) il faut indiquer : `*:1111` ; • pour exclure de l'analyse le trafic du domaine par n'importe quel port, indiquez : `site:*`

4. Cliquez sur **OK**. L'application sélectionnée va apparaître dans la liste.
5. Si nécessaire, reproduisez la marche à suivre pour y ajouter d'autres programmes.

Gestion des objets dans la liste

Pour gérer les objets dans le tableau, les éléments de gestion suivants sont fournis :

- Bouton  : ajout d'un objet dans la liste des exclusions.
- Bouton  : édition de l'objet sélectionné dans la liste des exclusions.
- Bouton  : suppression de l'objet sélectionné de la liste des exclusions.

  Ces actions sont également disponibles dans le menu contextuel qui s'ouvre si vous cliquez droit sur un ou plusieurs objets.
- Si vous cliquez sur  , les actions suivantes seront disponibles :
  - **Exporter** : cette option permet de sauvegarder la liste créée des exclusions pour l'utiliser sur un autre ordinateur sur lequel Dr.Web est installé.
  - **Importer** : cette option permet d'utiliser la liste des exclusions créée sur un autre ordinateur.
  - **Désélectionner tout** : cette option permet de supprimer tous les objets de la liste des exclusions.

14. Statistiques de fonctionnement des composants

Vous avez la possibilité de voir les statistiques de fonctionnement des principaux composants de Dr.Web.

Pour aller aux statistiques sur les événements importants des composants de protection

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Centre de protection**.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Statistiques**.
3. La fenêtre des statistiques s'ouvre. Les rapports pour les groupes suivants sont disponibles :
   - Rapport détaillé
   - Menaces
   - Pare-feu

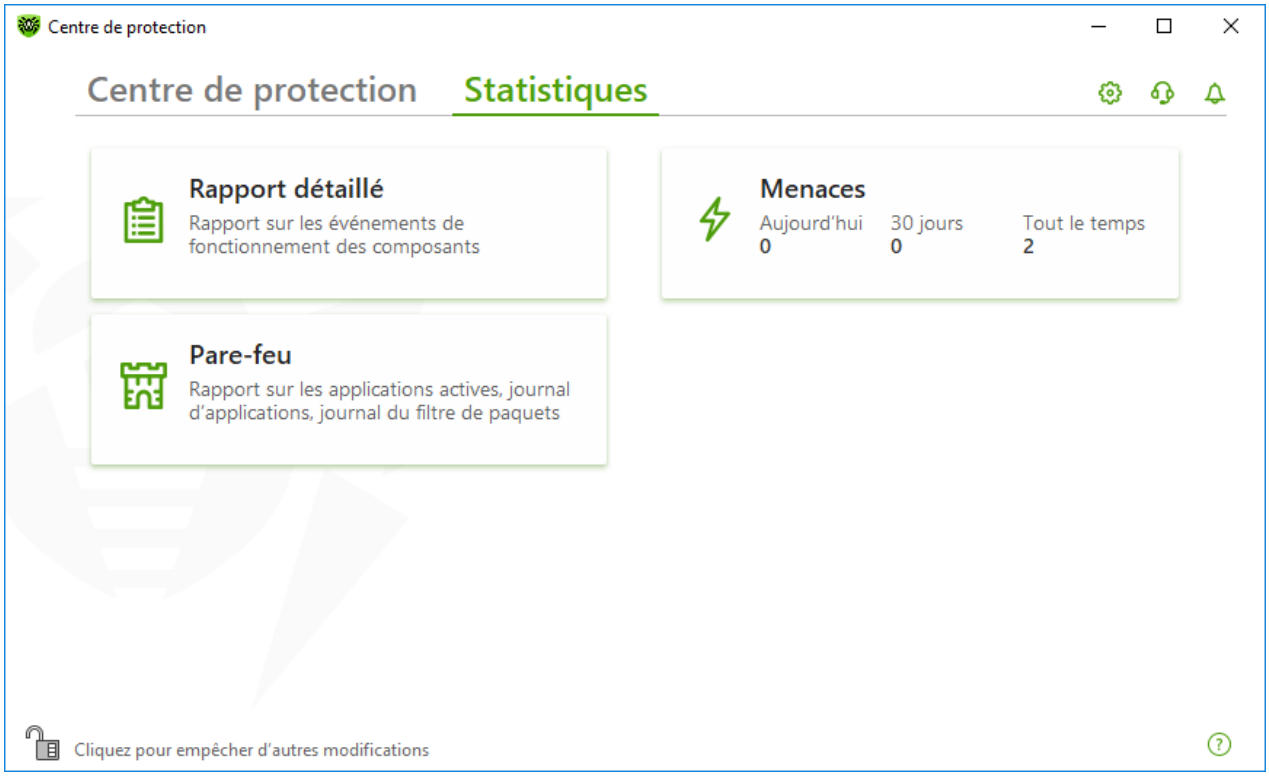

Figure 78. Statistiques de fonctionnement des composants

4. Sélectionnez un groupe pour voir les rapports.

Rapport détaillé

Dans cette fenêtre se trouvent les informations détaillées sur tous les événements survenus pendant toute la période de fonctionnement.

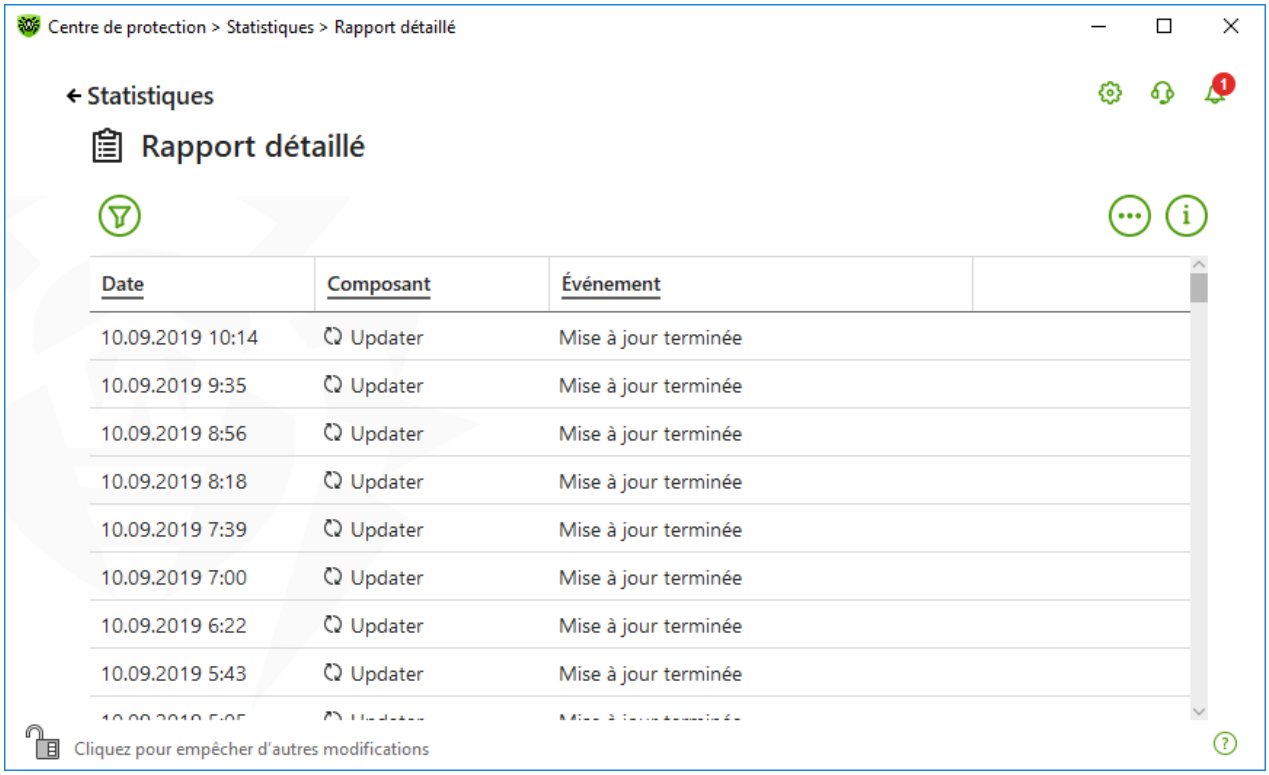

Figure 79. Fenêtre du rapport détaillé

Les informations suivantes sont enregistrées dans le rapport :

- **Date** date et heure de l'événement ;
- **Composant** : composant ou module auquel se rapporte l'événement ;
- **Événement** : brève description de l'événement.

Tous les événements survenus pendant le fonctionnement sont affichés par défaut.

Pour gérer les objets dans le tableau, les éléments de gestion , , sont utilisés.

Vous pouvez utiliser les filtres supplémentaires pour sélectionner les événements.

Menaces

La vignette **Menaces** dans la fenêtre principale d'affichage de statistiques contient toutes les informations sur le nombre de menaces pour un délai précis.

Si vous sélectionnez cette option, la fenêtre **Rapport détaillé** s'ouvrira avec tous les filtres préinstallés pour toutes les menaces.

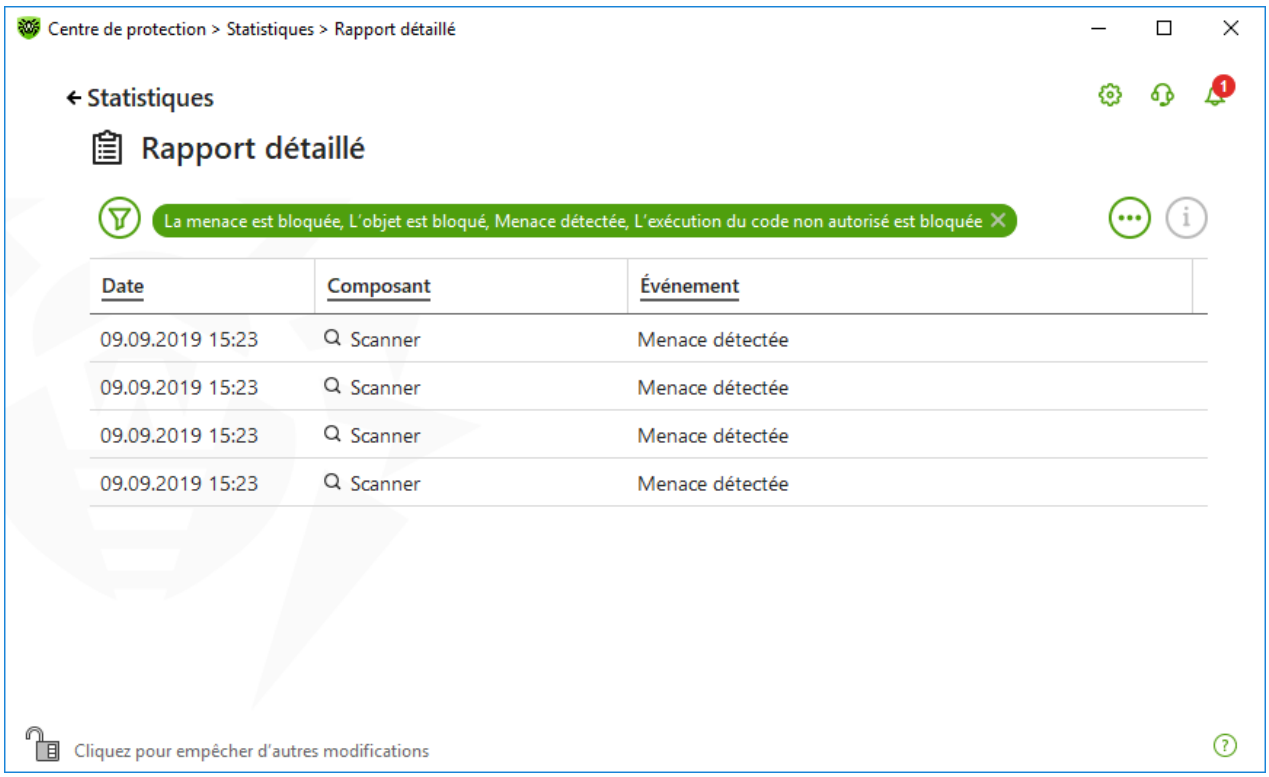

Figure 80. Fenêtre de statistiques par menaces

Les informations suivantes sont enregistrées dans le rapport :

- **Date** : date et heure de détection de la menace ;
- **Composant** : composant ayant détecté la menace ;
- **Événement** : brève description de l'événement.

Tous les événements survenus pendant le fonctionnement sont affichés par défaut.

Pour gérer les objets dans le tableau, les éléments de gestion sont utilisés.

Vous pouvez utiliser les filtres supplémentaires pour sélectionner les événements.

Activité réseau

Si Pare-feu Dr.Web est installé, le rapport de l'activité réseau est disponible.

Vous pouvez voir les informations sur les applications en cours, le journal des applications et le journal du filtre de paquets. Pour ce faire, sélectionnez l'objet nécessaire dans la liste déroulante.

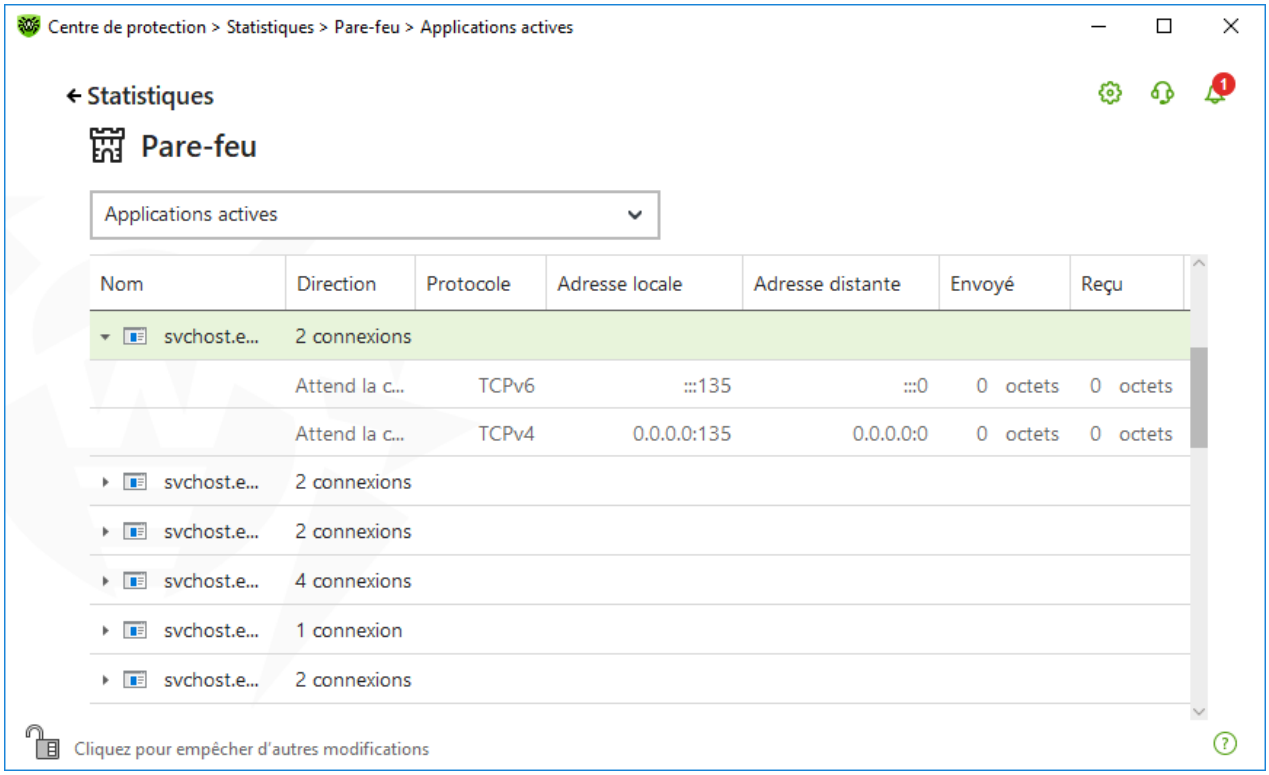

Figure 81. Fenêtre de statistiques de l'activité réseau

Les informations suivantes sont affichées pour chaque connexion :

- direction de transmission de données ;
- protocole de fonctionnement ;
- adresse locale ;
- adresse distante ;
- taille du paquet de données envoyé ;
- taille du paquet de données reçu.

Vous pouvez bloquer l'une des connexions courantes ou autoriser une connexion bloquée auparavant. Pour ce faire, sélectionnez la connexion nécessaire et cliquez droit dessus. Une seule option correspondante au statut de la connexion est disponible.

Dans le journal d'applications, les informations suivantes sont affichées :

- heure de début du fonctionnement de l'application ;
- nom de l'application ;
- nom de la règle du traitement de l'application ;
- direction de transmission de données ;
- action ;
- adresse cible.

Vous pouvez activer la journalisation des applications dans la fenêtre d'ajout ou d'édition de la règle de l'application, dans la section **Pare-feu**. Pour en savoir plus, consultez la rubrique Configuration des paramètres de règles pour les applications.

Dans le journal du filtre de paquets, les informations suivantes sont affichées :

- heure de début du traitement du paquet de données ;
- direction de la transmission du paquet de données ;
- nom de la règle de traitement ;
- interface ;
- contenu du paquet.

Vous pouvez activer la journalisation du filtre de paquets dans la fenêtre d'ajout ou d'édition de la règle de paquet, dans la section **Pare-feu**. Pour en savoir plus, consultez la rubrique Ensemble de règles de filtrage de paquets.

Si vous cliquez sur une colonne, les événements sont triés par ordre croissant ou décroissant.

Filtres

Pour voir dans la liste uniquement les événements qui correspondent aux paramètres déterminés, utilisez les filtres. Pour tous les rapports il existe des filtres préinstallés qui s'affichent lorsque vous cliquez sur . Vous pouvez également créer vos propres filtres d'événements.

Boutons de gestion des éléments dans le tableau :

- Si vous cliquez sur , les actions suivantes seront disponibles :
  - Sélection du filtre préinstallé par période précise ou du filtre par événement de mise à jour.
  - Sauvegarde du filtre utilisateur actuel. Il est possible de supprimer le filtre utilisateur déjà créé.
  - Suppression de tous les filtres installés pour le moment.
- Si vous cliquez sur , les actions suivantes seront disponibles :
  - **Copier les éléments sélectionnés** : permet de copier la ligne (les lignes) sélectionnée dans le presse-papier.
  - **Exporter les objets sélectionnés** : permet d'exporter la ligne (les lignes) sélectionnée au format .csv dans le dossier spécifié.
  - **Exporter les objets sélectionnés** : permet d'exporter toutes les lignes du tableau au format .csv dans le dossier spécifié.
  - **Supprimer les éléments sélectionnés** : permet de supprimer l'événement (les événements) sélectionné.
  - **Tout supprimer** : permet de supprimer tous les événements du tableau de statistiques.

- Quand vous cliquez sur le bouton ⓘ, les informations détaillées sur l'événement s'affichent. Le bouton devient disponible si vous sélectionnez une ligne quelconque. Un nouveau clic sur le bouton masque les données détaillées sur l'événement.

Pour utiliser le filtre utilisateur

1. Pour trier par un paramètre, cliquez sur l'en-tête de la colonne nécessaire :
   - Tri par date. Vous pouvez choisir une période prédéfinie dans la partie gauche de la fenêtre ou spécifier votre propre période. Pour spécifier la période nécessaire, sélectionnez dans le calendrier la date du début et de la fin de période ou bien, indiquez les dates dans la ligne **Période**. Le tri par date se fait dans l'ordre croissant ou décroissant.

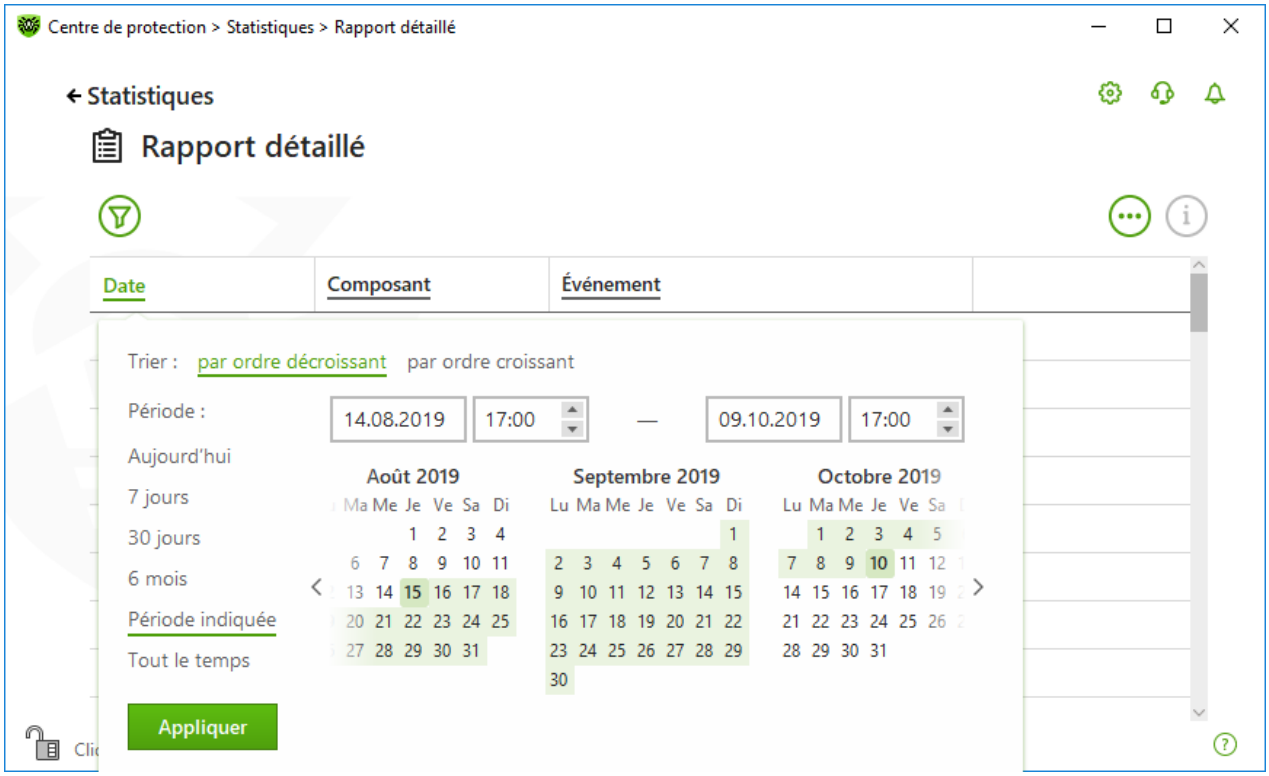

Figure 82. Tri pour date

   - Tri par composant. Vous pouvez marquer les composants dont les informations seront affichées dans le rapport ou trier les entrées dans l'ordre croissant ou décroissant.
   - Tri par événement. Vous pouvez marquer les événements à afficher dans le rapport ou trier les entrées dans l'ordre croissant ou décroissant.
2. Après avoir choisi les paramètres de filtrage, cliquez sur **Appliquer**. Les éléments sélectionnés seront affichés au dessus du tableau.
3. Pour sauvegarder le filtre, cliquez sur ⧩ et sélectionnez **Enregistrer le filtre**.
4. Dans la fenêtre qui s'affiche, indiquez le nom du nouveau filtre. Cliquez sur **Enregistrer**.

15. 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 :

- consultez les dernières versions des descriptions et des manuels à l'adresse https://download.drweb.com/doc/ ;
- lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/ ;
- 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 :

- remplissez le formulaire de question dans la section correspondante de la rubrique https://support.drweb.com/ ;
- appelez au numéro : 0 825 300 230.

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/.

15.1. Aide à la résolution de problèmes

La Quand vous contactez le support technique de Doctor Web, vous pouvez avoir besoin d'un rapport sur votre système d'exploitation et le fonctionnement de Dr.Web.

Pour créer un rapport avec l'Assistant de rapports

1. Ouvrez le menu de Dr.Web et sélectionnez l'élément **Support**.
2. Dans la fenêtre qui s'affiche, cliquez sur le bouton **Aller à l'Assistant de rapports**.

Vous pouvez également ouvrir cette fenêtre en cliquant sur en haut de la fenêtre **Centre de protection**.

Figure 83. Support

3. Dans la fenêtre qui s'affiche, cliquez sur le bouton **Créer un rapport**.

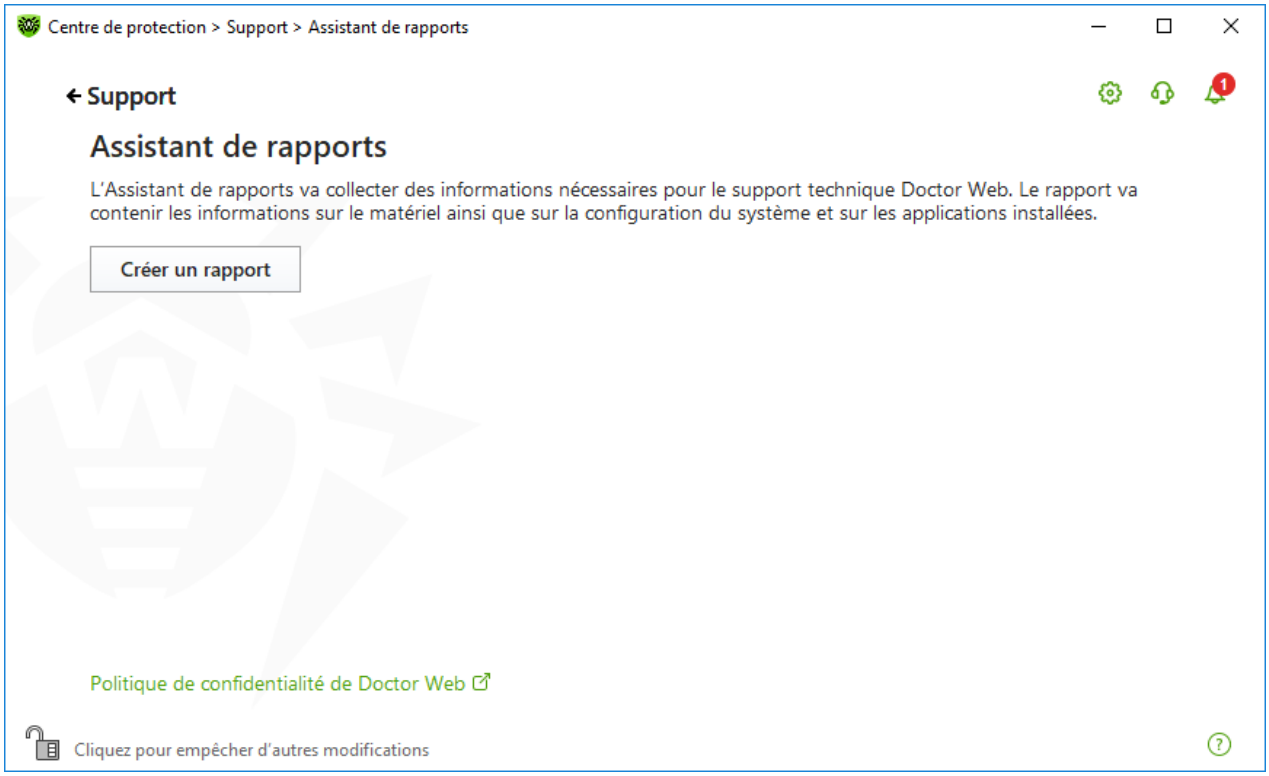

Figure 84. Création d'un rapport pour le support technique

4. La création du rapport va commencer.

Création d'un rapport avec la ligne de commande

Pour générer le rapport, utilisez la commande suivante :

`/auto`, par exemple : `dwsysinfo.exe /auto`

Vous pouvez également utiliser la commande :

`/auto /report:`[<*chemin_complet_vers_le_fichier_de_rapport*>], par exemple : `dwsysinfo.exe /auto /report:C:\report.zip`

Le rapport sera enregistré sous forme d'une archive dans le dossier Doctor Web se trouvant dans le dossier du profil utilisateur %USERPROFILE%. Vous pouvez accéder à l'archive en cliquant sur le bouton **Ouvrir le dossier** après la création de l'archive.

Informations incluses dans le rapport

Le rapport contient les informations suivantes :

1. Informations techniques sur le système d'exploitation :
   - généralités sur l'ordinateur,
   - informations sur les processus en cours d'exécution,
   - informations sur les tâches programmées,
   - informations sur les services et pilotes,
   - informations sur le navigateur par défaut,
   - informations sur les applications installées,
   - informations sur la politique de restrictions,
   - informations sur le fichier HOSTS,
   - informations sur les serveurs DNS,
   - journal des événements système ;
   - liste des répertoires système ;
   - branches de la base de registre ;
   - fournisseurs Winsock ;
   - connexions réseau ;
   - rapports du débogueur Dr.Watson ;
   - indice de performances.
2. Informations sur le produit installé Dr.Web :
   - type et version du produit installé Dr.Web ;
   - informations sur l'ensemble de composants installés ; informations sur les modules Dr.Web ;

- configuration et paramètres de configuration du produit Dr.Web ;
- informations sur la licence ;
- journaux de fonctionnement Dr.Web.

Les informations sur le fonctionnement de Dr.Web se trouvent dans le Journal des événements du système d'exploitation Windows, dans la section **Journaux des applications et services** → **Doctor Web**.

15.2. A propos du logiciel

La section **A propos du logiciel** contient les informations sur :

- la version du produit ;
- la date et l'heure de la dernière mise à jour.

Dans la fenêtre **A propos de Dr.Web**, vous pouvez trouver les informations sur la version des composants installés et la date de mise à jour des bases virales.

Pour accéder à cette fenêtre

1. Ouvrez le menu principal et sélectionnez l'élément **Support**.
2. Dans la fenêtre qui s'affiche, cliquez sur le bouton **Détails**.

Vous pouvez également ouvrir cette fenêtre en cliquant sur en haut de la fenêtre **Centre de protection**.

Figure 85. Accès à la fenêtre A propos de Dr.Web

16. Annexe A. Paramètres de ligne de commande

Les paramètres de ligne de commande sont utilisés pour définir les paramètres des programmes qui se lance par l'ouverture d'un fichier exécutable. Cela concerne le Scanner Dr.Web, le Scanner en ligne de commande et le Module de mise à jour automatique. Les clés peuvent spécifier des paramètres manquants dans le fichier de configuration ou des paramètres qui sont présents, mais qui possèdent une priorité supérieure.

Les clés commencent par le signe « / » et sont séparées par des espaces comme les autres paramètres en ligne de commande.

16.1. Paramètres du Scanner et du Scanner en ligne de commande

Clé	Description
/AA	Appliquer automatiquement les actions aux menaces détectées (uniquement pour le Scanner).
/AC	Scanner les packages d'installation. L'option est activée par défaut.
/AFS	Utiliser un slash droit pour spécifier l'imbrication dans l'archive. L'option est désactivée par défaut.
/AR	Scanner les archives. L'option est activée par défaut.
/ARC:<*taux_de_compression*>	Taux maximum de compression. Si le scanner détecte que le taux dépasse le maximum spécifié, l'extraction depuis l'archive ne se fait pas et le scan d'une telle archive ne sera pas effectué. Par défaut — illimité.
/ARL:<*niveau_d'imbrication*>	Niveau maximum d'imbrication de l'archive scannée. Par défaut — illimité.
/ARS:<*taille*>	Taille maximum de l'archive scannée, en Ko. Par défaut — illimité.
/ART:<*taille*>	Seuil de vérification du taux de compression (la taille minimum du fichier dans l'archive à partir de laquelle s'effectue la vérification du taux de compression), en Ko. Par défaut — illimité.
/ARX:<*taille*>	Taille maximum des objets archivés à scanner, en Ko. Par défaut — illimité.

Clé	Description
/BI	Afficher les informations sur les bases de données virales. L'option est activée par défaut.
/CUSTOM	Lancer le Scanner sur la page de l'analyse personnalisée. Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets à analyser ou les paramètres /TM, /TB), l'analyse personnalisée des objets spécifiés sera lancée. (Uniquement pour le Scanner).
/CL	Utiliser le service cloud Dr.Web. L'option est activée par défaut. (Uniquement pour le Scanner en ligne de commande).
/DCT	Ne pas afficher la durée calculée d'analyse. (Uniquement pour le Scanner en ligne de commande).
/DR	Scanner les dossiers de manière récursive (analyser les sous-dossiers). L'option est activée par défaut.
/E:<*nombre_de_flux*>	Effectuer une analyse à un nombre spécifié de flux.
/FAST	Lancer l'analyse rapide du système. Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets à analyser ou les paramètres /TM, /TB), les objets spécifiés seront également analysés. (Uniquement pour le Scanner).
/FL:<*nom_du_fichier*>	Analyser les chemins spécifiés dans le fichier.
/FM:<*masque*>	Analyser les fichiers par un masque. Par défaut, tous les fichiers seront analysés.
/FR:<*expression_régulière*>	Analyser les fichiers par une expression régulière. Par défaut, tous les fichiers sont scannés.
/FULL	Lancer l'analyse complète de tous les disques durs et de tous les supports amovibles (y compris les secteurs d'amorçage). Si dans ce cas, les paramètres avancés sont spécifiés (par exemple, les objets pour l'analyse ou les paramètres /TM, /TB), l'analyse rapide et l'analyse des objets spécifiés seront lancées. (Uniquement pour le Scanner).
/FX:<*masque*>	Exclure de l'analyse les fichiers qui correspondent au masque. (Uniquement pour le Scanner en ligne de commande).
/GO	Mode de fonctionnement du Scanner lors duquel les questions impliquant des réponses d'utilisateur sont ignorées ; les décisions impliquant un choix sont prises automatiquement. Il est utile d'utiliser ce mode pour l'analyse automatique des fichiers, par exemple, lors de l'analyse quotidien ou hebdomadaire du disque

Clé	Description
	dur. Dans la ligne de commande, il est nécessaire de spécifier l'objet à analyser. Vous pouvez utiliser les paramètres `/LITE`, `/FAST`, `/FULL` avec le paramètre `/GO`. Dans ce mode, l'analyse s'arrête en cas de passage en fonctionnement sur batterie.
`/H ou /?`	Afficher la rubrique d'aide sur le fonctionnement du programme. (Uniquement pour le Scanner en ligne de commande).
`/HA`	Effectuer une analyse heuristique des fichiers afin d'y rechercher des menaces inconnues. L'option est activée par défaut.
`/KEY:<`*fichier_clé*`>`	Spécifier le chemin vers le fichier clé. Le paramètre est nécessaire si le fichier clé se trouve dans un dossier autre que le dossier dans lequel se trouve le scanner. Par défaut, `drweb32.key` ou une autre clé appropriée depuis le dossier `C:\Program Files\DrWeb\` sera utilisée.
`/LITE`	Effectuer une analyse du système y compris la mémoire vive, les secteurs d'amorçage de tous les disques, effectuer une recherche des rootkits. (Uniquement pour le Scanner).
`/LN`	Analyser les fichiers par raccourcis associés. L'option est désactivée par défaut.
`/LS`	Analyser sous le compte LocalSystem. L'option est désactivée par défaut.
`/MA`	Analyser les fichiers de messagerie. L'option est activée par défaut.
`/MC:<`*nombre_de_tentatives* `>`	Spécifier le nombre maximum de tentatives de désinfecter le fichier. Par défaut — illimité.
`/NB`	Ne pas créer les copies de sauvegardes des fichiers désinfectés/supprimés. L'option est désactivée par défaut.
`/NI[:X]`	Niveau d'utilisation des ressources système, en pourcentage. Ce paramètre détermine le volume de la mémoire utilisée pour le processus de scan et la priorité système de la tâche de scan. Par défaut — illimité.
`/NOREBOOT`	Annule le redémarrage et l'arrêt du système après la fin de l'analyse. (Uniquement pour le Scanner).
`/NT`	Analyser les flux NTFS. L'option est activée par défaut.

Clé	Description
/OK	Afficher la liste complète des objets scannés et accompagner les objets sains de la remarque Ok. L'option est désactivée par défaut.
/P:<*priorité*>	Priorité de la tâche de scan en cours dans la file des tâches de scan : 0 : inférieure. L : basse. N : normale. Priorité par défaut. H : supérieure. M : maximum.
/PAL:<*niveau_d'imbrication*>	Niveau d'imbrication maximum des outils de compression d'un fichier exécutable. Si le niveau d'imbrication dépasse la valeur spécifiée, l'analyse va uniquement jusqu'au niveau d'imbrication spécifié. Par défaut — 1000.
/QL	Afficher la liste de tous les fichiers mis en quarantaine sur tous les disques. (Uniquement pour le Scanner en ligne de commande).
/QL:<*nom_du_disque_logique*>	Afficher la liste de tous les fichiers mis en quarantaine sur le disque logique spécifié. (Uniquement pour le Scanner en ligne de commande).
/QNA	Afficher les chemins entre guillemets doubles.
/QR[:[d][:p]]	Supprimer du disque spécifié <d> (nom_du_disque_logique) les fichiers se trouvant dans la quarantaine pendant plus de <p> jours. Si les valeurs <d> et <p> ne sont pas spécifiées, tous les fichiers se trouvant dans la quarantaine seront supprimés de tous les disques logiques (uniquement pour le Scanner en ligne de commande).
/QUIT	Fermer le Scanner après l'analyse (indépendamment de l'application/non application des actions aux menaces détectées). (Uniquement pour le Scanner).
/RA:<*nom_du_fichier*>	Ajouter le rapport du fonctionnement du programme dans le fichier spécifié. Par défaut, le rapport n'est pas enregistré dans le journal (lors du lancement du Scanneur depuis la ligne de commande).
/REP	Analyser par les liens symboliques. L'option est désactivée par défaut.

Clé	Description
/RK	Analyse pour la présence de rootkits. L'option est désactivée par défaut.
/RP:<*nom_du_fichier*>	Enregistrer le rapport du fonctionnement du programme dans le fichier spécifié. Par défaut, le rapport n'est pas enregistré dans le journal (lors du lancement du Scanneur depuis la ligne de commande).
/RPC:<*s*>	Délai de connexion au moteur de scan Scanning Engine, en secondes. Par défaut — 30 s. (Uniquement pour le Scanner en ligne de commande).
/RPCD	Utiliser l'identificateur dynamique RPC. (Uniquement pour le Scanner en ligne de commande).
/RPCE	Utiliser l'adresse cible dynamique RPC. (Uniquement pour le Scanner en ligne de commande).
/RPCE:<*adresse_cible*>	Utiliser l'adresse cible RPC spécifiée. (Uniquement pour le Scanner en ligne de commande).
/RPCH:<nom_d'hôte>	Utiliser le nom d'hôte spécifié pour les appels RPC. (Uniquement pour le Scanner en ligne de commande).
/RPCP:<*protocole*>	Utiliser le protocole spécifié RPC. Il est possible d'utiliser les protocoles : lpc, np, tcp. (Uniquement pour le Scanner en ligne de commande).
/SCC	Afficher le contenu des objets complexes. L'option est désactivée par défaut.
/SCN	Afficher le nom du package d'installation. L'option est désactivée par défaut.
/SLS	Afficher les logs sur l'écran. L'option est activée par défaut. (Uniquement pour le Scanner en ligne de commande).
/SPN	Afficher le nom de l'outil de compression. L'option est désactivée par défaut.
/SPS	Afficher la progression du processus de scan. L'option est activée par défaut (uniquement pour le Scanner en ligne de commande).
/SST	Afficher la durée du scan. L'option est désactivée par défaut.
/ST	Lancement du Scanner en tâche de fond. Si le paramètre /GO n'est pas spécifié, le mode graphique s'affiche uniquement en

Clé	Description
	cas de détection d'une menace. Dans ce mode, l'analyse s'arrête en cas de passage en fonctionnement sur batterie.
/TB	Analyser les secteurs de boot et les secteurs MBR du disque dur.
/TM	Détecter les menaces dans la mémoire vive (y compris la partie système de Windows).
/TR	Vérifier les points de restauration système.
/W:<*s*>	Durée maximum de scan, en secondes. Par défaut — illimité.
/WCL	Affichage compatible avec drwebwcl. (Uniquement pour le Scanner en ligne de commande).
/X:S[:R]	A la fin du scan, basculer la machine vers un mode de fonctionnement spécifié : arrêt/redémarrage/mode veille/mode veille prolongée.

Vous pouvez configurer les actions à appliquer aux objets divers (C — désinfecter, Q — déplacer vers la quarantaine, D — supprimer, I — ignorer, R — informer. L'action R est applicable uniquement au Scanner en ligne de commande. Par défaut, pour tous les objets — notifier (uniquement pour le Scanner en ligne de commande)) :

Action	Description
/AAD:<*action*>	actions appliquées aux adwares (actions possibles : DQIR)
/AAR:<*action*>	actions appliquées aux archives infectées (actions possibles : DQIR)
/ACN:<*action*>	actions appliquées aux packages d'installation infectés (actions possibles : DQIR)
/ADL:<*action*>	actions appliquées aux dialers (actions possibles : DQIR)
/AHT:<*action*>	actions appliquées aux hacktools (actions possibles : DQIR)
/AIC:<*action*>	actions appliquées aux fichiers incurables (actions possibles : DQR)
/AIN:<*action*>	actions appliquées aux fichiers infectés (actions possibles : CDQR)
/AJK:<*action*>	actions appliquées aux canulars (actions possibles : DQIR)
/AML:<*action*>	actions appliquées aux fichiers de messagerie infectés (actions possibles : QIR)
/ARW:<*action*>	actions appliquées aux riskwares (actions possibles : DQIR)
/ASU:<*action*>	actions appliquées aux fichiers suspects (actions possibles : DQIR)

Certaines clés peuvent avoir des modificateurs activant ou désactivant le mode de fonctionnement de manière explicite. Par exemple :

`/AC-`	le mode est explicitement désactivé
`/AC, /AC+`	le mode est explicitement activé

Cette option peut être utile dans le cas où le mode serait activé/désactivé par défaut ou selon le paramétrage du fichier de configuration. Les clés pouvant être utilisées avec des modificateurs sont les suivantes :

`/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.`

En cas de clé `/FL`, le modificateur « – » signifie : scanner les chemins listés dans le fichier spécifié et supprimer ce fichier.

En cas de clés `/ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL, /RPC, /W`, la valeur du paramètre « 0 » signifie que le paramètre est utilisé sans restrictions.

Exemple d'utilisation des clés lors du démarrage du Scanner en ligne de commande :

`[<`*chemin_vers_le_programme*`>]dwscancl /AR- /AIN:C /AIC:Q C:\`

scanner tous les fichiers se trouvant sur le disque C, excepté les archives ; désinfecter les fichiers infectés ; placer dans la quarantaine les fichiers incurables. Pour lancer le Scanner pour Windows de manière analogique, à la place de `dwscancl`, saisissez la commande `dwscanner`.

16.2. Paramètres du Module de mise à jour

Paramètres généraux :

Paramètre	Description
-h [--help]	Afficher à l'écran la rubrique d'aide abrégée sur le programme.
-v [--verbosity] arg	Niveau de détail du journal : `error` (standard), `info` (élevé), `debug` (débogage).
-d [--data-dir] arg	Répertoire dans lequel sont conservés le référentiel et les paramètres.
--log-dir arg	Répertoire dans lequel le fichier de journal sera sauvegardé.
--log-file arg (=dwupdater.log)	Nom du fichier de journal.
-r [--repo-dir] arg	Répertoire du référentiel, (par défaut <*data_dir*>`/repo`).

Paramètre	Description
-t [--trace]	Activer le traçage.
-c [--command] arg (=update)	Commande à exécuter : `getversions` — obtenir les versions, `getcomponents` — obtenir les composants, update — mise à jour, `uninstall` — supprimer, `exec` — exécuter, `keyupdate` — mettre à jour la clé, `download` — télécharger.
-z [--zone] arg	Liste des zones à utiliser à la place des zones spécifiées dans le fichier de configuration.

Paramètres de la commande de mise à jour (update) :

Paramètre	Description
-p [--product] arg	Le nom du produit. Si un nom est spécifié, seul le produit correspondant sera mis à jour. Si aucun produit n'est spécifié, ni aucun composant, alors tous les produits seront mis à jour. S'il y a des composants spécifiés, ces composants seront mis à jour.
-n [--component] arg	Liste des composant à mettre à niveau vers une révision spécifiée. Syntaxe : <*name*>, <*target revision*>.
.-x [--selfrestart] arg (=yes)	Redémarrage après la mise à jour du Module de mise à jour. La valeur par défaut – `yes`. En cas de valeur `no`, une notification sur la nécessité de redémarrer sera affichée.
--geo-update	Obtenir une liste des adresses IP `update.drweb.com` avant la mise à jour.
--type arg (=normal)	Peut prendre l'une des valeurs suivantes : • `reset-all` : forcer la mise à jour de tous les composants ; • `reset-failed` : annuler toutes les modifications pour les composants corrompus ; • `normal-failed` : essayer de mettre à niveau les composants y compris ceux qui sont corrompus, vers la dernière version ou vers une version spécifiée ; • `update-revision` : mettre à jour les composant au sein de la révision courante ; • `normal` : mettre à jour tous les composants.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <*adresse*>: <*port*>.
-u [--user] arg	Nom de l'utilisateur du serveur proxy.

Paramètre	Description
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
--param arg	Transmettre les paramètres supplémentaires vers le script. Syntaxe : <*nom*>: <*valeur*>.
-l [--progress-to-console]	Afficher sur la console les informations sur le chargement et l'exécution du script.

Paramètres de la commande d'obtention des composants (getcomponents) :

Paramètre	Description
-s [--version] arg	Numéro de version.
-p [--product] arg	Spécifiez le nom du produit pour consulter les composants inclus. Si aucun produit n'est spécifié, tous les composants correspondant à la version courante seront affichés.

Paramètres de la commande d'obtention des révisons (getrevisions) :

Paramètre	Description
-s [--version] arg	Numéro de version.
-n [--component] arg	Nom du composant.

Paramètres de la commande de suppression (uninstall) :

Paramètre	Description
-n [--component] arg	Nom du composant à supprimer.
-l [--progress-to-console]	Afficher sur la console des informations sur l'exécution de la commande.
--param arg	Transmettre les paramètres supplémentaires vers le script. Syntaxe : <*nom*>: <*valeur*>.
-e [--add-to-exclude]	Composants qui seront supprimés, leur mise à jour ne sera pas réalisée.

Paramètres de la commande de mise à jour automatique de la clé (keyupdate) :

Paramètre	Description
-m [--md5] arg	Somme de contrôle md5 de l'ancien fichier clé.
-o [--output] arg	Nom du fichier.
-b [--backup]	Copie de sauvegarde de l'ancien fichier clé s'il existe.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <*adresse*>: <*port*>.
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
-l [--progress-to-console]	Afficher sur la console des informations sur le téléchargement du fichier clé.

Paramètres de la commande de téléchargement (download) :

Paramètre	Description
--zones arg	Fichier contenant la liste des zones.
--key-dir arg	Répertoire dans lequel se trouve le fichier clé.
-l [--progress-to-console]	Afficher sur la console des informations sur l'exécution de la commande.
-g [--proxy] arg	Serveur proxy pour la mise à jour au format <*adresse*>: <*port*>.
-u [--user] arg	Nom de l'utilisateur du serveur proxy.
-k [--password] arg	Mot de passe de l'utilisateur du serveur proxy.
-s [--version] arg	Nom de la version.
-p [--product] arg	Nom du produit à télécharger.

16.3. Codes de retour

Les valeurs possibles du code de retour et les événements y correspondant sont les suivants :

Code de retour	Événement
0	Aucun virus ou soupçon de virus n'est détecté.
1	Les virus connus sont détectés.
2	Les modifications de virus connus sont détectées.
4	Les objets suspects sont détectés.
8	Les virus connus sont détectés dans une archive, un conteneur ou dans une boîte e-mail.
16	Les modifications de virus connus sont détectées dans une archive, un conteneur ou dans une boîte e-mail.
32	Les objets suspects sont détectés dans une archive, un conteneur ou dans une boîte e-mail.
64	Au moins un objet infecté a été désinfecté avec succès.
128	La désinfection/la renomination/le déplacement d'au moins un fichier infecté est effectué.

Le code de retour final, formé à la fin du scan, est égal à la somme des codes des événements survenus lors du scan (les termes peuvent être reconstitués d'après le code final).

Par exemple, le code de retour 9 = 1 + 8 signifie que des virus connus (un virus) ont été détectés lors du scan, y compris dans les archives ; la désinfection n'a pas été effectuée ; il n'y avait plus aucun événement viral.

17. Annexe B. Menaces et méthodes de neutralisation

Avec le développement des technologies IT et des solutions réseau, les programmes malveillants de différents types, conçus pour attaquer les utilisateurs, deviennent de plus en plus répandus. Leur développement a commencé au moment d'apparition de l'informatique. Les outils de protection contre les programmes malveillants ont progressé en même temps. Néanmoins, il n'existe toujours pas de classification commune pour toutes les menaces potentielles en raison du caractère imprévisible de leur développement et de leur constante amélioration.

Les programmes malveillants peuvent être diffusés via Internet, les réseaux locaux, les e-mails et les supports amovibles. Certains d'entre eux comptent sur l'imprudence des utilisateurs et leur manque d'expérience et peuvent fonctionner en mode complètement automatique. D'autres sont des outils contrôlés par un cybercriminel et peuvent endommager même le système le plus sécurisé.

Ce chapitre décrit les types de programmes malveillants les plus connus et les plus répandus, contre lesquels luttent les produits de l'entreprise Doctor Web.

17.1. Types de menaces informatiques

Sous le terme *« menace »*, ce classement comprend tout logiciel pouvant endommager directement ou indirectement l'ordinateur, le réseau, l'information ou porter atteinte aux droits de l'utilisateur (programmes malicieux ou indésirables). Dans le sens plus large du terme, « menace » peut signifier un danger potentiel pour l'ordinateur ou pour le réseau (une vulnérabilité pouvant être utilisée pour des attaques de pirates).

Tous les types de logiciels décrits ci-dessous peuvent présenter un danger pour les données de l'utilisateur et pour leur confidentialité. Les logiciels qui ne dissimulent pas leur présence dans le système (par exemple, certains logiciels de diffusion de spam ou analyseurs du trafic), normalement ne sont pas 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 plus conforme à l'original. La majeure partie des virus est conçue pour endommager ou exterminer les données.

En fonction du type d'objet infecté, Doctor Web classifie les virus selon les types suivants :

- *Les virus de fichier* infectent les fichiers du système d'exploitation (fichiers exécutables, bibliothèques dynamiques). Ces virus sont activés lors de l'accès au fichier infecté.
- Les *macrovirus* infectent les documents qui utilisent les applications de Microsoft Office (et d'autres programmes utilisant des commandes macros écrits, par exemple, en Visual Basic). Les *macros*, ce sont des programmes intégrés, écrits en langage de programmation totalement

fonctionnel, qui sont automatiquement lancés sous des conditions déterminées (par exemple, dans Microsoft Word, les macros peuvent se lancer quand vous ouvrez, fermez ou sauvegardez un document).

- Les *virus script* sont écrits en langages de scénarios (langages de script). Ils infectent dans la plupart des cas d'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 de démarrage des disques et des partitions aussi bien que les principaux secteurs de démarrage 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 soient effectués.

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 diviser les virus selon les principes de protection contre la détection :

- Les *virus cryptés* chiffrent leur code à chaque nouvelle infection ce qui empêche leur détection dans un fichier, un secteur de démarrage ou une mémoire. Toutes les copies de tels virus contiennent seulement un petit fragment de code commun (procédure de décryptage) qui peut être utilisé comme une signature de virus.
- Les *virus polymorphes* chiffrent 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.
- *Virus furtifs* : ils 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 programmes malveillants de type « ver informatique » sont devenus beaucoup plus répandus que les virus et les autres programmes 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 à 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.
- *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 programmes 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 Trojan 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 la 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 intégré dans 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 malicieux et afficher la publicité, par exemple, sur des navigateurs Internet. 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

Les 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.

17.2. Actions appliquées aux menaces détectées

Il existe plusieurs méthodes de neutralisation des menaces. Les produits de l'entreprise Doctor Web combinent ces méthodes pour la protection la plus fiable des ordinateurs et des réseaux en utilisant une configuration conviviale et flexible. Les principales actions de neutralisation des programmes malveillants sont les suivantes :

1. **Désinfecter** : l'action appliquée aux virus, vers et Trojans. Ceci implique la suppression du code malveillant des fichiers infectés ou la suppression de copies de programmes malveillants, ainsi que la restauration des objets infectés (c'est-à-dire la restauration de la structure et du fonctionnement de l'objet tels qu'ils étaient avant son infection) si possible. Tous les programmes malveillants ne peuvent être désinfectés. Cependant, les produits de l'entreprise Doctor Web sont basés sur les plus efficaces algorithmes de désinfection et de restauration de fichiers infectés.
2. **Déplacer en quarantaine** : il s'agit de déplacer l'objet malveillant dans un dossier spécial et de l'isoler du reste du système. Cette action est préférable en cas d'impossibilité de désinfecter et pour tous les objets suspects. Il est recommandé d'envoyer des copies de ces fichiers au laboratoire antivirus de Doctor Web afin qu'elles soient analysées.
3. **Supprimer** : l'action efficace de neutralisation des menaces. Elle peut s'appliquer à n'importe quel type d'objet malveillant. Notez que la suppression sera parfois appliquée aux objets pour lesquels la désinfection était sélectionnée. Ceci arrive si l'objet contient uniquement le code malveillant et ne contient pas d'information utile. Par exemple, la désinfection d'un ver d'ordinateur signifie la destruction de toutes ses copies opérationnelles.
4. **Bloquer** : cette action permet également de neutraliser des programmes malveillants. Cependant, des copies totalement fonctionnelles de ces programmes demeurent dans le système. Toutes les tentatives d'accès vers ou depuis l'objet malveillant sont bloquées.

18. Annexe C. Principes de nomination des menaces

En cas de détection d'un code viral les composants Dr.Web le signalent à l'utilisateur à l'aide des outils de l'interface et inscrivent le nom du virus, attribué par les spécialistes de l'entreprise Doctor Web, dans le fichier du rapport. Ces noms sont créés en fonction de certains principes et reflètent un modèle de menace, des catégories d'objets vulnérables, l'environnement de diffusion (OS et applications) et d'autres caractéristiques. Le fait de savoir ces principes peut être utile pour la compréhension du logiciel et les vulnérabilités organisationnelles du système protégé. Vous trouverez ci-dessous le bref exposé de ces principes, la version complète de cette classification qui est mise à jour constamment se trouve sur https://vms.drweb.com/classification/.

Dans certains cas, cette classification est conventionnelle, car certains virus possèdent plusieurs caractéristiques en même temps. De plus, elle ne devrait pas être considérée comme exhaustive car de nouveaux types de virus apparaissent constamment et la classification devient de plus en plus précise.

Le nom complet d'un virus se compose de plusieurs éléments, séparés par des points. Certains éléments au début du nom (préfixes) et à la fin du nom (suffixes) sont standards dans la classification.

Préfixes généraux

Préfixes du système d'exploitation

Les préfixes listés ci-dessous sont utilisés pour nommer les virus infectant les fichiers exécutables de certains OS :

- `Win` : programmes 16 bits Windows 3.1 ;
- `Win95` : programmes 32 bits Windows 95/98/Me ;
- `Win95` : programmes 32 bits et 64 bits Windows NT/2000/XP/Vista/7/8/8.1/10 ;
- `Win32` : programmes 32 bits de différents environnements Windows 95/98/Me et Windows NT/2000/XP/Vista/7/8/8.1/10 ;
- `Win64` : programmes 64 bits Windows XP/Vista/7/8/8.1/10 ;
- `Win32.NET` : programmes Microsoft .NET Framework ;
- `OS2` : programmes OS/2 ;
- `Unix` : programmes dans différents systèmes basés sur UNIX ;
- `Linux` : programmes Linux ;
- `FreeBSD` : programmes FreeBSD ;
- `SunOS` : programmes SunOS (Solaris) ;
- `Symbian` : programmes Symbian OS (OS mobile).

Notez que certains virus peuvent infecter les programmes d'un système même s'ils sont créés pour fonctionner dans un autre système.

Virus infectant les fichiers MS Office

La liste des préfixes pour les virus qui infectent les objets MS Office (le langage des macros infectées par de tels virus est spécifié) :

- `WM` : Word Basic (MS Word 6.0-7.0) ;
- `XM` : VBA3 (MS Excel 5.0-7.0) ;
- `W97M` : VBA5 (MS Word 8.0), VBA6 (MS Word 9.0) ;
- `X97M` : VBA5 (MS Word 8.0), VBA6 (MS Word 9.0) ;
- `A97M` : bases de données de MS Access'97/2000 ;
- `PP97M` : présentations MS PowerPoint ;
- `O97M` : VBA5 (MS Office'97), VBA6 (MS Office 2000) ; ce virus infecte les fichiers de plus d'un composant de MS Office.

Préfixes de langage de programmation

Le groupe de préfixes `HLL` est utilisé pour nommer les virus écrits en langages de programmation de haut niveau comme C, C++, Pascal, Basic et d'autres. On utilise des modificateurs, indiquant l'algorithme de fonctionnement de base, notamment :

- `HLLW` : vers ;
- `HLLM` : vers de messagerie ;
- `HLLO` : virus qui réécrivent le code du programme victime ;
- `HLLP` : virus parasites ;
- `HLLC` : virus compagnon.

Le préfixe suivant se réfère également à un langage de développement :

- `Java` : virus destinés à la machine virtuelle Java.

Chevaux de Troie

`Cheval de Troie` : nom général pour désigner différents programmes de Troie (Trojans). Dans de nombreux cas, les préfixes de ce groupe sont utilisés avec le préfixe Trojan.

- `PWS` : Trojan voleur de mots de passe ;
- `Backdoor` : Trojan avec la fonction de RAT (Remote Administration Tool – utilitaire d'administration à distance) ;
- `IRC` : Trojan qui utilise des canaux Internet Relay Chat ;

- `DownLoader` : Trojan qui télécharge discrètement les différents programmes malveillants sur Internet ;
- `MulDrop` : Trojan qui télécharge discrètement des virus contenus dans son corps ;
- `Proxy` : Trojan qui autorise une tierce personne à travailler anonymement sur Internet via l'ordinateur infecté ;
- `StartPage` (synonyme : `Seeker`) : Trojan qui remplace sans autorisation la page d'accueil du navigateur (page de démarrage) ;
- `Click` : Trojan qui redirige l'utilisateur vers un site spécial (ou des sites) ;
- `KeyLogger` : Trojan spyware qui suit et enregistre des touches saisies ; il peut envoyer les données collectées à un cybercriminel ;
- `AVKill` : stoppe ou supprime les programmes antivirus, pare-feu, etc. ;
- `KillFiles`, `KillDisk`, `DiskEraser` : supprime certains fichiers (des fichiers dans certains répertoires, des fichiers selon certains masques, tous les fichiers sur les disques etc.) ;
- `DelWin` : supprime les fichiers vitaux pour le fonctionnement de l'OS Windows ;
- `FormatC` : formate le disque C : (synonyme : `FormatAll` : formate certains disques ou tous les disques) ;
- `KillMBR` : corrompt ou supprime le contenu du secteur principal d'amorçage (MBR) ;
- `KillCMOS` : corrompt ou supprime la mémoire CMOS.

Outil exploitant les vulnérabilités

- `Exploit` : un outil exploitant les vulnérabilités connues d'un OS ou d'une application pour introduire un code malveillant ou effectuer des actions non autorisées.

Outils d'attaques réseaux

- `Nuke` : outils destinés à attaquer certaines vulnérabilités connues des systèmes d'exploitation afin de provoquer l'arrêt du système attaqué ;
- `DDoS` : programme-agent destiné à provoquer une attaque par déni de service (Distributed Denial of Service) ;
- `FDoS` (synonyme : Flooder) : Flooder Denial Of Service – programmes destinés à effectuer des actions malveillantes sur Internet reposant sur l'idée des attaques par déni de service ; contrairement aux DDoS où plusieurs agents sur différents ordinateurs sont utilisés simultanément pour attaquer un système, un programme FDoS opère comme un programme indépendant « autosuffisant ».

Virus-script

Préfixes des virus écrits en différents langages de script :

- `VBS` : Visual Basic Script ;
- `JS` : Java Script ;

- `Wscript` : Visual Basic Script et/ou Java Script ;
- `Perl` : Perl ;
- `PHP` : PHP ;
- `BAT` : langage d'interprète de commande de l'OS MS-DOS.

Programmes malveillants

Préfixes des objets qui ne sont pas des virus, mais des programmes malveillants :

- `Adware` : publicité ;
- `Dialer` : programme dialer (il redirige les appels du modem vers des numéros payants) ;
- `Joke` : canular ;
- `Program` : un programme potentiellement dangereux (riskware) ;
- `Tool` : programme utilisé pour faire du piratage (hacktool).

Divers

Le préfixe `generic` est utilisé, après un autre préfixe décrivant l'environnement ou la méthode de développement, pour nommer un représentant typique de ce type de virus. Un tel virus ne possède aucune caractéristique (comme des séries de texte, des effets spécifiques etc.) qui permettrait de lui donner un nom particulier.

Auparavant le préfixe `Silly` était utilisé avec les modificateurs différents pour nommer les virus simples, sans signe particulier.

Suffixes

Les suffixes sont utilisés pour nommer des objets viraux particuliers :

- `generator` : un objet qui n'est pas un virus, mais un générateur de virus ;
- `based` : un virus développé à l'aide d'un générateur spécifique ou d'un virus modifié. Dans les deux cas, les noms de virus de ce type sont génériques et peuvent définir des centaines voire des milliers de virus ;
- `dropper` : un objet qui n'est pas un virus mais l'installateur du virus indiqué.

19. Annexe D. Termes essentiels

A

Applications de confiance : applications dont les signatures sont ajoutées dans la liste de confiance dans drwbase.db. Les applications de confiance comprennent les logiciels populaires, tels que Google Chrome, Firefox, les applications de Microsoft.

B

Bus de périphériques : sous-systèmes de transmission de données entre les blocs fonctionnels de l'ordinateur (par exemple, le bus USB).

C

Classes de périphériques : périphériques exécutant les mêmes fonctions (par exemple, les périphériques d'impression).

E

Émulation : imitation de fonctionnement d'un système avec les outils d'un autre système sans pertes fonctionnelles et falsification des résultats par des outils spéciaux.

Exploits : programme, fragment de code ou séquence de commandes qui utilise les vulnérabilités de logiciels et attaque le système.

H

Heuristique : hypothèse dont la signification statistique est confirmée par l'expérience.

M

Miroir de mise à jour : dossier dans lequel sont copiées des mises à jour. Le miroir de mise à jour peut être utilisé en tant que source de mises à jour pour les ordinateurs du réseau local qui ne sont pas connectés à Internet.

Mode administrateur : mode de Dr.Web qui fournit l'accès à tous les paramètres des composants de protection et les paramètres du logiciel. Pour passer en mode administrateur, il faut cliquer sur le cadenas  .

Modification d'un virus : code du virus modifié de telle manière que le scanner peut le détecter mais les algorithmes de neutralisation appropriés au virus d'origine n'y peuvent pas être appliqués.

R

Réseau antivirus : ensemble d'ordinateurs sur lesquels sont installés les produits Dr.Web (Antivirus Dr.Web pour Windows, Antivirus Dr.Web pour serveurs Windows ou Dr.Web Security Space) et qui sont connectés au même réseau local.

S

Signature (entrée virale) : séquence continue et finie d'octets qui est nécessaire et suffisante pour identifier une menace.

Signature numérique : référence à un document électronique destinée à protéger ce document électronique contre falsification. Elle est obtenue grâce à la transformation cryptographique des informations avec la clé privée de la signature numérique et elle permet d'identifier le propriétaire du certificat de la clé de signature et déterminer si les informations dans le document électronique ont été modifiées ou non.

Somme de contrôle : identificateur de fichier unique représentant une séquence de chiffres et de lettres. Il est utilisé pour vérifier l'intégrité des données.