Dr.WEB®
depuis 1992

Protégez votre univers

Gamme de produits Dr.Web Security Suite

Guide des licences

Dernière mise à jour le 10.06.2016

Sommaire

10.06.2016

A propos de Doctor Web

Doctor Web est un éditeur russe de solutions de sécurité informatique.

La société propose des solutions efficaces contre les virus et le spam destinées aux grandes entreprises et aux administrations, aussi bien qu'aux utilisateurs individuels. Les produits antivirus de Dr.Web sont édités depuis 1992 et ne cessent de montrer d'excellents résultats de détection des logiciels malveillants, correspondant aux standards de sécurité mondiaux. La création de la société Doctor Web au mois de décembre 2003 a marqué le début d'une croissance rapide des ventes des produits Dr.Web en Russie et à l'étranger.

Le nom Dr.Web® appartient à Doctor Web. L'entreprise est propriétaire du moteur Dr.Web® et dispose de son propre laboratoire antivirus ainsi que de son propre service de supervision virale.

Les gammes de produits développées par Doctor Web intègrent un large spectre de systèmes d'exploitation et d'applications compatibles.

Parmi nos clients, nous comptons des particuliers du monde entier, de petites et de grandes entreprises, ainsi que des groupes internationaux. Nous les remercions de leur soutien et de leur fidélité à l'égard des produits Dr.Web®.

La distribution des produits de sécurité Dr.Web s'appuie sur un réseau de partenaires revendeurs. Doctor Web ne vend pas ses produits directement à l'utilisateur final.

Technologies Dr.Web

Dr.Web est une famille de logiciels créés par des développeurs russes de talent sous la direction d'Igor Daniloff.

Les produits antivirus de Doctor Web sont édités sur la base de sa propre technologie. Doctor Web est un de rares vendeurs mondiaux possédant sa propre technologie unique de détection et de désinfection des logiciels malveillants ; ainsi que son propre service de surveillance antivirale et son laboratoire analytique. Tout cela donne la possibilité aux spécialistes de la société de réagir rapidement aux menaces récentes et de venir rapidement en aide aux clients.

Une autre particularité très importante des produits Dr.Web est leur architecture modulaire. Tous les produits et solutions contiennent un noyau antiviral Dr.Web commun, ils utilisent aussi le même système de mises à jour des bases virales et un système global de support technique. Les technologies de Dr.Web permettent de mettre en œuvre une protection antivirus solide pour les réseaux d'entreprises, grandes et petites ou pour un ordinateur individuel.

Outre les virus et les logiciels malveillants, Dr.Web est capable de détecter et d'éliminer de l'ordinateur d'autres logiciels nuisibles (logiciels publicitaires, dialers, jokes, logiciels potentiellements dangereux, spyware/riskware), le spam et les messages malveillants (scamming, phishing, pharming et bounce).

Technologies

Un des indices les plus importants de la qualité de fonctionnement d'un logiciel antivirus est non seulement sa capacité à dépister les virus, mais également celle de désinfecter les fichiers, sans les éliminer, et de les restaurer dans leur état initial « sain ». Dr.Web est très attentif au traitement des fichiers de ses utilisateurs.

Traitement des virus

L'aptitude d'un logiciel antivirus, non seulement à détecter les virus, mais également à les désinfecter, est un indice important de sa qualité. Il ne doit pas supprimer les fichiers atteints si leur contenu est nécessaire à l'utilisateur, mais les rendre de nouveau « sains ».

10.06.2016

Les virus complexes créés pour gagner de l'argent sont souvent testés par les pirates avec les antivirus les plus utilisés du marché. Ils s'assurent ainsi que les virus ne seront pas détectés dès leur lancement. Ainsi, avant que des exemplaires de ces virus soient analysés dans les laboratoires, ils ne sont détectés par aucun antivirus.

Dr.Web est efficace dans la détection et dans le traitement des virus

- La possibilité de fonctionner sur un ordinateur déjà infecté et une résistance exclusive aux virus distinguent les logiciels Dr.Web des autres produits antivirus.
- L'utilisation de technologies uniques de traitement des processus en mémoire, combinées aux excellentes fonctionnalités de neutralisation des infections actives permettent d'installer Dr.Web directement sur une machine infectée (sans désinfection préalable) et même depuis un support amovible, sans installation sur le système (par exemple depuis une clé USB).
- Nouveau ! l'Antirootkit est intégré à l'installateur, ce qui permet à Dr.Web de résister aux menaces actives et de traiter le PC au moment de l'installation, même si le PC est infecté par des programmes malveillants complexes.
- Nouveau ! Le sous-système de scan de fond et de neutralisation des menaces actives avec l'Anti-rootkit Dr.Web (Anti-rootkit API, arkapi) réside en permanence en mémoire et recherche les menaces actives dans les objets critiques Windows: objets autorun, processus et modules lancés, objets système, mémoire vive, MBR/VBR des disques, BIOS du PC. En cas de détection, le sous-système bloque et traite les processus malveillants.
- Dr.Web est capable de détecter et de neutraliser les virus dans la mémoire vive, c'est-à-dire les virus qui n'existent pas sous la forme de fichiers. **Peu nombreux sont les antivirus sachant les traiter**.
- Dr.Web est capable de détecter les objets malveillants compressés, même avec des méthodes qu'il ne connaît pas. Il les analyse composant par composant pour détecter les menaces cachées. Seul Dr.Web est capable de scanner les archives de tous niveaux d'emboitement. Ainsi, même si des outils de compression différents ont été utilisés pour compresser l'objet malveillant à de nombreuses reprises, Dr.Web va quand même le détecter.

Autoprotection de haut niveau

Une immunité solide contre toutes les tentatives des logiciels malveillants d'entraver le fonctionnement de Dr.Web est garantie par le composant d'autoprotection Dr.Web SelfPROtect.

- **Dr.Web SelfPROtect** fonctionne comme un driver au niveau le plus bas du système. L'arrêt de son fonctionnement n'est pas possible sans redémarrer le système. De cette manière, les logiciels malveillants ne peuvent pas détériorer le système d'autoprotection.
- **Dr.Web SelfPROtect** limite l'accès des objets suspects au réseau, aux fichiers et aux dossiers ainsi qu'à certaines branches du registre et aux supports de données amovibles au niveau du driver système, protège contre les tentatives des logiciels anti-antivirus d'arrêter le fonctionnement de Dr.Web.
- A la différence de certains autres produits, qui doivent modifier certains éléments du noyau de Windows pour se protéger (captent les interruptions, substituent les tableaux des vecteurs, utilisent les fonctionnalités non-documentées), ce qui peut perturber le fonctionnement de l'OS et faciliter l'exploitation des vulnérabilités du système, le module de protection **Dr.Web SelfPROtect** est autosuffisant.
- Restauration automatique des modules d'autoprotection.

Technologies avancées de la protection préventive

- **FLY-CODE** — ne technologie unique de décompression permettant de détecter les virus compressés même par des méthodes inconnues de Dr.Web.

10.06.2016

- La technologie unique **Origins Tracing**™ de détection non basée sur les signatures permet à Dr.Web de détecter les virus inconnus de la base virale Dr.Web.
- **Le moteur d'analyse heuristique de Dr.Web** dont l'analyse se fonde sur des caractéristiques typiques de différents groupes de malwares, détecte la plupart des menaces connues.
- **Dr.Web Process Heuristic** fournit une protection contre les nouveaux programmes malveillants conçus pour éviter d'être détectés par les mécanismes traditionnels basés sur l'analyse par signature ou par l'analyse heuristique classique, qui n'ont par conséquent pas encore été analysés par le Laboratoire, et ne sont pas répertoriés dans la base de données virales Dr.Web au moment de leur intrusion dans le système. Le module analyse le comportement du malware et s'il conclut à sa nocivité, la menace est neutralisée. La nouvelle technologie de protection des données contre l'endommagement permet de minimiser les pertes liées à l'activité d'un virus inconnu.
- **L'analyse complète des menaces empaquetées** améliore considérablement la détection des soi-disant « nouvelles menaces », connues de la base virale Dr.Web mais dissimulées sous de nouveaux packers. Elle permet d'éviter l'ajout de nombreuses nouvelles entrées à la base virale. La compacité des bases virales Dr.Web permet de ne pas modifier constamment les pré-requis système et assure une compacité des mises à jour, tout en gardant la même qualité de détection et de désinfection.

Analyse complète de tout le trafic

- Trafic sécurisé : tout le trafic est analysé via tous les ports selon les protocoles pris en charge par Dr.Web, y compris les protocoles sécurisés (si l'utilisateur a activé SSL).
- Naviguez sur Internet en toute sécurité : Si l'utilisateur surfe via les moteurs de recherche Google, Yandex, Yahoo!, Bing, Rambler, seuls les sites web qui ne sont pas dangereux selon l'estimation des moteurs de recherche et de Dr.Web seront affichés dans les résultats. Ceci grâce à la fonctionnalité Safe Search : le contenu non sécurisé est filtré par les moteurs de recherche eux-mêmes !
- Communication sécurisée : le filtrage du trafic dans les clients IM tels que Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin et autres. Les liens redirigeant vers des sites malveillants et/ou de phishing sont ôtés des messages. Les pièces jointes sont analysées afin que le transfert de pièces jointes potentiellement dangereuses soit bloqué.

Protection instantanée grâce au Cloud

- Les URL peuvent être analysé via les serveurs Doctor Web grâce au service Dr.Web Cloud dans le cadre du Contrôle parental et de l'antivirus web SpIDer Gate.
- Lorsque l'utilisateur souhaite visiter des sites web, les URL correspondantes sont envoyées pour analyse aux serveurs de Doctor Web. La vérification est effectuée en temps réel, indépendamment de l'état des bases virales Dr.Web sur l'ordinateur de l'utilisateur et des paramètres de mises à jour.
- Aucune information personnelle permettant d'identifier l'utilisateur n'est transmise.

Technologie de filtrage antispam

L'antispam Dr.Web analyse les messages en se basant sur plusieurs milliers de règles, qui peuvent être subdivisées en quelques groupes.

Analyse heuristique

La technologie intelligente de l'analyse heuristique porte sur toutes les parties du message: objet, corps du message etc. et analyse également les pièces jointes s'il y en a. Le moteur d'analyse heuristique ne cesse d'évoluer et de nouvelles règles s'y ajoutent régulièrement. Son fonctionnement lui permet de détecter des genres encore inconnus de spam avant même le lancement d'une mise à jour correspondante.

Filtrage des anti antispam

C'est une des technologies les plus efficaces et avantageuses de l'antispam Dr.Web. Elle consiste à détecter les méthodes utilisées par les spammeurs pour contourner les filtres antispam.

Analyse basée sur les signatures HTML

Les messages qui contiennent un code HTML sont comparés à des exemples de signatures HTML de la bibliothèque antispam. Cette comparaison, combinée aux données sur les dimensions des images typiques du spam, protège les internautes contre les messages spam comportant un code HTML, qui contiennent souvent des images en ligne.

Technologie de détection du spam selon les objets des messages

La détection des falsifications des « tampons » des serveurs SMTP et des autres éléments des objets des messages est une direction nouvelle dans le développement des méthodes de lutte contre le spam. L'adresse de l'expéditeur doit toujours être mise en doute car les pirates peuvent la falsifier. Les messages falsifiés contiennent non seulement du spam mais également des messages de fausses alertes, voire des messages visant à exercer une pression sur le personnel (lettre anonymes ou menaces). Les technologies spécifiques de l'antispam Dr.Web permettent de mettre en évidence les adresses falsifiées et ne pas laisser passer de tels messages. Cela assure une économie considérable du trafic, mais également une protection sûre des employés contre ce type de messages, qui pourraient les pousser à agir de manière imprévue.

Analyse sémantique

Grâce à l'analyse sémantique, les mots et les combinaisons de mots contenus dans les messages sont comparés au lexique spécifique du spam. Cette comparaison s'effectue grâce à un dictionnaire spécial et l'analyse porte non seulement sur des mots évidents, mais également sur des expressions et des signes spécifiques qui sont dissimulés par des outils techniques spécialisés.

Technologie anti-scamming

Les messages scamming (ainsi que les messages pharming, qui sont une de leur variété) est un des types de spam les plus dangereux. On compte parmi eux les « nigérians », des alertes sur des soi-disant prix remportés au loto ou au casino, ainsi que des messages falsifiés de banques et de sociétés de crédit. Un module spécial est prévu dans l'antispam Dr.Web pour filtrer ces arnaques.

Filtrage du spam technique

Des notifications automatiques du courrier électronique – des messages bounce – sont utilisées pour informer les internautes sur les défaillances du système de messagerie (par exemple, quand un message n'est pas livré au destinataire). Des messages analogues peuvent être utilisés par des pirates. Par exemple, réception d'une fausse alerte « technique » prétendant qu'un worm peut s'introduire dans le système. Un module spécialisé de l'antispam Dr.Web est chargé de détecter ces messages malveillants.

Avantages de l'antispam Dr.Web

- Il filtre le courrier entrant et sortant en temps réel.
- Le fonctionnement de l'antispam ne dépend pas du logiciel de messagerie utilisé et il ne prolonge presque pas le délai de réception du courrier.
- L'Antispam n'exige pas de paramétrage avant son utilisation, il commence à fonctionner automatiquement dès la réception du premier message.
- Différentes technologies de filtrage assurent une haute probabilité de détection du spam, ainsi que des messages phishing, pharming, scamming et bounce. Tandis que la probabilité de faux positifs est presque égale à zéro.
- Il n'élimine pas les messages suspects, mais les place dans un dossier spécial de la boîte de réception, où vous pouvez les analyser pour vérifier qu'il n'y a pas de faux positifs.
- Le module de l'analyseur du spam est absolument autonome : il n'exige pas de lien constant avec un serveur extérieur pour fonctionner ou d'accès à une base de données, ce qui permet d'économiser le trafic. Il ne demande pas plus d'une mise à jour en 24 heures. Les technologies uniques de détection des messages malveillants, qui se basent sur des milliers de règles, délivrent l'utilisateur de la nécessité de télécharger souvent des mises à jour volumineuses.

Organisation unique de la base virale Dr.Web

La base virale Dr.Web est une des plus petites parmi celles de tous les logiciels antivirus existants. Cela est possible grâce à une technologie développée par Dr.Web de création d'une base virale à l'aide d'une langue très flexible, spécialement conçue à cet effet. Contrairement aux bases des autres éditeurs, sa petite taille assure une grande économie de trafic et permet d'occuper moins de place sur le disque et dans la mémoire vive après l'installation. Ses dimensions restreintes favorisent une interaction stable des composants du logiciel Dr.Web en mode super-rapide sans charger excessivement le processeur.

Quel est le rôle essentiel d'un antivirus ? Assurer une protection solide contre les virus. Cette protection est assurée entre autres via l'introduction régulière de signatures dans la base virale, ce qui permet de dépister les virus. Mais on ne peut pas juger de la capacité de détection d'une base virale au nombre de signatures qu'elle contient. Pour comprendre pourquoi le nombre de signatures dans la base virale de Dr.Web est moins important que celui des bases virales des autres éditeurs, il faut savoir que tous les virus ne sont pas uniques. Il existe des familles entières de virus semblables. Les développeurs d'autres antivirus munissent chaque virus, même des virus jumeaux, d'une signature à part, ce qui rend leur base virale plus volumineuse. Un autre principe est utilisé dans la base virale de Dr.Web, où une seule signature permet de neutraliser des centaines et des milliers de virus semblables.

Avantages de la base virale de Dr.Web

- Petit nombre de signatures.
- Petit volume de mises à jour.
- Une seule signature permet de détecter des centaines voir des milliers de virus semblables.

La différence de principe entre la base virale de Dr.Web et les bases des autres antivirus consiste en ce qu'elle permet de détecter un plus grand nombre de virus et de logiciels malveillants avec un nombre de signatures beaucoup plus petit.

Quels sont les avantages de la base virale compacte de Dr.Web et d'un nombre plus restreint de signatures pour l'utilisateur ?

- Economie de l'espace disque
- Préservation des ressources mémoires de l'ordinateur
- Préservation de la bande passante Internet lors du téléchargement des mises à jour
- Fourniture de bases de données virales rapides à installer
- Traitement rapide des informations lors de l'analyse
- Détection des virus à venir et basés sur la modification de virus existants

Système global de mises à jour de Dr.Web (Dr.Web GUS)

- Le système global de veille antivirale Dr.Web permet d'obtenir des échantillons de virus de tous les coins de la planète.
- Les mises à jour sortent dès la détection d'une nouvelle menace virale.
- Avant d'être mises à disposition, les nouvelles mises à jour sont testées sur un grand nombre de fichiers sains.
- Les mises à jour sont téléchargées depuis plusieurs serveurs se trouvant à différents endroits dans le monde entier, ce qui minimise le temps de leur réception. Les serveurs de mises à jour sont toujours accessibles.
- Le processus de mise à jour des bases virales et des composants du logiciel est complètement automatisé et transparent pour les utilisateurs et s'effectue via Internet, à la demande ou selon un horaire prédéfini.
- Les mises à jour sont disponibles en téléchargement sous forme d'archives.

Licences et Certificats

A la différence d'autres solutions, les composants de Dr.Web Enterprise Security Suite possèdent des certificats de conformité du FSTEC (Federal Service on Technical and Export Control) et du FSB (Federal Security Service). Cela signifie que cet ensemble peut être utilisé dans les organisations exigeant un niveau élevé de sécurité.

Dr.Web est certifié par le Ministère de la Défense de la Fédération de Russie.

Dr.Web est conforme aux exigences de la loi sur la protection des données personnelles relative aux produits antivirus. Il peut être installé sur des réseaux exigeant un niveau maximal de sécurité.

A ce jour, Doctor Web possède les licences et certifications suivantes :

- licences FSTEC sur l'accomplissement de travaux liés au développement d'outils de protection informatique et au développement et/ou à l'édition de moyens de protection de l'information confidentielle ;
- certification du Ministère de la Défense de Russie relative au développement des outils de protection informatique ;

  certification du FSB relative à l'activité liée à l'accès aux secrets d'Etat ;
- certification du centre de Certification, d'Attestation et de Protection des secrets d'Etat du FSB relative au développement et\ou à l'édition d'outils de protection informatique;
- certificats de conformité du FSB ;
- certificats de conformité du FSTEC.

Toute la certification de Doctor Web :

http://company.drweb.fr/licenses_and_certificates/

Certificat de licence Dr.Web


CERTIFICAT
d'authenticite

Dr.WEB®

Ce certificat atteste que ce logiciel est une licence légale Doctor Web, développeur et propriétaire en titre des produits de sécurité **Dr.WEB®**

Titulaire de la licence	
Produit	
Numéro de série Dr.Web Server Security Suite	
Numéro de série Dr.Web CureIt!	
Numéro de série Dr.Web CureNet!	
Objets protégés	
Postes de travail	Serveurs
Utilisateurs du courrier	Utilisateurs de la passerelle
Outils portables	Centre de gestion
Durée de la licence	Fournisseur

Doctor Web
B.Sharov, PDG

«Доктор Веб»
«Doctor Web, Ltd»

Le Certificat de licence Dr.Web est un document prouvant la légitimité d'utilisation du logiciel Dr.Web pour les organismes de contrôle.

IMPORTANT ! Le Certificat de licence Dr.Web ne peut pas servir à renouveler la licence ou à obtenir une remise de renouvellement.

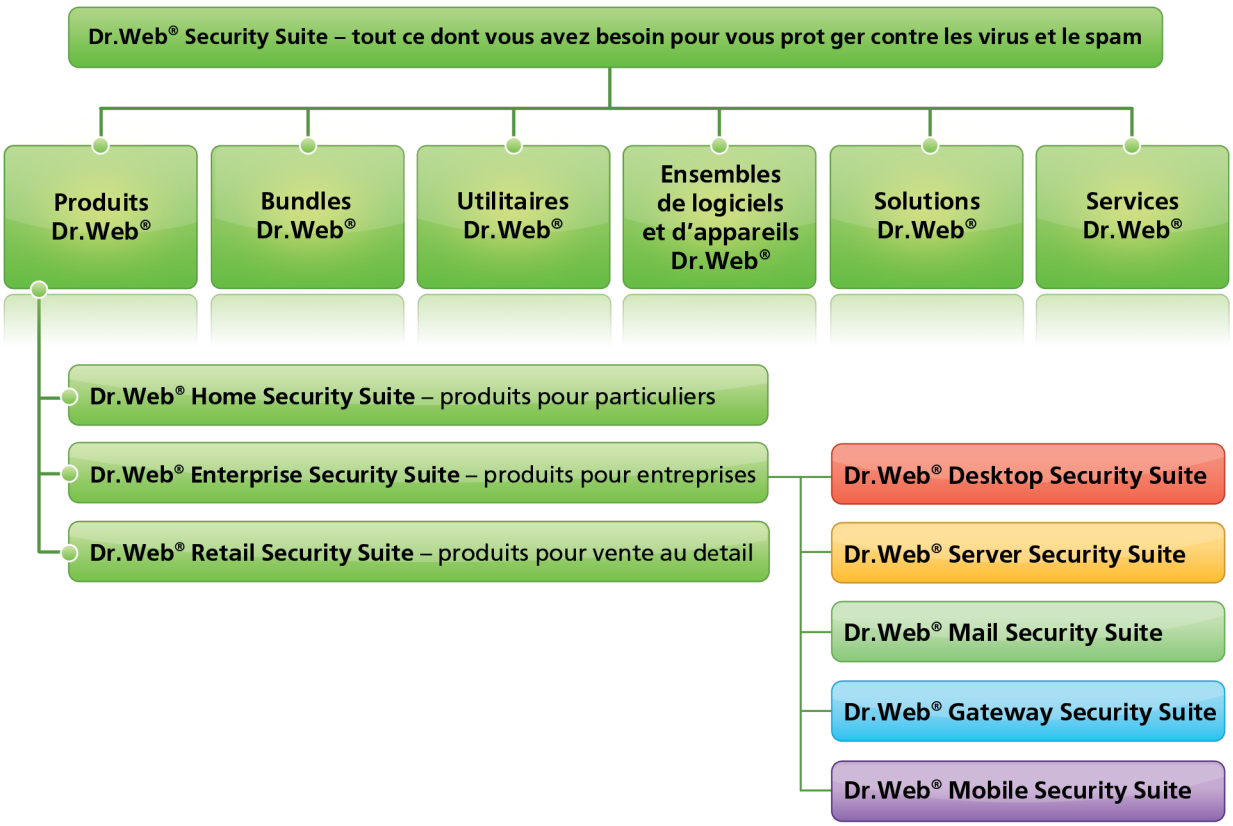
Ce Certificat est infalsifiable grâce à son treillis guilloché spécial.

La fourniture du Certificat de licence aux personnes morales, pour tous les produits Dr.Web, est obligatoire !

Vous pouvez générer vous-même la copie électronique du Certificat de Licence Dr.Web à la page http://products.drweb.fr/register/certificate/.

Gamme de produits Dr.Web Security Suite

La gamme de produits Dr.Web Security Suite se compose de produits pour particuliers et pour entreprises, de bundles, d'utilitaires, de solutions et de services.



Licensing des produits Dr.Web

1. Vous pouvez acheter une licence Dr.Web pour 12, 24 et 36 mois. Dr.Web Security Space et Dr.Web Antivirus pour Windows sont accessibles également pour 3 et 6 mois.
2. Les licences de Dr.Web sont fonction du nombre d'objets à protéger.
3. Les objets protégés sont:
   - Postes de travail, clients de terminal servers, clients de systèmes embarqués ;
   - Serveurs de fichiers et serveurs d'applications (y compris terminal servers) ;
   - Utilisateurs de messageries électroniques ;
   - Utilisateurs des passerelles de messagerie et des passerelles Internet ;
   - Appareils portables.
4. Deux types de **licences de base** sont prévus :
   1) Antivirus (muni d'un pare-feu) ;
   2) Protection complète.

5. La licence de base **Protection complète** est destinée seulement aux produits de protection des postes de travail.
6. La licence **Protection complète** comprend les composants suivants : antivirus, antispam, antivirus web, contrôle parental (utilisateurs particuliers), Office control (entreprises), pare-feu.
7. Si les utilisateurs ont besoin de composants supplémentaires, ils peuvent les ajouter à la licence de base. En revanche, l'achat d'un ou de plusieurs composants supplémentaires est impossible si vous n'avez pas de licence de base.
8. A chaque type d'objet protégé, correspond un type de licence et un jeu de composants supplémentaires.

Objets protégés	OS et plateformes supportés	Licence de base	Composants supplémentaires
Dr.Web Desktop Security Suite Protection des postes de travail, des clients de serveurs virtuels et terminal server ainsi que des systèmes embarqués.	Windows 8.1/8/7/Vista/XP	Protection complète	■ Centre de gestion
	Linux glibc 2.7 ou supérieur	Antivirus	■ Centre de gestion
	OS X 10.7 ou supérieur		
	MS-DOS OS/2		
Dr.Web Server Security Suite La protection des serveurs de fichiers et des serveurs d'applications (y compris terminal server et serveurs virtuels)	Windows	Antivirus	■ Centre de gestion
	Novell NetWare		
	OS X Server		
	UNIX (Samba)		
Dr.Web Mail Security Suite Protection de la messagerie	UNIX MS Exchange	Antivirus	■ Centre de gestion ■ Antispam ■ SMTP proxy
	Lotus (Windows/Linux)		■ Antispam ■ SMTP proxy
	Kerio (Windows/Linux)		■ SMTP proxy
Dr.Web Gateway Security Suite Protection pour les passerelles	Les passerelles Internet Kerio (Windows/Linux) Les passerelles Internet UNIX	Antivirus	■ Centre de gestion
	Qbik WinGate		■ Antispam
	MIMEsweeper		
	Microsoft ISA Server et Forefront TMG		
Dr.Web Mobile Security Suite Protection pour les appareils mobiles	Android 2.1 ou supérieur	Protection complète	■ Antispam ■ Centre de gestion
	Windows Mobile	Antivirus	■ Antispam
	Symbian OS		

Modes de fourniture des produits Dr.Web

Les produits Dr.Web sont fournis sous forme de licences électroniques ou sous forme de packages média.

1. Licence en ligne de Dr.Web

Fournie sous forme d'un numéro de série Dr.Web :

- Via email ;
- Sur le certificat de licence.

2. Package média Dr.Web

Fourniture :

- Boîte avec label de Doctor Web ;
- Certificat de licence ;
- Guide d'installation et d'enregistrement ;
- CD/DVD dans une enveloppe;
- Etiquette adhésive ;
- Etiquette « Protégé par Dr.Web » ;
- Clé USB (seulement pour le produit Dr.Web pour OS X + Dr.Web Security Space).

3. Solution Dr.Web en boîte

Solution pour un ou plusieurs produits Dr.Web Enterprise Security Suite.

Fourniture :

- Boîte avec le label Dr.Web ;
- Formulaire du Contrat de licence ;
- DVD avec les fichiers d'installation des logiciels Dr.Web dans une enveloppe avec le label de Dr.Web.

5. Package de licence Dr.Web

Solution pour un ou plusieurs produits Dr.Web Enterprise Security Suite.

Fourniture :

- Boîte avec le label de Dr.Web ;
- Formulaire du Contrat de licence.

6. Carte scratch

avec le numéro de série de Dr.Web, caché sous la bande scratch.

7. Fourniture des licences OEM de Dr.Web

Produits OEM de Dr.Web

Cartes OEM avec une bande scratch

Dr.Web Security Space

1 PC/3 mois

- Carte OEM avec une bande scratch, collée sur un flyer OEM.

  Il est possible de fabriquer des cartes OEM avec le logo du partenaire. Quantité minimale de cartes co-brandées – 250.

  Fourniture

  La fourniture de Dr.Web OEM Universel pour les partenaires Dr.Web est effectuée sous la forme de 250 cartes et plus. La fourniture des éléments (cartes et licence électronique) n'est possible que pour les entreprises ayant le statut de Partenaire certifié (en savoir plus sur ce programme http://partners.drweb.com/service).

Il existe un programme de renouvellement des licences OEM pour les partenaires :
https://pa.drweb.com/products/oem/universal/protection/

Liens utiles

https://st.drweb.com/static/new-www/files/Pamyatka_OEM_fr.pdf

Dr.Web Home Security Suite. Produits pour particuliers

Composition des produits

Dr.Web Security Space	Dr.Web Mobile Security
Protection des appareils mobiles et des ordinateurs	Protection pour les appareils mobiles
Les logiciels Dr.Web	
■ Dr.Web Security Space ■ Dr.Web Antivirus pour Windows ■ Dr.Web Antivirus pour OS X ■ Dr.Web Antivirus pour Linux	–
■ Dr.Web pour Android ■ Dr.Web pour Symbian ■ Dr.Web pour Windows Mobile	■ Dr.Web pour Android ■ Dr.Web pour Symbian ■ Dr.Web pour Windows Mobile

Composants de protection Dr.Web Security Space

Composants de protection	Windows	OS X	Linux
Antivirus	+	+	+
Antispam	+		
Filtre du trafic web	+	+	
Contrôle parental	+		
Pare-feu	+		
Réseau antivirus	+		
Services pour Windows			
Protection contre la perte de données (sauvegardes)	+		
Dr.Web Cloud	+		
Blocage des supports amovibles	+		

Licensing Dr.Web Security Space

1. Le produit est soumis à licence par nombre de PC protégés (1 – 5).
2. Types de licence Protection complète.
3. Durée des licences commerciales : 3, 6, 12, 24 ou 36 mois. Durée des licences OEM : 3 ou 6 mois.
4. Les remises de renouvellement sont standards.
5. Pas d'autres remises disponibles.
6. Les acheteurs de ce produit peuvent utiliser gratuitement Dr.Web Mobile Security Suite. Le nombre d'appareils mobiles protégés correspond au nombre d'ordinateurs protégés.

Extension de la licence (achat supplémentaire)

1. Pour étendre la licence Dr.Web Security Space il faut : a) migrer de Dr.Web Antivirus vers Dr.Web Security Space ou b) augmenter le nombre d'objets protégés.

2. La licence d'achat supplémentaire est automatiquement activée lors de sa génération, avec les données spécifiées lors de l'enregistrement de la licence précédente.
3. Si la durée de la licence **dépasse 3 mois**, le prix de l'extension est égal à celui de la licence de renouvellement. Le code de cette licence est D. La licence est renouvelée automatiquement.
4. Si la durée de la licence **ne dépasse pas 3 mois** :
   - l'extension de la licence est gratuite via le service d'extension de licence;
   - La licence précédente sera bloquée dans 24 heures après la génération de la nouvelle ;
   - Le code de la nouvelle licence est C, et le prix de cette licence est zéro. Le client pourra ensuite renouveler cette licence avec une remise.

Dr.Web Security Space

Protection complète pour Windows, Dr.Web Antivirus pour OS X et Linux

- Solution complète pour la protection des ordinateurs sous Windows.
- Protection en ligne.
- Possibilité d'installation et du fonctionnement sur une machine infectée et une résistance exceptionnelle aux virus.
- Détection efficace et le nettoyage du système de tous les types de menaces.
- Haute vitesse du scan grâce à l'utilisation des possibilités de systèmes multi-processeurs.
- Nouveau ! Protection contre les menaces, conçues d'être indétectables par les moyens de l'analyse heuristique ou basés sur les signatures.
- Nouveau ! La protection des données contre les dommages.
- Nouveau ! Analyseur de menaces empaquetées.
- Analyse complète des archives quel que soit le niveau d'emboîtement.
- Détection et neutralisation des virus complexes améliorée.
- Filtrage de spam et de touts les messages non-sollicités sans la nécessité de l'apprentissage de l''antispam.
- Nouveau ! Scan complet « à la volée » de tout le trafic transitant via tous les ports.
- Nouveau ! Naviguez sur Internet en toute sécurité : Si l'utilisateur surfe via les moteurs de recherche Google, Yandex, Yahoo!, Bing, Rambler, le contenu non sécurisé est filtré par les moteurs de recherche mêmes grâce à la fonctionnalité Safe Search !
- Nouveau ! Communication sécurisée : le filtrage du trafic dans les clients IM.
- La protection efficace des enfants contre les contenus inappropriés.
- Protection contre l'utilisation non-autorisée des supports amovibles et de l'ordinateur.
- Service Dr.Web Cloud pour analyser les URL aux serveurs de Doctor Web.
- Protection contre l'accès non autorisés, prévention de fuites des données, blocage des connexions suspects au niveau des paquets et applications.
- Administration distant des ordinateurs appartenant à un réseau local, sans installer le Centre de Gestion Dr.Web.

Composants de protection

Détection efficace et neutralisation de tous types de menaces dans le système (Scanner Dr.Web)

- Haute vitesse de scan grâce à l'utilisation de systèmes multiprocesseurs.

- Le scan antivirus rapide et complet de la mémoire vive, des secteurs d'amorçage, des disques durs et supports amovibles.
- Neutralisation uniquement des menaces opérationnelles.
- Détection des logiciels espions potentiellement dangereux, des adwares, outils de piratage et jokes en utilisant la base virale.
- L'Antirootkit Dr.Web Shield™, faisant partie du scanner, détecte les virus complexes utilisant les technologies rootkit et capables de dissimuler leur présence dans le système infecté.
- Dr.Web Console Scanner est conçu pour les utilisateurs expérimentés et permet d'effectuer une analyse en ligne de commande. Il prévoit une configuration élargie y compris dans les systèmes multiprocesseurs.

Protection en temps réel (moniteur de fichiers SpIDer Guard)

- Le moniteur de fichiers SpIDer Guard assure la surveillance continue de la santé de l'ordinateur. Interception à la volée des requêtes aux fichiers sur les disques durs, lecteurs CD/DVD/Blu-ray, cartes flash et à puce.
- Haute résistance aux tentatives de perturber le fonctionnement de SpIDer Guard ou de l'arrêter.
- Les technologies du noyau antivirus Dr.Web permettent de contrôler la charge sur les ressources du système tout en assurant une protection efficace.
- Hautes performances sur les machines traitant des flux de fichiers importants (en cas d'utilisation intensive de systèmes de fichiers, par exemple, lors du téléchargement de fichiers à partir de trackers torrent, compilation et rendering).

Protection contre les menaces inconnues (Protection préventive)

- **FLY-CODE** une technologie unique de décompression permettant de détecter les virus compressés même par des méthodes inconnues de Dr.Web.
- La technologie unique **Origins Tracing**™ de détection non basée sur les signatures permet à Dr.Web de détecter les virus inconnus de la base virale Dr.Web.
- **Le moteur d'analyse heuristique de Dr.Web** dont l'analyse se fonde sur des caractéristiques typiques de différents groupes de malwares, détecte la plupart des menaces connues.
- **Dr.Web Process Heuristic** fournit une protection contre les nouveaux programmes malveillants conçus pour éviter d'être détectés par les mécanismes traditionnels basés sur l'analyse par signature ou par l'analyse heuristique classique, qui n'ont par conséquent pas encore été analysés par le Laboratoire, et ne sont pas répertoriés dans la base de données virales Dr.Web au moment de leur intrusion dans le système. Le module analyse le comportement du malware et s'il conclut à sa nocivité, la menace est neutralisée. La nouvelle technologie de protection des données contre l'endommagement permet de minimiser les pertes liées à l'activité d'un virus inconnu.
- **L'analyse complète des menaces empaquetées** améliore considérablement la détection des soi-disant « nouvelles menaces », connues de la base virale Dr.Web mais dissimulées sous de nouveaux packers. Elle permet d'éviter l'ajout de nombreuses nouvelles entrées à la base virale. La compacité des bases virales Dr.Web permet de ne pas modifier constamment les pré-requis système et assure une compacité des mises à jour, tout en gardant la même qualité de détection et de désinfection.

Le filtrage du trafic Internet (Antivirus Web SpIDer Gate)

- Antivirus Web SpIDer Gate scanne en temps réel le trafic HTTP entrant et sortant, intercepte toutes les connexions HTTP, filtre les données, bloque automatiquement les pages infectées dans tous les navigateurs web, vérifie les fichiers dans les archives, protège contre les sites dangereux et de phishing.
- Trafic internet sécurisé : tout le trafic est analysé via tous les ports selon les protocoles pris en charge par Dr.Web, y compris les protocoles sécurisés (si l'utilisateur a activé SSL).
- Naviguez sur Internet en toute sécurité : Si l'utilisateur surfe via les moteurs de recherche Google, Yandex, Yahoo!, Bing, Rambler, seuls les sites web qui ne sont pas dangereux selon l'estimation

des moteurs de recherche et de Dr.Web seront affichés dans les résultats. Ceci grâce à la fonctionnalité Safe Search : le contenu non sécurisé est filtré par les moteurs de recherche eux-mêmes !

- Communication sécurisée : le filtrage du trafic dans les clients IM tels que Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin et autres. Les liens redirigeant vers des sites malveillants et/ou de phishing sont ôtés des messages. Les pièces jointes sont analysées afin que le transfert de pièces jointes potentiellement dangereuses soit bloqué.
- L'analyse des connexions sécurisées SSL (HTTPS).
- Le blocage de sites Internet selon la base de données de sites non recommandés ou de sites sources de virus.
- Base de données des sites web diffusant des contenus non autorisés — protection des copyrights.
- Possibilité de désactiver l'analyse du trafic entrant ou sortant, ainsi que de créer une liste d'applications dont le trafic HTTP sera toujours complètement analysé (liste noire). Il existe aussi la possibilité d'exclure de l'analyse le trafic de certaines applications (liste blanche).
- Réglage de la priorité du scan du trafic (équilibrage du scan). Cet équilibrage affecte les performances du processeur et la vitesse de la connexion Internet.
- Le fonctionnement de SpIDer Gate ne dépend pas du navigateur utilisé.
- Son fonctionnement n'affecte pas les performances du PC ni la vitesse de connexion Internet ou de la transmission de données.
- Par défaut, le composant ne nécessite pas de réglages : SpIDer Gate commence le scan dès son installation dans le système.
- Vérification des URL sur les serveurs de Doctor Web via le service Dr.Web Cloud. Lorsque l'utilisateur souhaite visiter des sites web, les URL correspondantes sont envoyées pour analyse aux serveurs de Doctor Web. La vérification est effectuée en temps réel, indépendamment de l'état des bases virales Dr.Web sur l'ordinateur de l'utilisateur et des paramètres de mises à jour.

La messagerie sans virus, spam ni messages indésirables (Moniteur antivirus SpIDer Mail™ + Antispam)

- Tout le trafic est analysé via tous les ports selon les protocoles pris en charge par Dr.Web, y compris les protocoles sécurisés (si l'utilisateur a activé SSL).
- Le moniteur SpIDer Mail analyse les emails avant qu'ils ne soient traités par le client de messagerie et ne permet pas aux malwares — qui se propagent via le spam — de profiter des vulnérabilités des logiciels.
- La vérification des emails en temps réel via les protocoles SMTP/POP3/NNTP/IMAP4.
- L'analyse des connexions sécurisées SSL (SMTPS/POP3S/IMAP4S).
- L'analyse n'affecte pas la vitesse du client de messagerie et n'augmente pas le délai de réception des emails.
- Chaque type de programme malveillant est traité de façon individuelle : les virus, les logiciels potentiellement dangereux, les logiciels publicitaires, les utilitaires pirates, dialers, canulars.
- L'Analyse de la composition du message et de la durée de l'envoi des messages sortants permet de détecter une activité virale et de protéger ainsi contre les envois massifs effectués par des vers de courrier.

Antispam

- L'Antispam n'exige pas de paramétrage et fonctionne dès la réception du premier message.
- Différentes technologies de filtrage assurent une reconnaissance efficace du spam, des messages de phishing, pharming, scamming et bounce.
- Vous ne ferez pas partie de botnets et votre fournisseur de service ne refusera pas de travailler avec vous en vous considérant comme spammeur.
- Les messages considérés comme non-sollicités sont placés dans un dossier spécial de votre messagerie où vous pouvez les consulter quand vous voulez.

- Le module d'analyse du spam est absolument autonome, il n'a pas besoin de connexion au serveur ou à la base de données, ce qui permet d'économiser le trafic Internet.

Protection des enfants et des proches. Le contrôle de la navigation sur Internet et le blocage de l'accès à certaines ressources (Contrôle parental Dr.Web)

Trafic Internet sécurisé

- Vérification de tout le trafic transitant via tous les ports.
- Vérification des URL en temps réel sur les serveurs de Doctor Web via le service Dr.Web Cloud — indépendamment de l'état des bases de données virales Dr.Web sur l'ordinateur et des paramètres de mises à jour.
- Blocages des sites web selon 10 groupes thématiques (armement, drogues, jeux, pornographie etc.).
- Protection de vos enfants contre les sites indésirables.

Limitation de l'accès au PC et aux ressources Internet

- Restriction du temps de navigation sur Internet et du temps d'utilisation du PC.
- Une option permet de bloquer le changement de l'heure système et le fuseau horaire afin d'éviter que les enfants utilisent l'ordinateur durant les heures non autorisées par les parents.

Le blocage de l'accès aux fichiers et dossiers

- La prévention du vol et/ou de la suppression de données sensibles grâce à l'interdiction d'utilisation de certains fichiers et dossiers.

En plus.

- Les profils du Contrôle parental pour chaque utilisateur.

Le blocage des appareils afin d'éliminer toutes les voies de pénétration des menaces

- Limitation de l'accès aux appareils — supports amovibles, lecteurs DVD/CD-ROM, clavier, souris, cartes réseau, outils vidéo et audio, consoles de jeux, appareils USB, ports COM/LPT.
- La prévention du vol et/ou de la suppression de données sensibles grâce à l'interdiction d'utilisation des supports amovibles (clés USB, dispositifs USB), des dispositifs réseau ou de certains fichiers et dossiers.
- Les listes blanches des périphériques de confiance protègent contre la connexion non autorisée de périphériques amovibles à l'ordinateur protégé par Dr.Web. Les données confidentielles sont protégées contre le vol via des lecteurs flash USB qui sont souvent utilisés pour l'intrusion de virus dans le système.
- Export/import de listes blanches.
- Blocage de l'envoi de tâches d'impression : protection contre l'impression non autorisée de documents confidentiels ou diminution de la consommation de papier.

Protection contre les attaques réseau (pare-feu Dr.Web)

- Protection contre l'accès non autorisé, prévention des fuites de données, blocage des connexions suspectes au niveau des paquets et des applications.
- Le Pare-feu Dr.Web utilise sa propre base de données des applications de confiance. L'application est considérée comme application de confiance d'après son certificat numérique : tous les programmes légitimes du point de vue de Dr.Web sont autorisés à se connecter à n'importe quelle adresse via n'importe quel port. Exception : Si l'application ne possède pas de signature valide, ou qu'il n'y a pas de signature (application open source par exemple), une requête pour la création d'une règle sera affichée.
- Le contrôle des connexions au niveau des applications permet de contrôler l'accès des applications ou processus aux ressources réseau et d'enregistrer cette activité dans les logs des applications.

- Le filtrage au niveau des paquets permet de contrôler l'accès à Internet quelle que soit l'application qui a initié la connexion. Le log du filtre des paquets enregistre des informations sur les paquets transmis via les interfaces réseau.
- En mode jeu, en plein écran, les notifications de l'antivirus s'affichent « par-dessus » toute application en cours d'exécution.
- Surveillance des applications utilisant le réseau en temps réel avec une option permettant de forcer l'arrêt de la connexion.

La gestion de la protection de tous les ordinateurs de votre famille (Réseau antivirus)

- Le Réseau antivirus permet une gestion et une configuration des antivirus Dr.Web dans le même réseau local.
- L'installation du Centre de gestion n'est pas nécessaire.
- La connexion peut être établie depuis tout ordinateur du réseau.
- La gestion prévoit : la possibilité d'obtenir les statistiques et les logs, de voir et de modifier les configurations des modules, de lancer ou d'arrêter les modules depuis un poste de travail distant. Il est également possible d'enregistrer ou remplacer le numéro de série sur le poste de travail distant.
- Il est nécessaire d'activer un accès distant sur le poste.

Pré-requis système

Pour Dr.Web Security Space

- Windows 8/7/Vista (64- bits) et Windows 8/7/Vista/XP SP2 (32- bits). Espace libre sur le disque dur: ~550 Mb. Les fichiers temporaires durant l'installation demanderont plus de place. 7 Mb supplémentaires sont nécessaires pour l'installation du pare-feu.

Supplémentaire: un accès Internet est nécessaire pour s'enregistrer et mettre à jour l'antivirus.

Licences

Type de licence

- Nombre de postes de travail protégés.

Licence

- Protection complète

Description : http://products.drweb.fr/win/security_space/

Dr.Web Antivirus pour Windows

NOUVELLE VERSION

Protection standard contre les programmes malveillants pour Windows, OS X, Linux

- Solution complète pour la protection de l'ordinateur sous Windows.
- Protection en ligne.
- Possibilité d'installation et du fonctionnement sur une machine infectée et une résistance exceptionnelle aux virus.
- Détection efficace et le nettoyage du système de tous les types de menaces.
- Haute vitesse du scan grâce à l'utilisation des possibilités de systèmes multi-processeurs.
- Nouveau ! Protection contre les menaces, conçues d'être indétectables par les moyens de l'analyse heuristique ou basés sur les signatures.
- Nouveau ! Analyseur de menaces empaquetées.
- Analyse complète des archives quel que soit le niveau d'emboîtement.
- Détection et neutralisation des virus complexes améliorée.
- Nouveau ! Scan complet « à la volée » de tout le trafic transitant via tous les ports.
- Protection contre l'accès non autorisés, prévention de fuites des données, blocage des connexions suspects au niveau des paquets et applications.

Composants de la protections

Détection efficace et neutralisation de tous types de menaces dans le système (Scanner Dr.Web)

- Haute vitesse de scan grâce à l'utilisation de systèmes multiprocesseurs.
- Le scan antivirus rapide et complet de la mémoire vive, des secteurs d'amorçage, des disques durs et supports amovibles.
- Neutralisation uniquement des menaces opérationnelles.
- Détection des logiciels espions potentiellement dangereux, des adwares, outils de piratage et jokes en utilisant la base virale.
- L'Antirootkit Dr.Web Shield™, faisant partie du scanner, détecte les virus complexes utilisant les technologies rootkit et capables de dissimuler leur présence dans le système infecté.
- Dr.Web Console Scanner est conçu pour les utilisateurs expérimentés et permet d'effectuer une analyse en ligne de commande. Il prévoit une configuration élargie y compris dans les systèmes multiprocesseurs.

Protection en temps réel (moniteur de fichiers SpIDer Guard)

- Le moniteur de fichiers SpIDer Guard assure la surveillance continue de la santé de l'ordinateur. Interception à la volée des requêtes aux fichiers sur les disques durs, lecteurs CD/DVD/Blu-ray, cartes flash et à puce.
- Haute résistance aux tentatives de perturber le fonctionnement de SpIDer Guard ou de l'arrêter.
- Les technologies du noyau antivirus Dr.Web permettent de contrôler la charge sur les ressources du système tout en assurant une protection efficace.
- Hautes performances sur les machines traitant des flux de fichiers importants (en cas d'utilisation intensive de systèmes de fichiers, par exemple, lors du téléchargement de fichiers à partir de trackers torrent, compilation et rendering).

Protection contre les menaces inconnues (Protection préventive)

- **FLY-CODE** une technologie unique de décompression permettant de détecter les virus compressés même par des méthodes inconnues de Dr.Web.

- La technologie unique **Origins Tracing™ de détection non basée sur les signatures** permet à Dr Web de détecter les virus inconnus de la base virale Dr.Web.
- **Le moteur d'analyse heuristique de Dr.Web** dont l'analyse se fonde sur des caractéristiques typiques de différents groupes de malwares, détecte la plupart des menaces connues.
- **Dr.Web Process Heuristic** fournit une protection contre les nouveaux programmes malveillants conçus pour éviter d'être détectés par les mécanismes traditionnels basés sur l'analyse par signature ou par l'analyse heuristique classique, qui n'ont par conséquent pas encore été analysés par le Laboratoire, et ne sont pas répertoriés dans la base de données virales Dr.Web au moment de leur intrusion dans le système. Le module analyse le comportement du malware et s'il conclut à sa nocivité, la menace est neutralisée. La nouvelle technologie de protection des données contre l'endommagement permet de minimiser les pertes liées à l'activité d'un virus inconnu.
- **L'analyse complète des menaces empaquetées** améliore considérablement la détection des soi-disant « nouvelles menaces », connues de la base virale Dr.Web mais dissimulées sous de nouveaux packers. Elle permet d'éviter l'ajout de nombreuses nouvelles entrées à la base virale. La compacité des bases virales Dr.Web permet de ne pas modifier constamment les pré-requis système et assure une compacité des mises à jour, tout en gardant la même qualité de détection et de désinfection.

La messagerie sans virus (Moniteur antivirus SpIDer Mail ™)

- Tout le trafic est analysé via tous les ports selon les protocoles pris en charge par Dr.Web, y compris les protocoles sécurisés (si l'utilisateur a activé SSL).
- Le moniteur SpIDer Mail analyse les emails avant qu'ils ne soient traités par le client de messagerie et ne permet pas aux malwares - qui se propagent via le spam - de profiter des vulnérabilités des logiciels.
- La vérification des emails en temps réel via les protocoles SMTP/POP3/NNTP/IMAP4.
- L'analyse des connexions sécurisées SSL (SMTPS/POP3S/IMAP4S).
- L'analyse n'affecte pas la vitesse du client de messagerie et n'augmente pas le délai de réception des emails.
- Chaque type de programme malveillant est traité de façon individuelle : les virus, les logiciels potentiellement dangereux, les logiciels publicitaires, les utilitaires pirates, dialers, canulars.
- L'Analyse de la composition du message et de la durée de l'envoi des messages sortants permet de détecter une activité virale et de protéger ainsi contre les envois massifs effectués par des vers de courrier.

Protection contre les attaques réseau (pare-feu Dr.Web)

- Protection contre l'accès non autorisé, prévention des fuites de données, blocage des connexions suspectes au niveau des paquets et des applications.
- Le Pare-feu Dr.Web utilise sa propre base de données des applications de confiance. L'application est considérée comme application de confiance d'après son certificat numérique : tous les programmes légitimes du point de vue de Dr.Web sont autorisés à se connecter à n'importe quelle adresse via n'importe quel port. Exception : Si l'application ne possède pas de signature valide, ou qu'il n'y a pas de signature (application open source par exemple), une requête pour la création d'une règle sera affichée.
- Le contrôle des connexions au niveau des applications permet de contrôler l'accès des applications ou processus aux ressources réseau et d'enregistrer cette activité dans les logs des applications.
- Le filtrage au niveau des paquets permet de contrôler l'accès à Internet quelle que soit l'application qui a initié la connexion. Le log du filtre des paquets enregistre des informations sur les paquets transmis via les interfaces réseau.
- En mode jeu, en plein écran, les notifications de l'antivirus s'affichent « par-dessus » toute application en cours d'exécution.
- Surveillance des applications utilisant le réseau en temps réel avec une option permettant de forcer l'arrêt de la connexion.

Pré-requis système

- Intel® Pentium® IV à 1,6 GHz.
- 512 Mo de RAM Les fichiers temporaires créés lors de l'installation nécessitent de l'espace supplémentaire.
- 330 Mo d'espace libre sur le disque
- Windows 2012/8/7/2008/Vista/2003/XP/SP 2 (32 et 64-bits)
- OS X 10.7 et plus (32- et 64- bits).
- Linux 2.6 et plus (32- et 64- bits).

Supplémentaire: un accès Internet est nécessaire pour s'enregistrer et mettre à jour l'antivirus.

Licences

Types de licence

- Nombre de postes de travail à protéger

Licences possibles

- Antivirus (licence contient les composants suivants : antivirus, antiespion, antirootkit, pare-feu)

Liens utiles

Description : http://products.drweb.fr/win/

Migration vers la version avec un pare-feu : http://promotions.drweb.fr/upgrade/security_space

Dr.Web Antivirus pour OS X

NOUVELLE VERSION

Protection contre les logiciels malveillants créés pour infecter non seulement OS X, mais aussi pour d'autres systèmes d'exploitation.

Ce produit est inclu dans les licences Dr.Web Security Space et Dr.Web Antivirus.

Fonctionnalités

- Scan des objets d'auto-démarrage, des supports amovibles, des disques logiques et réseau, des différents formats d'e-mail, des fichiers et dossiers, y compris ceux compressés.
- Sélectionnez le type d'analyse: rapide, complète ou sélective.
- Scan antivirus à la demande, automatique ou selon une planification.
- Protection des paramètres du moniteur SpIDer Guard® avec un mot de passe contre des modifications non autorisées
- Application d'actions aux objets contaminés, suspects, et objets d'autre type y compris le traitement, déplacement en quarantaine et suppression, même si l'action sélectionnée précédemment est impossible à effectuer.
- Exclusion de fichiers (et du chemin vers ces fichiers) à la demande de l'utilisateur.
- Détection et suppression des virus masqués sous des packers inconnus.
- Journalisation de l'heure des événements, des objets analysés et du type d'action appliquée.
- Les nouveautés de la version 10 ! L'antivirus Web Dr.Web SpIDer Gate® – l'analyse du trafic HTTP et le contrôle d'accès aux ressources Internet.
- Les nouveautés de la version 10 ! Protection contre les tentatives de visiter des pages indésirables (violence, jeux de hasard etc).
- Téléchargement des mises à jour automatiquement (selon une planification) ou à la demande.
- Notifications automatiques (y compris sonores) sur la détection de virus.
- Isolation des fichiers contaminés en quarantaine avec la possibilité de spécifier la durée de stockage des objets en quarantaine et de paramétrer sa taille maximale.
- Traitement, restauration ou suppression des objets placés en quarantaine.
- Journalisation détaillée du fonctionnement.
- Disponibilité des modules sous la forme d'utilitaires dans l'interface en ligne de commande, avec la possibilité de les intégrer aux Apple Scripts.

Pré-requis système

Dr.Web Antivirus pour OS X

- OS X 10.7 ou supérieur.
- RAM – selon les pré-requis système.
- Une connexion Internet est nécessaire : pour l'enregistrement et les mises à jour.

Liens utiles

Description : http://products.drweb.fr/mac/

Dr.Web Antivirus pour Linux

Protection de base contre les virus

Fonctions clés

- Détection et neutralisation des virus et des objets malveillants sur les disques durs et les supports de données amovibles.
- Détection des virus dans les archives de tout niveau de complexité et à l'intérieur des objets empaquetés.
- Contrôle des fichiers compressés par des outils même inconnus, à l'aide de la technologie FLY-CODE™.
- Protection contre les menaces inconues à l'aide des technologies de recherche sans signatures Origins Tracing™ et du moteur d'analyse heuristique Dr.Web.
- Différents types d'analyse : rapide, complète, sélective ou selon le paramétrage des utilisateurs.
- Surveillance continue de la santé de l'ordinateur – une interception instantanée de toutes les requêtes vers les fichiers situés sur les disques, les disquettes et les lecteurs CD/DVD/ Blue-ray, les cartes Flash et smart.
- Protection des composants de l'antivirus contre les tentatives des logiciels malveillants d'empêcher leur fonctionnement.
- Isolement des fichiers contaminés et des autres objets suspects en quarantaine ; restauration des fichiers se trouvant en quarantaine. Fonction de réduction de la taille de la quarantaine.
- Collecte de toutes les statistiques sur le fonctionnement de l'antivirus.
- Mise à jour automatique des bases virales Dr.Web sur demande d'après des horaires déterminés.

Avantages

- Centre de gestion convivial
- Analyse « à la volée »
- Paramétrage des scans utilisateurs
- Quarantaine gérée
- Mises à jour automatiques
- Interface moderne

Pré-requis système

- Système d'exploitation : Distributions GNU/Linux, avec la version du noyau 2.6.37.(ou supérieurs) et Intel x86/amd64 utilisant la bibliothèque glibc en version 2.13 (et supérieurs)
- 512 Mo d'espace libre sur le disque
- Connexion Internet pour l'enregistrement et les mises à jour.

Liens utiles

Description : http://products.drweb.fr/linux/

10.06.2016

Scanners en ligne de commande Dr.Web

Protection antivirale aux fonctionnalités d'automatisation élargies pour les utilisateurs expérimentés.

Les scanners en ligne de commande Dr.Web sans interface graphique utilisent une base virale commune et le module de recherche Dr.Web et sont destinés à fonctionner sous les systèmes d'exploitation MS DOS, OS/2 et Windows. Pour gérer la protection antivirale, il est nécessaire de savoir utiliser la ligne de commande.

Avantages

- Pré-requis système minimaux – les scanners fonctionnent même sur des systèmes embarqués et sont capables de protéger les ordinateurs peu performants d'anciennes générations.
- Facilité d'analyse : l'administrateur peut sélectionner un scan « à la main » ou bien une analyse d'après un horaire défini.
- Désinfection des postes de travail et des serveurs contaminés, même ceux qui sont inaccessibles depuis le réseau.
- Haut niveau de résistance aux virus et possibilité d'installation sur un ordinateur contaminé.
- Automatisation de tâches quotidiennes avec utilisation de riches capacités de la ligne de commande.
- Elimination ou mise en quarantaine des virus inconnus de Dr.Web.
- Démarrage depuis tout support amovible (disque ou clé USB).

Liens utiles

Description : http://products.drweb.fr/console/

Dr.Web Mobile Security

Protection pour les appareils mobiles

Composants de protection de Dr.Web Mobile Security

Composants de protection	Android	Symbian	Windows Mobile
Antivirus	+	+	+
Antispam	+	+	+
Antivol	+		
Cloud Checker	+		
Pare-feu	+		
Contrôleur de sécurité	+		

Licenze di Dr.Web Mobile Security

1. Le produit est soumis à licence par nombre d'appareils mobiles protégés (1 – 5).
2. Durée des licences commerciales : 6, 12, 24 ou 36 mois. Durée des licences OEM : 3 ou 6 mois.
3. Aucune remise disponible, y compris celle de renouvellement. Si vous voulez continuer à utiliser le produit après l'expiration de la licence ou que vous souhaitez augmenter le nombre d'appareils protégés (achat supplémentaire), vous devez acheter une nouvelle licence sans remise.

Dr.Web pour Android

Fonctionnalités et avantages

- Le scan rapide ou complet du système de fichiers, ainsi que l'analyse de fichiers et dossiers sur demande de l'utilisateur.
- L'analyse du système de fichiers en temps réel par le moniteur SpIDer Guard lors de la sauvegarde de fichiers en mémoire.
- La détection de nouvelles menaces grâce à la technologie unique Origins Tracing™.
- La protection de la carte SD contre l'infection par des fichiers autorun et Exploit.Cpllnk, qui représentent un danger pour Windows.
- Le placement de menaces détectées en Quarantaine avec la possibilité de restaurer les fichiers.
- Impact minimal sur la vitesse du système d'exploitation.
- Une utilisation modérée de la batterie.
- Des mises à jour de la base virale de petite taille pour économiser le trafic, ce qui est très important pour les utilisateurs qui ont un accès Internet limité.
- Des statistiques détaillées sur les actions de l'antivirus.
- Des Widgets de bureau commodes et informatifs pour accéder à l'application.

L'Antispam

La protection contre les messages et les appels non sollicités.

- Plusieurs modes de filtrage des appels et des messages.
- Possibilité de créer son propre profil de filtrage.
- La modification de la liste black (les numéros de la part desquels les messages et appels sont bloqués).
- Affichage des appels et messages bloqués.

Antivol

Antivol permettra de trouver le mobile en cas de vol ou de perte et de supprimer à distance les données confidentielles.

- Bloquer le mobile après le redémarrage.
- Bloquer le téléphone et exiger un mot de passe (le nombre d'erreurs possibles est limité).
- Déblocage via SMS.
- Obtenir les coordonnées GPS du mobile en recevant un lien sur Google Maps.
- Suppression des données sur le téléphone et sur la carte SD à distance.
- Activation d'un signal sonore fort et blocage de l'écran.
- Possibilité d'entrer son propre texte qui sera affiché sur l'écran du mobile s'il est bloqué.
- Possibilité de créer une liste des personnes proches qui recevront des notifications en cas de changement de carte SIM sur le mobile perdu. Depuis ces numéros de téléphone, vous pourrez gérer l'Antivol, notamment débloquer le mobile si vous avez oublié le mot de passe de déblocage.

Filtre URL Cloud Checker

Le service Cloud Checker permet de restreindre les visites sur les pages non-sollicitées. L'accès aux ressources potentiellement dangereuses sera bloqué selon les catégories suivantes :

- Drogues.
- Sources connues de virus.
- Grossièretés.
- Terrorisme.
- Violences.
- Armes.
- Sites pour les adultes etc.

Contrôleur de sécurité

- Analyse le système afin de détecter les problèmes de sécurité et propose des solutions.

Nouveauté ! Déblocage de l'appareil contre les logiciels malveillants

Cette option vous permet de débloquer l'appareil, infecté par les Trojans bloqueurs. Fonctionnalités :

- l'arrêt de processus malveillants même si l'appareil est complètement bloqué ;
- la résistance aux bloqueurs non inclus à la base virale de Dr.Web ;
- la sauvegarde de données sans payer une rançon aux attaquants.

Pare-feu

Contrôle l'activité réseau des applications.

- Le filtrage du trafic des applications installées sur l'appareil et celles du système - sur choix de l'utilisateur (Wi-Fi, réseau cellulaire) et d'après les règles personnalisées (par les adresses IP et / ou les ports, les réseaux, la zone d'adresses) ;
- Le contrôle du trafic - avec des statistiques sur les adresses/ports de connexion et le volume du trafic entrant et sortant ;
- Les logs détaillés.

Le pare-feu Dr.Web est compatible avec Android 4.0 ou supérieur.

Dr.Web Enterprise Security Suite. Produits pour entreprises

Dr.Web Enterprise Security Suite – est un produit Dr.Web qui inclut des outils de protection de tous les éléments du réseau de l'entreprise et un centre de gestion centralisée, servant à administrer la plupart d'entre eux. Les produits sont répartis en 5 groupes selon le type d'objets protégés. Cela facilite le processus de sélection d'un produit déterminé conforme aux exigences du client.

Groupe de produits	Logiciels
Dr.Web Desktop Security Suite Protection des postes de travail, des clients de terminal server, des clients des serveurs virtuels et des clients des systèmes embarqués	Dr.Web pour Windows
	Dr.Web pour Linux
	Dr.Web pour OS X
	Dr.Web pour MS DOS*
	Dr.Web pour OS/2*
Dr.Web Server Security Suite Protection des serveurs de fichiers et des serveurs d'applications (serveurs virtuels et terminal servers inclus)	Dr.Web pour les serveurs Windows
	Dr.Web pour les serveurs UNIX
	Dr.Web pour les serveurs Novell NetWare
	Dr.Web pour les serveurs OS X Server
Dr.Web Mail Security Suite Protection de messagerie	Dr.Web pour les serveurs de messagerie et les passerelles UNIX
	Dr.Web pour MS Exchange
	Dr.Web pour IBM Lotus Domino sous Windows
	Dr.Web pour IBM Lotus Domino sous Linux
	Dr.Web pour les serveurs de messagerie Kerio sous Windows
	Dr.Web pour les serveurs de messagerie Kerio sous Linux
	Dr.Web pour les serveurs de messagerie Kerio sous OS X
Dr.Web Gateway Security Suite Protection des passerelles (SMTP et passerelles Internet)	Dr.Web pour les passerelles internet UNIX
	Dr.Web pour les passerelles Internet Kerio
	Dr.Web pour MS ISA Server et Forefront TMG*
	Dr.Web pour MIMEsweeper*
	Dr.Web pour Qbik WinGate*
Dr.Web Mobile Security Suite Protection des appareils portables	Dr.Web pour Windows Mobile
	Dr.Web pour Symbian OS*
	Dr.Web pour Android

* La gestion centralisée n'est pas prévue.

Algorithme de choix d'un produit

1. Qu'est-ce que voulez-vous protéger ?	2. Sous quel OS/ sur quelle plateforme fonctionnent les appareils protégés ?*	3. Avez-vous besoin d'un antivirus ou d'une protection complète ?	4. Avez-vous besoin de vous protéger contre des attaques réseau (pare-feu) ?	5. Combien d'objets voulez-vous protéger ?	6. Durée de la licence ?	7. La licence demandée, correspond-elle au premier achat,au renouvellement de la licence, à l'achat supplémentaire ou à l'achat supplémentaire avec un renouvellement; Est-ce que le client peut bénéficier d'une remise ?
Déterminons le produit	Déterminons l'OS/ plateforme	Déterminons la licence de base	Déterminons des composants supplémentaires	Déterminons le nombre de licences	Détermination de la durée de la licence	Détermination du type de licence et des remises applicables
Postes de travail (Dr.Web Desktop Security Suite)	■ Windows 8/7/ Vista/XP SP2/ 2000 SP4 + Rollup 1	■ Protection complète ■ Antivirus	■ Centre de gestion	1....	2, 24 ou 36 mois	
	■ OS X ■ Linux	■ Antivirus	■ Centre de gestion			
	MS DOS, OS/2					
Serveurs de fichiers (Dr.Web Server Security Suite)	■ Windows ■ Novell NetWare ■ OS X Server ■ UNIX	■ Antivirus	■ Centre de gestion	1...		
Trafic de messagerie (Dr.Web Mail Security Suite)	■ UNIX ■ MS Exchange ■ Lotus Domino ■ Kerio	■ Antivirus	■ Antispam ■ SMTP Proxy ■ Centre de gestion	■ Nombre illimité d'utilisateurs ■ Serveurs avec le nombre d'utilisateurs protégés ne dépassant pas 3 000		
IT trafic (Dr.Web Gateway Security Suite)	■ Passerelles Internet Kerio ■ Passerelles de messagerie UNIX	■ Antivirus	■ Centre de gestion	■ Nombre illimité d'utilisateurs ■ Serveurs avec le nombre d'utilisateurs protégés ne dépassant pas 3 000		
	■ Qbik WinGate ■ MIMEsweeper ■ Microsoft ISA Server et Forefront TMG		■ Antispam			
Appareils portables (Dr.Web Mobile Security Suite)	■ Windows Mobile ■ Android	■ Protection complète	■ Centre de gestion	■ Nombre illimité de portables		
	■ Symbian					
Vous possédez maintenant toutes les données nécessaires au calcul du prix de la licence						

* Cette étape n'a d'importance que pour les postes de travail, comme leur jeu de composants accessibles dépend de l'OS utilisé (voir « Licensing des produits »).

Centre de gestion Dr.Web

Gestion centralisée de la protection de tous les éléments du réseau d'entreprise.

Fonctions clés

Gestion centralisée de tous les composants de la protection, surveillance de l'état de tous les éléments du réseau, configuration de la réaction automatique aux incidents viraux.

Avantages

- Une gestion du système de la protection du réseau d'entreprise très économique, à partir d'un seul poste de travail (via l'Administrateur web), même s'il se trouve en dehors du réseau géré de l'entreprise, depuis n'importe quel coin du globe.
- Un coût total minimal par rapport aux analogues concurrents dû à la possibilité de déploiement du réseau sous des serveurs Windows et UNIX, à la simplicité de son installation et à la solidité de la protection.
- Le système de protection peut être déployé pratiquement dans tout réseau d'entreprise indépendamment de ses dimensions et de ses particularités : quantité d'employés, de succursales, situation géographique, présence ou absence du serveur Active Directory.
- La possibilité de déployer les agents sur les postes de travail de manière qui convient le plus à l'administrateur : via des politiques Active Directory, scripts de démarrage, mécanismes d'une installation à distance. L'installation est possible même si un élément du réseau est inaccessible au serveur antiviral.
- La réalisation des politiques de sécurité individuelles pour chaque entreprise et pour chaque groupe de collaborateurs.
- Automatisation du travail grâce à l'intégration avec le système Windows NAP.
- Le Centre de gestion Dr.Web montre une flexibilité exceptionnelle dans des réseaux de toute dimension et de toute complexité. Il s'adapte aussi bien aux petits réseaux qu'aux intranets comptant des dizaines de milliers de postes. Cette flexibilité est assurée par une option permettant de créer une hiérarchie entre plusieurs serveurs du Centre de gestion Dr.Web interagissant et exploitant un seul serveur SQL pour stocker les données. La création d'une structure d'interaction entre les serveurs et les éléments protégés du réseau contribue également à la flexibilité de la solution.
- Il assure le support simultané de plusieurs protocoles entre les postes protégés et le serveur : TCP/IP (y compris IPV6), IPX/SPX et NetBios ce qui rend possible son utilisation dans différents réseaux.
- Un échangé sécurisé des données entre les éléments du réseau grâce au cryptage.
- Un faible débit du réseau local. La compression des données entre le client et le serveur est assurée par un protocole spécial d'échange d'information dans les réseaux, basé sur les protocoles TCP/IP, IPX/SPX ou NetBios.
- La transparence du fonctionnement : le registre des opérations des administrateurs permet de suivre toutes les étapes d'installation et de paramétrage du système. Tous les composants du réseau antivirus sont capables de rédiger des rapports à un niveau de détails paramétré. Tout un système d'alertes de l'administrateur sur les éventuels problèmes est également prévu.
- La possibilité de nommer un administrateur à part pour chaque groupe, ce qui permet d'utiliser Le Centre de gestion dans les entreprises ayant des exigences élevées en matière de sécurité aussi bien que dans les sociétés aux multiples succursales.
- La possibilité de paramétrer les politiques de sécurité pour tous les types d'utilisateurs, tous les postes de travail y compris les portables ainsi que les postes déconnectés du réseau durant un moment.
- L'incapacité de changer les configurations de la protection par des utilisateurs eux-mêmes sans autorisation de l'administrateur.
- La possibilité de protéger les réseaux qui n'ont pas accès à Internet.

- La possibilité d'utiliser la plupart des bases de données existantes, internes et externes. Parmi les dernières on peut nommer Oracle, PostgreSQL, Microsoft SQL Server ou Microsoft SQL Server Compact Edition, tout Système de gestion des bases des données supportant SQL-92 via ODBC.
- La possibilité de traiter les événements dans n'importe quelle langue script donne accès aux interfaces internes du Centre de gestion.
- La possibilité de tester les mises à jour : même si le processus de mises à jour a provoqué une erreur, l'élément du réseau ne restera pas sans protection.
- Une grande compatibilité avec les logiciels d'éditeurs tiers, ce qui contribue à minimiser les frais pour l'établissement du système de sécurité.
- Une clarté absolue du système de contrôle de l'état de la protection et un système de recherche très convivial des postes de travail.
- La possibilité d'effectuer le choix des composants récemment mis à jour de la liste des produits et contrôle des migrations vers de nouvelles versions permettent aux administrateurs d'installer seulement des mises à jour nécessaires et préalablement testées.

Liens utiles

http://download.drweb.com/live_demo/

Dr.Web Desktop Security Suite

Protection des postes de travail, des clients des terminal servers, des clients des serveurs virtuels et des clients des systèmes embarqués.

- Dr.Web pour Windows certifié par le FSTEC
- Dr.Web pour Linux certifié par le FSTEC
- Dr.Web pour OS X
- Dr.Web pour MS DOS, OS/2

OS supportés

Dr.Web pour Windows	Dr.Web pour Linux	Dr.Web pour OS X	Scanners en ligne de commande Dr.Web
Windows 2012/8/7/2008/ Vista/2003/XP/SP 2 (32 et 64-bits)	Distributions GNU/Linux, avec la version du noyau 2.6.37.(ou supérieurs) et Intel x86/amd64 utilisant la bibliothèque glibc en version 2.13 (et supérieurs)	OS X 10.7 et supérieure (32- et 64-bits)	Windows, MS DOS, OS/2

Licensing de Dr.Web Desktop Security Suite

Types de licences

Selon le nombre de postes de travail, des clients se connectant au terminal server, des clients se connectant au server virtuel ou des clients des systèmes embarqués.

Vous pouvez acheter le produit Dr.Web Desktop Security Suite séparément ou au sein de l'ensemble Dr.Web Enterprise Security Suite. Dans le dernier cas, vous deviendrez également possesseur du Centre de gestion Dr.Web Enterprise Security Suite (sauf les scanners en ligne Dr.Web), et du Pare-feu (qui n'existe que pour Dr.Web pour Windows 7/Vista/XP/2000 SP4 + Rollup 1).

Variantes de licences

	Windows 8/7/ Vista	Windows 8/7/ Vista/XP SP2/ 2000 SP4 + Rollup 1	Linux	OS X	MS DOS, OS/2
Licence de base	Protection complète	Antivirus Windows 8/7/Vista/XP SP2/2000 SP4 + Rollup 1			
Composants de protection de la licence de base	■ Antivirus ■ Anti -espion ■ Antirootkit ■ Antispam ■ Web antivirus ■ Office control ■ Pare-feu	■ Antivirus ■ Anti-espion ■ Antirootkit ■ Pare-feu	■ Antivirus ■ Anti-espion	■ Antivirus ■ Anti-espion ■ Antirootkit	■ Antivirus ■ Anti-espion ■ Antirootkit
Composants supplémentaires					
Centre de gestion	+	+	+	+	–

Vous pouvez acheter Dr.Web Desktop Security Suite au sein des bundles économiques Dr.Web pour PME.

Toutes les informations sur Dr.Web pourWindows, OS X, Linux ainsi que sur les scanners en ligne de commande se trouvent dans la rubrique Dr.Web Home Security Suite. Produits pour particuliers. Les informations sur le produit Dr.Web Security Space se trouvent dans la licence Protection complète.

Dr.Web Server Security Suite

Protection des serveurs de fichiers et des serveurs d'applications (y compris les serveurs virtuels et terminal servers)

- Dr.Web pour les serveurs Windows certifié par le FSTEC
- Dr.Web pour les serveurs Novell NetWare
- Dr.Web pour les serveurs OS X Server
- Dr.Web pour les serveurs UNIX (Samba) certifié par le FSTEC

OS supportés

Dr.Web pour les serveurs Windows	Dr.Web pour les serveurs UNIX	Dr.Web pour les serveurs Novell NetWare	Dr.Web pour les serveurs OS X Server
Windows NT /2000/2003/ 2008 (32- et 64-bits)	■ Linux avec la version du noyau 2.4.x et supérieure ■ FreeBSD de la version 6.x et supérieure pour plateforme Intel x86 ■ Solaris version 10 pour plateforme Intel x86	Novell NetWare v. 4.11– 6.5	OS X Server 10.7 + 32- et 64-bits)

Vous pouvez acheter le produit Dr.Web Server Security Suite séparément ou au sein de l'ensemble Dr.Web Enterprise Security Suite.

	Windows	Novell NetWare	OS X Server	UNIX
Licence de base	Antivirus			
Composants supplémentaires				
Centre de gestion	+	+	+	+

Le produit Dr.Web Server Security Suite fait également partie des bundles économiques Dr.Web pour PME.

Dr.Web pour les serveurs Windows

Protection antivirale des serveurs de fichiers et de terminal servers sous Windows, y compris des serveurs d'applications

Avantages

- Haute rentabilité et stabilité de fonctionnement.
- Haute vitesse d'analyse de grands volumes de données, utilisation minimum des ressources de l'OS, ce qui permet à Dr.Web de fonctionner sur des serveurs de n'importe quelle configuration.
- Fonctionnement continu de l'antivirus dans le mode automatique.
- Répartition flexible de la charge sur le système de fichiers du serveur grâce à une technologie unique d'analyse reportée des fichiers ouverts en lecture seule.
- Système de paramétrage flexible orienté client : choix des actions à appliquer à des virus détectés ou à des fichiers suspects.
- Administration conviviale, simplicité d'installation.
- Protection aussitôt après l'installation (avec les paramètres par défaut).
- Transparence : fichiers-rapports émis régulièrement : détaillés ou non selon la prescription de l'administrateur.

Fonctions clés

- Analyse du serveur selon un horaire prédéterminé ou à la demande de l'administrateur.
- Scan « à la volée » – lors de l'enregistrement ou lors de l'ouverture des fichiers sur le serveur depuis les postes de travail.
- Analyse multi flux.
- Déconnexion automatique du serveur de fichiers client qui représente un danger viral.
- Envoi des alertes instantanées à l'administrateur, aux autres utilisateurs et aux groupes sur les incidents viraux par courriel, sur le portable ou sur le messager de poche.
- Isolation des fichiers infectés en quarantaine.
- Désinfection, restauration ou suppression des fichiers de la quarantaine.
- Journal des actions de l'antivirus.
- Mises à jour automatiques des bases virales.

Pré-requis système

- Processeur: supportant le système de commande i686 et supérieur.
- Système d'exploitation: Microsoft Windows Server 2000/2003/2008 (32- et 64-bits)
- Mémoire vive: 512 Mo et plus.

Liens utiles

Description : http://products.drweb.fr/fileserver/win/

Dr.Web Antivirus pour OS X Server

Protection de base contre les virus pour les plateformes serveur OS X Server

Fonctions clés

Analyse des objets d'auto-démarrage, des supports amovibles, des disques réseaux et logiques, des courriers de différents formats, des fichiers et des répertoires, y compris archivés et compressés.

- Trois types d'analyse: rapide, complète, sélective.
- Lancement de l'analyse antivirale manuellement, automatiquement ou sur planification.
- Protection des paramètres du moniteur SpIDer Guard® contre des modifications non-autorisées à l'aide d'un mot de passe.
- Choix des actions liées aux objets infectés, suspects et autres, y compris la neutralisation, la mise en quarantaine et leur élimination, si les deux actions précédentes se sont avérées inefficaces.
- Exclusion de l'analyse de certains fichiers et de leurs chemins sur demande de l'utilisateur.
- Détection et élimination des virus masqués utilisant des outils de compression inconnus.
- Enregistrement de l'heure des événements, de l'analyse des objets et du type d'attaque.
- Mises à jour automatiques des bases de données virales et des modules logiciels via Internet, sur demande ou sur planification.
- Notifications, y compris sonores, sur les événements viraux.
- Isolation des fichiers contaminés en quarantaine ainsi que la possibilité de paramétrer la durée de leur isolation et le volume maximal de la quarantaine.
- Désinfection, restauration ou suppression des objets mis en quarantaine.
- Rapport détaillé sur le travail de l'antivirus.
- Accès aux modules depuis la ligne de commande et possibilité de les intégrer aux systèmes Apple Scripts en tant qu'utilitaires de service.

Avantages

- Centre de gestion convivial
- Rapidité du scan
- Création de profiles de scan personnalisés profils instead of profiles
- Protection solide en temps réel
- Charge minimale sur le système protégé
- Economie du trafic lors de la mise à jour
- Paramétrages divers
- Simplicité de gestion
- Interface moderne

Pré-requis système

- OS X 10.7 Server ou supérieur (32- et 64-bits).
- Processeur Intel.
- RAM – selon les pré-requis système.
- Accès à Internet : pour enregistrement et la réception des mises à jour.

Liens utiles

Description : http://products.drweb.fr/fileserver/mac/

Dr.Web pour les serveurs Novell NetWare

Protection antivirale des dépôts de fichiers

Fonctions clés

- Analyse des volumes du serveur selon un horaire prédéterminé ou sur demande de l'administrateur
- Analyse « à la volée » de tous les fichiers transitant par le serveur.
- Analyse de plusieurs trafics.
- Possibilité de configurer la charge du processeur ce qui permet de fixer les priorités du scan.
- Déconnexion automatique du serveur du poste de travail qui devient source de contamination potentielle.
- Protocole d'analyse ; gestion des détails du protocole.
- Notifications sur les objets infectés détectés.
- Traitement, suppression ou mise en quarantaine des objets infectés.
- Administration de l'antivirus, surveillance de ses actions de protection du serveur, optimisation du paramétrage, configuration du système d'alertes sur les événements viraux à l'aide de la console du serveur ou une console distante.
- Collecte des statistiques de scan et enregistrement de toutes les actions de l'antivirus.
- Mise à jour automatique des bases virales.

Avantages

- Support d'une large gamme de versions Novell NetWare –de 4.11 à 6.5
- Support de l'espace des noms NetWare
- Haute vitesse d'analyse de grands volumes de données, utilisation minimum des ressources de l'OS – en temps réel comme sur demande de l'administrateur
- Installation simple
- Système de paramétrage flexible des actions sur les virus détectés ou les fichiers suspects, orienté client

Pré-requis système

- Novell NetWare version 4.11-6.5 avec des suppléments installés depuis Minimum patch list.

Liens utiles

Description : http://products.drweb.fr/fileserver/novell/

Dr.Web pour les serveurs UNIX

La protection antivirus des serveurs de fichiers Unix

Avantages

- Haute rentabilité et stabilité de fonctionnement.
- Haute vitesse d'analyse de grands volumes de données, utilisation minimum des ressources de l'OS, ce qui permet à Dr.Web de fonctionner sur des serveurs de n'importe quelle configuration.
- Système de paramétrage flexible : choix des objets à analyser et des actions à appliquer aux virus détectés et aux fichiers suspects.
- Compatibilité sans égal : n'entre jamais en conflit avec les écrans inter-réseau ou moniteurs de fichiers.
- Compatibilité avec les systèmes de surveillance (Nagios, Cacti, Zabbix, Munin, etc.).
- Administration conviviale, simplicité d'installation et de paramétrage.

Fonctions clés

- Analyse des données du serveur selon un horaire prédéterminé ou sur demande de l'administrateur
- Amélioré ! Analyse « à la volée » de tous les fichiers transitant par le serveur
- Analyse multi flux
- Déconnexion automatique du serveur du poste de travail qui devient source de contamination potentielle
- Alerte transmise à l'administrateur et aux utilisateurs sur les événements viraux, par email, sur leurs téléphones portables, ou messagers de poche
- Amélioré ! Isolation des fichiers infectés en quarantaine
- Traitement, restauration ou suppression des objets infectés de la quarantaine
- Journal de toutes les actions de l'antivirus
- Mise à jour automatique des bases virales

OS supportés

- GNU/Linux (avec la version du noyau 2.6.37.(ou supérieurs), utilisant la bibliothèque glibc en version 2.13 (et supérieurs)) ;
- FreeBSD ;
- Solaris — uniquement pour Intel x86/amd64.

Les systèmes d'exploitation doivent utiliser le serveur Samba en version 3.0 ou supérieur, ainsi que lemécanisme d'authentification PAM.

Si la version 64 bits du système d'exploitation est utilisée, elle doit être capable d'exécuter des applications 32 bits.

Espace disque dur :

- Au moins 1 Go

Le fonctionnement du logiciel a été testé avec les distributions suivantes : Debian (7.8, 8), Fedora (20, 21), Ubuntu (12.04, 14.04, 14.10, 15.04), CentOS (5.11, 6.6, 7.1), Red Hat Enterprise Linux (5.11, 6.6, 7.1), SUSE Linux Enterprise Server (11 SP3, 12), FreeBSD (9.3, 10.1), Solaris (10 u11).

Liens utiles

Description : http://products.drweb.fr/fileserver/unix/

Dr.Web Mail Security Suite

Protection de messagerie

- Dr.Web pour les serveurs de messagerie UNIX certifié par le FSTEC
- Dr.Web pour MS Exchange certifié par le FSTEC
- Dr.Web pour IBM Lotus Domino (Windows, Linux)
- Dr.Web pour les serveurs de messagerie Kerio (Windows, Linux)

OS supportés

Produit Dr.Web	Windows	Linux	FreeBSD	Solaris
		Pour la plateforme Intel x86		
Dr.Web pour les serveurs de messagerie UNIX		version du noyau 2.4.x et supérieure	versions 6.x et supérieures	versions 10
Dr.Web pour MS Exchange	Server 2000 / 2003 / 2008/ 2012			
Dr.Web pour IBM Lotus Domino	2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 (32- et 64-bits)	Red Hat Enterprise Linux (RHEL) versions 4 et 5, Novell SuSE Linux Enterprise Server (SLES)versions 9 et 10 (seulement les versions de 32 bits)		
Dr.Web pour les serveurs de messagerie Kerio	2000/XP/Vista/7, Server 2003/2008/2012	Red Hat 9.0; Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0, 11.1; CentOS Linux 5.2, 5.3; Debian 5.0; Ubuntu 8.04 LTS		

Licence Dr.Web Mail Security Suite

Types de licences

- Selon le nombre d'utilisateurs protégés (il est illimité).
- Selon le nombre de serveurs : pour l'analyse d'une quantité illimitée de messages sur un serveur au nombre d'utilisateurs protégés ne dépassant pas 3 000.

Les produits logiciels Dr.Web destinés à protéger la messagerie sont disponibles à part ou dans l'ensemble Dr.Web Enterprise Security Suite.

Variantes de licences

	Dr.Web pour MS Exchange	Dr.Web pour IBM Lotus Domino	Dr.Web pour les serveurs de messagerie UNIX	Dr.Web pour les serveurs de messagerie Kerio
Licence de base	Antivirus			
Composants supplémentaires				
Antispam	+	+	+	
SMTP proxy*	+	+	+	+
Centre de gestion	+	+	+	+

*L'utilisation commune des produits de protection de messagerie et du composant supplémentaire SMTP proxy renforce la sécurité du réseau en général et diminue les charges sur les serveurs et les postes de travail internes.

Les produits Dr.Web destinés à protéger la messagerie sont accessibles également dans les bundles Dr.Web pour PME.

Dr.Web pour serveurs de messagerie UNIX

Technologie intelligente de contrôle et de traitement antiviral et antispam de grands volumes de messages

Fonctions clés

- Filtrage antivirus et antispam du courrier.
- Analyse de tous les éléments de message.
- Traitement de la plupart des types d'archive connus y compris les archives multi-volumes et auto-extractibles (SFX).
- Black et white listes.
- Notifications paramétrables.
- Journalisation des statistiques sur tous les aspects relatifs au fonctionnement du système.
- Protection de ses propres modules contre d'éventuelles failles.

Avantages

Configuration flexible orientée client

Il est possible de paramétrer les règles de filtrage pour Dr.Web pour serveurs UNIX et de les modifier en fonction des besoins individuels du client. C'est pourquoi Dr.Web pour serveurs de messagerie UNIX se distingue d'autres solutions par son système de paramétrage flexible permettant de définir un ensemble de règles spécifiques. Cela distingue ce produit de ses concurrents, dont les fichiers de configuration sont souvent statiques. Le filtrage et les modifications des messages dépendent des politiques prédéfinies, mais l'administrateur peut configurer des règles de traitement différentes pour chaque message, ainsi que créer des groupes et différents utilisateurs. Grâce à cela, le produit satisfait les exigences de toutes les entreprises en matière de sécurité informatique.

Le produit ne nécessite pas un haut niveau de qualification

Malgré la richesse de ses fonctionnalités, Dr.Web pour serveurs de messagerie UNIX n'exige pas de configuration spéciale avant sa mise en marche.

Hautes performances

Grâce à sa fonction d'analyse multi-flux, Dr.Web pour serveurs de messagerie UNIX est capable de traiter simultanément un grand volume de courriel. Le traitement des messages s'effectue « à la volée », parallèlement au traitement du courriel déjà reçu. Cela permet de recevoir les messages pratiquement instantanément.

Avantages supplémentaires de l'antispam Dr.Web:

- N'exige pas de formation préalable et commence à fonctionner effectivement dès son installation, ce qui le différencie des antispams basés sur l'algorithme de Bayes (Panda, Kaspersky).
- La définition du spam ne dépend pas de la langue du message.
- Permet de configurer les actions à appliquer aux différentes catégories de spam.
- Utilise ses propres black et white listes, ce qui rend impossibles toutes tentatives de compromettre les entreprises en les inscrivant dans des listes d'adresses non-sollicitées.
- Évite les faux positifs.
- N'a besoin que d'une mise à jour par jour : les technologies uniques de détection des courriels indésirables, basées sur des milliers de règles, permettent d'éviter le téléchargement de mises à jour volumineuses et fréquentes.

Protection de l'information confidentielle

Ce produit permet de restaurer les messages éliminés par erreur, ainsi que de réaliser des enquêtes sur les fuites de données, grâce à la gestion de la quarantaine via une interface web avec un utilitaire spécial et la mise en archive de tous les messages entrants.

Facilité d'administration

L'utilisation de l'interface web pour le paramétrage et pour la gestion du produit permet de l'administrer facilement, de n'importe quel endroit du globe.

Compatibilité

Dr.Web pour serveurs de messagerie UNIX peut s'intégrer dans les solutions d'autres éditeurs. En outre, grâce à une API ouverte, vous pouvez toujours lui ajouter des fonctionnalités.

Connexion d'un nombre illimité de plugins

La conception de Dr.Web pour serveurs de messagerie UNIX permet d'augmenter ses fonctionnalités pratiquement sans limites, et tout plugin édité fonctionne avec tous les serveurs de messagerie supportés. Les plugins suivants fonctionnent dans le produit **Dr.Web pour serveurs de messagerie UNIX** :

- **Dr.Web** – plugin d'analyse antivirus du courrier avec le moteur antivirus Dr.Web
- **vaderetro** – plugin de filtrage antispam du courrier avec la bibliothèque Vade Retro
- **headersfilter** – plugin de filtrage des messages par leurs en-têtes

OS et messageries supportés

- Linux (glibc 2.2 et ultérieure), FreeBSD 5.x, 6.x, Solaris 10 (Intel uniquement).
- CommuniGate Pro, Courier MTA, Exim, Postfix, QMail, Sendmail, ZMailer.

Dr.Web SMTP proxy

Dr.Web pour serveurs de messagerie UNIX muni du module Dr.Web SMTP proxy peut être installé dans la zone démilitarisée (DMZ), ainsi qu'à l'intérieur du système de messagerie. Grâce à l'emplacement du serveur dans la DMZ, et à son isolement d'Internet, même en cas d'effraction du serveur, le pirate n'aura pas d'accès à l'information confidentielle et importante pour l'entreprise. Une analyse complète du courriel selon les protocoles SMTP/LMTP est assurée.

Avantages

- Une amélioration considérable de la qualité de filtrage grâce à l'absence de restrictions imposées par le serveur de messagerie.
- Diminution de la charge sur les serveurs de messagerie internes, les serveurs de filtrage de contenu, les passerelles de messagerie et Internet, ainsi que les postes de travail.
- Renforcement de la stabilité de l'analyse des messages et de la sécurité du réseau entier.

Protection contre les attaques de spammeurs

L'administrateur peut réduire les paramètres de la session SMTP, excluant par ce fait toute possibilité d'attaque de la part des spammeurs.

Protection contre le spam masqué

Grâce à la fonction de vérification d'authenticité de l'adresse IP, votre entreprise est protégée contre le spam camouflé sous une fausse adresse IP de l'expéditeur.

Protection contre les hackers

Ce produit permet de résister avec succès aux attaques passives (du type PLAIN, LOGIN etc.), ainsi qu'aux attaques par force brute (brute force attacks).

Contrôle des destinataires

Dr.Web SMTP proxy analyse le destinataire pour contrôler que ce n'est pas un spam trap.

Protection contre les messages inhabituels

Le produit bloque les messages avec des champs expéditeurs vides, mais traite correctement les messages des clients de messagerie, même ceux ayant une forme inhabituelle.

Economie du trafic Internet

L'utilisation de Dr.Web SMTP proxy permet de limiter la taille des pièces jointes.

Limitation pour les serveurs Open Relays

En cas d'installation de ce type de serveur, l'administrateur peut limiter la liste des domaines pour la réexpédition les messages à l'aide de Dr.Web SMTP proxy.

Liens utiles

Description : http://new-download.drweb.com/maild

Dr.Web pour MS Exchange

Analyse antivirus et antispam du trafic transmis via les serveurs de messagerie MS Exchange 2000/2003/2007/2010/2013/2016

Avantages

- Installation et paramétrage flexibles en fonction des besoins de l'entreprise
- Rapidité du scan et charge minimale du système d'exploitation, ce qui permet à Dr.Web de fonctionner sur les serveurs de toutes configurations
- Antispam interne qui n'exige pas de configuration spéciale avant sa mise en marche et fonctionne dès son installation, diminuant la charge du serveur et facilitant le travail du personnel
- Utilisation de black et white listes propres, ce qui rend possible d'exclure certaines adresses de l'analyse et d'augmenter son efficacité
- Filtrage selon les types de fichiers, ce qui permet aux entreprises de diminuer le trafic
- Mécanisme de création de groupes qui permet de configurer différents paramètres pour différents groupes d'employés, ce qui diminue le temps de mise en exploitation et simplifie le maintien du produit
- Haute productivité et stabilité de fonctionnement grâce à la fonction d'analyse multiflux
- Technologies uniques de détection des outils de compression inconnus jusqu'à présent ainsi que des objets malveillants
- Lancement du logiciel totalement automatisé (au démarrage du système)
- Système convivial de mises à jour à l'aide du planificateur Windows
- Manuels en français

Fonctions clés

- Analyse antivirus et antispam des messages « à la volée » ainsi que des pièces jointes
- Surveillance antivirale des messages dans les boîtes des utilisateurs ainsi que des fichiers dans les dossiers partagés
- Analyse antivirus du trafic de courrier transitant via le serveur MS Exchange
- Désinfection des fichiers infectés
- Création de groupes d'utilisateurs à l'aide d'ActiveDirectory
- Paramètres de scan : choix de la taille maximale et des types d'objets à analyser , des actions à appliquer (même aux fichiers dont l'analyse est impossible), ainsi que des moyens de traitement des objets infectés
- Détection des objets malveillants dans les fichiers compressés plusieurs fois
- Application de différentes actions suivant le type de spam, y compris la mise en quarantaine et l'ajout du préfixe à l'objet du message
- En cas de besoin, l'administrateur peut ajouter un texte aux messages envoyés
- Isolation des objets contaminés et suspects en quarantaine
- Alertes sur les événements envoyées à l'administrateur et aux utilisateurs
- Recueil de statistiques
- Mises à jour automatiques

Pré-requis système

- Microsoft Exchange Server 2000/2003:
  Pentium 133 MHz (733 MHz recommandé). RAM: 512 Mo. Espace disponible sur le disque dur: 512 Mo. Microsoft® Windows Server® 2003 (versions Standard, Enterprise ou Datacenter) (SP1 ou supérieur).
- Microsoft Exchange Server 2007/2010:
  Intel de l'architecture x64 avec support de la technologie Intel 64; AMD compatible avec AMD64. RAM: 2 Go. Espace disponible sur le disque dur: 512 Mo. Microsoft® Windows Server® 2003 R2 x64 (SP2); Microsoft® Windows Server® 2008 x64 ; Microsoft® Windows Server® 2008 R2.
- Microsoft Exchange Server 2013/2016:
  Intel de l'architecture x64 avec support de la technologie Intel 64; AMD compatible avec AMD64. RAM: 4 Go. Espace disponible sur le disque dur: 1 Go. Microsoft® Windows Server® 2008 R2 ; Microsoft® Windows Server® 2012 ; Microsoft® Windows Server® 2012 R2.

Liens utiles

Description : http://products.drweb.fr/exchange/

Dr.Web pour IBM Lotus Domino

Protection antivirus et antispam de la plateforme IBM Lotus Domino sous Windows et Linux

Avantages

Coût minimal

Dr.Web pour IBM Lotus Domino fonctionne sur les serveurs isolés et sur les serveurs- partitions et les clusters de Lotus Domino. Des copies de l'antivirus sur différentes sections fonctionnent dans la mémoire du PC de manière autonome, utilisant en commun les bases et les fichiers exécutables. Vous n'avez besoin d'une licence que pour une seule copie, ce qui diminue vos frais de protection antivirale.

Ready for IBM Lotus software

Dr.Web pour IBM Lotus Domino figure dans le catalogue des solutions IBM Lotus Business Solutions Catalog et possède le label Ready for IBM Lotus software. Ce label confirme la compatibilité du produit avec le système Lotus Domino et témoigne de sa conformité aux exigences d'IBM.

Rapidité du scan

L'organisation du système Dr.Web pour IBM Lotus Domino, des méthodes d'analyse uniques et une gestion flexible du processus de scan permettent d'atteindre une rapidité exclusive de scan et de diminuer la consommation des ressources système.

Simplicité de déploiement et flexibilité de configuration

Dr.Web pour IBM Lotus Domino se caractérise par un déploiement automatisé et facilement gérable. Ce logiciel supporte les scripts administratifs et possède une ample documentation. La convivialité de gestion du produit est assurée grâce à sa configuration flexible via la console d'administration. L'accès à une configuration détaillée des actions de l'antivirus selon les résultats du scan permet d'envoyer les notifications sur les virus détectés aux administrateurs système, aux destinataires et aux expéditeurs des messages, de sauvegarder les objets des messages, les pièces jointes etc.

Convivialité d'administration

Le mécanisme des groupes facilite considérablement la tâche de l'administrateur en matière de gestion de la protection antivirus.

Fonctions clés

- Analyse et filtrage antispam et antivirus du courrier à la volée (en temps réel) ou à la demande de l'administrateur.
- Filtrage antispam complété par des white et black listes.
- Analyse antivirus des fichiers dans les bases nsf spécifiées.
- Analyse des objets sur demande à l'aide de la fonction de lancement/arrêt des tâches pour lancer un scan manuellement.
- Décomposition des messages permettant l'analyse ultérieure de ses composants.
- Désinfection des messages contaminés et des fichiers infectés en pièce jointe.
- Détection des objets malveillants dans les fichiers compressés plusieurs fois.
- Utilisation du mécanisme de dépistage des logiciels malveillants dissimulés par des compresseurs inconnus.
- Technologie supplémentaire de détection des objets malveillants inconnus, qui augmente la probabilité de détection des virus récents.
- Mise en quarantaine des objets infectés ou suspects (le client Lotus Notes assure l'accès aux objets mis en quarantaine).
- Envoi des notifications aux destinataires ainsi qu'aux personnes concernées par les résultats de l'analyse. Les notifications sont rédigées à l'aide des modèles (templates) préinstallés, ce qui permet d'afficher des informations de façon optimale.
- Récolte des statistiques sur tous les aspects de l'activité système.
- Protection de ses propres modules contre les incidents de fonctionnement.
- Mises à jour automatiques.

OS supportés

Version pour Windows

- Système d'exploitation : Windows Server 2000/2003/2008/2008R2/2012/2012 R2 (32 et 64-bits).
- Lotus Domino en version R6.0 ou supérieur (32 et 64-bits).
- Intel Pentium 133 ou supérieur.
- RAM 128 Mo (512 Mo recommandé).
- Espace libre sur le disque : 128 Mo.

Version pour Linux

- Système d'exploitation : Red Hat Enterprise Linux (RHEL) versions 4 et 5, Novell SuSE Linux Enterprise Server (SLES) version 9 et 10 (32-bits seulement)
- Lotus Domino en version 7.x ou 8.x.
- Lotus Notes 6.5 (ou supérieur) pour Windows.
- Intel Pentium 133 ou supérieur.
- RAM 64 Mo (128 Mo recommandé).
- Espace libre sur le disque : 90 Mo.

Liens utiles

Description : http://products.drweb.fr/lotus/

Dr.Web pour serveurs de messagerie Kerio

Analyse antivirale des pièces jointes du courriel transmis via les protocoles SMTP/POP3

Avantages

- Compatibilité absolue avec les serveurs de messagerie Kerio, confirmée par les tests Kerio Technologies.
- Mode de protection centralisée assurée par le Centre de gestion Dr.Web Enterprise Security Suite.
- Dr.Web est le seul plugin antivirus russe destiné aux serveurs de messagerie Kerio, ce qui est important pour les établissements publics.
- Support clients en français.
- Délai minimal de livraison des alertes grâce à une analyse multi flux.
- Est peu exigeant en ressources système et charge au minimum le réseau local.
- Système de configuration flexible orienté client : sélection des objets à analyser et des actions à appliquer aux virus ou objets suspects détectés.
- Possibilité de sélectionner les actions à appliquer aux fichiers dont l'analyse est impossible.
- Administration conviviale depuis la console d'administration du serveur de messagerie Kerio.

Fonctions clés

- Analyse des pièces jointes des messages électroniques entrant et sortant.

OS supportés

Version pour Windows

- Espace disque dur : au moins 350 Mo.
- Système d'exploitation : Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008/2012 (32 et 64-bits)
- Le serveur de messagerie : Kerio MailServer 6.2 ou supérieur, Kerio Connect 7.0.0 ou supérieur.

Version pour Linux

- Espace disque dur : au moins 290 Mo.
- Système d'exploitation : Red Hat 9.0; Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0 et 11.1; CentOS Linux 5.2 et 5.3; Debian 5.0; Ubuntu 8.04 LTS.
- Le serveur de messagerie : Kerio MailServer 6.2 ou supérieur, Kerio Connect 7.0.0 ou supérieur.

Version pour OS X

- Espace disque dur : au moins 55 Mo.
- Système d'exploitation : OS X 10.7 ou supérieur.
- Le serveur de messagerie : Kerio MailServer 6.2 ou supérieur, Kerio Connect 7.0.0 ou supérieur.

Liens utiles

Description : http://products.drweb.fr/mailserver/kerio/

Dr.Web Gateway Security Suite

Protection des passerelles

- Dr.Web pour les passerelles Internet UNIX certifié par le FSTEC
- Dr.Web pour les passerelles Internet Kerio
- Dr.Web pour MIMEswepper
- Dr.Web pour Qbik WinGate

OS supportés

	Windows	Linux	FreeBSD	Solaris
		Pour la plate-forme Intel x86		
Dr.Web pour les passerelles Internet UNIX		version du noyau 2.4.x et supérieure	version 6.x et supérieure	version 10
Dr.Web pour les passerelles Internet Kerio	2000 / XP / 2003 / 2008 / 7			
Dr.Web pour MIMEsweeper	2000 Server SP4 ou supérieur / Server 2003 ou superieur			
Dr.Web pour Qbik WinGate	Vista / Server 2008 / Server 2003 / XP / 2000 (32- et 64-bits)			
Dr.Web pour Microsoft ISA Server et Forefront TMG	**Microsoft ISA Server:** ■ Microsoft® Windows Server® 2003 x86 c Service Pack 1 (SP1); ■ Microsoft® Windows Server® 2003 R2 x86 **Microsoft Forefront TMG:** ■ Microsoft® Windows Server® 2008 SP2 ■ Microsoft® Windows Server® 2008 R2			

Licensing de Dr.Web Gateway Security Suite

Types de licences

- Selon le nombre d'utilisateurs protégés (il est illimité).
- Selon le nombre de serveurs : pour l'analyse d'une quantité illimitée de messages sur un serveur au nombre d'utilisateurs protégés ne dépassant pas 3 000.

Les produits logiciels Dr.Web destinés à protéger les passerelles sont disponibles à part ou dans l'ensemble Dr.Web Enterprise Security Suite.

Variantes de licences

	Dr.Web pour les passerelles Internet UNIX	Dr.Web pour les passerelles Internet Kerio	Dr.Web pour MIMEsweeper	Dr.Web pour Qbik WinGate	Dr.Web pour Microsoft ISA Server et Forefront TMG
Licence de base	Antivirus				
Composants supplémentaires					
Antispam			+	+	+
Centre de gestion	+	+			

Les produits Dr.Web destinés à protéger la messagerie sont accessibles également dans les bundles Dr.Web pour PME.

Dr.Web pour les passerelles Internet UNIX

Analyse antivirale du trafic HTTP et FTP passant via la passerelle Internet de l'entreprise munie d'un serveur proxy supportant les protocoles ICAP

Fonctions clés

- Analyse antivirale du trafic FTP et HTTP
- Gestion centralisée via l'administrateur Web du Centre de gestion de Dr.Web Enterprise Security Suite
- Filtrage de l'accès selon le type MIME, la taille des fichiers et le nom de l'hôte
- Réglage de l'accès aux ressources web
- Optimisation de l'analyse du trafic à l'aide de la technologie Preview
- Travail avec les protocoles IPv4 et IPv6
- Analyse et application de différentes actions aux fichiers selon leurs types
- Isolation des objets contaminés en quarantaine
- Convivialité de la forme des rapports
- Gestion centralisée de la configuration des serveurs de protection et réception des rapports
- Traitement de plusieurs requêtes utilisateurs à la fois durant une seule session
- Protection contre un accès non-autorisé
- Surveillance et restauration automatiques du fonctionnement du système
- Alertes sur les tentatives de téléchargement d'une page malveillante ou sur le dépistage d'un virus

Avantages

- Larges possibilités de configuration d'une protection complète contre les menaces du trafic web entrant
- Livraison d'un contenu « sain » à l'intérieur du réseau protégé
- Filtrage effectif du trafic au niveau du serveur ICAP, pratiquement sans ralentir la vitesse de téléchargement du contenu
- Résistance effective contre la pénétration de logiciels malicieux de tous types
- Flexibilité exceptionnelle
- Capacité de traiter de grands volumes d'information en temps réel
- Minimisation des coûts d'utilisation d'Internet
- Compatibilité extraordinaire : intégration à tout logiciel supportant le protocole ICAP, et à tous les pare-feux existants

- Support de tous les systèmes d'exploitation connus basés sur UNIX
- Bonne accommodation aux ressources système : le produit fonctionne sans problème sur les passerelles Internet de toute configuration
- Flexibilité et convivialité de l'administration : le produit permet de déployer les schémas de protection qui répondent le mieux à la politique de sécurité de l'entreprise

OS supportés

- Linux avec la version du noyau 2.4.x et supérieure
- FreeBSD de la version 6.x et supérieure (pour la plateforme Intel x86)
- Solaris version 10 (pour la plateforme Intel x86)

Les serveurs proxy supportant le protocole ICAP, en particulier :

- Squid au moins 3.0
- SafeSquid 3.0 et supérieur

Liens utiles

Description : http://products.drweb.fr/gateway/unix/

Dr.Web pour les passerelles Internet Kerio

Analyse antivirale du trafic transmis via les protocoles HTTP, FTP, SMTP et POP3, aussi bien que via le service web Kerio Clientless SSL VPN

Dr.Web pour les passerelles Internet Kerio – est un plugin antivirus qui se connecte à l'écran interréseau Kerio. Il est installé sur le même ordinateur que le Kerio et est utilisé par ce dernier en qualité de logiciel extérieur.

Avantages

- Protection robuste des accès à Internet des particuliers ainsi que des entreprises, indépendamment de leur taille et ou de leur activité.
- Administration conviviale : possibilité de recevoir des notifications sur les incidents liés aux tentatives d'infection virale par courriel et par SMS.
- Temps de livraison minimal des notifications grâce à une analyse multi flux.
- Mode de protection centralisée assurée par le Centre de gestion Dr.Web Enterprise Security Suite.

Fonctions clés

- Détection des objets malveillants transmis via les protocoles HTTP, FTP, SMTP et POP3 aussi bien que via le service web Kerio Clientless SSL VPN.
- Détection des pièces jointes infectées avant leur traitement par le serveur de messagerie.
- Création de la liste des protocoles d'échange des données analysées.
- Console web affichant les informations sur le fonctionnement du logiciel.
- Scan avec possibilité de paramétrage : choix de la taille maximale et du type d'objets analysés ainsi que des méthodes de traitement des fichiers infectés.
- Application des actions conformes aux paramétrages de Kerio aux menaces dépistées.
- Activation/désactivation de la détection des logiciels malveillants (selon leurs types).
- Enregistrement des erreurs et des événements dans le registre des logs (Event Log) ainsi que dans le registre textuel. Ces registres contiennent des informations sur les paramètres des modules, sur la détection des virus pour chaque message et pour chaque virus à part.
- Envoi des notifications sur des différents événements à des utilisateurs définis.
- Mise à jour des bases virales automatique.

Pré-requis système

Version pour Windows

- 350 Mo d'espace libre sur le disque.
- Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (32 et 64-bits)
- Le pare-feu Kerio WinRoute Firewall 6.2 ou supérieur, Kerio Control 7.0.0 ou supérieur.

Version pour Kerio Control VMware Virtual Appliance et Kerio Control Software Appliance

- 290 Mo d'espace libre sur le disque.
- Système d'exploitation Kerio Control VMware Virtual Appliance ou Kerio Control Software Appliance.
- Le pare-feu Kerio Control 8.x ou supérieur.

Liens utiles

Description : http://products.drweb.fr/gateway/kerio/

Dr.Web pour MIMEsweeper

Protection antivirus et antispam du trafic de mail transitant via les serveurs de filtrage de contenu ClearSwift MIMEsweeper

Avantages

Facile à installer et à paramétrer

Les outils de configuration implantés dans Dr.Web pour MIMEsweeper – masters de scénarios – permettent de créer des scénarios de scan des messages de façon centralisée (type 1 selon le classement de ClearSwift.

Compatibilité avec DEP

Dr.Web pour MIMEsweeper supporte la technologie de prévention d'exécution des données (Data Execution Prevention, DEP) permettant d'effectuer une vérification complémentaire de la mémoire afin d'empêcher l'exécution d'un code malicieux. Ainsi, les utilisateurs sont dispensés de modifier le mode de fonctionnement du DEP ce qui fournit une protection contre l'utilisation du mécanisme de traitement des exceptions inclus dans Windows par des programmes malicieux.

Configuration flexible

En cas de détection d'un objet infecté, le plugin essaie de le neutraliser ou le supprime si l'option « Neutraliser » n'est pas activée. Si le message contient plusieurs fichiers ou des archives jointes, seules les pièces jointes infectées seront neutralisées par le plugin. En cas de détection d'un virus dans le corps du message, le filtre de contenu déplace ce message vers quarantaine. Les courriers, fichiers et archives sains sont transférés au destinataire sans modifications. Les messages qui ne peuvent pas être neutralisés par le plugin Dr.Web seront marqués comme virus et par défaut verrouillés en quarantaine.

Fonctions clés

- Analyse des courriers y compris des archives en pièce jointe avant qu'ils n'arrivent sur le serveur de messagerie
- Neutralisation des objets contaminés
- Isolation des objets contaminés et suspects en quarantaine
- Filtrage antispam avec l'utilisation des white et black listes
- Récolte des statistiques sur le fonctionnement de l'ensemble
- Mises à jour régulières des bases virales

Pré-requis système

- OS Windows 2000 Server muni d'un paquet de mise à jour 4 (SP4) ou supérieur ou Windows Server 2003 ou sa version plus avancée.
- Filtre du contenu des messages ClearSwift MIMEsweeper™ for SMTP 5.2 ou sa version plus avancée.

Liens utiles

Description : http://products.drweb.fr/mimesweeper/

Dr.Web pour Qbik WinGate

Analyse antivirus et antispam du trafic transmis via les protocoles HTTP/POP3/FTP des serveurs proxy et SMTP Qbik WinGate

Fonctions clés

- Analyse antivirus et antispam des messages distribués via les protocoles SMTP et POP3, avec le contrôle des pièces jointes.
- Analyse antivirus et antispam des fichiers et des données transmis via les protocoles HTTP et FTP.
- Désinfection des fichiers transmis via le protocole HTTP.
- Enregistrement des erreurs et des événements dans le registre des logs (Event Log).
- Propres barre de commande et gestionnaire de quarantaine.
- Mises à jour automatiques des bases virales.

Avantages

- Dr.Web pour Qbik WinGate est le seul plugin avec la version russe de Qbik WinGate.
- Seul Dr.Web pour Qbik WinGate a une documentation et un support technique directs de l'éditeur.
- A la différence des concurrents, le produit de Doctor Web possède la capacité de filtrage antispam. Le module antispam effectif et compact n'exige pas de formation spéciale et permet de paramétrer différentes actions selon les catégories de spam, ainsi que de créer des listes noires et blanches d'adresses e-mail.
- Technologie unique de recherche sans signatures Origins Tracing™ qui permet à Dr.Web de dépister les virus inconnus et non encore répertoriés dans sa base virale avec un grand degré de probabilité.

Liens utiles

Description : http://products.drweb.fr/gateway/qbik/

Dr.Web Mobile Security Suite

Protection des appareils mobiles

- Dr.Web pour Symbian OS
- Dr.Web pour Windows Mobile
- Dr.Web pour Android

	Dr.Web pour Symbian OS	Dr.Web pour Windows Mobile	Dr.Web pour Android
Composants de la protection	Antivirus+Antispam	Antivirus + Antispam	Protection complète
Gestion centralisée de Dr.Web Enterprise Security Suite	–	+	+
OS supportés	Symbian S60, Symbian 9	Windows Mobile 2003/2003 SE/5.0/6.0/6.1/6.5	Android OS: 4.0-5.0
Fonctions clés			
Scan « à la volée »	+	+	+
Analyse des fichiers entrants via les connexions GPRS/ Infrarouge/Bluetooth/ Wi-Fi/USB ou pendant la synchronisation avec le PC	+	+	+
Deux types de scan : complet et sélectif	+	+	+
Activation/désactivation du scan permanent de la mémoire	+	+	+
Scan à la demande de l'ensemble des fichiers du système ou d'une sélection de fichiers et répertoires	+	+	+
Scan des fichiers dans les archives ZIP, SIS, CAB, RAR	+	+	+
Listes noires et blanches des appels entrants et des SMS	+	+	+
Elimination des fichiers infectés	+	+	+
Isolation en quarantaine des fichiers infectés	+	+	+
Restauration des fichiers de la quarantaine	+	+	+

Mises à jour à travers Internet : ■ Selon le protocole HTTP en utilisant le module interne GPRS; ■ Via connexion Infrarouge/Bluetooth/ Wi-Fi/USB; ■ Via synchronisation du PC, possédant un accès Internet via connexion ActiveSync	+	+	+
Rapports détaillés sur le scan du système	+	+	+
Gestion à distance de votre mobile en cas de perte ou de vol, grâce au système Antivol	+		
CloudChecker — vérification dans le Cloud des liens ouverts	+		
Déblocage contre les applications malveillantes sans équivalent chez les concurrents	+		

Licensing

La licence du produit Dr.Web destiné à protéger les outils portables est fonction du nombre d'appareils à protéger.

Variantes de licences

Dr.Web pour Windows Mobile	Dr.Web pour Symbian OS	Dr.Web pour Android
■ Antivirus + Antispam + Centre de gestion	■ Antivirus + Antispam	■ Protection complète + Centre de gestion

Les produits Dr.Web pour les outils portables sont accessibles dans les bundles Dr.Web pour PME.

Proposition spéciale

Tous les utilisateurs enregistrés des

- Logiciels Dr.Web en DVD
- Dr.Web Security Space
- Dr.Web Antivirus

Liens utiles

Description : http://products.drweb.fr/mobile/

Bundles Dr.Web

Les bundles comprennent les produits Dr.Web qui protègent tous types d'objets.

IMPORTANT! Aucune remise n'est prévue pour ces bundles, même la remise de renouvellement. Pour continuer à utiliser le bundle vous devez acheter une nouvelle licence. Mais vous pouvez bénéficier d'une remise lors de la migration d'un bundle vers des produits isolés Dr.Web.

Bundle « Dr.Web Formule Universelle »

C'est une protection complète pour les petites et moyennes entreprises.

Les petites ainsi que les moyennes entreprises ne peuvent pas se permettre parfois de dépenser des sommes considérables pour acheter une protection informatique complète. Le bundle Dr.Web « Formule universelle » est prévu pour eux. C'est une proposition économique pour des entreprises au nombre de PC de 5 à 100.

Objets protégés	Postes de travail	Serveurs	Utilisateurs de messageris	Utilisateurs des passerelles Internet et de messageris	Appareils portables
Licence	Protection complète	Antivirus	Antivirus + Antispam	Antivirus	Antivirus + Antispam
Fourniture	de 5 à 50	1	Est égale au nombre de postes	Est égale au nombre de postes (à partir de 25)	Est égale au nombre de postes

Liens utiles

Bundles Dr.Web: http://products.drweb.com/bundles/universal

Bundle Dr.Web pour écoles

Objets protégés	Dr.Web Desctop Security Suite	Dr.Web Server Security Suite	Dr.Web Mobile Security Suite
Licence	Protection complète + CG	Antivirus	
Fourniture	10 – 100	1 – 8	10 – 200

Utilitaires de désinfection

Les utilitaires de désinfection Dr.Web sont destinés à effectuer un diagnostic et à procéder à une désinfection d'urgence. Mais ils n'assurent pas une protection durable.

Dr.Web CureNet!

Désinfection centralisée des réseaux locaux de toute taille, même si l'antivirus d'un autre éditeur y est installé.

Utilisateurs potentiels	Petites, moyennes et grandes entreprises, y compris les entreprises de très grande envergure dont les réseaux sont protégés par l'antivirus d'un autre éditeur
Problèmes résolus	■ Désinfection centralisée des postes de travail et des serveurs tournant sous Windows ■ Analyse de la qualité de la protection antivirale utilisée
Particularités de l'utilitaire	■ Ne requiert pas la désinstallation de l'antivirus d'un autre éditeur avant de procéder à l'analyse et à la désinfection ■ Ne requiert pas de serveur ou d'installation de logiciel supplémentaire ■ Peut être utilisé dans des réseaux complètement isolés d'Internet ■ Le guide d'installation Dr.Web CureNet! peut être lancé depuis tout support extérieur même depuis une clé USB
Description du produit	http://www.drweb-curenet.com
OS supportés	MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32 et 64-bits)
Qu'est-ce que c'est que « Mon Dr.Web CureNet! » ?	C'est un espace privé où se trouve le lien de téléchargement du fichier d'installation durant toute la durée de validité de la licence. Vous pouvez également y entrer en contact avec le support technique pour envoyer un fichier suspect ou bénéficier des autres services.
Licences	L'utilitaire est soumis à licence d'après le nombre de postes de travail (5 minimum) pour 1, 2 et 3 ans.
Version démo	La fonction de désinfection n'est pas disponible

Dr.Web CureIt!

Désinfection urgente des PC et des serveurs sous Windows, même si l'antivirus d'un autre éditeur y est installé

Utilisateurs potentiels	Petites et moyennes entreprises, dont les postes sont protégés par l'antivirus d'un autre éditeur
Problèmes résolus	■ Désinfection urgente des postes de travail et des serveurs tournant sous Windows ■ Analyse de la qualité de la protection antivirale utilisée ■ Ne nécessite aucune installation et n'entraîne de conflits avec aucun autre antivirus : la désactivation de l'antivirus déjà installé n'est pas nécessaire pour effectuer le scan
Particularités de l'utilitaire	■ Autoprotection parfaite et mode de protection renforcée, ce qui lui permet de résister avec succès aux logiciels malveillants qui bloquent Windows ou son propre fonctionnement ■ Les mises à jour de **Dr.Web CureIt!** s'effectuent une ou plusieurs fois par heure. L'utilitaire peut être lancé depuis n'importe quel support extérieur même depuis une clé USB
Description du produit	http://free.drweb.com/cureit/
OS supportés	MS Windows 8/7/Vista/XP/2000/Server 2012/2008/2003 (systèmes 32x et 64x)
Licences	La licence de l'utilitaire est fonction du nombre de postes de travail, pour 1 ou 2 et 3 anns d'usage.
Particularités de licensing	Cet utilitaire est gratuit pour les particuliers
Version démo	Il n'existe pas de version démo

Solutions

Dr.Web Security Suite pour Appliance sous UNIX – est un groupe de solutions modulaires pouvant être installé sur des appliances fonctionnant sous les systèmes d'exploitation de la famille UNIX (Linux/FreeBSD/Solaris(x86)). Ces solutions modulaires fonctionnent comme des passerelles Internet d'entreprise – un serveur proxy est utilisé pour fournir l'accès Internet aux utilisateurs de l'Intranet.

	Dr.Web Mail Security Suite pour Appliance sous UNIX	**Dr.Web Gateway Security Suite pour Appliance sous UNIX**
Fonction clé	Filtrage antivirus et antispam des messages électroniques	Filtrage antivirus du trafic HTTP- et FTP
Variantes de licences	Antivirus Antivirus + Antispam	Antivirus

Types de licences

- En fonction du nombre d'utilisateurs, qui est illimité.
- En fonction du nombre de serveurs – pour effectuer l'analyse d'un volume illimité de courriel/du trafic sur un serveur avec un nombre d'utilisateurs ne dépassant pas 3 000.

Licencing du SDK

Le SDK est livré gratuitement avec le produit. Un développeur tiers est libre de développer et distribuer gratuitement les plugins créés via le SDK. La commercialisation de ce type de plugin requiert une certification.

Dr.Web ATM Shield

La protection centralisée des systèmes intégrés (DAB, GAB, terminaux de paiement, multi kiosques)

Les clients potentiels : Les banques (GAB, DAB), les chaînes de distribution (terminaux de paiement, multi kiosques), ainsi que les entreprises et les organisations qui contrôlent les processus de production (stations d'essence, les usines, etc.)

Description : http://solutions.drweb.com/atm_shield

Avantages

- facile à intégrer dans le réseau de DAB et terminaux de paiement ce qui réduit le temps de maintenance ;
- possibilité de travailler sur des ordinateurs à faibles performances (512 Mo), qui fonctionnent 24 sur 24 sans les redémarrages ;
- la gestion de façon centralisée du système de protection antivirus des systèmes embarqués ;
- Les composants de Dr.Web ATM Shield assurent la protection contre les malwares inconnus, qui n'ont pas encore été analysés par le Laboratoire, mais qui sont repérés grâce à des technologies comportementales, ainsi que contre les actions non-autorisées des employés ;
- la souplesse de la solution assure son fonctionnement dans les réseaux avec n'importe quel nombre de nœuds (grâce au système de protection hiérarchique) ;
- le fonctionnement dans les réseaux TCP/IP, IPX, NetBIOS ;
- le choix de la protection du système de gestion de base de données (SGBD) ;
- le trafic réseau minimal, basé sur un protocole spécialement développé, qui assure la compression des données entre le client et le serveur ;
- le cryptage de données lors de l'échange entre les composants du système ;

- le contrôle de l'état de tous les nœuds protégés du système ;
- le recueil centralisé de statistiques sur les incidents viraux ;
- la sauvegarde de données critiques sur le serveur de protection du réseau ;
- un fonctionnement transparent – les logs de l'activité des administrateurs fournissent des statistiques sur toutes les installations et configurations du système.

Attention ! En raison des particularités de l'utilisation des outils antivirus sur les appareils intégrés, il est fortement recommandé, avant d'installer Dr.Web ATM Shield, de consulter le Manuel Administrateur (dans l'Assistant de téléchargement) et le cours Dr.Web ATM Shield.

Licensing

- D'après le nombre d'appareils intégrés protégés.
- Le Centre de gestion Dr.Web ATM Shield est soumis à licence gratuitement.

Démo

Pour obtenir la licence démo, veuillez remplir le formulaire sur http://download.drweb.com/demoreq/atm_shield, en spécifiant le nombre d'appareils protégés, ainsi que l'OS (optionnel).

Attention ! Si le client utilise les OS Embedded (MS Windows Embedded 7, MS Windows Embedded 8 etc.), il faut le prévenir que ces OS ne ressemblent pas aux OS standard, car ils sont conçus pour chaque type d'appareil embarqué, donc ils peuvent ne pas posséder d'un tel ou tel composant, nécessaire pour déployer la protection antivirus. C'est pourquoi il faut que le département de recherche de Doctor Web teste cet appareil et délivre les conseils appropriés.

Outils de marketing pour les partenaires

https://pa.drweb.com/products/atm_shield

Services

Le Software as a service (SaaS) est un modèle consistant à fournir un logiciel sous forme de service.

Son utilisation en Russie était impossible avant 2007 à cause de l'absence de solutions nationales de ce niveau. Avec le lancement, au mois de mai 2007, du service Internet Dr.Web AV-Desk, développé par Doctor Web, un tout nouveau segment du marché informatique est apparu, celui des services de protection antivirale.

Service Internet Dr.Web AV-Desk

Qu'est-ce que c'est que Dr.Web AV-Desk ?	Dr.Web AV-Desk est un service Internet destiné à fournir un ensemble de services en ligne de protection informatique des ordinateurs et des serveurs au nombre illimité de clients, particuliers et entreprises. Dr.Web AV-Desk est un logiciel, permettant de gérer de manière centralisée le processus de prestation du service « Dr.Web Antivirus ». Dr.Web AV-Desk est un modèle commercial, à l'aide duquel vous pouvez attirer de nouveaux clients et augmenter vos revenus.
A qui est destiné le service Dr.Web AV-Desk ?	Aux fournisseurs de services Internet (FAI) et aux autres sociétés travaillant dans la sphère des technologies informatiques.
Qui sont des utilisateurs finaux du service « Dr.Web Antivirus » ?	Des personnes morales et physiques, les clients des fournisseurs du service.
Quel service le fournisseur peut –il proposer en utilisant Dr.Web AV-Desk ?	Un service de protection informatique des ordinateurs contre les virus, le spam et les logiciels malveillants de toute sorte. Ce service est fourni sous forme d'abonnement pour la durée que souhaite l'utilisateur selon ses besoins. La fourniture de ce service (et donc le droit d'utiliser le logiciel Dr.Web) s'effectue moyennant le paiement de cet abonnement.
Fonctionnalités du logiciel Dr.Web AV-Desk	Dr.Web AV-Desk fournit un service de protection antivirus des PC des clients du fournisseur, géré de façon centralisée.
Licencing de Dr.Web AV-Desk	Le fournisseur du service Dr.Web AV-Desk peut en disposer gratuitement. Le service « Dr.Web Antivirus » est fonction du nombre d'abonnés connectés au service pendant la période d'exercice (mois) et dont les licences ne sont pas expirées.

Comment ça marche ?

Fournisseur du service	Utilisateurs du service
■ Gère l'abonnement au service « Dr.Web Antivirus » via le Centre de gestion de l'abonnement ■ Fournit aux utilisateurs les mises à jour des bases virales et des modules Dr.Web ■ Assure un support technique (optionnel) ■ Surveille l'état du réseau antiviral et collecte les statistiques sur les infections virales ■ Fournit des services supplémentaires ■ Perçoit le paiement de l'abonnement	■ S'abonnent au service via le Centre de gestion de l'abonnement ■ Installent le logiciel Dr.Web ■ Gèrent les paramètres de l'abonnement ■ Paient l'abonnement au service à leur fournisseur

Dr.Web AV-Desk est un modèle commercial à plusieurs variantes. Les FAI ainsi que d'autres sociétés travaillant dans la sphère des technologies informatiques peuvent devenir fournisseurs du service « Dr.Web Antivirus ».

	Revendeur du service « Dr.Web Antivirus »	Fournisseur du service « Dr.Web Antivirus »	Distributeur du service Dr.Web AV-Desk
Mode d'utilisation du service	Cette société effectue l'abonnement au service « Dr.Web Antivirus » des utilisateurs finaux via le Centre de gestion de l'abonnement interne à son site.	Cette société implante le service Dr.Web AV-Desk et fournit le service « Dr.Web Antivirus » aux utilisateurs finaux.	Cette société possède des serveurs sur lesquels elle implante le service Dr.Web AV-Desk, tout en formant son propre réseau de revendeurs du service à qui elle fournit des sous-licences des Centres de gestion de l'abonnement. Le distributeur ne peut fournir le service aux utilisateurs finaux.

Pour en savoir plus sur Dr.Web AV-Desk et le service « Dr.Web Antivirus », nos partenaires peuvent envoyer des requêtes.

Liens utiles

https://pa.drweb.com/training/engineers/

https://pa.drweb.com/training/courses/tech/

Politique de remises

Les coefficients de remises ne sont appliqués qu'au prix de la licence dont la durée est d'un an (selon la liste des prix).

Si l'utilisateur a droit à plusieurs types de remises, elles ne se cumulent pas, mais la plus importante d'entre elle est appliquée (sauf les remises pour les fournisseurs de services IT).

Les remises ne sont appliquées qu'aux solutions figurant dans la liste des prix. Pour avoir la remise pour une solution qui n'y figure pas il faut la négocier avec les administrateurs de Doctor Web.

Remises pour le nombre de produits Dr.Web Enterprise Security Suite, soumisà licence

Les remises pour le nombre de produits achetés (types d'objets protégés) sont calculées à partir de la somme des prix des licences de base et des prix des licences des composants supplémentaires, pour chaque produit à part. Ces remises sont appliquées automatiquement dans le calculateur.

Nombre de produits achetés	Remise
4	30%
3	25%
2	20%

Exception : Aucune remise n'est disponible pour Dr.Web Mobile Security Suite.

Limitations

Les remises ne sont pas octroyées si

- Le nombre de serveurs représente moins de 10% du nombre de postes de travail, d'utilisateurs de la messagerie ou de passerelles ;
- Le nombre d'utilisateurs de la messagerie ou des passerelles est inférieur à 50% du nombre de postes de travail et vice versa ;
- Le nombre d'utilisateurs des passerelles est inférieur au nombre d'utilisateurs de la messagerie et vice versa ;
- Si l'un des produits achetés est Dr.Web Mobile Security Suite.

Tableau de remises

Ces remises sont appliquées par le calculateur si l'avantage correspondant est sélectionné.

Type de client	Causes de remise	Nouvelle licence			Renouvellement			Migration*		
		1 an	2 ans	3 ans	1 an	2 ans	3 ans	1 an	2 ans	3 ans
Catégories qui ne bénéficient pas d'avantages	Pour avoir une remise de renouvellement vous devez soumettre le fichier clé ou le numéro de série Dr.Web dont la durée est au minimum 6 mois pour un produit analogue à Dr.Web	–	1,6	2,2	0,6	1,17	1,72	0,5	1	1,5
	Pour avoir une remise de migration vous devez soumettre l'original de la licence/un fichier clé/un message confirmant l'achat de la version électronique de l' antivirus d'un autre éditeur									
Etablissements d'enseignement et de santé publique, bibliothèques et musées	Copie de licence sur l'activité éducative /du certificat d'enregistrement /de la licence du Ministère de santé publique et un questionnaire rempli	0,5	0,85	1,2	0,35	0,7	1,05			

Conditions de renouvellement

1. On peut renouveler avec remise une licence en vigueur ainsi qu'une licence expirée. Il n'existe pas d'ancienneté pour le renouvellement des licences Dr.Web.
2. Vous pouvez renouveler avec remise la licence pour un produit ou une solution Dr.Web analogue. La durée de la licence doit être d'au moins 6 mois.
3. La remise de renouvellement est accordée à condition de l'achat de la licence d'un, de deux ou de trois ans pour un produit analogue ou une solution analogue à ceux de Dr.Web.
4. La licence de renouvellement avec remise est accordée pour le nombre d'objets protégés ne dépassant pas le nombre de ceux indiqués dans l'ancienne licence que vous renouvelez.
5. Le fichier clé ou le numéro de série Dr.Web sont des moyens de réception d'une remise, mais ils ne peuvent être renouvelés qu'une fois.

Pour avoir une remise de renouvellement l'utilisateur doit soumettre le numéro de série ou le fichier clé (y compris OEM).

Ces remises sont calculées dans le calculateur à condition qu'un avantage soit sélectionné.

« Passez au vert ! »

Programme de migration avantageuse vers Dr.Web pour les utilisateurs d'antivirus d'autres éditeurs.

1. Cette offre spéciale n'est prévue que pour les produits Dr.Web. Les bundles, les utilitaires, les ensembles pour appliances, les services et les solutions ne participent pas au programme de migration avantageuse.
2. La remise n'est pas accordée aux particuliers. Elle peut être offerte aux entreprises, qui ne peuvent pas en bénéficier plus d'une fois.
3. La remise de migration n'est pas accessible aux utilisateurs des licences OEM.
4. Lors de la migration vers une licence Dr.Web d'un an, la remise est égale à 50%. Lors de la migration vers des licences de deux ou trois ans, vous devez multiplier le prix de la licence annuelle Dr.Web par les coefficients 1 et 1,5.
5. La remise lors de la migration d'un antivirus d'un autre éditeur est accordée seulement pour des produits analogues à Dr.Web (selon le type et le nombre d'objets protégés).
6. Pour avoir une remise de migration, l'utilisateur doit soumettre l'original de la licence, le fichier clé ou un message confirmant l'achat d'une licence en ligne de l'antivirus d'un autre éditeur et contenant les données d'enregistrement.
7. La réduction est accordée aux utilisateurs de licences en cours et de licences expirées, à condition que l'expiration ne soit pas supérieure à 30 jours au moment où l'utilisateur contacte un partenaire Dr.Web.
8. Si le délai d'utilisation de l'antivirus d'un autre éditeur n'a pas encore expiré au moment de la migration vers Dr.Web, le temps qui reste est additionné gratuitement à la durée de la nouvelle licence.
9. Le renouvellement ultérieur des licences se fait avec une remise ordinaire de renouvellement.
10. Les remises de migration ne se cumulent pas avec d'autres remises possibles.

Conditions générales de ventes

1. Nos partenaires doivent vendre les logiciels Dr.Web aux utilisateurs finaux conformément à la forme de fourniture prévue par Doctor Web et aux prix recommandés, fixés dans la liste de prix.
2. Pour tous les produits Dr.Web fournis de manière standard, le coût de mise à jour des bases virales et des modules ainsi que le support technique de base, accessible via un formulaire web à la page http://support.drweb.fr, sont inclus dans leur prix, indiqué dans la liste, pour toute la durée de validité de la licence.
3. Lorsque vous commandez des licences en boîte avec label, leur prix augmente. Le prix du package média est alors additionné (sauf l'onglet « DVD des packages média »).
4. Si l'acheteur a besoin de solutions pour protéger un nombre d'objets plus important que ceux indiqués dans la liste de prix, le partenaire doit s'informer des prix auprès de Doctor Web, en soumettant les données suivantes via un formulaire web à l'adresse https://pa.drweb.com/support/ :
   - nom de l'entreprise ;
   - adresse ;
   - e-mail ;
   - numéro de téléphone du responsable de la protection antivirale / du support technique client ;
   - contacts du support technique du partenaire.

Tous les types de remises accordés lors de l'achat de ces solutions doivent être définis en accord avec Doctor Web.

5. Les prix des licences qui ne sont pas mentionnées dans la liste des prix sont déterminés dans le Contrat de licence conclu entre Doctor Web et le fournisseur de ces solutions au client final.

Liens utiles

https://pa.drweb.com/support/price1/

L'achat supplémentaire pour Dr.Web Enterprise Security Suite

Règles générales

1. L'achat supplémentaire (ou extension) de la licence durant sa validité peut être :
   - **Qualitatif** – si de nouveaux composants de protection sont ajoutés à la licence, mais que la composition des produits de la licence ne change pas ;
   - **Quantitatif** – si vous augmentez le nombre d'objets protégés dans le cadre des produits de votre licence actuelle ;
   - **Produit** – si de nouveaux produits sont ajoutés.

L'achat supplémentaire peut également représenter la combinaison de ces trois types.

2. L'achat supplémentaire est possible pour les licences valides encore plus de trois mois.
3. La validité restante de la licence est calculée à partir du nombre de mois restants jusqu'à l'expiration de la licence déjà achetée (le mois incomplet doit être arrondi à 1 mois).
4. Le code de cette licence est C (achat supplémentaire).
5. La licence en achat supplémentaire est automatiquement activée lors de sa génération.
6. La licence précédente sera bloquée 24 heures après l'enregistrement de la licence en achat supplémentaire et il est impossible de la renouveler. Le client doit présenter la licence d'achat supplémentaire pour le renouvellement.

Achat supplémentaire + renouvellement

1. L'achat supplémentaire + renouvellement est possible pour une licence valide, ainsi que pour une licence expirée.
2. Lors d'un achat supp.+renouvellement effectué sur une licence encore valide, la durée de validité restante est ajoutée à la durée de la nouvelle licence.
3. Le code de la nouvelle licence est D (achat supplémentaire + renouvellement).
4. La licence d'achat supplémentaire est automatiquement activée lors de sa génération.
5. La licence précédente (celle qui est renouvelée) sera bloquée dans 24 heures après l'enregistrement de la nouvelle licence (achat supplémentaire + renouvellement) et il est impossible de la renouveler. Le client doit présenter la licence achat supplémentaire + renouvellement pour le renouvellement.
6. Si un achat supp. et un renouvellement sont effectués simultanément, le tarif des licences supplémentaires est basé sur la fourchette de prix correspondant au nombre total de licences achetées (supplémentaires + renouvelées). Le tarif des licences renouvelées est calculé sur la base de fourchette de prix correspondant au nombre total de licences renouvelées.

Règles de calcul du prix de l'achat supplémentaire

I. Achat supplémentaire qualitatif (ajout de composants à la licence tandis que le nombre et le type d'objets protégés ne change pas).

1. Upgrade **d'une licence Antivirus vers une licence Protection complète de Dr.Web Desktop Security Suite** : le tarif mensuel de la licence antivirus est augmenté de 20% puis multiplié par le nombre de mois restants.

Exemple

Un client a payé 1628€ pour la protection de 90 PC avec une licence Antivirus. Il décide de passer à la protection complète deux mois après l'activation de la licence.

1628€ ÷ 12 mois (restants) × 0,2 (20%) × 10 mois = 271€. (Supplément pour la migration vers la protection complète).

Coût total de la licence : **1889€**.

2. Ajout du composant **Antispam** pour Dr.Web Mail Security Suite ou Dr.Web Gateway Security Suite : le tarif de référence (Antivirus ou Antivirus + SMTP proxy) est augmenté de 40%.

Exemple

Il cliente ha acquistato per 1 101,60 Euro una licenza Antivirus per la protezione di 90 utenti della posta elettronica e due mesi dopo ha deciso di aggiungere l'Antispam.

Un client a payé 1300€ pour protéger 90 utilisateurs de messagerie. Il décide d'ajouter l'Antispam deux mois après l'activation de la première licence.

1300€ ÷ 12 mois × 0,4 (40%) × 10 mois = 433€ (Supplément pour l'achat de l'Antispam).

Coût total de la licence : **1733€**.

3. Ajout du composant **SMTP proxy** : le tarif de départ (licence Antivirus ou licence Antivirus+ Antispam) est augmenté de 20%.

Tableau récapitulatif des marges lors de l'achat supplémentaire qualitatif sans augmentation du nombre d'objets protégés

Produit	Licence actuelle	Nouvelle licence	Marge
Dr.Web Desktop Security Suite	Antivirus	Protection complète	20%
Dr.Web Mail Security Suite ou Dr.Web Gateway Security Suite	Antivirus	+ Antispam	40%
	Antivirus + SMTP proxy		
	Antivirus	+ SMTP proxy	20%
	Antivirus + Antispam		

II. Achat supplémentaire quantitatif (augmentation du nombre d'objets protégés)

Le prix de l'achat supplémentaire est calculé en se basant sur la liste de prix en vigueur en fonction du nombre total d'objets protégés, sans aucune remise.

III. Achat supplémentaire Produit (l'extension de la composition des produits)

Le prix de l'achat supplémentaire est calculé en se basant sur la liste de prix en vigueur sans remise pour le nombre de produits.

L'achat supplémentaire n'est pas disponible pour les produits entreprises suivants :

- Dr.Web Bundle TPE.
- Dr.Web Formule Universelle et Bundles Dr.Web pour écoles et lycées.

Pour étendre la licence pour ces produits, il faut migrer vers Dr.Web Enterprise Security Suite suivant les règles de l'achat supplémentaire + renouvellement.

Codes des produits, des bundles et des utilitaires Dr.Web

Règles de formation des codes

1. Chaque code se compose de 5 groupes.
2. Chaque groupe est séparé de l'autre groupe par un trait d'union.
3. Le code de la licence pour la catégorie « Produits » est formé pour chaque produit commercial Dr.Web séparément (voir la rubrique « Gamme des produits Dr.Web Security Suite »).
4. Les codes des DVD, des cartes scratch et des paquets média sont fixes et se trouvent dans la liste de prix.
5. Dans le code de licence « achat supplémentaire », 2 durées sont indiquées : durée générale de la licence achetée en supplément – deux-points – durée restante de la clé soumise en vigueur.
6. Dans le code de la licence « achat supplémentaire + renouvellement », 2 durées sont indiquées : durée commune de la licence renouvelée et de la licence supplémentaire – deux-points – durée restante de la clé soumise en vigueur.
7. Dans le code de la licence « achat supplémentaire», le nombre d'objets protégés est indiqué deux fois : nombre global de licences y compris l'achat supplémentaire – deux-points – nombre d'objets de la licence soumise en vigueur.
8. Dans le code de la licence « Achat supplémentaire+renouvellement, le nombre d'objets protégés est indiqué deux fois : nombre global de licences y compris l'achat supplémentaire et renouvellement – deux-points – nombre d'objets de la licence soumise en vigueur.

Tableau général des symboles de codes

Groupe 1			Groupe 2		Groupe 3	Groupe 4	Groupe 5	
Contenu	**Catégorie du produit**	**Objets protégés**	**Licence de base**	**Composants supplémentaires**	**Durée de la licence**	**Nombre d'objets protégés**	**Type de licence**	**Remise**
L – exemplaire du logiciel téléchargé sur le site	**B** – logiciel pour les entreprises **H** – logiciel pour les particuliers	**G** – utilisateurs de la passerelle	**A** – Antivirus	**A** – Antispam	**XXM** (XX est le nombre de mois)	Nombre	**A** – nouvelle licence	**1** – Education, une Santé, bibliothèque, musée
B – exemplaire du logiciel en boîte **A** – exemplaire du logiciel en boîte, en promotion	**X** – logiciel faisant partie de Dr.Web Office Shield	**M** – mobiles	**B** – Protection complète	**C** – Centre de gestion	**XXXD** (XXX est le nombre de jours)	**UL** – unlimited : Illimitée (pour une licence à durée illimitée)	**B** – prolongation de licence **C** – élargissement de licence	**2** – opération de promotion **3** – pas de remise spéciale
C – carte scratch	**Y** – utilitaire	**P** – utilisateurs de la messagerie	***** – licences pour plusieurs logiciels (uniquement pour les bundles)	**K** – sans composants supplémentaires			**D** – prolongation et élargissement	**4** – migration
D – exemplaire du logiciel en DVD	**Z** – Bundle	**S** – serveurs		**R** – Cryptographe			**F** – licence OEM	**5** – NFR licence pour le partenaire
K – enveloppe avec le certificat de licence		**W** – postes de travail		**S** – SMTP proxy			**G** – licence de service	**6** – NFR licence (démo) pour le client
M – exemplaire du logiciel sur CD/DVD/Clé USB Dr.Web (y compris OEM)		**Z** – tous les objets						**7** – frais marketing ou formation
N – exemplaire du logiciel dans le pack médias								**8** – bienfaisance
P – exemplaire du logiciel dans le pack médias pour les licences OEM								**9** – séparation d'une licence
								10 – rassemblement de plusieurs clés
								11 – remplacement de clé

Contacts

Russie

Doctor Web

2-12A, 3 ulitsa Yamskogo polya, 125124, Moscou, Russie
Tél.: +7 495 789-45-87
Fax: +7 495 789-45-97
www.drweb.com | www.av-desk.com | www.freedrweb.com

Deutschland

Doctor Web Deutschland GmbH

Deutschland, Rodenbacher Chaussee 6, D-63457 Hanau
Tél.: +49 (6181) 9060-1210
Fax: +49 (6181) 9060-1212
www.drweb-av.de

Kazakhstan

Doctor Web – Central Asia

165b/72g, rue Chevtchenko/rue Radostovtsa, office 910
050009, Ville d'Almaty, Kazakhstan
Tél.: +7 (727) 323-62-30, +7 (727) 323-62-31, +7 (727) 323-62-32
www.drweb.kz

Ukraine

Technical support center « Doctor Web »

Pushkinskaya, 27, office 6, Kiyev 01601, Ukraine
Tel/fax: +38 (044) 238-24-35
www.drweb.ua

France

Doctor Web France

333 b Avenue de Colmar, 67100 Strasbourg
Teléfono: +33 (0) 3-90-40-40-20
Fax: +33 (0) 3-90-40-40-21
www.drweb.fr

Japan

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F,
1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken
210-0005, Japan
www.drweb.co.jp

Chine

Doctor Web Software Company (Tianjin), Ltd.

112, North software tower, № 80, 4th Avenue, TEDA, Tianjin, China
天津市经济技术开发区第四大街80号软件大厦北楼112
Tel: +86-022-59823480
Fax: +86-022-59823480
E-mail: y.zhang@drweb.com
www.drweb.com