Besoin de protection ?

Nous avons Dr.WEB®
depuis 1992

Sommaire

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.

Les certificats et les décorations d'État témoignent d'une confiance méritée dont jouit l'antivirus Dr.Web, créé par des spécialistes russes.

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 des 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 potentiellement 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.

Désinfection

- La possibilité de fonctionner sur un ordinateur déjà infecté et une résistance exclusive aux virus distinguent les logiciels Dr.Web des autres produits antivirus
- Dr.Web montre le plus haut taux de désinfection effective des infections actives parmi les autres produits de l'industrie antivirus.
- L'utilisation de technologies uniques de traitement des processus de la mémoire vive et ses excellentes capacités de neutralisation d'une contamination active permettent d'installer Dr.Web directement sur une machine contaminée (sans désinfection préalable).
- La probabilité de réussir la désinfection lors du lancement du scan sur une machine contaminée, même depuis un support amovible, sans installation sur le système (par exemple depuis une clé USB) est très grande.

Autoprotection

Dr.Web possède une immunité solide contre toutes les tentatives des logiciels malveillants de le mettre hors service grâce au composant unique 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.
- Certains produits antivirus modifient le noyau Windows, ce qui peut avoir un impact négatif sur la stabilité du système et créer des vulnérabilités exploitables par les programmes malveillants. Le module Dr.Web SelfPROtect maintient la sécurité de l'antivirus et n'interfère pas dans le fonctionnement du noyau Windows.

Capacités uniques du noyau

- Vérification des archives de tout niveau de compression.
- Dépistage avec une grande précision des objets malveillants empaquetés, même par des outils inconnus de Dr.Web, et leur analyse détaillée afin de détecter les virus dissimulés.
- Excellente détection et neutralisation des virus complexes comme Shadow.based (Conficker), MaosBoot, Rustock.C, Sector.
- Technologies intelligentes de contrôle de la mémoire, permettant d'assurer un blocage des virus actifs avant leur apparition sur le disque dur, ce qui diminue la probabilité d'exploitation des vulnérabilités du système par des logiciels malveillants.
- Dépistage et neutralisation des virus sans corps dans la mémoire vive comme Slammer et CodeRed.

Lutte contre les dangers inconnus

- FLY-CODE une technologie de décompression sans précédent, permettant de décompresser des fichiers utilisant des outils inconnus de Dr.Web.
- 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.
- Le moteur d'analyse heuristique de Dr.Web détecte tous les types des menaces et les classe selon leurs symptômes caractéristiques.
- **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.

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 quelconque, ce qui permet d'économiser le trafic. Il ne demande pas plus d'une mise à jour en 24 heures. Les technologiques 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 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. 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 que les bases des autres éditeurs. 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 voire 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 jours 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.

Dr.Web Enterprise Security Suite

Produits pour entreprises

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 repartis en 5 groupes selon le type d'objets protégés.

Produits commerciaux de Dr.Web	Produits logiciels de Dr.Web
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 KATANA
	Dr.Web pour Linux
	Dr.Web pour macOS
	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 Antivirus pour macOS Server
	Dr.Web pour les serveurs Novell NetWare
Dr.Web Mail Security Suite Protection de messagerie	Dr.Web pour les serveurs de messagerie 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 pour macOS*
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 MIMEsweeper
	Dr.Web pour Qbik WinGate
Dr.Web Mobile Security Suite Protection des appareils portables	Dr.Web pour Android
	Dr.Web pour BlackBerry

Licensing de Dr.Web Enterprise Security Suite

Le licensing des produits, destinés à protéger chaque objet mentionné, est fait à part. Vous devez sélectionner une licence de base pour chacun et, si nécessaire, ajouter des 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 10/8/8.1/7/Vista SP2/XP SP2+ (32-bits). ■ Windows 10/8/8.1/7/Vista SP2 (64-bits).	Protection complète	■ Centre de gestion
		Antivirus	
	■ Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32-bits). ■ Windows 10/8/8.1/7/Vista SP2 (64-bits).	KATANA	■ Centre de gestion
	Linux glibc 2.7 ou supérieur	Antivirus	
	macOS 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		
	macOS 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 Qbik WinGate MIMEsweeper Microsoft ISA Server et Forefront TMG	Antivirus	■ Centre de gestion ■ Antispam
Dr.Web Mobile Security Suite Protection pour les appareils mobiles	Android 4.0–7.1	Protection complète	■ Centre de gestion
	BlackBerry 10.3.2+		

Universalité

Conformément au choix du client, un fichier-clé Dr.Web unique pour la protection de tous les objets sélectionnés sera généré. Le fichier-clé comporte les produits de Dr.Web assurant la protection des objets tournant sous tous les OS et plateformes supportés par Dr.Web. Si l'utilisateur migre d'UNIX vers Windows, et que sa licence est toujours valide, il n'aura pas besoin de changer de clé – il pourra télécharger gratuitement le logiciel nécessaire sur le site www.drweb.fr.

Liens utiles

Description : http://products.drweb.com/enterprise_security_suite/control_center

Centre de gestion Dr.Web

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

Fonctions clé

- 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

- La protection centralisée de tous les nœuds, dispositifs et services du réseau.
- Un prix total minimal par rapport aux logiciels des concurrents grâce à la possibilité de déployer les serveurs sous Windows et UNIX, facilité d'installation et fiabilité de protection.
- La compatibilité avec les versions 32 et 64-bits des systèmes d'exploitation.
- L'Agent antivirus peut être installé sur une machine infectée avec une forte probabilité de traitement.
- L'antivirus offre une utilisation réduite des ressources des ordinateurs et des serveurs grâce à la compacité du moteur antivirus et de ses technologies modernes.
- L'administration à distance via l'interface Web à partir de tout navigateur web.
- Le Centre de Gestion mobile pour les appareils sous Android/iOS.
- L'application des politiques de sécurité souhaitées pour les groupes d'employés.
- La possibilité de nommer des administrateurs qui peuvent être affectés à différents groupes, ce qui rend possible l'utilisation du Centre de Gestion dans des entreprises exigeant un niveau maximal de sécurité, ainsi que dans des sociétés à succursales multiples.
- La configuration de la politique de sécurité pour tous les utilisateurs, y compris mobiles et pour tous les postes de travail - même s'ils ne sont pas présents dans le réseau - ce qui permet d'assurer une protection à jour à tout moment.
- La protection contre la modification de paramètres par les utilisateurs.
- Le blocage de l'accès aux supports amovibles, ressources du réseau local et Internet - protection contre les actions de l'utilisateur.
- La protection des réseaux sans connexion Internet.
- La possibilité de déployer des agents sur les postes de travail via la politique Active Directory, les scripts de démarrage, les mécanismes d'installation à distance. L'installation est possible même si le nœud de réseau est fermé et inaccessible via l'administrateur Web du Centre de Gestion.
- Il est possible d'utiliser la plupart des bases de données existantes, internes et externes. Parmi les dernières supportées, on peut nommer Oracle, PostgreSQL, Microsoft SQL Server, tout Système de gestion de bases de données supportant SQL-92 via ODBC.
- la possibilité de créer des gestionnaires d'événements, ce qui permet d'avoir un accès direct aux interfaces internes du Centre de Gestion.
- Compatibilité - ce produit permet à l'administrateur d'installer et de synchroniser des produits additionnels, ce qui réduit le coût de déploiement de systèmes de sécurité informatique.
- Le système de surveillance de la sécurité est visible, la recherche de postes de travail efficace et facile.
- Il est possible de sélectionner la liste des composants actualisés et de contrôler la migration vers les nouvelles versions permettent aux administrateurs d'installer uniquement les mises à jours nécessaires et testées dans le réseau.

Licensing

Le Centre de gestion possède sa propre licence : il est présent au sein de l'ensemble Dr.Web Enterprise Security Suite, et en qualité d'option lors de l'achat de licence d'un produit isolé Dr.Web. Le Centre de gestion offre la possibilité de diriger les agents de tous les objets protégés, indépendamment de leurs types : postes de travail, serveurs, passerelles Internet et appareils portables. La licence du Centre de gestion est gratuite.

Liens utiles

Description :
http://products.drweb.com/esuite/control_center

Dr.Web Desktop Security Suite

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

- Dr.Web pour Windows
- Dr.Web KATANA
- Dr.Web pour Linux
- Dr.Web pour macOS
- Dr.Web pour 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 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).

Variantes de licence

	Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32-bits) Windows 10/8/8.1/7/Vista SP2 (64-bits)		Windows 10/8/8.1/7/ Vista SP2/XP SP2+ (32-bits) Windows 10/8/8.1/7/ Vista SP2 (64-bits)	Linux	macOS	MS DOS, OS/2
Licence de base	Protection complète	Antivirus	KATANA	Antivirus		
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	■ L'antivirus sans signatures ■ Dr.Web Cloud ■ Centre de gestion	■ Antivirus ■ Anti-espion	■ Antivirus ■ Anti-espion ■ Antirootkit	■ Antivirus ■ Anti-espion ■ Antirootkit
Composants supplémentaires						
Centre de gestion	+	+	+*	+	+	–

* La licence Dr.Web KATANA BE.

Vous pouvez acheter Dr.Web Desktop Security Suite (sauf les scanners en ligne de commande), au sein des bundles économiques Dr.Web pour PME.

OS supportés

Dr.Web pour Windows	Dr.Web pour Linux	Dr.Web pour macOS	Scanners en ligne de commande Dr.Web
Antivirus, Protection complète Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32-bits) Windows 10/8/8.1/7/Vista SP2 (64-bits) **KATANA** Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32-bits) Windows 10/8/8.1/7/Vista SP2 (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)	macOS 10.7 et supérieure (32- et 64-bits)	Windows, MS DOS, OS/2

Dr.Web pour Windows

Protection des postes de travail, des systèmes embarqués, des clients de terminal server et de clients de serveur virtuel

Avantages

- **Licensing flexible**
  A la différence de plusieurs solutions concurrentes, Dr.Web Enterprise Security Suite possède un système flexible et polyvalent de licensing. Le client n'achète que les composants de protection dont il a vraiment besoin et ne paie pas pour des éléments ou des solutions superflues, qu'il n'utilisera peut-être jamais.
- **Gestion centralisée**
  Si une gestion centralisée de la protection des postes de travail est nécessaire, vous devez obtenir la licence du Centre de gestion Dr.Web Enterprise Security Suite. Le Centre de gestion Dr.Web montre un fonctionnement sûr et stable 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
- **Protection complète contre toutes les menaces connues**
  Dr.Web pour Windows assure une protection solide contre presque toutes les menaces existantes. Une qualité de désinfection inégalée et un haut niveau d'autoprotection ne laissent pas de chances aux virus et aux autres objets malveillants de pénétrer dans le réseau protégé. Le pare-feu interne et la fonction Office Control (licence « Protection complète ») ferment l'accès aux virus via les vulnérabilités des systèmes et des logiciels et assure un contrôle solide du fonctionnement des applications installées.
- **Amélioration de la productivité du travail**
  L'implémentation des composants Dr.Web pour Windows assure un effet positif instantané. La diminution du flux de spam (licence «Protection complète») quasiment jusqu'à zéro permet au personnel de travailler avec plus d'efficacité. Les messages importants ne seront plus perdus parmi le courriel non sollicité. La contamination des éléments du réseau n'est plus possible, ce qui réduit les les temps morts liés à la restauration de l'information perdue à cause des virus..
- **Maintien de la réputation de l'entreprise**
  L'implémentation de Dr.Web pour Windows empêche les pirates de transformer le réseau local en source de virus et du spam, qui peuvent atteindre les clients de l'entreprise. L'utilisation de notre produit est une garantie solide pour la réputation de toute entreprise comme bon partenaire d'affaires.

Fonctionnalités principales

- Solution complète pour la protection de l'ordinateur sous Windows.
- Protection en ligne.
- Possibilité d'installation et de fonctionnement sur une machine infectée et résistance exceptionnelle aux virus.
- Détection efficace et neutralisation de tous types de menaces dans le système.
- Haute vitesse de scan grâce à l'utilisation de systèmes multiprocesseurs.
- Protection contre les menaces conçues pour être indétectables par l'analyse heuristique classique ou la détection basée sur les signatures.
- Protection des données contre l'endommagement par les Trojan Encoder.
- Analyse des menaces empaquetées.
- Analyse complète des archives quel que soit le niveau d'emboîtement.
- Détection et neutralisation des virus complexes améliorée.
- Filtrage du spam et de tous les messages non-sollicités sans apprentissage de la part de l'antispam.
- Scan complet «à la volée» de tout le trafic transitant via tous les ports.
- 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 eux-mêmes grâce à la fonctionnalité Safe Search !
- 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 via les serveurs de Doctor Web.
- Protection contre l'accès non autorisé, prévention des fuites de données, blocage des connexions suspectes au niveau des paquets et des applications.
- Administration distante des ordinateurs appartenant à un réseau local, sans installer le Centre de Gestion Dr.Web.

Pré-requis système

OS supportés

- 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)

Liens utiles

Description : http://products.drweb.com/win/workstations

Dr.Web Antivirus pour macOS

Protection standard contre les virus et autres logiciels malveillants développés pour infecter macOS ainsi que les autres systèmes d'exploitation

Avantages

- Une protection fiable contre tous les programmes malveillants
- Une grande vitesse de scan grâce à la technologie de scan asynchrone
- Le Centre de gestion Dr.Web pratique est soumis à licence gratuitement
- Connexion facile au système de protection antivirus centralisé de l'entreprise
- Charge minimale sur le système protégé et consommation faible du trafic lors des mises à jour qui rendent le fonctionnement de Dr.Web pour macOS très discret et presque invisible
- Le style de l'interface rend l'utilisation intuitive et très facile

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.

Pré-requis système

- macOS10.7 ou supérieur (32- et 64-bits)
- RAM - selon les pré-requis système
- Accès à Internet : pour l'enregistrement et la réception des mises à jour.

Liens utiles

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

Dr.Web Antivirus pour Linux

Protection standard contre les virus

Avantages

- Une protection fiable contre tous les programmes malveillants - y compris ceux non encore analysés par le Laboratoire antivirus de Doctor Web.
- Le Centre de Gestion permet de gérer d'une façon centralisée le système de protection antivirus des postes de travail sous Windows, Linux, macOS et d'autres composants du réseau. Connexion facile au système de protection antivirus centralisé de l'entreprise.Le Centre de gestion est soumis à licence gratuitement.
- La charge minimale sur le système protégé et la faible consommation du trafic lors des mises à jour rendent le fonctionnement de Dr.Web pour Linux très discret et presque invisible.
- La technologie de scan asynchrone permet à l'utilisateur d'effectuer instantanément toutes opérations sur tous types de fichiers.
- La nouveauté de la version 10 ! L'analyse complète du trafic HTTP et le contrôle de l'accès aux ressources Internet.
- La nouveauté de la version 10 ! Protection contre les menaces ciblant Windows, lancées sous Linux.
- Même en cas d'erreur lors du scan, Dr.Web pour Linux ne provoque pas de plantage du système d'exploitation.
- L'interface de Dr.Web Antivirus pour Linux rend l'utilisation de Dr.Web intuitive et très facile.

Avantages

- Centre de gestion convivial.
- Analyse « à la volée ».
- Paramétrage des scans utilisateurs.
- Quarantaine gérée.
- Mises à jour automatiques.
- Interface moderne.
- L'analyse complète du trafic HTTP et le contrôle de l'accès aux ressources Internet.
- Protection contre les menaces ciblant Windows, lancées sous Linux.

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.com/linux

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 des 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.com/console

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
- Dr.Web pour les serveurs Novell NetWare
- Dr.Web pour macOS Server
- Dr.Web pour les serveurs UNIX (Samba)

Licensing de Dr.Web Server Security Suite

	Dr.Web pour les serveurs Windows	Dr.Web pour les serveurs Novell NetWare	Dr.Web pour macOS Server	Dr.Web pour les serveurs UNIX
Licence de base	Antivirus	Antivirus	Antivirus	Antivirus
Composants supplémentaires				
Centre de gestion	+	+	+	–

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

OS supportés

Dr.Web pour les serveurs Windows	Dr.Web pour les serveurs Novell NetWare	Dr.Web pour macOS Server	Dr.Web pour les serveurs UNIX
Windows NT/2000/ 2003/2008 (32- et 64-bits)	Novell NetWare version 4.11–6.5	macOS Server 10.7+	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

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

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

- Possibilité d'application à des réseaux exigeant un niveau maximal de sécurité et conformité aux exigences de la loi sur la protection des données personnelles relative aux produits antivirus. Certificats du FSB et du FSTEK.
- 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 fichier 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 fonctionnant 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.com/fileserver/win

Dr.Web pour les serveurs Novell NetWare

Protection antivirale des dépôts de fichiers

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.

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 d'effectuer la configuration de 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.

Pré-requis système

- Novell NetWare 4.11 à 6.5.

Liens utiles

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

Dr.Web Antivirus pour macOS

Protection de base contre les virus et autres logiciels malveillants pour macOS Server

Avantages

- Centre de gestion convivial.
- Rapidité du scan.
- Création de profils de scan personnalisés.
- 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.

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.

Pré-requis système

- macOS 10.7 Server ou supérieur.
- 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.com/fileserver/mac

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.

Pré-requis système

- Dr.Web Daemon (drwebd) version 5.0 ou supérieures.
- Samba 3.0 et supérieure.

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 le mécanisme 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.com/fileserver/UNIX

Dr.Web Mail Security Suite

Protection de messagerie

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

Licensing de 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.

Types 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	Antivirus	Antivirus	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.

OS supportés

Produit	Windows	Linux	FreeBSD	Solaris
		Pour la plate-forme 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	Server 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		

Dr.Web pour les serveurs de messagerie UNIX

Protection antivirus et antispam du trafic de messagerie transitant par les serveurs proxy tournant sous UNIX

Avantages

- **Configuration flexible orientée client**

  Pour configurer Dr.Web pour les serveurs de messagerie UNIX, vous pouvez utiliser les règles de filtrage prédéfinies mais également les modifier selon les besoins individuels du client. Ceci montre la flexibilité du produit par rapport à d'autres solutions, dont la configuration des paramètres ne peut être modifiée. 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 aux besoins de toutes les entreprises en matière de sécurité informatique, en répondant notamment aux exigences de la Loi sur la protection des données personnelles.

- **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.

Fonctions clés

- Filtrage des messages et leur répartition en virus et en spam.
- Analyse des messages et de tous leurs composants.
- Traitement correct de tous les types connus d'archives, y compris les archives multi volume set les archives auto-extractibles (SFX).
- Black et white listes.
- Notifications paramétrées.
- Recueil de statistiques sur tous les aspects de fonctionnement du système.
- Auto protection ment des modules contre les défaillances éventuelles.

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

Plugins :

- Dr.Web est un plugin qui contrôle les emails à la recherche de virus via le moteur Dr.Web
- vaderetro est un plugin filtrant le spam via son propre répertoire Vade Retro
- headersfilter est un plugin qui filtre les messages en fonction de leurs en-têtes

Dr.Web SMTP proxy

La structure modulaire du produit Dr.Web pour les serveurs de messagerie UNIX permet de l'utiliser comme un filtre SMTP proxy, qui traite les messages avant qu'ils n'atteignent le serveur de messagerie.

Le module Dr.Web SMTP proxy est un composant du produit Dr.Web pour les serveurs de messagerie UNIX – peut être installé dans la zone démilitarisée (DMZ), ainsi qu'à l'intérieur du système de messagerie. Grâce à l'emplacement du serveur du contrôle de la messagerie dans la DMZ, et à ce que le serveur de messagerie est isolé 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.

L'utilisation de Dr.Web SMTP proxy:

- renforce la protection du réseau ;
- améliore considérablement la qualité de filtrage grâce à l'absence de restrictions imposées par le serveur de messagerie ;
- diminue 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 ;
- renforce la stabilité de l'analyse des messages et de la sécurité du réseau entier.

Avantages

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.

Vérification d'authenticité de l'adresse IP

Dr.Web SMTP proxy possède la fonction de vérification d'authenticité de l'adresse IP, et 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.

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

Dr.Web SMTP proxy 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, à l'aide de Dr.Web SMTP proxy l'administrateur peut limiter la liste des domaines pour la réexpédition les messages.

OS supportés

- Logiciels d'installation de Linux, au noyau version 2.4.x et supérieure.
- FreeBSD version 6.x et supérieure pour la plateforme Intel x86.
- Solaris version 10 pour la plateforme Intel x86.

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

- Utilisation dans des réseaux d'entreprises exigeant un niveau maximal de sécurité – le produit répond pleinement aux exigences de la législation de la Fédération de Russie et possède des certificats de conformité du FSB et du FSTEK.
- 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.ru/mailserver/exchange

Dr.Web pour IBM Lotus Domino

Protection antivirus et antispam de la plate-forme 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.com/lotus

Dr.Web pour les 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.
- 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 entrants et sortants.

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 macOS

- Espace disque dur : au moins 55 Mo.
- Système d'exploitation : macOS 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.com/mailserver/kerio

Dr.Web Gateway Security Suite

Protection des passerelles Internet et des passerelles de messagerie

- Dr.Web pour les passerelles Internet UNIX
- Dr.Web pour les passerelles Internet Kerio
- Dr.Web pour MIMEswepper
- Dr.Web pour Qbik WinGate

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
Licence de base	Antivirus	Antivirus	Antivirus	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.

OS supportés

Produit	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 les passerelles UNIX

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

Avantages

- Filtrage effectif du trafic au niveau du serveur ICAP, pratiquement sans ralentir la vitesse de téléchargement du contenu.
- Haute évolutivité.
- 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.
- Bonne accommodation aux ressources système.
- Flexibilité et convivialité de l'administration.

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.

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.
- Shweby au moins 1.0.
- SafeSquid 3.0 et supérieur.

Liens utiles

Description : http://products.drweb.com/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 inter-réseau 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.

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 analysés.
- 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 desinformations sur les paramètres des modules, sur la détection des virus pour chaque message et pour chaque virus à part.
- 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).
- 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.
- Pare-feu :
  Kerio Control 8.x ou supérieur.

Liens utiles

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

Dr.Web pour Microsoft ISA Server et Forefront TMG

Avantages

- Plus de possibilités d'installation et de configuration en fonction des exigences de l'entreprise.
- La possibilité d'être utilisé sur tous les serveurs, quelle que soit leur configuration, y compris avec peu de RAM.
- Protection des serveurs virtuels et réels.
- Haute vitesse de scan avec une charge minimale sur le système protégé grâce à la technologie d'analyse multi flux et du contrôle d'utilisation des ressources du serveur.
- L'antispam intégré ne nécessite pas d'apprentissage et fonctionne dès son installation, ce qui permet de réduire considérablement la charge sur le serveur ainsi que d'accroître la productivité des employés de la société.
- Blocage de l'accès aux ressources Web et possibilité de filtrage selon les types de fichiers, permettant de prévenir la pénétration des virus à partir des sites malveillants connus, ainsi que de réduire le volume de trafic.
- Technologie unique de détection des nouvelles menaces (inconnues) et des packers.
- Un système de mise à jour pratique.
- Documentation détaillée en français.

Fonctionnalités principales

La gestion centralisée du produit à partir de (pratiquement) tout ordinateur. la gestion centralisée est assurée via le navigateur en utilisant le protocole sécurisé HTTPS, sans la nécessité d'installer d'autres logiciels.

Antivirus

- Analyse antivirus de tout le trafic entrant , y compris les pièces jointes, via HTTP (y compris FTP sur HTTP) ;
- **Nouveau !** Support des solutions de cluster. Dr.Web pour Microsoft ISA Server et Forefront TMG vous permet de combiner les serveurs avec les pare-feux Microsoft, en un seul cluster (arborescence des serveurs principaux et subordonnés) et de gérer la protection à partir d'un seul serveur
- **Nouveau !** Contrôle du fonctionnement de l'application. En cas d'erreurs de l'application, le service Dr.Web SSM le relance ou le redémarre.
- L'analyse avec des paramètres personnalisés : la sélection de la taille maximale et du type de fichiers analysés, des actions (y compris pour les fichiers invérifiables), et des moyens de traitement des objets infectés.
- Détection des objets malveillants dans les fichiers archivés à plusieurs reprises.
- Traitement des fichiers infectés.
- Blocage de l'accès aux données infectées pour tous les utilisateurs de réseau local.
- Limitation de l'accès des utilisateurs à certains sites Web à l'aide d'Office Control.
- Utilisation de différentes actions en fonction du type de spam.
- Isolation des fichiers infectés et suspects en quarantaine.
- Notification de l'administrateur sur les incidents viraux.
- Journalisation du fonctionnement du logiciel.

Attention !

Dr.Web Antivirus pour Microsoft ISA Server et Forefront TMG traite plus vite les paquets HTTP et les liens par rapport à la version avec l'antispam.

Antivirus + Antispam

En plus des fonctionnalités de l'antivirus :

- Le filtrage antispam du trafic de la messagerie via SMTP et POP3.
- La création de groupes utilisateurs et l'attribution de profils de protection.
- L'ajout d'un texte d'accompagnement aux messages e-mails contenant des menaces.

Pré-requis système

Pour Microsoft ISA Server :

- CPU : Pentium ® III 733 MHz ou supérieur
- RAM : 1 Go et plus.

Espace disponible sur le disque dur : 700 Mo requis pour l'installation. Espace libre supplémentaire requis pour stocker temporairement les données lors de l'analyse antivirus. Elle est déterminée par l'intensité des requêtes des utilisateurs et la taille des fichiers téléchargés par les utilisateurs.

- OS : Microsoft® Windows Server® 2003 x86 avec Service Pack 1 (SP1), Microsoft® Windows Server® 2003 R2 x86.
- Serveur proxy : Microsoft® ISA Server 2004, Microsoft®
- ISA Server 2006.

Pour Microsoft Forefront TMG :

- CPU : Pentium ® III 1.86 GHz ou supérieur.
- RAM : 2 Go et plus.

Espace disponible sur le disque dur : 700 Mo requis pour l'installation. Espace libre supplémentaire requis pour stocker temporairement les données lors de l'analyse antivirus. Elle est déterminée par l'intensité des requêtes des utilisateurs et la taille des fichiers téléchargés par les utilisateurs.

- OS : Microsoft® Windows Server® 2008 SP2, Microsoft® Windows Server® 2008 R2.
- Serveur proxy : Microsoft® Forefront® TMG 2010.

Liens utiles

Description :
http://products.drweb.com/gateway/isa

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 la 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

- Espace sur le disque dur – au moins 35 Mo d'espace libre sur le disque dur.
- 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.com/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

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.

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.

Liens utiles

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

Dr.Web Mobile Security Suite

Protection des appareils portables

- Dr.Web pour Android
- Dr.Web pour BlackBerry

Licensing de Dr.Web Mobile Security Suite

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 Android	Dr.Web pour BlackBerry
■ Protection complète + Centre de gestion	■ Protection complète

Le produit Dr.Web pour Windows Mobile peut être acheté à part aussi bien qu'au sein de l'ensemble Dr.Web Enterprise Security Suite. Dans le dernier cas, vous aurez en supplément une licence du Centre de gestion Dr.Web Enterprise Security Suite.

Les produits Dr.Web pour les outils portables sont accessibles au sein des bundles Dr.Web pour PME.

	Dr.Web pour Android	Dr.Web pour BlackBerry
Composants de la protection*	Antivirus Antispam** Antivol** Filtre URL Pare-feu Contrôleur de sécurité	Antivirus Contrôleur de sécurité
Gestion centralisée de Dr.Web Enterprise Security Suite	+	
OS supportés	Android OS: 4.0–7.1. Le parefeu Dr.Web est compatible avec Android 4.0 ou supérieur, Android TV 5.0+	BlackBerry 10.3.2+
Fonctions clés		
Analyse multi flux avec la répartition des tâches entre les noyaux du processeur	+	
Scan des fichiers reçus via GPRS/Infrarouge/Bluetooth/Wi-Fi/connexion USB ou lors de la synchronisation avec le PC	+	+
Deux types de scan : complet et personnalisé	+	+
Possibilité d'activer/désactiver le scan permanent de la carte mémoire	+	
Restauration du fonctionnement automatique	+	
Scan à la demande du système de fichiers ou de fichiers et dossiers particuliers	+	+
Scan des archives APK, ZIP, SIS, CAB, RAR, JAR	+	+
Interdiction du lancement sur l'appareil mobile des applications non incluses à la liste des applications autorisées par l'administrateur	+	
Configuration des règles pour chaque application	+	
Contrôle du trafic entrant et sortant de chaque application	+	
Option permettant de limiter le trafic lié à l'utilisation de l'Internet mobile	+	
Possibilité de définir des limites pour des applications spécifiques en roaming	+	
Prévention d'accès aux ressources non recommandées sur Internet	+	
Protection contre l'accès non autorisé lors de la connexion aux réseaux sans fil	+	
Déblocage contre les ransomwares	+	
Scanner des vulnérabilités	+	
Création de listes noires et blanches des appels et SMS entrants/sortants	+	
Possibilité d'utiliser plusieurs cartes SIM	+	
Suppression des fichiers infectés	+	+
Isolation des fichiers suspects en Quarantaine	+	+
Restauration des fichiers de la Quarantaine	+	+
Actualisation via Internet : ■ via HTTP en utilisant le module GPRS ; ■ via connexion infrarouge/Bluetooth/Wi-Fi/USB ; ■ via la synchronisation avec le PC avec connexion Internet via ActiveSync	+	+
Rapports détaillés sur les scans du système	+	+
Affichage des informations sur les menaces détectées sur le panneau de verrouillage avec la possibilité de basculer vers la liste des menaces	+	
Notification sur la détection des actions qui sont typiques pour les programmes malveillants	+	
Administration distante de l'appareil mobile en cas de perte ou vol via l'antivol	+	
Réception des coordonnées GPS de l'appareil mobile dans le message SMS	+	

* Pour les appareils sous Android TV seuls les composants Antivirus , Contrôleur de sécurité et Pare-feu sont disponibles.

** Il est impossible d'utiliser ce composant sur les appareils sans emplacement SIM.

Liens utiles

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

Bundles Dr.Web

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

Important! Aucune remise ne s'applique à ce bundle, même la remise de renouvellement. Pour continuer à utiliser cet ensemble de produits vous devez acheter une nouvelle licence. Vous bénéficierez de remise seulement en cas de migration vers des produits isolés de Dr.Web.

Bundle Dr.Web « Formule universelle »

Protection complète pour les PME

Les petites entreprises parfois ne peuvent pas investir des sommes considérables dans une protection informatique complète. Le bundle Dr.Web « Formule universelle » est édité spécialement pour elles. C'est une solution économique pour les entreprises possédant un nombre d'ordinateurs allant de 5 à 50.

Produits	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mail Security Suite	Dr.Web Gateway Security Suite	Dr.Web Mobile Security Suite
Objets protégés	Postes de travail	Serveurs	Utilisateurs de messagerie	Utilisateurs de passerelles de messagerie et Internet	Appareils portables
Licence	Protection complète	Antivirus	Antivirus + Antispam	Antivirus	Antivirus
Nombre	De 5 à 50	1	Est égal au nombre des postes de travail	Est égal au nombre de postes de travail (à partir de 25)	Est égal au nombre des postes de travail

Liens utiles

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

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://curenet.drweb.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), iPhone 4, iPod touch 4 iOS 7.0+.
Qu'est-ce que c'est que «Mon Dr.Web CureNet!»?	C'est un espace privé où est sauvegardé le lien de téléchargement du fichier d'installation durant toute la période de validité de la licence. Vous pouvez également accéder au 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.
Pré-requis système	**Guide** ■ PC sous 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). ■ RAM : au moins 360 Mo. ■ Espace disponible sur le disque dur : au moins 200 Mo. ■ Connexion TCP/IP à tous les postes de travail analysés. ■ Une connexion Internet est nécessaire pour actualiser les composants et les bases virales de Dr.Web CureNet! **Scanner** ■ PC sous MS Windows XP Professional et versions supérieures, sauf Windows® Server 2003 x64 Edition et Windows® XP Professional SP2 x64 Edition. ■ RAM : au moins 360 Mo. ■ Espace disponible sur le disque dur : au moins 200 Mo.

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. ■ L'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 10/8/7/Vista/2012/2008 (32- et 64-bits), XP/2003 (32-bits)
Licences	Vous pouvez acheter une licence pour 12, 24 et 36 mois.
Particularités de licensing	Cet utilitaire est gratuit pour les particuliers.
Version démo	Il n'existe pas de version démo.

Russie

SARL Doctor Web

12A/2, 3-ème rue Yamskogo polya, 125040, Moscou, Russie

Téléphone : +7 (495) 789-45-87

Fax : +7 (495) 789-45-97

www.drweb.ru | curenet.drweb.ru | www.av-desk.com | free.drweb.ru

France

Doctor Web France

333b, Avenue de Colmar, 67100 Strasbourg

Téléphone : +33 (0) 3 90 40 40 20

www.drweb.fr

Allemagne

Doctor Web Deutschland GmbH

Allemagne, 63457, Hanau-Wolfgang, Rodenbacher Chaussee 6

Téléphone : +49 (6181) 9060-1210

Fax : +49 (6181) 9060-1212

www.drweb-av.de

Kazakhstan

SARL Doctor Web –Asie Centrale

165b/72g, rue Chevtchenko/rue Radostovtsa, office 910
050009, Ville d'Almaty, Kazakhstan

Téléphone : +7 (727) 323-62-30, 323-62-31, 323-62-32

www.drweb.kz

Ukraine

Centre de support technique Doctor Web

01601, Ukraine, Kiev, Pushkinskaya, 27, oficina 6

Teléfono/Fax: +380 (44) 238-24-35

www.drweb.ua

Japan

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F,
1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken
210-0005, Japan

Tel: +81 (0) 44-201-7711

www.drweb.co.jp

China

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: D.Liu@drweb.com

www.drweb.com