Dr.WEB®
desde 1992

Protege lo creado

Línea de productos Dr.Web® Security Suite

Guía de licenciamiento

Vigente desde el 01.07.2013
Actualizado al 10.06.2016

Contenido

Sobre la compañía Doctor Web 5
Tecnologías Dr.Web 5
Tecnologías 5
Desinfecta los virus 6
Dr.Web detecta y desinfecta los virus con eficacia 6
Alto nivel de autodefensa 6
Tecnología avanzada de protección preventiva 7
Tecnologías de filtrado antispam 7
Ventajas de Antispam Dr.Web 8
Organización especial de base de datos de virus Dr.Web 8
Ventajas de la base de datos de virus Dr.Web 9
¿Qué le da al usuario el pequeño tamaño de la base Dr.Web y el número de entradas inferior? 9
Sistema global de actualizaciones Dr.Web (Dr.Web GUS) 9
Licencias y Certificados 10
Certificado de licencia Dr.Web 11
Línea de productos Dr.Web® Security Suite 12
Licenciamiento de productos Dr.Web 12
Tipos de entrega de productos Dr.Web 14
Licencia electrónica Dr.Web 14
Media kit Dr.Web en caja de cartón 14
Solución particular en caja de cartón 14
Paquete de medios certificado 15
Paquete de licencia Dr.Web 15
Scratch Card 15
Productos OEM Dr.Web 16
Dr.Web Home Security. Productos para el hogar 18
Composición de los productos 18
Componentes de protección de Dr.Web Security Space 18
Dr.Web Security Space 20
Componentes de protección 20
Antivirus Dr.Web para Windows 24
Dr.Web Katana 26
Antivirus Dr.Web para OS X 28
Antivirus Dr.Web para Linux 29
Escáneres de consola Dr.Web 30
Dr.Web Mobile Security 31
Componentes de protección Dr.Web Mobile Security 31
Dr.Web para Android 31
Dr.Web para Blackberry 33
"Dr.Web Universal" (para clientes ASC) 33
Dr.Web Enterprise Security Suite. Productos para empresas 34
Algoritmo para seleccionar el producto deseado 35
Centro de Control Dr.Web. 36
Dr.Web Desktop Security Suite 38
Sistemas operativos compatibles 38
Licenciamiento Dr.Web Desktop Security Suite 38
Opciones de licencias 38
Dr.Web Server Security Suite 39
Sistemas operativos compatibles 39

10.06.2016

Opciones de licencias ... 39
Dr.Web para servidores Windows ... 40
Dr.Web para OS X Server ... 41
Dr.Web para servidores Novell NetWare ... 42
Dr.Web para servidores UNIX ... 43
Dr.Web Mail Security Suite ... 45
Sistemas operativos compatibles ... 45
Licenciamiento Dr.Web Mail Security Suite ... 45
Opciones de licencias ... 46
Dr.Web para servidores de correo y puertas de enlace UNIX ... 46
Proxy SMTP Dr.Web ... 48
Dr.Web para MS Exchange ... 49
Dr.Web para IBM Lotus Domino ... 50
Dr.Web para servidores de correo Kerio ... 52
Dr.Web Gateway Security Suite ... 53
Sistemas operativos compatibles ... 53
Licenciamiento Dr.Web Gateway Security Suite ... 54
Opciones de licencias ... 54
Dr.Web para puertas de enlace UNIX ... 55
Dr.Web para puertas de enlace Kerio ... 56
Dr.Web para MIMEsweeper ... 57
Dr.Web para Qbik WinGate ... 58
Dr.Web para Microsoft iSA Server y Forefront TMG* ... 58
Dr.Web Mobile Security Suite ... 60
Licenciamiento Dr.Web Mobile Security Suite ... 61
Opciones de licencias ... 61
Dr.Web Retail Security Suite. Productos para la venta al por menor ... 62
"Dr.Web Universal" (para clientes ASC) ... 62
Kits Dr.Web ... 63
Kit Dr.Web «Universal» ... 63
Kit Dr.Web para escuelas ... 63
Utilidades ... 64
Dr.Web CureNet! ... 64
Dr.Web Cureit! ... 65
Dr.Web LiveDemo ... 65
Soluciones ... 66
Dr.Web Security Suite para UNIX Appliance ... 66
Dr.Web ATM Shield ... 66
Servicios ... 68
Servicio de internet Dr.Web AV-Desk ... 68
¿Cómo funciona? ... 69
Política de descuento ... 70
Descuentos disponibles por la cantidad de productos licenciados Dr.Web Enterprise Security Suite ... 70
Tabla de descuentos ... 70
"¡Cambie a verde!" ... 71
Condiciones generales de venta ... 72
Compra adicional para Dr.Web Enterprise Security Suite ... 73
Cuadro general de sobretasas en la compra adicional cualitativa sin aumentar el número de objetos protegidos ... 74
Códigos de productos, kits, herramientas — conjuntos de software y hardware Dr.Web ... 75

10.06.2016

Tabla general de símbolos de códigos 76
Ejemplos 77
Ejemplos de códigos de licencia para la categoría “Productos” 77
Ejemplos de códigos de licencia para la categoría “Kits” 77
Ejemplos de códigos de licencia para la categoría “Utilidades” 77
Contactos 78

Sobre la compañía Doctor Web

La compañía Doctor Web es el famoso elaborador ruso de medios de protección de información.

Los productos de Dr.Web se están elaborando desde el año 1992 y demuestran constantemente los excelentes resultados de detección de malware. La fundación de Doctor Web en diciembre de 2003 marcó el comienzo del crecimiento rápido de ventas de productos Dr.Web tanto en Rusia como en otros países.

Hoy en día Doctor Web es una compañía exitosa de crecimiento rápido, que desempeña un papel principal en el mercado de la seguridad informática. Cuenta con el núcleo antivirus de su propio elaboración, tiene su propio laboratorio de antivirus, un servicio global de monitoreo de virus y el servicio de soporte técnico.

El objetivo estratégico de la compañía en que se concentran los esfuerzos de todo el personal, consiste en crear medios de protección antivirus que satisfacen todos los requisitos modernos. No menos importante es el desarrollo de nuevas soluciones tecnológicas que permiten a los usuarios enfrentar todo tipo de amenazas informáticas. La línea de productos antivirus de Doctor Web cubre una amplia gama de sistemas operativos y aplicaciones compatibles.

La distribución de los productos se basa en una red de socios, evitando las ventas directas a los usuarios finales.

Los consumidores de productos Dr.Web son los usuarios domésticos de diferentes partes del mundo, grandes empresas rusas, las organizaciones pequeñas y grandes corporaciones, a quienes el equipo de Doctor Web está agradecido por el apoyo y confianza de muchos años a los productos. Certificados y premios estatales demuestran alta confianza en el antivirus Dr.Web creado por los programadores rusos ingeniosos.

Tecnologías Dr.Web

Antivirus Dr.Web es una familia de programas informáticos creados por los programadores rusos ingeniosos bajo la dirección de Igor Danilov.

Doctor Web es uno de los pocos vendedores antivirus en el mundo que tiene sus propias tecnologías únicas para detectar y desinfectar los programas maliciosas. La compañía tiene su propio servicio de monitoreo del virus y laboratorio analítico. Debido a eso, los expertos pueden responder rápidamente a las nuevas amenazas de virus y ser capaz de atender a sus clientes en la solución de problemas de cualquier complejidad en cuestión de horas.

Una característica importante de Dr.Web es su arquitectura modular. Todos los productos y soluciones incluyen un núcleo antivirus común, y también utilizan un único sistema de actualizaciones de la base de datos de virus y el sistema global de soporte técnico. Las tecnologías Dr.Web permiten organizar la protección de información fiable tanto en grandes redes corporativas, como en el ordenador de casa o una oficina de casa.

Además de los virus y malware, Dr.Web puede detectar y eliminar programas no deseados (adware, programas de sonido, programas de bromas, software de riesgo, programas de descifrado – spyware/riskware), spam y los correos electrónicos no deseados (phishing, pharming, estafas y mensajes rebote).

Tecnologías

El antivirus de calidad debe ser capaz no sólo de localizar virus, sino también de tratarlo. Por un lado se trata de eliminar los archivos infectados junto con información valiosa, y por otra parte, convertirlos en su estado original "saludable". Dr.Web trata con cuidado los archivos de usuario.

Desinfecta los virus

Un indicador importante de la calidad de funcionamiento de una aplicación antivirus no es sólo su capacidad de detectar los virus, sino también desinfectarlos, sin tener que eliminar los archivos infectados junto con información importante para el usuario, y devolverlos a su estado "de salud" original.

Los virus tecnológicamente sofisticados y peligrosos, especialmente creados para fines comerciales, están comprobados en todas las bases de datos de virus por sus autores antes de su implementación, para que el virus no se detecte por antivirus el mayor tiempo posible. Estos virus no pueden ser detectados por ningún antivirus antes de que sus firmas ingresen al laboratorio.

Dr.Web detecta y desinfecta los virus con eficacia

- La posibilidad de instalar Dr.Web en un equipo infectado y su resistencia excepcional contra los virus, lo distinguen entre todas las aplicaciones similares.
- El uso de tecnologías únicas de gestión de procesos en la memoria y excelentes capacidades de neutralización de infección activa, permiten instalar Dr.Web en un equipo infectado (sin necesidad de desinfección previa), hasta desde una unidad extraíble (por ejemplo USB-stick) y realizar la desinfección de amenazas activas en el proceso de instalación.
- La integración del paquete de instalación (instalador) con Antirootkit Dr.Web actualizado permite enfrentar las amenazas activas y al momento de instalación realizar la desinfección del equipo, aunque esté infectado por aplicaciones malware sofisticadas.
- El subsistema del escaneo de fondo y neutralización de amenazas activas en Antirootkit Dr.Web (Antirootkit API, arkapi) reside en la memoria y realiza la búsqueda de amenazas activas en las siguientes áreas críticas de Windows: objetos de inicio automático, procesos y módulos ejecutados, heuristicas de objetos del sistema, memoria operativa, discos de MBR/VBR, BIOS del sistema. Al detectar una amenaza, el subsistema realiza la desinfección y bloquea los efectos peligrosos.
- Dr.Web ha implementado la posibilidad de detectar y neutralizar los virus existentes en la memoria, nunca detectados como archivos separados. **Hasta ahora hay pocos antivirus capaces de tratarlos**.
- Dr.Web puede identificar con máxima precisión el malware empaquetado, comprimido con un método desconocido por Dr.Web, descifrar sus componentes y analizarlos detalladamente con el fin de detectar las amenazas ocultas.
- Sólo Dr.Web es capaz de analizar por completo los archivos de cualquier nivel de anidación. Por lo tanto, incluso si el objeto malware ha sido comprimido varias veces y han sido utilizados varios tipos de archivadores, Dr.Web detectará y desinfectará la amenaza sin falta.

Alto nivel de autodefensa

La inmunidad resistente frente a cualquier malware que intente poner fuera de servicio Dr.Web, se proporciona gracias a un componente de autodefensa de Dr.Web SelfPROtect, que no tiene análogos en el mercado de antivirus.

- Dr.Web SelfPROtect esta implementado como un controlador, que opera en el nivel más bajo del sistema. La eliminación y la detención de este proceso no es posible sin reinicio del sistema.
- Dr.Web SelfPROtect restringe el acceso de elementos malware a la red, archivos y carpetas, algunas ramas de registro y unidades extraíbles a nivel de controlador del sistema, protege contra los intentos de aplicaciones contra antivirus de detener el funcionamiento de Dr.Web.
- A diferencia de otros productos competidores que modifican el kernel de Windows (interceptan interrupciones, sustituyen las tablas de vectores, utilizan las funciones no do-

cumentadas y etc.), que puede conducir a problemas importantes en el funcionamiento del sistema operativo y crea nuevas formas de uso de vulnerabilidades, el módulo de protección de Dr.Web SelfPROtect es completamente autónomo.

- Posibilidad de restauración automática de propios módulos.

Tecnología avanzada de protección preventiva

- FLY-CODE es una tecnología de extracción universal que no tiene análogos, y permite detectar los virus, comprimidos por archivadores incluso desconocidos por Dr.Web.
- La tecnología única de búsqueda no basada en firmas Origins Tracing™ permite detectar con alta probabilidad los virus, aún desconocidos por las bases de datos de virus Dr.Web.
- El analizador heurístico Dr.Web detecta todos los tipos de amenazas difundidas, determinando su clase según los resultados del análisis y sus características.
- A partir de la versión 8.0 los productos Dr.Web utilizan tecnologías (que están mejorándose constantemente) de protección preventiva del ordenador contra la infección mediante el bloqueo de modificación automática de objetos críticos de Windows, así como control de ciertas acciones inseguras.

Tecnologías de filtrado antispam

Tecnologías de filtrado de Antispam Dr.Web se componen de varios miles de reglas que condicionalmente pueden ser divididos en varios grupos.

Análisis heurístico

Tecnología extremadamente compleja y altamente intelectual del análisis empírico de todas las partes del mensaje: campo de encabezado, el cuerpo del mensaje, etc. Se analiza no sólo el mensaje en sí, sino también el contenido de archivo adjunto, si hubiese. El analizador heurístico se está mejorando constantemente añadiendo nuevas reglas permanentemente. El analizador heurístico funciona "en el avance" y permite identificar la variedad hasta ahora desconocida del spam de nueva generación antes de que aparezcan actualizaciones pertinentes.

Filtrado de oposición

Filtrado de oposición es una de las tecnologías más avanzadas y eficientes de antispam Dr.Web. Consiste en reconocimiento de los trucos utilizados por los spammers para eludir los filtros antispam.

Análisis basado en el código HTML-firma

Los mensajes, que incluyen código HTML se comparan con muestras de firmas HTML antispam de la biblioteca. Tal comparación, en combinación con los datos sobre el tamaño de las imágenes que normalmente utilizan los spammers, protege a los usuarios contra mensajes spam con código HTML, que a menudo incluyen imágenes en línea.

Tecnología de detección de spam por los sobres de mensajes

Detección de falsificaciones en "matasellos" de servidores SMTP y en otros elementos contenidos en los encabezados de los mensajes de correo, es la última tendencia en el desarrollo de métodos de lucha con el spam. No se debe confiar en la dirección del remitente de correo electrónico, ya que éste puede ser falso. Correos falsos no son sólo de spam, podría ser un engaño o un medio de presión sobre el personal, por ejemplo, anónimos e incluso amenaza. Las tecnologías especiales de antispam Dr.Web permite definir direcciones falsas y no recibirlos. Esto ahorra el tráfico y protege a los empleados de la recepción de correos electrónicos falsos que pueden dar lugar a acciones impredecibles.

Análisis semántico

Este análisis compara las palabras y frases del mensaje con las palabras y modismos típicos para el spam. La comparación se basa en un diccionario especial, donde se analizan palabras, frases y símbolos tanto visibles como ocultos a los ojos humanos por medio de trucos técnicos especiales.

Tecnología anti scamming

Mensajes scam (así como pharming mensajes, que son una especie de scam), quizás, el tipo más peligroso de los mensajes de spam, lo que incluye las llamadas "estafas nigerianas", lotería, casino, cartas falsas de los bancos e instituciones de crédito. Para su filtrado el antispam Dr.Web utiliza un módulo especial.

Filtrado de spam técnico

Los llamados mensajes bounce se producen como reacción a virus o una manifestación de la actividad viral, por ejemplo, como resultado de actuación de gusano de correo electrónico, que envía cartas o mensajes sobre correos no entregados, que no son menos deseables que el spam. El módulo especial de antispam Dr.Web detecta tales mensajes como no deseados.

Ventajas de Antispam Dr.Web

- La comprobación de correo electrónico entrante y saliente se realiza en tiempo real.
- El funcionamiento de Antispam no depende del programa de correo utilizado y no aumenta el tiempo, al recibir el correo.
- El antispam no requiere configuraciones y comienza a actuar automáticamente, al recibir el primer mensaje.
- Diferentes técnicas de filtrado proporcionan una alta probabilidad de detectar el spam, phishing, pharming, estafas y mensajes rebote con casi cero falsos positivos.
- Los mensajes de correo electrónico filtrados no se eliminan, sino se mueven a una carpeta especial de su programa de correo electrónico, donde se puede verificar las falsas alarmas en el tiempo más conveniente para el usuario.
- El módulo de analizador de spam es absolutamente autónomo; para su funcionamiento no se requiere conexión al servidor externo o acceso a alguna base de datos, lo que permite ahorrar el tráfico significativamente.
- Antispam Dr.Web se actualiza diariamente. Tecnologías únicas de detección de correo electrónico no deseado basadas en varias miles de normas permiten ejecutar actualizaciones no más de una vez al día, ahorrando el tráfico.

Organización especial de base de datos de virus Dr.Web

El tamaño de base de datos de virus Dr.Web es el más pequeño entre todos los programas antivirus existentes. Esto ha sido posible gracias al desarrollo de la tecnología propia para crear la base de virus a base de un lenguaje muy flexible, desarrollado especialmente para la descripción de las bases. El tamaño pequeño de la base de virus asegura el ahorro de tráfico, permite ocupar menos espacio en la unidad una vez instalada, así como en la memoria operativa, en comparación con las bases de otros productores. El tamaño pequeño de la base de virus permite a los componentes del programa Dr.Web interactuar en modo de alta velocidad, sin sobrecargar el procesador.

¿Qué es lo más importante en el antivirus? Asegurar la protección contra los virus. Se asegura la protección, entre otras cosas, introduciendo en la base de virus las entradas (firmas), lo que permite detectar los virus. Pero el número de las entradas en la base de virus no dice

nada sobre cuántos virus realmente captura uno u otro programa antivirus. Para explicar por qué el número de entradas en la base de virus Dr.Web es inferior al número de entradas en las bases de virus de algunos otros productores, hay que saber que no todos los virus son únicos. Hay familias enteras de virus familiares (similares), hay virus diseñados por constructores de virus. Los desarrolladores de algunos otros antivirus, describen tal virus gemelo con un registro separado, lo que aumenta el peso de base de datos. Otro principio se aplica en la base de virus Dr.Web, donde una sola entrada de virus permite neutralizar docenas y centenas, y a veces hasta miles de los virus semejantes uno a otro.

Ventajas de la base de datos de virus Dr.Web

- El número de registros es espectacularmente mínimo.
- Pequeño tamaño de actualizaciones.
- Sólo una entrada detecta decenas, cientos o incluso miles de virus similares.

La diferencia principal de la base de virus Dr.Web de las bases de virus de otros programas consiste en que, disponiendo del número inferior de entradas, permite detectar el mismo número (e incluso superior) de virus y programas maliciosas.

¿Qué le da al usuario el pequeño tamaño de la base Dr.Web y el número de entradas inferior?

- Ahorro de espacio en disco. Ahorro de memoria operativa
- Ahorro del tráfico al descargar la base.
- Alta velocidad de instalación de la base y de su procesamiento, al analizar los virus.
- Posibilidad de detectar los virus que aparecerán en el futuro por medio de modificar los conocidos.

Sistema global de actualizaciones Dr.Web (Dr.Web GUS)

- Servicio de monitoreo de virus Dr.Web recoge muestras de virus de todo el mundo.
- Actualizaciones "calientes" se emiten inmediatamente después de un nuevo análisis de amenazas de virus y preparación de actualizaciones.
- Antes de lanzar una actualización, se la ponen a prueba en una enorme cantidad de archivos "limpios".
- Las actualizaciones llegan a los usuarios desde varios servidores ubicados en diferentes partes del mundo, lo que minimiza el tiempo para las actualizaciones.
- El proceso de actualización de bases de datos y los módulos de programa está totalmente automatizado. Las actualizaciones pueden descargarse como un archivo comprimido.

Licencias y Certificados

A diferencia de soluciones concurrentes, productos Dr.Web Enterprise Security Suite versión 6 tienen los certificados de conformidad FSTEK, FSB y el Ministerio de defensa de la Federación de Rusia. Lo cual permite usarlos en organizaciones con altas demandas en el nivel de seguridad.

Dr.Web está certificado por FSTEK para corresponder:

- TU y NDV4 sobre el uso en el subsistema de protección antivirus dentro de sistemas informativas de los datos personales (ISPDn) de clase K1;
- a los requisitos (cuatro mínimo en el nivel de control) del documento dirigente de la Comisión Técnica Estatal de Rusia sobre "Protección contra el acceso no autorizado a la información". Parte 1. Software de protección de información. Clasificación en el nivel de control de ausencia de capacidades no declaradas y los requisitos de condiciones técnicas.

Dr.Web completamente satisface las exigencias de la ley "Sobre los datos personales" planteadas para productos antivirus en términos de protección contra el acceso no autorizado y protección centralizada de canales de transmisión de datos, y puede ser utilizado en las redes, que corresponden al nivel máximo posible de seguridad.

La compañía Doctor Web tiene siguientes licencias y certificados:

- licencias del Servicio Federal de Control Técnico y de Exportación de la Federación de Rusia (FSTEK) para realizar actividades relacionadas con la elaboración de medios de seguridad de información, así como las actividades de desarrollo y (o) producción de medios de protección de la información confidencial;
- licencia del Ministerio de Defensa de la Federación de Rusia sobre las actividades en el campo de elaboración de herramientas de protección de la información;
- licencia FSB de Rusia para ejecución de trabajos relacionados con el uso de la información que constituye secreto de Estado;
- licencia de Centro de licenciamiento, certificación y protección de los secretos de Estado de FSB de Rusia para el desarrollo y (o) la producción de medios de protección de la información confidencial;
- certificados de conformidad FSB de Rusia;
- certificados de conformidad FSTEK de Rusia.

Todas las licencias y certificados de Doctor Web:
http://company.drweb.com/licenses_and_certificates

Certificado de licencia Dr.Web

Certificado de licencia Dr.Web es la certificación documental de la legalidad del uso de software Dr.Web para los organismos de control.

¡IMPORTANTE! El certificado de licencia Dr.Web no es motivo para la renovación de licencias y para obtención de descuento en renovación.

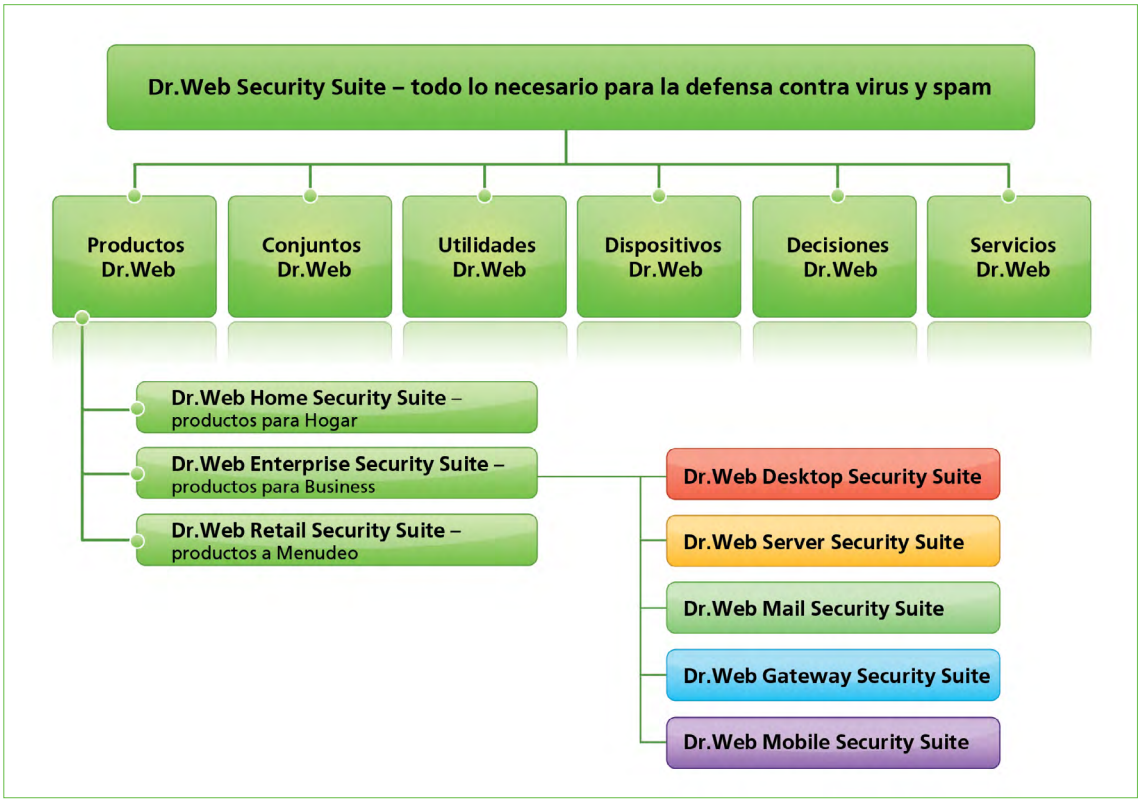
El certificado tiene alto grado de protección. Gracias a una red guilloquis especial su falsificación se hace imposible.

Entrega del formulario del Certificado de Licencia con cualquier producto Dr.Web para las personas jurídicas es obligatoria.

- Una copia electrónica del Certificado de Licencia Dr.Web se puede obtener en la página web http://products.drweb.com/register/certificate.

Línea de productos Dr.Web® Security Suite

Línea de productos Dr.Web Security Suite se compone de productos comerciales para el hogar, negocio y al por menor, kits, herramientas, conjuntos de software y hardware, soluciones y servicios.



Licenciamiento de productos Dr.Web

1. Los productos Dr.Web® están disponible para 12, 24 y 36 meses. Dr.Web Security Space y Dr.Web Antivirus también tienen licencias de 3 y 6 meses.
2. Los productos de Dr.Web están licenciados según el tipo de objetos protegidos.
3. Los objetos protegidos incluyen:
   - estaciones de trabajo, clientes de servidores terminales y clientes de sistemas integrados;
   - archivo y servidores de aplicaciones (incluyendo servidores terminales);
   - usuarios de correo;
   - los usuarios de correos y puertas de enlace de Internet; dispositivos móviles.
4. Existen 2 tipos de **licencias básicas**:
   - Antivirus;
   - Protección completa.
5. La licencia básica **Protección completa** está destinada sólo a los productos para la protección de estaciones de trabajo bajo OS Windows.
6. La licencia **Protección completa** incluye los siguientes componentes: antivirus, antispam, antivirus web, control paterno (de oficina), firewall.
7. Los componentes adicionales de protección que los clientes necesiten, se agregan a la licencia básica. La venta de licencias para uno o más componentes adicionales por separado de la licencia básica no se admite.
8. Para cada tipo de objetos protegidos existen sus tipos de licencias básicas y su conjunto de componentes adicionales.

Objetos protegidos	Sistemas operativos compatibles y plataformas	Licencia básica	Componentes adicionales:
Dr.Web Desktop Security Suite Estaciones de trabajo Clientes de servidores terminales Clientes de servidores virtuales Clientes de sistemas integrados	Windows 8.1/8/7/Vista/XP	Protección completa	▪ Centro de Control
		Antivirus	
	OS X Linux	Antivirus	▪ Centro de Control
	MS DOS OS/2		–
Dr.Web Server Security Suite Servidores de archivos Servidores de aplicaciones Servidores terminales Servidores virtuales	Windows Novell NetWare OS X Server UNIX (Samba)	Antivirus	▪ Centro de Control
Dr.Web Mail Security Suite Usuarios de correo electrónico	UNIX MS Exchange	Antivirus	▪ Centro de Control ▪ Antispam ▪ SMTP proxy
	Lotus (Windows/Linux)		▪ Antispam ▪ SMTP proxy
	Kerio (Windows/Linux)		▪ SMTP proxy
Dr.Web Gateway Security Suite	Gateways de Internet Kerio Gateways de Internet UNIX	Antivirus	▪ Centro de Control
	Microsoft ISA Server y Forefront TMG MIMEsweeper Qbik WinGate		▪ Antispam
Dr.Web Mobile Security Suite Dispositivo móvil	Android	Protección completa	▪ Centro de Control ▪ Antispam
	Symbian OS	Antivirus	▪ Antispam
	Windows Mobile		

Tipos de entrega de productos Dr.Web

Programas Dr.Web se entregan en forma de licencia electrónica o como media kit en el paquete.

1. Licencia electrónica Dr.Web

Se entrega como número de serie Dr.Web:

- por correo electrónico;
- en el certificado de licencia.

2. Media kit Dr.Web en caja de cartón

Contenido del paquete:

- caja de cartón de marca; certificado de licencia;
- breve manual de instalación y registro;
- unidad de DVD;
- un sobre de marca para el disco; pegatina emplomada;
- pegatina “Protegido por Dr.Web”; memoria USB (sólo para producto Dr.Web para OS X + Dr.Web Security Space).

3. Solución particular en caja de cartón

Solución particular para uno o más productos Dr.Web Enterprise Security Suite.

Contenido del paquete:

- caja de cartón de marca Dr.Web;
- formulario de licencia de certificado;
- unidad de DVD con la distribución de software Dr.Web en un sobre de marca.

4. Paquete de medios certificado

Solución particular para uno o más productos Dr.Web Enterprise Suite de Seguridad, certificado por FSTEK de Rusia.

Contenido del paquete:

- caja corporativa de cartón Dr.Web;
- formulario de licencia de certificado;
- unidad de DVD con la distribución de software Dr.Web en un sobre de marca.
- formulario con pegatina holográfica FSTEK.

5. Paquete de licencia Dr.Web

Solución particular para uno o más productos Dr.Web Enterprise Security Suite.

Contenido del paquete:

- caja corporativa de cartón Dr.Web;
- formulario del certificado de licencia.

6. Scratch Card

Tarjeta rasca que contiene número de serie Dr.Web escondido.

7. Productos OEM Dr.Web

Dr.Web OEM universal (licencia para un solo usuario)

Se entrega como tarjetas OEM con zona de rascar pegada al volante OEM. Proporciona protección para 1 PC y 1 dispositivo móvil durante 3 meses.

Composición de licencia:

- Dr.Web Security Space
- Antivirus Dr.Web para OS X
- Antivirus Dr.Web para Linux
- Dr.Web Mobile Security
- Dr.Web para Android OS Dr.Web para Symbian OS Dr.Web para Windows Mobile

Renovación

- Para renovar la licencia OEM Dr.Web, se debe adquirir la licencia de renovación (su precio incluye el descuento en la renovación).
- También se puede renovar la licencia por medio de productos en caja Dr.Web Security Space o Antivirus Dr.Web (sin descuento en renovación). En este caso, se añadirán al plazo de la nueva licencia 300* días de bonificación.

* A condición de que usted compra un producto en caja Dr.Web con una licencia para protección de 2 PCs por 1 año y registre ambos números de serie consecutivamente para la protección de 1 PC.

Entrega

La entrega de productos Dr.Web OEM Universal a los socios Doctor Web se hace sólo en forma de tarjetas de rasca y gana, con la cantidad mínima de 250 unidades. Entrega de tarjetas rasca o licencias electrónicas en cantidad de 50 a 499 unidades se hace sólo a las compañías que tienen el estatus del Centro de Servicio Autorizado Dr.Web (más información sobre el programa para CSA – http://partners.drweb.com/service).

Para grandes proveedores de licencias OEM existe programa de protección de renovaciones de licencias OEM:
https://pa.drweb.com/products/oem/universal/protection/

Servidor OEM Dr.Web (licencia corporativa)

Otorga el derecho de usar cualquier producto Dr.Web Enterprise Security Suite durante 3 meses. Viene en forma de media kit.

Composición de licencia:

- Centro de Control Dr.Web Enterprise Security Suite
- Dr.Web Desktop Security Suite – 100 PC
- Dr.Web Server Security Suite – 10 servidores
- Dr.Web Mail Security Suite – 100 usuarios
- Dr.Web Gateway Security Suite – 100 usuarios
- Dr.Web Mobile Security Suite – 100 dispositivos

Contenido de media kit:

- Sobre corporativo Dr.Web
- CD con la presentación de todos productos Dr.Web
- Certificado de licencia Dr.Web con número de serie para Dr.Web Enterprise Security Suite por 3 meses
- Folleto "Dr.Web Enterprise Security Suite"
- Pegatina "Dr.Web OEM"

Renovación

Para renovar la licencia Dr.Web OEM, se debe adquirir una licencia, que incluye en el precio un descuento de 40% para la renovación por 1 año.

Programa de bonificación

Para los proveedores de licencias OEM de servidor está prevista un programa de bonificación especial. Leer más aquí https://pa.drweb.com/products/oem/kod/bonuses.

Memo para el proveedor OEM:
https://st.drweb.com/static/new-www/files/Pamyatka_OEM_ru.pdf

Dr.Web Home Security. Productos para el hogar

Composición de los productos

Dr.Web Security Space	Dr.Web Mobile Security
Protección de todos dispositivos	Protección de dispositivos móviles
Productos software Dr.Web	
▪ Dr.Web Security Space ▪ Antivirus Dr.Web para Windows ▪ Antivirus Dr.Web para OS X ▪ Antivirus Dr.Web para Linux	–
▪ Dr.Web para Android ▪ Dr.Web para Symbian ▪ Dr.Web para Windows Mobile	▪ Dr.Web para Android ▪ Dr.Web para Symbian ▪ Dr.Web para Windows Mobile

Componentes de protección de Dr.Web Security Space

Componentes de protección	Windows	OS X	Linux
Antivirus	+	+	+
Antispam	+		
Web antivirus	+		
Control Paterno	+		
Firewall	+		
Red antivirus			

Licenciamiento Dr.Web Security Space

1. El producto es licenciado por la cantidad de PC protegidos (1-5).
2. Opciones de licencias: protección completa.
3. Plazos de licencias comerciales: 3, 6, 12, 24 ó 36 meses. Plazos de licencias OEM: 3 ó 6 meses.
4. Se aplican descuentos estándares en la renovación.
5. Otros descuentos no están previstos.
6. Los compradores del producto tienen derecho al uso gratuito del Dr.Web Mobile Security Suite. El número de dispositivos móviles protegidos es igual al número de PC protegidos.

Ampliación de licencia (compra adicional)

1. Ampliación de licencia para Dr.Web Security Space consiste en: a) la transición del antivirus Dr.Web al Dr.Web Security Space o b) aumento de número de objetos protegidos.

2. La activación de licencia de compra adicional se produce automáticamente al generarla, con los datos especificados al registrar la licencia anterior.
3. Si la licencia expira dentro de más de 3 meses, la ampliación se produce de acuerdo al costo de renovación de la licencia. Tipo de licencia en el código de dicha licencia es "D". Licencia se renueva automáticamente.
4. Si la licencia expira en menos de 3 meses:
   - la ampliación de la licencia se produce gratis a través del servicio gratuito de ampliación;
   - la licencia anterior se bloqueará al día siguiente después de generarse la nueva;
   - el código de la nueva licencia es "C", la licencia de este tipo no tendría el costo.

Posteriormente el cliente podrá renovar tal licencia con descuento;

Dr.Web Security Space

Protección completa para Windows, Antivirus para OS X y Linux.

- Solución completa para proteger su PC bajo Windows.
- Protección en línea.
- Posibilidad de instalar y ejecutar en el ordenador ya infectado con una excepcional resistencia a los virus.
- La detección operativa y limpieza del sistema de todo tipo de amenazas.
- La capacidad de escaneo de alta velocidad utilizando los sistemas multiprocesador.
- Protección contra los últimos malware desconocidos diseñados con la expectativa de que no se los detecten por mecanismos basados en firmas y heurísticas tradicionales.
- Protección de datos contra el daño.
- Analizador complejo de amenazas comprimidas.
- Chequeo completo de los archivos en cualquier nivel de anidamiento.
- Mejor detección y neutralización de los virus complejos.
- Filtración de spam y de todo tipo de mensajes no deseados, sin necesidad de formación de antispam.
- Análisis completo "al vuelo" de todo tipo del tráfico en todos los puertos.
- Navegación segura en Internet en sistemas de búsqueda Google, Yandex, Yahoo!, Bing, Rambler, debido a la activación de la función "Búsqueda segura" — ¡el contenido inseguro se filtra por los sistemas de búsqueda!
- Comunicación segura — filtra el tráfico en los mensajes instantáneos. La protección efectiva para los niños de contenido no deseado.
- Protección contra conexión no autorizada de dispositivos extraíbles al ordenador.
- El servicio Dr.Web Cloud verifica URL en los servidores de la compañía Doctor Web.
- Protección contra el acceso no autorizado desde fuera, prevención de fuga de datos importantes, bloqueo de conexiones sospechosas en paquetes y aplicaciones.
- Control remoto de Dr.Web en otros ordenadores dentro de una red local sin necesidad de instalar el Centro de Control Dr.Web.

Componentes de protección

Detección eficaz y desinfección del sistema contra todos tipos de amenazas (Escáner Dr.Web)

El uso de varios flujos de diagnóstico en sistemas multiprocesadores provee alta velocidad del análisis.

- El análisis detallado máximo de memoria operativa, sectores de descarga, discos duros y unidades extraíbles en busca de virus, troyanos y otras aplicaciones malware.
- Sólo se detectan amenazas de virus viables.
- Amplias bases de datos para detectar spyware, malware potencialmente peligroso, adware, hacktools y programas de bromas.
- El antirootkit Dr.Web Shield™ incluido en el escáner detecta los virus complejos que utilizan las tecnologías de rootkit y ocultan su presencia en el sistema infectado.
- El escáner de consola, que también forma parte de productos Dr.Web, está diseñado para usuarios avanzados y permite realizar el análisis en modo de línea de comandos. Tiene

opciones avanzadas de configuración y está diseñado incluso para funcionar en sistemas multiprocesadores.

Protección en tiempo real (monitor de archivos SpIDer Guard®)

- **¡Mejorado!** El rendimiento en equipos con flujo de archivos intenso (en el trabajo intensivo con los sistemas de archivos, por ejemplo, al descargar archivos de torrent y sharing trackers , de compilación y rendering) — gracias al subsistema de verificación interior rediseñada radicalmente en Dr.Web SpIDer Guard.
- SpiDer Guard realiza monitoreo constante de estado del ordenador — intercepta
- "en vuelo" el acceso a los archivos en discos, disquetes, CD/DVD /Blu-ray-drives, flash y tarjetas inteligentes.
- Posee alta resistencia a los intentos de malware de perjudicar o detener el funcionamiento de SpIDer Guard.
- Las tecnologías implementadas en el núcleo antivirus Dr.Web controlan dinámicamente la presencia de los recursos libres y limitan "apetito" de antivirus sin reducir la eficacia de la protección.

Correo electrónico sin virus, spam y mensajes no deseados

- Tráfico seguro en Internet — controla todo tipo de tráfico en todos los puertos soportados por protocolos de Dr.Web, incluyendo protegidos (si el usuario ha habilitado SSL).
- Análisis de correo electrónico en busca de virus y spam en tiempo real por medio de protocolos SMTP/POP3/NNTP/IMAP4.
- Análisis de conexiones cifradas SSL (SMTPS/POP3S/IMAP4S).
- El análisis no influye en el funcionamiento de correo electrónico y casi no aumenta el tiempo de recepción de correo.
- Se aplican reglas individuales para procesar diferentes tipos de malware — virus potencialmente peligroso, adware, hacktools, dialers, programas de bromas.
- La protección contra el envío masivo de correo electrónico por los gusanos, debido al análisis del contenido y hora de envío de correo electrónico, que conducen a una conclusión sobre la actividad de virus.

Antispam

- El antispam no requiere configuraciones y comienza a actuar automáticamente al recibir el primer mensaje.
- Diferentes tecnologías de filtración proporcionan una alta probabilidad de detección de spam, phishing, pharming, scamming y mensajes de rebote.
- Protección contra botnets — el proveedor no le quitará el acceso a Internet por envío masivo de spam.
- Los mensajes de correo electrónico filtrados no se eliminan, sino se mueven a una carpeta especial de su programa de correo electrónico, donde se puede verificar las falsas alarmas en el tiempo más conveniente para usted.
- El módulo de analizador de spam es absolutamente autónomo; para su funcionamiento no se requiere conexión al servidor externo o acceso a alguna base de datos, lo que permite ahorrar el trafico significativamente.

Escudo contra amenazas de Internet (Web Antivirus SpIDer Gate™)

- El módulo SpIDer Gate analiza el trafico HTTP entrante en tiempo real, intercepta todas las conexiones HTTP, realiza la filtración de datos, bloquea las páginas infectadas en cualquier navegador automáticamente, analiza los archivos comprimidos (por ejemplo, des-

cargados con un asistente de descargas, y otras aplicaciones que intercambian datos con servidores web), protege contra recursos de Internet de fishing y otros peligros.

- Tráfico seguro en Internet — controla todo tipo de tráfico en todos los puertos soportados por protocolos de Dr.Web, incluyendo protegidos (si el usuario ha habilitado SSL).
- Navegación segura en Internet — cuando el usuario trabaja en los sistemas de búsqueda Google, Yandex, Yahoo!, Bing, Rambler, en resultado de búsqueda se visualizan sólo sitios Web seguros desde el punto de vista de los sistemas de búsqueda y de Dr.Web, debido a la activación de la opción de "Búsqueda segura" — ¡el contenido inseguro se filtra por los sistemas de búsqueda!
- Comunicación segura — filtrado de tráfico en los mensajes instantáneos Mail.Ru Agent, ICQ, Jabber. Los enlaces encontrados que conducen a sitios de malware y phishing, son recortados de los mensajes. Se produce el análisis antivirus de archivos adjuntos enviados, la transmisión de archivos potencialmente peligrosos se bloquea.
- Análisis de conexiones cifradas SSL (HTTPS).
- Bloqueo de sitios web según la base de datos de virus conocidos y sitios web no recomendados. Base de datos separada de los sitios que distribuyen contenido sin licencia — protección del contenido del titular de los derechos.
- Posibilidad de desactivar el análisis del tráfico saliente y entrante, así como formar una lista de aplicaciones, cuyo tráfico HTTP va a verificarse de toda forma y en su totalidad (lista negra). También existe la posibilidad de excluir algunas aplicaciones del análisis de tráfico (lista blanca).
- Se puede configurar la prioridad del análisis del tráfico (equilibrio del análisis). El equilibrio influye sobre la distribución de recursos del procesador del ordenador y la velocidad de conexión con Internet.
- El funcionamiento de SpIDer Gate no depende del navegador que se utiliza.
- La filtración prácticamente no influye en el rendimiento del equipo, la velocidad de Internet y la cantidad de datos transmitidos.
- El modo "por defecto" no requiere ninguna configuración: SpIDer Gate comienza el análisis inmediatamente después de su instalación en el sistema.
- Prueba de URL en los servidores de Doctor Web se ejecuta a través del servicio Dr.Web Cloud. Cuando el usuario intente acceder a sitios web, las URL se enviarán a los servidores de Doctor Web para su análisis. El análisis se realiza en tiempo real, independientemente del estado de las bases de datos de virus Dr.Web en el ordenador del usuario y configuraciones de actualización.

Control de navegación por Internet y bloqueo de unidades extraíbles (Control Paterno Dr.Web)

- Tráfico de Internet seguro — comprueba todo el tráfico en todos los puertos. Protección de niños contra las páginas no deseadas.
- Limita el tiempo de trabajo del usuario en Internet y en el ordenador.
- Bloqueo de cambio del horario de sistema y zona horaria — hace imposible que el niño trabaje en el ordenador en el horario no autorizado por los padres.
- Perfiles de configuración de Control Paterno separados para cada usuario.
- Limitación de acceso a dispositivos — unidades de disco, DVD/CD-ROM, teclado, mouse, adaptadores de red, dispositivos de audio y vídeo, dispositivos de juegos, dispositivos USB, puertos COM/LPT.
- Bloqueo de sitios web según 10 grupos temáticos (armas, drogas, juegos, pornografía, etc.)

- Prohibición del uso de unidades extraíbles (memoria USB, dispositivos USB), dispositivos de red, así como los archivos y directorios individuales — una opción adicional para proteger sus datos e información importante contra pérdida o robo por los piratas informáticos.
- Lista blanca de dispositivos confiables protegerá contra la conexión no autorizada de unidad extraíble a un ordenador protegido por Dr.Web, conservará los datos confidenciales del robo vía memoria USB, no permitirá que los virus penetren en el sistema a través de este fuente popular de distribución de virus. Listas blancas de exportación/importación.
- Verifica la URL en los servidores de Doctor Web a través de servicio Dr.Web Cloud en tiempo real, independientemente del estado de las bases de datos de virus Dr.Web en el ordenador del usuario y configuraciones de actualización.
- Prohibición de hacer impresiones — protección contra la impresión no autorizada de documentos confidenciales o gastos de papel.

Protección contra ataques de red (Firewall Dr.Web)

- Protección contra acceso no autorizado, prevención de fuga de datos importantes en red, bloqueo de conexiones sospechosas a nivel de paquetes y aplicaciones.
- Nuevo tipo de base de Firewall Dr.Web es una mayor comodidad para que el usuario pueda crear reglas. Firewall Dr.Web ahora utiliza su propia base de datos de aplicaciones de confianza. Las aplicaciones de confianza están basadas en certificado digital — todos los programas, legítimos desde el punto de vista de Dr.Web, pueden conectarse con cualquier dirección y por cualquier puerto. Excepción: si la aplicación no tiene una firma válida, tiene firma digital inválida o no la tiene en absoluto (por ejemplo, "onomástico" u open source) — se hace solicitud para crear reglas.
- Control de conexiones a nivel de aplicaciones permite controlar el acceso de programas y procesos específicos a los recursos de red y registrar información sobre los intentos de acceso en el registro de aplicaciones.
- La filtración a nivel de paquetes permite controlar el acceso a Internet, independientemente de los programas que se utilizan. El registro de filtro de paquetes conserva la información acerca de los paquetes transmitidos a través de las interfaces de red.
- Al iniciar el llamado "modo de juego" aparece una ventana, solicitando crear una regla encima de cualquier aplicación ejecutada en modo de pantalla completa.
- El monitoreo de aplicaciones que utilizan la red en tiempo real, con capacidad de finalizar la conexión en forma obligatoria.

Control remoto

- El componente red de antivirus contiene el control remoto y configuración de los antivirus Dr.Web, instalados en los equipos dentro de una red local.
- Para el control remoto no es necesario instalar el Centro de Control Dr.Web.
- Es posible conectar cualquier equipo con otro equipo.
- Las posibilidades de control incluyen: obtención de estadísticas y logos desde la estación remota, lectura y modificación de configuración de módulos, su ejecución y detención. Asimismo, están disponibles el registro del número de serie y sustitución del archivo clave en la estación remota.
- Se debe establecer permiso para el acceso remoto en la estación remota.

Antivirus Dr.Web para Windows

Protección mínima contra el malware para Windows, OS X, Linux

Solución completa para protección de PC bajo Windows.

- Protección en línea.
- Posibilidad de instalar y ejecutar en el ordenador ya infectado con una excepcional resistencia a los virus.
- La detección operativa y limpieza del sistema de todo tipo de amenazas.
- La capacidad de escaneo de alta velocidad utilizando los sistemas multiprocesador.
- Protección contra los últimos malware desconocidos diseñados con la expectativa de que no se los detecten por mecanismos basados en firmas y heurísticas tradicionales.
- Protección de datos contra el daño.
- Analizador complejo de amenazas comprimidas.
- Chequeo completo de los archivos en cualquier nivel de anidamiento.
- Mejor detección y neutralización de los virus complejos.
- Filtración de spam y de todo tipo de mensajes no deseados, sin necesidad de formación de antispam.
- Análisis completo "al vuelo" del tráfico en todos los puertos.
- Protección contra el acceso no autorizado desde fuera, prevención de fuga de datos importantes, bloqueo de conexiones sospechosas en paquetes y aplicaciones.

Componentes de protección

- Detección eficaz y desinfección del sistema contra todos tipos de amenazas (Escáner Dr.Web)
- El uso de varios flujos de diagnóstico en sistemas multiprocesadores provee alta velocidad del análisis.
- El análisis detallado máximo de memoria operativa, sectores de descarga, discos duros y unidades extraíbles en busca de virus, troyanos y otras aplicaciones malware.
- Sólo se detectan amenazas de virus viables.
- Amplias bases de datos para detectar spyware, malware potencialmente peligroso, adware, hacktools y programas de bromas.
- El antirootkit Dr.Web Shield™ incluido en el escáner detecta los virus complejos que utilizan las tecnologías de rootkit y ocultan su presencia en el sistema infectado.
- El escáner de consola, que también forma parte de productos Dr.Web, está diseñado para usuarios avanzados y permite realizar el análisis en modo de línea de comandos. Tiene opciones avanzadas de configuración y está diseñado incluso para funcionar en sistemas multiprocesadores.

Protección en tiempo real (monitor de archivos SpIDer Guard®)

- **¡Mejorado!** El rendimiento en equipos con flujo de archivos intenso (en el trabajo intensivo con los sistemas de archivos, por ejemplo, al descargar archivos de torrent y sharing trackers, de compilación y rendering) — gracias al subsistema de verificación interior rediseñada radicalmente en Dr.Web SpIDer Guard.
- **SpiDer Guard** realiza monitoreo constante de estado del ordenador — intercepta "en vuelo" el acceso a los archivos en discos, disquetes, CD/DVD /Blu-ray-drives, flash y tarjetas inteligentes.
- Posee alta resistencia a los intentos de malware de perjudicar o detener el funcionamiento de SpIDer Guard.
- Las tecnologías implementadas en el núcleo antivirus Dr.Web controlan dinámicamente la presencia de los recursos libres y limitan "apetito" de antivirus sin reducir la eficacia de la protección.

Correo sin virus

- Tráfico seguro en Internet — controla todo tipo de tráfico en todos los puertos soportados por protocolos de Dr.Web, incluyendo protegidos (si el usuario ha habilitado SSL).
- Análisis de correo electrónico en busca de virus y spam en tiempo real por medio de protocolos SMTP/POP3/NNTP/IMAP4. Análisis de conexiones cifradas SSL (SMTPS/POP3S/IMAP4S).
- El análisis no influye en el funcionamiento de correo electrónico y casi no aumenta el tiempo de recepción de correo.
- Se aplican reglas individuales para procesar diferentes tipos de malware — virus potencialmente peligroso, adware, hacktools, dialers, programas de bromas.
- La protección contra el envío masivo de correo electrónico por los gusanos, debido al análisis del contenido y hora de envío de correo electrónico, que conducen a una conclusión sobre la actividad de virus.

Protección contra ataques de red (Firewall Dr.Web)

- Protección contra acceso no autorizado, prevención de fuga de datos importantes en red, bloqueo de conexiones sospechosas a nivel de paquetes y aplicaciones.
- Nuevo tipo de base de Firewall Dr.Web es una mayor comodidad para que el usuario pueda crear reglas. Firewall Dr.Web ahora utiliza su propia base de datos de aplicaciones de confianza. Las aplicaciones de confianza están basadas en certificado digital — todos los programas, legítimos desde el punto de vista de Dr.Web, pueden conectarse con cualquier dirección y por cualquier puerto. Excepción: si la aplicación no tiene una firma válida, tiene firma digital inválida o no la tiene en absoluto (por ejemplo, "onomástico" u open source) — se hace solicitud para crear reglas.
- Control de conexiones a nivel de aplicaciones permite controlar el acceso de programas y procesos específicos a los recursos de red y registrar información sobre los intentos de acceso en el registro de aplicaciones.
- La filtración a nivel de paquetes permite controlar el acceso a Internet, independientemente de los programas que se utilizan. El registro de filtro de paquetes conserva la información acerca de los paquetes transmitidos a través de las interfaces de red.
- Al iniciar el llamado "modo de juego" aparece una ventana, solicitando crear una regla encima de cualquier aplicación ejecutada en modo de pantalla completa.
- El monitoreo de aplicaciones que utilizan la red en tiempo real, con capacidad de finalizar la conexión en forma obligatoria.

Requisitos del sistema

- Intel® Pentium® IV con frecuencia de 1,6 GHz.
- 512 MB de memoria operativa.
- Los archivos temporales creados durante la instalación requerirán un espacio extra.
- No menos de 330 MB en el disco duro
- Windows 2012/8/7/2008/Vista/2003/XP SP 2 (sistemas de 32 y 64 bits).
- OS X 10.7 o superior (32 y 64 bits).
- Linux 2.6 y superior (sistemas de 32 y 64 bits).

Licenciamiento

Tipos de licencias

- Por el número de estaciones de trabajo protegidos.

Opciones de licencias

- Antivirus (la licencia incluye los siguientes componentes de protección: antivirus, antispyware, antirootkit, firewall).

Dr.Web Katana

Un antivirus no basado en firmas para la protección preventiva contra las amenazas activas más nuevas, los ataques objetivo e intentos de penetración, sobre todo a través de las vulnerabilidades del «día cero», aún desconocidas para su antivirus..

Ventajas

- Neutraliza las amenazas más nuevas, aún desconocidas para su antivirus, desarrolladas para no ser detectadas por los mecanismos de firmas y heurísticos tradicionales.
- Proporciona la seguridad casi desde el momento de inicio del sistema operativo - ¡Dr.Web Katana empieza a proteger antes de finalizar el inicio del antivirus de firmas tradicional!
- A diferencia de un antivirus tradicional, Dr.Web Katana casi no consume recursos.
- Controla todos los procesos del sistema, detecta los nocivos por su comportamiento característico y los bloquea. Analiza el comportamiento de cada programa iniciado «al vuelo», consultando la nube de reputación Dr.Web actualizada constantemente, y a base del conocimiento actual sobre cómo se comportan los programas nocivos, saca conclusiones sobre el peligro del mismo, y luego toma las medidas necesarias para neutralizar la amenaza.
- No requiere ninguna configuración, y empieza a funcionar de forma eficaz enseguida una vez instalado.
- Protege el sistema incluso sin acceso de su PC a Internet.

Características

- Protege las partes críticas del sistema contra la modificación por los programas nocivos.
- Detecta y detiene los scripts y procesos nocivos, sospechosos o no seguros.
- Detecta los cambios de archivos no deseados, supervisando el funcionamiento de todos los procesos en el sistema en busca de acciones características para los programas nocivos (por ejemplo, de troyanos extorsionistas) impidiendo que los objetos nocivos se implementen en los procesos de otros programas.
- Detecta y neutraliza las amenazas más nuevas: troyanos extorsionistas (cigfradores), injectors, objetos nocivos administrados de forma remota (difundidos para organizar botnets y espionaje), así como empaquetadores de virus.
- Protege contra los exploits — objetos nocivos que para penetrar en el sistema intentan usar las vulnerabilidades, así mismo, aún desconocidas para todos excepto los creadores de virus (las así llamadas vulnerabilidades del «día cero»).
- Supervisa el funcionamiento no solo de los navegadores más populares, sino de cualquier complemento para los mismos; protege contra los bloqueadores de navegadores.
- Bloquea la posibilidad de cambio de secciones de carga de la unidad por los programas nocivos para impedir el inicio (por ejemplo, de troyanos) en un equipo.
- Previene la desactivación del modo seguro de Windows bloqueando los cambios del registro.
- Impide que los programas nocivos añadan a la lógica del funcionamiento del sistema operativo la realización de las nuevas tareas necesarias para los malintencionados. Bloquea algunas opciones en el registro de Windows, lo que impide, por ejemplo, que los virus cambien la visualización correcta del Escritorio u oculten la presencia del troyano en el sistema por un rootkit.
- No permite que un software malintencionado modifique las reglas del inicio de programas.

- Impide la carga de controladores nuevos o desconocidos sin que el usuario lo sepa.
- Bloquea el autoinicio de programas nocivos, así como de aplicaciones determinadas, por ejemplo, de anti antivirus, impidiendo que los mismos se registren en el registro para el inicio posterior.
- Bloquea las ramas del registro responsables de controladores de dispositivos virtuales, lo que imposibilita la instalación del nuevo dispositivo virtual.
- Bloquea las comunicaciones entre los componentes del software espía y el servidor que los controla.
- Impide que el software malintencionado afecte al funcionamiento correcto de servicios del sistema, por ejemplo, afectar a la creación ordinaria de copias de seguridad de archivos.

Requisitos del sistema

- Windows 10/8/8.1/7/Vista SP2/XP SP2+ (sistemas de 32 bits)
- Windows 10/8/8.1/7/Vista SP2 (sistemas de 64 bits)
- Memoria operativa: no menos de 512 MB.
- Espacio libre en el disco duro: ~150 MB. Los archivos temporales creados durante la instalación requerirán un espacio extra.

Antivirus Dr.Web para OS X

Protección contra el malware creado para infectar no sólo OS X, sino también otros sistemas operativos. Este producto forma parte de licencias de Dr.Web Security Space y Antivirus Dr.Web.

Ventajas

- La tecnología de verificación asíncrona permite al usuario instantáneamente realizar todo tipo de operación en archivos de cualquier tipo — una carga baja en el sistema hace prácticamente invisible el funcionamiento de antivirus Dr.Web para OS X
- Para Dr.Web para OS X no existe situación en la que el archivo verificable "detiene" el sistema operativo, incluso si el proceso falla.
- En la mayoría de los casos, al establecer configuraciones por defecto el usuario no debe reaccionar ante las acciones del antivirus y distraerse de la realización de las tareas corrientes.
- El estilo de la interfaz Apple OS X Aqua hace el trabajo con Dr.Web comprensible y lo más simple posible.

Posibilidades

- Chequeo de objetos de inicio automático, medios extraíbles, unidades lógicas y de red, formatos de correo, archivos y directorios, incluyendo comprimidos y almacenados en archivos.
- Selección de tipo de escaneo: rápido, completo y a elección.
- Escaneo de antivirus manual, automático o de acuerdo con el horario predeterminado.
- Protección de la configuración del monitor SpIDer Guard® con el uso de contraseña contra los cambios no autorizados.
- Aplicación de acciones para los objetos infectados, sospechosos, y objetos de otro tipo, incluyendo el tratamiento, traslado a la cuarentena y eliminación, en caso de que la acción seleccionada anteriormente resultó ser imposible.
- Exclusión del chequeo de los enlaces y los archivos a petición del usuario.
- Detecta y elimina virus ocultos bajo empacadores desconocidos.
- Registra el tiempo de evento, objeto del chequeo y tipos de influencia sobre el mismo.
- Descarga actualizaciones automáticamente (según el horario) o en la demanda.
- Notificación automática (incluyendo las notificaciones de sonido) sobre el virus.
- Aislamiento de los archivos infectados en la cuarentena especificando el tiempo de mantenimiento y el tamaño máximo.
- Tratamiento, recuperación o eliminación de objetos movidos a la cuarentena.
- Lleva un informe detallado sobre el trabajo.
- Disponibilidad de módulos en forma de utilidades de línea de comandos, con la posibilidad de su integración en los que se utilizan para mantener el sistema Apple Scripts.

Requisitos del sistema

- OS X 10.7 o superior (32 y 64 bits).
- Memoria operativa — de conformidad con los requisitos del sistema operativo.
- Acceso a Internet para el registro y obtención de actualizaciones.

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

Antivirus Dr.Web para Linux

La protección mínima necesaria contra los virus

Funciones principales

- Detección y neutralización de virus y objetos maliciosos en discos duros y medios extraíbles.
- Detección de virus en archivos de cualquier nivel de anidación y objetos empaquetados.
- Escaneo de los archivos comprimidos por los empacadores, incluyendo los desconocidos, con la ayuda de tecnología FLY-CODE™.
- Protección contra amenazas desconocidas utilizando la tecnología no basada en firmas Origins Tracing™ y analizador heurística intelectual Dr.Web.
- Escaneo rápido, completo, selectivo o personalizado.
- El monitoreo continuo del ordenador para interceptar "en vuelo" el acceso a los archivos en los discos, disquetes, CD/DVD/Blue-ray-drives, flash y tarjetas inteligentes.
- Protección de sus propios componentes de los intentos de los programas maliciosos detener el antivirus.
- Aislamiento de objetos infectados en cuarentena con la posibilidad de recuperación, la función de limitación del tamaño de cuarentena.
- Proporciona estadísticas completas sobre el funcionamiento de antivirus.
- Las actualizaciones automáticas según el horario predeterminado o en la demanda.

Ventajas

- Centro de control cómodo.
- Capacidad de analizar "en vuelo". Configuración de control personalizado. Una cuarentena controlada.
- Actualizaciones automáticas. Interfaz moderno.

Requisitos del sistema

- Sistema operativo: distribuciones GNU/Linux que funcionan en plataforma Intel x86/amd64 a base del núcleo 2.6.37 (y superior) y usan la biblioteca glibc de versión 2.13 (y superior).
- No menos de 512 MB del espacio libre en el disco.
- Acceso a Internet para registrarse y recibir actualizaciones.

Descripción: http://products.drweb.com/linux

10.06.2016

Escáneres de consola Dr.Web

Protección antivirus con características ampliadas de automatización para usuarios avanzados.

Escáneres de consola Dr.Web sin una interfaz gráfica utilizan una base de datos de virus común y módulo de búsqueda Dr.Web, adecuados para su uso en los sistemas operativos MS DOS, OS/2 y Windows. Para gestionar la protección antivirus se requiere experiencia en uso de la línea de comandos.

Ventajas

- Requisitos mínimos del sistema — escáneres funcionan normalmente incluso en los sistemas incorporados y son capaces de proteger de forma segura los equipos de poca potencia de las generaciones anteriores.
- Comodidad de escaneo — el administrador puede seleccionar el escaneo "manual" o programada.
- Tratamiento de las estaciones de trabajo y servidores infectados, incluyendo los no disponibles en la red. Alta resistencia a los virus y la posibilidad de instalar en el equipo infectado.
- La automatización de trabajos de rutina utilizando la línea de comandos con muchas oportunidades.
- Eliminación garantizada de virus desconocidos a Dr.Web o colocados en archivos de formatos incógnitos.
- Se ejecuta desde cualquier medio de almacenamiento externo (unidad de CD-ROM o USB).

Descripción: http://products.drweb.com/console

Dr.Web Mobile Security

Protección de dispositivos móviles

Componentes de protección Dr.Web Mobile Security

Componentes de protección	Android	Symbian OS	Windows Mobile	BlackBerry
Antivirus	+	+	+	+
Antispam	+	+	+	
Antirrobo	+			
Filtro URL	+			+

Licencias Dr.Web Mobile Security

1. El producto tiene licencia por número de PC protegidos (1–5).
2. Plazos de licencias comerciales: 12, 24 o 36 meses. Plazos de licencias OEM: 3 o 6 meses.
3. No están previstos descuentos para este producto, incluyendo descuentos en renovación. Para continuar usando el producto después de caducar la licencia, o para aumentar el número de dispositivos protegidos (compra adicional), se debe adquirir una nueva licencia sin descuento.

Dr.Web para Android

Funciones y ventajas

- Escaneo rápido o completo del sistema de archivos, así como el chequeo de archivos y carpetas individuales a petición del usuario.

  El monitor SpIDer Guard escanea el sistema de archivos en tiempo real cuando se trata de guardar los archivos en la memoria del dispositivo.
- Detección de malware nuevo y desconocido, usando la tecnología única Origins Tracing™.
- Protección de tarjeta SD de la infección por los archivos de autoinicio y Exploit.CplLnk, que representan un riesgo para los dispositivos bajo Windows.
- Traslada a la cuarentena las amenazas detectadas con la capacidad de restaurar los archivos desde allí.
- Influencia mínima en la velocidad del sistema operativo. El uso cuidadoso de los recursos de la batería.
- Ahorro del tráfico debido al pequeño tamaño de las actualizaciones de la base de datos de virus, lo cual es importante para los usuarios de tarifas móviles limitadas.
- Las estadísticas detalladas sobre el funcionamiento de antivirus.

  Widgets cómodos e informativos en el escritorio para acceder a la aplicación.

Antispam

Protege contra las llamadas no deseadas y mensajes SMS.

- Selección de modos de filtrado de llamadas y mensajes.
- Capacidad de crear sus propios perfiles de filtrado.

- Edición de la lista negra (los números de los que usted desea bloquear las llamadas y mensajes entrantes).
- Posibilidad de ver llamadas y mensajes bloqueados.

Antirrobo

Ayuda a encontrar el dispositivo móvil en caso de pérdida o robo y, si es necesario, de forma remota borrar información confidencial.

- Bloqueo de teléfono después de reinicio.
- Bloqueo de teléfono requiriendo introducir la contraseña para su desbloqueo (el número de intentos de introducir la contraseña es limitado).
- Desbloqueo a través de SMS.
- Obtención de coordenadas GPS del dispositivo como un enlace a Google Maps.
- La capacidad de borrar de forma remota los datos del teléfono y de la tarjeta SD.
- Activación de la señal acústica alta en el dispositivo y bloqueo de la pantalla.
- Habilidad para determinar su propio texto que se mostrará en la pantalla del dispositivo bloqueado.
- Capacidad de crear una lista de personas cercanas que van a recibir las notificaciones del cambio de tarjeta SIM en el dispositivo perdido. Desde estos números se puede controlar utilizando el antirrobo, asimismo se puede desbloquear el teléfono si usted olvida la contraseña de desbloqueo.

Filtro URL Cloud Checker

Filtro de nube Cloud Checker restringirá el acceso a los recursos de Internet no deseados. El bloqueo de acceso a los sitios no recomendados y potencialmente peligrosos se realiza en base de las siguientes categorías:

- Drogas.
- Fuentes conocidas de los virus. Lenguaje obsceno.
- Terrorismo. Violencia.
- Armas.
- Sitios para adultos, etc.

¡IMPORTANTE!

Algunos competidores de Dr.Web afirman tener como parte de sus productos de protección para OS Android el componente Control paterno.

Crear un control completo para este sistema operativo actualmente es IMPOSIBLE.

Las configuraciones predeterminadas del navegador para Android y el navegador Google Chrome para Android no permiten utilizar el control paterno en el pleno sentido de la palabra, porque cualquier usuario puede abrir la página de forma anónima, y ningún software podría monitorear sus acciones.

Por lo tanto, a diferencia de sus competidores, Doctor Web no está posicionando el filtro URL Cloud Checker como control paterno.

Dr.Web para BlackBerry

Ventajas:

- Escaneo rápido/ completo del sistema de archivos, así como el análisis de archivos separados y carpetas por el escáner, por solicitud de usuario, análisis de la tarjeta de memoria, de archivos archivados.
- Escaneo del sistema de archivos en modo de tiempo real por el monitor SpIDer Guard al intentar guardar los archivos en la memoria del dispositivo y al instalar programas.
- Protección de la tarjeta SD contra la infección por los archivos de autoinicio y Exploit. Cpllnk que son de amenaza para dispositivos Windows.
- Ahorro del tráfico gracias al volumen insignificante de las bases de virus, lo que es muy importante para los usuarios de tarifas limitadas de móviles.
- Transferencia de las amenazas detectadas a la cuarentena con posibilidad de recuperar los archivos de la misma.
- Impacto mínimo a la velocidad de funcionamiento del sistema operativo.
- Gasto económico de los recursos de la batería.
- Estadísticas detalladas de las amenazas detectadas, el funcionamiento del antivirus, así como el registro de eventos.
- Diagnóstico del dispositivo en busca de vulnerabilidades en el mismo. Ayuda para eliminar los problemas de seguridad y las vulnerabilidades del dispositivo.

"Dr.Web Universal" (para clientes ASC)

Protección completa para PC y ordenadores portátiles para los clientes de los centros de servicio autorizado Dr.Web.

Las licencias electrónicas del producto «Dr.Web Universal» están disponibles sólo para los centros de servicio autorizado Dr.Web.

"Dr.Web Universal" protege 1 PC y 1 dispositivo móvil durante 1 año.

Composición de licencia:

- Dr.Web Security Space
- Antivirus Dr.Web para OS X
- Antivirus Dr.Web para Linux
- Dr.Web Mobile Security Suite
- Dr.Web para Android OS
- Dr.Web para Symbian OS
- Dr.Web para Windows Mobile

Más información acerca de los centros autorizados Dr.Web — http://partners.drweb.com/service

Dr.Web Enterprise Security Suite. Productos para empresas

NUEVA VERSIÓN

Dr.Web Enterprise Security Suite – es un grupo de productos Dr.Web que incluye elementos de seguridad de todos los nodos de la red corporativa y centro de control común para la mayoría de ellos.

Productos se dividen en 5 grupos según el tipo de objetos protegidos. Si el cliente tiene determinados requisitos es más fácil encontrar el producto deseado.

Producto	Software
Dr.Web Desktop Security Suite Protección de estaciones de trabajo, clientes de servidores terminales, clientes de servidores virtuales y clientes de sistemas integrados	Dr.Web para Windows
	Dr.Web para Linux
	Dr.Web para OS X
	Dr.Web para MS DOS*
	Dr.Web para OS/2*
Dr.Web Server Security Suite Protección de servidores de archivos y servidores de aplicaciones (incluyendo los virtuales y terminales)	Dr.Web para servidores Windows
	Dr.Web para servidores UNIX
	Dr.Web para servidores Novell NetWare
	Dr.Web para servidores OS X Server
Dr.Web Mail Security Suite Protección de correo electrónico	Dr.Web para servidores de correo y puertas de enlace UNIX
	Dr.Web para MS Exchange
	Dr.Web para IBM Lotus Domino para Windows
	Dr.Web para IBM Lotus Domino para Windows
	Dr.Web para servidores de correo Kerio para Windows
	Dr.Web para servidores de correo Kerio para Linux
	Dr.Web para servidores de correo Kerio para OS X
Dr.Web Gateway Security Suite Protección de puertas de enlace	Dr.Web para puertas de enlace UNIX
	Dr.Web para puertas de enlace Kerio
	Dr.Web para MIMEsweeper*
	Dr.Web para Qbik WinGate
	Dr.Web para Microsoft ISA Server y Forefront TMG*
Dr.Web Mobile Security Suite Protección de dispositivos móviles	Dr.Web para Windows Mobile
	Dr.Web para Symbian OS*
	Dr.Web para Android

* Gestión centralizada aún no ha sido implementada.

Algoritmo para seleccionar el producto deseado

1	2	3	4	5	6	7
¿Qué desea proteger?	**¿Bajo qué OS/ plataforma funcionan dispositivos protegidos?***	**¿Requiere sólo antivirus o protección completa?**	**¿Desea administrar desde un solo lugar?**	**¿Cuántos objetos hay que proteger?**	**¿Por cuánto tiempo se requiere licencia?**	**La licencia requerida es una compra primaria, renovación, compra adicional, compra adicional más renovación, tiene el cliente beneficios?**
Determinamos el producto	Definimos OS/ plataforma	Definimos la licencia básica	Definimos componentes adicionales	Determinamos cantidad de licencias	Definimos el período de la licencia	Determinamos el tipo de licencia y descuentos posibles
Estaciones de trabajo (Dr.Web Desktop Security Suite)	▪ Windows 8/7/Vista/ XP/2000 SP4 + Rollup 1 (32 y 64 bit)	▪ Protección completa ▪ Antivirus	▪ Centro de control	1...	12, 24 ó 36 meses	
	▪ OS X ▪ Linux ▪ MS DOS ▪ OS/2	▪ Antivirus	▪ Centro de control			
Servidores de archivo Dr.Web Server Security Suite)	▪ Windows ▪ Novell NetWare ▪ OS X Server ▪ UNIX	▪ Antivirus	▪ Centro de control	1...		
El tráfico de correo (Dr.Web Mail Security Suite)	▪ UNIX ▪ MS Exchange ▪ Lotus Domino ▪ Kerio	▪ Antivirus	▪ Antispam ▪ SMTP Proxy ▪ Centro de control	▪ Cantidad ilimitada de usuarios ▪ Servidores – con el número de usuarios protegidos no más de 3000		
Tráfico de Internet (Dr.Web Gateway Security Suite)	▪ Gateways de Internet Kerio ▪ Gateways de Internet UNIX	▪ Antivirus	▪ Centro de control	▪ Número ilimitado de usuarios		
	▪ Qbik WinGate ▪ MIMEsweeper ▪ Microsoft ISA Server y Forefront TMG		▪ Antispam	▪ Servidores – con el número de usuarios protegidos no más de 3000		
Dispositivos móviles (Dr.Web Mobile Security Suite)	▪ Windows Mobile ▪ Android	▪ Protección completa	▪ Centro de control	▪ Número ilimitado de los dispositivos móviles		
	▪ Symbian OS					
Ahora usted tiene todos los datos necesarios para el cálculo de costo de la licencia.						

* Este paso es importante sólo cuando se elige la protección para estaciones de trabajo, porque el conjunto de componentes adicionales en el sistema depende del sistema operativo utilizado (véase "Licenciamiento de productos").

Centro de Control Dr.Web.

Control centralizado de la seguridad de todos los nodos de la red corporativa.

Funciones principales

El control centralizado de todos los componentes de seguridad, el seguimiento del estado de todos los nodos protegidos, configuración de respuesta automática a los incidentes virales.

Ventajas

- La gestión del sistema de protección de bajo coste en la red corporativa desde cualquier parte del mundo de un solo lugar (a través de administrador de web), donde quiera que fuera, incluso fuera de la red corporativa.
- El costo total mínimo en comparación con los programas competidores gracias a la posibilidad de desplegar una red bajo Windows y servidores UNIX, facilidad de instalación y seguridad de protección.
- El sistema de protección puede ser implementada en cualquier red corporativa, sin considerar su tamaño y características — el número total de empleados y sucursales, la topología, la presencia o ausencia del servidor Active Directory.
- La capacidad de desplegar agentes en estaciones de trabajo de una forma conveniente para el administrador — por medio de la política de Active Directory, los scripts de inicio, mecanismos de instalación remota. La instalación se hace posible, incluso si el nodo de red se encuentra cerrado e inaccesible para el servidor antivirus.
- Capacidad para realizar políticas de seguridad individuales para una empresa en particular y los grupos de empleados independientes.
- Automatización de trabajo debido a la integración con el sistema NAP de Windows.
- Extensibilidad excepcional para redes de cualquier tamaño y complejidad. La extensibilidad se provee debido a las oportunidades de uso de una jerarquía de servidores antivirus de Centro de Control y un servidor de SQL independiente para almacenar datos, así como la presencia de una estructura compleja de interacción entre ellos y nodos de la red protegidos.
- Transmisión segura de datos entre los componentes del sistema debido a la posibilidad de cifrado.
- El tráfico de red mínimo. La compresión de datos entre el cliente y el servidor provee un protocolo especialmente diseñado para intercambio de información.
- La transparencia del funcionamiento, el registro de acciones de administradores permite realizar el seguimiento de todos los pasos para instalar y configurar el sistema. Todos sus componentes pueden llevar archivos de informes con un nivel personalizado de detalle.
- Un sistema cómodo de notificar al administrador sobre los problemas en la red antivirus.
- Posibilidad de asignar administradores para los distintos grupos, lo que permite utilizar el Centro de control tanto en las empresas con altas exigencias en materia de seguridad, como en las organizaciones con múltiples sucursales.
- Posibilidades de personalización de las políticas de seguridad para todo tipo de usuarios, incluidos los de dispositivos móviles, y para todas las estaciones — incluso ausentes en el momento en la red — que permiten garantizar la pertinencia de la protección en cualquier momento.
- Los usuarios no tendrán capacidad de cambiar la configuración de seguridad independientemente.

- Capacidad de proteger las redes que no tienen acceso a Internet.
- Capacidad de utilizar la mayoría de las bases de datos existentes, tanto internos como externos. Al mismo tiempo éstos pueden ser Oracle, PostgreSQL, Microsoft SQL Server, cualquier base de datos compatible con SQL-92 a través de ODBC.
- Capacidad de redacción de procesadores de eventos en cualquier lenguaje de script lo que otorga acceso directo a las interfaces internas del Centro de control.
- Posibilidad de restablecer actualizaciones, incluso si el proceso de actualización ha causado un error, el nodo de red no se quedará sin protección.
- La transparencia, con la ayuda de esta opción el administrador de sistema puede configurar y sincronizar productos adicionales de terceros, lo que también reduce el costo de la construcción de los sistemas de seguridad informativa.
- Visibilidad del sistema de control de estado de protección, la eficiencia es insuperable y la facilidad de búsqueda de estaciones de red.
- Las posibilidades de selección de la lista de componentes actualizados del producto y el control de cambio a las nuevas versiones permiten a los administradores instalar sólo las actualizaciones necesarias y verificadas en su red.

Servicio de test en línea Dr.Web LiveDemo
http://download.drweb.com/live_demo/?lng=en

Dr.Web Desktop Security Suite

Protección de estaciones de trabajo, clientes de servidores terminales, clientes de servidores virtuales y clientes de sistemas incorporados.

- Dr.Web para Windows está certificado por FSTEK de Rusia
- Dr.Web para Linux está certificado por FSTEK de Rusia
- Dr.Web para OS X
- Escáner de consola Dr.Web para Windows, MS DOS, OS/2

Sistemas operativos compatibles

Dr.Web para Windows	Dr.Web para Linux	Dr.Web para OS X	Escáneres de consola Dr.Web
Windows 2012/8/7/2008/ Vista/2003/XP SP 2 (sistemas de 32 y 64 bits)	Distribuciones GNU/Linux que funcionan en plataforma Intel x86/amd64 a base del núcleo 2.6.37 (y superior) y usan la biblioteca glibc de versión 2.13 (y superior)	OS X 10.7 y superior	Windows, MS DOS, OS/2

Licenciamiento Dr.Web Desktop Security Suite

Tipos de licencias

Según el número de estaciones de trabajo protegidas, clientes que se conectan a un terminal o un servidor virtual, o clientes de sistemas integrados (a partir de 5).

El software de Dr.Web Desktop Security Suite se puede comprar por separado o dentro del grupo Dr.Web Enterprise Security Suite. En el último caso el Centro de Control de Dr.Web Enterprise Security Suite está licenciado adicionalmente (excepto de escáner de consola Dr.Web).

Opciones de licencias

	Windows 8/7/Vista	Windows 8/7/ Vista/XP SP2/2000 SP4 + Rollup 1	Linux	OS X	MS DOS, OS/2
Licencia básica	Antivirus	Antivirus Windows 8/7/Vista/XP SP2/2000 SP4 + Rollup 1 (Sistemas de 32 y 64 bits)			
Componentes de protección de licencia básica	▪ Protección completa ▪ Antivirus ▪ Antiespía ▪ Antirootkit ▪ Antispam ▪ Antivirus web ▪ Control de oficina ▪ Firewall	▪ Antivirus ▪ Antiespía ▪ Antirootkit ▪ Firewall	▪ Antivirus ▪ Antiespía	▪ Antivirus ▪ Antiespía ▪ Antirootkit	▪ Antivirus ▪ Antiespía ▪ Antirootkit
Componentes adicionales:					
Centro de control	+	+	+	+	–

También los productos Dr.Web Desktop Security Suite (excepto los escáneres de consola) están disponibles en Kits Dr.Web económicos para empresas pequeñas y medianas.

La información sobre productos Dr.Web para Windows, OS X, Linux y escáneres de consola se encuentra en la sección Dr.Web Home Security Suite. Productos para el hogar. La información del producto Dr.Web Security Space corresponde a la licencia de protección completa.

Dr.Web Server Security Suite

Protección de servidores de archivos y servidores de aplicaciones (incluyendo servidores terminales)

- Dr.Web para servidores Windows Server está certificado por FSTEK de Rusia
- Dr.Web para OS X Server
- Dr.Web para servidores Novell NetWare
- Dr.Web para servidores UNIX (Samba) está certificado por FSTEK de Rusia

Sistemas operativos compatibles

Dr.Web para servidores Windows	Dr.Web para servidores UNIX	Dr.Web para servidores Novell NetWare	Dr.Web para OS X Server
Microsoft Windows Server 2000*/ 2003 (x32 y x64*)/ 2008/2012 (x64)	▪ Linux con kernel 2.4.x y superior ▪ FreeBSD versión 6.x y superior para plataforma Intel x86 ▪ Solaris versión 10 para plataforma Intel x86	Novell NetWare versiones 4.11–6.5	OS X Server 10.7 y superior

* Están compatibles sólo para la versión 7.0.

El software Dr.Web Desktop Security Suite se puede comprar por separado o como parte del grupo Dr.Web Enterprise Security Suite. En este último caso, el Centro de control Dr.Web Enterprise Security Suite está licenciado adicionalmente.

Opciones de licencias

	Dr.Web para servidores Windows	Dr.Web para servidores Novell	Dr.Web para servidores UNIX	Dr.Web para OS X Server
Licencia básica	Antivirus			
Componentes adicionales:				
Centro de control	+	+	+	+

Todos los productos Dr.Web Server Security Suite están disponibles en Kits Dr.Web económicos para empresas pequeñas y medianas.

Dr.Web para servidores Windows

La protección antivirus de los servidores de archivos y terminales bajo Windows, incluyendo servidores de aplicaciones

Ventajas

- Posibilidad de utilizar en las compañías que requieren alto nivel de seguridad, el producto cumple totalmente con los requisitos de la legislación rusa y tiene certificados de conformidad con FSTEK y FSB.
- Alto rendimiento y estabilidad en funcionamiento.
- Alta velocidad de escaneo con carga mínima en el sistema operativo que permite que Dr.Web funcione perfectamente en servidores con cualquier configuración.
- Funcionamiento sin interrupciones del antivirus de modo automático.
- Distribución flexible de carga en el sistema de archivos del servidor debido a la tecnología única de prueba postergada de los archivos que se abren "para la lectura".
- El sistema de configuración flexible orientada al cliente — la elección de objetos para escaneo, acciones con virus detectado o archivos sospechosos.
- Es fácil de instalar y administrar.
- Protección completa inmediatamente después de la instalación (con la configuración predeterminada).
- Transparencia — archivos de informes detallados con el grado de detalle requerido para el administrador.

Funciones principales

- Comprobación de volúmenes de servidor según el horario predeterminado o a la demanda del administrador.
- Análisis "en vuelo" se produce directamente al copiar o al abrir archivos en el servidor desde estaciones de trabajo.
- Verificación multiproceso
- Desactivación automática del servidor de la estación, de la fuente de amenaza de virus.
- Alerta inmediata al administrador, a otros usuarios y grupos sobre incidentes de virus por correo electrónico o mediante el envío de una notificación a un teléfono celular o un mensáfono.
- El aislamiento de los archivos infectados en cuarentena
- Tratamiento, recuperación y/o eliminación de los archivos de la cuarentena. Registro de acciones de antivirus.
- Las actualizaciones automáticas de bases de datos de virus.
- El consumo cuidadoso de los recursos del sistema y el control de potencia de hardware Dr.Web Cloud, respuesta inmediata a las amenazas más recientes*.
- Protección preventiva es una protección segura contra amenazas desconocidas mediante la prohibición de la modificación de los objetos críticos de Windows y el control de los hechos inseguros*.

Requisitos del sistema

- Procesador: soporta el sistema de comandos i686 y mayores.
- Sistema operativo: Microsoft Windows Server 2000**/2003 (x32 y x64**)/2008/2012 (x64)
- Memoria: 512 MB y más.

* Disponible para SO Windows Server 2008 y superiores.
** Sólo es compatible con la versión 7.0.

Descripción: http://products.drweb.com/fileserver/win

Dr.Web para OS X Server

Protección antivirus para estaciones de trabajo bajo versiones de servidor OS X

Funciones principales

- Chequeo de objetos de inicio automático, medios extraíbles, unidades lógicas y de red, formatos de correo, archivos y directorios, incluyendo comprimidos y almacenados en archivos.
- Escaneo rápido, completo y personalizado.
- Escaneo de antivirus manual, automático o de acuerdo con el horario predeterminado.
- Protección de la configuración del monitor SpIDer Guard® con el uso de contraseña contra los cambios no autorizados.
- Aplicación de acciones para los objetos infectados, sospechosos, y objetos de otro tipo, incluyendo el tratamiento, traslado a la cuarentena y eliminación, en caso de que la acción seleccionada anteriormente resultó ser imposible.
- Exclusión del chequeo de los enlaces y los archivos a petición del usuario.
- Detecta y elimina virus ocultos bajo empacadores desconocidos.
- Registra el tiempo de evento, objeto del chequeo y tipos de influencia sobre el mismo.
- Descarga actualizaciones automáticamente (según el horario) o en la demanda.
- Notificación automática (incluyendo las notificaciones de sonido) sobre el virus.
- Aislamiento de los archivos infectados en la cuarentena especificando el tiempo de mantenimiento y el tamaño máximo.
- Tratamiento, recuperación o eliminación de objetos movidos a la cuarentena.
- Lleva un informe detallado sobre el trabajo.
- Disponibilidad de módulos en forma de utilidades de línea de comandos, con la posibilidad de su integración en los que se utilizan para mantener el sistema Apple Scripts.

Ventajas

- Centro de control cómodo. Escaneado de alta velocidad.
- Capacidad de crear propios perfiles de filtrado. Protección segura en tiempo real.
- Carga mínima en el sistema protegido. Gasto de tráfico mínimo durante las actualizaciones.
- Variedad de configuraciones. Simplicidad de control.
- Interfaz moderno y cómodo.

Requisitos del sistema

- OS X Server 10.7 o superior.
- Procesador Intel.
- Memoria operativa — según los requerimientos del SO
- Acceso a Internet: para registro y obtener actualizaciones.

Descripción: http://products.drweb.com/fileserver/mac

10.06.2016

Dr.Web para servidores Novell NetWare

Protección antivirus de almacenamiento de archivos

Funciones principales

- Comprobación de volúmenes de servidor según el horario o a la demanda del administrador.
- Verificación de todos los archivos "en vuelo" que pasan a través del servidor.
- Verificación multiproceso.
- Capacidad para ajustar la potencia de la CPU, lo que le permite especificar la prioridad del proceso de escaneo en el sistema.
- Desactivación automática del servidor de la estación, de la fuente de amenaza de virus.
- Registro del chequeo; gestión de detalles de protocolo.
- Aviso sobre la detección de objetos infectados.
- Tratamiento, eliminación o traslado de los objetos infectados a la cuarentena.
- Administración de antivirus utilizando las consolas del servidor o la consola remota.
- Lleva la estadística de escaneo y el registro de las acciones del antivirus.
- Las actualizaciones automáticas de bases de datos de virus.

Ventajas

- Una amplia gama de versiones compatibles Novell NetWare de 4.11 a 6.5. Apoyo de extensión de nombres NetWare.
- Alta velocidad de escaneo de cantidades enormes de datos con una carga mínima sobre el sistema operativo.
- Simplicidad de instalar.
- Sistema flexible orientado al cliente de configuración de parámetros de escaneo y de acciones con objetos maliciosos detectados.

Requisitos del sistema

- Novell NetWare versiones 4.11–6.5 con suplementos instalados desde Minimum patch list.

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

Dr.Web para servidores UNIX

Protección antivirus de servidores de archivos Unix

Ventajas

- Alto rendimiento y estabilidad en funcionamiento.
- Alta velocidad de escaneo con carga mínima en el sistema operativo que permite que Dr.Web funcione perfectamente en servidores con cualquier configuración.
- El sistema de configuración flexible orientada al cliente — la elección de objetos para escaneo, acciones con virus detectado o archivos sospechosos.
- Excelente compatibilidad — no entra en conflicto con el firewall conocidos y archivo de monitores.
- Soporte de sistemas de supervisión (Cacti, Zabbix, Munin, Nagios etc.)
- Administración cómoda, simplicidad en instalación y configuración.

Funciones principales

- Comprobación de volúmenes de servidor según el horario predeterminado o a la demanda del administrador.
- Mejorado! Análisis "en vuelo" se produce directamente al grabar o abrir archivos en el servidor desde estaciones de trabajo.
- Verificación multiproceso.
- Desactivación automática del servidor de la estación, de la fuente de amenaza de virus.
- Alerta inmediata al administrador, a otros usuarios y grupos sobre incidentes de virus por correo electrónico o mediante el envío de una notificación a un teléfono celular o un mensáfono.
- Mejorado! El aislamiento de los archivos infectados en cuarentena
- Tratamiento, recuperación y/o eliminación de los archivos de la cuarentena. Registro de acciones de antivirus.
- Las actualizaciones automáticas de bases de datos de virus.

Requisitos del sistema

- Samba 3.0 y superior.

Sistemas operativos compatibles

- GNU/Linux (a base del núcleo con versión no inferior a 2.6.37 y que usa la biblioteca glibc de versión 2.13 y superior);
- FreeBSD;
- Solaris — solo para plataformas Intel x86/amd64.

Los sistemas operativos usados deben usar el servidor Samba de versión no inferior a 3.0, así como el mecanismo de autenticación PAM.

En caso de usar la versión del sistema operativo de 64 bits debe estar activado el soporte de ejecución de aplicaciones de 32 bits.

Espacio en el disco duro:

- No menos de 1 GB

Se realizaron las pruebas del funcionamiento del conjunto en distribuciones: 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).

Descripción: http://products.drweb.com/fileserver/unix

Dr.Web Mail Security Suite

Protección de correo electrónico

- Dr.Web para UNIX está certificado por FSTEK de Rusia
- Dr.Web para MS Exchange está certificado por FSTEK de Rusia
- Dr.Web para IBM Lotus Domino (Windows, Linux)
- Dr.Web para servidores de correo Kerio (Windows, Linux)

Sistemas operativos compatibles

Producto Dr.Web	Windows	Linux	FreeBSD	Solaris
		para plataforma Intel x86		
Dr.Web servidores de correo UNIX		versión del kernel 2.4.x y superior	versión 6.x y superior	versión 10
Dr.Web para MS Exchange	Server 2000/ 2003/2008/ 2012			
Dr.Web para IBM Lotus Domino	Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 (sistemas de 32 y 64 bits)	Red Hat Enterprise Linux (RHEL) versión 4 y 5, Novell SuSE Linux Enterprise Server (SLES) versiones 9 y 10 (sólo 32 bits)		
Dr.Web para servidores de correo 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		

Licenciamiento Dr.Web Mail Security Suite

Tipos de licencias

- Número de usuarios protegidos (mínimo 5).
- Licencia para cada servidor es para el escaneo de cantidad ilimitada de correspondencia en un solo servidor, el número de usuarios protegidos no debe exceder 3000.

El software de Dr.Web para proteger el correo se puede comprar por separado o como parte del grupo Dr.Web Enterprise Security Suite. En este último caso, el Centro de Control de Dr.Web Enterprise Security Suite, Antispam y proxy SMTP están licenciados adicionalmente.

El uso de productos para proteger el correo junto con el componente adicional SMTP proxy no sólo mejora significativamente la seguridad general de la red, sino reduce la carga de tra-

bajo en los servidores de correo internos y estaciones de trabajo.

Opciones de licencias

	Dr.Web para MS Exchange	Dr.Web para IBM Lotus Domino	Dr.Web para servidores de correo UNIX	Dr.Web para servidores de correo Kerio
Licencia básica	Antivirus			
Componentes adicionales:				
Antispam	+	+	+	
Proxy SMTP	+	+	+	+
Centro de Control	+	+	+	+

También los productos Dr.Web para proteger el correo electrónico están disponibles en Kits Dr.Web para las empresas pequeñas y medianas.

Dr.Web para servidores de correo y puertas de enlace UNIX

Protección antivirus y antispam para el tráfico de correo electrónico que pasa a través de servidores bajo UNIX (Linux/FreeBSD/Solaris (x86))

Funciones principales

- Filtrado de mensajes de correo electrónico en busca de virus y spam.
- Análisis de mensajes de correo electrónico y de todos sus componentes.
- Procesamiento correcto de la mayoría de los tipos de archivos conocidos, incluyendo multivolumenes y autoextraíble (SFX).
- Listas blancas y negras. Notificaciones personalizadas.
- Registro de estadísticas, teniendo en cuenta todos los aspectos del sistema. La protección de propios módulos de fallas.

Conformidad con los requisitos de la legislación rusa

Dr.Web para servidores de correo UNIX tiene certificados de conformidad con FSTEK y FSB. Esto permite utilizar el producto en las empresas que requieren alto nivel de seguridad, incluyendo en el subsistema de protección antivirus de sistemas de información de los datos personales de grupo K1. Asimismo, la posibilidad de archivar de todos los correos permite que el producto se utilice como parte de los sistemas de información de las entidades de crédito.

Adaptación flexible a las necesidades de los usuarios

Para configurar Dr.Web para UNIX se puede aplicar reglas. Esto aumenta considerablemente la flexibilidad del producto y lo distingue de productos de la competencia, para la configuración de los cuales se aplican los parámetros estáticos del archivo de configuración. La filtración y el cambio de mensajes se producen en función de las políticas existentes. El administrador puede determinar reglas individuales de procesamiento no sólo para diferentes usuarios y grupos, sino para cada uno correo electrónico. Debido a eso el producto es capaz de satisfacer cualquier requisito de empresa relacionado al nivel de la seguridad informativa. Es importante, especialmente, cuando se trata de la entrada en vigor de la ley sobre la protección de datos personales.

Poca exigencia a la calificación del administrador

A pesar de la gran cantidad de características, Dr.Web para servidores de correo UNIX no requiere ajustes continuos antes de su funcionamiento.

Respuesta de alta velocidad

Tecnología de escaneo multiproceso provee alta velocidad de respuesta del sistema. Los mensajes se verifican en cada caso "en vuelo", de forma paralela, procesando archivos recibidos anteriormente. Esto permite que los usuarios reciban correo casi instantáneamente.

Ventajas adicionales de antispam Dr.Web:

- no requiere de capacitación y empieza a funcionar de manera efectiva desde el momento de instalación — a diferencia de antispam basado en el uso de Bayes (Panda, Kaspersky);
- la definición de es spam/no es spam no depende del idioma del mensaje; permite hacer varias configuraciones para diferentes categorías de correo no deseado;
- utiliza sus propias listas blancas y negras, lo que hace imposible comprometer a las empresas por medio de la introducción deliberada de las mismas en las listas de correos no deseados;
- admite un número mínimo récord de falsos positivos;
- debe ser actualizado una vez al día — las tecnologías únicas de detectar el correo no deseado basadas en varios miles de reglas excluye la necesidad de descargar actualizaciones frecuentes y engorrosos.

Protección de la información confidencial

El producto permite recuperar los mensajes eliminados accidentalmente de los buzones de correo, así como realizar investigaciones relacionadas con la fuga de información. Esto contribuye tanto a la gestión de cuarentena a través de interfaz web, o a través de una utilidad especial, así como la capacidad de archivar todos los mensajes que entran.

Comodidad en administración.

La capacidad de utilizar la interfaz web para configurar y administrar el producto permite administrar fácilmente la protección desde cualquier parte del mundo.

Transparencia

Dr.Web para servidores de correo UNIX pueden integrarse en las soluciones de otros fabricantes. Además, gracias a la API abierta, pueden añadirse nuevas funcionalidades.

La capacidad de conectar un número ilimitado de plugins

Dr.Web para servidores de correo UNIX permite aumentar capacidad funcional de forma ilimitada, cualquier plugin desarrollado funciona a la vez con todos compatibles con MTA. Plugins comercializados:

- Plugin Dr.Web para el escaneo antivirus de correo con el motor antivirus Dr.Web;
- vaderetro es un plugin que filtra spam a través de su propia biblioteca Vade Retro;
- headersfilter es un plugin que filtra los mensajes por sus encabezados.

Sistemas operativos compatibles

- Distribuciones de Linux, con kernel 2.4.x y superior.
- FreeBSD con versión 6.x y superior para la plataforma Intel x86.
- Solaris con versión 10 para Intel x86.

Proxy SMTP Dr.Web

El módulo proxy Dr.Web SMTP es el componente del producto Dr.Web para servidores de correo UNIX que puede ser instalado en una zona desmilitarizada (DMZ), y dentro del sistema postal. Debido al hecho de que el servidor del análisis de mensajes puede ser puesto en la zona desmilitarizada, y el servidor de correo esté aislado de Internet, incluso en caso de atacar el servidor el cibercriminal no obtendrá acceso a la información importante de la empresa. La solución implementa un análisis completo de correo en los protocolos SMTP/LMTP.

El uso de proxy SMTP Dr.Web:

- aumenta significativamente la seguridad global de la red;
- hace posible mejorar significativamente la calidad de la filtración debido a la ausencia de restricciones impuestas por los servidores de correo;
- reduce la carga en los servidores de correo internos y estaciones de trabajo; aumenta la estabilidad de sistema de chequeo de la correspondencia en general.

Ventajas

- Protección contra ataques de spammers, con el proxy Dr.Web SMTP el administrador tiene la oportunidad de limitar los parámetros de sesiones SMTP, identificando las señales de ataques de spam.
- Autentificación de direcciones IP. Proxy Dr.Web SMTP permite verificar la autenticidad de dirección IP y proteger a la empresa contra spam disfrazado bajo dirección IP falso del remitente.
- Protección contra ataques de hackers. Proxy Dr.Web SMTP puede efectivamente resistir los ataques "pasivos" (como PLAIN, LOGIN, etc.) y los ataques activos sin reventar el diccionario.
- Protección de las trampas de spam. Proxy Dr.Web SMTP permite realizar la verificación del destinatario en cuanto a la trampa del spam.
- Protección contra mensajes con formatos incorrectos. Dr.Web SMTP proxy permite bloquear las cartas con los campos vacíos, pero, al mismo tiempo, procesar correctamente los mensajes de los clientes de correo que crean cartas incorrectamente.
- Ahorro del tráfico de Internet. El uso de proxy Dr.Web SMTP ahorra el tráfico y bloquea el envío de los archivos adjuntos demasiado grandes a los empleados.
- Restricciones de los servidores Open Relays. Cuando una compañía tiene necesidad de organizar tal servidor, usando proxy SMTP Dr.Web el administrador puede limitar la lista de dominios autorizados para retransmitir el correo.

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

Dr.Web para MS Exchange

Escaneo antivirus y antispam del tráfico que se transmite a través del servidor de correo MS Exchange 2000/2003/2007/2010/2013/2016

Ventajas

- Posibilidad de utilizar en las compañías que requieren alto nivel de seguridad, el producto cumple totalmente con los requisitos de la legislación rusa y tiene certificados de conformidad con FSTEK y FSB.
- Grandes oportunidades para la instalación y configuración en función de las necesidades de la empresa.
- Alta velocidad de escaneo con carga mínima en el sistema operativo que permite que Dr.Web funcione perfectamente en servidores con cualquier configuración.
- El apoyo al concepto de funciones de servidor y los agentes de transporte de MS Exchange Server 2007/2010 para revisar los correos electrónicos en busca de virus y spam se puede realizar tanto a nivel de transporte, como a nivel de soporte de la interfaz antivirus VSAPI. Esto provee el nivel óptimo de protección a las empresas.
- El antispam integrado no requiere de formación (entra en vigor desde el momento de instalación), reduce considerablemente la carga en el servidor y aumenta la productividad de los empleados.
- Posibilidad de filtrar según las listas blancas y negras, lo que permite excluir de escaneo las direcciones específicas y aumentar su eficacia.
- Nueva posibilidad de configuración flexible de parámetros de protección de la aplicación a través del navegador de un modo cómodo para el usuario utilizando la consola de administración web.
- Capacidad de filtrar según tipos de archivo, permitiendo a la empresa a reducir el volumen de tráfico.
- Un mecanismo de agrupación que permite configurar diversos parámetros para diferentes grupos de empleados, y por lo tanto, reduce significativamente la introducción del sistema de protección antivirus y simplifica el mantenimiento del producto.
- Configuración flexible de parámetros de protección de la aplicación a través del navegador de un modo cómodo para el usuario utilizando la consola de administración web.
- Alto rendimiento y estabilidad gracias a la verificación multiproceso.
- Tecnologías únicas para detectar empacadores desconocidos (nuevos) y objetos maliciosos.
- Inicio de aplicaciones es completamente automatizado (al iniciar el sistema). Sistema de actualizaciones cómoda utilizando el programador de Windows.

Funciones principales

- Escaneo antivirus y antispam de mensajes de correo electrónico, incluyendo los archivos adjuntos “en vuelo”.
- Escaneo antivirus de mensajes en los buzones de los usuarios, así como de los archivos en las carpetas compartidas.
- Comprobación antivirus del flujo de correo de tránsito que pasa a través del servidor de MS Exchange. El tratamiento de los archivos infectados.
- La agrupación de los usuarios mediante Active Directory.
- Apoyo al concepto de funciones de servidor y los agentes de transporte para MS Exchange Server 2007/2010.

- Escaneo utilizando los parámetros especificados: selección de tamaño máximo y de tipos de objetos analizados, acciones (incluyendo los archivos que no pueden ser comprobados), así como las formas de procesar los objetos infectados.
- Detección de objetos maliciosos en múltiples archivos zip.
- Aplicación de diferentes acciones, en función del tipo de spam, incluyendo mover en cuarentena y añadir un prefijo al tema del mensaje.
- En caso necesario se puede añadir un texto arbitrario a las cartas. Aislamiento de archivos infectados y sospechosos en cuarentena.
- Notificación al administrador u otros usuarios sobre los incidentes de virus. Lleva la estadística del funcionamiento del kit.
- Actualizaciones automáticas.

Requisitos del sistema

Si se utiliza Microsoft Exchange Server 2000/2003:

- Procesador Pentium 133 MHz (733 MHz recomendado). RAM: 256 MB (512 MB recomendado).
- Espacio libre en disco: 20 MB para la instalación;
- 50 MB para el registro de eventos.
- Microsoft® Windows® 2000 Server o Advanced Server con SP4 instalado; Microsoft® Windows Server® 2003 (versión Standard, Enterprise o Datacenter) con SP1 o superior instalado.

Si se utiliza Microsoft Exchange Server 2007/2010:

- Procesador Intel con arquitectura x64 que soporta Intel 64 o AMD compatible con plataforma AMD64.
- RAM: 2 GB.
- Espacio libre en disco: 20 MB para la instalación; 50 MB para el registro de eventos.Microsoft® Windows Server® 2003 R2 x64 con SP2 instalado; Microsoft® Windows Server® 2008 x64.

Si se utiliza Microsoft Exchange Server 2013/2016:

- Procesador Intel con arquitectura x64 que soporta Intel 64 o AMD compatible con plataforma
- AMD64.
- RAM: 4 GB.
- Espacio libre en disco: 1 GB.
- Microsoft® Windows Server® 2008 R2; Microsoft® Windows Server® 2012; Microsoft® Windows Server® 2012 R2.

Descripción: http://products.drweb.com/mailserver/exchange

Dr.Web para IBM Lotus Domino

Protección antivirus y antispam para plataforma IBM Lotus Domino bajo Windows y Linux

Ventajas

- **Costo total mínimo**

  Dr.Web para IBM Lotus Domino no sólo funciona en servidores independientes, sino también en los servidores partitions y clústeres de Lotus Domino. Las copias de antivirus en diferentes secciones operan de manera autónoma en la memoria del ordenador utilizando bases de datos comunes y archivos ejecutables. En este caso, es necesario licenciar sólo una copia, lo que reduce significativamente el coste de la protección antivirus.

- **Ready for IBM Lotus software**

  Dr.Web para IBM Lotus Domino se encuentra dentro del catálogo de soluciones IBM Lotus Business Solutions Catalog y tiene una seña Ready for IBM Lotus software. Esta seña confirma la compatibilidad del producto con el sistema de Lotus Domino e indica que cumple todos los requisitos de conformidad con IBM.

- **Escaneo de alta velocidad**

  Organización de Dr.Web para IBM Lotus Domino, una implementación especial del método de verificación y la posibilidad de gestionar este proceso de manera flexible llevaron a un escaneo de alta velocidad con bajo consumo de recursos del sistema.

- **Instalación fácil y configuración flexible**

  Está previsto el despliegue automatizado y controlado fácilmente de Dr.Web para IBM Lotus Domino. El programa soporta los scripts administrativos y dispone de documentación detallada. La facilidad de uso está garantizada debido a una configuración flexible a través de la consola de administrador. Las herramientas de configuración "fina" de los algoritmos de antivirus según los resultados de escaneo permiten enviar una notificación de virus detectados al remitente, destinatario y a los administradores del sistema, guardar los encabezados de mensajes de correo electrónico y archivos adjuntos, etc.

- **Comodidad en administración**

  La agrupación de los mecanismos y grupos de control simplifican notablemente la administración de protección antivirus.

Funciones principales

- Escaneo y filtrado de mensajes de correo electrónico y todos sus componentes en busca de virus, spam y los mensajes no deseados "en vuelo" o según instrucciones del administrador.
- Filtración de spam, utilizando inclusive las listas de direcciones blancas y negras. Revisión de documentos en las bases NSF especificadas en busca de virus.
- Revisión de objetos a demanda mediante el arranque manual y detención de tareas de escáner.
- Análisis de mensajes de correo electrónico destacando todos los componentes de la carta para su posterior análisis.
- El tratamiento de los mensajes de correo electrónico infectados y archivos adjuntos. Detección de objetos maliciosos en múltiples archivos zip.
- Uso de mecanismo para detectar programas maliciosos ocultos por empacadores desconocidos.
- El uso de tecnología adicional de detección de objetos maliciosos desconocidos que aumenta la probabilidad de captura de los últimos tipos de virus.
- Almacenamiento de objetos infectados y sospechosos en cuarentena (el acceso a los objetos colocados en cuarentena se ejecuta a través de Lotus Notes).
- Notificación al administrador sobre los resultados de escaneo utilizando modelos descritos en el sistema, que proporciona información en un formato cómodo.
- Registro de estadísticas del sistema.
- La protección de propios módulos de fallas. Actualizaciones automáticas.

Sistemas operativos compatibles

- **Versión para Windows**
  Sistema operativo: Windows Server 2000/2003/2008/2008R2/2012/2012 R2 (versiones de 32 y 64 bits).
  Lotus Domino de versión R6.0 y superior (versiones de 32 y 64 bits).
  Procesador Intel Pentium 133 y superior.
  RAM 128 MB (se recomienda 512 MB).
  Espacio libre en el disco: 128 MB.
- **Versión para Linux**
  Sistema operativo: Red Hat Enterprise Linux (RHEL) de versión 4 y 5, Novell SuSE Linux Enterprise Server (SLES) de versión 9 y 10 (solo de 32 bits).
  Lotus Domino de versión 7.x o 8.x.
  Lotus Notes 6.5 (o más reciente) para Windows.
  Procesador Intel Pentium 133 y superior.
  RAM 64 MB (se recomienda 128 MB).
  Espacio libre en el disco: 90 MB.

Descripción: http://products.drweb.com/lotus

Dr.Web para servidores de correo Kerio

Verificación antivirus de los archivos adjuntos de los mensajes transferidos por SMTP/POP3

Ventajas

- Excelente compatibilidad con servidores de correo Kerio, que se confirma con las pruebas de Kerio Technologies.
- Capacidad para trabajar en modo de protección centralizada utilizando el Centro de Control Dr.Web Enterprise Security Suite.
- El día de hoy Dr.Web es el único plugin antivirus ruso para servidores de correo Kerio, que es lo importante en el suministro de productos para organizaciones gubernamentales.
- Apoyo localizado para los usuarios.
- El tiempo mínimo de entrega de mensajes y fiabilidad elevada del producto mediante el uso de la tecnología multiproceso.
- Requisitos del sistema simplificados sin carga en la red.
- Configuración flexible del sistema orientado al cliente: la elección de objetos para escaneo y acciones con virus detectado o archivos sospechosos.
- Elección de acciones para los archivos que no son verificables.
- Control cómodo desde la consola de administración del servidor de correo Kerio.

Funciones principales

- Comprobación de los archivos adjuntos de los mensajes de correo electrónico entrantes y salientes.

Sistemas operativos compatibles

- Versión para Windows
  Espacio en el disco duro: no menos de 350 MB.
  Sistema operativo: Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 /2012 (versiones de 32 y 64 bits).
  Servidor de correo: Kerio MailServer 6.2 o superior, Kerio Connect 7.0.0 o superior.
- Versión para Linux
  Espacio en el disco duro: no menos de 290 MB.
  Sistema operativo: 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 y 11.1; CentOS Linux 5.2 y 5.3; Debian 5.0; Ubuntu 8.04 LTS.
  Servidor de correo: Kerio MailServer 6.2 o superior, Kerio Connect 7.0.0 o superior.
- Versión para OS X
  Espacio en el disco duro: no menos de 55 MB.
  Sistema operativo: OS X 10.7 y superior.
  Servidor de correo: Kerio MailServer 6.2 o superior, Kerio Connect 7.0.0 o superior.

Descripción: http://products.drweb.com/mailserver/kerio

Dr.Web Gateway Security Suite

Protección de correo y puertas de enlace

- Dr.Web para gateways Unix son certificados por FSTEK de Rusia
- Dr.Web para gateways Kerio
- Dr.Web para MIMEswepper Dr.Web para Qbik WinGate
- Dr.Web para Microsoft ISA Server y Forefront TMG

Sistemas operativos compatibles

	Windows	Linux	FreeBSD	Solaris
		para plataforma Intel x86		
Dr.Web para gateways de Internet Unix		versión del kernel 2.4.x y superior	versión 6.x y superior	versión 10
Dr.Web para gateways Kerio	2000/XP/2003/2008/7			
Dr.Web para MIMEsweeper	2000 Server SP4 o superior/Server 2003 o superior			
Dr.Web para Qbik WinGate	Vista/Server 2008/Server 2003/XP/2000 (sistemas de 32 y 64 bits)			
Dr.Web para Microsoft ISA Server y Forefront TMG	Si se utiliza Microsoft iSA Server: ▪ Microsoft® Windows Server® 2003 x86 con Service Pack 1 (SP1) ▪ Microsoft® Windows Server® 2003 R2 x86 Si se utiliza Microsoft Forefront TMG: ▪ Microsoft® Windows Server® 2008 SP2 ▪ Microsoft® Windows Server® 2008 R2			

Licenciamiento Dr.Web Gateway Security Suite

Tipos de licencias

- Número de usuarios protegidos (mínimo 5).
- Licencia para cada servidor es para el escaneo de cantidad ilimitada de correspondencia en un solo servidor, el número de usuarios protegidos no debe exceder 3000.

El software de Dr.Web para proteger el correo se puede comprar por separado o como parte del grupo Dr.Web Enterprise Security Suite. En este último caso, el Centro de Control de Dr.Web Enterprise Security Suite están licenciados adicionalmente (para gateways Kerio y UNIX) y Antispam (excepto gateways UNIX y Kerio).

Opciones de licencias

	Dr.Web para gateways Unix	Dr.Web para gateways Kerio	Dr.Web para MIME-sweeper	Dr.Web para Qbik WinGate	Dr.Web para Microsoft ISA Server y Forefront TMG
Licencia básica	Antivirus				
Componentes adicionales:					
Antispam			+	+	+
Centro de Control	+	+			

También los productos Dr.Web para proteger gateways están disponibles en Kits Dr.Web para las empresas pequeñas y medianas.

Dr.Web para puertas de enlace UNIX

Comprobación antivirus de tráfico HTTP y FTP que pasa a través de la puerta de enlace corporativa — el servidor proxy

Funciones principales

- Comprobación antivirus de tráfico HTTP y FTP.
- Gestión centralizada a través del administrador de web del Centro de Control de Dr.Web Enterprise Security Suite.
- Filtrado de acceso por el tipo MIME y tamaño de archivo o el nombre del host. Ajuste del acceso a los recursos de la web.
- Optimización del análisis de tráfico debido al uso de la tecnología de Preview. Trabajo tanto con el protocolo IPv4, como con el protocolo de próxima generación IPv6.
- Escaneo y aplicación de diferentes acciones en función del tipo de archivos que deben analizarse. Aislamiento de objetos infectados en cuarentena.
- El informe se presenta en un formato cómodo.
- El procesamiento de múltiples solicitudes en una sola conexión. Protección contra el acceso no autorizado.
- Monitoreo y recuperación automática del sistema.
- Aviso al usuario sobre los intentos de descarga de página maliciosa o detección de virus.

Ventajas

- Oportunidades amplias en el establecimiento de una protección completa contra amenazas que se hallan en el tráfico web entrante.
- Sólo se provee el contenido seguro dentro de la red protegida.
- Filtración eficiente del tráfico en el servidor ICAP no disminuye prácticamente la velocidad de entrega de contenido.
- Ahorros significativos de gastos en el uso de Internet.
- Resistencia eficaz a la penetración de cualquier tipo de malware. Alta escalabilidad — la capacidad de procesar grandes volúmenes de información en tiempo real.
- La capacidad de procesar grandes volúmenes de información en tiempo real. Excelente compatibilidad — la integración con cualquier software que soporte el protocolo ICAP, con todos firewall conocidos.
- Soporta casi todos los sistemas operativos utilizados actualmente bajo UNIX.
- Poca exigencia a los recursos del sistema, el producto opera de forma ideal en los gateways de casi cualquier configuración.
- Flexibilidad y facilidad de administración, el producto permite implementar el plan de protección que corresponde a la política de seguridad de la empresa.

Sistemas operativos compatibles

- Linux con kernel 2.4.x y superior
- FreeBSD con versión 6.x y superior (para la plataforma Intel x86).
- Solaris versión 10 (para plataforma Intel x86)
- Cualquier servidor proxy compatible con el protocolo ICAP, en particular: Squid no inferior a 3.0.
- Shweby no inferior a 1.0.
- SafeSquid no inferior a 3.0.

Descripción: http://products.drweb.com/gateway/unix

Dr.Web para puertas de enlace Kerio

Análisis antivirus del tráfico que se transmite por HTTP, FTP, SMTP y POP3, así como a través de servicio web Kerio Clientless SSL VPN

Dr.Web para gateways Kerio es un plugin antirvirus que se conecta a Firewall Kerio. Se instala en el mismo equipo donde está instalado Kerio y se utiliza como un software antivirus externo.

Ventajas

- Detección de objetos maliciosos que se transmiten por HTTP, FTP, SMTP y POP3, así como a través de servicio web Kerio Clientless SSL VPN
- Protección fiable de acceso a Internet tanto para usuarios particulares, como para las empresas de cualquier tamaño y tipo de actividad.
- Capacidad para trabajar en modo de protección centralizada utilizando el Centro de Control Dr.Web Enterprise Security Suite.
- Facilidad de administración. Es posible recibir mensajes de incidentes virales a través de la notificación por correo, o vía SMS.
- El tiempo mínimo de entrega de mensajes mediante el uso de la tecnología multiproceso.

Funciones principales

- Detección de objetos maliciosos que se transmiten por HTTP, FTP, SMTP y POP3, así como a través de servicio web Kerio Clientless SSL VPN
- Detección de archivos adjuntos infectados en el correo electrónico antes de ser procesados por el servidor de correo.
- Formación de una lista de protocolos de intercambio de datos verificables. Visualización de la información sobre el funcionamiento del programa por medio de la consola web.
- Escaneo con la posibilidad de ajustar la configuración: selección del tamaño máximo, tipos de objetos verificados, los métodos de tratamiento de los archivos infectados.
- Empleo de acciones para las amenazas detectadas de acuerdo con la configuración Kerio. Activar/desactivar la detección de malware (según el tipo).
- Registro de errores y eventos en el registro de sucesos (Event Log) y en registro de texto.
- Envío de notificaciones por correo electrónico sobre diferentes eventos a los usuarios seleccionados. Las actualizaciones automáticas de bases de datos de virus.

Requisitos del sistema

Versión para Windows

- No menos de 350 MB de espacio libre en el disco.
- Sistema operativo Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (versiones de 32 y 64 bit).
- Firewall Kerio WinRoute Firewall 6.2 o superior, Kerio Control 7.0.0 o superior.

Versión para Kerio Control VMware Virtual Appliance y Kerio Control Software Appliance

- No menos de 290 MB de espacio libre en el disco.
- Sistema operativo Kerio Control VMware Virtual Appliance o Kerio Control Software Appliance.
- Firewall Kerio Control 8.x o superior.

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

Dr.Web para MIMEsweeper

Protección antivirus y antispam de tráfico de correo electrónico que pasa a través de los servidores de filtrado de contenidos de ClearSwift MIMEsweeper

Ventajas

Simplicidad de instalación y configuración

Herramientas de configuración incorporadas en Dr.Web para MiMEsweeper — asistente de escenarios — permitirá crear los escenarios más avanzados de escaneo de mensajes (tipo 1 según ClearSwift).

Compatibilidad con DEP

Dr.Web para MIMEsweeper es compatible con la tecnología de prevención de ejecución de datos (Data Execution Prevention, DEP), que permite efectuar un análisis adicional de la memoria y evita la ejecución de código. Gracias a esto, los usuarios no tienen que cambiar el modo de operación DEP — los programas maliciosos no podrán usar el mecanismo de control de excepciones de Windows.

Los ajustes flexibles

Tras la detección de un objeto infectado, el plugin trata de curarlo o eliminarlo de inmediato, si la opción de tratamiento no ha sido seleccionada. Si en un mensaje de correo están adjuntos varios archivos, el plugin neutraliza solo archivos adjuntos infectados. Cuando se detecta un virus en el cuerpo del mensaje, el filtro de contenido traslada la carta a la cuarentena. Mensajes de correo electrónico "limpios" y los archivos comprimidos se transfieren al destinatario sin ninguna modificación. Las cartas maliciosas que el plugin Dr.Web no puede neutralizar, se marcan y por defecto se trasladan a la cuarentena.

Funciones principales

- Analiza los mensajes de correo electrónico y sus archivos adjuntos, incluyendo archivos, antes de ser procesados por el servidor de correo.
- Tratamiento de los objetos infectados.
- Aislamiento de archivos infectados y sospechosos en cuarentena.
- Filtrado de spam en el correo, con el uso de listas blancas y negras.
- Registro de estadística del funcionamiento del kit.
- Actualizaciones automáticas.

Requisitos del sistema

- OS Windows 2000 Server Service Pack 4 (SP4) o superior, o Windows Server 2003 o posterior.
- Filtro de contenido de correo ClearSwift MIMEsweeper™ para SMTP 5.2 o posterior.

Descripción: http://products.drweb.com/mimesweeper

10.06.2016

Dr.Web para Qbik WinGate

Comprobación del tráfico antivirus y antispam a través de protocolos HTTP/POP3/FTP del servidor proxy y servidor SMTP Qbik WinGate

Ventajas

- Dr.Web Qbik Wingate es el único plugin para Qbik Wingate que al día de hoy está completamente rusificado.
- Sólo Dr.Web para Qbik WinGate tiene tanto la documentación, como el soporte técnico directamente del fabricante.
- A diferencia de productos competidores, el producto de Doctor Web tiene la capacidad de filtrado antispam. El módulo eficiente y compacto de antispam no requiere capacitación, permite establecer diferentes acciones para cada una de las tres categorías del spam previstas por el programa, así como crear listas blancas y negras de direcciones de correo electrónico.
- La presencia de una tecnología adicional de detección de malware desconocido (Origins Tracing), incluyendo archivos con un formato desconocido, que no tiene análogos.

Funciones principales

- Escaneo antivirus y antispam de mensajes de correo que se transmiten a través de SMTP y POP3, incluyendo el análisis de los archivos adjuntos.
- Análisis antivirus de archivos y datos transferidos a través de HTTP y FTP.
- Tratamiento de los archivos infectados transferidos a través de HTTP.
- Registro de eventos.
- Propio panel de control y gestión de cuarentena.
- Las actualizaciones automáticas de bases de datos de virus.

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

Dr.Web para Microsoft iSA Server y Forefront TMG*

Comprobación del tráfico antivirus y antispam a través de servidores de Microsoft ISA Server y Forefront TMG

Ventajas

- Escaneo de todos los objetos en un tiempo mínimo mediante las tecnologías de análisis dinámico de las necesidades de otros servicios de servidores en los recursos y el cambio automático instantáneo entre tareas.
- Aprovecha las capacidades de las plataformas para acelerar la velocidad de escaneo.
- Capacidad para operar en servidores de cualquier configuración — incluyendo los que tienen poca cantidad de RAM.
- Protección de los servidores reales y virtuales.
- El antispam integrado no requiere de formación (entra en vigor desde el momento de instalación), reduce considerablemente la carga en el servidor y aumenta la productividad de los empleados.
- Bloqueo de acceso a una variedad de recursos de Internet y la posibilidad de filtrar por tipos de archivos que permite a la compañía detener la penetración de los virus que contienen recursos maliciosos y reducir el volumen de tráfico.

- Tecnologías únicas para detectar empacadores desconocidos (nuevos) y objetos maliciosos.
- Grandes oportunidades para la instalación y configuración en función de las necesidades de la empresa.

Funciones principales

- Comprobación antivirus y antispam de todo el tráfico, incluidos los archivos adjuntos.
- Posibilidad de escaneo de archivos "en vuelo" detectando objetos maliciosos en múltiples archivos zip.
- El tratamiento de los archivos infectados.
- Aplicación de diferentes acciones en función del tipo de correo no deseado.
- Se adjunta el texto a los mensajes de correo que contenían amenazas de seguridad.
- Bloqueo del acceso a los datos infectados para todos los usuarios en las redes locales.
- Restricción del acceso de usuario a los recursos de Internet utilizando el control de oficina. Aislamiento de archivos infectados y sospechosos en cuarentena.
- Notificación al administrador sobre los incidentes de virus. Registro de estadística del funcionamiento del kit.
- Actualizaciones automáticas.

Requisitos para OS y software

Si se utiliza Microsoft ISA Server:

- Procesador Pentium III 733 MHz o superior.
- RAM: 1 GB o más.
- Espacio libre en disco: 300 MB para la instalación. El tamaño adicional requerido para el espacio libre en disco es necesario para almacenar datos de forma temporal en la etapa de escaneo antivirus.
- OS: Microsoft® Windows Server® 2003 x86 con Service Pack 1 (SP1), Microsoft® Windows Server® 2003 R2 x86.
- Servidor proxy. Microsoft® ISA Server 2004, Microsoft® ISA Server 2006.

Si se utiliza Microsoft Forefront TMG:

- Procesador Pentium III 1.86 HHz o superior.
- RAM: 2 GB o superior.
- Espacio libre en disco: 300 MB para la instalación. El tamaño adicional requerido para el espacio libre en disco es necesario para almacenar datos de forma temporal en la etapa de escaneo antivirus.
- OS: Microsoft® Windows Server® 2008 SP2, Microsoft® Windows Server® 2008 R2.
- Servidor proxy: Microsoft® Forefront® TMG 2010.

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

Dr.Web Mobile Security Suite

Protección de dispositivos móviles

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

	Dr.Web para Android	Dr.Web para Symbian OS	Dr.Web para Windows Mobile
Componentes de protección	Protección completa*	Antivirus + Antispam	Antivirus + Antispam
Administración centralizada dentro de Dr.Web Enterprise Security Suite	+	–	+
Sistemas operativos compatibles	OS Android 4.0-5.0. Firewall es compatible con Android 4.0 y más	S60, Symbian 9 y superior	Windows Mobile 2003/ 2003 SE/5.0/6.0/6.1/ 6.5
Funciones claves			
Escaneo "en vuelo"	+	+	+
Comprobación de los archivos recibidos a través de GPRS/infrared/Bluetooth/Wi–Fi/USB-conexión o durante sincronización con PC	+	+	+
Hay dos tipos de escaneo: completa y personalizada	+	+	+
Posibilidad de activar/desactivar la tarjeta de memoria de prueba permanente	+	–	+
Análisis bajo demanda del sistema de archivos entero o archivos y carpetas individuales	+	+	+
Comprobación de los archivos en formatos ZIP, SiS, CAB, RAR	+	+	+
Listas blancas y negras de llamadas y mensajes SMS entrantes	+	+	+
Eliminación de archivos infectados	+	+	+
Traslado de los archivos sospechosos a la cuarentena	+	+	+
Restauración de archivos de la cuarentena	+	+	+
Actualizaciones vía Internet: ▪ a través de HTTP utilizando módulo integrado GPRS; ▪ a través de infrared/Bluetooth/Wi-Fi/ conexión USB; ▪ mediante la sincronización de PC con acceso a Internet a través de la conexión ActiveSync	+	+	+
Los informes detallados sobre el escaneo del sistema	+	+	+
Control remoto de dispositivo móvil en caso de su pérdida o robo — usando "Antirrobo"			+

* La licencia incluye los siguientes componentes de seguridad: antivirus, antispam, antirrobo, control paterno.

Licenciamiento Dr.Web Mobile Security Suite

Dr.Web para la protección de los dispositivos móviles está licenciado por el número de dispositivos móviles protegidos.

Opciones de licencias

Dr.Web para Windows Mobile	Dr.Web para Symbian OS	Dr.Web para Android
▪ Antivirus + Antispam + Centro de Control	▪ Antivirus + Antispam	▪ Protección completa + Centro de Control

También los productos Dr.Web para proteger los dispositivos móviles están disponibles en Kits Dr.Web económicos para las empresas pequeñas y medianas.

Oferta especial

La licencia gratuita para Dr.Web Mobile Security Suite se otorga a los usuarios registrados de Dr.Web Security Space y Antivirus Dr.Web.

Descripción: http://products.drweb.com/mobile/biz

Dr.Web Retail Security Suite.
Productos para la venta al por menor

Dr.Web Security Space
2 PC/1 año

Dr.Web Antivirus
2 PC/1 año

Kit "Empresa pequeña"
5 PC/1 servidor/1 año

Bonificación

- Licencia para Dr.Web Mobile Security para proteger los dispositivos móviles bajo Android OS, Symbian OS, Windows Mobile. El número de dispositivos protegidos equivale al número de PC protegidos.
- Licencia para la utilidad de desinfección Dr.Web CureIt!

"Dr.Web Universal" (para clientes ASC)

Media kit «Dr.Web Universal» se abastece sólo a los centros de servicio autorizado Dr.Web y está disponible para los clientes ASC a un precio especial.

El producto provee la protección de 1 PC y 1 dispositivo móvil durante 1 año.

Composición de licencia:

- Dr.Web Security Space Antivirus
- Dr.Web para OS X Antivirus
- Dr.Web para Linux
- Dr.Web Mobile Security
- Dr.Web para Android OS
- Dr.Web para Symbian OS
- Dr.Web para Windows Mobile

Conjunto de entrega

- Sobre corporativo
- Certificado de licencia
- Disco de instalación

Bonificación

- Dr.Web Mobile Security
- Dr.Web CureIt
- Dr.Web CureNet!

Más información acerca de los centros autorizados Dr.Web — http://partners.drweb.com/service

Memo para el vendedor de productos al por menor — https://st.drweb.com/static/new-www/files/booklets/pamyatka_site_a5/Pamyatka_ru.pdf

Kits Dr.Web

El kit incluye productos Dr.Web para la protección de todo tipo de objetos.

¡IMPORTANTE! Ningún tipo de descuento está previsto para el kit, incluyendo el de renovación. Para seguir utilizando el kit, se debe adquirir una licencia nueva a precio completo. El descuento en renovación se otorga al cambiar el kit por ciertos productos Dr. Web.

Kit Dr.Web «Universal»

Una protección completa accesible de clase empresarial para empresas pequeñas y medianas

Las empresas medianas a menudo carecen de la oportunidad de hacer inversiones significativas en la protección completa de información. El kit Dr.Web "Universal" está diseñado para dichas empresas, siendo una propuesta económica para las compañías con el número de PCs de 5 a 50.

Productos	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
Objetos protegidos	Estaciones de trabajo	Servidores	Usuarios de correo electrónico	Usuarios de correo y gateway	Dispositivos móviles
Licencia	Protección completa	Antivirus	Antivirus + Antispam	Antivirus	Antivirus
Contenido del paquete	de 5 a 50	1	Equivale al número de estaciones	Equivale al número de estaciones (a partir de 25)	Equivale al número de estaciones

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

Kit Dr.Web para escuelas

Objetos protegidos	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mobile Security Suite
Licencia	Protección completa + CC	Antivirus	
Contenido del paquete	10 – 200	1–8	10–200

Utilidades

Utilidades de desinfección Dr.Web están diseñadas para analizar y neutralizar amenazas en caso de necesidad. No proveen protección permanente de su equipo.

Dr.Web CureNet!

Tratamiento centralizado de redes locales de cualquier tamaño, inclusive si tienen el antivirus instalado de otro fabricante

Los usuarios potenciales	Las empresas pequeñas, medianas, grandes, en las redes de área local está instalado el antivirus de otro fabricante.
Tareas desempeñadas	▪ Tratamiento centralizado de forma remota de las estaciones de trabajo y de los servidores de Windows. ▪ Comprobación de la calidad de la protección antivirus de otro elaborador.
Características de la utilidad	▪ No requiere la desinstalación de antivirus de otro elaborador antes de escaneo y tratamiento. ▪ No requiere de un servidor o de instalar software adicional. ▪ Puede ser utilizado en redes que están completamente aislados de Internet. ▪ Asistente Dr.Web CureNet! se puede ejecutar desde cualquier unidad externa, inclusive USB.
Descripción del producto	http://curenet.drweb.com
OS compatibles	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 (arquitectura de 32- y 64-bit).
¿Qué es "Mi Dr.Web CureNet!"?	Es un área personal que contiene un enlace personal para descargar la distribución actualizada durante la vigencia de la licencia. También en el área personal se puede ponerse en contacto con soporte técnico, enviar un archivo sospechoso para el análisis, usar otros servicios.
Licenciamiento	La utilidad se licencia por el número de estaciones (5 como mínimo) por 1, 2 y 3 años de uso.
Versión demo Sin función de tratamiento.	Sin función de tratamiento.
Requisitos del sistema	**Asistente** ▪ Cualquier PC bajo la administración de 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 (arquitectura de 32- y 64-bit) ▪ Memoria operativa libre: no menos de 360 MB. ▪ Espacio libre en el disco duro: no menos de 200 MB. ▪ Conexión a todas las estaciones escaneadas a través del protocolo TCP/IP. ▪ Acceso a Internet: para actualizar las bases de virus y componentes de Dr.Web CureNet! **Escáner** ▪ Cualquier PC bajo la administración de MS Windows XP Professional y versiones posteriores, excepto Windows® Server 2003 x64 Edition y Windows® XP Professional SP2 x64 Edition. ▪ Memoria operativa libre: no menos de 360 MB. ▪ Espacio libre en el disco duro: no menos de 200 MB.

Dr.Web Cureit!

El tratamiento de emergencia de PC y servidores bajo Windows, incluyendo si está instalado el antivirus de otro fabricante

Usuarios potenciales	Pequeñas y medianas empresas en los equipos y servidores de las cuales está instalado el antivirus de otro fabricante
Tareas por resolver	▪ Desinfección emergente de estaciones de trabajo y servidores Windows. ▪ Comprobación de la calidad de la protección antivirus de otro fabricante.
Características de la utilidad	▪ No requiere instalación, no produce conflictos con ningún antivirus, es decir, para escanear no hace falta deshabilitar el antivirus de otro fabricante instalado. ▪ Autoprotección mejorada y modo avanzado para la resistencia eficaz a los bloqueadores de Windows. ▪ Actualizaciones una vez o varias cada hora. ▪ La utilidad puede iniciarse desde cualquier unidad externa, entre ellas, desde USB.
Descripción del producto	http://www.freedrweb.com/cureit/?lng=es
OS compatibles	MS Windows 8/2012/7/2008/Vista/2003/XP Professional/2000 (32 y 64 bits)
Licenciamiento	Utilidad está licenciada por el número de estaciones, para 1, 2 y 3 años de uso
Características de licenciamiento	Utilidad es gratuita para el tratamiento de PC particular de hogar
Versión demo	No hay versión demo.

Dr.Web LiveDemo

El servicio de test en línea remoto Dr.Web LiveDemo permite incluso antes de comprar el conjunto de hardware y software, probar la configuración seleccionada en la red local virtual del servidor de Doctor Web.

Servicio de test en línea Dr.Web LiveDemo
http://download.drweb.com/live_demo/?lng=ru

Soluciones

Dr.Web Security Suite para UNIX Appliance

Grupo de soluciones modulares diseñado para la integración con los sistemas de hardware y software construidas sobre la base de los sistemas operativos UNIX (Linux/FreeBSD/Solaris (x86)).

Soluciones cumplen la función de puerta de enlace de Internet corporativo – servidor proxy que se utiliza para organizar el acceso de los usuarios de la intranet interna a los recursos de Internet.

	Dr.Web Mail Security Suite para UNIX Appliance	Dr.Web Gateway Security Suite para UNIX Appliance
Función clave	Filtrado de mensajes de correo electrónico de virus y spam	Filtrado de tráfico HTTP y FTP de virus
Opciones de licencias	▪ Antivirus ▪ Antivirus + Antispam	Antivirus

Tipos de licencias

- Por el número de usuarios protegidos (es ilimitado).
- La licencia para cada servidor sirve para el escaneo de cantidad ilimitada de correspondencia en un solo servidor, el número de usuarios protegidos no debe exceder 3000.

Licenciamiento SDK

SDK se distribuye gratuitamente dentro del producto. Los desarrolladores terceros pueden desarrollar y distribuir fácilmente plugins en base de SDK en condiciones no comerciales. Para la distribución comercial se debe pasar el proceso de certificación.

Dr.Web ATM Shield

Protección antivirus centralizada de sistemas integrados (cajeros automáticos, terminales, multi-quioscos).

Los usuarios potenciales son los bancos (ATM), cadenas de tiendas (POS, multi-quioskos), así como las empresas y organizaciones que controlan los procesos de producción (gasolineras, fábricas, etc.).

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

Ventajas

- fácil integración en la red de cajeros automáticos y dispositivos de caja y, en consecuencia, una reducción significativa en el tiempo de su mantenimiento;
- oportunidad de operar en equipos basados en una plataforma débil de hardware (512 MB), que funcionan durante mucho tiempo sin la posibilidad de reinicios – en modo de 24/7;
- gestión centralizada de todos los componentes de protección antivirus de los sistemas integrados;
- la solución contiene componentes que permiten proporcionar protección contra los malware incógnitos que aún no hayan ingresado para el análisis en el laboratorio antivirus, así como contra otras actividades no autorizadas del personal de servicio;
- escalabilidad fácil que permite su uso en redes con un número indeterminado de nodos (debido a la estructura jerárquica de la red antivirus);

- funcionamiento en redes basadas en TCP/IP, IPX, NetBIOS;
- oportunidad de elegir el tipo de protección del servidor de base de datos;
- el tráfico de red mínimo basado en un intercambio de información de protocolo de diseño especial que admite la compresión de datos entre el cliente y el servidor;
- capacidad de cifrar los datos intercambiados entre los diversos componentes del sistema; vigilancia del estado de todos los nodos protegidos de la red;
- recogida centralizada de estadísticas sobre incidentes de virus; copia de seguridad de datos críticos del servidor de protección de la red;
- transparencia del funcionamiento, el registro de acciones de administradores permite realizar el seguimiento de todos los pasos para instalar y configurar el sistema.

¡Atención! Debido al hecho de que el uso de la protección antivirus en los dispositivo integrados tiene una serie de características, se recomienda encarecidamente a los clientes antes de usar Dr.Web Shield ATM leer la Guía del Administrador (está disponible en el asistente de descarga después de solicitar el demo) y estudiar el curso de formación para este producto.

Licenciamiento

- Por el número de dispositivos integrados protegidos.
- El Centro de Control Dr.Web Shield ATM está licenciado gratuitamente.

Demo

Para obtener una licencia de prueba se debe completar una solicitud de http://download.drweb.com/ demoreq/atm_shield, indicando el número de dispositivos protegidos, y de preferencia el sistema operativo utilizado.

¡Atención! Si en los dispositivos integrados del cliente se utilizan OS tales como Embedded (MS Windows Embedded 7, MS Windows Embedded 8, etc.), hay que advertir de que tales sistemas operativos no son análogos completos de sistemas operativos comunes, han sido compuestos para cada tipo de dispositivo integrado, por lo que pueden carecer de ciertos componentes, potencialmente necesarios para la implementación de protección antivirus. En ese sentido, el dispositivo protegido (en forma de una imagen) puede ser probado por el departamento de elaboración o de desarrollo de la compañía Doctor Web, en resultado (en caso de ausencia de tales componentes) pueden darse recomendaciones para su instalación.

Herramientas de marketing para partners https://pa.drweb.com/products/atm_shield

Servicios

El software as a service (SaaS) es un modelo difundido ampliamente fuera de Rusia de concesión de software como un servicio.

Hasta el 2007 este modelo no se utilizaba en la industria antivirus rusa. Esto se debía a una simple ausencia de soluciones domésticas de tipo similar. El cambio se produjo en mayo de 2007, cuando la compañía rusa Doctor Web lanzó su propio servicio de Internet Dr.Web AV-Desk. En el mercado de servicios de TI en Rusia apareció un nuevo segmento — el segmento de servicios de protección antivirus. El primero de ellos fue el servicio de Antivirus Dr.Web.

Servicio de internet Dr.Web AV-Desk

¿Qué es Dr.Web AV-Desk?	Dr.Web AV-Desk — un servicio de internet que proporciona servicios en línea de seguridad de la información de los PC y servidores a un número ilimitado de clientes — usuarios domésticos y empresas. Dr.Web AV-Desk es un software que permite el control centralizado del proceso de prestación de servicio Antivirus Dr.Web. Dr.Web AV-Desk es un modelo de negocio DAV por el cual se puede atraer nuevos clientes y aumentar los ingresos.
¿Para quién es el servicio Dr.Web AV-Desk?	Está destinado para ISPs y otras compañías que trabajan en el campo de las tecnologías informativas.
¿Para quién es el servicio "Antivirus Dr.Web"?	Está destinado para las personas naturales y jurídicas — los clientes de los proveedores de servicios.
¿Qué servicios puede ofrecer un proveedor utilizando Dr.Web AV-Desk?	Servicios de protección de la información de PC del cliente contra los virus, el spam y todo tipo de malware. Están disponibles como una suscripción por un plazo más conveniente para el usuario. Por el derecho de utilización de las funciones de protección de software Dr.Web se cobrará la cuota mensual.
Funcionalidad de software Dr.Web AV-Desk	El paquete de software para la gestión centralizada de los procesos de prestación de servicios de protección de información de PC para los clientes de proveedores del servicio.
Licenciamiento Dr.Web AV-Desk	El servicio Dr.Web AV-Desk se proporciona al proveedor de forma gratuita. A su vez, el servicio Antivirus Dr.Web está licenciado por cantidad de abonados conectados al servicio durante el período de referencia (mes), el plazo del servicio debe ser vigente.

¿Cómo funciona?

El proveedor de servicios	Clientes del servicio
▪ Organiza la suscripción al servicio Antivirus Dr.Web a través del centro de control de suscripción. ▪ Provee a los clientes del servicio las actualizaciones de las bases de datos de virus y el programa de los módulos de Dr.Web. ▪ Presta apoyo técnico (opcionalmente). ▪ Supervisa el estado de la red antivirus y recoge información estadística sobre la infección viral. ▪ Proporciona servicios adicionales. ▪ Cobra a los clientes por utilizar el servicio.	▪ Efectúan suscripción en el Centro de suscripciones. ▪ Instalan el software Dr.Web. ▪ Administran los parámetros de suscripción independientemente. ▪ Abonan una cuota mensual al proveedor de servicios.

Dr.Web AV-Desk es un modelo de negocio de múltiples variantes. Los proveedores de servicio Antivirus Dr.Web pueden convertirse en proveedores de servicios de Internet o en otro tipo de empresas que trabajan en el campo de las tecnologías informativas.

	Revendedor del servicio Antivirus Dr.Web	Proveedor de servicio Antivirus Dr.Web	Servicio agregador Dr.Web AV-Desk
Negocio principal	La compañía vende la suscripción al servicio Antivirus Dr.Web para el usuario final a través del Centro de suscripciones integrado en su sitio web.	La compañía introduce el servicio Dr.Web AV-Desk y proporciona servicio Antivirus Dr.Web para el usuario final.	La compañía es la propietaria de las capacidades del servidor en las que introduce Dr.Web AV-Desk, forma su propia red de revendedores de servicio y otorga licencias para centros de control de suscripción sin derecho de realizar el servicio a los usuarios finales.

Más información sobre el servicio Dr.Web AV-Desk y "Antivirus Dr.Web" se provee a la demanda del partner.

- **Nuevo examen del curso DWCERT-004 Dr.Web AV-Desk v.6**
  https://pa.drweb.com/training/engineers
- **Nuevo examen del curso DWCERT-010-3 "Antivirus Dr.Web"**
  https://pa.drweb.com/training/courses/sales

Política de descuento

Coeficientes de descuento se aplican al precio de una licencia por 1 año (según la lista de precios).

Si el usuario tiene derecho a varios tipos de descuentos, éstos no se suman, sino se utiliza el mayor de ellos (a excepción de los descuentos para los ISP).

Los descuentos sólo se aplican a las soluciones en la lista de precios. Los descuentos para soluciones que no se encuentran en la lista de precios deben coordinarse con los representantes de Doctor Web.

Descuentos disponibles por la cantidad de productos licenciados Dr.Web Enterprise Security Suite

Los descuentos disponibles por la cantidad de productos licenciados (tipo de objetos licenciados se calculan partiendo del precio de licencias básicas y precios de licencias para los componentes adicionales – por separado para cada producto). Estos descuentos se aplican automáticamente en la calculadora.

El número de productos licenciados	Descuento
4	30%
3	25%
2	20%

Excepción: descuentos no se aplican a productos Dr.Web Mobile Security Suite.

Restricciones

Los descuentos no se aplican en caso si:

- el número de servidores es menos del 10% del número de las estaciones, de los usuarios de correo o gateways;
- el número de usuarios de correo o gateway es menor que el de las estaciones;
- el número de usuarios de gateways es menor que la cantidad de usuarios de correo y viceversa.

Tabla de descuentos

Tipo de cliente	Razón del descuento	Nueva licencia			Renovación			Migración*		
		1 año	2 años	3 años	1 año	2 años	3 años	1 año	2 años	3 años
Categorías no preferenciales	Para el descuento en renovación se requiere el archivo clave o número de serie Dr.Web, cuya vigencia es al menos 3 meses para un producto similar Dr.Web.	–	1,6	2,17	0,6	1,17	1,72	0,5	1	1,5
	Para obtener descuento en migración se requiere el original de la licencia/archivo de clave/correo confirmando el hecho de comprar una versión electrónica de antivirus de otros elaboradores.									
Instituciones educativas, bibliotecas, museos e instituciones de salud	Una copia de la licencia para la actividad educativa/certificado de registro/licencias del Ministerio de Salud de la Federación de Rusia y el formulario rellenado.	0,5	0,85	1,2	0,35	0,7	1,05			

Condiciones para renovación

1. Es posible prolongar con descuento tanto la licencia válida como la expirada. No hay plazo de prescripción para prolongar las licencias Dr.Web.
2. Es posible prolongar con descuento una licencia de un producto o de una solución Dr.Web similar. El periodo de validez de esta licencia no debe ser inferior a 3 meses.
3. El descuento de renovación se concede en caso de adquirir licencias por 1, 2 o 3 años de un producto similar o una solución Dr.Web.
4. La licencia de prolongación con descuento se concede para el número de objetos protegidos que no supere el número de objetos protegidos indicado en la licencia anterior (la que se prolonga).
5. La razón para recibir el descuento de prolongación puede ser el archivo de claves o el número de serie Dr.Web que pueden ser prolongados solo una vez.
6. Para recibir el descuento de prolongación, el usuario debe presentar al vendedor el número de serie o el archivo de claves.

"¡Cambie a verde!"

El programa de migración Doctor Web que ofrece grandes incentivos a los clientes corporativos que pasan a los productos antivirus Dr.Web.

1. Dicha oferta especial es válida solamente para productos Dr.Web. Los kits, utilidades, servicios y soluciones no participan en el programa de migración de privilegio.
2. El descuento no se aplica a las personas naturales. Sólo está disponible para la organización o la empresa por una sola vez.
3. El descuento no está disponible para los usuarios de licencias OEM.
4. Se otorga un 50% de descuento al pasar a una licencia anual Dr.Web. Durante el cambio a las licencias de dos y tres años para el cálculo de costo se aplica el coeficiente de 1 ó 1.5, respectivamente, que se multiplica por el precio de una licencia anual Dr.Web.
5. El descuento de cambio de otro antivirus sólo está disponible para el producto análogo Dr.Web (por el tipo y número de objetos protegidos).
6. Para recibir el descuento, el usuario debe proporcionar el original de la licencia, el archivo de clave o un correo electrónico de confirmación de compra de antivirus de otro fabricante con información de registro.
7. El descuento está disponible para los usuarios de licencias tanto vigentes como vencidas, siempre cuando desde el momento de la expiración de la licencia no hayan transcurrido más de 30 días.
8. Si al momento de compra de la licencia de transición, el plazo de la licencia para el antivirus de otro fabricante no se ha vencido, el tiempo restante se añade al término de la nueva licencia.
9. La renovación posterior de licencia de cambio se produce con el descuento común en renovación.
10. Descuentos en migración no se acumulan con otros descuentos.

Condiciones generales de venta

1. Los partners están obligados a vender a los usuarios finales los programas Dr.Web estrictamente de acuerdo con el contenido de producto y en base a los precios recomendados fijados en la lista de precios.
2. Para todos los productos Dr.Web de contenido estándar el costo de actualización de módulos del programa y bases de datos de virus, así como la asistencia técnica básica a través del formulario en la página web http://support.drweb.com están incluidos en el costo de la licencia reflejada en la lista de precios para todo el período de su vigencia.
3. Al realizar el pedido de licencias en caja corporativa, el precio se aumenta por el costo de los media kits (excepto la pestaña "Cajas — media kits").
4. Si el comprador requiere una solución para proteger más objetos de los están en la lista de precios, el partner deberá solicitar precio a la compañía Doctor Web y presentar a través del formulario web https://pa.drweb.com/support los siguientes datos del cliente:
   - el nombre de la organización; dirección;
   - correo electrónico;
   - teléfono de atención al cliente del técnico responsable de la protección antivirus;
   - datos de contacto de servicio de soporte técnico del partner.

   Todos tipos de descuentos en la compra de tales soluciones se otorgan al usuario final consultando con la compañía Doctor Web.
5. Los precios para soluciones que no aparecen en la lista de precios están determinados por el acuerdo de licencia que Doctor Web concluye con el proveedor de soluciones al usuario final.

La forma de solicitud para los precios de productos antivirus Doctor Web:
https://pa.drweb.com/support/price1

Compra adicional para Dr.Web Enterprise Security Suite

Reglas generales

1. La compra adicional (o ampliación) de la licencia vigente puede ser:
   - **cualitativa** es cuando a la licencia vigente se añaden nuevos componentes de protección, la composición de productos de la licencia sigue siendo sin alteración;
   - **cuantitativa** es cuando se aumenta la cantidad de objetos protegidos en el marco de los productos de la licencia actual;
   - **de producto** es cuando a la licencia vigente se agregan nuevos productos.

   Asimismo la compra adicional puede combinar los tipos descritos anteriormente.
2. El plazo mínimo de la licencia en la compra adicional es de 3 meses, el máximo es de 33 meses.
3. El tiempo restante del plazo de la licencia se calcula en función del número de meses que quedan hasta la expiración de la licencia comprada previamente (el mes incompleto se redondea a 1 mes).
4. Compra adicional está disponible sólo para licencias vigentes, que expiran dentro de más de 3 meses, de lo contrario, se aplica compra adicional con renovación.
5. El tipo de licencia en el código de la nueva licencia es C (compra adicional).
6. Activación de la licencia de compra adicional se produce automáticamente en el momento de su generación.
7. La licencia anterior se bloqueará en veinticuatro horas después de registrar la licencia adquirida, y será imposible extenderla. Para poder renovar el cliente debe presentar la licencia adquirida.

Compra adicional más renovación

1. Es posible efectuar la compra adicional con renovación para las licencias tanto vigentes, como caducadas.
2. Cuando se hace la compra adicional y renovación de la licencia vigente, el plazo de la licencia vigente se suma con el de la nueva licencia (compra adicional con renovación).
3. El tipo de licencia en el código de la nueva licencia es D (compra adicional + renovación).
4. Activación de la licencia de compra adicional se produce automáticamente en el momento de su generación.
5. La licencia anterior (renovada) se bloqueará en veinticuatro horas después de registrar la nueva licencia (compra adicional con renovación), y será imposible extenderla. Para poder renovar el cliente debe presentar la licencia adquirida.
6. Si al mismo tiempo se hace la renovación más compra adicional, el costo de licencias ADQUIRIDAS se calcula en la escala de precios de la cantidad total de licencias ADQUIRIDAS (renovables + adquiridas adicionalmente). El costo de las licencias RENOVABLES se calcula sobre la escala de la cantidad total de licencias RENOVABLES.

Reglas para el cálculo del costo de las licencias compradas adicionalmente

I. **Compra adicional cualitativa (se agregan componentes adicionales a la licencia conservando el número de objetos protegidos y la composición del producto).**
   1. Si se requiere una ampliación de Antivirus a la Protección completa para productos Dr.Web Desktop Security Suite, se aplica un 20% de incremento sobre el costo de la licencia para Antivirus, dividido proporcionalmente en la cantidad de meses que quedan hasta el final del período de licencia.

Ejemplo:

El cliente ha pagado 1,628 euros por la licencia de Antivirus para 90 PC. Luego el cliente ha decidido a pasar a la protección completa dentro de 2 meses después de la activación de la licencia.

1,628 euros ÷ 12 meses × 0,2 (20% de sobretasa) × 10 meses = 271 euros (pago extra por la transición a la protección completa).

Costo total de la licencia para el cliente – **1,889 euros**.

2. Si se requiere comprar adicionalmente Antispam para productos Dr.Web Mail Security Suite o Dr.Web Gateway Security Suite, se aplica un 40% de sobretasa sobre el monto pagado por la licencia de Antivirus o Antivirus+ proxy SMTP.

Ejemplo:

El cliente ha pagado 1300 euros por compra de una licencia de Antivirus para la protección de 90 usuarios de correo. En 2 meses ha decidido a comprar el Antispam adicionalmente.

1300 euros ÷ 12 meses × 0,4 × 10 meses = 433 euros (pago extra por compra adicional de Antispam).

Costo total de la licencia para el cliente – **1,733 euros.**

3. Si se necesita hacer compra adicional de proxy SMTP, se aplica un incremento de 20% sobre el costo de licencia para Antivirus o Antivirus + Antispam.

Cuadro general de sobretasas en la compra adicional cualitativa sin aumentar el número de objetos protegidos

Producto	Licencia vigente	Nueva licencia	Sobretasa
Dr.Web Desktop Security Suite	Antivirus	Protección completa	20%
	Antivirus	+Criptógrafo	
	Protección completa		
Dr.Web Mail Security Suite o Dr.Web Gateway Security Suite	Antivirus	+Antispam	40%
	Antivirus + Proxy SMTP		
	Antivirus	+Proxy SMTP	20%
	Antivirus + Antispam		

II. **Compra adicional cuantitativa (aumento del número de objetos protegidos)**

El costo de las licencias adicionales se calcula en base a la lista de precios vigente en escala de la cantidad total de objetos protegidos **sin ningún tipo de descuento**.

III. **Compra adicional de productos (ampliación del producto)**

El costo de las licencias adicionales se calcula en base a la lista de precios vigente sin descuento por cantidad.

Productos para empresas, para los cuales la compra adicional es imposible

- Producto en caja Dr.Web "Empresa pequeña".
- Kits «Dr.Web Universal» y Dr.Web para escuelas.

Para ampliar la licencia para estos productos, se aplica la transición a Dr.Web Enterprise Security Suite de acuerdo con las reglas de compra adicional con renovación.

Códigos de productos, kits, herramientas — conjuntos de software y hardware Dr.Web

Reglas de formación de códigos

1. El código siempre consiste de 5 grupos.
2. Cada grupo del código está separada del otro grupo con un guión.
3. El código de licencia para la categoría de "productos" se forma para cada producto comercial Dr.Web por separado (véase la sección "Línea de productos Dr.Web Security Suite").
4. Los códigos de conjuntos de software y hardware Dr.Web Office Shield consisten en dos códigos:
   - código de dispositivos de hardware
   - código de licencia.
5. Los códigos de los productos en caja, tarjetas scratch y media kits, así como los códigos de hardware Dr.Web Shield Oficina véase en la lista de precios, los códigos son fijos.
6. En el código de la licencia "compra adicional" se indican 2 plazos: el plazo total de la licencia adicional, dos puntos, el plazo restante de clave adjunta (vigente).
7. En el código de la licencia "compra adicional más renovación" se indican 2 plazos: el plazo total de la licencia adicional y licencia renovada, dos puntos, el plazo restante de clave adjunta (renovado).
8. En el código de la licencia "compra adicional" se indican 2 cantidades de objetos protegidos: cantidad total de las licencias teniendo en cuenta compra adicional, dos puntos, la cantidad de objetos con la licencia vigente (adjunta).
9. En el código de la licencia "compra adicional más renovación" se indican 2 cantidades de objetos protegidos: cantidad total de las licencias teniendo en cuenta compra adicional y renovación, dos puntos, la cantidad de objetos con la licencia vigente (adjunta).

Tabla general de símbolos de códigos

Grupo 1			Grupo 2		Grupo 3	Grupo 4	Grupo 5	
Contenido del paquete	Categoría de producto	Objetos protegidos	Licencia básica	Componentes adicionales	Plazo de licencia	Número de objetos protegidos	Tipo de licencia	Exención
L – un ejemplar del programa (producto) bajado de la página web	**B** – producto para negocio **H** – productos para el	**G** – usuarios de puertas de enlace	**A** – Antivirus	**A** – Antispam	**XXM** – donde XX es el número de meses	Cualquier número	**A** – nueva licencia	**1** – establecimientos educativos, centro de salud, biblioteca, museo
B – un ejemplar del programa en caja de cartón	**X** – un ejemplar del programa que se suministra junto con Dr.Web Office Shield	**M** – dispositivos móviles	**B** – Protección completa	**C** – Centro de control	**XXXD** – donde XXX es el número de días	**UL** – ilimitado (para licencia ilimitada)	**B** – renovación	**2** – promoción
A – ejemplar del programa en paquete promocional							**C** – compra adicional	**3** – no hay exención
C – tarjeta con barra de rasca	**Y** – herramienta	**P** – usuarios de correo electrónico	**K** – Katana	**K** – no hay componentes adicionales			**D** – renovación con compra adicional	**4** – migración
D – ejemplar del programa en la unidad de DVD	**Z** – Kit	**S** – servidores	* – licencias para varios productos (sólo para kits)	**R** – Criptógrafo			**R** – Rescue Pack	**5** – Licencia NFR para partners
K – ejemplar de programa en el paquete de licencia		**W** – estaciones de trabajo		**S** – Proxy SMTP			**F** – licencia OEM	**6** – Licencia NFR (demo) para cliente
M – ejemplar del programa en el disco corporativo (incluyendo OEM)		**Z** – todos los objetos					**G** – licencia de servicio	**7** – necesidades de marketing/enseñanza
N – ejemplar de programa en media kit certificado							**H** – sin soporte técnico	**8** – caridad
P – ejemplar de programa en media kit para licencias OEM							**V** – cliente importante	**9** – división de un número de serie
Q – ventas por SMS								**10** – unión de varios números de serie
								11 – reemplazo de número de serie

Ejemplos

Ejemplos de códigos de licencia para la categoría "Productos"

1	El cliente, la institución educativa, requiere la protección para 200 PCs con el Centro de Control, protección completa + Firewall, por 12 meses, licencia electrónica. Dr.Web se adquiere por primera vez.	LBW-BRC-12M-200-A1
2	El cliente, la institución educativa, tiene una licencia válida para proteger 200 PCs con el Centro de Control, la protección completa + Firewall, por 12 meses, la licencia electrónica que vence en seis meses. El cliente necesita comprar adicionalmente protección para 10 estaciones.	LBW-BRC-6M:6M-210:200-C1
3	El cliente – la institución educativa tiene una licencia del Ejemplo 2, la cual expira en 7 meses. Necesitaba comprar protección para 10 estaciones adicionales y al mismo tiempo, renovar su licencia por 2 años más.	LBW-BRC-31M:7M-210:200-D1

Ejemplos de códigos de licencia para la categoría "Kits"

1	El cliente requiere un kit Dr.Web «Universal», para 50 PC con el Centro de Control, Protección completa, por 12 meses, licencia electrónica.	LZZ-*CR-12M-50-A3
2	El cliente requiere un kit Dr.Web «Universal», para 50 PC con el Centro de Control, Protección completa, por 12 meses, licencia electrónica.	LZZ-*C-12M-50-A3
3	El cliente – la institución educativa (escuela) requiere protección para 100 PCs.	LZZ-*C-12M-100-A1

Ejemplos de códigos de licencia para la categoría "Utilidades"

1	El cliente necesita el tratamiento para 100 PC durante 10 días. PC no están conectados a la red corporativa.	LYW-AC-10D-100-A3
2	El cliente necesita el tratamiento para 10 PC durante 30 días. PC no están conectados a la red corporativa.	LYW-AK-30D-10-A3

Vídeo de capacitación: https://pa.drweb.com/marketing/video

Contactos

Rusia	**Doctor Web** 125124, Federación de Rusia, Moscú, 3-a calle Yamskogo Polya, ed. 2-12a Teléfono: + 7 (495) 789-45-87 (multicanal) Fax: +7 (495) 789-45-97 www.drweb.com | www.av-desk.com | www.freedrweb.com
Alemania	**Doctor Web Deutschland GmbH** Alemania, 63457 Hanau, Rodenbacher Chaussee 6 Tel.: +49 (6181) 9060-1210 Fax: +49 (6181) 9060-1212 www.drweb-av.de
Kazajistán	**Doctor Web — Asia Central** República de Kazajstán, 050009, Almaty, calle Shevchenko 165B, oficina 910 Tel.: +7 (727) 323-62-30, +7 (727) 323-62-31, +7 (727) 323-62-32 www.drweb.kz
Ucrania	**Centro de soporte técnico Doctor Web** 01601, Ucrania, Kiev, c/Pushkinskaya 27, planta 5, oficina 6 Tel./Fax: +38 (044) 238-24-35 www.drweb.ua
Francia	**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
Japón	**Doctor Web Pacific, inc.** NKF Kawasaki building 2F, 1−2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken 210-0005 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 www.drweb.com