Tiene algo que proteger?

Tenemos Dr.WEB®
desde 1992

Índice

Acerca de ... Doctor Web

La empresa Doctor Web es un elaborador ruso de software de seguridad informática. Los productos Antivirus Dr.Web se están elaborando desde el año 1992. Siempre han mostrado excelentes resultados en detección de aplicaciones malware de todo tipo y cumplen con las normas de seguridad internacionales. Nuestros numerosos clientes de todo el mundo son una clara evidencia de la máxima confianza depositada en nuestros productos.

Todos los productos de Dr.Web cuentan con su propia tecnología antivirus. Doctor Web es uno de los pocos proveedores de antivirus que posee sus propias tecnologías para la detección y desinfección de malware, servicio de control de virus y un laboratorio analítico. Esto asegura una respuesta rápida a las amenazas nuevas y permite resolver los problemas de cualquier complejidad en el menor tiempo posible.

El objetivo estratégico de Doctor Web es la creación de un software antivirus que siempre cumple con las necesidades actuales de seguridad informática. Otra de las principales prioridades de la empresa es el desarrollo de las nuevas tecnologías para que los usuarios puedan enfrentarse a todo tipo de amenazas informáticas. La línea de productos de Dr.Web ofrece los antivirus para la más amplia gama de sistemas operativos y aplicaciones compatibles.

Doctor Web distribuye sus productos a través de su red de partners en lugar de llevar a cabo las ventas directas. El tamaño relativamente pequeño de la empresa permite que se mantenga flexible y móvil en los negocios. La resolución de problemas y el beneficio mutuo son los principios básicos de la empresa. Doctor Web ofrece a sus partners muchos incentivos. Todas las empresas que venden los productos de Dr.Web tienen derecho a soporte técnico y de marketing. Doctor Web también ofrece programas de formación para los usuarios finales y partners que quieran utilizar el software de Dr.Web.

Amplia gama de clientes de Doctor Web incluye los usuarios domésticos de muchos países, las principales empresas rusas, las empresas pequeñas, y las organizaciones superiores. Doctor Web les agradece a todos sus clientes su lealtad y apoyo durante años.

Tecnologías de Dr.Web

Los antivirus de Dr.Web se estan elaborando por los hábiles programadores rusos dirigidos por Igor Danilov — el autor de Dr.Web y el propietario de Doctor Web.

Los productos antivirus de Dr.Web, basados en la exclusiva tecnología de detección y desinfección, han sido desarrollados por nuestra empresa para darle una ventaja competitiva, algo, que pueden ofrecer muy pocos fabricantes de antivirus. Doctor Web tiene su propio servicio de control de virus y un laboratorio analítico, que garantiza una respuesta rápìda a las nuevas amenazas de virus. La empresa también ofrece soluciones de antivirus y antispam fiables para negocios, entidades del gobierno y para el uso personal.

Tecnologias

Una buena aplicación antivirus puede detectar los virus. Eliminar un archivo infectado que puede contener información importante es una cosa, pero restaurar el archivo a su estado original "sano" es totalmente otra. Dr.Web trata los archivos de usuario con gran cuidado.

Desinfección de los virus

- La función de instalar Dr.Web en un equipo infectado y su resistencia excepcional contra los virus, lo distinguen entre todas las aplicaciones similares.
- Dr.Web tiene la mayor tasa de éxito en la industria para neutralizar las infecciones activas.
- No es necesario desinfectar el sistema antes de instalar Dr.Web; Es debido a la tecnología única del análisis de procesos de memoria y su capacidad extraordinaria de neutralizar las infecciones activas.
- Alta probabilidad de iniciar un proceso del análisis en el sistema infectado incluso desde un dispositivo de almacenamiento de datos remoto sin necesidad de instalación (por ejemplo, desde una unidad flash USB).
- **Dr.Web Process Heuristic** protege contra los nuevos programas malintencionados más actuales desarrollados para no ser detectados por los mecanismos tradicionales de firmas y heurísticos que todavía no han llegado al laboratorio antivirus para el análisis y, por lo tanto, son desconocidos para la base de virus Dr.Web en el momento de penetrar en el sistema. Analiza el comportamiento del programa peligroso y saca conclusiones si el mismo es malintencionado, luego se toman las medidas necesarias para neutralizar la amenaza. La nueva tecnología para proteger los datos contra el daño permite reducir al mínimo las pérdidas por causa de las acciones de un virus desconocido.
- **El analizador integral de amenazas empaquetadas** aumenta significativamente el nivel de detección de las supuestas "nuevas amenazas" — conocidas para la base de virus Dr.Web, pero ocultas por los nuevos empaquetadores, y, asimismo, permite evitar la necesidad de añadir las nuevas entradas de amenazas a las bases. La posibilidad de mantener las bases de virus Dr.Web compactas, a su vez, no requiere el aumento continuo de requerimientos al sistema y asegura el tamaño tradicionalmente pequeño de actualizaciones, y al mismo tiempo la calidad de detección y desinfección sigue siendo la misma.

Autodefensa

Dr.Web es inmune a los intentos de aplicaciones malware de interrumpir su funcionamiento. Dr.Web SelfPROtect es el único componente antivirus que mantiene la seguridad de los antivirus.

- Dr.Web SelfPROtect se implementa como un controlador que opera en el nivel más bajo del sistema. El controlador no puede ser detenido sin reiniciar el sistema. No hay forma de que una aplicación malware pueda interrumpir el funcionamiento del módulo de autodefensa.

- Dr.Web SelfPROtect restringe el acceso a la red, los archivos y carpetas, algunas ramas del registro de Windows y dispositivos de almacenamiento de datos extraíbles en el nivel de controlador del sistema y protege el software de los anti-antivirus, que intentan interrumpir el funcionamiento de Dr.Web.
- Algunos antivirus modifican el kernel de Windows mediante interceptación de interrupciones y el cambio de las tablas de vectores o mediante otras funciones indocumentadas. Esto puede ocasionar efectos negativos en la estabilidad del sistema y preparar nuevas formas para las aplicaciones malware de penetrarse en el sistema. Al mismo tiempo, Dr.Web SelfPROtect mantiene la seguridad del antivirus y no interfiere con las rutinas del kernel de Windows.

Las características únicas del motor

- Analiza los archivos comprimidos de cualquier nivel de anidación.
- Detecta de forma fiable los objetos empaquetados sin importar si Dr.Web reconoce o no el formato de compresión y realiza su análisis detallado dirigido a exponer las amenazas ocultas.
- Un líder en la detección y neutralización de rootkits complejos (Shadow.based (Confi□ker), MaosBoot, Rustock.C, Sector).
- Un análisis de memoria inteligente permite bloquear los virus en la RAM antes de que se repliquen en el disco duro, por lo que es menos probable que el malware pueda aprovechar la vulnerabilidad de una aplicación de terceros o el sistema operativo.
- Dr.Web puede detectar y neutralizar los virus que se pueden encontrar únicamente en la memoria RAM y no existen como archivos en los discos, por ejemplo, Slammer o CodeRed.

Detección de amenazas desconocidas

- FLY-CODE es una tecnología de descompresión única y universal que permite a Dr.Web desempaquetar los datos que han sido comprimidos con empaquetadores desconocidos.
- La innovadora tecnología del análisis sin utilizar las firmas de virus de Origins Tracing™ garantiza la alta probabilidad de detección de los virus desconocidos por Dr.Web.
- El analizador heurístico, cuyos análisis se basan en los criterios típicos para diversos grupos de aplicaciones malware, detecta las amenazas más conocidas.
- Dr.Web Process Heuristic

  protege contra los nuevos programas malintencionados más actuales desarrollados para no ser detectados por los mecanismos tradicionales de firmas y heurísticos que todavía no han llegado al laboratorio antivirus para el análisis y, por lo tanto, son desconocidos para la base de virus Dr.Web en el momento de penetrar en el sistema. Analiza el comportamiento del programa peligroso y saca conclusiones si el mismo es malintencionado, luego se toman las medidas necesarias para neutralizar la amenaza. La nueva tecnología para proteger los datos contra el daño permite reducir al mínimo las pérdidas por causa de las acciones de un virus desconocido.
- El analizador integral de amenazas empaquetadas

  aumenta significativamente el nivel de detección de las supuestas "nuevas amenazas" — conocidas para la base de virus Dr.Web, pero ocultas por los nuevos empaquetadores, y, asimismo, permite evitar la necesidad de añadir las nuevas entradas de amenazas a las bases. La posibilidad de mantener las bases de virus Dr.Web compactas, a su vez, no requiere el aumento continuo de requerimientos al sistema y asegura el tamaño tradicionalmente pequeño de actualizaciones, y al mismo tiempo la calidad de detección y desinfección sigue siendo la misma.

Tecnología de filtración de spam

El antispam de Dr.Web analiza los mensajes de correo electrónico utilizando miles de reglas que se pueden dividir en varios grupos.

- Análisis heurístico

  Una tecnología inteligente que analiza empíricamente todas las partes del mensaje: encabezado, cuerpo y archivos adjuntos. Permite detectar los tipos de spam desconocidos. El analizador heurístico se está mejorando constantemente; las reglas nuevas de añaden con frecuencia. Permite detectar los mensajes de spam de nueva generación, incluso antes de que se crea una regla correspondiente.
- Filtrado de técnicas de evasión

  La filtración de técnicas de evasión es una de las tecnologías más avanzadas y eficientes de Antispam de Dr.Web. Esto ayuda a reconocer las técnicas y trucos utilizados por los spammers para evitar la detección.
- Firmas de HTML

  Los mensajes que contienen el código HTML se comparan con las firmas de HTML de la biblioteca de antispam. Tal comparación en combinación con los datos sobre el tamaño de las imágenes que normalmente utilizan los spammers ayuda a proteger a los usuarios contra los mensajes de spam en el código de HTML, que a menudo contiene imágenes online.
- Detección basada en el remitente SMTP

  La detección del falso remitente y el receptor en SMTP y valores falsos de los campos de cabecera es la última tendencia en el desarrollo de tecnologías antispam. La dirección del remitente que figura en un mensaje recibido es fácil de falsificar y por lo tanto no se debe ser considerada como fiable. Sin embargo, el correo electrónico no deseado no está limitado por el spam. También incluye bromas o amenazas anónimas. La tecnología antispam de Dr.Web permite determinar si una dirección es falsa y marcar el mensaje como no deseado. Reduce el tráfico y protege a los empleados del contenido de correo electrónico no deseado que puede tener un impacto impredecible sobre el comportamiento de las personas.
- Análisis semántico

  Las palabras y frases de un mensaje se comparan con las palabras y frases del diccionario de spam.

  Las palabras, frases y símbolos se analizan - tanto si son visibles para el ojo humano o ocultos por los trucos de los spammers.

- Tecnoligía antispam

  Las estafas (así como los mensajes de pharming - un tipo de las estafas) son el tipo más peligroso de spam. El ejemplo más notorio de una estafa es lo que se llama "estafas nigerianas", estafas de lotería, préstamos y otras estafas en casinos y mensajes falsos de bancos y entidades de crédito. Un módulo especial de antispam de Dr.Web se utiliza para filtrar las estafas.

Actualización de la base de firmas de virus y sistema de actualización global

Organización Especial

Los productos de Dr.Web tienen la base de firmas de virus más pequeña entre los antivirus existentes. Esto se proporciona gracias a una tecnología propia de creación de bases de firmas de virus a base de un idioma flexible, desarrollado especialmente para la descripción de las bases.

La base de datos compacta asegura una interacción rápida entre los componentes del antivirus y la baja carga de la CPU.

¿Qué es lo más importante en un antivirus? Seguramente debe proporcionar una protección contra los virus. La adición de firmas de virus a la base de datos es esencial para el proceso. Sin embargo, no existe ninguna correlación entre el número de entradas en la base de datos y la tasa de detección. Para entender por qué hay menos entradas en la base de firmas de virus de Dr.Web® que en las de su competencia, hay que recordar que muchos virus no son únicos. Hay familias enteras compuestas por variaciones de un único virus, y hay virus creados mediante una herramienta de construcción de virus. Algunos fabricantes de antivirus crean una entrada para cada firma de virus en la base de datos que aumenta su volumen. Un enfoque diferente se utiliza para la base de firmas de virus de Dr.Web, donde una sola entrada es capaz de detectar docenas o incluso cientos de virus similares.

Ventajas de la base de firmas de virus de Dr.Web

- Número de entradas de registro y tamaño de actualizaciones muy reducido.
- Una entrada en la base de firmas de virus de Dr.Web proporciona detección de cientos o incluso miles de virus similares
- La principal diferencia entre la base de firmas de virus de Dr.Web y las bases de datos de otros antivirus es que con el menor número de entradas permite la detección del mismo (o mayor) número de virus.

Base de datos pequeña con menor número de entradas

- Bajo consumo del espacio en el disco duro.
- Bajo consumo de memoria.
- Disminución del tráfico al descargar actualizaciones.
- Análisis de virus más rápido.
- Detección de futuras modificaciones de los virus conocidos.

Servicio de control de virus

- El servicio de control de virus de Dr.Web recoge las muestras de aplicaciones malware de Internet para crear los antídotos y lanzar actualizaciones tan pronto como el análisis este completo - varias veces por hora.
- Tan pronto como se lance una actualización, los usuarios pueden descargarla a través de los servidores ubicados en numerosos puntos del mundo.
- Para evitar falsos positivos, antes de lanzar la actualización, se comprueba en un gran número de archivos infectados.
- El sistema inteligente añade las entradas de virus similares a las bases de datos automáticamente, lo que garantiza la neutralización inmediata de las amenazas emergentes.

Siempre actualizado

- La actualización a través de Internet, automática o programada por el usuario, no requiere interferencia del usuario. También se puede iniciar la actualización de forma manual.
- Las actualizaciones son muy pequeñas — 50-200 KB y se necesita muy poco tiempo para descargarlas, incluso con una conexión a Internet lenta.
- Los servidores de actualizaciones siempre están disponibles.
- En la mayoría de los casos, no es necesario reiniciar el sistema para completar la actualización; Dr.Web empieza a utilizar los módulos actualizados y últimas definiciones de virus inmediatamente.
- Para ahorrar el tráfico, se puede configurar el antivirus para actualizar únicamente las bases de firmas de virus. Sin embargo, no se recomienda habilitar esta opción. Para contrarrestar las amenazas más recientes, Dr.Web se está mejorando constantemente. Las nuevas características han sido incorporadas en los módulos actualizados del paquete de antivirus y se descargan desde el servidor de Doctor Web de forma automática. Para proteger un sistema de nuevo malware, todos los componentes de un antivirus deben permanecer actualizados.
- También puede reducir el tráfico descargando actualizaciones como ficheros de parche archivados. Los ficheros de parche se utilizan para incorporar adiciones minores y soluciones para la base de firmas de virus o módulos de programa. El algoritmo de compresión especial aplicado a estos parches reduce radicalmente la cantidad de datos transferidos.

Dr.Web Enterprise Security Suite

Productos para negocio

Dr.Web Enterprise Security Suite. Productos para negocio

Dr.Web Enterprise Security Suite consiste de 5 productos de Dr.Web diseñados para proteger todos los hosts de una red corporativa y un centro de control único que facilita la administración de muchos de los productos.

Producto comercial	Producto de software
Dr.Web Desktop Security Suite Protección de estaciones de trabajo, clientes de servidores terminales, clientes de servidores virtuales, clientes de sistemas integrados	Dr.Web para Windows
	Dr.Web KATANA
	Dr.Web para Linux
	Dr.Web para macOS
	Dr.Web para MS DOS
	Dr.Web para OS/2
Dr.Web Server Security Suite Protección de almacenes de archivos y servidores de aplicaciones (Incluyendo servidores terminales y virtuales)	Dr.Web para servidores de Windows
	Dr.Web para servidores de UNIX
	Dr.Web para Novell NetWare Server
	Dr.Web para servidores de macOS
Dr.Web Mail Security Suite Protección de correo electrónico	Dr.Web para servidores de correo electrónico de UNIX
	Dr.Web para MS Exchange
	Dr.Web para IBM Lotus Domino para Windows
	Dr.Web para IBM Lotus Domino para Linux
	Dr.Web para Kerio Mail Server (para Windows)
	Dr.Web para Kerio Mail Server (para Linux)
	Dr.Web para Kerio Mail Server (para macOS)
Dr.Web Gateway Security Suite Protección para escuelas	Dr.Web para gateways de Internet de UNIX
	Dr.Web para gateways de Internet de Kerio
	Dr.Web para Microsoft ISA Server y Forefront TMG
	Dr.Web para MIMEsweeper
	Dr.Web para Qbik WinGate
Dr.Web Mobile Security Suite Protección para dispositivos móviles	Dr.Web para Android
	Dr.Web para BlackBerry

Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite consiste de un conjunto de productos Dr.Web diseñados para proteger todos los hosts de una red corporativa y un centro de control único que facilita la administración de muchos de los productos.

Licencias

Los productos poseen licencia según el tipo de objetos que necesitan protección. Sólo tiene que seleccionar cualquier licencia básica que necesita, así como los componentes adicionales que desee. Por ejemplo, el antivirus y la protección completa son licencias básicas para estaciones de trabajo, mientras que el firewall es un componente adicional.

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 10/8/8.1/7/Vista SP2/XP SP2+ (32 bits). ▪ Windows 10/8/8.1/7/Vista SP2 (64 bits).	Protección completa	▪ Centro de Control
		Antivirus	
	▪ Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 bits). ▪ Windows 10/8/8.1/7/Vista SP2 (64 bits).	KATANA	
	Linux glibc 2.7 y superior	Antivirus	
	macOS 10.7 y superior		
	MS-DOS OS/2		–
Dr.Web Server Security Suite Servidores de archivos Servidores de aplicaciones Servidores terminales Servidores virtuales	Windows Novell NetWare macOS 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 Microsoft ISA Server y Forefront TMG MIMEsweeper Qbik WinGate	Antivirus	▪ Centro de Control ▪ Antispam
Dr.Web Mobile Security Suite Dispositivo móvil	Android OS 4.0—7.1, Android TV 5.0+	Protección completa	▪ Centro de Control
	BlackBerry 10.3.2+		

Flexibilidad

Como nuestro cliente, recibirá un archivo clave único que le permitirá utilizar el producto de Dr.Web para proteger cualquier objeto que necesite para una plataforma deseada. Por ejemplo, un archivo clave le permitirá elegir entre la protección antivirus para un servidor de archivos de UNIX y un servidor de archivos de Windows. Si usted cambia su plataforma de UNIX a Windows, mientras que su licencia es válida, no es necesario que obtenga un archivo clave nuevo En cambio, podrá dirigirse a www.drweb.com para descargar e instalar de forma gratuita un archivo de distribución del programa que desee.

Enlaces de interés

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

Centro de Control

Administración centralizada de todos los hosts de la red corporativa

El Centro de Control de Dr.Web Enterprise Security Suite proporciona una administración centralizada de seguridad para todos los hosts de la red corporativa:

- estaciones de trabajo, servidores terminales, servidores virtuales, clientes de sistemas integrados;
- servidores de archivos y servidores de aplicaciones (incluyendo servidores terminales y virtuales)
- servidores de correo electrónico, gateways, dispositivos móviles.

Ventajas

- Posibilidad de protección centralizada de todos los nodos, dispositivos y servicios de red;
- coste total mínimo comparado con los programas de competencia gracias a la posibilidad de implementar la red usando los servidores Windows y Unix, instalación fácil y protección segura;
- posibilidad de instalación en versiones de 32- y 64-bits de sistemas operativos;
- posibilidad de instalar la parte agente en un equipo ya infectado y alta probabilidad de desinfección;
- uso mínimo de recursos de equipos y de servidores gracias al tamaño reducido del núcleo antivirus y uso de las nuevas tecnologías en el mismo;
- administración remota por medio de la interfaz basada en la Web a través de cualquier explorador web;
- centro de control móvil para los dispositivos Android/ iOS;
- posibilidad de realizar las directivas de seguridad necesarias para una empresa en concreto y grupos de empleados separados;
- posibilidad de asignar varios administradores para varios grupos, lo que permite usar el Centro de Control tanto en empresas con altos requisitos de seguridad como en empresas multifilial;
- posibilidad de configurar las directivas de seguridad para cualquier tipo de usuarios, entre ellos, los móviles, y para cualquier estación – incluso las que no están en la red en el momento – permite asegurar la protección actual en cualquier momento;
- protección contra el cambio de configuración por los usuarios mismos;
- bloqueo de acceso para dispositivos extraíbles, recursos de la red local y la red Internet - protección contra las acciones accidentales o realizadas a propósito por los usuarios;
- posibilidad de proteger las redes que no tienen acceso a Internet;

- posibilidad de implementar los agentes en las estaciones de trabajo de forma conveniente para el administrador – a través de directivas Active Directory, scripts de inicio, mecanismos de instalación remota. Es posible instalar incluso si el nodo de la red es privado y no está disponible a través del administrador web del Centro de Control;
- posibilidad de usar la mayoría de las bases de datos existentes. Asimismo, como bases de datos externas pueden servir Oracle, PostgreSQL, Microsoft SQL Server o cualquier sistema de administración de bases de datos con soporte de SQL-92 a través de ODBC;
- posibilidad de crear sin ayuda los procesadores de eventos lo que ofrece el acceso directo a las interfaces internas del Centro de Control;
- solución abierta – usando este conjunto, el administrador de sistemas puede instalar y sincronizar los productos adicionales de terceros productores, lo que permite reducir los gastos de creación de los sistemas de seguridad de información;
- claridad del sistema de control del estado de protección, búsqueda de estaciones de red muy eficaz y cómoda;
- posibilidades de seleccionar un listado de componentes de productos actualizados y control de posibilidades de pasar a las nuevas versiones permiten a los administradores instalar solo las actualizaciones necesarias y comprobadas en su red.

Dr.Web Desktop Security Suite

Protección de estaciones de trabajo, clientes de servidores terminales, clientes de servidores virtuales, clientes de sistemas integrados

- Dr.Web para Windows
- Dr.Web KATANA
- Dr.Web para Linux
- Dr.Web para macOS
- Dr.Web para MS DOS, OS/2

Licencias de Dr.Web Desktop Security Suite

Tipos de licencia

- Según el número de estaciones de trabajo protegidas.
- Según el número de clientes conectados al servidor terminal.
- Según el número de clientes conectados al servidor virtual.
- Según el número de clientes que utilizan sistemas integrados.

Dr.Web Antivirus para Windows está disponible por separado o como componente de Dr.Web Enterprise Security Suite.

Variedades de licencia

	Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 bits). Windows 10/8/8.1/7/Vista SP2 (64 bits).		Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 bits). Windows 10/8/8.1/7/Vista SP2 (64 bits).	Linux	macOS	MS DOS, OS/2
Licencia básica	Antivirus	Antivirus	KATANA			
Componentes de protección de licencia básica	▪ Protección completa ▪ Antivirus ▪ Antiespía ▪ Antirootkit ▪ Antispam ▪ Antivirus web ▪ Control de oficina ▪ Firewall	▪ Antivirus ▪ Antiespía ▪ Antiroot-kit ▪ Firewall	▪ Un antivirus no basado en firmas ▪ Dr.Web Cloud ▪ Centro de control	▪ Antivi-rus ▪ An-tiespía	▪ Antivirus ▪ Antiespía ▪ Antiroot-kit	▪ Antivirus ▪ Antiespía ▪ Antiroot-kit
Componentes adicionales:						
Centro de control	+	+	+*	+	+	–

* Dr.Web KATANA BE.

Dr.Web Desktop Security Suite también está incluido en los kits económicos para empresas pequeñas y medianas.

Compatible con sistemas operativos

Dr.Web para Windows	Dr.Web para Linux	Dr.Web para macOS	Escáneres de consola Dr.Web
Antivirus, Protección completa Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 bits). Windows 10/8/8.1/7/Vista SP2 (64 bits). **KATANA** Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 bits). Windows 10/8/8.1/7/Vista SP2 (64 bits).	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)	macOS 10.7 y superior	Windows, MS DOS, OS/2

Dr.Web para Windows

Protección de estaciones de trabajo, clientes de sistemas integrados, clientes de servidores terminales y clientes de servidores virtuales

Ventajas

- **Protección completa contra amenazas actuales**

  Dr.Web para Windows ofrece una protección segura contra la mayoría de las amenazas existentes. Su insuperable calidad de desinfección y autoprotección fiable no dejan resquicio para los virus y otro malware

  para meterse en el entorno protegido. El Firewall y el Control de Oficina integrado ayudan a evitar que los virus aprovechen las vulnerabilidades de los sistemas operativos y aplicaciones y permite controlar el funcionamiento de los programas instalados.

- **Aumento de la productividad laboral**

  El despliegue de Dr.Web para Windows proporciona un efecto positivo inmediato. Debido a que el producto ofrece una protección completa, la entrada de spam está totalmente bloqueada, lo que proporciona un entorno de trabajo más productivo - los mensajes importantes no se pierden entre volúmenes elevados de mensajes de spam. Además, los equipos

  de red ya no están en riesgo de ser infectados, lo que elimina el tiempo de inactividad debido a ataques de virus y posteriores procesos necesarios para la restauración del sistema.

- **Defendiendo la reputación**

  Con Dr.Web para Windows de guardia, los delincuentes no pueden convertir sus estaciones de trabajo, clientes de sistemas integrados y clientes de servidores terminales en fuentes de virus y spam que podría llegar a los equipos de sus clientes. Dr.Web para Windows le ayuda a proteger su reputación como un socio digno de confianza.

- **Licencias flexibles**

  A diferencia de muchas soluciones de la competencia, Dr.Web para Windows goza de una licencia multiopcional más flexible (véase la ficha Licencias). Doctor Web permite a los clientes adquirir únicamente los componentes que necesitan, los clientes no están obligados a pagar las funciones que nunca van a utilizar.

- **Administración centralizada**

  El Centro de Control, que permite que la protección de la estación de trabajo pueda administrarse de forma centralizada. está incluido en la licencia de Dr.Web Enterprise Security Suite. El Centro de Control es igual de fiable en redes de cualquier escala y complejidad estructural - desde pequeños grupos de trabajo hasta intranets distribuidas con decenas de miles de hosts. El centro de Control también ofrece administración centralizada de los antivirus para servidores de archivos y aplicaciones, incluyendo servidores terminales con Windows y Novell NetWare, UNIX para servidores de correo electrónico, Microsoft Exchange, IBM Lotus, Kerio, y también para Dr.Web para dispositivos móviles con Windows Mobile.

Funciones clave

- Solución integral para la protección de PC bajo la administración de Windows.
- Protección en modo en línea.
- Posibilidad de instalar y trabajar en un equipo ya infectado y resistencia excepcional a los virus.
- Detección eficaz y limpieza del sistema de todos l os tipos de amenazas.
- Alta velocidad de escaneo gracias al uso de posibilidades de sistemas multiprocesador.
- Protección contra los programas malintencionados más actuales desarrollados para no ser detectados por los mecanismos tradicionales de firmas y heurísticos.
- Protección de datos contra daños de un troyano-cifrador.
- Analizador integral de amenazas comprimidas.
- Escaneo completo de archivos de cualquier nivel de anidamiento.
- Mejor detección y neutralización de los virus complejos.
- Filtrado de spam y todos los tipos de mensajes no deseados sin necesidad de formación para antispam.
- Análisis completo "al vuelo" de todo el tráfico en todos los puertos.
- Navegación segura en Internet en los sistemas de búsqueda Google, Yandex, Yahoo!, Bing, Rambler gracias a la activación en los buscadores de la funcionalidad «Búsqueda segura» — ¡el contenido no seguro se bloquea por los buscadores mismos!
- Comunicación segura - filtrado del tráfico en mensajes instantáneos.
- Protección eficaz a los niños contra el contenido no deseado.
- Bloqueo de posibilidad de uso no autorizado de dispositivos extraíbles y del equipo.
- Servicio en la Nube Dr.Web Cloud — escanéo de URL en los servidores de la empresa Doctor Web.
- Protección contra el acceso no sancionado desde fuera, prevención de la filtración de los datos importantes, bloqueo de conexiones sospechosas a nivel de paquetes y aplicaciones.
- Control remoto de Dr.Web en otros equipos dentro de la red misma local sin necesidad de instalar el Centro de Control de Dr.Web.

Requerimientos al 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).

Enlaces de interés

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

Antivirus Dr.Web para macOS

Protección básica contra los virus y otro malware dirigido a macOS y otros sistemas operativos

Ventajas

- Protección segura contra todos los programas malintencionados.
- Alta velocidad de escaneo antivirus gracias a la tecnología de escaneo asíncrono
- Centro de Control cómodo que se licencia de forma gratuita.
- Conexión fácil al sistema centralizado de protección antivirus de la empresa.
- Carga mínima del sistema protegido y pocos gastos del tráfico al actualizar, lo que hace el funcionamiento del Antivirus Dr.Web para macOS casi invisible.
- Interfaz de control intuitiva.

Posibilidades

- Posibilidad de administración centralizada de configuración de todos los componentes.
- Control contínuo de todos los objetos que pueden ser infectados - dispositivos de información extraíbles, formatos, catálogos y archivos de correo, entre ellos, los empaquetados y archivados.
- Protección de amenazas desconocidas usando la tecnología de búsqueda sin usar firmas Origins Tracing™ y analizador inteligente heurístico Dr.Web.
- Detección y eliminación de programas malintencionados ocultos bajo los empaquetadores desconocidos, usando la tecnología FLY-CODE™.
- Desinfección de virus, programas troyanos y otros tipos de objetos malintencionados.
- Amplias bases de datos para detectar spyware, software potencialmente peligroso, adware, hacktools y programas bromas.
- Alta resistencia a intentos de impedir el funcionamiento de SpIDer Guard o detener su funcionamiento por los programas malintencionados.
- Protección de la configuración del monitor SpIDer Guard® con una contraseña contra los cambios no sancionados.
- Escaneo antivirus manual, automático o según la programación creada anteriormente.
- Seleccionar el tipo de escaneo: rápido, completo y selectivo.
- Aplicación de acciones para objetos infectados, sospechosos y objetos de otro tipo, asimismo, la desinfección, transferencia a cuarentena y eliminación, asimismo, si la acción previamente seleccionada resultó ser imposible.
- Excluir las rutas y los archivos del escaneo por solicitud del usuario.
- Aislamiento de archivos infectados en cuarentena con posibilidad de establecer el periodo de almacenamiento de objetos en la cuarentena y el tamaño máximo de la misma.
- Desinfección, recuperación o eliminación de objetos movidos a cuarentena.
- Registro de la hora del evento, objeto de escaneo y tipo de acción para el mismo.
- Descarga automática de actualizaciones (según la programación) o por demanda.
- Notificación automática (asimismo, usando las notificaciones sonoras) sobre eventos de virus.
- Posibilidad de llevar un informe detallado sobre el trabajo.
- Accesibilidad de módulos como utilidades de la línea de comandos, con posibilidad de incorporarlas en Apple Scripts usados para el servicio del sistema.

Requerimientos al sistema

- macOS 10.7 o superior (32&64 bits).
- Intel.
- Memoria operativa — según los requisitos del SO.
- Acceso a Internet para registro y actualización.

Enlaces de interés

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

Antivirus Dr.Web para Linux

Protección antivirus básica

Ventajas

- Centro de Control fácil de manejar.
- Protección en tiempo real. Análisis personalizado.
- Cuarentena manejable.
- Administrador de licencias facil de usar.
- Control desde la línea de comandos.
- Interfaz elegante.
- Escaneo completo del tráfico HTTP y control de acceso a recursos de Internet.
- Protección contra amenazas para SO Microsoft Windows iniciados bajo el SO Linux.

Posibilidades

- Posibilidad de administración centralizada de configuración de todos los componentes.
- Control continuo de todos los objetos que pueden ser infectados - dispositivos de información extraíbles, formatos, catálogos y archivos de correo, entre ellos, los empaquetados y archivados.
- Protección de amenazas desconocidas usando la tecnología de búsqueda sin usar firmas Origins Tracing™ y el analizador inteligente heurístico Dr.Web.
- Detección y eliminación de programas malintencionados ocultos bajo los empaquetadores desconocidos, usando la tecnología FLY-CODE™.
- Desinfección de virus, programas troyanos y otros tipos de objetos malintencionados.
- Amplias bases de datos para detectar spyware, software potencialmente peligroso, adware, hacktools y programas bromas.
- Arquitectura de la solución desarrollada para reducir la carga del CPU y el consumo de la memoria.
- **¡Novedad!** Posibilidad de instalar, configurar el antivirus y de funcionamiento del mismo sin usar la interfaz gráfica.
- Alta resistencia a intentos de impedir el funcionamiento de SpIDer Guard o detener su funcionamiento por los programas malintencionados.
- **¡Novedad!** Escaneo multiflujo que permite aumentar significativamente la velocidad del trabajo en procesadores multinúcleo.
- Escaneo antivirus con posibilidad de seleccionar el tipo del mismo: rápido, completo o personalizado - manual, automático o según la programación previamente establecida.
- **¡Novedad!** Análisis de procesos para la neutralización de las amenazas activadas, incluidas las amenazas de Windows que se ejecutan a través de Wine.
- Aplicación de acciones para objetos infectados, sospechosos y objetos de otro tipo, entre ellas, la desinfección, transferencia a cuarentena y eliminación, asimismo, si la acción previamente seleccionada resultó ser imposible.
- Exclusión de las rutas y los archivos del escaneo por solicitud del usuario.
- **¡Novedad!** Escaneo completo del tráfico HTTP y control de acceso a recursos de Internet.
- Aislamiento de archivos infectados en cuarentena con posibilidad de establecer el periodo de almacenamiento de objetos en la cuarentena y el tamaño máximo de la misma.
- Desinfección, recuperación o eliminación de objetos movidos a cuarentena.
- Registro de la hora del evento, objeto de escaneo y tipo de acción para el mismo.
- Descarga automática de actualizaciones (según la programación) o por demanda.
- **¡Novedad!** Aplicación del cambio de la configuración del antivirus y de la clave de licencia "al vuelo".
- Notificación automática (asimismo, usando las notificaciones sonoras) sobre eventos de virus.
- Disponibilidad de los módulos del producto como utilidades de la línea de comandos, con posibilidad de uso autónomo de los mismos.

Además:

- Posibilidad de usar en empresas que requieren un nivel alto de seguridad.

Requerimientos al sistema

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

Enlaces de interés

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

Dr.Web Escáneres de consola

Protección antivirus para los usuarios avanzados

Los escáneres de consola de Dr.Web incorporan una base de firmas de virus estándar y el escáner de Dr.Web. Se pueden utilizar con MS DOS, OS/2, y Windows. Para hacer uso de todas las funciones del escáner de la consola, necesita saber cómo utilizar la línea de comandos.

Ventajas

- Requisitos mínimos del sistema - los escáneres funcionan perfectamente incluso en sistemas integrados y proporcionan una protección fiable en equipos de bajo nivel.
- Modos del análisis - los administradores pueden elegir entre el análisis manual y programado.
- Es posible desinfectar las estaciones de trabajo y servidores de Windows, incluso si no están disponibles a través de la red.
- Alta resistencia a los virus; puede ser instalado en sistemas infectados.
- La automatización de las rutinas diarias por medio de un gran número de opciones que se pueden definir utilizando la línea de comandos.
- Eliminación garantizada de los virus desconocidos incluyendo malware en archivos de formatos desconocidos.
- Ejecutable desde una unidad extraíble (por ejemplo, CD o USB).

Enlaces de interés

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

Dr.Web Server Security Suite

Protección de almacenes de archivos y servidores de aplicaciones, incluyendo servidores terminales y servidores virtuales

- Dr.Web para Windows Server
- Dr.Web para Novell NetWare Server
- Dr.Web para macOS Server
- Dr.Web para UNIX Server

icencias de Dr.Web Server Security Suite

Tipos de licencia

- Según el número de servidores protegidos.

Opciones de licencia

- Antivirus.
- Antivirus + Centro de control (excepto Dr.Web para UNIX Server).

Puede adquirir el producto de Dr.Web Server Security Suite como un producto separado o como componente de Dr.Web Enterprise Security Suite.

	Dr.Web para Windows Servers	Dr.Web para Novell NetWare Servers	Dr.Web para macOS Server	Dr.Web para UNIX Servers
Licencia básica	Antivirus	Antivirus	Antivirus	Antivirus
Componentes adicionales				
Centro de control	+	+	+	+

Dr.Web Server Security Suite también está incluido en los kits económicos para empresas pequeñas y medianas.

Sistemas operativos compatibles

Dr.Web para servidores Windows	Dr.Web para servidores Novell NetWare	Dr.Web para macOS Server	Dr.Web para servidores UNIX
Microsoft Windows Server 2000/2003 (x32, x64)/2008 /2012 (x64)	Novell NetWare de versión 4.11-6.5 con estras instaladas de Minimum patch list	macOS Server 10.7 y superior	Linux v. 2.4.x y superior FreeBSD v. 6.x y superior para Intel x86 Solaris v. 10 para Intel x86

Dr.Web para servidores de Windows

Protección antivirus para servidores de Windows

Ventajas

- Alto rendimiento y estabilidad.
- El análisis de alta velocidad combinado con un bajo consumo de recursos del sistema permite a Dr.Web funcionar perfectamente en cualquier hardware del servidor.
- Funcionamiento automático libre de problemas.
- La tecnología del análisis retardado se aplica a los archivos abiertos para la lectura y proporciona un equilibrio de carga flexible para un sistema de archivos del servidor.
- Configuración del análisis flexible orientada al cliente y acciones a aplicar a los virus detectados o archivos sospechosos.
- Instalación y administración fácil.
- Protección sólida inmediatamente después de la instalación (con la configuración predeterminada).
- Funcionamiento transparente – registros detallados con nivel de detalle personalizable.

Características principales

- Análisis planificado de volúmenes de servidores bajo demanda.
- Análisis de todos los archivos transferidos a través del servidor sobre la marcha.
- Análisis bajo demanda. Análisis programado. Análisis de virus heurístico.
- Análisis de archivos comprimidos y empaquetados.
- Notificaciones tras detección de objetos infectados.
- Administración del antivirus desde la consola del servidor o consola remota: permite configurar el sistema de notificaciones, supervisar la protección y optimizar la configuración.
- Estadísticas del análisis que muestran el tiempo de operación, el número de archivos analizados e información acerca de los virus detectados. Análisis multiproceso.
- Desconexión automática de estaciones de trabajo desde el servidor si se conviertan en fuentes de amenaza.
- Notificaciones personalizables.
- Notificaciones instantáneas para los administradores y sus grupos.
- Aislamiento de archivos infectados o sospechosos en cuarentena.
- Desinfección y eliminación o desplazamiento de objetos infectados a cuarentena.
- Registro de acciones del antivirus.
- Actualización automática de las bases de firmas de virus.

Requerimientos al sistema

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

Enlaces de interés

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

Dr.Web para Novell NetWare

Protección antivirus para servidores de archivos

Ventajas

- La gama más amplia de las versiones compatibles de Novell Netware
- Desde 4.11 hasta 6.5.
- Soporte de namespace de NetWare.
- Soporte simultáneo de varios protocolos de red. Análisis de alta velocidad de grandes cantidades de datos con el consumo mínimo de recursos del sistema, tanto en tiempo real como bajo demanda.
- Consumo de recursos de CPU manejable mediante ajuste de prioridad del proceso de análisis.
- Proceso de instalación simple.
- Configuración del análisis flexible orientada al cliente y acciones a aplicar a los virus detectados o archivos sospechosos.
- Panel de control.

Características principales

- Análisis planificado de volúmenes de servidores bajo demanda.
- Análisis de todos los archivos transferidos a través del servidor sobre la marcha.
- Análisis multiproceso.
- Desconexión automática de estaciones de trabajo desde el servidor si se convierten en fuentes de amenaza.
- Análisis bajo demanda.
- Análisis programado.
- Análisis de archivos por formato utilizando la lista de extensiones, directorios, excepciones de volúmenes, análisis de todos los objetos..
- Análisis de virus heurístico.
- Análisis de archivos comprimidos, empaquetados y archivos de correo electrónico.
- Registros del análisis; registros detallados con nivel de detalle personalizable.
- Notificaciones tras detección de objetos infectados.
- Desinfección y eliminación o desplazamiento de objetos infectados a cuarentena.
- Administración del antivirus a través de la consola del servidor o una consola remota: permite configurar el sistema de notificaciones, controlar la protección y optimizar la configuración.
- Notificaciones instantáneas para los administradores y sus grupos a través del correo electrónico.
- Notificaciones personalizables.
- Estadísticas del análisis que muestran el tiempo de operación, número de archivos analizados e información acerca de los virus detectados.
- Registro de acciones del antivirus.
- Actualización automática de las bases de firmas de virus.

Requerimientos al sistema

- Novell NetWare de versión 4.11 a versión 6.5.

Enlaces de interés

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

Dr.Web para macOS Server

Protección antivirus para las estaciones de trabajo con versiones de servidores de macOS

Ventajas

- Centro de Control fácil de manejar. Alta velocidad del análisis. Perfiles del análisis personalizables.
- Protección fiable en tiempo real.
- Consumo mínimo de recursos del sistema. Bajo tráfico de actualizaciones.
- Configuración flexible.
- Interfaz elegante y fácil de usar.
- Interfaz cómodo y estilizado.

Características principales

- Análisis de elementos de inicio automático, dispositivos de almacenamiento extraíbles, unidades de red y unidades lógicas, mensajes de correo electrónico, archivos y directorios, incluidos los archivos comprimidos.
- Tres tipos del análisis: rápido, completo y personalizado. Análisis automático, manual y programado.
- La configuración de SpIDer Guard® está protegida por contraseña contra modificaciones no autorizadas.
- Diferentes acciones se pueden aplicar a diferentes tipos de objetos: desinfectar, mover a cuarentena, eliminar; las secuencias de acción permiten definir la acción que se aplicará a un objeto si no es posible aplicar la primera acción.
- Archivos y rutas a excluir definidos por el usuario.
- Detección y neutralización de los virus disfrazados con empaquetadores desconocidos.
- El registro de antivirus contiene la hora de cada evento, el nombre del objeto analizado y el tipo de acción aplicada al objeto.
- Actualización automática bajo demanda (programable) Notificaciones de virus, incluyendo eventos de sonido, para todos los eventos de virus.
- Cuarentena para aislar los archivos infectados; se puede especificar el tiempo de memorización y el tamaño máximo de la cuarentena. Desinfección, restauración y eliminación de objetos en cuarentena.
- Registro de operaciones detallado
- Los módulos están disponibles como herramientas de línea de comandos que se pueden utilizar con Apple Scripts.

Requerimientos al sistema

- macOS Server 10.7 o superior.
- Procesador Intel.
- Memoria operativa — según los requisitos del SO
- Acceso a Internet: para registrarse y recibir actualizaciones.

Enlaces de interés

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

Dr.Web para servidores de UNIX

Protección antivirus de servidores de archivos Unix

Ventajas

- Alto rendimiento y estabilidad.
- El análisis de alta velocidad combinado con un bajo consumo de recursos del sistema permite a Dr.Web funcionar perfectamente en cualquier hardware del servidor.
- Configuración del análisis flexible orientada al cliente y acciones a aplicar a los virus detectados o archivos sospechosos.
- Compatibilidad perfecta - el antivirus no entra en conflicto con ningún Firewall conocido o monitor de archivos.
- Soporte de sistemas de supervisión (Cacti, Zabbix, Munin, Nagios etc.)
- Administración fácil, instalación y configuración simple.

Características principales

- Análisis planificado de volúmenes de servidores bajo demanda.
- Mejorado! Análisis sobre la marcha - analiza los archivos en busca de virus, antes de abrirlos o escribir en ellos.
- Análisis multiproceso.
- Desconexión automática de estaciones de trabajo del servidor tan pronto como se identifuquen como fuentes de amenaza.
- Mejorado! Notificaciones instantáneas para los administradores y sus grupos a través de e-mail, mensajes cortos enviados a un teléfono o buscapersonas.
- Aislamiento de archivos infectados en cuarentena. Desinfección, restauración y eliminación de objetos en cuarentena
- Registro de acciones del antivirus.
- Actualización automática de las bases de firmas de virus.

Requerimientos al sistema

- Dr.Web Daemon (drwebd) de versión no inferior a 5.0.
- Samba 3.0 y superior.

SO soportados

- 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).

Enlaces de interés

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

Dr.Web Mail Security Suite

Protección del correo electrónico

- Dr.Web para UNIX Mail server
- Dr.Web para MS Exchange
- Dr.Web para IBM Lotus Domino (Windows, Linux)
- Dr.Web para Kerio Mail Server (Windows, Linux, macOS)

Licencias para Dr.Web Mail Security Suite

Tipos de licencia

- Según el número de usuarios protegidos.
- Licencia por servidor – análisis ilimitado del tráfico de correo electrónico del servidor para una cantidad de usuarios hasta 3.000.

Puede adquirir el producto de Dr.Web Mail Security Suite como un producto separado o como componente de Dr.Web Enterprise Security Suite. En este último caso la licencia también cubre el Centro de Control de Dr.Web Enterprise Security Suite y antispam (excepto Kerio).

Una licencia de Dr.Web Mail Security Suite también puede incluir SMTP proxy como un componente adicional. Usar estos productos juntos mejora la seguridad de la red en general y reduce la carga de trabajo de los servidores de correo electrónico locales y estaciones de trabajo.

Variedades de licencia

	Dr.Web para MS Exchange	Dr.Web para IBM Lotus Domino	Dr.Web para UNIX Mail Server	Dr.Web para Kerio Mail Server
Licencia básica	Antivirus	Antivirus	Antivirus	Antivirus
Componentes adicionales				
Antispam	+	+	+	–
SMTP proxy	+	+	+	+
Centro de control	+	+	+	+

Dr.Web Mail Security Suite también está incluido en los kits económicos para empresas pequeñas y medianas.

SO soportados

Producto	Windows	macOS	Linux	FreeBSD	Solaris
			Para Intel x86		
Dr.Web para UNIX Mail Servers			v. 2.4.x y superior	v. 6.x y superior	v. 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 (32&63 bits)		Red Hat Enterprise Linux (RHEL) v.v. 4 y 5, Novell SuSE Linux Enterprise Server (SLES) v.v. 9 y 10 (sólo 32 bits)		
Dr.Web para servidores de correo Kerio	2000/XP/Vista/7, Server 2003/2008/2012	macOS 10.7 y superior	Red Hat 9.0; Red Hat Enterprise Linux 4/5; Fedora Core 7/8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0, 11.1; CentOS Linux 5.2, 5.3; Debian 5.0; Ubuntu 8.04 LTS		

Dr.Web para UNIX Mail Servers

Protección antivirus y antispam inteligente para grandes cantidades de tráfico de correo electrónico

Ventajas

- Configuración flexible. Administración simple. Bajos requisitos del sistema TCO mínimo.
- Escalabilidad perfecta. Respuesta rápida.
- Filtrado eficiente del correo electrónico no deseado.
- Seguridad mejorada para el correo electrónico corporativo.
- Protección de la información confidencial.
- Solución abierta.
- Número de plugins ilimitado.

Características principales

- Filtrado del correo electrónico en busca de virus y spam.
- Análisis de los e-mails y de todos sus componentes.
- Análisis de la mayoría de los tipos de archivos, incluyendo archivos multivolumen y archivos autoextraíbles (SFX).
- Listas Blancas / Negras. Notificaciones personalizables. Informes estadísticos.
- Autoprotección.

- **Configuración flexible**

  Dr.Web para Unix Mail Servers puede ser configurado mediante reglas que proporcionan una mayor flexibilidad en comparación con soluciones de la competencia, que sólo pueden ser configuradas usando parámetros estáticos en los archivos de configuración. Los mensajes se filtran y se modifican de acuerdo con las políticas establecidas, donde el administrador puede configurar las reglas individuales de procesamiento para diferentes usuarios y grupos e incluso para cada mensaje de correo electrónico. Eso permite que el producto cumpla todos los requisitos de la seguridad corporativa.

- **Administración simple**

  Aunque rico en características, Dr.Web para Unix Mail Servers no requiere mucha configuración para empezar a usarlo. Por otra parte, también está disponible como parte de Dr.Web Office Shield, que cumple plenamente con el principio de "conectar y olvidar".

- **Bajos requisitos del sistema**

  Los requisitos del sistema de Dr.Web para UNIX Mail Servers son muy bajos, por eso la aplicación funciona perfectamente con cualquier hardware del servidor.

  Esto hace el antivirus una opción perfecta para las empresas que no pueden modernizar su hardware del servidor de forma regular para satisfacer los requerimientos crecientes de la mayoría de las soluciones antivirus.

- **TCO mínimo**

  A diferencia de muchas soluciones de la competencia, Dr.Web para UNIX MAIL Servers goza del servicio de concesión de licencias flexible y multiopcional.

  El cliente adquiere únicamente los componentes que necesita y no paga por el software innecesario que **nunca utilizará.**

- **Escalabilidad perfecta**

  Dr.Web para UNIX Mail Servers cumple con los requisitos de las empresas pequeñas que utilizan un solo servidor de correo electrónico, así como con los de proveedores de telecomunicaciones multinacionales que analizan grandes cantidades de datos. Las capacidades para proceder grandes cantidades de datos en tiempo real, fiabilidad y flexibilidad.

- **Respuesta rápida**

  El análisis multihílo asegura una respuesta rápida del antivirus que le permite analizar los datos que se reciben en tiempo real junto con los archivos recibidos anteriormente y mensajes a enviar a usuarios finales sin retrasos notables.

- **Filtrado eficiente de correo electrónico no deseado**

  El antispam de Dr.Web se suministra como un componente de la solución (pero nunca como un producto separado). Se instala en el servidor, donde está instalado el producto antivirus. Simplifica la administración de la solución y disminuye su TCO en comparación con soluciones de la competencia.

Ventajas del antispam de Dr.Web

- El antispam no requiere configuración o formación previa. A diferencia de soluciones antispam basadas en filtro de Bayes, comienza a funcionar tan pronto como llega el primer mensaje.
- Detecta los mensajes de spam sin importar el idioma. Acciones personalizables para diferentes categorías de spam. Las listas personalizadas blancas y negras excluyen la posibilidad de que la empresa sea desacreditada agregándola deliberadamente a las listas de direcciones no deseadas. Escaso número de falsos positivos.
- Queda relevante con una actualización en 24 horas — tecnología única de detección de spam basada en varios miles de reglas que permiten que el antispam este al día sin frecuentes descargas de actualizaciones voluminosas.

Seguridad mejorada para el correo corporativo

La estructura modular de Dr.Web para UNIX Mail Servers permite la integración del producto con diferentes sistemas de correo electrónico o usandolo como un SMTP proxy- un filtro para analizar los e-mails antes de ser recibidos por el servidor de correo electrónico. Uso simultáneo de Dr.Web para UNIX Mail Servers y un componente adicional de SMTP proxy establece lo siguiente:

- Mejora de la seguridad global de la red.
- Mejora de la calidad de filtrado sin limitaciones causadas por el servidor de correo electrónico.
- Baja carga de trabajo de los servidores de correo electrónico locales y estaciones de trabajo.
- Mayor estabilidad del sistema de filtrado de correo electrónico.

Protección de la información confidencial

La cuarentena se gestiona a través de la interfaz web o a través de una herramienta especial y la opción de archivar todos los mensajes de correo electrónico transferidos a través del filtro permite el seguimiento de causas de fugas de datos y restaurar los mensajes eliminados por error por los usuarios de sus buzones de correo electrónico.

Solución abierta

Dr.Web para UNIX Mail Servers puede integrarse con las soluciones de otros fabricantes. Con open API, los usuarios pueden agregar nuevas características al producto.

Número de plugins ilimitado

Nuevas características para la protección de correo electrónico pueden añadirse al producto sin ninguna limitación para que cualquier plugin escrito empieze a fuincionar con todas las MTA soportados inmediatamente.

Plugins implementados:

- Dr.Web – análisis antivirus de correo electrónico con Dr.Web Engine.
- vaderetro – plugin de filtración de spam.
- headersfilter – plugin de filtración de correo electrónico por los encabezados.

SO soportados

- Distribuciones Linux de versión del núcleo 2.4.x y superior.
- FreeBSD de versión 6.x y superior para plataforma Intel x86 y amd64.
- Solaris de versión 10 para plataforma Intel x86 y amd64.

Dr.Web SMTP proxy

Es un componente de Dr.Web para UNIX Mail Server. Puede ser instalado en DMZ o integrado con el sistema de correo electrónico existente. Con el servidor del análisis de correo electrónico ubicado en DMZ, el servidor de correo electrónico no tiene conexión directa a Internet. En este caso, incluso si un hacker logra poner el servidor en peligro, no obtendrá acceso a la información confidencial de la empresa. La solución realiza un análisis completo del tráfico SMTP/LMTP del correo electrónico.

Ventajas

- Calidad de filtrado mejorada sin limitaciones causadas por un servidor de correo electrónico.
- Menor carga de trabajo para servidores de correo electrónico internos, servidores de filtración del contenido, gateways de correo electrónico y de Internet y estaciones de trabajo.
- Mayor estabilidad del análisis de correo electrónico y mejor seguridad de la red en general.

Protección contra ataques de spammers — un administrador puede restringir los parámetros de la sesión SMTP para prevenir los ataques de spammers.

Protección contra el spam con la opción de validación de IP, su empresa estará protegida contra los mensajes de spam enviados con direcciones IP de remitentes falsos.

Protección contra ataques de hackers — el producto puede resistir los ataques pasivos como PLAIN y LOGIN, así como ataques activos desconocidos.

Protección contra las trampas de spam — Dr.Web para UNIX Mail Gateways puede comprobar si la dirección del destinatario es una trampa de spam.

El procesamiento correcto de los mensajes de correo electrónico con formato incorrecto — el producto puede bloquear los mensajes con el campo de remitente vacío, pero procesa correctamente los mensajes que infringen las normas, porque están malformados por ciertos clientes de correo electrónico.

Reducción del tráfico de Internet — Dr.Web para UNIX Mail Gateways permite limitar el tamaño de los archivos adjuntos del correo electrónico.

Servidores de retransmisión abiertos con la lista de retransmisión limitada — si una empresa necesita utilizar un servidor de retransmisión de correo abierto, Dr.Web para UNIX Mail Gateways ayudará a un administrador restringir la lista de dominios a los que el servidor transmitirá los mensajes.

Enlaces de interés

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

Dr.Web para MS Exchange

Protección Antivirus y Antispam del tráfico de correo electrónico dirigido a través de MS Exchange 2000/2003/2007/2010/2013/2016 servers

Ventajas

- El cumplimiento con los estándares de seguridad más altos - el producto está certificado por el Servicio Federal de Seguridad de Rusia (FSB) y el Servicio Federal del Control Tecnológico y de Exportación (FSTEC).
- Amplia gama de opciones de instalación y configuración que cumplen con los requisitos de casi cualquier empresa.
- El análisis de alta velocidad combinado con un bajo consumo de recursos del sistema permite a Dr.Web funcionar perfectamente en cualquier hardware del servidor.
- El antispam integrado no requiere ningún tipo de formación, reduce la carga de trabajo del servidor y mejora la productividad del empleado.
- El filtrado basado en las listas negras y blancas permite excluir ciertas direcciones del análisis y aumentar la eficiencia.
- Filtrado de archivos por tipo, lo que contribuye a un menor tráfico. La agrupación permite especificar diferentes parámetros de filtrado para diferentes grupos de empleados, lo que contribuye a una implementación más rápida y mantenimiento más cómodo. Alto rendimiento y estabilidad alcanzada con el análisis multihílo.
- Detección y neutralización de los virus comprimidos con empaquetadores desconocidos.
- Inicio automático al arrancar el sistema.
- Sistema de actualización fácil de usar con Windows Task Scheduler.

Características principales

- Análisis antivirus y antispam instantáneo del correo electrónico, incluyendo los archivos adjuntos.
- Seguimiento antivirus de los buzones de correo electrónico de usuarios y directorios públicos.
- Protección antivirus del tráfico de correo electrónico a través del servidor de MS Exchange.
- Desinfección de archivos infectados.
- Agrupación de usuarios mediante Active Directory. Parámetros del análisis ajustables: el tamaño máximo y los tipos de objetos a analizar, acciones a aplicar a los objetos infectados.
- Detección de objetos malware comprimidos con múltiples empaquetadores.
- Acciones personalizables para diferentes tipos de spam, incluyendo desplazamiento de los mensajes a cuarentena o añadiéndoles un prefijo especificado en sus campos temáticos.
- Texto personalizable insertado en los mensajes salientes.
- Aislamiento de archivos infectados y sospechosos en cuarentena.
- Envío de notificaciones de incidentes de virus a administradores y otros usuarios.
- Registro de operaciones.
- Actualizaciones automáticas.

Requerimientos al sistema

Procesador

- Para Microsoft Exchange Server 2000/2003: Intel Pentium 133 MHz (se recomienda 733 MHz).
- Para Microsoft Exchange Server 2007/2010/2013/2016: Intel con arquitectura x64 y soporte de la tecnología Intel 64; AMD con soporte de la plataforma AMD64.

Memoria operativa

- Para Microsoft Exchange Server 2000/2003: 512 MS o superior.
- Para Microsoft Exchange Server 2007/2010: 2 GB o superior.
- Para Microsoft Exchange Server 2013/2016: 4 GB o superior.

Espacio libre en el disco

- Para Microsoft Exchange Server 2000/2003/2007/2010: 512 MB.
- Para Microsoft Exchange Server 2013/2016: 1 GB.

SO soportados

- Para Microsoft Exchange Server 2000/2003: Microsoft® Windows® 2000 SP4, Microsoft® Windows Server® 2003 SP1 o superior.
- Para Microsoft Exchange Server 2007/2010: Microsoft® Windows Server® 2003 R2 SP2 x64/2008 x64/2008 R2.
- Para Microsoft Exchange Server 2013/2016: Microsoft® Windows Server® 2012/2008 R2.

Enlaces de interés

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

Dr.Web para IBM Lotus Domino

Protección Antivirus y Antispam para IBM Lotus Domino con Windows y Linux

Ventajas

- TCO mínimo

  Dr.Web para IBM Lotus Domino es capaz de funcionar en un servidor independiente, así como en un servidor de particiones o en clústeres de Lotus Domino. Las copias del antivirus en diferentes particiones se ejecutan como procesos separados en la RAM pero utilizan una base de datos única y los mismos archivos ejecutables.

  En este caso, sólo una copia está sujeta a la concesión de licencias, lo que permite una configuración más flexible y reduce los gastos para la protección antivirus.

- Licencias y certificados

  Dr.Web para IBM Lotus Domino cumple con los estándares de seguridad más exigentes - el producto está certificado por el Servicio Federal de Seguridad de Rusia (FSB) y el Servicio Federal del Control Tecnológico y de Exportación (FSTEC).

- Listo para IBM Lotus

  Dr.Web para IBM Lotus Domino cuenta con la marca Ready for IBM Lotus software y está incluido en el catálogo de IBM Lotus Business Solutions. La marca confirma la compatibilidad de Dr.Web para IBM Lotus Domino con Lotus Domino y su cumplimiento con todos los requisitos de compatibilidad de IBM.

- Resistencia excepcional a los virus

  Dr.Web puede ser instalado en un servidor Lotus Domino infectado y es capaz de desinfectarlo sin recurrir a los servicios públicos adicionales. Todas las bases de datos pueden ser analizadas bajo demanda después de la instalación. Para garantizar la máxima eficiencia del análisis, puede actualizar las bases de firmas de virus antes del análisis antivirus y utilizar las últimas definiciones del virus.

- Análisis de alta velocidad

  La organización eficiente de Dr.Web para IBM Lotus Domino, un algoritmo del análisis especial y administración flexible del proceso proporcionan un análisis de alta velocidad más eficiente. El análisis multihílo permite al antivirus procesar de forma simultánea grandes cantidades de datos. Esta ventaja permite a Dr.Web funcionar en casi cualquier hardware de servidor.

- Instalación fácil y configuración flexible

  El despliegue de Dr.Web para IBM Lotus Domino puede ser automatizado y controlado fácilmente mediante administración de scripts y documentación detallada. Con la interfaz web, un administrador puede utilizar cualquier navegador (Internet Explorer, Firefox y Opera) para controlar el funcionamiento del antivirus. Dr.Web para IBM Lotus Domino proporciona una administración del sistema con abundantes herramientas para configuración flexible de las acciones del antivirus aplicadas después del análisis, envío de notificaciones al remitente, destinatario y administrador del sistema tras detección de los virus, almacenamiento de los encabezados de los mensajes recibidos y archivos adjuntos.

- Administración fácil

  La agrupación permite diferentes parámetros de filtrado que se especifican para diferentes grupos de empleados, lo que contribuye a una implementación más rápida y mantenimiento más fácil. La misma configuración puede especificarse para varios grupos mediante la edición del perfil correspondiente.

- Filtrado de spam eficiente sin necesidad de formación previa

  La tecnología antispam integrada disminuye la carga de trabajo del servidor y mejora la productividad de los empleados. El filtrado basado en las listas negras y blancas permite excluir del análisis ciertas direcciones y aumentar la eficiencia.

Características principales

- El análisis de todos los componentes de los mensajes de correo electrónico en busca de virus y spam, y filtrado de spam en tiempo real o en una fecha programada por el administrador.
- Filtrado de spam, incluyendo filtrado de mensajes según las listas negras y blancas.
- Análisis antivirus de los documentos en las bases nsf especificadas. La función de "lanzar y parar" del escáner manual proporciona un análisis de los objetos bajo demanda.
- Análisis sintáctico de mensajes de correo electrónico para su posterior análisis.
- Desinfección de los mensajes infectados y sus archivos adjuntos. Detección de objetos malware comprimidos con empaquetadores múltiples.
- Detección y neutralización de los virus comprimidos con empaquetadores desconocidos.
- La tecnología adicional, capaz de detectar amenazas desconocidas aumenta la probabilidad de detectar nuevas especies de malware.
- Almacenamiento de los objetos infectados y sospechosos en la cuarentena (al acceder con Lotus Notes).
- Los informes se generan utilizando plantillas que son fáciles de leer.
- Registro de operaciones.
- Protección de propios módulos de los errores.
- Actualizaciones automáticas.

SO soportados

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.

Enlaces de interés

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

Dr.Web para Kerio Mail Servers

Análisis antivirus de los mensajes y sus archivos adjuntos, enviados a través de SMTP y POP3

Ventajas

- Compatibilidad perfecta con Kerio mail servers, comprobada por Kerio Technologies.
- Tiempo mínimo de entrega del mensaje logrado gracias al análisis miltihílo.
- Bajos requisitos del sistema y mínimo uso del tráfico local.
- Sistema flexible y fácil de configurar: lista personalizable de objetos analizados y acciones aplicadas a los virus detectados o archivos sospechosos.
- Acciones personalizables para los archivos que no se pueden analizar. Mantenimiento y configuración a través de la consola de Kerio mail server.

Características principales

- El antivirus se conecta a Kerio Mail Server y analiza los archivos adjuntos y los mensajes entrantes y salientes.

SO soportados

Versión para Windows

- Espacio en el disco duro: No menos de 350 MB.
- 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 libre en disco duro: No menos de 290 MB.
- 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 macOS

- Espacio en el disco duro: No menos de 55 MB.
- macOS 10.7 y superior.
- Servidor de correo: Kerio MailServer 6.2 o superior, Kerio Connect 7.0.0 o superior.

Enlaces de interés

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

Dr.Web Gateway Security Suite

Protección de gateways

- Dr.Web para gateways de UNIX
- Dr.Web para gateways de Kerio
- Dr.Web para Microsoft ISA Server y Forefront TMG
- Dr.Web para MIMEsweeper
- Dr.Web para Qbik WinGate

Licencias para Dr.Web Gateway Security Suite

Tipos de licencia

- Según el número de usuarios protegidos.
- Según licencia del servidor – análisis ilimitado del tráfico de correo electrónico del servidor para hasta 3.000 usuarios protegidos.

Puede adquirir el producto de Dr.Web Mail Security Suite como un producto separado o como componente de Dr.Web Enterprise Security Suite.

Variedades de licencia

	Dr.Web para UNIX Gateways	Dr.Web para Kerio Gateways	Dr.Web para MIMEsweeper	Dr.Web para Qbik WinGate
Licencia básica	Antivirus	Antivirus	Antivirus	Antivirus
Componentes adicionales				
Antispam	–	–	+	+
Centro de control	–	+	–	–

Dr.Web Mail Security Suite también está incluido en los kits económicos para empresas pequeñas y medianas.

SO soportados

Producto	Windows	Linux	FreeBSD	Solaris
		Para Intel x86		
Dr.Web para gateways de UNIX		v. 2.4.x y superior	v. 6.x y superior	v. 10
Dr.Web para gateways de Kerio	2000/ XP/2003/2008/7			
Dr.Web para Microsoft ISA Server y Forefront TMG	En caso de usar Microsoft ISA Server: Microsoft® Windows Server® 2003 x86 Service Pack 1 (SP1); Microsoft® Windows Server® 2003 R2 x86 En caso de usar Microsoft Forefront TMG: Microsoft® Windows Server® 2008 SP2 Microsoft® Windows			
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 gateways de Internet de UNIX

Análisis antivirus del tráfico HTTP y FTP en gateway – proxy-server de Internet corporativo

Ventajas

- Una amplia gama de opciones para establecer una protección completa contra las amenazas escondidas en el tráfico de Internet entrante.
- Envío del contenido libre de virus a la red protegida.
- El filtrado eficiente del tráfico por el servidor ICAP no retrasa la entrega del contenido.
- Protección contra la penetración de la defensa por cualquier tipo de malware.
- Alta escalabilidad.
- Capacidad de procesar grandes cantidades de datos en tiempo real. Reducción sustancial de los costos de Internet.
- Compatibilidad perfecta – integración con cualquier aplicación compatible con ICAP, con todos los firewalls.
- Soporte de prácticamente todos los sistemas operativos basados en UNIX , utilizados actualmente.
- Bajos requisitos de sistema permiten que el producto funcione sin problemas en cualquier hardware del servidor.
- Flexibilidad y facilidad de administración, el producto permite implementar configuraciones de protección que cumplen las políticas de seguridad de su empresa.

Características principales

- Análisis antivirus del tráfico HTTP y FTP.
- Administración centralizada a través del panel de control Web del centro de control de Dr.Web Entreprise Security Suite.
- Filtrado por nombre de host, tipo de MIME, o tamaño de archivo.
- Control de acceso a los recursos Web.
- Tecnología del análisis preliminar para el tráfico optimizado.
- Soporte de IPv4 e IPv6.
- Varias acciones a aplicar a diferentes tipos de archivos analizados.
- Aislamiento de archivos infectados en cuarentena. Informes fáciles de leer.
- Administración centralizada de los servidores de protección y recogida de informes de los servidores.
- Procesamiento simultáneo de varias solicitudes por conexión individual.
- Protección contra el acceso no autorizado.
- Control de operaciones del sistema y restablecimiento automático después de un error.
- Notificaciones de usuarios acerca de la presencia de los virus o códigos malware en las páginas web.

SO soportados

- Linux con versión del núcleo 2.4.x y superior.
- FreeBSD de versión 6.x y superior (para plataforma Intel x86 y amd64).
- Solaris de versión 10 (para plataforma Intel x86 y amd64).
- Cualquier servidor proxy que soporta completamente el protocolo ICAP, y también Squid no inferior a 3.0, SafeSquid no inferior a 3.0.

Requerimientos al sistema

- Espacio en el disco duro: no menos de 50 MB.
- Sistema operativo: Microsoft Windows 2000/XP/Vista/2012, Microsoft Windows Server 2000/2003/2008 (sistemas de 32 y 64 bits).
- Servidor proxy: Qbik WinGate 6.

Enlaces de interés

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

Dr.Web para gateways de Internet de Kerio

Análisis antivirus de HTTP, FTP, SMTP, POP3 y tráfico de Kerio Clientless SSL VPN

Ventajas

- Protección fiable de conexiones a Internet para usuarios domésticos y empresas de todo tipo y tamaño.
- Administración fácil — reciba notificaciones de todos los eventos de virus mediante correo electrónico o mensajes de texto.
- Tiempo mínimo de entrega del mensaje logrado a través del análisis miltihílo.

Características principales

- Detección de objetos malware transmitidos a través de HTTP, FTP, SMTP, POP3 y Kerio Clientless SSL VPN traffic.
- Detección de archivos adjuntos del correo electrónico infectados antes de que sean procesados por un servidor de correo electrónico.
- Lista personalizable de protocolos de transferencias de datos a analizar.
- Parámetros del análisis ajustables: Tamaño máximo y tipo de objetos a analizar, acciones a aplicar a los objetos infectados.
- Acciones emprendidas para neutralizar una amenaza se aplican de acuerdo con la configuración de Kerio.
- Activar/desactivar la detección de determinados tipos de aplicaciones malware.
- Registro de errores y eventos en el Event Log y text log; el registro contiene la información acerca del módulo parámetros, notificaciones acerca de los virus detectados en cada mensaje infectado.
- Actualización automática de las bases de firmas de virus.

Requerimientos al 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 bits)
  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

Enlaces de interés

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

Dr.Web para Microsoft ISA Server y Forefront TMG

Ventajas

- Amplia gama de opciones para la instalación y configuración.
- Posibilidad de funcionar en los servidores de cualquier configuración - incluso con poca RAM.
- Protección de servidores reales y virtuales.
- Alta velocidad del análisis del tráfico con carga mínima del sistema operativo mediante el uso de una tecnología del análisis multiproceso y análisis dinámico de los recursos necesarios.
- El antispam integrado no requiere formación previa (comienza a funcionar desde el momento de instalación), reduce la carga de trabajo del servidor y mejora la productividad de los empleados.
- Reducción del riesgo de infección de los recursos malware y tráfico reducido debido al bloqueo del acceso a diversos recursos de Internet y filtrado del tráfico por tipo de archivo.
- Detección y neutralización de virus y empaquetadores desconocidos.
- Sistema de actualizaciones fáciles. Soporte técnico en Inglés.

Características principales

Gestión de productos centralizada desde cualquier equipo. La gestión se realiza a través de su navegador web mediante un protocolo seguro HTTPS y no requiere instalación de software adicional.

Antivirus

- Análisis antivirus de HTTP/FTP sobre el tráfico HTTP, incluidos los archivos adjuntos;
- **¡Novedad!** Soporte para soluciones de clúster. Dr.Web para Microsoft ISA Server y Forefront TMG permite combinar los servidores, donde los firewalls de Microsoft están instalados en un mismo clúster (el árbol de servidores maestro y esclavo) y gestionar todo el sistema desde un servidor;
- **¡Novedad!** Control de aplicaciones. En caso de un error en la aplicación, Dr.Web SSM realiza su reinicio;
- El análisis con los parámetros definidos: selección del tamaño máximo y tipos de objetos analizados, acciones (incluyendo archivos que no pueden ser analizados) y también las formas de procesamiento de los objetos infectados;
- Detección de objetos malware comprimidos con múltiples empaquetadores.
- Desinfección de archivos infectados;
- Bloqueo del acceso a los datos infectados para todos los usuarios de la red local;
- Restricción del acceso de usuarios a los recursos en línea con el Control de Oficina;
- Aplicación de diferentes acciones dependiendo del tipo de spam;
- Aislamiento de archivos infectados o sospechosos en cuarentena;
- Notificaciones de incidencias de virus para los administradores y otros usuarios;
- Registro de operaciones del sistema.

¡Atención! Dr.Web para Microsoft ISA Server y Forefront TMG tienen una mayor velocidad del análisis de paquetes de HTTP y enlaces en comparación con la versión de antispam.

Antivirus + Antispam

- Adiciones a las funciones del antivirus.
- Filtrado antispam del tráfico de correo electrónico en SMTP/POP3.
- Creación de grupos de usuarios y asignación de perfiles de protección antivirus para ellos.
- Agregación del texto adjunto a los mensajes de correo electrónico que contienen amenazas.
- Desplazamiento de los archivos infectados y sospechosos a cuarentena. Filtrado de spam; filtrado de mensajes de acuerdo con filtros de las listas negras y blancas.
- Registro de operaciones.
- Actualizaciones automáticas.

Requerimientos al sistema

	Para Microsoft ISA Server	Para Microsoft Forefont TMG
CPU	CPU Pentium® III 733 MHz o superior	CPU Pentium® III 1,86 GHz o superior
RAM	1 GB o superior	2 GB o más
Espacio libre en disco duro	300 MB para instalar.	
	Se requiere espacio adicional en el disco necesario para el almacenamiento de datos durante en análisis, determinado por la intensidad de solicitudes de usuarios y el tamaño de los archivos cargados por los usuarios.	
Pantalla	Compatible con VGA	

Requisitos del sistema operativo y software

Característica	Requisitos	
CPU	CPU Pentium® III 733 MHz o superior	CPU Pentium® III 1,86 GHz o superior
Sistema operativo	Uno de los siguientes: Microsoft® Windows Server® 2003 x86 con Service Pack 1 (SP1); Microsoft® Windows Server® 2003 R2 x86	Uno de los siguientes: Microsoft® Windows Server® 2008 SP2. Microsoft® Windows Server® 2008 R2
Sistema de archivos	NTFS	NTFS
Proxy server	Microsoft® ISA Server 2004 Microsoft® ISA Server 2006	Microsoft® Forefront® TMG 2010
Otro software	Microsoft Windows Installer 3.1 o superior. NET Framework 3.5 SP1 Internet Explorer 6 o superior o Mozilla Firefox 3 o superior	

Enlaces de interés

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

Dr.Web para MIMEsweeper

Protección antivirus y antispam de tráfico del correo electrónico, transmitido a través de los servidores de filtrado del contenido Clear-Swift MIMEsweeper

Ventajas

- **Fácil de instalar y configurar**

  Las herramientas de configuración - asistentes de escenarios - integrados en Dr.Web para MIMEsweeper permiten crear los escenarios del análisis de mensajes más avanzados de forma automática (tipo 1 por clasificación de 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 realizar el análisis de memoria adicional y evitar la ejecución del código malintencionado. Debido a esto, los usuarios no necesitan cambiar el modo de funcionamiento de DEP – las aplicaciones malware no harán uso del mecanismo de procesamiento de excepciones de Windows.

- **Configuración flexible**

  Al detectar un objeto infectado el plugin intenta desinfectarlo o lo elimina, si la opción de desinfectar no está seleccionada. Si el mensaje de correo electrónico tiene varios archivos adjuntos, el plugin desinfectará solo los archivos adjuntos infectados. Si se detecta un virus dentro del cuerpo del mensaje, el filtro de contenido mueve el mensaje a cuarentena. Los mensajes de correo electrónico, archivos y archivos comprimidos "limpios" se transfieren al destinatario sin ninguna modificación. Los mensajes de correo electrónico infectados, que no se pueden neutralizar, se marcan y por defecto se mueven a cuarentena.

Características principales

- Análisis de los mensajes del correo electrónico y archivos adjuntos, incluidos los archivos comprimidos, antes de que sean procesados por el servidor del correo electrónico.
- Desinfección de objetos infectados.
- Aislamiento de archivos infectados y sospechosos en cuarentena.
- Filtrado del correo electrónico en busca de spam, incluso utilizando las listas blancas y negras.
- Mantenimiento de estadísticas del conjunto.
- Actualizaciones automáticas.

Requerimientos al sistema

- Windows 2000 Server (SP4) o superior.
- Windows Server 2003 o superior.

Enlaces de interés

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

Dr.Web para Qbik WinGate

Análisis antivirus y antispam del tráfico HTTP/POP3/FTP, SMTP y servidor proxy de Qbik WinGate

Ventajas

- A diferencia de otros productos para Qbik WinGate, Dr.Web dispone del filtro de antispam. El antispam no requiere configuración o formación previa, sino comienza a funcionar tan pronto como se recibe el primer mensaje, por lo tanto el antispam no requiere formación diaria por el administrador del sistema.
- La tecnología vanguardista del análisis sin utilizar las firmas de virus de Origins Tracing™ proporciona una alta probabilidad de detección de los virus, desconocidos por Dr.Web, incluso en archivos comprimidos.

Características principales

- Análisis antivirus y antispam de los mensajes y sus archivos adjuntos enviados a través de SMTP y POP3.
- Análisis antivirus de archivos y datos transferidos a través de HTTP y FTP.
- Desinfección de archivos infectados transferidos a través de HTTP.
- Lista personalizable de protocolos de transferencias de datos a analizar.
- Configuración del análisis ajustable, por ejemplo, el tamaño máximo y los tipos de objetos a analizar y las acciones a aplicar a los objetos infectados.
- Activación/Desactivación de detección de ciertos tipos de malware; cuando se detecta una amenaza, la configuración de Qbik WinGate determina las acciones que se deben aplicar para neutralizarla.
- Acciones personalizables para los archivos que no se pueden analizar.
- Detección de objetos malware comprimidos con varios empaquetadores.
- El módulo antispam compacto y eficiente hace la diferencia entre Dr.Web para Qbik WinGate y su competencia.
- El antispam no requiere formación previa y permite establecer diferentes acciones para varias categorías de spam y crear listas blancas y negras de correo electrónico.
- Acciones personalizables a aplicar a diferentes tipos de objetos, como por ejemplo moverlos a cuarentena o añadir prefijos específicos a sus áreas temáticas.
- Registro de errores y eventos en Event Log, que contiene la información acerca de los parámetros del módulo, así como las notificaciones acerca de los virus detectados en los mensajes infectados y brotes individuales.
- Aislamiento de archivos infectados en la cuarentena de Dr.Web y cuarentena de WinGate.
- Visualización del contenido de cuarentena y posterior restauración y/o reenvío de archivos en cuarentena.
- Copia de seguridad de los archivos desinfectados en cuarentena.
- Panel de control y Asistente de cuarentena.
- Actualización automática.

Requerimientos al sistema

- Espacio libre en el disco duro: No menos de 50 MB.
- Sistema operativo: Microsoft Windows 2000/XP/Vista/2012, Microsoft Windows Server 2000/2003/2008 (sistemas de 32 y 64 bits).
- Servidor proxy: Qbik WinGate 6.

Enlaces de interés

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

Dr.Web Mobile Security Suite

Protección para dispositivos móviles

- Dr.Web para Android
- Dr.Web para BlackBerry

Licencias para Dr.Web Mobile Security Suite

Dr.Web Mobile Security Suite se licencia según el número de dispositivos protegidos.

Variedades de Licencia

Dr.Web para Android	Dr.Web para BlackBerry
Protección completa + Centro de control	Protección completa

Dr.Web Mobile Security Suite también está incluido en los kits económicos para empresas pequeñas y medianas.

	Dr.Web per Android	Dr.Web per BlackBerry
Componentes de la protección*	Antivirus Filtro de llamadas y SMS** Antirrobo** URL filtro Firewall Auditor de seguridad	Antivirus Auditor de seguridad
Administración Centralizada dentro de Dr.Web Enterprise Security Suite	+	
Sistemas operativos compatibles	OS Android 4.0-7.1. Firewall es compatible con Android 4.0 y más	BlackBerry 10.3.2+
Funciones clave		
Escaneo multiflujo con la distribución de las tareas entre los núcleos del procesador	+	
Escaneo de archivos que llegan a través de conexiones GPRS/Infrared/Bluetooth/Wi-Fi/USB o durante la sincronización con PC	+	+
Dos tipos de escaneo: completo y personalizado	+	+
Posibilidad de habilitar/deshabilitar el escaneo permanente de la tarjeta de memoria	+	
Recuperación automática de funcionamiento	+	
Escaneo por demanda de todo el sistema de archivos o de archivos y carpetas por separado	+	+
Escaneo de archivos en archivos APK, ZIP, SIS, CAB, RAR, JAR	+	+
Prohibición de iniciar en un dispositivo móvil las aplicaciones que no están en el listado de permitidas por el administrador.	+	
Configuración de las reglas de funcionamiento para cada aplicación	+	
Control operativo del tráfico entrante y saliente para cada aplicación	+	
Posibilidad de restringir el tráfico de uso de Internet móvil	+	
Posibilidad de establecer restricciones para aplicaciones en concreto en roaming	+	
Prevención del acceso a los recursos no recomendados de la red Internet	+	
Protección contra acceso no sancionado al conectarse a las redes inalámbricas	+	
Desbloqueo de troyanos extorsionistas	+	
Escáner de vulnerabilidades	+	
Listas blancas y negras de llamadas de teléfono entrantes y mensajes SMS	+	
Soporte de varias tarjetas SIM de confianza	+	
Eliminación de archivos infectados	+	+
Transferencia de archivos sospechosos a cuarentena	+	+
Recuperación de archivos de la cuarentena	+	+
Actualizaciones por Internet: ■ a través del protocolo HTTP usando el módulo incorporado GPRS; ■ a través de infrarrojos / Bluetooth / Wi-Fi / USB-conexión; ■ sincronizando el equipo que tiene acceso a la red Internet, a través de la conexión ActiveSync	+	+
Informes detallados sobre el escaneo del sistema	+	+
Visualización de la información sobre amenazas encontradas en el panel de bloqueo con posibilidad de ir al listado de amenazas	+	
Notificación sobre la detección de acciones típicas para programas nocivos	+	
Administración remota del dispositivo móvil en caso de pérdida o robo del mismo – usando el "Antirrobo"	+	
Recepción de las coordenadas GPS del dispositivo móvil por SMS	+	

* Para los dispositivos bajo la administración de Android TV están disponibles solo el Antivirus, Auditor de seguridad y Firewall.
** No es posible usar este componente en dispositivos sin ranura para tarjetas SIM.

Enlaces de interés

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

Kits de Dr.Web

Seguridad antivirus de clase enterprise para empresas pequeñas y medianas

Todos los productos de Dr.Web para la protección de correo electrónico están incluidos en los kits económicos para empresas pequeñas y medianas. Es una oferta económica única. Empresas pequeñas con el número de equipos de 5 a 50 que no pueden permitirse soluciones de antivirus de protección completa para empresas grandes, que pueden aprovechar los kits de Dr.Web que incluyen productos de protección para todos los tipos de objetos: estaciones de trabajo, tráfico de correo electrónico, servidores de archivos y gateways de Internet.

Importante! No hay descuentos disponibles para los kits, incluyendo descuentos de renovación o migración. Para continuar usando el kit, debe adquirir una licencia nueva. Si el usuario desea renovar una licencia para algun(os) producto(s) del kit, el descuento de renovación se concede para este producto o productos.

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 gateways	Dispositivos móviles
Licencia	Protección completa	Antivirus	Antivirus + Antispam + SMTP proxy	Antivirus	Antivirus
Cantidad	5 – 50	1	Igual al número de WSs	25	Igual al número de WSs

Enlaces de interés

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

Kits Dr.Web Escuelas

Producto	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mobile Security Suite
Licencia	Protección completa + Centro de Control	Antivirus	Antivirus
Cantidad	10 – 200	1 – 8	10 – 200

Dr.Web — herramientas de desinfección

Las herramientas de desinfección de Dr.Web están diseñadas para el análisis y desinfección en casos de emergencia. No proporcionan protección continua.

Dr.Web CureNet!

Desinfección remota centralizada para las estaciones de trabajo y servidores de cualquier red de Windows, incluso aquella que tiene instalado otro software antivirus.

Clientes potenciales	Empresas pequeñas, medianas y grandes que actualmente utilizan otros productos antivirus en los equipos y servidores en sus redes.	
Funciones	■ Desinfección de emergencia para servidores y estaciones de trabajo de Windows. ■ Verificación de la calidad del software antivirus que se utiliza actualmente.	
Características	■ No requiere desinstalación del antivirus actual antes del análisis y desinfección con Dr.Web CureNet!. ■ No requiere servidor en ejecución o software adicional. Funciona en redes aisladas de Internet. ■ Dr.Web CureNet! El Asistente puede ejecutarse desde una unidad extraíble, incluyendo dispositivos de almacenamiento de datos USB.	
Descripción del producto	http://curenet.drweb.com/	
Sistema operativo compatible	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 bits), iPhone 4, iPod touch 4 iOS 7.0+.	
¿Qué es "Mi Dr.Web CureNet!"?	Este es el área privada, donde se encuentra el enlace para descargar Dr.Web CureNet!, disponible durante todo el periodo de validez de la licencia. "Mi Dr.Web CureNet!" también se utiliza para contactar con el servicio de soporte técnico, enviar un archivo sospechoso para el análisis y utilizar otros servicios.	
Licencias	La utilidad se licencia por el número de estaciones (5 como mínimo) por 1, 2 y 3 años de uso.	
Versión demo	No tiene función de desinfección.	
Requerimientos al 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!

Desinfección de emergencia para las estaciones de trabajo y servidores de Windows, incluso aquellos que tienen instalado el antivirus de otro fabricante.

Clientes potenciales	Las empresas pequeñas, medianas y grandes que actualmente están utilizando los antivirus de otros fabricantes en sus equipos y servidores.
Funciones	■ Desinfectar las estaciones de trabajo y servidores de Windows. ■ Verificar la calidad del software antivirus usado actualmente.
Características	■ Dr.Web CureIt! no requiere instalación y no entra en conflicto con ningún antivirus conocido; por consiguiente no hay necesidad de desactivar el antivirus que se utiliza actualmente para analizar el sistema con Dr.Web CureIt!. ■ Autoprotección avanzada y modo mejorado para contramedidas más eficientes contra los bloqueadores de Windows. ■ Dr.Web CureIt! se actualiza al menos una vez por hora. ■ La herramienta se puede ejecutar desde una unidad extraíble incluyendo dispositivos de almacenamiento USB.
Descripción del producto	http://free.drweb.com/cureit
Sistemas operativos compatibles	MS Windows 10/8/7/Vista/2012/2008 (sistemas de 32 y 64 bits), XP/2003 (sistemas de 32 bits)
Licencias	La utilidad se licencia por 12, 24 y 36 meses.
Términos de licencia	La herramienta está disponible de forma gratuita siempre y cuando se utiliza para fines no comerciales.
Versión demo	N/A.
Requerimientos al sistema	PC bajo la administración del SO MS Windows 8/7 Vista/2012/2008 (sistemas de 32 y 64 bits), XP/2003 (sistemas de 32 bits)

Rusia

Doctor Web, S.L

125040, Moscú, C./ 3ª Yamskogo Polya, edf. 2, entrada 12A

Teléfono: +7 (495) 789-45-87 (Multicanal)

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

Teléfono gratuito de soporte técnico: 8-800-333-7932

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

Alemania

Doctor Web Deutschland GmbH

Rodenbacher Chaussee 6, D-63457 Hanau

Teléfono: +49 (6181) 9060-1210

Fax: +49 (6181) 9060-1212

www.drweb-av.de

China

Doctor Web Software Company (Tianjin), Ltd.

Área de desarrollo económico y tecnológico de Tianjin, 4ª avenida, nº 80, centro tecnológico "Tianda", edificio norte «software»

天津市经济技术开发区第四大街80号软件大厦北楼112

Teléfono: +86-022-59823480

Fax: +86-022-59823480

E-mail: D.Liu@drweb.com

www.drweb.fr

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.

Edificio NKF Kawasaki 2F1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken 210-0005

Teléfono: +81 (0) 44-201-7711

www.drweb.co.jp

Kazajstán

Doctor Web – Asia Central, S.L

050009, Almaty, c./ Shevchenko / rincón con c./ Radostovtsa,165b/72g, oficina 910

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

www.drweb.kz

Ucrania

Centro de soporte técnico "Doctor Web"

01601, Ucrania, Kiev, c/Pushkinskaya 27, planta 5, oficina 6

Teléfono/Fax: +38 (044) 238-24-35

www.drweb.ua