You have what to protect?

We have Dr.WEB®

since 1992

Contents

About Doctor Web

Doctor Web is a Russian developer of information security software. Dr.Web anti-virus products have been developed since 1992. They have always shown perfect results detecting malicious programs of all types and comply with international security standards. Our numerous customers around the world are clear evidence of the utmost trust placed in our products.

All Dr.Web products feature unique proprietary anti-virus technology. Doctor Web is one of the few anti-virus vendors to have its own technologies for malware detection and curing, a virus monitoring service, and an analytical laboratory. This ensures a rapid response to the latest threats and allows problems of any complexity to be solved in the shortest time possible.

Doctor Web's strategic goal is to create anti-virus software that always meets the most current information security needs. Another of the company's highest priorities is to develop new technologies to arm users against all types of computer threats. The Dr.Web product line provides anti-viruses for the widest range of operating systems and compatible applications.

Doctor Web distributes its products via its partner network instead of conducting sales directly. The company's comparatively small size allows it to stay flexible and mobile in business. Outside-of-the-box problem solving and mutual benefit are the company's basic principles. Doctor Web offers its partners many incentives. All companies selling Dr.Web products are given marketing and informational support. Doctor Web also provides training programs for end-users and partners who want to use Dr.Web software.

Doctor Web's wide range of customers includes home users from many countries, major Russian enterprises, small organizations, and parent companies. Doctor Web is grateful to all of its customers for their loyalty and support through the years.

Dr.Web technologies

Dr.Web anti-viruses are developed by skilful Russian programmers headed by Igor Daniloff – the author of Dr.Web and the owner of Doctor Web.

Dr.Web anti-virus products, based on the unique technology of detection and curing, have been developed by our company to give you the competitive edge, something very few anti-virus vendors can offer. Doctor Web has its own virus-monitoring service and analytical laboratory, guaranteeing a rapid response to new virus threats. The company offers proven anti-virus and anti-spam solutions for businesses, government entities, and personal use.

Technologies

A good anti-virus application can detect viruses. Deleting an infected file that may contain important information is one thing, but restoring the file to its original "healthy" state is entirely another. Dr.Web treats user files with great care.

Cures viruses

- The Dr.Web anti-virus functions on infected computers; its exceptional resistance to viruses makes it stand out among other anti-viruses.
- Dr.Web has the highest success rate in the industry for curing active infections.
- There is no need to cure a system prior to installing Dr.Web; this is due to the product's unique technologies for scanning memory processes and its outstanding ability to neutralize active infections.
- High probability to launch a scanning process in the infected system successfully even from a remote data-storage device without installation (e.g. from a USB flash drive).

Self–protection

Dr.Web is immune to any attempts by malicious programs to disrupt its operation. Dr.Web SelfPROtect is the unique anti-virus component that maintains the anti-virus' security.

- Dr.Web SelfPROtect is implemented as a driver that operates on the lowest system level. The driver can't be stopped or unloaded without a system reboot. There is no way for a malicious program to disrupt operation of the self-protecting module.
- Dr.Web SelfPROtect restricts access to a network, files and folders, certain branches of the Windows Registry and removable data-storage devices on the system driver level and protects the software from anti-viruses aiming to disrupt the operation of Dr.Web.
- Some anti-viruses modify the Windows kernel through intercept interrupts, changing vector tables or using other undocumented features. This may have a negative impact on the stability of a system and pave new ways for malicious programs to get into a system. At the same time, Dr.Web SelfPROtect maintains security of the anti-virus and doesn't interfere with routines of the Windows kernel.

Unique engine features

- Scans archived files at any nesting level.
- Reliably detects packed objects regardless of whether or not Dr.Web recognizes the compression format and their detailed analysis aimed at exposing hidden threats.
- Leader in detecting and neutralizing complex rootkits (Shadow.based (Confi ker), MaosBoot, Rustock.C, Sector).
- Intelligent memory scan technologies allow viruses to be blocked in the RAM before replicating themselves to the hard drive, making it less likely for malware to exploit the vulnerability of a third-party application or the operating system.
- Dr.Web can detect and neutralize viruses that can be found only in RAM and do not exist as files on disks, e.g. Slammer or CodeRed.

Detection of unknown threats

- FLY-CODE is a unique universal decompression technology enabling Dr.Web to unpack data that has been compressed with unknown packers.
- The cutting-edge, non-signature scan technology Origins Tracing™ ensures the high probability that viruses unknown to Dr.Web will be detected.
- The heuristic analyzer, whose analyses are based on criteria that is typical of various groups of malicious programs, detects most known threats.
- Dr.Web Process Heuristic protects systems against new, highly prolific malicious programs that are capable of avoiding detection by traditional signature-based analysis and heuristic routines because they haven't yet been analysed in the anti-virus laboratory and, therefore, are unknown to Dr.Web at the moment of intrusion. It analyses behaviour of a suspicious program to determine if it is malignant and takes necessary steps to neutralise the threat, if there is any. The new technology protects data from corruption to minimize losses from actions of an unknown virus.
- The comprehensive analysis of packed threats significantly improves detection of supposedly "new" malicious programs that were known to the Dr.Web virus database before they were concealed by new packers. In addition, with such an analysis there is no need to add redundant definitions of new threats into the virus database. With Dr.Web virus databases kept small, a constant increase in system requirements is not needed. Updates remain traditionally small, while the quality of detection and curing remains at the same traditionally high level.

Spam filtering technologies

The Dr.Web anti-spam analyzes messages using several thousands of rules which can be divided into several groups.

- Heuristic analysis

  A highly intelligent technology that empirically analyzes all parts of a message: header, body, and attachments. It allows detecting unknown types of spam. The heuristic analyzer is being constantly improved; new rules are frequently added. It allows detecting next generation spam messages even before a corresponding rule is created.

- Counteraction filtering

  The counteraction filtering is one of the most advanced and efficient technologies of Dr.Web anti-spam. It helps recognize techniques and tricks used by spammers to avoid detection.

- HTML-patterns

  Messages containing HTML code are compared with HTML patterns from the anti-spam library. Such comparison in combination with data on sizes of images typically used by spammers helps protect users against spam messages featuring HTML-code, which often contains online images.

- Detection based on SMTP envelope

  Detection of fake sender and receiver in an SMTP envelope and fake values of header fields is the latest trend in development of anti-spam technologies. A sender address contained in the received message is easy to fake and therefore should not be trusted. Yet unsolicited mail is not limited by spam. It also includes hoaxes or anonymous threats. Dr.Web anti-spam technologies allow to determine if an address is fake and mark the message as unsolicited. It saves traffic and protects employees from unwanted e-mails contents of which may have unpredictable impact on people's behaviour.

- Semantic analysis

  Words and phrases of a message are compared with words and phrases from the spam dictionary. All words, phrases and symbols are analyzed – both visible to the human eye and those hidden by spammer tricks.

- Anti-scam technologies

  Scams (as well as pharming messages – a type of scams) are the most dangerous type of spam. The most notorious example of scam is so-called "Nigerian" scams, loan scams, lottery and casino scams and false messages from banks and credit organizations. A special module of Dr.Web anti-spam is used to filter scams.

- Technical spam filtering

  Automatic e-mail notifications or bounces are designed to notify a user if a failure in operation of a mail system occurs (e.g the message couldn't be delivered at the specified address). Similar messages can be used by criminals. For example, a worm or ordinary spam can get to a computer as a notification. A special module of Dr.Web anti-spam detects such unwanted messages.

Advantages of Dr.Web anti–spam

- The anti-spam doesn't require configuration or training. Unlike anti-spam solutions based on Bayesian filtering, it starts working as soon as the first message arrives, so the anti-spam doesn't require daily training by the system administrator.
- It detects spam messages regardless of their language.
- No e-mail receipt delays.
- Real-time e-mail filtering.
- High-speed filtering with low consumption of system resources.
- Scanning objects at any nesting level.
- It can choose a processing technology for the target object depending on the message envelope or upon detection of blocking objects.
- Messages that have been filtered out are placed in a separate folder so one can always check them to make sure that no false detection has occurred.
- With the unique technologies there is no need for blacklists. No company will be discredited after it has been deliberately added to such a list.
- Completely stand-alone: a constant connection to an external server or access to a database are not required which saves traffic significantly.
- Doesn't need to be updated more often than once in 24 hours – unique spam detection technologies based on several thousands of rules allow the anti-spam to stay up to date without frequent downloads of bulky updates.

Dr.Web Virus Database and Global Updating System

Special Organization

Dr.Web products have the smallest virus database among existing anti-viruses. Extremely flexible database descriptive language helped us make the database smaller, saving disk and memory and making frequent updates unnecessary. The compact database ensures rapid interaction between components of the anti-virus and low CPU load.

What is the most important thing about an anti-virus? Surely it should provide virus protection. Adding virus signatures to the database is essential to the process. However, there is no correlation between the number of entries in the database and the actual detection rate. To understand why there are fewer entries in the Dr.Web® virus database than in those of its competitors', it helps to remember that many viruses are not unique. There are whole families comprised of variations of one virus, and there are viruses created using a virus constructor utility. Some anti-virus developers create an entry for each viral twin in the virus database which adds to its bulk. A quite different approach is used for the Dr.Web® database where one entry can detect dozens or even hundreds of similar viruses.

Dr.Web Virus Database Benefits

- Record-small number of entries.
- Small updates.
- One entry added to Dr.Wb virus database provides detection of hundreds or even thousands of similar viruses.

The main difference between the Dr.Web virus database and databases of other anti-viruses is that with the smaller number of entries it enables detection of the same (or even greater) number of viruses.

Small Database with Smaller Number of Entries

- Lower disk usage.
- Lower memory usage.
- Lower updating traffic.
- Faster virus scan.
- Detection of future modifications of known viruses.

Virus monitoring service

- The Doctor Web virus monitoring service collects samples of malicious programs all over the Internet to create antidotes and release updates as soon as analyses are completed – as often as several times per hour.
- As soon as an update is released, users can retrieve it from several servers located at various points of the globe.
- To avoid false positives, an update is tested over a huge number of uninfected files before it is released.
- The intelligent system automatically adds entries for similar viruses into the database, ensuring the prompt neutralization of emerging threats.

Always up-to-date

- Updating over the Internet, whether automatically or according to a schedule, doesn't require user interference. Updating can also be launched manually.
- Updates are very small – just 50-200 KB, and it takes very little time to download them even if a slow Internet connection is used.
- Updating servers are always available.
- In most cases, there is no need to reboot the system to complete updating; Dr.Web starts using the updated modules and latest virus definitions right away.
- To save traffic, the anti-virus can be set to update virus databases only. However, enabling this option is not recommended. To counter the latest threats, Dr.Web undergoes constant refinement. New features are incorporated in the anti-virus package's updated modules and are downloaded from Doctor Web's server automatically during regular updating sessions. To protect a system from new malware, all components of an anti-virus must remain up-to-date.
- You can also reduce traffic by downloading updates as archived patch files. Patch files are used to deliver minor additions and fixes for virus database or program modules. The special compression algorithm applied to such patches dramatically reduces the amount of transferred data.

Dr.Web Enterprise Security Suite

Products for business

Dr.Web Enterprise Security Suite. Products for business

Dr.Web Enterprise Security Suite consists of a set of 5 Dr.Web products designed to protect all hosts in a corporate network and a single control center that facilitates the administration of many of the products.

Commercial product	Software product
Dr.Web Desktop Security Suite Protection of workstations, clients of terminal servers, clients of virtual servers, clients of embedded systems	Dr.Web for Windows
	Dr.Web KATANA
	Dr.Web for Linux
	Dr.Web for macOS
	Dr.Web for MS DOS
	Dr.Web for OS/2
Dr.Web Server Security Suite Protection of file storages and application servers (including terminal and virtual servers)	Dr.Web for Windows Servers
	Dr.Web for UNIX Server
	Dr.Web for Novell NetWare Server
	Dr.Web for macOS Server
Dr.Web Mail Security Suite Protection of e-mail	Dr.Web for UNIX Mail Server
	Dr.Web for MS Exchange
	Dr.Web for IBM Lotus Domino for Windows
	Dr.Web for IBM Lotus Domino for Linux
	Dr.Web for Kerio Mail Server (for Windows)
	Dr.Web for Kerio Mail Server (for Linux)
	Dr.Web for Kerio Mail Server (for macOS)
Dr.Web Gateway Security Suite Protection of gateways	Dr.Web for UNIX Internet Gateways
	Dr.Web for Internet Gateways Kerio
	Dr.Web for Microsoft ISA Server and Forefront TMG
	Dr.Web for MIMEsweeper
	Dr.Web for Qbik WinGate
Dr.Web Mobile Security Suite Protection of mobile devices	Dr.Web for Android
	Dr.Web for BlackBerry

Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite consists of a set of Dr.Web products designed to protect all hosts in a corporate network and a single Control center that facilitates the administration of many of the products.

Licensing

Products are licensed according to the type of objects needing protection. Simply select whatever basic license you need as well as any additional components you desire. For example, Anti-virus and Comprehensive protection are basic licenses for workstations, while the firewall is an additional component.

Protected objects	Supported OS and platforms	Basic license	Additional components
Dr.Web Desktop Security Suite **Workstations** **Terminal server clients** **Virtual server clients** **Embedded system clients**	Windows 10/8/8.1/7/Vista SP2/ XP SP2+ (32-bit systems). Windows 10/8/8.1/7/Vista SP2 (64-bit systems).	Comprehensive protection	■ Control center
		Anti-virus	
	Windows 10/8/8.1/7/Vista SP2/ XP SP2+ (32-bit systems). Windows 10/8/8.1/7/Vista SP2 (64-bit systems).	KATANA	■ Control center
	Linux glibc 2.7 and later	Anti-virus	■ Control center
	macOS 10.7 and later		
	MS-DOS OS/2		
Dr.Web Server Security Suite **File and application servers**	Windows	Anti-virus	■ Control center
	Novell NetWare		
	macOS Server		
	Unix (Samba)		
Dr.Web Mail Security Suite **E-mail users**	Unix	Anti-virus	■ Control center ■ Anti-spam ■ SMTP proxy
	MS Exchange		
	Lotus (Windows/Linux)		■ Anti-spam ■ SMTP proxy
	Kerio (Windows/Linux)		■ SMTP proxy
Dr.Web Gateway Security Suite **Gateway users**	Internet gateways Kerio (Windows/Linux) Internet gateways UNIX Qbik WinGate MIMEsweeper Microsoft ISA Server and Forefront TMG	Anti-virus	■ Control center ■ Anti-spam
Dr.Web Mobile Security Suite **Mobile devices**	Android OS 4.0–7.1	Comprehensive protection	■ Control center
	BlackBerry 10.3.2+		

Versatility

As a customer, you'll be given a single key file that will allow you to use a Dr.Web product to protect whatever objects you require for a desired platform. For example, a key file will let you choose between anti-virus protection for a UNIX file server and a Windows file server. If you change your platform from UNIX to Windows while your license is valid, you don't need to get a different key file. Instead you will be able to go to www.drweb.com to download and install free of charge a distribution file of the program you require.

Useful links

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

Dr.Web Enterprise Security Suite Control Center

Central administration of all host in your corporate network

Dr.Web Enterprise Security Suite Control Center provides centralized security administration for all hosts in the corporate network:

- workstations, terminal servers, virtual servers, clients of embedded system;
- file servers and application servers (including terminal servers and virtual servers);
- mail servers;
- gateways;
- mobile devices.

Advantages

- protection of all network hosts, devices and services.
- support of Windows and Unix server platform, simple installation procedure and reliable protection providing minimal TCO compared with competitive solutions.
- support of 32- and 64-bit operating systems.
- installation of agent software in an infected system with a high probability for successful curing.
- minimal consumption of system resources achieved through implementation of a small-sized engine featuring latest technologies.
- remote administration through Web interface of any Web-browser.
- mobile Control Center for Android/iOS-powered devices.
- implementation of individual security policies for a company and groups of employees at the company.
- several administrators can manage different groups separately, so the Control Centre can be put to good use by companies with high security requirements as well as by multi-branch organizations.
- configurable security policies for any type of users including mobile users and for any workstation even if it is currently unavailable ensure up-to-date protection at any time.
- protection of the solution's settings against modification by users.
- block access to removable data-storage devices, local network folders and the Internet — protection against accidental or deliberate harmful actions.
- protection for all networks that are isolated from the Internet.
- deploy agents on workstations in a convenient for an administrator way - using Active Directory policies, launch scripts the built-in remote installation procedure. Installation can still be performed even if the host is unreachable through the Web-administrator.
- support of a wide range of DBMSs including Oracle, PostgreSQL, Microsoft SQL Server or any other DBMS that supports SQL-92 over ODBC can be used as an external database.
- support of custom event handlers written in any script language providing direct access to internal interfaces of the Control Center.
- Dr.Web Enterprise Security Suite is an open solution allowing a system administrator to use it to install and synchronize products from other developers which also lowers information security system deployment costs.
- easy-to-understand protection control system and unsurpassed usability and efficiency of network stations search.
- customizable list of components of products to be updated and version upgrade control enable an administrator to distribute only updates that are necessary and have been tested in the network.

Dr.Web Desktop Security Suite

Protection of workstations, clients of terminal servers, clients of virtual servers, embedded system clients

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

Licensing of Dr.Web Desktop Security Suite

Types of licenses

- Per number of protected workstations.
- Per number of clients connected to the terminal server.
- Per number of clients connected to the virtual server.
- Per number of clients used in embedded systems.

Dr.Web Anti-virus for Windows is licensed separately or as a component of Dr.Web Enterprise Security Suite.

License options

	Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32-bit) Windows 10/8/8.1/7/Vista SP2 (64-bit)		Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32-bit) Windows 10/8/8.1/7/Vista SP2 (64-bit)	Linux	macOS	MS DOS, OS/2
Basic license	Comprehensive protection	Anti-virus	KATANA	Anti-virus		
Basic license components	■ Anti-virus ■ Anti-spy ■ Anti-rootkit ■ Anti-spam ■ HTTP-monitor ■ Office control ■ Firewall	■ Anti-virus ■ Anti-spy ■ Anti-rootkit ■ Firewall	■ Non-signature anti-virus ■ Dr.Web Cloud ■ Control Center	■ Anti-virus ■ Anti-spy	■ Anti-virus ■ Anti-spy ■ Anti-rootkit	■ Anti-virus ■ Anti-spy ■ Anti-rootkit
Additional components						
Control center	+	+	+*	+	+	–

* Only for Dr.Web KATANA BE.

Dr.Web Desktop Security Suite is also included in low-cost bundles for small and medium companies.

Supported OS

Dr.Web for Windows	Dr.Web for Linux	Dr.Web for macOS	Dr.Web console scanners
Anti-virus, Comprehensive protection: Windows 10/8/8.1/7 Vista SP2/XP SP2+ (32 bit) Windows 10/8/8.1/7 Vista SP2 (64 bit)	GNU/Linux for Intel x86/amd64 with kernel 2.6.37 (and later) and glibc 2.13 (and later)	macOS v.10.7 and higher (32&64-bit systems)	Windows, MS DOS, OS/2
KATANA: Windows 10/8/8.1/7 Vista SP2/XP SP2+ (32 bit) Windows 10/8/8.1/7 Vista SP2 (64 bit)			

Dr.Web for Windows

Protection of workstations, embedded system clients, terminal server clients and virtual server clients

Benefits

- **Comprehensive protection from existing threats**

  Dr.Web for Windows provides reliable protection from most existing threats. Its unsurpassed quality of curing and reliable self-protection capabilities leave no loophole for viruses and other malware to find their way into the protected environment. The built-in firewall and the office control help prevent viruses from exploiting the vulnerabilities of operating systems and applications and allow you to control the operation of installed programs.

- **Increased labour productivity**

  Deployment of Dr.Web for Windows provides a positive effect instantly. Because the product provides comprehensive protection, the inflow of spam is cut completely, resulting in a much more productive working environment —important messages no longer get lost in a hefty volume of spam e-mails. In addition, computers in the network are no longer at risk of getting infected, which eliminates downtimes due to virus attacks and subsequent necessary system restoration processes.

- **Upholding reputations**

  With Dr.Web for Windows standing guard, criminals can't turn your workstations, embedded system clients, and terminal server clients into sources of viruses and spam that could get onto your customers' computers. Dr.Web for Windows helps you safeguard your reputation as a trustworthy partner.

- **Flexible licensing**

  Unlike many competitive solutions, Dr.Web for Windows enjoys the most flexible multi-optional licensing (see the Licensing tab). Doctor Web lets customers buy only the components they need; customers are not made to pay for features they will never use.

- **Centralized administration**

  The Control Center, which allows workstation protection to be centrally administered, is included under a Dr.Web Enterprise Security Suite license. The Control Center is equally reliable in networks of any scale and structural complexity—from small workgroup networks to distributed intranets with tens of thousands of hosts. The Control Center also affords the centralized administration of anti-viruses for file servers and application servers, including terminal servers, under Windows and Novell NetWare, for UNIX mail servers, Microsoft Exchange, IBM Lotus, Kerio, and also for Dr.Web for mobile devices running Windows Mobile.

Key features

- Efficient detection and neutralization of all types of threats.
- Fast multi-thread scanning powered by multi-core systems.
- Protection from latest malicious programs designed to bypass detection by traditional signature-based scan and heuristic analysis.
- Protection of data against corruption.
- Comprehensive analysis of packed threats.
- Scan of archived files at any nesting level.
- Best detection and neutralization of complex viruses.
- Filters spam and other types of unsolicited messages without training the anti-spam.
- Real time scanning of traffic on all ports.
- With secure search, Google, Yandex, Yahoo!, Bing and Rambler will only return links to content considered safe by the search engines—unsafe content is filtered out by the search engines!
- Secure communication - instant messenger traffic filtering.
- Efficient protection of children against exposure to objectionable content
- Prevent unauthorized use of removable devices and the computer.
- Dr.Web Cloud - check URLs on Doctor Web's servers.
- Protects against unauthorized access by a network; prevents data leaks; blocks suspicious connections on package and application layers.
- Remote administration from other computers in the local network without installing the Dr.Web Control Center

System requirements

Supported OS

- Intel® Pentium® IV 1.6 GHz.
- 512 MB RAM. Temporary files created during installation will require additional disk space.
- At least 330MB of free disk space.
- Windows 2012/8/7/2008/Vista/2003/XP SP 2 (32&64 bit).

Useful links

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

Dr.Web Anti-virus for macOS

Basic protection from viruses and other malware targeting macOS and other operating systems

Advantages

- Reliable protection from all malicious programs.
- You can scan the system quickly with asynchronous scanning.
- The user-friendly Control Center available free of charge.
- Easily connects to the centralised corporate anti-virus protection system.
- Minimal consumption of resources in the protected system and low updating traffic make the Dr.Web for macOS's operation virtually invisible.
- User-friendly interface.

Features

- Centralized configuration of all components.
- Constant monitoring of all objects at risk of infection—removable media, email, files and directories, including packaged and archived data.
- Protection from unknown threats using the improved non-signature detection technology Origins Tracing™ and the intelligent heuristic analyser.
- With the unique FLY-CODE™ technology at its disposal, Dr.Web detects and removes malware disguised with unknown packers.
- Neutralizes viruses, Trojans and other malware.
- Comprehensive databases for detecting spyware, riskware, adware, hack tools, and jokers.
- SilDer Guard® file monitor is highly resistant to attempts by malicious programs to disrupt its operation.
- Settings of SpIDer Guard® are protected by password against unauthorized modification.
- Automatic, manual and scheduled scans.
- Three types of scanning: express, full and custom.
- Different actions can be performed with different types of objects; cure, move to the quarantine, delete; action sequences allow you to define which action will be applied to an object if the first action can't be performed.
- Scanning exceptions.
- **New in version 10!** Full HTTP traffic scanning and Internet access control.
- Quarantine to isolate infected files; quarantine storage time and maximum size can be specified.
- Curing, restoring and removal of quarantined objects.
- The anti-virus log contains time of each event, name of the scanned object and the type of action applied to the object.
- Automatic (scheduled) and on-demand updating.
- Virus notifications (that include event sounds) on viral events.
- Detailed operation log.
- Modules are available as command line utilities that can be used with Apple Scripts.

System requirements

- macOS 10.7 and higher (32&64 bit systems).
- Intel.
- RAM—as required by the OS.
- Internet access for registration and updating.

Useful links

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

Dr.Web Anti-virus for Linux

Basic anti-virus protection

Advantages

- Easy-to-use control center.
- Real-time protection.
- Custom scan.
- Manageable quarantine.
- User-friendly license manager.
- Control over the command line.
- Stylish interface.
- Full HTTP traffic scanning and Internet access control.
- Protection from Windows-specific threats launched under Linux.

Features

- Centralized configuration of all components.
- Constant monitoring of all objects at risk of infection—removable media, email, files and directories, including packaged and archived data.
- Protects against unknown threats using the improved non-signature detection technology Origins Tracing™ and an intelligent heuristic analyzer.
- With the unique FLY-CODE™ technology at its disposal, Dr.Web detects and removes malware disguised with unknown packers.
- Neutralizes viruses, Trojans and other malware.
- Comprehensive databases for detecting spyware, riskware, adware, hack tools, and jokers.
- The solution's architecture has been specifically designed to reduce CPU load and memory consumption.
- **New!** Install, configure and run the anti-virus via the command line.
- File monitor is highly resistant to attempts by malicious programs to disrupt its operation.
- **New!** Multi-thread scanning significantly improves performance in multi-core systems.
- Anti-virus scan modes include express, full and custom scan—the latter can be launched manually.
- **New!** Scan running processes to neutralise active threats including Windows malware for launched via Wine.
- Different actions can be performed with different types of objects; cure, move to the quarantine, delete; action sequences allow you to define which action will be applied to an object if the first action can't be performed.
- User-defined file and path exceptions.
- **New!** Full HTTP traffic scanning and Internet access control.
- The quarantine isolates infected files; quarantine storage time and maximum size can be customized.
- Curing, restoring and removal of quarantined objects.
- The anti-virus log contains time of each event, name of the scanned object and the type of action applied to the object.
- Automatic (scheduled) and on-demand updating.
- **New!** Apply configuration changes and add new key files on the fly.
- Virus notifications, including event sounds, for all viral events.
- The anti-virus modules are available as command prompt utilities which can be used independently.

And also:

- A good choice for an organisation with the highest security standards.

System requirements

- Operating system:GNU/Linux distributions supporting Intel x86/amd64 with kernel 2.6.37 (and later) and glibc 2.13 (and later).
- At least 512 xB of free disk space.
- Internet access for registration and updating.

Useful links

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

Dr.Web Console Scanners

Anti-virus protection for experienced users

Dr.Web console scanners incorporate the standard virus database and the Dr.Web scanner. They can be used under MS DOS, OS/2, and Windows. In order to make use of all of the console scanner's features, you need to know how to use the command line.

Advantages

- Minimum system requirements – scanners run smoothly even in embedded systems and provide reliable protection even for low-end machines.
- Scanning modes –administrators can choose between manual and scheduled scanning.
- Windows workstations and servers can be cured even if they can't be accessed over the network.
- High resistance to viruses; can be installed in infected systems.
- Automation of daily routines by means of a large number of options that can be defined using the command line.
- Guaranteed removal of unknown viruses including malware in archives of unknown formats.
- Launchable from removable media (e.g. CD or USB flash-drive).

Useful links

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

Dr.Web Server Security Suite

Protection of file storages and applications servers, including terminal servers and virtual servers

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

Licensing of Dr.Web Server Security Suite

Types of licenses

- Per number of protected servers.

License options

- Anti-virus.
- Anti-virus + Control center (except for Dr.Web for UNIX Server).

Dr.Web Server Security Suite can be purchased as a separate product or as a component of Dr.Web Enterprise Security Suite.

	Dr.Web for Windows Servers	Dr.Web for Novell NetWare Servers	Dr.Web for macOS Server	Dr.Web for UNIX Servers
Basic license	Anti-virus	Anti-virus	Anti-virus	Anti-virus
Additional components				
Control center	+	+	+	+

Dr.Web Server Security Suite is also included in low-cost bundles for small and medium companies.

Supported OS

Dr.Web for Windows Servers	Dr.Web for Novell NetWare Servers	Dr.Web for macOS Server	Dr.Web for UNIX Servers
Windows Server 2000* / 2003 (x32 and x64*) / 2008 / 2012 (x64)	Novell NetWare v. 4.11–6.5 with installed additions from Minimum patch list	macOS Server 10.7 and higher	Linux distributions with kernel version 2.6.x (32- and 64-bit systems)

* Only for version 7.0.

Dr.Web for Windows Servers

Anti-virus protection for Windows servers

Advantages

- High performance and stability.
- High-speed scanning combined with low consumption of system resources allows Dr.Web to run smoothly on any server hardware.
- Trouble-free automatic operation.
- The delayed scan technology applied to files opened for reading provides flexible load balancing for a server file system.
- Flexible client-oriented configuration of scanning and actions performed with detected viruses or suspicious files.
- Simple installation and administration.
- Sound protection immediately after installation (with default settings).
- Transparent operation – detailed logs with customizable verbosity.

Key features

- On-demand and scheduled scanning of server volumes.
- On-the-fly scanning of all files transferred via the server.
- On-demand scan.
- Scheduled scan.
- Heuristic virus scan.
- Scan of packed and archived files.
- Notifications upon detection of infected objects.
- Anti-virus administration from the server console or a remote console: configure the notification system, monitor protection, and optimize configurations.
- Scanning statistics displaying process operational time, number of scanned files, and information about detected viruses.
- Multi-thread scan.
- Automatic disconnection of workstations from the server if they become threat sources.
- Customizable notifications.
- Instant notifications for the administrators and their groups.
- Isolation of infected or suspicious files in the quarantine.
- Curing, and removal or moving of infected objects to the quarantine.
- Anti-virus actions log.
- Automatic updating of virus databases.
- Smart optimisation takes into account available system resources.
- Dr.Web Cloud – immediate response to the latest threats*.
- Proactive protection against unknown threats by prohibiting modification of critical Windows objects and controlling unsafe actions*.

System requirements

- Processor: support of i686 and higher.
- Operating system: Microsoft Windows Server 2000**/ 2003 (x32 and x64**) / 2008 / 2012 (x64)
- Hard disk space: at least 512 MB.

Useful links

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

* Available for Windows Server 2008 and above.

** Only for version 7.0.

Dr.Web for Novell NetWare

Anti-virus protection of file servers

Advantages

- Widest range of supported versions of Novell Netware – from 4.11 up to 6.5.
- Support of NetWare namespace.
- Simultaneous support of several network protocols.
- High-speed scanning of huge amounts of data at minimum consumption of system resources both real-time and on demand.
- Manageable consumption of CPU resources by adjusting the priority of the scanning process.
- Simple installation procedure.
- Flexible client-oriented configuration of scanning and actions performed with detected viruses or suspicious files.
- User control panel.

Key features

- On-demand and scheduled scanning of server volumes.
- On-the-fly scanning of all files transferred via the server.
- Multi-thread scan.
- Automatic disconnection of workstations from the server if they become threat sources.
- On-demand scan.
- Scheduled scan.
- Scanning of files by format or using the list of extensions, directories, and volumes exceptions, scanning of all objects.
- Heuristic virus scan.
- Scan of packed, archived, and mail files.
- Scan logging; adjustable logging verbosity.
- Notifications upon detection of infected objects.
- Curing, and removal or moving of infected objects to the quarantine.
- Anti-virus administration from the server console or a remote console: configure the notification system, monitor protection, and optimize configurations.
- Instant notifications for the administrators and their groups over – mail.
- Customizable notifications.
- Scanning statistics displaying process operational time, number of scanned files, and information about detected viruses.
- Anti-virus actions log.
- Automatic updating of virus databases.

System requirements

- Novell NetWare v.4.11-6.5

Useful links

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

Dr.Web for macOS Server

Anti-virus protection of workstations operated by macOS server versions

Advantages

- Easy-to-use control center.
- High scanning speed.
- Custom scanning profiles.
- Reliable real-time protection.
- Minimal consumption of system resources.
- Low updating traffic.
- Flexible configuration.
- Stylish and user-friendly interface.

Key features

- Scan of autorun objects; removable data storage devices; network and logical drives; e-mails; files; and directories, including archives.
- Three types of scanning: express, full, and custom.
- Automatic, manual, and scheduled scan.
- Settings of SpIDer Guard® are password protected against unauthorized modification.
- Different actions can be performed with different types of objects: cure, move to the quarantine, delete; action sequences allow you to define which action will be applied to an object if the first action can't be performed.
- User-defined file and path exclusions.
- Detection and neutralization of viruses disguised with unknown packers.
- The anti-virus log contains the time of each event, the name of the scanned object, and the type of action applied to the object.
- Automatic (scheduled) and on-demand updating.
- Virus notifications, including event sounds, for all viral events.
- Quarantine to isolate infected files; quarantine storage time and maximum size can be specified. Curing, restoring, and removal of quarantined objects.
- Detailed operation log.
- Modules are available as command line utilities that can be used with Apple Scripts.

System requirements

- macOS Server 10.7 or higher.
- Intel.
- RAM—as required by the OS.

Useful links

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

Dr.Web for UNIX Server

Anti-virus protection for Unix file servers

Advantages

- High performance and stability.
- High-speed scanning combined with low consumption of system resources allows Dr.Web to run smoothly on any server hardware.
- Flexible, client-oriented configuration of scanning and actions performed with detected viruses or suspicious files.
- Perfect compatibility – the anti-virus doesn't conflict with any known firewall or file monitor.
- Supports monitoring software (Cacti, Zabbix, Munin, Nagios, etc.)
- Easy administration, simple installation, and configuration.

Key features

- On-demand and scheduled scanning of server volumes.
- Improved! On-the-fly scan –checks files for viruses as they are about to be written or opened.
- Multi-thread scan.
- Automatic disconnection of workstations from the server as soon as they've been identified as threat sources.
- Instant notifications for the administrators and their groups via e-mail, short messages sent to a phone, or pager.
- Improved! Isolation of infected files in the quarantine.
- Curing, restoration, and removal of quarantined objects.
- Anti-virus actions log.
- Automatic updating of virus databases.

System requirements

- Dr.Web Daemon (drwebd) atleast v.5.0 or higher.
- Samba 3.0 or higher.

Supported OS

- GNU/Linux (kernel 2.6.37 and later and glibc 2.13 and later);
- FreeBSD;
- Solaris — Intel x86/amd64 only
- The operating system should run Samba 3.0 or later and use PAM authentication.
- If you use a 64-bit operating system version, it must be able to run 32-bit applications.
- Free disk space:
  At least 1 GB
- The software has been tested under the following OS distributions: 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), and Solaris (10 u11).

Useful links

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

Dr.Web Mail Security Suite

Protection of e-mail

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

Licensing of Dr.Web Mail Security Suite

Types of licenses

- Per number of protected users.
- Per server license –unlimited scanning of server e-mail traffic for as many as 3,000 protected users.

Dr.Web Mail Security Suite can be purchased as a separate product or as a component of Dr.Web Enterprise Security Suite. In the latter case the license also covers the Control Center of Dr.Web Enterprise Security Suite and Anti-spam (except for Kerio).

A Dr.Web Mail Security Suite license may also include the SMTP proxy as an additional component. Using these products together improves overall network security and reduces the workload of local mail servers and workstations.

License options

	Dr.Web for MS Exchange	Dr.Web for IBM Lotus Domino	Dr.Web for UNIX Mail Server	Dr.Web for Kerio Mail Server
Basic license	Anti-virus	Anti-virus	Anti-virus	Anti-virus
Additional components				
Anti-spam	+	+	+	–
SMTP proxy	+	+	+	+
Control center	+	+	+	+

Dr.Web Mail Security Suite is also included in low-cost bundles for small and medium companies.

Supported OS

Product	Windows	Linux	macOS	FreeBSD	Solaris
Dr.Web for UNIX Mail Servers		v. 2.4.x and higher		v. 6.x and higher	v. 10
Dr.Web for MS Exchange	Server2000/2003/ 2008/2012				
Dr.Web for IBM Lotus Domino	Server 2000/2003/ 2008/2008 R2/ 2012/2012 R2 (32&63 bit systems)	Red Hat Enterprise Linux (RHEL) v.v. 4 and 5, Novell SuSE Linux Enterprise Server (SLES) v.v. 9 and 10 (32 bit only)			
Dr.Web for Kerio Mail Server	2000/XP/ Vista/7, Server 2003/2008/2012	Red Hat 9.0; Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0, 11.1; CentOS Linux 5.2, 5.3; Debian 5.0; Ubuntu 8.04 LTS	macOS 10.7 and higher		

Dr.Web for UNIX Mail Servers

Highly intelligent anti-virus and anti-spam protection system for large amounts of e-mail traffic

Advantages

- Flexible configuration.
- Simple administration.
- Low system requirements.
- Minimal TCO.
- Perfect scalability.
- Rapid response.
- Efficient filtering of unsolicited e-mails.
- Enhanced security for corporate mail.
- Protection of confidential information.
- Open solution.
- Unlimited number of plugins.

Key features

- Filtering of e-mail for viruses and spam.
- Parsing of e-mails and analysis of every component of an e-mail.
- Correct scan of most types of archives, including multi volume and self-extracting (SFX).
- White/Blacklists.
- Customizable notifications.
- Statistical reports.
- Self protection.

Flexible configuration

Dr.Web for UNIX Mail Servers can be configured using rules providing greater flexibility compared with competitive solutions that can only be set up using static parameters in configuration files. Messages are filtered and modified according to established policies where the administrator can configure individual processing rules for different users and groups and even for each e-mail. It allows the product to meet any requirements to corporate security.

Simple administration

Though rich in features, Dr.Web for UNIX Mail Servers doesn't require a lot of configuration work before you start using it. Moreover, it is also available in the Dr.Web Office Shield appliance that fully complies with the plug and forget principle.

Low system requirements

The system requirements of Dr.Web for UNIX Mail Servers are very low allowing it to run on any server hardware. It makes the anti-virus a perfect choice for companies that can't afford modernizing their server hardware on a regular basis to meet ever growing requirements of most anti-virus solutions.

Minimal TCO

Unlike many competitive solutions Dr.Web for UNIX Mail Servers enjoys the most flexible multi-optional licensing. A customer buys only components they need and doesn't pay for software they don't need and will never use.

Perfect scalability

Dr.Web for UNIX Mail Servers meets demands of small companies using one mail server as well as requirements of multi-national telecom providers for scan of huge amounts of data. Capabilities for processing huge amounts of data real-time, reliability and flexibility.

Rapid response

Multi-thread scanning ensures rapid response of the anti-virus allowing it to scan arriving data real-time along with files received earlier and to deliver e-mails to end-users without a notable delay.

Efficient filtering of unsolicited e-mails

Dr.Web anti-spam is shipped as a solution component (but never as a separate product). It is installed on the server where the anti-virus product resides. It simplifies administration of the solution and lowers its TCO compared with competitive solutions.

Advantages of Dr.Web anti-spam

- The anti-spam doesn't require configuration or training. Unlike anti-spam solutions based on Bayesian filtering, it starts working as soon as the first message arrives.
- It detects spam messages regardless of their language.
- Customizable actions for different categories of spam.
- The white and black lists of its own rule out a possibility for a company to be discredited by adding it deliberately to lists of unwanted addresses.
- Record-low number of false positives.
- Stays relevant with one update in 24 hours – unique spam detection technologies based on several thousands of rules allow the anti-spam to stay up to date without frequent downloads of bulky updates.

Enhanced security for corporate mail

The modular structure of Dr.Web for UNIX Mail Servers allows integrating the product with various mail systems or using it as an SMTP proxy —a filter processing e-mails before they are received by the mail server. Simultaneous use of Dr.Web for UNIX Mail Servers and an additional SMTP proxy component provides:

- Better overall network security.
- Improved filtering quality with no limitations caused by a mail server.
- Lower workload of local mail servers and workstations.
- Greater stability of the mail filtering system.

Protection of confidential information

The quarantine managed over the web-interface or by means of a special utility and the option for archiving all e-mails transferred through the filter allow tracking causes of data leaks and restoring messages accidentally deleted by users from their mail boxes.

Open solution

Dr.Web for UNIX Mail Servers can be integrated with solutions from other developers. With the open API users can also add new features to the product.

Unlimited number of plugins

New features for protection of e-mail can be added to the product without any limitations so that any written plugin will immediately work with all supported MTA.

Implmented plugins:

- Dr.Web – anti-virus scan of e-mails by the Dr.Web engine.
- vaderetro – spam filtering plugin.
- headersfilter – plugin filtering e-mails by headers.

Supported OS

- Linux v.2.4.x and higher.
- FreeBSD v. 6.x and higher for Intel x86 and amd64
- Solaris v. 10 for Intel x86 and amd64.

Dr.Web SMTP proxy

This is a component of Dr.Web for UNIX Mail Server. It can be installed in the demilitarized zone (DMZ) or integrated with an existing mail system. With the mail scanning server placed in the demilitarized zone, a mail server is not connected to the Internet directly. In this case, even if a hacker succeeds in compromising the server, he won't get access to sensitive company information. The solution performs a full scan of SMTP/LMTP mail traffic.

Advantages

- Improved filtering quality with no limitations caused by a mail server.
- Decreased workload for internal mail servers, content filtering servers, mail and Internet gateways, and workstations.
- Increased stability of mail scanning and better overall network security.

Protection from spammer attacks – an administrator can restrict parameters of the SMTP-session to prevent spammer attacks.

Protection from disguised spam – with the IP validation feature, your company is protected from spam messages sent with forged sender IP addresses.

Protection from hacker attacks – the product can withstand passive attacks such as PLAIN and LOGIN, as well as active non-dictionary attacks.

Protection from spam traps – Dr.Web for UNIX Mail Gateways can check whether the recipient address is a spam trap.

Correct processing of malformed e-mails – the product can block messages with an empty sender field but correctly processes messages that violate standards due to malforming by certain mail clients.

Reduction of Internet traffic – Dr.Web for UNIX Mail Gateways allows the size of mail attachments to be restricted.

Open Relay servers with limited relay list – if a company needs to use an open mail relay server, Dr.Web for UNIX Mail Gateways will help an administrator restrict the list of domains to which the server will relay messages.

Useful links

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

Dr.Web for MS Exchange

Anti-virus and anti-spam protection of mail traffic directed through MS Exchange 2000/2003/2007/2013/2016 servers

Advantages

- Compliance with the highest security standards – the product is certified by Russia's Federal Security Service (FSB) and Federal Service for Technological and Export Control (FSTEC).
- Wide range of installation and configuration options that meet the requirements of almost any company.
- High-speed scanning combined with low consumption of system resources allows Dr.Web to run smoothly on any server hardware.
- The built-in anti-spam doesn't require training, lowers server workload and improves employee productivity.
- Filtering based on black and white lists allows certain addresses to be excluded from scanning and efficiency to be increased.
- Filtering of files by type, contributing to lower traffic.
- Grouping allows different filtering parameters to be specified for different groups of employees which contributes to faster deployment and easier maintenance.
- High performance and stability achieved with multi-thread scanning.
- Detection and neutralization of viruses disguised with unknown packers.
- Automatic launch on system start-up.
- Easy-to-use updating system using Windows Task Scheduler.

Key features

- On-the-fly anti-virus and anti-spam scan of e-mails, including attached files.
- Anti-virus monitoring of user mailboxes and public directories.
- Anti-virus protection of mail traffic passing through the MS Exchange server.
- Curing of infected files.
- Grouping users by means of Active Directory.
- Adjustable scanning parameters: the maximum size and types of objects to be scanned objects, actions to be performed with infected objects.
- Detection of malicious objects compressed with multiple packers.
- Customizable actions performed with different types of spam, including moving messages to the quarantine or adding a specified prefix into their subject fields.
- Customizable wording inserted in outgoing e-mails.
- Isolation of infected and suspicious files in the quarantine.
- Sending notifications on virus incidents to administrators and other users.
- Operation logging.
- Automatic updates.

System requirements

- Processor
  For Microsoft Exchange Server 2000/2003: Pentium 133 MHz, recommended – Pentium 733 MHz.
  For Microsoft Exchange Server 2007/2010/2013/2016: Intel x64 supporting Intel 64; AMD supporting AMD64.RAM
  For Microsoft Exchange Server 2000/2003: 512 xB and more.
  For Microsoft Exchange Server 2007/2010: 2GB and more.
  For Microsoft Exchange Server 2013/2016: 4GB and more.Free disk space
  For Microsoft Exchange Server 2000/2003/2007/2010: 512 MB.
  For Microsoft Exchange Server 2013: 1 GB.

Supported OS

- For Microsoft Exchange Server 2000/2003: Microsoft® Windows® 2000 SP4, Microsoft® Windows Server® 2003 SP1 or higher.
  For Microsoft Exchange Server 2007/2010: Microsoft® Windows Server® 2003 R2 SP2 x64/2008 x64/2008 R2.
  For Microsoft Exchange Server 2013/2016: Microsoft® Windows Server® 2012/2008 R2.

Useful links

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

Dr.Web for IBM Lotus Domino

Anti-virus and anti-spam protection of IBM Lotus Domino under Windows and Linux

Advantages

- **Minimal TCO**

  Dr.Web for IBM Lotus Domino can run on a standalone server as well as on a partitions server or in Lotus Domino clusters. Copies of the anti-virus on different partitions run as separate processes in the RAM but use one database and the same executables. In this case, only one copy is subject to licensing which makes operation more flexible and lowers anti-virus protection costs.

- **Licenses and certificates**

  Dr.Web for IBM Lotus Domino complies with the highest security standards – the product is certified by Russia's Federal Security Service (FSB) and Federal Service for Technological and Export Control (FSTEC).

- **Ready for IBM Lotus**

  Dr.Web for IBM Lotus Domino has the Ready for IBM Lotus software mark and is included in the IBM Lotus Business Solutions Catalogue. The mark confirms the compatibility of Dr.Web for IBM Lotus Domino with Lotus Domino and its compliance with all IBM compatibility requirements.

- **Exceptional resistance to viruses**

  Dr.Web can be installed on an infected Lotus Domino server and is capable of curing it without resorting to any additional utilities. All databases can be scanned on demand right after the installation. To ensure maximum scanning efficiency, you can update virus databases prior to the virus check and use the latest virus definitions for scanning.

- **High-speed scan**

  The efficient organization of Dr.Web for IBM Lotus Domino, a special scanning algorithm, and flexible administration of the scanning process provide high-speed and resource-efficient scanning. The multi-thread scan enables the anti-virus to process simultaneously huge amounts of data. This advantage allows Dr.Web to run smoothly on virtually any server hardware.

- **Simple installation and flexible configuration**

  The deployment of Dr.Web for IBM Lotus Domino can be automated and easily controlled using administration scripts and detailed documentation. With the web interface, an administrator can use any browser (Internet Explorer, Firefox, and Opera) to control anti-virus operation. Dr.Web for IBM Lotus Domino provides a system administrator with abundant tools for flexible configuration of anti-virus actions performed after scanning a message scan and for sending notifications to a sender, recipient and system administrator upon detection of viruses, store headers of received messages and attachments.

- **Easy administration**

  Grouping allows different filtering parameters to be specified for different groups of employees, which contributes to faster deployment and easier maintenance. The same settings can also be specified for several groups by editing a corresponding profile.

- **Efficient filtering of junk mail without training**

  The built-in anti-spam lowers server workload and improves employee productivity. Filtering based on black and white lists allows certain addresses to be excluded from scanning, boosting efficiency.

Key features

- Scanning of all components of e-mails for viruses and spam, and filtering of spam real-time or as scheduled by an administrator.
- Filtering of spam including filtering of messages according to black and white lists.
- Anti-virus scan of documents in specified nsf bases.
- The manual scanner jobs launch-and-stop feature provides on-demand scanning of objects.
- Parsing of e-mails for further analysis.
- Curing of infected messages and their attached files.
- Detection of malicious objects compressed with multiple archivers.
- Detection and neutralization of viruses disguised with unknown packers.
- Additional technology that can detect unknown threats increases the likelihood that the newest species of malware will be detected.
- Storage of infected and suspicious objects in the quarantine (accessed with Lotus Notes).
- Reports are generated using templates that are easy to read.
- Operation logging.
- Protection of its own modules from failures.
- Automatic updates.

Supported OS

Version for Windows

- OS: Windows Server 2000/2003/2008/2008R2/2012/2012 R2 (32- and 64-bit); Lotus Domino v. R6.0 or higher (32- and 64-bit); CPU Pentium 133 and higher; RAM 128 MB (512 MB recommended); Free disk space: 128 MB.

Version for Linux

- OS: Red Hat Enterprise Linux (RHEL) v. 4 and 5, Novell SuSE Linux Enterprise Server (SLES) v. 9 and 10 (32-bit only); Lotus Domino v. 7.x or 8.x.; Lotus Notes 6.5 (or later) for Windows.
  CPU Pentium 133 and higher.
  RAM 64 MB (128 MB recommended).
  Free disk space: 90 MB.

Useful links

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

Dr.Web for Kerio Mail Servers

Anti-virus scan of messages and their attachments sent via SMTP and POP3

Advantages

- Perfect compatibility with Kerio mail servers tested by Kerio Technologies.
- Minimal message delivery time achieved through multi-thread scanning.
- Low system requirements and minimal use of local traffic.
- Flexible, user-friendly configuration system: customizable list of scanned objects and actions performed with detected viruses or suspicious files.
- Customizable actions for files that can't be scanned.
- Maintenance and configuration from Kerio mail server administration console.

Key features

- The anti-virus connects to the Kerio Mail Server and scans attached files and incoming and outgoing messages.

Supported OS

Version for Windows

- Hard disk space: at least 350 MB.
- OS: Microsoft Windows 2000, SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008/2013 (32- and 64-bit versions)
- Mail server: Kerio MailServer 6.2 or higher, Kerio Connect 7.0.0 or higher.

Version for Linux

- Hard disk space: at least 290 MB.
- OS: 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.
- Mail server: Kerio MailServer 6.2 or higher, Kerio Connect 7.0.0 or higher.

Version for macOS

- Hard drive space: at least 55 MB.
- Operating system: macOS 10.6 Snow Leopard, macOS 10.5 Leopard, macOS 10.4 Tiger.
- Mail server: Kerio MailServer 6.2 or later, Kerio Connect 7.0.0 or later.

Useful links

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

Dr.Web Gateway Security Suite

Protection of gateways

- Dr.Web for UNIX gateways
- Dr.Web for Kerio gateways
- Dr.Web for Microsoft ISA Server and Forefront TMG
- Dr.Web for MIMEswepper
- Dr.Web for Qbik WinGate

Licensing of Dr.Web Gateway Security Suite

Types of licenses

- Per number of protected users.
- Per server license –unlimited scanning of server e-mail traffic for as many as 3,000 protected users.

Dr.Web Gateway Security Suite can be purchased as a separate product or as a component of Dr.Web Enterprise Security Suite

License options

	Dr.Web for UNIX gateways	Dr.Web for Kerio gateways	Dr.Web for Microsoft ISA Server and Forefront TMG	Dr.Web for MIMEsweeper	Dr.Web for Qbik WinGate
Basic license	Anti-virus	Anti-virus	Anti-virus	Anti-virus	Anti-virus
Additional components					
Anti-spam	–	–	+	+	+
Control center	–	+	–	–	–

Dr.Web Gateway Security Suite is also included in low-cost bundles for small and medium companies.

Supported OS

Product	Windows	Linux	FreeBSD	Solaris
Dr.Web for UNIX Gateways		v. 2.4.x and higher	v. 6.x and higher	v. 10
Dr.Web for Kerio Gateways	2000/XP/2003/2008/7			
Dr.Web for Microsoft ISA Server and Forefront TMG	**For Microsoft ISA Server:** Microsoft® Windows Server® 2003 x86 Service Pack 1 (SP1); Microsoft® Windows Server® 2003 R2 x86 **For Microsoft Forefront TMG:** Microsoft® Windows Server® 2008 SP2 Microsoft® Windows Server® 2008 R2			
Dr.Web for MIMEsweeper	2000 Server SP4 or higher Server 2003 or higher			
Dr.Web for Qbik WinGate	Vista/Server 2008/Server 2003/XP/2000 (32- and 64-bit systems)			

Dr.Web for Internet Gateways UNIX

Anti-virus scan of the HTTP and FTP traffic on a corporate Internet gateway — proxy-server

Advantages

- A wide range of options for establishing comprehensive protection from threats lurking in inbound Web traffic.
- Delivery of virus-free content into the protected network.
- Efficient filtering of traffic by the ICAP server doesn't delay content delivery.
- Protection from penetration of the defence by any type of malware.
- High scalability.
- Ability to process huge amounts of data in real-time.
- Substantial reduction of Internet costs.
- Perfect compatibility – integration with any application supporting ICAP, with all known firewalls.
- Support of virtually all UNIX-based operating systems currently in use.
- Low system requirements allow the product to run smoothly on any server hardware.
- Flexibility and easy administration; the product lets you implement protection configurations that are in compliance with your company's security policies.

Key features

- Anti-virus scan of HTTP and FTP traffic.
- Centralized administration over the Dr.Web Enterprise Security Suite Control Center's Web administrator.
- Filtering by host name, MIME type, or file size.
- Web resources access control.
- Preview technology for optimized traffic scanning.
- Support of IPv4 and IPv6.
- Application of various actions to different types of scanned files.
- Isolation of infected files in the quarantine.
- Easy-to-read reports.
- Centralized administration of protection servers and collection of reports from the servers.
- Simultaneous processing of several requests per individual connection.
- Protection from unauthorized access.
- Monitoring of the system's operation and automatic restoration after a failure.
- User notifications about the presence of viruses or malicious codes in web pages.

Supported OS

- Linux with kernel 2.4.x and higher.
- FreeBSD 6.x and later (Intel x86 and amd64).
- Solaris 10 (Intel x86 and amd64).

Any proxy server with the full support of ICAP such as:

- Squid at least 3.0.
- SafeSquid at least 3.0.

Useful links

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

Dr.Web for Internet Gateways Kerio

Anti-virus scan of HTTP, FTP, SMTP, POP3 and Kerio Clientless SSL VPN traffic

Advantages

- Reliable protection of Internet connections for home users and businesses of any type and size.
- Easy administration – receive notifications on all virus events via e-mail or short messages.
- Minimal message delivery time is achieved through multi-thread scanning.

Key features

- Detection of malicious objects transferred with HTTP, FTP, SMTP, POP3 and Kerio Clientless SSL VPN traffic.
- Detection of infected e-mail attachments before they are processed by a mail server.
- Customizable list of data transfer protocols for scanning.
- Adjustable scanning parameters: maximum size and types of objects to be scanned, actions to be performed with infected objects.
- Actions undertaken to neutralize a threat are performed according to Kerio settings.
- Enabling/disabling detection of selected types of malicious programs.
- Logging errors and events in the Event Log and in the text log; the log contains information about module parameters, notifications about viruses detected in each infected message.
- Automatic updating of virus databases.

System requirements

- Version for Windows
  At least 350 MB of free disk space.
  Microsoft® Windows 2000. SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (32- and 64-bit versions)
  Firewall: Kerio WinRoute Firewall 6.2 or higher;
  Kerio Control 7.0.0 or higher
- Version for Kerio Control VMware Virtual Appliance and Kerio Control Software Appliance
  At least 290 MB of free disk space
  OS: Kerio Control VMware Virtual Appliance or Kerio Control Software Appliance
  Firewall: Kerio Control 8.x or higher

Useful links

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

Dr.Web for Microsoft ISA Server and Forefront TMG

Advantages

- Wide range of options for installing and fine-setup.
- Possibility to work on servers of any configuration – including with less RAM.
- Protection of real and virtual servers.
- High scan speed of traffic with minimum load on the OS by using multi-threaded scanning technology and dynamic analysis of the necessary resources.
- The built-in anti-spam doesn't require training (starts to work from the installation), reduces server workload and improves employee productivity.
- Reduced risk of infection from malicious resources and reduced traffic due to the blocking of access to various Internet resources and filtering of traffic by file types.
- Detection and neutralization of unknown packers and viruses.
- Easy updates system.
- Technical support in English.

Key features

Centralized product management is possible from any computer The management is done through your browser over a secure HTTPS protocol and does not require installation of additional software.

Anti-virus

- Anti-virus scan of HTTP/FTP over HTTP traffic, including attachments;
- **New!** Support for cluster solutions. Dr.Web for Microsoft ISA Server and Forefront TMG allows you to combine the servers on which Microsoft firewalls are installed in a single cluster (the tree of master and slave servers) and manage the entire system from one server;
- **New!** Application control. In case of an error in the application Dr.Web SSM restarts it, or reloads it;
- Scan with defined parameters: the choice of max size and types of scanned objects, actions (including the files that cannot be checked) and also the ways of processing of infected objects;
- Detection of malicious objects compressed with multiple packers;
- Curing infected files;
- Disabling of access to infected data for all local network users;
- Restricting of access to on-line resources with Office Control for users;
- Applying of different actions depending on the type of spam;
- Isolation of infected and suspicious files in the quarantine;
- Notifications on virus incidents to administrators and other users;
- System's operation logging.

Attention! Dr.Web for Microsoft ISA Server and Forefront TMG has higher scan speed of HTTP-packages and links in comparison with the anti-spam version.

Anti-virus + Anti-spam

Additions to the anti-virus functions.

- Anti-spam filtering of e-mail traffic on SMTP/POP3.
- Creating user groups and assigning profiles of anti-virus protection to them.
- Adding the attached text to email messages that contain threats.

System requirements

Hardware requirements

Characteristic	Requirement	
	For Microsoft ISA Server	For Microsoft Forefront TMG
CPU	CPU Pentium® III 733 MHz or higher	CPU Pentium® III 1.86 GHz or higher
RAM	1 GB or more	2 GB or more
Free disk space	350 MB for installation. Additional required free disk space necessary for the data storage during scanning.	300 MB for installation. Additional required free disk space necessary for the data storage during scanning.
Display	VGA-compatible	

OS and software requirements

Characteristic	Requirement	
	For Microsoft ISA Server	For Microsoft Forefront TMG
CPU	CPU Pentium® III 733 MHz or higher	CPU Pentium® III 1.86 GHz or higher
OS	One of the listed below: ■ Microsoft® Windows Server® 2003 x86 with Service Pack 1 (SP1); ■ Microsoft® Windows Server® 2003 R2 x86	One of the listed below: ■ Microsoft® Windows Server® 2008 SP2. ■ Microsoft® Windows Server® 2008 R2
File system	NTFS	NTFS
Proxy server	Microsoft® ISA Server 2004 Microsoft® ISA Server 2006	Microsoft® Forefront® TMG 2010
Other software	Microsoft Windows Installer 3.1 or higher Microsoft. NET Framework 3.5 SP1 Internet Explorer 6 and above or Mozilla FireFox 3 or higher	

Useful links

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

Dr.Web for MIMEsweeper

Anti-virus and anti-spam protection of mail traffic directed through a ClearSwift MIMEsweeper content filtering server

Advantages

- **Easy installation and configuration**

  The scenario wizard of Dr.Web for MIMEsweeper allows the most up-to-date filtering scenarios to be created automatically (Type 1 in the ClearSwift classification system).

- **Flexible configuration**

  When the plugin detects an infected object, it attempts to cure it or removes it if curing hasn't been enabled. If an e-mail has several files attached (even if archived), the plugin will disarm only infected attachments. If malicious code is found in the message body, the message will be moved to the quarantine. Clean messages and attachments are directed to a recipient unchanged. Messages that can't be disarmed by the Dr.Web plugin are marked as infected and go to the quarantine.

- **DEP compatibility**

  Dr.Web for MIMEsweeper supports Data Execution Prevention (DEP) which lets additional checks of RAM to be run and prevents the execution of malicious code. A user doesn't need to change DEP settings, which in turn prevents malware from using Windows' exception processing mechanism.

Key features

- Checks e-mails including archived attachments before they are processed by a mail server.
- Cures infected objects.

- Isolates infected and suspicious files in the quarantine.
- Filters spam; filters messages according to black and white lists.
- Operation logging.
- Automatic updates.

System requirements

- Windows 2000 Server (SP4) or higher.
- Windows Server 2003 or higher.

Useful links

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

Dr.Web for Qbik WinGate

Anti-virus and anti-spam scan of HTTP/POP3/FTP traffic of an SMTP and proxy server Qbik WinGate

Advantages

- Unlike other products for Qbik WinGate, Dr.Web has anti-spam filter. The anti-spam doesn't require configuration or training; it starts working as soon as the first message arrives, so the anti-spam doesn't require daily training by the system administrator.
- The cutting-edge non-signature scan technology Origins Tracing™ provides a high probability of detection of viruses unknown to Dr.Web, even in archives.

Key features

- Anti-virus and anti-spam scanning of messages and their attachments sent via SMTP and POP3.
- Anti-virus scanning of files and data transferred over HTTP and FTP.
- Curing of infected files transferred over HTTP.
- Customizable list of data transfer protocols for scanning.
- Adjustable scanning parameters, e.g. the maximum size and types of objects to be scanned and the actions to be performed with infected objects.
- Enabling/disabling detection of particular types of malicious programs; when a threat is detected, Qbik's settings determine what action is to be taken to neutralize it.
- Customizable actions for files that cannot be scanned.
- Detection of malicious objects compressed with various packers.
- The compact and efficient anti-spam module sets Dr.Web for Qbik WinGate apart from its competitors.
- The anti-spam requires no training and allows you to set different actions for different categories of spam, and to create white and black e-mail lists.
- Customizable actions performed with different types of objects, e.g. including moving them to the quarantine or adding specific prefixes into their subject fields.
- Log of errors and events in the Event Log, which contains information about module parameters, as well as notifications about viruses detected in infected messages and individual outbreaks.
- Isolation of infected files in either the Dr.Web quarantine or the WinGate quarantine.
- Viewing contents of the quarantine and then restoring and/or forwarding quarantined files.
- Back up of cured files in the quarantine.
- Features native control panel and quarantine manager.
- Automatic updating.

Useful links

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

Dr.Web Mobile Security Suite

Protection of mobile devices

- Dr.Web for Android
- Dr.Web for BlackBerry

Licensing of Dr.Web Mobile Security Suite

Dr.Web Mobile Security Suite is licensed per number of protected devices.

License options

Dr.Web for Android	Dr.Web for BlackBerry
■ Comprehensive protection + Control center	■ Comprehensive protection

Dr.Web Mobile Security Suite is also included in low-cost bundles for small and medium companies.

	Dr.Web for Android	Dr.Web for BlackBerry
Protection components*	Anti-virus Anti-spam** Anti-theft** Firewall The Security Auditor	Anti-virus The Security Auditor
Centralized administration in Dr.Web Enterprise Security Suite	+	
Supported OS	Android 4.0–7.1 The firewall supports Android 4.0 and higher	BlackBerry 10.3.2+
Key features		
Multi-threaded scanning with tasks distributed between CPU cores	+	
Scan files received via a GPRS/Infrared/Bluetooth/Wi-Fi/USB connection or while synchronizing with a computer	+	+
On-demand scanning	+	+
Enable/disable resident protection for memory cards	+	
Automated self-recovery	+	
Scan on demand a device's entire file system or separate files and folders	+	+
Scan APK, SIS, CAB, ZIP, RAR and JAR archives	+	+
Block applications that are not on the administrator allowed list	+	
Customisable rules for each application	+	
Instant control over inbound and outbound traffic for each application	+	
Ability to restrict mobile data traffic	+	
Ability to set roaming restrictions for specific applications	+	
Ability to block access to non-recommended sites	+	
Protection from unauthorized access via wireless networks	+	
Neutralisation of ransomware lockers	+	
Vulnerability scanner	+	
Black- and whitelists to filter incoming calls and SMS	+	
Support for multiple trusted SIM cards	+	
Delete infected files	+	+
Quarantine suspicious objects	+	+
Restore files from the quarantine	+	+
Updating over the Internet: ■ via HTTP using the GPRS module; ■ via Infrared/Bluetooth/Wi-Fi/USB; ■ While synchronising over ActiveSync with a computer connected to the Internet	+	+
Detailed system scanning reports	+	+
Lock screen displays information about detected threats and links to the threat list	+	
Notifications about activity detected that is typical of malware	+	
Ability to manage a device remotely with the Anti-theft if it has been lost or stolen	+	
Mobile device GPS coordinates deliverable via SMS	+	

* These components cannot be used on a device without a SIM-card.

** Only an Anti-virus is available on a device under Android TV.

Useful links

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

Dr.Web Bundles

Enterprise-Level Anti-Virus Security for Small and Medium Businesses

All Dr.Web products for e-mail protection are included in low-cost bundles for small- and medium-sized companies. This is a unique low-cost offer. Small companies with 5-50 computers that can't afford comprehensive anti-virus solutions for large businesses can take advantage of Dr.Web bundles that include protection products for all types of objects: workstations, mail traffic, file servers, and Internet gateways.

Important! There are no discounts for bundles, including renewal or migration discounts. To continue using a bundle, new license should be purchased. If a customer wants to renew a license for some product(s) of a bundle, the renewal discount is granted for this product or products in this case.

	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
Protected objects	Workstations	Servers	E-mail users	Gateway users	Mobile devices
License	Comprehensive protection	Anti-virus	Anti-virus + Anti-spam + SMTP proxy	Anti-virus	Anti-virus
Quantity	5 – 50	1	Equals to number of WSs	Equals to number of WSs (from 25)	Equals to number of WSs

Useful links

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

Dr.Web Safe School bundle

Product	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mobile Security Suite
License	Comprehensive protection + Control center	Anti-virus	Anti-virus
Quantity	10 – 200	1 – 8	10 – 200

Dr.Web curing utilities

Dr.Web curing utilities are designed for scanning and emergency curing. They do not provide resident protection.

Dr.Web CureNet!

Remote centralized curing for any network's Windows workstations and servers even those running other anti-virus software.

Prospective customers	Small, medium, and large companies that are currently using other anti-virus products on the computers and servers in their networks.	
Functions	■ Emergency curing for Windows workstations and servers. ■ Verifies the quality of the anti-virus software currently in use.	
Features	■ Does not require that the current anti-virus be uninstalled before scanning and curing with Dr.Web CureNet!. ■ Requires no running server or additional software. ■ Operates in networks isolated from the Internet. ■ Dr.Web CureNet! Master can be launched from removable media including USB data storage devices.	
Product description	http://curenet.drweb.com/	
Supported OS	MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32- and 64-bit architecture) or iPhone 4, iPod touch 4 running iOS 7.0+.	
What is "My Dr.Web CureNet!"?	This is the personal area where an individual Dr.Web CureNet! download link is stored for as long as a subscription is valid. "My Dr.Web CureNet!" can also be used to contact technical support, submit a suspicious file for analysis, and use other services.	
Licensing	The utility is licensed per number of workstations (at least 5) for 1, 2, or 3 years.	
Demo version	No curing is provided.	
System requirements	Master	■ Any computer running Windows 2012/8, 8.1 (Professional/Enterprise)/2008 SP2/7 (Professional/Enterprise/Ultimate)/2008/Vista SP1 (Business/Enterprise/Ultimate)/2003 SP1/XP Professional SP2 (32- and 64-bit architecture) ■ Free RAM: at least 360 MB. ■ Free disk space: at least 200 MB. ■ A TCP/IP connection to all target hosts. ■ Internet access: to update the virus databases and components of Dr.Web CureNet!.
	Scanner	■ Any PC running MS Windows XP Professional and later versions, except for Windows® Server 2003 x64 Edition and Windows® XP Professional SP2 x64 Edition. ■ Free RAM: at least 360 MB. ■ Free disk space: at least 200 MB.

Dr.Web CureIt!

Emergency curing for Windows workstations and servers including those running other anti-virus software

Prospective customers	Small, medium, and large companies currently using other anti-viruses on computers and servers.
Functions	■ Cure Windows workstations and servers. ■ Verifies the quality of the anti-virus software currently in use.
Features	■ Dr.Web CureIt! doesn't require installation and doesn't conflict with any known anti-virus; consequently there is no need to disable the anti-virus currently in use to check a system with Dr.Web CureIt!. ■ Improved self-protection and an enhanced mode for more efficient countermeasures against Windows blockers. ■ Dr.Web CureIt! is updated at least once an hour. ■ The utility can be launched from removable media including USB storage devices.
Product description	http://free.drweb.com/cureit
Supported OS	MS Windows 10/8/7/Vista/2012/2008 (32- and 64-bit systems), XP/2003 (32-bit systems).
Licensing	The utility can be licensed for 12, 24 and 36 months.
Licensing features	The utility is available for free when used for non-business purposes.
Demo version	N/A.
System requirements	■ Computer running OS MS Windows 8/7/Vista/2012/2008 (32- and 64-bit systems), XP/2003 (32-bit systems)

Russia

Doctor Web

3d street Yamskogo polya 2-12A, Moscow, Russia, 125040

Tel: +7 (495) 789-45-87

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

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

China

Doctor Web Software Company (Tianjin), Ltd.

112, North software tower, № 80, 4th Avenue,
TEDA, Tianjin, China

天津市经济技术开发区第四大街80号软件大厦北楼112

Tel: +86-022-59823480

Fax: +86-022-59823480

E-mail: y.zhang@drweb.com

www.drweb.cn

France

Doctor Web France

333b, Avenue de Colmar, 67100 Strasbourg

Tel.: +33 (0) 3 90 40 40 20

www.drweb.fr

Germany

Doctor Web Deutschland GmbH

63457, Hanau-Wolfgang, Rodenbacher Chaussee 6

Tel: +49 (6181) 9060-1210

Fax: +49 (6181) 9060-1212

www.drweb-av.de

Japan

Doctor Web Pacific, Inc.

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

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

www.drweb.co.jp

Republic of Kazakhstan

Doctor Web – Central Asia

Republic of Kazakhstan, 050009, Almaty, Shevchenko, 165b
office 910

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

www.drweb.kz

Ukraine

Doctor Web Technical Support Centre

Office 6, 27 Pushkinskaya str., Kiyev 01601, Ukraine

Tel/fax: +380 (44) 238-24-35,

www.drweb.com.ua