



Defend what you create

Dr.Web® Security Suite product line

Licensing guide

Updated on 10.06.2016

Table of contents

About Doctor Web	4
Dr.Web technologies	4
Dr.Web license certificate	9
Dr.Web Security Suite	10
Licensing Dr.Web products	10
Delivery of Dr.Web products	12
Dr.Web Home Security Suite	16
Product components	16
Dr.Web Security Space	17
Dr.Web Anti-virus for Windows	22
Dr.Web Katana	24
Dr.Web Anti-virus for OS X	26
Dr.Web Anti-virus for Linux	27
Dr.Web Console Scanners	27
Dr.Web Mobile Security	28
Dr.Web for Android	28
Dr.Web for Blackberry	30
Dr.Web Universal (for ASC customers)	30
Dr.Web Enterprise Security Suite. Products for business	31
How to choose a right product?	32
Dr.Web Enterprise Security Suite Control Center	33
Dr.Web Desktop Security Suite	34
Dr.Web Server Security Suite	35
Dr.Web for Windows Servers	35
Dr.Web for OS X Server	37
Dr.Web for Novell NetWare	38
Dr.Web for UNIX Server	39
Dr.Web Mail Security Suite	40
Dr.Web for UNIX Mail Servers	40
Dr.Web for MS Exchange	44
Dr.Web for IBM Lotus Domino	45
Dr.Web for Kerio Mail Servers	47
Dr.Web Gateway Security Suite	48
Dr.Web for Internet Gateways UNIX	49
Dr.Web for Internet Gateways Kerio	50

Dr.Web for MIMESweeper.....	51
Dr.Web for Qbik WinGate	52
Dr.Web Mobile Security Suite	53
Dr.Web Retail Security Suite	54
Dr.Web Universal (for ASC customers)	55
Dr.Web Bundles.....	56
Utilities	57
Solutions.....	58
Services	59
Discount policy	61
General terms of sale.....	63
Dr.Web Enterprise Security Suite additional purchase	64
Dr.Web license codes.....	66
Contacts.....	69

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

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.

Technologically complex and highly dangerous viruses especially designed for commercial gain are normally tested by virus writers using all known anti-virus software before they release such viruses into the wild; that way the viruses exist undetected by anti-viruses for as long as possible. Before samples of such viruses get into the lab, they cannot be detected by any anti-virus.

Dr.Web detects and cures viruses

- The Dr.Web anti-virus functions on infected computers; its exceptional resistance to viruses makes it stand out among other anti-viruses.
- 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. It can even be run from external media without installing into the system (for example, from a USB-stick) and cure active threats during installation.
- Integration of the installation package (the installer) with the updated Dr.Web Anti-rootkit can repel active threats and cure a PC as it is being installed, even if the computer is infected with sophisticated malware.
- Part of Dr.Web Anti-rootkit (Anti-rootkit API, or arkapi), the resident background scan subsystem searches for active threats among such critical Windows areas as start-up objects, running processes and modules, system object heuristics, RAM, MBR/VBR, and BIOS. When threats are detected, the subsystem cures them and blocks harmful effects.
- Dr.Web is capable of detecting and neutralizing viruses that only reside in RAM and never exist as separate files. **There are still few anti-viruses that can cure such viruses.**
- Dr.Web is able to reliably detect packed malicious objects regardless of whether Dr.Web recognizes the compression format, and disassemble and analyze them in detail to expose hidden threats.
- Only Dr.Web can fully check archives at any nesting level. That means that the Dr.Web anti-virus will detect and neutralize a threat even if it has been compressed many times with various supported archiving programs.

High level of self-protection

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

- Dr.Web SelfPROtect is implemented as a driver that operates at the lowest system level. It cannot be stopped or unloaded until a system is rebooted.
- Dr.Web SelfPROtect restricts access to networks, files and folders, certain branches of the Windows Registry, and removable data-storage devices at the system driver level, and protects software from anti-viruses aiming to disrupt Dr.Web's operation.
- Some anti-viruses modify the Windows kernel by intercepting interruptions, changing vector tables, using other undocumented features, etc. 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 the security of the anti-virus and does not interfere with Windows kernel routines.
- Automatic restoration of its own modules.

Advanced technologies of preventive protection

- **FLY-CODE** is a unique universal decompression technology that allows viruses packed with packers, unknown even to Dr.Web, to be detected.
- The cutting-edge, non-signature scan technology Origins Tracing™ ensures the high probability that viruses still unknown to Dr.Web will be detected.
- **The heuristic analyzer**, whose analyses are based on criteria 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.

Full scan of all traffic

- **Safe traffic**— scanning on all ports is carried out on traffic transmitted via Dr.Web-supported protocols, including secure connections (if the user has enabled the option to scan SSL traffic).
- **Safe Internet Surfing** — with secure search, Google, Yandex, Yahoo!, Bing and Rambler will only return links to content considered safe by the search engines and Dr.Web. Dangerous sites will be excluded from search results altogether!
- **Secure Communication**— Filtering traffic of instant messengers such as Mail.Ru Agent, ICQ, Jabber. Links that lead to malware and phishing sites are removed from messages. The anti-virus scans transmitted attachments. The transfer of potentially dangerous files is blocked.

Instant cloud-based protection

- The parental control and SplDer Gate enable you to check URLs with the Dr.Web Cloud service on servers of Doctor Web.
- As a user goes to a website, the respective URL is sent to Doctor Web to determine whether the site is safe to visit. The URL is checked in real time regardless of updating settings or how up-to-date the virus definitions on the user’s computer are.
- Dr.Web Cloud transmits no information to Doctor Web that may help identify the user.

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-scams technologies

Scams (as well as phishing 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 vi-

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.Web 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 license certificate

CERTIFICATE of authenticity

Dr.WEB®

This is to certify that this software is legally licensed with **Doctor Web** — the developer and the owner of the Title to **Dr.WEB®** security products

License owner

Licensed product

Serial number

Serial number

Serial number

Protected objects

Workstations	Servers
E-mail users	Gateway users
Mobile devices	Control Center

License period

Reseller

Doctor Web
B.Sharov, CEO

[Signature]

[Seal: «Доктор Веб» Doctor Web, Ltd.]

Dr.Web license certificate confirms that Dr.Web software was legally purchased with the Dr.Web Licensors.

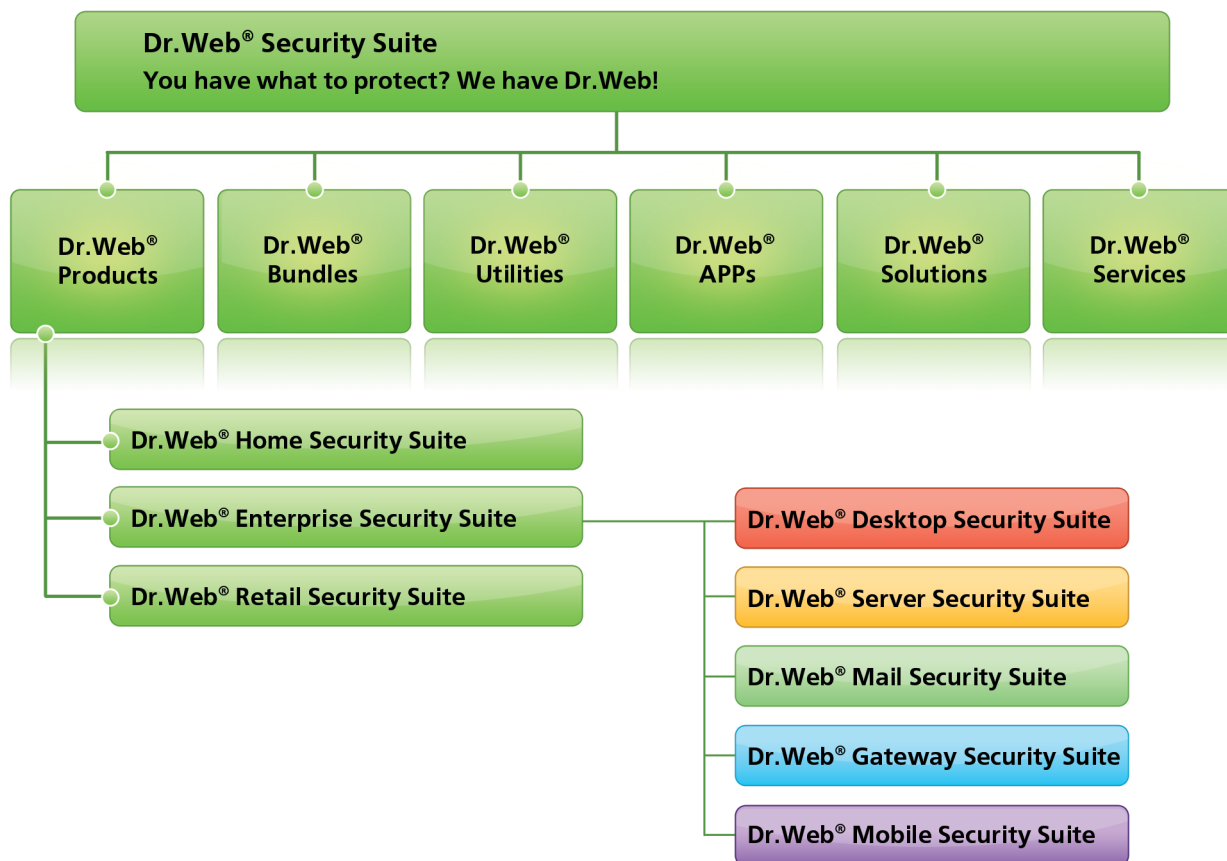
Important! Dr.Web license certificate is not a ground for renewal with a discount. Only key file or a serial number can be a ground for a renewal with a discount.

You can generate an e-copy of the certificate at <http://products.drweb.com/register/certificate/>.

[Faint version of the certificate form]

Dr.Web Security Suite

The products line called Dr.Web Security Suite consists of commercial products for home, business and retail, bundles, utilities, APPs, solutions and services.



Licensing Dr.Web products

1. Dr.Web products are licensed for 12, 24 and 36 months. Dr.Web Security Space and Dr.Web anti-virus for Windows are also licensed for 3 and 6 months.
2. Dr.Web products are licensed according to the number of protected objects.
3. Objects that can be protected by Dr.Web:
 - Workstations, embedded system clients and terminal server clients
 - File servers and application servers (including terminal servers)
 - E-mail users
 - Users of mail and Internet gateways
 - Mobile devices
4. Two types of **basic licenses** are available:
 - 1) Anti-virus
 - 2) Comprehensive protection
5. The **Comprehensive protection** license is only available for anti-viruses protecting Windows PCs. Such licenses cover the following components: anti-virus, anti-rootkit, anti-spy, anti-spam, HTTP-monitor, office control, firewall.

6. If a customer needs additional components for better protection, they can be included into the basic license. Additional components are not licensed separately.
7. Specific types of basic licenses and sets of additional components are provided for each type of objects.

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 XP/2003/ Vista/2008/7/8/2012/ 10 (32- & 64- bit systems)	Comprehensive protection	■ Control center
		Anti-virus	
	OS X 10.7 and later Linux glibc 2.7 and later	Anti-virus	■ Control center
	MS DOS OS/2		
Dr.Web Server Security Suite File and application servers	Windows Novell NetWare OS X Server Unix (Samba)	Anti-virus	■ Control center
Dr.Web Mail Security Suite E-mail users	UNIX MS Exchange	Anti-virus	■ Control center ■ Anti-spam ■ SMTP proxy
	Lotus (Windows/Linux)		■ Anti-spam ■ SMTP proxy
	Kerio (Windows/Linux)		■ SMTP proxy
Dr.Web Gateway Security Suite Gateway users	Internet gateways Kerio Internet gateways UNIX	Anti-virus	■ Control center
	MIMESweeper Qbik WinGate Microsoft ISA Server and Fore-front TMG		■ Anti-spam
Dr.Web Mobile Security Suite Mobile devices	Android	Comprehensive protection	■ Control center ■ Anti-spam
	Windows Mobile	Anti-virus	■ Anti-spam
	Symbian OS		

Delivery of Dr.Web products

Dr.Web software is delivered as an e-license and in a packaging.

1. Dr.Web e-license

Supplied as Dr.Web serial numbers:

- by e-mail;
- printed on a license certificate.

2. Dr.Web cardboard packaging



Packaging:

- Cardboard package
- License certificate
- Users manual
- DVD
- Dr.Web branded envelope for the disk
- Seal sticker
- Sticker "Protected by Dr.Web"
- USB-device (for Dr.Web for OS X + Dr.Web Security Space Pro product only)

3. Customizable delivery in a box

It is used to deliver to a customer one or several Dr.Web Enterprise Security Suite products.



Packaging:

- Dr.Web cardboard package;
- License certificate;
- DVD-disk with Dr.Web software in an envelope.

4. Dr.Web license package

It is used to deliver to a customer one or several Dr.Web Enterprise Security Suite products.



Packaging:

- Cardboard envelope;
- License certificate.

5. Scratch-cards

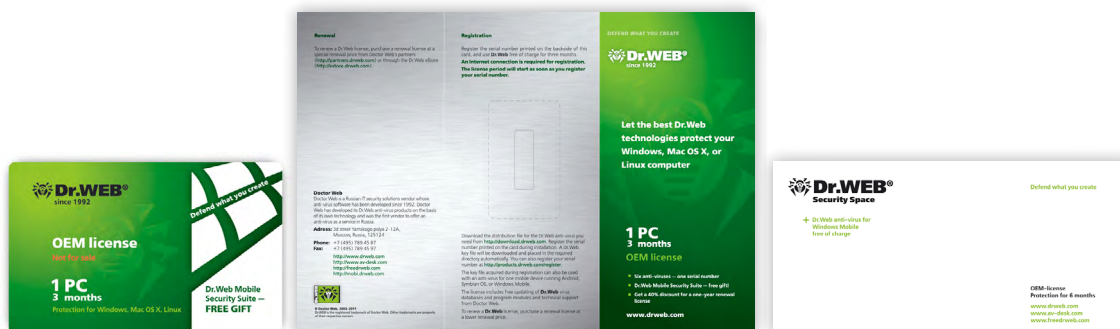
Dr.Web scratch cards with a serial number.



6. Dr.Web OEM products

Dr.Web OEM Universal (single-user licenses)

Supplied as an OEM card with a scratch band glued to the OEM-flyer. Provides protection for 1 PC and 1 mobile device for 3 months.



The license covers the following products:

- Dr.Web Security Space
- Dr.Web anti-virus for OS X
- Dr.Web anti-virus for Linux
- Dr.Web Mobile Security (Android OS, BlackBerry, Symbian OS, Windows Mobile)

Renewal

- To extend the validity period of a Dr.Web OEM license, purchase a renewal license at a renewal discount.
- If you want to renew your license, you can also purchase Dr.Web Security Space or Dr.Web Anti-virus in a box (without a renewal discount). In this case you will have 300 bonus days added to the new license period.
- If you purchase a Dr.Web product in a box with a license to protect 2 PCs for 1 year and register the serial numbers sequentially for protection of the same PC.

Delivery

Dr.Web OEM Universal is delivered to Doctor Web's partners only as scratch-cards with the minimum quantity of 250 cards. Scratch cards and electronic licenses in quantities from 50 to 500 are only delivered to companies that have the Authorized Dr.Web Service Center status (more about the ASC programme – <http://partners.drweb.com/service>).

A renewal protection programme is also available to large OEM-license distributors:
<https://pa.drweb.com/products/oem/universal/protection/>

Dr.Web OEM Server (corporate licenses)

Use any product from Dr.Web Enterprise Security Suite for 3 months Delivered as a media-kit.

The license covers the following products:

- Dr.Web Enterprise Security Suite Control Center
- Dr.Web Desktop Security Suite – 100 PC
- Dr.Web Server Security Suite – 10 servers
- Dr.Web Mail Security Suite – 100 users
- Dr.Web Gateway Security Suite – 100 users
- Dr.Web Mobile Security Suite – 100 devices



Media-kit contents

- Corporate Dr.Web envelope
- A CD containing a presentation of all Dr.Web products
- A Dr.Web license certificate with a serial number for Dr.Web Enterprise Security Suite for 3 months
- Dr.Web Enterprise Security Suite flyer
- Dr.Web OEM sticker

Renewal

To extend validity of a Dr.Web OEM license, purchase a one year renewal license at a 40 renewal discount.

Bonuses programme

A special bonus programme is available to suppliers of OEM-server licenses. You can find more information here <https://pa.drweb.com/products/oem/kod/bonuses>.

 More information about OEM:

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

Dr.Web Home Security Suite

Product components

Dr.Web Security Space	Dr.Web Mobile Security
Protection for any devices	Protection for mobile devices
<ul style="list-style-type: none"> ■ Dr.Web Security Space ■ Dr.Web Anti-virus for Windows ■ Dr.Web Anti-virus for OS X ■ Dr.Web Anti-virus for Linux 	—
<ul style="list-style-type: none"> ■ Dr.Web for Android ■ Dr.Web for BlackBerry ■ Dr.Web for Symbian ■ Dr.Web for Windows Mobile 	<ul style="list-style-type: none"> ■ Dr.Web for Android ■ Dr.Web for BlackBerry ■ Dr.Web for Symbian ■ Dr.Web for Windows Mobile

Protection components

Protection components	Windows	OS X	Linux
Anti-virus	+	+	+
Anti-spam	+		
HTTP monitor	+	+	
Parental control	+		
Firewall	+		
Anti-virus network	+		
Preventive protection	+		
Services for Windows			
Protection against data loss (backup)	+		
Dr.Web Cloud	+		
Block access to removable devices	+		

Licensing Dr.Web Security Space

1. The product is licensed per number of protected computers (1–5).
2. Available commercial license terms: 3, 6, 12, 24 or 36 months. OEM licenses are available for a term of 3 or 6 months.
3. Standard renewal discounts are available.
4. No other discounts are provided.
5. Customers purchasing this product are entitled to use Dr.Web Mobile Security for free. The number of protected mobile devices is equal to the number of PCs covered by the license purchased.

License expansion (additional purchase)

1. A home user can expand their license for Dr.Web Security Space in one of two ways, either by upgrading from Dr.Web Anti-virus to Dr.Web Security Space or increasing the number of protected objects.
2. A license covering expanded product usage is activated automatically, from the moment the license is generated, and includes all the data specified when the initial license was registered.

3. If the remaining license period is longer than 3 months, the license is expanded at a renewal price. The license type in the code of such a license is D. The license is renewed automatically.
4. If **the license expires in less than 3 months**:
 - The license is expanded for free via the [free expansion service](#).
 - The old license is blocked within 24 hours after the new one is generated.
 - The license type in the license code is C; the price of such a license is zero. The license can subsequently be renewed at a discount.

► Dr.Web Security Space



Comprehensive protection

- **Improved!** Comprehensive protection for Windows PCs from all types of known and unknown Internet threats.
- **Improved!** Protection from the latest malicious programs designed to bypass detection by traditional signature-based scanning and heuristic analysis.
- **New!** Protection from zero-day vulnerability exploits.
- **Improved!** Can be installed and operate in an infected system.
- **Improved!** Highly immune to any attempts made by malicious programs to disrupt Dr.Web's operation.
- **Improved!** Fast multi-thread scanning powered by multi-core systems.
- **Improved!** Real-time protection, with no impact on system performance.
- **Improved!** Rapid filtration of web traffic and email with no delays when playing online games, streaming video or listening to the radio.
- **New!** Brand-new backup routine for generating and storing backups of important files using the Data Damage Prevention feature. Sparing use of system resources when creating backups of any size!
- Scanning of archived files at any nesting level.
- Access is blocked to sites that are used to distribute malicious or potentially dangerous programs, phishing sites, and sites that use social engineering techniques to misguide users.
- Spam and other types of unsolicited messages are filtered; no anti-spam training is required.
- **Improved!** Real-time scanning of traffic on all ports.
- Secure searching on Google, Yandex, Yahoo!, Bing and Rambler – unsafe content is filtered out by the search engines!
- Secure communication – instant messenger traffic is filtered.
- **Improved!** Effective protection for children against exposure to objectionable content.
- **Improved!** Ability to prevent the unauthorized use of the computer and removable devices.
- Dr.Web Cloud – instant URL check on Doctor Web's servers.
- **New!** Cloud reputation service verifies the safety of specific URLs.
- Protection against unauthorized access by a network; blocks suspicious connections on package and application layers.
- Remotely manage other computers in your local network without installing the Dr.Web Control Center.

Protection components

Efficient detection and neutralization of all types of threats (Dr.Web Scanner)

- **What's new in Version 11!** Virus scanning is faster than ever thanks to the enhanced Dr.Web Scanning Engine.
- High-speed scanning with several scanning threads powered by multi-core systems

- Thorough scanning of RAM, boot sectors, hard drives and removable data-storage devices, for viruses, Trojans and other malware.
- Detection of active virus threats only.
- Comprehensive databases for detecting spyware, riskware, adware, hack tools, and jokers.
- The Dr.Web Shield™ anti-rootkit used by the Scanner detects complex viruses that use rootkit technologies and are able to conceal themselves in an infected system.
- The console scanner intended for experienced users enables the anti-virus to be run from the command line. It offers users a wide range of options and also utilizes multi-core features.

Real-time protection (SpIDer Guard® file monitor)

- SpIDer Guard monitors system health in real time and intercepts “on the fly” all calls to files located on local drives, floppy discs, CD/DVD/ Blue-ray disks, flash drives, or smart cards.
- The file monitor is highly resistant to attempts by malicious programs to disrupt or halt its operation.
- State-of-the-art technologies implemented in the Dr.Web anti-virus engine enable it to monitor the availability of system resources and control its “appetite”, while maintaining effective protection.
- High performance on machines involved in intensive data stream processing (involving heavy use of file systems, downloading files via torrents, compiling and video rendering).

Protection against unknown threats (preventive protection)

The technologies incorporated into Dr.Web Preventive Protection enhance traditional signature-based detection with cutting-edge behavioural analysis. With preventive protection Dr.Web can:

- Protect 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;
- Detect unwanted file modification, monitor the operation of all system processes to detect actions that are typical of malware (e.g., encryption ransomware activities), and prevent malicious objects from injecting their code into other processes;
- Detect and neutralise threats that have not yet been discovered and entered in the Dr.Web virus database: encryption ransomware, injectors, remotely controlled malware used for espionage and to create botnets, and malware packers.

And those are just a few of the things that Dr.Web Preventative Protection can do.

High level of self-protection

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

- Dr.Web SelfPROtect is implemented as a driver that operates at the lowest system level. It cannot be stopped or unloaded until a system is rebooted.
- Dr.Web SelfPROtect restricts access to networks, files and folders, certain branches of the Windows Registry, and removable data-storage devices at the system driver level, and protects software from anti-viruses aiming to disrupt Dr.Web's operation.
- Some anti-viruses modify the Windows kernel by intercepting interruptions, changing vector tables, using other undocumented features, etc. 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 the security of the anti-virus and does not interfere with Windows kernel routines.
- Automatic restoration of its own modules.

New in version 11! The new Dr.Web Hypervisor component uses state-of-the art CPU capabilities to upgrade threat detection and neutralisation routines and to strengthen Dr.Web's self-protection capabilities. The component runs beneath the operating system to maintain control over all programs,

processes, and the operation of the OS. It makes sure no malware can gain control over a system protected by Dr.Web.

Dr.Web developers adopted this approach to overcome the limitations that exist for anti-viruses running on 64-bit platforms when an anti-virus has to operate on the layer used by malware.

The component is compatible with VirtualBox, VmWare, Hyper-V, Parallels.

Filtering Internet traffic (SpIDer Gate HTTP monitor)

- New in version 11! Thanks to modernised Dr.Web Net filtering Service traffic interception routines, downloading files from the Internet has become much faster. The revamped routines for scanning media content make sure that online video and audio is streamed without delays. CPU usage for file transfers via browsers and download managers has decreased significantly. Fans of Dr.Web and online games will notice the difference in scanning speed!
- New in version 11! New exception settings for faster scanning. For example, you can exclude:
 - Data transmitted via HTTPS;
 - Traffic generated by applications with valid digital signatures.
 - The new settings will help prevent conflicts between Dr.Web and third-party applications during traffic filtering and yet maintain the desired security level.
- The HTTP monitor SpIDer Gate scans incoming and outgoing HTTP traffic in real time, intercepts all HTTP connections, filters out data, blocks infected web pages in any browser, scans files in archives, and protects users from phishing sites and other dangerous web resources.
- Safe Internet traffic— scanning on all ports is carried out on traffic transmitted via Dr.Web-supported protocols, including secure connections (if the user has enabled the option to scan SSL traffic).
- Safe Internet Surfing — with secure search, Google, Yandex, Yahoo!, Bing and Rambler will only return links to content considered safe by the search engines and Dr.Web. Dangerous sites will be excluded from search results altogether!
- Secure Communication— Filtering traffic of instant messengers such as Mail.Ru Agent, ICQ, Jabber. Links that lead to malware and phishing sites are removed from messages. The anti-virus scans transmitted attachments. The transfer of potentially dangerous files is blocked.
- Scan encrypted SSL traffic (HTTPS).
- Block access to sites that distribute malicious or potentially dangerous programs, phishing sites, and sites that use social engineering techniques to trick visitors (more info).
- Separate database of sites that distribute unlicensed content—protection of copyright holders.
- Disable the scan of outgoing or incoming traffic and create a blacklist of applications whose HTTP traffic will be scanned no matter what (black list). Define applications whose traffic will not be scanned (white list).
- Prioritize the traffic you want to scan (i.e., do a balance test). Balancing impacts both the way a PC's CPU resources are distributed and the speed of the Internet.
- SpIDer Gate operates independently from web browsers.
- Filtering does not affect overall system performance, surfing speed, and traffic.
- No configuration is required in the default mode; Dr.Web SpIDer Gate starts scanning right after installation.
- Checking URLs on Doctor Web's servers via Dr.Web Cloud. As a user goes to a website, the respective URL is sent to Doctor Web to determine whether the site is safe to visit. The URL is examined in real time regardless of what the update settings are or how current the virus definitions on the user's computer are.

Email free from viruses and spam (SpIDer Mail anti-virus and anti-spam)

- Scanning on all ports is carried out on traffic transmitted via Dr.Web-supported protocols, including secure connections (if the user has enabled the option to scan SSL traffic).
- SpIDer Mail scans mail before e-mails are received by a mail client and prevents malware that is mainly distributed by spam from exploiting software vulnerabilities.
- Real-time anti-virus and anti-spam scanning of e-mails over SMTP/POP3/NNTP/IMAP4.
- Scanning of encrypted SSL connections (SMTPS/POP3S/IMAP4S).

- Scanning does not interrupt operation of mail clients and doesn't cause a receipt delay.
- Individual processing rules are applied for each type of malicious object – viruses, riskware, adware, hack tools, paid dialers, and jokers.
- An analysis of message contents and sending time allows the characteristics of malicious activities to be detected and prevents mail worms from carrying out mass mailings

Anti-spam

- The anti-spam does not require configuration and starts working as soon as the first message is received.
- Different filtering technologies ensure the high probability of detecting spam, phishing, pharming, scamming, and bounce messages.
- With the anti-botnet feature, your computer will not be disconnected from the Internet for sending spam.
- Messages that have been filtered out are never deleted. Instead, they are placed in a separate folder where you can always verify that no false detection has occurred.
- Standalone anti-spam analyzer module; no permanent connection to an external server or access to a database is required, which significantly saves traffic.

Security for the entire family Control over Internet surfing and block access to dubious sites (Dr.Web Parental Control)

Secure Web traffic

- Scanning traffic on all ports.
- Check of URLs on Doctor Web's server regardless of update settings or how up-to-date virus databases on the user's computer are.
- Blocking of websites categorized into 10 thematic groups (adult content, violence, weapons, drugs, gambling, etc.).
- Protection of children from exposure to objectionable content.

Restricting access to a PC and the Internet

- Limiting Internet and computer time.
- Block any adjustments to the system time and time zone to prevent children from using the computer without their parents' permission.
- **New in version 11!** A new option lets parents specify the amount of time (30 minutes minimum) that their children can spend on the computer.
- **New in version 11!** Automatically block access to a PC at night.
- **New in version 11!** Time-limit profiles can also be created.

Block access to files and folders

- Blocking of access to files, folders, or network drives, an additional measure to protect data from deletion or unauthorized access.
- **New in version 11!** The access mode parameter (deny access or grant access in the read-only mode) offers more ways to configure access.

and

- Parental Control lets you set profiles individually for each user.
- Settings can be imported between user accounts.
- The Parental Control can be disabled for a particular user account.

Block access to devices to cover all possible intrusion paths

- Restriction of access to devices such as disk drives, DVD-/CD-ROM drives, keyboard, mouse, network adapters, audio and video cards, gaming devices, USB devices, and COM/LPT ports.
- Blocking of access to removable data storage devices (flash drives, USB devices), files, folders, or network drives, an additional measure to protect data from deletion or unauthorized access.

- White lists of trusted devices that prevent unauthorized use of removable devices on the protected computer, confidential data thefts, infections via removable media.
- **Improved in version 11!** New options have been added for device whitelists for more flexible access to devices.
- Export/import of white lists.
- Disable printing jobs from being started to prevent confidential documents from being printed and to save printing paper.

Protection from network attacks (Dr.Web Firewall)

- Protection against unauthorized access by a network; prevention of data leaks; blocking of suspicious connections on package and application layers.
- The Dr.Web Firewall uses its own database of trusted applications. These are programs that incorporate a digital certificate. Applications that Dr.Web believes to be legitimate can connect to any address via any port. Exception: if a program is not digitally signed, its signature is invalid, or there is no signature at all, (e.g., those created by enthusiasts or open source programs), the user is prompted to create a rule.
- application layer connection control makes it possible to monitor the interaction of applications and processes with network resources and to register all access attempts in the applications log;
- Packet-layer filtering makes it possible to control the connection to the Internet regardless of what application is using it. The packet-filter log stores information about packets sent over network interfaces.
- In Game Mode, a rule dialogue window will appear above any application running in full-screen mode.
- Real-time monitoring of application networking activities and forced disconnection of applications from the network, if necessary.

Manage protection of all the computers in your household network

- The Anti-virus Network component enables Dr.Web software installed on computers in the local network to be administered and configured locally.
- Remote control does not require the Dr.Web Control Center.
- You can establish a remote connection from any computer to any other computer.
- Administration includes retrieving statistics and logs from a remote machine, viewing and changing module settings, and starting and stopping anti-virus components. You can also register a serial number and replace a key file on a remote computer.
- To use this feature, a remote connection must be allowed on a target machine.

System requirements

- Windows 10/8/7/Vista (64-bit) and Windows 10/8/7/Vista/XP SP2 (32-bit).
- RAM: at least 512 MB.
- Free disk space: 1 GB. Temporary files created during installation will require additional disk space.

Additional requirements: Internet connection for registration and updating.

Licensing

Types of licenses

- Per number of protected workstations

License options

- Dr.Web Security Space. The license includes the following protection components: Anti-virus, Anti-spy, Anti-rootkit, Anti-spam, HTTP monitor, Parental Control, Firewall.

🌐 Description: http://products.drweb.com/win/security_space

🌐 Upgrade to version with firewall: http://promotions.drweb.com/upgrade/security_space

► Dr.Web anti-virus for Windows



Basic anti-virus protection

- **Improved!** Protection from the latest known and unknown Internet threats and malicious programs designed to bypass detection by traditional signature-based scanning and heuristic analysis.
- **New!** Protection from zero-day vulnerability exploits.
- **Improved!** Can be installed and operate in an infected system.
- **Improved!** Highly immune to any attempts made by malicious programs to disrupt Dr.Web's operation.
- **Improved!** Fast multi-thread scanning powered by multi-core systems.
- **Improved!** Real-time protection, with no impact on system performance.
- Scanning of archived files at any nesting level.
- Protection against unauthorized access by a network; blocks suspicious connections on package and application layers.

Protection components

Efficient detection and neutralization of all types of threats (Dr.Web Scanner)

- **What's new in Version 11!** Virus scanning is faster than ever thanks to the enhanced Dr.Web Scanning Engine.
- High-speed scanning with several scanning threads powered by multi-core systems
- Thorough scanning of RAM, boot sectors, hard drives and removable data-storage devices, for viruses, Trojans and other malware.
- Detection of active virus threats only.
- Comprehensive databases for detecting spyware, riskware, adware, hack tools, and jokers.
- The Dr.Web Shield™ anti-rootkit used by the Scanner detects complex viruses that use rootkit technologies and are able to conceal themselves in an infected system.
- The console scanner intended for experienced users enables the anti-virus to be run from the command line. It offers users a wide range of options and also utilizes multi-core features.

Real-time protection (SplDer Guard® file monitor)

- SplDer Guard monitors system health in real time and intercepts "on the fly" all calls to files located on local drives, floppy discs, CD/DVD/ Blue-ray disks, flash drives, or smart cards.
- The file monitor is highly resistant to attempts by malicious programs to disrupt or halt its operation.
- State-of-the-art technologies implemented in the Dr.Web anti-virus engine enable it to monitor the availability of system resources and control its "appetite", while maintaining effective protection.
- High performance on machines involved in intensive data stream processing (involving heavy use of file systems, downloading files via torrents, compiling and video rendering).

Protection against unknown threats (preventive protection)

The technologies incorporated into Dr.Web Preventive Protection enhance traditional signature-based detection with cutting-edge behavioural analysis. With preventive protection Dr.Web can:

- Protect 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;
- Detect unwanted file modification, monitor the operation of all system processes to detect actions that are typical of malware (e.g., encryption ransomware activities), and prevent malicious objects from injecting their code into other processes;
- Detect and neutralise threats that have not yet been discovered and entered in the Dr.Web virus database: encryption ransomware, injectors, remotely controlled malware used for espionage and to create botnets, and malware packers.

And those are just a few of the things that Dr.Web Preventative Protection can do.

High level of self-protection

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

- Dr.Web SelfPROtect is implemented as a driver that operates at the lowest system level. It cannot be stopped or unloaded until a system is rebooted.
- Dr.Web SelfPROtect restricts access to networks, files and folders, certain branches of the Windows Registry, and removable data-storage devices at the system driver level, and protects software from anti-viruses aiming to disrupt Dr.Web's operation.
- Some anti-viruses modify the Windows kernel by intercepting interruptions, changing vector tables, using other undocumented features, etc. 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 the security of the anti-virus and does not interfere with Windows kernel routines.
- Automatic restoration of its own modules.

New in version 11! The new Dr.Web Hypervisor component uses state-of-the-art CPU capabilities to upgrade threat detection and neutralisation routines and to strengthen Dr.Web's self-protection capabilities. The component runs beneath the operating system to maintain control over all programs, processes, and the operation of the OS. It makes sure no malware can gain control over a system protected by Dr.Web.

Dr.Web developers adopted this approach to overcome the limitations that exist for anti-viruses running on 64-bit platforms when an anti-virus has to operate on the layer used by malware.

The component is compatible with VirtualBox, VmWare, Hyper-V, Parallels.

Virus-free email (SpIDer Mail monitor)

- Scanning traffic on all ports transmitted via Dr.Web-supported protocols, including secure connections (if the user has enabled the option to scan SSL traffic).
- SpIDer Mail scans mail before e-mails are received by a mail client and prevents malware that is mainly distributed by spam from exploiting software vulnerabilities.
- Real-time anti-virus and anti-spam scanning of e-mails over SMTP/POP3/NNTP/IMAP4.
- Scanning of encrypted SSL connections (SMTPS/POP3S/IMAP4S).
- Scanning does not interrupt the operation of mail clients and does not cause a delivery delay.
- Individual processing rules are applied for each type of malicious object – viruses, riskware, adware, hack tools, paid dialers, and jokers.
- An analysis of message contents and sending time allows the characteristics of malicious activities to be detected and prevents mail worms from sending out mass mailings.

Protection from network attacks (Dr.Web Firewall)

- Protection against unauthorized access by a network; prevention of data leaks; blocking of suspicious connections on package and application layers.
- The Dr.Web Firewall uses its own database of trusted applications. These are programs that incorporate a digital certificate. Applications that Dr.Web believes to be legitimate can connect to any address via any port. Exception: if a program is not digitally signed, its signature is invalid, or there is no signature at all, (e.g., those created by enthusiasts or open source programs), the user is prompted to create a rule.
- Application layer connection control makes it possible to monitor the interaction of applications and processes with network resources and to register all access attempts in the applications log;
- Packet-layer filtering makes it possible to control the connection to the Internet regardless of what application is using it. The packet-filter log stores information about packets sent over network interfaces.
- In Game Mode, a rule dialogue window will appear above any application running in full-screen mode.
- Real-time monitoring of application networking activities and forced disconnection of applications from the network, if necessary.

System requirements

- Windows 10/8/7/Vista (64-bit) and Windows 10/8/7/Vista/XP SP2 (32-bit).
- RAM: at least 512 MB.
- Free disk space: 750 MB. Temporary files created during installation will require additional disk space.

Additional requirements: Internet connection for registration and updating.

Licensing

Types of licenses

- Per number of protected workstations

License options

- Anti-virus (the license includes the following protection components: Anti-virus, Anti-spy, Anti-rootkit, Firewall)

🔍 Description: <http://products.drweb.com/win/av>

► Dr.Web Katana

A non-signature anti-virus offering preventive protection against the latest active threats, targeted attacks, and attempts by Trojans and exploits to use vulnerabilities, including zero-day ones, to penetrate systems, that is unknown to your anti-virus.

Benefits

- Neutralises the latest malicious programs that have been designed to bypass detection by traditional signature-based scanning and heuristic mechanisms and that are completely new and not yet known to your anti-virus.
- Starts protecting a system during the boot-up phase, even before the traditional, signature-based anti-virus is loaded!
- Neutralises the actions of active malware programs without overloading the system.
- Analyses the behaviour of each threat in real time by comparing it with the reputation information stored in the Dr.Web Cloud which is constantly being updated. Immediately neutralises harmful scripts and processes that your anti-virus didn't manage to recognise. Monitors all system processes and blocks those that exhibit malicious behaviour. Determines whether a program is dangerous and then takes whatever measures are necessary to neutralise the threat.
- Does not require any configuration and starts operating effectively as soon as it's installed.
- Protects the system even if a PC is not connected to the Internet.

Features

- Protects critical system areas from being modified by malware.
- Detects and stops the execution of malicious, suspicious or unreliable scripts and processes.
- Detects unwanted file modification, monitors the operation of all processes to detect actions that are typical of malware (e.g., the activities of encryption ransomware), and prevents malicious objects from injecting their code into other processes.
- Detects and neutralises threats that have not yet been discovered and entered in the Dr.Web virus database: encryption ransomware, web injectors.
- Protects against exploits—malicious objects that take advantage of software flaws, including those not yet known to anyone except for the intruders who created them (i.e., zero-day vulnerabilities).

- Controls the operation of the most popular browsers and their associated plugins; protects against browser blockers.
- Blocks malware's ability to modify boot disk areas in order to prevent the launch of Trojan horses, for example, on your computer.
- Blocks changes from being made to the Windows Registry to ensure that the safe mode won't be disabled.
- Prevents malicious programs from altering basic system routines. By blocking certain Windows Registry keys, it prevents malware from changing the appearance of the desktop or hiding a Trojan with a rootkit.
- Prevents malware from changing launch permissions.
- Prevents new or unknown drivers from being downloaded without user consent.
- Prevents malware and certain other applications, such as anti-antiviruses, from adding their entries into the Windows Registry where they could be launched automatically.
- Locks registry sections containing information about virtual device drivers, ensuring that no new virtual devices are created.
- Blocks connections between spyware components and the server that controls them.
- Prevents malware from disrupting system routines such as scheduled backups.

System requirements

Dr.Web Anti-virus for OS X

- Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32-bit)
- Windows 10/8/8.1/7/Vista SP2 (64-bit)
- RAM: at least 512 MB.
- Free disk space: ~150 MB. Temporary files created during installation will require additional disk space.

► Dr.Web Anti-virus for OS X

Protection against malicious programs targeting OS X as well as malware written for other platforms. This product is available in Dr.Web Security Space and Dr.Web Anti-virus.

Features

- Scan of autorun objects, removable data-storage devices, network and logical drives, emails, files and directories including archives.
- Three types of scanning: express, full and custom.
- Automatic, manual and scheduled scans.
- Settings of SplDer Guard® are protected by password 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.
- Scanning exceptions.
- Detection and removal of viruses disguised with unknown packers.
- The anti-virus log contains time of each event, name of the scanned object and the type of action applied to the object.
- The HTTP monitor Dr.Web SplDer Gate® – HTTP-traffic scan and Internet access control.
- Internet access control and protection from exposure to objectionable content (violence, gambling etc).
- Automatic (scheduled) and on-demand updating.
- Virus notifications (that include event sounds) on 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

Dr.Web Anti-virus for OS X

- OS X 10.7 and later
- RAM – as required by the OS
- Internet connection for registration and updating

🔗 Description: <http://products.drweb.com/mac>

► Dr.Web Anti-virus for Linux

Basic anti-virus protection

Key features

- Detects and neutralizes viruses on hard drives and removable data storage devices;
- Detects viruses in archives at any nesting level and in packed objects;
- Scans files using FLY-CODE™ technology, including those compressed with unknown packers;
- Protects against unknown threats using the improved non-signature detection technology Origins Tracing™ and an intelligent heuristic analyzer;
- Offers four types of scanning: full, express, custom, and user-defined presets;
- Monitors system health in real-time; intercepts all calls to files located on local drives, floppy discs, CD/DVD/ Blue-ray disks, flash drives, or smart cards;
- Self-protection against attempts by malicious programs to disrupt operation of the anti-virus;
- The quarantine lets you isolate infected files, allowing files to be restored to their original location and the maximum size of the quarantine to be restricted;
- Detailed statistics on the anti-virus' operation;
- Automatic (scheduled) and on-demand updating.

Advantages

- Easy-to-use control center
- Real-time protection
- Custom scan
- Manageable quarantine
- User-friendly license manager
- Control over the command line
- Stylish interface

System requirements

- Operating System: GNU/Linux for Intel x86/amd64 with kernel 2.6.37 (and later) and glibc 2.13 (and later)
- At least 512 MB of free disk space.
- Internet connection for registration and updating

🌐 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).

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

► Dr.Web Mobile Security

Protection for mobile devices

Protection components of Dr.Web Mobile Security

Protection components	Android	Symbian	Windows Mobile	BlackBerry
Anti-virus	+	+	+	+
Anti-spam	+	+	+	
Anti-theft	+			
URL filter	+			
Firewall	+			
Security auditor	+			+

Dr.Web Mobile Security licensing

1. The product is licensed per number of protected mobile devices (1–5).
2. Available commercial license terms: 12, 24 or 36 months. OEM licenses are available for a term of 3 or 6 months.
3. No discounts, including the renewal discount, are available for this product. To continue using the product after the license has expired, or to increase the number of protected devices (i.e., to make an additional purchase), you must purchase a new license at the full price.

► Dr.Web for Android

Features and advantages

- Performs a quick or full scan of the file system, as well as a custom scan of files and folders specified by user.
Provides a real-time file system scan with SpIDer Guard monitor while trying to save files in the memory.
- Detects new unknown malware using unique Origins Tracing™ technology.
- Protects SD cards from infection with autorun files and Exploit.Cpllnk, both of which may be dangerous for devices running Windows.
- Moves detected threats to the quarantine from which the isolated files can be restored, if needed.
- Minimally impacts system performance.
- Economizes battery resources.

- Economizes traffic due to the small size of the virus database updates, which is particularly important for users of limited mobile tariffs.
- Collects statistics on detected threats and actions performed.
- Offers handy and informative desktop widgets to access the application.

Anti-spam

Helps avoid unwanted calls and SMS messages.

- Offers a choice of modes for filtering calls and messages.
- Lets you create your own filtering profiles.
- Permits you to edit your blacklist (to block incoming calls and messages from certain numbers).
- Displays information about blocked calls and messages.

Anti-theft

Helps you find your mobile device if it has been lost or stolen, and if necessary, wipe your confidential information from the device remotely.

- Lets you lock the device after a reboot.
- Lets you lock your phone which can only be unlocked by entering a password (the number of unlock attempts is limited).
- Lets you unlock the device with an SMS message.
- Allows you to see the device's location at Google Maps.
- Erases data on the device and SD cards remotely.
- Starts a loud audio playback on the device and locks the screen.
- Permits you to customize the message to be displayed on the screen of the blocked device.
- Lets you create a list of numbers to which notifications will be sent regarding a change of SIM cards on the lost device. Allows you to control the anti-theft by sending messages from these numbers to unlock the device if you have forgotten the unlock password.

Cloud Checker

The Cloud Checker filter will restrict access to undesirable Internet sites. Lets you block access to non-recommended or potentially dangerous sites according to the following categories:

- Drugs.
- Known sources of infection.
- Abusive language.
- Terrorism.
- Violence.
- Weapons.
- Adult content, etc.

The Security Auditor

- Troubleshoots the device to identify security problems and offers solutions to address them.

Remover of ransomware lockers

- Terminates malicious processes even if the device is locked.
- Neutralises lockers which are not present in the Dr.Web virus database yet.
- Keeps your data without paying a ransom.

Firewall

Controls application network activity

- Filters the external network traffic of the applications installed on the device and system applications. Choose between Wi-Fi and cellular network filtering, and take advantage of customisable rules (filter by IP addresses and/or ports, and by entire networks or IP ranges).
- Monitors current and previously transmitted traffic; gives you information about the addresses/ports to which applications are connecting and the amount of inbound and outbound traffic.
- Detailed logs.

The firewall is compatible with Android 4.0 or higher.

► Dr.Web for BlackBerry

Features and advantages

- Performs quick or full file system scans, and custom scans of user-specified files and folders.
- Offers real-time file system scanning with the SpIDer Guard monitor when attempts are made to save files in the device memory and when installing software.
- Protects SD cards from becoming infected with autorun files and Exploit.Cpllnk, both of which may be dangerous for Windows-running devices.
- Economizes traffic due to small virus database update sizes, which is particularly important for users whose mobile device plans have usage limits.
- Moves detected threats to the quarantine from which isolated files can be restored, if needed.
- Minimally impacts system performance.
- Economizes battery resources.
- Includes detailed statistics on detected threats and the anti-virus's operation, and also an event log.
- Scans for device vulnerabilities.
- Provides assistance in eliminating security problems and device vulnerabilities.

► Dr.Web Universal (for ASC customers)


Comprehensive protection for desktops and laptops for customers of Dr.Web Authorized Service Centers.

Electronic licenses for Dr.Web Universal are delivered only to Dr.Web Authorized Service Centers and available to ASC customers at a special price.

Dr.Web Universal provides protection for one PC and one mobile device for one year.

The license covers the following products:

- Dr.Web Security Space
- Dr.Web anti-virus for OS X
- Dr.Web anti-virus for Linux
- Dr.Web Mobile Security (Android OS, BlackBerry, Symbian OS, Windows Mobile)

 More information about the authorized centers Dr.Web

<http://partners.drweb.com/service>

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 for Linux
	Dr.Web for OS X
	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 Server
	Dr.Web for UNIX Server
	Dr.Web for Novell NetWare Server
	Dr.Web for OS X 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 Gateway Security Suite Protection of gateways	Dr.Web for UNIX Internet Gateways
	Dr.Web for Internet Gateways Kerio
	Dr.Web for MIMESweeper
	Dr.Web for Qbik WinGate
	Microsoft ISA Server and Forefront TMG
Dr.Web Mobile Security Suite Protection of mobile devices	Dr.Web for Windows Mobile
	Dr.Web for Symbian OS
	Dr.Web for Android

* In development

How to choose a right product?

1. What do you need to protect?	2. Which operating system do you use?*	3. You need an anti-virus or comprehensive protection?	4. You want to administer the protection from one place?	5. How many objects do you need to protect?	6. Do want to protection for 1 year? 2 years? 3 years?	7. Is it a new customer? Or a returning customer? An additional purchase? Or both renewal and additional purchase? Or a customer is qualified for a discount?
Define Dr.Web product	Define OS/ platform	Define basic license	Define additional components	Define the quantity of licenses	Define the license term	Define possible discounts
Workstations, clients of terminal servers, clients of virtual servers, clients of embedded systems (Dr.Web Desktop Security Suite)	<div><div></div> Windows 8/7/Vista/XP SP2/2000 SP4 + Rollup 1 (32&64 bit)</div>	<div><div></div> Comprehensive protection</div> <div><div></div> Anti-virus</div>	<div><div></div> Control center</div>	1....	12, 24 or 36 months	
	<div><div></div> OS X</div> <div><div></div> Linux</div> <div><div></div> MS DOS</div> <div><div></div> OS/2</div>	<div><div></div> Anti-virus</div>	<div><div></div> Control center</div>			
File server, application server, virtual server or terminal server (Dr.Web Server Security Suite)	<div><div></div> Windows</div> <div><div></div> Novell NetWare</div> <div><div></div> OS X Server</div> <div><div></div> UNIX</div>	<div><div></div> Anti-virus</div>	<div><div></div> Control center</div>	1...		
E-mail traffic (Dr.Web Mail Security Suite)	<div><div></div> UNIX</div> <div><div></div> MS Exchange</div> <div><div></div> Lotus Domino</div> <div><div></div> Kerio</div>	<div><div></div> Anti-virus</div>	<div><div></div> Anti-spam</div> <div><div></div> SMTP Proxy</div> <div><div></div> Control center</div>	<div><div></div> Any number of users</div> <div><div></div> Servers — any number of users less than 3 000</div>		
Traffic (Dr.Web Gateway Security Suite)	<div><div></div> UNIX Internet gateways</div> <div><div></div> Kerio Internet gateways</div>	<div><div></div> Anti-virus</div>	<div><div></div> Control center</div>	<div><div></div> Any number of gateway users</div> <div><div></div> Servers — any number of users less than 3 000</div>		
	<div><div></div> Qbik</div> <div><div></div> MIMESweeper</div> <div><div></div> Microsoft ISA Server and Forefront TMG</div>		<div><div></div> Anti-spam</div>			
Mobile devices (Dr. Web Mobile Security Suite)	<div><div></div> Windows Mobile</div> <div><div></div> Android</div>	<div><div></div> Comprehensive protection</div>	<div><div></div> Control center</div>	<div><div></div> Any number (depends on Dr.Web Desktop Security Suite license)</div>		
	<div><div></div> Symbian OS</div>					
Now you have all necessary data to calculate the price.						

* This step is essential for choosing protection for workstations only, as the choice of the license depends on OS.

► 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.

Dr.Web Enterprise Suite unique features

- comprehensive protection from most known threats powered by the built-in anti-virus, anti-spam, firewall and office control (available with a comprehensive protection license);
- support of Windows and UNIX server platform, simple installation procedure and reliable protection providing minimal TCO compared with competitive solutions;
- centralized protection of all network hosts: workstations, mail and file servers as well as application servers including terminal servers;
- support of 32- and 64-bit operating systems;
- installation of agent software in an infected system with a high probability for successful curing;
- minimal network load achieved through implementation of a small-sized engine featuring latest technologies;
- highly efficient detection of threats including unknown viruses;
- administration of the entire network protection infrastructure from one computer (over the administration web-interface) from any location even outside the corporate network;
- implementation of individual security policies for groups of employees at the company;
- several administrators can manage different groups separately making Dr.Web Enterprise Suite a good choice for companies with high security requirements as well as for 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;
- protection of networks that are not connected to the internet;
- several installation methods – active directory policies, launch scripts and the built-in remote installation procedure. Installation can still be performed even if the host is unreachable for a Dr.Web enterprise suite server;
- support of most known internal and external databases. Oracle, PostgreSQL, Microsoft SQL Server or any other DBMS that supports SQL-92 over ODBC;
- support of custom event handlers written by the user in any script language providing direct access to internal interfaces of Dr.Web Enterprise Suite;
- updates rollback – even if updating causes an error, the host won't remain unprotected;
- Dr.Web Enterprise Suite is an open solution allowing a system administrator to use it to install and synchronize products from other developers thus lowering 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.
- low traffic. A special information exchange protocol facilitates compression of data transferred between clients and the server.

 Dr.Web LiveDemo online testing service: http://download.drweb.com/live_demo

► 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 for Linux
- Dr.Web for OS X
- Dr.Web for MS DOS, OS/2

Supported OS

Dr.Web for Windows	Dr.Web for Linux	Dr.Web for OS X	Dr.Web console scanners
Windows 2012/8/7/2008/ Vista/2003/XP SP 2 (32- and 64-bit)	GNU/Linux for Intel x86/amd64 with kernel 2.6.37 (and later) and glibc 2.13 (and later)	OS X v.10.7 and higher (32&64-bit systems)	Windows, 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 8/7/Vista	Windows 8/7/Vista/ XP/2000 SP4 + Rollup 1	Linux	OS X	MS DOS, OS/2
Basic license	Comprehensive protection	Anti-virus Windows 8/7/Vista/XP SP2/2000 SP4 + Rollup 1 (32&64 bit)			
Basic license components	<ul style="list-style-type: none"> ■ Anti-virus ■ Anti-spy ■ Anti-rootkit ■ Anti-spam ■ HTTP-monitor ■ Office control ■ Firewall 	<ul style="list-style-type: none"> ■ Anti-virus ■ Anti-spy ■ Anti-rootkit ■ Firewall 	<ul style="list-style-type: none"> ■ Anti-virus ■ Anti-spy 	<ul style="list-style-type: none"> ■ Anti-virus ■ Anti-spy ■ Anti-rootkit 	<ul style="list-style-type: none"> ■ Anti-virus ■ Anti-spy ■ Anti-rootkit
Additional components					
Control center	+	+	+	+	-

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

Read descriptions of Dr.Web for Windows, OS X, Linux and console scanners in the Dr.Web Home Security Suite section. Dr.Web Security Space equals to the Comprehensive protection license.

► Dr.Web Server Security Suite

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

- Dr.Web for Windows Server
- Dr.Web for Novell NetWare Server
- Dr.Web for OS X Server
- Dr.Web for UNIX (Samba) Server

Supported OS

Dr.Web Windows Server	Dr.Web UNIX Server	For OS X Server	Dr.Web Novell NetWare Server
Microsoft Windows Server 2000* / 2003 (x32 & x64*) / 2008 / 2012 (x64)	<ul style="list-style-type: none"> ■ Linux v. 2.4.x and higher ■ FreeBSD v. 6.x and higher for Intel x86 ■ Solaris v.10 for Intel x86 	OS X Server v.10.7 and higher	Novell NetWare v. 4.11–6.5

* Only for version 7.0.

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

	Windows	Novell NetWare	OS X Server	UNIX
Basic license	Anti-virus			
Additional components				
Control center	+	+	+	

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

► 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 functions

- 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
- Neutralisation of threats even during installation
- Smart optimisation takes into account available system resources
- Multi-thread scanning technology and performance optimisation yield maximum scanning speed
- Notification system does not distract the user with multiple pop-ups
- 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*
- Background scanning and active threat neutralization subsystem – Dr.Web 8.0 for Windows can eliminate any threat, no matter how resistant it is to removal
- Within the local network, the Dr.Web anti-virus for Windows can be controlled from any computer connected to the LAN, without installing Dr.Web Control Center.
- Express/Full/Custom scan of RAM, logical drives, CDs, network drives, folders, files, email files, boot records and other objects in the system

System requirements

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

☀ Description: <http://products.drweb.com/fileserver/win>

* Available for Windows Server 2008 and above.

** Only for version 7.0.

► Dr.Web for OS X Server

Anti-virus protection of workstations operated by OS X server versions

Key functions

- 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.

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

System requirements

- OS X Server 10.7 or higher
- Intel
- RAM — as required by the OS
- Internet access for registration and updating

🔗 Description: <http://products.drweb.com/fileserver/mac>

► Dr.Web for Novell NetWare

Anti-virus protection of file servers

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

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

System requirements

- Novell NetWare v.4.11-6.5 with updates from Minimum patch list installed

🌐 Description: <http://products.drweb.com/fileserver/novell>

► 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) 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).

🔍 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, OS X*)

* Under development.

Supported OS

Dr.Web product	Windows	Linux	FreeBSD	Solaris
		for Intel x86		
Dr.Web for UNIX Mail Servers		v. 2.4.x and higher	v. 6.x and higher	v. 10
Dr.Web for MS Exchange	Server 2000/2003/ 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		

Licensing 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

	MS Exchange	IBM Lotus Domino	UNIX	Kerio
Basic license	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.

► Dr.Web for UNIX Mail Servers

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

Key functions

- 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.

Implemented 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;
- Solaris v. 10 for Intel x86.

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.

🔗 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

- Microsoft Exchange Server 2000/2003:
Pentium 133 MHz, recommended – Pentium 733 MHz. RAM: 512 MB. Free disk space: 512 MB. Microsoft® Windows Server® 2003 (Standard, Enterprise or Datacenter edition) with installed SP1 or later.
- Microsoft Exchange Server 2007/2010:
Intel x64 supporting Intel 64; AMD supporting AMD64. RAM: 2 GB. Free disk space: 512 MB. Microsoft® Windows Server® 2003 R2 x64 with SP2 installed; Microsoft® Windows Server® 2008 x64; Microsoft® Windows Server® 2008 R2.
- Microsoft Exchange Server 2013/2016:
Intel x64 supporting Intel 64; AMD supporting AMD64. RAM: 4 GB. Free disk space: 1 GB. Microsoft® Windows Server® 2008 R2; Microsoft® Windows Server® 2012; Microsoft® Windows Server® 2012 R2.

🌐 Description: <http://products.drweb.com/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.

System requirements

Version for Windows

- OS: Windows Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 (32- and 64-bit);
- Lotus Domino v. R6.0 or higher;
- 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 7.x or 8.x;
- CPU Pentium 133 and higher;
- RAM 64 MB (128 MB recommended)
- Free disk space: 90 MB.

🔗 Descriptions: <http://products.drweb.com/lotus>

► Dr.Web for Kerio Mail Servers

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

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

Advantages

- Perfect compatibility with Kerio mail servers tested by Kerio Technologies;
- Operation in the centrality-managed protection mode when the anti-virus is administered via the Dr.Web Enterprise Security Suite Control Center;
- 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.

System requirements

Version for Windows

- Hard disk space: at least 350 MB;
- Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008/2012 (32- and 64-bit);
- Mail server – Kerio MailServer 6.2 or later, Kerio Connect 7.

Version for Linux

- Hard disk space: at least 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 и 11.1; CentOS Linux 5.2 и 5.3; Debian 5.0; Ubuntu 8.04 LTS;
- Mail server – Kerio MailServer 6.2 or later, Kerio Connect 7.

🌐 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 MIMesweeper
- Dr.Web for Qbik WinGate

Supported OS

	Windows	Linux	FreeBSD	Solaris
		for Intel x86		
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 MIMesweeper	2000 Server SP4 and higher/Server 2003 and higher			
Dr.Web for Qbik WinGate	Vista/Server 2008/ Server 2003/ XP/2000 (32&64 bit systems)			

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

		UNIX gateways	Kerio gateways	MIMesweeper	Qbik
Basic license	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.

► Dr.Web for Internet Gateways UNIX

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

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.

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.

Supported OS

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

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

- Squid 3.0 or later
- SafeSquid 3.0 or later

☼ Descriptions: <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

Dr.Web for Internet Gateways Kerio is an anti-virus plugin connected to Kerio Firewall. The plugin is installed onto a computer running the firewall and is then used by that computer as an external anti-virus.

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;
- Operation in the centrality-managed protection mode when the anti-virus is administered via the Dr.Web Enterprise Security Suite Control Center;
- 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;
- Information on the program's operation accessible through the web console;
- 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;
- Customizable list of notification mail recipients;
- Automatic updating of virus databases.

System requirements

Windows version

- 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).
- Kerio WinRoute Firewall 6.2 or later, Kerio Control 7.0.0 or later.

The version for Kerio Control VMware Virtual Appliance and Kerio Control Software Appliance

- At least 290 MB of free disk space.
- Kerio Control VMware Virtual Appliance or Kerio Control Software Appliance.
- Kerio Control 8.x or later.

🌐 Description: <http://products.drweb.com/gateway/kerio>

► **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 with SP4 or higher or Windows Server 2003 or later
- ClearSwift MIMESweeper™ for SMTP 5.2 or later.

🌐 Descriptions: <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.

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.

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.

🌐 Description: <http://products.drweb.com/gateway/qbik>

► Dr.Web Mobile Security

Protection of mobile devices

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

	Dr.Web for Symbian OS	Dr.Web for Windows Mobile	Dr.Web for Android
Protection components	Anti-virus & anti-spam	Anti-virus & Anti-spam	Comprehensive protection*
Centralized administration in Dr.Web Enterprise Security Suite	—	+	+
Supported OS	S60, Symbian 9 or later	Windows Mobile 2003/2003 SE/5.0/6.0/6.1/6.5	Android 4.0-5.0 The firewall supports Android 4.0 and higher
Key features			
Real-time scan	+	+	+
Scan of files received over GPRS/Infrared/Bluetooth/Wi-Fi/USB-connection or while synchronizing with a PC	+	+	+
Two types of scan: full and custom	+	+	+
Toggling on/off memory card scan	+	+	+
On-demand scan of the entire file system or of separate files and folders	+	+	+
Scan of APK, ZIP, SIS, CAB, RAR, JAR archives	+	+	+
Black and white lists for numbers from which calls and short messages are received	+	+	+
Deletion of infected files	+	+	+
Moving suspicious files to the quarantine	+	+	+
Restoring files from the quarantine	+	+	+
Updating over the Internet: <ul style="list-style-type: none"> ■ over HTTP by means of the embedded GPRS module; ■ over Infrared/Bluetooth/Wi-Fi/USB-connection; ■ over an ActiveSync connection during synchronization with a PC 	+	+	+
Detailed scanning reports	+	+	+
Control your lost mobile device remotely with the Anti-theft function			+
CloudChecker — web link check			+

* The license covers the following components: anti-virus, anti-spam, anti-theft, parental control.

Licensing of Dr.Web Mobile Security

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

License options

Dr.Web for Windows Mobile	Dr.Web for Symbian OS	Dr.Web for Android
■ Anti-virus + Anti-spam + Control center	■ Anti-virus + Anti-spam	■ Comprehensive protection + Control Center

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

🔍 Description: <http://products.drweb.com/mobile/biz>

Dr.Web Retail Security Suite



Dr.Web Security Space



Dr.Web Anti-virus



Dr.Web SOHO bundle
5 PC / 1 file server

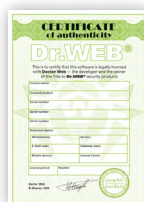
Dr.Web Universal (for ASC customers)

Dr.Web Universal media-kits are delivered only to Dr.Web Authorized Service Centers and available to ASC customers at a special price.

The product provides protection for one PC and one mobile device for one year.

The license covers the following products:

- Dr.Web Security Space
- Dr.Web anti-virus for OS X
- Dr.Web anti-virus for Linux
- Dr.Web Mobile Security Suite
- Dr.Web for Android OS
- Dr.Web for Symbian OS
- Dr.Web for Windows Mobile



Dr.Web Enterprise Suite is delivered as follows

- Corporate envelope
- License Certificate
- Distribution disc

More information about Dr.Web authorized centers: <http://partners.drweb.com/service>

Dr.Web retail sales handbook:
https://st.drweb.com/static/new-www/files/booklet_85x210_12pages_for_site_en.pdf

Dr.Web Bundles

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

All Dr.Web products 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 Universal Bundle

Product	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 + Anti-spam
Quantity	5–50	1	Equals to number of WSs	Equals to number of WSs (from 25)	Equals to number of WSs

☼ 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

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	<ul style="list-style-type: none">■ Emergency curing for Windows workstations and servers■ Verifies the quality of the anti-virus software currently in use
Features	<ul style="list-style-type: none">■ 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)
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

► 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	<ul style="list-style-type: none"> ■ Cure Windows workstations and servers ■ Verifies the quality of the anti-virus software currently in use
Features	<ul style="list-style-type: none"> ■ 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 8/7/Vista/XP/2000/Server 2012/2008/2003 (32- and 64-bit systems)
Licensing	The utility is licensed per number of workstations for 1, 2, or 3 years of use.
Licensing features	The utility is available for free when used for non-business purposes.
Demo version	N/A

Solutions

Dr.Web Security Suite for UNIX Appliance is a modular set of solutions for integration with appliances running UNIX-like operating systems (Linux/FreeBSD/Solaris(x86)).

The solutions operate as a corporate Internet gateway (proxy-server) used by users of an intranet to access resources of the Internet.

	Dr.Web Mail Security Suite for UNIX Appliance	Dr.Web Gateway Security Suite for UNIX Appliance
Key features	Virus and spam filtering for e-mail	Virus filtering for HTTP- and FTP-traffic
Licence options	Antivirus Antivirus + Anti-spam	Antivirus

Licence types

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

SDK licensing

The SDK is distributed free of charge and is shipped with the product. Third-party developers can create plugins using the SDK and distribute them for free. Certification is required for commercial distribution of such plugins.

Services

Doctor Web was the first vendor to offer an anti-virus as a service in Russia.

► Dr.Web AV-Desk



Dr.Web AV-Desk was created in 2007. The number of service providers that deliver the Dr.Web anti-virus service in different regions of Russia and also in the Ukraine, France, Spain, Netherlands, Mongolia, Kazakhstan, Kyrgyzstan, Bulgaria and Estonia and other countries exceeds 250.

What is Dr.Web AV-Desk?	Dr.Web AV-Desk is a business model that will help a provider attract new customers and increase its profits. It is the Internet-service used to deliver anti-virus and anti-spam protection services to an unlimited number of subscribers. It is also the software for centralized management of the delivery process.
Who are customers of Dr.Web AV-Desk?	ISPs and various IT-security service providers.
Who are customers of Dr.Web anti-virus as a service?	Any individual or a company that signs a contract with the provider regarding the delivery of the service on a subscription basis.
What services can be delivered with the help of Dr.Web AV-Desk?	Dr.Web anti-virus service which is a time-limited right (a license) to use Dr.Web to protect the subscribers' PCs on a monthly payment base.
What is the functionality of Dr.Web AV-Desk	This is a software for IT service providers designed to centrally administer anti-virus security services for an unlimited number of customers.
Licensing of Dr.Web AV-Desk	Dr.Web AV-Desk is licensed free of charge. Dr.Web Anti-virus as a service is licensed per number of customers to whom the service was delivered in the reported month.

How does it work?

IT service provider	Customers
<ul style="list-style-type: none"> ■ Delivers subscriptions to its customers ■ delivers to customers updates of the virus database (optional) ■ supports customers (optional) ■ monitors the operation of the anti-virus network using the administrator console (optional) ■ provides with additional services ■ collects the subscription fee 	<ul style="list-style-type: none"> ■ subscribe to the service and install Dr.Web for Windows ■ manage the subscription: activate \ suspend \ terminate the subscription ■ pay a subscription fee

Any ISP or any IT service provider can become a supplier of Dr.Web as a service.

Service Reseller	Service Provider	Service aggregator
A company uses the Subscription Control Centre integrated into its web-site to provide its customers with subscriptions to the Dr.Web anti-virus service.	A company deploys Dr.Web AV-Desk and delivers the Dr.Web anti-virus service to its subscribers.	A company owns server hardware on which it deploys Dr.Web AV-Desk. The company creates a reseller network and delivers the Subscription Control Centre to resellers on the sublicensing basis. Can't deliver the service directly to end-users.

More details about Dr.Web AV-Desk and Dr.Web anti-virus as a service is provided to partners upon request.

🔗 New test for the course DWCERT-004 Dr.Web AV-Desk v.6:

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

🔗 New test for the course DWCERT-010-3 Dr.Web anti-virus as a service:

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

Discount policy

Discount multipliers are applied to the price of a one-year license as defined in the price list.

If a customer is entitled to several discounts, they are not combined. Instead the customer receives the largest of the discounts.

Discounts are available for the price list offers only. Discounts for special orders must be agreed upon with Doctor Web's sales managers.

Discounts are given for the number of licensed Dr.Web Enterprise Security Suite products

In each case, product quantity discounts (per types of licensed objects) are determined according to the total amount due for basic licenses as well as for the additional components purchased separately for each product. The calculator applies the discounts automatically.

Number of licensed products	Discount
4	30%
3	25%
2	20%

Exception: discounts do not apply to Dr.Web Mobile Security Suite.

Restrictions

These discounts are not available to customers if:

- The number of servers amounts to less than 10% of the number of workstations, e-mail users, or gateways;
- The number of e-mail users or gateways is smaller than the number of workstations and vice versa;
- The number of e-mail users is smaller than the number of gateway users and vice versa.

Discount table

Customer type	Discount condition – required documentation	New license			Renewal			Migration*		
		1 year	2 years	3 years	1 year	2 years	3 years	1 year	2 years	3 years
Returning customer	Renewal discount – Dr.Web key file or serial number for a similar Dr.Web product that is valid for at least six months									
Migrating customer	Migration discount – original copy of the license / key file / confirmation e-mail received upon purchasing an electronic license for the other vendor's anti-virus	–	1,6	2,2	0,6	1,17	1,72	0,5	1	1,5
Educational institutions, libraries, museums, and health care institutions	A completed application and a copy of a document, issued by a competent authority, that authorizes the entity in question to carry out education- or healthcare-related activities	0,5	0,85	1,2	0,35	0,7	1,05			

Renewal terms

1. Both valid and expired licenses can be renewed. No expiration date limitation is placed on Dr.Web licenses that are subject to renewal.
2. A renewal discount is provided only if the term of the previous license is at least six months in duration.
3. A renewal discount is provided only if a one-, two-, or three-year license is purchased for a similar Dr.Web anti-virus product.
4. A renewal discount is provided for protected objects whose number is less than or equal to the number of protected objects covered by the previous license that is subject to renewal.
5. To receive a discount, a Dr.Web key file or a serial number must be provided (for renewals, each such key file or serial number can be submitted only once).
6. To receive a renewal discount, a customer must present a serial number or a key file (including OEM) to the salesperson carrying out the transaction.

«Switch to Green»

The Doctor Web migration program that offers great incentives to corporate customers switching to Dr.Web Anti-virus products

1. This special offer concerns only Dr.Web products. Bundles, utilities, appliances, services, and solutions are not included in the migration program.
2. "Switch to Green" is a one-time offer for corporate customers only.
3. The migration discount is not available for holders of OEM licenses.
4. If a customer migrates to a one-year Dr.Web license, the discount is applied is 50%. If a customer migrates to a two- or three-year license, multipliers of 1 and 1.5 respectively are applied to the price of a one-year Dr.Web license.
5. A migration discount is given only for a similar Dr.Web anti-virus product (the type and number of protected objects must be the same).
6. To receive a migration discount, one of the following must be supplied: an original copy of a license, a key file, or a purchase confirmation e-mail containing registration information.
7. Users of valid and expired licenses are granted a discount provided that a user contacted a Doctor Web partner not later than 30 days since a license has expired.
8. If the license period of the anti-virus, from which a customer is migrating, is still valid on the date the customer purchases the Dr.Web license, the remaining term of the customer's original license will be added to the term of the new Dr.Web license free of charge.
9. The subsequent renewal of a migration license is subject to standard renewal discounts.
10. Migration discounts cannot be combined with any other discounts.

General terms of sale

1. Partners must sell Dr.Web products to end users at the prices shown in the price list.
2. The prices for all Dr.Web products with standard packaging as shown in the price list include updating program modules and virus databases and basic technical support via a support request form located at <http://support.drweb.com>.
3. If licenses are ordered in boxes, the cost of a media kit is added to the price.
4. If a customer needs a solution to protect a number of objects that exceeds the maximum quantity set in the price list, the partner must contact Doctor Web and request a price using the form located at <https://pa.drweb.com/support/>. The following information about the customer must be provided:
 - Company name
 - Address
 - E-mail
 - Telephone number of the engineer responsible for anti-virus software maintenance
 - Partner technical support contact information

Any discounts for such customers must be agreed upon with Doctor Web.

🔗 Request a price: <https://pa.drweb.com/support/price1/>

Dr.Web Enterprise Security Suite additional purchase

General rules

1. An additional license purchase (or license expansion) during its period of validity can be:
 - **Qualitative** – if new protection components are added to the license while the products in the license remain unchanged.
 - **Quantitative** – if the number of protected objects is increased but the products covered by the license remain unchanged.
 - **Product** – new products are added to the current license.

An additional purchase can consist of a combination of the types listed above.

2. The minimum license period for an additional purchase is 3 months.
3. The remaining license period is set according to the period remaining for the objects covered by the previously purchased license (an incomplete month is rounded up to 1 month).
4. An additional purchase is only available for valid licenses that expire in no less than 3 months' time; otherwise an additional purchase is combined with a renewal.
5. License type in the code of the new license is C (additional purchase).
6. The license for an additional purchase is activated automatically, as soon as it is generated.
7. The previous license is blocked within 24 hours after the license for the additional purchase has been registered, and it can't be renewed. To renew, the customer has to provide information about the additional license purchased.

Additional purchase and renewal

1. Additional purchase and renewal' is available for valid and expired licenses.
2. When 'additional purchase and renewal' is provided for a license that is still valid, the period remaining on the previous (unexpired) license is added to the term of the new license (the 'additional purchase and renewal' license).
3. License type in the code of the new license is D (additional purchase+renewal).
4. When generated, an 'additional purchase' license is activated automatically.
5. The previous (renewed) license is blocked within 24 hours after the 'additional purchase and renewal' license has been registered, and it can't be renewed. To renew, the customer has to provide information about the license for the additional purchase.
6. If an additional purchase and a renewal are made simultaneously, the price of the additional purchased licenses is calculated according to the price group for the total number of purchased licenses (renewed + purchased). The price of RENEWED licenses is calculated according to the price group for the number of RENEWED licenses.

Additional purchase price calculation rules

I. Qualitative additional purchase (components are added to the license while the number of protected objects and the product contents remain unchanged).

1. If an upgrade is required from the Anti-virus to **Comprehensive protection for Dr.Web Desktop Security Suite products**, the per-month price of the anti-virus license is increased by 20% and then multiplied by the number of months remaining on the license.

Example

A customer paid 1,628 Euro for a new license to protect 90 PCs with Dr.Web Anti-virus. The customer decided to upgrade to comprehensive protection two months after the license was activated.

$1,628 \text{ Euro} \times 12 \text{ months} \times 0.2 \text{ (marked up by 20\%)} \times 10 \text{ months} = 271 \text{ Euro (the upgrade fee)}$.

The total cost of the license to the client is **1,899 Euro**.

2. If the customer wants to make an additional purchase of the **Anti-spam** for Dr.Web Mail Security Suite or Dr.Web Gateway Security Suite, the price they paid for the Anti-virus or Anti-virus + SMTP proxy license is marked up by 40%.

Example

A customer paid 1,300 Euro for an Anti-virus license to protect 90 mail users. Two months later, they decided to add the Anti-spam to their license.

$1,300 \text{ Euro} \div 12 \text{ months} \times 0.4 \times 10 \text{ months} = 433 \text{ Euro (the surcharge for adding the Anti-spam to the license)}$.

The total cost of the license to the customer is **1,733 Euro**.

3. If an **SMTP proxy** needs to be added to the license, the price paid for the Anti-virus license or the Anti-virus + Anti-spam license is marked up by 20%.

The table of surcharges for a qualitative additional purchase when the number of protected objects remains unchanged

Product	Current License	New license	Surcharge
Dr.Web Desktop Security Suite	Anti-virus	Comprehensive protection	20%
Dr.Web Mail Security Suite or Dr.Web Gateway Security Suite	Anti-virus	+ Anti-spam	40%
	Anti-virus + SMTP proxy		
	Anti-virus	+ SMTP proxy	20%
	Anti-virus + Anti-spam		

II. Quantitative additional purchase (the number of protected objects is increased)

The additional purchase price is calculated on the basis of the current price list according to the total number of protected objects, **without any discount**.

III. Product additional purchase (the expansion of product contents)

The price of the license for the additional purchase is calculated on the basis of the current price list with **no discount for the number of products**.

Business products for which 'additional purchase' is unavailable

- Dr.Web SOHO bundle box.
- Dr.Web Universal and Dr.Web Safe School bundles.

To expand their license for any of these products, the customer must upgrade to Dr.Web Enterprise Security Suite according to the 'additional purchase and renewal' terms.

Dr.Web license codes

Rules

1. A code always consists of 5 groups.
2. Each group is separated from another group(s) by a hyphen.
3. A separate license code is formed for each Dr.Web Product.
4. The codes for boxed products and OEM-products are in the price list.
5. If an additional purchase is required, 2 license terms are specified in a code: the whole desired license term and – with a column – the remaining period of the current license.
6. If an additional purchase + renewal is required, 2 license terms are specified in a code: the whole desired license term and – with a column – the remaining period of the current license.
7. If an additional purchase is required, 2 quantities of protected objects are specified in a code: the whole desired quantity and – with a column – the quantity of the current license.
8. If an additional purchase + renewal is required, 2 quantities of protected objects are specified in a code: the whole desired quantity and – with a column – the quantity of the current license.

Code symbols

1 group			2 group		3 group	4 group	5 group	
Packaging	Product line category	Protected objects	Basic license	Additional components	License term	Quantity of protected objects	License type	Discount
L – an e-license	B – product for business	G – users of gateways	A – Anti-virus	A – Anti-spam	XXM – where XX is the number of months	Any number	A – new license	1 – educational discount
	H – product for home							
B – a boxed product	X – a license supplied in Dr.Web Office Shield	M – mobile devices	B – Comprehensive protection	C – Control center	XXXD – where XXX is the number of days	UL – unlimited (for unlimited license)	B – renewal	2 – promotion
A – a promotional boxed product							C – additional purchase	3 – no discount
C – scratch-card	Y – curing utility	P – users of e-mail	K – Katana	K – no additional components			D – renewal + additional purchase	4 – migration
D – delivery in a DVD box	Z – bundle	S – servers	* – a license for several products (used in Bundles)	R – Cryptograph			R – Rescue Pack	5 – NFR license for partner
K – delivery in a license package		W – workstations		S – SMTP proxy			F – OEM-license	6 – NFR- license (demo) for customer
M – delivery on a disk (OEM including)		Z – all objects					G – service license	7 – marketing
N – delivery in a certified license package							H – technical support not included	8 – charity
P – delivery in an OEM-package							V – an important customer	9 – key split
Q – sales via SMS								10 – key combining
								11 – key change

Examples

Examples for Products

1.	A new customer – an education establishment – wants to protect 200 WS with a Control center, Comprehensive protection, for 12 months.	LBW-BC-12M-200-A1
2.	A customer – an education establishment – bought a license for protection of 200 WS with a Control center, Comprehensive protection, for 12 months. The remaining license period is 6 months. A customer wants to additionally buy protection for 10 WSs.	LBW-BRC-6M-210:200-C1
3.	A customer has a license from example 2. The remaining license period is 7 months. A customer wants to additionally buy protection for 10 WSs and renew his license for 12 months.	LBW-BRC-31M:7M-210:200-D1

Examples of codes for Bundles

1.	A customer wants to buy Dr.Web Universal to protect 50 WSs, for 12 months, e-license.	LZZ-*C-12M-50-A3
2.	A customer – a school – wants to protect 100 WSs.	LZZ-*C-12M-100-A1

Examples of codes for curing utilities

1.	A customer wants to check and cure 100 WSs of the corporate network during 10 days.	LYW-AC-10D-100-A3
2.	A customer wants to check and cure 10 stand alone WSs during 30 days.	LYW-AK-30D-10-A3

Contacts

Russia

Doctor Web

125124, Russia, Moscow, 3d street Yamskogo polya 2-12A
Phone: +7 (495) 789-45-87, +7 (495) 789-45-86 (support)
Fax: +7 (495) 789-45-97
www.drweb.com | www.av-desk.com | www.freedrweb.com

Deutschland

Doctor Web Deutschland GmbH

Rodenbacher Chaussee 6, D-63457 Hanau
Tel: +49 (0) 6039-939 54 14
Fax: +49 (0) 6039-939 54 15
Web-site: www.drweb-av.de

Kazakhstan

Doctor Web — Central Asia

Kazakhstan, 050009, Alma-Ata, Shevchenko street, 165B, office 910
Tel: +7 (727) 323-62-30, +7 (727) 323-62-31, +7 (727) 323-62-32
Sales department: sales@drweb.kz
Support department: support@drweb.kz
Web-site: www.drweb.kz

Ukraine

Technical support center "Doctor Web"

Pushkinskaya, 27, office 6, Kiyev 01601, Ukraine
Tel/fax: +38 (044) 238-24-35
E-mail: dr.web@drweb.ua
Web-site: www.drweb.ua

France

Doctor Web France

333b, Avenue de Colmar, 67100 Strasbourg
Tel: 03 90 40 40 20
Fax: 03 90 40 40 21
E-mail: p.curien@drweb.com
Web-site: www.drweb.fr

Japan

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F,
1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken
210-0005, Japan Tel: +81(0)44-201-7711
Web-site: www.drweb.co.jp

China

Doctor Web Software Company (Tianjin), Ltd.

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