Dr.WEB®
Made in Russia

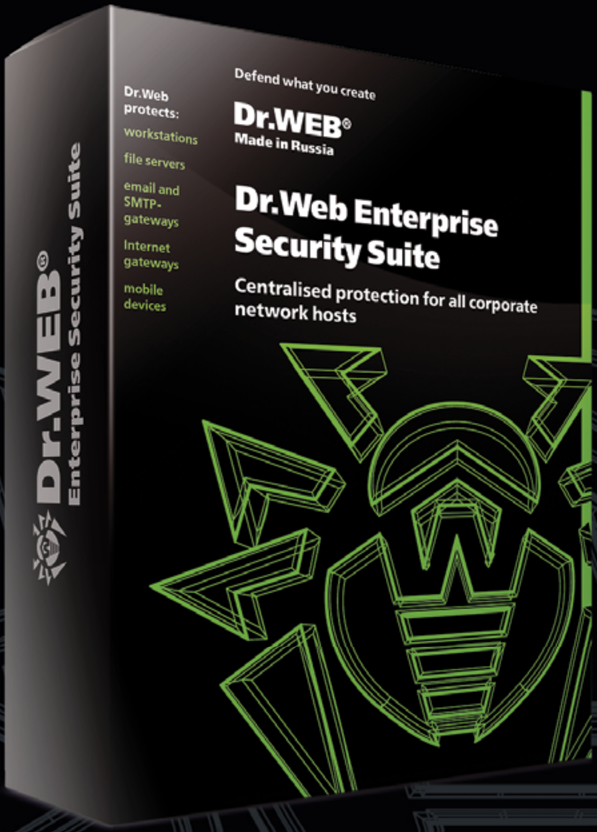
DEFEND WHAT YOU CREATE

Dr.Web Mail Security Suite

For MS Exchange

https://www.drweb.com

A highly intelligent anti-virus and anti-spam protection system for large volumes of email traffic



- Company employees who use their unprotected personal PCs and devices for work send their clients and partners emails containing malicious attachments.

Installing an anti-virus and an anti-spam on your employees' workstations won’t interfere with their ability to send and receive email on their personal devices.

- Once a company's employees receive phishing emails from cybercriminals, they try to open them and launch attachments, thus, violating security requirements.
- Top managers forward emails sent by cybercriminals to their employees, and those employees perform the required actions.

Infected email and spam must not reach employee computers or be forwarded from their unprotected devices.

Dr.Web for MS Exchange:

Filters email messages for malware, spam, and phishing emails.	Removes previously unknown malicious programs from mailboxes.	Filters mail traffic according to specified criteria.
Guarantees secure conditions for employees who work at home and on business trips.	Accelerates mail-traffic processing due to spam messages getting filtered out.	Individual settings for both different groups of employees and service administrators.
Analyses of statistics using a filter system.	Searches for needed events according to specified parameters.	Analyses of email infection sources.

A malicious attachment has no chance of being launched on a computer if it is filtered out on the mail server.

Dr.Web для MS Exchange means clean in-coming traffic from your partners and customers. Even if your domain gets hacked or your traffic gets intercepted by cybercriminals, they won't be able to send you viruses and spam, for example, in the form of a response to an email.

If a company's network gets infected, it is email that can become a source of viruses and a way for viruses to invade all the network nodes; this is because the malicious programs on an infected machine have access to the user’s address book which may contain both your colleagues' addresses and your customers' addresses.

The benefits of Dr.Web for MS Exchange

- It can be installed on both a separate server and a server cluster.
- Detects malicious files and spam whose samples have not yet been analysed.
  - By installing the Dr.Web anti-virus, a company can prevent situations where their server becomes a source of infection.
- High-speed scanning combined with low consumption of system resources and special technology that protects servers from large volumes of spam allow Dr.Web to run smoothly even during mail server attacks.
- The built-in anti-spam, which requires no training (starts working as soon as you install it) and operates on the basis of rules, significantly lowers the server workload.
- Additional email traffic filtering features (filter by email address and domain blacklists and whitelists, certain types of messages, and file types) allow you to receive only those email messages that correspond to specified criteria.
- The high level of filtering for spam and fraudulent emails improves employee productivity.
- File filtering according to file type excludes attacks via file types that are not used by your employees and results in less traffic if your offices are geographically dispersed.
- Anti-virus scanning of MS Exchange storages to detect previously unknown malware.
- The ability to rescan attachments considered malicious in order to clarify the "diagnosis". A target object can be backed up before it is cured or deleted.
- Supports administration using Active Directory features.
- The ability to manage security settings using the method most convenient for the administrator — via a browser or the administrator console.
- The ability to update over the LAN in a network that is disconnected from the Internet.
- High operational performance and stability is achieved thanks to the multi-threaded scan feature.
- Detailed documentation in English.

Do your employees click on all the links in emails and open malicious attachments?
Deploying Dr.Web Enterprise Security Suite will solve this problem!

! **For maximum filtration quality**, use Dr.Web SMTP proxy — a filter that processes email messages before they reach your mail server.

Dr.Web Anti-spam filters unsolicited emails efficiently

Requires no training Starts protecting as soon as it is installed.	Successfully identifies spam messages **in any language**.	Actions can be customised for different categories of spam.
Record-low number of false positives.	Requires updating only once a day.	Uses its own blacklists and whitelists.
Effectively filters out messages containing the most recently released malicious attachments whose samples haven't yet been analysed by anti-virus laboratories.		

Dr.Web anti-spam technologies

Licensing

Dr.Web solutions use a single license for all mail servers. You do not have to change your license or make an additional purchase to transfer it to other mail servers, including when you switch operation systems!

Types of licenses	License options
▪ Per number of protected users ▪ Per-server license (up to 3,000 users) ▪ Unlimited license	▪ Anti-virus ▪ Anti-virus + Control Center ▪ Anti-virus + SMTP proxy ▪ Anti-virus + Control Center + SMTP proxy ▪ Anti-virus + Anti-spam ▪ Anti-virus + Anti-spam + Control Center ▪ Anti-virus + Anti-spam + SMTP proxy ▪ Anti-virus + Anti-spam + Control Center + SMTP proxy The Control Center is provided free of charge All licensing conditions

The Dr.Web SMTP proxy additional license allows incoming and outgoing email traffic on a mail proxy server to be filtered after the mail server has been disconnected from the Internet. This means:

The filtering quality is significantly improved due to the absence of any mail server restrictions.	A company’s mail server is protected from malicious attacks.	The workload decreases for local mail servers and workstations.	The mail-filtering system’s stability is improved.

System requirements are described in the product documentation.

Pre-sales support	Technical support
▪ Free Dr.Web product testing—in the customer's network or remotely. ▪ Deployment and assistance during the implementation process (by phone or via the tracker).	▪ 24/7 by phone and via the web form at https://support.drweb.com ▪ Free support services for price list licenses. ▪ The cost of support for ex-price and unlimited licenses is negotiated separately. ▪ Paid VIP support.

Services

Dr.Web vxCube

Designed for security researchers and cybercrime investigators, Dr.Web vxCube performs intelligent and interactive cloud-based analyses of suspicious objects to determine the extent to which they are malicious.

In situations when a malicious file has penetrated the protected system or you have reason to believe that an "impostor" has infiltrated your infrastructure, the cloud-based interactive analyser Dr.Web vxCube is indispensable.

In one minute, Dr.Web vxCube will assess how malicious a file is and provide you with a curing utility that will eliminate the effects of its activity. This lets you disarm a new threat extremely quickly, without waiting for your anti-virus to eventually receive an update that would address it.

Thanks to its versatility, Dr.Web CureIt! can operate without being installed in any system where another (non-Dr.Web) anti-virus is in use; this may particularly come in handy for companies that haven't yet chosen Dr.Web to be their primary means of protection.

Analysis results are provided in a report. Reports can be viewed in your Dr.Web vxCube account area or downloaded as archives.

Trial access: https://download.drweb.com/vxcube

Learn more about Dr.Web vxCube: https://www.drweb.com/vxcube

Anti-virus research

Malware analysis by Doctor Web security researchers

No automated routine can ever replace the experience and knowledge of a security researcher. If Dr.Web vxCube returns a “safe” verdict on your analysed file, but you still have your doubts about this result, Doctor Web's security researchers, who have a wealth of experience analysing malware, are ready to assist you.

With this service, a malicious file of any complexity can be analysed. The resulting report includes:

- Information about the malware’s basic principles of operation and that of its modules;
- An object assessment: downright malicious, potentially dangerous (suspicious), etc.;
- An analysis of the malware's networking features and the location of its command and control servers;
- The impact on the infected system and recommendations on how the threat can be neutralised.

You can submit an anti-virus research request here: https://support.drweb.com.

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web products have been developed since 1992.

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040
Phone: +7 495 789-45-87 (multichannel), fax: +7 495 789-45-97
https://www.drweb.com