Dr.WEB®

Made in Russia

Dr.Web Mail Security Suite

for MIMEsweeper

https://www.drweb.com

Anti-virus and anti-spam protection for mail traffic passing through ClearSwift MIMEsweeper content-filtering servers

- Included in the Register of Russian Computer Programs and Databases
- Minimum system requirements
- Protection even against unknown malicious programs

Defend what you create

Dr.WEB®
Made in Russia

Dr.Web Enterprise Security Suite

Centralised protection for all corporate network hosts

Dr.Web protects:

workstations

file servers

email and SMTP-gateways

Internet gateways

mobile devices
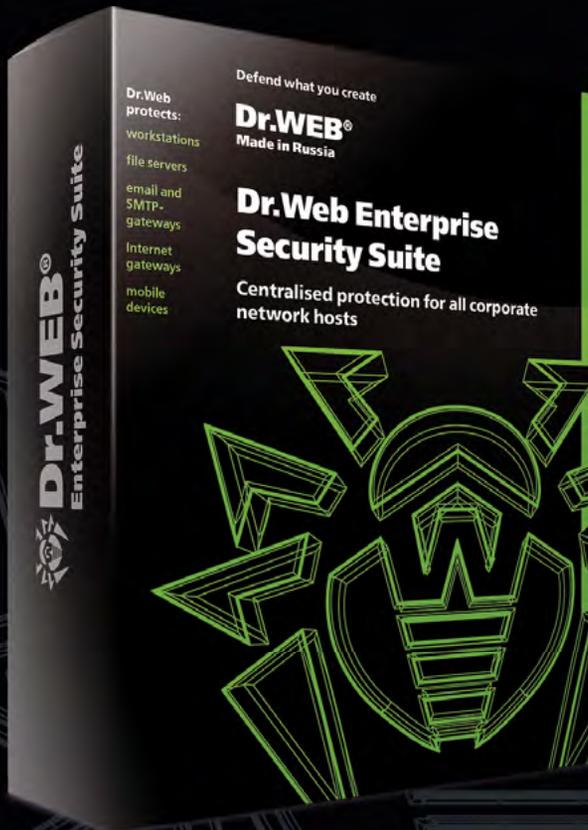
## Mail traffic is the main transport for viruses and spam

Many companies' business processes depend on their mail systems operating flawlessly and being free of viruses and spam.

If a network gets infected, it is email that can become a source of viruses: 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.

Dr.Web for MIMEsweeper is installed on the server on which the MIMEsweeper content filter has already been installed and works as the first-level scenario recommended by ClearSwift.

The product connects to MIMEsweeper as an anti-virus and anti-spam policy for checking mail and filters out viruses, spam, and other unsolicited messages. If a threat is detected, Dr.Web for MIMEsweeper classifies the message according to policies assigned by ClearSwift MIMEsweeper and disarms detected malicious objects.

Key features
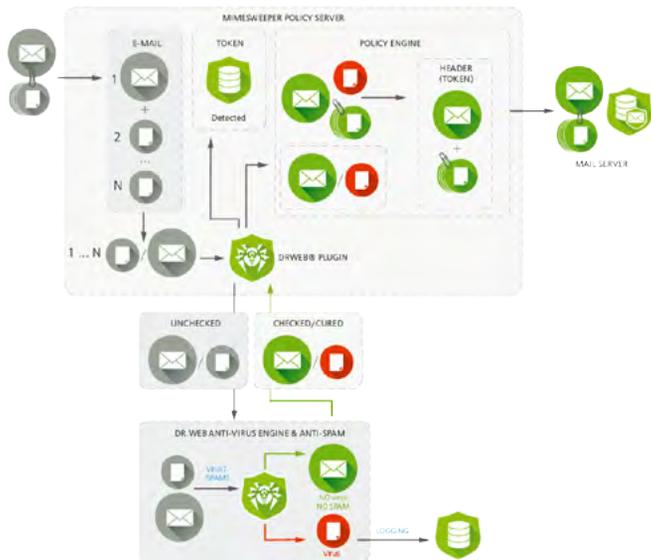
- Checks emails and attachments, including archives, before they are processed by the mail server.
- Cures infected objects.
- Isolates infected and suspicious files in the quarantine.
- Filters spam, including through the use of blacklists and whitelists.
- Operation logging.

Dr.WEB®
since 1992

Dr.Web for MIMEsweeper licensing

Types of licenses	License options
▪ Per number of protected users ▪ Per-server license ▪ Unlimited license	▪ Antivirus ▪ Antivirus + Antispam All licensing terms: https://license.drweb.com/products/biz

! ! A mail server is a service located on a standard file server. Therefore, you additionally need to protect the server itself and the channels that communicate with it.

When purchasing Dr.Web to protect both email and a server, customers receive a **20% discount**.

Pre-sales support	Technical support
▪ Free Dr.Web product testing. ▪ Deployment, assistance during the implementation process — by phone or on site (in Moscow only). ▪ Presentation, webinar, seminar. ▪ Assistance with writing or verifying technical specifications. ▪ Free training courses on the administration of Dr.Web products.	▪ 24/7 by phone and via the web form at https://support.drweb.com. ▪ Russian, English, German, French and Japanese spoken. ▪ The cost of support for ex-price and unlimited licenses is negotiated separately. ▪ Paid VIP support.

Services
Dr.Web vxCube

▪ Intelligent and interactive cloud-based analyses of suspicious objects for viruses

▪ An immediately generated curing utility based on analysis results

▪ For security researchers and cybercrime investigators

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. The examination takes from one to several minutes! Analysis results are provided in a report. Reports can be viewed in your Dr.Web vxCube account area or downloaded as archives.

If a file poses a threat, the user is instantly provided with a custom Dr.Web CureIt! build (if available under their license) that will neutralise the malware and undo any harm it has caused to the system.

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.

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

Find out 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

Virus-related computer incident expert consultations (VCI)

If malware has wreaked havoc in your corporate infrastructure and you require the expertise of security researchers to investigate the incident, Doctor Web's information security task force is at your service.

About VCI consultations: https://antifraud.drweb.com/expertise

Submit your consultation request here: https://support.drweb.ru/expertise

https://www.drweb.com • https://free.drweb.com • https://curenet.drweb.com