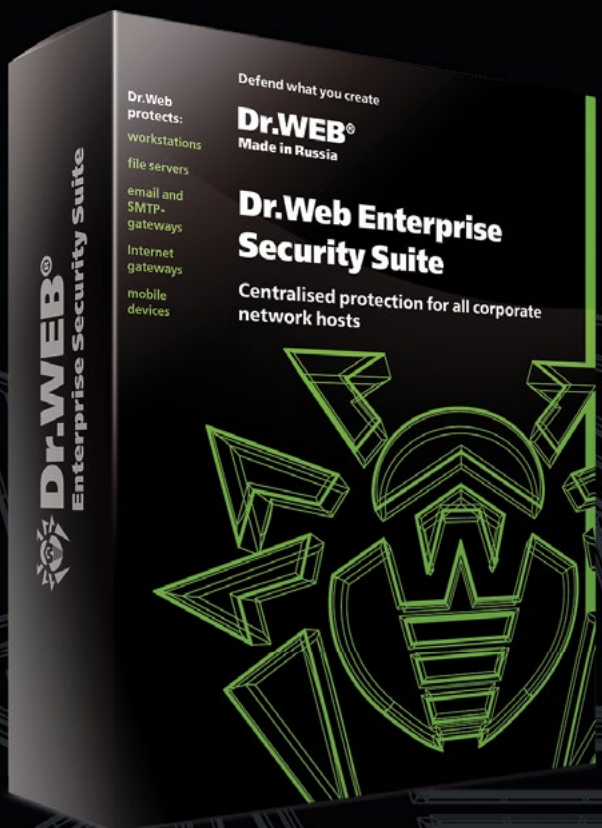
Dr.WEB®
Made in Russia

DEFEND WHAT YOU CREATE

Dr.Web Desktop Security Suite

For Linux

www.drweb.com



Dr.WEB®
Enterprise Security Suite

Attacking Linux-based workstations and devices is a trend right now. Their massive lack of security attracts criminals of all types.

Every day sees the emergence of up to 1,000 and more malicious programs for Linux, including miners and encryption ransomware. When employee-operated computers and devices get infected, companies lose not only the time spent working to restore them and the ransom money paid to get access to the infected devices, but also important documents: often the attackers themselves cannot decrypt the data they've encrypted but regularly take the ransom paid to get it back.

Installing the Dr.Web anti-virus prevents cybercriminals from engaging in activities that will lead to the loss of a company's information or the theft of its resources.

Dr.Web for Linux

▪ **Reliably protects** against all malicious programs, including those not yet analysed by Doctor Web	▪ **Protects against Windows-specific threats** launched under Linux — including with the help of Dr.Web Cloud	▪ **Scans HTTP traffic,** including secure connections	▪ **Remotely scans systems on which an anti-virus cannot be installed**	▪ **Possesses high operational performance and stability**
▪ **Periodically scans file system objects**	▪ **Blocks access to potentially dangerous sites,** using thematic databases, blacklists and whitelists	▪ **Blocks outgoing and incoming emails containing malware or unwanted links**	▪ **Helps protect workstations even during business trips and vacations** when the Anti-virus Control Center cannot be accessed	▪ **Network connection monitoring**

Dr.Web for Linux significantly r**educes an enterprise's expenses** and **makes its business processes more reliable**.

The ability to scan remote devices

Dr.Web for Linux lets you conduct remote scans not only of desktop computers but also of devices comprising the so-called Internet of Things—routers and set-top boxes.

High-speed scanning and up-to-date, 24-hour protection

Compact virus databases; Origins Tracing™, the non-signature technology used to scan for unknown viruses; and advanced heuristic analysis permit any, even unknown, malicious programs to be detected—at the moment of attack.

Protection against unknown malicious programs

Technology designed to detect the latest species of unknown malicious objects, including those hidden by unknown packers, is used to scan protected files and documents the moment they are requested.

Dr.WEB®
Enterprise Security Suite

Simple installation and flexible configuration — the deployment of Dr.Web can be controlled easily; flexible configuration options are available via the administrator console.	**Easily administered** from the web interface and via the command-line utility.	**Flexible choice of scanning types.**

You do not have to change your license or make an additional purchase to change your operation system!

Dr.Web Desk Security Suite licensing

Types of licenses	License options
▪ Per number of protected workstations ▪ Per number of users connected to the terminal server ▪ Per number of clients connected to the virtual server ▪ Per number of embedded system clients	▪ Anti-virus ▪ Anti-virus + Control Center The Control Center is provided free of charge. All licensing conditions

Pre-sales support	Technical support
▪ Free Dr.Web product testing—in the customer's network or remotely ▪ Deployment, assistance during the implementation process (by phone) ▪ Presentation, webinar, seminar	▪ 24/7 by phone and via the web form at https://support.drweb.com ▪ For licenses from the price list: free support services and free recovery of files that have been corrupted by encryption ransomware ▪ 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 (VCI) expert consultations

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.com/expertise

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
Phones (multichannel): +7 (495) 789-45-87, 8-800-333-7932 (Toll free in Russia)

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