



Dr.WEB®

Made in Russia

Dr.Web Server Security Suite

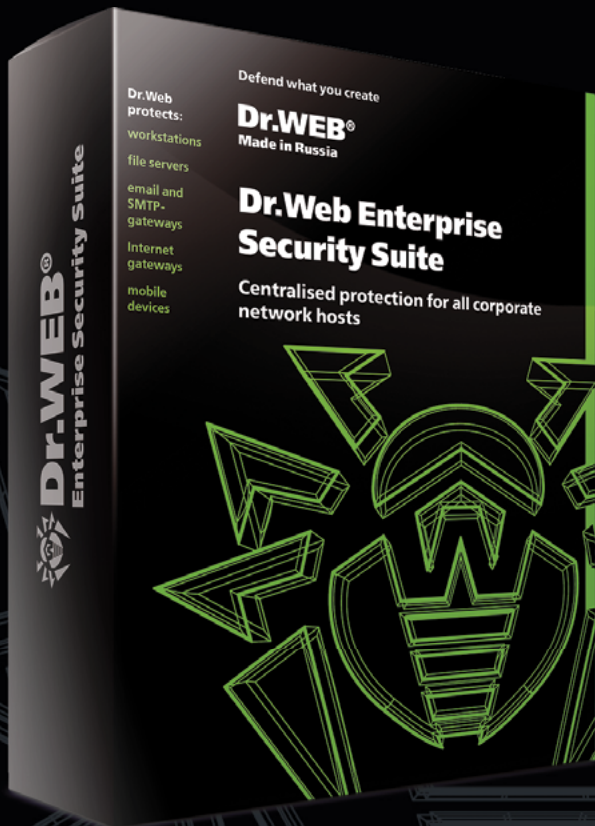
for MS Windows Server 2000* / 2003
(x32 и x64*) / 2008 / 2012 / 2016

* For Dr.Web 7.0 only

www.drweb.com

DEFEND WHAT YOU CREATE

**Protection for file servers
and application servers
(including terminal and virtual servers)**



Advantages

- Performs a preventive analysis on running applications so that any unknown encryption ransomware and banking trojans are detected.
- Prevents critical system areas from being modified by malware.
- Protects against exploits — malicious programs that exploit vulnerabilities in software applications.
- Blocks active content located on removable media.
- Machine-learning rules allow threats that have not been added to the anti-virus databases to be detected and neutralised.
- The data loss prevention feature protects files from being corrupted by encryption ransomware.
- Protects against unknown threats by prohibiting the modification of critical Windows objects and controlling unsafe actions.
- Dr.Web Cloud ensures an immediate response to the latest threats*.
- Protects the OS kernel and its own modules against failures, malware, and accidental modification.
- High-speed scanning combined with low consumption of system resources allows Dr.Web to run smoothly on any server hardware.
- Simple installation and administration.
- Transparent operation – detailed logs with customisable verbosity.

* Available for Windows Server 2008 or higher only.

Features

- Manage the anti-virus protection of the file servers and PCs within your local network from any Dr.Web-protected computer — the Dr.Web Enterprise Security Suite Control Center is not required.
- Use Active Directory policies and Login Script to install the anti-virus remotely.
- Smart optimisation takes into account available system resources.
- The notification system does not distract users with multiple pop-ups*.
- Multi-thread scanning ensures a minimal response time.
- Background scanning means unknown active threats that avoid detection and resist deletion are neutralised.
- The product's integrity is restored if its files are deliberately or accidentally damaged.
- Viruses are detected in archives at any nesting level and in packed objects.
- Access to an infected object can be blocked.
- File server disconnection notifications can be sent to users when virus threats are detected on their machines.

* Available for Windows Server 2008 or later only.

Product system requirements can be found in the [documentation](#).

Dr.Web for MS Windows Server licensing

Types of licenses	License options
<ul style="list-style-type: none">▪ Per number of protected servers	<ul style="list-style-type: none">▪ Anti-virus▪ Anti-virus + Control Center <p>The Control Center is provided free of charge.</p> <p>All licensing terms</p>

Technical support

- 24/7 by phone and via the web form at <https://support.drweb.com>
- Free support services and free decryption services for data compromised by encryption ransomware for licenses from the price list (up to 250 email addresses)
- 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**
- **An immediately generated curing utility based on analysis results**
- **For security researchers and cybercrime investigators**

Our cloud-based interactive analyser Dr.Web vxCube is an indispensable solution in situations when a malicious file has managed to get inside your antivirus-protected network or you have reason to believe that an «impostor» has infiltrated your infrastructure.

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 just a minute or more! Analysis results are provided in a report that can be viewed in your Dr.Web vxCube account area or downloaded as archives.

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

This way you can 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>

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 2003-2020

Doctor Web is the Russian developer of Dr.Web anti-virus software.

Dr.Web anti-virus software has 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>

