



Dr.WEB®

Made in Russia

Dr.Web Server Security Suite

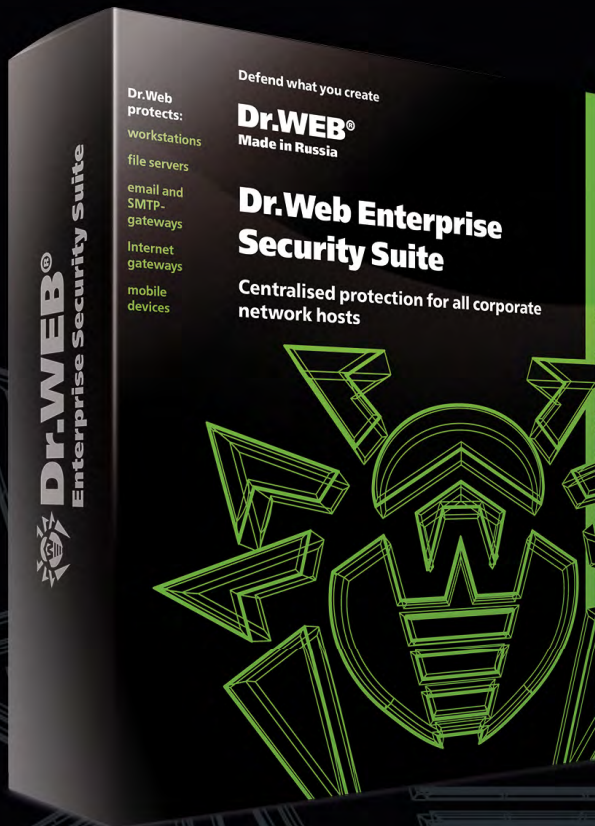
for Novell NetWare

<https://www.drweb.com>

DEFEND WHAT YOU CREATE

File storage protection

- Included in the Register of Russian Computer Programs and Databases



File servers are fundamental to a company's stable operation and the objective of criminals during a targeted attack

All of a company's business processes depend on its servers and services working flawlessly.

If cybercriminals infect the computers and devices of a company's employees, their next step is to attack the servers—once they've gained control over them, the attackers can dictate their terms the company.

By installing the Dr.Web anti-virus, a company can prevent situations where their server becomes a source of infection.

Dr.Web for Novell NetWare servers:

Provides on-demand and scheduled scanning of server volumes	Monitors the file system	Detects unknown threats at the moment of attack	Automatically disconnects workstations from the server as soon as they've been determined to be a source of viruses
---	--------------------------	---	---

Dr.Web for Novell NetWare servers significantly reduces an enterprise's expenses and makes its business processes more reliable.

<p>Protection for any Novell NetWare configurations</p> <p>Supports NetWare namespace. Simultaneously supports multiple network protocols.</p>	<p>High-speed scanning of huge amounts of data</p> <p>with minimum consumption of system resources, both in real time and on administrator demand.</p> <p>Scanning of files by format or by a preassigned list of extensions; scanning exclusions for directories or volumes; scanning of all objects.</p>	<p>Flexible configuration of scanning activities and the actions to be performed with detected viruses or suspicious files. Simple installation, user control panel.</p>
<p>Anti-virus administration, monitoring of the anti-virus's server protection activities, settings optimisation, and the ability to configure the virus-event notification system using the server console or a remote console.</p>	<p>Multi-threaded scanning</p> <p>On-the-fly scans of all the files transferred via the server. Scans of packed, archived, and mail files. On-demand and scheduled scans.</p>	<p>Manageable consumption of CPU resources by adjusting the priority of the scanning process.</p>

<p>Infected objects can be cured, deleted, or moved to the quarantine</p> <p>Automatic virus database updating.</p>	<p>Anti-virus actions log.</p> <p>Viewable scan statistics: process operational time, number of files scanned, and information about detected viruses. Scan logging; adjustable logging verbosity.</p>	<p>Notifications that infected objects have been detected</p> <p>Customisable notifications. Instant email notifications for the administrator, other users, and user groups.</p>
---	---	--

Dr.Web for Novell NetWare 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 conditions: https://license.drweb.com/sss/</p>
Pre-sales support	Technical support
<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 24/7 by phone and via the web form at https://support.drweb.com. Russian, English, German, French, and Japanese languages spoken. 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 a 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: <https://support.drweb.ru/expertise>

