Dr.WEB®
Made in Russia

Dr.Web Server Security Suite

for macOS Server

www.drweb.com

Dr.Web protects:

workstations

file servers

email and SMTP-gateways

Internet gateways

mobile devices

Defend what you create

Dr.WEB®
Made in Russia

Dr.Web Enterprise Security Suite

Centralised protection for all corporate network hosts

Dr.WEB®
Enterprise Security Suite

Dr.WEB®
Enterprise Security Suite
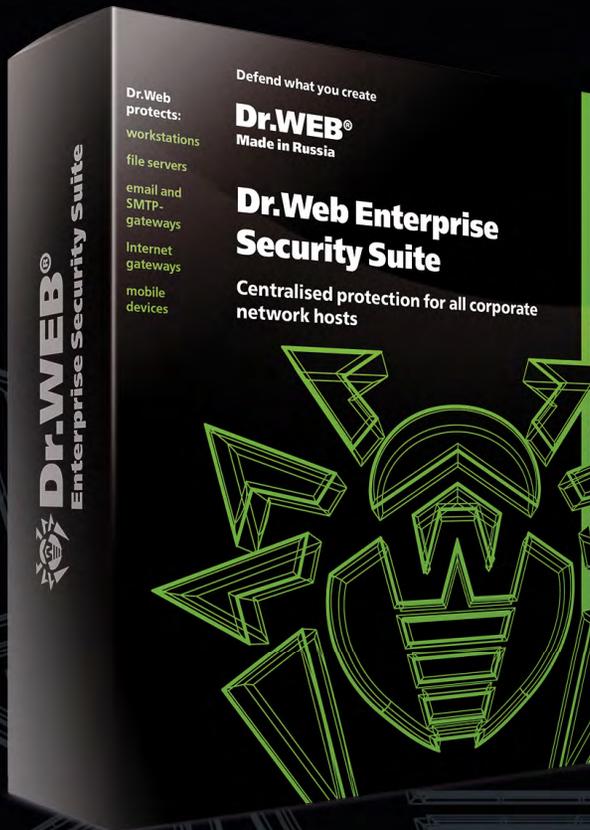
File servers are fundamental to a company's stable operation and the objective of criminals during a targeted attack.

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 to 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 macOS Server:

Provides on-demand and scheduled server scanning.	Protects the file system.	Detects unknown threats at the moment of attack.	Protects against Windows-specific threats launched under macOS.

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

Anti-virus scanning of any file server system objects, removable media, and downloaded files, including packed files and archived data. Detects and neutralises viruses disguised with unknown packers.	**High-speed scanning of huge amounts of data** with minimum consumption of system resources, both in real time and on administrator demand. High performance and operational stability.	**Password-protected SpIDer Guard settings** means unauthorised changes cannot be made. In most cases, when the default settings are in use, Dr.Web does not require users to respond to the anti-virus in any way and will not distract them from their tasks.
Different actions can be performed with infected and suspicious objects, as well as with other types of objects, including cure, move to the quarantine, and delete.	**Cloud-based protection** Dr.Web Cloud protects against threats without having to wait for the latest updates.	**Automatic, manual, and scheduled scans.** Three types of scanning: express, full, and custom.
Infected objects can be cured, deleted or moved to the quarantine.	The product can operate as part of a centrally managed anti-virus network.	Notifications that infected objects have been detected.

Dr.WEB®
Enterprise Security Suite

Dr.Web for macOS Server licensing

Types of licenses	License options
▪ Per number of protected servers	▪ Anti-virus ▪ Anti-virus + Control Center The Control Center is provided free of charge. All licensing terms: https://license.drweb.com/sss/

! When simultaneously purchasing Dr.Web to protect workstations and servers, 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 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
- ▪ 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.

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