



**Dr.WEB®**

**Anti-virus & Anti-spam**  
for Unix mail servers

## **Benefits**

High performance and stable operation

Outstanding scalability

Support of most known archivers and packers

Flexible configuration and ease of administration

Allows to implement any security policies

Industry's widest range of supported OS and mail systems

# Dr.Web® for Unix mail servers

**Dr.Web for Unix mail servers** is a modular solution for processing and filtering of incoming and outgoing traffic in mail servers under Unix-based operating systems (Linux/FreeBSD/Solaris(x86)). The solution can be integrated into an existing mail system or can be used as an SMTP-proxy that performs full check of mail messages via SMTP/LMTP (Dr.Web Mail Gateway).

## Key features

Depending on a number of licenced components Dr.Web for Unix mail servers allows:

- Detecting and neutralizing viruses and other malicious programmes, spam, phishing, pharming, scamming and bounce-messages;
- Correct scanning of most known archives including multi-volume and self-extracting archives (SFX);
- Protecting its own modules to ensure no errors occur;
- Sending reports to message recipients or to other people;
- Isolating infected objects and spam in the quarantine;
- Collecting statistics of all aspects of a system functioning;
- Implementing any security policies.

## Wide range of supported OS and mail systems:

- Linux (glibc 2.2 or later), FreeBSD 5.x, 6.x, Solaris 10 (Intel only).
- CommuniGate Pro, Courier MTA, Exim, Postfix, QMail, Sendmail, ZMailer.

## Available plug-ins

**Dr.Web** — the plug-in used to scan mail messages for viruses using the Dr.Web engine.

**vaderetro** — spam filtering plug-in that uses its own library (Vade Retro).

**headersfilter** — a plug-in that filters e-mails analyzing message headers.

## Benefits

### □ Unlimited number of connected plug-ins

**Dr.Web for Unix mail servers** allows to extend the functionality of the solution to an unlimited extent. Any connected plug-in will work with all supported MTAs. The modular architecture makes the solution compatible with mail systems not included in the supported systems list for which a user can develop a module he or she needs. The system can be integrated into a mail server or may function on its own.

### □ Open solution

**Dr.Web for Unix mail servers** is based on the system of plug-ins open for independent developers. Any user with appropriate skills can implement any additional feature as a plug-in using SDK supplied with the solution.

### □ Flexible configuration and easy administration

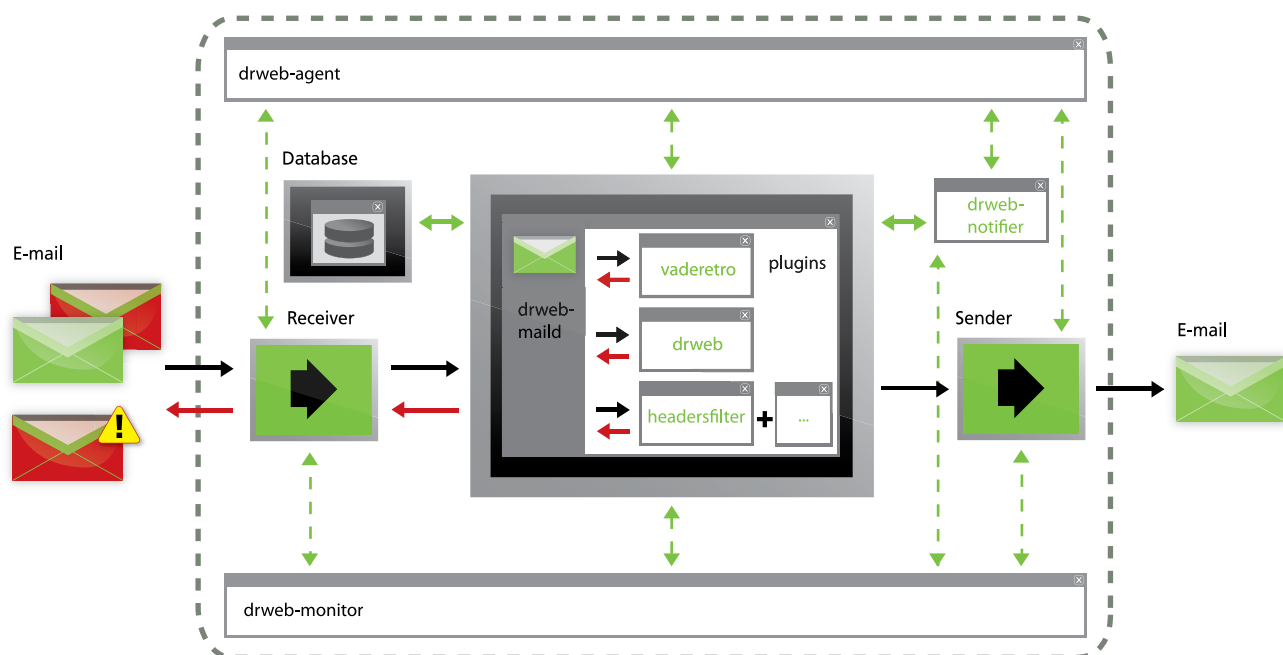
**Dr.Web for Unix mail servers** has a flexible configuration system that allows using virtually any available set of rules.

### □ Outstanding scalability

Flexible configuration, exceptional stability and capability to process huge amounts of data in a real-time mode allow the solution to meet demands of a small company using one mail server as well as demands for scanning of unlimited amount of e-mail traffic of a transnational communication service provider.

### □ High performance and stable operation

Multi-thread scanning feature of **Dr.Web for Unix mail servers** allows the solution to process a lot of mail messages simultaneously. The modular structure of the solution makes it impossible to disable the anti-virus (if attacked). Low system resources requirements allow **Dr.Web for Unix mail servers** to smoothly function on mail servers of almost any configuration.



## Dr.Web Anti-virus for Unix mail servers

E-mail messages are filtered for viruses, spyware, adware, suspicious programmes, hack-tools and jokers by the DrWeb anti-virus plug-in.

### □ **Stable operation**

The plug-in structure of the solution and a special self-protection module makes it impossible to disable the anti-virus (if attacked).

### □ **Quick response**

The multi-threaded e-mail scanning technology provides high system response speed. Files are checked on-the-fly, instead of placing them in a queue to process.

### □ **High protection level**

A virus database with thousands of entries and constantly improved heuristic analyzer leave no chance to viruses to penetrate into users' workstations via e-mail.

### □ **Correct scanning of most known archives**

The DrWeb plug-in provides correct scanning of most known archives including multi-volume and self-extracting archives.

### □ **Quarantine**

Infected and suspicious files can be placed to the quarantine so one can extract important information, cure or delete.

### □ **Easy administration**

Flexible configuration file of the anti-virus plug-in allow for customization.

## Dr.Web Anti-spam for Unix mail servers

E-mail messages are filtered for spam by the vaderetro plug-in.

### □ **High performance filtering**

Dr.Web Anti-spam for Unix mail servers scans over 100 messages on-the-fly in one second (1.9GHz Pentium 4 CPU)), which means it will scan 8.64 million messages in 24 hours!

### □ **The anti-spam does not require tuning!**

Unlike anti-spam solutions based on the Bayesian filtering technologies, Dr.Web Anti-spam for Unix mail servers doesn't require any initial tuning or setup; it begins working effectively upon install.

### □ **Intelligent spam detection system**

Different technologies are used for different types of undesired mail – spam, phishing, pharming, scamming, and bounce-messages to produce an exceptionally high detection rate.

### □ **Autonomous filtering saves traffic**

The stand-alone anti-spam analyzer module doesn't require connection to an external server or access to a database; this helps save on traffic substantially.

### □ **Unique technologies!**

A unique spam-filtering technology allows to avoid blacklists which means that a company can't be discredited by a deliberate adding it to a blacklist.

### □ **Regular updates**

Due to dynamically updated code of the anti-spam library the quality of detection is constantly improving. Updates are released on a daily basis and are downloaded by the Dr.Web automatic updating utility.

### □ **Dr.Web smtp-proxy for Unix mail servers**

Dr.Web smtp-proxy is installed on a separate server which increases general stability of a mail system and security of a company. Depending on the topology of a network Dr.Web smtp-proxy can be installed in a demilitarized zone (DMZ) or in a company network.

### □ **Dynamic protection from spammer attacks**

Not only the e-mail messages itself, but also parameters of an SMTP-session can help identify a message is a spam. Some of the typical properties of a spam message (or a spammer attack) is a large number of recipients, or a lot of messages sent using one IP, or an invalid sender address. Dr.Web smtp-proxy enables an administrator to restrict parameters of an SMTP-session.

### □ **Validation of IP-addresses**

One of the properties of a spam message is an invalid sender IP. Spammers have to hide their servers (or spam-bots – infected user workstations) to avoid blocklisting. Dr.Web smtp-proxy allows performing an IP validity verification.

### □ **Protection from hack attacks**

Dr.Web smtp-proxy allows to counter both "passive" attacks (PLAIN, LOGIN, etc.), and active non-dictionary attacks.

### □ **Protection from spam traps**

Dr.Web smtp-proxy allows to check if a recipient is a spam trap and do not send messages to this address.

### □ **Protection from malformed messages**

Dr.Web smtp-proxy is capable of blocking messages with empty sender fields but works correctly with messages from mail clients which fail to comply with Internet Message format.

### □ **Saving on Internet traffic**

Using Dr.Web smtp-proxy saves on Internet traffic and blocks messages that have extremely large attachments.

### □ **Open Relays servers restriction**

Dr.Web smtp-proxy allows to specify domains for which mailing is allowed.

## Global updating system

□ Dr.Web Virus Monitoring Service collects virus samples all over the world.

□ Updates are received from several servers located in various parts of the globe.

□ «Hot» add-ons are released immediately after an emerged threat has been analyzed.

□ Every update is tested over a huge number of clean files before it is released.

□ Dr.Web virus database is the most compact one. It makes scanning process faster, saves time and system resources and allows instant updating. Just one entry in Dr.Web virus database provides detection of hundreds or even thousands of similar viruses.

□ Virus databases and programme modules are updated automatically.

## Technical support

While a licence is valid a customer can use Doctor Web, Ltd. support services free of charge. They include:

- Unlimited number of requests via a web-form in the Support section of the company web-site <http://support.drweb.com/>;
- Free updating of Dr.Web virus databases;
- Free upgrading of Dr.Web programme modules;
- Unlimited number of distributions` downloads;
- Free access to the knowledge base;
- Dr.Web users` forums.

## Licencing

### Licence options

- Anti-virus
- Anti-virus + Anti-spam

### Licence types

- Address licence
- Per server licence
- Unlimited licence
- SDK licence

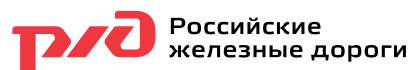
## About Doctor Web

Doctor Web is a Russian IT security solutions developer Dr.Web anti-virus solutions have been developed since 1992, they have always shown perfect results of malicious programmes detection and comply with international security standards. Various certificates and awards and a lot of customers all over the world can be seen as a clear evidence of the utmost trust to the products of the company.

There are few anti-virus vendors in the world that have their own technologies for detecting and curing malware, a virus monitoring service and analytical laboratory. It provides a rapid response to latest threats and allows to solve any problems of our customers in a few hours.

### Large enterprise-network experience

Customers of Doctor Web include large and well-known companies: Russian and, international banks, state and educational institutions, research departments with dozens of thousands computers in their networks. Highest government institutions and oil and gas companies of Russia entrust their information security to Doctor Web.



---

Dr.Web is a registered trademark of Doctor Web



125124, Russia, Moscow, 3-ya ulitsa Yamskogo polya 2-12A  
Tel: +7 (495) 789-45-87  
Fax: +7 (495) 789-45-97  
<http://www.drweb.com>  
<http://www.freedrweb.com>  
<http://www.av-desk.com>