Dr.WEB®
since 1992

Why Dr.Web server anti-viruses are needed to filter corporate email

- "I was emailed a request for an accounts report; I uploaded the file and opened the archive."
- "...I prematurely opened a zip folder that had been emailed to me".
- "I received an email and downloaded and opened "Order information 08-18-11-2019.xls". .

Help requests submitted to Doctor Web's Technical Support Service

Как правило, троянцы попадают на компьютер в результате каких-либо действий пользователей — например, отключивших антивирус вопреки политике компании и затем перешедших по ссылке из письма или открывших вложение. Даже простое открытие письма уже может дать информацию злоумышленникам о существовании конкретного почтового адреса в компании — и стать отправной точкой целевой атаки.

Mail is the main source for the spread of infection-carrying malicious programs and the way that corporate networks get infected.

As a rule, trojans get into computers when users act carelessly with removable media or email—for example, when they go against company policy and disable the anti-virus and then follow a link in an email or attachment. Even if an employee just opens an email, that action can let attackers know that specific email addresses exist within the company—and this can be the starting point for a targeted attack.

- Everything that a company receives or sends via email must be scanned BEFORE it reaches user computers and devices. The user simply must not receive an infected email.

Having an anti-virus and an anti-spam installed on a mail server guarantees that a company's security policies will be complied with and that at the workstation level, the integrity of its local network won't be compromised.

Dr.Web for Mail Servers can* :

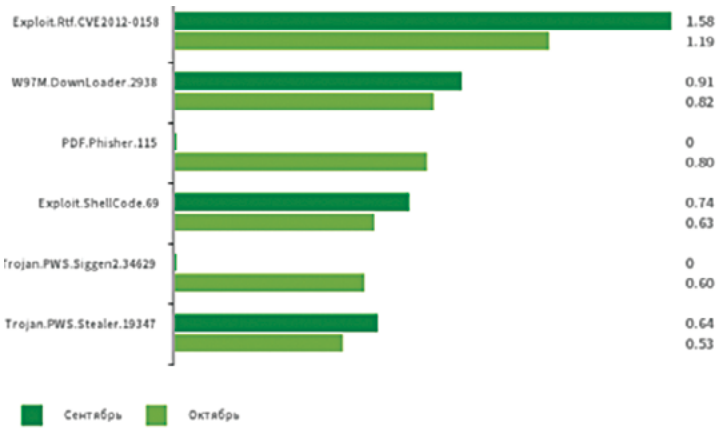
- MS Exchange Linux filter both the external (incoming and outgoing) and the internal mail for viruses and spam — on both company-controlled servers and company-leased servers;
- MS Exchange Linux filter email at the gateway, i.e., by isolating a mail server from the Internet;
- MS Exchange scan emails stored on a server for the presence of previously undetected threats;
- MS Exchange Linux establish different policies for various user groups;
- Linux implement a deep statistical analysis of senders and recipients;
- Linux filter email messages according to the contents of the email, its senders, recipients, and types of attachments;
- Linux use gray Internet lists to filter spam;
- MS Exchange Linux move filtered email to the quarantine for later analysis;
- Linux recover messages that were accidentally or intentionally deleted from employee mailboxes, and, thus, allow companies to conduct investigations into their data leaks.

* *The features of the solutions incorporated into Dr.Web Mail Security Suite depend on the company mail server being used.*

How malware penetrates a company's network via email

Cybercriminals do not just try to run a variety of encryption ransomware programs on company computers. Two of the five most actively distributed malicious programs are aimed at stealing passwords and confidential information. This data can be sold or used to carry out other attacks on a company—after all, it's common knowledge that people often use the same password to access all of their resources.

Statistics concerning malicious programs discovered in email traffic (October 2019)



Exploit.Rtf.CVE2012-0158 is a malicious Microsoft Word document that leverages the CVE2012-0158 vulnerability.

W97M.DownLoader.2938 encompasses an entire trojan downloader family that exploits vulnerabilities in Microsoft Office documents.

Exploit.ShellCode.69 is a malicious Microsoft Word document that leverages the VE-2017-11882 vulnerability.

Trojan.PWS.Siggen2.34629 and Trojan.PWS.Stealer.19347 — malicious programs that steal passwords and other confidential information.

https://news.drweb.com/show/review/?lng=en&i=13519

Local network users:

- do not use or disable anti-virus solutions when working with company email on their personal PCs and devices;
- put off installing notifications and wait too long to restart their systems so that updates can be applied. In 2019, the Exploit.Rtf.CVE2012-0158 was leveraging a vulnerability that had been discovered back in 2012 (!);
- do not perform timely updates on their own PCs (including when working from home), which results in the anti-virus software not being able to protect their systems effectively.

"According to the report, the anti-virus databases are updated less frequently than updates are released".

The result of an analysis of a local network infection caused by a user opening an email

When a company installs the anti-virus on their mail server, which is under the full control of security experts, it will block malicious emails and attackers will not be able to use social engineering techniques to attack the company.

Employees working remotely on personal devices will not be able to send infected emails to the company's clients

Cybercriminals:

- can create a unique build for each of their victims;
- can use obfuscation and encryption to disguise already known code, or use fileless storage and launch techniques;
- use automated services to create and test malware samples.

By using automated services, attackers can create new versions of known malware more quickly than the anti-virus databases of a conventional anti-virus can be updated. As a result, a malicious program that has already been received for analysis and whose information has already been added to the virus databases can be used to attack a company before its virus databases have had their next scheduled update applied.

Dr.Web for mail servers is not just an anti-virus module

The anti-spam used in Dr.Web for mail servers, even without the help of the anti-virus engine, filters out more than 90% of malicious programs, keeping our customers protected even against the latest malware.

Dr.Web Anti-spam's operation is based on rules. It works within email traffic to effectively remove malware-laced phishing messages that are temporarily not being detected by traditional anti-virus technologies.

Dr.Web Anti-spam:

- is delivered as part of a single solution (not as a separate product);
- is installed with a virus-filtering product on the same server.

This simplifies administration and ensures that overall costs are lower than they would be if buying our competitors' solutions.

Advantages of Dr.Web anti-spam

- The anti-spam doesn't require training. Unlike anti-spam solutions based on Bayesian filtering, it starts working as soon as it is installed.
- It detects spam messages regardless of their language.
- Actions can be customised for different categories of spam.
- It uses its own whitelists and blacklists, which makes it impossible to discredit companies by deliberately adding them to lists of unwanted addresses.
- Low number of false positives.

Our top rule is that our radio stations operate normally and that all of our processes are flawless. This also applies to the security of our mail servers. Dr.Web Mail Security Suite has significantly improved the reliability of our system".

Alexander Suganov,
Head of the System Administration Department of "Radio GPM"

- "Our mail administrators are complaining that an unauthorised mailing was carried out today from two of their workstations to unknown email addresses".
- "Our administrators are concerned about possibly sending out malware from their PCs when they send off corporate email in their scheduled mailings to users (this occurs frequently, including today, for example)".
- "In..., several company email addresses were compromised, and then they were used for spam mailings".
- "Something was launched with an email that I sent to myself from Outlook 2010. I did not open any emails".

Help requests submitted to Doctor Web's Technical Support Service

A password leaks, a customer launches malware, or a criminal takes advantage of an unknown vulnerability—that's all it takes for a malware program to settle onto a computer and transmit spam or malware-laced messages to the user's address book contacts. With an anti-virus and anti-spam installed on a company's server, such messages won't reach employees.

Users work from home and when on vacation. They always need to be able to contact their managers! But their personal computers and devices are usually (in 60% of cases!) not protected and are often infected. The server anti-virus will not allow your employees to send infected emails to your partners or customers.

Is your reputation important to you?

Email should be filtered in its entirety

Using an anti-virus that has no anti-spam:

- gets companies added onto spam lists, which can cause their mail to be blocked by the mail servers of their partner companies and customers and their reputation as a reliable, security-conscious partner to be damaged;
- reduces the productivity of all the employees who have to spend time deleting spam from their mailboxes;
- lets hackers carry out attacks on a company's mail servers and the email clients used by its employees; sometimes just receiving an email can be sufficient to infect a machine or disrupt its operation;
- leads to increased traffic costs;
- increases unproductive, spurious loads on mail servers.

Dr.Web anti-virus will filter email on the server once, rather than several times on each PC—this will improve performance, and employees will be much less likely to complain about low PC performance.

Thanks to the anti-spam incorporated into Dr.Web Mail Security Suite, the mail server won't be involved in processing large volumes of spam (spam can make up 98% of all email traffic, and filtering it out will improve mail server performance). Delivery delays and lost emails will be rare events!

"Our virus analyst discovered that workstations were infected from that mail server".

The result of a Doctor Web employee analysing an incident.

After gaining access to a company's server, attackers can do whatever they want. They can encrypt company data and demand a ransom, copy it, and sell it. A trojan can add a role for an MS Exchange mail server and use it to change email messages or copy the information they need from those messages—after the messages are scanned by the mail anti-virus.

In addition to protecting your mail service, you also need to protect the server itself—at the file system level.

- Only by protecting the server itself and the channels that communicate with it (both internal and external) can you protect the server from becoming a source of infection when an unknown virus penetrates the network.

- Any server needs protection—both one that is located within a company's premises and a leased external server.

Technical consequences of a server infection	Commercial consequences of a server infection
▪ The deletion of company data that is stored on the server and available from it. ▪ The blocking of the mail server operation, including data encryption. ▪ Denial of service – a company is disconnected from the Internet or placed on blacklists for sending out spam if it has become part of a botnet. ▪ Server performance slows down or crashes. ▪ An increase in the internal network load and a decrease in the performance of network resources and channel bandwidth. ▪ An increase in IT infrastructure costs (paying for "spurious" traffic/more servers/mail storage costs, including those for spam).	▪ A breach in the continuity of business processes: ✓ Delayed fulfilment of the company's obligations towards its customers; ✓ customers leaving because they don't want to use the company's services; ✓ delays in staff being able to carry out their duties; ✓ The company gets blacklisted so its partners don't get the company's email messages. ▪ A worsening reputation in the eyes of consumers and partners—including because the company is starting to be perceived as technologically inept.

Правильное решение: Dr.Web Server Security Suite + Dr.Web Mail Security Suite

Скидка 20% при покупке двух продуктов

- 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.
- Windows The preventive protection technologies will protect against even unknown threats and exploits as well as against communication attempts between remotely managed malicious objects and a malicious server (to control botnets and for espionage)—without any dependency on virus databases and the frequency with which they are updated.
- Windows If a cybercriminal does not have full permission on a target station, Dr.Web SelfPROtect, a unique anti-virus component, neutralises any attempts made by malicious programs to disrupt the Dr.Web anti-virus's operation — email filtering won't be stopped and the server backup will be protected from encryption attempts and vandalism.
- It launches before the OS boots up and operates on the lowest possible system level—this won't leave cybercriminals any time to attack!

The right decision: Dr.Web Server Security Suite + Dr.Web Mail Security Suite

Get 20% off when you buy 2 products

ONE KEY for all the Dr.Web Mail Security Suite products you buy

Dr.Web mail-filtering products

Dr.Web Mail Security Suite

Unix:	MS Exchange	IBM Lotus Domino	Kerio
✓ Sendmail ✓ Postfix ✓ Exim ✓ QMail ✓ Communigate Pro ✓ Courier ✓ ZMailer			

Licensing

Per number of addresses	Per-server license (up to 3,000 addresses)	Unlimited license for any number of servers

Types of licenses

- Anti-virus
- Anti-virus + Anti-spam
- Anti-virus + Anti-spam + SMTP Proxy
- Anti-virus + SMTP Proxy
- Anti-spam+ SMTP Proxy

Dr.Web совместим как с **MS Exchange**, **Lotus**, **Kerio**, так и с почтовыми серверами, работающими на платформе **Unix**, — в том числе на операционных системах, создаваемых в рамках импортозамещения.

- Detailed documentation for each product.
- Round-the-clock technical support, seven days a week, without holidays—the quickest way to solve your urgent questions about Dr.Web software's operation.
- VIP support and a dedicated technical specialist.
- Training services for our customers' specialists.

About Doctor Web

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web products have been developed since 1992. All rights to Dr.Web technologies are reserved by Doctor Web. The company is one of the few anti-virus vendors in the world to have its own technologies for detecting and curing malware. Doctor Web has its own anti-virus laboratory, global virus-monitoring service, and technical support service.

The company is a key player on the Russian market for software that meets the fundamental need of any business — information security. Russia's State Duma, Central Election Committee, Ministry of Defence, Supreme Court, Federation Council, Central Bank, and many other government institutions and large companies have chosen to rely on Dr.Web products.

Here are just some of our customers: https://customers.drweb.com

Doctor Web has received state certificates and awards; our satisfied customers spanning the globe are clear evidence that the quality of our products, created by a talented team of Russian programmers, is undisputed.

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040
Phone: +7 (495) 789-45-87 (multichannel)
Fax: +7 (495) 789-45-97

https://www.drweb.com