Dr.WEB®
since 1992

# How to choose an anti-virus

## A methodology for selecting anti-virus software

For business owners, heads of IT departments in enterprises and organisations, and those specialising in enterprise anti-virus protection systems

# CONTENTS

# Introduction

Currently, the market offers a sufficient number of anti-virus products. One would think that it would be easy to select the best solution—just steer towards the winners of anti-virus tests. After all, you can find free anti-viruses among the test leaders—a great opportunity to save! But if everything was that easy, we wouldn’t see this...

- Hello, my system was compromised by an encryption ransomware program; my anti-virus ... did not help.
- Hello, dear Dr.Web command. Please help decrypt my WannaCry-compromised PC. It got infected while I was visiting some websites (I don’t know which of them contained the virus—I didn’t immediately notice that the infection had occurred); I was using ... anti-virus.

The dots in the quotations above replace the names of the anti-viruses that were being used by the two users; they contacted Doctor Web seeking decryption services after their systems were compromised by WannaCry—this was an outbreak that affected even the largest of companies.

Add to that the fact that the descriptions of the technologies anti-viruses use to detect malware sound like magic spells, and the problem of selecting a solution that actually offers protection becomes a real problem.

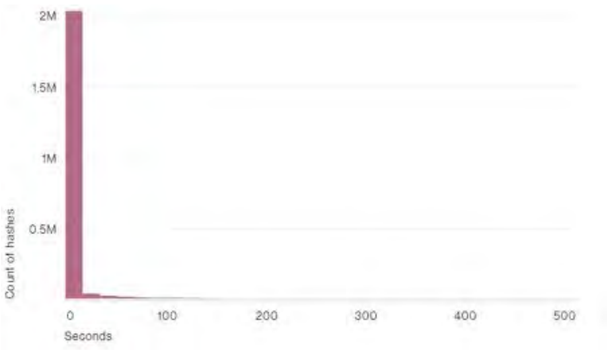
# I. Main causes of infection and counteractive measures

Almost daily in the mass media, one hears reports of a variety of companies and organisations being impacted by infections. Sometimes, multi-million-dollar losses are reported. Most of these companies weren’t using an anti-virus to protect their systems at the moment of infection. Why does this happen?

1. Cybercriminals can automate the development of malware, and as a result, the number of malware samples received by Doctor Web for analysis in a single day approaches one million!

- The need to rapidly add new rules into the anti-virus databases and the rules databases for the firewall and the preventive protection component leads to those databases becoming “littered”.  Therefore, Doctor Web regularly purges these databases of duplicate entries without impacting the quality of detection.
- The Dr.Web anti-virus databases possess a unique feature—an algorithm for a signature search in the anti-virus databases, as well as in the rules databases for the firewall and behaviour analyser, that does not increase the search time if the number of database entries increases.

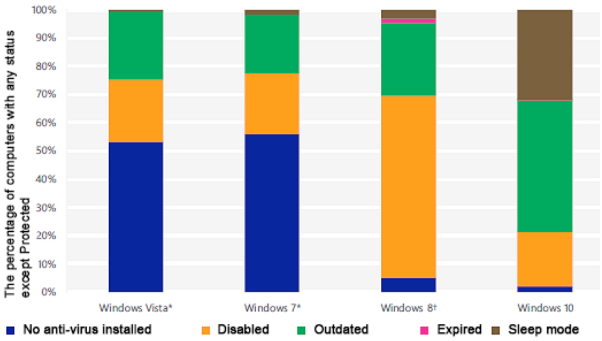
**An anti-virus should not slow down!**

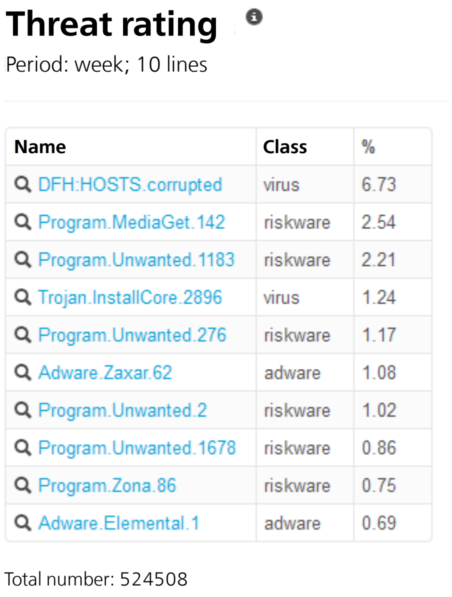


Over 99% of malicious samples (hashes) have a “life expectancy” of 58 seconds or less!

2. Users of anti-virus solutions do not update them, or they even disable them after installation.

- Statistics related to PCs that have been scanned with the emergency scanning utility Dr.Web CureIt! show that up to 60% of computers are inadequately protected.
- Almost 30% of users of the Dr.Web CureIt! free version use Microsoft Windows Defender, an anti-virus built into Windows 7 and 10.





## Threat rating

Period: week; 10 lines

| Name | Class | % |
|---|---|---|
| DFH:HOSTS.corrupted | virus | 6.73 |
| Program.MediaGet.142 | riskware | 2.54 |
| Program.Unwanted.1183 | riskware | 2.21 |
| Trojan.InstallCore.2896 | virus | 1.24 |
| Program.Unwanted.276 | riskware | 1.17 |
| Adware.Zaxar.62 | adware | 1.08 |
| Program.Unwanted.2 | riskware | 1.02 |
| Program.Unwanted.1678 | riskware | 0.86 |
| Program.Zona.86 | riskware | 0.75 |
| Adware.Elemental.1 | adware | 0.69 |

Total number: 524508

Dr.Web CureIt! scan statistics

**Dr.Web does detect threats!**

3. Users of anti-viruses ignore security system alerts and configure the system in such a way that the malicious files penetrating it are not checked by the anti-virus.

- One of the most common ways malware gets on PCs is through users deciding to exclude from anti-virus scanning programs that have Internet access and computer disks.
- Another way to lower the anti-virus protection level is to lower the protection level of the Preventive Protection component.

**! Most infections penetrate computer systems because of the actions of company employees, and their clients or partners.**

4. Updates go uninstalled in local networks for long periods of time, and vulnerable services are allowed to be used.

- The exploits used to penetrate a target system are aimed at vulnerabilities that were found three or more years ago! In effect, a vulnerability can be exploited for the duration of an operating system's lifetime!
- WannaCry spread using an exploit that was designed for a Microsoft vulnerability that had already been closed!

# II. Determining the requirements for the means of protection to be used

An anti-virus protection system should:

- **detect unknown malicious programs.** Virus writers extensively test their "creations" on specialised services, and as a consequence, the presence of just heuristic routines in an anti-virus does not guarantee that the newest malicious programs will be detected. The most common way to evade known signatures is to repack previously created malicious programs; this includes using packer formats with formats that are unknown to the protection system. To counter this method, Dr.Web solutions incorporate technologies that can search for known but repacked malicious programs (**Dr.Web Fly-Code**), as well as proactive protection tools that detect actions typical of malware and require no information about their signatures (**Dr.Web Preventive Protection**).

- **have a reliable self-defence system** that cannot be disabled by the latest malware or employees who want to bypass their company's existing security policies. Such a system allows anti-virus solutions to resist the attacks of malicious programs until they receive updates that block the source of the attack.

- **have the option to block individuals from disabling the anti-virus protection**. For this, it is essential to use centralised protection, which allows users' rights to be restricted depending on their employment duties, and password protection for system protection settings on workstations that are not centrally managed.

- **support the relevancy of updates**. The Dr.Web update system uses servers located worldwide. The update technologies update all the stations in the protected system simultaneously without burdening the local network. With centralised protection, users can update network stations according to a schedule and remotely restart workstations; the protection settings of workstations not under centralised management can be password protected to ensure updates cannot be refused.
- **keep the license up to date**. Dr.Web products incorporate a system that ensures licenses are automatically renewed by your anti-virus software supplier.

# III. Selecting security measures

An anti-virus protection system must not only block known malicious programs but also prevent the spread of unknown malicious software inside the network and beyond its borders.

1. The local network host on which it is possible to install an anti-virus must be protected—this includes Linux and Mac operating systems, mail servers, Internet gateways, and mobile devices. Employee personal handhelds and home computers must also be protected. If employees refuse to protect their personal computers and handhelds, the company must protect the mail servers and Internet gateways used by its employees to access company services.
2. Systems vulnerable to viruses (including printers) that cannot be protected by an anti-virus must be air-gapped from the rest of the local network.

**An anti–virus for workstations must:**
1) Know how to neutralise malware programs—both those penetrating the system at any given moment and those already running in the system that were previously unknown;
2) detect known malware samples packed in files with an unknown format;
3) use additional mechanisms (except signature and heuristic ones) for detecting unknown malware, including preventive protection and cloud components;
4) incorporate the following components to protect itself against malware programs that are unknown at the moment of infection:

- a personal firewall, which prevents the local network from being scanned and protects against intranet-based attacks;
- a system for restricting access to removable media and local network resources, including removable disks, directories, and websites;
- a centralised system for regularly scanning inactive malware and known vulnerabilities;

5) check all files entering the local network prior to their being processed by the respective applications. This rules out the possibility that malicious applications will exploit the unknown vulnerabilities within these applications;
6) have a self-defence system that will prevent an unknown malware program from disrupting the operation of the anti-virus and ensure that the anti-virus protection system is operational before it receives an update that will enable it to neutralise the threat;

7) have routines for collecting information that make it possible to quickly send to the anti-virus laboratory all the information needed to solve a problem. One must never rely on having to collect information manually, including on remote workstations and servers, each time a system gets infected.
8) deploy anti-virus databases in the memory in order to avoid loading them (including mounting) from the hard disk, which would cause the anti-virus scanning processes to decelerate;
9) ensure multi-thread scanning, preventing a queue of files from forming;
10) run on operating systems no longer supported by their manufacturer;
11) use an anti-spam (anti-phishing) that does not require constant training to protect against unknown malicious program sent in email messages;
12) use a system of automatic load analysis to exclude the need to manually configure CPU load settings.

**The centralised control system of anti–virus protection should:**
1) like an anti-virus update system: be independent from the corresponding mechanisms used in operating systems; be included in the anti-virus self-defence system to prevent malware from intercepting updates. An anti-virus should not use system components that are not protected by the anti-virus self-defence system;
2) use an anti-virus that includes a proactive behaviour analyser and a personal firewall—on all workstations and servers;
3) ensure the fastest possible delivery of virus database updates for the protected PCs and servers; this includes delivering updates on demand even if the protected network's overall performance is negatively impacted. A constant connection between the protected hosts and the updating server and the small size of the updates will minimise the update retrieval time;
4) be able to apply individual settings to groups and selected users;
5) be able to provide for a full or custom scan of a network host for virus threats, both on the command of a user or administrator and according to a schedule;
6) be able to centrally install updates and configure the anti-virus software, including on network hosts not accessible from the server;
7) be able to run in networks divided into separate segments.

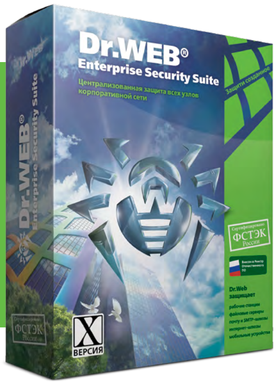
**In addition to using anti–virus protection, it is recommended to:**

1. Restrict user permissions. This includes:
   1) refusing to use administrator permissions on workstations;
   2) restricting access permissions to local and network resources;
   3) restricting the use of removable media. In this case, one must take into account that device lists are usually ineffective because all the device IDs in a lot are the same.

2. Divide the local network into separate isolated segments and install a traffic-filtration system between them.
3. Remove unused products, services, and features.
4. Use a back-up system located on a separate server.
5. Place databases on separate servers, block access to them, and use versioning for stored files and documents.
6. Block all programs, except allowed ones, from accessing the Internet and local network.
7. Prohibit the use of administrator domain passwords on workstations.
8. Centrally install all security updates for all the products in use. Regularly update all the software installed on workstations.

To perform an emergency scan on potentially compromised workstations, use a network anti-virus scanner and a bootable anti-virus disk/removable media device.

# IV. Dr.Web Enterprise Security Suite—a set of products for business users



For corporate customers, Doctor Web offers its flagship product–Dr.Web Enterprise Security Suite which has a number of unique features:

- centralised protection for all network hosts: PCs, mail and file servers and application servers, including terminal servers, Internet gateways, and mobile devices;
- comprehensive workstation protection powered by the built-in anti-virus, anti-spam, firewall and office control and able to withstand most known threats;
- support for the Windows and Unix server platforms, a simple installation procedure, and reliable protection at a minimal TCO compared with competitive solutions; with Dr.Web Enterprise Security Suite, your company won't have to purchase expensive hardware;
- the agent software can be installed on machines that are already infected, with a high probability that they will be cured.
- a small-sized engine featuring the latest technologies guarantees minimal use of workstation and server resources;
- highly efficient detection of threats, including unknown viruses;
- the entire network protection infrastructure can be administered from one computer (by means of the Web-administrator) from anywhere in the world;
- individual security policies can be implemented for companies or groups of employees;
- assigning individual administrators to different groups makes Dr.Web Enterprise Security Suite a perfect choice for both companies with high security requirements and multi-affiliate organisations;
- configurable security policies for any type of user, including mobile users, and for any workstation (even if currently unavailable) to ensure up-to-date, 24-hour protection;
- protection for all networks, including those that are isolated from the Internet;
- support for a wide range of DBMSs; Oracle, PostgreSQL, Microsoft SQL Server or any other DBMS that supports SQL-92 over ODBC can be used as an external database;
- custom event handlers written in any script language, providing direct access to the Control Center's internal interfaces;
- an easy-to-understand protection control system that offers unsurpassed usability and efficiency with regards to searches for network stations;

- a customisable list of product components for updating and version upgrade control, enabling administrators to install only those updates that are necessary and have been tested in the network.

Dr.Web Enterprise Security Suite includes the following products:

**Dr.Web Desktop Security Suite** – protection for PCs, embedded system clients, virtual server and terminal server clients

**Dr.Web Server Security Suite** – protection for file and application servers (including terminal and virtual servers)

**Dr.Web Mail Security Suite** – protection for email

**Dr.Web Gateway Security Suite** – protection for Internet gateways

**Dr.Web Mobile Security Suite** – protection for mobile devices

Dr.Web Enterprise Security Suite is included in the Register of Russian Computer Programs and Databases and allows you to comply with the requirements of current legislation in the field of anti-virus security.

All Dr.Web Enterprise Security Suite products can be used free of charge for 30 days. We invite companies to request a trial and evaluate the reliability of the protection and the quality of Dr.Web's detection and treatment capabilities.

Description: https://products.drweb.com/enterprise_security_suite

Request a free trial: https://download.drweb.com/demoreq/biz/v2

# About Doctor Web

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web anti-virus software has been developed since 1992. The company is a key player on the Russian market for software that meets the fundamental need of any business – information security. Doctor Web is one of the few anti-virus vendors in the world to have its own technologies to detect and cure malware. Dr.Web anti-virus software allows IT environments to effectively withstand any threats, even those not yet known.

Doctor Web was the first company to offer an anti-virus as a service and, to this day, is still the undisputed Russian market leader in Internet security services for ISPs. 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 Russia

Phone: +7 (495) 789-45-87 (multichannel)
Fax: +7 (495) 789-45-97

антивирус.рф | www.drweb.com | estore.drweb.com | curenet.drweb.com | www.av-desk.com | free.drweb.com