Defend what you create

Dr.WEB®
since 1992

Why Dr.Web

1. Company

- Russian anti-virus software developer Doctor Web has been in operation since 1992.

Our customers

- The Russian government has trusted Doctor Web anti-virus products for many years. The products are used by the Russian military, Russia's State Duma, and the Administration of the President of the Russian Federation, and they are certified for use in governmental institutions, the national defence system, and the secret services. The certification process has confirmed that Dr.Web products contain no undeclared features and no vulnerabilities.
- Contemporary Russian elections have all been protected by the Dr.Web anti-virus; in 2002, we designed a special anti-virus for GAS ''Vybory'', the automated state information system that facilitates elections. In addition, we designed another special anti-virus for a special OS used by the Russian Ministry of Defence.
- Customers from all segments of industry use Dr.Web. Here are just some of our customers.
- Dr.Web Enterprise Security Suite protects both small to medium businesses and industry giants. Among the latter are customers who are protecting HUNDREDS of thousands of devices with Dr.Web. For example:
  - ✓ Russian Ministry of Defence — about * 00,000 devices;
  - ✓ Sberbank of Russia — 100,000 devices;
  - ✓ Information-computing centre in Udmurtia — 35,750 devices;
  - ✓ Russian Agricultural Bank — 24,000 devices.
- Doctor Web specialists designed a cloud-based solution based on the company's corporate anti-virus Dr.Web Enterprise Security Suite to deliver the anti-virus as a service through Internet service providers. Most of Russia's providers offer their customers the Dr.Web Anti-virus service. Some of those accounts have as many as tens of thousands of users. And Dr.Web handles such loads very well.

Technologies

- The company's software incorporates a proprietary anti-virus engine—only a few companies in the world have their own engine; most companies license one from other anti-virus vendors.
- All rights to Dr.Web technologies are reserved by Doctor Web.
- The company has over 26 years of experience studying the evolution of malware and creating anti-virus solutions to neutralise them. It has a deep knowledge of operating systems, software, and hardware and the ability to predict how malware will evolve.
- We develop what we excel at—basic, fundamental anti-malware protection and not new-fangled plugins (i.e., patches) for everything and anything. We are continuously improving our **basic, time-tested anti-virus** technologies (WannaCry was caught by our heuristic analyser, which we've been perfecting for almost 25 years) and developing **new advanced** anti-virus technologies (preventive protection, technologies powered by machine learning, etc.)
- We possess the highest competence in detecting and protecting customers' PCs from Internet threats.
- The best indicator of a quality anti-virus is not its ability to detect viruses but rather its ability to neutralise malware; its ability to not just delete compromised files containing important user information but also restore them to their original «healthy» state. The Dr.Web anti-virus functions on infected computers; its exceptional resistance to viruses makes it a standout among its competitors.

- Dr.Web is one of the few anti-viruses capable of detecting and neutralising viruses in RAM that never exist as files on disks. As yet, few anti-viruses can cure such viruses.
- Dr.Web can reliably detect packed malicious objects, regardless of whether Dr.Web recognises the compression format, and disassemble and analyse them in detail to expose hidden threats.
- Only Dr.Web can fully check archives at any nesting level. That means that the Dr.Web anti-virus will detect and neutralise a threat even if it has been compressed many times with various supported archiving programs.
- Unlike most of its competitors, Dr.Web can detect an infection in BIOS firmware, and starting with version 11.5—in UEFI firmware.
- Dr.Web has long been known as an anti-virus that uses system resources sparingly. This is thanks to special technologies that allow its databases to contain fewer entries and to the use of a specially designed database structure; as a consequence, the scanning speed doesn't change even as the number of known malicious programs increases.
- Unlike some other anti-viruses that have parts of their engine dynamically loaded into RAM, Dr.Web has its entire anti-virus engine stored in the memory. This enables Dr.Web to achieve the maximum database search speed and lower its hard-disk usage by not constantly sending queries to it.
- The Dr.Web virus databases possess a unique feature—an algorithm for searching for signatures in the virus databases, as well as in the firewall's and behaviour analyser's rules databases, which means the search time does not increase if the number of database entries increases.
- Just a single entry allows hundreds or even thousands of similar malicious files to be detected—including those that may be created by cybercriminals in the future. With the Dr.Web virus databases kept small, system requirements do not constantly need to be increased. Updates remain small, while the quality of detection and curing remains at the same traditionally high level.

Technologies powered by machine learning

Based on an accumulated knowledge of malware behaviour, these new technologies can detect signs of potential malicious behaviour **prior to a program's launch**. They have dramatically reduced Dr.Web's dependency on signatures, and significantly more newly released, unknown threats are being detected. Thanks to this new technology, the Dr.Web virus database stores the minimum amount of information, and the detection quality only improves with the record-low number of false positives.

Preventive protection technologies

- Dr.Web Preventive Protection analyses the behaviour of running processes, comparing them not to the rule database known to the application vendor, but to the rule database of typical malware behaviour. This feature allows Preventive Protection to avoid drawbacks that are common for our competitors' HIPS.
- The Dr.Web Preventive Protection rule database is small: the behaviour of all versions of all existing (and previous) software programs in the world do not need to be described—this means that Dr.Web performs scans faster, and the rule database itself uses fewer resources on user computers.
- Dr.Web Preventive Protection blocks up to 98% of encryption ransomware programs—and it does this solely on the basis of a description of their behaviour, without using signatures (if the component is enabled and properly configured).

2. Business products

- Within the company's sales structure, the share of Dr.Web licenses sold to businesses exceeds 62%.
- For many years, Doctor Web has been developing enterprise solutions. Dr.Web Enterprise Security Suite was released in 2003.
- Doctor Web has products that protect all corporate network nodes.

Dr.Web Enterprise Security Suite

- Dr.Web Enterprise Security Suite protects all networks, including those isolated from the Internet.
- The switch from a competitor's solution to Dr.Web can be carried out very quickly. Once it took us just two days to switch 1,000 computers to Dr.Web. That also speaks volumes about the quality of Dr.Web anti-viruses. Dr.Web lets you remove the anti-virus you were using previously when installing Dr.Web on workstations, servers, and mobile devices. In addition, you can request migration support from a Doctor Web technical support service specialist. Expenses related to migrating to Dr.Web are reimbursed with a 50% migration discount.
- Support for the Windows and Unix server platforms, a simple installation procedure, and reliable protection at minimal TCO compared with competitive solutions. With Dr.Web Enterprise Security Suite, your company won't have to purchase expensive hardware.
- The Control Center can be installed on any operating system.
- You can open the Dr.Web Control Center via your browser from anywhere in the world and even manage your anti-virus protection from your smartphone (via the mobile Control Center for Android/iOS). If a threat appears, you can instantly respond to it.
- You can even write event handlers in any script language, which gives you direct access to the Control Center's internal interfaces.
- The entire network protection infrastructure can be administered from one computer. Individual administrators can be assigned to different groups, making Dr.Web Enterprise Security Suite the perfect choice for both companies with high security requirements and multi-affiliate organisations.
- Unlike competitive solutions, Dr.Web has no restrictions on what databases can be used—most of today's DBMSs are supported. Oracle, PostgreSQL, Microsoft SQL Server or any other DBMS that supports SQL-92 over ODBC can be used as an external database.
- Dr.Web Enterprise Security Suite lets you implement the security policies needed for your specific company and separate groups of employees.
- Unlike competitive solutions that support very resource-consuming back-up systems for additional protection, for example to protect against encryption ransomware, Dr.Web provides long-term anti-virus protection for information in real time.
- The Dr.Web agent software can be installed on machines that are already infected, with a high probability of curing them during the installation process.

The non-signature anti-virus Dr.Web KATANA

- Aided by Dr.Web preventive technologies, Dr.Web KATANA protects against new threats that other developers' anti-viruses (not Dr.Web) cannot yet recognise: encryption ransomware and the penetration techniques most popular with today's virus writers—exploiting browser and office application vulnerabilities.
- Dr.Web KATANA starts protecting a system during the boot-up phase, even before the traditional, signature-based anti-virus is loaded.

- A non-signature anti-virus, Dr.Web KATANA can be installed on a device that already has an anti-virus without any conflict because it does not incorporate a file monitor.
- Dr.Web KATANA can operate completely autonomously, without an Internet connection and without being updated—a traditional anti-virus cannot provide protection under such conditions.
- Dr.Web KATANA detects malware as soon as it commences with its malicious activities and immediately blocks this process. Dr.Web KATANA does not use virus databases (and, therefore, does not have a virus database that requires updating). This is today's most lightweight, non-signature anti-virus—users can install it even on a low-power tablet.
- The product includes the Control Center.

Dr.Web Anti-spam

- Dr.Web Anti-spam is unique. It does not contain message examples and works according to rules. In fact, it is preventive mail protection. Dr.Web Anti-spam filters out up to 98% of malicious files trying to penetrate a system via email messages. Anti-spam is only available with Comprehensive Protection as part of Dr.Web Desktop Security Suite.
- The anti-spam doesn't require configuration or training. Unlike anti-spam solutions that require daily training based, for example, on Bayesian filtering, it starts working as soon as the first message arrives. Therefore, the anti-spam doesn't require daily training by the system administrator.
- It detects spam messages regardless of their language.
- No email receipt delays.
- Real-time email filtering.
- High-speed filtering with low consumption of system resources.
- It can scan objects at any nesting level.
- It can choose a processing technology for the target object depending on the message envelope or the blocked objects detected.
- Messages that have been filtered out are placed in a separate folder so they can always be checked to make that sure that no false detection has occurred.
- These unique technologies eliminate the need for blacklists. No company will be discredited because someone deliberately added it to such a list.
- Stands alone—requires no constant connection to an external server or access to a database, which results in significant traffic savings.
- Does not need to be updated more than once every 24 hours—unique spam detection technologies based on several thousand rules allow the anti-spam to remain current, without frequent downloads of bulky updates.
- Highly effective junk-mail filtering is combined with low consumption of system resources. This is why the Dr.Web anti-spam can operate efficiently on low-end hardware.

The cloud-based Dr.Web vxCube service

- Dr.Web vxCube is a unique, intelligent, cloud-based, interactive analyser of suspicious objects.
- Detects and identifies unknown malware for Windows and Android.
- If the analysis determines that Dr.Web is not yet able to detect the submitted file, a custom Dr.Web CureIt! build will instantly be generated for you to cure your system, allowing you to quickly neutralise infections that are unknown to your anti-virus.

Discounts and other benefits

- Customers migrating from a competitor's anti-virus to a one-year Dr.Web license receive a 50% discount. Customers migrating to a two-year Dr.Web license receive one year of protection for free.
- 20% off when purchasing two Dr.Web Enterprise Security Suite products; 25% off when purchasing three products.
- A renewal discount applies to additional purchase + renewal.
- Discounts for educational and medical institutions—50% for new licenses and 65% for renewal licenses.
- Files that have been corrupted by encryption ransomware can be recovered free of charge for Dr.Web business product users.

Technical support

- 24/7 technical support.
- Paid VIP support.
- Free technical presale — including during the trial period.

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

https://www.drweb.com | https://free.drweb.com | https://ru.av-desk.com | https://curenet.drweb.com