



Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks



Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks

A next-generation non-signature anti-virus that operates in tandem with your traditional anti-virus to better protect your computer

Any institution would regard the following as critical: breaches in the continuity of business processes, unauthorised device access, the exploitation of vulnerabilities, password cracking, phishing, and other illegal activities, including those occurring during virus-related computer incidents (VCIs) where malware has been deployed.

Unfortunately, today, for a whole range of reasons, it is imperative to not rely on the anti-virus protection of just one vendor.

Virus writers scan technologically sophisticated and highly dangerous viruses with all known anti-viruses before releasing them into the wild.

Therefore, if you rely on scanning that only utilises anti-virus databases — no matter how high-quality they are — attackers will always have a time advantage: malicious code may already be known to an anti-virus vendor, but the anti-virus on a user's device may not yet have received knowledge of it.

Computers are ALWAYS at risk of getting infected with brand-new UNKNOWN malicious programs.

When do users need two anti-viruses?

- When their main anti-virus misses threats.
- When their main anti-virus cannot be updated frequently.
- When their PC is out of the Internet access zone for a long time.
- When their PC is in an isolated network where updates are rarely delivered

A non-signature anti-virus is always required: you can't know whether or not your anti-virus missed a malicious program.

So that you can better protect your local network and its nodes from the newest and most dangerous malicious programs, including cryptolockers, we invite you to enhance the capabilities of your conventional, non-Dr.Web anti-virus with the non-signature anti-virus **Dr.Web KATANA**.

No anti-virus can detect 100% of malicious programs at the moment of penetration. Unfortunately, the most dangerous malware programs, such as encryption ransomware, can bypass traditional anti-virus security methods.

Even if the anti-virus you use is a frequent winner of various tests, you must remember that at the time of testing, analysts and test organisers are already familiar with the malicious programs being used in the testing. This means that the receipt of an award by an anti-virus is no indication that the anti-virus can neutralise active threats that are unknown at the moment of attack.

Why were so many companies whose networks were protected by anti-virus test winners affected by WannaCry? Their anti-viruses didn't have the new Trojan's signature, and their behaviour analysis modules failed to protect their systems.

Meanwhile, Dr.Web customers were not affected by WannaCry.

The best way to protect your system from brand-new threats that your signature-based anti-virus may not recognise is to rely on **Dr.Web KATANA** technologies, which look for signs of malicious behaviour in running processes as they analyse program behaviour. The product protects against threats not detected by traditional methods of detection (signatures).

All Trojans do this

Operate in a similar way:	Make the same mistake:
they exploit the same vulnerabilities and carry the same payload.	they make the first move (by attacking a system).

Any sign of malicious activity is enough for Dr.Web KATANA to spot it and neutralise it.

The non-signature anti-virus Dr.Web KATANA does what a traditional anti-virus does:

- detects malicious processes,
- deflects malware attacks,
- disrupts intrusion attempts,— but it accomplishes this in a more elegant way.

Dr.Web KATANA will detect malicious activity as soon as a Trojan attempts to make the first move.

- Many Trojans operate in a similar way; they exploit the same vulnerabilities and carry the same payload.
- All Trojans make the same mistake: they make the first move (by attacking a system).
- Any sign that a Trojan has become active is enough for Dr.Web KATANA to spot the enemy and deliver a killing blow.
- Dr.Web KATANA analyses the behaviour of each threat in real time and immediately neutralises harmful scripts and processes that your anti-virus didn't manage to recognise.

And no signatures are required, which makes Dr.Web KATANA a very lightweight weapon.

Common behaviour-analysis solutions rely upon well-defined behaviour patterns of known illegitimate programs.

Criminals know those patterns too!

They can exploit vulnerabilities to bypass security routines.

Instant detection with Dr.Web KATANA	Split-second analyses	No need to rummage through bloated databases
---	----------------------------------	---

Dr.Web KATANA keeps an eye on

- Legitimate application processes.
- Critical system areas and services—boot sectors and registry keys, including those responsible for virtual device drivers.
- Application usage rules.
- The disablement of Safe Mode.
- The deployment of new system routines by intruders.
- The installation of any new drivers.
- Communications between spyware programs and their control servers.
- Scheduled backups.
- All popular web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Vivaldi Browser).
- MS Office applications (Word/Excel/InfoPath/Lync/Access/Outlook/Visio/WordPad), Windows Media Player.
- System utilities.
- Applications that use java- (Java 1.8 / 6/7), flash- and pdf-technologies (Acrobat Reader).

Dr.Web KATANA's functional capabilities

- Protects critical system areas from being modified by malware.
- Detects and stops the execution of malicious, suspicious or unreliable scripts and processes.
- Detects unwanted file modification, monitors the operation of all processes to detect actions that are typical of malware (e.g., the activities of encryption ransomware), and prevents malicious objects from injecting their code into other processes.
- Detects and neutralises the latest threats: encryption ransomware, injectors, remote-controlled malware used for espionage and to create botnets, and malware packers.
- Protects against exploits—malicious objects that take advantage of software flaws, including those not yet known to anyone except for the intruders who created them (so-called zero-day vulnerabilities).
- Controls the operation of the most popular browsers and their associated plugins; protects against browser blockers.
- Blocks malware's ability to modify boot disk areas in order to prevent the launch of Trojan horses, for example, on your computer.
- Blocks changes from being made to the Windows Registry to ensure that the safe mode won't be disabled.
- Prevents malicious programs from altering basic system routines. By blocking certain Windows

Registry keys, it prevents malware from changing the appearance of the desktop or hiding a Trojan with a rootkit.

- Prevents malware from changing launch permissions.
- Prevents new or unknown drivers from being downloaded without user consent.
- Prevents malware and certain other applications, such as anti-antiviruses, from adding their entries into the Windows Registry so that they could be launched automatically.
- Locks registry sections containing information about virtual device drivers, ensuring that no new virtual devices are created.
- Blocks connections between spyware components and the server that controls them.
- Prevents malware from disrupting system routines such as scheduled backups.

How Dr.Web KATANA works

- If it detects attempts to exploit a vulnerability, Dr.Web will end the attacked process immediately. It won't perform any actions with application files and won't move any files to the quarantine.
- Users will also see notifications about a thwarted attempt to perform malicious actions; no response on their part will be required.
- An entry about the disrupted attack is added to the Dr.Web event log.
- The cloud will also be instantly notified about the incident. If necessary, Doctor Web specialists will instantly respond, for example, by upgrading the system monitoring routine.

How Dr.Web Cloud helps

Dr.Web Cloud contains:

- information about the routines used by programs with malicious intentions;
- information about files that are 100% clean;
- information about compromised digital signatures of well-known software developers;
- information about digital signatures used by adware and riskware;
- protection routines used by applications.

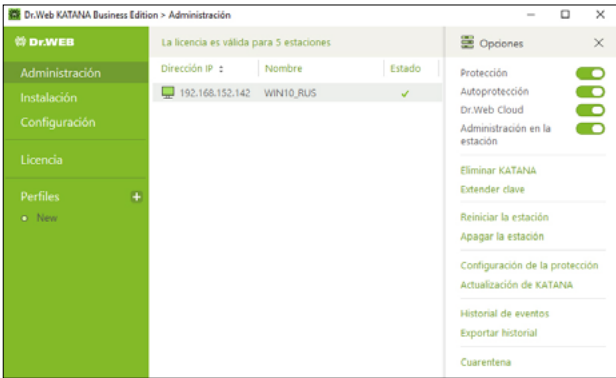

Dr.Web KATANA's cloud system can collect information about the work Dr.Web KATANA is doing on protected PCs, including data about brand-new threats, which enables Doctor Web to respond promptly to discovered defects and update rules stored on a computer locally.

We do not transmit user files from a protected system to Doctor Web's servers!

Maximum advanced protection	Exceptionally reliable protection	Offline mode
<ul style="list-style-type: none"> Dr.Web KATANA starts protecting a system during the boot-up phase. It starts protecting even before the traditional, signature-based anti-virus (your other anti-virus) is loaded! 	<ul style="list-style-type: none"> Dr.Web incorporates a unique self-defence module: Dr.Web SelfPROtect. If a Trojan disables the other anti-virus, it will then have to disable Dr.Web KATANA, but the self-defence module will rise up against it. Thanks to its ability to defend itself, Dr.Web KATANA will prevail, while the malicious process will be terminated. 	<ul style="list-style-type: none"> Trojans can't replicate themselves. Employees carry Trojans from one computer to another on USB flash drives and other removable devices. The non-signature anti-virus Dr.Web KATANA will help in situations where the installation of a "heavy" signature anti-virus is impossible. It has minimum system requirements and can run on a PC that has no Internet access.

Management

<ul style="list-style-type: none"> Centralised installation on protected network stations, configuration and monitoring of virus events and Dr.Web KATANA's status on protected stations. 	<ul style="list-style-type: none"> Pre-installed protection scripts (optimal, medium, paranoid) — the product works right "out-of-the-box". 	<ul style="list-style-type: none"> The user can create flexible rules for trusted applications to prevent conflicts that may otherwise be caused by Dr.Web KATANA. 	<ul style="list-style-type: none"> A Dr.Web KATANA user can configure Dr.Web's control parameters to protect a specific application so that it receives access only to certain resources.
--	--	---	--

Control Center	Agent
 <p>The screenshot shows the 'Administración' (Administration) window of Dr.Web KATANA Business Edition. It features a sidebar with navigation options: Administración, Instalación, Configuración, Licencia, and Perfiles. The main area displays a table with columns for 'Dirección IP', 'Nombre', and 'Estado'. Below the table, there are sections for 'Opciones' (Protection, Autoprotección, Dr.Web Cloud, Administración en la estación), 'Eliminar KATANA', 'Reiniciar la estación', 'Apagar la estación', 'Configuración de la protección', 'Historial de eventos', and 'Cuarentena'.</p>	 <p>The screenshot shows the 'Configuración' (Configuration) window of the Dr.Web KATANA Agent. It includes a sidebar with options: Principal, Actualización, Autoprotección, Dr.Web Cloud, and Protección. The main area is titled 'Modo de funcionamiento' (Operation mode) and shows a dropdown menu set to 'Óptimo (recomendado)'. Below this, there are sections for 'Protección contra exploits' (Exploit protection) and 'Protección contra exploits' (Exploit protection) with a dropdown menu set to 'Bloquear la ejecución de código no autorizado' (Block execution of unauthorized code).</p>

Compatibility

While in development, Dr.Web KATANA was deemed compatible with products produced by TrendMicro, Symantec, Kaspersky, McAfee, ESET, and others.

New! Dr.Web vxCube

Intelligent and interactive cloud-based analyses of suspicious objects for security researchers and cybercrime investigators

Dr.Web vxCube:

- Remotely analyses an object in an environment that matches your situation
- Allows users to observe the analysis
- Reproduces any of the suspicious object's actions for further research
- Provides a complete analysis report

A custom Dr.Web CureIt! build will be generated for you if a threat is detected so that your system can be cured—before the problem could be solved by your anti-virus.

Dr.Web CureIt! can operate without being installed in your system even when another anti-virus is present.

[Learn more about Dr.Web vxCube](#)

Virus-related computer incident expert consultations (VCI)

The consultations include:

- An initial assessment of the incident, the scope of the investigation, and the measures required to remedy the consequences of the incident.
- An examination of the computer and other related items (hard disks, and text, audio, photo, and video materials) that are presumably related to the VCI.
- **Exclusive!** A psychological evaluation of individuals (company personnel) to identify possible accomplices involved in/assisting with/covering up or supporting illegal activities against the customer (a comprehensive risk assessment) as well as facts related to inaction or dereliction of duty.
- Recommendations on the deployment of an anti-virus protection system that would prevent VCIs or reduce them to a minimum in the future.

[Learn more about Doctor Web consultations \(VCI\)](#)

Consultation requests can be submitted here:

<https://support.drweb.ru/expertise>

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 was the first company on the Russian market 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.

Customers trust Dr.Web

Doctor Web's IT security experts possess a wide range of capabilities, which allows the company to thoroughly understand the operational nuances of all kinds of businesses and offer its customers the best selection of quality products at minimal TCO.

The fact that Doctor Web has satisfied customers—home users, major corporations, and small businesses—all over the world is clear evidence that the quality of its products, created by a talented team of Russian programmers, is undisputed.

Here are just some Dr.Web customers: <https://customers.drweb.com>.

Why Dr.Web?

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.



© **Doctor Web**
2003–2021

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125124

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>