Dr.WEB®

Enterprise Security Suite

The best comprehensive protection solution for your local network

Defend what you create

This document describes distinguishing features of **Dr.Web Enterprise Security Suite Control Center** compared with competitive products. The comparison is based on information about features described by corresponding vendors in documentation for respective products.

This document provides comparison of the following products:

Similar competitive solution*				
Eset	**Kaspersky Lab**	**McAfee**	**Trend Micro**	**Symantec**
Remote Administrator	Administration Kit	ePolicy Orchestrator	Client Server / Client Server Messaging Security for SMB	Endpoint Security Services (Endpoint Protection and Network Access Control)

* The products' latest versions were used for this comparison

General feature comparison table

The table contains the following symbols:

- ✓ – feature is available;
- ✗ – feature is not available;
- if a cell is empty, no valid information, as to whether the feature in question is present in the product, is available.

Functionality	Dr.Web	McAfee	Kaspersky Lab	Eset	Trend Micro	Symantec
Support of different types of networks						
Multi-platform server software – server software available for Unix-like operating systems as well as for Windows	✓	✗	✗	✗	✗	✗
Different types of DBMS for the anti-virus server	✓	✗	✓	✓	✗	✓
Hierarchical multi-server anti-virus network structure	✓	✓	✓	✓	?	✓
Aggregation of information from several servers and its presentation as summary statistics	✓		?	?		
Support of TCP/IP (including IPv6), IPX/SPX, NetBIOS	✓	✓ / ✗ / ✗	✓ / ✗ / ✗		✓ / ✗ / ✗	
A mobile user policy including an option to update the software over the Internet	✓	✓	✓	Created manually / ✓	✗	✗
Option to encrypt communication between different system components	✓	✓	✓			

Dr.WEB®
Enterprise Security Suite

Functionality	Dr.Web	McAfee	Kaspersky Lab	Eset	Trend Micro	Symantec
Automatic distribution of agents between several servers for load balancing, retrieval of updates by a selected server	✔	✔	✘	✘		✘
Protected network size	No limits	Up to 250 thousand machines		no more than 1000 clients connected simultaneously to	One Trend Micro Security Server can serve up to 2500 clients	Unknown
Installation and updating						
Retrieval of updates by one server and their subsequent transfer to other servers directly or via other hosts	✔	✔	✔	✘	✘	Via computers in the network or via the LiveUpdate
Computers retreive updates via a proxy server	New!	✘				
Special data compression algorithms for traffic minimization	✔		✔			
Bandwidth allocation in selected IP subnets	New!		✔			
Bandwidth allocation in certain IP subnets for a specified period of time	✘		✔			
Centralized updating for virus databases and anti-virus software installed on protected computers	✔	✔	✔	✔	✔	✔
Centralized remote installation of anti-virus software on personal components and servers	✔	✔	✔	Procedure unclear	✔	✔
Restart updating after an error has occurred	✔	✔	✔	✔	✔	
Forced updating for failed components of the software installed on user machines	✔		✔			
On demand updating	✔	✔	✔	✔		
Automatic updating	✔	✔	✔	✔	✔	✔
Customizable updating schedules	✔	✔	✔		✔	✔
Configuration of client updating schedules from the administration server	✔		✔			
Create restore point prior to agent installation and restore deleted computers	New!					

Functionality	Dr.Web	McAfee	Kaspersky Lab	Eset	Trend Micro	Symantec
Version upgrade control, customizable list of updated components and verbosity level for the log of data exchange between the server and agents	✓		✗		✓ / ✗	
Adding custom components to products or new products, which also will be synchronized	✓				✗	✗
Installing products from third-party developers	✓	✓	✓	✓	✗	✗
Authorization required for remote installation	✓		✓	✓		✗
Remote installation according to Active Directory policies	✓	✗		✓	✗	✓
Centralized installation utilizing Login Script	✓	✓	✓	✓	✓	
A local computer connects to the server, in the case if the if it can't be established by the latter (blocked by a firewall, opening ports on a client machine is not allowed, client IP is unknown, etc.)	✓	✓	✓			
Scan network to detect unprotected computers	✓	✓	✓		✓	✓
Search and uninstall third-party security software	Improved!	✓	✗		✗	✗
Selection and configuration of software components before their installation	✓	✓	Custom installation packages are used for this purpose	✓		
Backup critical anti-virus server data	✓	✓	✗		✗	✓
Centralized quarantine	✓		✓			✓
Custom quarantine size	✓		✓			✓
Flexible information security policies						
Centralized configuration of the anti-virus software even for computers currently offline	✓ / ✓	✓	✓ / ✓	✓	✓ / ✗	
Settings updates by the server	✓	✓	✓	✗		✓
Simplified administration through the grouping mechanism, group replication between servers	✓	✓	✓	✓ / ✗	✓ / ✗	✓ / ?
Usage policies, policies prohibiting users to change anti-virus settings	✓	✓	✓	✗		✓

Functionality	Dr.Web	McAfee	Kaspersky Lab	Eset	Trend Micro	Symantec
Individual access permissions for different administrators and users	✓	✓	✓			✓
Configuration of anti-virus software by users according to their permissions	✓	✓	✓			✓
Switching between user and administrator management modes	Improved!					
Disable removal of the anti-virus software by a user	✓	✓	✓	✓	✓	✓
Include a computer into several groups	✓		✓			✓
Move and rename groups	✓		✓			✓
Network status monitoring						
Control network protection virtually from any computer — platform-independent admin- istration tools	✓	✗	✗			
Administrator web interface	✓	✓*	✗	✗	✓	Requires JRE
Easy protection monitoring with computers divided into groups according to their secu- rity status	✓	✓	✗			
Monitoring virus events and status of anti-virus software packages and operating systems on all protected computers	✓	✓	✓			
Computer search over the network, mask-based search	✓	✓	✓ / ✗	✓ / ✗	✓ / ✗	
Search for connected stations by pre-defined parameters	✓	✓	✓	✓	✓	
Verify compliance of protected computers with established policies, controlled access to the network	✓	✓	✓		✗	✓
Read-only access to the Control center	Improved!	✓	✓	✓		
Administration audit	Improved!	✓	✓	✗		
Adjustableclient and administrator permissions	New!				✓	✓

Dr.WEB®
Enterprise Security Suite

Functionality	Dr.Web	McAfee	Kaspersky Lab	Eset	Trend Micro	Symantec
Hosts protection						
Control over protection of Windows PCs and servers	✔	✔	✔		✔	✔
Administer anti-virus software for Novell NetWare file servers	✔					
Administer anti-virus software used on devices running Windows Mobile	✔					
Administer anti-virus software for Unix mail servers	✔	✘	✘	✔	✘	
Spam filtering	✔	Separate product	✔	✔	✔	
Protection from all types of malicious objects	✔	✘**	✔	✔	✔	✔
Adjustable scanning priority	✔		✔ / ✘		✘	
Multi-thread scanning	BurstScan	✘	✘			
Forced disconnection from the network while scanning is being performed	New!					
SMTP, POP3, IMAP traffic scan	✔		✔			
POP3S traffic scan	New!		✔			
IMAP traffic scan	New!		✔			
HTTP-traffic scan	✔	Separate product	✔			
Customizable list of applications whose traffic will be scanned and scan exceptions. Adjustable controlled ports	✔	Separate product			✘ / ✔	
Block access to local resources and web-sites on the Internet	✔	Separate products	✔ / ✘			
Block access to protected directories and removable data-storage devices	✔	Separate product — Host DLP	✔		✔	
Firewall	New!				✔	✔
Protection of system files and Registry branches	System Protection					
Russification of the product, documentation and technical support in Russian	✔	✔ / ✘	✔	?		

Functionality	Dr.Web	McAfee	Kaspersky Lab	Eset	Trend Micro	Symantec
Notifications about threats of different types for administrators and users						
Notifications about detected threats for users	✔	✔	✔	✔	✔	✔
Information messages for users	✔	✔	✔	✔	✔	✔
Alerts sent if an action has been taken according to a redefined rule	✔***	✔	✔	✔		
Editable administrator notification templates	✔	✔	✖			✔
Customizable responses to incidents (notify an administrator via e-mail or via NetSend)	✔ / ✔	✔	✔		✔	✔ / ✖
Reports and statistics						
Built-in reporting system	✔	✔	✔		✔	✔
Generating reports according to the administrator-defined schedule and sending such reports over e-mail and mailing of reports	✔ / ✔	? / ✖	✔ / ✔	✔		
Generate virus activity graphs, retrieve statistics regarding detected malware and actions performed with viruses.	✔	✔	✔			✔
Customizable list of information types that will be added to statistics table and stored in the server's database	✔		✔			✔
Centralized analysis of statistical information from several servers	✔		✖			
Возможность экспорта отчетов	✔	✔				✔

* Requires Java Runtime Environment Another disadvantage is that Installation of JRE requires a system reboot.

** No anti-phishing for a browser or e-mail client, no HTTP real-time scan. A separate product is available to scan traffic at the entry point between the local network and the Internet (the former title is Web Washer).

*** Including an opportunity to write a custom event handler using any script language.

Conclusions

The comparison provided in the table above shows that **Dr.Web Enterprise Security Suite** is a unique product.

Comprehensive protection from existing threats

Dr.Web Enterprise Security Suite provides reliable protection from most existing threats. Its quality of curing and reliable self-protection capabilities leave no loophole for viruses and other malware to find their way into the protected environment. The built-in firewall and the office control help prevent viruses from exploiting the vulnerabilities of operating systems and applications and allow you to control the operation of installed programs.

Increased labour productivity

A deployment of **Dr.Web Enterprise Security Suite** gives an instant effect. Because the product provides comprehensive protection, the inflow of spam is cut completely, resulting in a much more productive working environment — important messages no longer get lost in a hefty volume of spam e-mails. In addition, computers in the network are no longer at risk of getting infected, which eliminates downtimes due to virus attacks and subsequent necessary system restoration.

Upholding reputation

With **Dr.Web Enterprise Security Suite** protecting the network criminals won't be able to turn it into the source of viruses and spam that may get onto customers' computers. Doctor Web's software helps you safeguard your reputation as a trustworthy partner.

Lower unrelated costs

With **Dr.Web Enterprise Security Suite** in a network, system administrators no longer spend time dealing with virus outbreaks. The solution also decreases the number of outages, as there are no virus incidents to neutralize or damages to repair.

Saved local traffic

The solution utilizes a specifically-designed data transfer protocol for TCP/IP, IPX and NetBIOS networks supporting special traffic compression algorithms to ensure low bandwidth consumption. The optimized protocol supporting data compression between an agent and a server ensures low traffic usage.

Simple license configuration

Dr.Web Enterprise Security Suite enjoys a flexible licensing system. With Dr.Web you purchase only components you need and nothing more. System administrators can take advantage of the Dr.Web LiveDemo service to test a desired software configuration on Doctor Web's server before purchasing it.

Minimal cost

Dr.Web Enterprise Security Suite is a comprehensive solution. It encompasses all required protection components and the single Control center. System administrators don't need to install a variety of products that may often suffer compatibility issues and can collect statistics with one press of a button. This product's support of Unix and its built-in database distinguish it from numerous competitive solutions and allow it to be deployed at minimal cost. Customers do not need to purchase expensive new hardware to use Dr.Web.

Experience with large projects

Among Doctor Web's customers are major national and international companies and banks, as well as Russia's government and educational institutions and scientific research institutes. Many of these entities have tens of thousands of computers in their networks. Moreover, Russia's highest government institutions entrust their information security to Doctor Web.

Single anti-virus control center

Dr.Web Enterprise Security Suite is an integrated solution that allows to deploy a protection system using one distribution. It simplifies deployment and often reduces acquisition costs. **Dr.Web Enterprise Security Suite** is a client-server software that enables control over protection of:

- Desktops and laptops running Microsoft Windows and Mac OS X.
- Winidows and Novell NetWare file servers.
- Unix, Microsoft Exchange, IBM Lotus, mail servers.
- Mobile devices running Windows Mobile.

A system administrator can choose to deploy a **Dr.Web Enterprise Security Suite** network via the webinterface, take advantage of the Active Directory or install the software manually. Installation can still be performed even if the host is unreachable for the anti-virus server.

Manage the anti-virus network with **Dr.Web Enterprise Security Suite** from virtually any computer connected to the Internet, regardless of its operating system. The only requirement is a web browser. **Dr.Web Enterprise Security Suite** allows administrators working within the network or remotely over the Internet to centrally manage all components of the anti-virus protection, monitor the status of all protected hosts, receive notifications about virus incidents and set up automatic responses to them. You only need a connection between the administrator's computer and the anti-virus server. Easy deployment and administration, flexible configuration of client installer packages, quick and efficient distribution of virus databases' updates between clients without additional configuration and update schedule are distinguishing advantages of **Dr.Web Enterprise Security Suite**.

Low-cost administration

The Control Center's maintenance costs are reduced to a minimum thanks to simple administration routines and the Web-administrator's ability to provide an at-a-glance view of the entire corporate antivirus network from anywhere in the world. The versatile Web-administrator, combined with the solution's seamless integration with Windows NAP and the option to create custom event handlers in any script language, reduces the workload of system administrators by freeing them of daily anti-virus routines. The deployment of **Dr.Web Enterprise Security Suite** on all nodes in the network can reduce to zero restoration costs arising after a viral attack.

Exceptional scalability

Equally reliable in networks of any scale and structural complexity, from small workgroup networks to distributed intranets with tens of thousands of hosts, the Control Center offers exceptional scalability. Interaction between the anti-virus servers of the Control Center (which is connected to a SQL-server used for data storage) and between the servers and protected workstations that make up the complex communication system is organized hierarchically.

This results in a single anti-virus network of interconnected workstations, making it possible to collect information about the entire network on one server. The hierarchical organization makes the Control Center the perfect choice for multi-branch companies whose networks are not connected to the Internet. Even if one server is disconnected from the network the network will still maintain a required level of security. The hierarchical organization makes the Control Center the perfect choice for multi-branch companies whose networks are not connected to the Internet.

Widest range of supported operating systems and networking protocols

The architecture of the **Dr.Web Enterprise Security Suite** server software lets you use it on servers running both Windows, and UNIX, the feature unavailable in competitive solutions. **Dr.Web Enterprise Security Suite** can be installed under virtually any operating system. Installation does not require any changes in the existing infrastructure.

The solution can work with several network protocols simultaneously to establish communication between the anti-virus sever and agents: TCP / IP, IPX / SPX, NetBIOS, which allows the use **Dr.Web Enterprise Security Suite** in a variety of networks. Communication between different components of the system can be encrypted to ensure secure communication between anti-virus network components, thus making it safe to administer the network from any computer anywhere in the world. The integrated

backup routines guarantee that operation of **Dr.Web Enterprise Security Suite** will be restored even after a server crash.

The operation of a Dr.Web anti-virus network is completely transparent. An administration audit log records all installation and configuration activities. All components can record their activities in separate log files with customized verbosity, and all file operations performed by the anti-virus software are reflected in the statistics. A notification system informs administrators about problems in the network. Such notifications can be displayed by the Web-administrator or sent via e-mail.

Key features

The key features of **Dr.Web Enterprise Security Suite**:

- Comprehensive protection of workstations from most known threats powered by the built-in anti-virus, anti-spam, firewall and office control Support of Windows and Unix server platform, simple installation procedure and reliable protection Minimal TCO Centraliy managed end-point security for the entire network: PCs, mail, file and application servers, including terminal servers.
- Support of 32- and 64-bit operating systems.
- Installation of the agent software onto an infected machine and a high probability of its successful curing.
- A small-sized engine featuring the latest technologies guarantees minimal usage of workstation and server resources.
- Efficiently detects threats including future viruses Flexible traffic scan settings allow to choose applications that will be allowed or prohibited to access local and Internet resources Protection of information from unauthorized access and occasional damage: **Dr.Web Enterprise Security Suite** scans files and traffic for viruses and spam and is also capable of blocking access to local resources including directories and removable data storage devices.
- Scanburst: **Dr.Web Enterprise Security Suite** can improve scanning speed by 30% by utilizing capabilities of modern computers.
- Administration of the entire anti-virus network infrastructure through a single control center from any computer.
- Facilitates the implementation of individual security policies for a company or for groups of employees which makes **Dr.Web Enterprise Security Suite** a perfect choice for companies with high security requirements and multi-affiliate organizations.
- Configurable security policies for any type of user, including mobile users, and for any workstation to ensure up-to-date, 24-hour protection Prevents settings' modification by users Protects networks isolated from the Internet Several installation methods – Active Directory policies, launch scripts and the built-in remote installation procedure. Installation can still be performed even if the host is unreachable for an anti-virus server.
- Support of a wide range of DBMSs; **Dr.Web Enterprise Security Suite** can work both with internal and an external database. An anti-virus server works equally well with Oracle, PostgreSQL, Microsoft SQL Server Compact Edition or any other DBMS that supports SQL-92 over ODBC.
- Custom event handlers written in any script language provide direct access to **Dr.Web Enterprise Security Suite**'s internal interfaces simultaneously supports several network protocols (TCP/IP including IPV6, IPX/SPX, NetBIOS) allowing the anti-virus network to be deployed using an existing network infrastructure.
- Administration from any machine over the Internet or from inside the local network, easy-to-use software controls and powerful hosts search allow an administrator to provide reliable security with little effort.
- Powerful self-protection system preventing attempts of malicious programs to disrupt operation of the solution.
- Customizable list of product components for updating and version upgrade control, enabling administrators to distribute only those updates that are necessary and have been tested in the network Hierarchical organization of the protection system and collection of overall network statistics on one server.
- **Dr.Web Enterprise Security Suite** is certified by FSTEC and FSB and therefore can be used in networks with high security requirements.

With **Dr.Web Enterprise Security Suite** you can:

- Ensure comprehensive protection against existing threats.
- Increase the employee productivity.
- Reduce non-core expenses.
- Uphold the company's reputation.
- Save local traffic.
- Install the software on the day of purchase.

System requirements

	Server	Control system	Administration agent
Dr.Web	■ Intel ® Pentium ® III CPU 667 MHz or higher ■ 512 MB RAM ■ up to 20 GB of hard disk space ■ Windows 2000 and later, Linux, FreeBSD or Solaris.	Internet Explorer 7 or greater or Mozilla Firefox 3.0 and later.	■ Intel ® Pentium ® IV CPU 1,6 GHz or higher; ■ 512 MB RAM ■ 180 MB hard disk space ■ Windows 98 and above * (both 32 - and 64-bit systems), UNIX (Linux, FreeBSD, Solaris), Windows Mobile, Novell NetWare.
McAfee	■ 500 MB Free disk space minimum (first-time instal-lation); 1GB minimum (upgrade); 2GB recom-mended. ■ 512 MB available RAM; 1GB recommended. ■ Intel Pentium II-class or higher; 450 MHZ or higher. ■ Windows 2000 Server/Ad-vanced Server SP3 or later ■ Windows Server 2003 Standard/Enterprise/Web SP1 or later. ■ Microsoft Internet Explorer 6.0 SP1or later. ■ SQL Server 2005 ■ MSDE 2000 ■ SQL 2000	Microsoft Internet Explorer 6.0 with SP1or later.	■ 540 KB RAM. ■ Intel Pentium 166 MHZ or higher ■ 120 MB free disk space ■ Сеть Microsoft or Novell NetWare (TCP/IP) ePolicy Orchestrator are supported: Citrix Metaframe XP/1.8 for Windows. Microsoft Cluster Server (MSCS) is supported ■ Operating system Windows 2000 with SP1, 2, 3, or 4. Windows NT 4.0 with SP4, 5, 6, or 6a. Windows Server 2003 Windows XP SP Windows Vista ■ Linux Red Hat Enterprise ■ Solaris 8, 9, 10 ■ Macintash (before Leopard) ■ Linux (for use with Linux Shield) ■ Novell NetWare
Kaspersky Lab	■ Microsoft Data Access Com-ponents (MDAC) version 2.8 or higher ■ MSDE 2000 SP3 or Mst SQL Server 2000 SP 31 and above or MySQL version 5.0.32, or Microsoft SQL 2005 and higher or Micro-soft SQL 2005 Express and higher ■ Windows 2000 SP 1 and later; Windows XP Profes-sional/64 SP 1 or higher; Windows Vista/64 ■ Intel Pentium III 800 MHz or higher 128 MB RAM ■ 400 MB disk space.	■ Microsoft Windows 2000 SP1 and later; Microsoft Windows XP Professional SP1 and later; Microsoft Windows XP Home Edition SP1 and later; Microsoft Windows XP Professional x64 and later; Microsoft Windows Server 2003 and later; Micro-soft Windows Server 2003 x64 and later; Microsoft Windows NT4 SP6a and later; Microsoft Windows Vista/64 ■ Microsoft Management Con-sole version 1.2 and later ■ Intel Pentium II 400 MHz and later 64 MB RAM ■ 10 MB of disk space.	■ Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 SP1 and later Microsoft Windows NT4 SP6a or higher; Microsoft Windows XP Professional/64 SP1 or later, Microsoft Windows Server 2003/64 and above; Microsoft Windows Vista/64, Novell NetWare 6 SP3 and above; Novell NetWare 6.5 SP3 or higher ■ Intel Pentium 233 MHz or faster 32 MB RAM ■ 10 MB of disk space.
Eset	OS Windows: NT4, 2000, XP, 2003, Vista и 2008.		■ administrative share ADMIN ■ Clients can respond to PING-queries ■ There are administrator login and password on client machines ■ the Simple File Sharing service is disabled ■ Server, Remote Registry and Files and printer sharing services are running.

* SpIDer Gate, SelfPROtect, Firewall, Office control and Dr.Web for Outlook work under Windows 2000 (SP4) and later.
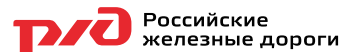
About Doctor Web

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 products of the company.

Doctor Web is one of the few anti-virus vendors in the world that owns its technologies for detecting and curing malware, has its own virus monitoring service and analytical laboratory.

This provides a rapid response to latest threats and allows to solve any problems of customers in a few hours.

Large enterprise-network experience

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