

Survey of Products for the Protection of Workstations on Corporate Networks

For use by Kaspersky Lab sales departments and partners only



Table of Contents

1 Purpose of this document	3
2 Why INTEGRATED protection	3
3 Comparison of the main features of competitor solutions	4
4 Why Kaspersky Anti-Virus 6.0 for Windows Workstations	7
5 Why NOT Symantec	12
6 Why NOT Trend Micro	14
7 Why NOT McAfee	15

1 Purpose of this document

This document provides a comparative analysis of **Kaspersky® Anti-Virus 6.0 for Windows Workstations** and **Kaspersky® Administration Kit**, an administration tool, **with competing integrated products** that protect workstations running under Microsoft Windows on corporate networks.

Kaspersky Administration Kit is a free tool that provides the functionality necessary for remote administration of all features of the program.

The purpose of this document is to provide thorough explanations of the advantages of **Kaspersky Lab products for potential customers and journalists**.

As used in this document, the term “integrated products” refers to solutions that provide protection from all known types of computer threats, including viruses, hacker attacks, spyware, spam, phishing attacks and undesirable Internet content.

The following solutions are analyzed in this document:

Developers	Product names (versions)
Kaspersky Lab	Kaspersky Anti-Virus 6.0 for Windows Workstations and Kaspersky Administration Kit 6.0
Symantec	Symantec Client Security 3.1 & Symantec System Center 10.1
Trend Micro	Trend Micro OfficeScan 7.0 Client / Server Edition & Trend Micro Control Manager 3.5
McAfee	McAfee VirusScan Enterprise 8.5i & McAfee ePolicy Orchestrator 3.6.0

2 Why INTEGRATED protection

Rather than a set of separate components from different vendors

Contemporary computer threats are integrated or blended. Installing only an antivirus, firewall or anti-spyware program cannot guarantee complete security. What is required is an integrated approach to security that will provide protection from all known types of threats.

Today, corporate users are becoming increasingly mobile (with the help of laptop computers and other mobile devices) and consequently, the concept of network perimeter is eroding. As a result, integrated protection needs to be provided at the level of every computer (host), not only at the network perimeter.

Comprehensive protection of a personal computer can be provided only by using an integrated set of components that share the same operating logic, because only this can ensure complete integration, eliminate software conflicts and provide a high level of protection.

3 Comparison of the main features of competitor solutions

	Kaspersky Anti-Virus 6.0 for Windows Workstations	Symantec Client Security 3.1	Trend Micro OfficeScan 7.0 Client/Server Edition	McAfee VirusScan Enterprise 8.5i
Protection quality				
Overall detection rate (%)*	99.06	98.13	-	92.40
Detection rate for compressed files (%)**	83	49	28	74
New threat response time (hours)***	0 to 2	10 to 12	4 to 6	8 to 10
Average number of updates per month****	664	33	32	24
Influence of the antivirus on system's performance (time in seconds required for standard operations) *****	174	208	236	196
Installation on infected computers and treatment of active infections	✓ Advanced Disinfection and self-defense technology	-	- Only scanning prior to installation	- Only scanning prior to installation
Proactive protection				
Heuristic analyzer	✓	✓	✓	✓
Behavior blocker (monitoring of dangerous activity)	✓	- Individual elements only	- Individual elements only	- Individual elements only
Rootkit detection	✓	-	-	-
Malicious change rollback	✓	-	-	-
File antivirus and on demand scanning				
Protection level selection. Configuration of the balance between scanning depth and speed	✓	-	-	-
The option to define the part of the disk that will be monitored by the antivirus monitor (i.e., to narrow down the protection scope).	✓	-	-	-
The option not to scan files downloaded from computers on the local network on which the antivirus is installed	✓ Network iSwift	-	-	-
Technology for suspending scanning during increased user activity	✓	✓	-	✓
Treatment of objects in archived and compressed files	✓ ZIP, ARJ, CAB, RAR, LHA	✓ ZIP, LHA	✓ ZIP, RAR2, LHA	✓ ZIP

	Kaspersky Anti-Virus 6.0 for Windows Workstations	Symantec Client Security 3.1	Trend Micro OfficeScan 7.0 Client/Server Edition	McAfee VirusScan Enterprise 8.5i
Mail antivirus	✓	✓	✓	✓
Protection level selection. Configuration of the balance between scanning depth and speed	✓	-	-	-
Scanning of POP3 and SMTP traffic	✓	✓	✓	✓
Scanning of IMAP4 traffic	✓	-	-	-
Web antivirus (scanning of HTTP traffic)	✓	-	-	-
Detection of spyware and other potentially hostile software	✓	✓	✓	✓
Protection from network attacks	✓	✓	✓	✓
Selection of the level of protection from network attacks	✓	✓	✓	-
Personal firewall	✓	✓	✓	✓
Intrusion detection / prevention subsystem (IDS/IPS)	✓	✓	✓	✓
Anti-phishing protection				
Protection from phishing attacks in emails	✓	-	-	-
Protection from phishing attacks when opening websites in the browser	✓	-	-	-
Antispam protection	✓	-	-	-
Scanning of SMTP, POP3 and IMAP4 mail	✓	-	-	-
Choice of stringency level for spam filtration	✓	-	-	-
Technology for analyzing message headers before downloading messages to the computer	✓	-	-	-
Trainable system based on a Bayesian algorithm	✓	-	-	-
Image analysis technology for spam recognition	✓	-	-	-
Protection from unwanted advertising (popup windows, banners)	✓	✓	-	-

*On demand comparative (Andreas Clementi, AV-Comparatives) (<http://www.av-comparatives.org>).

** Andreas Marx of Av-Test.org, May 2006.

***Ranking Response Times for Anti-Virus Programs (Andreas Marx of Av-Test.org); http://blog.washingtonpost.com/securityfix/2005/12/ranking_response_times_for_ant.html.

**** Andreas Marx of Av-Test.org, March 2006.

***** CNET Labs, October 2006.

	Kaspersky Administration Kit 6.0	Symantec System Center 10.1	Trend Micro Control Manager 3.5	McAfee ePolicy Orchestrator 3.6.0
Administration system	✓	✓	✓	✓
Centralized antivirus installation using Push Install	✓	✓	✓	✓
Centralized antivirus installation using Login Script	✓	✓	✓	✓
Automatic scanning of the network for unprotected computers. Scanning of IP-subnetworks / Active Directory / Windows Network	✓✓✓	✓!-	✓!- Vulnerability Scanner	-!✓
Automatic installation of antivirus applications on newly detected computers	✓	-	✓	-
Support for uniting computers into groups and subgroups and inheriting settings from higher levels in the hierarchy	✓ Unlimited number of groups and hierarchy levels	✓ Unlimited number of groups and hierarchy levels	✓ Unlimited number of groups and hierarchy levels	✓
Support for defining different access levels for different administrators / operators	✓	✓	✓	✓
Support for an unlimited number of levels in the administration server hierarchy	✓	-	-	-
Automatic centralized updating of antivirus databases and application modules on computers	✓	✓	✓	✓
Push updating	✓	✓	✓	✓
Multicast updating	✓	-	-	-
Special policy for mobile users activated on the client computer in the event of an interrupted connection with the administration server	✓	✓	-	-
Support for generating reports at the time specified by the administrator / send them to an email address for timely notification of the current protection level	✓!✓	✓!-	✓!✓	-!-
Support for Wake-on-LAN / Shut Down, enabling computers to be turned on / off remotely in order to perform scheduled tasks	✓!✓	-!	-!	-!
Backup copying of administrative server data	✓	-	✓	-

4 Why Kaspersky Anti-Virus 6.0 for Windows Workstations

Comparative analysis of the functionality of Kaspersky Anti-Virus 6.0 for Windows Workstations and Kaspersky Administration Kit demonstrates their overall superiority over competitor solutions.

- **Kaspersky Anti-Virus 6.0 for Windows Workstations is an integrated solution** that protects workstations from all known threat types, including viruses, spyware and other undesirable programs, hacker attacks, spam and phishing attacks.

All components of Kaspersky Anti-Virus 6.0 for Windows Workstations have the same operating logic and a single traffic interception and scanning point. This helps achieve conflict-free operation of all components, improves the product's performance and makes it more compact by reducing the size of the program's distribution package, as well as RAM and disk space requirements.

- **Proven superiority of Kaspersky Lab's antivirus engine:**
 - **Virus detection rates** confirmed by independent tests **are among the industry's highest:**

On demand comparative (Andreas Clementi, AV-Comparatives)

<http://www.av-comparatives.org>;

Comparative tests of antivirus programs (Virus.gr)

<http://www.virus.gr/english/fullxml/default.asp?id=82&mnu=82>



Source: On demand comparative (Andreas Clementi, AV-Comparatives)

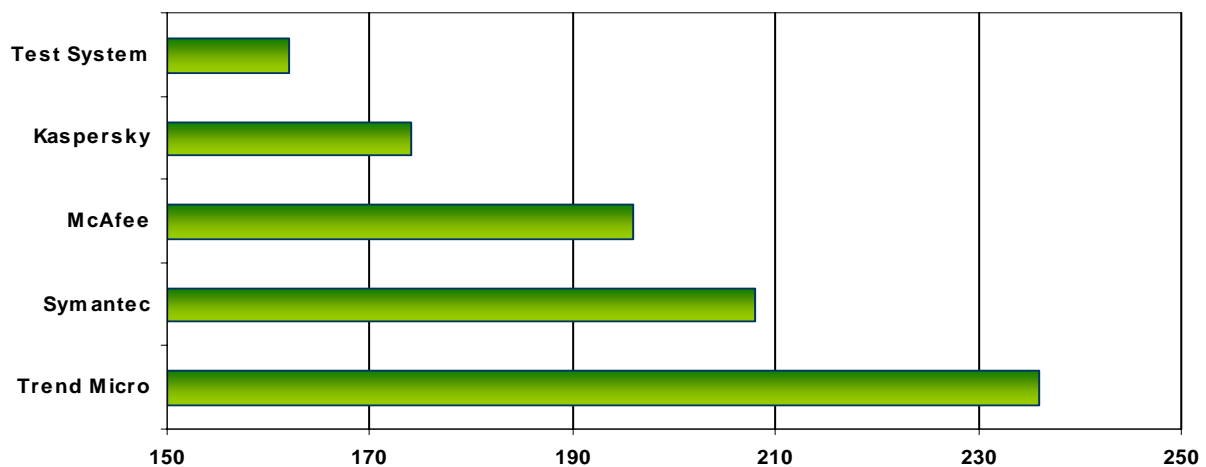
- **The shortest new threat response time:**

Average response time	2005	2004
0 to 2 hours	Kaspersky Lab	-
2 to 4 hours	BitDefender, Dr. Web, F-Secure, Norman, Sophos	Kaspersky Lab, BitDefender
4 to 6 hours	AntiVir, Command, Ikarus, Trend Micro	AntiVir, Dr. Web, F-Secure, Panda Software, RAV
6 to 8 hours	F-Prot, Panda Software	Quickheal, Sophos
8 to 10 hours	AVG, Avast, CA eTrust-InocuLAN, McAfee, VirusBuster	AVG, Command, F-Prot, Norman, Trend Micro, VirusBuster
10 to 12 hours	Symantec	Avast, CA eTrust-CA
12 to 14 hours	-	Ikarus, McAfee
14 to 16 hours	-	CA eTrust-VET, Symantec

Source: Ranking Response Times for Anti-Virus Programs (Andreas Marx of Av-Test.org), http://blog.washingtonpost.com/securityfix/2005/12/ranking_response_times_for_ant.html.

- **minimal influence of the antivirus program on the system's performance.** According to an independent test of the influence of antivirus software on the system's performance, Kaspersky Anti-Virus 6.0 for Windows Workstations demonstrated better results than competitor products.

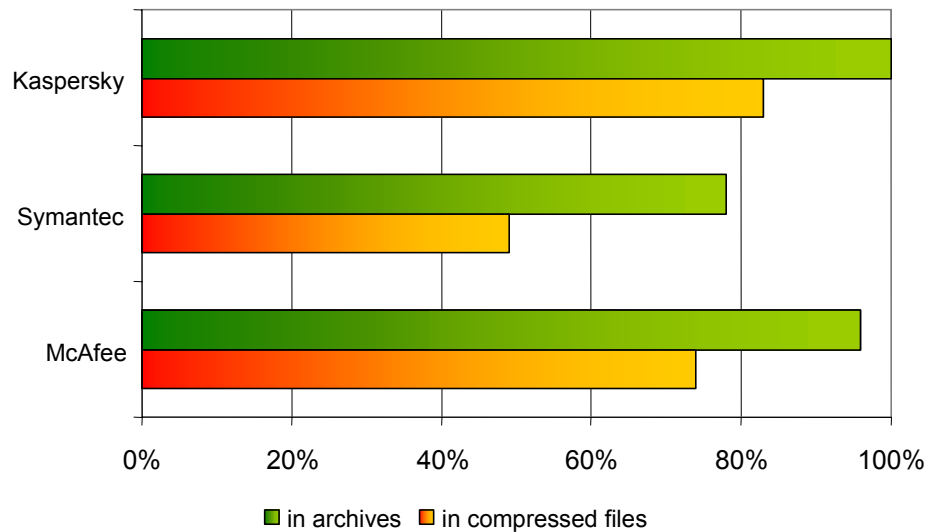
Influence of the antivirus program on the system's performance (time required to perform standard operations in seconds)



Источник: CNET Labs

- **Support for over 2000 archiving and compression utility formats** puts Kaspersky Anti-Virus 6.0 for Windows Workstations completely beyond the reach of competitors in terms of detection of viruses in compressed files. Packers (UPX, ASPack, etc.) are used to compress executable files (COM, EXE or DLL). When launched, a compressed file unpacks and executes itself in RAM, bypassing the hard drive. Consequently, if the antivirus program is unable to recognize the compression utility's format, the malicious code will not be detected, enabling it to be loaded in RAM, where it will be unpacked and executed. Most contemporary malicious programs are packed with one compression utility or another. In the spring of 2006, the AV-test.org team studied the capabilities of solutions in the internet security class in terms of detecting malicious programs in compressed files and archives within the framework of research conducted at the request of *PC World* magazine. The results of these tests are shown below:

Detection of malicious programs



Source: AV-test.org

- Kaspersky Anti-Virus 6.0 for Windows Workstations includes a powerful proactive defense module** that includes a heuristic analyzer, behavior blocker (which monitors the execution of executable modules and VBA documents), application and Windows registry integrity control and rollback of malicious changes made to the system. This suite of technologies provides an unparalleled level of protection from malicious code, blocking all possible penetration paths for new threats. **NONE** of the competitor solutions analyzed includes proactive protection with comparable capabilities.

Principal proactive defense features:

- Detection of attempts to launch the browser without the user's knowledge.** Proactive protection is able to intercept attempts to launch the Internet browser with parameters without the user's knowledge, which can be used by malicious programs, e.g., to send confidential data to cybercriminals.
- Code injection control.** Many malicious programs disguise their processes as processes of applications that are safe to run (such as Notepad, Internet Explorer, etc.). Proactive protection intercepts any attempts to inject code into other processes.
- Detection of hidden processes (e.g., rootkits).** Proactive protection detects rootkits, i.e., programs that make files, folders, registry keys, running programs, system services, drivers and network connections / activity invisible to the user.
- Window hook control.** The proactive defense module intercepts attempts to inject a dynamic link library into all active processes in the system. This blocks any attempts to retrieve passwords and other information entered on the keyboard.
- Detection of suspicious values in the registry.** Proactive protection intercepts attempts to create hidden keys in the registry that are not displayed by regular programs (such as regedit).
- Prevention of mail worm replication.** The application blocks attempts of mail worms to spread, preventing outbreaks on the local network if one of the computers becomes infected.
- Rollback of malicious changes.** As the antivirus solution registers all suspicious actions in the system, after a process is categorized as dangerous it can not only remove the malicious program but also roll back all unwanted changes and results of its activity. This makes it possible, e.g., to recover data encrypted by Gpcode.

The effectiveness of proactive protection in Kaspersky Anti-Virus 6.0 for Windows Workstations **has been proven through independent tests:**

- **Security Watch: Blackworm Blows Up On Friday** (AV-Test org) <http://www.pcmag.com/article2/0,1895,1916880,00.asp>.
- **Kaspersky Proactive Defense Test** http://www.av-comparatives.org/seiten/ergebnisse/KAV6_PDM_test.PDF.
- **The high performance of Kaspersky Anti-Virus 6.0 for Windows Workstations** is achieved by:
 - Using **iSwift and iChecker proprietary technologies (for scanning of new and modified files only – this feature is NOT available in competitor solutions)** and **scanning of potentially hostile objects only** (a system that recognizes the types of the files being scanned). These technologies provide optimization and acceleration of antivirus scanning without compromising quality.
 - Using the **UNIQUE Network iSwift technology**, which eliminates the need to re-scan files received from a computer on the same local network with Kaspersky Anti-Virus 6.0 installed. This optimizes the use of resources on the local network and reduces file transfer delays.
 - **Configuring the balance between security level and scanning speed.** By configuring the security level, the user determines the relation between scanning speed and the number of files scanned: the smaller the number of files that are scanned for viruses the faster the scanning speed (a similar feature is **NOT available in competitor solutions**).
 - Defining the disk area controlled by the antivirus monitor (**narrowing down protection scope**), helping to optimize protection and significantly affecting the performance of the system as a whole. The user can specify the protection scope by listing only those objects that are to be protected. **None of the competitor solutions includes this feature.**
- **Kaspersky Anti-Virus 6.0 for Windows Workstations includes a number of features that make antivirus protection even more effective:**
 - **Installation of Kaspersky Anti-Virus 6.0 for Windows Workstations on an infected machine, made possible by technologies of self-defense and treatment of active infections (Advanced Disinfection technology).**
 - **On-the-fly scanning of HTTP traffic by Kaspersky Anti-Virus 6.0 for Windows Workstations** using SafeStream, a stream scanning technology. Kaspersky Anti-Virus 6.0 for Windows Workstations scans data transferred via HTTP before it is delivered to the user's computer. This technology is capable of detecting viruses that can launch without creating files on the user's local drive (such viruses can't be detected by ordinary file antivirus programs) and prevents network attacks by scanning traffic for their signatures **None of the competitor products includes this feature.**
 - **Kaspersky Anti-Virus 6.0 for Windows Workstations** includes **antivirus scanning of critical system areas (available only in the Symantec solution)** and **autostart objects**, i.e., the option to perform quick antivirus scans of important system areas that are most prone to infection (**NOT available in competitor products**).
 - **Kaspersky Anti-Virus 6.0 for Windows Workstations** includes on-the-fly antivirus scanning of emails delivered via the popular **IMAP4 protocol**. IMAP4 mail traffic is scanned irrespective of the email client used. **None of the competitor products includes this feature.**
 - **Kaspersky Anti-Virus 6.0 for Windows Workstations** treats files in **ZIP, ARJ, CAB, RAR and LHA archives. (Symantec treats files in ZIP and LHA archives; Trend Micro – in ZIP, RAR2 and LHA, and McAfee only in ZIP archives).**

- **The Anti-Hacker module (firewall) in Kaspersky Anti-Virus 6.0 for Windows Workstations is based on cutting-edge technologies for scanning network traffic and operates as a stateful inspection firewall.** Stateful inspection (unlike stateless firewalls) enables the firewall to dynamically track the state and type of network connections, ensuring high traffic filtering performance and positively affecting the performance of the application as a whole.

The Anti-Hacker module includes a large set of **predefined operating rules** (for more than 250 popular applications), helping to avoid unnecessary prompts from the program if the user is working with standard applications.

The intrusion detection and prevention system (IDS/IPS) that is part of the Anti-Hacker module detects activity typical of network attacks. In the event of an attempt to attack the computer, the system blocks any network activity from the attacking computer for one hour. The system also displays an alert about the network attack attempt with information about the attacking computer.

Protection from unauthorized connections from the outside is only one part of a firewall's purpose. Another, which is no less important, is to protect from unauthorized transmission of data from the inside. The Firewallleaktester.com team tests firewalls for "leaks" from the inside using leak tests, i.e., special programs that imitate the actions taken by Trojans to evade protection. These tests have demonstrated the effectiveness of the Anti-Hacker module in Kaspersky Anti-Virus 6.0 for Windows Workstations (http://www.firewallleaktester.com/reward_stats.htm).

The Firewallleaktester.com also tests firewalls for their ability to withstand attacks targeting the firewalls themselves (KILL Tests). Such attacks have an obvious purpose: to disable protection in order to perform malicious actions without hindrance. **In these tests, Kaspersky Lab's Anti-Hacker module also proved to be superior to Symantec and McAfee solutions** (http://www.firewallleaktester.com/termination_overview.php).

- **Kaspersky Anti-Virus 6.0 for Windows Workstations is THE ONLY** product in this survey **that includes an Anti-Spam module.** The module uses a combination of spam filtration methods, including:
 - **filtration by message header;**
 - **image analysis technology;**
 - **training of the antispam module on outgoing messages, on existing Microsoft Outlook / Microsoft Outlook Express databases** or during the course of processing emails (using a button in the mail client toolbar).

Training of the Anti-Spam module on spam and legitimate mail samples enables the module to recognize a particular user's unwanted and legitimate mail more accurately.

The Anti-Spam module includes the **Mail Dispatcher feature**, which enables the user to view the subject of all incoming messages and assess them without downloading them from the mail server in order to save time and traffic (**NO similar feature is available in competitor solutions analyzed in this paper**).

- **Of the solutions covered in this survey, ONLY Kaspersky Anti-Virus 6.0 for Windows Workstations includes protection against PHISHING ATTACKS,** including:
 - Protection from phishing attacks **at the mail client level (NO similar features in competitor solutions);**
 - Protection from phishing attacks **when opening websites in the browser. None of the competitor solutions includes this feature.**
- **Kaspersky Anti-Virus 6.0 for Windows Workstations uses a technology which significantly reduces the size of updates** by comparing the files of antivirus databases and program modules on the local computer and on the update server and downloading only those files that are not present on the local computer, saving time and traffic.

- **Kaspersky Administration Kit**, a free tool supplied with Kaspersky Anti-Virus 6.0 for Windows Workstations, provides **centralized administration of the antivirus system installed on complex computer networks with up to several tens of thousands of nodes, with support for remote offices and mobile users.** In addition to **being distributed free of charge**, it has a number of indisputable advantages over competitor products:
 - **The option to scan for new / unprotected computers on the network** based on the structure of the **enterprise's physical network, the Active Directory service or IP address ranges**, making it possible to automatically add new computers to the logical structure and remove inactive computers (**fully-functional scanning is implemented only in the McAfee product, while the Symantec and Trend Micro products perform scanning ONLY by IP subnetwork**).
 - **Kaspersky Administration Kit** supports **server and administration group hierarchy of any nesting level**, enabling it to manage the antivirus system on complex networks of any configuration, with protection management structure completely matching the topology of the customer's network. **Competitor administration systems do not support unlimited hierarchies of administrative servers.**
 - **Support for the use of IP multicast technology** to distribute updates significantly reduces peak traffic values on the corporate network (**NO similar features in competitor products**).
 - **A special policy for mobile clients**, which is activated on the client computer when it has no connection to the administrative server. The policy defined by the network administrator includes rules according to which the antivirus program will operate outside the office, including update sources and frequency, scanning schedule, enabled protection components, etc. (**a similar feature is available only in the Symantec product**).
 - Support for using **intermediate update distribution centers** (subordinate servers or workstations), to significantly reduce traffic (**this feature is NOT available in competitor products**).
 - **Support for Wake-on-LAN and Shut Down** to remotely turn on computers to perform scheduled tasks and shut them down after the tasks have been performed (**NO similar features in competitor solutions**).
 - The product supports **creating reports on schedule and sending created reports by email**, providing administrators with timely information on the status of protection on the network (**sending reports by email is available only in the Trend Micro product**).

5 Why NOT Symantec

- **Symantec Client Security 3.1 lags behind Kaspersky Anti-Virus 6.0 for Windows Workstations in scanning quality.** In a comparative test conducted by Andreas Clementi in August 2006 (http://www.av-comparatives.org/seiten/ergebnisse_2006_08.php). The difference in malicious program detection between Symantec and Kaspersky is about 1%, but in reality this small difference represents thousands of viruses. Furthermore, according to the results of testing conducted by Virus.gr (<http://www.virus.gr/english/fullxml/default.asp?id=82&mnu=82>), Symantec is as far back as 22nd place, while according to AV-test.org testing, the company's new threat response time is 10 to 12 hours (http://blog.washingtonpost.com/securityfix/2005/12/ranking_response_times_for_ant.html).

- **Symantec slows down the system.** According to the results of testing conducted by CNET Labs in October 2006, the time it takes to perform standard operations on a computer with running Symantec antivirus increases by 44 seconds, while Kaspersky Anti-Virus increases this time only by 12 seconds.
- In the Symantec product, proactive protection is limited to a heuristic analyzer and the Internet Worm Protection technology that detects some types of network worms based on their behavior. **There is no fully functional behavior blocker that tracks dangerous activity of all applications, application integrity control or registry control in Symantec Client Security.**
- Symantec Client Security **does not include detection of active modules that conceal malicious programs (i.e., rootkits).**
- Symantec Client Security **does not include protection from phishing attacks at the browser and mail client levels.**
- Symantec Client Security **does not provide on-the-fly scanning of HTTP traffic (regardless of the browser used),** making it possible for viruses that can launch without creating a file to penetrate the user's computer.
- Symantec Client Security **does not provide on-the-fly scanning of email traffic transferred via the IMAP4 protocol, regardless of the mail client used.**
- In Symantec Client Security, **it is impossible to define the area on the hard drive that will be monitored for threats (narrow down the scope of protection),** a feature that is capable of improving an antivirus program's performance.
- Symantec Client Security **does not provide a tool for setting a balance between security and performance or an option to scan only new and modified files.** This reduces the program's performance.
- Symantec Client Security **does not include a feature that excludes files received from computers with antivirus installed from scanning.** This feature could significantly reduce scanning time.
- Symantec Client Security **does not include an antispam module,** which is an essential component of integrated protection.
- Symantec System Center 10.1 (a centralized administration system) does not support an unlimited number of levels in the administration server hierarchy, which imposes limitations on protection systems on complex, ramified networks. **Symantec System Center does NOT include such features as:**
 - **Scanning for new / unprotected computers on the network** based on the structure of the **enterprise's physical network or the Active Directory service** and **automatic installation of antivirus applications on the computers found,** which helps keep the structure of enterprise network protection up to date.
 - **Support for the use of IP multicast technology** to distribute updates, which significantly reduces peak traffic values on the corporate network.
 - Support for the use of **intermediate update distribution centers** (subordinate servers or workstations) to significantly reduce traffic.
 - **Support for Wake-on-LAN and Shut Down** to remotely turn on computers to perform scheduled tasks and shut them down after the tasks have been performed.
 - **Support for sending reports created on schedule to the administrator's email address.**

6 Why NOT Trend Micro

- **Trend Micro OfficeScan 7.0 Client Server Edition (Trend Micro OfficeScan) lags far behind Kaspersky Anti-Virus 6.0 for Windows Workstations in scanning quality.** In a comparative test conducted by Andreas Clementi (http://www.av-comparatives.org/seiten/ergebnisse_2005_08.php), the difference in malicious program detection between Trend Micro and Kaspersky Lab's product is almost 9% and according to the results of testing conducted by Virus.gr (<http://www.virus.gr/english/fullxml/default.asp?id=82&mnu=82>), **Trend Micro shows the lowest results among all vendors analyzed.** Also, according to AV-test.org tests, the average new threat response time shown by Trend Micro is 6 to 8 hours (http://blog.washingtonpost.com/securityfix/2005/12/ranking_response_times_for_ant.html).
- **Trend Micro significantly slows down the system.** According to the results of testing conducted by CNET Labs in October 2006, the time it takes to perform standard operations on a computer with Trend Micro antivirus running increases by 74 seconds, while Kaspersky Anti-Virus increases this time only by 12 seconds.
- **Trend Micro uses a heuristic analyzer to protect from unknown threats. There is no fully functional behavior blocker that tracks dangerous activity of all applications, application integrity control or registry control in OfficeScan.**
- Trend Micro OfficeScan **does not include detection of active modules that conceal malicious programs (i.e., rootkits).**
- Trend Micro OfficeScan **does not include protection from phishing attacks at the browser and mail client levels.**
- Trend Micro OfficeScan **does not provide on-the-fly scanning of HTTP traffic (regardless of the browser used),** making it possible for viruses that can launch without creating a file to penetrate the user's computer.
- Trend Micro OfficeScan **does not provide on-the-fly scanning of email traffic transferred via the IMAP4 protocol, regardless of the mail client used.**
- In Trend Micro OfficeScan, **it is impossible to define the area on the hard drive that will be monitored for threats (narrow down the scope of protection),** a feature that is capable of improving an antivirus program's performance.
- Trend Micro OfficeScan **does not provide a tool for setting a balance between security and performance or an option to scan only new and modified files.** This reduces the program's performance.
- Trend Micro OfficeScan **does not include a feature that excludes files received from computers with antivirus installed from scanning.** This feature could significantly reduce scanning time.
- Trend Micro OfficeScan **does not include a mechanism that automatically suspends scanning when user activity (CPU load) is increased,** potentially leading to full system load.
- Trend Micro OfficeScan **does not include a feature that blocks banners and popup windows** when browsing the Internet, which could help to reduce traffic.
- Trend Micro OfficeScan **does not include an antispam module,** which is an essential component of integrated protection.

- **Trend Micro Control Manager 3.5 (a centralized administration system) does not support an unlimited number of levels in the administration server hierarchy, which imposes limitations on protection for systems on complex, ramified networks.** Also, the administration module does NOT include such features as:
 - **Scanning for new / unprotected computers on the network** based on the structure of the enterprise's physical network or the Active Directory service, which helps keep the structure of the enterprise network protection up to date.
 - **Support for the use of IP multicast technology** to distribute updates, which significantly reduces peak traffic values on the corporate network.
 - **A special policy for mobile clients**, which guarantees full-scale protection for mobile PCs outside the office.
 - Support for the use of **intermediate update distribution centers** (subordinate servers or workstations) to significantly reduce traffic.
 - **Support for Wake-on-LAN and Shut Down** to remotely turn on computers to perform scheduled tasks and shut them down after the tasks have been performed.

7 Why NOT McAfee

- **McAfee VirusScan Enterprise 8.5i (McAfee VSE) lags far behind Kaspersky Anti-Virus 6.0 for Windows Workstations in scanning quality.** In a comparative test conducted by Andreas Clementi in August 2006 (http://www.av-comparatives.org/seiten/ergebnisse_2006_08.php), the difference in malicious program detection between McAfee and Kaspersky Lab's product is almost 7%, and according to the results of testing conducted by Virus.gr (<http://www.virus.gr/english/fullxml/default.asp?id=82&mnu=82>), McAfee lies in the 14th position. Also, according to AV-test.org tests, the average new threat response time shown by McAfee is 8 to 10 hours (http://blog.washingtonpost.com/securityfix/2005/12/ranking_response_times_for_ant.html).
- **McAfee slows down the system.** According to the results of testing conducted by CNET Labs in October 2006, the time it takes to perform standard operations on a computer with McAfee antivirus running increases by 34 seconds, while Kaspersky Anti-Virus increases this time only by 12 seconds.
- To protect from unknown threats, McAfee uses a heuristic analyzer, a script behavior blocker and a technology for detection of some types of network worms based on their behavior. **Nevertheless, McAfee VirusScan Enterprise 8.5i does not include a fully functional behavior blocker that tracks dangerous activity of all applications or application integrity control.**
- McAfee VSE **does not include protection from phishing attacks at the browser and mail client levels.**
- McAfee VSE **does not provide on-the-fly scanning of HTTP traffic (regardless of the browser used)**, making it possible for viruses that can launch without creating a file to penetrate the user's computer.
- McAfee VSE **does not provide on-the-fly scanning of email traffic transferred via the IMAP4 protocol, regardless of the mail client used.**
- In McAfee VSE, **it is impossible to define the area on the hard drive that will be monitored for threats (narrow down the scope of protection)**, a feature that is capable of improving an antivirus program's performance.
- McAfee VSE **does not provide a tool for setting a balance between security and performance or an option to scan only new and modified files.** This reduces the program's performance.

- McAfee VSE **does not include a feature that excludes files received from computers with antivirus installed from scanning.** This feature could significantly reduce scanning time.
- McAfee VSE **does not include a feature that blocks banners and popup windows** when browsing the Internet, which could help to reduce traffic.
- McAfee VSE **does not include an antispyware module**, which is an essential component of integrated protection.
- **McAfee ePolicy Orchestrator 3.6.0 (a centralized administration system) does not support an unlimited number of levels in the administration server hierarchy**, which imposes limitations on protection for systems on complex, ramified networks. Also, the **administration module (McAfee ePolicy Orchestrator) does NOT include such features** as:
 - **Scanning for new / unprotected computers on the network** based on the structure of the **enterprise's physical network or the Active Directory service** and **automatic installation of antivirus applications on the computers found**, which helps keep the structure of enterprise network protection up to date.
 - **Support for the use of IP multicast technology** to distribute updates, which significantly reduces peak traffic values on the corporate network.
 - **A special policy for mobile clients**, which guarantees full-scale protection for mobile PCs outside the office.
 - Support for the use of **intermediate update distribution centers** (subordinate servers or workstations) to significantly reduce traffic.
 - **Support for Wake-on-LAN and Shut Down** to remotely turn on computers to perform scheduled tasks and shut them down after the tasks have been performed.
 - **Support for sending reports created on schedule to the administrator's email address.**