
Panda
Internet Security
MEGA DETECTION
2008
PANDA
G DATA
InternetSecurity
2008
Internet Security
3 PCs
1 JAHRES-
bitdefender
INTERNET SECURITY
2008
Kaspersky
Anti-Virus
Version 7.0
PROTECTSTAR™
AWARD
2008
Norton
Internet Security
2008
ESET
Smart
Security
McAfee
Internet Security Suite
OUTPOSTPRO
SECURITY SUITE
2008
AntiVir
Internet Security
BULLGUARD
INTERNET SECURITY
OneCare

ProtectStar™ Comparison Test
2008 Internet Security Suites

TABLE OF CONTENTS:

A.) Tested Products and Versions

Manufacturer	Product Name	Setup file size	Release (version)
Agnitum	OutpostPro Security Suite 2008	30,4 MB	6.0.2225.232.0465
Avira	Premium Security Suite 2008	18,8 MB	7.06.00.168
BitDefender	Internet Security 2008	41,8 MB	n/a
BullGuard	BullGuard 8.0	30,4 MB	n/a
ESET	Smart Security 3.0	18.0 MB	3.0.621
F-Secure	Internet Security 2008	81,9 MB	n/a
G DATA	Internet Security 2008	201,8 MB	18.0.7295.201
Kaspersky	Internet Security 7.0	28,9 MB	7.0.1.321
McAfee	Internet Security 2008	38,7 MB	n/a
Microsoft	Live OneCare 2.0	n/a	2.0.2500.14
Panda	Internet Security 2008	50,0 MB	12.00.00
Symantec	Norton Internet Security 2008	61,5 MB	n/a
Trend Micro	Internet Security 2008	88,3 MB	16.00.1645

n/a = no details available as not shown in program itself

B.) Background Information

The ProtectStar™ TestLab (www.protectstar-testlab.org) is regularly asked about secure and modern security solutions for IT and communication systems of all kinds, and increasingly the questions are coming from individuals with responsibility for IT matters within their organisations who find the test results published in specialist forums and magazines both irritating and confusing.

For instance, it can be mystifying for a user to see one magazine pick “Security Suite A” as its no. 1 (out of ten or more contenders) while another specialist journal only rates the product as “average”, putting it in seventh or eighth spot. The ways in which firewalls are tested for user-friendliness, performance and security can also be very vague or simply not dealt with at all.
Users generally seem to be more satisfied with how virus detection rates are arrived at. However, complaints about a certain imprecision or generalisation in this area are also still quite common as many comparison tests only focus on how well the products detect malware.

Given the clamour for clear and meaningful test results, ProtectStar™ felt compelled to carry out a comparison test on the Internet security suites that are currently available. In doing so, the main focus of the test series lay on the security settings of the products as supplied to the customer (default settings following installation). We also asked:

how good is the security provided by the suite following installation and without any configuration changes?

are the program alerts and user information coherent?

is system performance impacted?

Thirteen of the **Internet security suites** currently available on the IT security market were tested. The ProtectStar™ TestLab is planning to compare all of the suites available worldwide with one another in the future. Therefore, suites which were not available for this test, such as those from avast!, AVG, Norman, Sophos, Trustport, ZoneAlarm, and many more, will be taken into consideration in the next comparison test.

C.) General Explanation of the Test Procedures

Testing was carried out under **laboratory and real conditions.** In the area of **SECURITY**, the focus lay on the external and internal protection provided by the integrated personal firewall. The main spotlight was placed on the factory settings, i.e. the security suites in the state in which they are delivered to customers. **“External protection”** means that a security check was carried out with a PC or laptop directly connected to the Internet, e.g. by directly connecting the PC/laptop to a DSL modem (not via a router, hardware firewall or the like). **“Internal protection”** means that security tests were carried out on the personal firewall while the computer was within a LAN. A LAN (such as a home or corporate network) is considered a trusted zone and many personal firewalls only monitor it with low security settings as a result. In this area, analysis was carried out on what could happen if a LAN computer had already been infected or a guest computer acted as a hacker. Comprehensive analysis of the virus and malware detection rates of the engines in the Internet security suites that were tested was carried out in cooperation with AV-Comparatives (www.av-comparatives.org).

The term “malware” as used here incorporates viruses, worms, trojans, etc. In the area of **USER-FRIENDLINESS**, we looked at the installation and removal of the suite, the coherence of the information and the individual setting and

configuration options, both during and after the installation. Attention was also given to the manual (sometimes included in delivery in a printed form) and its coherence, the online help available and FAQs. Scrutiny of the availability of a boot CD (rescue CD/DVD) and the possibility to create a rescue CD rounded off this area. In the **PERFORMANCE** segment, a wide range of computer systems were available for the thirteen Internet security suites.

Features of the test computers (from – to):

Operating system:
Windows XP with Service Pack 2 and/or Windows Vista

CPU:
566MHz [single-core] – 2400 MHz [quad-core] (average: 1.8GHz dual-core)

RAM:
256–4096 MB SDRAM and DDR-RAM (average: 1024 MB DDR-RAM)

Hard drive:
10–1000 GB, IDE and S-ATA (average: 120 GB S-ATA hard drive)

Outside of the range, we evaluated whether the products could also be used as required by users if only the minimum system requirements specified by the manufacturers were available.

PRICE/EQUIPMENT RATIO: What is the relationship between the price of a security suite and what it contains? In other words, what additional software modules (such as backup, tuning, etc.) are delivered to the user and how many licences are included? The price difference between the boxed and download versions when purchasing the suite from the manufacturer and the so-called "street" price on Amazon, the online mail-order company, was also evaluated.

D.) Evaluation Criteria

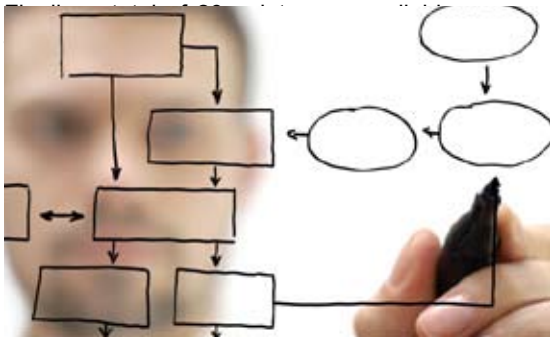
All of the 13 Internet security suites tested are exclusively security solutions which promise and should, above all, guarantee the user excellent protection from modern risks such as hackers, viruses, rootkits, keyloggers, phishing and pharming attacks, and much more. As these are **security products,** the main focus necessarily had to lie on the security functions contained within the respective security suites.
Besides security, both **user-friendliness** and **performance** are particularly essential in practice. For this reason, both areas received equal weighting in the evaluation.

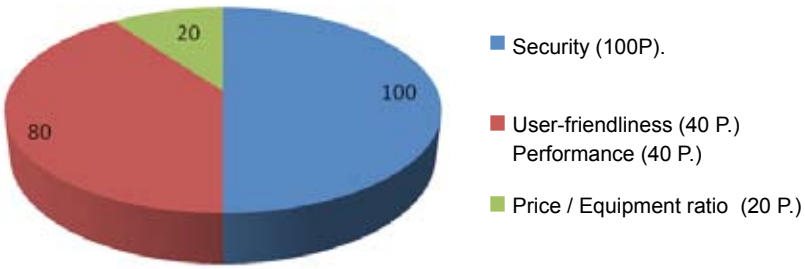
Less essential for the security of a product, but still worth mentioning, is the **price/equipment ratio.** A modern Internet security suite should – in a comparison with products from competitors – guarantee maximum security regardless of how high or low the purchase price is. In this respect, the user should not initially be significantly influenced by additional features such as tuning or backup programs or extra licences thrown in with the purchase. On the other hand, there are particular savings to be made by the user if he doesn't have to purchase a separate backup program because a storage solution of equal value is already included in the Internet security suite he has purchased. The same applies to system optimisation and parental control programs.

For the reasons mentioned above, 10% of the overall evaluation was based on the rice/equipment ratio.
Therefore, the ProtectStar™ TestLab decided to use the following **200-point** system as the basis for the evaluation:

Of the **200** points available in total, the biggest portion (**100** points) was allocated to **security**. These 100 points were divided such that max. 30 points could be allocated for the firewall's external protection, 20 points for its internal protection, 45 points for malware detection [in the case of malware detection, 1 point was subtracted for every 1% lacking in the detection rate] and a further 5 points for miscellaneous security functions such as the quality of the alerts, log files, intrusion prevention systems, host protection, multiple anti-virus scanners, etc. [30 + 20 + 45 + 5 = 100 points].

80 points in total were available for **user-friendliness** and **performance**. Each of these areas could receive a maximum of **40 points.**





E.) Test: SECURITY

1.) THE FIREWALL–external protection

Every security suite evaluated by the ProtectStar™ TestLab contained an integrated personal firewall monitoring **incoming and outgoing** connections. The personal firewalls were analysed in their default settings, i.e. as they are configured when delivered to the customer. As already mentioned in the "General Explanation of the Test Procedures" section, two aspects of the personal firewalls were analysed: the **external protection** (attacker -> Internet -> test computer) of the firewall and the **internal protection** (attacker -> LAN -> test computer).

During the run-throughs to check the external protection, the firewalls integrated into the security suites successfully passed all of the **14,037** different **attack and security tests** known when the test was carried out (as of February 2008). The kinds of **denial of service** (DOS) attacks we are currently aware of were tested along with **vulnerabilities** in the operating systems, applications, brute force, CGI abuses, useless services, backdoors and security checks.

Various risk levels (low, medium, high) were applied with respect to **DOS attacks**, e.g. in the case of the "Microsoft SMS Client", the "ping of death", "RPC DCOM Interface DoS", "MS RPC Services null pointer reference DoS", "WinLogon.exe DoS", and many more.

The **Microsoft bulletins** and **Windows attacks** included, amongst others, "Buffer Overrun in Messenger Service (828035)", "Buffer Overflow in Windows Troubleshooter ActiveX Control (826232)", "Windows Network Manager Privilege Elevation (Q326886)", "Checks for MS HOTFIX for snmp buffer overruns", "WINS Code Execution (870763)", "Vulnerability in NetDDE Could Allow Code Execution", "MS Task Scheduler vulnerability", and much more. Standardised port scans looked for open TCP and UDP ports in the **default setting.** The scan range covered all ports (0 – 65535). In a **second step**, the firewalls were subjected to a SYN port scan (half-open), known as a stealth scan. Furthermore, the personal firewalls were exposed to 33 **specific attack variations** for **firewalls**. All of the personal firewalls **successfully** fended off these attacks.

The port scans which were carried out (tcp-connect and syn/half-open) did **not** detect any open ports or unnecessary services that usually pose security issues. Neither the **automatic** test routines of the proprietary hardware-based **ProtectStar™ security** scanner, which conducted an additional **10257** (as of February 2008) security tests and attack tactics on the firewalls, nor the **manually** executed inspections were able to find any vulnerabilities or security risks. The firewalls also **successfully** passed the endurance **penetration test**, which was conducted over a number of hours, without any appreciable performance loss.

None of the security suites showed any deficiencies or security risks with respect to **external protection**. However, the alerts, log files and pop-ups shown to the user when their computer is under attack could be improved upon in some products or the attacks could be sorted according to their priority. For example, if a port scan doesn't represent an attack in the truest sense of the meaning, then the user should only be informed of a port scan if it originates from the trusted zone.

With regard to alerts and alarms, the security suites from **Agnitum**, **BullGuard** and **Symantec** were **exemplary**, even in their default settings. The firewalls integrated into the security suites of **Agnitum** and **BullGuard** are particularly commendable with respect to their configuration options. In the case of both products, and particularly in the case of **BullGuard**, even the **minutiae** of the settings can be changed. However, the user should have sufficient experience and knowledge of IT security before manually modifying or redefining the rules.

It would be desirable, however, if the security suites could detect and alert the user of **more attack techniques** in the future. The majority of the security suites analysed simply limited their alerts in this area to reporting detected port scans. Specific brute force and denial of service attacks were blocked, however the user wasn't alerted to the type of attack, even when it persisted for an hour.

THE FIREWALL – internal protection

The preceding test showed that all of the personal firewalls integrated into the security suites provide **sufficient protection** against attacks from the Internet. However, how do they cope when one or more computer systems are attacked directly from the "trusted zone", the LAN? Increasingly, households have more and more networked computers, whether for children to play games on or as part of a home office for the parents. Also, computer-based building service controls are becoming increasingly popular. Security solutions are often turned off in children's rooms because they can impact on the performance of online games. During this time, the computers are at the mercy of almost all kinds of hacker attacks, worms, viruses and trojans and might then „infect" other computers in the household.

Also, it can often arise, both in a home office or a business, that a visitor wishes to connect their computer to your network, perhaps a friend or acquaintance who

would like to quickly check their e-mails. What happens if this guest computer has already been infected with a worm or trojan? Are the other "protected" computers in the LAN going to be impacted by this?

Therefore, the security experts in the ProtectStar™ TestLab carried out various **attack and security tests** to analyse the protection offered by the personal firewalls within the LAN in their default settings. The currently known kinds of **denial of service** (DOS) attacks were tested along with **vulnerabilities** in the operating systems, applications, brute force, CGI abuses, useless services, backdoors and other security checks.

Some products showed **various weaknesses** in this area, completely at odds with their otherwise good external protection. In order to give due consideration to increasing demands for greater user-friendliness, some manufacturers set up their firewalls for the LAN or trusted zone as standard. As a result, computers are able to exchange files between the networked computers, use common printers and access released folders and files without the user having to make any manual configuration changes.

For this reason, the tcp ports **135** (msrpc), **139** (netbios-ssn) and **445** (microsoft-ds) are **insufficiently protected** by the firewalls integrated into the security suites of various manufacturers. This could be seen in the solutions from G DATA, Kaspersky, McAfee and Trend Micro.

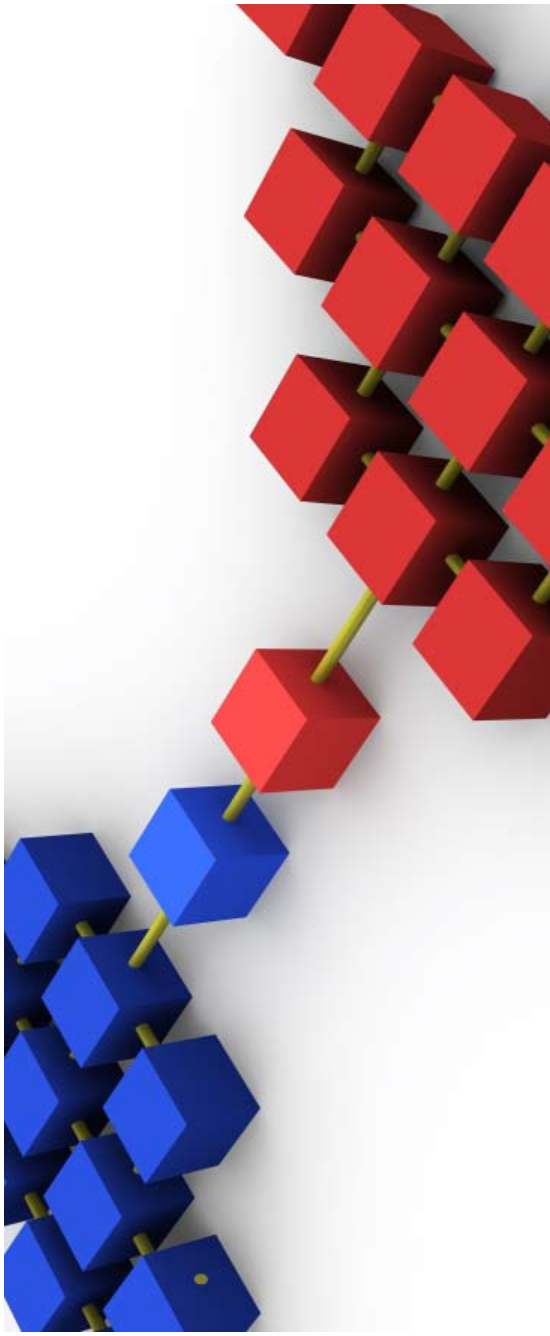
The solutions from BitDefender, ESET, Microsoft and Symantec were an exception - after installing "**BitDefender Internet Security 2008**", "**Eset Smart Security Suite 3.0**", "**Microsoft Live OneCare 2.0**" or "**Norton Internet Security 2008**", the user can select whether or not the PC should communicate with other computers in the LAN. Accordingly, the tcp ports mentioned are either protected by the firewall or left open. The security suites from **BitDefender, ESET, Microsoft and Symantec** were **exemplary** in this regard. Other manufacturers should also consider this possibility as it saves inexperienced users having to implement manual port blocking as an extra step. However, it's worth mentioning that "port forwarding in a LAN" is not a security risk in the conventional sense. Only experienced Internet security specialists could get different information as a result of the open ports which could serve as the basis for further attacks.

For example, hazards such as a T**CP sequence prediction** attack and **IP ID FIELD prediction vulnerabilities** can result from this. This means that the TCP/IP stack is not fully protected. In a serious case, this can result in the attacker predicting or guessing the sequence number, thereby being in a position to manipulate existing connections.

In addition to this, information such as the domain name, MAC address, computer name, etc. can be discovered, and could make it possible for the attacker to carry out further specific attacks, provided, of course, that the attacker is within the trusted zone (LAN) and has the necessary know-how. We informed the manufacturer **G DATA**, for example, of this finding.

We were told that the G DATA firewall is "*meant to act that way*". An engineer from G DATA also told us that if "*a user uses a data transmission connection (i.e. without a router), the 'direct connection to the Internet' rule is automatically selected. In such an instance, no open port can be seen from outside. In a corporate network, you can work intelligently with this rule, as network drives connected via a login script, for example, will not function. In the "networks" area, you can set up the corresponding rule for each network if you are not satisfied with the default setting.*"

The security experts from the **ProtectStar™ TestLab** were able to confirm that the answer from **G DATA** was correct and apply this to the solutions from Kaspersky, McAfee and Trend Micro which also exhibited this property. However, when external ProtectStar™ testers with varying degrees of experience were included, it was clear that the "firewall security (scroll) bars" in the security suites can lead to misunderstandings in some cases. For example, it is wrong to assume that open ports for trusted networks are closed by increasing the security level. In the case of the suites from **G DATA, Kaspersky, McAfee and Trend**



Micro, these ports were still open in the LAN when the security level was increased to “maximum/highest security“.

The hazards mentioned above - **TCP sequence predictions and IP ID FIELD prediction vulnerabilities** – are **not** exhibited when the default settings of the products from Agnitum, Avira, BitDefender, Eset, F-Secure, Microsoft, Panda Security and Symantec are used.

The solutions from Agnitum, BullGuard, BitDefender, Kaspersky, Symantec and Trend Micro all have an **advantage** in the area of the „internal protection provided by the firewall” due to good alerts and log files. The suites from **BullGuard** and **Trend Micro** have a further **plus factor** due to their very detailed alerts and user-friendly user interaction messages.

Criticism can be levelled at some security suites that do inform the user (via pop-ups) of an attack from the Internet against his computer but not about attacks originating from the LAN, i.e. Eset, G DATA, McAfee, Microsoft and Trend Micro.

In the case of these products, an entry was only made to the log file and this only if the security level of the firewall was set to “maximum/highest security”. The table below gives an overview of the risks (relating to external and internal protection) found with the security suites:

Direct attacks via the Internet
(sorted according to risk level + number of risks found)

Direct attacks via the LAN
(sorted according to risk level + number of risks found)

Manufacturer	High / Medium / Low	High	Medium	Low	Other
Agnitum	0	0	0	0	A*, G*
Avira	0	0	0	1	B*
BitDefender	0	0	0 / 0	0 / 0	E*
BullGuard	0	0	0	0	A*, G*
ESET	0	0	0 / 3	0 / 9	C*
F-Secure	0	0	0	0	-
G DATA	0	0	3	7	D*
Kaspersky	0	0	3	9	-
McAfee	0	0	3	9	-
Microsoft	0	0	0 / 3	0 / 7	E*
Panda	0	0	0	0	-
Symantec	0	0	0	0	-
Trend Micro	0	0	3	7	F*, G*

Status as of:
February 2008

Number of attacks (Internet):
14.037 + 10.257 = ***24.294***

Number of attacks (LAN):
10.257

Product analysed in:
default settings

Legend:

A*	Firewall was able to withstand the attacks
B*	1x “Low Level” security risk as “Remote system answers to PING command”
C*	Shows the difference between the “Strict Control” and “Allow Sharing” options which can be selected following installation.
D*	After setting the security scroll bar of the firewall to various different security levels, no difference at all between the default setting and “highest security”.
E*	Shows the difference between the “Public Area” and “Home or Work Zone” options which can be selected following installation.
F*	After setting the security scroll bar of the firewall to various different security levels, no difference at all between the default setting and “highest security”/”maximum” in response to attacks from the LAN.
G*	Helpful log files and warning pop-ups during the attack

3.) MALWARE DETECTION

In cooperation with the independent and renowned test centre AV-Comparatives (www.av-comparatives.org), the malware detection rates of the malware scanners integrated into the thirteen security suites were analysed.

In order to be able to arrive at a precise detection rate, all of the security suites were analysed on one day and then "frozen" so that it was no longer possible for the products to be automatically updated. In addition to this, the products were optimally configured so that as many pests as possible could be detected.

It is important to mention at this stage that only the signature-based and heuristic protection (on-demand/on-access) of the malware scanners was tested. Some products offer further security mechanisms which, for example, detect a virus from its behaviour (proactive security) if the action has already been performed by the user. Proactive security techniques were not analysed!

The malware test set consisted of **1,683,364** samples in total which were tested by every integrated malware scanner. In detailed terms, the test set consisted of Windows viruses (**149,202**), macro viruses (**95,059**), script viruses (**14,284**), worms (**190,952**), backdoors/bots (**400,986**), trojans (**817,043**) and other pests (**15,838**). Please note that Agnitum is based on the malware engine from VirusBuster and BullGuard on the engine from BitDefender. Below are the detailed results:

Pos	Manufacturer	detected samples/ detection in %
1.	Avira	1.676.963 99,6%
2.	G Data	1.675.358 99,5%
3.	Kaspersky	1.653.991 98,3%
4.	Trend Micro	1.649.191 98,0%
5.	Symantec	1.644.006 97,7%
6.	Eset	1.643.957 97,7%
7.	F-Secure	1.641.228 97,5%
8.	BitDefender & BullGuard	1.624.123 96,5%
9.	McAfee	1.598.078 94,9%
10.	Microsoft	1.580.981 93,9%
11.	Panda Security	1.439.175 85,5%
12.	Agnitum	1.273.142 75,6%

4.) SECURITY RECOMMENDATIONS FROM PROTECTSTAR™

In addition to the tests, the ProtectStar™ TestLab would like to make some general recommendations in relation to the security of the security suites tested.

Every solution should be **password protected** by the user in order to increase the security of the suite. All of the products tested have such a feature, but it is deactivated in the default settings. The password function should be activated by the user and a password consisting of at least eight characters (made up of letters, numbers and special symbols) should be entered (see http://www.protectstar-research.com/de.informationen-passworter.html).

This will prevent the entire suite or individual products within it, such as anti-virus scanners, personal firewalls, etc., from being deactivated or even removed. The default settings of some of the personal firewalls integrated into the security suites have largely been set up well for the needs of the end user. However, if the user manually changes the personal firewall to the so-called "**learning mode**" or **"training mode**" (e.g. in the case of Agnitum or Kaspersky), he should take sufficient time to study the multitude of alerts about programs and services trying to connect to the Internet which appear immediately after the computer has been rebooted for the first time following installation.

Oftentimes, "block connection" can be quickly clicked here and this can then lead to further problems if the automatic update service from Windows is blocked, for example.

If the user is running a **(home) network** and doesn't wish to share any released folders, files, printers, etc. with other computers in the network, he should accordingly block the netbios services (e.g. ports 139, 443, etc.). This has to be done **manually** in the case of the G DATA, Kaspersky and McAfee suites. "My computer is in a public network" or similar should be selected **after installing** the suites from Agnitum, BitDefender, BullGuard, Eset, Microsoft and Symantec. The **Agnitum** and **BullGuard** security suites **do not** automatically deactivate the Windows firewall. The **BullGuard** program does inform the user in detail after the installation that the Windows firewall should be deactivated by the user. Nevertheless, many testers quickly forgot this. Dual operation of both firewalls is not advised.

The user should be aware that operating a personal firewall uses up extra CPU power and that the data transmission speed can also be reduced if larger or large quantities of data are being monitored. This phenomenon presents itself with online computer games, for example. For this reason, some gamers often turn off their security software when playing online games.

The products from **AVIRA, BitDefender and G DATA** come with a "**gaming mode**" which is supposed to prevent the problems mentioned to a large degree through specific configuration settings on the firewall and malware scanner.

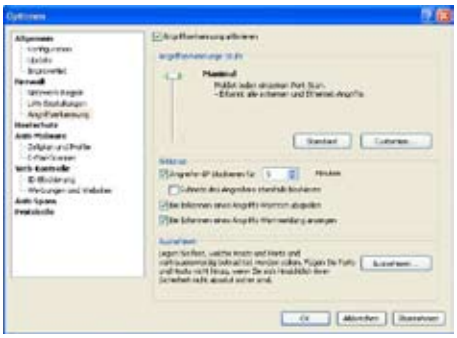
F.) Test: USER-FRIENDLINESS

Bezüglich der Benutzerfreundlichkeit, sind dem ProtectStar™ TestLab folgende Eigenschaften aufgefallen:

In relation to user-friendliness, the following properties attracted the attention of the ProtectStar™ TestLab:

Agnitum OutpostPRO Security Suite 2008 offers experienced users strong setting and configuration options in relation to the firewall, reports, host protection and intrusion detection. Pop-up intrusion detection is very well implemented and informs the users of possible breaches of security.

The main menu is simple and clearly laid-out so that the user can quickly access all settings.
Advanced users will enjoy the setup



options; however, less technically-versed users may quickly become frustrated with the flood of alerts if they change the suite's default settings.

AVIRA Premium Security Suite 2008 offers users detailed and good log files in relation to detected malware. By using the "expert mode", the suite can be comprehensively adapted and configured in accordance with the user's individual requirements. The ways in which the integrated firewall can be configured are sufficient for most users, however they are not as extensive as with BullGuard and Agnitum, for example.
The user interface is clearly laid-out but, in contrast to the other solutions, it doesn't really look modern. The update is set to 24 hours and should be changed by the user following installation to 1-3 hour(s).

A bootable CD is not available and cannot be created either. However, this should be

available in Version 8.0, to be released in the 2nd quarter of 2008.

BitDefender Internet Security 2008 gives the user the impression of a modern solution with a personal firewall, malware scanner, parental control, anti-spam and a licence for the mobile anti-virus scanner. However, the main menu in the new 2008 version takes some getting used to - BitDefender has remodelled the interface by using four buttons which are supposed to make the security suite simpler to use.

The user does indeed get a quick overview of the current security status, but the testers bemoaned the lack of a conventional interface with setup options. This could only be found after a small bit of searching by the user. The user should

receive detailed alerts on attacks from the Internet and/or the trusted zone (LAN) in its default state without having to make manual changes to the setup first.

BullGuard 8.0 is as yet unknown in some countries. Nevertheless, the suite can hold its own with the better known solutions. In relation to user-friendliness, the testers felt that the configuration options were quick and easy to use due to the clearly laid-out main menu, but actions such as "malware scan of the workstation" have to be started in a separate menu/tab. This will initially seem unusual to users who have been using solutions from other manufacturers in the past. The alerts about attacks from the Internet and/or LAN are exemplary and very detailed.

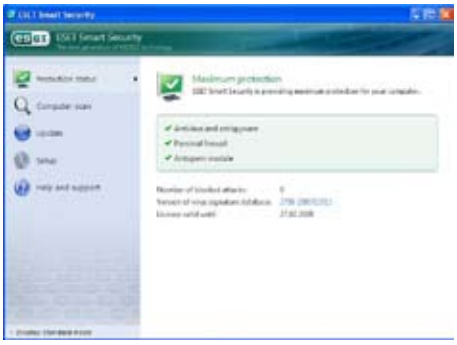
There isn't a http scanner to filter undesirable or dangerous content from websites. Neither is there a bootable emergency CD and nor can one be created by the user. User-defined installation is not possible.An excellent live support chat feature helps users with questions or problems.

ESET Smart Security 3.0 has a superb suite on offer for both experienced users and those who are less technically proficient as the user interface can be changed with „toggle advanced mode" according to the user type.

However, a vast number of configuration options are hidden at first glance and can only be found under „Setup" after a short familiarisation period.

Apart from the clearly laid-out user interface, the report files are also excellent. Worth mentioning with regard to the default settings is that the user is only informed of incidents if they represent a risk. A reboot is not needed after installation.

However, the suite is limited to the basic security modules such as anti-malware scanner (anti-virus, anti-rootkit, personal firewall and anti-spam). For example, users will search in vain to find parental control.



The http scanner is already activated in the default settings, but a bootable emergency CD is not available and cannot be created either.

F-Secure Internet Security 2008

Unlike the previous 2007 version, the current 2008 version from the Finnish manufacturer F-Secure has been improved by modern technology with regard to the detection of adware and spyware. The suite also includes parental control which can be optionally installed during the installation. The user interface is user-friendly and not only clearly displays the security status but also security information (information from F-Secure about new security features, viruses in circulation, and much more) to the users.

In general, it's clear that the menu is easier to understand than those in the security suites from BitDefender, BullGuard, Eset and Symantec. By clicking on "advanced" in the main menu, a multitude of individual settings can also be accessed. However, we noticed that the user is not reminded after the installation to run a full malware scan, unlike all of the other suites we tested. We would recommend that users do so.

The alerts and logs are understandable and sufficient for most users. However, the http scanner is deactivated and must be manually activated. A bootable emergency CD is included, however it doesn't provide any support for NTFS partitions and cannot be updated with new signature data either.

G DATA Internet Security 2008

The current Internet security suite from G DATA has a number of improved features over its previous version – however, not a new user interface or new functions.
The manual not only gives a very detailed explanation of the product but also provides general tips on computer security. It is included with the retail packaging in printed form but is also available as a PDF

file on the enclosed CD-ROM. The user can decide on the scope of the installation. All of the individual options are sufficiently described and make the decision-making process simpler.

All of the program's alerts and logs are detailed and clear. Every signature update, virus detected and search run is logged. These logs themselves can be looked at in an „extended" form (so that they indicate non-scanned files). The user interface is clearly structured. The user can click on the tabs to see the individual elements of the suite and double-click on a term to start the chosen option. Overall, the user-friendliness of the solution is pleasing as the individual security modules are clearly delimited from one another and the program is very clear as a whole.

Kaspersky Internet Security 7.0 offers a user-defined installation. An emergency boot CD can also be created from the program. However, the extra BartPe program (available as a free download) is needed and would be somewhat complicated for an inexperienced user to deal with.
The Kaspersky security suite also has a modern user interface, comprehensive reporting and a good task planner.
Spam and suspicious e-mails can be directly deleted on the server. The remaining term of the licence is clearly indicated in the program window. It is possible to upgrade to newer versions during the term of the licence.

McAfee Internet Security 2008

The installation of the McAfee security suite was simple and very user-friendly. A reboot is not needed after installation. The interface is clearly laid-out and will particularly appeal to home users who do not want to deal with technical settings or technical IT security jargon. However, the user interface seems somewhat antiquated. It has barely been updated since the last McAfee versions. If the integrated firewall

is attacked, there aren't any warning pop-ups or information.

Microsoft Live OneCare 2.0

The Live OneCare 2.0 security suite from Microsoft presents itself as a complete package for your computer's security and systems maintenance.

The installation of the solution took longer than average as the user must download information from the Internet despite the installation CD. The main menu looks unfamiliar at first glance and unclearly arranged with lots of text and labelling. Nevertheless, the interface is tidy and all information, such as the "virus and spyware monitoring", "last virus and spyware scan" and much more, are clearly visible to the users.

Coloured accentuations also help show the user which action is necessary on his part (e.g. signature update or data backup configuration). The solution also provides convenient access to Windows functions and system optimisations.

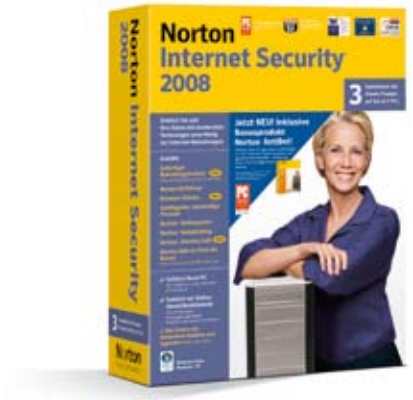
Norton Internet Security 2008

Compared with other solutions, this installation took longer than average. There was no way to influence the installation according to the user's wishes, to deselect individual modules or change the installation path.

A reboot of the Windows operating system is not requested by the Symantec suite and it is (almost) ready to use - except Symantec insists on a customer account being set up. Otherwise, the installation cannot be completed. Once the installation has finished, three modules are available - Norton Auto-Protect (the real-time scanner), Norton Security Center (it provides an overview of the status of the suite but Window's own security centre can also be integrated) and the actual program interface, called „Internet Security 2008".

It is clear that the firewall has been automated to the greatest degree possible and that it can detect and configure independently used applications and online games.

However, in terms of user-friendliness, the relatively few configuration options must be mentioned. Only the heuristic technology ("Bloodhound") can be switched on. It should be mentioned that Symantec has made a new security module called "Norton AntiBot" available as a free download for its "Norton Internet Security 2008" product (as well as Norton AntiVirus 2008 and Norton 360). Norton AntiBot does not need signature updates (process observer) and reliably detects malicious code from its behaviour.



Panda Internet Security 2008

Installing this comprehensive software was a smooth and user-friendly process. While installing the suite, a malware scanner checks for possible malicious software. In most cases, this scanner found spyware present on the test computers during the installation stage.

Little or nothing has changed about the menu interface since the last version. There isn't any manual available for users, just online help.

Unlike previous versions of Panda Security, the current version comes equipped with a backup tool and a new feature - the Totalscan Pro online scanner. It carries out an additional check on the computer for anything malicious and passes on

information about infected files for analysis to the manufacturer. As a result, the manufacturer promises all users of the software that it will be able to provide a quick(er) signature update.

Trend Micro Internet Security 2008
The security suite from Trend Micro gives the user one of the most clearly laid-out and tidy user interfaces in comparison with the other twelve competitors tested. All settings and menu navigations are immediately recognisable at a glance. The optimal use of colours and symbols make child's play of navigating the menu for both beginners and advanced Internet users.

The options which allow users to determine how the program should behave at a particular point in time and when and how a scan or update will take place are also user-friendly. A self-diagnosis may even be needed to sustain the security level. Options regarding whether the user should be warned with pop-ups and/or acoustic signals when incidents are detected, and much more, can be set.

G.) TEST: PERFORMANCE

As already mentioned in the "General Explanation of the Test Procedures" section, the performance – along with the capabilities and speed of the product – is very crucial.

Modern security suites, such as the 13 products tested by the ProtectStar™ TestLab, contain a multitude of individual security modules which are combined to create a so-called **Internet security suite.** An **anti-malware scanner, personal firewall and anti-spam filter** are usually always included in these security modules. All of the security suites contain these in one or other form as a minimum. ESET Smart Security 3.0 has limited itself exclusively to these **three basic security modules**. Norton Internet Security 2008 from Symantec only has the anti-spam filter available as a free add-on pack with integrated parental control. All of the other security suites analysed, such as those from BitDefender, BullGuard, GDATA, Kaspersky, McAfee, Microsoft, Panda Security and Trend Micro, include further security modules and programs in the delivery which go far beyond the three basic security modules in some cases.

In previous years, extra security components have increasingly been integrated into the security suites, such as intrusion prevention, personal wireless network monitor, Internet and e-mail control, search for security vulnerabilities, anti-phishing, anti-pharming, worm protection and much more. Increasingly we are also finding extra tools such as a PC clean assistant, data backup, data shredder, system optimisation and parental control.

All of the security modules and tools mentioned in the security suites offer the user a **higher degree of security and user-friendliness**, but can have a **strong impact on** the CPU in some cases due to the multitude of security components.

This manifests itself through delays in bringing up Internet pages. There are delays when starting programs and with the system start. Depending on the security solution and configuration, the delays may be a full 75% longer or more than without the security suite.

However, a generalisation such as "the more products contained in a suite, the more it will slow down the computer" can**not** always be made. Rather, the delays are caused by the different settings for the „guardians" in the background, such as anti-malware scanners, personal firewalls, etc. and their consumption of memory resources. **Norton Internet Security 2008**, for example, places unusual performance restrictions on computer systems with only 256 to 512 MB main memory under Windows XP/Windows Vista. Therefore, working on such systems with this suite only makes sense in exceptions.

The computer systems on which **F-Secure Internet Security 2008** was installed initially slowed significantly following the first reboot of the computer; regardless of whether an older computer system or more modern ones with Intel QuadCore processors and 4 GB main memory were used. The reason for this is that the suite updates itself via the Internet following installation while simultaneously actively scanning programs and services. The user is only informed of this via an icon next to the system clock when operating under Windows. Users are advised to leave the computer to work quietly after installing the suite from F-Secure for about two to four minutes so that the software can successfully update itself and the installation can be completed.

G DATA Internet Security 2008 represents a special case in performance matters. Due to the two integrated anti-malware scanners, the system experiences a delay when the computer is started and when files and programs are opened. Therefore, users should have a powerful computer if they are to avoid having to put up with long delays. Operating the suite with older computer systems with less than 512 MB main memory is simply not recommended.

However, the performance can be improved through various settings. The guardians in particular can be precisely adjusted to your wishes. Both engines are active (performance optimised) in the default settings and can be individually adjusted to the needs of the user, whereby an increase in performance can be achieved though at the expense of some security.

The security suites from **AVIRA, BitDefender, ESET, McAfee, Microsoft and Trend Micro made a positive impression** without exception with regard to performance.

The **Outpost PRO Security Suite 2008** from Agnitum and **Norton Internet Security 2008** from Symantec, for example, showed averagely good performance properties in the default settings. However, these are sharply restricted if the user changes the standard setting to the “maximum security level”. At the same time, an enormous amount of alerts are generated.

AVIRA Premium Security 2008, McAfee Internet Security 2008, Microsoft Live OneCare 2.0 and Trend Micro Internet Security 2008 showed **good performance properties**, even on older computer systems with only 512 MB main memory.

The **front-runner** in the performance test is unbeaten: **ESET Smart Security 3.0.** It was also established that the **minimum technical requirements** given by the manufacturers usually represent an absolute **minimum** only, i.e. that which is needed to be able to install the respective security solution at all.

However, smooth working was not possible and there were enormous delays in some areas (starting programs, opening Internet pages, etc.).

H.) Test: RICE/EQUIPMENT RATIO

Manufacturer	*Price (box)*	*Price (download)*	*Amazon-price*	*Licences*	*Content (software)*	*Points* max. 20	*Evaluation*
Agnitum	49,95	49,95	---	1x	AV, FW, PF, AS	***14***	***satisf.***
Avira	39,95	39,95	31,95	1x	AV, FW, PF, AS, KS, (BP)	***16***	***good***
BitDefender	29,95	29,95	20,95	1x	AV, FW, PF, AS, KS, ID	***19***	***very good***
BullGuard	69,95	69,95	46,99	3x	AV, FW, PF, AS, BP	***15***	***satisf.***
Eset	44,95	44,95	---	1x	AV, FW, PF, AS	***14***	***satisf.***
F-Secure	39,95	37,95	30,45	1x	AV, FW, PF, AS, KS	***15***	***satisf.***
G Data	39,95	35,95	29,95	1x	AV, FW, PF, AS, WF, DS	***18***	***very good***
Kaspersky	48,45	39,95	28,95	1x	AV, FW, PF, AS, WF, KS, ID	***15***	***satisf.***
McAfee	69,95	69,95	---	3x	AV, FW, PF, AS, KS, BP	***15***	***satisf.***
Microsoft	49,95	49,95	47,95	3x	AV, FW, PF, BP, ST	***16***	***good***
Panda	69,95	69,95	49,99	1x	AV, FW, PF, AS, KS, BP, ID, ON	***15***	***satisf.***
Symantec	29,99	29,99	25,95	1x	AV, FW, PF, AS, KD, ID, AB	***20***	***excellent***
Trend Micro	49,95	49,95	48,95	3x	AV, FW, PF, AS, KS, ID, WiFi	***18***	***very good***

Legende:
AV = antivirus scanner
FW = firewall
PF = phishing filter
PC = parental control
BP = Backup
ID = identity protection
WF = web filter
DS = data shredder
ON = online scanner
ST = system tuner
WiFi = WLAN protection
AB = Norton AntiBot

When evaluating the price/equipment ratio, it was clear that there are significant differences in some cases between the manufacturer's recommended price or the price in the manufacturers' online shops and the Amazon price (mostly incl. free delivery). Therefore, it's always worth shopping around. Many manufacturers try to attract buyers by offering cheaper follow-up licences or discounts if you subscribe for two to three years at once. In such instances, you should also take into account whether the offer from the online mail-order company might not still be better value.

The same applies in the case of multiple licences. You might think you're getting a good deal by subscribing for a longer term, but you could be wrong.

I.) CONCLUSION

Before the final result of this comparison test is now announced, some significant findings should first be mentioned.

There is no such thing as the perfect security suite. This comparison test proved this unequivocally. None of the security suites we tested were bad, but none were really excellent either.

A suite with a strong personal firewall and thoroughly good results in many other respects can fall down when it comes to the malware detection rate. “Agnitum Outpost Security Suite 2008” and “Microsoft Live OneCare 2.0” are two examples of this. This resulted in points being deducted from both suites although they otherwise consistently achieved good to excellent results in all other test areas.

This particularly impacted on the suites from **Panda Security** and **Agnitum**. With a malware detection rate of 75.6%, Agnitum not only brought up the rear in terms of the detection rate of the tested products but also came in last in this comparison test. Therefore, interested parties are advised to subject the stand-alone firewall solution from “Agnitum OutPost Pro Firewall 2008” to closer scrutiny and to use a product from another manufacturer such as Avira/G DATA/ESET/Symantec for the anti-virus scanner.

G DATA Internet Security 2008 and **Trend Micro Internet Security 2008** showed excellent results. However, both suites lost points due to defects found in the area of the firewall‘s internal protection abilities.
ESET Smart Security 3.0 was docked slightly for malware detection and the price/equipment ratio so that the manufacturer Eset **just barely missed out** on a top spot.

When the test series is evaluated with regard to security, user friendliness, performance and the price/equipment ratio in accordance with the evaluation criteria that were laid down (see C – Evaluation Criteria), the following detailed picture emerges:

MANUFACTURER	SECURITY (external/internal/malware/ other.)	USER-FRIENDLINESS & PERFORMANCE	PRICE/ EQUIPMENT	POINTS	%
Symantec	**30 / 20 / 42.7 / 05**	**36 / 35**	**20**	**188.7**	**94.35%**
Trend Micro	**30 / 18 / 43.0 / 04**	**39 / 36**	**18**	**188.0**	**94.00%**
Avira	**30 / 20 / 44.6 / 03**	**36 / 38**	**16**	**187.6**	**93.80%**
G DATA	**30 / 18 / 44.5 / 05**	**38 / 33**	**18**	**186.5**	**93.25%**
ESET	**30 / 20 / 42.7 / 03**	**36 / 40**	**14**	**185.7**	**92.85%**
BitDefender	**30 / 20 / 41.5 / 04**	**35 / 35**	**19**	**184.5**	**92.25%**
Microsoft	**30 / 20 / 38.9 / 03**	**36 / 37**	**16**	**180.9**	**90.45%**
F-Secure	**30 / 20 / 42.5 / 04**	**37 / 32**	**15**	**180.5**	**90.25%**
BullGuard	**30 / 20 / 41.5 / 04**	**35 / 35**	**15**	**180.5**	**90.25%**
Kaspersky	**30 / 17 / 43.3 / 04**	**36 / 35**	**15**	**180.3**	**90.15%**
McAfee	**30 / 17 / 39.9 / 03**	**36 / 37**	**15**	**177.9**	**88.95%**
Panda	**30 / 20 / 30.5 / 04**	**36 / 35**	**15**	**170.5**	**85.25%**
Agnitum	**30 / 20 / 20.6 / 04**	**36 / 34**	**14**	**158.6**	**79.30%**

According to the points evaluation system (maximum possible points receivable = 200), places 1 to 3 go to the following security suites:

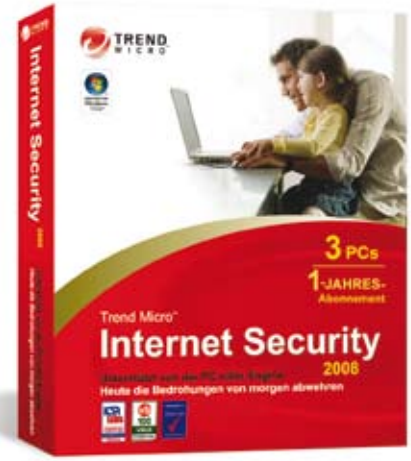
1st place with **188.7** points to: Norton Internet Security 2008

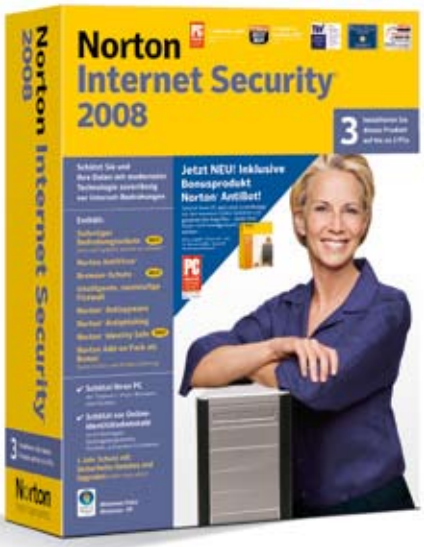
2nd place with **188.0** points to: Trend Micro Internet Security 2008

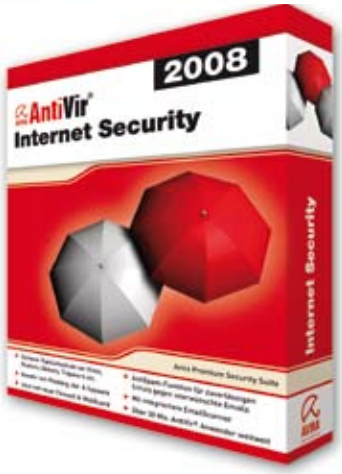
3rd place with **187.6** points to: Avira Premium Security Suite 2008

The **winner** of this large comparison test is the **NORTON INTERNET SECURITY 2008 product from SYMANTEC.**

Due to the very tight and extremely close points placing – with a difference of just one point or less – the ProtectStar™ TestLab has decided to award all of the security suites which finished in the top three with the **ProtectStar™ AWARD 2008.**





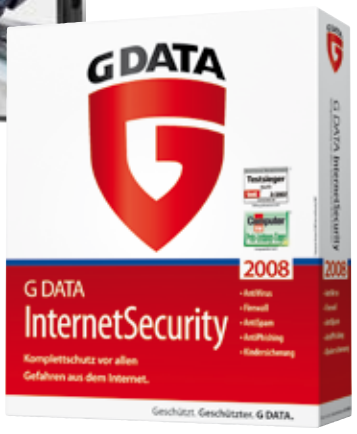


J.) J.) CONCLUSION II (recommendations)

A points evaluation system such as was used in **I.) Conclusion** is not helpful for every user group. Depending on the level of user knowledge and how the computer/ notebook is equipped, different decision criteria can be relevant.

Experienced users and professionals tend to switch over to individual solutions from various different manufacturers, for example. This user group also uses several anti-virus scanners in dual operation in order to create the best possible security suite for themselves.

The ProtectStar™ TestLab can recommend both the **G DATA Internet Security 2008 and ESET Smart Security 3.0** security solutions for experienced and less technically-versed users, whether they be in the home or business area. The product from **G DATA** stands out with its comprehensive modules, dual malware scanners and a high level of user-friendliness while ESET impressed with its unbeatable performance and outstanding security modules. Both solutions have been awarded the **ProtectStar™ Excellent Security** recommendation.



Comments, Criticism and Donations

The ProtectStar™ TestLab and AV Comparatives work strictly independently. The test analysis carried out here, the preparation and generation of the test results, the design of the test report, translations, publications, etc. have been financed by ProtectStar™, Inc only. The manufacturers mentioned in the test report simply provided the test versions and licences needed for the test series.

In order to be able to continue to improve the test series in the future, ProtectStar™ TestLab is grateful for any kind of comment or criticism from its readers. Please let us know what you particularly liked and which test you believe could have been carried out in greater detail. Could further test criteria which have been forgotten in the current test report be integrated in the future?

If you enjoyed the test report and it has helped you in making a purchase decision or if you have been able to find out something new through adding to your expert knowledge in the area of IT security, we would be very grateful for **your support** for the charitable and international **ProtectStar™ Foundation.**

Your support will benefit non-profit aid programs all over the world in the areas of training, health, poverty and IT-security for schools.

Further information on the non-profit **ProtectStar™ Foundation** can be found at:

www.protectstar-foundation.org

Copyright

Contact

Corporate Headquarter:
ProtectStar, Inc.
TestLab
1901 60th Place
Suite L3604
34203 Bradenton, FL
USA

Phone: +1 888 218 4123
Fax : +1 888 218 8505
e-Mail: testcenter@protectstar.com
Web : www.protectstar-testlab.org

European Headquarter:
ProtectStar, Inc.
Test Lab
Daws House
33-35 Daws Lane
London NW7 4SD
UK

Phone: +44 20 8906 6651
Fax : +44 20 8906 6611
e-Mail: testcenter@protectstar.com
Web : www.protectstar-testlab.org