

Whole Product “Real-World” Dynamic Protection Test



August-November 2011

Language: English

December 2011

Last revision: 16th December 2011

www.av-comparatives.org

Content



Introduction	3
Test Procedure.....	4
Preparation for Test Series	4
Lab-Setup.....	4
Hardware and Software.....	4
Settings.....	5
Preparation for Every Testing Day	5
Testing Cycle for each malicious URL	5
Source of test cases	6
Test Set.....	6
Comments	7
Tested products	7
Test Cases	7
Diagrammatic Overview.....	10
Results	9
Summary Results.....	10
Whole-Product False Alarm Test.....	11
Wrongly blocked domains (while browsing)	11
Wrongly blocked files (while downloading/installing)	11
Award levels reached in this test.....	13
Copyright and Disclaimer.....	14

Introduction

The threat posed by malicious software is growing day by day. Not only is the number of malware programs increasing, also the very nature of the threats is changing rapidly. The way in which harmful code gets onto computers is changing from simple file-based methods to distribution via the Internet. Malware is increasingly infecting PCs through e.g. users deceived into visiting infected web pages, installing rogue/malicious software or opening emails with malicious attachments.

The scope of protection offered by antivirus programs is extended by the inclusion of e.g. URL-blockers, content filtering, anti-phishing measures and user-friendly behaviour-blockers. If these features are perfectly coordinated with the signature-based and heuristic detection, the protection provided against threats increases.

In spite of these new technologies, it remains very important that the signature-based and heuristic detection abilities of antivirus programs continue to be tested. It is precisely because of the new threats that signature/heuristic detection methods are becoming ever more important too. The growing frequency of zero-day attacks means that there is an increasing risk of malware infection. If this is not intercepted by “conventional” or “non-conventional” methods, the computer will be compromised, and it is only by using an on-demand scan with signature and heuristic-based detection that the malware can be found (and hopefully removed). The additional protection technologies also offer no means of checking existing data stores for already-infected files, which can be found on the file servers of many companies. Those new security layers should be understood as an addition to good detection rates, not as replacement.

In this test all features of the product contribute protection, not only one part (like signatures/ heuristic file scanning). So the protection provided should be higher than in testing only parts of the product. We would recommend that all parts of a product should be high in detection, not only single components (e.g. URL blocking protects only while browsing the web, but not against malware introduced by other means or already present on the system).

The Whole-Product Dynamic Protection test is a joint project of AV-Comparatives and the University of Innsbruck’s Faculty of Computer Science and Quality Engineering. It is partially funded by the Austrian Government.



Test Procedure

Testing dozens of antivirus products with hundreds of URLs each per day is a lot of work which cannot be done manually (as it would be thousands of websites to visit and in parallel), so it is necessary to use some sort of automation.

Preparation for Test Series

Every security program to be tested is installed on its own test computer. All computers are connected to the Internet (details below). The system is frozen, with the operating system and security program installed.

Lab-Setup

The entire test is performed on real workstations. We do not use any kind of virtualization. Each workstation has its own internet connection with its own external IP. We have special agreements with several providers (failover clustering and no traffic blocking) to ensure a stable internet connection. The tests are performed using a live internet connection. We took the necessary precautions (with specially configured firewalls, etc.) not to harm other computers (i.e. not to cause outbreaks).

Hardware and Software

For this test we used identical workstations, an IBM BladeCenter and network attached storage.

	Vendor	Type	CPU	RAM	Hard Disk
Workstations	Fujitsu	E3521 E85+	Intel Core 2 Duo	4 GB	80 GB
BladeCenter	IBM	E Chassis	-	-	-
Blades	IBM	LS20	AMD Dual Opteron	8 GB	76 GB
NAS	QNAP	TS-859U-RP	Atom Dual Core	1 GB	16 TB Raid 6

The tests are performed under Windows XP SP3 with no further updates. Some further installed vulnerable software includes:

Vendor	Product	Version	Vendor	Product	Version
Adobe	Flash Player ActiveX	10.1	Microsoft	Internet Explorer	7
Adobe	Flash Player Plug-In	10	Microsoft	Office Professional	2003
Adobe	Acrobat Reader	8.0	Microsoft	.NET Framework	3.5
Apple	QuickTime	7.1	Sun	Java	6.0.140

Settings

We use every security suite with its default (out-of-the-box) settings. If user interactions are required, the default option is considered. Our whole-product dynamic protection test aims to simulate real-world conditions as experienced every day by users. Therefore, if there is no predefined action, we will always use the same action where we consider the warning/message to be very clear and definitive. If the message leaves it up to the user, we will mark it as such, and if the message is very vague, misleading or even suggests trusting e.g. the malicious file/URL/behaviour, we will consider it to be a miss, as the ordinary user would. We consider “protection” to mean that the system is not compromised. This means that the malware is not running (or is removed/terminated) and there are no significant/malicious system changes. An outbound-firewall alert about a running malware process, which asks whether or not to block traffic from the users’ workstation to the internet is too little, too late and not considered by us to be protection.

Preparation for every Testing Day

Every morning, any available security software updates are downloaded and installed, and a new base image is made for that day. This ensures that even in the case the security product would not finish a bigger update during the day (products are being updated before each test case) or is not reachable, it would at least use the updates of the morning, as it would happen to the user in the real world.

Testing Cycle for each malicious URL

Before browsing to each new malicious URL/test-case we update the programs/signatures. New major product versions (i.e. the first digit of the build number is different) are installed once at the begin of the month, which is why in each monthly report we only give the product main version number. Our test software starts monitoring the PC, so that any changes made by the malware will be recorded. Furthermore, the recognition algorithms check whether the antivirus program detects the malware. After each test case the machine is reverted to its clean state.

Protection

Security products should protect the user’s PC. It is not very important at which stage the protection takes place. This can either be while browsing to the website (e.g. protection through URL Blocker), while an exploit tries to run or while the file is being downloaded/created or while the malware is executed (either by the exploit or by the user). After the malware is executed (if not blocked before), we wait several minutes for malicious actions and also to give e.g. behaviour-blockers time to react and remedy actions performed by the malware. If the malware is not detected and the system is indeed infected/compromised, the process goes to “Malware Not Detected”. If a user interaction is required and it is up to the user to decide if something is malicious, and in the case of the worst user decision the system gets compromised, we rate this as “user-dependent”. Due to that, the yellow bars in the results graph can be interpreted either as protected or not protected (it’s up to the user).

Due to the dynamic nature of the test, i.e. mimicking real-world conditions, and because of the way several different technologies (such as cloud scanners, reputation services, etc.) work, it is a matter of fact that such tests cannot be repeated or replicated in the way that e.g. static detection rate tests can. Anyway, we try to log as much as reasonably possible to prove our findings and results. Vendors are invited to provide useful logs inside their products which can provide the additional data they want in case of disputes. Vendors were given after each testing month the possibility to dispute our conclusion about the compromised cases, so that we could recheck if there were maybe some problems in the automation or with our analysis of the results.

In the case of cloud products, we will only consider the results that the products had at the time of testing; sometimes the cloud services provided by the security vendors are down due to faults or maintenance downtime by the vendors, but these cloud-downsides are often not disclosed/communicated to the users by the vendors. This is also a reason why products relying too much on cloud services (and not making use of local heuristics etc.) can be risky, as in such cases the security provided by the products can decrease significantly. Cloud signatures/ reputation should be implemented in the products to complement the other local/offline protection features and not replace them completely, as e.g. offline cloud services would mean the PCs being exposed to higher risks.

Source of test cases

We use our own crawling system to search continuously for malicious sites and extract malicious URLs (including spammed malicious links). We also research manually for malicious URLs. If our in-house crawler does not find enough valid malicious URLs on one day, we have contracted some external researchers and resources to provide additional malicious URLs first exclusively to AV-Comparatives.

Test Set

We are not focusing on zero-day exploits/malware (although it is possible that they are also present in the URL pool), but mainly on current, visible and relevant malicious websites/malware that are currently out there and problematic to the ordinary users. We are trying to include only about 30-50% URLs pointing directly to malware (for example, if the user is tricked by social-engineering into follow links in spam mails or websites, or if the user is tricked into installing some Trojan or other rogue software). The rest/bigger part are exploits/drive-by downloads - these usually seem to be well covered by almost all major security products. According to a study¹ released by Microsoft about propagation methods, it seems that nowadays exploits represent only a minority and that social-engineering/user-interaction is by far the most prevalent propagation method. We may eventually adapt the distribution in future tests.

In this kind of testing, it is very important to use enough test cases. If an insufficient number of samples are used in comparative tests, differences in results may not indicate actual differences among the tested products². In fact, we consider even in our tests (with thousands of test-cases) products in the same protection cluster to be more or less equally good; as long as they do not wrongly block clean files/sites more than the industry average.

¹ Microsoft Security Intelligence Report, Volume 11, page 13: <http://www.microsoft.com/security/sir/default.aspx>

² Read more in the following paper: <http://www.av-comparatives.org/images/stories/test/statistics/somestats.pdf>

Comments

Most operating systems already include their own firewalls, automatic updates, and may even ask the user before downloading or executing files if they really want to do that, warning that downloading/executing files can be dangerous. Mail clients and web mails include spam filters too. Furthermore, most browsers include Pop-Up blockers, Phishing/URL-Filters and the ability to remove cookies. Those are just some of the build-in protection features, but despite all of them, systems can get infected anyway. The reason for this in most cases is the ordinary user, who may get tricked by social engineering into visiting malicious websites or installing malicious software. Users expect a security product not to ask them if they really want to execute a file etc. but expect that the security product will protect the system in any case without them having to think about it, and despite what they do (e.g. executing unknown files). We try to deliver good and easy-to-read test reports for end-users. We are continuously working on improving further our automated systems to deliver a better overview of product capabilities.

Tested products

The following products were tested in the official Whole-Product Dynamic Protection main test series³. In this type of test we usually include Internet Security Suites, although also other product versions fit (and are included/replaced on vendors request), because what is tested is the "protection" provided by the various products against a set of real-world threats.

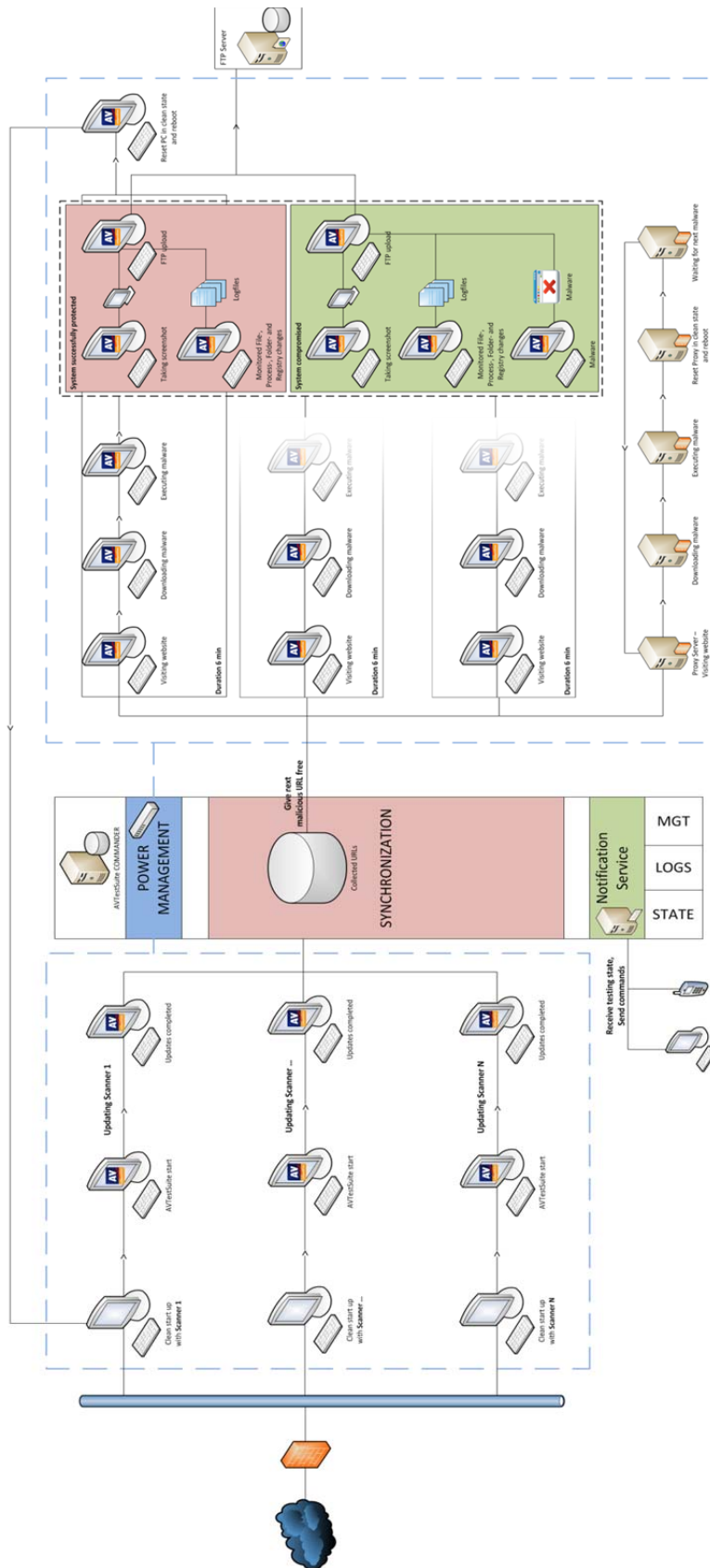
Main product versions used for the monthly test-runs:

Vendor	Product	Version August	Version September	Version October	Version November
Avast	Antivirus Free	6.0	6.0	6.0	6.0
AVG	Internet Security	2011	2011	2012	2012
Avira	Premium Security Suite	10.2	10.2	12.0	12.0
Bitdefender	Internet Security	2012	2012	2012	2012
ESET	Smart Security	4.2	4.2	5.0	5.0
F-Secure	Internet Security	2011	2011	2012	2012
G DATA	Internet Security	2012	2012	2012	2012
K7	Total Security	11.1	11.1	11.1	11.1
Kaspersky	Internet Security	2012	2012	2012	2012
McAfee	Total Protection	2011	2011	2011	2012
Panda	Cloud Free Antivirus	1.51	1.51	1.51	1.51
PC Tools	Internet Security	2011	2011	2011	2012
Qihoo 360	Internet Security	2.0	2.0	2.0	2.0
Sophos	Endpoint Security	9.7	9.7	9.7	9.7
Symantec	Norton Internet Security	2011	2012	2012	2012
Trend Micro	Titanium Internet Security	2012	2012	2012	2012
Webroot	Internet Security Complete	7.0	7.0	7.0	7.0

³ The results from March to June 2011 can be found here:

http://www.av-comparatives.org/images/stories/test/dyn/wpdt2011_1_en.pdf

Diagrammatic Overview⁴



⁴ As of August 2010. Some enhancements/changes/additions have been implemented since then.

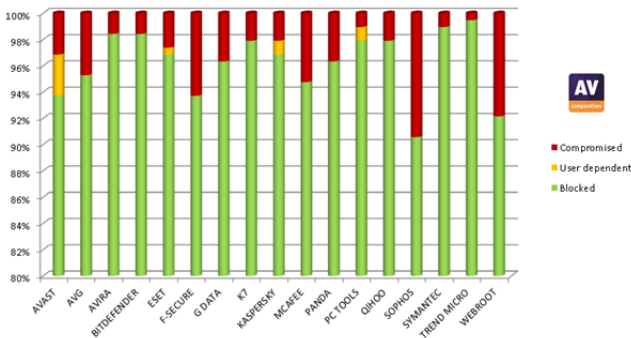
Test Cases

Test period	Test-cases
4 th to 22 nd August 2011	191
1 st to 23 rd September 2011	608
3 rd to 28 th October 2011	503
6 th to 25 th November 2011	596
TOTAL	1898

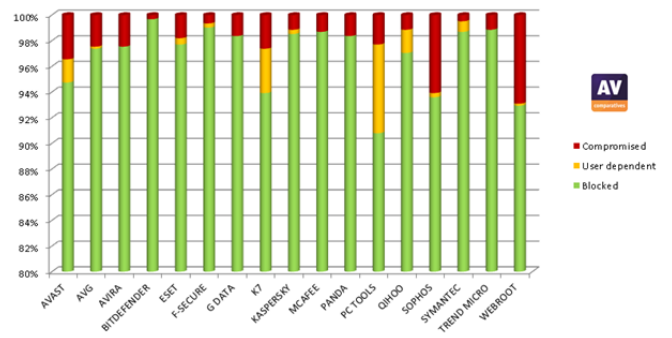
Results

Below you see an overview of the past single testing months. Percentages can be seen on the interactive graph on our website⁵.

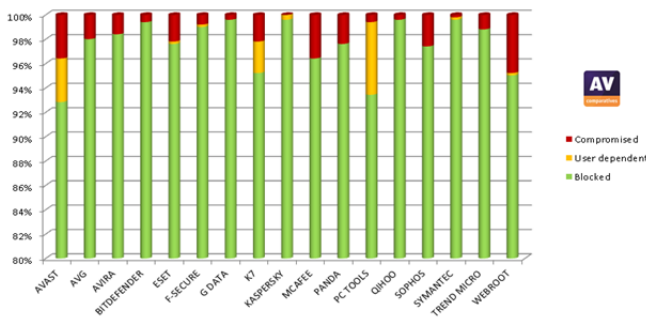
August 2011 – 191 test cases



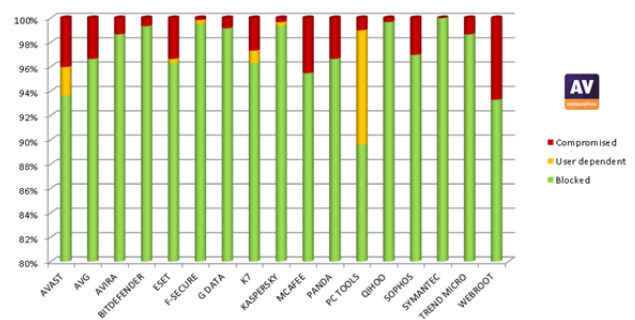
September 2011 – 608 test cases



October 2011 – 503 test cases



November 2011 – 596 test cases



We do not give in this report exact numbers for the single months on purpose, to avoid the little differences of few cases being misused to state that one product is better than the other in a given month and test-set size. We give the total numbers in the overall reports, where the size of the test-set is bigger, and more significant differences may be observed. Interested users who want to see the exact protection rates (without FP rates) every month can see the monthly updated interactive charts on our website⁶.

⁵ <http://www.av-comparatives.org/comparativesreviews/dynamic-tests>

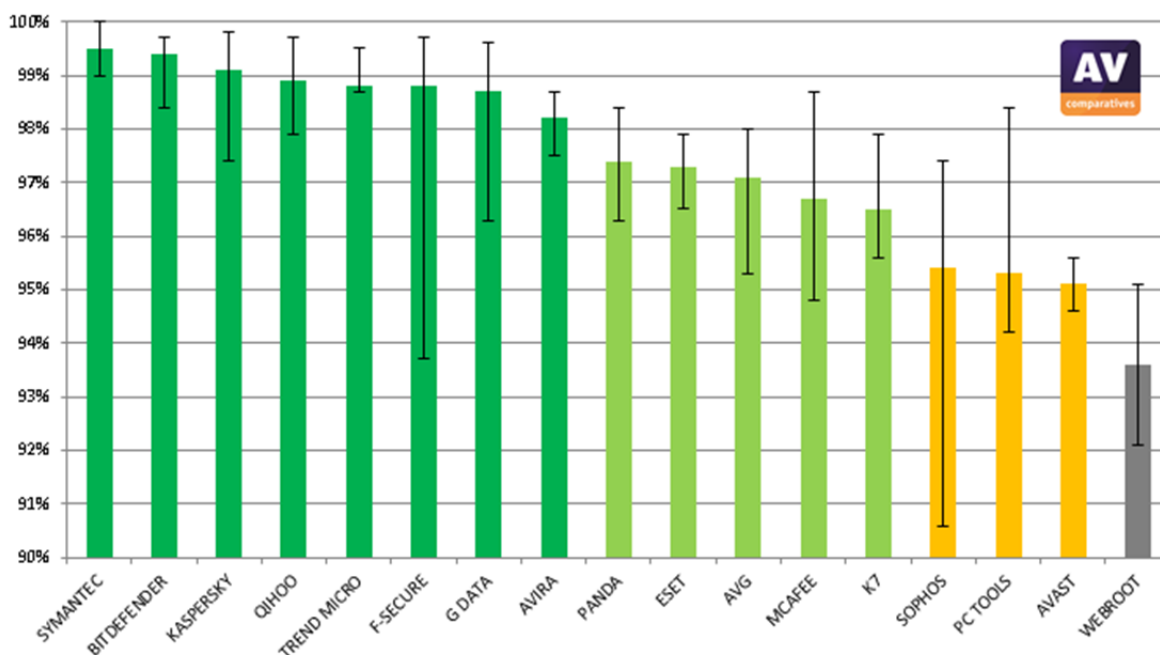
⁶ <http://chart.av-comparatives.org/chart2.php> and <http://chart.av-comparatives.org/chart3.php>

Summary Results (August-November)

Test period: August – November 2011 (1898 Test cases)

	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2] ⁷	Cluster ⁸
Symantec	1886	6	6	99,5%	1
Bitdefender	1886	-	12	99,4%	1
Kaspersky	1877	8	13	99,1%	1
Qihoo	1872	11	15	98,9%	1
Trend Micro	1876	-	22	98,8%	1
F-Secure	1872	5	21	98,8%	1
G DATA	1874	-	24	98,8%	1
AVIRA	1864	-	34	98,2%	1
Panda	1849	-	49	97,4%	2
ESET	1844	7	47	97,3%	2
AVG	1843	1	54	97,1%	2
McAfee	1835	-	63	96,7%	2
K7	1811	40	47	96,5%	2
Sophos	1810	2	86	95,4%	3
PC Tools	1743	130	25	95,3%	3
Avast	1780	49	69	95,1%	3
Webroot	1775	2	121	93,6%	4

The graph below shows the above protection rate (all samples), including the minimum and maximum protection rates for the individual months.



⁷ User-dependent cases were given a half credit. Example: if a program gets 80% blocked-rate by itself, plus another 20% user-dependent, we give credit for half the user-dependent one, so it gets 90% altogether.

⁸ Hierarchical Clustering Method: defining four clusters using average linkage between groups (Euclidian distance) on the protection rate. Statistically, products in same cluster don't significantly differ from each other.

Whole-Product "False Alarm" Test (wrongly blocked domains/files)

The false alarm test in the Whole-Product Dynamic test consists of two parts: wrongly blocked domains (while browsing) and wrongly blocked files (while downloading/installing). It is necessary to test both scenarios because testing only one of the two above cases could penalize products which focus mainly on one type of protection method, either e.g. URL/reputation-filtering or e.g. on-access / behaviour / reputation-based file protection.

a) Wrongly blocked domains (while browsing)

We used around two thousand randomly chosen popular domains. Blocked non-malicious domains/URLs were counted as false positives (FPs). The wrongly blocked domains have been reported to the respective vendors for review and should now no longer be blocked.

By blocking whole domains, the security products are not only risking causing distrust in their warnings, but also eventually causing potential financial damage (beside the damage on website reputation) to the domain owners, including loss of e.g. advertisement revenue. Due to this, we strongly recommend vendors to block whole domains only in the case where the domain's sole purpose is to carry/deliver malicious code, and to otherwise block just the malicious pages (as long as they are indeed malicious). Products which tend to block URLs based e.g. on reputation may be more prone to this and score also higher in protection tests, as they may block many unpopular/new websites.

b) Wrongly blocked files (while downloading/installing)

We used about one hundred different applications listed either as top downloads or as new/recommended downloads from about a dozen different popular download portals. The applications were downloaded from the websites (if original developer site was given, we used that source instead of the download portal host), saved to disk and installed to see if they get blocked at any stage of this procedure. Additionally, we included a few files whose status as malware had been disputed over the past months of the Dynamic Test.

The duty of security products is to protect against malicious sites/files, not to censor or limit the access only to well-known popular applications and websites. If the user deliberately chooses a high security setting, which warns that it may block some legitimate sites or files, then this may be considered acceptable. However, we do not regard it to be acceptable as a default setting, where the user has not been warned. None of the products blocked extremely popular applications. As the test is done at points in time and FPs on very popular software/websites are usually noticed and fixed within a few hours, it would be surprising to encounter FPs on very popular applications. Due to this, FP tests which are done e.g. *only* on very popular applications, or which use *only* the top 50 files from whitelisted/monitored download portals would be a waste of time and resources. Users do not care whether they are infected by malware which affects only them, just as they do not care if the FP count affects only them. While it is preferable that FPs do not affect many users, it should be the goal to avoid having any FPs and to protect against any malicious files, no matter how many users are affected or targeted. Prevalence of FPs based on user-base data is of interest for internal testing of AV vendors, but for the ordinary user it is important to know how accurately its product distinguishes between clean and malicious files.

The below table shows the numbers of wrongly blocked domains/files:

	Wrongly blocked clean domains/files (blocked / user-dependent⁹)	Wrongly blocked score¹⁰
AVG	- / - (-)	-
Kaspersky	- / 1 (1)	0.5
ESET, Panda	1 / - (1)	1
G DATA	3 / - (3)	3
Symantec	2 / 2 (4)	3
Bitdefender, McAfee, Qihoo, Sophos	4 / - (4)	4
Avast	1 / 7 (8)	5
F-Secure	5 / 4 (9)	7
	<i>average (12)</i>	<i>12</i>
K7	15 / - (15)	15
AVIRA	17 / - (17)	17
PC Tools	18 / - (18)	18
Trend Micro	26 / - (26)	26
Webroot	81 / - (81)	81

To determine which products have to be downgraded in our award scheme due to the rate of wrongly blocked sites/files, we backed up our decision by using a clustering method and by looking at the average scores. The following products with above average FPs have been downgraded: AVIRA, K7, PC Tools, Trend Micro and Webroot.

⁹ Although user dependent cases are extremely annoying (esp. on clean files) for the user, they were this time counted only as half for the "wrongly blocked rate" (like for the protection rate).

¹⁰ Lower is better.

Award levels reached in this test

The awards are decided and given by the testers based on the observed test results (after consulting statistical models). The following awards are for the results reached in the Whole-Product Dynamic Protection Test:

AWARD LEVELS	PRODUCTS
	Symantec Bitdefender Kaspersky Qihoo F-Secure G DATA
	Trend Micro* AVIRA* Panda ESET AVG McAfee
	K7* Sophos Avast
	PC Tools* Webroot*

* downgraded by one rank due to the score of wrongly blocked sites/files (FPs).

<i>Simplified¹¹ system to illustrate ranking model</i>	Protection score Cluster ¹² 4	Protection score Cluster 3	Protection score Cluster 2	Protection score Cluster 1
< Ø FPs	Tested	Standard	Advanced	Advanced+
> Ø FPs	Tested	Tested	Standard	Advanced

Expert users who do not care about wrongly blocked files/websites (false alarms) are free to rely on the protection rates on page 10 instead of our awards ranking which takes FPs in consideration.

¹¹ We look mainly on the distance between the groups (clusters), but the mean is easier to illustrate to readers.

¹² See protection score clusters on page 10.

Copyright and Disclaimer

This publication is Copyright © 2011 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted with the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss which might occur as a result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No-one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use (or inability to use), the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives e.V. (December 2011)

**Every second counts.
Who is attacking you? And how?**

**Even the best AV solution leaves you exposed
to zero-day and custom malware attacks.**

**Get real-time analysis.
No waiting for signature updates.**



validEDGE
www.validedge.com

*ValidEdge Malware Analysis Appliances
Free 30-day evaluation.*

DETECT

ANALYZE

HEAL