# IT Security Survey 2012


Language: English

Last Revision: 7th April 2012

**www.av-comparatives.org**

## Overview

The Internet has without a doubt changed our lives. Online banking, shopping, gaming, and digital communication with other people, have become as much a part of our daily lives as flicking a light switch.

But how do computer users deal with the subject of digital security? Are they as careless as suggested by some media reports, or are they far more cautious than antivirus vendors and computer magazines would have us believe?

AV-Comparatives set out to find how ordinary users regard computer security. One reason for the survey was to optimise the institute's test with regard to what readers want; the other was to help antivirus manufacturers refine their products in line with user feedback.

## Survey Methodology

The answers given here are based on an Internet survey run by AV-Comparatives between 15th December 2011 and 15th January 2012. A total of 2,118 computer users from around the world anonymously answered the questions on the subject of computers and security. Answers from respondents who work in the antivirus industry were filtered out.
The survey contained control questions which allowed invalid answers, and respondents attempting to unfairly influence the result, to be recognised and removed from the results.

## Key results

Internet users have a very clear idea of how to protect their PCs, and thus their digital lives.

## Up-to-date computer software

Two thirds of PC users now run Windows 7, which has overtaken Windows XP in terms of both security and popularity.

64 per cent of users employ a paid-for antivirus solution; only a third trust in free protection.
2. Users take responsibility for their own security.

## Proactive users

Users are proactive when it comes to protecting their computers. Three quarters of respondents regularly scan their PCs for malware; more than half do this every week.

Disabling the virus scanner, e.g. to improve performance, is no longer seen as a viable option. Only one in ten survey participants admitted to switching off their antivirus software on a daily or weekly basis. Those who do do this are mostly online gamers, who want to get maximum performance from their computers. It is a very risky practice, however.

**Better virus detection demanded**

Valuable insights into the requirements of PC users came from both antivirus software manufacturers and publishers of computer magazines that review such programs. Four out of five respondents expect a high rate of virus detection combined with a low impact on system performance. Responses indicate that users may be dissatisfied with current anti-malware products, and are no longer prepared to accept any perceptible slowing down of the computer by the security software.

Technical support and the number of features unrelated to security (e.g. toolbars) appear not to be very important to users; sometime they think it is only annoying.

**Cloud scepticism**

With regard to the Cloud and its related data traffic, users are concerned about data protection. Just about half of respondents found the idea of automatically sending files to the AV manufacturer for analysis to be unacceptable. A further third would only consider allowing this if they were asked whether a specific file could be sent or not.

Survey participants were particularly wary of unknown (to the AV program) files being classified as suspicious and uploaded; this could include documents with sensitive information that should not leave the user's own computer.

**Conclusions**

Computer/Internet users appear to be better informed with regard to IT security than they were a few years ago. They are more careful, and keep themselves informed on issues of computer security and protection.

They are however worried about data protection when it comes to Cloud-based security programs, or those with Cloud components. The manufacturers of antivirus solutions would be well advised to listen to their customers and improve their products accordingly.

AV-Comparatives' Whole-Product Dynamic Real-World Protection Test takes Cloud security into account (along with other protection features). It tests antivirus products under real-life conditions, and so demonstrates as realistically as possible how well PC security products do their job. AV-Comparatives is currently one of the world's leading institutes with regard to real-world testing.

Survey respondents deemed AV-Comparatives to have the best reputation for effective tests and reliable results, out of all the testing institutes listed. This compliment is easily incentive enough to continue to aim for the highest quality results, using the most modern test methods and presenting the results in the most transparent way possible. Both users and antivirus manufacturers will benefit from this approach.

Test results are available to everyone for free at www.av-comparatives.org.

# Security Survey 2012

To improve our service we made a survey and asked users for their opinions on various topics related to anti-virus software testing and anti-virus software in general. The results are very helpful to us and we want thank all those who took the time to complete the survey.

## 1. Key data

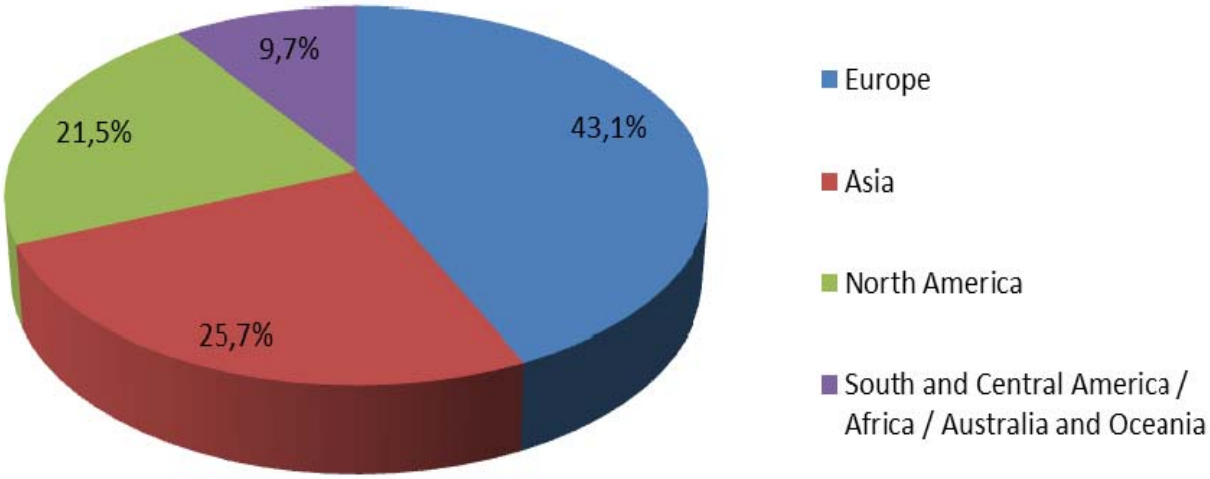
Survey Period: **15th December 2011 - 15th January 2012**

Valid responses of real users: **2118**

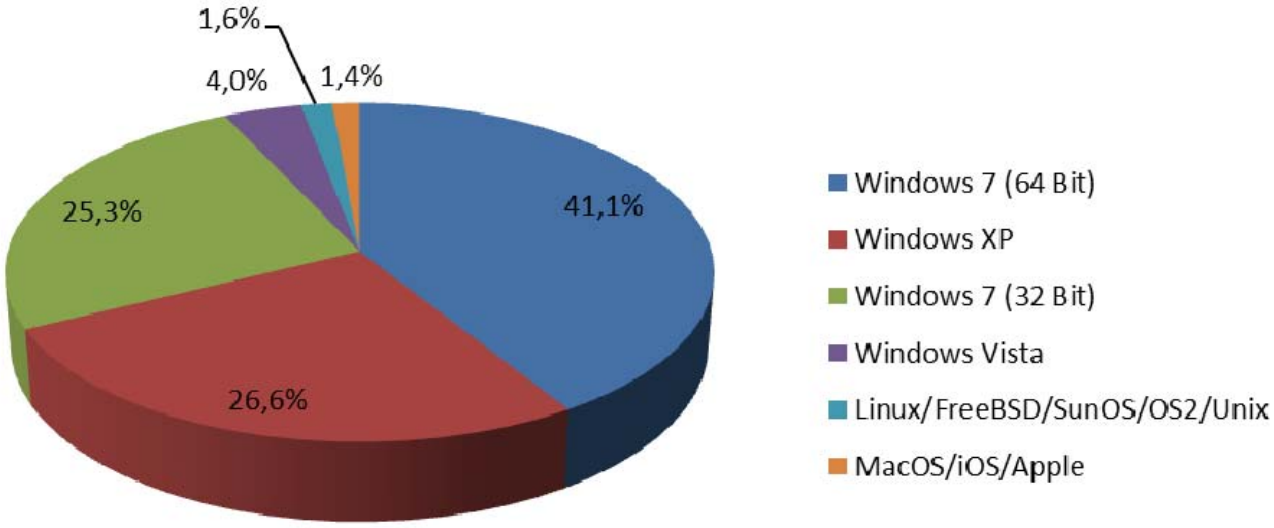
The survey contained some control questions and checks to allow us to filter out invalid responses and users who tried to distort the results by e.g. giving impossible/conflicting answers. As we were primarily interested in the opinions of everyday users, the survey results in this public report do not take into account the (approx. 200) responses of participants who are involved with anti-virus companies.

The results of the survey are very valuable to us; you will find in this report the results of some of the survey questions, which we would like to share with you.

## 2. Where are you from?



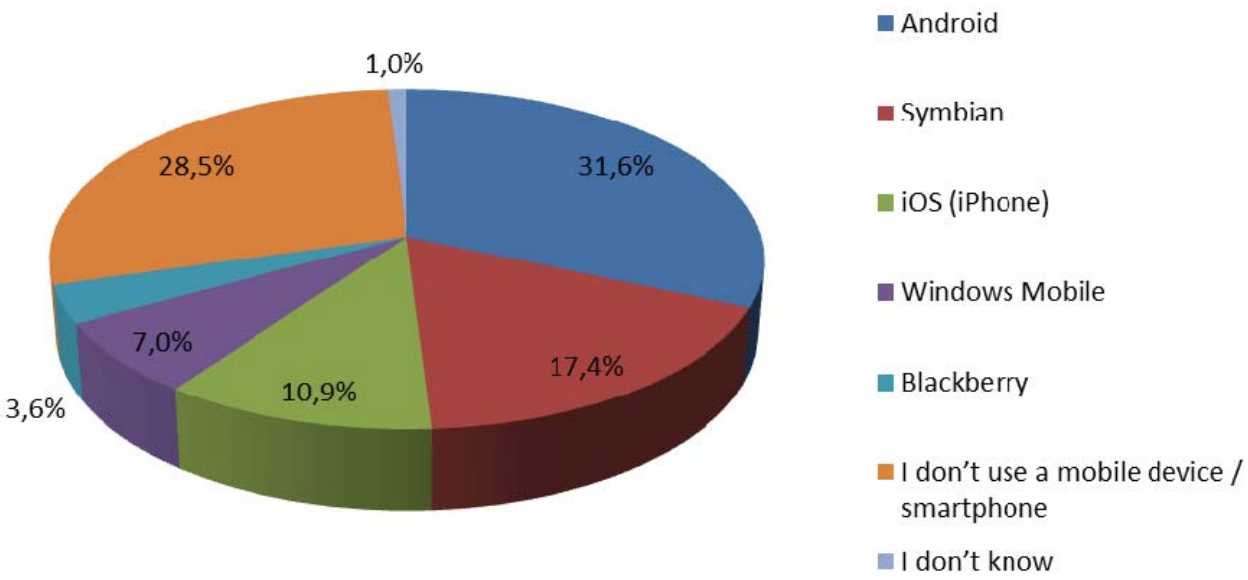

## 3. Which operating system do you primarily use?




Windows 7 is now the dominant operating system, with over two thirds of survey participants using it. The 64-bit version alone is more popular than XP.

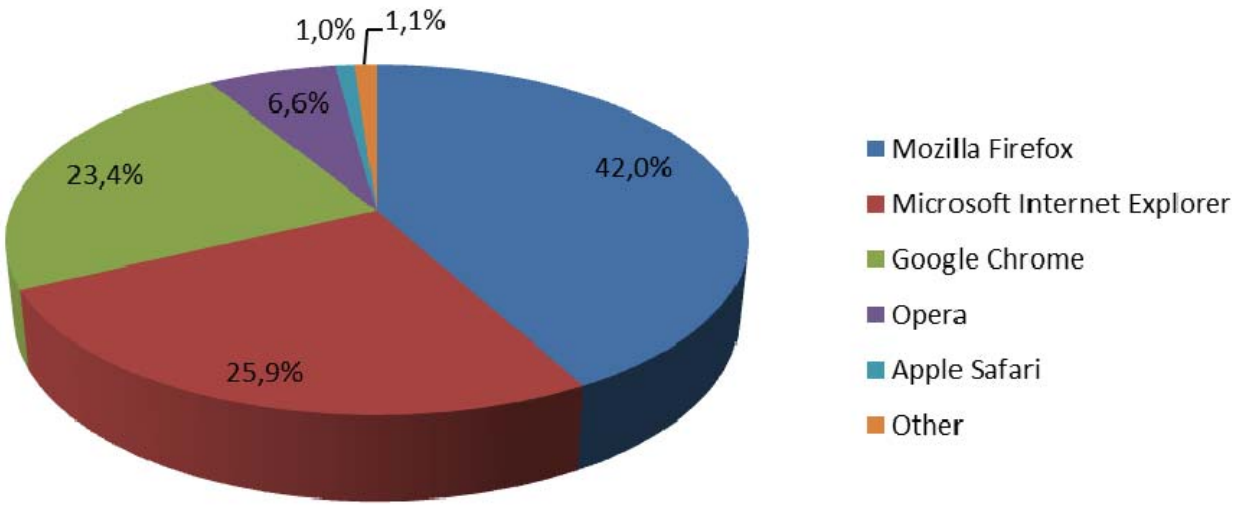
Although in file detection tests there is practically no difference between different operating systems used, there is definitely a difference in other factors such as performance. That's why we now perform most tests under Windows 7. We are also considering switching to Windows 7 for the whole product tests in the future. Currently we still perform them under Windows XP, as we want primarily to evaluate the protection provided by the security products, rather than the protection provided by a specific OS. If all users used up-to-date and patched operating systems and software, there almost certainly wouldn't be so many successful malware attacks in the world.

## 4. Which mobile operating system do you use?



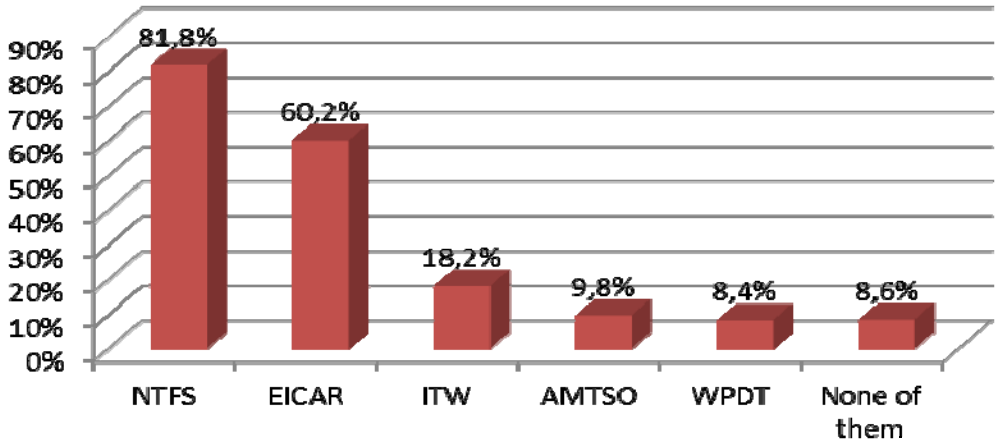

On Smartphones the Android mobile operating system is prevailing and steadily gaining more and more market share, meaning that malware authors are increasingly targeting Android phones. During this year we will provide a test and review of various mobile security products.

## 5. Which browser do you primarily use?

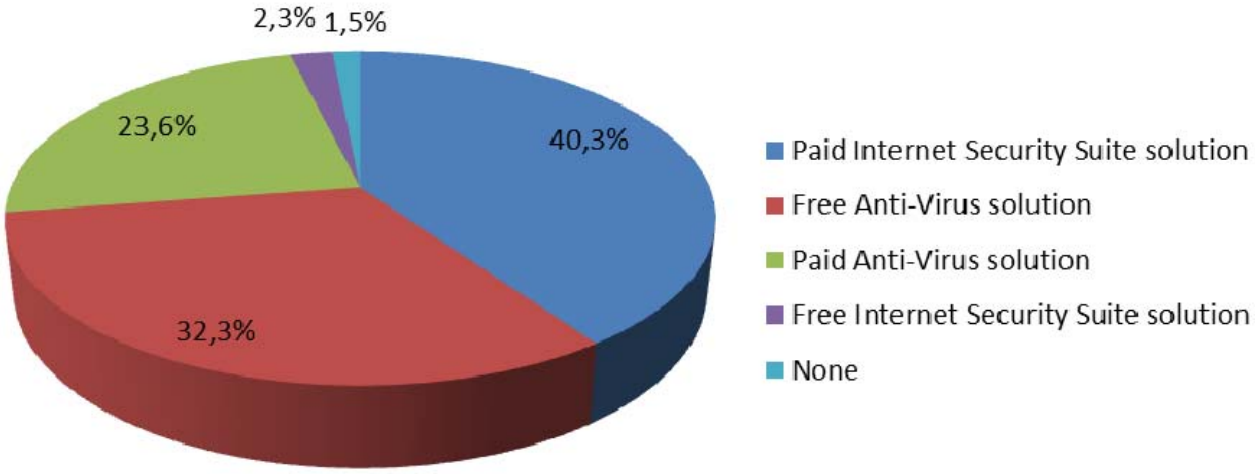



Over two fifths of the users who took part in our survey use Mozilla Firefox to browse the web, followed by MS Internet Explorer. Chrome is not far behind.

## 6. Which of those acronyms are known to you?




## 7. Which type of security solution are you currently primarily using?




Most users are willing to pay for a security product.

## 8. Which security solution are you currently using?

The list below shows the manufacturers of the products most commonly used by survey participants, in order of popularity:

**avast!**

**AVIRA**

**Kaspersky**

**ESET**

**Microsoft**

**Symantec**

**Bitdefender**

**F-Secure**

**Panda**

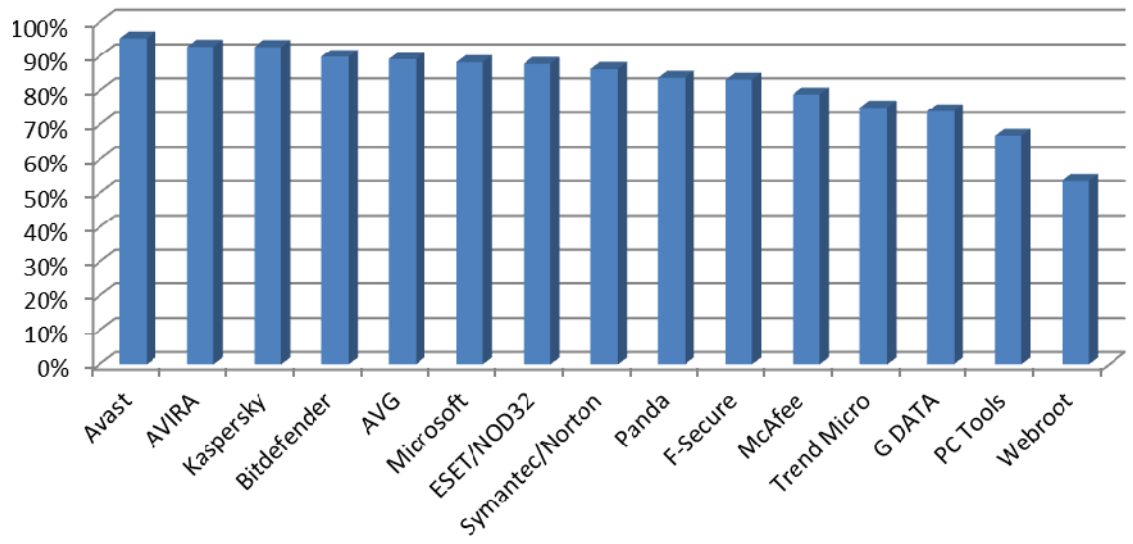
**AVG**

**McAfee**

**G DATA**

## 9. Which security solutions would you most like to see in our yearly public main-test series?

Below are the 15 top requested products (with over 50% of users voting for them, products with less than 50% are not listed). Users had to choose 15 products.



All the products above have been tested last year. This year our test series will also include some new products which were requested in last year's survey, and whose vendors have agreed to participate:

**AhnLab**

**Bullguard**

**Fortinet**

**GFI Vipre**

Additionally, two highly requested Chinese products (included only in the Chinese report) are now in the test series:

**Qihoo**

**Tencent**

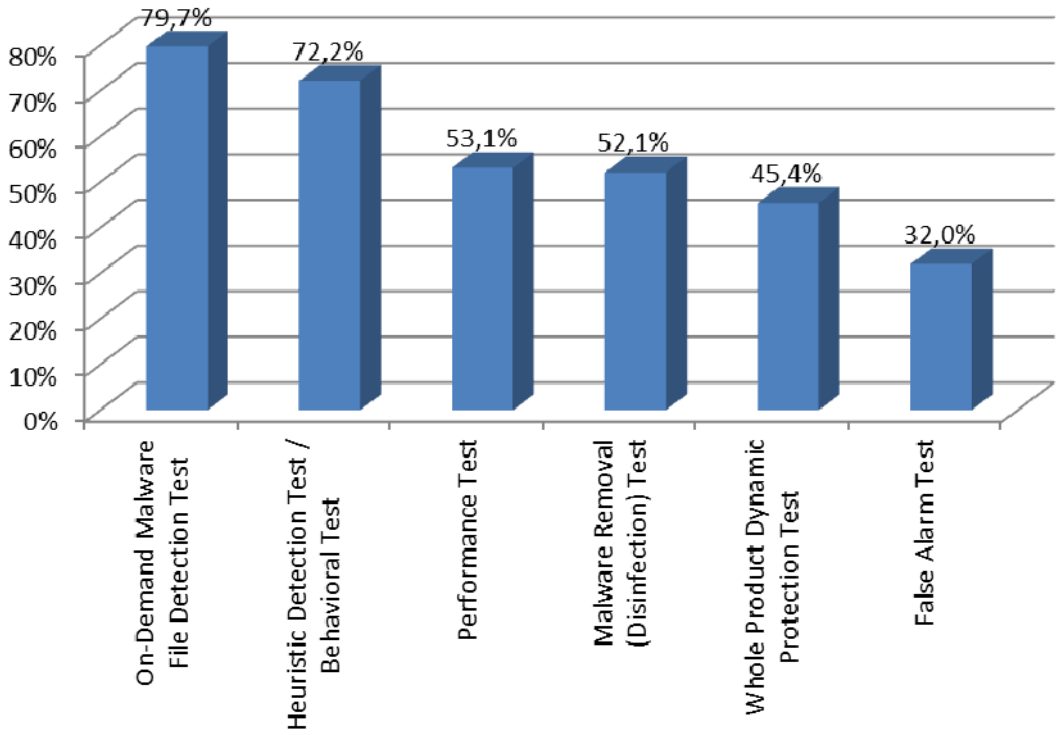
Two other products (which were already in last year's test series) are included: **eScan and Sophos**.

Although we wanted to include only a total of 16-20 vendors in our tests this year (because testing more products increases e.g. the time taken to produce and release reports), we ended up including some more, as many vendors wanted to subscribe to our public test series. We removed some products, and added some others from the previous year's waiting list. For reasons of time and resources, we could not include all the vendors who wanted to take part, although we have most of them.

Symantec only wanted to take part in our public tests if they could choose which of the tests from our yearly public test-series they participated in; specifically, they did not want to take the File Detection Test (formerly called On-Demand Test). As an independent testing organization, we require all vendors to take part in all the basic tests in the series, and do not allow them to cherry-pick tests. We feel that the File Detection Test is essential to showing the overall capabilities of an anti-virus product, especially with regard to threats that do not come directly from web pages, but are spread via email, LAN or flash drive. Other independent testing organizations (such as AV-Test, VirusBulletin, ICSALabs, WestCoastLabs) include, or rely exclusively on, file detection tests. We know that such tests are not easy to pass, especially considering the need to minimise false positives. As we cannot allow any vendor to opt out of any of the core public tests, Symantec has decided not to take part into our public tests this year[1].

[1] http://www.av-comparatives.org/forum/index.php?page=Thread&threadID=1060

## 10. Which type of tests are you most interested in?




Clearly the great majority of users are interested in on-demand malware file detection rate tests, as well as proactive tests which evaluate heuristics etc. This year we are only carrying out one retrospective test, but this will additionally include a behavioural element, which evaluates a product's behavioural protection, as requested by some users. The percentage shown above for the heuristic/behavioural test is a combined figure for the two tests; the percentage for the heuristic test alone would have been 55.6%. As the file detection test is the most requested test by users (and magazines) and also due to some business requirements (our file detection test results are used/required by certain analysts and corporations for their certification programs), we will continue to perform such tests regularly in the future (although only a couple of times a year), along with our real-world protection (Whole-Product Dynamic) tests and others.

Over half of the survey participants found malware removal and performance testing to be valuable.

Surprisingly, the Whole-Product Dynamic "Real-World" Protection Test, which aims to perform an in-depth test of the security software under real-world conditions and which is promoted by the AV industry as the best type of test to reflect product capabilities, once again only comes a modest 5th in the respondents' list of requested tests.

AV-Comparatives is currently one of the leaders in providing real-world protection tests, as part of our yearly public test-series.

## 11. How often do you perform any sort of on-demand scan (e.g. a full-system scan, a scan of a removable drives or a scan of single files)?

| | |
|---|---|
| About once a week | 33.0% |
| More than once a week | 21.0% |
| About once a month | 19.9% |
| Sporadically, when I want to be sure | 19.5% |
| Never | 3.2% |
| I don't know/I assume that my product has scheduled full-system scans | 2.2% |
| I've only done it once so far | 1.3% |

Over half of respondents perform an on-demand scan at least once a week.

## 12. How often do you turn off your security product?

| | |
|---|---|
| Never | 50.9% |
| About once a month | 15.9% |
| About once a week | 11.4% |
| I've only done it once so far | 9.1% |
| More than once a week | 7.2% |
| Daily (or real-time protection always turned off) | 4.3% |
| I don't know | 1.2% |

Fortunately most users do not turn off their security product, although some users seem to do it. Some of the reasons given were to increase performance, turn off annoying messages or because they did not see it as important to have real-time protection.

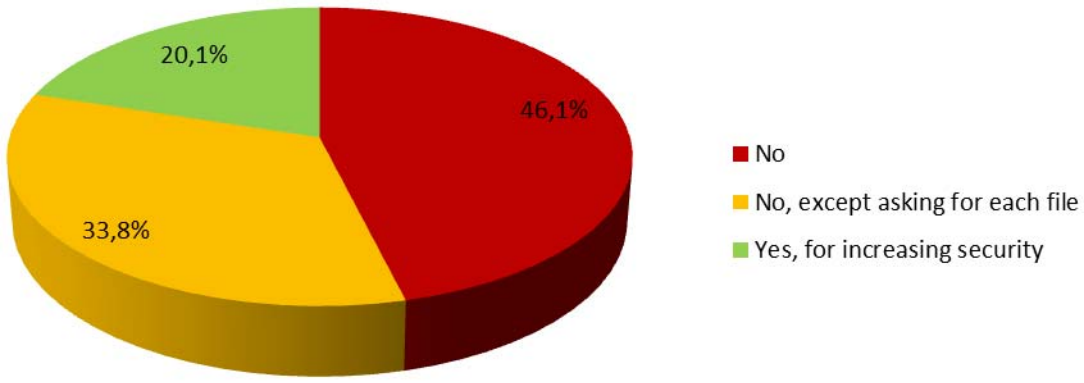
## 13. Do you usually read the EULA (End-User License Agreement) while installing a product?

| | |
|---|---|
| No, I just click on "Agree" in order to proceed with the installation | 65.5% |
| Yes, I have always a quick look over it. | 31.0% |
| Yes, I read it in full | 3.5% |

As expected, most users do not read the EULA when installing a program.

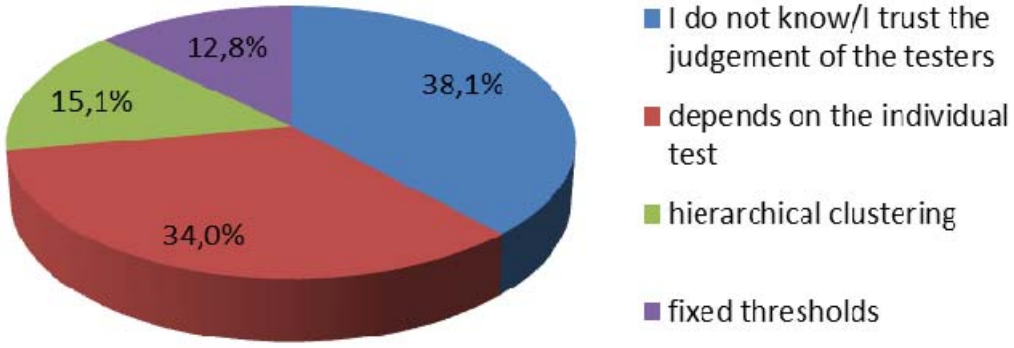
## 14. Would you use a security product which sends some of your files to the "cloud" without your knowledge and without asking for permission before sending them?

| | |
|---|---|
| No. | 46.1% |
| Only if the product asked me before sending whether I want to submit a specific file or not. | 33.8% |
| Yes, if it helps to increase the security, otherwise no. | 20.1% |




Considering that most products make use of the cloud by (amongst other things) sending files (in some cases, including personal documents), users should ask their product vendor whether the program submits "suspicious" files (which could be anything) to the cloud by default. Some products may not ask/inform the users before submitting the files, as the users have already accepted this when installing the product (as they are supposed to have read/accepted the EULA).

## 15. We use different approaches for ranking (distributing awards), e.g. fixed thresholds (for false alarm tests, heuristic tests, etc.) and hierarchical clustering (for file detection rate tests, Whole-Product Dynamic Protection tests, etc.). Which approach is better for ranking products: clustering or fixed thresholds? Which approach gives more reasonable result in your opinion?




The two most popular responses were "trust the judgement of the testers" and "depends on the individual test", with only a few respondents favouring one or other of the ranking methods. Consequently, we intend to continue using different methods for different tests.

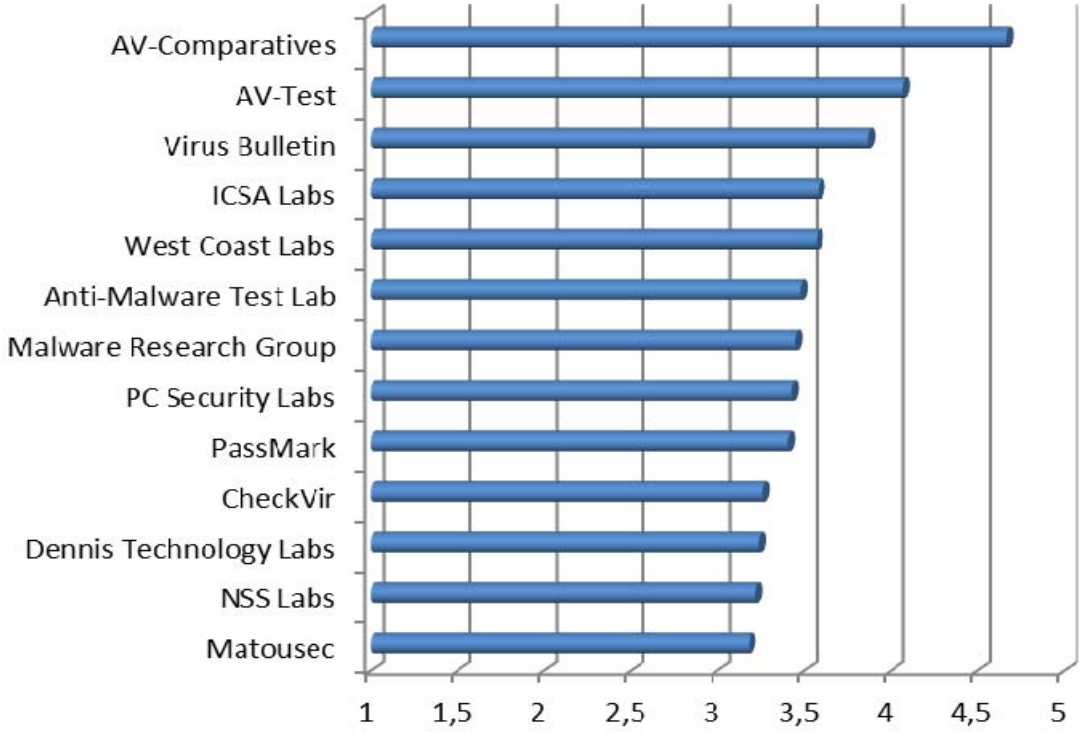
## 16. Do you usually read the whole reports we provide or do you only look at the awards or only at the percentages?

| | |
|---|---|
| I read the reports provided by AV-Comparatives in full to better understand the tests and results | 41.9% |
| I read one report for each test type in full. When another test comes out of the same type, I just look at the results/awards. | 23.7% |
| I usually look at the raw percentages/results given by AV-Comparatives | 21.5% |
| I usually look mainly only at the awards given by AV-Comparatives | 12.9% |

We were pleased to see that most of our readers don't just look at the results and awards, but read the entire reports. We feel it is important to understand the aims and methodology of a particular test so that the results can be put into context and interpreted correctly. Very often, the methodology of a particular test does not change for some time, so it's enough to read one report in full, and then just look at the results for further tests of the same type.

## 17. Please rate the quality of the tests/reports provided by the following testing labs

Users had to rate the most common/best-known security product testing labs and institutes. There are many more such bodies, but we removed the ones which according to last year's survey are unknown or considered unreliable. Survey participants were asked to rate the testing organisations from "very poor" (1) to "very good" (5). Labs with an average score of less than 3 (mediocre) are not displayed.

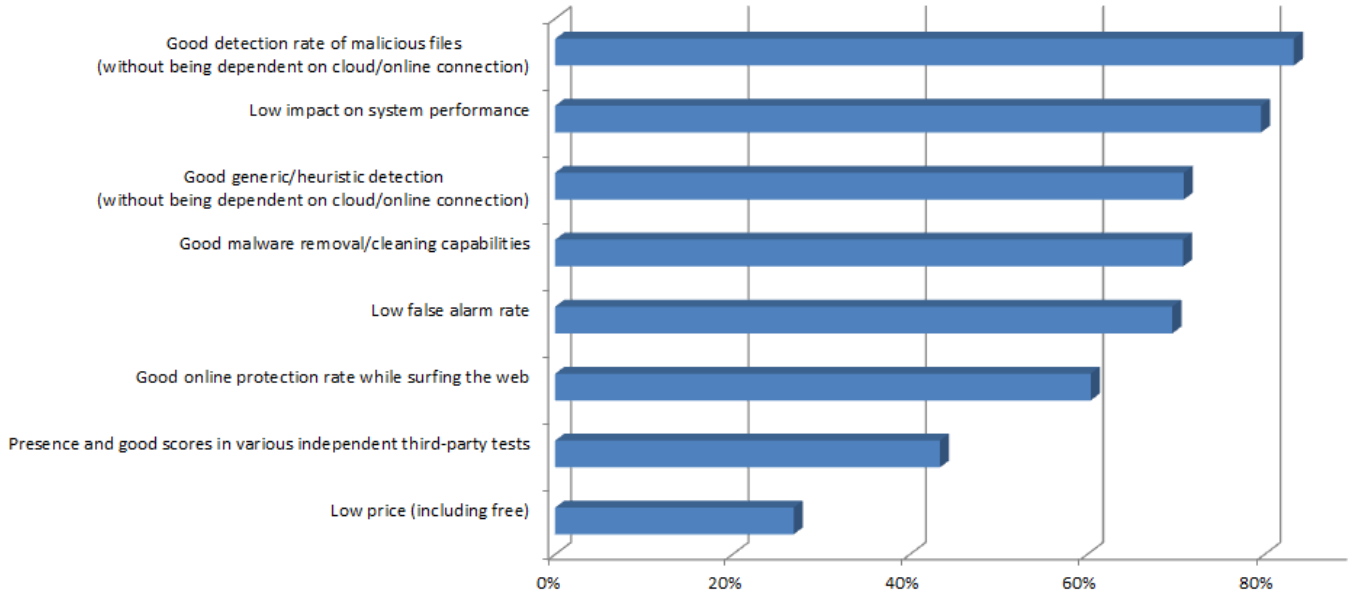



AV-Comparatives, AV-Test and Virus Bulletin are the most well-known independent testing labs.

For products which are not tested by us, we generally recommend our readers to look at the tests done by AV-Test. AV-Test also carries out a wide variety of tests, and makes the results available to the public for free. Virus Bulletin is another reliable source of information on programs that we don't test ourselves, although the tests currently carried out are largely only file detection tests. Please note that Virus Bulletin charges for access to some of its tests/detailed results.

## 18. What is important for you in a security product?

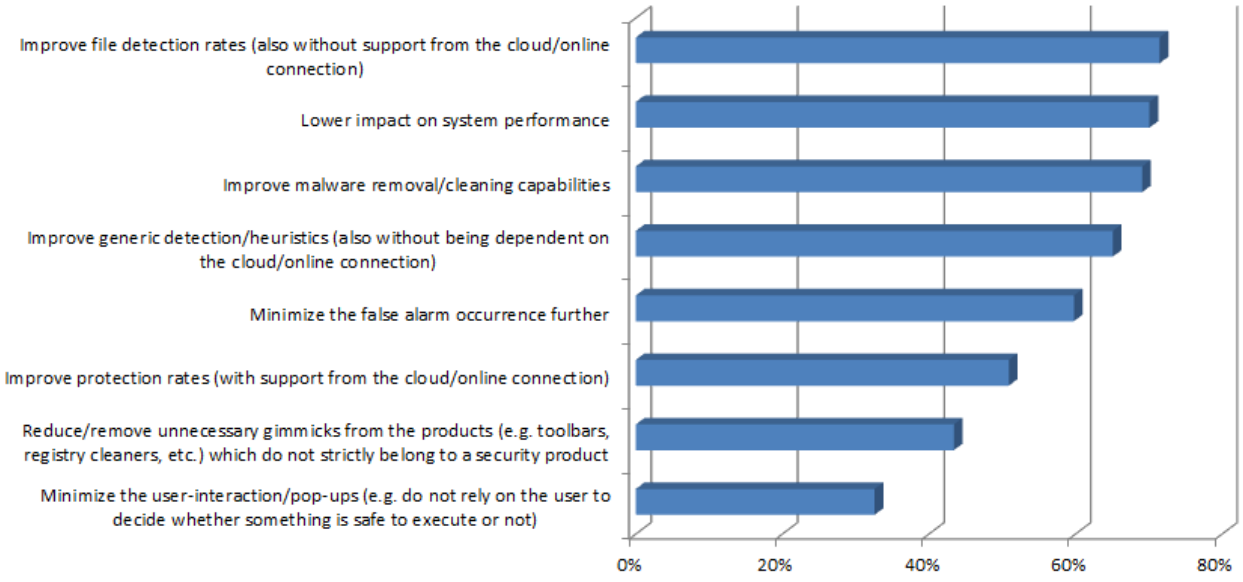
| | |
|---|---|
| Good detection rate of malicious files (without being dependent on cloud/online connection) | 83.3% |
| Low impact on system performance | 79.6% |
| Good generic/heuristic detection(without being dependent on cloud/online connection) | 70.9% |
| Good malware removal/cleaning capabilities | 70.8% |
| Low false alarm rate | 69.6% |
| Good online protection rate while surfing the web | 60.4% |
| Presence and good scores in various independent third-party tests | 43.4% |
| Low price (including free) | 26.9% |
| Respecting my privacy/no private data in the cloud | 21.8% |
| Strong default settings providing already maximum protection/detection | 20.9% |
| Ease of use/manageability | 19.2% |
| Fast on-demand scanner | 17.4% |
| Low user interaction/pop-ups from the security product | 16.9% |
| Many customizable features/options inside the product | 13.6% |
| Good/Fast support | 12.5% |




Users were asked to select six charactersistics of an anti-virus product which they considered most important to them. A majority of respondents chose the following: good detection rates of malicious files, including proactive detection, without using the cloud; minimal impact on system performance; good malware cleaning abilities; a low rate of false positives; good protection against web-based threats.

## 19. What should AV vendors try to improve more, in your opinion?

| | |
|---|---|
| Improve file detection rates (also without support from the cloud/online connection) | 71.5% |
| Lower impact on system performance | 70.1% |
| Improve malware removal/cleaning capabilities | 69.1% |
| Improve generic detection/heuristics (also without being dependent on the cloud/online connection) | 65.1% |
| Minimize the false alarm occurrence further | 59.8% |
| Improve protection rates (with support from the cloud/online connection) | 50.9% |
| Reduce/remove unnecessary gimmicks from the products (e.g. toolbars, registry cleaners, etc.) which do not strictly belong to a security product | 43.4% |
| Minimize the user-interaction/pop-ups (e.g. do not rely on the user to decide whether something is safe to execute or not) | 32.6% |
| Lower the prices of the products (or provide them for free) | 28.9% |
| Improve on-demand scanning speed | 27.3% |
| Make the default settings stronger to ensure maximum security by default | 24.6% |
| Rely less on the cloud (and do not send files from users to the cloud without explicit consent) | 24.0% |
| Make the products easier to use | 17.0% |
| Add more options/customizable features inside the product | 13.1% |
| Provide better customer support | 12.7% |




Users had to select 6 product aspects which in their opinion AV vendors should improve further. The graph above shows the 8 most selected product aspects. It may be an indication of what users *feel* to be weak aspects of the products**.** The answers largely echo the respondents' responses to the question above the most important qualities of an anti-virus program. At least half the users wanted to see better file detection rates (without using the cloud), lower impact on system performance, improved malware cleaning, better proactive detection, and fewer false alarms.

## Copyright and Disclaimer



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

AV-Comparatives (April 2012)