



Anti-Virus Protection and Performance

ANNUAL REPORT 2015

Dennis Technology Labs

www.DennisTechnologyLabs.com

Follow @DennisTechLabs on Twitter.com

CONTENTS

Annual Report 2015.....	1
Contents	2
Introduction.....	3
Executive summary	3
Protection Summary.....	4
Protection Variation over Time	5
Performance Summary	6
Malware Protection Test.....	7
1. Total Accuracy Ratings	7
2. Protection Ratings	9
3. Protection Scores	11
4. Protection Details.....	12
5. Legitimate Software Ratings	13
6. Protection Tests.....	16
7. Protection Test Details	17
Performance Impact Test.....	20
8. Performance Impact Ratings.....	20
9. Performance Test Results	22
10 Performance Test Rating Weightings.....	31
Conclusions.....	32
Appendices	34
Appendix A: Terms Used	34
Appendix B: FAQs.....	35
Appendix C: Product versions	36

Document version 1. 02. Written 15th April 2015. Edited 7th October 2015: Corrected typographical errors.
Edited 12th October: Corrected typographical errors.

INTRODUCTION

The ideal anti-virus product prevents 100 per cent of threats, never wrongly condemns a legitimate application and has no impact on the system's performance. In other words, it should keep you safe but be otherwise unnoticeable.

Some products are stronger than others in different areas and this report attempts to show how effective and impactful many popular anti-malware products were in 2014.

We have collated data from our own protection and performance tests of enterprise, small business and consumer computer security products and services. The tests were conducted regularly during the previous year (2014), starting in January and ending in December.

This report illustrates how well such products performed during that time in terms of protecting from internet threats and impacting the systems' performance.

For the protection test the products were exposed to internet threats that were live during the test period. This exposure was carried out in a realistic way, closely reflecting a potential victim's experience.

The performance test results are drawn from a range of benchmarking tests that seek to emulate realistic user behavior and demonstrate the impact that the security products make on the system.

EXECUTIVE SUMMARY

- **The effectiveness of free and paid-for anti-malware security suites varies widely.**
The most effective protected against between 97 to 100 per cent of threats, while the least effective (**Microsoft's**) was compromised by 42 per cent of the threats. For protection, the top five products were from **Kaspersky Lab**, Symantec (**Norton**), **ESET**, **Avast!** and **McAfee**.
- **Most products provided consistent levels of protection over the year.**
In most cases each product won the same set of awards every three months throughout the year. Products from **Kaspersky**, **Symantec** and **ESET** won AAA awards each time, while **Avast!** and **McAfee** won AA - AAA awards over the year. **Microsoft** failed to achieve an award in any test. **BitDefender** Internet Security and **AVG** Internet Security were the least consistent products.
- **Patching works**
Using Windows Update regularly massively increases the level of protection. Microsoft's anti-malware product plus Windows Updates achieved a 99 per cent protection rate.
- **Blocking malicious sites based on reputation is an effective approach.**
Those products that prevented users from visiting the malicious sites in the first place gained a significant advantage.
- **Some anti-malware programs are too harsh when evaluating legitimate software**
Most of the products would delegate some decisions to users when installing legitimate software. **Trend Micro's** was the most paranoid and onerous to use. Products from **Kaspersky Lab** and **Microsoft** were unobtrusive, asking no questions and not blocking a single program.
- **System performance impact**
Most performance impacts occurred when booting the systems and copying files. The least impactful products were from **Webroot**, **Malwarebytes**, **Microsoft**, **ESET**, **Kaspersky** and **Symantec**.
- **Which was the best product?**
The most accurate programs were **Kaspersky Internet Security 2015**, **Norton Security** and **ESET Smart Security 7**, all of which won our AAA award in this test.

PROTECTION SUMMARY

The following results summarize how accurately the products handled websites that served malware and legitimate software.

Awards are based on the Total Accuracy rating, which is calculated according to how each product handles both threats and legitimate software.

See *1. Total Accuracy Ratings* on page 7 for details on how the calculations are made.

The regular products win the following 2014 annual awards. Guest products are rated only for the single period during which they were tested.

Regular products

Product	Protected	Legitimate accuracy	Total Accuracy	Award
Kaspersky Internet Security	100%	100%	100%	AAA
Norton Security	99%	99%	99%	AAA
ESET Smart Security	97%	99%	96%	AAA
Avast! Free Antivirus	94%	98%	94%	AA
McAfee Internet Security	93%	96%	91%	AA
Trend Micro Titanium Internet Security	96%	92%	90%	AA
BitDefender Internet Security	89%	99%	88%	A
AVG Anti-Virus Free	82%	99%	83%	B
Microsoft Security Essentials	58%	100%	66%	-

Guest products

Product	Protected	Legitimate accuracy	Total Accuracy	Award	Test
Microsoft Security Essentials + Windows Update	99%	100%	99%	AAA	2014 Q2
F-Secure Internet Security 2014	99%	90%	92%	AA	2014 Q4
Qihoo 360 360Safe Internet Security	99%	90%	90%	AA	2014 Q3
Avira Internet Security	90%	98%	84%	B	2014 Q1
Malwarebytes Anti-Malware Free	63%	98%	67%	-	2014 Q2

The products tested in this report were the latest versions available from each vendor on the date that they were tested.

Specific 'build numbers' are available in Appendix C: Product versions on page 35.

PROTECTION VARIATION OVER TIME

The awards shown in *Protection Summary* on page 4 are based on each product's performance over the entire year, using results from the four tests conducted during that time.

As such these annual report awards represent the products' overall general effectiveness during that time.

However, the products may not have performed consistently over the year.

The results below show how they performed on a test-by-test basis and illustrate which products were most consistent and which did well during some months and less well in others.

Regular products

Product	Q1	Q2	Q3	Q4
Kaspersky Internet Security	AAA	AAA	AAA	AAA
Norton Security	AAA	AAA	AAA	AAA
ESET Smart Security	AAA	AAA	AAA	AAA
Avast! Free Antivirus	AA	AA	AAA	AA
McAfee Internet Security	AA	AA	AA	AA
Trend Micro Titanium Internet Security	AA	B	AA	AA
BitDefender Internet Security	A	AA	B	AA
AVG Internet Security	AA	C	C	A
Microsoft Security Essentials	-	-	-	-

PERFORMANCE SUMMARY

The following results summarize how much impact the different products made on systems as they performed a range of tasks.

For details on how the impact ratings are calculated see 9. Performance Test Results on page 22 and 10 Performance Test Rating Weightings on page 31.

Regular products

Product	Impact	Award
Webroot SecureAnywhere AntiVirus	0%	AAA
Malwarebytes Anti-Malware Free	0%	AAA
Microsoft Security Essentials	4%	AAA
ESET Smart Security 7	5%	AAA
Kaspersky Internet Security	7%	AAA
Symantec Norton Security	7%	AAA
Avast Free Anti-Virus	8%	AA
McAfee Internet Security	9%	AA
Trend Micro Titanium Internet Security	9%	AA
Avira Internet Security	11%	A
AVG Free	11%	A
Qihoo 360 360Safe Internet Security	12%	A
Bullguard Internet Security	13%	A
G-Data Internet Security	14%	B
F-Secure Internet Security	17%	C
BitDefender Internet Security	17%	C

MALWARE PROTECTION TEST

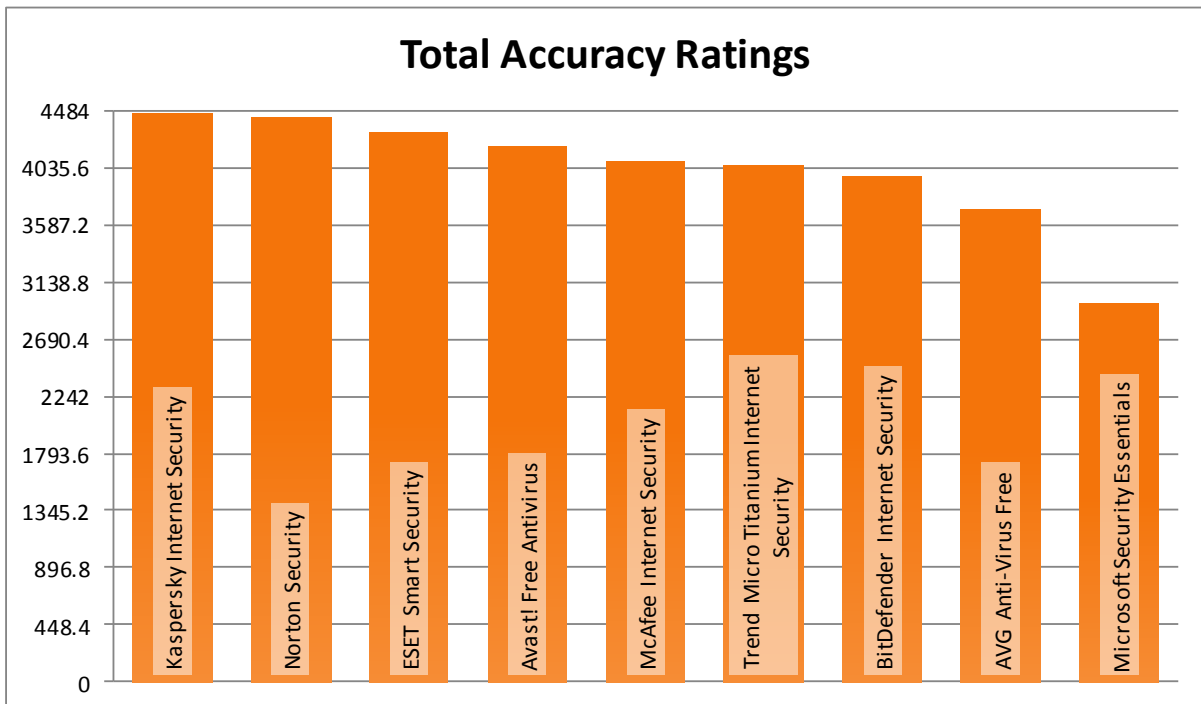
I. TOTAL ACCURACY RATINGS

The total accuracy ratings provide a way to judge how effectively the security programs work by looking at a single graph.

Anti-malware software should not just detect threats. It should allow legitimate software to run unhindered as well.

The results below take into account how accurately the programs treated threats and handled legitimate software.

Regular products



The total accuracy ratings take into account successes and failures with both malware and legitimate applications.

We ran two distinct tests: one that measured how the products handled internet threats and one that measured how they handled legitimate programs.

The ideal product would block all threats and allow all legitimate applications.

When a product fails to protect the system against a threat it is compromised. When it warns against, or even blocks, legitimate software then it generates a 'false positive' result.

Products gain points for stopping threats successfully and for allowing users to install and run legitimate software. Products lose points for

failing to stop threats and when they handle legitimate files incorrectly.

Each product then receives a final rating based on its performance in each of the 'threat' and 'legitimate software' tests.

These results show a combined accuracy rating, taking into account each product's performance with both threats and non-malicious software.

There is a maximum possible score of 4,484 and a minimum of -5,284.

See 5. *Legitimate Software Ratings* on page 13 for detailed results and an explanation on how the false positive ratings are calculated.

TOTAL ACCURACY RATINGS

Product	Total Accuracy Rating	Percentage	Award
Kaspersky Internet Security	4467	100%	AAA
Norton Security	4425.5	99%	AAA
ESET Smart Security	4311	96%	AAA
Avast! Free Antivirus	4194	94%	AA
McAfee Internet Security	4088.5	91%	AA
Trend Micro Titanium Internet Security	4049.5	90%	AA
BitDefender Internet Security	3964	88%	A
AVG Anti-Virus Free	3705	83%	B
Microsoft Security Essentials	2966	66%	-

■ Awards

The following products win Dennis Technology Labs awards for protection:



Kaspersky Internet Security
Norton Internet Security
ESET Smart Security 7



Avast! Free Antivirus
McAfee Internet Security
Trend Micro Titanium Internet Security



BitDefender Internet Security



AVG Anti-Virus Free

2. PROTECTION RATINGS

The following results show how each product was scored for its accuracy in handling malware only. They do not take into account false positives.

■ Neutralize (+1)

If the product terminated a running threat the result was a neutralization. The product protected the system and was awarded one point.

■ Neutralize, complete remediation (+2)

The product was awarded a bonus point if, in addition to stopping the malware, it removed all hazardous traces of the attack.

■ Defense (+3)

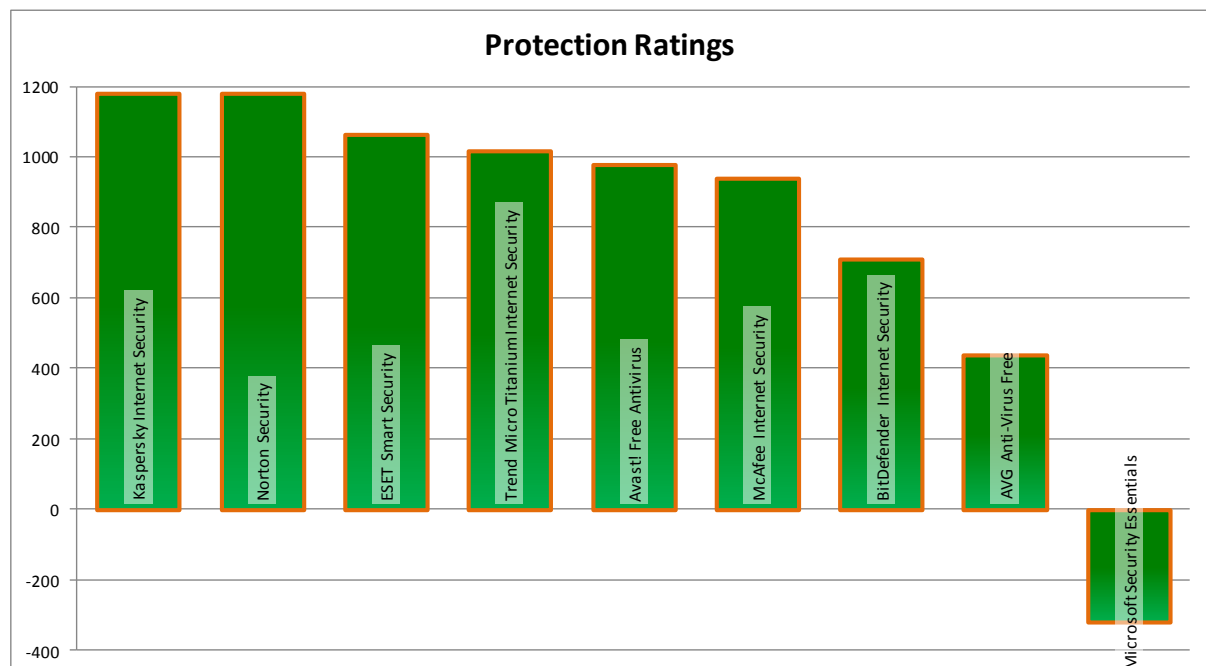
Products that prevented threats from running 'defended' the system and were awarded three points.

■ Compromise (-5)

If the threat ran uninhibited on the system, or the system was damaged, five points were deducted.

The best possible protection rating is 1,200 and the worst is -2,000.

Regular products



With protection ratings we award products extra points for completely blocking a threat, while removing points when they are compromised by a threat.

How we calculate the ratings

The protection ratings are calculated like this:

$$\begin{aligned} \text{Protection rating} = & \\ & (3 \times \text{number of defenses}) + \\ & (1 \times \text{number of neutralizations} + \\ & (1 \times \text{number of complete remediations})) + \\ & (-5 \times \text{number of compromises}) \end{aligned}$$

Note that the 'number of complete remediations' value refers only to cases of neutralization for

which full remediation was achieved. Full remediation is automatically assumed for all cases of 'defense'.

The score weighting gives credit to products that deny malware any opportunity to tamper with the system and penalizes heavily those that fail.

It is possible to apply your own weightings if you feel that compromises should be penalized more or less heavily. To do so use the results from 4. *Protection Details* on page 12.

PROTECTION RATINGS

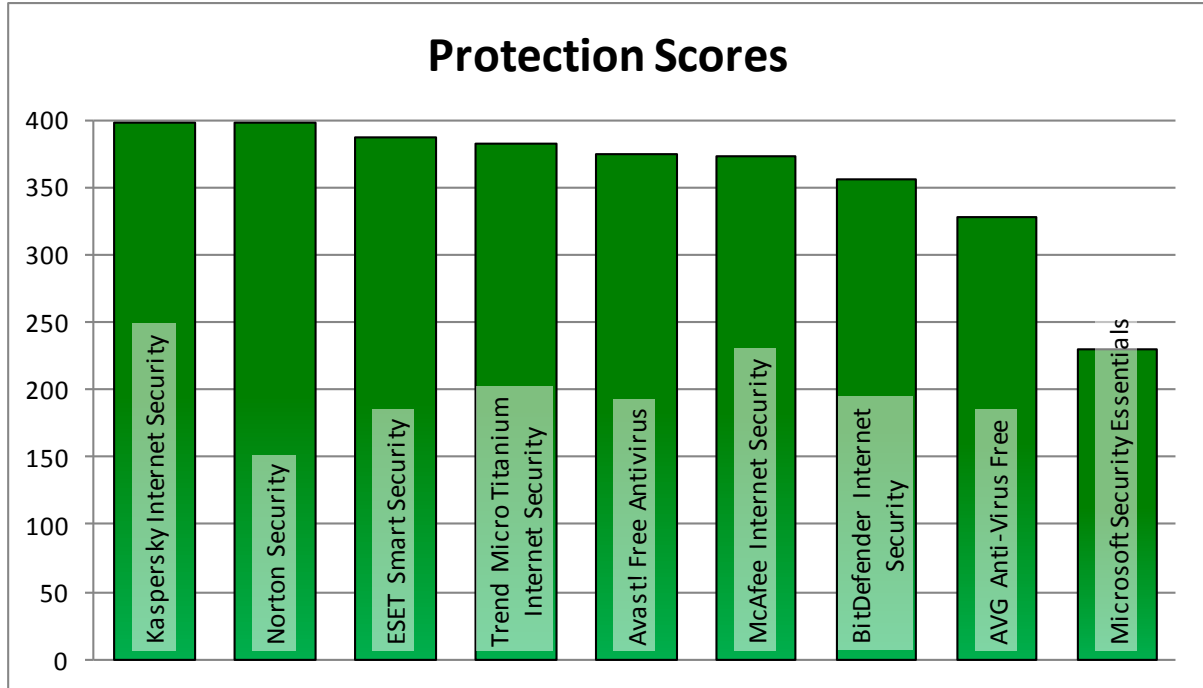
Product	Protection Rating
Kaspersky Internet Security	1183
Norton Security	1182
ESET Smart Security	1066
Trend Micro Titanium Internet Security	1018
Avast! Free Antivirus	978
McAfee Internet Security	942
BitDefender Internet Security	710
AVG Anti-Virus Free	441
Microsoft Security Essentials	-318

3. PROTECTION SCORES

The following illustrates the general level of protection, combining defended and neutralized results. There is no distinction made between

these different levels of protection. Either a system is protected or it is not.

Regular products



The protection scores simply indicate how many time each product prevented a threat from compromising the system.

PROTECTION SCORES

Product	Protected Scores	Percentage
Kaspersky Internet Security	399	100%
Norton Security	398	100%
ESET Smart Security	388	97%
Trend Micro Titanium Internet Security	383	96%
Avast! Free Antivirus	375	94%
McAfee Internet Security	373	93%
BitDefender Internet Security	356	89%
AVG Anti-Virus Free	328	82%
Microsoft Security Essentials	231	58%

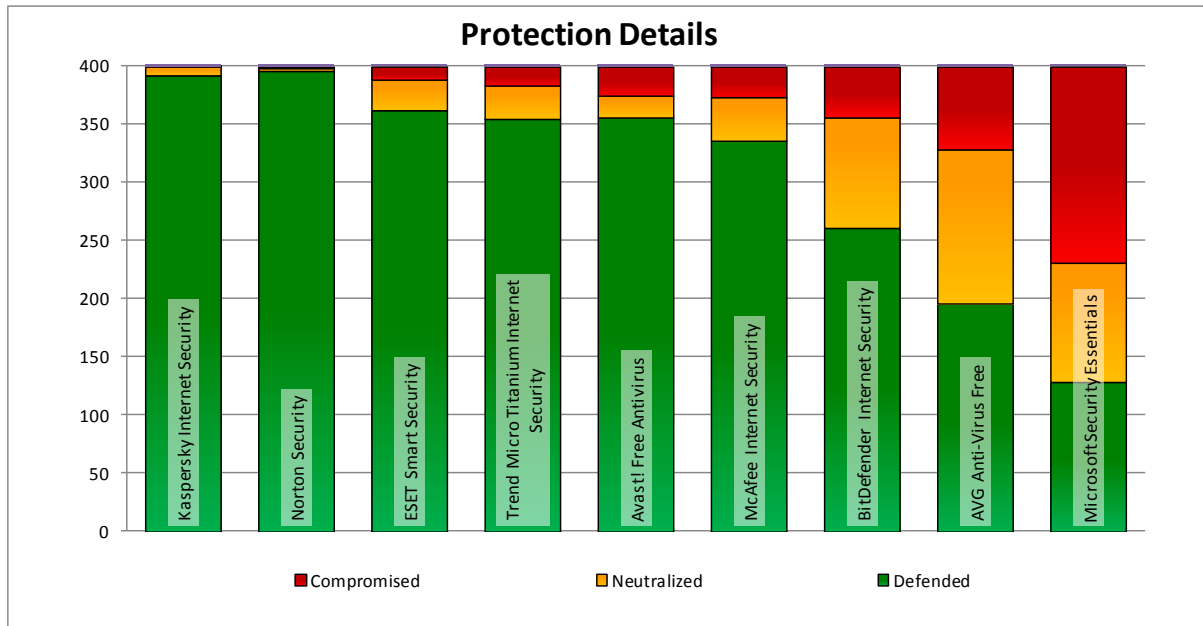
(Average: 90 per cent)

4. PROTECTION DETAILS

The security products provided different levels of protection. When a product *defended* against a threat, it prevented the malware from gaining a foothold on the target system. A threat might have

been able to exploit or infect the system and, in some cases, the product *neutralized* it either after the exploit ran or later. When it couldn't the system was *compromised*.

Regular products



The graph shows details on how the products handled the attacks. They are ordered according to their protection scores. For overall protection scores see 3. Protection Scores on page 11.

PROTECTION DETAILS

Product	Defended	Neutralized	Compromised
Kaspersky Internet Security	392	7	1
Norton Security	396	2	2
ESET Smart Security	362	26	12
Trend Micro Titanium Internet Security	354	29	17
Avast! Free Antivirus	356	19	25
McAfee Internet Security	336	37	27
BitDefender Internet Security	261	95	44
AVG Anti-Virus Free	196	132	72
Microsoft Security Essentials	128	103	169

5. LEGITIMATE SOFTWARE RATINGS

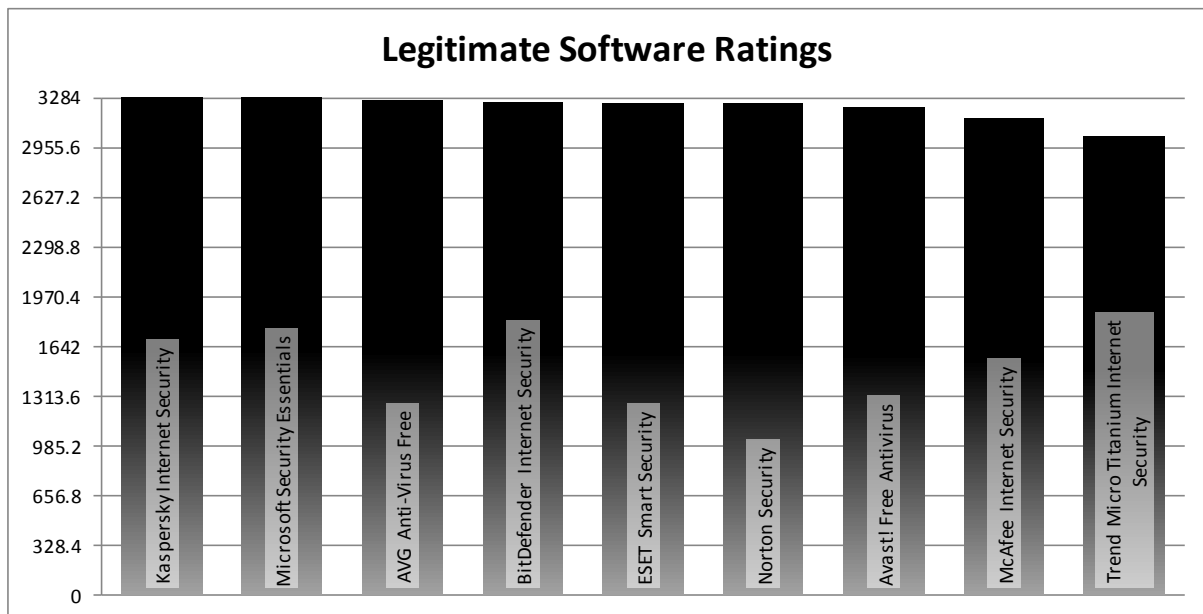
The legitimate software accuracy ratings provide a way to judge how effectively the security programs handle non-malicious software by looking at a single graph.

Anti-malware software should allow legitimate software to run unhindered. These results take

into account the level of interaction that the product demands of the user, as well as the prevalence of the legitimate program.

To understand how we calculate these ratings see 5.3 Accuracy ratings on page 15.

Regular products



When a product misclassified a popular program it faced a stronger penalty than if the file was more obscure.

LEGITIMATE SOFTWARE RATINGS

Product	Accuracy Rating
Kaspersky Internet Security	3284
Microsoft Security Essentials	3284
AVG Anti-Virus Free	3264
BitDefender Internet Security	3254
ESET Smart Security	3245
Norton Security	3243.5
Avast! Free Antivirus	3216
McAfee Internet Security	3146.5
Trend Micro Titanium Internet Security	3031.5

5.1 Interaction ratings

A security product needs to be able to protect the system from threats, while allowing legitimate software to work properly. When legitimate software is misclassified as malware a false positive is generated.

In an effort to protect the system some security products will ask the user questions when it encounters software that it is not certain is either fully legitimate or definitely malware.

When measuring how effective each product is we take into account all of the likely outcomes, whether the product allows, blocks or asks different types of questions. In each case a score is allocated.

A product gains top marks if it allows legitimate software to install without requiring the user to answer questions or otherwise interact. It loses points the more interaction is required and the less accurately it behaves.

If a product actually generates a genuine false positive (e.g. “software is malicious”) it is penalized heavily.

The results grid below shows the most likely possibilities, along with some outcomes that could only happen if a product was not working properly (e.g. A5 – Object is safe but is blocked automatically).

		Interaction					
		None (allowed)	Click to allow (default allow)	Click to allow/block (no recommendation)	Click to block (default block)	None (blocked)	
Classification	Object is safe	2	1.5	1			A
	Object is unknown	2	1	0.5	0	-0.5	B
	Object is not classified	2	0.5		-0.5	-1	C
	Object is suspicious	0.5	0	-0.5	-1	-1.5	D
	Object is unwanted	0	-0.5	-1	-1.5	-2	E
	Object is malicious				-2	-2	F
		1	2	3	4	5	

Top marks to products that are accurate; those that ask too many questions or are overly suspicious are penalized.

Consumer suites

LEGITIMATE SOFTWARE INCIDENTS

Product	Interaction	Total
Trend Micro Titanium Internet Security	None (blocked)	22
McAfee Internet Security	Click to block (default block)	5
	None (blocked)	5
Avast! Free Antivirus	None (blocked)	6
Norton Security	Click to block (default block)	2
	None (blocked)	2
ESET Smart Security	Click to block (default block)	2
	None (blocked)	1
BitDefender Internet Security	None (blocked)	1
AVG Anti-Virus Free	Click to block (default block)	1

■ 5.2 Prevalence ratings

The prevalence of each piece of software is significant. If a security product interferes with common applications then the situation is more serious than if it does so with rare ones. That said, it is usually expected that anti-malware programs should not interfere with any legitimate software.

The programs selected for the legitimate software testing were organized into five groups:

Very High Impact; High Impact; Medium Impact; Low Impact; and Very Low Impact.

The table below shows the relative importance of each group expressed as a numerical value. A Very High Impact application is ranked as being five times more significant than a Very Low Impact program.

LEGITIMATE SOFTWARE PREVALENCE RATING MODIFIERS

Impact category	Rating modifier
Very High Impact	5
High Impact	4
Medium Impact	3
Low Impact	2
Very Low Impact	1

These categories were attributed to software programs based on their individual weekly download numbers as reported by third-party download sites including Download.com at the time of testing.

Files were downloaded from their original sources, excluding third-party download sites, such as Download.com, wherever possible. This was to reduce the chances that the software had been altered in any way, perhaps having potentially unwanted add-ons included with the installer.

The presence of potentially unwanted add-ons transforms the legitimate software into a product that could be blocked or altered justifiably by anti-malware software. As such they are not suitable for this legitimate software test.

The ranges for these categories, in terms of weekly downloads, are recorded in the table Legitimate Software Prevalence Categories.

LEGITIMATE SOFTWARE PREVALENCE CATEGORIES

Impact category	Prevalence
Very High Impact	>20,000
High Impact	1,000 - 20,000
Medium Impact	100 - 999
Low Impact	25 - 99
Very Low Impact	< 25

■ 5.3 Accuracy ratings

The legitimate software accuracy ratings are calculated by multiplying together the interaction and prevalence ratings.

$$\text{accuracy rating} = \text{number of programs} \times (\text{interaction rating} \times \text{prevalence rating})$$

For example, if a product allows 10 legitimate, Medium Impact programs to install without any interference then its rating would be calculated like this:

$$\text{accuracy rating} = 10 \times (2 \times 3) = 60$$

This formula creates the impact-weighted accuracy ratings used in the graph 5. Legitimate Software Ratings on page 13.

■ 5.4 Distribution of impact categories

Products that scored highest were the most accurate when handling the legitimate applications used in the test.

The best theoretical score possible is 4,000, while the worst would be -4,000 (assuming that all applications were classified as Very High Impact).

In fact the distribution of applications in the impact categories was not restricted only to Very High Impact. The table below shows the true distribution:

LEGITIMATE SOFTWARE CATEGORY FREQUENCY

Prevalence Rating	Frequency
Very High Impact	202
High Impact	108
Medium Impact	42
Low Impact	26
Very Low Impact	22

6. PROTECTION TESTS

■ 6.1 The threats

Providing a realistic user experience was important in order to illustrate what really happens when a user encounters a threat on the internet.

For example, in these tests web-based malware was accessed by visiting an original, infected website using a web browser, and not downloaded from a CD or internal test website.

All target systems were fully exposed to the threats. This means that any exploit code was allowed to run, as were other malicious files. They were run and permitted to perform exactly as they were designed to, subject to checks made by the installed security software.

A minimum time period of five minutes was provided to allow the malware an opportunity to act.

■ 6.2 Test rounds

Tests were conducted in rounds. Each round recorded the exposure of every product to a specific threat. For example, in 'round one' each of the products was exposed to the same malicious website.

At the end of each round the test systems were completely reset to remove any possible trace of malware before the next test began.

■ 6.3 Monitoring

Close logging of the target systems was necessary to gauge the relative successes of the malware and the anti-malware software. This included recording activity such as network traffic, the creation of files and processes and changes made to important files.

■ 6.4 Levels of protection

The products displayed different levels of protection. Sometimes a product would prevent a threat from executing, or at least making any significant changes to the target system.

In other cases a threat might be able to perform some tasks on the target (such as exploiting a security vulnerability or executing a malicious program), after which the security product would intervene and remove some or all of the malware.

Finally, a threat may be able to bypass the security product and carry out its malicious tasks unhindered. It may even be able to disable the security software.

Occasionally Windows' own protection system might handle a threat while the anti-virus program ignored it. Another outcome is that the malware may crash for various reasons.

The different levels of protection provided by each product were recorded following analysis of the log files.

If malware failed to perform properly in a given incident, perhaps because of the very presence of the security product, rather than any specific defending action that the product took, the product was given the benefit of the doubt and a Defended result was recorded.

If the test system was damaged, becoming hard to use following an attempted attack, this was counted as a compromise even if the active parts of the malware had eventually been removed by the product.

■ 6.5 Types of protection

All of the products tested provided two main types of protection: real-time and on-demand. Real-time protection monitors the system constantly in an attempt to prevent a threat from gaining access.

On-demand protection is essentially a 'virus scan' that is run by the user at an arbitrary time.

The test results note each product's behavior when a threat is introduced and afterwards. The real-time protection mechanism was monitored throughout the test, while an on-demand scan was run towards the end of each test to measure how safe the product determined the system to be.

Manual scans were run only when a tester determined that malware had made an interaction with the target system. In other words, if the security product claimed to block the attack at the initial stage, and the monitoring logs supported this claim, the case was considered closed and a Defended result was recorded.

7. PROTECTION TEST DETAILS

■ 7.1 The targets

To create a fair testing environment, each product was installed on a clean Windows 7 Home Premium 64-bit target system. The operating system was updated with Service Pack 1 (SP1), although no later patches or updates were applied.

We test with Windows 7 SP1 due to the high prevalence of internet threats that work with this operating system. The prevalence of these threats suggests that there are many systems with this level of patching currently connected to the internet.

At the time of testing Windows 7 was being used heavily by consumers and businesses.

Additionally we ran one system fully patched and protected by Microsoft Security Essentials to determine the combined effect. Patching will inevitably improve the security of the system and readers are advised to keep all software updated.

According to Net Applications, Windows 7 accounted for 48 per cent of the desktop operating system market at the time of testing. It was the market leader, with Windows XP coming second (29 per cent).

Windows 8 and Windows Vista came a distant third and fifth (11 per cent and three per cent) respectively¹. Mac OS X came fourth.

A selection of legitimate but vulnerable software was pre-installed on the target systems. These posed security risks, as they contained known security issues. They included versions of Adobe Flash Player, Adobe Reader and Java.

A different security product was then installed on each system. Each product's update mechanism was used to download the latest version with the most recent definitions and other elements.

Due to the dynamic nature of the tests, which were carried out in real-time with live malicious websites, the products' update systems were allowed to run automatically and were also run manually before each test round was carried out.

¹Net Market Share (Net Applications), <http://www.netmarketshare.com/>

The products were also allowed to 'call home' should they be programmed to query databases in real-time. Some products might automatically upgrade themselves during the test. At any given time of testing, the very latest version of each program was used.

Each target systems was a physical PC, not a virtual machine, and was connected to the internet via its own virtual network (VLAN) to avoid cross-infection of malware.

■ 7.2 Threat selection

The malicious web links (URLs) used in the tests were not provided by any anti-malware vendor.

They were picked from lists generated by Dennis Technology Labs' own malicious site detection system, which uses popular search engine keywords submitted to Google. It analyses sites that are returned in the search results from a number of search engines and adds them to a database of malicious websites.

In all cases, a control system (Verification Target System - VTS) was used to confirm that the URLs linked to actively malicious sites.

Malicious URLs and files are not shared with any vendors during the testing process.

■ 7.3 Test stages

There were three main stages in each individual test:

1. Introduction
2. Observation
3. Remediation

During the *Introduction* stage, the target system was exposed to a threat. Before the threat was introduced, a snapshot was taken of the system. This created a list of Registry entries and files on the hard disk. The threat was then introduced.

Immediately after the system's exposure to the threat, the *Observation* stage is reached. During this time, which typically lasted at least 10 minutes, the tester monitored the system both visually and using a range of third-party tools.

The tester reacted to pop-ups and other prompts according to the directives described below (see *7.5 Observation and intervention* on page 18).

In the event that hostile activity to other internet users was observed, such as when spam was being sent by the target, this stage was cut short.

The *Observation* stage concluded with another system snapshot. This 'exposed' snapshot was compared to the original 'clean' snapshot and a report generated. The system was then rebooted.

The *Remediation* stage is designed to test the products' ability to clean an infected system. If it defended against the threat in the *Observation* stage then we skipped it. An on-demand scan was run on the target, after which a 'scanned' snapshot was taken. This was compared to the original 'clean' snapshot and a report was generated.

All log files, including the snapshot reports and the product's own log files, were recovered from the target.

In some cases the target may become so damaged that log recovery is considered impractical. The target was then reset to a clean state, ready for the next test.

■ 7.4 Threat introduction

Malicious websites were visited in real-time using the web browser. This risky behavior was conducted using live internet connections. URLs were typed manually into the browser.

Web-hosted malware often changes over time. Visiting the same site over a short period of time can expose systems to what appear to be a range of threats (although it may be the same threat, slightly altered to avoid detection).

Also, many infected sites will only attack a particular IP address once, which makes it hard to test more than one product against the same threat.

In order to improve the chances that each target system received the same experience from a malicious web server, we used a web replay system.

When the verification target systems visited a malicious site, the page's content, including malicious code, was downloaded, stored and loaded into the replay system. When each target system subsequently visited the site, it received exactly the same content.

The network configurations were set to allow all products unfettered access to the internet

throughout the test, regardless of the web replay systems.

■ 7.5 Observation and intervention

Throughout each test, the target system was observed both manually and in real-time. This enabled the tester to take comprehensive notes about the system's perceived behavior, as well as to compare visual alerts with the products' log entries.

At certain stages the tester was required to act as a regular user. To achieve consistency, the tester followed a policy for handling certain situations, including dealing with pop-ups displayed by products or the operating system, system crashes, invitations by malware to perform tasks and so on.

This user behavior policy included the following directives:

1. Act naively. Allow the threat a good chance to introduce itself to the target by clicking OK to malicious prompts, for example.
2. Don't be too stubborn in retrying blocked downloads. If a product warns against visiting a site, don't take further measures to visit that site.
3. Where malware is downloaded as a Zip file, or similar, extract it to the Desktop then attempt to run it. If the archive is protected by a password, and that password is known to you (e.g. it was included in the body of the original malicious email), use it.
4. Always click the default option. This applies to security product pop-ups, operating system prompts (including Windows firewall) and malware invitations to act.
5. If there is no default option, wait. Give the prompt 20 seconds to choose a course of action automatically.
6. If no action is taken automatically, choose the first option. Where options are listed vertically, choose the top one. Where options are listed horizontally, choose the left-hand one.

■ 7.6 Remediation

When a target is exposed to malware, the threat may have a number of opportunities to infect the system. The security product also has a number of

chances to protect the target. The snapshots explained in 7.3 Test stages on page 17 provided information that was used to analyze a system's final state at the end of a test.

Before, during and after each test, a 'snapshot' of the target system was taken to provide information about what had changed during the exposure to malware. For example, comparing a snapshot taken before a malicious website was visited to one taken after might highlight new entries in the Registry and new files on the hard disk.

Snapshots were also used to determine how effective a product was at removing a threat that had managed to establish itself on the target system. This analysis gives an indication as to the levels of protection that a product has provided.

These levels of protection have been recorded using three main terms: defended, neutralized, and compromised. A threat that was unable to gain a foothold on the target was *defended* against; one that was prevented from continuing its activities was *neutralized*; while a successful threat was considered to have *compromised* the target.

A defended incident occurs where no malicious activity is observed with the naked eye or third-party monitoring tools following the initial threat introduction. The snapshot report files are used to verify this happy state.

If a threat is observed to run actively on the system, but not beyond the point where an on-demand scan is run, it is considered to have been neutralized.

Comparing the snapshot reports should show that malicious files were created and Registry entries were made after the introduction. However, as long as the 'scanned' snapshot report shows that either the files have been removed or the Registry entries have been deleted, the threat has been neutralized.

The target is compromised if malware is observed to run after the on-demand scan. In some cases a product might request a further scan to complete the removal. We considered secondary scans to be acceptable, but continual scan requests may be ignored after no progress is determined.

An edited 'hosts' file or altered system file also counted as a compromise.

■ 7.7 Automatic monitoring

Logs were generated using third-party applications, as well as by the security products themselves.

Manual observation of the target system throughout its exposure to malware (and legitimate applications) provided more information about the security products' behavior.

Monitoring was performed directly on the target system and on the network.

Client-side logging

A combination of Process Explorer, Process Monitor, TcpView and Wireshark were used to monitor the target systems. Regshot was used between each testing stage to record a system snapshot.

A number of Dennis Technology Labs-created scripts were also used to provide additional system information. Each product was able to generate some level of logging itself.

Process Explorer and TcpView were run throughout the tests, providing a visual cue to the tester about possible malicious activity on the system. In addition, Wireshark's real-time output, and the display from the web proxy (see Network logging, below), indicated specific network activity such as secondary downloads.

Process Monitor also provided valuable information to help reconstruct malicious incidents.

Network logging

All target systems were connected to a live internet connection, which incorporated a transparent web proxy and a network monitoring system. All traffic to and from the internet had to pass through this system.

An HTTP replay system ensured that all target systems received the same malware as each other. It was configured to allow access to the internet so that products could download updates and communicate with any available 'in the cloud' servers.

PERFORMANCE IMPACT TEST

8. PERFORMANCE IMPACT RATINGS

The number of separate performance tests were conducted. The result of each of these tests is weighted and combined to create an overall rating.

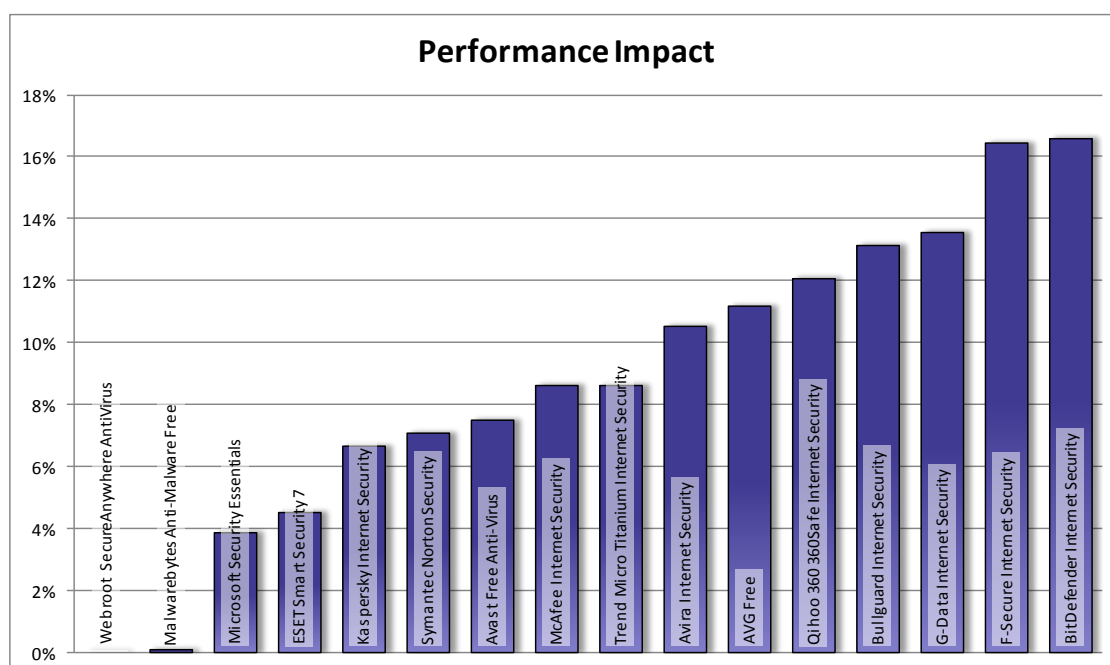
It is possible to apply your own weightings if you feel that our weights don't match your priorities or expectations of a product's behavior.

For example, we think that users really care about startup times and so the startup time ratings are given a importance weighting of 10 out of 10.

We don't believe that most people care about the speed of the initial anti-malware scan so we allocated an importance weight of two out of ten.

To see our weighting decisions, and learn how to customize the results to match your own preferences, see *10 Performance Test Rating Weightings* on page 31.

Regular products



The products to the left made the least impact on system performance.

We ran tests to measure the impact that different products made on system performance.

The ideal product would make no impact on the system or could, potentially, speed the system up, scoring an impact rating of below zero.

Awards are given to products that make low amounts of impact. Products that make less than 5.5 per cent impact achieve a AAA award. Those that create an impact of 21 per cent or more do not receive an award.

These tests included the following:

1. Software size on disk
2. System startup
3. System shutdown
4. First full scan
5. Subsequent scan time
6. Benchmark results
7. Benchmark results with full scan
8. File copying
9. Application launch times
10. Encode MP3

PERFORMANCE IMPACT RATINGS

Product	Impact	Award
Webroot SecureAnywhere AntiVirus	0%	AAA
Malwarebytes Anti-Malware Free	0%	AAA
Microsoft Security Essentials	4%	AAA
ESET Smart Security 7	5%	AAA
Kaspersky Internet Security	7%	AAA
Symantec Norton Security	7%	AAA
Avast Free Anti-Virus	8%	AA
McAfee Internet Security	9%	AA
Trend Micro Titanium Internet Security	9%	AA
Avira Internet Security	11%	A
AVG Free	11%	A
Qihoo 360 360Safe Internet Security	12%	A
Bullguard Internet Security	13%	A
G-Data Internet Security	14%	B
F-Secure Internet Security	17%	C
BitDefender Internet Security	17%	C

■ Awards

The following products win Dennis Technology Labs awards for performance:



Webroot SecureAnywhere AntiVirus
 Malwarebytes Anti-Malware Free
 Microsoft Security Essentials
 ESET Smart Security 7
 Kaspersky Internet Security
 Symantec Norton Security



Avast Free Anti-Virus
 McAfee Internet Security
 Trend Micro Titanium Internet Security



Avira Internet Security
 AVG Free
 Qihoo 360 360Safe Internet Security
 Bullguard Internet Security



G-Data Internet Security



F-Secure Internet Security
 BitDefender Internet Security

9. PERFORMANCE TEST RESULTS

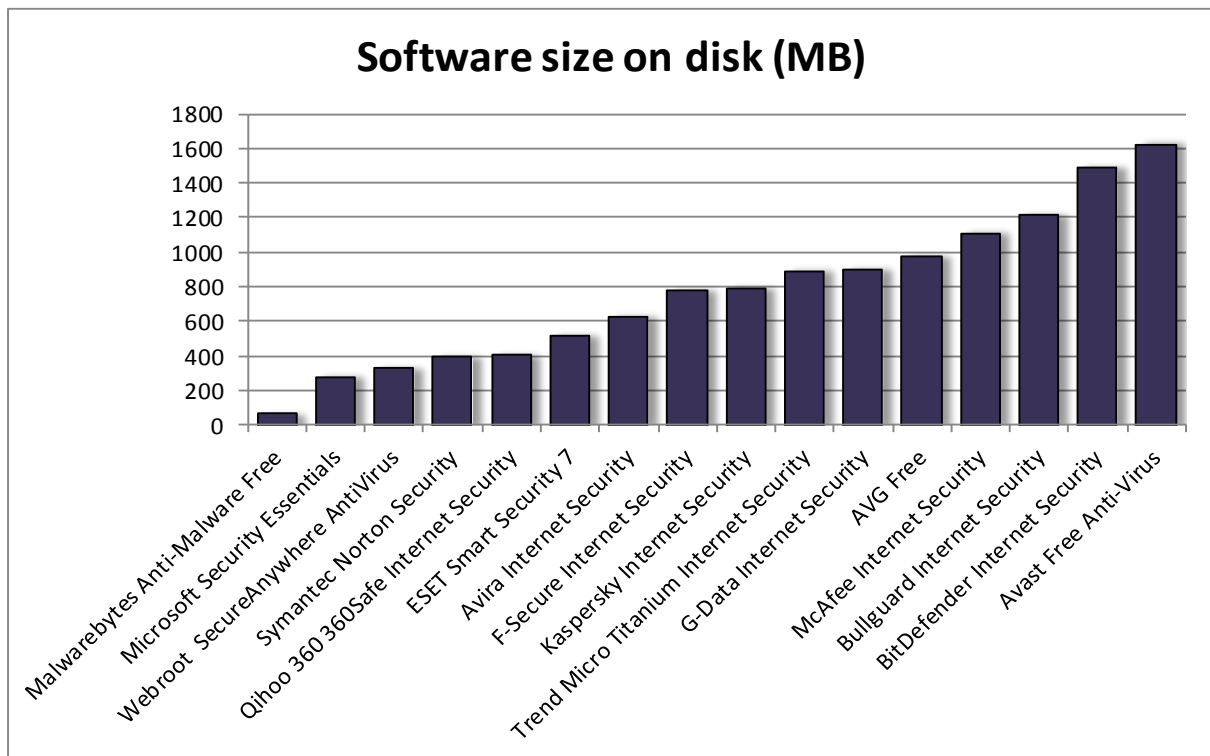
■ 9.1 Software size on disk

Windows applications may install files into different folders on the system. This test measured the disk use of each program by comparing how much disk space was free before and after its installation.

The calculation took into account various Windows features that can vary the amount of free disk space available over time.

Disk use, as presented here, is determined immediately after the products' installation and after requesting that the product update itself. As updates become available over time products may be expected to consume increasing amounts of disk space.

The frequency and amount of this consumption will vary depending on the approach taken by the different security product vendors.



The 'software size on disk' results show the amount of disk space used by each application immediately after installation

SOFTWARE SIZE ON DISK

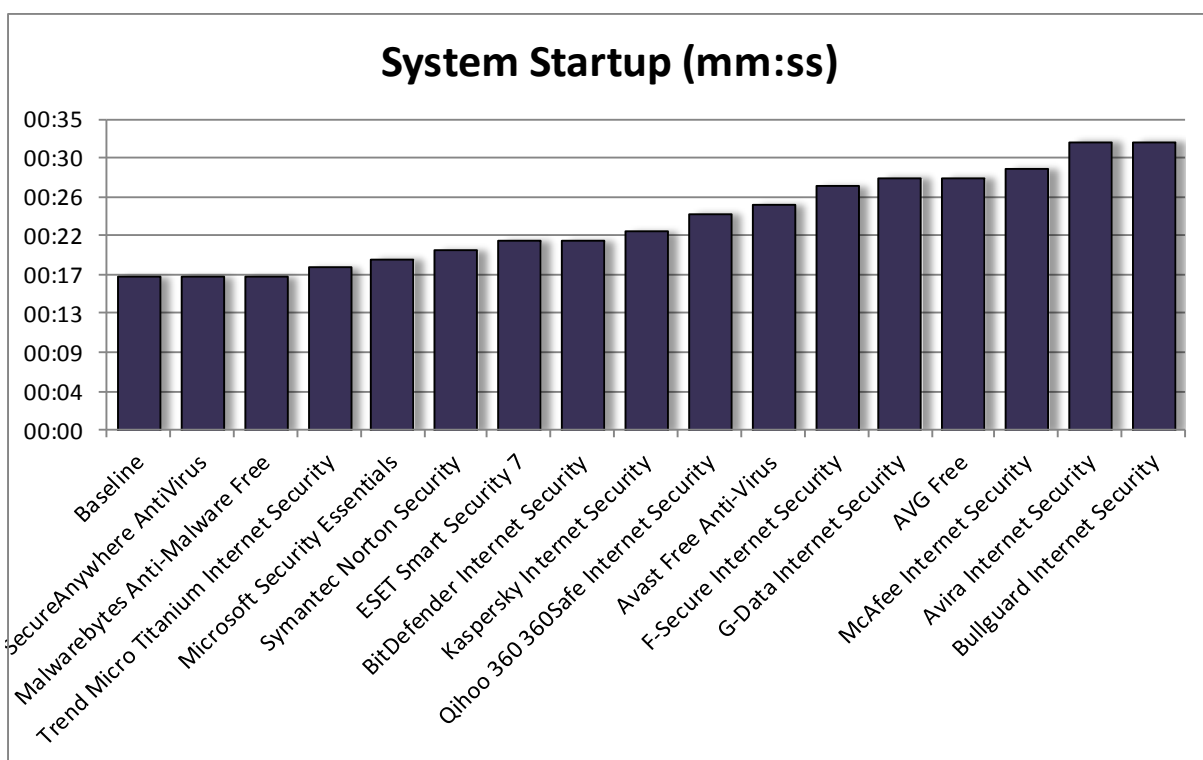
Product	Software size on disk (MB)
Malwarebytes Anti-Malware Free	61
Microsoft Security Essentials	279
Webroot SecureAnywhere AntiVirus	329
Symantec Norton Security	393
Qihoo 360 360Safe Internet Security	401
ESET Smart Security 7	515
Avira Internet Security	627
F-Secure Internet Security	779
Kaspersky Internet Security	789
Trend Micro Titanium Internet Security	891
G-Data Internet Security	899
AVG Free	973
McAfee Internet Security	1109
Bullguard Internet Security	1210
BitDefender Internet Security	1485

■ 9.2 System startup

A number of different methods were used to measure the systems' startup times. The aim was not simply to observe how quickly the system presented a Windows Desktop after being powered on.

The Desktop had to provide a usable session too.

The following figures are derived from the Microsoft Windows Performance Toolkit, which closely matched other measurements taken with third-party tools and real user experience.



The system startup test measures the time it takes to boot the PC to the point of a useable Desktop session.

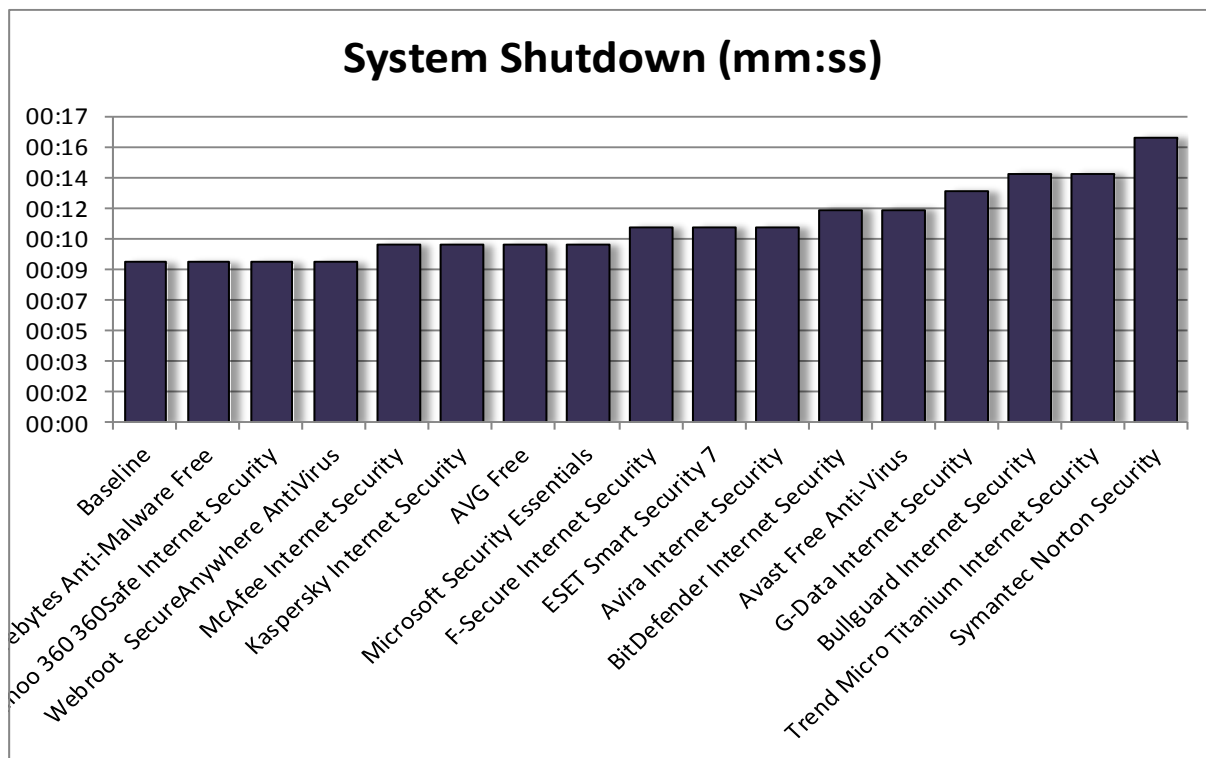
SYSTEM STARTUP

Product	System startup (mm:ss)
Baseline	00:17
Webroot SecureAnywhere AntiVirus	00:17
Malwarebytes Anti-Malware Free	00:17
Trend Micro Titanium Internet Security	00:18
Microsoft Security Essentials	00:19
Symantec Norton Security	00:20
ESET Smart Security 7	00:21
BitDefender Internet Security	00:21
Kaspersky Internet Security	00:22
Qihoo 360 360Safe Internet Security	00:24
Avast Free Anti-Virus	00:25
F-Secure Internet Security	00:27
G-Data Internet Security	00:28
AVG Free	00:28
McAfee Internet Security	00:29
Avira Internet Security	00:32
Bullguard Internet Security	00:32

■ 9.3 System shutdown

As with the startup times, a number of different methods were used to measure the systems' shutdown times.

The following figures are derived from Microsoft Windows' own internal logs, which closely matched other measurements taken with third-party tools and real user experience.



The system shutdown test times how long it takes for a PC to log the user off and power down.

SYSTEM SHUTDOWN

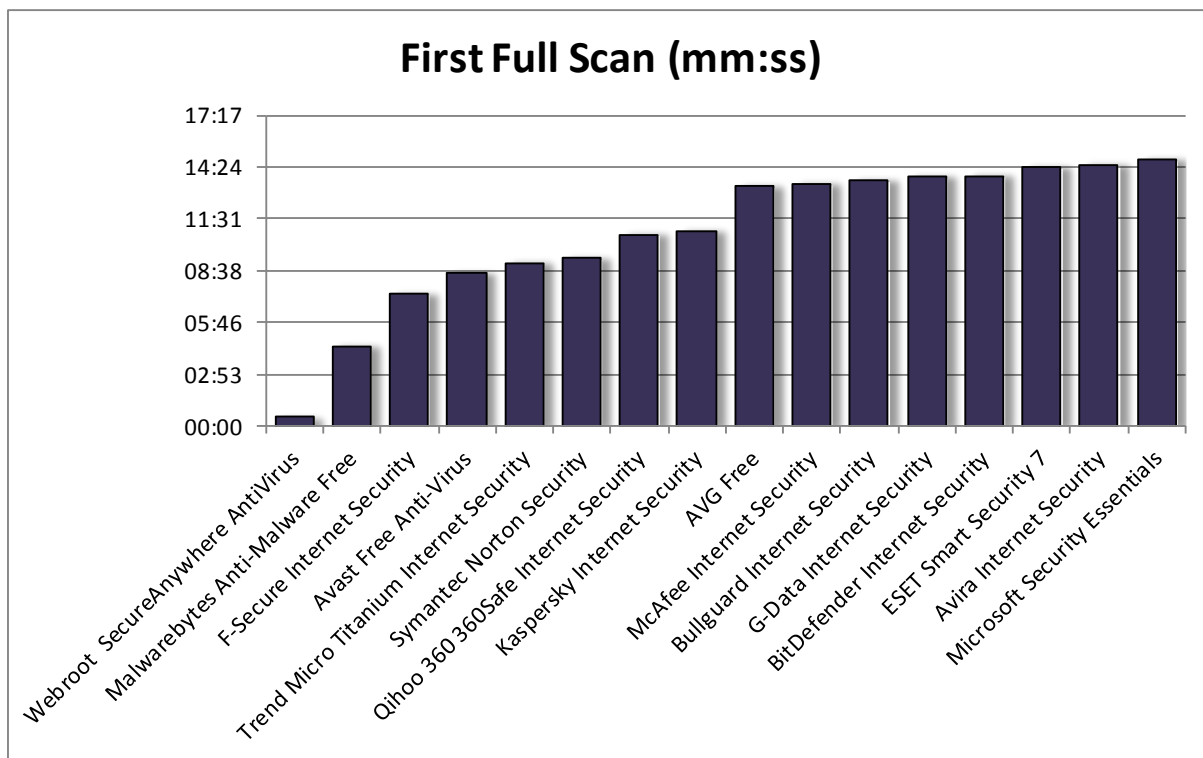
Product	System shutdown (mm:ss)
Baseline	00:09
Malwarebytes Anti-Malware Free	00:09
Qihoo 360 360Safe Internet Security	00:09
Webroot SecureAnywhere AntiVirus	00:09
McAfee Internet Security	00:10
Kaspersky Internet Security	00:10
AVG Free	00:10
Microsoft Security Essentials	00:10
F-Secure Internet Security	00:11
ESET Smart Security 7	00:11
Avira Internet Security	00:11
BitDefender Internet Security	00:12
Avast Free Anti-Virus	00:12
G-Data Internet Security	00:13
Bullguard Internet Security	00:14
Trend Micro Titanium Internet Security	00:14
Symantec Norton Security	00:16

■ 9.4 First full scan

Each product was used to scan the test systems' hard disk for malware. The systems were clean of threats.

A fast scan time does not necessarily denote an efficient and thorough scanner. Some products may scan more files than others.

This scan was started manually and recorded times do not include any scans that a product might make during its installation process.



The first full scan test times how long the initial manual malware scan takes to complete.

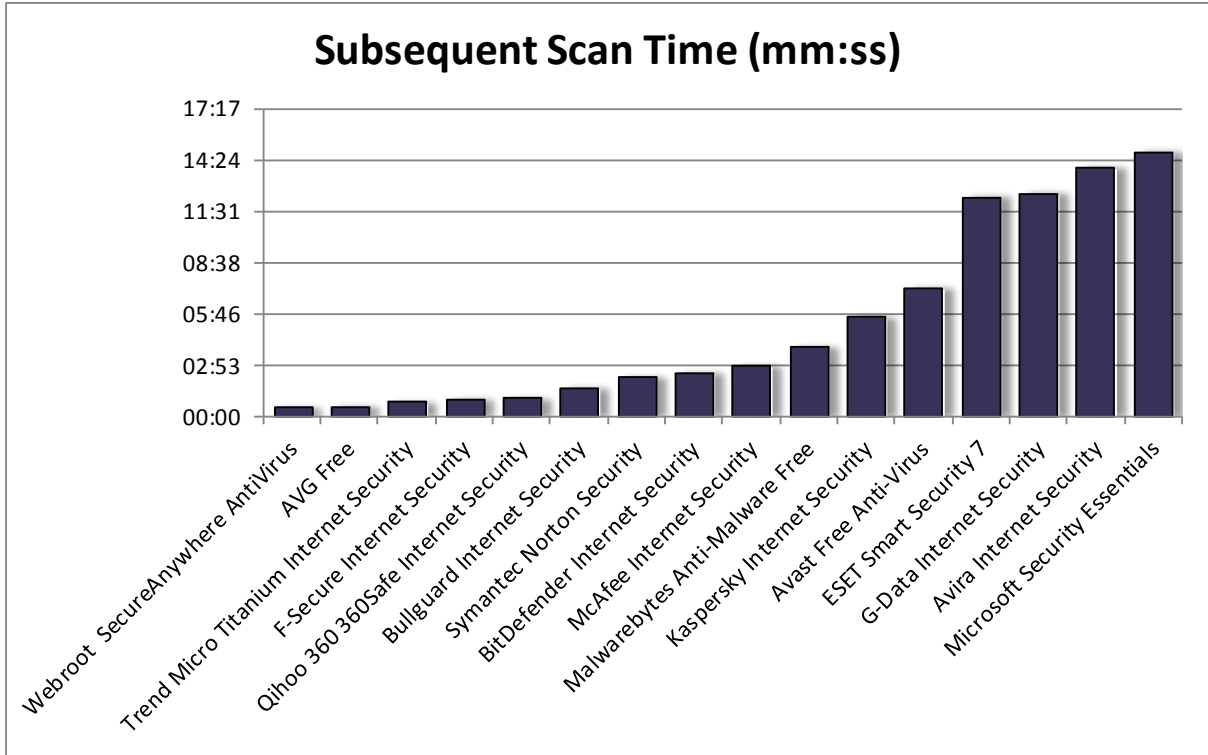
FIRST FULL SCAN

Product	First full scan time (mm:ss)
Webroot SecureAnywhere AntiVirus	00:29
Malwarebytes Anti-Malware Free	04:28
F-Secure Internet Security	07:21
Avast Free Anti-Virus	08:29
Trend Micro Titanium Internet Security	09:04
Symantec Norton Security	09:19
Qihoo 360 360Safe Internet Security	10:39
Kaspersky Internet Security	10:50
AVG Free	13:18
McAfee Internet Security	13:26
Bullguard Internet Security	13:37
G-Data Internet Security	13:50
BitDefender Internet Security	13:53
ESET Smart Security 7	14:21
Avira Internet Security	14:30
Microsoft Security Essentials	14:46

■ **9.5 Subsequent scan time**

After the initial full system scan the products were instructed to perform a series of subsequent scans. Some products optimize these later scans to run

faster than the initial scan, ignoring files already determined as being safe.



Subsequent scans may run faster than initial scans if the products don't rescan files that have already been checked.

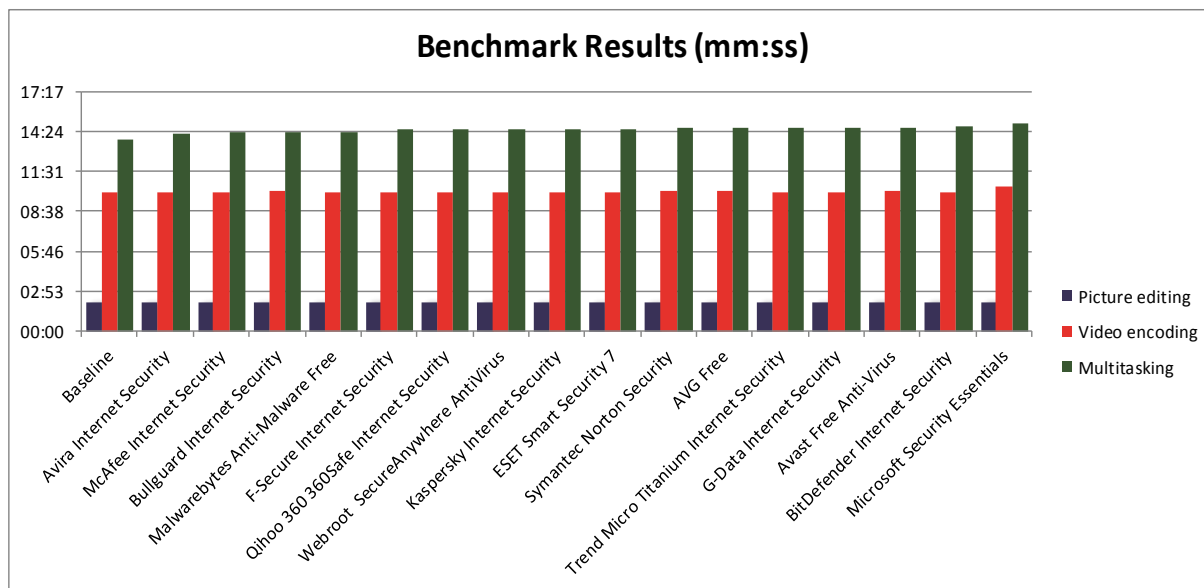
SUBSEQUENT SCAN TIME

Product	Subsequent scan time (mm:ss)
Webroot SecureAnywhere AntiVirus	00:24
AVG Free	00:29
Trend Micro Titanium Internet Security	00:43
F-Secure Internet Security	00:54
Qihoo 360 360Safe Internet Security	00:55
Bullguard Internet Security	01:32
Symantec Norton Security	02:09
BitDefender Internet Security	02:23
McAfee Internet Security	02:46
Malwarebytes Anti-Malware Free	03:50
Kaspersky Internet Security	05:30
Avast Free Anti-Virus	07:08
ESET Smart Security 7	12:16
G-Data Internet Security	12:28
Avira Internet Security	13:54

9.6 Benchmark results

Dennis Technology Labs' own PC performance benchmark suite was run on each product.

The multitasking test runs both the picture editing and video encoding tests simultaneously in order to emulate a busy computer.



The benchmark results show how much impact the security products have on a working computer's performance.

BENCHMARK RESULTS

Product	Picture editing	Video encoding	Multitasking
Baseline	02:02	10:01	13:46
Avira Internet Security	02:03	10:01	14:13
McAfee Internet Security	02:03	10:03	14:20
Bullguard Internet Security	02:03	10:04	14:20
Malwarebytes Anti-Malware Free	02:03	10:01	14:21
F-Secure Internet Security	02:05	10:01	14:30
Qihoo 360 360Safe Internet Security	02:04	10:02	14:30
Webroot SecureAnywhere AntiVirus	02:03	10:02	14:30
Kaspersky Internet Security	02:03	10:03	14:35
ESET Smart Security 7	02:03	10:02	14:35
Symantec Norton Security	02:03	10:08	14:37
AVG Free	02:03	10:09	14:39
Trend Micro Titanium Internet Security	02:04	10:02	14:39
G-Data Internet Security	02:03	10:03	14:41
Avast Free Anti-Virus	02:06	10:05	14:42
BitDefender Internet Security	02:05	10:03	14:46
Microsoft Security Essentials	02:06	10:24	14:56

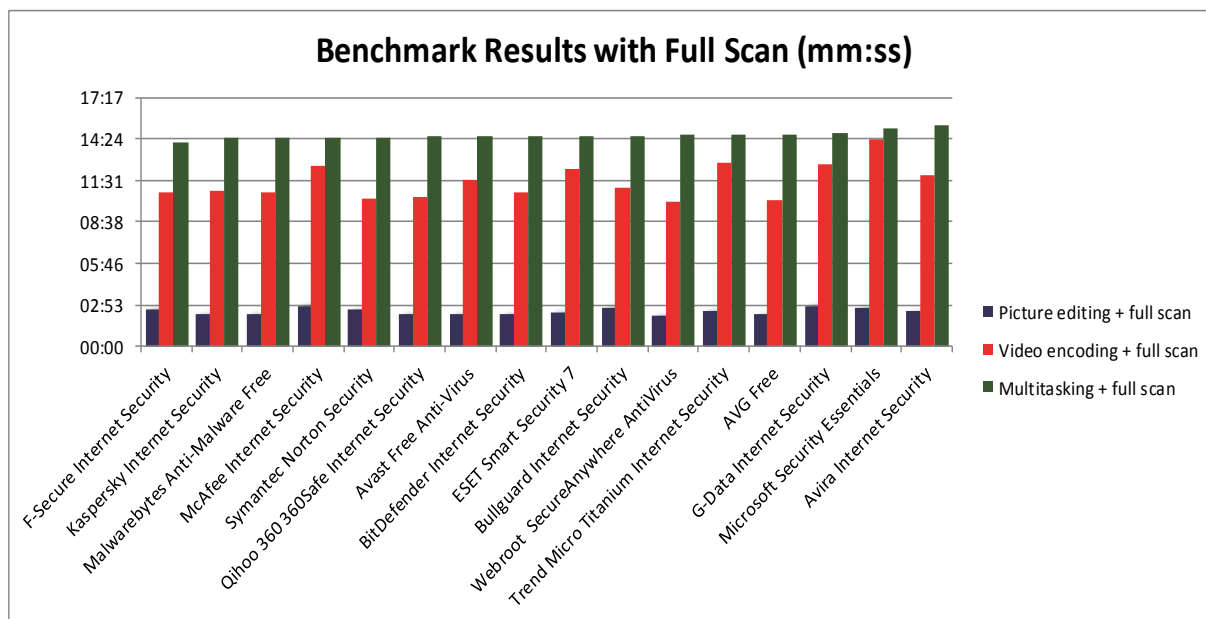
9.7 Benchmark results with full scan

This test involves running the same benchmarking software as in the 'Benchmark results' test while simultaneously running a full anti-malware scan.

Products that fail to optimise subsequent scans efficiently, as is evident with Microsoft Security Essentials, are at a notable disadvantage as the

virus scan will run throughout the course of the benchmark test, potentially slowing it down.

Products that run short scans, either due to good efficiency or electing to scan only a small number of files, should score better (with lower score values).



Running an anti-malware scan while running other tasks can have an impact on the system's performance.

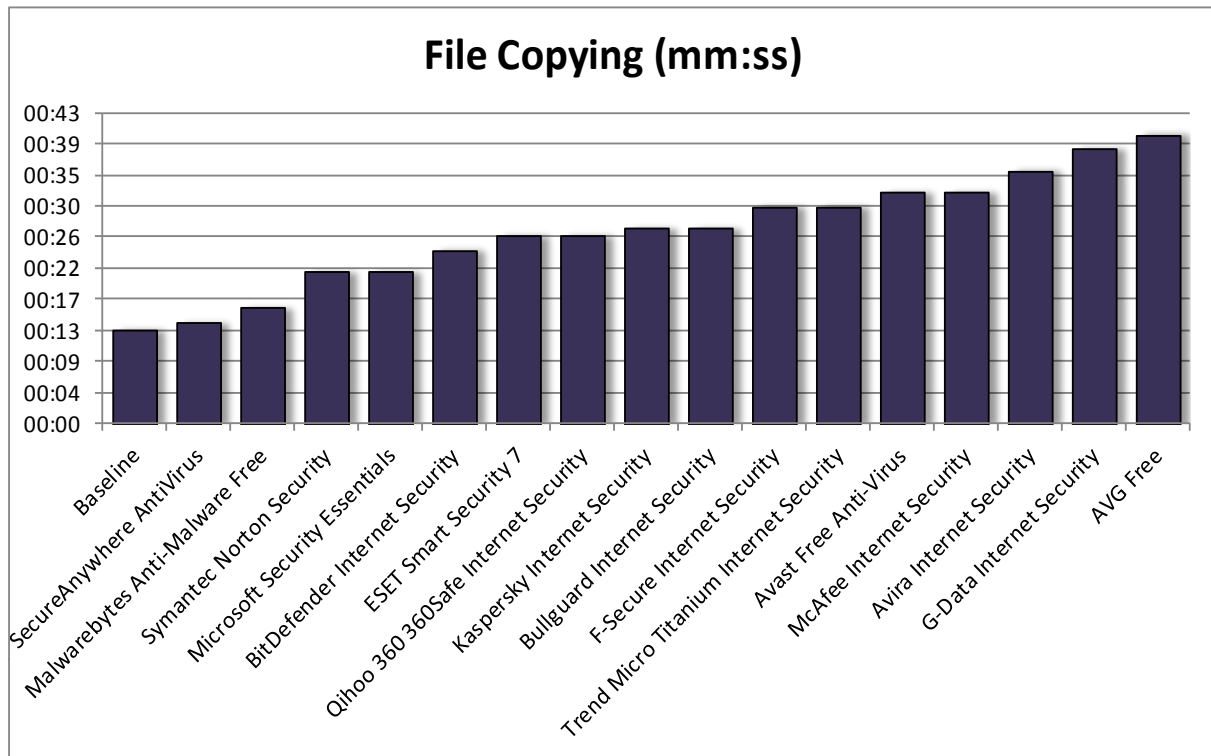
BENCHMARK RESULTS WITH FULL SCAN

Product	Picture editing + full scan	Video encoding + full scan	Multitasking + full scan
F-Secure Internet Security	02:35	10:42	14:12
Kaspersky Internet Security	02:14	10:47	14:27
Malwarebytes Anti-Malware Free	02:14	10:40	14:29
McAfee Internet Security	02:49	12:33	14:30
Symantec Norton Security	02:31	10:14	14:31
Qihoo 360 360Safe Internet Security	02:14	10:23	14:33
Avast Free Anti-Virus	02:12	11:33	14:35
BitDefender Internet Security	02:13	10:43	14:37
ESET Smart Security 7	02:21	12:21	14:37
Bullguard Internet Security	02:41	11:01	14:37
Webroot SecureAnywhere AntiVirus	02:07	10:03	14:41
Trend Micro Titanium Internet Security	02:29	12:46	14:42
AVG Free	02:11	10:07	14:44
G-Data Internet Security	02:47	12:38	14:45
Microsoft Security Essentials	02:40	14:25	15:09

■ 9.8 File copying

A large number of files were copied locally, from one folder on the hard disk to another.

The results below show how the speed of this copying process was affected by the security products installed.



Anti-malware products often scan files when they are being copied, which can slow down the process.

FILE COPYING

Product	File copy operation (mm:ss)
Baseline	00:13
Webroot SecureAnywhere AntiVirus	00:14
Malwarebytes Anti-Malware Free	00:16
Symantec Norton Security	00:21
Microsoft Security Essentials	00:21
BitDefender Internet Security	00:24
ESET Smart Security 7	00:26
Qihoo 360 360Safe Internet Security	00:26
Kaspersky Internet Security	00:27
Bullguard Internet Security	00:27
F-Secure Internet Security	00:30
Trend Micro Titanium Internet Security	00:30
Avast Free Anti-Virus	00:32
McAfee Internet Security	00:32
Avira Internet Security	00:35
G-Data Internet Security	00:38

■ 9.9 Application launch times

This test measures the time it took to launch a variety of common applications. The results as presented are average figures based on a number of launches.

Windows itself optimises application launch times so usually the first launch time of an application is longer than subsequent launches.

APPLICATION LAUNCH TIMES

Product	Internet Explorer (mm:ss)	Word (mm:ss)	Excel (mm:ss)	Acrobat (mm:ss)	Microsoft Paint (mm:ss)
Baseline	00:01	00:02	00:01	00:01	00:01
Microsoft Security Essentials	00:01	00:02	00:02	00:01	00:01
AVG Free	00:01	00:02	00:02	00:01	00:01
Avast Free Anti-Virus	00:01	00:02	00:01	00:01	00:01
BitDefender Internet Security	00:01	00:02	00:02	00:03	00:01
ESET Smart Security 7	00:01	00:02	00:01	00:01	00:01
Kaspersky Internet Security	00:01	00:02	00:02	00:01	00:01
McAfee Internet Security	00:01	00:02	00:01	00:01	00:01
Symantec Norton Security	00:01	00:02	00:01	00:01	00:01
Trend Micro Titanium Internet Security	00:01	00:02	00:02	00:01	00:01
F-Secure Internet Security	00:01	00:02	00:02	00:01	00:01
Avira Internet Security	00:01	00:02	00:01	00:01	00:01
Malwarebytes Anti-Malware Free	00:01	00:02	00:01	00:01	00:01
Webroot SecureAnywhere AntiVirus	00:01	00:02	00:01	00:01	00:01
Bullguard Internet Security	00:01	00:02	00:02	00:01	00:01
Qihoo 360 360Safe Internet Security	00:02	00:02	00:02	00:01	00:01
G-Data Internet Security	00:01	00:02	00:02	00:01	00:01

■ 9.10 Encode MP3

Each system was instructed to encode a large WAV audio file into MP3 format.

This was achieved using a scripted encoder rather than a utility with a graphical user interface.

Product	Convert WAV to MP3 (mm:ss)
Malwarebytes Anti-Malware Free	02:33
Baseline	02:33
Symantec Norton Security	02:34
Avira Internet Security	02:34
Qihoo 360 360Safe Internet Security	02:34
Webroot SecureAnywhere AntiVirus	02:34
F-Secure Internet Security	02:34
Bullguard Internet Security	02:34
Trend Micro Titanium Internet Security	02:35
AVG Free	02:35
Kaspersky Internet Security	02:35
BitDefender Internet Security	02:35
ESET Smart Security 7	02:35
G-Data Internet Security	02:35
Avast Free Anti-Virus	02:35
McAfee Internet Security	02:36
Microsoft Security Essentials	02:36

10 PERFORMANCE TEST RATING WEIGHTINGS

Each product is scored according to how much impact it makes on the system for each of the tests. This score is then weighted according to the details below.

Weighted scores are combined and expressed as a percentage of the total impact that the product has made on the system's performance. It is this final percentage upon which the report ultimately basis its verdict and awards.

The baseline system, which has no security product installed, is used to determine what constitutes 'zero impact'. Each system running a product is tested and compared to the baseline.

If the baseline system takes exactly 20 seconds to boot and another system running a product takes 40 seconds then the impact that product makes is 20 (40-20 seconds) seconds.

This impact difference is expressed as a percentage so, in the example above, the impact difference is 100%.

$$(40-20) / 20 \times 100 = 100 \text{ per cent}$$

Similarly, if a system running another product takes exactly 25 seconds to boot then the impact it makes is expressed like this:

$$(25-20) / 20 \times 100 = 25 \text{ per cent}$$

Note that the values presented in the tables of this report have been rounded up to the nearest integer, but the underlying calculations that generate the percentages are made using the floating point values stored in the test's database.

As a result, if you try to recalculate our figures using the tables presented here you will get close to, but not exactly, the same answers as we present.

The table below shows the weights applied to each individual test. Readers who do not share our opinion on which test results are most important may change the weightings to fit their own requirements and calculate a customized set of results.

You may notice that some tests, such as the scan time and 'benchmark with scan' tests are not listed. This is because these cannot be compared with the baseline system (which cannot run scans).

Additionally, it is exceptionally hard to know exactly what each product is scanning, so comparing them on scan speeds is relatively pointless. For example, the fastest might not scan any files, while the slowest might be far more thorough than most.

TEST WEIGHTING

Test	Weight
System startup (mm:ss)	10
System shutdown (mm:ss)	10
DTL Benchmarks (Picture editing)	8
DTL Benchmarks (Video encoding)	7
DTL Benchmarks (Multitasking)	5
File copy operation (mm:ss)	8
Launch time - Internet Explorer (secs)	10
Launch time - Word (secs)	10
Launch time - Excel (secs)	10
Launch time - Acrobat (secs)	10
Launch time - Microsoft Paint (secs)	10
Convert WAV to MP3 (mm:ss)	5

CONCLUSIONS

■ **Where are the threats?**

The threats used in this test were genuine, real-life threats that were infecting victims globally at the time that we tested the products.

The types of infected or malicious sites were varied, which demonstrates that effective anti-virus software is essential for those who want to use the web using a Windows PC.

Most threats installed automatically when a user visited the infected webpage. This infection was often invisible to a casual observer.

■ **Where does protection start?**

There were a significant number of compromises in this test, as well as a relatively large number of neutralizations.

The strongest products blocked the site before it was even able to deliver its payload. The weakest tended to handle the threat after it had started to interact with the target system.

■ **Sorting the wheat from the chaff**

Kaspersky Internet Security 2015 scored highest in terms of malware protection, while Norton Security took a very close second place.

Guest product F-Secure Internet Security 2014 came third, while ratings for products from Trend Micro and ESET were only slightly lower.

The Kaspersky and Symantec's product gained the highest protection ratings because they prevented all of the threats from infecting the target.

F-Secure's product came third in the protection ratings because it was compromised once and neutralized two other threats.

Products were compromised, on average, eight times. Most products were compromised fewer than five times. Of these, none were free.

The products compromised most often were BitDefender Internet Security, AVG Anti-Virus Free and Microsoft Security Essentials.

That said, Microsoft Security Essentials users who patched their systems fully at the time of testing would have experienced a level of protecting that closely rivals the front-running paid-for anti-malware applications.

Patching aside, the top three products, in terms of overall accuracy, were all paid-for products.

■ **False positives?**

Anti-malware products need to be able to distinguish between malicious and non-malicious programs. This is where some products failed to excel and F-Secure Internet Security 2014, McAfee Internet Security and Trend Micro Titanium Internet Security were the most distracting and inaccurate.

F-Secure Internet Security was the worst, blocking five legitimate applications automatically and recommending to block two more.

In contrast, products from AVG, Kaspersky Lab and Microsoft were 100 per cent accurate when handling legitimate software.

Overall, considering each product's ability to handle both malware and legitimate applications, the winners were Kaspersky Internet Security 2015, Norton Security and ESET Smart Security 7. They win AAA awards.

■ **Anti-virus is important (but not a panacea)**

This test shows that with even a relatively small sample set of 100 threats there is a significant difference in performance between the anti-virus programs. Most importantly, it illustrates this difference using real threats that attacked real computers at the time of testing.

The average protection level of the tested products is 90 per cent (see 3. *Protection Scores* on page 11). This figure is much lower than some detection results typically quoted in anti-malware marketing material.

The presence of anti-malware software can be seen to decrease the chances of a malware infection even when the only sites being visited are proven to be actively malicious. That said, only two products achieved a 100 per cent protection rate, while most of those tested mishandled legitimate software.

■ **How much disk space?**

The anti-malware products tested differed greatly in their disk space requirements. The least

demanding were products from MalwareBytes, Microsoft, Webroot, Symantec and Qihoo 360.

At the other end of the scale products from McAfee, Bullguard, BitDefender and Avast! required over 1GB.

■ **Stopping and starting**

Most products added small but relatively minor delays to the systems' boot times. Seven seconds or less was a typical difference between a system running an anti-malware product and a system without one installed.

Products from Avira and Bullguard made a notable impact on startup times, nearly doubling the time it took to reach a useable Desktop session.

Shutdown times were much less variable and no product made a significant impact, although Symantec's product added the most delay (seven seconds).

■ **Work slow-down**

Most benchmark tests illustrated that the products made relatively little impact on the systems when users were starting and running applications.

The most obvious difference came when copying files, a process almost guaranteed to push an anti-malware product into action. The most impactful products trebled the time it took to copy the files without an anti-malware product. The slowest scanners were provided by G-Data and AVG.

■ **Protection and performance**

Of the products that provided the least performance impact only three also provided excellent protection. These were from Kaspersky Lab, Symantec and ESET. They prove that providing good protection from internet threats does not necessitate heavy products that slow down the system.

APPENDICES

APPENDIX A: TERMS USED

Compromised	Malware continues to run on an infected system, even after an on-demand scan.
Defended	Malware was prevented from running on, or making changes to, the target.
False Positive	A legitimate application was incorrectly classified as being malicious.
Introduction	Test stage where a target system is exposed to a threat.
Neutralized	Malware or exploit was able to run on the target, but was then removed by the security product.
Observation	Test stage during which malware may affect the target.
On-demand (protection)	Manual 'virus' scan, run by the user at an arbitrary time.
Prompt	Questions asked by software, including malware, security products and the operating system. With security products, prompts usually appear in the form of pop-up windows. Some prompts don't ask questions but provide alerts. When these appear and disappear without a user's interaction, they are called 'toasters'.
Real-time (protection)	The 'always-on' protection offered by many security products.
Remediation	Test stage that measures a product's abilities to remove any installed threat.
Round	Test series of multiple products, exposing each target to the same threat.
Snapshot	Record of a target's file system and Registry contents.
Target	Test system exposed to threats in order to monitor the behavior of security products.
Threat	A program or other measure designed to subvert a system.
Update	Code provided by a vendor to keep its software up to date. This includes virus definitions, engine updates and operating system patches.

APPENDIX B: FAQs

- This test was unsponsored.
- The test rounds were conducted between 25th April 2014 and 11th Nov 2014 using the most up to date versions of the software available on any given day.
- All products were able to communicate with their back-end systems over the internet.
- The products selected for this test were chosen by Dennis Technology Labs.
- Samples were located and verified by Dennis Technology Labs.
- Products were exposed to threats within 24 hours of the same threats being verified. In practice there was only a delay of up to three to four hours.
- Details of the samples, including their URLs and code, were provided to partner vendors only after the test was complete.
- The sample set comprised 100 actively-malicious URLs and 100 legitimate applications and URLs.

Do participating vendors know what samples are used, before or during the test?

No. We don't even know what threats will be used until the test starts. Each day we find new ones, so it is impossible for us to give this information before the test starts. Neither do we disclose this information until the test has concluded.

What is the difference between a vendor and a partner vendor?

Partner vendors contribute financially to the test in return for a preview of the results, an opportunity to challenge results before publication and the right to use award logos in marketing material. Other participants first see the results on the day of publication and may not use award logos for any purpose.

Do you share samples with the vendors?

Partner vendors are able to download samples from us after the test is complete.

Other vendors may request a small subset of the threats that compromised their products in order for them to verify our results and further understand our methodology. The same applies to client-side logs, including the network capture files. There is a small administration fee for the provision of this service.

What is a sample?

In our tests a sample is not simply a set of malicious executable files that runs on the system. A sample is an entire replay archive that enables researchers to replicate the incident, even if the original infected website is no longer available. This means that it is possible to reproduce the attack and to determine which layer of protection it was able to bypass. Replaying the attack should, in most cases, produce the relevant executable files. If not, these are usually available in the client-side network capture (pcap) file.

APPENDIX C: PRODUCT VERSIONS

A product's update mechanism may upgrade the software to a new version automatically so the version used at the start of the test may be different to that used at the end.

Vendor	Product	Build
Avast!	Free Antivirus	2014.9.0.2021
AVG	Anti-Virus Free	2015.0.5315
BitDefender	Internet Security	18.15.0.1127
ESET	Smart Security 7	7.0.317.4
Kaspersky	Internet Security	15.0.0.463(a)
F-Secure	Internet Security 2014	2.15 build 358 until 15.10.2015, then 14.115 build 100
McAfee	Internet Security	13.6.1012
Microsoft	Security Essentials	4.6.305.0
Symantec	Norton Security	22.0.2.17
Trend Micro	Titanium Internet Security	8.0.1133

WHILE EVERY EFFORT IS MADE TO ENSURE THE ACCURACY OF THE INFORMATION PUBLISHED IN THIS DOCUMENT, NO GUARANTEE IS EXPRESSED OR IMPLIED AND DENNIS PUBLISHING LTD DOES NOT ACCEPT LIABILITY FOR ANY LOSS OR DAMAGE THAT MAY ARISE FROM ANY ERRORS OR OMISSIONS.