Tracking Anti-Malware Protection 2015

A TIME-TO-PROTECT ANTI-MALWARE COMPARISON TEST

Dennis Technology Labs
www.DennisTechnologyLabs.com
Follow @DennisTechLabs on Twitter.com

This report aims to measure how reactive anti-malware products are to new malware. It compares the effectiveness of products over a period of time, noting how quickly they adapt to protect against the latest threats.

This test compares free anti-malware products provided by well-known security companies with Symantec's latest consumer product Norton Security.

The products were repeatedly exposed to live internet threats. This exposure was carried out in a realistic way, closely reflecting a customer's experience.

These results reflect what would have happened if a user was running one of the products and visited an infected website with a clean PC each day over the period of a week.

EXECUTIVE SUMMARY

- **Products tested**

Avast! Free Antivirus	AVG AntiVirus Free 2014	Symantec Norton Security
Avira Free Antivirus	Microsoft Security Essentials	

Product names

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

Specific 'build numbers' are available for those who wish to ascertain the exact versions that were used for testing.

These are listed in Appendix C: Product versions on page 14.

- **The effectiveness of anti-malware security suites varies widely.**
  There was significant difference between the protection capabilities of the products on their first encounter with the threats. This difference narrowed considerably over time.

- **Protect by day three, or not at all.**
  If a product failed to protect against a new threat it either adapted to achieve protection by around the third day or, failing that, usually did not manage to adapt at all.

- **The results demonstrate the importance of updating anti-malware software**
  Users of anti-malware software who fail to allow their products to update will clearly miss a significant benefit in protection levels.

- **Which was the best product?**
  The most accurate program was Norton Security. The best of the free products was Avast! Free Antivirus, which came a close second.

Simon Edwards, Dennis Technology Labs, 16th September 2014

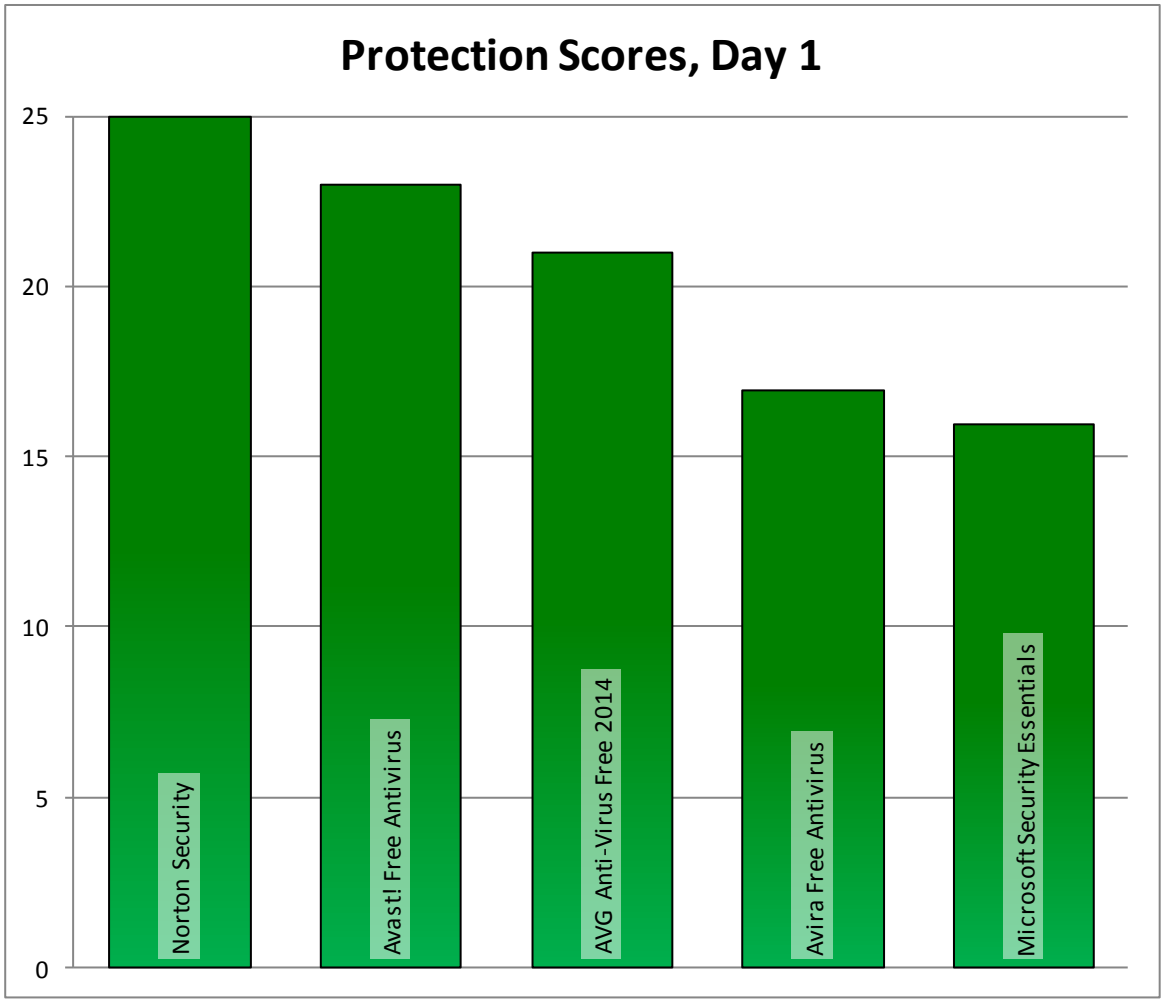
CONTENTS

Document version 1. 0. Written 16th September 2014.

1. Protection Scores, Day One

If users of these products visited each of the infected websites just once, on the first day of the test, then the levels of protection provided would look like the graph below.

These results are a sub-set of those published in the companion PC Anti-Malware Protection 2015 report[i].



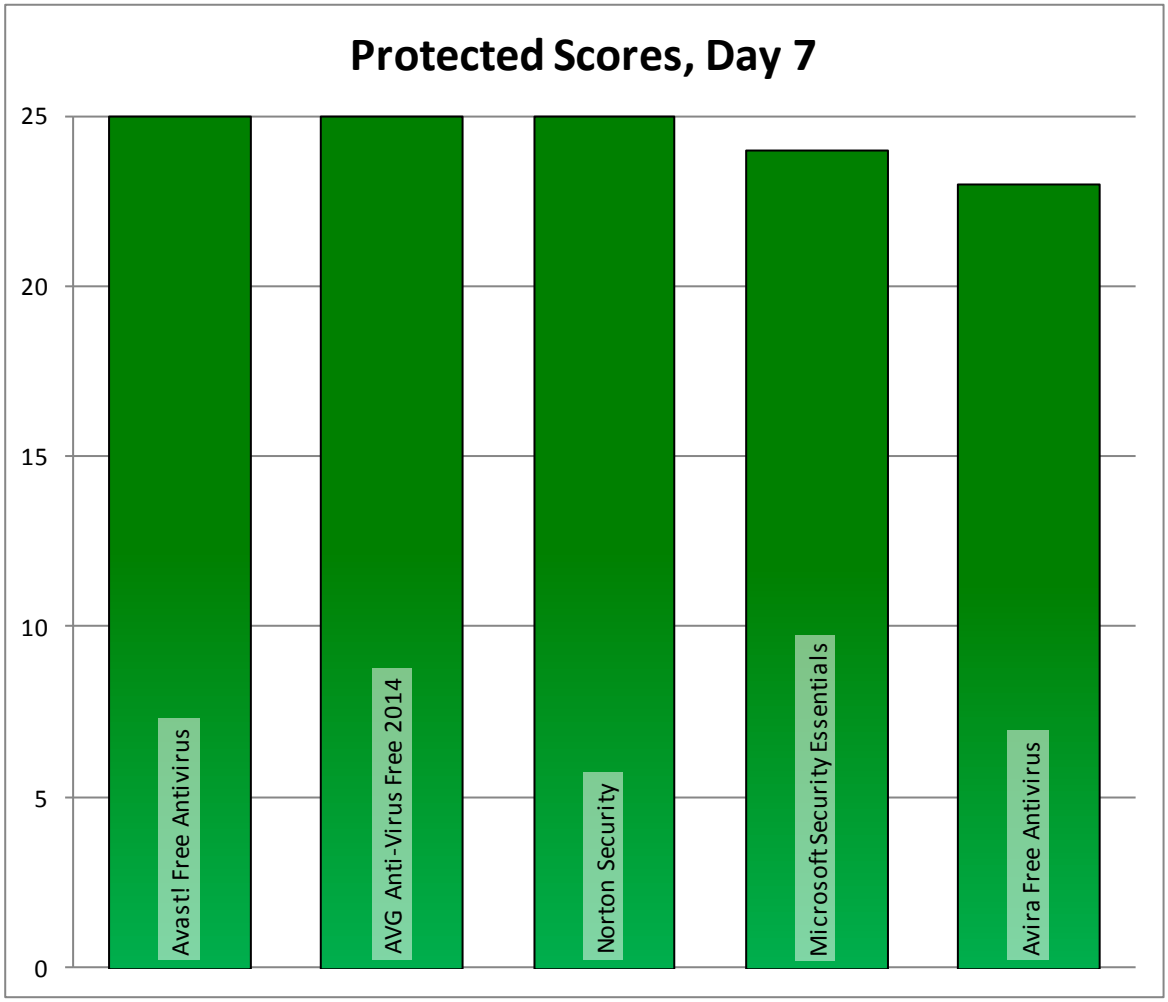
The protection scores simply indicate how many time each product prevented a threat from compromising the system.

PROTECTION SCORES

Product	Protected Scores
Norton Security	25
Avast! Free Antivirus	23
AVG Anti-Virus Free 2014	21
Avira Free Antivirus	17
Microsoft Security Essentials	16

2. PROTECTION SCORES, DAY SEVEN

If users of these products visited each of the infected websites just once, on the seventh day of the test, then the levels of protection provided would look like the graph below.



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

PROTECTION SCORES

Product	Protected Scores
Avast! Free Antivirus	25
AVG Anti-Virus Free 2014	25
Norton Security	25
Microsoft Security Essentials	24
Avira Free Antivirus	23

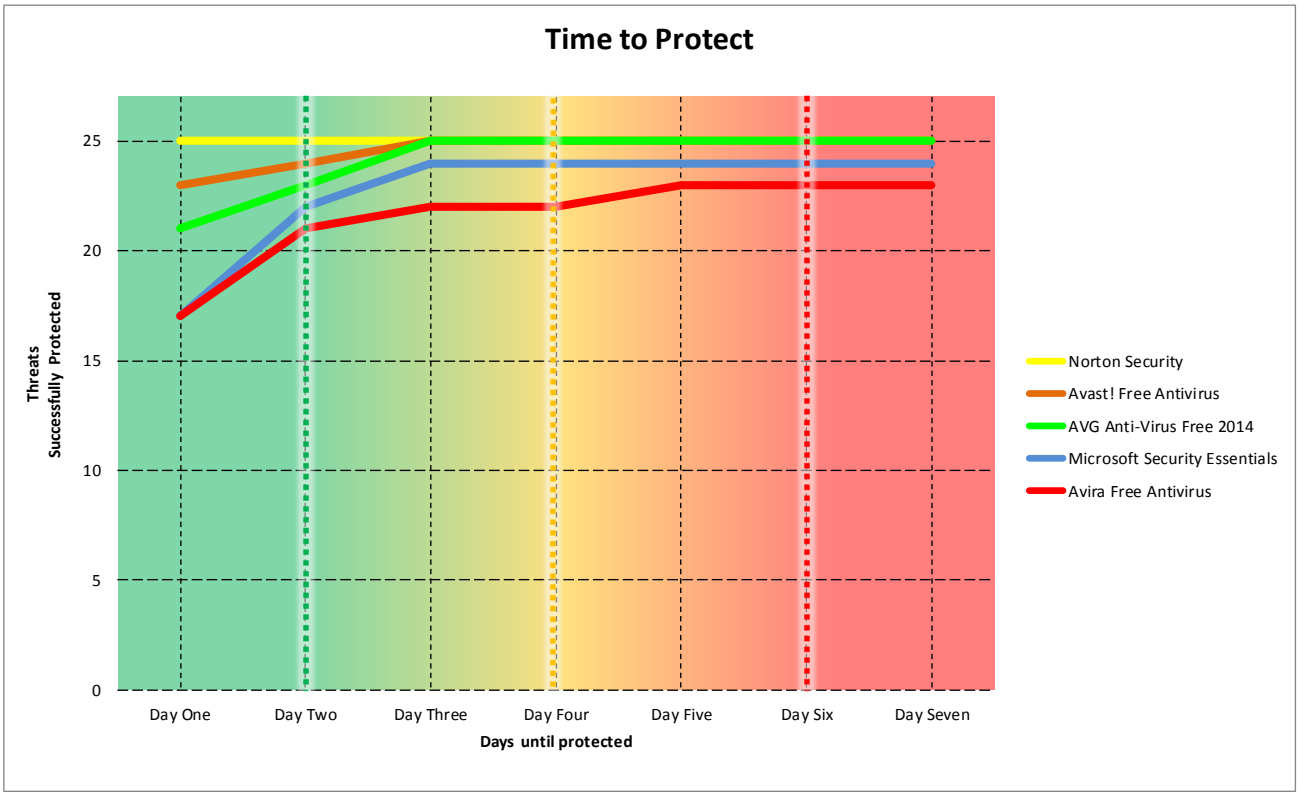
3. Protection over Time

The following graph shows the protection levels provided by each product over the period of a week.

If a product did not protect against a threat then it was re-tested the next day.

This process continued until either the product successfully protected the system or until seven days elapsed, whichever was soonest.

Clearly detecting and protecting as early as possible is the most desirable result.



The Time to Protect graph tracks the progress made by anti-malware products in detecting and protecting against new threats over time.

Days protected	Norton Security	Avast! Free Antivirus	AVG Anti-Virus Free 2014	Microsoft Security Essentials	Avira Free Antivirus
Day One	25	23	21	17	17
Day Two	25	24	23	22	21
Day Three	25	25	25	24	22
Day Four	25	25	25	24	22
Day Five	25	25	25	24	23
Day Six	25	25	25	24	23
Day Seven	25	25	25	24	23

4. The Tests

4.1 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.

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

4.2 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.

If the product failed to detect and protect against a threat it was tested again on consecutive days until it either protected against the threat or seven days elapsed, whichever was soonest.

4.3 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.

4.4 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.

4.5 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.

5. Test Details

5.1 The targets

To create a fair testing environment, each product was installed on a clean Windows 7 Professional 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.

According to Net Applications, which monitors the popularity of operating systems and web browsers, Windows 7 accounted for 48 per cent of the desktop operating system market. It was the market leader, with Windows XP coming a close second (29 per cent).

Windows 8 and Windows Vista came a distant third and fifth (11 per cent and three per cent) respectively[1]. Mac OS X came fourth.

Our aim is to test the security product and not the protection provided by keeping systems completely up to date with patches and other mechanisms. Patching will inevitably improve the security of the system and readers are advised to keep all software updated.

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.

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.

5.2 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.

5.3 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.

[1] Net Market Share (Net Applications), http://www.netmarketshare.com/

The tester reacted to pop-ups and other prompts according to the directives described below (see *5.5 Observation and intervention* below.

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.

5.4 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.

5.5 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.

5.6 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 8 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.

5.7 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.

6. 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 and end?

There were a significant number of compromises in this test on the first day.

The strongest products blocked the site before it was even able to deliver its payload. The weakest eventually adapted to handle most of the threats.

The products tended to handle new threats up to around the third day of the threat being used. After that they were much less likely to achieve new protection results.

The results show a fairly wide spread of capabilities on day one, which narrows quickly by day three.

Sorting the wheat from the chaff

Norton Security scored highest in terms of malware protection. Avast! Free Antivirus came a close second.

AVG's product failed to block four threats on the first day that it encountered them, but provided full protection by the third day, matching Avast! and Norton Security.

Microsoft Security Essentials was a little slower to catch up with the latest threats but ultimately managed to protect against all but one.

Avira Free Antivirus was much slower than the other products and was still showing improvements in protection by the fifth day. After that it failed to add any new protection and was unable to protect against two of the threats by the time the test ended.

Overall, considering each product's ability to handle malware early or within a reasonable time thereafter the strongest products are Norton Security and Avast! Free Antivirus.

Anti-virus is a service not a static product

This test shows that with even a small sample set of 25 threats there is a significant difference in performance between the anti-malware programs, not only when comparing initial detection and protection but also in the vendors' abilities to update their products to handle new threats.

For users to feel the benefit of these updates requires that they ensure their anti-malware software is up to date, which is usually an automatic process run by the security software itself.

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 sponsored by Symantec.
- The test rounds were conducted between 29th July 2014 and 13th August 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 Symantec.
- 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 Symantec only after the test was complete.
- The sample set comprised 25 actively-malicious URLs and 25 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.

Do you share samples with the vendors?

Sponsors 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 is 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
Avira	Free Antivirus	14.0.6.552
AVG	Anti-Virus Free	2014.0.4745
Microsoft	Security Essentials	4.5.216.0
Symantec	Norton Security	22:0.0.82

APPENDIX D: RELATED LINKS

[i] PC Anti-Malware Protection 2015, http://www.dennistechnologylabs.com/av-protection2015.pdf