Windows Updates vs. Web Threats

How well do Windows updates protect against malware?

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

This test explores how much additional protection anti-malware software provides to fully-patched Windows 7 PCs.

It also notes the consequences of failing to apply the very latest Windows updates.

The results show the level of benefit obtained when patching fully, when combining full patching with anti-malware software and when using anti-malware software without the patches applied.

Executive Summary

- **Updating Windows improves system security by nearly a third**

Thirty two per cent of the threats used in this test were rendered harmless by updating the Windows 7 systems fully.

- **Patching supplements, but should not replace, anti-malware protection**

Without all patches applied, the average level of protection provided by anti-malware products was 92 per cent. With patches applied this figure rose to 95 per cent.

- **Strongest anti-malware products gain least benefit from Windows updates**

Products that already scored well, without the benefit of recent Windows updates, saw minimal further advantage once these were applied. Some weaker products benefited from the extra protection provided by Windows updates.

Simon Edwards, Dennis Technology Labs, 18th February 2014

INTRODUCTION

This test explores how much additional protection anti-malware software provides to fully-patched Windows 7 PCs. It also notes the consequences of failing to apply the very latest Windows updates.

Security experts and technology journalists advise readers regularly to update their software as part of a general plan to keep their personal computers secure.

The reason for such advice is that updates often plug security holes that may be abused by attackers in order to take some level of control over a victim's system.

Updating, or 'patching', software running on a PC is one way in which to provide protection against malware-based threats. Running anti-malware software also provides protection.

How effective are security updates?

But how much additional protection do third-party anti-virus programs provide? Is it enough to simply patch PCs and steer clear of websites hosting dubious content? Or can users simply run anti-virus software and ignore Windows Updates?

This test aims to show the level of benefit obtained when patching fully, when combining full patching with anti-malware software and when using anti-malware software without the patches applied.

Related reports

Windows Updates vs. Web Threats is a companion report to an anti-malware comparison test we published late last year.

The results contained in this document are directly comparable to the *Home Anti-Virus Protection* report that we published on the 7th October 2013.

For more information about this related report please see *7. The Tests, How were the tests run?* on page 16.

Report structure

This report is split into two main sections:

Anti-malware versus updates

Results show the level of protection provided by anti-malware software without Windows Updates enabled, compared with a fully-patched system running without anti-malware software.

Anti-malware and updates

Results show the protection levels available when Windows updates are applied to all systems, with and without anti-malware protection.

CONTENTS

Document version 1.0

1. PROTECTION RATINGS (ANTI-MALWARE VS. UPDATES)

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

This set of results compares how much protection the anti-malware products provided in comparison to running a system with no protection other than that provided by installing all Windows updates.

We have included additional results for Microsoft Security Essentials on systems with and without Windows updates. All other anti-malware products are installed on systems without Windows updates

- **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 300 and the worst is -500.

How we calculate the ratings

Norton Internet Security 2014 defended against 99 of the 100 threats. It gained three points for each defense (3x99). One compromise (-5x1) reduced the rating from 297 to 292.

BitDefender's software scored much lower, although it protected the system against 94 per cent of the threats. This is because it often neutralized threats and failed to completely remediate them. It defended 80 times; neutralized threats 14 times (never with full remediation); and was compromised six times. Its score is calculated like this: (3x80) + (1x14+(0x1)) + (-5x6) = 224.

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

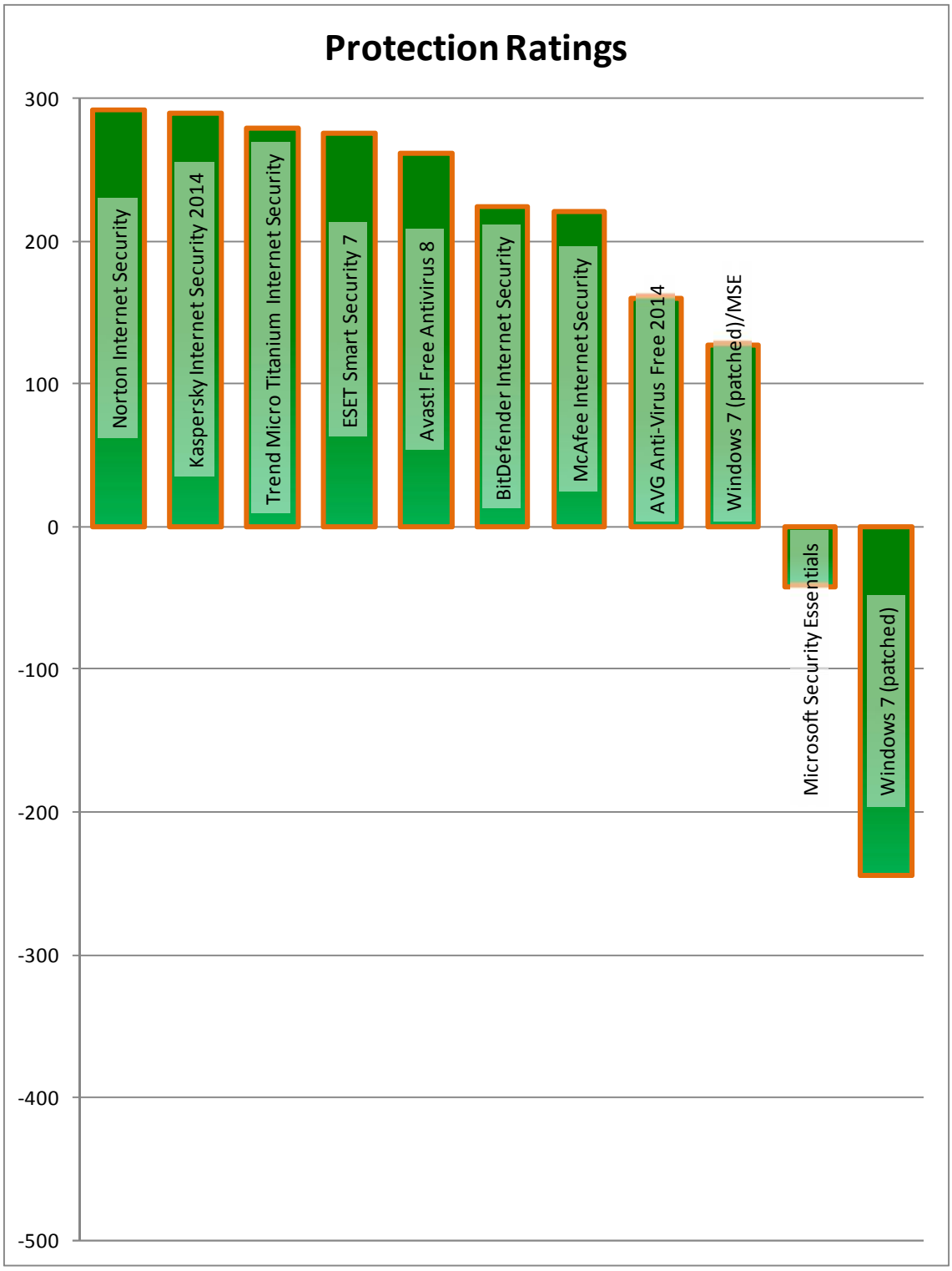
It is possible to apply your own weightings if you feel that compromises should be penalized more or less heavily.

To do so use the results from *3. Protection Details (anti-malware vs. updates)* on page 8.

PROTECTION RATINGS (ANTI-MALWARE VS. UPDATES)

Product	Protection Rating
Norton Internet Security	292
Kaspersky Internet Security 2014	290
Trend Micro Titanium Internet Security	279
ESET Smart Security 7	276
Avast! Free Antivirus 8	262
BitDefender Internet Security	224
McAfee Internet Security	221
AVG Anti-Virus Free 2014	160
Windows 7 (patched)/MSE	128
Microsoft Security Essentials	-42
Windows 7 (patched)	-244

PROTECTION RATINGS (ANTI-MALWARE VS. UPDATES)



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

2. PROTECTION SCORES (ANTI-MALWARE VS. UPDATES)

The following results illustrate the general level of protection achieved, 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.

There are no penalties for failing to stop the threat, just a lack of a score point.

The best possible protection score is 100 and the worst is zero.

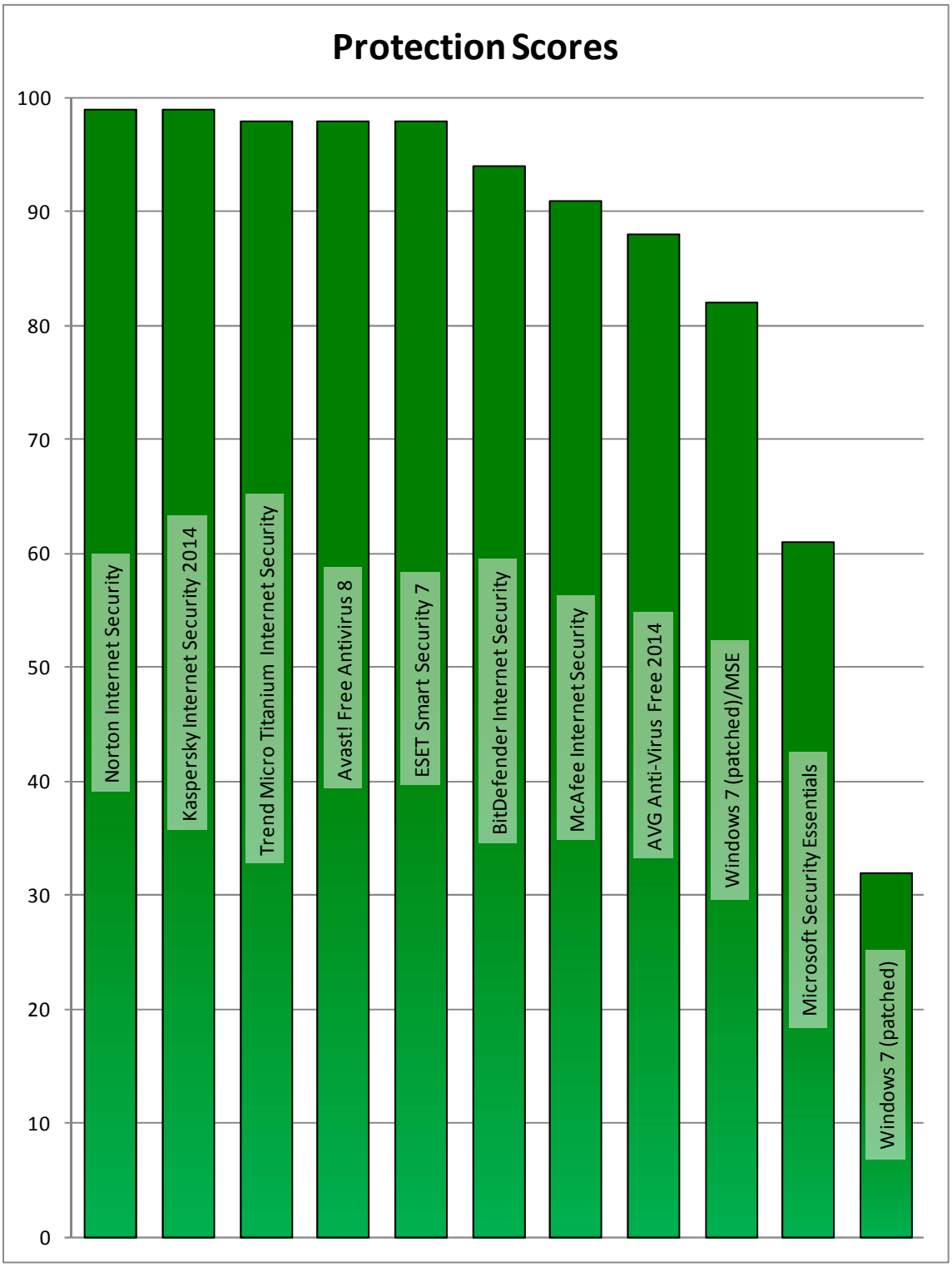
The industry average protection score in this part of the test was 92 per cent.

This figure is based on protection provided by the anti-malware products and excludes the Windows 7 (patched)/MSE and Windows 7 (patched) results shown in the table.

PROTECTION SCORES (ANTI-MALWARE VS. UPDATES)

Product	Protected Scores
Norton Internet Security	99
Kaspersky Internet Security 2014	99
Trend Micro Titanium Internet Security	98
Avast! Free Antivirus 8	98
ESET Smart Security 7	98
BitDefender Internet Security	94
McAfee Internet Security	91
AVG Anti-Virus Free 2014	88
Windows 7 (patched)/MSE	82
Microsoft Security Essentials	61
Windows 7 (patched)	32

PROTECTION SCORES (ANTI-MALWARE VS. UPDATES)



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

3. PROTECTION DETAILS (ANTI-MALWARE VS. UPDATES)

The security products provided different levels of protection.

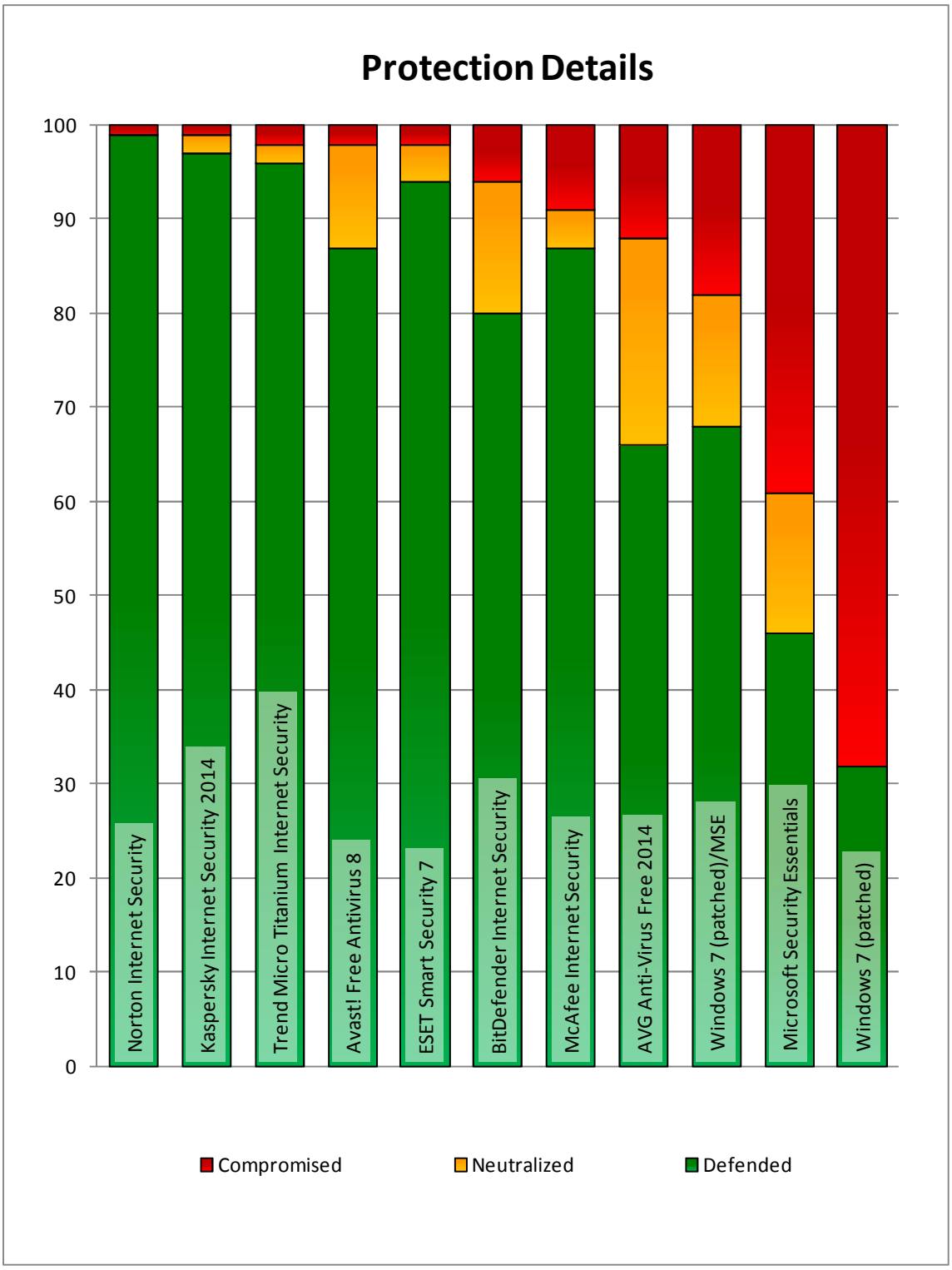
When a product *defended* against a threat, it prevented the malware from gaining a foothold on the target system. A threat might have been able to exploit or infect the system and, in some cases, the product *neutralized* it either after the exploit ran or later.

When it couldn't the system was *compromised*.

PROTECTION SCORES (ANTI-MALWARE VS. UPDATES)

Product	Defended	Neutralized	Compromised	Protected
Norton Internet Security	99	0	1	99
Kaspersky Internet Security 2014	97	2	1	99
Trend Micro Titanium Internet Security	96	2	2	98
Avast! Free Antivirus 8	87	11	2	98
ESET Smart Security 7	94	4	2	98
BitDefender Internet Security	80	14	6	94
McAfee Internet Security	87	4	9	91
AVG Anti-Virus Free 2014	66	22	12	88
Windows 7 (patched)/MSE	68	14	18	82
Microsoft Security Essentials	46	15	39	61
Windows 7 (patched)	32	0	68	32

PROTECTION SCORES (ANTI-MALWARE VS. UPDATES)



The graph shows details on how the products handled the attacks. They are ordered according to their protection scores. For overall protection scores see *2. Protection Scores (anti-malware vs. updates) on page 6*

4. PROTECTION RATINGS (ALL SYSTEMS UPDATED)

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

This set of results compares how much protection the anti-malware products provided when running on systems updated fully with Windows updates.

We have included results for 'Windows 7 (patched)' to provide a reference point that shows the protection levels provided by patching only.

- **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 300 and the worst is -500.

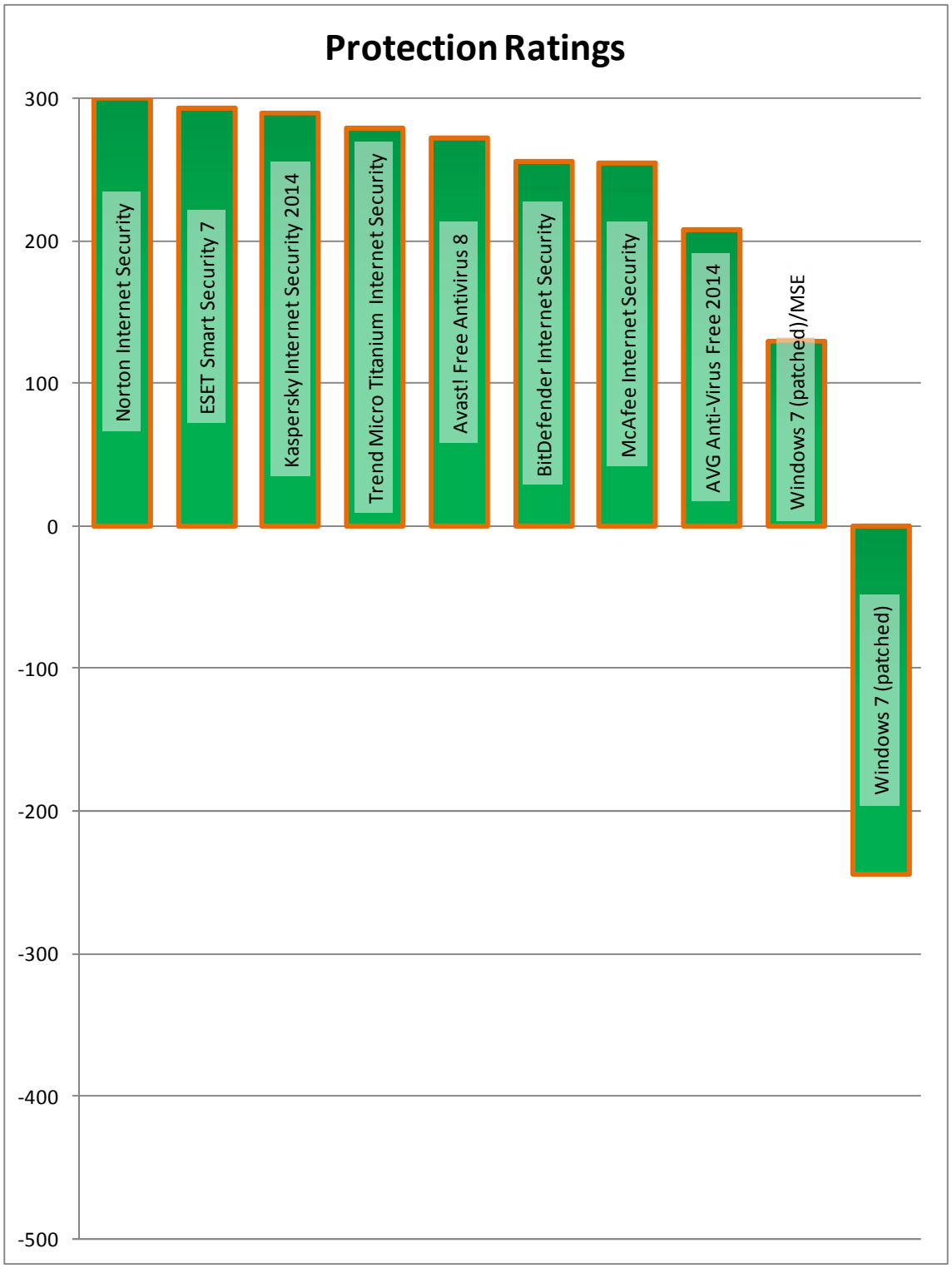
How we calculate the ratings

Please see *1. Protection Ratings (anti-malware vs. updates)* on page 4.

PROTECTION RATINGS (ALL SYSTEMS UPDATED)

Product	Protection Rating
Norton Internet Security	300
ESET Smart Security 7	294
Kaspersky Internet Security 2014	290
Trend Micro Titanium Internet Security	279
Avast! Free Antivirus 8	272
BitDefender Internet Security	256
McAfee Internet Security	255
AVG Anti-Virus Free 2014	208
Windows 7 (patched)/MSE	130
Windows 7 (patched)	-244

PROTECTION RATINGS (ALL SYSTEMS UPDATED)



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

5. PROTECTION SCORES (ALL SYSTEMS UPDATED)

The following results illustrate the general level of protection achieved, 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.

There are no penalties for failing to stop the threat, just a lack of a score point.

The best possible protection score is 100 and the worst is zero.

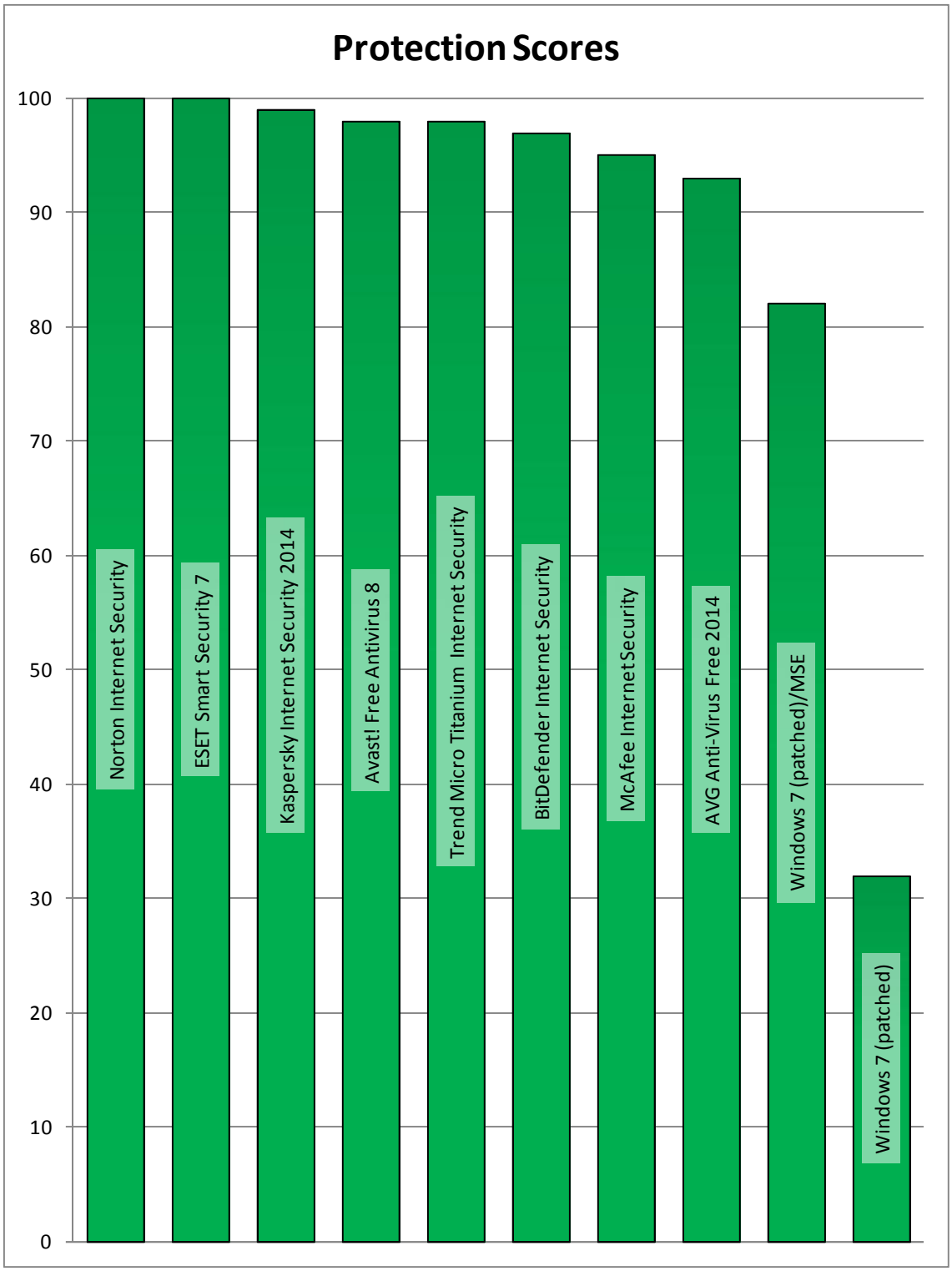
The industry average protection score in this part of the test was 96 per cent.

This figure is based on protection provided by the anti-malware products and excludes the Windows 7 (patched) results shown in the table.

PROTECTION SCORES (ALL SYSTEMS UPDATED)

Product	Protected Scores
Norton Internet Security	100
ESET Smart Security 7	100
Kaspersky Internet Security 2014	99
Avast! Free Antivirus 8	98
Trend Micro Titanium Internet Security	98
BitDefender Internet Security	97
McAfee Internet Security	95
AVG Anti-Virus Free 2014	93
Windows 7 (patched)/MSE	82
Windows 7 (patched)	32

PROTECTION SCORES (ALL SYSTEMS UPDATED)



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

6. PROTECTION DETAILS (ALL SYSTEMS UPDATED)

The security products provided different levels of protection.

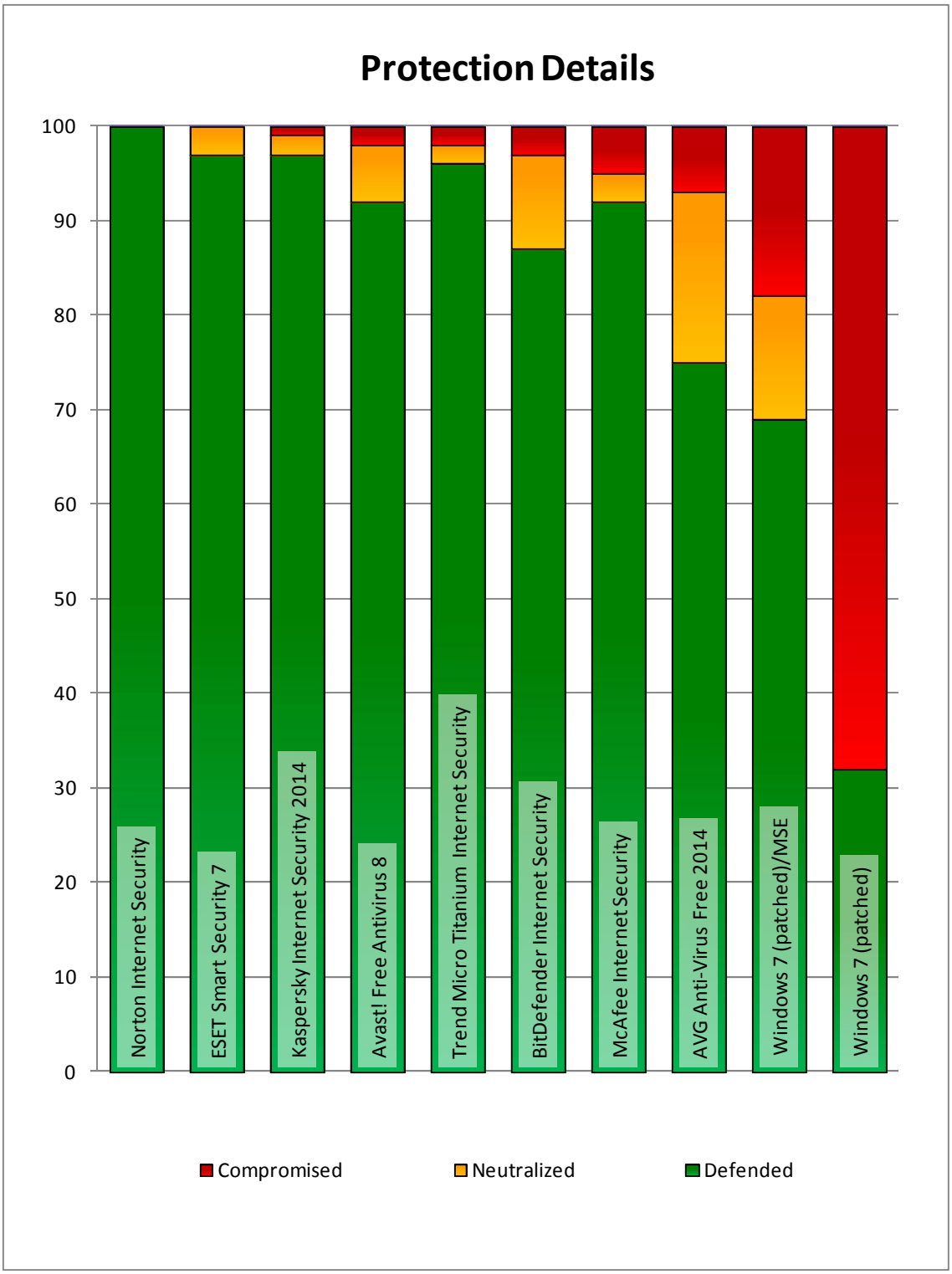
When a product *defended* against a threat, it prevented the malware from gaining a foothold on the target system. A threat might have been able to exploit or infect the system and, in some cases, the product *neutralized* it either after the exploit ran or later.

When it couldn't the system was *compromised*.

PROTECTION DETAILS (ALL SYSTEMS UPDATED)

Product	Defended	Neutralized	Compromised	Protected
Norton Internet Security	100	0	0	100
ESET Smart Security 7	97	3	0	100
Kaspersky Internet Security 2014	97	2	1	99
Avast! Free Antivirus 8	92	6	2	98
Trend Micro Titanium Internet Security	96	2	2	98
BitDefender Internet Security	87	10	3	97
McAfee Internet Security	92	3	5	95
AVG Anti-Virus Free 2014	75	18	7	93
Windows 7 (patched)/MSE	69	13	18	82
Windows 7 (patched)	32	0	68	32

PROTECTION DETAILS (ALL SYSTEMS UPDATED)



The graph shows details on how the products handled the attacks. They are ordered according to their protection scores. For overall protection scores see *5. Protection Scores (all systems updated) on page 12*.

7. THE TESTS

How were the tests run?

In this test each target system ran Windows 7 Home Premium SP1. Testers ran Windows Update each day before exposing the targets to live web threats. These threats may or may not rely on security holes present in the operating system.

The test's methodology is nearly identical to that used in our *Home Anti-Virus Protection, October – December 2013*[1] test.

The above report includes full details of how the test was run, testing policies, tools used and a definition of terms.

The only differences between the reports are the inclusion of additional patching beyond Service Pack 1 and the lack of legitimate software testing in this report. The latter was omitted because we considered it extremely unlikely that patching would block legitimate software.

What were the threats?

Anti-malware products classify malware using different systems and naming conventions. Some give very specific labels to threats, while others apply more general labels to the same threats.

For example, in this test Norton Internet Security labelled one attack, "Web Attack: Neutrino Exploit Kit website" while AVG Anti Virus Free 2014 identified it simply as, "Threat: general behavioural detection."

Trend Micro Titanium Internet Security explained why it blocked the same URL with this message, "Dangerous Page. Trend Micro has confirmed that this website can transmit malicious software or has been involved in online scams or fraud."

Listing the threats used in a meaningful way is challenging but, in this test, we wanted to explain in some detail the types of attacks that the products faced. Knowing this is helpful in drawing conclusions about the benefits of patching particular software programs.

If, for example, we discovered that attackers were focussed solely on Java-based attacks then we might expect non-Java-based Windows updates to have little positive effect. If, however, attackers focussed mainly on Internet Explorer then Windows updates should improve security by adding a strong baseline of protection to any anti-malware installed on the target system.

When consensus between products was strong we correlated the classifications. In more than half of cases the threats encountered were as a result of exploit-based toolkits.

Below is the list of 54 threats found in our overall database of 100 attacks used.

Toolkit Type	Number of incidents
Sweet Orange	14
Neutrino	12
Blackhole	7
Gongda	4
Nuclear	4
Exploit Toolkit	3
Sibhost	3
Red	3
Cool	3
Styx	1

There are different versions of these exploit kits in use. We have grouped those above into general 'families'.

Patching agendas

Patching software vulnerabilities is supposed to provide protection against threats that target those vulnerabilities. As such we are often asked why we don't test routinely using systems that are fully updated.

Some critics believe that the majority of Windows users apply all updates nearly as soon as they become available. They claim that testing with a fully-patched system is more realistic than choosing not to update it completely.

Other readers believe that running a test with a very vulnerable system is unfair to the anti-

[1] Home Anti-Virus Protection, October – December 2013, http://dennistechnologylabs.com/reports/s/a-m/2013/DTL_2013_Q4_Home.1.pdf

malware product. It is trying to protect a system that is not being maintained properly, they argue.

Additionally, operating system vendors want customers and potential customers to see their products in the best possible light and so most likely will prefer to see testing undertaken with their software running optimally, with all security patches applied.

However, it is hard to determine how many systems exist that are connected to the internet and have fewer than the full range of security updates applied. It is similarly hard to know how many have all updates installed.

Anecdotally it is clear that not every computer on the internet is fully patched. The very existence and apparent success of threats that attack vulnerabilities for which updates are available provides some evidence that less than 100 per cent of systems are fully updated.

When conducting comparative anti-malware tests it's generally considered fair to install the security products on systems that are set up in a similar way, running the same version of Windows with the same level of security patches applied.

In the past Dennis Technology Labs has used the most popular version of Windows and updated it to the latest service pack, but no further.

We usually test without patching fully because, when assessing anti-malware software, we attempt to examine the relative effectiveness of those products and not the general security of Windows or third-party applications such as Oracle Java or Adobe Reader.

Windows Updates

This report examines the effect on security resulting from updating fully the Windows 7 operating system before testing anti-malware products.

It aims to show the level of benefit obtained when patching fully, when combining full patching with anti-malware software and when using anti-malware software without the patches applied.

The security updates involved are provided by Windows Update only. We have not updated vulnerable third-party software such as Java. Doing so would almost certainly improve the systems' security further.

It is worth noting that updating Windows may also update the default browser. Internet Explorer 11, which became available in November 2013, adds additional protection that Microsoft claims prevents exploit-based attacks.

8. CONCLUSIONS

- **Windows Updates protects systems**

There is no doubt that applying security updates prevents attackers from abusing the vulnerabilities that those updates address.

This report shows that 32 per cent of the threats discovered and used in this test were rendered harmless by updating the Windows 7 system fully.

As many of the threats targeted vulnerabilities in applications such as Java, and not in Windows itself, it is almost inevitable that updating these third-party programs would bring further levels of protection.

- **Patching supplements, but should not replace, anti-malware protection**

Updating Windows provides some protection but using anti-malware software provides much higher levels of additional protection.

There is a significant overlap in protection, where anti-malware software can prevent threats that would have also been foiled with Windows updates alone.

In relatively low numbers of cases, updating Windows provided additional protection to that offered by anti-malware software.

In other words, if you had to choose between simply updating Windows or installing anti-malware software and not updating Windows, using anti-malware software is the most effective choice.

Ideally users would both update Windows and install anti-malware software.

The industry average figure for protection scores is 92 per cent when Windows was updated no further than Service Pack 1. This increased to 96 per cent when later updates were applied to systems running anti-malware software.

A four per cent increase over the industry average is a low figure. However, benefits in patching are more obvious when examining results for certain anti-malware products that performed at the lower end of the spectrum.

For example, Microsoft Security Essentials' protection score rose from 61 per cent to 82 per cent after updates were applied.

Similarly, AVG Anti-Virus Free 2014 improved its score from 88 per cent to 93 per cent.

- **Strongest anti-malware products gain least benefit from Windows updates**

Products that already scored well, without the benefit of recent Windows updates, saw minimal further advantage once these were applied.

Symantec Norton Internet Security scored 99 per cent without Windows updates and 100 per cent with.

Products from Kaspersky Lab, Trend Micro and Avast! all maintained the same scores (98 per cent or higher) regardless of whether or not any additional Windows updates were applied.

- **Updating the web browser brings significant security benefits**

Updating Windows 7 beyond Service Pack 1 replaces Internet Explorer 10 with Internet Explorer 11. This later version of Microsoft's web browser includes additional protection mechanisms that allow it to attempt to prevent the effects of exploits.

APPENDIX A: FAQS

- This test was unsponsored.
- The test rounds were conducted between 1st October 2013 and 21 November 2013 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.
- The sample set comprised 100 actively-malicious URLs.

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

No. Even we don't 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?

Vendors may request a subset of the threats that compromised their products in order for them to verify our results.

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.

For more information about malware samples please see the blog post: *What is a malware sample?*[2]

[2] What is a malware sample?, Simon PG Edwards, http://www.spgedwards.com/2013/07/what-is-malware-sample.html