

VB100 COMPARATIVE REVIEW – FEBRUARY 2018

Martijn Grooten

INTRODUCTION

Pick the odd one out: Fancy Bear; the Equation Group; the Lazarus Group; you.

The answer is you – with very few exceptions, you yourself are the only one you really need to worry about when it comes to online security. It is *you* who might enable those macros that are ‘needed’ to view that invoice you just received via email; it is *you* who might believe there really is a free version of that useful software; it is *you* who might choose not to update your software with the patches that have long been available.

If you are reading this and thinking that you, personally, do not do any of these things, try reading ‘you’ in the plural form and take it to include your co-workers and employees as well.

Anti-malware solutions, though certainly not powerless against more advanced attacks, are particularly good at stopping the often non-targeted threats that can reach our systems at least in part due to human error. Almost all malware attacks fall into this category.

In the more than 20 years that *Virus Bulletin*’s anti-malware tests have been running, their primary aim has been to verify that products are able to keep up with the latest, confirmed threats. On this occasion, we were able to do this for no fewer than 29 of the tested products, from 26 different vendors, each of which received a ‘VB100’ award.

NO GUARANTEE, BUT AN IMPORTANT MITIGATION

At *Virus Bulletin*, we are critical of bold marketing claims made by vendors about their products’ capabilities. In the

same spirit, we also warn readers against taking this test report to mean more than it claims to: a VB100 award does not mean that a product is guaranteed to protect you against any possible threat, or even against any piece of malware.

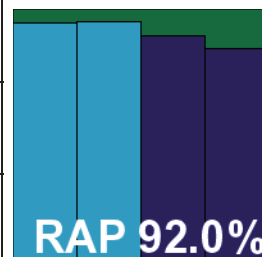
What it does mean is that the product has demonstrated that it is able to keep up with the latest threats, and that it doesn’t erroneously block widely used legitimate software.

A lot of malware infections can be avoided by patching software and operating systems and by making users more security aware. Some things will always slip through the net though, and anti-virus plays an important role, at various points in the infection chain, in seriously mitigating these kinds of incidents.

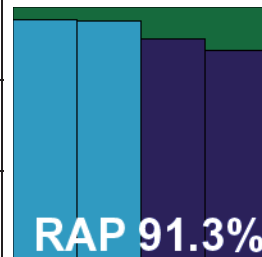
RESULTS

In order to provide some extra detail on the performance of the products in our tests, alongside the certification tests the VB100 reports include the ‘Reactive and Proactive’ (‘RAP’) test – a test which measures how quickly products detect new malware. The RAP scores give a good indication as to how quickly a product catches up when it comes to detecting new malware statically. In the results on the following pages, the RAP images display an average of the RAP scores across the two test platforms.

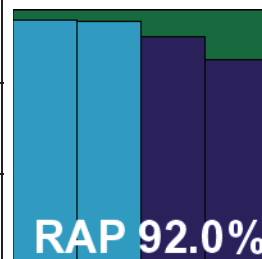
ad-aware antivirus pro		
	Windows 7	Windows 10
Main version	12.2.889.11556	12.2.889.11556
ItW catch rate	100.00%	100.00%
False positives	0	0



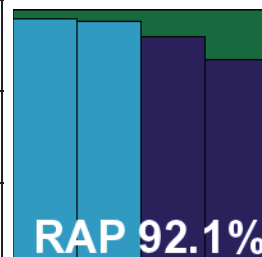
Arcabit AntiVirus		
	Windows 7	Windows 10
Main version	2018.01.11	2018.01.11
ItW catch rate	100.00%	100.00%
False positives	0	0



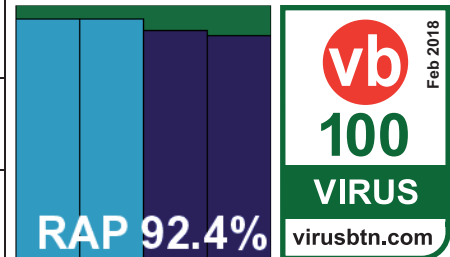
Avast Free Antivirus		
	Windows 7	Windows 10
Main version	17.9.2322	17.1.2286
ItW catch rate	100.00%	100.00%
False positives	0	0



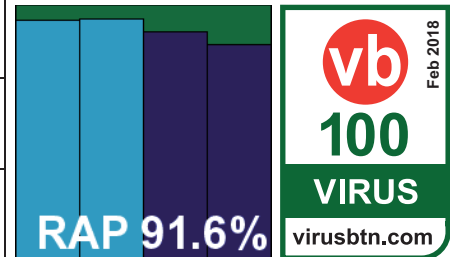
AVG Internet Security		
	Windows 7	Windows 10
Main version	17.9.3040	17.7.3032
ItW catch rate	100.00%	100.00%
False positives	0	0



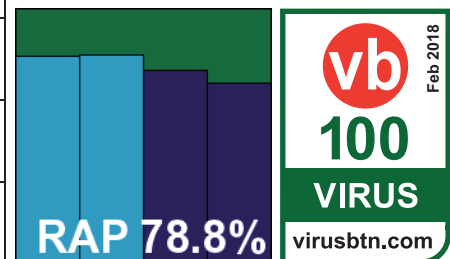
Bitdefender Endpoint Security		
	Windows 7	Windows 10
Main version	6.2.28.973	6.2.28.973
ItW catch rate	100.00%	100.00%
False positives	0	0



CompuClever Antivirus PLUS		
	Windows 7	Windows 10
Main version	19.6.0.326	19.6.0.326
ItW catch rate	100.00%	100.00%
False positives	0	0

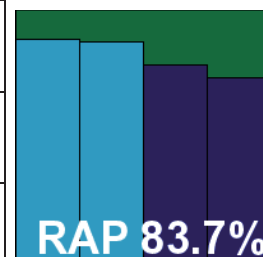


Cyren Command Anti-Malware		
	Windows 7	Windows 10
Main version	5.1.38	5.1.38
ItW catch rate	100.00%*	100.00%
False positives	0	0

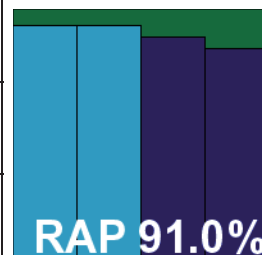


*Numbers based on two completed certification parts; data for one part was discarded due to technical issues.

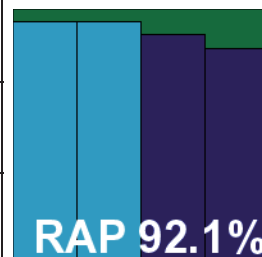
Defenx Security Suite		
	Windows 7	Windows 10
Main version	15.1.0108	15.1.0108
ItW catch rate	99.86%	99.86%
False positives	0	0



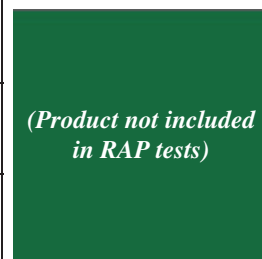
Emsisoft Anti-Malware		
	Windows 7	Windows 10
Main version	2017.12.1.8340	2017.12.1.8340
ItW catch rate	100.00%	100.00%
False positives	0	0



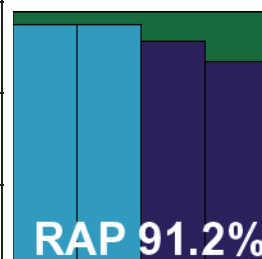
eScan Internet Security Suite for Windows		
	Windows 7	Windows 10
Main version	14.0.1400.1979	14.0.1400.1979 DB
ItW catch rate	100.00%	100.00%
False positives	0	0



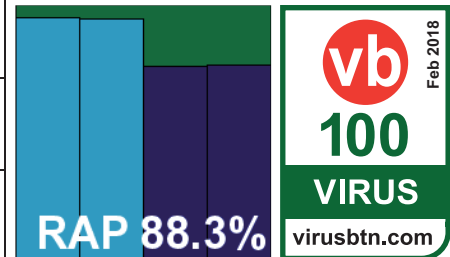
ESET Internet Security		
	Windows 7	Windows 10
Main version	11.0.159.0	10.1.235.0
ItW catch rate	100.00%	100.00%
False positives	0	0



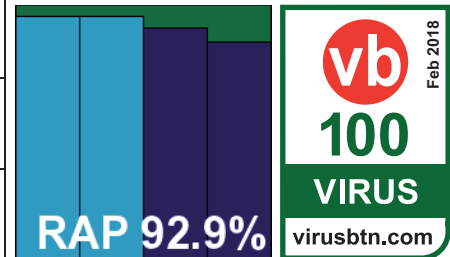
Essentware PCKeeper Antivirus PRO		
	Windows 7	Windows 10
Main version	8.3.48.142	8.3.48.144
ItW catch rate	100.00%	100.00%
False positives	0	0



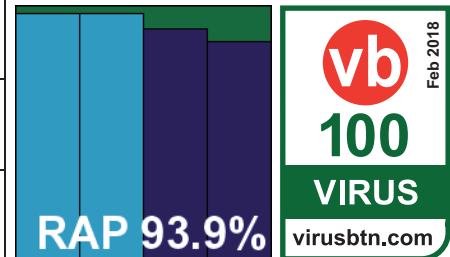
ESTsecurity ALYac		
	Windows 7	Windows 10
Main version	3.0.1.3	3.0.1.3
ItW catch rate	100.00%	100.00%
False positives	0	0



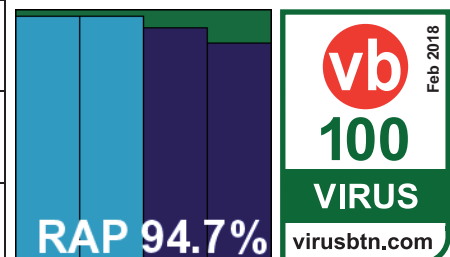
Faronics Anti-Virus		
	Windows 7	Windows 10
Main version	4.12.3102.401	4.12.3102.401
ItW catch rate	100.00%	100.00%
False positives	0	0



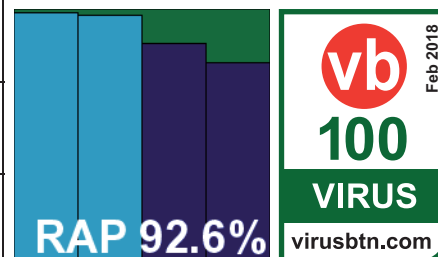
Fortinet FortiClient		
	Windows 7	Windows 10
Main version	5.6.2.1117	5.6.2.1117
ItW catch rate	100.00%	100.00%
False positives	0	0



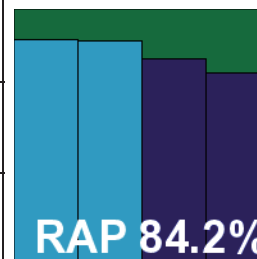
G DATA Antivirus		
	Windows 7	Windows 10
Main version	25.4.0.2	25.4.0.2
ItW catch rate	100.00%	100.00%
False positives	0	0



IKARUS anti.virus		
	Windows 7	Windows 10
Main version	2.16.20	2.16.20
ItW catch rate	100.00%	100.00%
False positives	0	0



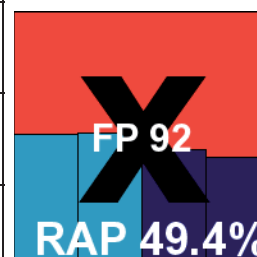
K7 Total Security		
	Windows 7	Windows 10
Main version	15.1.0324	15.0.0324
ItW catch rate	99.86%	99.86%
False positives	0	0



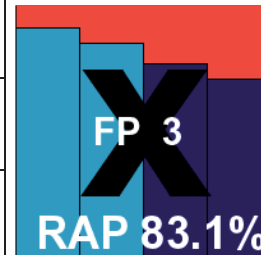
Kaspersky Endpoint Security 10 for Windows		
	Windows 7	Windows 10
Main version	10.3.0.6294	10.3.0.6294 AES256
ItW catch rate	100.00%	100.00%
False positives	0	0



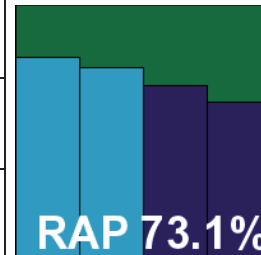
MINUSOFT KIDO		
	Windows 7	Windows 10
Main version	2.0.1194.0	2.0.1194.0
ItW catch rate	71.44%	71.44%
False positives	46	46



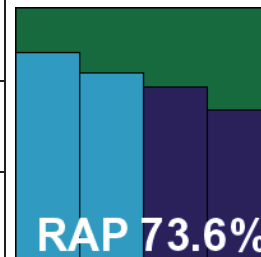
NANO Antivirus		
	Windows 7	Windows 10
Main version	1.0.100.86370	1.0.100.86370
ItW catch rate	100.00%	100.00%
False positives	2	1



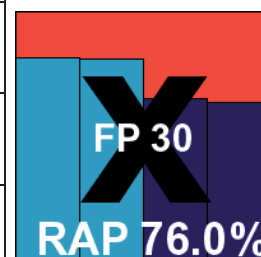
Panda Endpoint Protection Plus		
	Windows 7	Windows 10
Main version	7.70.0	18.03.00
ItW catch rate	100.00%	100.00%
False positives	0	0



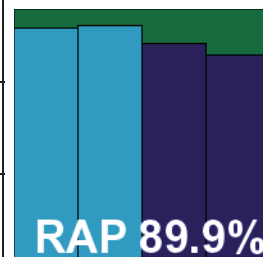
Panda Free Antivirus		
	Windows 7	Windows 10
Main version	18.03.00	18.03.00
ItW catch rate	100.00%	100.00%
False positives	0	0



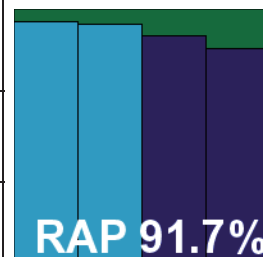
Rising Security Cloud Client		
	Windows 7	Windows 10
Main version	3.0.0.73	3.0.0.73
ItW catch rate	100.00%	100.00%
False positives	18	12



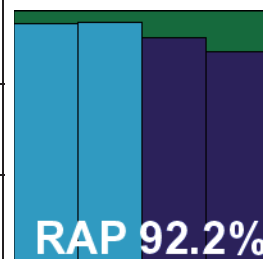
TACHYON Endpoint Security		
	Windows 7	Windows 10
Main version	5.0.0.0	2.16.20
ItW catch rate	100.00%	100.00%
False positives	0	0



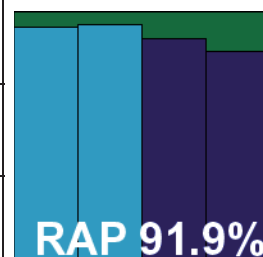
TeamViewer ITbrain Anti-Malware		
	Windows 7	Windows 10
Main version	1.0.91508	1.0.91508
ItW catch rate	100.00%	100.00%
False positives	0	0



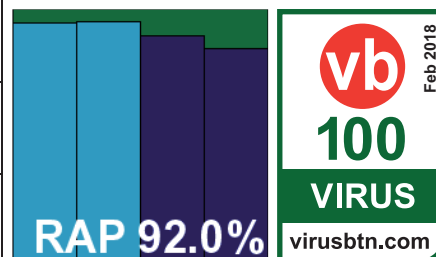
Tencent PC Manager		
	Windows 7	Windows 10
Main version	12.3.26525.901	12.3.26525.901
ItW catch rate	100.00%	100.00%
False positives	0	0



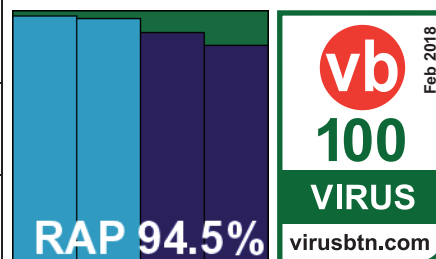
Total Defense Internet Security Suite		
	Windows 7	Windows 10
Main version	9.0.0.747	9.0.0.747
ItW catch rate	100.00%	100.00%
False positives	0	0



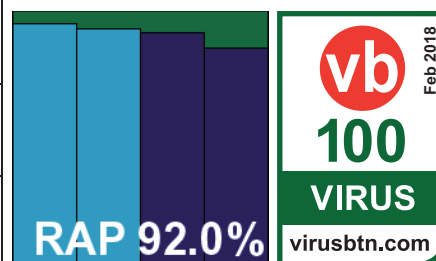
Total Defense Premium Internet Security		
	Windows 7	Windows 10
Main version	9.0.0.747	9.0.0.747
ItW catch rate	100.00%	100.00%
False positives	0	0



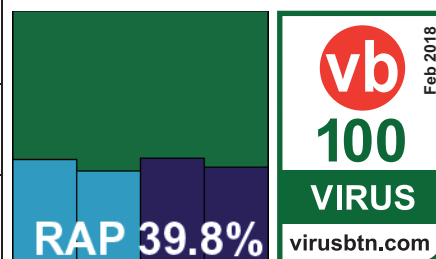
TrustPort Antivirus Sphere		
	Windows 7	Windows 10
Main version	17.0.3.7038	17.0.3.7038
ItW catch rate	100.00%	100.00%
False positives	0	0



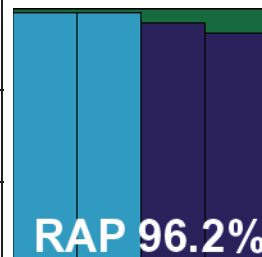
VIPRE Advanced Security		
	Windows 7	Windows 10
Main version	10.1.4.33	10.1.4.33
ItW catch rate	100.00%	100.00%
False positives	0	0



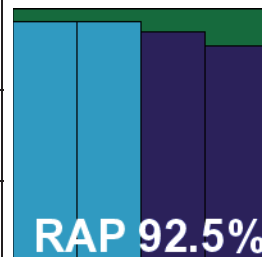
VirIT eXplorer PRO		
	Windows 7	Windows 10
Main version	8.5.90	8.5.90
ItW catch rate	100.00%	100.00%
False positives	0	0



Wontok SafeCentral Security Suite		
	Windows 7	Windows 10
Main version	2.0.1337	2.0.1337
ItW catch rate	100.00%	100.00%
False positives	0	0



Zemana Endpoint Security		
	Windows 7	Windows 10
Main version	6.2.18.885	6.2.18.885
ItW catch rate	100.00%	100.00%
False positives	0	0



Certification tests	Windows 7				Windows 10				VB100
	FPs	FP rate	WildList misses	WildList catch rate	FPs	FP rate	WildList misses	WildList catch rate	
ad-aware antivirus pro	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Arcabit AntiVirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Avast Free Antivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
AVG Internet Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Bitdefender Endpoint Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
CompuClever Antivirus PLUS	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Cyren Command Anti-Malware	0	0.00%	0*	100.00%*	0	0.00%	0	100.00%	
Defenx Security Suite	0	0.00%	9	99.86%	0	0.00%	9	99.86%	
Emsisoft Anti-Malware	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
eScan Internet Security Suite for Windows	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
ESET Internet Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Essentware PCKeeper Antivirus PRO	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
ESTsecurity ALYac	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Faronics Anti-Virus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Fortinet FortiClient	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
G DATA Antivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
IKARUS anti.virus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	

* Numbers based on two completed certification parts; data for one part was discarded due to technical issues.

Certification tests contd.	Windows 7				Windows 10				VB100
	FPs	FP rate	WildList misses	WildList catch rate	FPs	FP rate	WildList misses	WildList catch rate	
K7 Total Security	0	0.00%	9	99.86%	0	0.00%	9	99.86%	
Kaspersky Endpoint Security 10 for Windows	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
MINUSOFT KIDO	46	0.01%	1796	71.44%	46	0.01%	1796	71.44%	
NANO Antivirus	2	0.001%	0	100.00%	1	0.0003%	0	100.00%	
Panda Endpoint Protection Plus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Panda Free Antivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Rising Security Cloud Client	18	0.005%	0	100.00%	12	0.003%	0	100.00%	
TACHYON Endpoint Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
TeamViewer ITbrain Anti-Malware	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Tencent PC Manager	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Total Defense Internet Security Suite	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Total Defense Premium Internet Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
TrustPort Antivirus Sphere	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
VIPRE Advanced Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
VirIT eXplorer PRO	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Wontok SafeCentral Security Suite	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Zemana Endpoint Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	

RAP (Reactive And Proactive) tests – Windows 7	Reactive		Reactive average	Proactive		Proactive average	RAP weighted average [‡]
	Set -2*	Set -1*		Set +1 [†]	Set +2 [†]		
ad-aware antivirus pro	94.10%	94.49%	94.29%	89.36%	84.38%	86.87%	91.82%
Arcabit AntiVirus	95.41%	94.56%	94.99%	87.23%	82.78%	85.00%	91.66%
Avast Free Antivirus	95.72%	95.83%	95.77%	88.61%	79.85%	84.23%	91.93%
AVG Internet Security	95.93%	95.55%	95.74%	89.18%	80.14%	84.66%	92.05%
Bitdefender Endpoint Security	94.22%	93.88%	94.05%	88.98%	87.32%	88.15%	92.08%
CompuClever Antivirus PLUS	93.64%	94.60%	94.12%	89.30%	84.28%	86.79%	91.68%
Cyren Command Anti-Malware	80.38%	82.50%	81.44%	74.88%	69.94%	72.41%	78.43%
Defenx Security Suite	88.18%	87.28%	87.73%	78.03%	73.22%	75.62%	83.70%
Emsisoft Anti-Malware	91.52%	92.07%	91.79%	87.65%	83.18%	85.42%	89.67%
eScan Internet Security Suite for Windows	95.06%	94.28%	94.67%	89.06%	83.45%	86.25%	91.87%
Essentware PCKeeper Antivirus PRO	94.12%	94.87%	94.50%	87.33%	79.31%	83.32%	90.77%
ESTsecurity ALYac	95.22%	94.21%	94.71%	76.04%	76.51%	76.27%	88.57%
Faronics Anti-Virus	95.78%	94.95%	95.37%	91.08%	85.38%	88.23%	92.99%
Fortinet FortiClient	96.86%	96.76%	96.81%	91.67%	86.01%	88.84%	94.15%
G DATA Antivirus	97.03%	97.31%	97.17%	92.67%	86.59%	89.63%	94.65%
IKARUS anti.virus	98.14%	97.27%	97.70%	86.00%	78.72%	82.36%	92.59%
K7 Total Security	86.35%	87.43%	86.89%	80.46%	74.75%	77.61%	83.80%
MINUSOFT KIDO	52.58%	50.57%	51.58%	45.84%	42.93%	44.39%	49.18%
NANO Antivirus	90.43%	85.01%	87.72%	76.93%	70.50%	73.71%	83.05%
Panda Endpoint Protection Plus	77.09%	75.39%	76.24%	68.49%	61.75%	65.12%	72.53%
Panda Free Antivirus	81.36%	76.67%	79.02%	68.65%	58.07%	63.36%	73.80%
Rising Security Cloud Client	83.35%	79.73%	81.54%	65.74%	64.44%	65.09%	76.06%
TACHYON Endpoint Security	91.91%	93.21%	92.56%	86.20%	81.64%	83.92%	89.68%
TeamViewer ITbrain Anti-Malware	94.91%	93.01%	93.96%	89.38%	84.41%	86.90%	91.60%
Tencent PC Manager	94.95%	94.75%	94.85%	89.02%	83.84%	86.43%	92.05%
Total Defense Internet Security Suite	93.90%	94.93%	94.41%	89.38%	84.39%	86.89%	91.90%
Total Defense Premium Internet Security	94.17%	94.60%	94.38%	89.38%	84.26%	86.82%	91.86%
TrustPort Antivirus Sphere	97.53%	96.97%	97.25%	91.49%	86.34%	88.91%	94.47%
VIPRE Advanced Security	94.90%	94.98%	94.94%	91.08%	85.45%	88.27%	92.72%
VirIT eXplorer PRO	41.32%	37.62%	39.47%	42.25%	38.68%	40.46%	39.80%
Wontok SafeCentral Security Suite	97.94%	98.30%	98.12%	94.08%	90.44%	92.26%	96.17%
Zemana Endpoint Security	94.54%	94.73%	94.63%	90.94%	85.24%	88.09%	92.45%

*Set -1 = Samples discovered 1 to 5 days before testing; Set -2 = Samples discovered 6 to 10 days before testing.

[†]Set +1 = Samples discovered 1 to 5 days after updates frozen; Set +2 = Samples discovered 6 to 10 days after updates frozen.

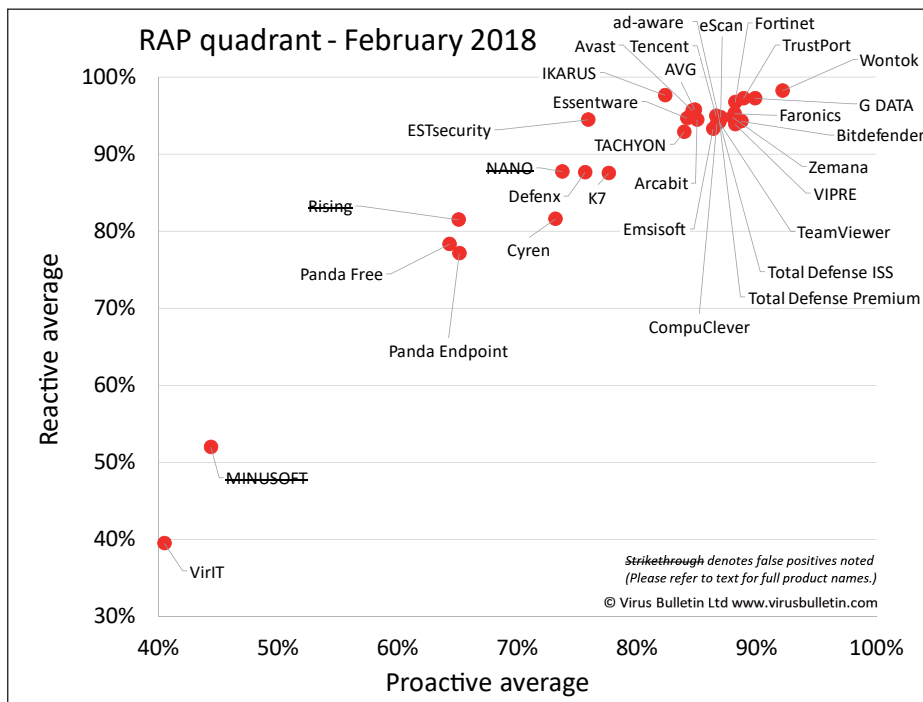
[‡]Weighted average gives equal emphasis to the two reactive weeks and the whole proactive part.

RAP (Reactive And Proactive) tests – Windows 10	Reactive		Reactive average	Proactive		Proactive average	RAP weighted average [‡]
	Set -2*	Set -1*		Set +1 [†]	Set +2 [†]		
ad-aware antivirus pro	94.82%	94.81%	94.81%	89.40%	84.41%	86.91%	92.18%
Arcabit AntiVirus	93.60%	94.21%	93.90%	87.23%	82.78%	85.00%	90.94%
Avast Free Antivirus	96.02%	95.14%	95.58%	89.60%	80.33%	84.97%	92.04%
AVG Internet Security	96.33%	95.17%	95.75%	89.60%	80.33%	84.97%	92.16%
Bitdefender Endpoint Security	94.57%	94.36%	94.46%	90.54%	88.07%	89.31%	92.74%
CompuClever Antivirus PLUS	93.76%	93.96%	93.86%	89.10%	84.05%	86.57%	91.43%
Cyren Command Anti-Malware	81.91%	81.38%	81.65%	76.59%	71.25%	73.92%	79.07%
Defenx Security Suite	88.27%	86.97%	87.62%	78.05%	73.22%	75.63%	83.63%
Emsisoft Anti-Malware	94.59%	94.76%	94.68%	89.82%	84.82%	87.32%	92.22%
eScan Internet Security Suite for Windows	94.55%	95.00%	94.78%	90.76%	84.66%	87.71%	92.42%
Essentware PCKeeper Antivirus PRO	94.89%	94.86%	94.87%	89.24%	80.91%	85.07%	91.61%
ESTsecurity ALYac	94.38%	93.95%	94.17%	75.44%	75.64%	75.54%	87.96%
Faronics Anti-Virus	94.88%	95.40%	95.14%	90.88%	85.15%	88.01%	92.77%
Fortinet FortiClient	96.54%	96.91%	96.73%	90.08%	85.07%	87.57%	93.67%
G DATA Antivirus	97.38%	97.09%	97.23%	93.17%	86.90%	90.03%	94.83%
IKARUS anti.virus	98.06%	97.22%	97.64%	86.00%	78.72%	82.36%	92.55%
K7 Total Security	89.40%	87.03%	88.22%	80.46%	74.75%	77.61%	84.68%
MINUSOFT KIDO	50.58%	54.08%	52.33%	45.84%	42.93%	44.39%	49.68%
NANO Antivirus	90.90%	84.54%	87.72%	76.93%	70.50%	73.71%	83.05%
Panda Endpoint Protection Plus	81.12%	74.81%	77.97%	68.49%	61.75%	65.12%	73.68%
Panda Free Antivirus	83.01%	72.11%	77.56%	68.65%	61.84%	65.25%	73.46%
Rising Security Cloud Client	80.34%	82.65%	81.50%	65.74%	64.44%	65.09%	76.03%
TACHYON Endpoint Security	92.88%	93.51%	93.19%	86.20%	81.64%	83.92%	90.10%
TeamViewer ITbrain Anti-Malware	94.43%	94.24%	94.34%	89.34%	84.38%	86.86%	91.84%
Tencent PC Manager	94.78%	95.44%	95.11%	89.46%	84.13%	86.79%	92.34%
Total Defense Internet Security Suite	94.08%	94.68%	94.38%	89.34%	84.36%	86.85%	91.87%
Total Defense Premium Internet Security	94.49%	94.90%	94.69%	89.38%	84.39%	86.89%	92.09%
TrustPort Antivirus Sphere	97.62%	96.97%	97.29%	91.49%	86.34%	88.91%	94.50%
VIPRE Advanced Security	94.99%	90.63%	92.81%	90.92%	85.26%	88.09%	91.23%
VirIT eXplorer PRO	41.93%	36.86%	39.40%	42.25%	38.68%	40.46%	39.75%
Wontok SafeCentral Security Suite	98.33%	98.36%	98.35%	93.98%	90.15%	92.06%	96.25%
Zemana Endpoint Security	95.13%	94.73%	94.93%	90.74%	85.01%	87.88%	92.58%

*Set -1 = Samples discovered 1 to 5 days before testing; Set -2 = Samples discovered 6 to 10 days before testing.

[†]Set +1 = Samples discovered 1 to 5 days after updates frozen; Set +2 = Samples discovered 6 to 10 days after updates frozen.

[‡]Weighted average gives equal emphasis to the two reactive weeks and the whole proactive part.



APPENDIX: THE TEST SET-UP

The main test on each platform was run in three parts, over three consecutive weeks. Products were installed on clean installations of both *Windows 7* and *Windows 10*. At the beginning of each part of the test we made sure the latest updates were downloaded, while throughout the test, products were connected to the Internet, thus allowing for real-time cloud look-ups.

The products as we tested them are available to the general public. However, in a few instances we have allowed vendors to make modifications to the product to adapt to our specific test scenario. None of these modifications would have an impact on the real-world performance of the affected products.

For each part of the test, we used the most recent version of the WildList, together with one third of our constantly updated collection of widely used legitimate software. Using a shared drive, the files were copied onto the client machine and we recorded whether (and how) files were blocked by the anti-malware product.

If files weren't blocked, a custom-built tool was used to open the file, thus triggering AV detection by products that don't (always) scan files on being copied.

A product passed the test if, and only if, *on both platforms* it blocked all files from the WildList, and didn't generate any false positives (i.e. incorrect detections) when scanning the full clean set.

The clean set consists of more than 450,000 files, all widely used programs, with any files that show suspicious behaviour being excluded from the set.

For the 'RAP' (reactive and proactive) test, the same set-up was used, but for the proactive part of the test products were not connected to the Internet. This allowed us to measure their proactive detection abilities by having a 'frozen' version of each product scan two sets of malware files: those seen in the wild between one day and five days after the product 'freeze' date, and those seen in the wild between six and 10 days after this date.

Note: A slightly different approach when it comes to tidying up the set of malware, as well as a different approach to testing, means the individual RAP scores should not be compared with those seen in tests prior to April 2017.

Editor: Martijn Grooten

Head of Testing: Peter Karsai

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuț Răileanu, Chris Stock

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

© 2018 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139 Email: editor@virusbulletin.com

Web: <https://www.virusbulletin.com/>