OCTOBER 2017

virus BULLETIN

Covering the global threat landscape

VB100 COMPARATIVE REVIEW – OCTOBER 2017

Martijn Grooten

My favourite kind of security product marketing is one where the vendor acknowledges that the product isn't a silver bullet, but that it plays a role in the wider security ecosystem, which together intends to mitigate the threat.

The same applies to test reports. It would be wrong to consider this report – or any test report for that matter – a guide to the absolute best product. Rather, it helps paint part of the picture, but we encourage readers also to check out reports by other testing organizations – for example those that focus on runtime detection or vulnerabilities in the products.

The focus of the VB100 reports has always been to measure products' ability to keep up with threats, to avoid false positives, and to do so in a consistent manner; hence we expect products to block 100% of the malware in the WildList and to generate no false positives among our own, well-curated set of popular legitimate software. This is also why we test regularly – to be able to paint a more continuous picture of products' performance.

This month, we tested 32 products from 27 vendors, with some new names appearing in addition to many of the regular ones, showing that the anti-virus market remains very much alive. Twenty eight of the products achieved the VB100 certification.

BAD TROJANS, GOOD TOOLS

Ransomware, banking trojans, espionage tools: there is no shortage of malicious threats facing computer users. Despite what the box may say, no security product blocks or detects them all, but the very least you should expect is for a product to block the malware found on the WildList, a well-vetted list of malware that has both been confirmed to be malicious and confirmed to have been seen in the wild.

As usual, this month's WildList contained a good mix of such threats, which even included tools developed by the NSA and leaked by the infamous Shadow Brokers group. We were pleased to see that products generally had few problems blocking the files from this list.

At the same time as blocking such threats, you should also expect an anti-virus product *not* to prevent you from using a video editor, a printer driver, or any other type of legitimate software; this is why we require products to scan a collection of clean files, and penalize any that generate false detections within this set. We were pleased to find that, here too, there were few problems.

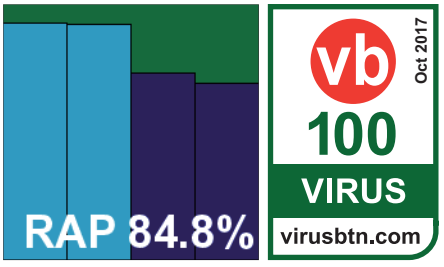
The full test set-up is described in the Appendix at the end of this report.

RESULTS

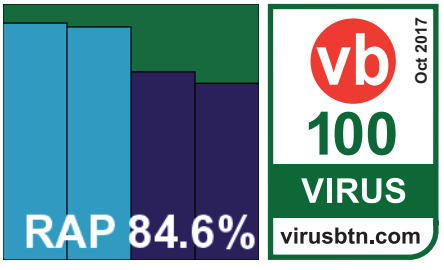
In the results on the following pages, the RAP images display an average of the RAP scores across the two platforms.

ISSN 1749-7027

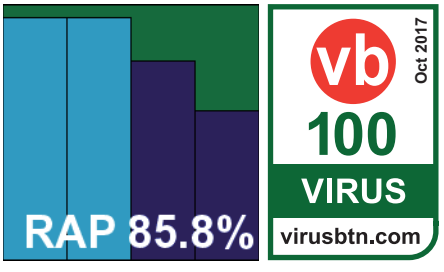
ad-aware antivirus pro		
	Windows 7	**Windows 10**
Main version	12.0.649.11190	12.0.649.11190
ItW catch rate	100.00%	100.00%
False positives	0	0



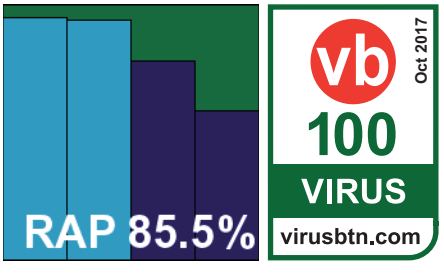
Arcabit AntiVirus		
	Windows 7	**Windows 10**
Main version	2017.09.06	2017.09.05
ItW catch rate	100.00%	100.00%
False positives	0	0



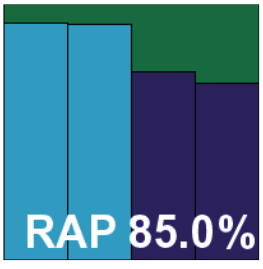
Avast Free Antivirus		
	Windows 7	**Windows 10**
Main version	17.6.2310	17.6.2310
ItW catch rate	100.00%	100.00%
False positives	0	0



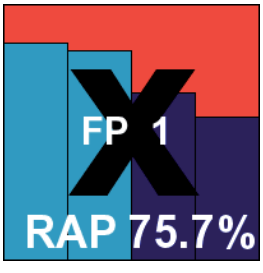
AVG Internet Security		
	Windows 7	**Windows 10**
Main version	17.6.3029	17.6.3029
ItW catch rate	100.00%	100.00%
False positives	0	0



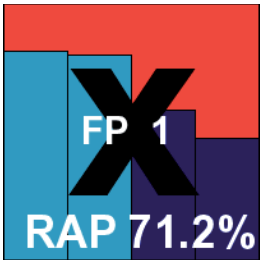
CompuClever Antivirus PLUS		
	Windows 7	**Windows 10**
Main version	19.6.0.326	19.6.0.326
ItW catch rate	100.00%	100.00%
False positives	0	0



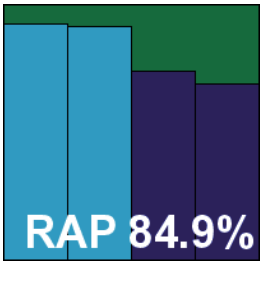
Cyren Command Anti-Malware		
	Windows 7	**Windows 10**
Main version	5.1.38	5.1.38
ItW catch rate	100.00%	99.96%
False positives	0	1



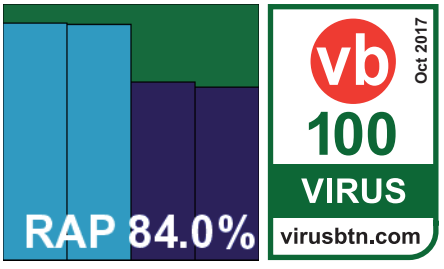
Defenx Security Suite		
	Windows 7	**Windows 10**
Main version	15.1.0107	15.1.0107
ItW catch rate	100.00%	99.93%
False positives	1	1



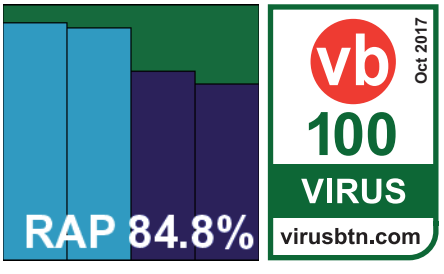
Emsisoft Anti-Malware		
	Windows 7	**Windows 10**
Main version	2017.7.0.73037	2017.7.0.73049
ItW catch rate	100.00%	100.00%
False positives	0	0



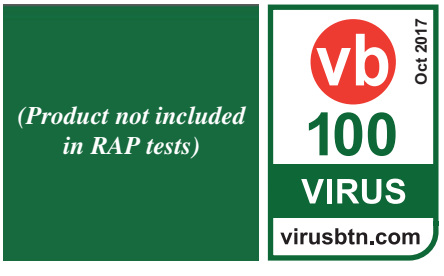
Endpoint Security by Bitdefender		
	Windows 7	**Windows 10**
Main version	6.2.24.938	6.2.24.938
ItW catch rate	100.00%	100.00%
False positives	0	0



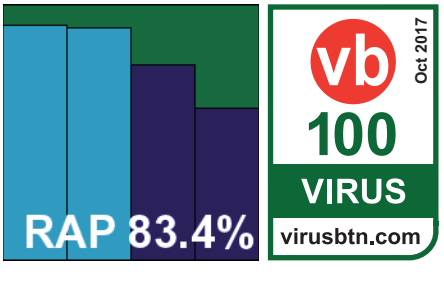
eScan Internet Security Suite for Windows		
	Windows 7	**Windows 10**
Main version	14.0.1400.1979	14.0.1400.1979 DB
ItW catch rate	100.00%	100.00%
False positives	0	0



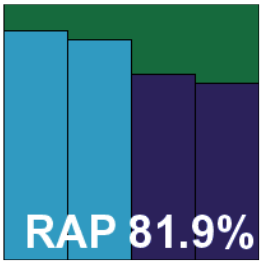
ESET Internet Security		
	Windows 7	**Windows 10**
Main version	10.1.219.0	10.1.210.0
ItW catch rate	100.00%	100.00%
False positives	0	0



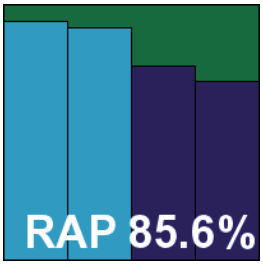
Essentware PCKeeper Antivirus PRO		
	Windows 7	**Windows 10**
Main version	8.3.48.14	8.3.48.16
ItW catch rate	100.00%	100.00%
False positives	0	0



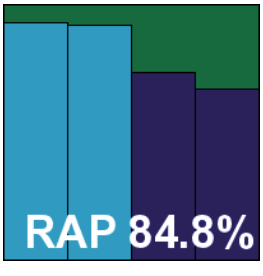
ESTsecurity ALYac		
	Windows 7	**Windows 10**
Main version	3.0.1.3	3.0.1.3
ItW catch rate	100.00%	100.00%
False positives	0	0



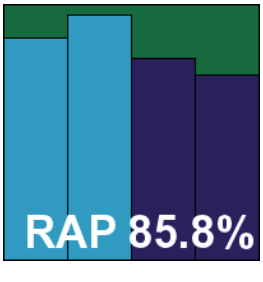
Faronics Anti-Virus		
	Windows 7	**Windows 10**
Main version	3.0.3.794	4.0.3102.369
ItW catch rate	100.00%	100.00%
False positives	0	0



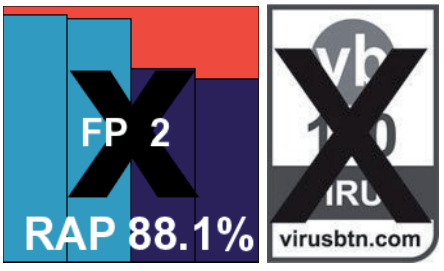
Fortinet FortiClient		
	Windows 7	**Windows 10**
Main version	5.4.1.0840	5.4.1.0840
ItW catch rate	100.00%	100.00%
False positives	0	0



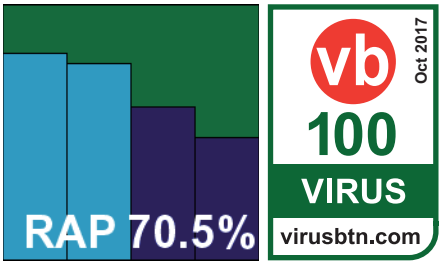
G DATA Antivirus		
	Windows 7	**Windows 10**
Main version	25.3.0.1	25.3.0.3
ItW catch rate	100.00%	100.00%
False positives	0	0



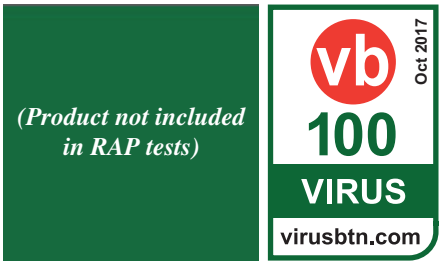
IKARUS anti.virus		
	Windows 7	**Windows 10**
Main version	2.16.7	2.16.7
ItW catch rate	100.00%	100.00%
False positives	0	2



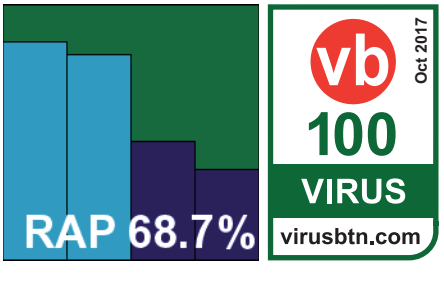
K7 Total Security		
	Windows 7	**Windows 10**
Main version	15.1.0314	15.1.0314
ItW catch rate	100.00%	100.00%
False positives	0	0



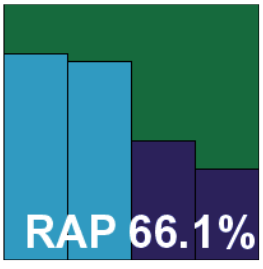
Kaspersky Endpoint Security 10 for Windows		
	Windows 7	**Windows 10**
Main version	10.3.0.6294	10.3.0.6294 AES256
ItW catch rate	100.00%	100.00%
False positives	0	0



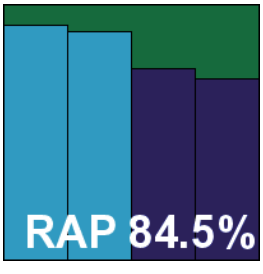
Panda Endpoint Protection Plus		
	Windows 7	**Windows 10**
Main version	7.70.0	7.70.0
ItW catch rate	100.00%	100.00%
False positives	0	0



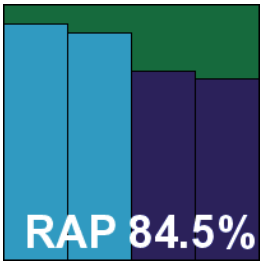
Panda Free Antivirus		
	Windows 7	**Windows 10**
Main version	18.01.00	18.01.00
ItW catch rate	100.00%	100.00%
False positives	0	0



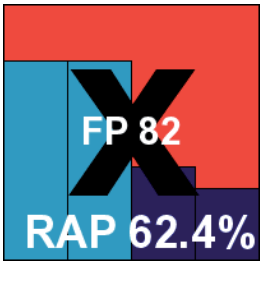
Quick Heal Seqrite Endpoint Security		
	Windows 7	**Windows 10**
Main version	17.00	17.00
ItW catch rate	100.00%	100.00%
False positives	0	0



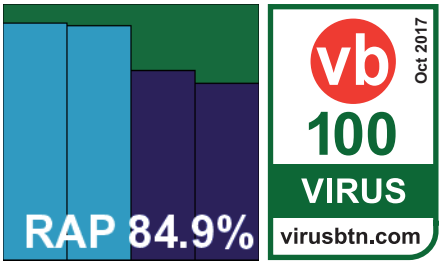
Quick Heal Total Security		
	Windows 7	**Windows 10**
Main version	17.00	17.00
ItW catch rate	100.00%	100.00%
False positives	0	0



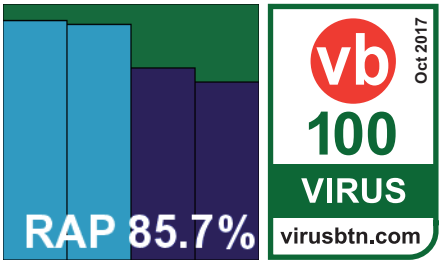
Rising Security Cloud Client		
	Windows 7	**Windows 10**
Main version	3.0.0.73	3.0.0.73
ItW catch rate	100.00%	100.00%
False positives	41	41



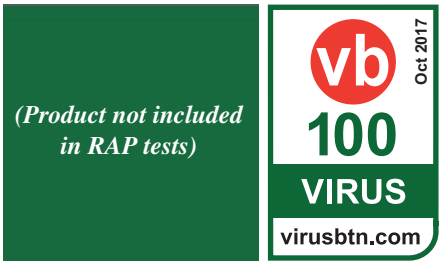
TeamViewer ITbrain Anti-Malware		
	Windows 7	**Windows 10**
Main version	1.0.76588	1.0.76588
ItW catch rate	100.00%	100.00%
False positives	0	0



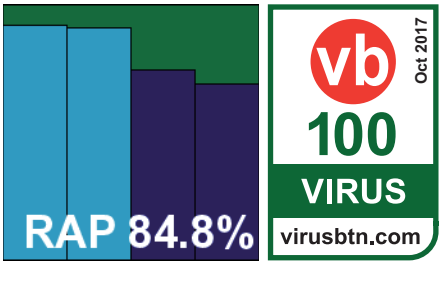
Tencent PC Manager		
	Windows 7	**Windows 10**
Main version	12.3.26476.901	12.3.26476.901
ItW catch rate	100.00%	100.00%
False positives	0	0



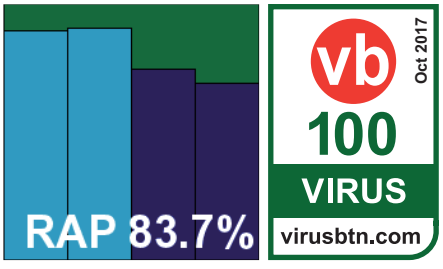
Tencent PC Manager – TAV		
	Windows 7	**Windows 10**
Main version	12.3.26476.901	12.3.26476.901
ItW catch rate	100.00%	100.00%
False positives	0	0



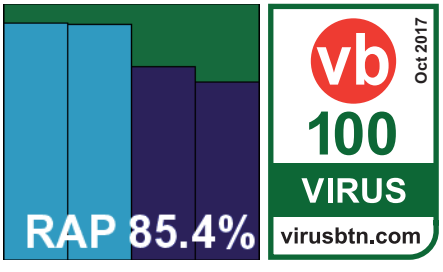
Total Defense Internet Security		
	Windows 7	**Windows 10**
Main version	9.0.0.645	9.0.0.645
ItW catch rate	100.00%	100.00%
False positives	0	0



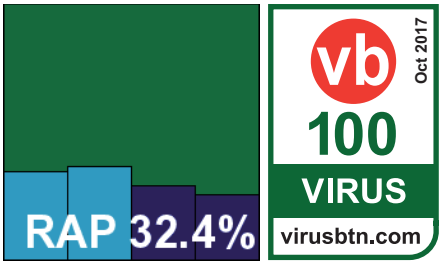
Total Defense Premium		
	Windows 7	**Windows 10**
Main version	9.0.0.645	9.0.0.645
ItW catch rate	100.00%	100.00%
False positives	0	0



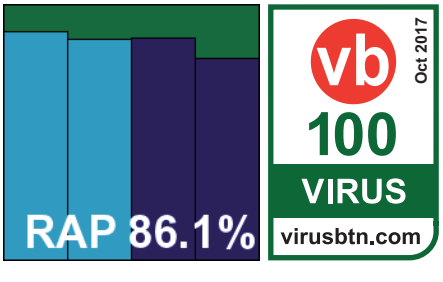
VIPRE Advanced Security		
	Windows 7	**Windows 10**
Main version	10.1.4.33	10.1.4.33
ItW catch rate	100.00%	100.00%
False positives	0	0



VirIT eXplorer PRO		
	Windows 7	**Windows 10**
Main version	8.5	8.5
ItW catch rate	100.00%	100.00%
False positives	0	0



Wontok SafeCentral Security Suite		
	Windows 7	**Windows 10**
Main version	2.0.1318	2.0.1318
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%	VIRUS 100
Arcabit AntiVirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Avast Free Antivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
AVG Internet Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
CompuClever Antivirus PLUS	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Cyren Command Anti-Malware	0	0.00%	0	100.00%	1	0.0003%	1	99.96%	X
Defenx Security Suite	1	0.0003%	0	100.00%	1	0.0003%	2	99.93%	X
Emsisoft Anti-Malware	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Endpoint Security by Bitdefender	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
eScan Internet Security Suite for Windows	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
ESET Internet Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Essentware PCKeeper Antivirus PRO	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
ESTsecurity ALYac	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Faronics Anti-Virus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Fortinet FortiClient	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
G DATA Antivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
IKARUS anti.virus	0	0.00%	0	100.00%	2	0.0005%	0	100.00%	X

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%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Kaspersky Endpoint Security 10 for Windows	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Panda Endpoint Protection Plus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Panda Free Antivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Quick Heal Seqrite Endpoint Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Quick Heal Total Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Rising Security Cloud Client	41	0.01%	0	100.00%	41	0.01%	0	100.00%	X
TeamViewer ITbrain Anti-Malware	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Tencent PC Manager	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Tencent PC Manager – TAV	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Total Defense Internet Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Total Defense Premium	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
VIPRE Advanced Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
VirIT eXplorer PRO	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Wontok SafeCentral Security Suite	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100

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	92.31%	91.08%	91.69%	72.51%	68.73%	70.62%	84.67%
Arcabit AntiVirus	92.10%	90.71%	91.41%	74.58%	68.97%	71.77%	84.86%
Avast Free Antivirus	94.82%	94.54%	94.68%	77.85%	58.00%	67.93%	85.77%
AVG Internet Security	94.84%	94.51%	94.67%	77.72%	58.00%	67.86%	85.74%
CompuClever Antivirus PLUS	92.62%	90.80%	91.71%	73.14%	68.70%	70.92%	84.78%
Cyren Command Anti-Malware	84.65%	81.91%	83.28%	65.32%	55.72%	60.52%	75.70%
Defenx Security Suite	81.25%	79.73%	80.49%	57.85%	47.36%	52.60%	71.19%
Emsisoft Anti-Malware	92.22%	91.02%	91.62%	72.74%	68.80%	70.77%	84.67%
Endpoint Security by Bitdefender	91.95%	91.46%	91.70%	65.81%	65.99%	65.90%	83.10%
eScan Internet Security Suite for Windows	92.47%	90.98%	91.72%	72.60%	68.77%	70.69%	84.71%
Essentware PCKeeper Antivirus PRO	92.22%	90.37%	91.30%	74.60%	59.01%	66.81%	83.14%
ESTsecurity ALYac	91.03%	86.97%	89.00%	72.49%	68.75%	70.62%	82.87%
Faronics Anti-Virus	93.44%	90.76%	92.10%	75.87%	69.54%	72.71%	85.64%
Fortinet FortiClient	92.53%	92.35%	92.44%	75.16%	66.97%	71.07%	85.32%
G DATA Antivirus	96.10%	95.83%	95.97%	78.61%	72.19%	75.40%	89.11%
IKARUS anti.virus	96.49%	94.58%	95.53%	75.50%	71.13%	73.31%	88.13%
K7 Total Security	81.50%	76.84%	79.17%	59.76%	47.76%	53.76%	70.70%
Panda Endpoint Protection Plus	84.25%	81.38%	82.82%	46.18%	35.22%	40.70%	68.78%
Panda Free Antivirus	82.54%	80.36%	81.45%	46.29%	35.12%	40.71%	67.87%
Quick Heal Seqrite Endpoint Security	92.11%	88.80%	90.45%	75.52%	70.94%	73.23%	84.71%
Quick Heal Total Security	92.32%	88.75%	90.54%	73.67%	70.91%	72.29%	84.45%
Rising Security Cloud Client	78.06%	77.76%	77.91%	36.23%	27.62%	31.93%	62.58%
TeamViewer ITbrain Anti-Malware	92.15%	91.20%	91.68%	73.09%	68.73%	70.91%	84.75%
Tencent PC Manager	92.94%	91.77%	92.36%	73.80%	69.33%	71.57%	85.43%
Total Defense Internet Security	92.35%	90.53%	91.44%	74.47%	68.97%	71.72%	84.87%
Total Defense Premium	92.36%	90.78%	91.57%	74.47%	68.97%	71.72%	84.95%
VIPRE Advanced Security	92.26%	91.00%	91.63%	74.54%	69.35%	71.94%	85.07%
VirIT eXplorer PRO	33.96%	36.03%	34.99%	28.96%	25.24%	27.10%	32.36%
Wontok SafeCentral Security Suite	85.18%	79.14%	82.16%	86.94%	78.99%	82.96%	82.43%

*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.

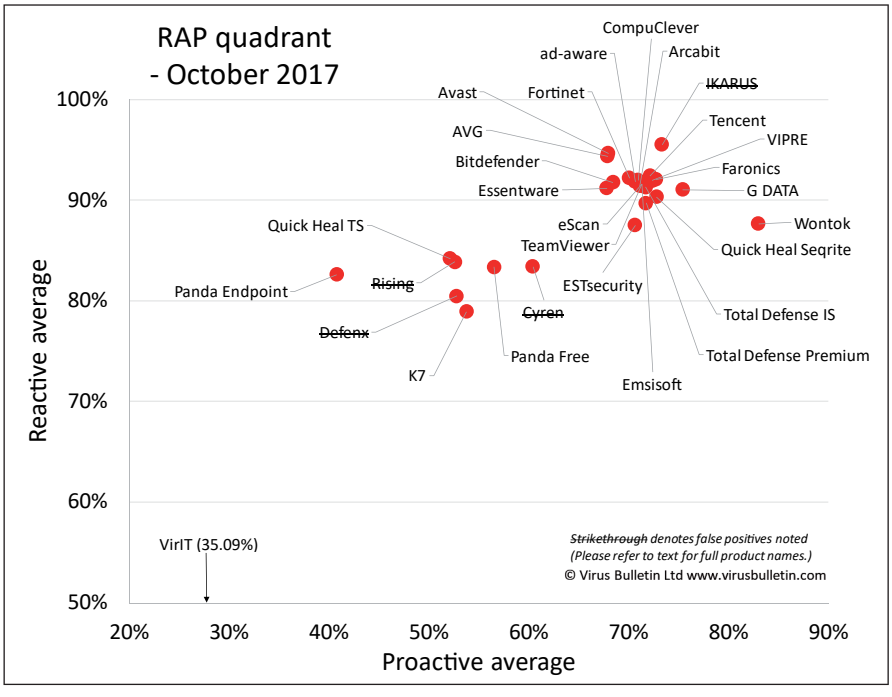
‡Weighted average gives equal emphasis to the two reactive weeks and the whole proactive part.

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	91.86%	92.18%	92.02%	72.51%	68.73%	70.62%	84.89%
Arcabit AntiVirus	92.10%	90.71%	91.41%	72.16%	68.73%	70.44%	84.42%
Avast Free Antivirus	94.82%	94.53%	94.68%	77.85%	58.03%	67.94%	85.77%
AVG Internet Security	94.96%	93.18%	94.07%	77.77%	58.00%	67.89%	85.34%
CompuClever Antivirus PLUS	92.02%	92.58%	92.30%	73.16%	68.70%	70.93%	85.18%
Cyren Command Anti-Malware	85.23%	81.80%	83.51%	64.88%	55.70%	60.29%	75.77%
Defenx Security Suite	81.24%	79.72%	80.48%	58.34%	47.50%	52.92%	71.29%
Emsisoft Anti-Malware	92.24%	91.04%	91.64%	74.76%	69.04%	71.90%	85.06%
Endpoint Security by Bitdefender	92.06%	91.65%	91.86%	73.16%	68.73%	70.94%	84.89%
eScan Internet Security Suite for Windows	92.75%	90.20%	91.47%	74.72%	69.01%	71.87%	84.94%
Essentware PCKeeper Antivirus PRO	90.85%	91.32%	91.09%	78.10%	59.45%	68.77%	83.65%
ESTsecurity ALYac	87.36%	84.78%	86.07%	72.49%	68.75%	70.62%	80.92%
Faronics Anti-Virus	93.09%	90.95%	92.02%	75.87%	69.54%	72.71%	85.58%
Fortinet FortiClient	92.73%	91.25%	91.99%	71.56%	66.59%	69.07%	84.35%
G DATA Antivirus	77.00%	95.28%	86.14%	78.61%	72.19%	75.40%	82.56%
IKARUS anti.virus	96.49%	94.58%	95.53%	75.50%	71.13%	73.31%	88.13%
K7 Total Security	80.35%	76.98%	78.67%	59.78%	47.76%	53.77%	70.37%
Panda Endpoint Protection Plus	85.85%	78.94%	82.39%	46.36%	35.22%	40.79%	68.53%
Panda Free Antivirus	78.36%	74.03%	76.19%	46.29%	35.12%	40.71%	64.37%
Quick Heal Seqrite Endpoint Security	90.90%	89.54%	90.22%	73.67%	70.91%	72.29%	84.24%
Quick Heal Total Security	91.80%	89.21%	90.50%	73.69%	70.94%	72.31%	84.44%
Rising Security Cloud Client	77.18%	77.44%	77.31%	36.23%	27.62%	31.93%	62.18%
TeamViewer ITbrain Anti-Malware	92.32%	90.89%	91.60%	74.54%	68.97%	71.75%	84.99%
Tencent PC Manager	93.24%	91.70%	92.47%	75.81%	69.59%	72.70%	85.88%
Total Defense Internet Security	91.43%	90.88%	91.15%	74.38%	68.94%	71.66%	84.66%
Total Defense Premium	85.84%	89.87%	87.86%	74.47%	68.97%	71.72%	82.48%
VIPRE Advanced Security	92.36%	92.20%	92.28%	75.87%	69.59%	72.73%	85.76%
VirIT eXplorer PRO	34.36%	36.02%	35.19%	28.96%	25.24%	27.10%	32.49%
Wontok SafeCentral Security Suite	93.34%	92.92%	93.13%	86.94%	78.99%	82.96%	89.74%

*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 almost 400,000 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

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

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