virus BULLETIN

Covering the global threat landscape

VB100 COMPARATIVE REVIEW – DECEMBER 2017

Martijn Grooten

The need for IT security has grown considerably in the past decade. If you are responsible for IT security within your organization, this is no doubt something you have noticed in your daily work – but the plus side of the situation is that there are plenty of security solutions available to help mitigate the issues you and your organization are facing and to make your work easier.

While there exist a handful of well established products and brands, the majority of these solutions are produced by lesser known vendors, and you may, quite rightly, wonder: 'How can I be sure that the solution I am considering buying satisfies at least some minimum expectations?'

Virus Bulletin's certification tests in general, and the VB100 certification for anti-malware/endpoint security solutions in particular, can help provide an answer to this question. For those with purchasing power, we recommend looking for products that pass the VB100 test regularly. At the same time, we also encourage the reading of tests by other testing organizations that focus on other aspects of protection.

At the end of this, the last VB100 test of 2017, 31 products from 27 vendors were able to add a VB100 award to their tallies.

WILDLIST, CLEAN SET AND RAP

With hundreds of thousands of new malicious files being discovered every single day, you will probably not be surprised to learn that many such files are not strictly malicious: they may be broken versions of known malware, or files that simply engage in behaviour similar to that shown by malware. In quite a few cases, the maliciousness of a file depends on the availability of a remote server that delivers a payload and that may have been taken offline at the time of execution.

For a testing organization like *Virus Bulletin* this matters, as we can only expect security products to detect files that are proven to be malicious. Hence, for many years, we have based part of our certification requirements on full detection of the WildList, a regularly updated and strictly vetted list of malware known to have been seen in the wild.

We are equally strict, albeit in a different way, with our own 'clean set' – a set of clean files used to measure whether a product generates false positives. Here, we require files in the test set to be widely used in the real world and not to engage in any malicious or otherwise deceptive behaviour.

In order to provide some extra detail on the performance of the products in our tests, the VB100 reports have, for almost a decade, included 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.

RESULTS

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	12.2.876.11542	12.2.876.11542
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 85.3%

vb 100 VIRUS
Dec 2017
virusbtn.com
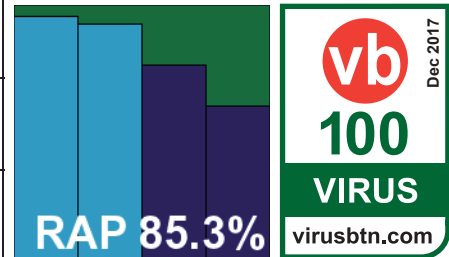
Arcabit AntiVirus		
	Windows 7	**Windows 10**
Main version	2017.11.02	2017.11.02
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 84.5%

vb 100 VIRUS
Dec 2017
virusbtn.com
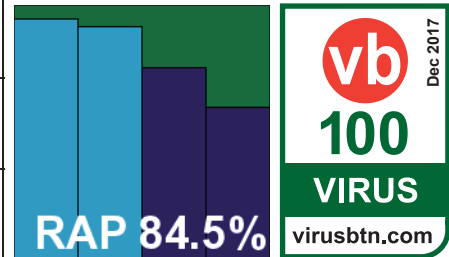
Avast Free Antivirus		
	Windows 7	**Windows 10**
Main version	17.7.2314	17.7.2314
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 86.6%

vb 100 VIRUS
Dec 2017
virusbtn.com
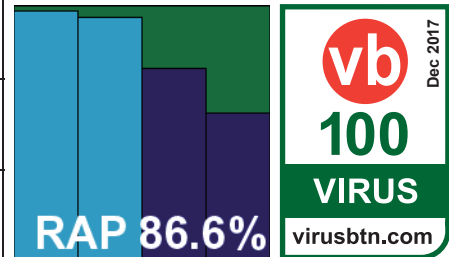
AVG Internet Security		
	Windows 7	**Windows 10**
Main version	1.211.3.13021	1.211.3.13021
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 87.1%

vb 100 VIRUS
Dec 2017
virusbtn.com
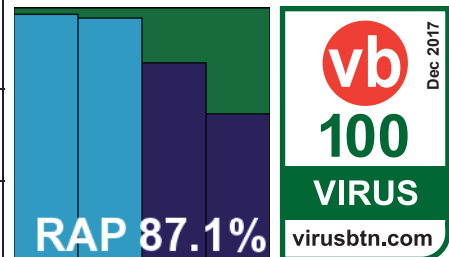
Bitdefender Endpoint Security

	Windows 7	Windows 10
Main version	6.2.25.953	6.2.25.953
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 87.7%

vb 100 VIRUS
Dec 2017
virusbtn.com
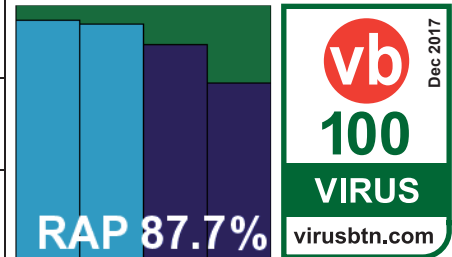
CompuClever Antivirus PLUS

	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

RAP 84.5%

vb 100 VIRUS
Dec 2017
virusbtn.com
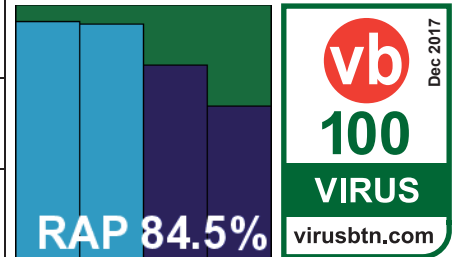
Cyren Command Anti-Malware

	Windows 7	Windows 10
Main version	5.1.38	5.1.38
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 69.7%

vb 100 VIRUS
Dec 2017
virusbtn.com
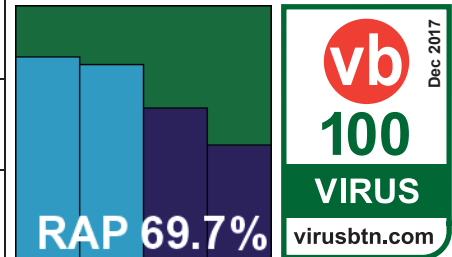
Defenx Security Suite

	Windows 7	Windows 10
Main version	15.1.0108	15.1.0108
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 78.5%

vb 100 VIRUS
Dec 2017
virusbtn.com
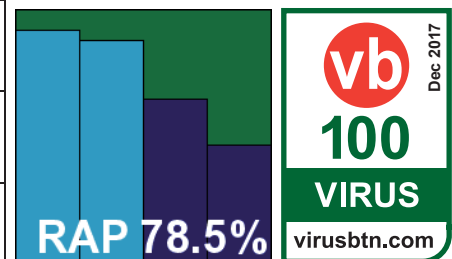
Emsisoft Anti-Malware

	Windows 7	Windows 10
Main version	2017.10.1.8165	2017.10.1.8165
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 85.9%

vb 100 VIRUS Dec 2017 virusbtn.com
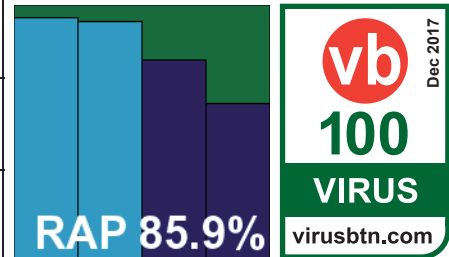
eScan Internet Security Suite for Windows

	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

RAP 87.4%

vb 100 VIRUS Dec 2017 virusbtn.com
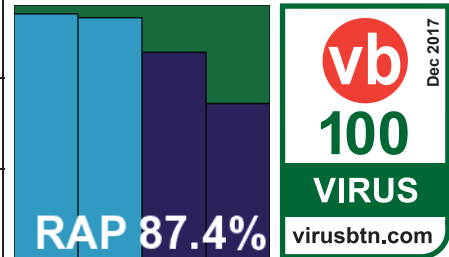
ESET Internet Security

	Windows 7	Windows 10
Main version	10.1.235.0	10.1.235.0
ItW catch rate	100.00%	100.00%
False positives	0	0

(Product not included in RAP tests)

vb 100 VIRUS Dec 2017 virusbtn.com

Essentware PCKeeper Antivirus PRO

	Windows 7	Windows 10
Main version	8.3.48.80	8.3.48.80
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 81.0%

vb 100 VIRUS Dec 2017 virusbtn.com
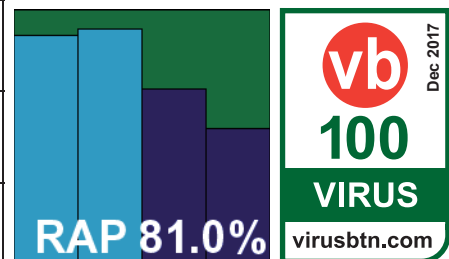
ESTsecurity ALYac

	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

RAP 84.8%
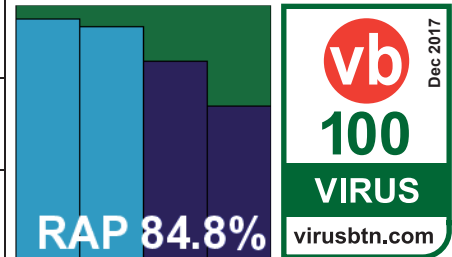
Faronics Anti-Virus

	Windows 7	Windows 10
Main version	4.12.3102.398	4.12.3102.398
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 87.0%
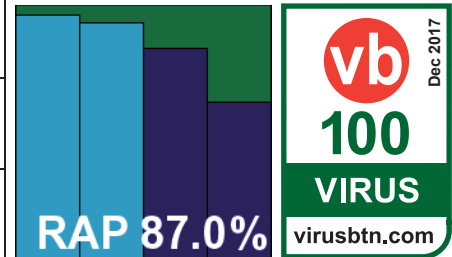
Fortinet FortiClient

	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

RAP 87.5%
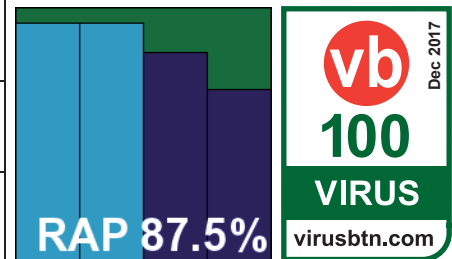
G DATA Antivirus

	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

RAP 89.9%
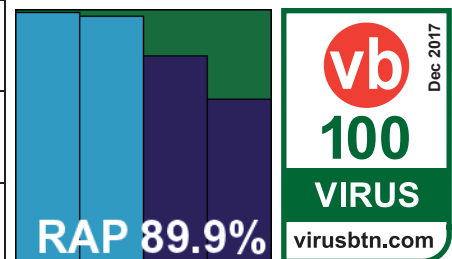
IKARUS anti.virus

	Windows 7	Windows 10
Main version	2.16.15	2.16.15
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 84.4%

vb 100 VIRUS Dec 2017 virusbtn.com
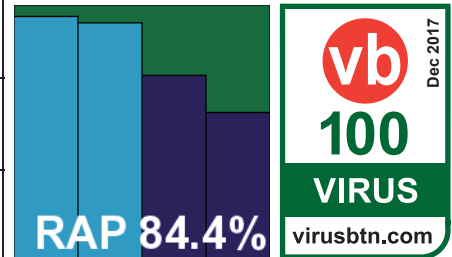
K7 Total Security

	Windows 7	Windows 10
Main version	15.1.0318	15.1.0318
ItW catch rate	100.00%	100.00%
False positives	15	0

FP 15
RAP 78.8%
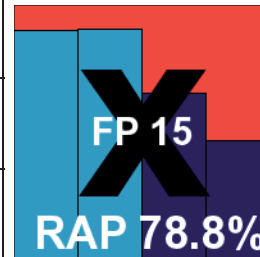
Kaspersky Endpoint Security 10 for Windows

	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

(Product not included in RAP tests)

vb 100 VIRUS Dec 2017 virusbtn.com

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

RAP 74.0%

vb 100 VIRUS Dec 2017 virusbtn.com
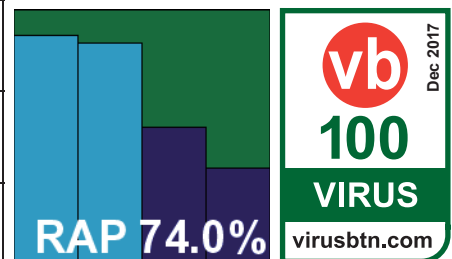
Panda Free Antivirus

	Windows 7	Windows 10
Main version	18.03.00	18.01.00
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 75.0%

vb 100 VIRUS virusbtn.com Dec 2017
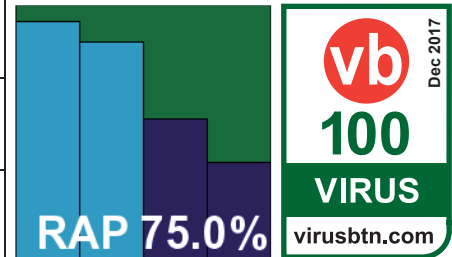
TACHYON Endpoint Security

	Windows 7	Windows 10
Main version	5.0.0.0	5.0.0.0
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 84.0%

vb 100 VIRUS virusbtn.com Dec 2017
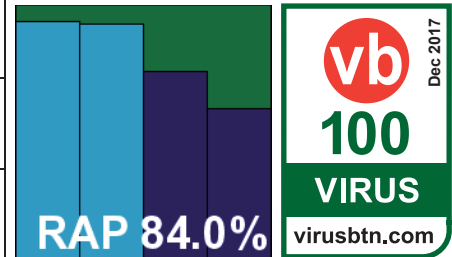
TeamViewer ITbrain Anti-Malware

	Windows 7	Windows 10
Main version	1.0.76588	1.0.76588
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 84.7%

vb 100 VIRUS virusbtn.com Dec 2017
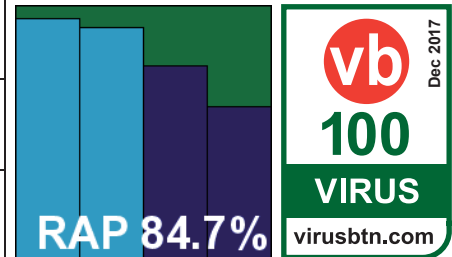
Tencent PC Manager

	Windows 7	Windows 10
Main version	12.3.26502.901	12.3.26502.901
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 87.2%

vb 100 VIRUS virusbtn.com Dec 2017
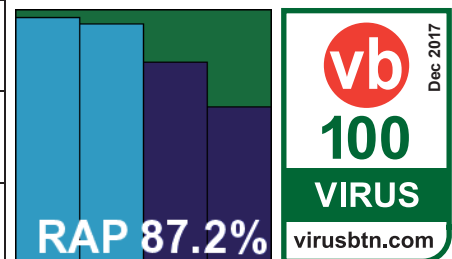
Tencent PC Manager – TAV

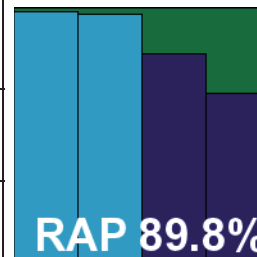|	Windows 7	Windows 10
Main version	12.3.26499.901	12.3.26499.901
ItW catch rate	100.00%	100.00%
False positives	0	0

(Product not included in RAP tests)

vb 100 VIRUS — Dec 2017 — virusbtn.com

Total Defense Internet Security

	Windows 7	Windows 10
Main version	9.0.0.645	9.0.0.747
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 85.2%

vb 100 VIRUS — Dec 2017 — virusbtn.com
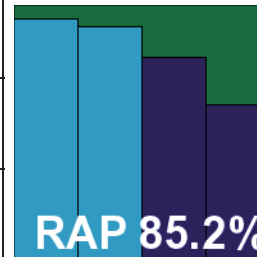
Total Defense Premium

	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

RAP 85.4%

vb 100 VIRUS — Dec 2017 — virusbtn.com
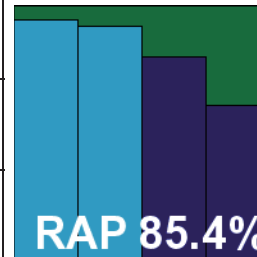
TrustPort Antivirus Sphere

	Windows 7	Windows 10
Main version	17.0.2.7025	17.0.2.7025
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 89.8%

vb 100 VIRUS — Dec 2017 — virusbtn.com

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

RAP 87.4%

vb 100 VIRUS
Dec 2017
virusbtn.com
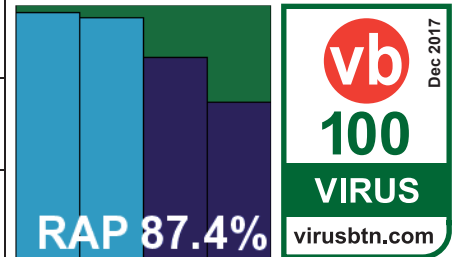
VirIT eXplorer PRO

	Windows 7	Windows 10
Main version	8.5.43	8.5.43
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 28.4%

vb 100 VIRUS
Dec 2017
virusbtn.com
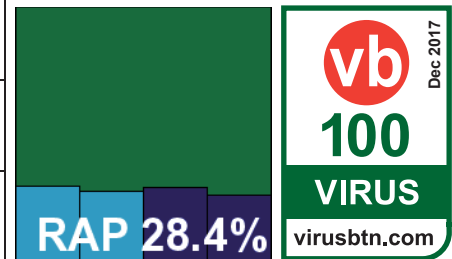
Wontok SafeCentral Security Suite

	Windows 7	Windows 10
Main version	2.0.1318	2.0.1318
ItW catch rate	100.00%	100.00%
False positives	0	0

RAP 88.2%

vb 100 VIRUS
Dec 2017
virusbtn.com
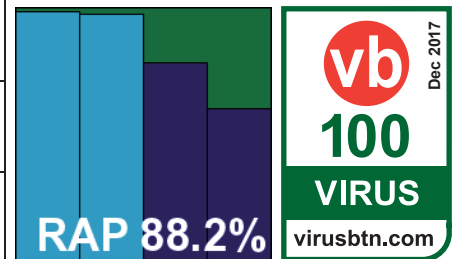
Zemana Endpoint Security

	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

RAP 81.2%

vb 100 VIRUS
Dec 2017
virusbtn.com
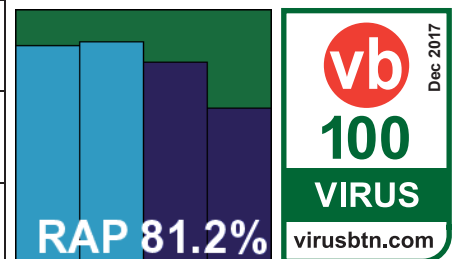
Certification tests	Windows 7				Windows 10				VB100
	FPs	FP rate	WildList misses	WildList catch rate	FPs	FP rate	WildList misses	WildList catch rate	
ad-aware antivirus pro	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Arcabit AntiVirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Avast Free Antivirus	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
Bitdefender Endpoint 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%	0	0.00%	0	100.00%	VIRUS 100
Defenx Security Suite	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
Emsisoft Anti-Malware	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

Certification tests contd.	Windows 7				Windows 10				VB100
	FPs	FP rate	WildList misses	WildList catch rate	FPs	FP rate	WildList misses	WildList catch rate	
IKARUS anti.virus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
K7 Total Security	15	0.004%	0	100.00%	0	0.00%	0	100.00%	X
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
TACHYON Endpoint Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	VIRUS 100
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
TrustPort Antivirus Sphere	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
Zemana Endpoint Security	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	94.67%	91.94%	93.31%	76.39%	60.11%	68.25%	84.95%
Arcabit AntiVirus	94.48%	91.41%	92.94%	75.42%	59.92%	67.67%	84.52%
Avast Free Antivirus	97.93%	95.27%	96.60%	75.32%	57.71%	66.51%	86.57%
AVG Internet Security	97.80%	95.23%	96.52%	75.18%	57.67%	66.43%	86.49%
Bitdefender Endpoint Security	92.93%	91.76%	92.34%	83.42%	69.15%	76.29%	86.99%
CompuClever Antivirus PLUS	91.88%	92.47%	92.18%	76.33%	60.07%	68.20%	84.18%
Cyren Command Anti-Malware	80.39%	76.47%	78.43%	59.57%	45.13%	52.35%	69.74%
Defenx Security Suite	91.62%	87.91%	89.77%	65.09%	46.90%	56.00%	78.51%
Emsisoft Anti-Malware	95.27%	92.67%	93.97%	78.19%	61.02%	69.60%	85.85%
eScan Internet Security Suite for Windows	96.33%	94.00%	95.16%	79.10%	61.02%	70.06%	86.79%
Essentware PCKeeper Antivirus PRO	88.76%	91.89%	90.33%	68.69%	53.16%	60.92%	80.52%
ESTsecurity ALYac	94.20%	90.84%	92.52%	79.61%	60.62%	70.11%	85.05%
Faronics Anti-Virus	95.18%	90.64%	92.91%	82.88%	61.95%	72.41%	86.08%
Fortinet FortiClient	93.94%	93.90%	93.92%	82.45%	67.72%	75.09%	87.64%
G DATA Antivirus	99.24%	97.77%	98.51%	81.94%	64.64%	73.29%	90.10%
IKARUS anti.virus	95.33%	92.75%	94.04%	72.28%	57.82%	65.05%	84.37%
K7 Total Security	90.07%	89.65%	89.86%	65.17%	46.90%	56.04%	78.59%
Panda Endpoint Protection Plus	86.74%	82.64%	84.69%	53.50%	37.53%	45.51%	71.63%
Panda Free Antivirus	92.51%	87.77%	90.14%	56.37%	38.87%	47.62%	75.97%
TACHYON Endpoint Security	93.50%	92.11%	92.80%	73.76%	59.08%	66.42%	84.01%
TeamViewer ITbrain Anti-Malware	94.60%	91.40%	93.00%	76.36%	60.09%	68.23%	84.74%
Tencent PC Manager	96.41%	94.60%	95.51%	79.18%	61.61%	70.39%	87.14%
Total Defense Internet Security	94.50%	91.32%	92.91%	78.88%	60.45%	69.67%	85.16%
Total Defense Premium	93.78%	92.29%	93.04%	79.47%	60.58%	70.03%	85.37%‡
TrustPort Antivirus Sphere	98.12%	97.38%	97.75%	82.02%	66.39%	74.21%	89.90%
VIPRE Advanced Security	96.90%	94.62%	95.76%	79.39%	61.67%	70.53%	87.35%
VirIT eXplorer PRO	29.81%	27.66%	28.74%	29.06%	26.49%	27.77%	28.42%
Wontok SafeCentral Security Suite	98.26%	97.03%	97.65%	80.25%	60.75%	70.50%	88.60%
Zemana Endpoint Security	75.48%	78.93%	77.21%	79.23%	61.34%	70.28%	74.90%

[*]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	95.66%	93.01%	94.33%	76.39%	60.11%	68.25%	85.64%
Arcabit AntiVirus	94.30%	91.46%	92.88%	75.42%	59.97%	67.69%	84.49%
Avast Free Antivirus	97.93%	95.31%	96.62%	75.32%	57.71%	66.51%	86.58%
AVG Internet Security	97.12%	96.13%	96.62%	81.19%	59.02%	70.10%	87.78%
Bitdefender Endpoint Security	94.77%	93.19%	93.98%	84.92%	69.45%	77.18%	88.38%
CompuClever Antivirus PLUS	94.44%	91.56%	93.00%	76.33%	60.07%	68.20%	84.73%
Cyren Command Anti-Malware	79.49%	76.95%	78.22%	59.57%	45.13%	52.35%	69.60%
Defenx Security Suite	91.61%	87.91%	89.76%	64.66%	46.97%	55.81%	78.45%
Emsisoft Anti-Malware	94.72%	93.62%	94.17%	78.19%	61.02%	69.60%	85.98%
eScan Internet Security Suite for Windows	95.74%	95.91%	95.82%	83.07%	61.65%	72.36%	88.00%
Essentware PCKeeper Antivirus PRO	91.15%	92.21%	91.68%	69.06%	53.31%	61.19%	81.51%
ESTsecurity ALYac	94.29%	91.47%	92.88%	75.83%	60.01%	67.92%	84.56%
Faronics Anti-Virus	96.33%	95.13%	95.73%	82.88%	61.95%	72.41%	87.96%
Fortinet FortiClient	93.15%	94.07%	93.61%	82.37%	67.68%	75.02%	87.42%
G DATA Antivirus	98.67%	97.16%	97.91%	81.73%	64.56%	73.14%	89.66%
IKARUS anti.virus	95.33%	92.75%	94.04%	72.28%	57.82%	65.05%	84.37%
K7 Total Security	89.72%	91.20%	90.46%	65.09%	46.90%	56.00%	78.97%
Panda Endpoint Protection Plus	92.54%	90.83%	91.68%	53.56%	37.53%	45.54%	76.30%
Panda Free Antivirus	94.01%	82.24%	88.12%	53.77%	37.84%	45.81%	74.02%
TACHYON Endpoint Security	93.32%	92.07%	92.69%	73.79%	59.08%	66.43%	83.94%
TeamViewer ITbrain Anti-Malware	94.45%	91.40%	92.93%	76.36%	60.09%	68.23%	84.69%
Tencent PC Manager	96.74%	94.38%	95.56%	79.26%	61.63%	70.45%	87.19%
Total Defense Internet Security	94.33%	91.31%	92.82%	79.47%	60.58%	70.03%	85.22%
Total Defense Premium	94.53%	91.45%	92.99%	79.72%	60.60%	70.16%	85.38%
TrustPort Antivirus Sphere	98.28%	97.09%	97.68%	81.57%	66.31%	73.94%	89.77%
VIPRE Advanced Security	96.99%	94.66%	95.83%	79.39%	61.67%	70.53%	87.39%
VirIT eXplorer PRO	29.79%	27.55%	28.67%	29.06%	26.49%	27.77%	28.37%
Wontok SafeCentral Security Suite	98.28%	97.04%	97.66%	76.39%	60.11%	68.25%	87.86%
Zemana Endpoint Security	96.26%	95.65%	95.95%	79.23%	61.34%	70.28%	87.40%

*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 quadrant - December 2017
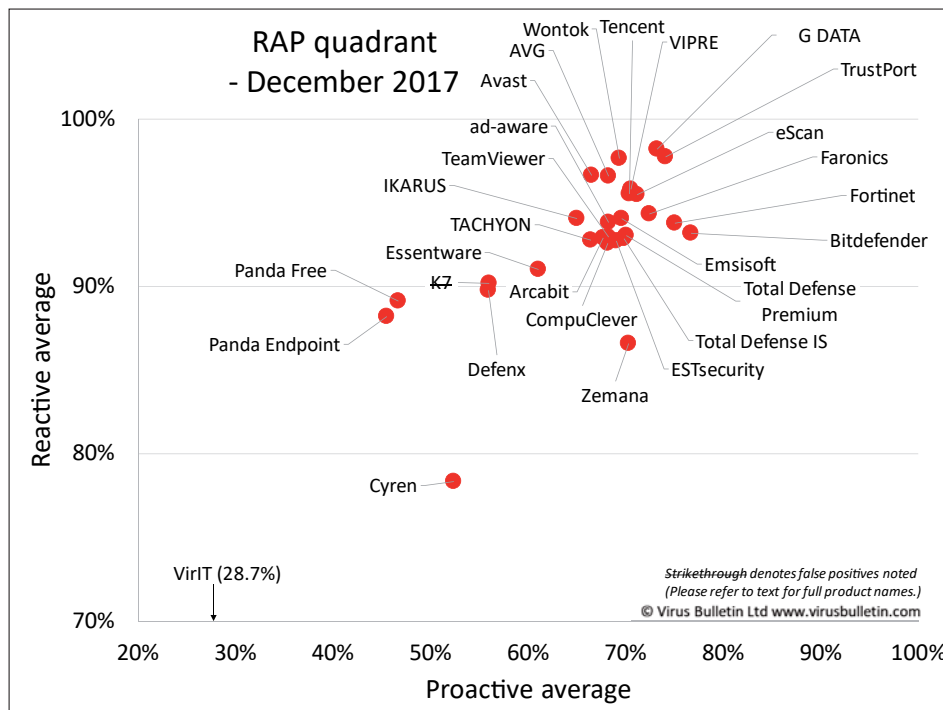
APPENDIX: THE TEST SET-UP

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.