AUGUST 2017

virus BULLETIN

Covering the global threat landscape

VB100 COMPARATIVE REVIEW – AUGUST 2017

Martijn Grooten

Another security testing organization stated recently that it has now seen 640 million different malware samples – a number that continues to grow rapidly.

The number itself isn't particularly meaningful – indeed, thanks to various kinds of polymorphism among malware, a lot of these 640 million samples are essentially the same – but the important message remains: there is a lot of malware out there. Therefore, if you hear a security vendor claiming that 'signature-based anti-virus is no longer good enough', they are right, and in fact this has been the case for at least a decade.

It is for this reason that endpoint security solutions include various kinds of heuristics that help them identify malware that has not previously been seen. And as we have shown repeatedly in the VB100 tests, it does a more than decent job of this: a version of the product that has been disconnected from the Internet for a period of time, and thus hasn't received any new updates for that period, still detects a decent percentage of new malware – for some products well over 50%.

Such (static) detection rates are impressive, but they are not good enough when it comes to known and confirmed malware. For such malware, the very *least* one would expect of a good anti-malware solution is that it detects them all, without exception, and does so without blocking a single file from a collection of recent and widely used legitimate software.

For many years, these have been the criteria for earning a VB100 award – one of longest running and most well respected awards for endpoint security solutions, and the one to look for to check that a product satisfies minimum standards. In this month's VB100 test, we put 30 solutions from 27 vendors through their paces; 24 of them earned a VB100 award.

We remind readers that our test only gives a very partial picture of product performance; we recommend readers of this report also read reports from other testing organizations, for instance to find out how products fare when tasked with blocking the execution of malware.

MISSING TROJANS

All but three products blocked 100% of the malware in the WildList, a vetted and curated list of malware known to have been seen in the wild. This is the least you should expect from an anti-malware product – i.e. that it blocks known malware still lurking on your systems.

The four files that were missed were all common trojans: Beta Bot, Perkesh, Qadars and Fareit.

On top of the near-perfect performance against the WildList, we found that the solutions recognized more than two thirds of very recent malware files as malicious – with some products performing even better than that. Given that this is just one of many detection layers that exist in anti-malware solutions, this can be considered a good performance.

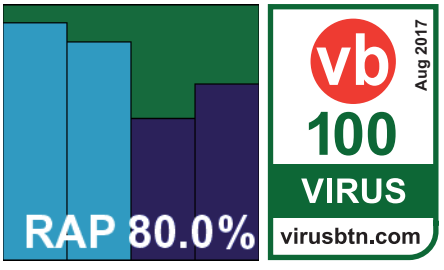
Interestingly, when it came to the proactive part of the RAP test, malware seen four days after products had been frozen was especially difficult to detect, which suggests that new or significantly modified malware families were launched around that time; malware seen later was easier to detect and thus the second proactive RAP score (against a set of malware discovered 6 to 10 days after product updates were frozen) was higher for most products than the first one (against samples discovered 1 to 5 days after product updates were frozen).

RESULTS

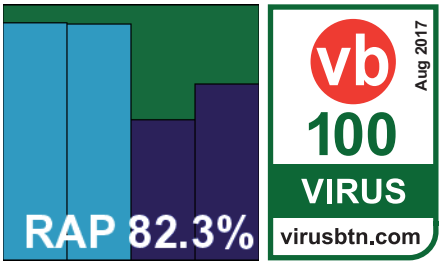
In the following results, the RAP images display an average of the RAP scores across the two platforms.

ISSN 1749-7027

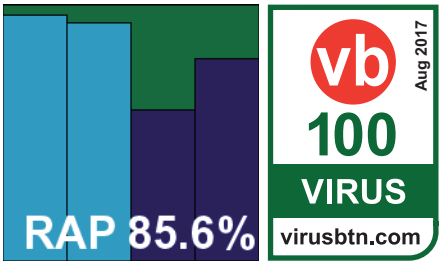
ad-aware antivirus pro		
	Windows 7	**Windows 10**
Main version	12.0.649.11190	12.0.649.11190
Update versions	7.72683, 7.72456, 7.72555, 7.72755	7.72682, 7.72455, 7.72555, 7.72788
ItW catch rate	100.00%	100.00%
False positives	0	0



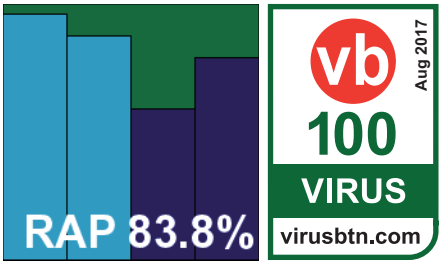
Arcabit AntiVirus		
	Windows 7	**Windows 10**
Main version	2017.08.07	2017.08.07
Update versions	2017.07.21, 2017.07.28, 2017.08.11	2017.07.21, 2017.07.28, 2017.08.11
ItW catch rate	100.00%	100.00%
False positives	0	0



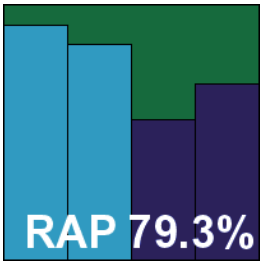
Avast Free Antivirus		
	Windows 7	**Windows 10**
Main version	17.5.2303	17.5.2303
Update versions	17080700, 17072102, 17072810, 17081108	17080700, 17072100, 17072810, 17081108
ItW catch rate	100.00%	100.00%
False positives	0	0



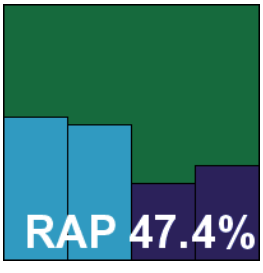
AVG Internet Security		
	Windows 7	**Windows 10**
Main version	1.162.2.62416	1.191.3.4720
Update versions	17.2.3419.0/17080700, 17.5.3022/17072006, 17.5.3022/17072806, 17.5.3022/17081102	17.5.3022/17080700, 17072200, 17073002, 17081300
ItW catch rate	100.00%	100.00%
False positives	0	0



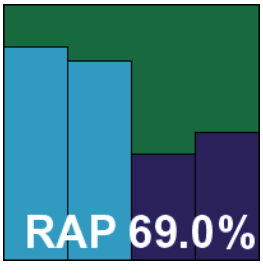
CompuClever Antivirus PLUS		
	Windows 7	**Windows 10**
Main version	19.6.0.326	19.6.0.326
Update versions	7.72684, 7.72492, 7.72554, 7.72787	7.72682, 7.72439, 7.72456, 7.72738
ItW catch rate	100.00%	100.00%
False positives	0	0



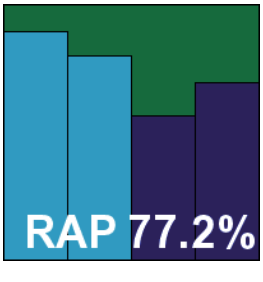
Cyren Command Anti-Malware		
	Windows 7	**Windows 10**
Main version	5.1.38	5.1.38
Update versions	5.4.25	5.4.25
ItW catch rate	99.97%	99.97%
False positives	0	0



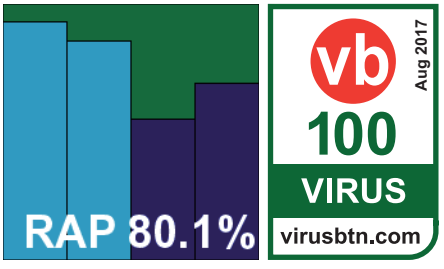
Defenx Security Suite		
	Windows 7	**Windows 10**
Main version	15.1.0107	15.1.0107
Update versions	10.20.24217, 15.1.0106/10.19.24053, 15.1.0107/10.20.24130, 15.1.0107/10.21.24276	10.20.24215, 10.19.24056, 10.20.24130, 10.21.24277
ItW catch rate	100.00%	100.00%
False positives	0	0



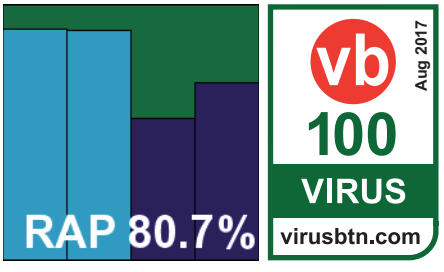
Emsisoft Anti-Malware		
	Windows 7	**Windows 10**
Main version	7.72684	7.72682
Update versions	7.72637, 7.72541, 7.72733	7.72808, 7.72613, 7.72734
ItW catch rate	100.00%	100.00%
False positives	0	0



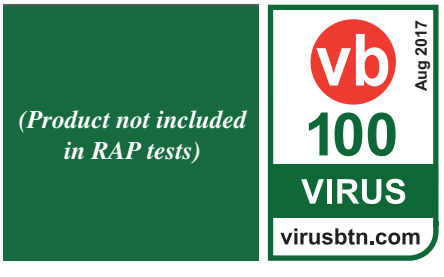
Endpoint Security by Bitdefender		
	Windows 7	**Windows 10**
Main version	6.2.22.923	6.2.22.923
Update versions	6.2.21.908/7.72682, 6.2.21.908/7.72436, 6.2.21.908/7.72543, 6.2.21.908/7.72737	7.72682, 7.72495, 7.72541, 7.72732
ItW catch rate	100.00%	100.00%
False positives	0	0



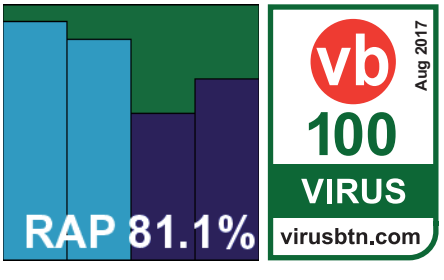
eScan Internet Security Suite for Windows		
	Windows 7	**Windows 10**
Main version	14.0.14000.1979	14.0.1400.1979
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0



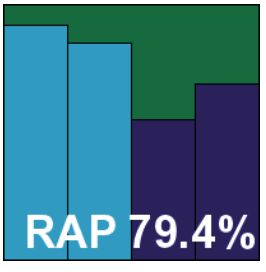
ESET Internet Security		
	Windows 7	**Windows 10**
Main version	10.1.215.0	10.1.215.0
Update versions	15873, 10.0.386.0/15787, 10.0.386.0/15826, 10.1.215.0/15903	15873, 10.1.210.0/15783, 10.1.210.0/15855, 10.1.210.0/15899
ItW catch rate	100.00%	100.00%
False positives	0	0



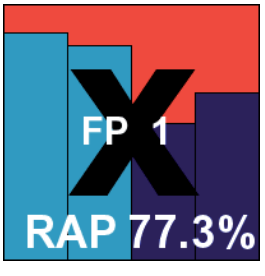
Essentware PCKeeper Antivirus PRO		
	Windows 7	**Windows 10**
Main version	8.3.46.16	8.3.46.16
Update versions	8.14.21.128, 8.3.44.104/8.14.18.84, 8.3.46.6/8.14.20.66, 8.3.46.22/8.14.22.182	8.14.21.128, 8.3.44.104/8.14.18.86, 8.3.46.14/8.14.21.16, 8.3.46.22/8.14.22.190
ItW catch rate	100.00%	100.00%
False positives	0	0



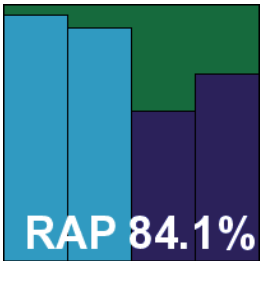
ESTsoft ALYac		
	Windows 7	**Windows 10**
Main version	3.0.1.3	3.0.1.3
Update versions	16.7.12.1/3.0.1.3.30307/656388.2017080721/7.72680/9859244.20170807, 650954.2017072209/7.72430/9584090.20170721, 653973.2017072913/7.72537/9742265.20170728, 57516.2017081221/7.72734/9906442.20170812	16.7.12.1/3.0.1.3.30307/656388.2017080721/7.72680/9859244.20170807, 650939.2017072219/7.72443/9600401.20170722, 655789.2017080323/7.72612/9803388.20170803, 657518.2017081301/7.72734/9906442.20170812
ItW catch rate	99.97%	100.00%
False positives	0	0



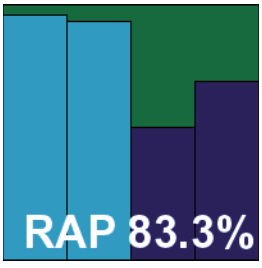
Fortinet FortiClient		
	Windows 7	**Windows 10**
Main version	5.4.1.0840	5.4.1.0840
Update versions	5.00247/50.00768, 50.00434, 50.00560, 50.00924	5.00247/50.00766, 5.4.1.0840/5.00247/50.00467, 50.00550, 50.00872
ItW catch rate	100.00%	100.00%
False positives	1	1



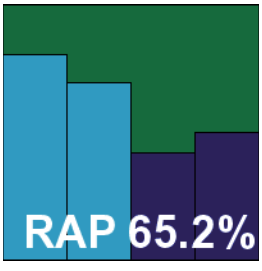
G DATA Antivirus		
	Windows 7	**Windows 10**
Main version	25.3.0.1	25.3.0.3
Update versions	AVA 25.13735/GD 25.10172, AVA 25.13539/GD 25.10071, AVA 25.13607/GD 25.10109, AVA 25.13836/GD 25.10200	AVA 25.13735/GD 25.10171, AVA 25.13487/GD 25.10049, AVA 25.13599/GD 25.10106, AVA 25.13789/GD 25.10198
ItW 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
Update versions	99606, 99553, 99577, 99619	99606, 99555, 99592, 99619
ItW catch rate	100.00%	100.00%
False positives	0	0



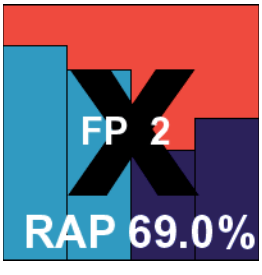
K7 Total Security		
	Windows 7	**Windows 10**
Main version	15.1.0312	15.1.0312
Update versions	10.20.24219, 15.1.0311/10.19.24070, 15.1.012/10.20.24168, 15.1.0312/10.21.24304	10.20.24218, 15.1.0311/10.19.24062, 15.1.0313/10.22.24326, 15.1.0312/10.21.24287
ItW catch rate	100.00%	100.00%
False positives	0	0



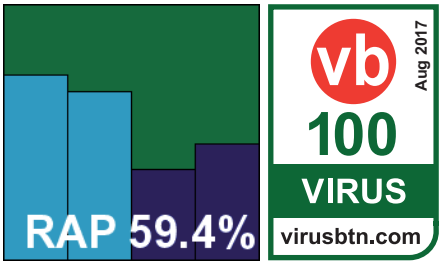
Kaspersky Endpoint Security 10 for Windows		
	Windows 7	**Windows 10**
Main version	10.3.0.6294 AES256	10.3.0.6294 AES256
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0

(Product not included in RAP tests)

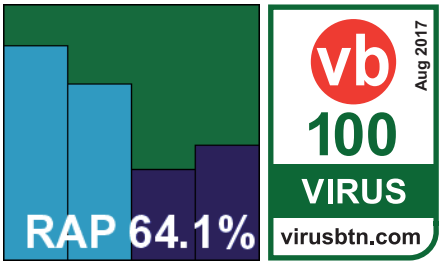
NANO Antivirus Pro		
	Windows 7	**Windows 10**
Main version	1.0.94.83913	1.0.94.83639
Update versions	0.14.28.9969, 1.0.76.83123/0.14.28.9707, 1.0.94.83639/0.14.28.9707, 1.0.94.83913/0.14.28.9969	0.14.28.9965, 1.0.92.83491/0.14.28.9883, 1.0.94.83639/0.14.28.9953, 1.0.94.83913/0.14.29.10008
ItW catch rate	100.00%	100.00%
False positives	2	1



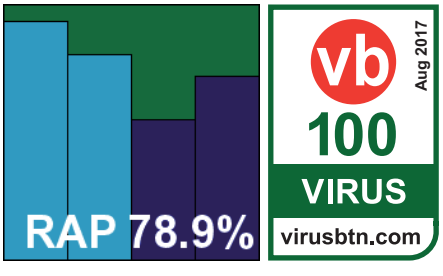
Panda Endpoint Protection Plus		
	Windows 7	**Windows 10**
Main version	7.70.0	7.70.0
Update versions	7.71.0	7.71.0
ItW catch rate	100.00%	100.00%
False positives	0	0



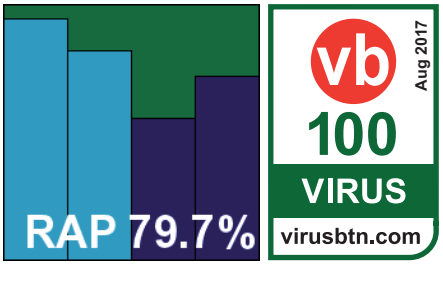
Panda Free Antivirus		
	Windows 7	**Windows 10**
Main version	18.01.00	18.01.00
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0



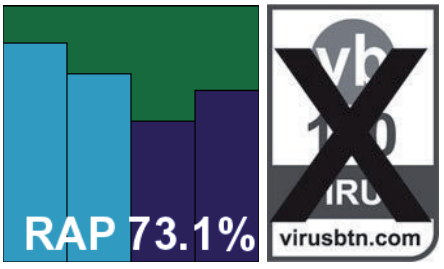
Quick Heal Seqrite Endpoint Security		
	Windows 7	**Windows 10**
Main version	17.00	17.00
Update versions	10.2.3.1	10.2.3.1
ItW catch rate	100.00%	100.00%
False positives	0	0



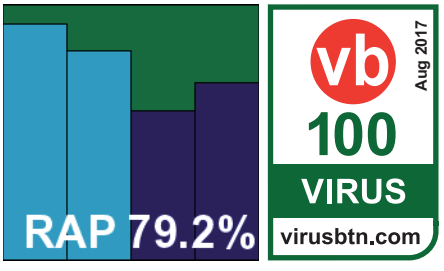
Quick Heal Total Security		
	Windows 7	**Windows 10**
Main version	17.00	17.00
Update versions	10.0.1.26	10.0.1.26
ItW catch rate	100.00%	100.00%
False positives	0	0



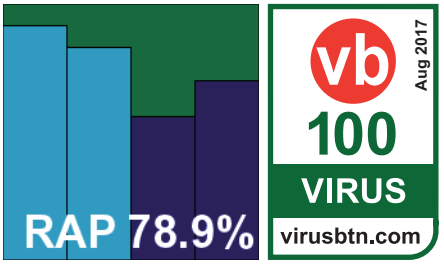
STOPzilla AntiVirus 8.0		
	Windows 7	**Windows 10**
Main version	8.0.3.270 PRO	8.0.3.270
Update versions	2.15.1.170052/7.72684, 7.72533, 7.72615, 7.72747	2.15.1.170052/7.72684, N/A, 7.72620, 7.72804
ItW catch rate	99.97%	100.00%
False positives	0	0



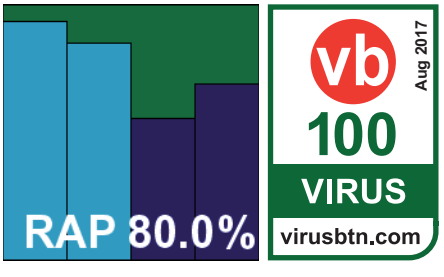
TeamViewer ITbrain Anti-Malware		
	Windows 7	**Windows 10**
Main version	1.0.76588	1.0.76588
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0



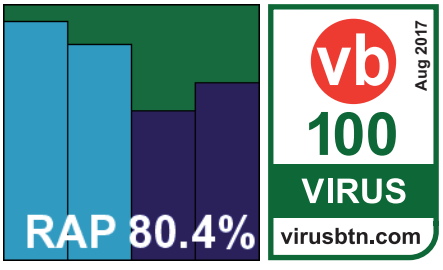
Tencent PC Manager		
	Windows 7	**Windows 10**
Main version	12.3.264.901	12.3.26464.901
Update versions	12.3.26458.901, 12.3.26462.901, 12.3.26464.901	12.3.26467.901, 12.3.26464.901, 12.26467.901
ItW catch rate	100.00%	100.00%
False positives	0	0



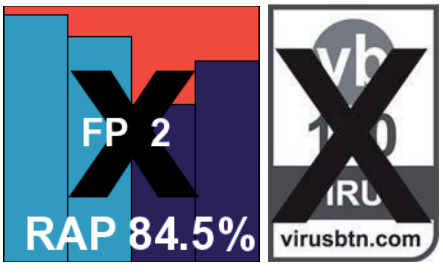
Total Defense Internet Security Suite		
	Windows 7	**Windows 10**
Main version	9.0.0.645	9.0.0.645
Update versions	3.0.2.1015	3.0.2.1015
ItW catch rate	100.00%	100.00%
False positives	0	0



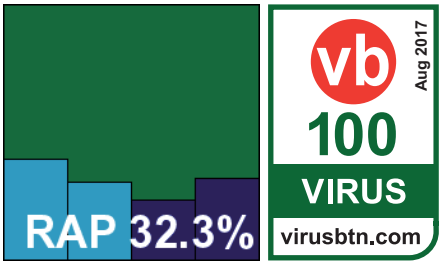
Total Defense Premium		
	Windows 7	**Windows 10**
Main version	9.0.0.645	9.0.0.645
Update versions	3.0.2.1015	3.0.2.1015
ItW catch rate	100.00%	100.00%
False positives	0	0



TrustPort Antivirus Sphere		
	Windows 7	**Windows 10**
Main version	17.0.2.7025	17.0.2.7025
Update versions	14787/7.72683, 14742/7.72510, 14769/7.72612, 14814/7.72741	14787/7.72681, 17.0.1.7022/14732/7.72491, 17.0.1.7022/14767/7.72606, 17.0.1.7022/14829/7.72783
ItW catch rate	100.00%	100.00%
False positives	2	2



VirIT eXplorer PRO		
	Windows 7	**Windows 10**
Main version	8.4.84	8.4
Update versions	8.4, 8.4.77, 8.4.81, 8.4.88	8.4.84, 8.4.73, 8.4.83, 8.4.88
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%	2	99.97%	0	0.00%	2	99.97%	X
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
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
ESTsoft ALYac	0	0.00%	2	99.97%	0	0.00%	0	100.00%	X
Fortinet FortiClient	1	0.0003%	0	100.00%	1	0.0003%	0	100.00%	X
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%	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	
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
NANO Antivirus Pro	2	0.0005%	0	100.00%	1	0.0003%	0	100.00%	X
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
STOPzilla AntiVirus 8.0	0	0.00%	2	99.97%	0	0.00%	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
Total Defense Internet Security Suite	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	2	0.0005%	0	100.00%	2	0.0005%	0	100.00%	X
VirIT eXplorer PRO	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	92.57%	86.54%	89.55%	55.21%	68.88%	62.04%	80.38%
Arcabit AntiVirus	92.94%	92.01%	92.48%	54.85%	68.76%	61.80%	82.25%
Avast Free Antivirus	95.79%	92.53%	94.16%	58.65%	78.55%	68.60%	85.64%
AVG Internet Security	95.79%	92.43%	94.11%	58.63%	78.55%	68.59%	85.60%
CompuClever Antivirus PLUS	91.66%	83.01%	87.34%	55.17%	68.76%	61.97%	78.88%
Cyren Command Anti-Malware	55.83%	53.70%	54.76%	29.55%	37.00%	33.27%	47.60%
Defenx Security Suite	84.59%	80.45%	82.52%	41.48%	49.84%	45.66%	70.23%
Emsisoft Anti-Malware	88.58%	79.16%	83.87%	56.59%	69.28%	62.94%	76.89%
Endpoint Security by Bitdefender	92.16%	85.27%	88.72%	54.83%	68.76%	61.79%	79.74%
eScan Internet Security Suite for Windows	93.21%	92.47%	92.84%	55.05%	69.08%	62.06%	82.58%
Essentware PCKeeper Antivirus PRO	93.44%	85.97%	89.71%	57.10%	70.68%	63.89%	81.10%
ESTsoft ALYac	92.18%	85.25%	88.72%	54.72%	68.76%	61.74%	79.72%
Fortinet FortiClient	88.40%	80.94%	84.67%	53.34%	65.30%	59.32%	76.22%
G DATA Antivirus	95.92%	86.04%	90.98%	58.08%	72.60%	65.34%	82.44%
IKARUS anti.virus	96.01%	93.84%	94.93%	51.81%	69.78%	60.79%	83.55%
K7 Total Security	82.17%	70.27%	76.22%	41.84%	49.90%	45.87%	66.10%
NANO Antivirus Pro	85.39%	73.94%	79.66%	44.39%	55.27%	49.83%	69.72%
Panda Endpoint Protection Plus	71.98%	64.54%	68.26%	35.04%	43.74%	39.39%	58.64%
Panda Free Antivirus	82.39%	70.67%	76.53%	35.22%	43.48%	39.35%	64.14%
Quick Heal Seqrite Endpoint Security	91.73%	79.32%	85.52%	54.99%	71.58%	63.28%	78.11%
Quick Heal Total Security	93.62%	82.22%	87.92%	54.99%	71.58%	63.28%	79.71%
STOPzilla AntiVirus 8.0	85.46%	76.29%	80.87%	54.96%	67.16%	61.06%	74.27%
TeamViewer ITbrain Anti-Malware	93.02%	82.37%	87.70%	55.26%	68.85%	62.06%	79.15%
Tencent PC Manager	94.23%	89.86%	92.04%	55.50%	69.57%	62.54%	82.21%
Total Defense Internet Security Suite	93.74%	83.85%	88.80%	55.26%	68.85%	62.06%	79.88%
Total Defense Premium	94.09%	82.13%	88.11%	61.19%	69.43%	65.31%	80.51%
TrustPort Antivirus Sphere	96.22%	89.01%	92.61%	61.54%	78.32%	69.93%	85.05%
VirIT eXplorer PRO	39.11%	30.11%	34.61%	23.24%	31.53%	27.39%	32.20%

*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.

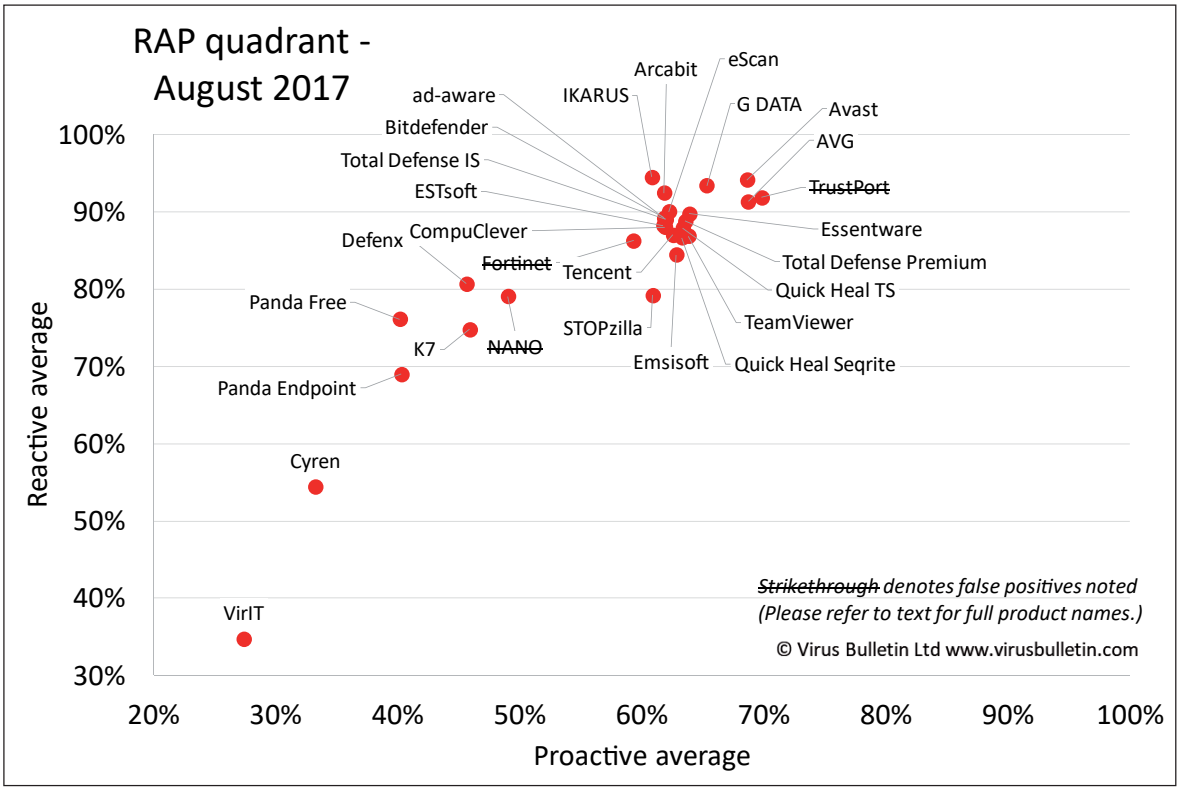
‡Weighted average gives equal emphasis to the two reactive weeks and the whole proactive part.

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	92.88%	84.02%	88.45%	54.88%	68.79%	61.84%	79.58%
Arcabit AntiVirus	92.94%	91.99%	92.46%	54.85%	68.76%	61.80%	82.24%
Avast Free Antivirus	95.79%	92.50%	94.14%	58.63%	78.55%	68.59%	85.63%
AVG Internet Security	95.29%	81.86%	88.57%	59.03%	78.55%	68.79%	81.98%
CompuClever Antivirus PLUS	92.22%	85.29%	88.75%	54.77%	68.73%	61.75%	79.75%
Cyren Command Anti-Malware	56.12%	51.96%	54.04%	29.41%	37.00%	33.20%	47.09%
Defenx Security Suite	82.40%	75.27%	78.83%	41.35%	49.84%	45.60%	67.76%
Emsisoft Anti-Malware	89.98%	80.00%	84.99%	56.16%	69.20%	62.68%	77.55%
Endpoint Security by Bitdefender	93.81%	85.71%	89.76%	54.83%	68.76%	61.79%	80.44%
eScan Internet Security Suite for Windows	87.14%	87.20%	87.17%	55.48%	69.17%	62.32%	78.89%
Essentware PCKeeper Antivirus PRO	93.18%	86.50%	89.84%	57.10%	70.68%	63.89%	81.19%
ESTsoft ALYac	91.77%	83.81%	87.79%	54.72%	68.76%	61.74%	79.11%
Fortinet FortiClient	89.05%	86.72%	87.88%	53.28%	65.30%	59.29%	78.35%
G DATA Antivirus	95.88%	95.82%	95.85%	57.97%	72.60%	65.28%	85.66%
IKARUS anti.virus	95.45%	92.76%	94.11%	51.81%	69.78%	60.79%	83.00%
K7 Total Security	78.53%	68.18%	73.35%	41.83%	49.90%	45.86%	64.19%
NANO Antivirus Pro	82.56%	74.35%	78.45%	41.52%	54.84%	48.18%	68.36%
Panda Endpoint Protection Plus	72.44%	67.04%	69.74%	35.72%	46.61%	41.16%	60.22%
Panda Free Antivirus	85.11%	66.37%	75.74%	35.50%	46.38%	40.94%	64.14%
Quick Heal Seqrite Endpoint Security	94.36%	81.23%	87.80%	54.99%	71.58%	63.28%	79.63%
Quick Heal Total Security	94.48%	81.31%	87.89%	55.05%	71.72%	63.38%	79.72%
STOPzilla AntiVirus 8.0	84.74%	70.40%	77.57%	54.68%	66.72%	60.70%	71.95%
TeamViewer ITbrain Anti-Malware	91.00%	81.03%	86.02%	61.57%	69.49%	65.53%	79.19%
Tencent PC Manager	88.71%	75.35%	82.03%	55.50%	69.57%	62.54%	75.53%
Total Defense Internet Security Suite	92.56%	86.12%	89.34%	54.83%	68.76%	61.79%	80.16%
Total Defense Premium	92.56%	86.37%	89.47%	54.83%	68.76%	61.79%	80.24%
TrustPort Antivirus Sphere	96.10%	86.15%	91.13%	61.19%	78.23%	69.71%	83.99%
VirIT eXplorer PRO	39.14%	30.76%	34.95%	23.24%	31.53%	27.39%	32.43%

*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.



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.

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, Ionuţ 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/