



virus

BULLETIN

Covering the global threat landscape

VB100 COMPARATIVE REVIEW – JUNE 2017

Martijn Grooten

For me, one of the most telling anecdotes of this May's WannaCry outbreak was that of an employee who brought their infected home laptop to work to have it disinfected, but in doing so accidentally infected the company network¹.

Unsurprisingly, when WannaCry started spreading on that doomed Friday, it was detected by few (heuristic) anti-virus signatures. However, such signatures are only half of the story: the malware was picked up in many cases by dynamic protection, for example anti-ransomware technology.

Still, the fact that WannaCry continued to spread across internal networks many days after the initial outbreak, sometimes even to machines without a direct connection to the Internet, is a good illustration of why static detection of malware remains an important first line of defence against malware: it has the potential to remove the actual threat rather than having to hope that it will be blocked once activated. It also explains why so many vendors continue to devote plentiful resources to making sure their static detection remains strong.

It is static detection that is put under the spotlight in the VB100 tests, which effectively ask: do anti-virus products manage to fulfil the important task of (statically) detecting malware shortly after it has been discovered? A good anti-virus product should have little problem passing this test most, if not all of the time – as such, we encourage readers to check the full VB100 test history for each product. To get a fuller picture of products' capabilities we also encourage

readers to consult reports by other testers, that may focus on other aspects of blocking malware.

This month's test saw 33 solutions from 29 different vendors from around the world on our test bench; 29 of the products passed the test and earned VB100 certification.

As in the last test, the products were run on both *Windows 7* and *Windows 10*. Though there was generally little difference in the products' performance on the two platforms, this did allow us to make sure they ran properly on the two most commonly used desktop operating systems.

We also noticed that various products make different choices when it comes to balancing performance and early detection, and it wasn't always trivial to trigger the scanning of all of the samples used in the test; however, the lessons learned from the last test meant that this caused fewer headaches than before.

PROACTIVE DETECTION: NOT PERFECT, BUT NOT POWERLESS EITHER

Though anti-virus is often criticized for its apparent inability to detect new malware, the reality is a bit more complicated. While malware downloaders are indeed constantly changing in an attempt to evade signatures, the actual malicious payload doesn't change (in a significant way) nearly as often.

For that reason, even static anti-virus engines aren't entirely powerless against future malware. Our RAP tests are a good demonstration of this.

The first ('Reactive') part of the two-part RAP test shows how well products detect malware seen in the wild up to ten days previously. Unsurprisingly, the newer the malware gets, the lower detection becomes, but even the newest malware is detected with a probability of at least

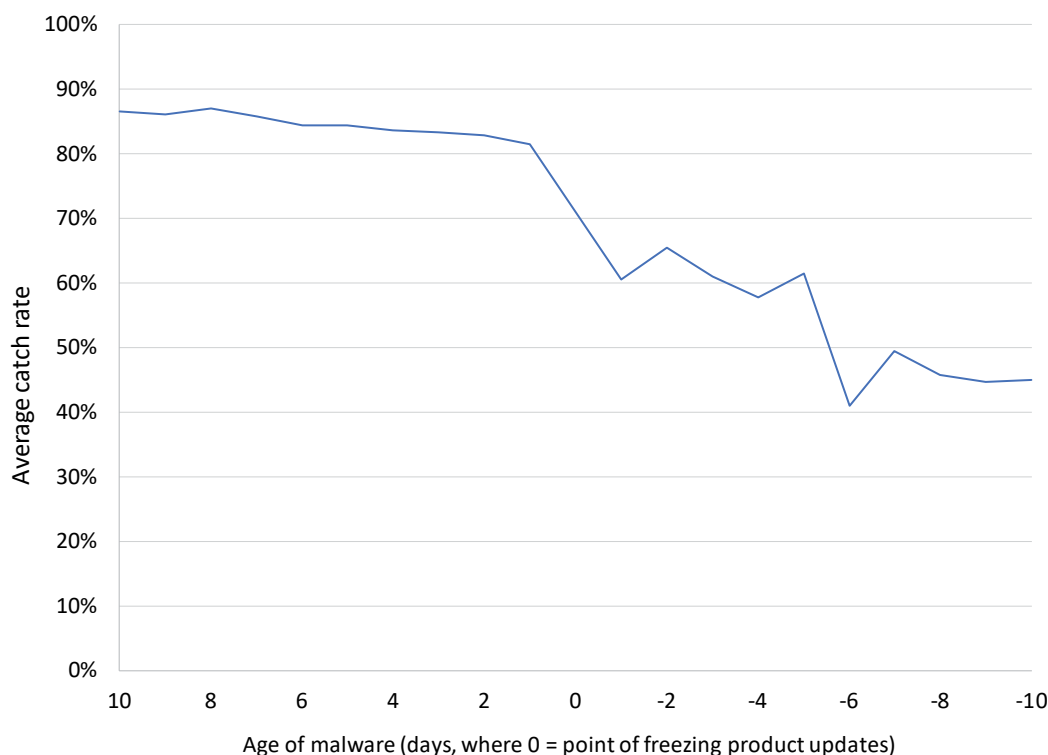
¹ <https://twitter.com/GossiTheDog/status/863348843408224257>

80%. Given that some of the samples used in our test are relatively uncommon, that this is a baseline score, and that in real-world use, this protection would be augmented with dynamic protection, this is pretty good.

For the second ('Proactive') part of the RAP test, we freeze the products with their latest updates installed and then disable Internet access. After ten days, we test the products using malware samples seen in the wild one to ten days *after*

the products were frozen, thus after they had last received updates. Even in these rather restricted circumstances, products still blocked 60% of the older samples and 45% of the samples from ten days after the freeze date.

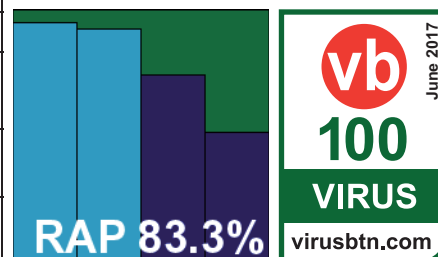
This demonstrates why anti-virus products have long stopped relying solely on their static detection engines, but it also shows why these engines remain an important component of these products.



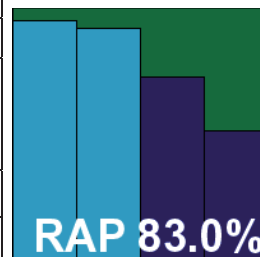
RESULTS

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

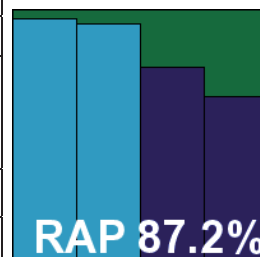
adaware antivirus pro		
	Windows 7	Windows 10
Main version	12.0.649.11190	12.0.649.11190
Update versions	7.71952, 7.71787, 7.71912, 7.71995	7.71959, 7.71671, 7.71908, 7.71995
ItW catch rate	100.00%	100.00%
False positives	0	0



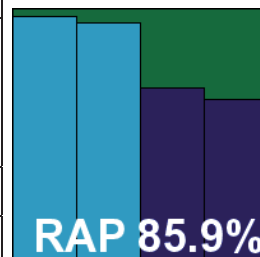
Arcabit Antivirus		
	Windows 7	Windows 10
Main version	2017.06.21	2017.06.21
Update versions	2017.05.26, 2017.06.16, 2017.06.23	2017.05.30, 2017.06.16, 2017.06.23
ItW catch rate	100.00%	100.00%
False positives	0	0



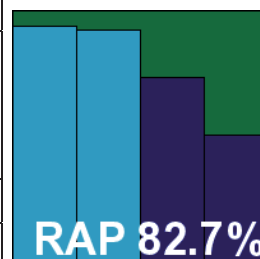
Avast Free Antivirus		
	Windows 7	Windows 10
Main version	17.4.2294	17.4.2294
Update versions	17062002, 17053004, 17061602, 17.5.2302/17062702	170620-2, 17.4.2294/17053004, N/A, 17.4.2294/17062304
ItW catch rate	100.00%	100.00%
False positives	0	0



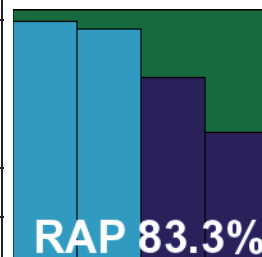
AVG Internet Security		
	Windows 7	Windows 10
Main version	17.2.3008	17.4.3014
Update versions	17052502, 17.4.3014/17052502, 17061600, 17062302	17062100, 17.4.3014/17060608, 17.4.3014/17061902, 17.4.3014/17062502
ItW catch rate	100.00%	100.00%
False positives	0	0



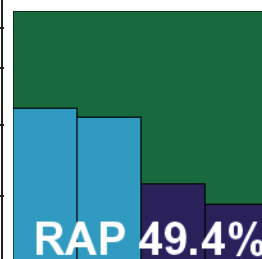
Bitdefender GravityZone Security for Endpoints		
	Windows 7	Windows 10
Main version	6.2.21.908	6.2.21.908
Update versions	7.71878, 6.2.19.899/7.71656, 6.2.21.908/7.71888, 6.2.21.908/7.71980	7.71954, 7.71841, 7.71885, 7.71985
ItW catch rate	100.00%	100.00%
False positives	0	0



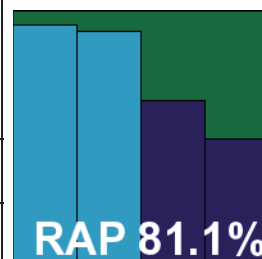
BullGuard Antivirus		
	Windows 7	Windows 10
Main version	17.0.331.3	17.1.333.5
Update versions	17.0.329.2	17.1.0.91, 17.0.331.3/16.0.0.88, 17.1.333.4/17.0.331.3, 17.1.333.5/17.1.0.91
ItW catch rate	100.00%	100.00%
False positives	0	0



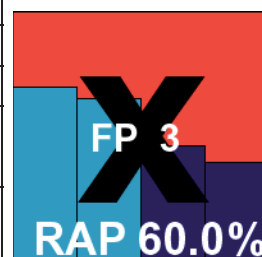
Clearsight Antivirus Business		
	Windows 7	Windows 10
Main version	4.1.19	4.1.19
Update versions	3.68.1/5.39	3.68.1/5.40
ItW catch rate	99.77%	99.77%
False positives	0	0



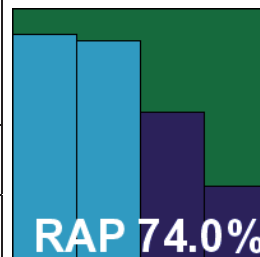
CompuClever Antivirus Plus		
	Windows 7	Windows 10
Main version	19.6.0.326	19.6.0.326
Update versions	8988141, 7.71664/8713936, 7.71953/8983234, 7.72026/9122639	7.71953, 7.71651, 7.71892, 7.71986
ItW catch rate	100.00%	100.00%
False positives	0	0



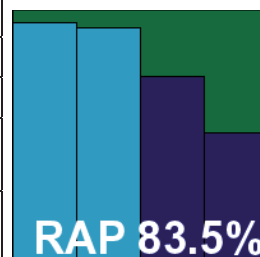
Cyren Command Anti-Malware		
	Windows 7	Windows 10
Main version	5.1.38	5.1.38
Update versions	5.4.25	5.4.25
ItW catch rate	99.97%	99.97%
False positives	3	3



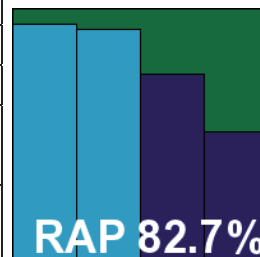
Defenx Security Suite		
	Windows 7	Windows 10
Main version	15.1.0106	15.1.0106
Update versions	10.16.23735, 15.1.0103/10.5.22722, 15.1.0106/10.16.23690, 15.1.0106/10.16.23765	10.16.23731, 10.14.23505, 10.16.23690, 10.16.23765
ItW catch rate	100.00%	100.00%
False positives	0	0



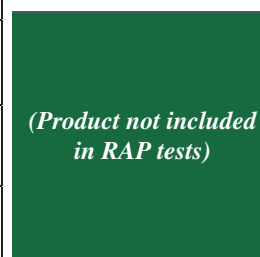
Emsisoft Anti-Malware		
	Windows 7	Windows 10
Main version	7.71953	7.71952
Update versions	7.71579, 7.71888, 7.71983	7.71646, 7.71890, 7.71985
ItW catch rate	99.86%	99.86%
False positives	0	0



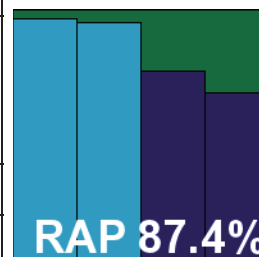
eScan Internet Security Suite for Windows		
	Windows 7	Windows 10
Main version	14.0.1400.1979	14.0.1400.1979
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0



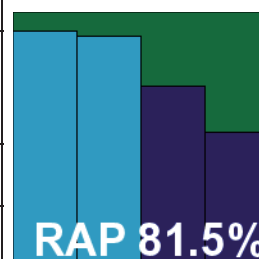
ESET Internet Security		
	Windows 7	Windows 10
Main version	10.0.386.0	10.1.210.0
Update versions	15620, 15486, 15614, 15637	15619, 15503, 15595, 15634
ItW catch rate	100.00%	100.00%
False positives	0	0



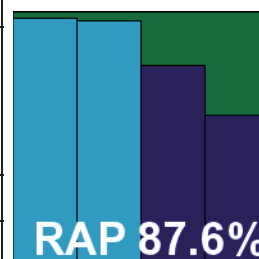
Essentware PCKeeper Antivirus PRO		
	Windows 7	Windows 10
Main version	8.3.44.90	8.3.44.90
Update versions	8.14.13.120, 8.3.44.66/ 8.14.9.116, 8.3.44.88/ 8.14.12.168, 8.3.44.92/ 8.14.14.50	8.14.13.120, 8.3.44.66/8.14.10.12, 8.3.44.88/8.14.12.168, 8.3.44.92/8.14.14.64
ItW catch rate	100.00%	100.00%
False positives	0	0



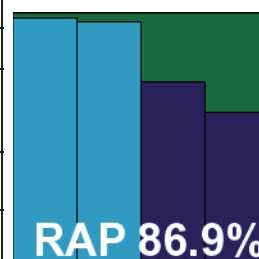
Fortinet FortiClient		
	Windows 7	Windows 10
Main version	5.4.1.0840	5.4.1.0840
Update versions	5.00247/49.00671, 48.00077, 49.00648, 49.00746	5.00247/49.00671, 48.00178, 49.00560, 49.00732
ItW catch rate	100.00%	100.00%
False positives	0	0



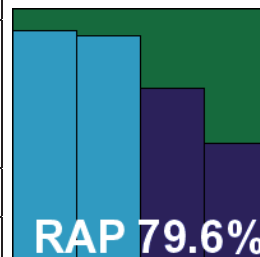
G DATA Antivirus		
	Windows 7	Windows 10
Main version	25.3.0.1	25.3.0.3
Update versions	AVA_25.12976/GD_25.9822, AVA_25.12593/GD_25.9633, AVA_25.12971/GD_25.9817, AVA_25.13031/GD_25.9849	AVA 25.12976/GD 25.9822, AVA 25.12775/GD 25.9726, AVA 25.12901/GD 25.9788, AVA 25.13019/GD 25.9843
ItW catch rate	100.00%	100.00%
False positives	0	0



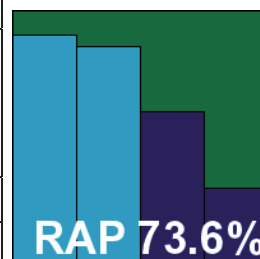
IKARUS anti.virus		
	Windows 7	Windows 10
Main version	2.13.19	2.13.19
Update versions	99459, 99382, 99467, 99445	99459, 99433, 99445, 99467
ItW catch rate	100.00%	100.00%
False positives	0	0



INCA nProtect AVS		
	Windows 7	Windows 10
Main version	4.0.0.10012	4.0.0.10012
Update versions	2017.06.22.01, 2017.05.30.01, 2017.06.21.01, 2017.06.26.01	2017.06.21.01, 2017.06.01.01, 2017.06.18.01, 2017.06.25.01
ItW catch rate	100.00%	100.00%
False positives	0	0



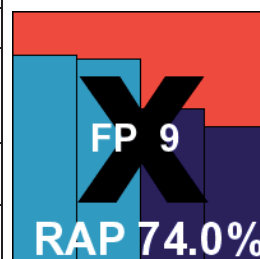
K7 Total Security		
	Windows 7	Windows 10
Main version	15.1.0307	15.1.0307
Update versions	10.16.23737, 15.1.0306/10.14.23488, 15.1.0307/10.16.23696, 10.16.23768	10.16.23735, 15.1.0306/10.14.23521, 15.1.0307/10.16.23696, 15.1.0307/10.16.23768
ItW catch rate	100.00%	100.00%
False positives	0	0



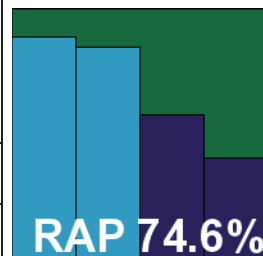
Kaspersky Internet Security		
	Windows 7	Windows 10
Main version	17.0.0.611e	17.0.0.611e
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0



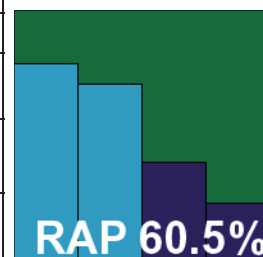
MSecure Endpoint ATP		
	Windows 7	Windows 10
Main version	99460	99460
Update versions	99411, 99459, 99474	99394, 99459, 99475
ItW catch rate	100.00%	100.00%
False positives	9	0



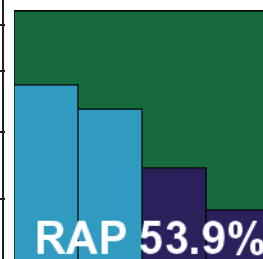
NANO Antivirus Pro		
	Windows 7	Windows 10
Main version	v1.0.76.83123	1.0.76.83123
Update versions	0.14.28.9707, v1.0.76.82925/0.14.28.9701	0.14.28.9707, 1.0.76.82716/0.14.28.9598, 1.0.76.83123/0.14.28.9713, 0.14.28.9731
ItW catch rate	100.00%	100.00%
False positives	0	0



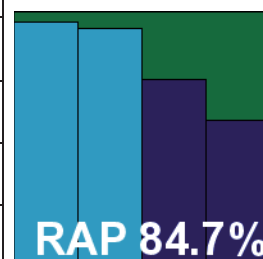
Panda Endpoint Protection		
	Windows 7	Windows 10
Main version	7.70.0	7.70.0
Update versions	7.71.0	7.71.0
ItW catch rate	100.00%	100.00%
False positives	0	0



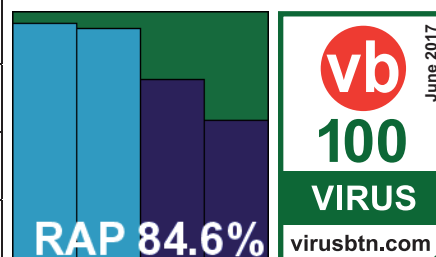
Panda Free Antivirus		
	Windows 7	Windows 10
Main version	18.01.00	18.01.00
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0



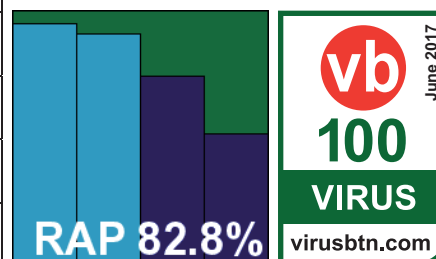
Quick Heal Seqrite Endpoint Security		
	Windows 7	Windows 10
Main version	17.00 (10.2.3.1) 64bit	17.00 (10.0.1.26) 64bit
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0



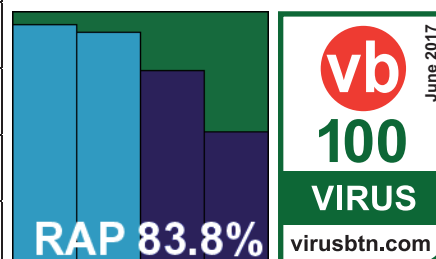
Quick Heal Total Security		
	Windows 7	Windows 10
Main version	17.00 (10.0.1.26) 64bit	17.00 (10.0.1.26) 64bit
Update versions	N/A	N/A
ItW catch rate	100.00%	100.00%
False positives	0	0



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



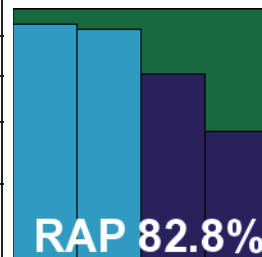
Tencent PC Manager		
	Windows 7	Windows 10
Main version	12.3.26436.901	12.3.26436.901
Update versions	N/A	12.3.26444.901
ItW catch rate	100.00%	100.00%
False positives	0	0



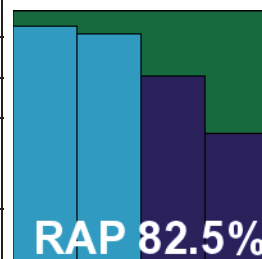
Tencent PC Manager – TAV		
	Windows 7	Windows 10
Main version	12.3.26436.901	12.3.26436.901
Update versions	N/A	12.3.26435.901, 12.3.26443.901
ItW catch rate	100.00%	100.00%
False positives	0	0



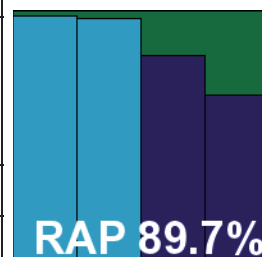
Total Defense Internet Security Suite		
	Windows 7	Windows 10
Main version	9.0.0.645	9.0.0.645
Update versions	3.0.2.1015	3.0.2.1015
ItW catch rate	100.00%	100.00%
False positives	0	0



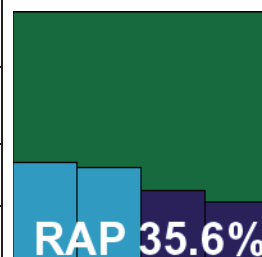
Total Defense Premium		
	Windows 7	Windows 10
Main version	9.0.0.645	9.0.0.645
Update versions	3.0.2.1015	3.0.2.1015
ItW catch rate	100.00%	100.00%
False positives	0	0





















TrustPort Antivirus Sphere		
	Windows 7	Windows 10
Main version	17.0.1.7021	17.0.1.7022
Update versions	17.0.1.7022	14585/7.71953, 14537/7.71729, 14594/7.71964, 14599/7.71986
ItW catch rate	100.00%	100.00%
False positives	0	0



VirIT eXplorer PRO		
	Windows 7	Windows 10
Main version	8.4.51	8.4
Update versions	8.4.44, 8.4.59, 8.4.55	8.4.51, 8.4.60, 8.4.48, 8.4.53
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	
adaware 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 GravityZone Security for Endpoints	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
BullGuard Antivirus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Clearsight Antivirus Business	0	0.00%	15	99.77%	0	0.00%	15	99.77%	X
CompuClever Antivirus Plus	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Cyren Command Anti-Malware	3	0.001%	2	99.97%	3	0.001%	2	99.97%	X
Defenx Security Suite	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Emsisoft Anti-Malware	0	0.00%	9	99.86%	0	0.00%	9	99.86%	X
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%	
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%	

Certification tests contd.	Windows 7				Windows 10				VB100
	FPs	FP rate	WildList misses	WildList catch rate	FPs	FP rate	WildList misses	WildList catch rate	
INCA nProtect AVS	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
K7 Total Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Kaspersky Internet Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
MSecure Endpoint ATP	9	0.002%	0	100.00%	0	0.00%	0	100.00%	X
NANO Antivirus Pro	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Panda Endpoint Protection	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%	
Quick Heal Seqrite Endpoint Security	0	0.00%	0	100.00%	0	0.00%	0	100.00%	
Quick Heal Total 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%	
Tencent PC Manager – TAV	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	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%	
VirIT eXplorer PRO	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†		
adaware antivirus pro	94.51%	92.51%	93.51%	73.24%	51.54%	62.39%	83.14%
Arcabit Antivirus	94.97%	91.68%	93.33%	72.39%	51.48%	61.94%	82.86%
Avast Free Antivirus	95.86%	94.00%	94.93%	76.38%	65.66%	71.02%	86.96%
AVG Internet Security	97.28%	94.30%	95.79%	60.72%	62.82%	61.77%	84.45%
Bitdefender GravityZone Security for Endpoints	92.72%	92.28%	92.50%	73.58%	51.48%	62.53%	82.51%
BullGuard Antivirus	95.13%	92.17%	93.65%	73.08%	51.54%	62.31%	83.20%
Clearsight Antivirus Business	57.71%	57.33%	57.52%	19.62%	16.45%	18.03%	44.36%
CompuClever Antivirus Plus	93.56%	91.24%	92.40%	56.60%	47.70%	52.15%	78.98%
Cyren Command Anti-Malware	69.71%	66.07%	67.89%	47.04%	40.58%	43.81%	59.86%
Defenx Security Suite	89.28%	87.58%	88.43%	59.87%	30.37%	45.12%	73.99%
Emsisoft Anti-Malware	95.14%	92.23%	93.69%	73.99%	51.73%	62.86%	83.41%
eScan Internet Security Suite for Windows	94.03%	91.32%	92.68%	74.25%	51.86%	63.05%	82.80%
Essentware PCKeeper Antivirus PRO	96.04%	94.29%	95.16%	75.85%	67.23%	71.54%	87.29%
Fortinet FortiClient	91.54%	90.10%	90.82%	70.79%	52.61%	61.70%	81.11%
G DATA Antivirus	97.15%	96.85%	97.00%	78.65%	59.48%	69.07%	87.69%
IKARUS anti.virus	97.69%	95.77%	96.73%	72.52%	60.81%	66.66%	86.71%
INCA nProtect AVS	90.26%	89.98%	90.12%	70.41%	47.45%	58.93%	79.72%
K7 Total Security	90.11%	84.96%	87.54%	60.35%	30.37%	45.36%	73.48%
MSecure Endpoint ATP	82.01%	81.43%	81.72%	61.76%	54.76%	58.26%	73.90%
NANO Antivirus Pro	88.86%	84.84%	86.85%	58.27%	41.15%	49.71%	74.47%
Panda Endpoint Protection	73.64%	66.93%	70.29%	40.38%	24.07%	32.22%	57.60%
Panda Free Antivirus	73.10%	61.54%	67.32%	39.03%	22.05%	30.54%	55.06%
Quick Heal Seqrite Endpoint Security	96.01%	92.93%	94.47%	73.33%	57.40%	65.37%	84.77%
Quick Heal Total Security	95.25%	93.36%	94.31%	73.33%	57.40%	65.37%	84.66%
TeamViewer ITbrain Anti-Malware	94.68%	91.12%	92.90%	73.36%	51.61%	62.49%	82.76%
Tencent PC Manager	95.19%	89.85%	92.52%	76.73%	52.99%	64.86%	83.30%
Total Defense Internet Security Suite	93.37%	91.10%	92.23%	75.22%	51.80%	63.51%	82.66%
Total Defense Premium	93.14%	91.52%	92.33%	75.22%	51.80%	63.51%	82.72%
TrustPort Antivirus Sphere	97.90%	96.95%	97.43%	82.45%	66.60%	74.53%	89.79%
VirIT eXplorer PRO	36.09%	46.67%	41.38%	30.00%	25.14%	27.57%	36.78%

*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.

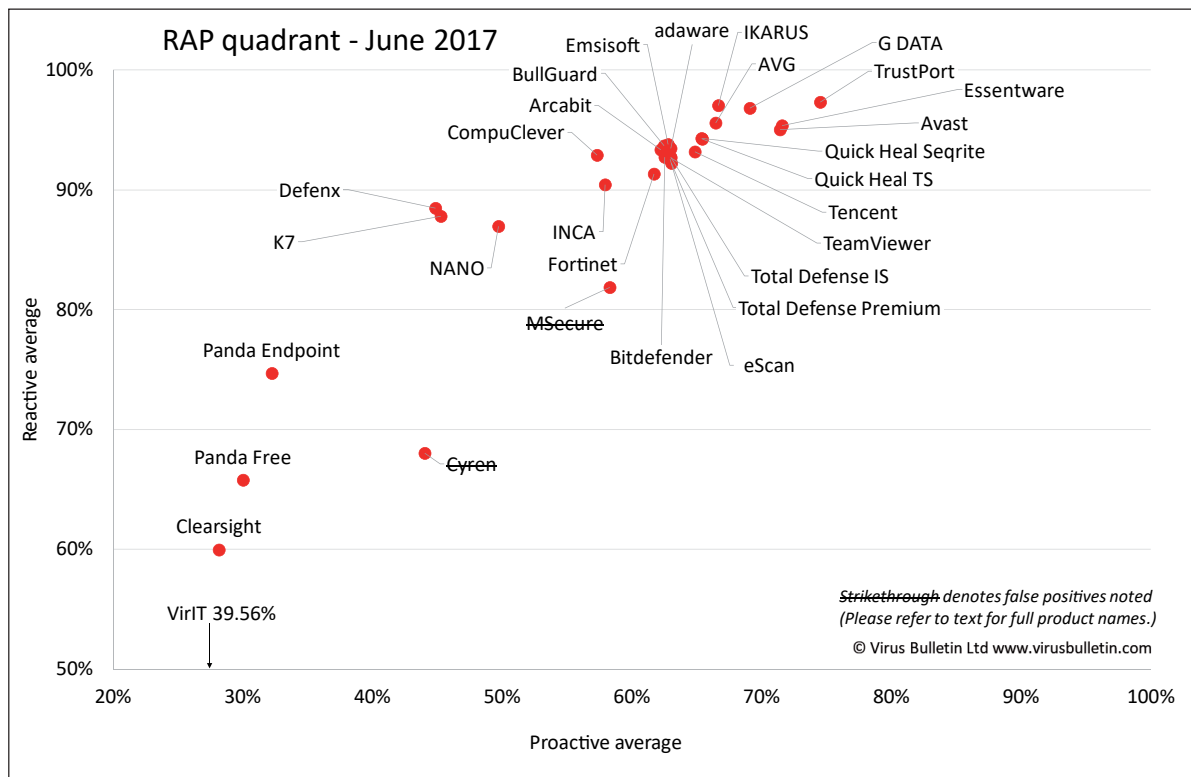
‡ Weighted average gives equal emphasis to the two reactive weeks and the whole proactive part.

RAP (Reactive And Proactive) tests – Windows 10	Reactive		Reactive average	Proactive		Proactive average	RAP weighted average ‡
	Set -2*	Set -1*		Set +1†	Set +2‡		
adaware antivirus pro	94.89%	91.93%	93.41%	75.31%	51.80%	63.56%	83.46%
Arcabit Antivirus	94.61%	92.22%	93.42%	73.36%	51.67%	62.52%	83.12%
Avast Free Antivirus	96.19%	94.19%	95.19%	77.96%	65.72%	71.84%	87.41%
AVG Internet Security	96.65%	94.08%	95.36%	76.57%	65.66%	71.12%	87.28%
Bitdefender GravityZone Security for Endpoints	94.31%	91.76%	93.03%	73.58%	51.48%	62.53%	82.87%
BullGuard Antivirus	95.08%	92.46%	93.77%	73.55%	51.61%	62.58%	83.37%
Clearsight Antivirus Business	65.47%	59.41%	62.44%	44.53%	32.01%	38.27%	54.38%
CompuClever Antivirus Plus	94.65%	92.25%	93.45%	73.30%	51.61%	62.45%	83.12%
Cyren Command Anti-Malware	70.36%	65.89%	68.12%	47.89%	40.45%	44.17%	60.14%
Defenx Security Suite	89.93%	87.24%	88.59%	58.90%	30.31%	44.60%	73.93%
Emsisoft Anti-Malware	94.86%	93.03%	93.94%	73.77%	51.67%	62.72%	83.53%
eScan Internet Security Suite for Windows	93.08%	91.75%	92.42%	73.84%	51.80%	62.82%	82.55%
Essentware PCKeeper Antivirus PRO	96.29%	94.88%	95.58%	75.85%	67.23%	71.54%	87.57%
Fortinet FortiClient	93.32%	90.40%	91.86%	70.79%	52.61%	61.70%	81.81%
G DATA Antivirus	97.57%	95.67%	96.62%	78.65%	59.48%	69.07%	87.44%
IKARUS anti.virus	97.99%	96.86%	97.43%	72.52%	60.81%	66.66%	87.17%
INCA nProtect AVS	92.63%	88.94%	90.78%	66.67%	47.07%	56.87%	79.48%
K7 Total Security	89.99%	86.22%	88.10%	59.87%	30.37%	45.12%	73.78%
MSecure Endpoint ATP	83.06%	80.92%	81.99%	61.76%	54.76%	58.26%	74.08%
NANO Antivirus Pro	89.10%	85.10%	87.10%	58.27%	41.15%	49.71%	74.64%
Panda Endpoint Protection	84.05%	74.12%	79.09%	40.38%	24.07%	32.22%	63.47%
Panda Free Antivirus	68.07%	60.48%	64.27%	37.11%	21.87%	29.49%	52.68%
Quick Heal Seqrite Endpoint Security	95.14%	93.17%	94.16%	73.33%	57.40%	65.37%	84.56%
Quick Heal Total Security	94.85%	93.60%	94.23%	73.33%	57.53%	65.43%	84.63%
TeamViewer ITbrain Anti-Malware	94.34%	90.59%	92.47%	75.22%	51.80%	63.51%	82.81%
Tencent PC Manager	94.17%	93.58%	93.88%	76.73%	52.99%	64.86%	84.20%
Total Defense Internet Security Suite	94.50%	92.00%	93.25%	73.36%	51.61%	62.49%	83.00%
Total Defense Premium	93.90%	90.41%	92.16%	73.55%	51.61%	62.58%	82.30%
TrustPort Antivirus Sphere	98.07%	96.49%	97.28%	82.45%	66.60%	74.53%	89.70%
VirIT eXplorer PRO	45.06%	30.44%	37.75%	30.00%	25.14%	27.57%	34.36%

*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.

As mentioned in the introduction, 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

© 2017 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/>