

virus

BULLETIN

Covering the global threat landscape

VB100 COMPARATIVE REVIEW ON WINDOWS XP PROFESSIONAL SP3

INTRODUCTION

This time last year, as our annual *XP* test got under way, I was commenting on the coming of spring to the countryside around our offices, waxing lyrical about the glow of the returning sun, the burgeoning greenery and the first splashes of colour. I was also describing the slow but steady decline of *XP*, which was being supplanted by newer and more advanced platforms. A year on, spring has yet to arrive, the skies remain grey, the temperatures decidedly chilly and the fields and forests appear drab, leafless and lifeless.

Similarly, the much-anticipated demise of *XP* seems to have been delayed, despite the arrival of yet another successor late last year. Thanks perhaps in part to the boom in mobile use, and the ensuing struggle for platform supremacy in that area, the desktop world seems to have remained more or less static in terms of operating system usage. Take-up of *Windows 8* has been very slow (yet to catch up even with the lame donkey of *Vista*) and the balance between *Windows 7* and *XP* remains much the same, the newer platform comfortably ahead but far from completely swamping the resilient and clearly much-loved old campaigner.

Estimated to be running on between 15% and 30% of systems, depending on your data source, *XP* is still an important platform, and we were intrigued to see whether the security vendors – many of whom seem to have been investing a lot of time and effort getting their solutions ready, both technically and aesthetically, for *Windows 8* – are still paying enough attention to its venerable forebear.

PLATFORM AND TEST SETS

Preparation of our test systems was a pretty simple process, with several well-settled *XP* images to choose from and the process of installing afresh very familiar and straightforward should we choose to go down that route. In

the end we opted to revive some old installs, which were tweaked a little to include a few more up-to-date tools (browsers, archive handlers, PDF viewers and so on) but with no updates of the platform itself. After so many years the user experience is extremely instinctive; everything we needed was easy to find, and the systems felt stable and responsive compared to our experiences with some newer platforms of late.

Preparation of the test sets was a similarly straightforward task, with a standard pattern now well established. RAP and Response sets were built around the product deadline of 13 February and the testing period through March using an automated process, with numbers mostly fairly steady throughout. Both set types totalled around 20,000 samples per week after sorting, validation and classification to emphasize more common and significant threats. The WildList sets were based on the same deadline, which meant using the December 2012 WildList, as the next one was not issued for a few more days. Our clean sets were also updated up until the deadline, with a fairly large chunk of new additions, most of which were taken from the most popular and most highly recommended items on a number of leading software download sites. As usual, these were installed, filtered for adware and other misbehaviours, and all relevant files were harvested for inclusion in the sets, along with the original installers. No changes were needed to the sample sets used for our speed and performance tests, and automation scripts were all well tuned to the environment, so things were quickly ready to go.

The deadline brought with it our usual fear of a flood of products, but numbers were not too crazy, thanks to the continued absence of a wide number of products using the former *VirusBuster* engine, still transitioning to its new owner, and the more surprising absence of several other regulars. The final total came in at 45 products, although we expected several to be struck off well before reaching the

final report stage. An impressive 14 products included the highly popular *Bitdefender* engine, with four each for *Avira* and the company formerly known as *GFI* (before which it was known as *Sunbelt Software*) and which has now spun off as a separate company called *ThreatTrack Security*.

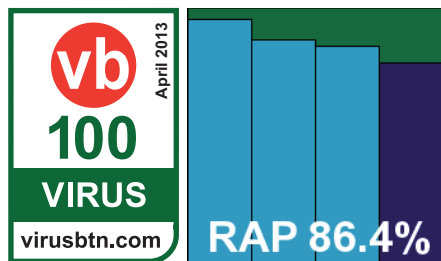
We expected this to cause some overcrowding on our detection rate graphs, as we anticipated that most of the products sharing engines would perform very similarly – but we hoped that our ever-expanding range of performance measures would help set them apart. To help with this we have devised a new visual aid: a scatter graph pitting detection rates in static scanning with cloud access, as recorded in our ‘Response’ tests, against the percentage slowdown observed when carrying out our sets of standard activities. Thanks to the different approaches taken by products – such as not scanning files on-read by default in some cases, allowing access initially and scanning in the background in others – some products may appear to do slightly better here than they might if they were to impose the more complete protection others offer by default. We have endeavoured to mark these products out; we have also added an indication of our stability rating to the chart, hopefully providing an at-a-glance impression of how products performed, at least in the context of our test environment – of course, your mileage may vary.

AhnLab V3 Internet Security 8.0

Main version: 8.0.7.5 (build 1398)
 Update versions: 2013.03.08.05, 2013.03.14.00, 2013.03.20.00

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.91%
False positives	0	Stability	Stable

First up this month, *AhnLab* is not the most regular of participants in our tests but usually puts in a reasonable performance. The 118MB



product installer worried us slightly by appearing to do nothing for quite some time before suddenly waking up and getting going, running through a fairly standard process to complete in a minute or so. Updates added a couple of minutes on average, but reboots were not needed and things were soon ready to go. The GUI is crisp and clear with a fair range of controls; logging is provided in a dedicated log

viewer tool, which gives good access to the data and allows it to be exported easily and reliably for external analysis.

Operation seemed fairly stable, although we did note some odd recurrence of on-access alert pop-ups at seemingly random times, and also saw no effect from adjusting the on-access scanning settings to include self-extracting archives, which appeared to remain unexamined. Speeds were not bad on demand, overheads perhaps a little on the high side on access, but resource use was well below average and our set of activities was completed in decent time too.

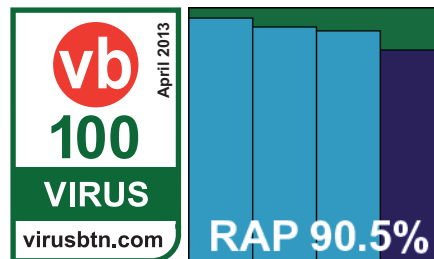
Detection was reasonable – a little behind the leaders, but not embarrassingly so, and the certification sets were handled well, with no issues to report in either the WildList or clean sets. A VB100 award is thus earned by *AhnLab*, getting things off to a good start. The vendor’s test history shows three passes from three entries in the last six tests; four passes and two fails in the last two years. With only a couple of pretty minor issues noted, the product gets a ‘Stable’ rating.

Avast Software avast! Free Antivirus

Main version: 7.0.1474
 Update versions: 130213-2, 8.0.1482/130305-0, 8.0.1483/130311-0, 130319-0

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

Avast released a much-heralded new major version shortly after the test deadline. We had hoped to review it in more depth in these pages,



but time and manpower sadly ruled that out – nevertheless, thanks to our policy of applying all product updates offered, we were able to see the new version in action throughout much of the test, with only the RAP test using the version originally submitted. Each install used the same 101MB for the old version 7 product, which ran through pretty speedily, completing in under a minute even when the option to install the *Google Chrome* browser was left in its default checked state. Updates were fast too, taking not much more than a minute even when the new version was added, although in these instances a reboot was needed to complete the set-up.

Certification tests	On demand		On access		Clean sets	
	Standard WildList	Extended WildList	Standard WildList	Extended WildList	FP	Warnings
AhnLab V3 Internet Security	100.00%	100.00%	100.00%	99.91%		
Avast Free Antivirus	100.00%	100.00%	100.00%	100.00%		
AVG Internet Security Business Edition	100.00%	100.00%	100.00%	100.00%		4
Avira Free Antivirus	100.00%	100.00%	100.00%	100.00%		
Avira Professional Security	100.00%	100.00%	100.00%	100.00%		
BeyondTrust PowerBroker EPP	100.00%	100.00%	100.00%	100.00%	1	
Bitdefender Antivirus Plus 2013	100.00%	100.00%	100.00%	100.00%		
BullGuard Antivirus 2013	100.00%	100.00%	100.00%	100.00%		
CommTouch Command	100.00%	100.00%	100.00%	100.00%	7	1
Comodo IS Premium	100.00%	99.27%	99.80%	98.02%		
Emsisoft Anti-Malware	100.00%	100.00%	100.00%	100.00%		
eScan Internet Security Suite	100.00%	100.00%	100.00%	100.00%		
ESET NOD32 Antivirus 6	100.00%	100.00%	100.00%	100.00%		4
Filseclab Twister Antivirus 8	97.98%	95.72%	97.98%	95.72%	8	
Fortinet FortiClient	100.00%	100.00%	100.00%	100.00%		
F-Secure Client Security	100.00%	99.95%	100.00%	99.95%		1
F-Secure Internet Security	100.00%	99.95%	100.00%	99.95%		1
G Data AntiVirus 2013	100.00%	100.00%	100.00%	100.00%		
Hauri ViRobot Internet Security 2011	100.00%	100.00%	100.00%	98.65%	1	
Ikarus anti.virus	100.00%	100.00%	100.00%	100.00%	1	
Iolo System Shield	100.00%	100.00%	100.00%	100.00%		
K7 Total Security	100.00%	100.00%	100.00%	100.00%		
Kaspersky Endpoint Security	100.00%	100.00%	100.00%	100.00%		3
Kingsoft Antivirus 2013	100.00%	100.00%	100.00%	100.00%		
Lavasoft Ad-Aware Pro Security	100.00%	100.00%	100.00%	100.00%		
Microsoft Security Essentials	100.00%	100.00%	100.00%	99.72%		
MSecure MalwareSecure	100.00%	99.54%	100.00%	94.76%	1	
Norman Security Suite	100.00%	99.91%	100.00%	99.91%		3
Optenet Security Pack	100.00%	100.00%	100.00%	99.26%		
Panda Cloud Antivirus FREE	100.00%	100.00%	100.00%	99.83%		
PC Pitstop PC Matic	100.00%	100.00%	100.00%	99.95%		
Qihoo 360 Antivirus	100.00%	100.00%	100.00%	100.00%		3
Quick Heal Total Security 2013	100.00%	100.00%	100.00%	100.00%		
Sophos Endpoint Security and Control	100.00%	100.00%	100.00%	100.00%		
Tencent PC Manager	100.00%	100.00%	100.00%	100.00%		
ThreatTrack VIPRE Antivirus 2013	100.00%	100.00%	100.00%	100.00%		
Total Defense for Business	100.00%	100.00%	100.00%	100.00%		
Total Defense Internet Security Suite	100.00%	100.00%	100.00%	100.00%	7	
TrustPort Antivirus 2013	100.00%	100.00%	100.00%	100.00%		
UnThreat AntiVirus Free Edition	100.00%	100.00%	100.00%	99.95%		

(Please refer to text for full product names.)

The design is another *Windows 8*-aping tiled affair, with a very impressive range of tools and gadgets on offer, many of which are new and some quite unheard of in security suites in our experience. When you burrow down to the anti-malware area though, things are pretty familiar, with a clear and sensible layout providing an irreproachable range of controls. Logging is clear, reliable and configurable.

The new interface seemed robust too, with no sign of wobbles even under extreme pressure. Scanning speeds were very good on demand, with overheads very light on access, and although this is helped by only some file types being covered on-read by default, the ‘full’ measures were still very good in most sets. Resource use was very low for RAM and below average for CPU too, with our activities taking a little while to get through, but not too much longer than the average for the month.

Detection was very good, with some impressive scores in all sets, RAP numbers dropping off just a little into the proactive week. With no problems in the WildList or clean sets, a VB100 award is comfortably earned. A blip in the recent *Linux* test means *Avast* has only five passes from the last six tests; ten passes and two fails in the last two years. This month’s performance was impressively stable, earning the product a ‘Solid’ rating.

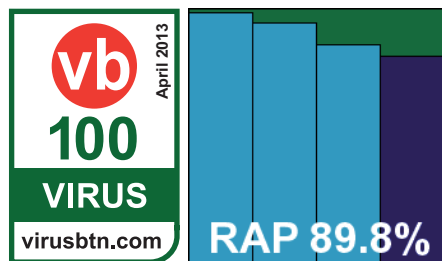
AVG Internet Security Business Edition

Main version: 2013.0.2897

Update versions: 2639/6085, 2013.0.2899/2641/6152, 2013.0.2904/2641/6164, 2641/6198

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Fair

We have already seen AVG’s flashy new version in our recent *Windows 8* test, with the new interface designed to fit in with



Windows 8 stylings. Installation from the 118MB package provided was fairly straightforward. An ‘express install’ option is offered, but only after several dialogs have been clicked through, and with another shortly afterwards, in this case offering a toolbar. Unusually, but commendably, all options default to unchecked. The process took a few minutes, with initial updates adding a few more minutes, but with no reboots required.

The interface is crisp and glossy but seemed a little wobbly in places. Configuration is ample and reasonably simple to navigate, but we did see a few instances of wonky rendering, and logging was very problematic, with logs of any significant size causing all kinds of headaches. Scans would complete happily, but trying to access or export log data brought a number of GUI freezes and crashes, or simply dumped out incomplete (and in some cases completely empty) logs. On a couple of occasions we had scans which initially reported large numbers of detections, but when revisited after recovering from a crash reported the same job had completed and found nothing. Although these issues mainly occurred when scanning large infected sets, which is unlikely to happen often in the real world, it is enough to dent our stability rating for the product fairly noticeably.

Scanning speeds were good though, zooming through the warm runs, and overheads were low, again with great improvements after initial familiarization. CPU and RAM use were around average, with impact on our set of tasks pretty light. Detection was very good too, with a solid position in both of our scatter graphs and a noticeable but slow decline through the weeks of the RAP sets. With no issues in the WildList sets, and just a few warnings about corrupt, unsigned or potentially over-packed files in the clean sets, a VB100 award is easily earned. AVG now has five passes and one fail in the last six tests; ten passes and two fails in the last two years. This product’s stability was a bit of a worry for *XP* users – perhaps suggesting that too much focus has been given to early adopters of *Windows 8* – and issues encountered with both the interface and logging mean a stability rating of no more than ‘Fair’.

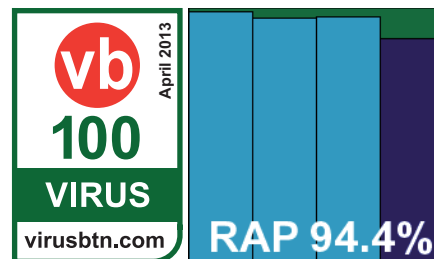
Avira Free Antivirus

Main version: 13.0.0.3185

Update versions: 7.11.60.212, 7.11.63.170, 7.11.64.152, 7.11.65.136

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

As usual in our desktop tests, we have a pair of products from *Avira*, starting with the free edition. The 108MB installer took a few seconds to unpack but then needed only a single



Product information	Install time (m)	Reboot required	Third-party engine technology	Stability score	Stability rating
AhnLab V3 Internet Security	3	N		2	<i>Stable</i>
Avast Free Antivirus	1:30	S		0	<i>Solid</i>
AVG Internet Security Business Edtn	6	N		9.5	<i>Fair</i>
Avira Free Antivirus	1:45	S		0	<i>Solid</i>
Avira Professional Security	2	S		0	<i>Solid</i>
BeyondTrust PowerBroker EPP	24	N	Norman	11	<i>Fair</i>
Bitdefender Antivirus Plus 2013	4	N		0	<i>Solid</i>
BullGuard Antivirus 2013	3	N	Bitdefender	0	<i>Solid</i>
CommTouch Command	1:10	N		4	<i>Stable</i>
Comodo IS Premium	6	Y		11.5	<i>Fair</i>
Emsisoft Anti-Malware	6	N	Bitdefender	12	<i>Fair</i>
eScan Internet Security Suite	10:30	Y	Bitdefender	25	<i>Buggy</i>
ESET NOD32 Antivirus 6	1:30	N		1	<i>Stable</i>
Filseclab Twister Antivirus 8	4	S		1	<i>Stable</i>
Fortinet FortiClient	8	N*		14.5	<i>Fair</i>
F-Secure Client Security	15	Y	Bitdefender	4	<i>Stable</i>
F-Secure Internet Security	14:45	Y	Bitdefender	3	<i>Stable</i>
G Data AntiVirus 2013	11	Y	Avast, Bitdefender	0	<i>Solid</i>
Hauri ViRobot Internet Security 2011	3:30	N	Bitdefender	4	<i>Stable</i>
Ikarus anti.virus	6	N		1	<i>Stable</i>
Iolo System Shield	1:30	Y	CommTouch	12	<i>Fair</i>
K7 Total Security	4	S		0	<i>Solid</i>
Kaspersky Endpoint Security	3	N		2	<i>Stable</i>
Kingsoft Antivirus 2013	2:30	N	Avira	2	<i>Stable</i>
Lavasoft Ad-Aware Pro Security	5	Y	ThreatTrack	3	<i>Stable</i>
Microsoft Security Essentials	3:30	N		6	<i>Fair</i>
MSecure MalwareSecure	2:10	N	Ikarus	2	<i>Stable</i>
Norman Security Suite	11	YY		4	<i>Stable</i>
Optenet Security Pack	2	Y	Bitdefender	19	<i>Buggy</i>
Panda Cloud Antivirus FREE	1:10	N		4	<i>Stable</i>
PC Pitstop PC Matic	9	N	ThreatTrack	9	<i>Fair</i>
Qihoo 360 Antivirus	2:30	N	Bitdefender	2	<i>Stable</i>
Quick Heal Total Security 2013	3	N		1	<i>Stable</i>
Sophos Endpoint Security and Control	3	N		0	<i>Solid</i>
Tencent PC Manager	1:30	N	Avira	0	<i>Solid</i>
ThreatTrack VIPRE Antivirus 2013	2	Y		3	<i>Stable</i>
Total Defense for Business	8	N	Bitdefender	9	<i>Fair</i>
Total Defense Internet Security Suite	4	YY		11	<i>Fair</i>
TrustPort Antivirus 2013	4	N	AVG, Bitdefender	3	<i>Stable</i>
UnThreat AntiVirus Free Edition	4:20	Y	ThreatTrack	38	<i>Flaky</i>

0 = *Solid*15 - 29.9 = *Buggy*S - *Reboot required after some updates*0.1 - 4.9 = *Stable*30+ = *Flaky*YY - *More than one reboot required on some installs*5 - 14.9 = *Fair** - *Reboot may be required to change browser version**(Please refer to text for full product names.)*

click to kick off an express install, which completed in under a minute including a ‘quick’ scan. Updates mostly took another minute or so, although on one occasion the product announced that a new version needed to be downloaded which would take around 23 minutes – in the end this took less than two minutes, but did require a reboot.

The interface is simple and unflashy, providing a decent if not quite complete level of control; logging is likewise workmanlike and reliable. Scanning speeds were reasonable considering the very thorough settings, very fast indeed over some of our sets, and overheads were not too high either, with RAM and CPU use pretty low. Our set of tasks did take quite some time to get through though.

Detection was superb as usual, with very little missed in any of our sets, and the product takes up a strong position in the leading cluster on our RAP chart. The core sets were properly dealt with – nothing was missed in the WildList set or flagged up in the clean sets, thus a VB100 award is comfortably earned. Participating only in our desktop tests, Avira’s free version has a strong record with three passes from three entries in the last six tests; six from six in the last two years. There were no stability problems, earning a ‘Solid’ rating.

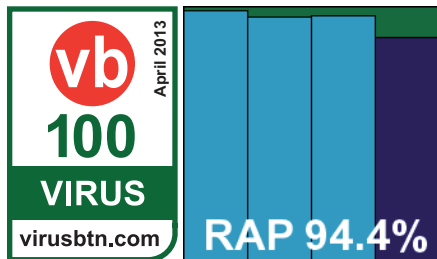
Avira Professional Security

Main version: 13.0.0.3185

Update versions: 7.11.60.212, 7.11.63.170, 7.11.64.152, 7.11.65.136

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

The Pro version of Avira’s product is not very different from its free sibling – the installer is a little larger at 121MB, but the general look



and feel is much the same. Once again, the installer offers an express path, which completes in a minute or so with no more than another minute needed for updates; again, in later instances a reboot was needed to complete a more thorough update.

The GUI is sober and sensible, with a comprehensive set of controls this time, and once again logging is solid and

dependable. Scanning speeds were similar, overheads a tiny bit higher in some areas, but a fraction lower in others, with RAM use a little higher and CPU use notably increased but both still well below average. Our set of activities did take rather a long time to complete, with a time very close to that of the free version.

Detection scores were pretty much identical to those of the free version across the board, meaning another excellent set of figures. The certification sets were properly dealt with, earning Avira another VB100 award. The mainline product’s test history now shows an impeccable 12 passes in the last two years. This month’s performance also earned a stability rating of ‘Solid’.

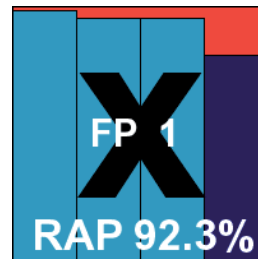
BeyondTrust PowerBroker Endpoint Protection for Desktops

Main version: 7.0.1

Update versions: 1.2.2534, 1.2.2570, 1.2.2579, 1.2.2591

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	1	Stability	Fair

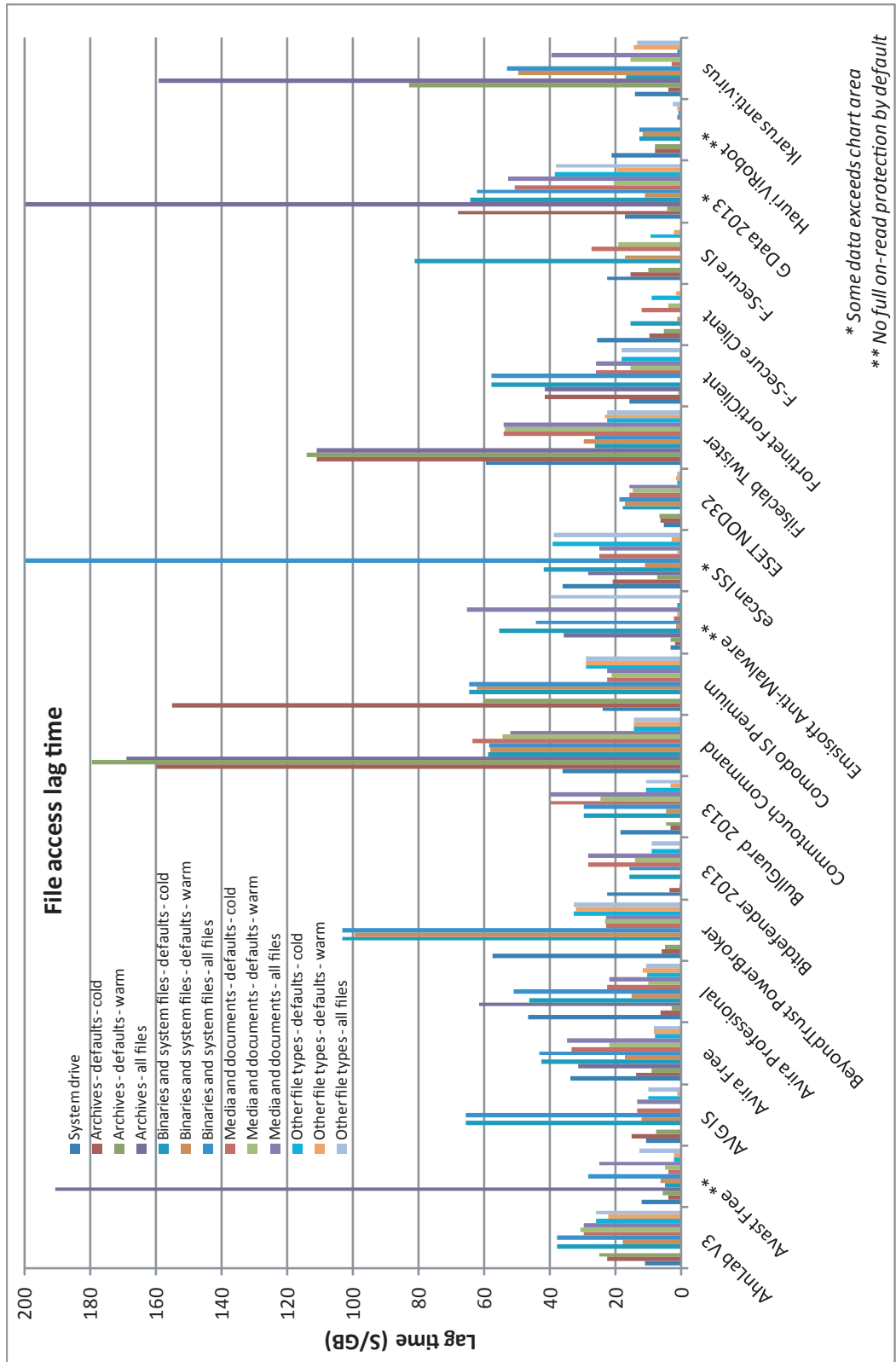
The company formerly known as eEye Digital Security has renamed the product formerly known as Blink to the rather less concise PowerBroker EPP for Desktops. There has been a fairly significant overhaul of the interface with apparently some serious improvements under the covers too, but the product is still recognizable. The fairly large 262MB installer runs through a few stages and requests a swathe of personal details towards the end, but does not need a reboot to complete. Updates pulled down well over 200MB of data, taking quite some time, and in some cases seemed to perform the same download several times, failing at an unspecified point with minimal information. On some occasions the updates refused even to start, although we found that this issue could be skirted around by tweaking the configuration of the updater module, or by installing a more recent IE version, which seemed to change some useful security settings. These annoyances added considerably to the overall install time.

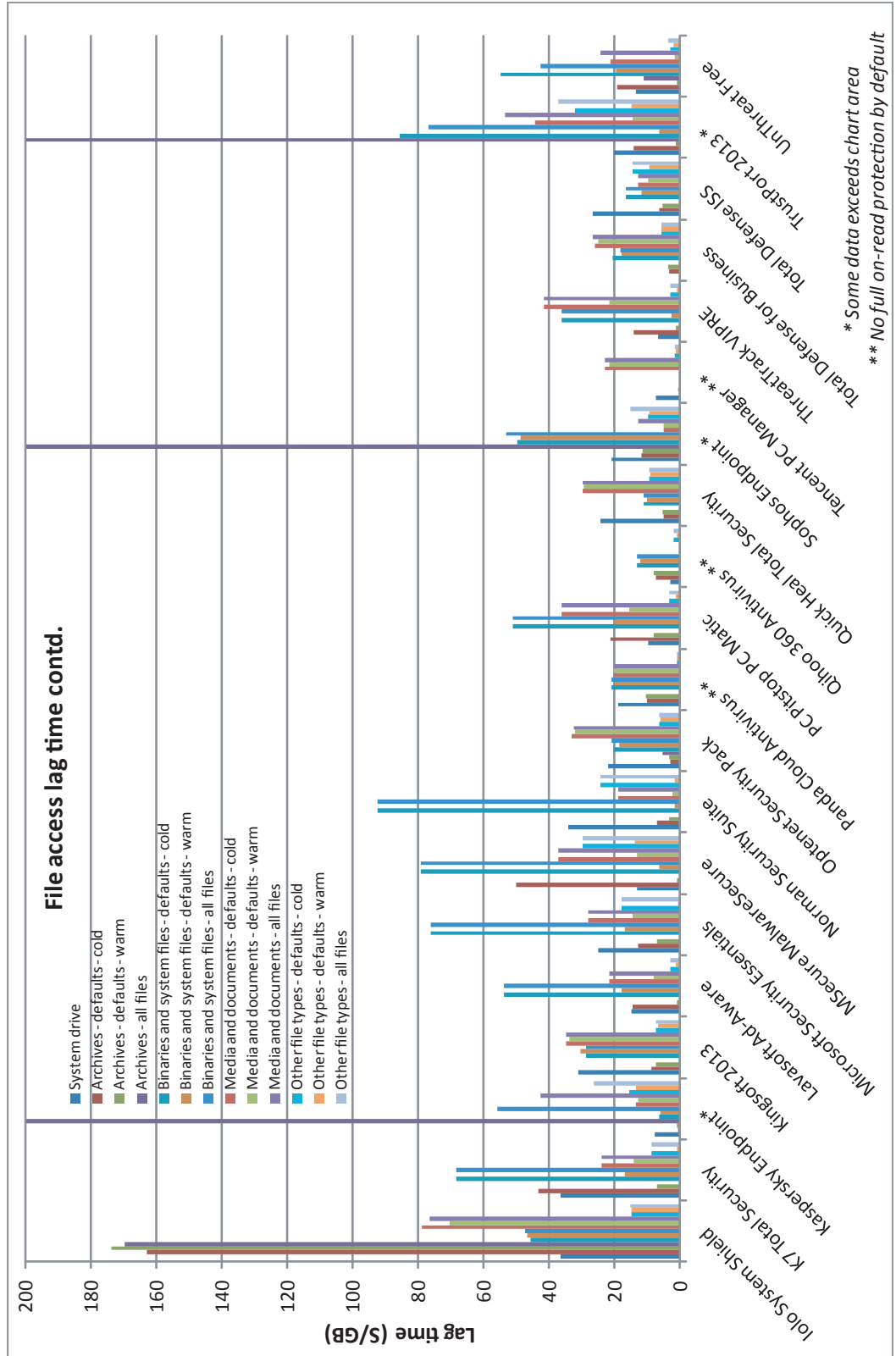


The interface is rather different, browser-based and laden with information, with plenty of options down one side, but the configuration dialog is pretty much as was, providing a range of controls for the various components, a good basic set for the anti-malware side of things. Logging is fairly

File access lag time (s/GB)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
AhnLab V3 IS	11.31	22.68	24.97	NA	38.09	17.87	38.09	29.78	30.77	29.78	26.18	22.44	26.18
Avast Free Antivirus†	12.17	4.12	5.57	190.59	5.10	6.52	28.33	3.98	5.07	24.88	2.41	2.51	12.90
AVG IS Business Edtn	10.82	15.37	7.81	NA	65.79	12.10	65.79	13.61	0.12	13.61	9.99	1.38	9.99
Avira Free Antivirus	33.85	13.90	9.21	31.40	42.82	17.26	43.21	33.44	22.07	35.01	8.25	8.33	8.57
Avira Pro Security	46.75	6.51	3.06	61.57	46.49	15.34	51.07	22.68	9.99	22.06	10.55	11.95	10.83
BeyondTrust PowerBroker	57.51	6.07	4.94	NA	103.35	99.59	103.35	23.10	23.35	23.10	32.90	32.05	32.90
Bitdefender Antivirus Plus	22.74	3.53	0.76	NA	15.79	0.08	15.79	28.49	14.36	28.49	8.97	0.65	8.97
BullGuard Antivirus 2013	18.59	3.48	4.71	NA	29.88	4.63	29.88	40.05	24.64	40.05	10.71	3.38	10.71
CommTouch Command	36.18	160.05	179.54	168.93	58.89	58.32	58.52	63.71	54.44	52.10	14.63	14.51	14.67
Comodo IS Premium	23.96	155.15	60.26	NA	64.71	62.26	64.71	22.84	21.29	22.84	29.24	28.98	29.24
Emsisoft Anti-Malware†	3.21	2.15	3.20	36.01	55.60	1.59	44.21	2.26	1.20	65.36	1.21	0.74	39.85
eScan ISS	36.29	20.84	7.49	28.32	42.13	11.04	1190.13	25.00	1.39	25.10	39.17	2.93	38.79
ESET NOD32 Antivirus 6	5.49	6.54	6.59	NA	17.87	17.19	18.83	15.81	14.89	15.81	1.30	1.81	1.30
Filseclab Twister Antivirus	59.74	111.05	114.08	111.05	26.31	29.66	26.31	54.05	53.72	54.05	22.56	23.51	22.56
Fortinet FortiClient	15.90	41.56	0.86	41.56	57.79	0.17	57.79	26.04	15.39	26.04	18.14	0.69	18.14
F-Secure Client Security	25.89	9.94	5.45	NA	15.53	1.43	NA	12.25	3.91	NA	9.18	1.55	NA
F-Secure Internet Security	22.69	15.69	10.06	NA	81.18	17.17	NA	27.52	19.20	NA	9.37	2.21	NA
G Data AntiVirus 2013	17.10	68.20	4.48	288.22	64.38	11.28	62.36	50.80	20.75	52.67	38.73	19.51	38.21
Hauri ViRobot IS†	21.34	8.18	8.25	NA	12.93	11.81	12.84	0.11	0.07	1.35	1.04	1.24	2.55
Ikarus anti.virus	14.21	4.00	82.95	159.32	16.93	49.87	53.22	2.92	15.67	39.50	1.39	14.47	13.69
Iolo System Shield	36.66	162.99	173.78	169.83	45.69	46.87	47.37	78.93	70.53	76.47	14.91	14.86	15.15
K7 Total Security	36.62	43.50	7.14	NA	68.38	16.82	68.38	23.94	14.22	23.94	8.68	0.85	8.68
Kaspersky ES	7.88	0.69	0.85	260.61	6.26	5.96	56.04	13.62	12.80	42.53	15.47	13.46	26.23
Kingsoft Antivirus 2013	31.19	8.92	7.52	NA	28.89	30.50	28.89	34.85	34.01	34.85	7.35	6.75	7.35
Lavasoft Ad-Aware‡	14.77	14.41	0.88	NA	53.81	17.86	53.81	21.56	7.96	21.56	2.87	1.44	2.87
Microsoft SE	24.88	12.79	7.18	NA	76.22	17.08	76.22	28.20	14.44	28.20	18.05	0.72	18.05
MSecure MalwareSecure	13.25	50.14	0.95	NA	79.41	6.27	79.41	37.38	13.32	37.38	29.64	13.90	29.64
Norman Security Suite	34.15	7.20	3.37	NA	92.49	1.62	92.49	19.05	2.50	19.05	24.27	1.61	24.27
Optenet Security Pack	21.85	3.12	3.51	5.55	20.29	18.45	20.97	33.20	32.02	32.42	6.30	5.91	6.41
Panda Cloud Antivirus†	18.92	10.20	10.37	NA	21.02	20.02	21.02	20.29	20.23	20.29	1.06	0.83	1.06
PC Pitstop PC Matic‡	9.74	21.27	7.99	NA	51.19	19.94	51.19	36.39	15.71	36.39	3.45	1.40	3.45
Qihoo 360 Antivirus†	3.14	7.34	8.07	NA	13.22	12.24	13.22	0.07	0.19	0.07	1.92	1.07	1.92
Quick Heal Total Security	24.35	4.93	5.39	NA	11.16	10.13	11.16	29.93	29.47	29.93	9.41	9.14	9.41
Sophos ESC	21.07	11.87	11.42	447.07	49.74	48.77	53.08	5.22	4.96	12.98	9.68	9.61	15.21
Tencent PC Manager†	7.27	0.44	0.50	NA	0.20	0.13	0.20	22.96	21.50	22.96	1.59	1.36	1.59
ThreatTrack VIPRE‡	6.84	14.18	1.22	NA	36.30	2.80	36.30	41.82	21.80	41.82	3.08	1.16	3.08
Total Defense for Business	N/A	3.42	3.85	NA	20.77	17.87	18.36	26.09	25.15	26.89	5.77	5.59	5.81
Total Defense ISS	26.90	6.30	5.42	NA	16.56	11.97	16.56	12.94	9.64	12.94	14.54	9.30	14.54
TrustPort Antivirus 2013	20.25	14.10	1.17	363.78	85.80	6.34	76.85	44.23	14.38	53.41	32.04	14.74	37.14
UnThreat AntiVirus‡	13.64	19.43	1.01	11.11	54.99	19.51	42.65	21.48	1.75	24.39	3.05	1.88	3.85

* System drive size measured before product installation. † No full on-read protection by default. ‡ On-read protection delayed in some cases. (Please refer to text for full product names.)





clear, exportable and usable, but not very efficient – large swathes of text are needlessly repeated on line after line. Stability was mostly good, although a few large scans did appear to give up halfway through and, rather worryingly, there was no indication that they had not covered the entire area requested.

Scanning speeds were decent if far from blinding, and on-access lag times were a little high in some areas. Use of RAM and CPU cycles were both high, but our set of tasks didn't take too long to complete. Detection was pretty good, with good scores in both the RAP and Response tests, and the WildList set was well handled too. In the clean sets, however, a single item was labelled as a threat – a fairly generic identification, but enough to deny *BeyondTrust* a VB100 award this month. The product's test history is a little rocky, with two passes and three fails in the last six tests; six passes and four fails in the last two years. A number of issues were noted this month, including some tricky updating problems, meaning a stability rating of only 'Fair'.

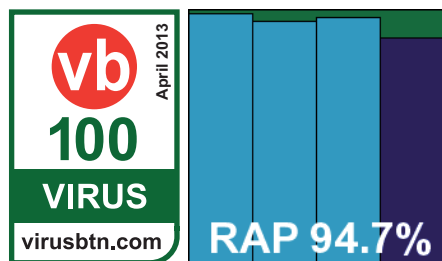
Bitdefender Antivirus Plus 2013

Main version: 16.26.0.1739

Update versions: 7.45417/8751169, 7.45851/9221234, 7.45990/9239152, 7.46152/9305085

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

Bitdefender's product range has also had a pretty snazzy overhaul recently, and the vendor's engine seems to get ever more popular among OEM vendors.



The installer submitted this month was a fairly large 268MB executable, with all latest updates included, and one of the first things it asks is whether a check should be made for a newer version. This seemed to find something to download every time we ran it, but it rarely took more than a few seconds to fetch what it needed. The install itself is another one-click affair, which runs through in a few minutes. Updates are then required despite the initial download, taking a few more minutes and usually fetching a little over 20MB of data. The whole process completes with no need to restart.

The interface is dark and brooding, but reasonably easy to navigate, offering a wide range of controls. Logging is in XML format and reasonably usable, and stability seems good throughout. Scanning speeds started off decent and ramped up hugely in the warm runs, while overheads were very light indeed. RAM and CPU use were both on the low side, and our set of tasks ran through in reasonable time. Detection was excellent, as we have come to expect, with very high scores in the RAP sets, even in the proactive week, and not far short of perfect through the Response sets. The certification sets were handled impeccably and a VB100 award is easily earned. *Bitdefender* is another member of the elite club of products achieving 12 VB100 passes in the last two years. Stability was flawless, earning a 'Solid' rating.

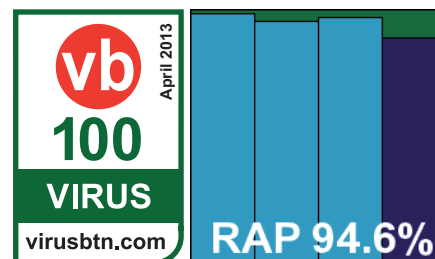
BullGuard Antivirus 2013

Main version: 13.0.256

Update versions: 7.45415, 7.45851, 7.45990, 7.46152

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

The first of the army of products including the *Bitdefender* engine amongst their armoury, *BullGuard* has a very solid record in our



tests of late. The installer weighed in at 171MB, and ran through with minimal input required, completing in under a minute, with a couple more minutes taken for initial updates. The interface is slick, stylish and simple, with a few little quirks of design, but with a little exploration it soon becomes clear as to where things are, and a decent level of configuration is provided. Logging is once again in XML format, with a viewer system in place to keep track of things, but exporting and external analysis is fairly simple.

Speeds were impressive on demand, with strong improvements in the warm runs, and overheads were fairly light too. Resource use was a little high though, with CPU use particularly rocketing up at busy times, but our set of tasks got through in good time, and detection was splendid, with highly impressive numbers across the board. The core sets proved no difficulty, and a VB100 is duly earned, putting *BullGuard* on ten passes in the last two years, only our annual *Linux* tests not entered. Stability was again impeccable, earning a 'Solid' rating.

Commtouch Command Anti-Malware

Main version: 5.1.20

Update versions: 5.3.20/201302130928, 201303072220, 201303140338, 201303212222

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	7	Stability	Stable

Commtouch's performances have left a little to be desired of late, with false positive issues rife in recent tests. The latest submission was a tiny 12MB installer, with updates similarly compact at 29MB. The install process runs along the usual lines, completing in under half a minute, and after a quick licensing stage updates are speedy too, the whole job done within under a minute (assuming speedy typing or pasting in of licence codes).

The interface is simple and a little lacking in modern sparkle, but does a reasonable job of providing a basic set of configuration options in an easily accessible manner. The GUI crashed a few times under heavy stress – mostly when running scans of large sets of infected samples or trying to export large logs – but protection never seemed to be impaired. Scanning speeds were a little on the slow side, and lag time accessing files considerably heavier than most. RAM use was low but CPU use high, and unsurprisingly our set of tasks took some time to get through – around double what they took on an unprotected system. Detection was a little low in the RAP sets, but much better in the Response sets thanks to heavy and clearly quite effective use of cloud look-ups.

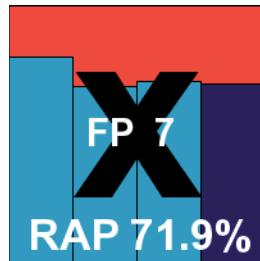
The WildList sets were handled well, but in the clean sets a number of items were alerted on with vague heuristic warnings, including some chipset drivers from a CD bundled with *ASUS* motherboards. This was enough to deny *Commtouch* a VB100 award, leaving the vendor with just one pass and four fails in the last six tests; three passes and seven fails in the last two years. A few minor issues with GUI stability were noted, but only under unusual pressure, so the product just qualifies for a 'Stable' rating.

Comodo Internet Security Premium

Main version: 6.0.264710.2708

Update version: 15495, 15558, 15649

ItW Std	100.00%	ItW Std (o/a)	99.80%
ItW Extd	99.27%	ItW Extd (o/a)	98.02%
False positives	0	Stability	Fair



Comodo has had little luck so far in our comparatives, but we've seen steady improvement in the vendor's products in terms of design, comprehensiveness of components and quality, all of which are highly encouraging. The latest version was provided as a 128MB installer, but seemed to pull down a lot of extras during the set-up process, which was nevertheless quick and required minimal interaction. A reboot was required at the end, and an impressive six desktop icons were put in place for the various components, including the company's 'Dragon' web browser. Updates weighed in at over 100MB in some cases, but rarely took more than a few minutes to complete.

The interface is very jazzy and glitzy, but on this platform seemed a touch laggy and prone to rendering errors. On several occasions it froze up entirely, and we had problems completing some scans thanks to further freezes. When working, though, the layout is clear and sensible and provides a good set of controls, with clear and usable logging.

Scanning speeds were no more than OK initially, but super-fast in the warm run, while overheads were a little on the high side throughout. Resource use was around average, as was impact on our set of tasks. Thanks to a problem with images taken on the deadline date, and no offline update package being provided by the vendor, detection scores were not available for the RAP sets, but the Response sets start pretty high, dropping steadily into the most recent few days (this may have been impacted by some parts of scan jobs failing to complete properly).

The clean sets were well dealt with, and the traditional WildList was covered without problems on demand, but on access several items were missed, with more issues on demand in the Extended set, meaning *Comodo* cannot be granted a VB100 award this month. The *IS* product is not a regular in our tests, with just this single entry in the last six tests; four fails from four attempts in the last two years. A number of issues with both the interface and scanning processes were seen this month, generally under heavy pressure only, meaning the product is given a 'Fair' rating for stability.

Emsisoft Anti-Malware

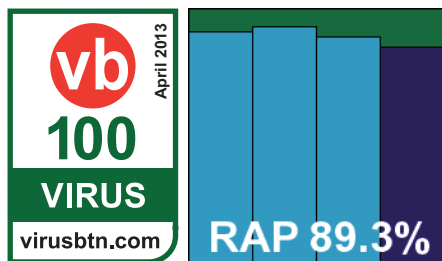
Main version: 7.0.0.18

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Fair

Having recently switched the underlying engine from *Ikarus* to *Bitdefender*, *Emsisoft's* prospects looked good from the off this month, given the performances already

detailed here. The 230MB installer was downloaded from the company's public website on the deadline day, and installed using



a familiar process that has changed little despite the radical changes under the hood. The initial process is fairly speedy, but updates took a while, fetching over 160MB of data in some cases and taking up to ten minutes to complete.

The GUI is a little quirky but clear and pleasant, with a good basic set of controls which were mostly responsive. Logging is clear and reliable, but on a number of occasions the GUI locked up and required a reboot to get itself back in order. This was particularly difficult in the RAP tests where several parts of the test could not be completed; we broke things down into the smallest parts possible to get the best cover we could, but scores will doubtless reflect the issues encountered.

Scanning speeds were not bad, though, when only covering clean samples, and overheads were very light, thanks in large part to the lack of full on-read scanning by default – they slowed down considerably in the ‘full’ measures, which approached more closely the standard settings for most other products. Resource use was fairly low, and impact on our set of tasks around average.

Detection was generally pretty decent despite the missing data – scores were not quite as good as they should have been, but still highly respectable, and most users would find their experience rather better. There were no false alarms and no issues in the WildList sets, and a VB100 award is earned. *Emsisoft*'s recent test history is good, with three passes and two fails from five entries in the last six tests; longer term things are less impressive, with seven fails and three passes in the last two years, but given the change of engine it looks likely that things will continue to improve. There were some problems this month, mostly during unusual circumstances like scanning large sets, but these mean the product earns only a ‘Fair’ rating for stability.

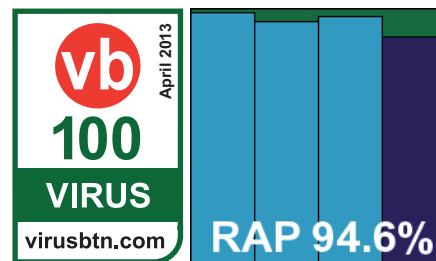
eScan Internet Security Suite

Main version: 14.0.1400.1351

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Buggy

Another product using the *Bitdefender* engine, and another that introduced a heavily redesigned GUI in our *Windows 8* test late last



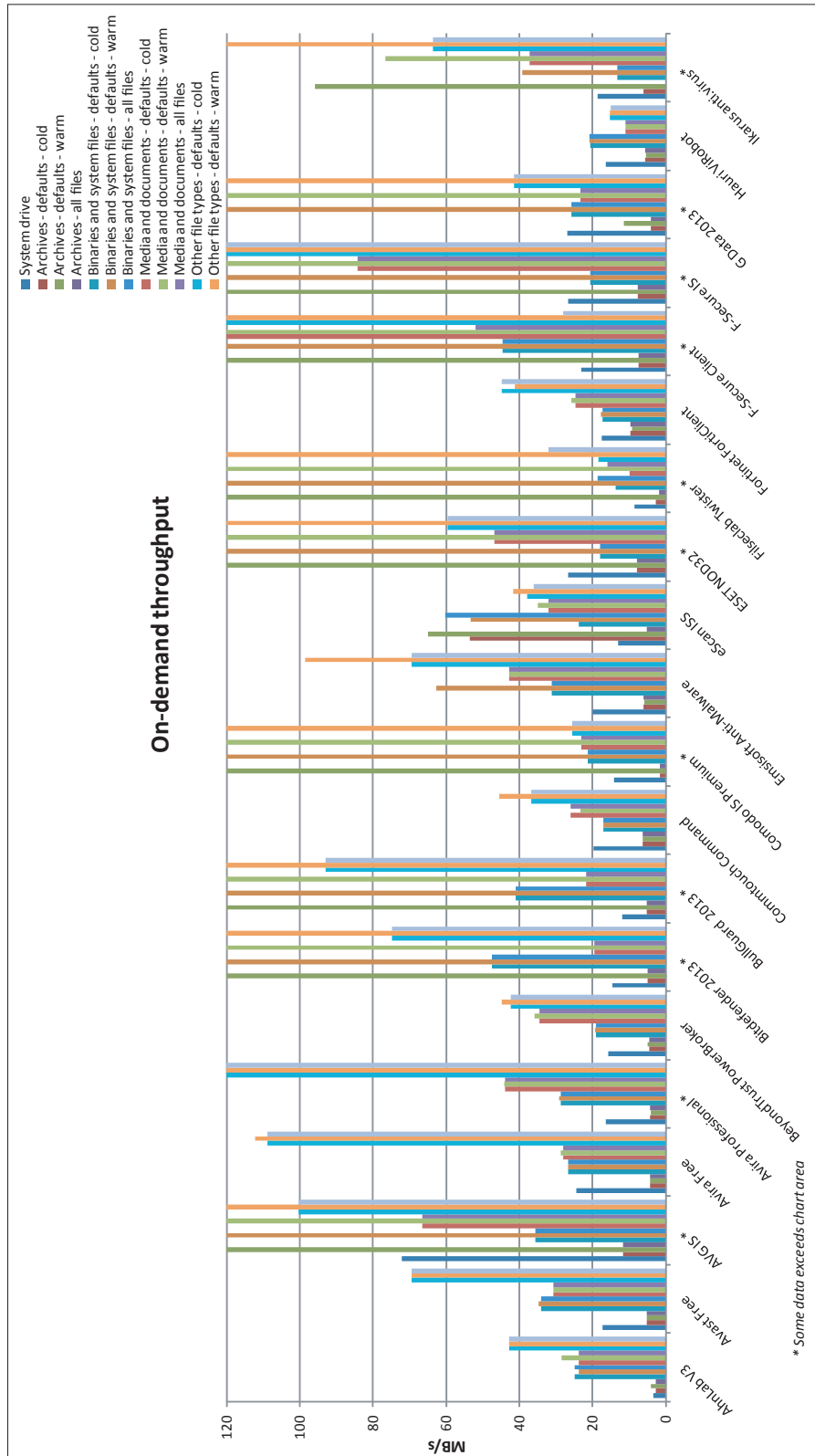
year, *eScan* is one of our most regular participants, and given the issues observed so far with glitzy new interfaces, we were intrigued to see how this one would fare on creaky old *Windows XP*. The installer was a monster 416MB, and got going after only a few clicks. The set-up process takes a few minutes, but keeps the operator entertained with a slideshow featuring a wide range of people smiling happily into their laptops. After five minutes or so a message appears announcing that a reboot is required to complete things, and offering to initiate one. Accepting the offer to reboot seemed to have no effect though, and trying to restart using all normal *Windows* methods also proved fruitless. It appeared that the product had disabled rebooting – one of the core functions of *Windows*.

Further probing found that by killing some of the *eScan* processes rebooting could be reinstated, but as the same issue emerged on each install (and also since one attempt to force a reboot caused a dreaded Blue Screen), we found it easier simply to hit the reset button each time we needed to restart. Once fully installed, the interface was much the same as we remembered: dark and glowering and fairly hard to see at times, but reasonably well laid out and providing ample controls. For the most part it remained fairly stable, although the disabling of reboots seemed permanent, and on a couple of occasions scans of our clean sets froze, refusing to complete or let themselves be cancelled. This seemed particularly prone to occurring when the on-access thoroughness settings were turned up.

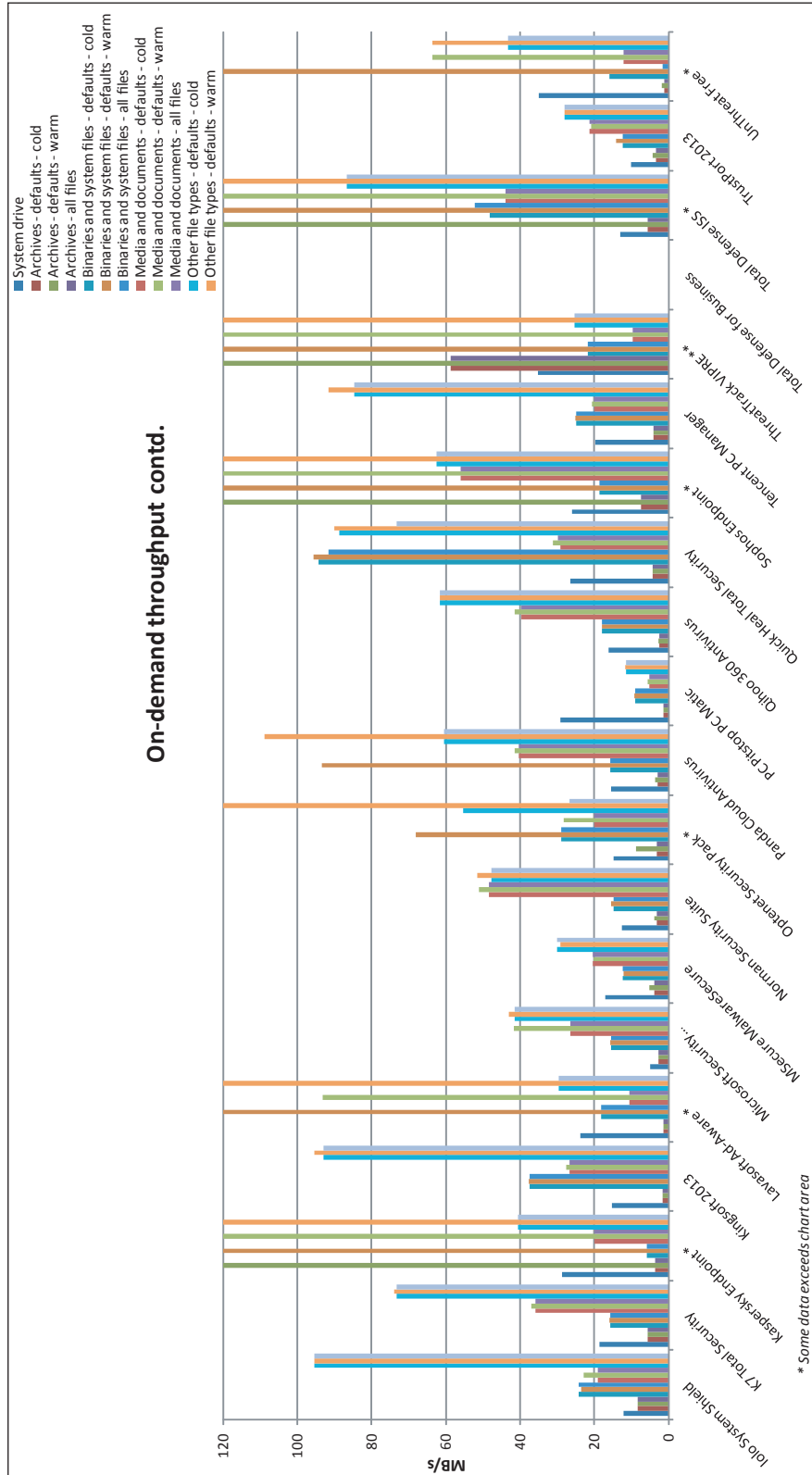
Scanning speeds were pretty decent, and overheads mostly not bad, although with the settings fully turned up our set of binaries took an age to complete. RAM use was a little high, but CPU use not too bad, and our set of tasks was slow to complete, but not excessively so. Detection was as excellent as we would expect, with all sets very well handled – even the proactive week of the RAP sets – and only a slight drop in the very latest day of the Response sets. The WildList set was dealt with perfectly, and the clean sets too, earning *eScan* VB100 certification and maintaining its flawless record of 12 passes in the last two years. However, there were some serious stability issues here: a *Windows* system that cannot reboot is like a house with no doors – usable, but rather awkward – and disabling this pivotal feature is a

On-demand throughput (MB/s)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
AhnLab V3 IS	3.47	2.68	4.01	2.68	24.86	23.71	24.86	23.83	28.41	23.83	42.84	42.84	42.84
Avast Free Antivirus	17.23	5.25	5.22	5.25	34.13	34.70	34.13	30.75	30.64	30.75	69.33	69.33	69.33
AVG IS Business Edtn	72.17	11.60	1366.06	11.60	35.68	997.14	35.68	66.51	571.95	66.51	100.35	762.62	100.35
Avira Free Antivirus	24.34	4.25	4.25	4.25	26.65	26.61	26.65	28.04	28.60	28.04	108.95	112.15	108.95
Avira Pro Security	16.35	4.37	4.05	4.37	28.70	29.01	28.70	44.00	44.22	44.00	131.49	131.49	131.49
BeyondTrust PowerBroker	15.62	4.58	4.85	4.58	18.96	19.21	18.96	34.45	35.75	34.45	42.37	44.86	42.37
Bitdefender Antivirus Plus	14.59	4.98	1093.01	4.98	47.48	861.16	47.48	19.59	476.63	19.59	74.77	635.52	74.77
BullGuard Antivirus 2013	11.83	5.26	1820.96	5.26	41.01	789.36	41.01	21.66	451.57	21.66	93.00	544.73	93.00
CommTouch Command	19.65	6.21	6.23	6.21	17.02	17.04	17.02	26.00	23.31	26.00	36.66	45.39	36.66
Comodo IS Premium	14.00	1.68	1820.96	1.68	21.19	1722.55	21.19	23.06	780.08	23.06	25.42	1040.13	25.42
Emsisoft Anti-Malware	19.93	6.15	5.91	6.15	31.11	62.73	31.11	42.68	42.68	42.68	69.33	98.62	69.33
eScan ISS	12.92	53.56	65.03	5.14	23.83	53.22	60.14	32.13	34.88	32.13	37.75	41.75	35.97
ESET NOD32 Antivirus 6	26.66	7.92	151.75	7.92	17.94	653.31	17.94	46.88	2859.76	46.88	59.58	408.56	59.58
Filseclab Twister Antivirus	8.47	2.60	1820.96	1.88	13.73	3790.44	18.52	9.96	2859.76	15.98	18.33	2288.78	32.04
Fortinet FortiClient	17.37	9.53	9.29	9.53	17.25	17.77	17.25	24.65	25.84	24.65	44.86	41.15	44.86
F-Secure Client Security	23.00	7.37	1820.96	7.37	44.47	2104.96	44.47	129.99	2145.36	52.00	762.62	3813.11	28.04
F-Secure Internet Security	26.66	7.68	1820.96	7.68	20.70	2706.76	20.70	84.11	2859.76	84.11	762.62	3813.11	762.62
G Data AntiVirus 2013	26.83	4.02	11.38	4.02	25.67	1894.65	25.67	23.25	1072.68	23.25	41.45	3813.11	41.45
Hauri ViRobot IS	16.29	5.50	5.41	5.50	20.64	20.84	20.84	10.96	10.96	10.96	15.31	15.31	15.07
Ikarus anti.virus	18.52	6.01	95.84	NA	13.27	39.22	13.27	37.14	76.60	37.14	63.55	254.21	63.55
Iolo System Shield	12.06	8.31	8.23	8.31	24.10	23.62	24.10	19.07	22.76	19.07	95.33	95.33	95.33
K7 Total Security	18.60	5.71	5.62	5.71	15.63	15.80	15.63	35.75	36.98	35.75	73.33	73.80	73.33
Kaspersky ES	28.67	3.64	1820.96	3.64	5.71	6314.88	5.71	19.86	2859.76	19.86	40.57	3813.11	40.57
Kingsoft Antivirus 2013	15.17	1.64	1.64	1.64	37.37	37.51	37.37	26.73	27.59	26.73	93.00	95.33	93.00
Lavasoft Ad-Aware	23.78	1.44	1.45	1.44	18.20	997.14	18.20	10.55	93.26	10.55	29.56	346.65	29.56
Microsoft SE	4.87	2.59	2.66	2.59	15.36	15.79	15.36	26.48	41.65	26.48	41.45	43.01	41.45
MSecure MalwareSecure	16.95	3.77	5.13	3.77	12.29	12.21	12.29	20.43	20.14	20.43	30.02	29.11	30.02
Norman Security Suite	12.57	3.21	3.71	3.21	14.89	15.41	14.89	48.47	51.07	48.47	47.66	51.53	47.66
Optenet Security Pack	14.69	3.21	8.77	3.21	28.84	68.15	28.84	20.00	28.31	20.00	55.26	170.74	26.67
Panda Cloud Antivirus	15.50	2.94	3.68	2.94	15.59	93.32	15.59	40.28	41.45	40.28	60.53	108.95	60.53
PC Pitstop PC Matic	29.07	1.31	1.27	1.31	8.91	9.11	8.91	5.13	5.51	5.13	11.49	11.76	11.49
Qihoo 360 Antivirus	16.23	2.56	2.70	2.56	17.89	17.96	17.89	39.72	41.45	39.72	61.50	61.50	61.50
Quick Heal Total Security	26.33	4.33	4.23	4.34	94.25	95.68	91.52	29.18	31.20	29.79	88.68	90.07	73.33
Sophos ESC	26.00	7.43	1820.96	7.43	18.63	2104.96	18.63	56.07	1429.88	56.07	62.51	1430.27	62.51
Tencent PC Manager	19.75	3.93	4.11	3.93	24.96	25.03	24.96	20.00	20.67	20.00	84.74	91.52	84.74
ThreatTrack VIPRE	35.18	58.74	1820.96	58.74	21.70	3157.44	21.70	9.73	714.94	9.73	25.25	1906.56	25.25
Total Defense for Business	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Total Defense ISS	13.08	5.55	606.99	5.55	48.21	947.33	52.19	44.00	504.72	44.00	86.66	602.10	86.66
TrustPort Antivirus 2013	10.11	3.42	4.18	3.42	12.41	14.00	12.41	21.34	20.72	21.34	28.04	28.04	28.04
UnThreat AntiVirus	34.88	1.06	1.88	1.06	15.87	757.82	1.58	12.12	63.55	12.12	43.33	63.55	43.33

* System drive size measured before product installation. (Please refer to text for full product names.)



(Please refer to text for full product names.)



(Please refer to text for full product names.)

fairly major error for any product. Along with a few other less significant problems, this pushes *eScan*'s stability rating deep into 'Buggy' territory.

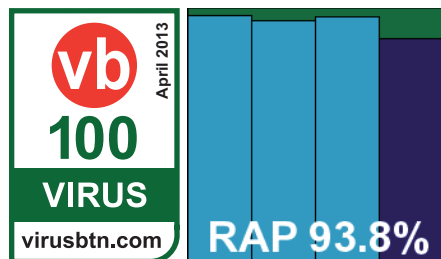
ESET NOD32 Antivirus 6

Main version: 6.0.308.0

Update versions: 8006/1381, 8085/1382, 8104/1382, 8135/1383

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Stable

ESET's submission this month came as a standard installer, with instructions to set up, update and freeze on the deadline day. Installation



was straightforward, the only thing of note being the unusual forced choice of whether or not to detect PUAs, and completed very rapidly. Updates were very speedy too. The interface is clear and unfussy, with comprehensive configuration, and logging is detailed, reliable and usable.

Stability was generally fine, although we did have a single instance of the GUI crashing – which was easily recovered from, did not affect protection and could not be reproduced despite our best efforts. Scanning speeds were zippy, overheads light, RAM use low, CPU use very low and impact on our set of tasks very reasonable too.

Detection was very strong, well up with the leading group in the RAP chart and hard to criticize in the Response sets; the WildList was covered without issue, and with just a handful of (quite accurate) alerts on potentially dodgy items in the clean sets, a VB100 award is well deserved, further extending *ESET*'s epic unbroken run of passes – 12 from 12 in the past two years, and stretching back much further than that. With just one odd incident, a 'Stable' rating is well deserved too.

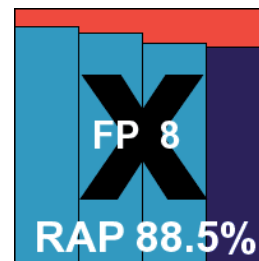
Filseclab Twister Antivirus 8

Main version: NA

Update versions: NA

ItW Std	97.98%	ItW Std (o/a)	97.98%
ItW Extd	95.72%	ItW Extd (o/a)	95.72%
False positives	8	Stability	Stable

Filseclab continues its quest for that elusive first VB100 pass, showing steady improvement with each appearance, particularly in the RAP tests. The latest build came as a 165MB installer, with offline updates in a 29MB package. The set-up process was very speedy, completing in under a minute with a reboot required after some updates. After install a brief set-up wizard asks some probing questions to figure out the user's level of competence before suggesting a more or less advanced version of the interface. The GUI itself is rather attractive, slick, and clear and easy to navigate, with a detailed configuration selection. Logging seemed lucid and reliable.



Scanning speeds were a little slow initially, but blazing fast through the warm runs, while on access things were also a little sluggish, sadly with no signs of improvement later on. RAM use was low but CPU use was decidedly high, and our set of tasks ran through rather slowly.

Detection was quite competitive in the RAP and Response sets, and not bad in the WildList sets either, although not quite reaching the 100% coverage required for certification. There were a handful of false alarms in the clean sets too, including components of *Audacity*, *Gimp*, *iCloud*, *Thunderbird* and *uTorrent*. Nevertheless, *Filseclab* continues to edge closer to the goal. The vendor has no passes from three entries in the last six tests; none from five entries in the last two years. Stability was good, with just a slight wobble during one of the updates, earning a 'Stable' rating.

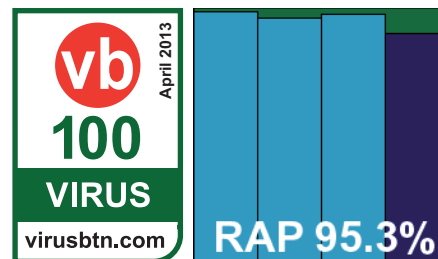
Fortinet FortiClient

Main version: 5.0.1.199

Update versions: 5.0.53/17.157/17.156, 17.248/17.218, 17.248/17.256, 17.335/17.312

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Fair

After a couple of tests with a 'Lite' version of *FortiClient*, this month saw another new version, although it was clear from



the submission details that, like the ‘Lite’ version, it did not offer the full range of controls featured in the old favourite from the last few years. The installer remains very compact at just 12MB, with an offline update package of 158MB also provided, and initial set-up is fast and simple, with just a couple of clicks required and taking little more than a minute.

Our first look at the interface was rather upsetting, with much of it clearly not functioning properly, and it took us a few minutes to realize that this was due to the browser installed on our systems – as the developers had informed us, the product requires a more recent version, but there is nothing in the product itself to warn of this. With the browser updated things worked a lot better, although it is clear that there is still work to do on the interface. It provides a reasonable range of basic controls, although they can be a little hard to find and operate, partly thanks to the laginess and shakiness that seems an inevitable part of a browser-based interface (making one wonder why anyone who didn’t specifically aim to irritate their users would opt for such an approach). There were a number of error messages, a few scans freezing up, and a few stranger oddities too, such as changing some *Windows* desktop and user access options without being asked to.

Once we had figured out how to operate things, though, the tests moved along reasonably well. Scanning speeds weren’t too bad, on-access lag times were a little high initially but much lighter in the warm runs, while resource use was high and our set of tests took a fair while to complete. Detection was excellent though, continuing an upward trend observed over recent tests as heuristics are gradually tweaked upwards. The core sets presented no issues, and *Fortinet* earns a VB100 award, putting it on five passes from five entries in the last six tests; ten from ten in the last two years with only our annual *Linux* tests missed. There’s clearly a little more work to do on this new GUI before it’s ready for real-world use though, and as it stands it only just scraped into the ‘Fair’ category.

F-Secure Client Security

Main version: 10.00 build 413

Update versions: 9.50 build 19031

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	99.95%	ItW Extd (o/a)	99.95%
False positives	0	Stability	Stable

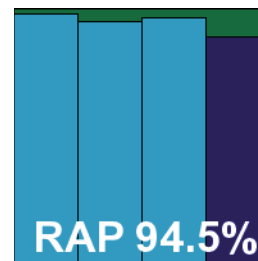
A pair of products were submitted by *F-Secure*, as usual, with this first one presumably the more corporate-focused of the two. In this case a 72MB installer was provided, but updates had to be performed online. Set-up was speedy, although a reboot was required, but the speed of updates was hard to measure, as they dribbled in slowly and only displayed progress deep in the settings area of the interface.

Despite clear messages in the interface stating that we were safe and secure from the off, trying to run tests before this process had completed showed some rather gaping holes in protection, so we had to wait it out each time.

The GUI itself is clean and sparse, providing a basic range of controls; it had a few wobbles here and there, including the apparent inability to run any kind of on-demand scan if an on-access detection had previously been made. A reboot was required to rectify this. Logging remains a little sketchy, with on-demand logs at least mostly reliable these days – the HTML file generated after each scan farms out the list of detections to a text file if it gets too large. On-access logging seems to be entirely absent, however.

Scanning speeds were quite fast, speeding up even further in the warm runs, with lag times quite low on simple file access. RAM use was around average too, but our CPU use measure was well into negative figures. The reason for this is the extreme length of time taken to complete our set of activities – each run taking close to half an hour where the baseline measures were little over two minutes. Worrying that this might be some kind of freak anomaly, we re-ran the job later but got similar figures, and this was confirmed by seeing similar times for the consumer product. We could only assume that it was trying to perform some kind of cloud look-ups, which were taking some time to complete. Either way, there was clearly a lot of idle time during the process, as our CPU measures taken every five seconds recorded very little activity.

Detection was solid though, keeping well up with, if not overtaking other products including the *Bitdefender* engine in the RAP and Response sets. The clean sets saw just a warning on a screensaver from *nVidia* flagged as suspicious by the cloud, and the WildList sets looked to be well handled until we noted a single item in the Extended WildList not being picked up, either on access or on demand, in any of the three runs. Closer investigation into this issue had both ourselves and the developers stumped for some time, as detection seemed fine on repeating the tests later on. It was eventually discovered that the item in question had been erroneously whitelisted in the cloud for a brief spell, which by shocking bad luck had coincided exactly with our testing period. This misfortune is enough to deny *F-Secure* a VB100 award this month, the history for this corporate solution showing three passes and a single fail in the last six tests; seven passes and two fails in the last two years. There were a few little issues noted, assuming the extreme slowdown in our activities set was normal, and the product earns a ‘Stable’ rating.



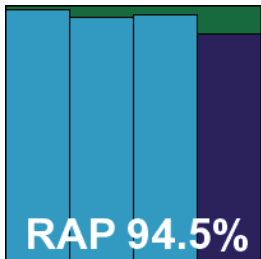
F-Secure Internet Security 2013

Main version: 12.71 build 102

Update versions: 10.00 build 18410

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	99.95%	ItW Extd (o/a)	99.95%
False positives	0	Stability	Stable

The consumer end of *F-Secure's* product line was provided in a rather different format, with a tiny 600KB executable all that was provided initially. This pulled down the rest of the product, and seemed to do so in commendably good time, the whole install process taking less than two minutes and completing with a reboot. Once again, updating is a little hard to keep track of, and again while this was going on the interface suggested that a greater level of protection was in place than was actually the case. The GUI itself is very similar to that of the product's corporate sister, providing a reasonable level of control and mostly seeming responsive and simple to navigate. Logging is just about usable and reasonably dependable these days, at least as far as on-demand data goes.



Performance measures were fairly similar, with scanning speeds a fraction slower, overheads a trifle higher, and RAM use much the same. Once again our set of tasks took an enormous amount of time to get through, and long idle periods meant extremely low CPU use during this period. Detection was splendid for the most part, but again that single item in the Extended WildList was ignored, and no VB100 award can be granted. This product line appears a little less regularly in our tests, now showing two passes and one fail from the last six tests, with no entries for a while before that. Stability was reasonable, falling into the 'Stable' category.

G Data AntiVirus 2013

Main version: 23.1.0.2

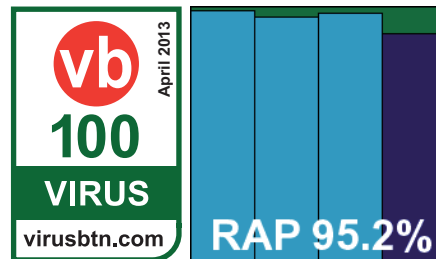
Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

G Data's desktop product came as a fairly large 298MB installer, which took half a minute or so to find its feet before things got moving. It ran through a few standard questions then took another minute to complete, needing a

reboot at the end. Updates were a little on the slow side, taking almost ten minutes on one occasion. The interface is businesslike, providing an exemplary range of controls in a simple, clear manner, and proved rock-solid under everything we could throw at it.

Scanning speeds were not bad to start with and a lot better in the warm runs, with overheads a little high initially and again improving a lot after an initial settling-in period. Resource use was a little above average, but our set of tasks completed in reasonable time. Detection rates were stellar, with all our sets brushed aside and very little indeed missed in our Response sets. With no issues in the certification sets a VB100 award is comfortably earned. *G Data* now has four passes from four entries in the last six tests; eight passes and one fail in the last two years. This month's performance earned a 'Solid' stability rating.



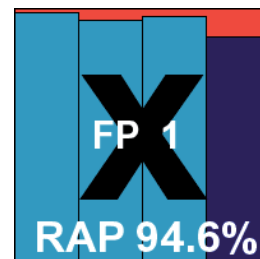
Hauri ViRobot Internet Security 2011

Main version: 6.0.0.0

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	98.65%
False positives	1	Stability	Stable

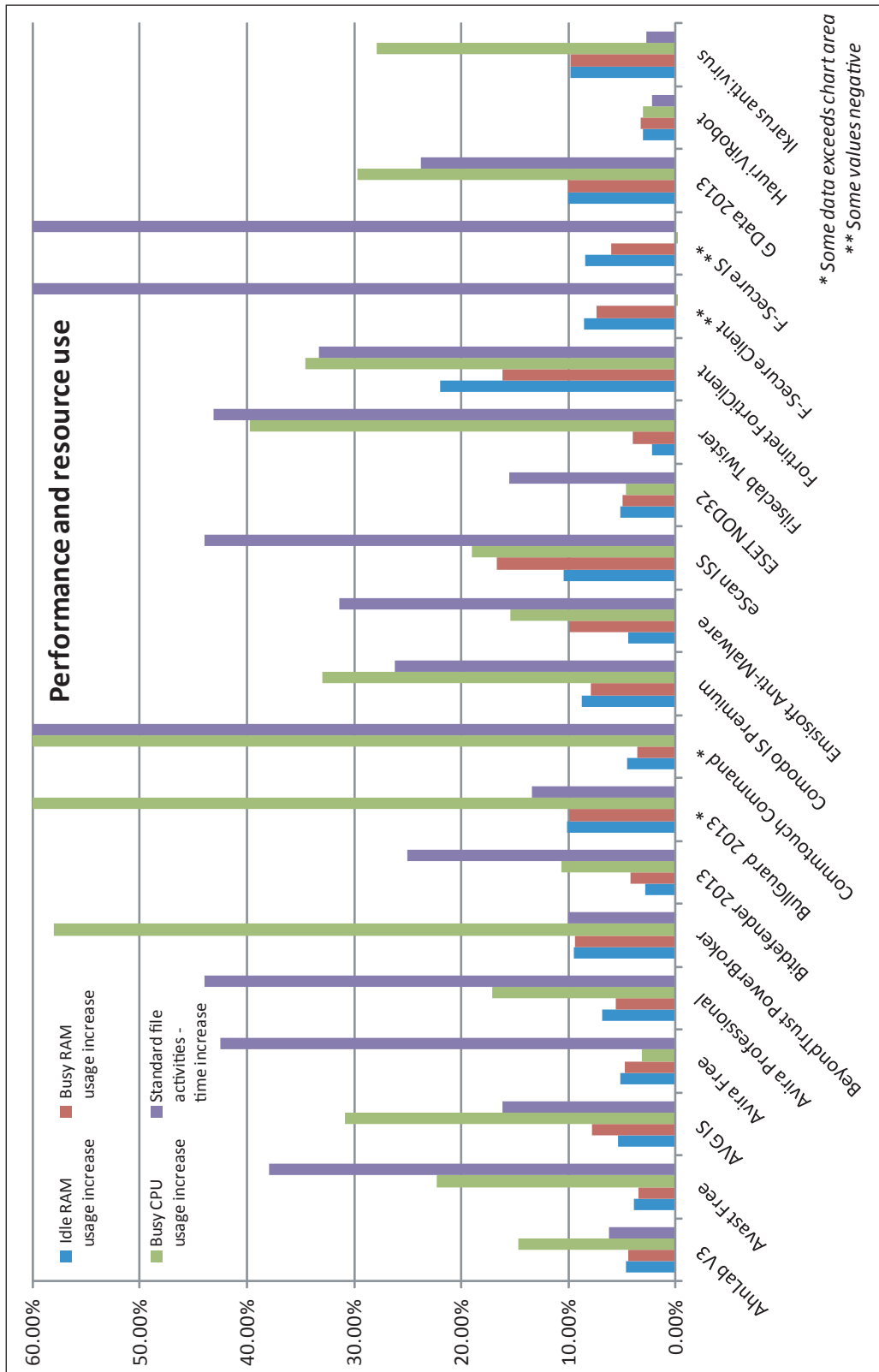
Hauri's products have given us some problems in recent tests, routinely underperforming compared to others based on the same *Bitdefender* engine. We hoped that some of the biggest issues would be fixed for this month's test. The installer was a fair size at 214MB, and ran through quite a few steps but took minimal working time, completing in little over a minute. Somewhat oddly, a warning appeared halfway through, stating that there was no web access, but initial updates (an area where we have had problems in the past) proceeded apace; this time all went fine, and we managed to get the definitions updated to current levels, somewhat to our surprise.



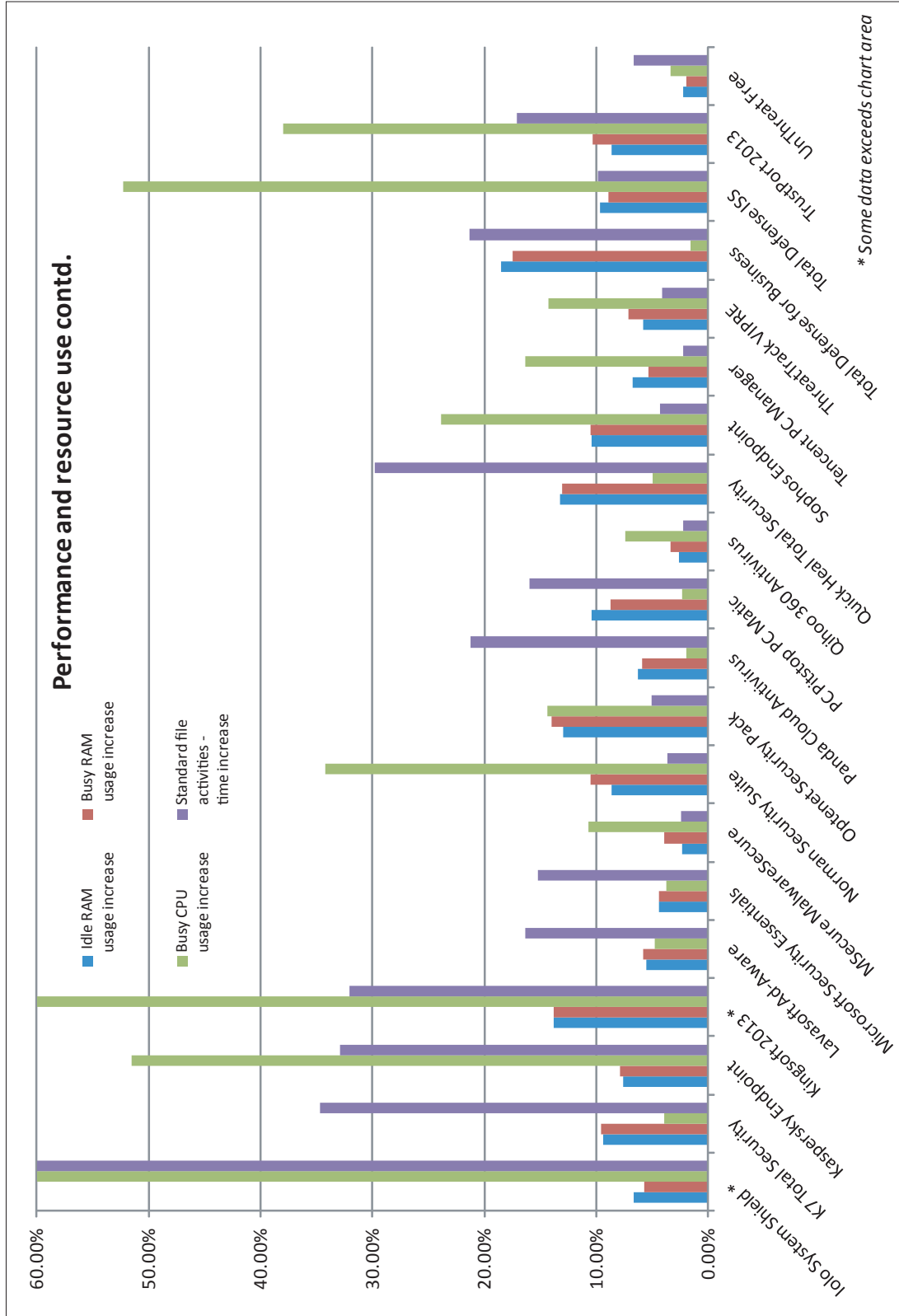
The interface is a little short on charm, but works reasonably well, providing at least some configuration, although much of it is less than clear. Logging is decent

Performance tests	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase	Standard file activities - time increase
AhnLab V3 Internet Security	4.67%	4.46%	14.71%	6.28%
Avast Free Antivirus	3.96%	3.51%	22.29%	37.90%
AVG Internet Security Business Edition	5.43%	7.82%	30.88%	16.13%
Avira Free Antivirus	5.17%	4.71%	3.22%	42.49%
Avira Professional Security	6.92%	5.59%	17.11%	44.01%
BeyondTrust PowerBroker EPP	9.53%	9.39%	58.00%	10.04%
Bitdefender Antivirus Plus 2013	2.81%	4.23%	10.65%	25.04%
BullGuard Antivirus 2013	10.12%	9.91%	212.30%	13.37%
CommTouch Command	4.49%	3.62%	71.77%	207.20%
Comodo IS Premium	8.73%	7.92%	33.01%	26.17%
Emsisoft Anti-Malware	4.42%	9.96%	15.44%	31.34%
eScan Internet Security Suite	10.43%	16.70%	19.02%	43.96%
ESET NOD32 Antivirus 6	5.21%	4.99%	4.68%	15.48%
Filseclab Twister Antivirus 8	2.17%	4.06%	39.73%	43.10%
Fortinet FortiClient	22.00%	16.19%	34.55%	33.33%
F-Secure Client Security*	8.55%	7.36%	-83.30%	1114.79%
F-Secure Internet Security*	8.48%	5.99%	-80.40%	1138.42%
G Data AntiVirus 2013	10.06%	10.08%	29.67%	23.78%
Hauri ViRobot Internet Security 2011	3.06%	3.29%	3.05%	2.21%
Ikarus anti.virus	9.84%	9.85%	27.96%	2.72%
Iolo System Shield	6.64%	5.70%	75.04%	207.98%
K7 Total Security	9.42%	9.62%	3.93%	34.73%
Kaspersky Endpoint Security	7.58%	7.91%	51.47%	32.92%
Kingsoft Antivirus 2013	13.83%	13.78%	62.35%	32.03%
Lavasoft Ad-Aware Pro Security	5.49%	5.83%	4.74%	16.35%
Microsoft Security Essentials	4.39%	4.38%	3.77%	15.26%
MSecure MalwareSecure	2.37%	3.89%	10.71%	2.45%
Norman Security Suite	8.67%	10.53%	34.22%	3.67%
Optenet Security Pack	12.98%	14.02%	14.37%	5.05%
Panda Cloud Antivirus FREE	6.30%	5.95%	1.92%	21.25%
PC Pitstop PC Matic	10.40%	8.71%	2.36%	15.99%
Qihoo 360 Antivirus	2.65%	3.34%	7.37%	2.21%
Quick Heal Total Security 2013	13.28%	13.02%	5.00%	29.79%
Sophos Endpoint Security and Control	10.46%	10.54%	23.85%	4.34%
Tencent PC Manager	6.79%	5.35%	16.39%	2.23%
ThreatTrack VIPRE Antivirus 2013	5.84%	7.11%	14.31%	4.12%
Total Defense for Business	18.49%	17.49%	1.57%	21.31%
Total Defense Internet Security Suite	9.63%	8.96%	52.23%	9.87%
TrustPort Antivirus 2013	8.62%	10.29%	37.93%	17.14%
UnThreat AntiVirus Free Edition	2.22%	1.96%	3.40%	6.61%

*Negative CPU measure due to long idle periods during testing. (Please refer to text for full product names.)



(Please refer to text for full product names.)



for the most part, but at least one scan clearly gave up well before it had finished, with no warning. Scanning speeds were sluggish, and overheads look light but cannot be compared with most products as there seems to be no on-read protection available. Use of resources and impact on our set of tasks also look light, and again the unusual approach to protection will doubtless have played a major part in this.

Detection was excellent in the RAP sets, well up with the leaders and closely clustered with other users of the *Bitdefender* engine, but in the Response sets numbers were well down, suggesting that perhaps updates were not as successful as they appeared. The WildList sets were well handled, but in the clean sets a single item, part of the *RealPlayer* package, was flagged as malware, denying *Hauri* a VB100 award this month. The vendor's test record shows a good run of late, with four passes and now a single fail in the last six tests; two fails and four passes over the last two years. A few wobbles were noted, earning a 'Stable' rating.

Ikarus anti.virus

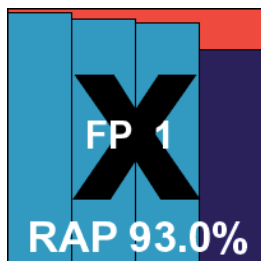
Main version: 2.2.14

Update versions: 1.4.0/83441, 83615, 83668, 83725

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	1	Stability	Stable

Quite a regular these days with a number of good showings of late, *Ikarus* provided its product in the form of a CD ISO image, along with a separate 150MB offline update bundle. The set-up process includes the requirement to install the .NET 2.0 framework, which is thoughtfully included in the ISO, and this adds a fair amount to the initial set-up time. Otherwise things moved along nicely, with a full set of stages to click through (including the option to provide automated feedback rather sneakily hidden on a greyed-out update settings page). The interface is plain and minimalist, with only a basic set of controls, but is reasonably simple to operate and provides ample, reliable logs of its activities. On a few occasions under heavy stress it became a little shaky, but quickly recovered itself without intervention.

Scanning speeds were impressive, and overheads very light indeed, with RAM use a fraction above average, CPU use a little below, but impact on our set of tasks barely perceptible. Detection was pretty good in the RAP



sets, tailing off very slightly into the proactive week, and excellent in the Response sets, with just the slightest decline in the most recent few days. The WildList sets were well handled, but in the clean sets a single item, part of the *Gimp* package, was mislabelled as malicious and *Ikarus* just misses out on a VB100 award this month. The vendor's test history now shows two passes and three fails in the last six tests; three passes and six fails in the last two years. This month's performance merited a 'Stable' rating.

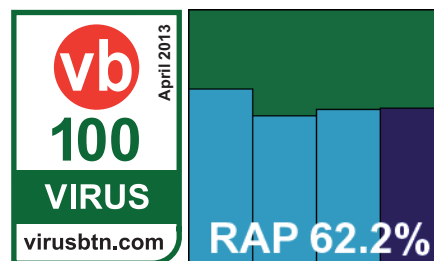
Iolo System Shield

Main version: 4.5.1.7

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Fair

Having been absent from our tests for a while, *Iolo* returns with its product looking much the same. The install package provided was



a tiny 500KB downloader which fetched the main 57MB installer from the web – an option is provided to keep this installer in case it is needed again. The initial set-up zips through, then pauses for a minute or so at a stage labelled 'finalize'. Eventually a reboot is needed, after which an update runs extremely quickly, completing in less than half a minute. The product interface has a brisk, professional but not unfriendly look, and provides a surprisingly detailed level of fine-tuning, although our preferred option, to only log malware detections, is absent. In this case it would be of little use anyway, as despite repeated requests to the developers we have been unable to find any information on how to decrypt the log data, which is stored in some unfriendly database format and is not exportable from the product GUI.

Stability was mostly good, but after running our performance tests it seemed as if something odd was going on: trying to disable the on-access element to replace some test samples appeared to have worked, but access was still being blocked, so the system was rebooted. On restart, however, a message appeared saying that the product could not access a required RPC service, and was therefore unusable. Despite much effort we could find no way of repairing things, and in the end had to wipe the system and reinstall to let us

Response tests	Day -7	Day -6	Day -5	Day -4	Day -3	Day -2	Day -1	Average
AhnLab V3 Internet Security	90.26%	91.16%	89.12%	85.62%	87.64%	91.15%	88.15%	89.01%
Avast Free Antivirus	98.31%	97.37%	97.77%	97.11%	97.96%	97.90%	95.42%	97.41%
AVG Internet Security Business Edition	94.72%	99.69%	99.56%	99.57%	99.31%	99.53%	97.60%	98.57%
Avira Free Antivirus	99.76%	99.74%	99.41%	99.73%	99.53%	98.43%	98.03%	99.23%
Avira Professional Security	99.76%	99.74%	99.41%	99.73%	99.53%	98.43%	98.03%	99.23%
BeyondTrust PowerBroker EPP	98.98%	98.93%	95.96%	84.80%	97.72%	97.64%	97.38%	95.92%
Bitdefender Antivirus Plus 2013	98.26%	98.75%	98.86%	98.69%	98.87%	98.82%	93.76%	98.00%
BullGuard Antivirus 2013	98.40%	98.77%	98.94%	98.80%	98.92%	98.86%	93.75%	98.06%
Commtouch Command	97.96%	97.33%	95.46%	90.62%	94.34%	93.32%	88.05%	93.87%
Comodo IS Premium	98.43%	86.98%	75.26%	76.83%	75.77%	53.88%	53.09%	74.32%
Emsisoft Anti-Malware	99.65%	99.50%	96.47%	90.25%	98.24%	99.69%	97.03%	97.26%
eScan Internet Security Suite	98.35%	98.77%	98.91%	98.79%	98.87%	98.79%	93.82%	98.04%
ESET NOD32 Antivirus 6	97.25%	97.87%	98.13%	98.34%	98.11%	97.56%	96.27%	97.65%
Filseclab Twister Antivirus 8	85.27%	86.79%	82.95%	89.60%	82.99%	70.22%	86.47%	83.47%
Fortinet FortiClient	99.69%	99.27%	99.63%	99.15%	96.76%	93.50%	96.50%	97.79%
F-Secure Client Security	98.28%	98.98%	99.21%	98.48%	99.11%	99.35%	94.73%	98.30%
F-Secure Internet Security	98.36%	98.88%	99.28%	98.70%	98.64%	96.97%	95.38%	98.03%
G Data AntiVirus 2013	99.95%	99.84%	99.74%	99.55%	99.71%	99.69%	98.94%	99.63%
Hauri ViRobot Internet Security 2011	76.42%	71.50%	77.51%	81.24%	82.41%	85.80%	61.18%	76.58%
Ikarus anti.virus	99.07%	98.97%	98.76%	99.33%	99.06%	97.48%	98.28%	98.71%
Iolo System Shield	73.34%	71.39%	70.59%	53.86%	68.40%	70.97%	69.65%	68.31%
K7 Total Security	84.58%	87.01%	81.68%	85.53%	88.93%	70.74%	80.82%	82.76%
Kaspersky Endpoint Security	95.10%	97.23%	97.27%	98.39%	97.59%	94.30%	95.54%	96.49%
Kingsoft Antivirus 2013	99.69%	99.60%	99.41%	99.70%	99.48%	98.38%	98.02%	99.18%
Lavasoft Ad-Aware Pro Security	99.47%	99.03%	99.38%	99.34%	98.42%	98.65%	96.46%	98.68%
Microsoft Security Essentials	94.73%	95.49%	94.16%	93.36%	94.91%	92.42%	95.21%	94.32%
MSecure MalwareSecure	98.90%	98.73%	98.60%	99.20%	98.85%	96.97%	98.17%	98.49%
Norman Security Suite	98.56%	98.19%	98.10%	98.33%	97.66%	96.17%	96.63%	97.66%
Optenet Security Pack	98.10%	98.82%	98.74%	99.20%	98.69%	95.71%	97.55%	98.12%
Panda Cloud Antivirus FREE	99.13%	94.26%	99.87%	77.96%	84.60%	82.55%	94.87%	90.46%
PC Pitstop PC Matic	99.25%	99.38%	99.60%	99.49%	98.73%	98.80%	95.39%	98.66%
Qihoo 360 Antivirus	98.30%	98.63%	98.82%	98.58%	98.66%	98.58%	93.85%	97.92%
Quick Heal Total Security 2013	80.59%	74.11%	75.16%	82.09%	71.64%	63.64%	65.17%	73.20%
Sophos Endpoint Security and Control	99.12%	98.83%	98.90%	98.56%	98.91%	98.59%	98.72%	98.80%
Tencent PC Manager	99.72%	99.74%	99.39%	99.73%	99.53%	98.43%	98.25%	99.25%
ThreatTrack VIPRE Antivirus 2013	99.26%	99.30%	99.53%	99.38%	98.71%	98.71%	96.92%	98.83%
Total Defense for Business	96.79%	98.54%	99.35%	96.87%	98.78%	96.59%	98.69%	97.94%
Total Defense Internet Security Suite	72.70%	70.81%	71.07%	63.61%	50.81%	76.52%	77.50%	69.00%
TrustPort Antivirus 2013	99.78%	99.70%	99.92%	99.59%	99.75%	99.57%	97.81%	99.45%
UnThreat AntiVirus Free Edition	98.73%	98.93%	99.26%	99.07%	98.10%	98.39%	96.62%	98.44%

(Please refer to text for full product names.)

move along. Otherwise, speed tests went well and seemed reasonably zippy, but overheads were very high on access; RAM use was low but CPU use very high, and our set of tasks was very heavily impacted, much as we saw with *Commtouch* whose engine is included in this product.

Detection rates in the RAP tests were disappointing, a little behind those of *Commtouch*, while Response scores lagged well behind, implying that only local detection is available here, without the additional cloud look-ups that so boosted *Commtouch*'s own scores. Thanks to the heavy slowdown in our activities measure, the product falls well outside the scope of our new detection-performance scatter chart. Note that these scores are based on our best interpretation of extremely unwieldy logs, and as in the past it seems likely that some data may have been rendered unreadable despite our efforts.

The WildList sets were handled well though, with no problems on access and, after much careful scrutiny, a full complement of detections were unscrambled from the on-demand logs. With no FPs either, a VB100 award is earned – *Iolo*'s first from two attempts in the last six tests. The vendor now has two passes and four fails from six entries in the last two years. Stability was generally OK, but one incident was pretty severe, albeit not reproducible, putting the product well down into the 'Fair' category.

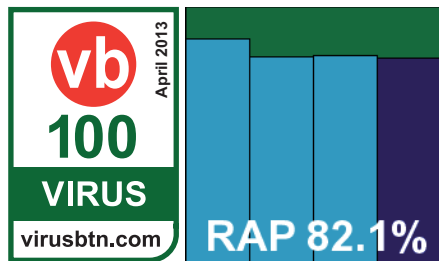
K7 Total Security

Main version: 12.2.0.174

Update versions: 9.160.8215, 13.1.0187/9.162.8300, 13.1.0188/9.163.8351, 9.164.8404

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

Having undergone a fairly radical redesign not too long ago, *K7*'s current product continues to draw appreciation from the lab



team for its clear and pleasant styling. The 93MB installer runs with a single click and completes very rapidly indeed, with updates taking between one and three minutes – only the later, slower one requiring a reboot. The GUI is crisp with a strong theme, and provides a solid level of control in easily accessible fashion. It operated cleanly and smoothly throughout testing.

Scanning speeds were pretty decent, and overheads not bad either with some good speed up in the warm runs. RAM use was a fraction above average but CPU use was low; our set of tasks took a little longer than average to complete. Detection was decent – not quite up with the leaders in the RAP test but not far behind, with similar figures in the Response test too. The core sets were well handled, and a VB100 award is earned without fuss. *K7* now stands on two passes and one fail from three entries in the last six tests; four passes and one fail in the last two years. This month's assured performance earns a 'Solid' stability rating.

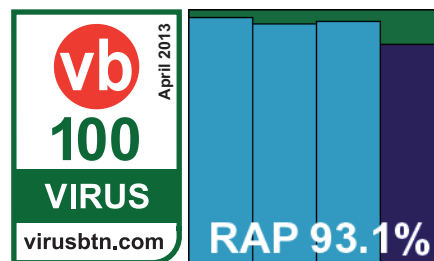
Kaspersky Endpoint Security 10 for Windows

Main version: 10.1.0.867

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Stable

Kaspersky's latest corporate product came as a jumbo 410MB installer, with an update bundle weighing in at 315MB but supporting



many other products. It ran through a number of steps to complete in around a minute and a half. Initial updates were reasonably speedy, adding a couple more minutes to the total install time. The product interface is glossy and slick, with a few quirks but little difficulty accessing the comprehensive set of controls for this multi-featured product. Logging is also comprehensive and easily manipulated, as befits a business-oriented product. Stability was mostly decent, with some significant slowness in exporting large logs and a single instance of the scanner crashing during a high-stress scan.

Scanning speeds were pretty slow to start with, especially in our set of executables and other binaries, but they sped up to almost instant in the warm runs. Overheads on access were light, with fairly high CPU use at busy times but use of memory and impact on our set of tasks were both around average. Detection was very strong – very steady through the RAP sets with just a small drop into the proactive week, and similarly stable in the Response sets with only a tiny dip into the latest few days. The WildList and clean sets brought no issues, and a VB100 award is easily earned by *Kaspersky*, which now stands on six passes out of six in the

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
AhnLab V3 Internet Security	OD	X	X	√	√	√	√	√	X	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Avast Free Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
AVG Internet Security Business Edtn	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Avira Free Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/6	X/√	X/6	X/6	X/6	X/6	X/√	X/7	X/√	√
Avira Professional Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BeyondTrust PowerBroker EPP	OD	X	3	1	3	1	1	1	8	2	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Bitdefender Antivirus Plus 2013	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X/2	X/1	X/1	2	X/2	X/2	X/1	1/2	1/2	√
BullGuard Antivirus 2013	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	2/√	X	X	X	1	1	√
CommTouch Command	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	2	2	2	2	2	√	2	1	2	2	√
Comodo IS Premium	OD	X	4	4	4	5	5	5	2	5	X	√
	OA	X	X	X	X	5	X	X	X	X	X	√
Emsisoft Anti-Malware	OD	√	√	X	X	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
eScan Internet Security Suite	OD	X/√	X/√	8	8	X/√	X/√	X/√	X/8	1/√	1/√	√
	OA	X/8	1/8	8	8	X/8	X/8	X/8	X	1/8	1/8	√
ESET NOD32 Antivirus 6	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Filseclab Twister Antivirus 8	OD	√	√	√	√	√	1	√	X	√	X	√
	OA	X	5	5	5	X	X	6	X	7	X	X
Fortinet FortiClient	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	√	√	√	√	√	√	√	√	√	√
F-Secure Client Security	OD	X	√	√	√	√	√	√	8	√	X	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
F-Secure Internet Security	OD	X	√	√	√	√	√	√	8	√	X	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
G Data AntiVirus 2013	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	8/√	8/√	√	√
Hauri ViRobot Internet Security 2011	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Ikarus anti.virus	OD	7	7	7	7	7	7	7	7	7	7	√
	OA	2	2	2	2	2	2	2	2	2	2	√

Key:

√ - Detection of EICAR test file up to ten levels of nesting
 X - No detection of EICAR test file
 X/√ - default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level
 * Detection of EICAR test file with randomly chosen file extension
 (Please refer to text for full product names.)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Iolo System Shield	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	5	5	5	5	5	√	5	2	5	5	√
K7 Total Security	OD	X	1	1	1	1	1	1	X	2	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Kaspersky Endpoint Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kingsoft Antivirus 2013	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Lavasoft Ad-Aware Pro Security	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Microsoft Security Essentials	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	1	1	X	X	X	X	1	X	√
MSecure MalwareSecure	OD	1	1	1	1	1	1	1	X	1	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Norman Security Suite	OD	X	√	√	√	√	√	√	√	√	X	√
	OA	X	X	1	3	X	X	X	X	X	X	√
Optenet Security Pack	OD	2	2	X	X	2	2	2	X	2	2	√
	OA	X	X	X	X	√	X	X	X	1	1	√
Panda Cloud Antivirus FREE	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	2	X	X
PC Pitstop PC Matic	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Qihoo 360 Antivirus	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	8	8	√	X	X	X	1	1	√
Quick Heal Total Security 2013	OD	X/2	2/5	1/2	1/2	2/5	X	2/5	1	2/5	X	√
	OA	2	X	2	2	1	X	X	X	1	X	√
Sophos Endpoint Security and Control	OD	X	5	5	5	5	5	5	5	5	5	√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Tencent PC Manager	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
ThreatTrack VIPRE Antivirus 2013	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Total Defense for Business	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X/2	X	X	X	X/1	X/1	√
Total Defense Internet Security Suite	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
TrustPort Antivirus 2013	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	1/√	√
UnThreat AntiVirus Free Edition	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√

Key:

√ - Detection of EICAR test file up to ten levels of nesting
 X - No detection of EICAR test file
 X/√ - default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level
 * Detection of EICAR test file with randomly chosen file extension
 (Please refer to text for full product names.)

last year; nine passes and two fails from 11 entries in the last two years. The product is given a 'Stable' rating this month.

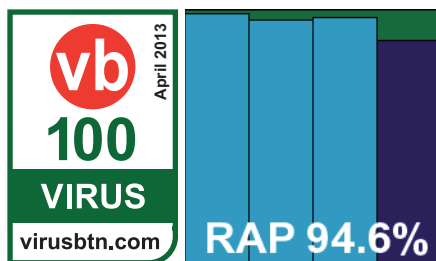
Kingssoft Antivirus 2013 SP2.0

Main version: 2013.SP2.0.020411

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Stable

After a fairly lengthy absence from our tests, *Kingssoft* returned late last year with a glitzy new look and a new third-party engine under



the hood, courtesy of *Avira*. Back for more this month, the 91MB installer has a very zippy and funky progress meter which blasts through in seconds. Updates are speedy too for the most part, although on one run a couple of attempts failed before finally doing the business. The GUI is glossy and stylish but not the easiest to navigate, with some rather confusing language, but a reasonable degree of configuration is provided once you've found your way around.

Scanning speeds were slow over archives but good elsewhere, while overheads were perhaps just a trifle high. Resource use was distinctly on the high side, particularly use of CPU cycles, but our set of activities completed in reasonable time. Detection was very strong, as we would expect from the *Avira* engine, with only the very slightest of drops in the most recent RAP and Response sets. The core certification sets were handled impeccably, thus the product easily earns a VB100 award. The vendor now has two passes from two entries in the last six tests, plus an extra one just under two years ago from its previous incarnation. *Kingssoft* earns a 'Stable' rating this month, let down only by some shakiness in the updater – next time, we are promised a Chinese-language-only version.

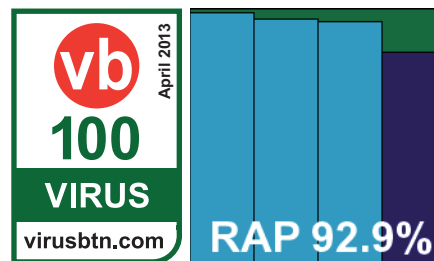
Lavasoft Ad-Aware Pro Security

Main version: 10.4.49.4168

Update versions: 15522, 10.5.1.4369/15898, 16018, 16322

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Stable

Lavasoft's Ad-Aware is the first of a clutch of products on this month's test bench that use the *VIPRE* engine (the company behind which



has recently been redesignated as *ThreatTrack* after splitting off from mother company *GFI*).

We have encountered some stability issues with the *Lavasoft* product in the past, but things seem to be improving gradually. The installer submitted was a tiny 5.8MB with no built-in detection data, and took us through a number of steps, including adding a browser plug-in and adjusting the default search engine to *Blekkio*. It also offered the option to perform a 'compatible' install, allowing it to operate alongside another solution. The main install took little more than a minute, with a reboot at the end, but updates were slightly slower, averaging four minutes for the first run.

The product interface is a little different from the norm but is colourful and looks professional; very minimal configuration is provided, at least as far as we could tell. Logging is in XML format and is fairly usable, but rather frustratingly it seems to wipe most of the data as soon as a task has ended – we lost a good chunk of time before we realized that this was the case. On one occasion, during a scan of part of the clean sets, the interface froze up completely and a reboot was needed to access the controls again – however, this seemed to be only a surface issue, with the scan completing successfully in the background.

Scanning speeds were very slow over archives, despite only a limited set of archive types being looked at, but not bad elsewhere, speeding up a lot in the warm runs in the other sets. On-access lag times were pretty light, although the fact that some scanning for time-consuming files has been moved to the background will have had an impact here. Resource use was low, particularly the CPU measure, and our set of tasks completed in reasonable time.

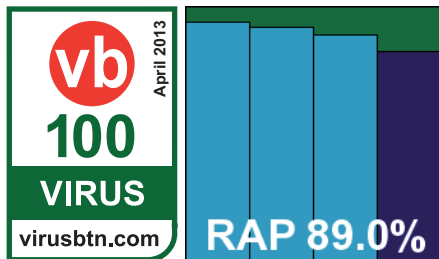
Detection rates were consistently high, with not much missed anywhere, and with nothing missed from the WildList set and no false positives either, a VB100 award is easily earned. This puts *Ad-Aware* on one pass and one fail from two entries in the last few months, with the vendor's last appearance way back in early 2011. There were a few little wobbles in the GUI, but nothing too serious and a 'Stable' rating is merited.

Microsoft Security Essentials

Main version: 4.2.223.0
 Update versions: 1.1.9103.0/1.143.2136.0,
 1.1.9203.0/1.145.1212.0, 1.1.9302.0/1.147.81.0,
 1.1.9302.0/1.147.556.0

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.72%
False positives	0	Stability	Fair

Microsoft's free-for-home-use desktop solution has become a fixture in our desktop tests and generally proves reliable.



The package provided this month was a slimline 10MB installer with offline updates also fairly small at 75MB. Set-up is very fast, with initial updates taking an extra couple of minutes, but no reboots were needed. The interface is neat and clean, although occasionally there were some rendering issues, and a good basic set of controls is provided. Logging is mostly detailed and clear, although on a couple of occasions scans seemed to complete without leaving any evidence of their passing. We also saw a couple of jobs fail to run at all, with rather stark error messages, and at one point there was a full crash of the interface during an overnight scan. Most jobs ended up including an overnight period, as it seemed that all our core malware tasks – which many products manage to complete in a couple of hours – would last longer than a working day.

In the end, though, we got everything done successfully, with scanning speeds not too bad over clean files, a little low in the archive sets but still quite acceptable given the thorough unpacking defaults. On-access lag times were pretty light and showed signs of good optimization in the warm runs, while resource use was very low and our set of tasks got through in good time. Detection was reliably decent in the Response sets, showing a gradual downward curve in the RAPs, but there were no issues in the WildList or clean sets and a VB100 award is well deserved. This puts *Microsoft Security Essentials*, which usually enters all desktop tests but missed out in the *Windows 8* test thanks to the built-in *Windows Defender*, on two passes from two entries in the last six tests; five from five in the last year. A few stability issues were noted, including failure to log data and a GUI crash, which nudges our rating just over the edge into 'Fair'.

MSecure Data Labs MalwareSecure

Main version: 1.1.107.0
 Update versions: 83441, 836155, 83668, 83725

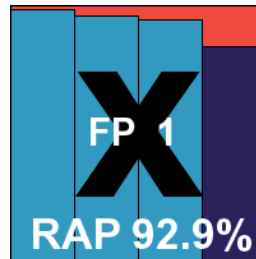
ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	99.54%	ItW Extd (o/a)	94.76%
False positives	1	Stability	Stable

A relative newcomer to our tests, *MSecure's* solution includes the *Ikarus* engine. Initial set-up was from a small 16MB installer, and followed a standard path, completing in good time.

Updates were provided offline, measuring 97MB, and when run online proved fairly speedy.

The interface is angular and a little cluttered in places, providing a basic but reasonable set of controls, and was mostly responsive with just a few moments of jerkiness.

Scanning speeds were on the slow side, and overheads started out fairly heavy too, but improved a lot in the warm runs. Resource use was low though, and our set of tasks completed in very good time indeed. Detection was very strong, with only the proactive week of the RAP sets showing any real decline. The WildList sets were well covered on demand, but on access a few items seemed to go unnoticed and this, coupled with the expected false alarm on part of the *Gimp* package in the clean sets, was enough to deny *MSecure* a VB100 award this month despite a reasonable showing. With only two entries under its belt, the vendor now has one pass and one fail; this month a 'Stable' rating is comfortably earned.

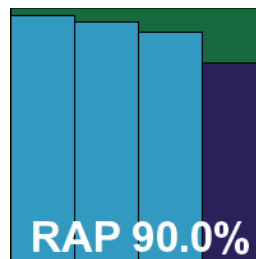


Norman Security Suite 10.00

Main version: 7.00.22
 Update versions: NA










ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	99.91%	ItW Extd (o/a)	99.91%
False positives	0	Stability	Stable

Norman's product is another that has been given a shiny new look to coincide with the arrival of *Windows 8*, and we were interested to see how well it worked on a rather older, plainer platform. The installer submitted was a fairly large 226MB, and after a few clicks the set-up



Reactive And Proactive (RAP) tests	VB100	Reactive			Reactive Average	Proactive Week +1	Overall Average
		Week -3	Week -2	Week -1			
AhnLab V3 Internet Security		95.43%	87.18%	84.78%	89.13%	78.34%	86.43%
Avast Free Antivirus		95.92%	92.22%	90.51%	92.88%	83.36%	90.50%
AVG Internet Security Business Edition		98.02%	94.24%	85.84%	92.70%	81.19%	89.82%
Avira Free Antivirus		98.33%	95.67%	96.13%	96.71%	87.62%	94.44%
Avira Professional Security		98.33%	95.67%	96.13%	96.71%	87.62%	94.44%
BeyondTrust PowerBroker EPP	X	98.17%	95.46%	95.12%	96.25%	80.62%	92.34%
Bitdefender Antivirus Plus 2013		98.05%	95.05%	96.73%	96.61%	88.86%	94.67%
BullGuard Antivirus 2013		98.06%	95.01%	96.60%	96.55%	88.79%	94.61%
CommTouch Command	X	79.51%	68.26%	70.20%	72.66%	69.46%	71.86%
Comodo IS Premium	X	N/T	N/T	N/T	N/T	N/T	N/T
Emsisoft Anti-Malware		90.92%	92.82%	88.56%	90.77%	84.91%	89.30%
eScan Internet Security Suite		98.05%	95.00%	96.58%	96.54%	88.76%	94.60%
ESET NOD32 Antivirus 6		96.82%	94.58%	96.37%	95.92%	87.51%	93.82%
Filseclab Twister Antivirus 8	X	92.64%	90.03%	86.42%	89.70%	84.85%	88.49%
Fortinet FortiClient		98.34%	95.88%	97.21%	97.14%	89.83%	95.31%
F-Secure Client Security	X	97.88%	94.90%	96.33%	96.37%	88.67%	94.45%
F-Secure Internet Security	X	98.06%	95.04%	96.32%	96.47%	88.76%	94.54%
G Data AntiVirus 2013		98.49%	95.84%	97.28%	97.20%	89.29%	95.23%
Hauri ViRobot Internet Security 2011	X	98.02%	95.01%	96.73%	96.59%	88.75%	94.63%
Ikarus anti.virus	X	98.21%	95.59%	94.35%	96.05%	83.92%	93.02%

(Please refer to text for full product names.)

Reactive And Proactive (RAP) tests contd.	VB100	Reactive			Reactive Average	Proactive Week +1	Overall Average
		Week -3	Week -2	Week -1			
Iolo System Shield		68.75%	58.19%	60.69%	62.55%	61.01%	62.16%
K7 Total Security		87.23%	80.46%	80.81%	82.83%	79.93%	82.11%
Kaspersky Endpoint Security		96.91%	94.10%	95.20%	95.40%	86.06%	93.07%
Kingsoft Antivirus 2013		98.32%	95.65%	96.61%	96.86%	87.88%	94.62%
Lavasoft Ad-Aware Pro Security		98.11%	95.57%	94.93%	96.20%	82.96%	92.89%
Microsoft Security Essentials		93.56%	91.54%	88.63%	91.24%	82.20%	88.98%
MSecure MalwareSecure	X	98.11%	95.54%	94.25%	95.97%	83.85%	92.94%
Norman Security Suite	X	96.88%	94.46%	90.42%	93.92%	78.04%	89.95%
Optenet Security Pack		97.54%	94.60%	96.33%	96.16%	88.54%	94.25%
Panda Cloud Antivirus FREE		N/T	N/T	N/T	N/T	N/T	N/T
PC Pitstop PC Matic		97.18%	94.16%	93.15%	94.83%	81.76%	91.56%
Qihoo 360 Antivirus		98.06%	95.05%	96.87%	96.66%	89.34%	94.83%
Quick Heal Total Security 2013		78.48%	76.97%	71.32%	75.59%	73.53%	75.08%
Sophos Endpoint Security and Control		88.31%	83.44%	85.52%	85.76%	79.26%	84.13%
Tencent PC Manager		98.34%	95.68%	96.65%	96.89%	87.92%	94.65%
ThreatTrack VIPRE Antivirus 2013		98.11%	95.54%	93.08%	95.57%	82.10%	92.20%
Total Defense for Business		97.54%	94.60%	96.28%	96.14%	88.51%	94.23%
Total Defense Internet Security Suite	X	N/T	N/T	N/T	N/T	N/T	N/T
TrustPort Antivirus 2013		98.45%	95.90%	97.38%	97.25%	89.21%	95.24%
UnThreat AntiVirus Free Edition		97.76%	95.34%	95.48%	96.19%	77.37%	91.49%

(Please refer to text for full product names.)

seemed to complete fairly quickly, but there was clearly much still going on in the background, with a message appearing several minutes later indicating it was finally done and requesting a reboot. Updates took quite a long time, and required another reboot, and on some occasions further updating went on after this. On a couple of occasions the installer crashed out with a less than helpful error message, but each time it ran without problems on the second attempt.

Once everything was set up, we found the new interface working rather well, looking bright and cheery, generally responding at reasonable speeds but occasionally lagging a little. Settings are basic but fairly simple to operate, and logging was good on demand, but a little baffling on access, with data often seeming to be entirely absent.

Scanning speeds were a little slow in some areas, but not bad at all in others, with lag times fairly high initially but dropping considerably in the warm runs. Resource use was a little above average, but thanks to the optimization our set of tasks completed very quickly. Detection was impressive, dropping off a fair bit in the proactive part of the RAP sets but solid elsewhere. There were no problems in the clean sets, but in the extended WildList set a couple of items were missed, rather surprisingly. On consultation with the vendor it was eventually spotted that a version of the scan service that was in use for only a brief period – which just coincided with the test – contained a small bug affecting a small number of detection identities, and it was this that caused the problems we observed. This bad luck denies *Norman* a VB100 award this month, putting the vendor on four passes and two fails in the last six tests; nine passes and three fails in the last two years. With a few little wobbles noted, a ‘Stable’ rating is earned.

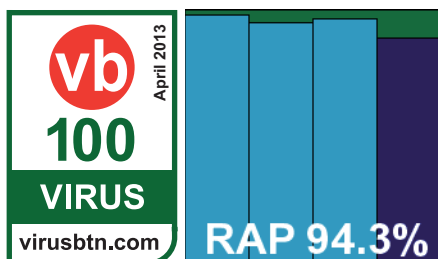
Optenet Security Pack

Main version: 10.9.82 (build 3350)

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.26%
False positives	0	Stability	Buggy

Optenet is not the most regular of participants in our tests, but generally performs decently, with its current product line



based on the *Bitdefender* engine. The submission for this month’s test was a small 26MB installer without built-in detection data, relying instead on initial updates. The set-up was a little confusing, with one dialog box appearing behind another, making us think at first that nothing was happening. After that it zipped through quite rapidly. Updates took a little while to complete though, and on one occasion seemed to get nowhere at all; after a full hour, the system was rebooted and the update process restarted, but after another two hours there was still no progress. The system was then reimaged and the product reinstalled, and left overnight, after which all seemed in order at last.

The interface has been redesigned fairly recently, with a browser-based affair prone to all the usual lags and wobbles. A preponderance of pop-ups caused some nasty issues in the on-access tests, where a fair number of samples are accessed in rapid succession; on several runs the flood of windows caused the system to grind to a crawl, with multiple error messages complaining of lack of memory, run-time errors and other ‘unexpected’ issues. Memory issues cropped up in on-demand scans too, with our RAP scan bringing the machine almost to a halt, an epic total 2GB of RAM being used by the product’s two main threads, 1.75GB for just one of them – little surprise, then, that the machine was having trouble.

These issues mostly occurred in fairly unusual circumstances (apart from the update problems), and our speed and performance measures, dealing mainly with clean samples, ran through OK. On-demand speeds were reasonable, with a small improvement in the warm runs, while on-access lag times were fairly decent too. RAM use was a little high, CPU use not bad, and our set of activities completed in pretty good time.

Detection was very strong, well up with other products based on the same engine, and with no issues in the core sets a VB100 award is duly earned. *Optenet* now has one pass and one fail in the last six tests; two passes and one fail in the last two years. There were a lot of issues here, mainly but not all occurring in stressful situations, and stability is rated as ‘Buggy’.

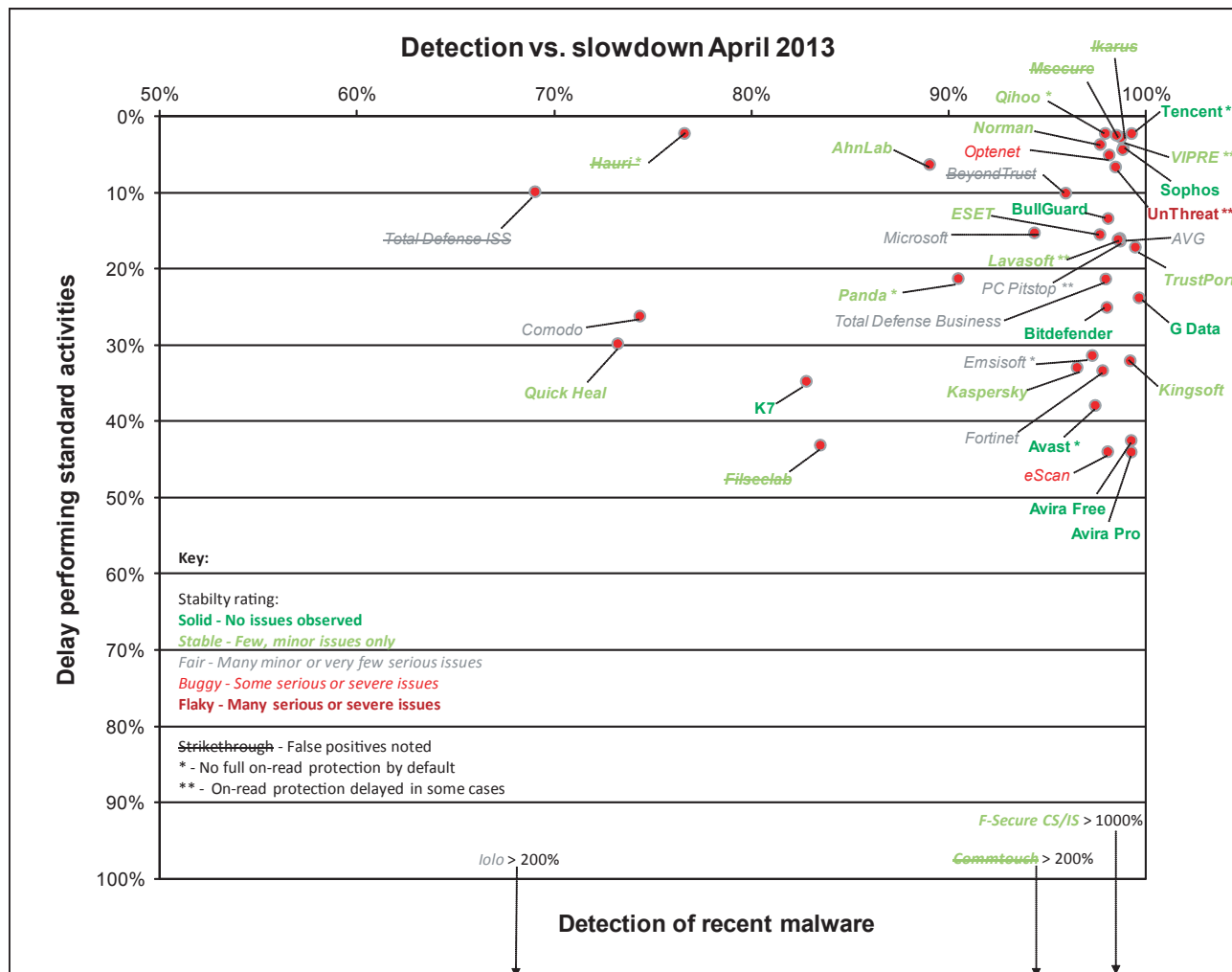
Panda Cloud Antivirus FREE

Main version: 2.1.1

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.83%
False positives	0	Stability	Stable

Panda’s free cloud-based solution has had a run of good performances since rejoining our tests in the middle of



(Please refer to text for full product names.)

last year. The set-up is performed from a tiny 800KB executable, with a few extra bits pulled down from the web in a few seconds, and the whole process is complete in under a minute. The interface is clean and simple, with little more than some basic stats and a scan button, but there is some configuration available. Stability was mostly good, but during large scans there seemed to be some occasional loss of connectivity to the cloud; on some installs, *Windows Update* appeared to have been enabled without being asked for, and on some of the jobs the system was very slow. After a reboot a message hovered over the system tray reading ‘detener antivirus’.

Things went smoothly almost all the time though, with scanning speeds pretty good – a little slow at first over



binaries and archives, but showing improvement in the warm runs. Overheads were fairly light, although not as light as one would expect given the lack of full on-read protection (only some file types seemed to be blocked on-read), while resource use was low and our set of tasks completed in pretty good time.

Detection was a little hard to measure, as standard logging is capped at a fairly low size, while the ‘advanced’ logging records a huge amount of data, but cuts out when it reaches 500MB (easily done with some of our bigger scans). Despite great care, splitting scan jobs into multiple small parts and frequently backing up logs, when the time came to process the data it still seemed to be incomplete, so averages of the available data had to be used. Scores were pretty decent in our Response sets though (bearing in mind some of the data was likely to be missing), and there was no RAP score as the product cannot operate without access

to the Internet. The WildList set caused no problems, and the clean sets were well handled too, earning *Panda* another VB100 award, its third from three appearances since rejoining our tests last year. A few fairly minor stability issues were noted this time, but a rating of ‘Stable’ is still just about earned.

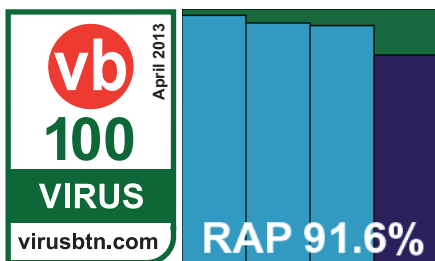
PC Pitstop PC Matic

Main version: 1.0.0.34

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.95%
False positives	0	Stability	Fair

The *PC Pitstop* products have been sent in for us to look at on a few occasions over the last year or so, but to date we have not been able to include one in



a full report – thanks in part to the way the on-access mode was implemented and in part to some trouble handling large infected sample sets. The current version, which is based on the *VIPRE* engine, promised some improvements which were expected to set things on the right lines.

The installation process is a little unusual, with a small 1.5MB package performing the initial set-up, most of which seems focused on system optimization and other rather dubious features. Once a user has logged into an account, further features become available, including the ‘Nitro’ download optimizer and ‘SuperShield’, the main anti-malware component. Installation of this portion runs in the background, with the stipulation that it could take quite some time to complete, but in most cases it seemed to be done within ten minutes or so. The real-time component seemed similar to that offered by *VIPRE* itself and other products using the same engine, with some scanning going on in the background, so that some files are rather disconcertingly granted access to at first, only to be condemned retrospectively. Oddly, though, when running the on-access component over the WildList set it took several hours to perform a job that most products handled in minutes.

There are few controls for this beyond on and off, while the on-demand component consists of a single catch-all scan function which promises all manner of checks, for a variety of things which might be suspected of slowing

a system down or rendering it vulnerable. The only way of scanning a folder for malware is to disable most of these checks and then set it to scan a specific area only – rather a fiddly task. Even after all this effort quite some time seems to be spent on other tasks, but in the end we managed to perform all the jobs we wanted to. Very few of them completed satisfactorily, with almost every scan which included a detection fading away with a variety of messages about Ajax errors and other GUI nasties. Logging was mostly OK in the background though (in the usual fussy XML format).

Speed measures were about the only tasks that did complete without errors, and showed some very slow speeds indeed, although on-access lag times were not too bad, showing some improvements in the warm runs (this will have been helped by the background scanning feature). RAM use was a little high, CPU use very low, and our set of activities completed at a good pace. Detection was as solid as we would expect, dipping very slightly in the latest day of the Response test and a little more deeply in the proactive week of the RAP test. With the WildList properly handled and the clean sets producing no surprises, *PC Pitstop* earns a VB100 award on its first full appearance. Stability was a little suspect though, with a number of GUI errors not all of which seemed to be caused by handling unusual amounts of malware, thus meriting a stability rating well into the ‘Fair’ category.

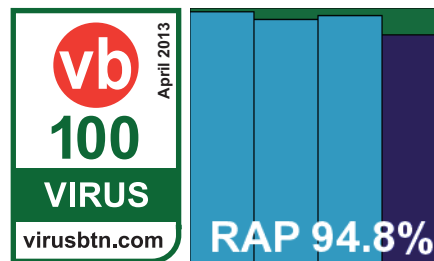
Qihoo 360 Antivirus

Main version: 4.0.0.4030

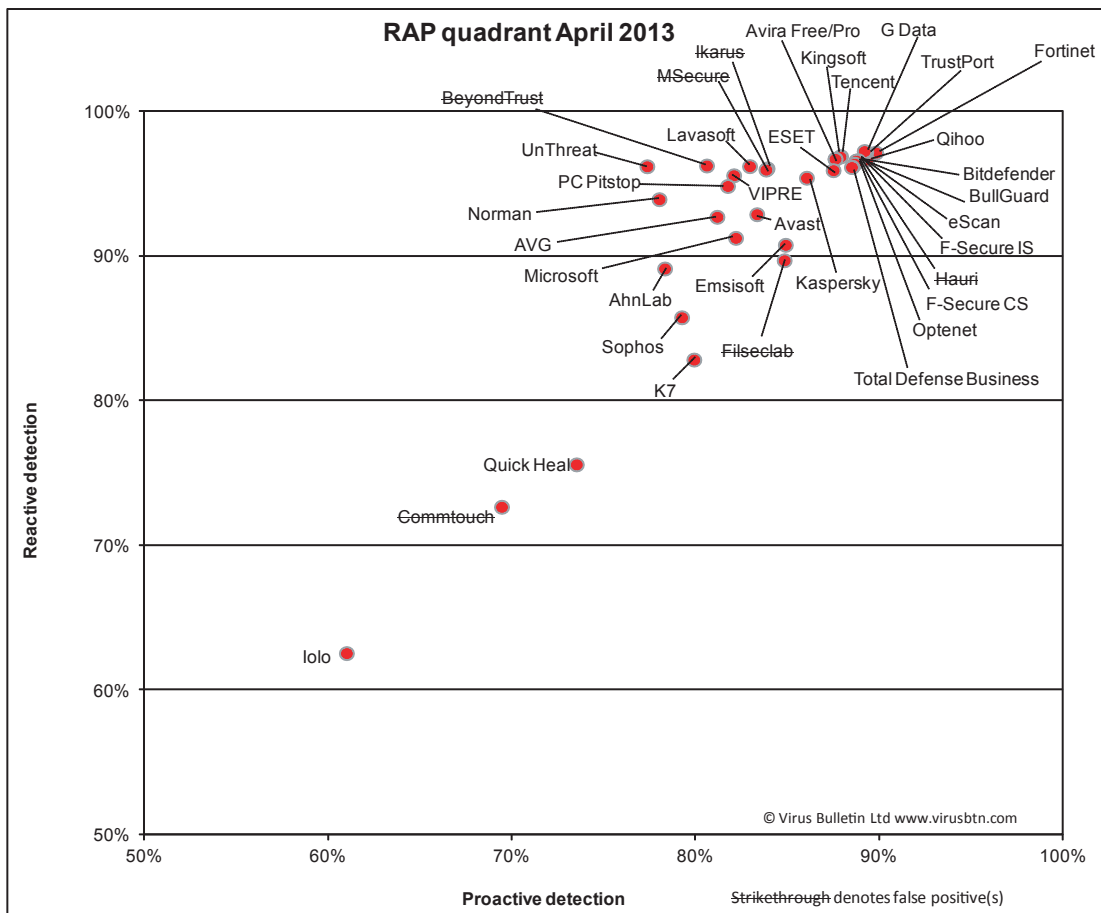
Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Stable

Qihoo’s 360 is another product with an unusual approach to ‘real-time’ protection – in past tests allowing malicious samples to



be copied and pasted, but somewhat later announcing that they had been found to be suspect and access blocked, although the files had been written. This time an installer of 157MB needed minimal interaction and finished rapidly; updates added a little less than a minute on average. The product interface is another to have had a *Windows 8*-style



(Please refer to text for full product names.)

tilted facelift, but the controls underneath are little changed, providing a reasonable level of fine-tuning. Logging is thorough and reliable.

Scanning speeds were slow in the archive sets but pretty zippy elsewhere, with very light overheads on access (thanks to not actually checking anything in real time), with correspondingly low resource use and impact on our set of tasks. Detection was splendid, in line with others based on the same *Bitdefender* engine, with only the slightest decline in the most recent parts of the sets; nothing was missed in the WildList, and with no issues in the clean sets a VB100 award is well deserved. *Qihoo* now has four passes from four entries in the last six tests; five passes and two fails in the last two years. Only a couple of very slight wobbles were noted, earning a 'Stable' rating.

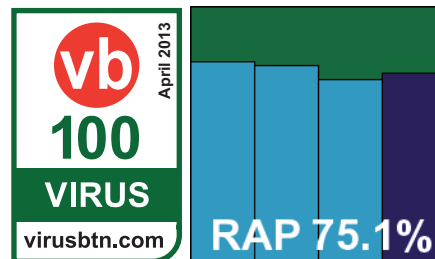
Quick Heal Total Security 2013

Main version: 14.00 (7.0.0.4)

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Stable

Another of our most regular participants, *Quick Heal's* current solution was provided as a 285MB installer, which required little



work and completed in under half a minute. Updating added a couple of minutes to the total set-up time. The interface is smooth and attractive, with a few odd quirks but a thorough level of configuration is available, once the layout has been mastered. Stability was good, with only a single small stumble in the RAP sets.

Speeds were zippy in most cases, only slowing down in the archive sets, although default settings are rather light.

On-access overheads were pretty light, as was CPU use, although RAM use was a little high; the time taken to complete our set of tasks was pretty much spot on the average for this month.

Detection was rather mediocre, declining slowly through the Response sets, remaining fairly steady through the RAP sets but lagging behind the top performers throughout. The core sets were well managed though, and a VB100 award is earned, putting *Quick Heal* on four passes and one fail from five attempts in the last six tests; seven passes and two fails from nine entries in the last two years. There were very few issues with stability, and the product earns a ‘Stable’ rating.

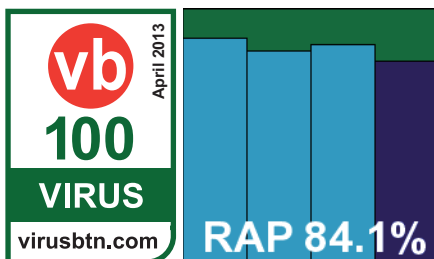
Sophos Endpoint Security and Control

Main version: 10.2.4

Update versions: 3.40.1/4.86G

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

Another of our regular entrants, *Sophos’s* product has remained little changed over the last few years. This month’s installer was a



100MB executable, with updates pretty small at 8MB. The set-up process involved unpacking to one location, then installing to another, with the whole job taking little more than a minute, initial updates adding about the same amount of time. The interface is clear and efficient, providing a wide range of controls in the main configuration areas and much more detail in an advanced dialog. Logging is comprehensive and reliable, and stability was impeccable throughout.

Scanning speeds were good to start with and blindingly fast in the warm runs. RAM use was a little above average, CPU use quite well below, and our set of activities completed in impressively short time. The certification sets were well handled and a VB100 award is easily earned, putting *Sophos* on a perfect six passes in the last six tests; ten passes and two fails in the last two years. There were no issues with stability, earning the product a ‘Solid’ rating.

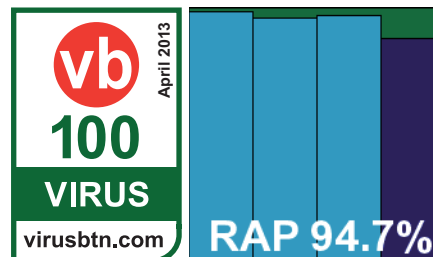
Tencent PC Manager

Main version: 7.4.24969.501

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Solid

Testing *Tencent’s* product is always a bit of a wild ride, the lack of any language options beyond the



company’s native Chinese making operation a bit of a lucky dip, even with the aid of the detailed guide provided by the developers. The installer is mid-sized at 119MB, set-up is fast and simple with only a handful of clicks required (although exactly what we are agreeing to remains something of a mystery); it completes within half a minute, with updates adding another minute or two.

The GUI looks fairly complicated, suggesting a wide range of components, with only one small area required for our needs. The limited controls we were party to were clear and simple enough. Logging seemed reliable, and scanning speeds were fast in some areas, average in others, and slow in the archive sets. Overheads were low, and once again (like others from the same region) on-read protection was absent, at least by default. Resource use seemed on the low side, and our set of tasks zipped through very rapidly, but this will have been helped by the less thorough level of analysis than is provided by most.

Detection was excellent, thanks to the underlying *Avira* engine, with a minimal number of misses, and the core sets were handled perfectly, easily earning the vendor another VB100 award. *Tencent* has an impeccable record of four passes from its first four appearances in our tests, and this month we once again saw no stability issues, earning it a ‘Solid’ rating.

ThreatTrack Security VIPRE Antivirus 2013

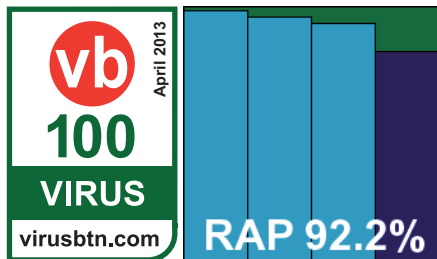
Main version: 6.1.5493

Update versions: 15502, 6.2.1.10/15900, 16018, 16194

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Stable

The team behind *VIPRE* have recently been farmed out from mother company *GFI* to form a new company called *ThreatTrack* – but the changes behind the scenes don’t seem to have had any great effect on the product itself so far. The installer is a compact 8MB, with offline updates

measuring 93MB. Installation requires an Internet connection and features a slideshow to keep the user from boredom



– however, there is little chance of that as it is over in no time, with initial updates bringing the whole process to around two minutes, with a reboot to complete. The product interface is fairly clear, sparse and simple but provides some basic controls, and seemed reasonably free from wobbles – although as usual handling large infected sets proved something of a lottery, with detection data stored in memory and scans becoming ever slower as space filled up.

Things mostly went well though, and scanning the clean sets was pretty speedy, becoming very fast indeed in the warm runs. Overheads were mostly light too, although somewhat oddly they were higher in the sets of media and documents than elsewhere, but again the warm runs showed great improvement. Resource use was below average and our set of tasks completed in excellent time. As noted elsewhere, moving some intensive tasks to the background may have contributed to this.

Detection was very good too, declining gently through the RAP sets but with a fair drop into the proactive week. The Response sets were well covered with only a slight decline in the last few days. The core sets were properly handled and a VB100 award is easily earned, putting *ThreatTrack* (formerly listed in our test history as *GFI*) on two passes and one fail from three entries in the last six tests; six passes and two fails in the last two years. Stability was pretty good this month, earning a ‘Stable’ rating.

Total Defense for Business

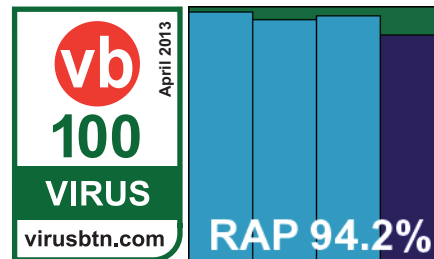
Main version: 5.0.0.313/12.163

Update versions: 5.0.1.0324/12.163, 5.0.0.0313/12.163, 5.0.0.0318/12.163

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Fair

There was something of a surprise this month, as not long after setting up the usual business solution from *Total Defense*, we started receiving urgent messages from the developers, requesting that we replace it with a cloud-oriented solution which has apparently been on the

market for several months but has not as yet appeared in our tests. Thus users of the traditional *Total Defense* business solution



(referred to as ‘r12’ or more recently ‘r14’) are urged either to replace it with this product, or to disregard the results reported here as they will not apply – this product features a third-party detection engine and has many other differences from the product we have looked at before. Set-up was rather baffling, perhaps in part thanks to rather limited initial communication from the developers, and for the first time ever, after putting well over 1,000 products through the VB100 process, we had to be led through the installation in a WebEx. Monitoring its progress, we were able to memorize the core points and repeat it later with reasonable success, although much searching through of options was required.

Both installation and configuration are run from a web console, with a local web console also available once things are installed, providing some basic controls. Navigation was clear in some areas, but much less so in others. Logging seemed very thorough, to the point of overwhelming with detail. Stability was a bit of a mixed bag, with initial attempts to run the on-access tests seeming unsuccessful, and only around half of our WildList samples were blocked, but running updates several times and rebooting the system to ensure they were fully in place seemed to make all the difference, with detection improving dramatically on the third and final attempt. The same effect seemed to repeat on each run, implying that full protection takes quite some time to come into play after updates. On one occasion the product seemed unable to load up at all, with a rather unhelpful message simply reading ‘module error’ in the product’s status box; this was easily fixed by using the ‘reinstall product’ feature – the very fact that this button is provided, as part of a GUI with very few controls indeed, suggests that this might be something that is needed on a regular basis.

The shortage of controls extended to basic scanning options, with the only choice being between a quick scan and a full scan, the latter covering all locally attached drives. Thus, our on-demand speed tests could not be performed, and all other on-demand tests had to be done by copying sets to the C: partition with the product disabled, unmounting all other partitions and then running the full scan – a rather unwieldy and time-consuming approach but one that seemed to work out OK. On-access overheads were measurable at least, and showed some reasonable times – a little heavy in the sets of

binaries and media files, but pretty light elsewhere. RAM use was pretty high, probably mostly thanks to the need for a browser to be running in order to access the product GUI, but CPU use was barely perceptible; our set of activities took a little while to get through, but not excessively long.

Detection rates were stellar though, thanks to the wise choice of third-party engine, putting the product well up amongst the leading cluster in our RAP chart and showing some pretty impressive scores in the Response tests too. The WildList and clean sets were properly dealt with, and *Total Defense* earns a VB100 award for its cloud-centric solution. This is the first VB100 for this particular product but in our history it will follow on from previous business offerings from the vendor, which now show four passes from four entries in the last year; eight passes and a single fail in the last two years. A few oddities were noted, some of which were fairly serious as they affected protection, resulting in only a 'Fair' rating for stability.

Total Defense Internet Security Suite

Main version: 8.0.0.215

Update versions: 6196.0.0.0, 6227.0.0.0, 6233.0.0.0, 6246.0.0.0

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	7	Stability	Fair

The second product from *Total Defense* this month is the company's rather more familiar consumer solution, based on its own detection technology. The set-up is run from a 172MB package, which runs through quickly and requires a reboot. Online updates ensue, lasting a couple more minutes, and then a second reboot is requested, followed in some cases by further update activity. On one install, applying the licence key supplied by the developers brought up a message insisting that the licence had expired, and that we should urgently renew it as the product (as yet unused) had already 'purged' three threats from the system – these appeared to be cookies dropped by the *MSN* website visited when we fired up *Internet Explorer* to check connectivity when first setting up the test machines. Both before and after this, however, the same licence key worked fine and seemed to have ample time remaining, so we were able to avoid spending a further \$69.99.

The product GUI suffers somewhat from style over substance, looking very glitzy and funky but often being a little tricky to operate and navigate, with some very confusing labels in places. A basic level of control is available though, after some exploration. Logging was mostly decent, but on a couple of runs it failed to produce any logging at all; fortunately it was a fairly zippy process

to re-run the scans and details were recorded. Some other scans in the Response sets froze up entirely and could not be completed, meaning some data had to be extrapolated by averaging results from other runs.

Detection rates in the Response sets were uneven and generally mediocre; as the developers insisted the product relies largely on the cloud, it was omitted from the RAP test, but an unofficial run over part of this showed that detection was indeed worse without web access. The WildList sets were properly handled, but in the clean sets a handful of false alarms were recorded, including parts of packages from *Adobe*, *Roxio* and *Vuze*. This was enough to deny *Total Defense* a VB100 award for its consumer suite this month, putting it on one pass and two fails from three entries in the last six tests; three passes and three fails in the last two years. A number of stability issues were observed, most of which were fairly minor, but there were enough of them for stability to be rated only as 'Fair'.

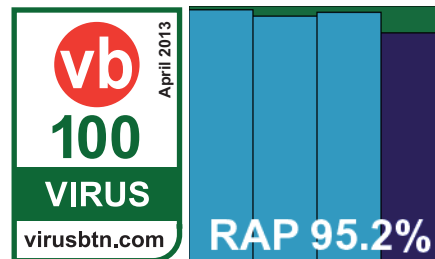
TrustPort Antivirus 2013

Main version: 13.0.9.5102

Update versions: NA

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives	0	Stability	Stable

Yet another product including the *Bitdefender* engine, this time in parallel with that of *AVG*, *TrustPort's* dual-engine



approach makes it routinely a high performer in our detection tests. The product is provided as a 240MB installer, which runs through the usual steps to complete within a minute or so; initial updates are not the fastest, adding a few more minutes to this process. The product interface is a little unusual, with some fairly basic buttons covering the main functions and everything else accessed via a couple of drop-down menus. Once it has been ferreted out, the 'advanced' configuration dialog provides ample fine-tuning options. Logging is a little unreliable, with a fixed size cap on the main records which seems not to change when the option for setting the cap is adjusted – dumping data which the user had every right to expect to see retained. Scan logs are also recorded in separate XML files though.

Scanning speeds were a little on the slow side, and overheads were a little high, especially with the scan depth

options turned to high, but speeds increased considerably in the warm runs. Resource use was a little high too, but our set of tasks got through in reasonable time. Detection was excellent, as one would expect, with superb scores in both the RAP and Response tests, and there were no problems in the core certification sets, thus earning *TrustPort* a VB100 award. The vendor now has four passes and a single fail in the last six tests, skipping only our annual *Linux* comparative; seven passes and two fails in the last two years. There were a few fairly minor issues noted, and the product earns a ‘Stable’ rating.

UnThreat AntiVirus Free Edition

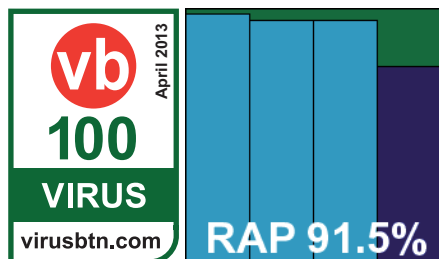
Main version: 6.1.36.15526/15526

Update versions: 6.1.36.15898/15898,

6.1.36.16018/16018, 6.1.36.16192/16192

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.95%
False positives	0	Stability	Flaky

UnThreat is another product that uses the *VIPRE* detection engine, and has given us a few headaches in the past. The current version



came as a small 11MB installer, which runs simply and rapidly, with updates a little slower, fetching down close to 100MB of data in the initial run, with a reboot needed afterwards. The product GUI is clear and simple, following usual standards and not trying to be too clever, and provides a decent level of control. Logging was mostly in a rather inefficient and repetitive XML format, but it was fairly simple to process thanks to a generic tool provided long ago by the engine developers. As in others using the same engine, logging is not written to disk until a scan completes, and in this case only the last log is kept.

Completing scanning proved far from simple, once again. Many, many scans died, froze, locked up the entire machine, or otherwise came to an end unsatisfactorily. Although we had several issues in the RAP sets, the scanning of malware samples seemed largely unaffected, with the Response tests mostly running through smoothly. The main problem seemed to be with some archive files, mostly JAR files, which could easily send the product into a bewildered and unusable state. Several attempts to get through sections of our clean sets were left running over weekends only

to sit stuck near the start for days on end, and generally a reboot was needed to clear things up. On one occasion (while scanning a batch of simple bitmap images inside Zip archives) we managed to kill a frozen task using the Task Manager, but found the system entirely unusable, with both the start button and *Windows Explorer* refusing to respond. Most of the clean sets and several parts of the speed sets had to be picked apart carefully to remove the files which seemed to cause upset, but in many cases we observed that there only seemed to be an issue with the files in specific locations: samples which were definitely causing crashes when scanned as part of the main sets were handled fine when moved to a different spot and scanned separately there. In the end we handed as much information as possible to the developers, gathered as much data as we could for ourselves, and made the best of a bad job.

With sets perhaps slightly depleted to allow us to get through them, scanning speeds proved pretty reasonable: slow to start with but speeding up a little in the warm runs. Overheads on access were a little heavy, again much better in the warm runs, and resource use was low, with a good time taken to complete our set of tasks. Detection was solid, with good scores throughout, and the WildList sets presented no difficulties. What was tricky was nursing the product through the clean sets, which took several times longer than most other products and required constant hands-on attention, but in the end we satisfied ourselves that all files had been examined with no false alarms reported, so a VB100 award is just about earned. With a fairly limited test history, *UnThreat* has one pass from a single entry in the last six tests; two from two in the last two years. Stability was a major worry this month though, with a number of issues mostly related to scans failing, some of which caused some nasty side effects on the test machines; a ‘Flaky’ rating is deserved.

UNTESTED PRODUCTS

Once again, a number of products were submitted for testing but quickly shelved after serious problems were noted. *AVWare’s Bluepex*, *ESTsoft’s ALYac* and sister product *Roboscan*, *SmartCOP* and *Inca NProtect* were all found to be insufficiently reliable for us to spend our valuable time shepherding them through the test suite, and were removed from the pile of products to test at an early stage. We will of course provide as much detail on the issues noted with these products (and with those that made the final report) to their developers for further investigation.

CONCLUSIONS

All in all, it was a bit of a mixed bag this month. As we had feared going into the test, there does appear to be a

trend among vendors towards decreasing support for the XP platform – with a lot of products extensively redesigned for *Windows 8*. In some cases it seems that only minimal effort has gone into ensuring full backwards compatibility, with a large number of problems noted – both minor issues with interfaces not displaying very well or proving difficult to operate, and more serious ones with detection and protection not running very dependably. This provided much meat for our stability rating scheme, with only a handful of products earning the top rating of ‘Solid’, quite a few in the mediocre ‘Fair’ category and some faring even worse. On the plus side, the pass ratio in the certification component was fairly high, which suggests that the bulk of the problems we noted were cosmetic and that, for the most part, protection was reasonably well provided.

Those which were denied certification were hit largely by false positives, as usual, with a handful having problems with the WildList, either through lack of access to the contents of the list, simple coding errors, or, in a few cases, erroneous whitelisting of malware known to be a significant threat. Of course, these accidents will happen, and it is an important part of the VB100 process to call them out when they do – for whatever reason a product fails to reach the certification requirements, failure should be considered an indication of some lack of complete care and caution on the part of the company behind the product, and while we would not advise putting too much stress on a single fail (or indeed a single pass), a consistent pattern of failing should be considered a strong indicator of underlying problems, just as consistent passing should demonstrate reliable and enduring ‘quality’ in every sense of the word.

The new scatter chart introduced in this month’s report will, we hope, provide a simple, at-a-glance impression of how all products are faring in terms of both detection and performance.

Next time, we will have an all-new platform in the shape of *Windows 2012 Server*, and hopefully a new set of test hardware to work with as well. This will give us an excuse for an overhaul of our speed and performance processes and sample sets, and will also free up the old hardware to set to work on new and improved tests in other areas. As always, we welcome any comments, suggestions or criticisms, and of course new products (email john.hawes@virusbtn.com).

Technical details:

Test environment: All products were tested on identical machines with *AMD Phenom II X2 550* processors, 4GB RAM, dual 80GB and 1TB hard drives, running *Microsoft Windows XP Professional, SP3*. For the full testing methodology see <http://www.virusbtn.com/vb100/about/methodology.xml>.

VIRUS BULLETIN

Editor: Helen Martin

Technical Editor: Dr Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Perl Developer: Tom Gracey

Consulting Editors:

Nick FitzGerald, *AVG, NZ*

Ian Whalley, *Google, USA*

Dr Richard Ford, *Florida Institute of Technology, USA*

SUBSCRIPTION RATES

Subscription price for Virus Bulletin magazine (including comparative reviews) for 1 year (12 issues):

- Single user: \$175
- Corporate (turnover < \$10 million): \$500
- Corporate (turnover < \$100 million): \$1,000
- Corporate (turnover > \$100 million): \$2,000
- *Bona fide* charities and educational institutions: \$175
- Public libraries and government organizations: \$500

Corporate rates include a licence for intranet publication.

Subscription price for Virus Bulletin comparative reviews only for 1 year (6 VBSpam and 6 VB100 reviews):

- Comparative subscription: \$100

See <http://www.virusbtn.com/virusbulletin/subscriptions/> for subscription terms and conditions.

Editorial enquiries, subscription enquiries, orders and payments:

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

Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com Web: <http://www.virusbtn.com/>

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated below.

VIRUS BULLETIN © 2013 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England. Tel: +44 (0)1235 555139. /2013/\$0.00+2.50. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.