DECEMBER 2011

virus BULLETIN

Fighting malware and spam

# VB100 COMPARATIVE REVIEW ON WINDOWS 7 PROFESSIONAL

## INTRODUCTION

This month has seen some major changes and a radical overhaul of our test methodology. While some parts remain much as before, a swathe of tweaks and adjustments have accompanied a significant shift of focus, which now sees most of our tests – including the core certification components – running with live Internet access, allowing for improved detection from ‘cloud’ look-up systems (and which, of course, also increases the chances of false positives). The changes should make our performance measures more accurate, taking into account the time taken to perform look-ups and the added effort of polling for updates. The core certification set has also been expanded to include the new Extended WildList set, which covers a wider range of malware types. The introduction of these changes was always certain to add to our hefty workload, so we hoped even more fervently than usual for good behaviour from the products taking part, knowing that any instability or flakiness could seriously upset our tight schedules.

## METHODOLOGY CHANGES

To summarize the new approach, each product is put through four test runs. One of these, the RAP test, operates just as in previous reviews, with product updates frozen on the deadline date and no access to the Internet permitted. For the other three, the product is set up and updated prior to the test run, with further updates permitted as per the product defaults as well as full access to look-up systems. On each run, detection of the WildList sample set is measured, both on demand and on access, and part of our clean sample set is scanned on demand. In order to achieve VB100 certification, the product must demonstrate full detection of the WildList set on each run, with no false positives in the clean set.

Each run also includes a ‘Response’ test – a scan of a set of recent malware samples gathered in the seven days prior to the run. The detection rates from these three runs are averaged to provide an insight into the product’s coverage of the most recent samples. Our standard suite of performance and speed measures are also performed during one or other of these runs.

During the introduction of the new Extended WildList, we decided to limit the certification requirement to on-demand detection of *Windows* malware only – ignoring the handful of *Android* samples included on recent lists – and also to permit what we would normally count as ‘suspicious’ alerts in the Extended list, as there are occasional items which some vendors choose to treat as adware or ‘potentially unwanted’ software. This initial run was hit by some teething problems, with the time-sensitive building of our daily trojans sets disrupted by a severe system failure. This meant that it was only possible to perform two runs per product, but hopefully the results are sufficiently representative to give a good idea of performance.

Full details of the new methodology can be found at http://www.virusbtn.com/vb100/about/methodology.xml.

## PLATFORM AND TEST SETS

This month’s platform was *Windows 7 Professional* 32-bit. Reviving system images from the last test on the platform (which was this time last year), few changes were required beyond some adjustments to fit in with new networking arrangements. This freed up some much-needed time to work on the test sets.

The first area dealt with was the clean sample sets. The existing clean set was tided a little to remove some older items, and split into three sections of fairly similar size and diversity of content. We continue to try to ensure that only more significant items are included, with the most minor packages left out of the set. This month saw a greater than

ISSN 1749-7027

usual expansion of the set, with the addition of a collection of CDs and DVDs provided with hardware and several batches of popular software from the leading download sites, including a selection of highly popular games. The sets used for speed measures were also completely revamped, compiled as previously from the entire contents of a handful of trusted systems – some more well-used than others – and covering the leading versions of *Windows*. The files were categorized into the same set of groups as previously.

The RAP sets were then put together with new malware samples from the weeks surrounding the deadline date of 12 October. These were classified and validated according to our standard procedures, to try to synchronize them with prevalence information and exclude unwanted sample types. The final sets averaged around 25,000 samples per week.

The same processes were used to build our daily sets of samples from the seven days prior to the test, to use for the 'Response' tests. However, with many sample sources running somewhat behind real time, and some less than regular, these sets proved rather smaller than the RAP sets and slightly less even in size. With much post-hoc filtering and sorting to ensure the best possible equivalence between days, there was still some variation, with some days barely reaching the 1,000 mark while others were closer to 20,000. We also tried to even things out in terms of sample types, and a good spread of family and threat types was achieved on most days. As in the RAP sets, greyware samples were excluded, as were true viruses where there was not enough time to replicate our own fresh samples. As mentioned earlier, we suffered a serious failure in one of our most critical systems just as the new tests were ready to come online, and with no time to delay testing we were forced to leave out one of the planned three runs this month – we hope that future tests will provide an even fairer and more accurate measure of detection rates over these most recent samples.

The WildList sets were prepared based on the latest lists available on our test set deadline of 7 October. That gave us the August 2011 lists, with the standard list containing the usual array of worms and bots, plus a single polymorphic variant of W32/Virut. In a change to past procedures, given that our sets will be exposed to possible data sharing we now plan to produce new batches of polymorphic samples for each test, to ensure that samples are being properly detected rather than simply matched by hash. This month a whole new set of Virut samples was generated from the WildList original – considerably larger than the batch used in the last round of testing. The Extended WildList also dated from August, and with ample notice by now the various labs should have had plenty of time to adjust their processes to ensure full coverage of these high-profile items. In total the two sets, including the polymorphic variants, added up to just under 5,000 samples. These were stored on the test systems in two ways: in one instance on their own for the on-access tests, and also scattered through the clean sets to ensure detection levels are not increased when encountering large batches of infections.

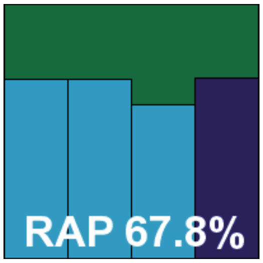
With everything in place, we were ready to make a start on a whole new type of test. With close to 60 products submitted on the test deadline, we knew we would have our work cut out fitting in four separate runs of each product. Whereas in the past we would have hoped to complete all tests for each product within a single 24-hour period, for this new style of test we allotted two full days per product, split over the four installs; this would leave our completion date perilously close to our deadlines, so any misbehaviour would have serious consequences.

## Agnitum Outpost Security Suite Pro

Main version: 7.5.1 (3791.596.1681)

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

vb Dec 2011 100 VIRUS virusbtn.com



First up on this month's roster, *Agnitum*'s product was initially provided as a 100MB installer package which included updates. This took some time to set up, with several stages covering the wide range of features included and a 'smart scan' at the end of the install. A reboot is required to complete the main set-up. Updates took an average of about half an hour from this base state when run a month or so later, but after that they seemed much faster. The interface is clean and clear with a good basic set of controls, and for the most part it operated smoothly, responding well to commands and adjustments.

The RAP tests were run first and these immediately hit a nasty snag: it was clear from the outset that some files in the set were tripping up the scanning engine quite badly. Scans moved along at normal speed at first, only to stop on a given file for a moment; the scan then zoomed to completion without registering any more detections, and no further scans could be performed, requiring forcible shutting down of the scanner service. The product's logs recorded a 'fatal error' while scanning, and all subsequent files were marked as unscannable. The same happened when trying to run on-access tests, except that access was blocked to all the subsequent files, while some other items on the system were also blocked, causing some bewildering results. It seemed almost as though the problem files were getting stuck inside the scan thread and preventing any new files from getting in there to be scanned. Eventually, after much painstaking work plodding through the sets removing each problem file as it was spotted, we managed to get what looked like a reasonably full set of results, showing some fairly respectable detection levels – which were remarkably even across the sets, apart from a slight dip in the 'week -1' set.

Moving on to the remaining test runs, these were performed with about a week in-between each, as planned, and did not suffer any of the problems encountered in the RAP sets. The clean sets were handled well, with just a couple of suspicious alerts on Themida-packed items, and the WildList sets showed flawless coverage. The new Response test showed decent detection in the earliest few days, declining a little into the most recent days. On-demand scanning speeds were pretty decent – extremely fast in the warm runs thanks to some good optimization – and the on-access overheads were also fair initially, and excellent once warmed up. Performance measures showed fairly high use of RAM and very high use of CPU cycles, with a hefty hit on our set of standard activities.

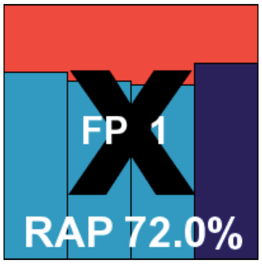
With the core certification sets properly dealt with, a VB100 award is duly earned by *Agnitum*, but the issues in the RAP sets and unexpectedly poor showing in the performance test indicate that there are some issues the developers need to address. The product has a strong past record with ten passes from ten attempts in the last two years, and only the annual *Linux* comparative not entered. With considerable extra work required to nurse it through the RAP sets, testing took around eight full days with a lot of hands-on time required – considerably longer than we hoped.

## AhnLab V3 Internet Security

Main version: 8.0.5.8 (Build 1070), Update version: SP3, Engine version: 2011.10.06.93

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 99.93% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 1 | | |

*AhnLab*'s product came as a 147MB installer including updates, and the set-up process was fairly speedy and simple, with no reboot required. Updates took an average of 25 minutes, and again no reboot was needed to apply the changes. The product is attractive and well laid out, with a decent level of controls, although these can be a little confusing in places. In general it responded well to input and applied changes consistently and accurately.



The RAP tests ran through smoothly with no issues emerging, although scores were no more than decent; the 'week +1' set showed an unexpected upturn in detection. Detection levels were respectable over the Response sets – a little lower in the most recent few days than the earlier ones, as expected. Data was a little harder to gather here, as once any online updates were run, on-demand scanning seemed to be fundamentally broken – scans of our clean and speed sets invariably crashed after only a few hundred files, and all our live tests were performed with the on-access component only. As the RAP scans had run without problems, we were forced to run the on-demand speed tests using the install set up for the RAP tests, without any further updates, after several attempts at each of the live installs failed to perform.

The results charts report on-demand scores for the WildList for simplicity, but all of these jobs, as well as the clean set scan, were performed using the on-access component. A single false positive was noted, and a handful of Extended WildList samples were also missed, so *AhnLab* does not earn VB100 certification.

The product's test history shows a rather uneven performance of late, with two passes and two fails in the last six tests. Longer term, things look a little better, with six passes and three fails from nine attempts in the last two years. The product clearly had some serious issues during the testing period, as the updates provided rendered it incapable of completing any kind of scan without crashing. The additional work this caused meant that testing took about four full days – double the time allotted.

## Auslogics Antivirus 2011

Main version: 14.0.28, Engine 7.39437

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

A new name on our lists, *Auslogics* hails from, surprise surprise, Australia, and is best known for its comprehensive range of system optimization tools. The company's *Antivirus* offering is essentially a rebrand of *BitDefender*'s 2011 product. The solution was provided as a tiny 500KB downloader file, which fetches the latest build of the main

| **Certification tests** | On demand | | On access | | Clean sets | |
|---|---|---|---|---|---|---|
| | Standard WildList | Extended WildList | Standard WildList | Extended WildList | FP | Suspicious |
| Agnitum Outpost | 100.00% | 100.00% | 100.00% | 100.00% | | 2 |
| AhnLab V3 | 100.00% | 99.93% | 100.00% | 99.93% | 1 | |
| Auslogics Antivirus | 100.00% | 100.00% | 100.00% | 100.00% | | |
| avast! Free Antivirus* | 100.00% | 99.73% | 100.00% | 99.73% | | |
| AVG Internet Security | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Avira AntiVir Free | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Avira AntiVir Pro | 100.00% | 100.00% | 100.00% | 100.00% | | |
| BitDefender Antivirus Plus | 100.00% | 100.00% | 100.00% | 100.00% | | |
| BullGuard Antivirus 10 | 100.00% | 100.00% | 100.00% | 99.93% | | |
| Central Command Vexira | 100.00% | 100.00% | 100.00% | 100.00% | 1 | |
| Clearsight Antivirus | 100.00% | 100.00% | 100.00% | 99.93% | | |
| Commtouch Command | 100.00% | 100.00% | 100.00% | 99.93% | 3 | 4 |
| Comodo Antivirus | 99.9999% | 99.87% | 99.9999% | 99.73% | 1 | |
| Comodo Internet Security | 99.9999% | 99.87% | 99.9999% | 99.73% | 1 | |
| Coranti 2012 | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Coranti Cora Antivirus | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Defenx Security Suite 2012 | 100.00% | 100.00% | 100.00% | 100.00% | | 2 |
| Digital Defender | 100.00% | 100.00% | 100.00% | 99.75% | | |
| eEye Blink Professional | 100.00% | 100.00% | 100.00% | 96.85% | | 2 |
| Emsisoft Anti-Malware | 99.9986% | 99.93% | 99.9960% | 87.17% | | 1 |
| eScan Internet Security | 100.00% | 100.00% | 100.00% | 100.00% | | |
| ESET NOD32 Antivirus | 100.00% | 100.00% | 100.00% | 100.00% | | 8 |
| ESTsoft ALYac | 100.00% | 100.00% | 100.00% | 100.00% | | 23 |
| Filseclab Twister | 99.98% | 98.99% | 99.98% | 98.61% | 33 | 10 |
| Fortinet FortiClient | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Frisk F-PROT | 100.00% | 100.00% | 100.00% | 99.60% | | |
| F-Secure Client Security | 100.00% | 100.00% | 100.00% | 100.00% | | 1 |

* Achieved full WildList detection in one of three tries.

† Achieved full WildList detection in two of three tries.

‡ Number of unique samples – alert total considerably higher.

(*Please refer to text for full product names.*)

| Certification tests contd. | On demand | | On access | | Clean sets | |
|---|---|---|---|---|---|---|
| | Standard WildList | Extended WildList | Standard WildList | Extended WildList | FP | Suspicious |
| G Data AntiVirus 2012 | 100.00% | 100.00% | 100.00% | 100.00% | | |
| GFI VIPRE Antivirus | 100.00% | 100.00% | 100.00% | 99.93% | 1 | |
| Ikarus virus.utilities | 99.999% | 99.93% | 99.999% | 99.93% | | |
| Iolo System Shield | 99.80% | 96.67% | 100.00% | 99.87% | | |
| K7 Total Security | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Kaspersky Endpoint Security 8 | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Kaspersky Internet Security 2012 | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Lavasoft Ad-Aware Total Security | 100.00% | 100.00% | 100.00% | 100.00% | | |
| McAfee VirusScan Enterprise | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Microsoft Security Essentials | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Nifty Security 24 | 100.00% | 100.00% | 100.00% | 100.00% | | 3 |
| Norman Security Suite | 100.00% | 100.00% | 100.00% | 100.00% | | |
| PC Tools Internet Security | 100.00% | 100.00% | 100.00% | 100.00% | | |
| PC Tools Spyware Doctor | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Preventon Antivirus | 100.00% | 100.00% | 100.00% | 99.93% | | |
| Qihoo 360 SD | 99.40% | 98.97% | 99.67% | 92.71% | | 1 |
| Quick Heal Total Security 2012 | 100.00% | 99.73% | 100.00% | 99.73% | 4 | |
| Returnil System Safe 2011 | 100.00% | 100.00% | 100.00% | 99.60% | | 2 |
| Sophos Endpoint Security and Control[†] | 100.00% | 99.96% | 100.00% | 99.96% | 1 | |
| SPAMfighter VIRUSfighter PRO | 100.00% | 100.00% | 100.00% | 99.93% | | |
| Symantec Norton Internet Security | 100.00% | 99.93% | 100.00% | 99.93% | | |
| Total Defense Inc ISS Plus | 99.9999% | 100.00% | 99.9999% | 100.00% | 5 | |
| Total Defense Inc Total Defense r12 | 99.9999% | 100.00% | 99.9999% | 100.00% | | |
| TrustPort Antivirus 2012 | 100.00% | 100.00% | 100.00% | 100.00% | | |
| UtilTool Antivirus | 100.00% | 100.00% | 99.60% | 99.13% | | |
| VirusBuster Professional | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Webroot SecureAnywhere | 81.07% | 79.01% | 66.87% | 47.17% | 2787[‡] | |

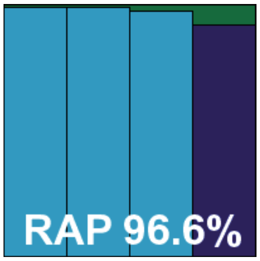
[*] Achieved full WildList detection in one of three tries.

[†] Achieved full WildList detection in two of three tries.

[‡] Number of unique samples – alert total considerably higher.

(*Please refer to text for full product names.*)

vb 100 VIRUS virusbtn.com Dec 2011



product. Given the distance to the company's headquarters, it was perhaps only to be expected that this took some time – well over an hour in each case – but it is to be hoped that customers in the company's home market will have a better experience. The set-up process was familiar to us thanks to previous exposure to very similar products, and was fairly simple and speedy once the download was finally complete. Updates are rapid and reliable, the whole process taking less than five minutes. The interface is angular and businesslike but not unattractive, and for the most part it seemed admirably well designed and responsive, with a splendid range of controls provided.

The RAP tests brought up an old issue: storing log data in memory rather than writing it to disk. This meant that an initial attempt at scanning the sets trundled along for over 48 hours, memory usage steadily climbing until, just as it neared the end, it crashed out, leaving nothing to show for all its hard work. The tests were re-run in smaller sections, taking another two days to complete, but finally producing some usable data.

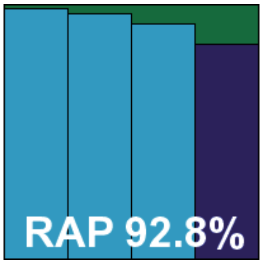
Speed and performance tests were considerably easier to run, with decent scanning speeds becoming super-fast on warm runs, and on-access overheads fairly light. Resource usage was low, particularly for memory, and impact on our set of tasks was not heavy either. The Response tests were run cautiously in small chunks, and again took some time to get through, but showed some stellar detection rates, very close to perfect across the board. The clean sets and WildLists were much more easily handled, and again showed a perfect score, with no misses in the WildList or false alarms in the clean sets. VB100 certification is comfortably earned by *Auslogics* on its first attempt.

The only problems encountered were in handling extremely large sets of infected samples, and are thus unlikely to impact real-world users; nevertheless, testing was made rather difficult, and took close to ten full days of precious lab time to complete.

### Avast Software avast! Free Antivirus

Main version: 6.0.1289

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 99.73% | **ItW Extd (o/a)** | 99.73% |
| **False positives** | 0 | | |



*Avast*'s free edition was provided as a 69MB installer, which ran through its business rapidly and without undue fuss, other than the offer to install *Google*'s *Chrome* browser. Updating proved a little problematic at first, the progress bar simply sitting still interminably, but after a reboot (which was not requested at the end of the initial install process), things seemed to run much more smoothly, updates completing within a couple of minutes. The interface is extremely easy on the eye and well designed, with a comprehensive set of controls laid out within easy reach. The only issue we had was with logging, which seems to be disabled by default in most areas and can be prone to accepting incorrect syntax and thus failing to record things where they might be expected.

Scanning speeds were around average, but on-access lag times were barely noticeable, thanks to most file types not being scanned on-read by default. Our set of activities should give a more accurate picture of system impact, and here the slowdown was on the low side of average, with low use of RAM but slightly above average use of CPU cycles when busy.

Scores were very good in the RAP and Response sets, the proactive week of the RAP sets showing a slight decline but the Response sets thoroughly covered throughout. The core certification sets showed no false positives and full coverage of the WildList sets in the first run, but in the subsequent runs detection appeared to have been removed for a handful of items in the Extended list. This was enough to deny *Avast* a VB100 award this month, despite an otherwise impressive showing.

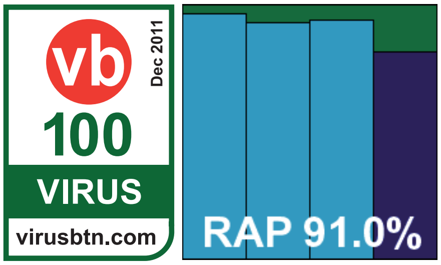
VB100 test history shows that this is the first time since the end of 2008 that *Avast* has missed out on an award. Other than the handful of misses there were no issues with stability or other complaints, and all tests were completed in excellent time, taking less than half the allotted 48 hours to complete.

### AVG Internet Security Business Edition 2012

Main version: 2012.0.1831

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

As usual, *AVG* opted to submit its corporate version, rather than the highly popular free edition. This was provided



as a 158MB installer with updates included. The installation process runs through a number of steps, including the offer of a security toolbar for browsers, and takes a little while to complete. While no reboot was needed to finalize the basic install, some updates did insist on restarting, and on some occasions an update would run for 10 minutes, demand a reboot, then spend another 10 minutes updating.

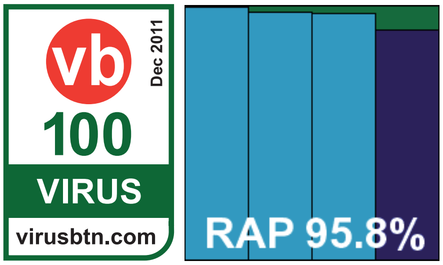
The interface is clear and well laid out, with a thorough set of configuration controls provided. Operation was smooth and stable through the tests, with good scores in the RAP sets, dropping off just a little in the proactive week. There was a solid showing in the new Response tests too, with high scores across the board, the most recent couple of days just a fraction lower than the earlier sets.

Scanning speeds started fast and the product blazed through the warm runs with some excellent optimization. The on-access measures were likewise light at first and barely noticeable thereafter. Resource use was fairly low, and impact on our set of activities not heavy either. The main sets were handled well, with perfect coverage of the WildList sets, and *AVG* earns a VB100 award with some ease. *AVG*'s test history shows five passes and one fail in the last six tests; ten passes, one fail and one no-entry in the last two years. With no problems encountered, and splendid speeds, tests completed in little over 24 hours – well within our targets.

## Avira Free AntiVirus

Main version: 12.0.0.855

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*Avira* once again submitted both its free version and its paid-for *Pro* version, with little obvious difference between them.

The installer for the free version measured just 81MB including updates. The set-up process included the offer of an 'Avira Search Toolbar', but otherwise followed the standard steps, completing rapidly. Updates also installed in good time, the full install averaging only five minutes or so over the three runs. The interface has had a bit of a makeover since the last time we saw it, looking much more glossy and appealing than in previous versions; the redesign extends to some of the controls, which are clearer and easier to use.

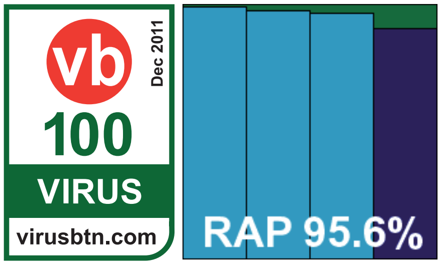
Testing ran through without issues, making splendid time. Speed measures showed good scanning speeds, light overheads, low resource use and low impact on our set of tasks. Detection rates were superb, with an excellent showing in the RAP sets, declining just a little in the proactive week, and very high levels across the response sets too. The core certification sets were handled well, and a VB100 award is comfortably earned.

*Avira*'s free edition has been entered for desktop tests only, but has a solid record with three passes from three entries in the last six tests; five passes from five attempts in the last two years. Testing ran through in less than a day with no problems to report.

## Avira Professional Security

Main version: 12.0.0.1192

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



The paid-for sibling of *Avira*'s free product was actually slightly smaller, at just 80MB, and installed even more quickly, with updates also running quickly and all installs taking less than five minutes. The interface is again considerably improved, with a better layout and much more attractive styling.

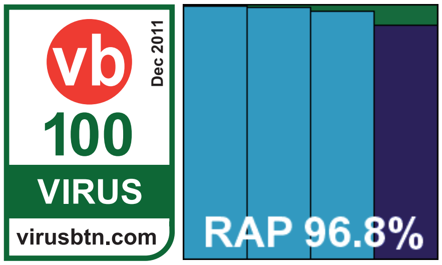
Once again, tests were problem-free, speeds good, overheads light and resource use low, while detection rates closely matched the free edition, with highly impressive levels across the board. Certification was comfortably earned with flawless coverage of the WildList sets and no issues in the clean sets.

The more complete history of *Avira*'s entries in our tests is impeccable, with 12 passes in the last two years. Again, tests completed in less than half the allotted two days, making the test team very happy.

### BitDefender Antivirus Plus 2012

Main version: 15.0.31.1283

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*BitDefender*'s entry this month gave us a first look at the new 2012 edition, complete with slick new dragon-wolf branding. The install package was a little larger than average at 228MB. Installation took only a few steps, but with download time for updates included it took an average of 15 minutes to complete. On one run, the installer simply froze and could not be made to complete, but after rebooting and restarting the process no further issues were observed.

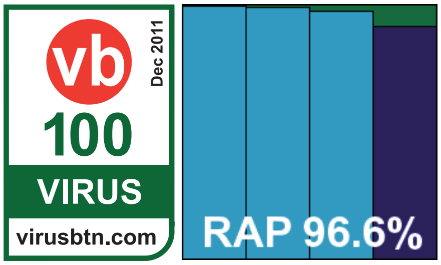
The new interface is slick and attractive, with easy-to-use controls, and under the covers the thorough set of fine-tuning options remains familiar from previous editions. The tests generally ran smoothly, although the RAP scans took rather longer than we would have liked at over 37 hours. Speed measures were decent at first and sped up hugely on the warm runs, with light lag times on access and low use of resources, our set of tasks completing in good time.

Detection rates were near perfect across the board, with even the proactive week of the RAP sets coming in with a score of more than 90%, and the Response sets were demolished with similar ease. The certification sets presented no difficulties, and a VB100 award is duly earned. The company's history shows six passes in the last six tests; ten passes, one fail and one no-entry in the last two years. Other than the long scan times over large infected sets (unlikely to affect real-world users) there were no issues, and testing took only a little over the 48 hours allotted.

### BullGuard Antivirus 10

Main version: 10.0.194

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 0 | | |



*BullGuard*'s product includes the *BitDefender* engine and routinely mirrors its results, so we hoped for great things. The 161MB installer gets going with only three clicks and runs through at good speed, with no need to reboot. With updates included, reboots were sometimes required and the total set-up time increased to close to ten minutes.

The interface is colourful and friendly, with a slightly unusual style which is fairly simple to operate after a little practice. Running the tests proved problem-free and pleasant, with the expected excellent scores in every set. Scanning speeds and overheads were not quite as impressive as those shown by *BitDefender*, and impact on our set of tasks was noticeably higher. The core sets were properly handled though, and *BullGuard* easily earns a VB100 award.

This gives the vendor five passes from five tries in the last six tests; seven from seven attempts in the last two years. With no problems noted, all tests completed in little over 24 hours.

### Central Command Vexira AntiVirus Professional 7.3

Main version: 7.3.33

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 1 | | |

Having already encountered some issues with products using the *VirusBuster* engine, we approached this one with some trepidation, tempered slightly by the knowledge that *Vexira* has a decent record of stability over the last few years. The installer was a compact 68MB, and ran through quite a few steps, but it ran quite quickly thereafter. Applying updates proved somewhat problematic, with little feedback discernable in the rather confusing interface. After clicking several buttons trying to spark an update, the logs and version information showed no changes, and in the end we simply had to leave it sitting installed overnight, to find that an update generally occurred within a few hours of installing.

Even before running any of the online tests we hit problems though, with the RAP sets once again causing severe hangs in the scanner. Even when running over sets with the known problem samples removed, hangs were frequent, and trying the task on access simply blue-screened the machine. The hangs offered no help with removing the offending samples, and in the end, after several days and multiple installs, we had to give up on the job altogether, with virtually no results to show for our labours.

Fortunately, the glut of tricky samples seemed limited to the RAP period, and the Response tests ran through more smoothly. Scores here were reasonable in the earlier days, dropping noticeably into the most recent few days. The WildList sets were handled well, as was the bulk of the clean set, but on analysing logs a single false positive was observed, denying *Central Command* a VB100 award this month.

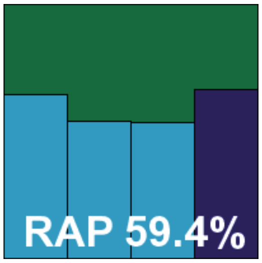
This marks the end of a solid run for the vendor, leaving it on five passes and this single fail in the last six tests; ten passes from 11 entries in the last two years. The problems encountered scanning the RAP tests and getting the product to update meant it took up one or other of our test systems for more than ten days – considerably longer than hoped.

### Clearsight Antivirus

Main version: 2.0.29

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 0 | | |

vb 100 VIRUS virusbtn.com Dec 2011



Another branch of the *VirusBuster* tree, and the first of the usual batch of products derived from the *Preventon* SDK, *Clearsight* came as a 72MB installer, which ran quickly and simply with no need to reboot. Updates were similarly zippy, and the whole set-up process took around seven minutes on each run. The interface has had a few adjustments of late, now looking a little more glossy but providing little extra by way of controls. The basic options available are generally simple to find and operate. Initial attempts at on-access testing elicited no response on several installs, but started working after a reboot.

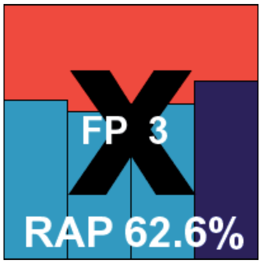
RAP testing brought the expected problems, with repeated freezes, but this time the on-access component seemed to suffer less. It took considerably longer than we would expect, but did at least manage to make it through in the end. There was some sign that protection was disabled momentarily after hitting one of the problem files in the set, but this only affected a small number of samples and hopefully the results are reasonably accurate. Scores were decent if not spectacular, with a slight upturn in the proactive set. Response tests showed reasonable scores in the earlier days too, with the expected downturn in the most recent few days. Scanning speeds were fairly average, with on-access overheads a little higher than many, and resource consumption was high on all counts, although our set of tasks ran through in decent time.

The core sets were handled well, with no repetition of the issues found in the RAP sets, and a VB100 award is safely earned. The product's test history shows five passes from five tries in the last six tests; five passes and a single fail in the last two years. Due to the issues in the RAP sets testing took a little longer than planned – around three full days – but these problems are likely to have less impact in the real world; nevertheless, we would urge the developers to improve the product's stability under pressure.

### Commtouch Command Anti-Malware 5

Main version: 5.1.15

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 3 | | |



*Command* arrived as a tiny 12MB installer, with updates in a separate 28MB bundle for use offline. The set-up process has few stages but takes a minute or two, and updates tended to run for 15 minutes or so on each fresh install. No reboot was required though.

The product GUI is plain, simple and unflashy – a little clunky looking, but generally usable. Controls are fairly minimal, but provide the basics. Scanning speeds were not especially fast, and overheads decidedly heavy. While RAM use was around average, CPU use was high and our set of tasks took quite some time to complete. Detection tests ran through without issues. The RAP scores were fairly mediocre, but again took a turn for the better in the proactive week. The Response sets were a little more encouraging, dropping slightly into the more recent few days. The WildList sets were well covered, but in the clean sets a handful of items were mislabelled as malware, all with the same heuristic description – suggesting that some overzealous rule was at fault.

This denies *Commtouch* a VB100 award this month. The vendor's recent history is a little rocky, with three fails and

| **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 |
| Agnitum Outpost | 16.52 | 15.16 | 5.79 | NA | 35.71 | 1.75 | 35.71 | 34.24 | 2.98 | 34.24 | 58.34 | 7.08 | 58.34 |
| AhnLab V3 | 22.04 | 29.65 | 29.24 | NA | 37.48 | 11.44 | 37.48 | 21.05 | 20.52 | 21.05 | 38.14 | 33.95 | 38.14 |
| Auslogics Antivirus | 12.08 | 11.98 | 8.26 | 177.70 | 35.83 | 14.80 | 42.40 | 20.00 | 6.59 | 24.63 | 29.02 | 10.77 | 50.58 |
| avast! Free Antivirus | 3.09 | 2.69 | 0.36 | 97.03 | 1.53 | 0.10 | 23.12 | 1.57 | 0.22 | 17.21 | 4.21 | 1.69 | 53.33 |
| AVG Internet Security | 5.12 | 8.91 | 3.79 | NA | 35.16 | 0.42 | 41.28 | 14.81 | 0.58 | 24.87 | 9.45 | 0.23 | 35.48 |
| Avira AntiVir Free | 32.71 | 6.40 | 3.98 | 38.02 | 15.76 | 0.45 | 17.69 | 17.77 | 10.92 | 18.50 | 30.57 | 30.25 | 41.36 |
| Avira AntiVir Pro | 31.09 | 11.40 | 8.38 | 47.82 | 30.19 | 0.64 | 29.67 | 18.65 | 11.73 | 19.60 | 31.60 | 31.52 | 43.77 |
| BitDefender Antivirus | 3.71 | 7.13 | 3.03 | NA | 27.51 | 6.38 | 27.51 | 22.13 | 6.72 | 22.13 | 29.26 | 5.04 | 29.26 |
| BullGuard Antivirus | 10.55 | 55.58 | 7.32 | 965.15 | 38.17 | 12.83 | 53.34 | 27.19 | 13.38 | 115.19 | 55.88 | 24.01 | 33.14 |
| Central Command Vexira | 27.92 | 5.45 | 1.38 | NA | 38.25 | 29.53 | 39.19 | 14.69 | 14.74 | 25.24 | 6.92 | 6.84 | 46.22 |
| Clearsight Antivirus | 22.18 | 73.26 | 24.82 | 207.50 | 39.26 | 11.86 | 39.90 | 2.29 | 1.80 | 29.78 | 6.33 | 21.39 | 63.49 |
| Commtouch Command | 37.47 | 115.26 | 122.26 | 121.83 | 42.36 | 42.56 | 42.61 | 52.21 | 52.34 | 52.39 | 66.28 | 66.52 | 66.63 |
| Comodo Antivirus | 23.63 | 8.14 | 5.74 | NA | 51.66 | 49.64 | 51.66 | 13.91 | 12.86 | 13.91 | 38.14 | 36.04 | 38.14 |
| Comodo IS | 29.72 | 3.94 | 2.19 | NA | 48.82 | 47.95 | 48.82 | 13.53 | 14.76 | 13.53 | 37.91 | 38.50 | 37.91 |
| Coranti 2012 | 1.76 | 27.14 | 5.85 | 38.14 | 63.95 | 14.23 | 61.93 | 17.22 | 10.39 | 43.16 | 9.20 | 7.57 | 63.88 |
| Coranti Cora Antivirus | 2.25 | 25.98 | 4.77 | 34.71 | 60.14 | 11.11 | 59.27 | 19.68 | 12.95 | 23.55 | 12.00 | 10.37 | 11.86 |
| Defenx Security Suite | 12.64 | 9.74 | 1.81 | 10.38 | 32.21 | 0.08 | 32.27 | 35.10 | 3.30 | 35.46 | 58.20 | 7.32 | 56.78 |
| Digital Defender | 29.80 | 73.93 | 73.89 | 163.98 | 38.28 | 38.14 | 38.55 | 1.83 | 1.76 | 28.66 | 5.91 | 5.76 | 62.61 |
| eEye Blink Pro | 65.47 | 19.30 | 19.71 | NA | 86.16 | 100.61 | 86.16 | 12.02 | 40.94 | 12.02 | 137.62 | 141.15 | 137.62 |
| Emsisoft Anti-Malware | 0.16 | 3.58 | 2.58 | NA | 9.61 | 5.91 | 9.61 | 7.45 | 6.15 | 7.45 | 7.16 | 3.76 | 7.16 |
| eScan IS | 13.88 | 8.23 | 0.33 | 19.09 | 18.12 | 2.13 | 18.68 | 10.74 | 0.79 | 11.65 | 16.91 | 2.97 | 21.74 |
| ESET NOD32 | 0.45 | 6.63 | 4.97 | NA | 20.52 | 10.44 | 21.34 | 11.71 | 7.36 | 12.38 | 15.68 | 7.64 | 19.08 |
| ESTsoft ALYac | 2.41 | 5.18 | 0.17 | NA | 39.93 | 3.33 | 39.93 | 10.56 | 0.18 | 10.56 | 30.45 | 1.53 | 30.45 |
| Filseclab Twister | 20.64 | 17.27 | 17.26 | 16.52 | 24.77 | 24.70 | 24.29 | 23.43 | 23.25 | 22.73 | 4.30 | 4.08 | 3.72 |
| Fortinet FortiClient | 43.82 | 102.07 | 0.65 | 102.07 | 77.06 | 4.03 | 77.06 | 12.56 | 0.85 | 12.56 | 72.49 | 2.88 | 72.49 |
| Frisk F-PROT | 21.36 | 15.94 | 16.11 | NA | 37.73 | 38.07 | 37.73 | 8.93 | 8.67 | 8.93 | 23.10 | 23.10 | 23.10 |
| F-Secure CS | 6.10 | 8.93 | 6.18 | NA | 68.13 | 15.76 | 68.13 | 10.50 | 5.25 | 10.50 | 19.73 | 9.93 | 19.73 |

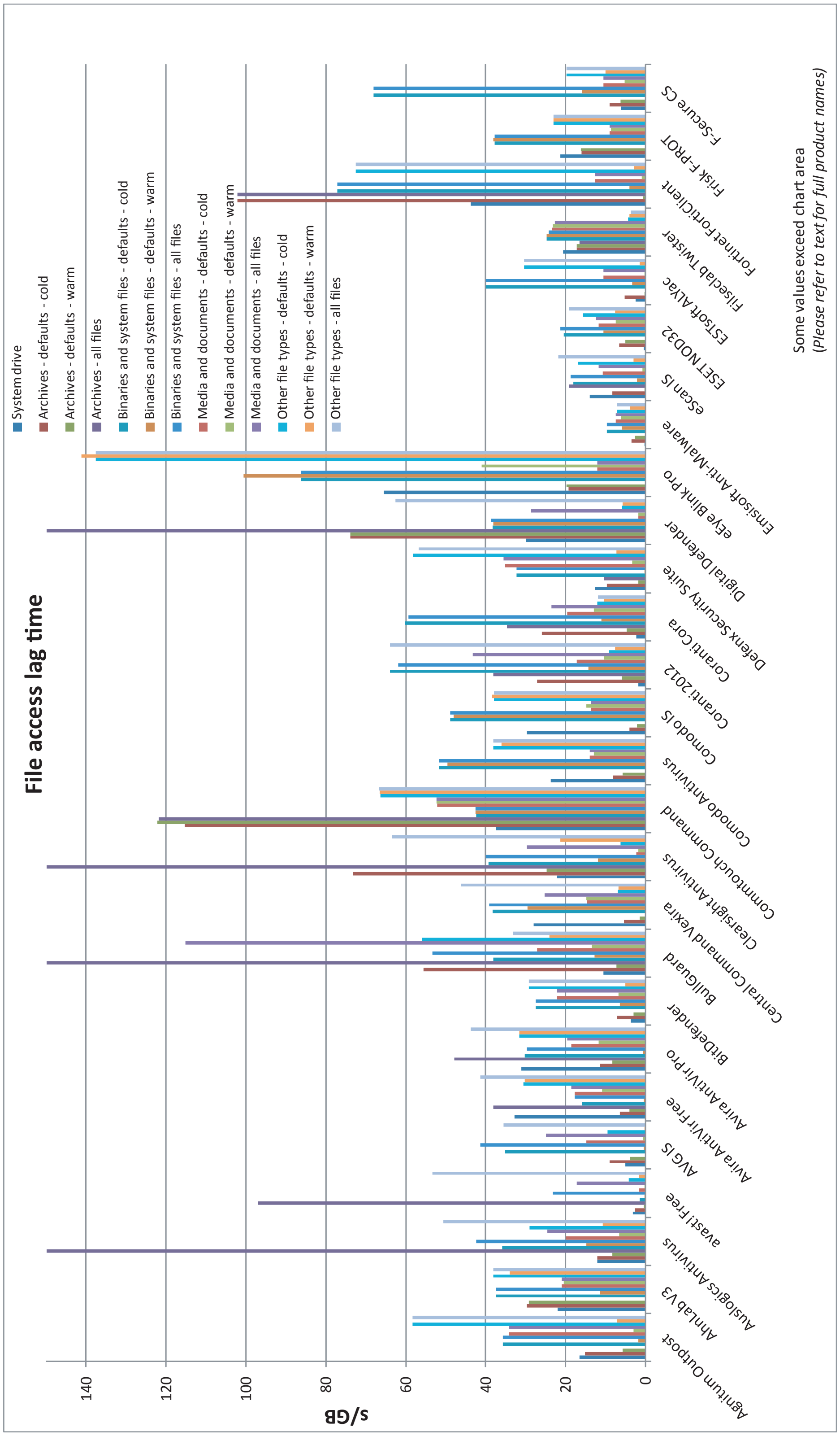
* System drive size measured before product installation.

(*Please refer to text for full product names.*)

| **File access lag time contd. (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 |
| G Data AntiVirus | 10.85 | 69.86 | 28.58 | 285.04 | 62.95 | 30.08 | 64.45 | 36.88 | 23.43 | 39.54 | 99.60 | 51.70 | 122.92 |
| GFI VIPRE Antivirus | 3.70 | 10.46 | 0.11 | NA | 50.52 | 1.09 | 50.52 | 31.00 | 2.21 | 31.00 | 7.91 | 1.84 | 7.91 |
| Ikarus virus.utilities | 29.78 | 151.52 | 151.00 | 151.52 | 48.20 | 45.21 | 48.20 | 17.30 | 16.85 | 17.30 | 41.47 | 39.33 | 41.47 |
| Iolo System Shield | 37.98 | 109.30 | 113.04 | 109.30 | 42.34 | 42.10 | 42.34 | 45.11 | 44.66 | 45.11 | 70.97 | 71.25 | 70.97 |
| K7 Total Security | 24.86 | 36.83 | 0.44 | NA | 75.75 | 3.41 | 75.75 | 18.73 | 0.36 | 18.73 | 55.42 | 3.30 | 55.42 |
| Kaspersky ES 8 | 5.98 | 6.43 | 0.05 | 129.58 | 32.49 | 3.71 | 46.10 | 10.80 | 1.05 | 17.27 | 35.97 | 4.82 | 71.17 |
| Kaspersky IS 2012 | 4.59 | 6.40 | 0.02 | 237.01 | 29.36 | 3.61 | 45.07 | 9.50 | 0.93 | 16.73 | 31.59 | 2.34 | 77.71 |
| Lavasoft Ad-Aware | 20.26 | 77.71 | 0.81 | 332.59 | 71.92 | 0.08 | 82.20 | 40.41 | 3.80 | 45.78 | 108.83 | 9.58 | 134.16 |
| McAfee VirusScan | 16.88 | 10.26 | 7.29 | 389.12 | 65.00 | 38.46 | 67.76 | 32.66 | 23.39 | 30.94 | 86.60 | 57.77 | 119.07 |
| Microsoft SE | 7.08 | 6.82 | 3.44 | NA | 52.33 | 6.56 | 52.33 | 18.53 | 7.81 | 18.53 | 34.41 | 6.07 | 34.41 |
| Nifty Security 24 | 4.53 | 11.24 | 4.08 | NA | 42.50 | 10.30 | 42.50 | 24.31 | 8.19 | 24.31 | 55.81 | 10.86 | 55.81 |
| Norman Security Suite | 75.71 | 20.12 | 19.88 | 21.26 | 98.82 | 98.05 | 276.12 | 29.78 | 29.58 | 29.72 | 134.70 | 134.35 | 153.02 |
| PC Tools IS | 11.28 | 16.78 | 4.48 | NA | 45.31 | 10.83 | NA | 27.58 | 10.28 | NA | 37.42 | 18.48 | NA |
| PC Tools SD | 9.77 | 12.48 | 0.66 | NA | 37.54 | 4.89 | NA | 23.67 | 4.58 | NA | 35.55 | 15.02 | NA |
| Preventon Antivirus | 19.84 | 80.48 | 55.44 | 215.20 | 42.86 | 28.91 | 43.40 | 2.34 | 2.11 | 28.19 | 6.29 | 4.91 | 63.44 |
| Qihoo 360 SD | 4.99 | 4.88 | 3.32 | NA | 10.10 | 9.26 | 10.10 | 6.42 | 5.45 | 6.42 | 5.16 | 1.74 | 5.16 |
| Quick Heal Total Security | 7.96 | 9.78 | 9.86 | 9.09 | 20.36 | 19.71 | 19.44 | 16.45 | 16.45 | 16.06 | 34.90 | 34.73 | 45.38 |
| Returnil System Safe | 32.98 | 45.81 | 49.59 | NA | 36.98 | 37.22 | 36.98 | 43.24 | 44.40 | 43.24 | 30.66 | 30.49 | 30.66 |
| Sophos ESC | 16.37 | 11.62 | 12.39 | 316.79 | 62.65 | 62.59 | 49.56 | 14.90 | 15.17 | 28.97 | 24.07 | 23.83 | 83.48 |
| SPAMfighter VIRUSfighter PRO | 29.95 | 77.64 | 78.29 | 107.65 | 55.20 | 55.38 | 55.57 | 3.31 | 3.31 | 29.20 | 7.92 | 7.69 | 64.49 |
| Symantec Norton Internet Security | 31.46 | 6.51 | 6.06 | NA | 24.12 | 17.20 | 24.12 | 23.79 | 23.58 | 23.79 | 51.88 | 48.93 | 51.88 |
| Total Defense ISS | 27.98 | 9.32 | 9.23 | NA | 32.02 | 30.50 | 32.02 | 12.17 | 11.97 | 12.17 | 31.52 | 27.83 | 31.52 |
| Total Defense TD r12 | 19.17 | 4.42 | 4.64 | 233.26 | 20.28 | 17.19 | 23.39 | 10.69 | 8.87 | 14.16 | 28.82 | 27.83 | 57.15 |
| TrustPort Antivirus | 14.25 | 11.30 | 0.28 | 397.50 | 52.13 | 0.02 | 55.03 | 33.63 | 2.24 | 38.50 | 99.97 | 7.92 | 154.30 |
| UtilTool Antivirus | 13.30 | 78.53 | 28.47 | 211.75 | 43.02 | 14.67 | 43.49 | 2.48 | 1.66 | 28.31 | 6.34 | 22.76 | 63.98 |
| VirusBuster Pro | 21.05 | 10.21 | 5.23 | 11.18 | 54.98 | 43.53 | 54.88 | 15.61 | 15.66 | 25.54 | 8.68 | 8.42 | 46.47 |
| Webroot SecureAnywhere | 5.23 | 0.32 | 0.42 | NA | 3.83 | 3.13 | NA | 0.55 | 0.00 | NA | 2.44 | 0.70 | NA |

* System drive size measured before product installation.

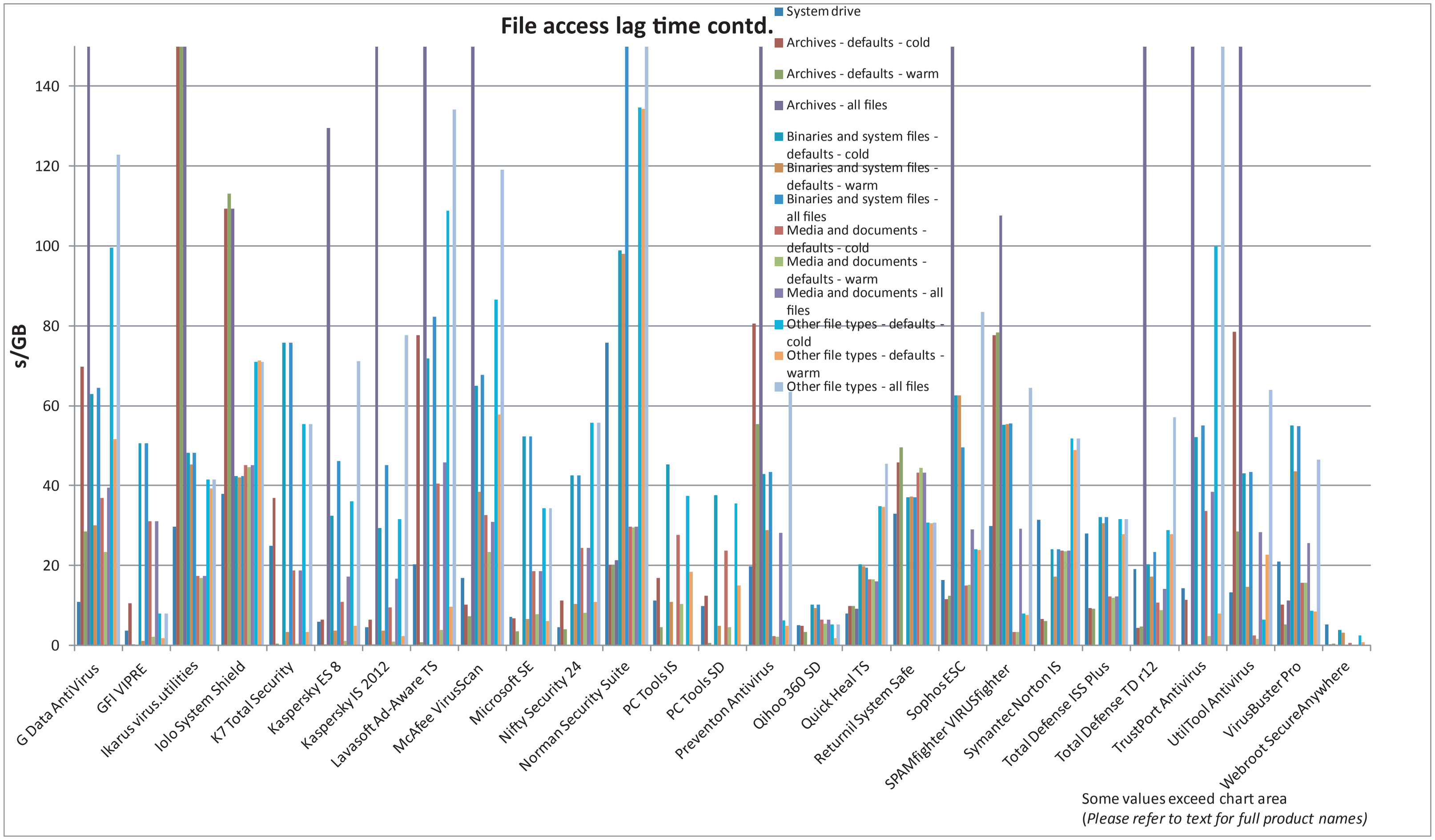
(*Please refer to text for full product names.*)



File access lag time

Some values exceed chart area

*(Please refer to text for full product names)*



File access lag time contd.

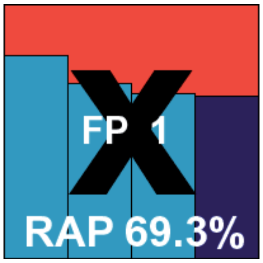
Some values exceed chart area
*(Please refer to text for full product names)*

two passes in the last six tests, the *Linux* test not entered; three passes and five fails in the last two years. Testing was not too problematic this month, but took a little longer than the scheduled two full days of system time.

## Comodo Antivirus

Main version: 5.8.211697.2124

| | | | |
|---|---|---|---|
| **ItW Std** | 99.99% | **ItW Std (o/a)** | 99.99% |
| **ItW Extd** | 99.87% | **ItW Extd (o/a)** | 99.73% |
| **False positives** | 1 | | |



*Comodo* once again submitted two products for testing, the company's full suite and its plain anti-virus offering – which, despite the name, includes a wealth of additional protective layers. The set-up from the compact 61MB installer is fairly straightforward, stepping through a fair number of stages but nothing too taxing, and completes in good time. Updating is rather more time consuming, with 85MB of data to download. This took over 20 minutes on average in our lab installs. The interface has had a few tweaks recently – it still looks good and provides good, simple controls but the range of options has been expanded somewhat to give a solid level of fine-tuning.

Running was smooth and problem-free, with none of the speed issues encountered in previous tests. Our performance tests showed both scanning speeds and overheads on the better side of average, with low RAM use, slightly high CPU use when busy, and low impact on our set of tasks. RAP scores were decent if not stellar, and detection rates in our Response sets were not bad either, dropping a little on the final day.

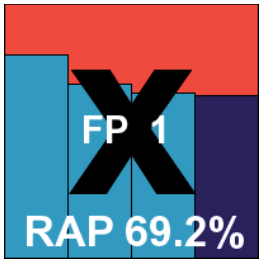
WildList coverage was decent in the standard list, although a single polymorphic sample was missed, while a handful of items in the Extended list also went undetected. Scanning of the clean sets mostly went well, but a single item was alerted on. While the threat ID in question included the word 'Suspicious' (which would normally be permitted in this set), not counting this ID type as a detection would have meant missing a far larger portion of the WildList set. No VB100 award can be granted this month, but performance was generally decent and things continue to look promising for *Comodo*.

The vendor's recent history shows five entries in the last two years for this product, with as yet no luck achieving certification. There were no stability problems during testing, and all completed within the two-day limit.

## Comodo Internet Security

Main version: 5.8.211697.2124

| | | | |
|---|---|---|---|
| **ItW Std** | 99.99% | **ItW Std (o/a)** | 99.99% |
| **ItW Extd** | 99.87% | **ItW Extd (o/a)** | 99.73% |
| **False positives** | 1 | | |



The more comprehensive version of *Comodo*'s product differs mainly in the inclusion of a firewall, and also the 'Geek Buddy' component – a remote support tool. Again the installation package is on the small side, at 61MB, has a fair few steps to run through but completes in reasonable time, with no need to update initially. Updates were again large and slow, averaging close to half an hour for the first run, with some requiring a reboot to apply. The look and feel is once again crisp and pleasant, with a good level of controls. Speeds were decent, with overheads not too oppressive, and use of resources was not too intrusive either, getting through our set of tasks in good time.

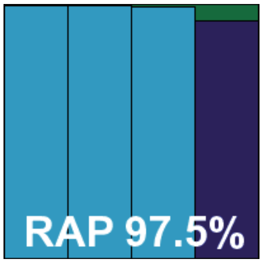
Detection rates were respectable in most areas, but again a few WildList misses and a single false positive deny *Comodo* certification. The suite product has achieved a pass before, with three fails and the one success in the last six tests; one pass and now five fails in the last two years. Stability was solid even under pressure, and with decent speeds, all testing fitted into the allotted 48-hour time slot.

## Coranti 2012

Main version: 1.005.00004

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

vb 100 VIRUS virusbtn.com Dec 2011



A double whammy from *Coranti* too this month, with this standard version accompanied by the '*Cora*' product produced by the vendor's Ukrainian branch. The installer is 45MB and takes some time to run through, only requiring the standard interactions. Updates weighed in at a hefty 246MB, covering the multiple engines included, but only required half an hour or so to complete on average. On some installs an additional 'product update' was requested after the standard update, but this generally seemed unable to complete properly. Nevertheless, things all seemed to be working fine. The interface is simple and unflashy, but is well laid out and provides a wealth of controls, all of which are generally easy to operate and responsive. Testing ran smoothly with no upsets – a little slower than the fastest this month thanks to the multi-pronged approach, but not excessively so.

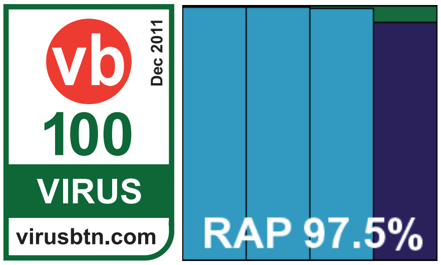
Speed tests showed some reasonable initial speeds much helped by optimization in the warm runs, and on-access lags were not too heavy. RAM use was a little high, but CPU use fairly low, and our set of tasks ran through in decent time. As expected, detection rates were superb, with excellent coverage everywhere – even where they dipped slightly, in the proactive week of the RAP sets and in the last few days of the Response sets, they remained highly impressive. The WildList sets were fully covered, and with no false alarms a VB100 award is easily earned.

The product's history shows two passes from three entries in the last six tests; four passes from seven entries in the last two years. Stability was solid, and despite slightly slower than average scan times in the infected sets, all tests completed in decent time, only slightly over-running our planned limits.

## Coranti Cora Antivirus

Main version: 2.003.00009

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



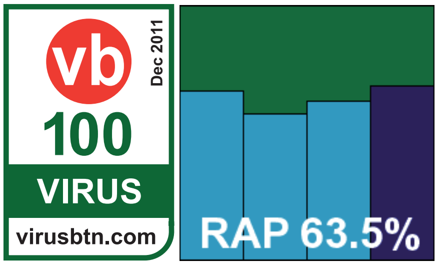
Pretty similar to its sibling, *Cora*'s 45MB installer took a little while to get set up and much longer to fetch its bulky updates, averaging around half an hour for its initial runs. The GUI is the same: wordy and busy, but not cluttered, generally simple to operate and with excellent configurability. Scanning speeds were initially a little slow but increased hugely in the warm runs, and overheads were around average, with high RAM use, average CPU drain and average impact on our suite of activities. Detection rates were once again very impressive, with solid scores everywhere, and again the core certification sets were well managed, comfortably earning *Cora* a VB100 award as well.

With two entries under its belt, *Cora* maintains a flawless record of two passes. Tests ran without issues and completed in a shade over the scheduled 48 hours.

## Defenx Security Suite 2012

Main version: 3734.575.1669

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



A sibling of *Agnitum*'s *Outpost*, *Defenx* has developed its own personality in our tests with a few noticeable differences. The set-up process from the 101MB installer is similar though, running through quite a few steps (mostly covering the firewall component), pausing for some time gathering data and running preliminary scans, and requiring a reboot to complete. Updates took an average of 20 minutes on each fresh install.

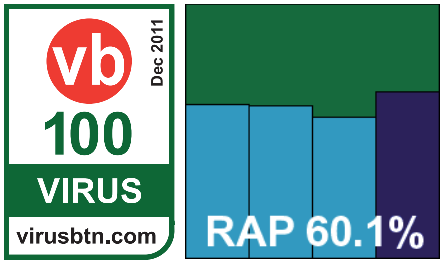
The interface also closely resembles *Agnitum*'s, providing a good basic set of controls in a pleasant and usable manner. It generally ran well, but once again some serious issues emerged in the RAP sets, with multiple samples causing it to tie itself in some pretty nasty knots. Shutting down the service seemed to free up the scanner, and we were eventually able to get through the whole set, with much painstaking work removing each file and restarting scans each time a snag was hit. These problems were not apparent in the later tests with connection to the Internet, however.

Scanning speeds were, as ever, not bad at first and very speedy in the warm runs, with fairly light overheads. RAM use was not high, but processor use was a little above average and our set of tasks took quite some time. Detection rates proved respectable, with reasonable levels in the RAP sets, and a decent showing in the Response sets, declining a little in the most recent few days. The core sets were well handled, with no issues in the WildList and just a couple of Themida-packed items alerted on as suspicious in the clean sets, and a VB100 award is duly earned. The product's history shows a solid record, with five passes from five entries in the last year; ten passes from ten entries over two years. Instability was limited to the large infected sets and thus should not have too much impact on users, but hitting one of these tricky files does cause serious problems – an issue which the developers need to address urgently. The additional work required to nurse the product through the test sets meant that testing took close to ten full days of system time.

## Digital Defender Antivirus

Main version: 3.0.2.9

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.75% |
| **False positives** | 0 | | |



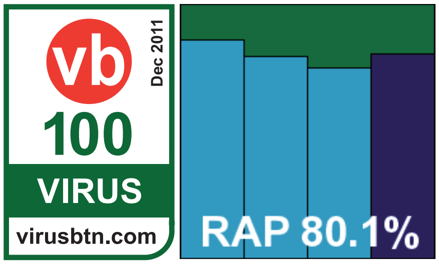
Another member of the *Preventon/ VirusBuster* range, here again we feared there would be issues in the RAP sets, and our fears were justified. After setting up fairly rapidly and simply from the 70MB installer, with no need to reboot and updates averaging less than five minutes, the new GUI seemed crisp and usable, with a basic set of controls. Most tests seemed to run OK, but in the RAP sets, and to a lesser degree the Response sets, things were rather trying, with frequent hangs and other freak-outs on demand. Resorting to on-access mode, tests moved along a little faster, but still some files snared up the scanner process, which stuck on them for a time before simply shutting down. Again much work, multiple retries and considerable frustration ensued, but tests were eventually completed, showing some reasonable but not hugely impressive scan times, fairly hefty overheads, high RAM use and only average impact on our set of tasks.

Detection rates were fairly mediocre in the RAP sets, with a slightly better showing in the Response sets, tailing off a little towards the end. The core sets were handled well though, and a VB100 award is just about earned. The last year looks good for *Digital Defender*, with five passes from five entries, but the two-year picture is less rosy: six passes from ten attempts. With the shaky and flaky scanning encountered, testing took eight full days to complete.

## eEye Digital Security Blink Professional

Main version: 4.9.4

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 96.85% |
| **False positives** | 0 | | |



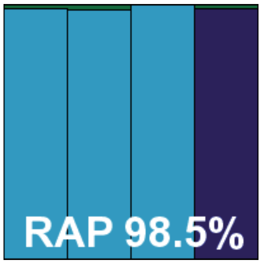
*Blink* came as a fairly hefty 199MB installer, which ran through a few steps, a fairly speedy initial set-up, then a licensing and configuration wizard. Updates took quite some time, with an initial data update, which occasionally required a reboot, followed by an update of other components. The full process regularly took more than two hours, and often it was less than clear as to whether the process had completed successfully. The interface looks good, but provides only basic controls. Testing was a long, slow process, with a number of issues: large scans repeatedly aborted only part-way through the sets, and scans of our clean sets seemed to come to a silent halt, not reaching the end of the job after several days. Speed tests were extremely slow too, and were aborted after each run took well over half an hour (most products managed all these jobs in less than five minutes each).

Eventually, we gathered what seemed to be a fairly complete set of data, showing some reasonable but unspectacular scores in the detection sets. As mentioned, scanning speeds were very slow and overheads were pretty high, although resource use and impact on our set of activities were unexceptional. The core sets were properly handled though, earning *Blink* another VB100 award. The product's history is pretty decent of late, with four passes from five tries in the last six tests. Longer term, things are slightly less impressive, with five passes and four fails in the last two years. Stability was a little shaky in a number of tests, and things moved very slowly, meaning that tests took eight full days to complete – several times the expected limit.

## Emsisoft Anti-Malware

Main version: 6.0.0.42

| | | | |
|---|---|---|---|
| **ItW Std** | 99.99% | **ItW Std (o/a)** | 99.99% |
| **ItW Extd** | 99.93% | **ItW Extd (o/a)** | 87.17% |
| **False positives** | 0 | | |



*Emsisoft*'s 99MB installer ran quickly with minimal interaction called for. Updating required 93MB of data to be drawn down, but this ran fairly speedily, completing the set-up in less than 15 minutes on average. On one of the installs, the set-up wizard crashed out, but ran successfully on a second attempt.

The interface has a few quirks, but is fairly simple to navigate, providing a limited range of controls. The tests mostly ran OK, but on-access scanning proved rather unpredictable, with the interface insisting it was on when clearly no protection was in place. After exposure to a fairly limited set of samples, protection would shut down and require a reboot to get things running again. After a few such incidents, it simply refused to come back on, and most test runs required several reinstalls to complete.

Data was gathered eventually though, with some reasonable scanning speeds, light on-access overheads (although on-read detection is off by default), low use of RAM and average CPU use; our set of tasks took quite some time to complete. Detection rates were excellent, with some stunning scores in the RAP sets – the proactive week was particularly impressive. Response sets also approached perfection, but in the certification sets a handful of polymorphic virus samples were not detected, denying *Emsisoft* certification this month.

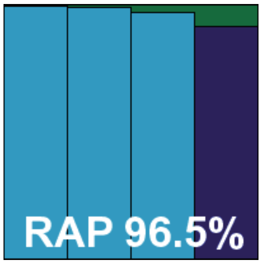
The product's history shows a pattern of five failures in the last six tests, the annual *Linux* test not entered. Over the last two years we see two passes and seven fails from nine entries. A number of stability issues were apparent during testing, and this added considerably to the time taken to complete our work, more than ten full days being required.

## eScan Internet Security for Windows

Main version: 11.0.1139.1083

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

vb 100 VIRUS virusbtn.com Dec 2011



This month's entry from *eScan* came as a fairly hefty 190MB installer, including some updates, but it ran through in reasonable time, with nothing too taxing required of the user. With an initial scan job and fetching the latest updates, installs averaged at around nine minutes.

The interface is bright and cheerful, with a funky design and reasonable usability. A good level of controls is provided – enough to satisfy the most demanding of users – and it generally responded well. Testing moved along nicely with no issues, showing fairly slow speeds in the throughput tests, light overheads on access, fairly high use of RAM, but average CPU use and impact on our set of tasks. Detection rates, as expected from seeing other products using the *BitDefender* engine included here, were extremely solid, with excellent levels across the sets; barely anything was missed anywhere, including in the WildList sets, which were dealt with perfectly. With no false positives either, *eScan* earns a VB100 award without fuss.

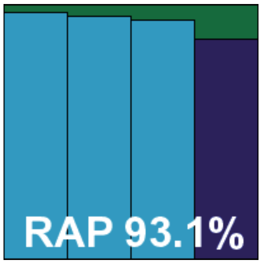
The vendor's test history shows five passes and a single fail in the last six tests; nine passes and three fails in two years. Testing brought up no issues, and was completed in good time, requiring less than the allotted two days of lab time.

## ESET NOD32 Antivirus 5

Main version: 5.0.94.0

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

vb 100 VIRUS virusbtn.com Dec 2011



Looking to continue an epic run of success into our new testing format, *ESET*'s product came as a petite 52MB package including all required updates. Set-up was straightforward and fairly quick, and online updates were fast and easy too, with most installs completing in under five minutes.

The GUI is very slick and attractive – a little more angular than expected, but still pleasant to look at and easy to use, with some improvements to the layout making the in-depth configuration easier to work with. Testing ran through simply, with good initial speeds and much faster speeds in the warm runs. Light overheads were recorded, with slightly higher than average RAM use but reasonable use of CPU cycles and average impact on our set of tasks. Detection rates were solid, dropping off slightly in the proactive week of the RAP sets but maintaining a good level throughout

| **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 |
| Agnitum Outpost | 15.00 | 2.69 | 1820.96 | 2.69 | 24.57 | 2104.96 | 24.57 | 27.76 | 3157.44 | 61.31 | 13.24 | 423.68 | 13.24 |
| AhnLab V3 | 10.85 | 4.67 | 4.71 | 4.67 | 24.76 | 24.86 | 24.76 | 47.66 | 101.85 | 105.25 | 20.28 | 20.50 | 20.28 |
| Auslogics Antivirus | 18.89 | 6.53 | 1820.96 | 6.53 | 22.24 | 420.99 | 22.24 | 40.28 | 485.76 | 88.94 | 20.84 | 81.13 | 20.84 |
| avast! Free Antivirus | 22.80 | 7.34 | 7.46 | 7.34 | 22.72 | 22.80 | 22.72 | 31.08 | 72.58 | 68.64 | 16.72 | 16.44 | 16.72 |
| AVG Internet Security | 31.24 | 10.84 | 1820.96 | 1820.96 | 49.34 | 1262.98 | 1578.72 | 66.51 | 2104.96 | 2104.96 | 23.11 | 317.76 | 293.32 |
| Avira AntiVir Free | 25.65 | 6.69 | 6.72 | 5.73 | 30.65 | 31.11 | 30.51 | 49.31 | 119.15 | 103.52 | 21.91 | 22.30 | 17.65 |
| Avira AntiVir Pro | 28.87 | 6.98 | 6.95 | 5.84 | 53.07 | 53.52 | 52.19 | 50.17 | 121.44 | 121.44 | 23.68 | 23.54 | 18.42 |
| BitDefender Antivirus Plus | 50.14 | 6.05 | 1820.96 | 6.05 | 28.84 | 6314.88 | 28.84 | 28.31 | 6314.88 | 62.52 | 16.80 | 3813.11 | 16.80 |
| BullGuard Antivirus | 19.50 | 10.17 | 1820.96 | 10.17 | 12.26 | 6314.88 | 12.26 | 28.31 | 6314.88 | 62.52 | 21.18 | 3813.11 | 21.18 |
| Central Command Vexira | 24.08 | 4.68 | 4.72 | 3.11 | 21.48 | 21.48 | 20.77 | 59.58 | 134.36 | 76.08 | 66.90 | 68.09 | 12.71 |
| Clearsight Antivirus | 19.42 | 3.70 | 3.68 | 3.70 | 16.66 | 16.62 | 16.66 | 23.63 | 53.07 | 52.19 | 10.33 | 10.31 | 10.33 |
| Commtouch Command | 19.76 | 6.34 | 6.32 | 6.34 | 17.54 | 17.69 | 17.54 | 28.89 | 64.44 | 63.79 | 14.12 | 14.23 | 14.12 |
| Comodo Antivirus | 12.34 | 3.89 | 3.65 | 3.89 | 25.88 | 26.20 | 25.88 | 55.00 | 128.88 | 121.44 | 16.23 | 15.89 | 16.23 |
| Comodo IS | 11.35 | 3.87 | 3.87 | 3.87 | 27.10 | 27.22 | 27.10 | 59.58 | 131.56 | 131.56 | 15.38 | 16.02 | 15.38 |
| Coranti 2012 | 17.71 | 3.71 | 56.90 | 3.71 | 7.83 | 43.25 | 7.83 | 16.72 | 128.88 | 36.93 | 9.58 | 52.23 | 9.58 |
| Coranti Cora | 20.65 | 3.88 | 140.07 | 3.52 | 10.79 | 60.14 | 13.73 | 18.22 | 146.86 | 45.11 | 9.78 | 53.71 | 9.32 |
| Defenx Security Suite 2012 | 15.07 | 2.81 | 8.39 | 2.81 | 20.18 | 161.92 | 20.18 | 23.63 | 263.12 | 52.19 | 11.70 | 165.79 | 11.70 |
| Digital Defender | 22.01 | 3.75 | 3.66 | 3.75 | 23.56 | 23.48 | 23.56 | 34.45 | 75.18 | 76.08 | 14.44 | 14.28 | 14.44 |
| eEye Blink Pro | 5.52 | 1.01 | 1.01 | 1.01 | 3.90 | 3.51 | 3.90 | 1.59 | 3.51 | 3.51 | 2.12 | 2.12 | 2.12 |
| Emsisoft Anti-Malware | 22.65 | 15.05 | 15.05 | 15.05 | 16.62 | 63.15 | 16.62 | 17.99 | 40.48 | 39.72 | 6.03 | 6.54 | 6.03 |
| eScan IS | 18.92 | 11.17 | 17.18 | 11.17 | 4.79 | 6.78 | 4.79 | 3.68 | 13.38 | 8.12 | 2.12 | 4.20 | 2.12 |
| ESET NOD32 | 98.08 | 6.65 | 1820.96 | 6.65 | 40.48 | 485.76 | 40.48 | 119.16 | 3157.44 | 263.12 | 34.05 | 224.30 | 34.05 |
| ESTsoft ALYac | 23.24 | 30.86 | 260.14 | 30.86 | 20.44 | 134.36 | 20.44 | 31.78 | 332.36 | 70.17 | 14.78 | 74.77 | 14.78 |
| Filseclab Twister | 13.08 | 1.19 | 1.16 | 1.19 | 12.94 | 12.86 | 12.94 | 14.37 | 31.73 | 31.73 | 5.00 | 4.98 | 5.00 |
| Fortinet FortiClient | 12.24 | 9.15 | 10.23 | 9.15 | 11.69 | 12.26 | 11.69 | 50.17 | 121.44 | 110.79 | 12.46 | 12.84 | 12.46 |
| Frisk F-PROT | 25.46 | 10.17 | 10.17 | 10.17 | 21.63 | 21.63 | 21.63 | 38.65 | 86.51 | 85.34 | 25.59 | 26.30 | 25.59 |
| F-Secure Client Security | 63.52 | 8.75 | 9.20 | 5.34 | 32.06 | 185.73 | 30.21 | 136.18 | 485.76 | 92.87 | 146.66 | 346.65 | 12.93 |

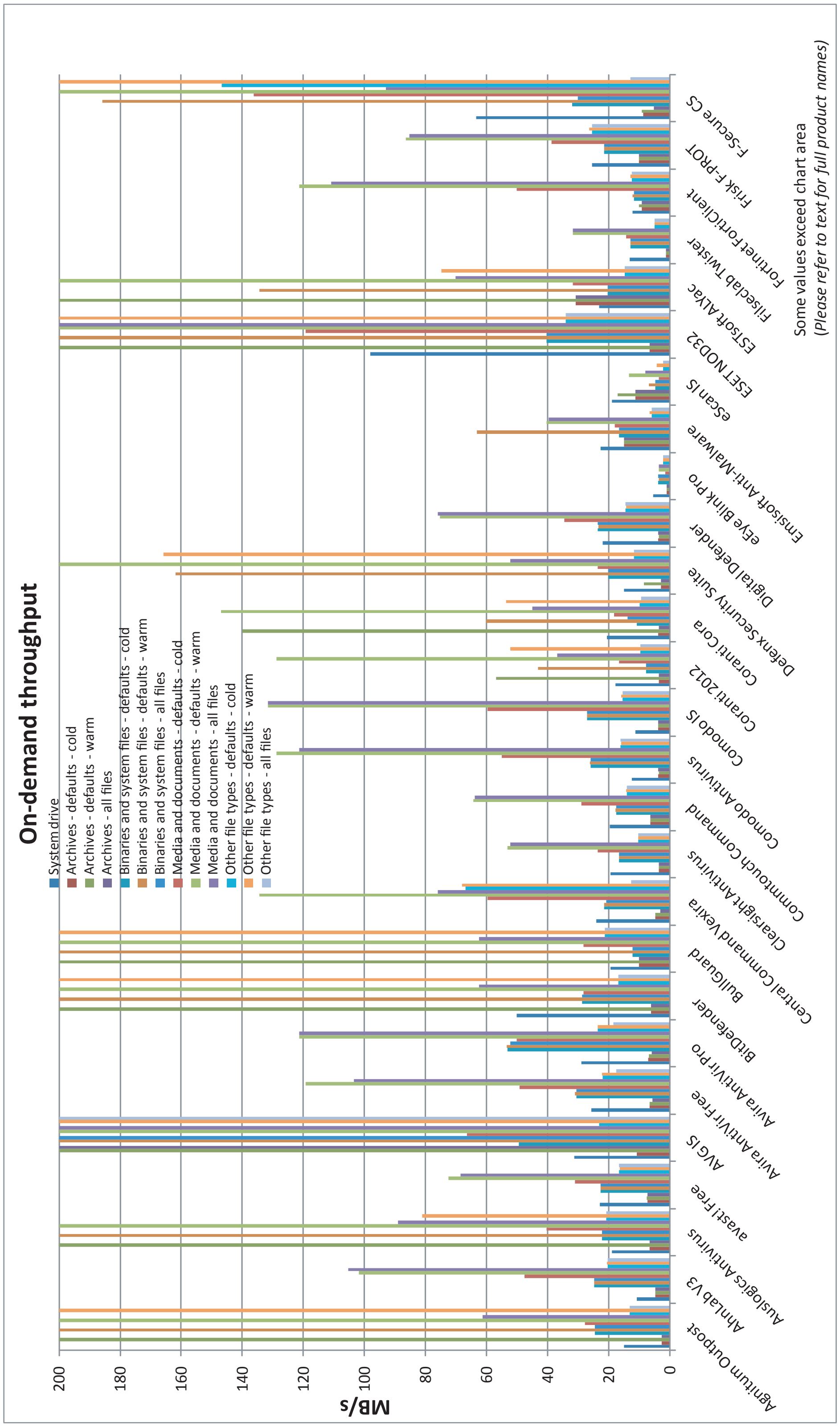
* System drive size measured before product installation.

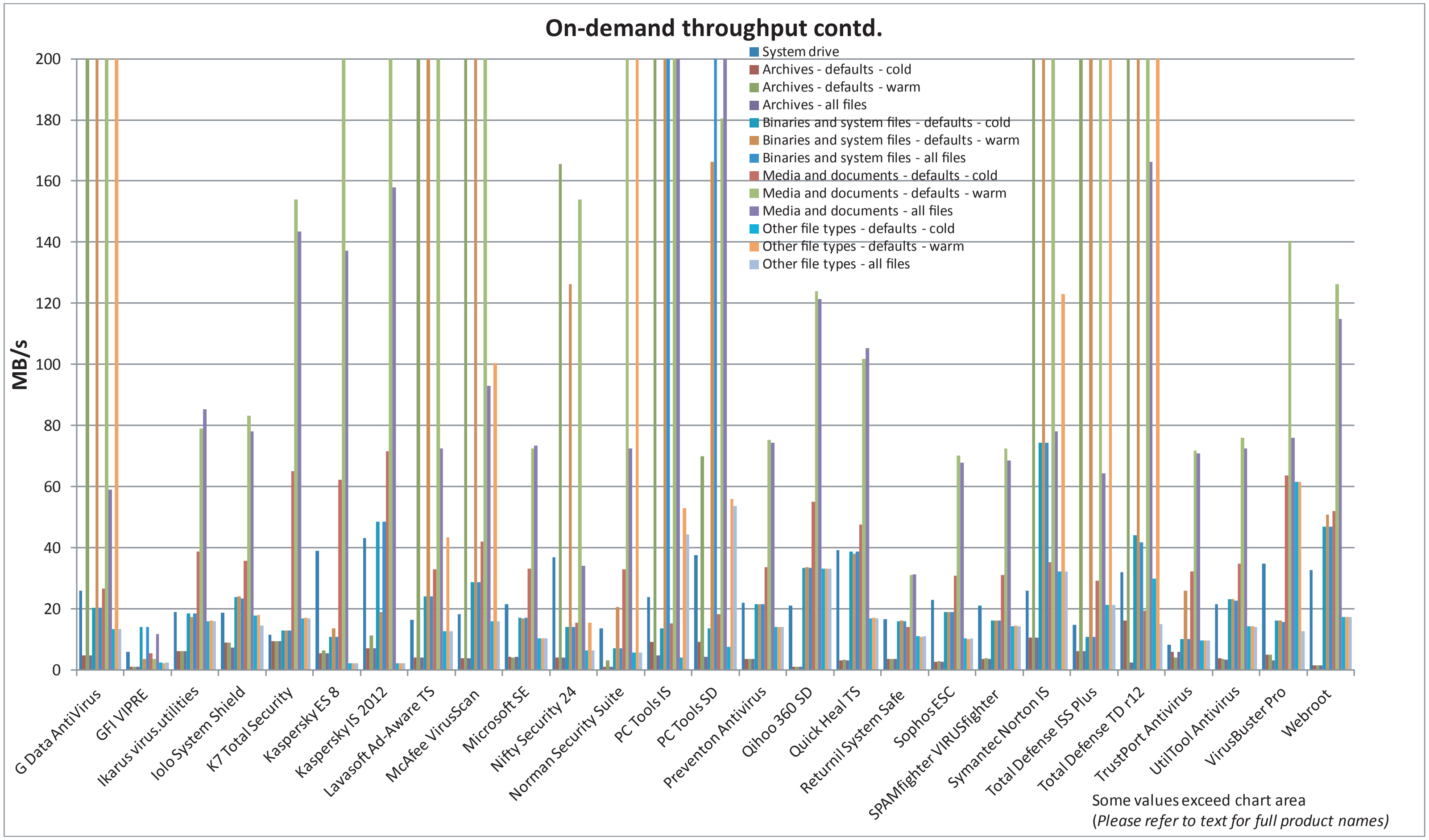
*(Please refer to text for full product names.)*

| **On-demand throughput contd. (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 |
| G Data AntiVirus | 26.05 | 4.72 | 1820.96 | 4.72 | 20.37 | 1578.72 | 20.37 | 26.73 | 2104.96 | 59.02 | 13.38 | 272.37 | 13.38 |
| GFI VIPRE | 5.92 | 1.01 | 1.01 | 1.01 | 14.13 | 3.51 | 14.13 | 5.37 | 3.51 | 11.85 | 2.38 | 2.12 | 2.38 |
| Ikarus virus.utilities | 18.92 | 6.09 | 6.24 | 6.09 | 18.41 | 17.44 | 18.41 | 38.65 | 78.94 | 85.34 | 16.02 | 16.09 | 16.02 |
| Iolo System Shield | 18.81 | 8.88 | 9.01 | 7.25 | 23.74 | 24.01 | 23.48 | 35.75 | 83.09 | 77.96 | 17.82 | 17.99 | 14.50 |
| K7 Total Security | 11.44 | 9.39 | 9.39 | 9.39 | 12.89 | 12.97 | 12.89 | 64.99 | 154.02 | 143.52 | 16.87 | 17.10 | 16.87 |
| Kaspersky ES | 38.89 | 5.48 | 6.48 | 5.48 | 10.76 | 13.70 | 10.76 | 62.17 | 210.50 | 137.28 | 2.12 | 2.12 | 2.12 |
| Kaspersky IS | 43.17 | 6.98 | 11.38 | 6.98 | 48.58 | 18.91 | 48.58 | 71.49 | 210.50 | 157.87 | 2.12 | 2.12 | 2.12 |
| Lavasoft Ad-Aware Total Security | 16.29 | 4.08 | 1820.96 | 4.08 | 24.19 | 574.08 | 24.19 | 32.87 | 701.65 | 72.58 | 12.71 | 43.33 | 12.71 |
| McAfee VirusScan | 18.30 | 3.93 | 303.49 | 3.93 | 28.70 | 263.12 | 28.70 | 42.06 | 350.83 | 92.87 | 15.89 | 100.35 | 15.89 |
| Microsoft SE | 21.62 | 4.25 | 3.95 | 4.25 | 17.11 | 16.98 | 17.11 | 33.25 | 72.58 | 73.43 | 10.39 | 10.39 | 10.39 |
| Nifty Security 24 | 36.95 | 4.10 | 165.54 | 4.10 | 14.03 | 126.30 | 14.03 | 15.46 | 154.02 | 34.13 | 6.42 | 15.38 | 6.42 |
| Norman Security Suite | 13.69 | 1.01 | 3.03 | 1.01 | 7.14 | 20.57 | 7.14 | 32.87 | 789.36 | 72.58 | 5.76 | 200.69 | 5.76 |
| PC Tools IS | 23.73 | 9.24 | 606.99 | 4.77 | 13.61 | 300.71 | 315.74 | 15.21 | 332.36 | 315.74 | 4.18 | 52.96 | 44.34 |
| PC Tools SD | 37.68 | 9.15 | 70.04 | 4.29 | 13.67 | 166.18 | 225.53 | 18.22 | 180.43 | 217.75 | 7.58 | 56.08 | 53.71 |
| Preventon | 22.05 | 3.56 | 3.56 | 3.56 | 21.48 | 21.41 | 21.48 | 33.64 | 75.18 | 74.29 | 14.18 | 14.18 | 14.18 |
| Qihoo 360 SD | 20.97 | 1.01 | 1.03 | 1.01 | 33.41 | 33.59 | 33.41 | 55.00 | 123.82 | 121.44 | 33.16 | 33.16 | 33.16 |
| Quick Heal TS | 39.23 | 3.11 | 3.27 | 3.11 | 38.74 | 38.04 | 38.74 | 47.66 | 101.85 | 105.25 | 16.80 | 17.18 | 16.80 |
| Returnil System Safe | 16.63 | 3.56 | 3.54 | 3.56 | 16.03 | 16.07 | 16.03 | 14.16 | 30.96 | 31.26 | 10.96 | 10.89 | 10.96 |
| Sophos ESC | 22.88 | 2.78 | 2.80 | 2.78 | 18.85 | 18.85 | 18.85 | 30.75 | 70.17 | 67.90 | 10.25 | 10.09 | 10.25 |
| SPAMfighter VIRUSfighter PRO | 20.94 | 3.55 | 3.72 | 3.55 | 16.23 | 16.19 | 16.23 | 31.08 | 72.58 | 68.64 | 14.28 | 14.61 | 14.28 |
| Symantec Norton Internet Security | 25.95 | 10.59 | 1820.96 | 10.59 | 74.29 | 631.49 | 74.29 | 35.31 | 789.36 | 77.96 | 32.31 | 123.00 | 32.31 |
| Total Defense Inc ISS Plus | 14.69 | 6.24 | 455.24 | 6.24 | 10.70 | 1052.48 | 10.70 | 29.18 | 1578.72 | 64.44 | 21.30 | 346.65 | 21.30 |
| Total Defense Inc TD r12 | 31.99 | 16.11 | 910.48 | 2.55 | 44.16 | 1052.48 | 41.82 | 19.32 | 1262.98 | 166.18 | 29.79 | 254.21 | 14.95 |
| TrustPort Antivirus | 8.36 | 6.03 | 3.98 | 6.03 | 10.20 | 25.99 | 10.20 | 32.13 | 71.76 | 70.95 | 9.70 | 9.65 | 9.70 |
| UtilTool Antivirus | 21.44 | 3.79 | 3.62 | 3.35 | 23.05 | 23.05 | 22.80 | 34.88 | 76.08 | 72.58 | 14.34 | 14.23 | 14.02 |
| VirusBuster Pro | 34.83 | 5.02 | 4.93 | 3.18 | 16.23 | 16.28 | 15.67 | 63.55 | 140.33 | 76.08 | 61.50 | 61.50 | 12.75 |
| Webroot SecureAnywhere | 32.77 | 1.58 | 1.46 | 1.58 | 46.78 | 50.93 | 46.78 | 52.00 | 126.30 | 114.82 | 17.33 | 17.41 | 17.33 |

* System drive size measured before product installation.

*(Please refer to text for full product names.)*


On-demand throughput
System drive
Archives - defaults - cold
Archives - defaults - warm
Archives - all files
Binaries and system files - defaults - cold
Binaries and system files - defaults - warm
Binaries and system files - all files
Media and documents - defaults - cold
Media and documents - defaults - warm
Media and documents - all files
Other file types - defaults - cold
Other file types - defaults - warm
Other file types - all files
MB/s
0
20
40
60
80
100
120
140
160
180
200
Agnitum Outpost
AhnLab V3
Auslogics Antivirus
avast! Free
AVG IS
Avira AntiVir Free
Avira AntiVir Pro
BitDefender
BullGuard
Central Command Vexira
Clearsight Antivirus
Commtouch Command
Comodo Antivirus
Comodo IS
Coranti 2012
Coranti Cora
Defenx Security Suite
Digital Defender
eEye Blink Pro
Emsisoft Anti-Malware
eScan IS
ESET NOD32
ESTsoft ALYac
Filseclab Twister
Fortinet FortiClient
Frisk F-PROT
F-Secure CS
Some values exceed chart area
(Please refer to text for full product names)



On-demand throughput contd.

Some values exceed chart area
*(Please refer to text for full product names)*

the Response tests. The core sets were handled impeccably, comfortably earning *ESET* another VB100 award and continuing the vendor's unbroken run of passes.

*ESET*'s record cannot be faulted, with 12 passes in the last two years. Testing this month was interrupted by a single interface crash under heavy pressure, but protection was not affected and simply reopening the GUI proved sufficient to get things moving along again. All tests completed in well under the allotted two days.

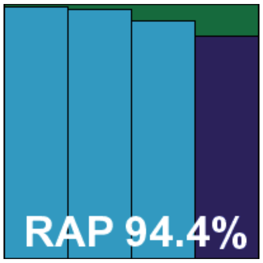
### ESTsoft ALYac Internet Security

Main version: 2.5.0.12

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

*ALYac* made its first appearance on our test bench in the last comparative, and did a pretty good job. With the *BitDefender* engine under the covers, we expected another impressive run. The installer weighed in at 159MB, and after a 20-second pause at the outset, it moved along quite nicely, completing in only a minute or two. It looked like running updates would take some time, but updating seemed to have finished after ten minutes or so, and testing proceeded. It was only on the third and final live install that we observed the update process not completing properly – considering that the only indication of this is a dialog which closes after five seconds, it's not surprising that we didn't spot it before. This put into doubt whether previous updates had worked, but as we had completed the required steps of running a manual update, rebooting the system and then running a second manual update, there was not much more we could do.

vb 100 VIRUS virusbtn.com Dec 2011



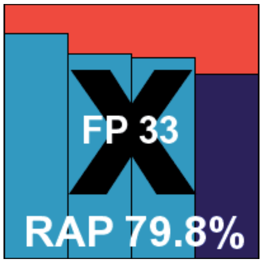
The tests ran smoothly otherwise, with a solid score in the RAP sets and rather less impressive, but still respectable levels in the Response sets (as could have been predicted if the updates had not functioned properly). The WildList set was handled with ease, and with no false alarms and just a few warnings of software which might be considered undesirable in the clean sets, *ESTsoft* makes the grade for VB100 certification for the second time in a row. The updating problem was the only issue noted, and it seems likely that this is in part due to our test lab's distance from the product's usual market space in South Korea. Even given the extra time devoted to trying to coax an update to work once we'd spotted the problem, all tests completed well within the two-day period.

### Filseclab Twister AntiVirus

Main version: 10.156.27493

| | | | |
|---|---|---|---|
| **ItW Std** | 99.98% | **ItW Std (o/a)** | 99.98% |
| **ItW Extd** | 98.99% | **ItW Extd (o/a)** | 98.61% |
| **False positives** | 33 | | |

Another company from the Far East, China's *Filseclab* has a longer history in our tests but rather less success so far. The 53MB installer came with a 48MB offline updater, and the set-up was fast and simple, with only a handful of clicks required. Updating online took considerably longer – over an hour in some instances – and averaged around 40 minutes, but again this could be partly due to our distance from the product's main target market. The interface is a little 'old-school' and feels clunky in places, but it generally functions well, providing a good basic set of controls once the layout has been figured out. Testing proved relatively simple, with no major issues. Scanning speeds were slow, overheads a touch heavy in places, but resource use and impact on our set of tasks were around average for the month.



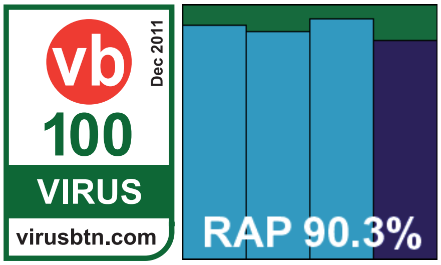
Detection rates were pretty decent, with a slight tailing off in the last few days of the Response tests, and the main WildList set was covered reasonably well too, with just a couple of polymorphic samples and a handful of Extended list items not spotted. A handful of false positives did crop up in the clean sets, most of them on fairly major packages from developers including *IBM*, *Sun*/*Oracle*, *SAP* and common consumer software such as *VLC*.

Overall, things continue to improve, and VB100 certification seems to be moving closer to *Filseclab*'s grasp. The vendor has yet to pass, but continues to battle bravely on, with five entries in the last two years. Testing proved fairly straightforward, and completed just within the allotted 48 hours.

### Fortinet FortiClient Endpoint Security

Main version: 4.1.3.143

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*Fortinet* provided its product as a tiny 10MB installer, with offline updates weighing in at 125MB. As might be expected, this made the set-up process pretty simple and speedy, but applying updates from the Internet took 45 minutes on average, with one run needing more than an hour to complete the install. Further updates are scheduled daily by default, and hopefully take less time once the initial package is in place. Occasionally updates required a reboot, but the main install did not request one.

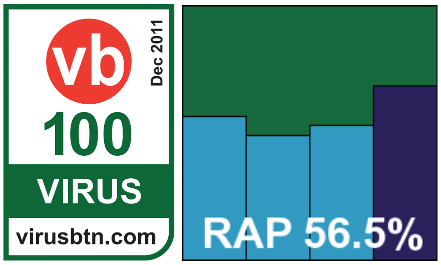
The interface is businesslike and efficient, providing a solid set of controls in easy-to-access format, and it remained stable throughout our tests. Speeds were decent, overheads a little on the heavy side, with resource use around average and our set of tasks considerably slower than most. Detection rates continue to impress though, maintaining the good level of improvement observed in recent months, and on our RAP chart the product is now well up in the cluster of top performers. Scores in the Response tests were good too, with a slight decline into the last few days.

The core sets were properly dealt with, with no issues to report, and *Fortinet* comfortably earns another VB100 award. The vendor's history is dependable, with four passes and a single fail in the last six tests, no entry in the *Linux* test, and eight passes and two fails in the last two years. With no stability problems or other complaints, all tests tripped through in good order, requiring not much more than one day of lab time.

## Frisk F-PROT AntiVirus for Windows

Main version: 6.0.5

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.60% |
| **False positives** | 0 | | |



*F-PROT* is another compact product, its main installer measuring 30MB, with updates adding an extra 58MB to the submission. The set-up process is fast and simple, requiring a reboot to complete, and updates are fairly speedy too. The GUI is minimal with only basic controls but is simple to operate and generally works well. As usual, some of our larger scans fell over from time to time, but with clear and dependable logging, it was no big problem to carry on where we'd left off.

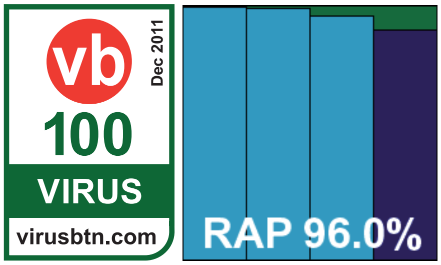
Scanning speeds were fairly average, as were on-access overheads and use of CPU cycles, with fairly low use of RAM and a very low impact on our set of activities. Detection rates continued to disappoint somewhat, dipping dangerously towards the mediocre in parts. The WildList sets were dealt with well though, and with no false alarms *Frisk* earns another VB100 award.

The vendor now has five passes and a single fail from the last six tests – a considerable improvement, as the two-year view shows four fails and eight passes. Other than heavy scans occasionally coming to a halt, no serious issues were spotted, and testing progressed well, completing within the two-day limit.

## F-Secure Client Security

Main version: 9.20 build 274

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*F-Secure*'s business-oriented solution is fairly lightweight, with the main installer measuring only 63MB. Installation runs through in good time with no surprises. Updates provided offline weighed in at 157MB, but updating online took less than ten minutes on each run. On one attempt, the update failed after five minutes with a connection timeout, but on retrying all went smoothly. The interface is a little unusual, but crisp and unfussy, with usage fairly intuitive and a reasonable level of fine-tuning available. Testing was generally uneventful, although when looking at the RAP figures we did observe that scores for one set were considerably lower than expected, given those achieved by other products using the *BitDefender* engine. Re-running the job resulted in the same set of figures, and we were about to assume that the data was correct and move along when a third and final attempt yielded the much higher numbers anticipated. The reason for the poor scores on the first two attempts remains a mystery.

Otherwise, things went well, with some good scanning speeds, fairly light overheads, low resource use – particularly the CPU cycle measure – and a slightly above average impact on our set of tasks. The certification sets were dealt with well, with no misses or false positives, and *F-Secure* earns another VB100 award. The vendor's history shows a strong record, with no fails in over four years; ten passes from ten attempts in the last two years.

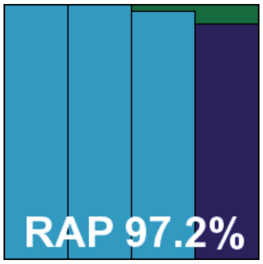
## G Data AntiVirus 2012

Main version: 22.1.0.0

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

*G Data*'s product is invariably a bit of a beast, and this month's submission came as a mighty 474MB install package. The set-up process is not overly complicated though, and runs through at good speed, needing a reboot at the end. Online updates are zippy too, averaging just 10 minutes from bare install to fully up-to-date – not bad at all, given the product's dual-engine approach. The interface is clear and simple, providing excellent depth of control without compromising usability, and it remained solid under the heaviest of bombardments.

vb 100 VIRUS virusbtn.com Dec 2011



Scanning speeds started off reasonable and became lightning fast in the warm runs, but on-access overheads were fairly heavy, and with average resource use, our set of tasks took forever to complete. Detection rates were awe-inspiring though, with barely anything missed across the sets, scoring in the high 99%s for each of the Response sets and even the proactive week of the RAP sets was above 90%. The WildList was brushed aside effortlessly, and with no false alarms a VB100 award is earned with minimal effort.

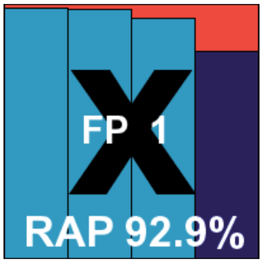
The product's history shows four passes and one fail in the last six tests, the *Linux* test being skipped, and the same pattern the previous year, making for eight passes and two fails from ten entries in the last two years. Testing ran without problems, completing in little over a day of lab time.

## GFI VIPRE AntiVirus

Main version: 4.0.4280

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 1 | | |

*GFI* had one of the smallest installers of this month's test, at only 13MB, and the update packages weighed in at 76MB. The set-up process took quite some time, with a reboot and some additional steps to complete at the end, but online updates were generally fairly speedy, averaging under 10 minutes. The interface is clear and professional-looking but configuration is a little non-standard, with many common options either absent or obscured by unclear descriptions. Operation was generally stable and reliable though.



Testing also took quite some time, with some very slow scanning speeds. Overheads were pretty light though, with very low RAM use, CPU use around average and our set of tasks zipping through very quickly. Detection tests as usual proved rather a chore, with scans having to be split into chunks to avoid the crashing and logging problems experienced in previous tests. Whether this precaution was effective or unnecessary, things went fairly smoothly and no data was lost. The RAP test alone took over 24 hours to complete (some of the faster products did the same job in less than two hours) and the product's performance in the Response test was similarly sluggish – the test was set up to run overnight and was still trundling along in the morning.

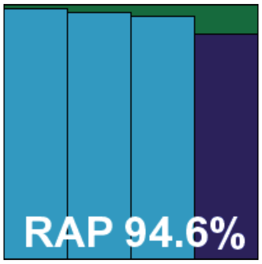
In the WildList sets, we suffered the usual problems with some samples not being scanned in actual real time – detection being delayed slightly for some background work. This rendered our file access tool's logs less than reliable. With the product's own on-access logging system also useless, we resorted to copying the unblocked samples around the system and watching as they were slowly removed, one by one, over a period of several minutes. In a couple of the runs a single sample seemed to go undetected, but after repeated attempts we finally managed to get full coverage. After all this work, a single sample in the clean sets – a component of a DVD-authoring suite from *Corel* offshoot *Ulead* – was labelled as a trojan, and *GFI* just misses out on certification this month.

The vendor's test history has been solid of late, with four passes and now a single fail in the last six tests, the *Linux* comparatives not entered, while the two-year view shows six passes and two fails from eight entries. Although there were no specific stability issues or crashes this month, testing was not entirely without problems, and coupled with the slow scanning times, the product used up one of our test systems for around six full days.

## Ikarus virus.utilities

Main version: 2.0.90

| | | | |
|---|---|---|---|
| **ItW Std** | 99.99% | **ItW Std (o/a)** | 99.99% |
| **ItW Extd** | 99.93% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 0 | | |



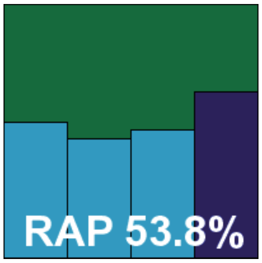
As usual, *Ikarus* provided its product in the form of an ISO image for an install CD, the whole thing measuring 200MB but doubtless including some extraneous components. Offline updates measured 65MB, and the set-up process involved a fair number of stages but didn't take too long. Running online updates was likewise speedy, completing in around five minutes. The interface has remained the same for some time – a little unusual, but fairly simple to work out with a little exploration, and it seemed to operate fairly stably throughout testing, although it did become a little slow to respond during large detection jobs.

Scanning speeds were fairly average, but overheads pretty hefty, with reasonable RAM use but quite high use of CPU cycles. Our set of tasks ran through in unexceptional time, but other tests seemed fairly speedy, with all detection tests completing in good time. RAP and Response scores were pretty impressive throughout, dropping only slightly into the proactive week, and the clean set was handled well too. The WildList sets were mostly covered, but a few Virut samples were missed, denying *Ikarus* a VB100 award this month. That leaves the company with no passes from four attempts in the last six tests; two passes from seven entries in the last two years. With no stability issues to note, testing powered through in good time, completing in a little more than 24 hours of system time.

## Iolo System Shield

Main version: 4.2.4

| | | | |
|---|---|---|---|
| **ItW Std** | 99.80% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 96.67% | **ItW Extd (o/a)** | 99.87% |
| **False positives** | 0 | | |



*Iolo*'s product provides malware detection based on the *Frisk* engine. It arrived as a 48MB installer which took a long time to run through its business and demanded a reboot, after which the system took much longer than usual to fully restart. The update process is not too sluggish though, and the interface has a clean and professional look, providing only basic controls but generally functioning properly. Scanning speeds were medium and on-access overheads very heavy, and while RAM use was low, CPU use was very high and the run time of our set of tasks was seriously impacted.

With quarantine or delete the only options available for dealing with infected items, scanning took a little longer than hoped, and once it had completed, even more time was required to decipher the bizarre and esoteric format of the raw log data. This cannot be exported to text and the developers have been unable to provide any kind of information or tools to assist in its deciphering, despite repeated requests. Once again, some rather ugly manual hacking was required to rip data into a usable format. Once the results had been deciphered, detection rates proved to be mediocre (like those shown by the *Frisk* product itself), but it came as a surprise to find that a higher score was achieved in the proactive week of the RAP sets than anywhere else.

The standard WildList was handled well on access, but despite lengthy searching we could find no mention of several items in the logs from the on-demand jobs, and with the items not deleted, they appeared to have been missed entirely. This was confirmed by re-running the scans over the missed items only. Thus, despite there being no false positives, *Iolo* does not qualify for a VB100 award on this occasion.

Our results history shows one pass and three fails from four attempts in the last six tests; two passes and four fails in the last two years. There were no stability issues, but a lack of options and horrible logging made for a lot of extra work, leaving the product on one of our test machines for more than twice the allotted 48 hours.

| **Archive scanning** | | ACE | CAB | EXE-RAR | EXE-ZIP | JAR | LZH | RAR | TGZ | ZIP | ZIPX | EXT* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Agnitum Outpost | OD | X | √ | X/√ | X/√ | X | √ | √ | X | √ | X | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| AhnLab V3 | OD | X | √ | 9 | 9 | 9 | 9 | 9 | X | 9 | X | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| Auslogics Antivirus | OD | √ | √ | X | X | √ | √ | √ | X | √ | √ | √ |
| | OA | X/√ | X/√ | X/√ | X/√ | 2/√ | X/√ | X/√ | X/√ | 1/√ | 1/√ | √ |
| avast! Free Antivirus | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X/√ | X/√ | √ | √ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| AVG Internet Security | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | X/√ |
| Avira AntiVir Free | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Avira AntiVir Professional | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| BitDefender Antivirus Plus | OD | √ | √ | 8 | 8 | √ | √ | √ | 8 | √ | √ | √ |
| | OA | X/√ | X/√ | 4/√ | 4/√ | 8/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| BullGuard Antivirus 10 | OD | √ | √ | 8 | 8 | √ | √ | √ | 8 | √ | √ | √ |
| | OA | 2 | 2 | 1 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | √ |
| Central Command Vexira | OD | 1 | √ | √ | √ | √ | X | √ | √ | √ | X/√ | X/√ |
| | OA | X | X | X | X | X | X | X | X | X | X | X/√ |
| Clearsight Antivirus | OD | 2 | 2 | X | X | 2 | X | 2 | 1 | 2 | 2 | √ |
| | OA | 1 | 1 | X | X | X/1 | X | 1 | X | 1 | X/1 | X/√ |
| Commtouch Command | OD | 5 | 5 | 5 | 5 | 5 | √ | 5 | 2 | 5 | 5 | √ |
| | OA | 2/4 | 2/4 | 2/4 | 2/4 | 2/4 | √ | 2/4 | 1/2 | 2/4 | 2/4 | √ |
| Comodo Antivirus | OD | X | 5 | 5 | 5 | 5 | 5 | 5 | 2 | 5 | X | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| Comodo Internet Security | OD | X | 5 | 5 | 5 | 5 | 5 | 5 | 2 | 5 | X | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| Coranti 2012 | OD | √ | √ | 8 | 8 | √ | √ | √ | 8 | √ | √ | √ |
| | OA | X/1 | X | X | X | X/√ | X | X | X | 1 | X/1 | X/√ |
| Coranti Cora Antivirus | OD | √ | √ | 8 | 8 | √ | √ | √ | 8 | 1 | √ | √ |
| | OA | X/1 | X | X | X | X/√ | X | X | X | 1 | X/1 | X/√ |
| Defenx Security Suite 2012 | OD | X | √ | √ | √ | √ | X | √ | √ | √ | X | √ |
| | OA | X | √ | 8 | √ | √ | X | √ | √ | √ | X | √ |
| Digital Defender | OD | 2 | 2 | X | X | 2 | X | 2 | 1 | 2 | 2 | √ |
| | OA | 1 | 1 | X | X | X/1 | X | 1 | X | 1 | X/1 | 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.*)

| Archive scanning contd. | | ACE | CAB | EXE-RAR | EXE-ZIP | JAR | LZH | RAR | TGZ | ZIP | ZIPX | EXT[*] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| eEye Blink Professional | OD | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | X/√ |
| Emsisoft Anti-Malware | OD | 2 | 2 | 7 | 2 | X | 2 | 2 | 3 | 2 | 2 | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| eScan Internet Security | OD | √ | 7 | 6 | 5 | 7 | 7 | 7 | 7 | 8 | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| ESET NOD32 Antivirus | OD | √ | √ | √ | √ | √ | √ | √ | 5 | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| ESTsoft ALYac | OD | X | X | 8 | 8 | X | X | X | X | X | X | √ |
| | OA | X | X | 8 | 8 | X | X | X | X | X | X | √ |
| Filseclab Twister | OD | 5 | 3 | 3 | 3 | 4 | 1 | 4 | X | 5 | X | √ |
| | OA | X | X | X | X | X | X | 1 | X | 2 | X | √ |
| Fortinet FortiClient | OD | X | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Frisk F-PROT | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X | X | 2 | 2 | X | X | X | 2 | 2 | √ |
| F-Secure Client Security | OD | X/√ | √ | √ | √ | √ | √ | √ | 8 | √ | X/√ | X/√ |
| | OA | X | X | X | X | X | X | X | X | X | X | X/√ |
| G Data AntiVirus 2012 | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| GFI VIPRE Antivirus | OD | X | X | √ | √ | √ | X | √ | X | √ | X | √ |
| | OA | X | X | √ | √ | X | X | X | X | X | X | √ |
| Ikarus virus.utilities | OD | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 3 | 7 | 7 | √ |
| | OA | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 3 | 7 | 7 | √ |
| Iolo System Shield | OD | 5 | 5 | 5 | 5 | 5 | √ | 5 | 5 | 5 | 5 | √ |
| | OA | 5 | 5 | 5 | 5 | 5 | √ | 5 | 5 | 5 | 5 | √ |
| K7 Total Security | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X | X/1 | X/1 | X | X | X | X | X/1 | X/1 | √ |
| Kaspersky ES 8 | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X/√ | X/√ | 1/√ | 1/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Kaspersky IS 2012 | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X/√ | X/√ | 1/√ | 1/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Lavasoft Ad-Aware TS | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | √ | √ | 3/√ | 4/√ | √ | √ | √ | 8/√ | 8/√ | √ | √ |
| McAfee VirusScan | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X/√ | 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.*)

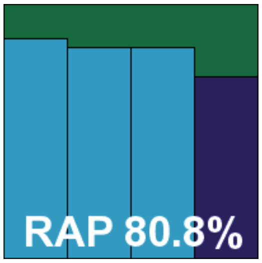
| **Archive scanning contd.** | | ACE | CAB | EXE-RAR | EXE-ZIP | JAR | LZH | RAR | TGZ | ZIP | ZIPX | EXT* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Microsoft SE | OD | √ | √ | 9 | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X | X | 1 | X | X | X | X | 1 | X | √ |
| Nifty Security 24 | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X | 1 | 1 | X | X | X | X | X | X | √ |
| Norman Security Suite | OD | X | √ | √ | 1 | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X | X/1 | X/1 | X | X | X | X | X | X | √ |
| PC Tools Internet Security | OD | 1 | √ | 7 | √ | √ | √ | √ | 5 | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | X |
| PC Tools Spyware Doctor | OD | 1 | √ | 7 | √ | √ | √ | √ | 5 | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | X |
| Preventon Antivirus | OD | 2 | 2 | X | X | 2 | X | 2 | 1 | 2 | 2 | √ |
| | OA | 1 | 1 | X | X | X/1 | X | 1 | X | 1 | X/1 | X/√ |
| Qihoo 360 SD | OD | 1 | √ | 1 | 1 | 1 | √ | √ | √ | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| Quick Heal Total Security | OD | X/2 | 2/5 | X | X | 2/5 | X | 2/5 | 1 | 2/5 | X | X/√ |
| | OA | 2 | X | X | X | 1 | X | X | X | 1 | X | √ |
| Returnil System Safe | OD | 5 | 5 | 3 | 2 | 5 | 7 | 5 | 2 | 5 | 5 | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| Sophos ESC | 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/√ |
| SPAMfighter VIRUSfighter | OD | 1 | 1 | X | X | 1 | X | 1 | X | 1 | 1 | √ |
| | OA | X/1 | X/1 | X | X | X/1 | X | X/1 | X | X/1 | X/1 | X/√ |
| Symantec Norton IS | OD | √ | √ | √ | √ | √ | √ | √ | 5 | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| Total Defense Inc ISS | OD | X | √ | √ | √ | √ | √ | √ | √ | √ | √ | X/√ |
| | OA | X | X | X | X | 1 | X | X | X | 1 | X | √ |
| Total Defense Inc TD r12 | OD | X | X/√ | X/√ | X/√ | 1/√ | X/√ | X/√ | X/√ | 1/√ | X/√ | √ |
| | OA | X | X/√ | X/√ | X/√ | 1/√ | X/√ | X/√ | X/√ | 1/√ | X/√ | √ |
| TrustPort Antivirus 2012 | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X/√ | X/√ | X/√ | X/√ | √ | X/√ | X/√ | X/√ | √ | √ | √ |
| UtilTool Antivirus | OD | 1 | 1 | X | X | 1 | X | 1 | X | 1 | 1 | √ |
| | OA | 1 | 1 | X | X | X/1 | X | 1 | X | 1 | X/1 | X/√ |
| VirusBuster Professional | OD | √ | √ | √ | √ | √ | X | √ | √ | √ | X | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | X/√ |
| Webroot SecureAnywhere | OD | X | √ | X | X | √ | X | √ | X | √ | X | √ |
| | OA | 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.*)

## K7 Total Security Desktop Edition

Main version: 11.1

| | | | |
|---|---|---|---|
| **ItW Std** | 100.0% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



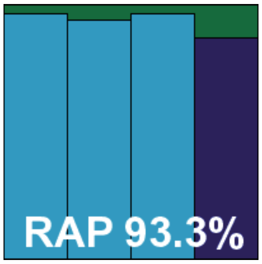
Returning after a few months' absence, *K7*'s product seems to have changed little in the interim. Its 81MB installer set up in good time, with a reboot needed only after some updates – which generally took only a few minutes to complete. The interface is bright and colourful to the point of gaudiness, and leans towards the wordy, but it is perfectly usable, provides an excellent array of options and remained solid and stable throughout testing.

Scanning speeds were reasonable, overheads fairly light, with average resource use and minimal impact on our set of tasks. Detection rates were solid if unremarkable, dropping away a little in the proactive week of the RAP set and the latter few days of the Response sets, but the WildList was covered impeccably, and with no false alarms *K7* earns another VB100 award. From sporadic entries, the vendor has achieved two passes from two tries in the last six tests; five from five in the last two years. Testing ran without causing us any stress, and completed in well under the anticipated 48 hours of system time.

## Kaspersky Endpoint Security 8 for Windows

Main version: 8.1.0.646

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*Kaspersky* submitted both its consumer and business offerings again this month. We started with the corporate product, *ES8*. The install package was a fairly hefty 243MB, and updates were included in a large bundle mirroring a full download site. Set-up was fairly speedy and straightforward though, the only moment of note being the option to add the command-line scanner to the system search path, which seems a useful thing to have in an enterprise situation. Update times varied widely depending on the age of the existing data, but never went over about 15 minutes even after several weeks without updates. No reboots were required.

The interface is simple and crisp, with a pleasantly curvy feel to it without straying into the cartoony. Settings are provided in extreme depth – suitable for the most demanding enterprise environment – and are, for the most part, simple to locate and operate. Everything seemed to run fairly smoothly, with speed measures showing decent rates – sometimes, but not always, improving on the warm runs. The on-access overheads likewise were medium at first and somewhat better on repeat visits. RAM use was a little high, and CPU use much more so, and our set of tasks took a fair while to complete.

Reckoning up detection rates was a little tricky, with the logging system only just coping with the heavy load of data pushed into it, and some quirks in the log format unearthing a minor bug in one of our log processing scripts. With everything properly parsed, it was clear that detection rates were as excellent as ever, with very solid levels across all the sets. The core sets were nicely dealt with, and VB100 certification is comfortably earned by *Kaspersky*'s business offering.

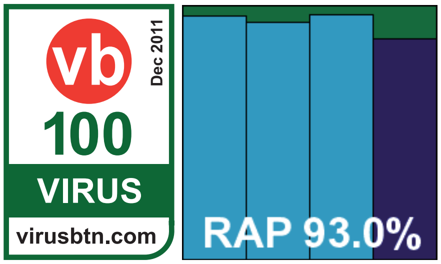
The product's history shows a few minor blips lately in an otherwise solid record, with three passes and two fails in the last six tests; seven passes and three fails in the last two years. With no major issues to report, some jobs were a little slow and testing took just a little longer than the 48-hour limit.

## Kaspersky Internet Security 2012

Main version: 12.0.0.374

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

*Kaspersky*'s home-user suite came as a much smaller 78MB installer, again using the offline update mirror, and here the set-up process was fairly slow and drawn out. No reboot was required, but updating took longer – over half an hour in some cases. This variant on the interface is again curvy and stylish, and reasonably easy to navigate after a little practice. A wealth of controls is available under the covers.



Scanning speeds were a fraction better here – again with some signs of smart optimization – and overheads were light, but in this case resource use was noticeably lower and our set of tasks ran through in short order.

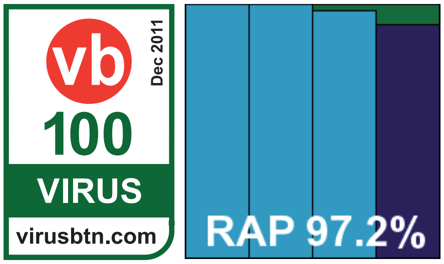
Detection rates were splendid, with good coverage everywhere, only the later parts showing any kind of decline and even there highly respectable scores were achieved. The core sets presented no problems, and a second VB100 award goes to *Kaspersky* this month.

The *IS* product has a slightly better history than its sibling, with four passes and a fail in the last six tests; nine passes and a single fail in the last two years. With no issues to report, testing took just a little longer than hoped, mainly thanks to lengthy scans over the large infected sets.

## Lavasoft Ad-Aware Total Security

Main version: 21.1.0.28

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*Lavasoft*'s *Total Security* product is based on *G Data*, with some extras of *Lavasoft*'s own rolled in. The installer is thus pretty hefty at 549MB, including latest updates. Set-up is not too strenuous though, requiring only a few clicks and a short wait, followed by a reboot. Online updating was fairly speedy too, averaging less than 15 minutes for the full installation process.

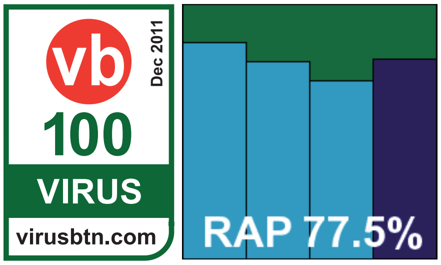
The interface is clear and information-packed, functional without lacking in style, and provides a splendid degree of fine-tuning while maintaining rock-like solidity through the toughest of tests. Scanning speeds were decent in the cold runs and lightning fast in the warm ones, while overheads started fairly heavy but quickly became feather-light once the product had settled into its surroundings. With average RAM use and CPU use perhaps a shade above average, our set of tasks did take a fair while to complete.

Detection scores were stratospheric though, with excellent coverage everywhere, and with no issues in the core sets a VB100 award is easily earned. Three passes have been achieved from three entries in the last six tests; three passes and two fails from five attempts in the last two years. With no issues to report, testing breezed through very pleasantly, finishing in little more than 24 hours' system time and bringing much joy and celebration to the lab team.

## McAfee VirusScan Enterprise

Main version: 8.8

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



Essentially unchanged for quite some time, *McAfee*'s tried and tested formula for enterprise protection was provided as a 37MB zip file containing the installer and related files, along with 121MB of updates. Set-up is fairly simple and speedy and does not insist on a reboot to complete (although one is required for full functionality of some of the components). Updates were not so zippy, but didn't take too long, averaging around 15 minutes. The interface is very stark with no concessions made to fads and fashions, but provides an ample set of controls and reporting in simple and accessible style, maintaining solid stability throughout our tests.

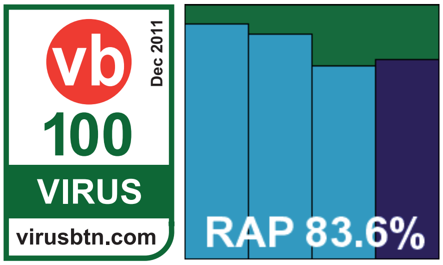
Scanning speeds started off at a reasonable rate and sped up nicely on warm runs, but on-access lags were a little heavy. Resource use and impact on our set of tasks were around average, and detection rates were decent in the RAP sets and a little better in the Response sets, showing the impact of the company's *Artemis* cloud look-up system. Nevertheless, levels dropped off a little in the most recent few days.

The core sets were well handled though, and a VB100 award is earned without fuss. Our history shows a rather uneven pattern of submissions, but three passes from three tries in the last six tests; longer term, things are a little more rocky, with five passes and two fails from seven entries in the last two years. No bugs or errors were encountered, and all tests completed within less than the assigned 48 hours of system time.

## Microsoft Security Essentials

Main version: 2.1.1116.0

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*Microsoft*'s free-for-personal-use solution surely wins the prize for smallest installer this month, with the main package measuring just 7.8MB, and the 67MB offline updater not too bloated either. Set-up is very simple and runs very quickly, while online updating completed in an average of six minutes, even more than a month after the release of the base installer. The interface has a few quirks, and provides no more than the bare minimum of controls, but is generally usable, and seemed to run without issues throughout testing.

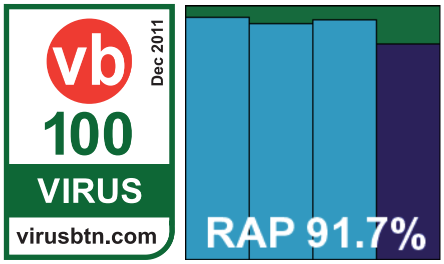
Speed tests showed scanning rates were nothing to write home about, but overheads were fairly light, and resource use on the low side, with good speed through our set of activities. Detection rates were pretty decent, a little unpredictable through the Response sets but fairly steady, and with no issues in the core sets a VB100 award is comfortably earned. This gives *Security Essentials* two passes from two entries in the last six tests; four passes from five entries with a single fail in the last two years. Testing revealed no issues, but took some time as usual, running for close to four full days.

## Nifty Corp. Security 24

Main version: 5.71

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

Shortly before finalizing this month's report, we heard that *Nifty* was not intending to participate in any more of our comparatives – news which was greeted with a certain amount of relief by the test team. Although the product is far from horrible, testing has invariably proved taxing, partly due to the lack of any translations from the original Japanese, but in the main thanks to inordinate slowness getting through the large jobs required by our testing system.



As usual, the installation process from the hefty 200MB package sent in was fraught with confusion, thanks to minimal rendering of characters in some places, but it seemed to run successfully, with a reboot taking us by surprise as ever. The interface is unusual to say the least, and we can't really comment on the depth of controls, but it seemed generally stable and responsive.

As anticipated, the RAP tests were extremely slow – taking over five days to complete a job some products managed in little over an hour. So far no explanation for this has emerged over several years of testing, the most convincing suggestion being something to do with the large amounts of data inserted into the *Windows* Event Logging system. Fortunately stability seemed sound, and results were gathered without undue effort after our long wait.

Other tests were much less strenuous, although on each reinstall running online updates took well over two hours – the distance of our test lab from the company's home market seems the most likely reason for this. Scanning speeds were decent, becoming much faster in the warm runs, while overheads were fairly light. Resource use was not excessive, and our set of tasks completed in good time. The Response tests again took much longer than we would like, more than 24 hours in each case, but further updates did not seem to be occurring automatically so the validity of the results should not have been compromised by this extreme lethargy. We also noted some extreme slowness in the clean sets, with .mshc help files taking an age to process.

Detection rates looked good, starting very strong and only tailing off a little into the proactive part of the RAP sets and the last few days of the Response test. With decent coverage of the WildList sets and no problems (other than the slowness) in the clean sets, *Nifty* earns another VB100 award on what is apparently its final visit to our test bench. The vendor's history is decent, although its entry rate is

| **Response tests** | Day-7 | Day-6 | Day-5 | Day-4 | Day-3 | Day-2 | Day-1 | Average |
|---|---|---|---|---|---|---|---|---|
| Agnitum Outpost | 76.0% | 76.2% | 80.1% | 80.6% | 65.6% | 68.9% | 59.1% | 72.4% |
| AhnLab V3 | 76.7% | 85.0% | 81.1% | 77.3% | 73.3% | 79.0% | 75.7% | 78.3% |
| Auslogics Antivirus | 98.7% | 99.3% | 99.4% | 99.2% | 98.6% | 99.0% | 98.9% | 99.0% |
| avast! Free Antivirus | 98.9% | 98.1% | 97.7% | 99.4% | 99.2% | 98.3% | 99.1% | 98.7% |
| AVG Internet Security | 97.9% | 98.8% | 98.6% | 98.1% | 97.4% | 97.0% | 95.8% | 97.7% |
| Avira AntiVir Free | 99.4% | 98.7% | 98.2% | 99.1% | 99.6% | 98.2% | 98.1% | 98.7% |
| Avira AntiVir Pro | 99.3% | 98.6% | 98.2% | 99.0% | 99.5% | 98.0% | 98.0% | 98.7% |
| BitDefender Antivirus Plus | 99.5% | 99.1% | 99.3% | 99.3% | 97.0% | 99.0% | 97.5% | 98.7% |
| BullGuard Antivirus 10 | 99.1% | 99.3% | 99.1% | 99.2% | 98.6% | 98.9% | 98.6% | 99.0% |
| Central Command Vexira | 78.2% | 77.8% | 83.3% | 79.5% | 54.5% | 64.9% | 63.5% | 71.7% |
| Clearsight Antivirus | 75.6% | 73.0% | 80.5% | 81.8% | 58.4% | 56.9% | 54.3% | 68.6% |
| Commtouch Command | 87.2% | 84.5% | 82.4% | 91.3% | 96.5% | 72.8% | 71.8% | 83.8% |
| Comodo Antivirus | 89.1% | 88.5% | 92.4% | 91.1% | 88.0% | 92.4% | 73.6% | 87.9% |
| Comodo Internet Security | 88.5% | 87.8% | 91.9% | 90.8% | 87.2% | 91.7% | 73.5% | 87.4% |
| Coranti 2012 | 96.8% | 99.2% | 99.0% | 98.0% | 97.1% | 97.6% | 96.2% | 97.7% |
| Coranti Cora Antivirus | 97.7% | 99.2% | 98.9% | 97.0% | 97.5% | 97.8% | 96.2% | 97.7% |
| Defenx Security Suite 2012 | 78.5% | 77.1% | 86.4% | 86.9% | 62.8% | 58.8% | 59.4% | 72.9% |
| Digital Defender | 76.8% | 74.4% | 77.1% | 79.9% | 75.1% | 50.7% | 58.9% | 70.4% |
| eEye Blink Professional | 88.2% | 87.0% | 85.9% | 76.8% | 94.2% | 93.4% | 86.1% | 87.4% |
| Emsisoft Anti-Malware | 99.6% | 99.9% | 99.7% | 99.6% | 99.7% | 98.4% | 99.8% | 99.5% |
| eScan Internet Security | 99.5% | 99.1% | 98.7% | 99.5% | 98.6% | 98.5% | 98.2% | 98.9% |
| ESET NOD32 Antivirus | 96.0% | 94.7% | 93.5% | 95.3% | 96.0% | 93.1% | 96.0% | 94.9% |
| ESTsoft ALYac | 70.0% | 71.6% | 65.3% | 70.1% | 77.6% | 70.0% | 54.4% | 68.4% |
| Filseclab Twister | 84.5% | 81.5% | 90.5% | 89.8% | 71.3% | 69.0% | 69.1% | 79.4% |
| Fortinet FortiClient | 97.0% | 95.6% | 93.0% | 91.6% | 94.5% | 89.8% | 72.8% | 90.6% |
| Frisk F-PROT | 60.8% | 66.8% | 59.3% | 62.2% | 73.2% | 75.8% | 68.9% | 66.7% |
| F-Secure Client Security | 99.4% | 99.2% | 99.5% | 98.8% | 99.0% | 98.8% | 97.8% | 92.0% |

(*Please refer to text for full product names.*)

| **Response tests contd.** | Day-7 | Day-6 | Day-5 | Day-4 | Day-3 | Day-2 | Day-1 | Average |
|---|---|---|---|---|---|---|---|---|
| G Data AntiVirus 2012 | 99.8% | 99.8% | 99.8% | 99.9% | 99.7% | 99.7% | 99.7% | 99.8% |
| GFI VIPRE Antivirus | 97.7% | 99.1% | 99.2% | 98.0% | 97.6% | 98.7% | 98.5% | 98.4% |
| Ikarus virus.utilities | 98.5% | 100.0% | 99.8% | 99.7% | 99.7% | 99.8% | 99.7% | 99.6% |
| Iolo System Shield | 64.4% | 72.5% | 73.0% | 52.7% | 52.2% | 49.7% | 61.7% | 60.9% |
| K7 Total Security | 94.0% | 94.0% | 94.3% | 95.6% | 90.1% | 88.5% | 87.6% | 92.0% |
| Kaspersky Endpoint Security 8 | 96.7% | 97.8% | 98.0% | 97.4% | 98.7% | 97.2% | 97.2% | 97.6% |
| Kaspersky Internet Security 2012 | 98.1% | 98.2% | 98.3% | 98.1% | 98.6% | 97.5% | 97.1% | 98.0% |
| Lavasoft Ad-Aware Total Security | 99.5% | 99.9% | 99.8% | 99.7% | 99.7% | 99.0% | 99.7% | 99.6% |
| McAfee VirusScan Enterprise | 92.9% | 92.0% | 85.6% | 83.7% | 89.1% | 83.5% | 64.0% | 84.4% |
| Microsoft Security Essentials | 92.9% | 89.5% | 87.7% | 89.0% | 93.3% | 90.0% | 91.6% | 90.6% |
| Nifty Security 24 | 98.0% | 95.9% | 97.8% | 97.3% | 98.0% | 95.7% | 89.0% | 96.0% |
| Norman Security Suite | 92.1% | 97.0% | 93.9% | 85.9% | 80.3% | 90.6% | 78.0% | 88.2% |
| PC Tools Internet Security | 76.6% | 81.9% | 87.3% | 84.5% | 75.3% | 69.1% | 72.6% | 78.2% |
| PC Tools Spyware Doctor | 76.6% | 81.9% | 87.3% | 84.7% | 75.3% | 69.1% | 72.6% | 78.2% |
| Preventon Antivirus | 76.8% | 74.4% | 77.1% | 79.9% | 75.1% | 50.7% | 58.9% | 70.4% |
| Qihoo 360 SD | 71.8% | 63.7% | 66.9% | 79.1% | 72.8% | 64.0% | 53.3% | 67.4% |
| Quick Heal Total Security 2012 | 64.7% | 75.7% | 54.5% | 68.9% | 55.9% | 46.7% | 51.8% | 59.7% |
| Returnil System Safe 2011 | 69.4% | 69.9% | 81.7% | 81.8% | 60.3% | 58.7% | 57.3% | 68.4% |
| Sophos Endpoint Security and Control | 95.5% | 93.3% | 93.3% | 94.0% | 92.4% | 93.3% | 76.5% | 91.2% |
| SPAMfighter VIRUSfighter PRO | 76.8% | 74.1% | 77.0% | 79.8% | 77.0% | 50.7% | 58.9% | 70.6% |
| Symantec Norton Internet Security | 86.2% | 95.1% | 90.1% | 89.5% | 81.0% | 90.7% | 74.7% | 80.0% |
| Total Defense Inc. ISS Plus | 92.9% | 82.1% | 92.3% | 91.6% | 88.7% | 95.1% | 93.0% | 90.8% |
| Total Defense Inc. Total Defense r12 | 75.4% | 93.3% | 85.9% | 79.7% | 92.4% | 90.2% | 77.6% | 66.5% |
| TrustPort Antivirus 2012 | 99.9% | 99.8% | 99.8% | 99.8% | 99.6% | 99.8% | 99.8% | 99.8% |
| UtilTool Antivirus | 75.9% | 73.2% | 80.6% | 81.9% | 61.7% | 59.2% | 55.4% | 69.7% |
| VirusBuster Professional | 79.4% | 78.3% | 74.7% | 75.6% | 81.4% | 76.8% | 38.6% | 72.1% |
| Webroot SecureAnywhere | 33.0% | 54.8% | 25.4% | 27.6% | 18.3% | 18.3% | 20.6% | 28.3% |

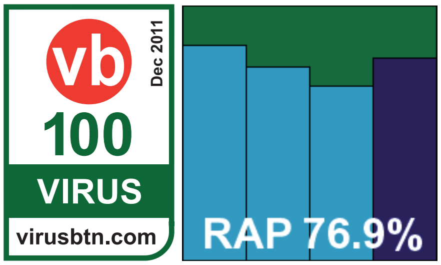
*(Please refer to text for full product names.)*

rather sporadic, with two passes from two attempts in the last six tests; four passes from five entries with a single fail in the last two years. With the extreme length of scans of infected sets and in some parts of the clean sets, testing took close to 15 full days.

## Norman Security Suite

Main version: 9.00

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*Norman* also has a history of taking quite some time to complete our tests, although in this case the reason is more obvious, with the company's renowned *Sandbox* system running deep analysis of unknown items. The installer was a reasonable size at 153MB with all updates included, and installed fairly speedily with little effort, requiring a reboot to complete. Updates were generally speedy too, averaging just seven minutes, although some of them required a further update to apply fully.

The interface is a little improved, with a clearer layout and slightly better stability, although it remains prone to periods of unresponsiveness, occasionally blurring out and losing important sections of controls. It also continues to defy its own logic, repeatedly disinfecting or quarantining items despite settings clearly having been changed to deny it this right. While such behaviour may be acceptable to home users, most enterprises will probably require more reliability and trustworthiness from their solutions.

As expected, testing was a long, slow process, with scans of both infected sets and clean sets crawling along. Speed measures were slow, but showed some notable improvement on repeat runs, which was pleasing. Overheads were high, but resource use was not too excessive, and our set of tasks did not take too much longer.

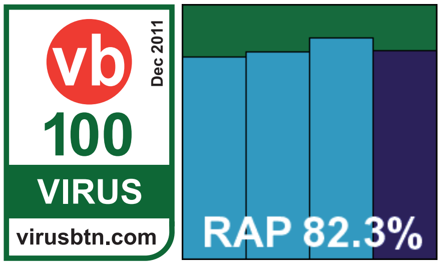
Detection rates were a little below par but showed some improvement over recent tests, and the Response test showed good scores, tailing off a little into the later few days. The WildList was properly covered, and with no false positives to report a VB100 award is earned.

The product's test history is pretty decent of late, with five passes and a single fail in the last six tests. Longer term, things are a little more uneven with seven passes and four fails in the last two years. Testing highlighted a handful of problems with the interface, notably the proper application of settings, but also some stability issues, and scanning was rather slow, meaning that testing took around five full days to complete.

## PC Tools Internet Security

Main version: 8.0.0.662

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



*PC Tools* returns to our test bench with its usual brace of submissions, the suite product coming up first alphabetically. The installer submitted was a fair size at 240MB, but set-up was fairly speedy, completing in a couple of minutes with just a few clicks and no need to reboot. Updates were not too sluggish either, generally taking 10–15 minutes in total, with some instances requiring a reboot half-way through the process.

The interface is bright and colourful, and seemed generally stable and responsive, but the layout can be confusing and little actual configuration is available beyond the very basic requirements. Logging has long been somewhat problematic in our tests, and a special tool was provided to ensure that logs were not removed from the local system on completion of each job.

Scanning speeds were fairly decent to start with and well optimized in the warm runs, with on-access lag times very light, especially after some familiarization with the system. Resource use was a little high, though, and our set of tasks took some time to complete.

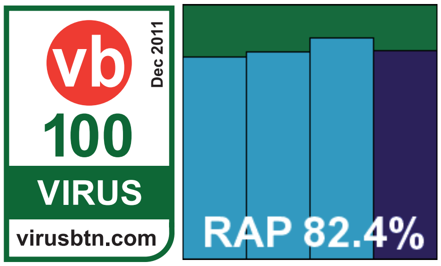
Detection rates were reasonable if uninspiring, and the clean sets were handled well. WildList scores seemed solid, although in one run a single item appeared to have been missed. On closer examination, this was found to be due to our failure to apply a licence to the product, causing it to run in trial mode with some features disabled. Re-running the test with the product fully active showed no problems, and a VB100 award is duly earned.

Entering only on desktop platforms, this suite edition has achieved two passes from three attempts in the last six tests; five from six in the last two years. Testing ran at a good speed, completing in around the two days allotted.

## PC Tools Spyware Doctor with AntiVirus

Main version: 8.0.0.662

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



The classic *Spyware Doctor* product is pretty similar to the suite these days, with only the lack of a firewall to distinguish it. The install package submitted was a little smaller, at 220MB, and again ran through smoothly and swiftly, completing in a couple of minutes with no need to restart. Again we noted some oddities in the update system, with one run downloading over 150MB of data, then requesting a reboot, following which it insisted that another update – also measuring 150MB – was required. Nevertheless, these tasks ran quickly, completing in less than 15 minutes even when it seemed that some work was duplicated.

On starting the product up, an initial scan reported a handful of threats, but these turned out to be ‘tracking cookies’ dropped on the machine when *Internet Explorer* was run to check connectivity prior to activation – it seems that *PC Tools* finds some of the activities of the browser’s default MSN.com homepage somewhat suspicious.

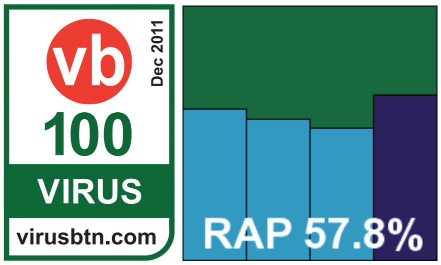
The interface is again a little quirky and lacking in fine-tuning, but seemed to operate well under pressure. Our tests were completed in good time, with good speed-ups in the warm runs helping things along nicely. On-access lags were low again, but resource use a little above average, with a fair impact on our set of activities.

Scores were respectable if a little uneven, and with the core sets properly handled another VB100 award is earned by *PC Tools* this month. Like the suite edition, the *Spyware Doctor* product only appears in desktop tests, and thus has two passes from three entries in the last six tests; five from six in the last two years. No issues were noted in testing, which completed in around two days as hoped.

## Preventon Antivirus

Main version: 5.0.2.9

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 0 | | |



The progenitor of several entries already covered this month, given the issues observed with those, we expected problems for *Preventon*. Installation from the 72MB package submitted was quick and simple, with no reboot needed, and updates were also fast, taking only a few minutes. The interface has had a minor revamp, but remains simple, clear and fairly usable, with a good basic set of controls. As usual, logging is a little odd, dumping large amounts of data to log by default, but capping log sizes and dumping old information very frequently. Registry tweaks were required to prevent this loss of data.

Speed tests showed some reasonable scan times, with on-access lags a little on the high side, high use of both RAM and CPU, and a medium impact on our set of activities. Detection scores were fairly mediocre, with the expected freezes in the infected sets meaning that much of the work had to be done on access, with settings tweaked to match the on-demand scanner. The core sets were properly handled though, and a VB100 award is duly granted.

It has been a solid year for *Preventon*, with five passes from five entries in the last six tests, only our annual *Linux* comparative being skipped. The two-year view shows six passes and two fails from eight attempts. With problems handling a large number of malicious samples in our sets and several repeat runs being needed, testing took close to four days to complete, almost double the time scheduled.

## Qihoo 360 SD

Main version: 3.0.1.2102

| | | | |
|---|---|---|---|
| **ItW Std** | 99.40% | **ItW Std (o/a)** | 99.67% |
| **ItW Extd** | 98.97% | **ItW Extd (o/a)** | 92.71% |
| **False positives** | 0 | | |

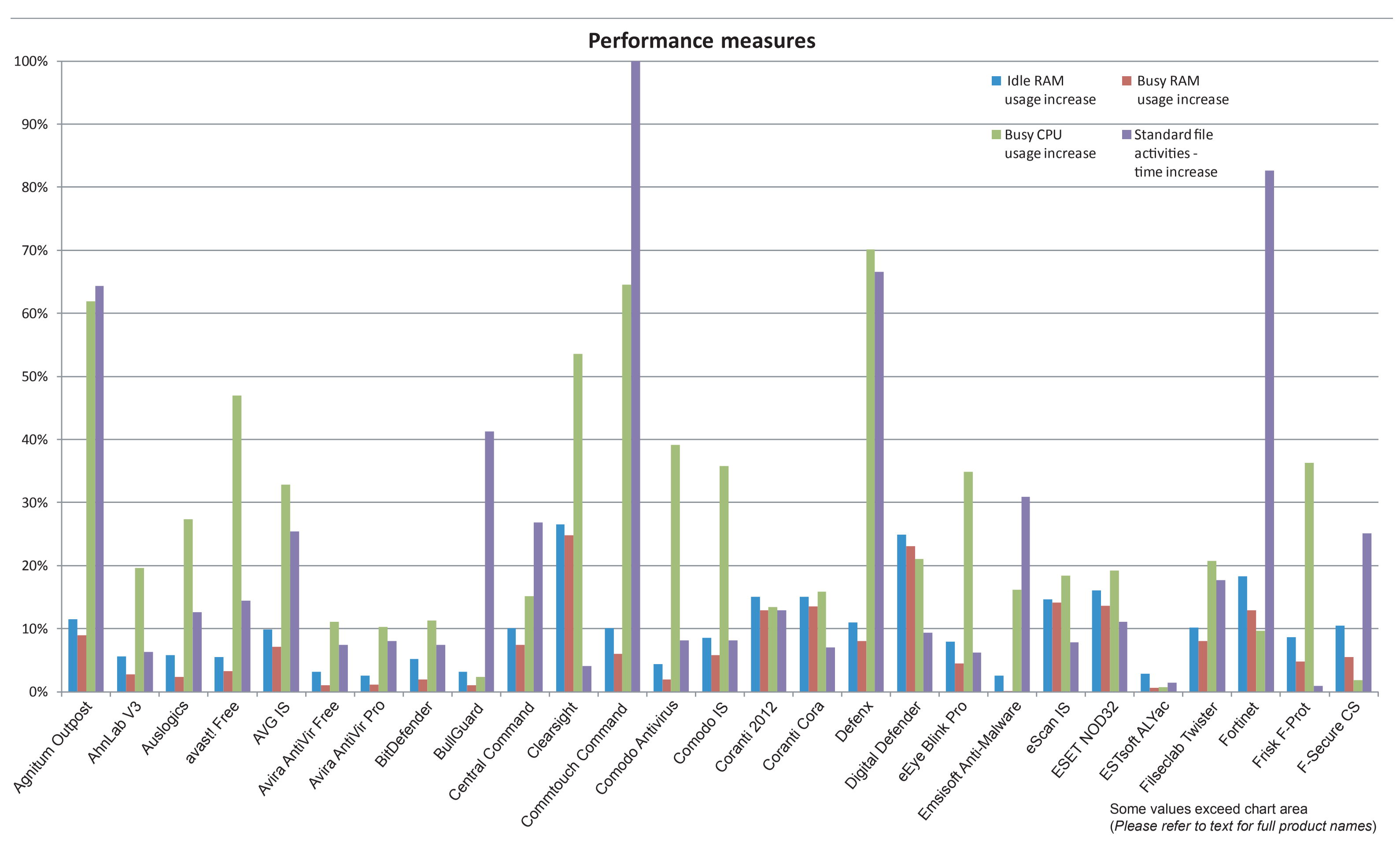
China’s *Qihoo* has become a regular participant in our tests, raising some eyebrows from time to time with its

| **Performance measures** | Idle RAM usage increase | Busy RAM usage increase | Busy CPU usage increase | Standard file activities - time increase |
|---|---|---|---|---|
| Agnitum Outpost | 11.44% | 9.00% | 61.94% | 64.37% |
| AhnLab V3 | 5.58% | 2.70% | 19.58% | 6.30% |
| Auslogics Antivirus | 5.80% | 2.39% | 27.38% | 12.57% |
| avast! Free Antivirus | 5.50% | 3.21% | 46.96% | 14.47% |
| AVG Internet Security | 9.85% | 7.15% | 32.83% | 25.42% |
| Avira AntiVir Free | 3.20% | 1.06% | 11.07% | 7.43% |
| Avira AntiVir Pro | 2.55% | 1.09% | 10.32% | 8.03% |
| BitDefender Antivirus Plus | 5.17% | 1.95% | 11.33% | 7.43% |
| BullGuard Antivirus 10 | 3.17% | 0.99% | 2.33% | 41.29% |
| Central Command Vexira | 10.11% | 7.39% | 15.18% | 26.80% |
| Clearsight Antivirus | 26.53% | 24.80% | 53.54% | 4.03% |
| Commtouch Command | 10.11% | 6.01% | 64.58% | 111.55% |
| Comodo Antivirus | 4.40% | 1.93% | 39.11% | 8.11% |
| Comodo Internet Security | 8.58% | 5.76% | 35.74% | 8.17% |
| Coranti 2012 | 15.04% | 12.96% | 13.42% | 12.87% |
| Coranti Cora Antivirus | 15.02% | 13.56% | 15.89% | 6.98% |
| Defenx Security Suite 2012 | 11.00% | 8.08% | 70.11% | 66.61% |
| Digital Defender | 24.87% | 23.11% | 21.00% | 9.40% |
| eEye Blink Professional | 7.93% | 4.43% | 34.82% | 6.25% |
| Emsisoft Anti-Malware | 2.53% | 0.02% | 16.12% | 30.95% |
| eScan Internet Security | 14.63% | 14.10% | 18.37% | 7.86% |
| ESET NOD32 Antivirus | 16.09% | 13.67% | 19.24% | 11.07% |
| ESTsoft ALYac | 2.86% | 0.60% | 0.72% | 1.41% |
| Filseclab Twister | 10.16% | 8.01% | 20.69% | 17.73% |
| Fortinet FortiClient | 18.29% | 12.87% | 9.62% | 82.67% |
| Frisk F-PROT | 8.69% | 4.80% | 36.29% | 0.87% |
| F-Secure Client Security | 10.50% | 5.51% | 1.83% | 25.10% |

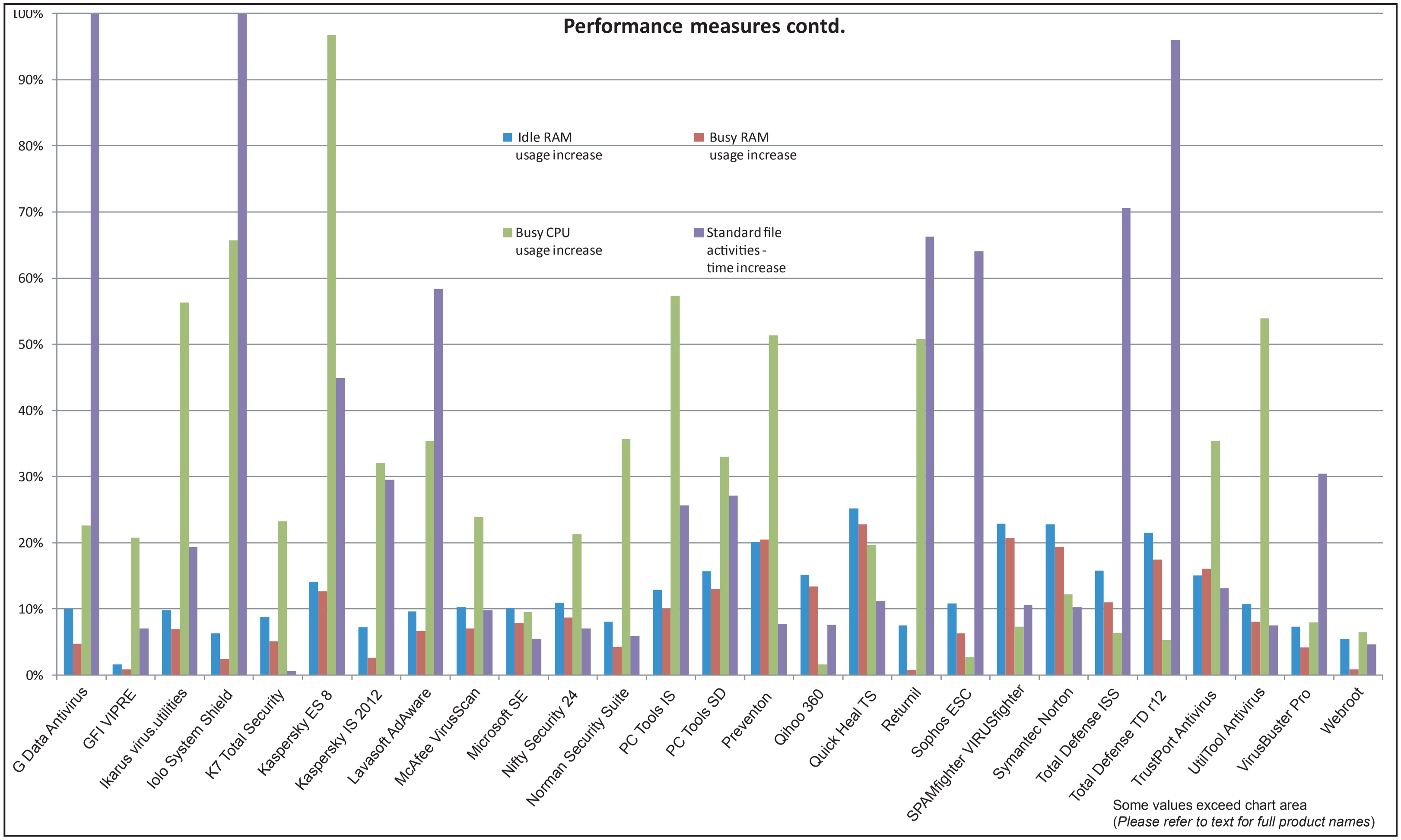
*(Please refer to text for full product names.)*

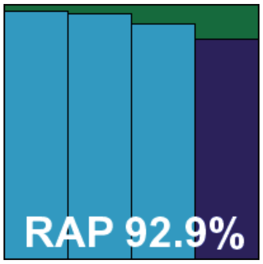
| **Performance measures contd.** | Idle RAM usage increase | Busy RAM usage increase | Busy CPU usage increase | Standard file activities - time increase |
|---|---|---|---|---|
| G Data AntiVirus 2012 | 10.02% | 4.72% | 22.64% | 161.37% |
| GFI VIPRE Antivirus | 1.65% | 0.90% | 20.79% | 7.08% |
| Ikarus virus.utilities | 9.84% | 6.94% | 56.35% | 19.37% |
| Iolo System Shield | 6.34% | 2.41% | 65.74% | 115.51% |
| K7 Total Security | 8.78% | 5.16% | 23.22% | 0.57% |
| Kaspersky ES 8 | 14.07% | 12.71% | 96.71% | 44.93% |
| Kaspersky IS 2012 | 7.20% | 2.66% | 32.09% | 29.54% |
| Lavasoft Ad-Aware Total Security | 9.65% | 6.69% | 35.45% | 58.32% |
| McAfee VirusScan | 10.24% | 7.09% | 23.88% | 9.78% |
| Microsoft SE | 10.18% | 7.88% | 9.49% | 5.45% |
| Nifty Security 24 | 10.89% | 8.67% | 21.31% | 7.04% |
| Norman Security Suite | 8.03% | 4.29% | 35.68% | 5.95% |
| PC Tools IS | 12.86% | 10.03% | 57.32% | 25.64% |
| PC Tools SD | 15.71% | 12.99% | 33.00% | 27.13% |
| Preventon Antivirus | 20.16% | 20.46% | 51.35% | 7.72% |
| Qihoo 360 SD | 15.20% | 13.44% | 1.57% | 7.64% |
| Quick Heal TS 2012 | 25.16% | 22.77% | 19.71% | 11.20% |
| Returnil System Safe | 7.48% | 0.81% | 50.75% | 66.27% |
| Sophos ESC | 10.82% | 6.30% | 2.71% | 64.09% |
| SPAMfighter VIRUSfighter PRO | 22.93% | 20.65% | 7.29% | 10.60% |
| Symantec Norton IS | 22.79% | 19.42% | 12.19% | 10.24% |
| Total Defense ISS Plus | 15.78% | 11.04% | 6.39% | 70.62% |
| Total Defense TD r12 | 21.50% | 17.44% | 5.33% | 95.99% |
| TrustPort Antivirus | 15.02% | 16.12% | 35.38% | 13.10% |
| UtilTool Antivirus | 10.72% | 8.06% | 53.95% | 7.52% |
| VirusBuster Pro | 7.29% | 4.19% | 8.00% | 30.43% |
| Webroot SecureAnywhere | 5.50% | 0.91% | 6.49% | 4.68% |

*(Please refer to text for full product names.)*



Some values exceed chart area
(*Please refer to text for full product names*)


Performance measures contd.
Idle RAM usage increase
Busy RAM usage increase
Busy CPU usage increase
Standard file activities - time increase
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
G Data Antivirus
GFI VIPRE
Ikarus virus.utilities
Iolo System Shield
K7 Total Security
Kaspersky ES 8
Kaspersky IS 2012
Lavasoft AdAware
McAfee VirusScan
Microsoft SE
Nifty Security 24
Norman Security Suite
PC Tools IS
PC Tools SD
Preventon
Qihoo 360
Quick Heal TS
Returnil
Sophos ESC
SPAMfighter VIRUSfighter
Symantec Norton
Total Defense ISS
Total Defense TD r12
TrustPort Antivirus
UtilTool Antivirus
VirusBuster Pro
Webroot
Some values exceed chart area
(Please refer to text for full product names)



many quirks but generally doing well thanks to the underlying *BitDefender* engine. The 156MB installer needed only a single click to get going, with the EULA available but not displayed by default, and no reboot was needed to complete. Updates averaged around 10 minutes, a pretty good showing given the lab's distance from the product's main market space.

The interface is clear and simple, and provides a decent level of options (although some of them can be a little tricky to decipher thanks to some quirky translations). Scanning speeds were pretty slow, but overheads were light, and while RAM use was a little above average, CPU use was barely noticeable and our set of tasks ran through at lightning speed. As previously observed, on-access protection does not appear to function in the normal fashion on read, or indeed on write, with detections alerted on but actions not blocked (in real time at least). Pop-ups insisted that access to items had been denied, but they seemed accessible and could even be copied around the system at first.

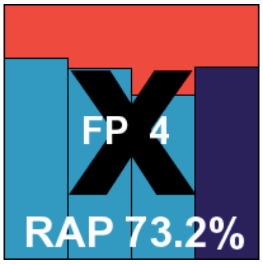
Pop-ups and log entries also took some time to appear – more than 12 hours in some cases – making accurate detection testing rather difficult. On-demand work was a little easier, but not always reliable. Scores were solid in the RAP sets, dropping slightly into the proactive week, with Response test scores notably lower than expected but still respectable. The clean sets were handled well, but coverage of the WildList sets proved highly uneven, and complete coverage could not be achieved despite repeated attempts. Thus *Qihoo* is denied VB100 certification this month.

The vendor now has two passes and one fail in the last six tests; five passes and two fails in the last two years. With the product's decidedly odd approach to protection, the difficulties this caused in measuring detection rates, and a couple of crashes running on-demand scans, testing took five days to complete.

## Quick Heal Total Security 2012

Main version: 13.00 (6.0.0.1)

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 99.73% | **ItW Extd (o/a)** | 99.73% |
| **False positives** | 4 | | |



One of our hard-core regulars, *Quick Heal* is more or less a fixture on the test bench, and the latest product came as a fairly large 276MB installer. Set-up was simple and speedy, and updates also rapid, completing in around three minutes on average. No reboots were required.

The interface is glossy, attractive and easy to use and provides a wealth of fine-tuning in a very accessible format. Testing ran through rapidly and the product was stable throughout, with decent scanning speeds, medium lag times, above average use of RAM but acceptable CPU drain and a decent amount of time taken to get through our set of tasks. Detection rates were somewhat mediocre, including in the Extended WildList where a handful of items went undetected. With a handful of false positives also noted in the clean sets, *Quick Heal* is denied certification this month.

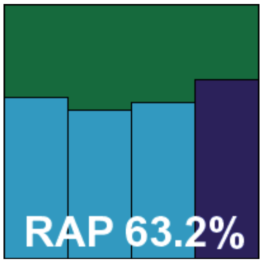
This breaks an impressive run of success for the company, leaving it with five passes from six attempts in the last six tests; ten from 12 in the last two years. Stability was solid and speeds decent, and testing completed in well under the two days allotted.

## Returnil System Safe 2011

Main version: 3.2.12471.5765-REL13

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.60% |
| **False positives** | 0 | | |

vb 100 VIRUS virusbtn.com Dec 2011



*Returnil*'s offerings have become fairly regular of late. Their main feature is a reversion system to undo unwanted changes, but anti-malware functionality is provided based, ultimately, on the *Frisk* engine. The installer is compact at 38MB, with an additional 28MB of updates. The set-up process has a number of stages but completes in good time, requesting a reboot at the end. Online updates generally took only a few minutes, but on one occasion a full product update was required, which took closer to 25 minutes.

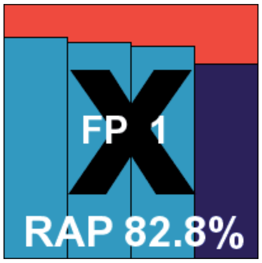
The GUI is clear and straightforward, with a basic range of options. It operated smoothly, generally remaining stable under pressure, although on one occasion a scan of the local system drive failed with a less than helpful error message. The product demonstrated reasonable scanning speeds, slightly high overheads, low use of RAM, but high CPU use and a heavy impact on our suite of standard activities. Detection rates were disappointing, tailing off noticeably in the more recent parts of the Response sets, but the core sets were handled well, with no misses in the WildList sets and a clean run through each part of the clean sets, earning *Returnil* another VB100 award.

The vendor's history shows a rather erratic pattern of late, with three passes and two fails from five entries in the last six tests; five passes from eight attempts in the last two years. Testing was relatively straightforward with only a single unexpected error, which was easily recovered from, and everything completed in just a little over 48 hours.

## Sophos Endpoint Security and Control

Main version: 9.7

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 99.96% | **ItW Extd (o/a)** | 99.96% |
| **False positives** | 1 | | |



Another stalwart of our tests, there have been few comparatives without a submission from *Sophos*. This month's submission weighed in at 93MB, with offline updates measuring only a few hundred KB. The installation process has a little more to it than the average home-user product, as one would expect from a corporate solution like this. No reboot is needed to complete though, and online updates generally only took a few minutes, with again no need to restart on any of the runs.

The interface is stern and businesslike, providing an epic range of fine-tuning for those keen to meddle with the sensible defaults. Stability was generally good, but in the RAP sets a number of samples seemed to snag the scanning process, leaving it sitting still for hours at a time and needing the service to be forcibly stopped to allow the scan window to be closed. Plodding slowly through the sets removing samples eventually got us through the tests, and subsequent analyses showed the issue to have been caused by a rogue identity – this was easily fixed, which rendered retesting considerably easier.

In the end, scores were a little underwhelming in the RAP sets, but much better in the Response sets where the company's 'live protection' cloud look-up system came into play; only the most recent day showed any downturn in coverage. Moving onto the core sets, in the clean sets a single item, a USB driver from a set-up CD accompanying a webcam, was mislabelled as generic malware, while in the WildList sets the performance was marred by a single item not alerted on in one of the three runs. This double-whammy of surprise means no VB100 award for *Sophos* this month.

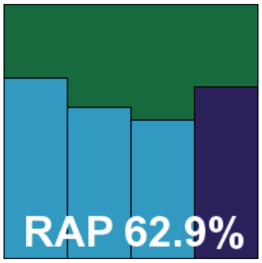
This upset brings to an end a long run of passes for *Sophos*, leaving the vendor with five passes and one fail from the last six tests; 11 passes in the last two years. The issues in the RAP sets gave us a lot of extra work, with several retries and some labour-intensive picking through of the sets meaning more than ten full days of system time were devoted to obtaining a full set of data.

## SPAMfighter VIRUSfighter

Main version: 7.0.267

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 0 | | |

vb Dec 2011 100 VIRUS virusbtn.com



Another *Preventon*-based product, *SPAMfighter*'s *VIRUSfighter* is a little different from its stablemates, putting a little more of its own work into the design and layout of the interface, but the installer is much the same size at 72MB. The installation process is similarly short and snappy, with minimal interaction, and all is completed in under a minute with no need to reboot.

The GUI is clear and follows standard practices, providing a decent basic set of controls. Once again though, logging is an issue, with no clear way of avoiding old data being discarded and registry tweaks needed to prevent every file visited being noted down in the log as 'OK'. We also experienced some issues with the scanner interfaces, which would routinely claim to be busy working when scans had long since completed, and on one occasion a scan of our set of archive files crashed completely, rebooting the system.

Progress through the RAP sets was, as expected, slow and riddled with issues, with large numbers of files causing the scanner to stumble. Here, even the on-access component seemed prone to tripping up. Results were thus a little

| **Reactive And Proactive (RAP) scores** | VB100 | Reactive | | | Reactive average | Proactive | Overall average |
|---|---|---|---|---|---|---|---|
| | | Week -3 | Week -2 | Week -1 | | Week +1 | |
| Agnitum Outpost* | VIRUS 100 | 70.14% | 70.40% | 60.05% | 66.86% | 70.67% | 67.82% |
| AhnLab V3 | | 73.18% | 69.86% | 68.12% | 70.38% | 76.92% | 72.02% |
| Auslogics Antivirus | VIRUS 100 | 98.90% | 98.56% | 97.21% | 98.22% | 91.67% | 96.59% |
| avast! Free Antivirus | | 98.01% | 96.40% | 92.16% | 95.52% | 84.46% | 92.76% |
| AVG Internet Security | VIRUS 100 | 96.43% | 92.65% | 93.57% | 94.22% | 81.35% | 91.00% |
| Avira AntiVir Free | VIRUS 100 | 99.07% | 97.37% | 96.52% | 97.65% | 90.25% | 95.80% |
| Avira AntiVir Pro | VIRUS 100 | 98.84% | 97.18% | 96.27% | 97.43% | 90.02% | 95.58% |
| BitDefender Antivirus Plus | VIRUS 100 | 99.20% | 98.75% | 97.40% | 98.45% | 91.74% | 96.77% |
| BullGuard Antivirus 10 | VIRUS 100 | 99.08% | 98.64% | 97.21% | 98.31% | 91.31% | 96.56% |
| Central Command Vexira | | N/T | N/T | N/T | N/T | N/T | N/T |
| Clearsight Antivirus * | VIRUS 100 | 64.19% | 53.87% | 53.28% | 57.11% | 66.32% | 59.41% |
| Commtouch Command | | 62.21% | 57.33% | 60.65% | 60.06% | 69.99% | 62.55% |
| Comodo Antivirus | | 79.56% | 68.51% | 64.96% | 71.01% | 63.97% | 69.25% |
| Comodo Internet Security | | 79.56% | 68.50% | 64.95% | 71.00% | 63.97% | 69.24% |
| Coranti 2012 | VIRUS 100 | 99.30% | 99.08% | 98.55% | 98.98% | 93.04% | 97.49% |
| Coranti Cora Antivirus | VIRUS 100 | 99.36% | 99.12% | 98.59% | 99.02% | 93.09% | 97.54% |
| Defenx Security Suite 2012 * | VIRUS 100 | 66.15% | 57.18% | 62.32% | 61.88% | 68.17% | 63.46% |
| Digital Defender * | VIRUS 100 | 60.29% | 59.77% | 55.41% | 58.49% | 65.09% | 60.14% |
| eEye Blink Professional | VIRUS 100 | 85.53% | 79.48% | 75.00% | 80.00% | 80.26% | 80.07% |
| Emsisoft Anti-Malware | | 98.37% | 97.94% | 99.66% | 98.66% | 98.17% | 98.53% |
| eScan Internet Security | VIRUS 100 | 99.07% | 98.63% | 96.99% | 98.23% | 91.27% | 96.49% |
| ESET NOD32 Antivirus | VIRUS 100 | 96.99% | 95.38% | 93.56% | 95.31% | 86.45% | 93.09% |
| ESTsoft ALYac | VIRUS 100 | 98.76% | 97.86% | 93.38% | 96.67% | 87.42% | 94.36% |
| Filseclab Twister | | 88.21% | 80.13% | 78.87% | 82.40% | 72.02% | 79.81% |
| Fortinet FortiClient | VIRUS 100 | 91.92% | 89.19% | 94.48% | 91.87% | 85.70% | 90.33% |
| Frisk F-PROT | VIRUS 100 | 56.04% | 48.90% | 52.65% | 52.53% | 68.29% | 56.47% |
| F-Secure Client Security | VIRUS 100 | 99.04% | 98.52% | 95.85% | 97.80% | 90.42% | 95.96% |

Key:

N/A – Not applicable.

N/T – Not testable.

* Problems gathering data .

(*Please refer to text for full product names.*)

| **Reactive And Proactive (RAP) scores contd.** | VB100 | Reactive | | | Reactive average | Proactive | Overall average |
|---|---|---|---|---|---|---|---|
| | | Week -3 | Week -2 | Week -1 | | Week +1 | |
| G Data AntiVirus 2012 | VIRUS 100 | 99.89% | 99.65% | 97.24% | 98.93% | 92.12% | 97.23% |
| GFI VIPRE Antivirus | | 98.32% | 97.96% | 94.08% | 96.78% | 81.37% | 92.93% |
| Ikarus virus.utilities | | 98.15% | 96.82% | 95.30% | 96.76% | 88.29% | 94.64% |
| Iolo System Shield | | 53.23% | 46.51% | 50.20% | 49.98% | 65.29% | 53.81% |
| K7 Total Security | VIRUS 100 | 86.17% | 82.96% | 82.61% | 83.91% | 71.31% | 80.76% |
| Kaspersky Endpoint Security 8 | VIRUS 100 | 96.36% | 93.56% | 96.23% | 95.38% | 86.94% | 93.27% |
| Kaspersky Internet Security 2012 | VIRUS 100 | 95.67% | 93.38% | 96.06% | 95.04% | 86.77% | 92.97% |
| Lavasoft Ad-Aware Total Security | VIRUS 100 | 99.88% | 99.73% | 97.29% | 98.97% | 91.99% | 97.22% |
| McAfee VirusScan Enterprise | VIRUS 100 | 84.80% | 77.36% | 69.75% | 77.30% | 78.25% | 77.54% |
| Microsoft Security Essentials | VIRUS 100 | 92.05% | 88.47% | 75.66% | 85.39% | 78.07% | 83.56% |
| Nifty Security 24 | VIRUS 100 | 95.04% | 92.51% | 94.05% | 93.87% | 85.06% | 91.67% |
| Norman Security Suite | VIRUS 100 | 84.46% | 75.69% | 68.15% | 76.10% | 79.16% | 76.86% |
| PC Tools Internet Security | VIRUS 100 | 79.39% | 81.11% | 86.94% | 82.48% | 81.85% | 82.32% |
| PC Tools Spyware Doctor | VIRUS 100 | 79.45% | 81.18% | 87.00% | 82.54% | 81.90% | 82.38% |
| Preventon Antivirus* | VIRUS 100 | 59.43% | 55.14% | 51.82% | 55.46% | 64.97% | 57.84% |
| Qihoo 360 SD | | 97.01% | 96.13% | 92.24% | 95.13% | 86.26% | 92.91% |
| Quick Heal Total Security 2012 | | 78.58% | 74.83% | 64.26% | 72.56% | 75.22% | 73.22% |
| Returnil System Safe 2011 | VIRUS 100 | 63.26% | 58.17% | 61.01% | 60.81% | 70.22% | 63.16% |
| Sophos Endpoint Security and Control* | | 86.75% | 84.57% | 83.50% | 84.94% | 76.41% | 82.81% |
| SPAMfighter VIRUSfighter PRO* | VIRUS 100 | 70.92% | 59.07% | 54.24% | 61.41% | 67.22% | 62.86% |
| Symantec Norton Internet Security | | N/A | N/A | N/A | N/A | N/A | N/A |
| Total Defense Inc ISS Plus | | 70.55% | 64.66% | 60.29% | 65.17% | 63.29% | 64.70% |
| Total Defense Inc Total Defense r12 | | 69.59% | 63.74% | 59.70% | 64.34% | 61.61% | 63.66% |
| TrustPort Antivirus 2012 | VIRUS 100 | 99.56% | 99.45% | 95.73% | 98.25% | 91.14% | 96.47% |
| UtilTool Antivirus* | | 59.40% | 62.87% | 49.70% | 57.32% | 31.65% | 50.91% |
| VirusBuster Professional | VIRUS 100 | N/T | N/T | N/T | N/T | N/T | N/T |
| Webroot SecureAnywhere | | N/A | N/A | N/A | N/A | N/A | N/A |

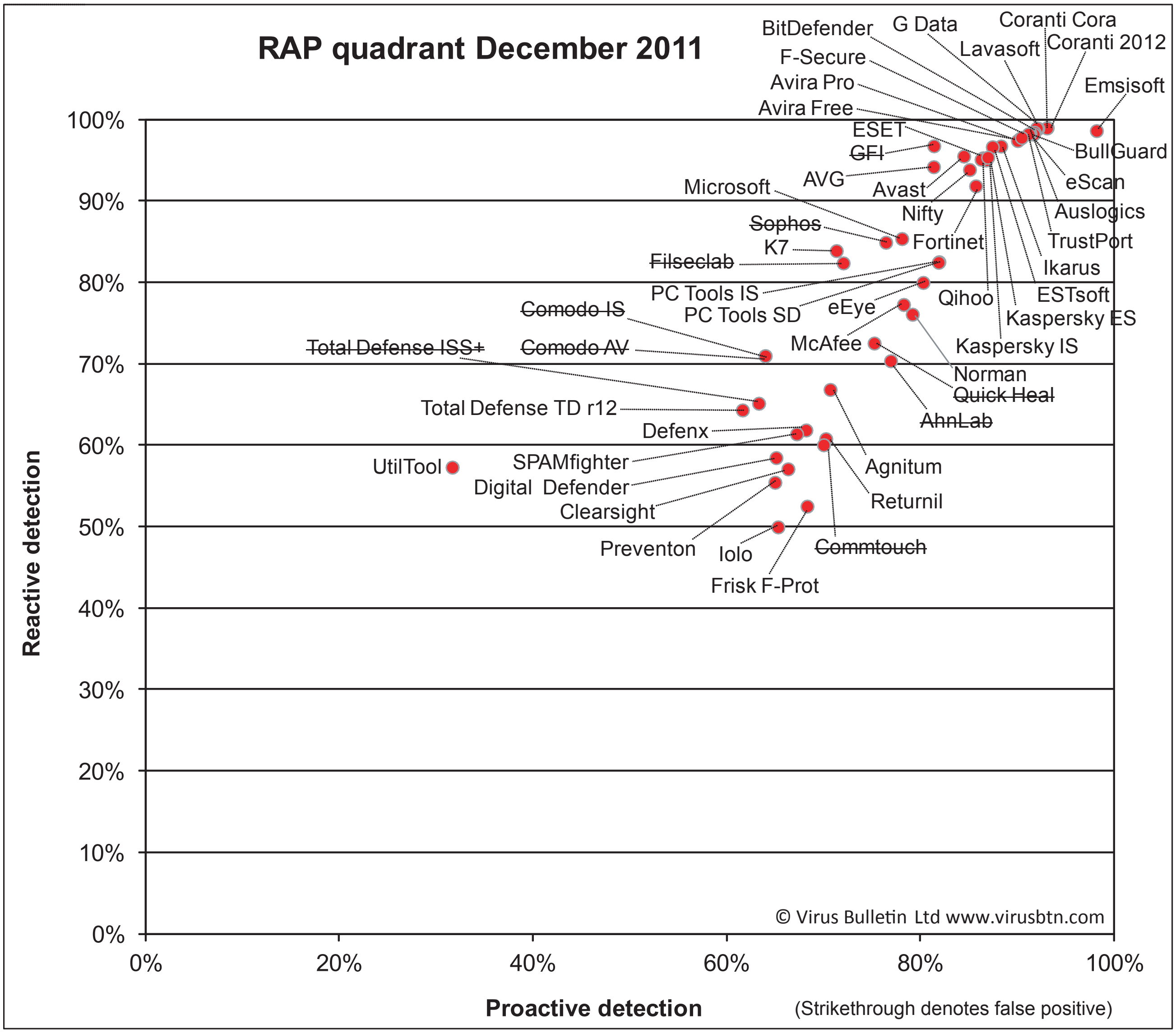
Key:

N/A – Not applicable.

N/T – Not testable.

* Problems gathering data.

(*Please refer to text for full product names.*)



unreliable, but showed more or less the expected levels: fairly disappointing in general, with the same rather odd upturn in the proactive week. Response scores were a little more encouraging in the earlier days, but tailed off rather in the last two days. The core sets were well handled though, meeting our requirements in the WildList sets and not turning up any false alarms in the clean sets, and thus a VB100 award is earned.

This gives *SPAMfighter* an impressive five passes from five attempts in the last six tests (no *Linux* product being available); longer term things are less assured, with six passes and three fails from nine entries in the last two years.

With a number of issues noted, testing took up one of our test systems for more than eight days in total.

### Symantec Norton Internet Security

Main version: 19.1.0.28

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 99.93% | **ItW Extd (o/a)** | 99.93% |
| **False positives** | 0 | | |

*Symantec* has become something of a stranger on the test bench recently, with its previous near-constant appearances dwindling to only a handful in the last couple of years. We hoped our new approach would tempt the vendor back, giving its developers the opportunity to show off their cloud reputation system and for us to measure the anticipated improvements in detection rates this would provide. The *Norton* home-user product is the clear market leader, and it was a considerable pleasure to see it on the test bench once again.

The package provided measured 106MB and installed reasonably simply, with good clear information. It was set up and updated in good order on the deadline day, although this proved an unnecessary step as the developers decided to withdraw from the RAP tests on the grounds that, without the cloud connection, these would not show the full capabilities of the product. Later updates were more troublesome, downloading over 140MB of data each time and taking around 20 minutes to complete on average; one run lingered for over an hour, then announced it had failed and would need to be re-run.

The interface is slick and stylish, and provides an impressive range of controls. While a little complex, it is fairly easy to navigate and operate, and seemed to remain stable under pressure. Speed tests ran through at a splendid pace, and the warm sets were powered through at lightning speed, while on-access overheads were very reasonable. RAM use was perhaps a little above average, but CPU use was fairly low and our set of activities completed in very good time.

Lacking any RAP results to refer to, scores in the Response test looked pretty decent, tailing off a little in the most recent day only, but this data was a little pesky to gather, with large scans taking a long time to complete and on several occasions dying with no results reported. Several retries were needed to obtain the full set of data.

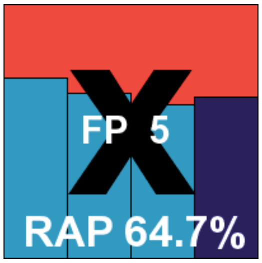
The clean sets were handled without incident, as was the standard WildList set with its large number of polymorphic samples, but in the Extended set a single item went undetected on each of the three runs. Surprised by this, we retested the sample against the version installed and updated on the deadline day, and saw that it was alerted on and labelled a high-risk trojan. On analysing the file with the product's built-in 'Insight' look-up option, it was reported as 'Trusted' by the cloud community. We queried this with the developers and it emerged that the sample in question had been labelled a false positive by another third-party test lab, causing the developers to label it as trusted despite its inclusion on the WildList and general agreement that it was malicious. At a later date this decision was reversed and detection was added back in for the sample, but for a period of at least several weeks while our tests were under way, it was flagged as trusted. This was enough to deny *Symantec* a VB100 award this month.

With only rare appearances of late, the company now has one pass and one fail from two entries in the last six tests; three passes from four attempts in the last two years. Problems handling our large infected sets and the subsequent re-runs meant testing took around five full days of system time in total.

## Total Defense Inc. Internet Security Suite Plus

Main version: 7.0.0.279

| | | | |
|---|---|---|---|
| **ItW Std** | 99.99% | **ItW Std (o/a)** | 99.99% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 5 | | |



The consumer offering from *Total Defense* is another part-timer, entered only into our desktop comparatives. As usual, set-up was run on the deadline day and images recorded for later testing. The initial set-up was fairly simple, with just a couple of steps including a quick initial scan, before a reboot was required. Then the activation process was run, gathering a fair amount of personal data, and updates zipped through in just a couple of minutes – which proved to be the average for subsequent runs as well.

The interface is heavily styled, with a very unusual approach to design and layout which can be a little difficult to comprehend at first (and even with some familiarity it maintains the ability to confuse). With initial checks of the settings complete, testing proceeded at good speed. Scanning speeds were OK to start with, very fast indeed in the warm runs, and on-access lag times were pretty low. Resource use was below average, but our suite of activities suffered a fairly heavy slowdown.

Detection tests as usual were split into the smallest possible chunks, as larger scans have proved extremely slow in past tests (probably thanks to storing results in memory until the completion of a job). Once available, logging is a little unmanageable – while logs display fairly readably on screen, there is no option to export to file, so data had to be ripped from an SQL database format.

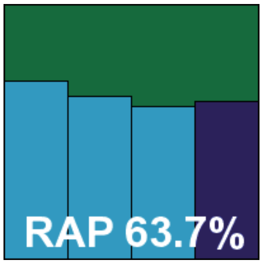
As expected, RAP scores were somewhat mediocre, but Response scores were more impressive. The WildList sets were handled well for the most part, but a single sample of W32/Virut was missed, indicating less than perfect handling of this particular strain. There were also a handful of false alarms in the clean sets, including popular items such as the *VLC* media player and an item from *Microsoft*. This combination of issues was more than enough to deny *Total Defense* a VB100 award for its consumer product.

Our records now show two passes from three entries in the last six tests for this product; three from six in the last two years. There were no stability problems, but the extra efforts we went to and the lengthy scan times required despite the splitting up of the sets meant that testing took around three full days of system time.

## Total Defense Inc. Total Defense R12

Main version: 12.0.528

| | | | |
|---|---|---|---|
| **ItW Std** | 99.99% | **ItW Std (o/a)** | 99.99% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |



The business big brother of *ISS+*, *Total Defense*, is a rather more regular participant in our tests, and as usual was installed from a full DVD provided by the developers. Issues with the management and deployment of the product noted in past tests can now be skirted thanks to the discovery of a standalone install option on the disk. This made for a rapid and simple set-up process, gathering a fair amount of data once again but completing in just a couple of minutes, ending with a reboot. Updates were rapid, averaging around three minutes through the three runs.

The interface is a little plainer and more straightforward than the consumer offering – much more suitable for a business environment – and provides a decent selection of options in a simple format. Stability was decent, but again great efforts were made to avoid known issues in handling larger test sets. Scanning speeds went from a zippy start to a blazing fast speed in the warm runs; overheads were light with the default settings and a little slower when turned up to the max, as one might expect. RAM use was around average, CPU use pretty low, and impact on our set of tasks decidedly high.

Detection rates were similar to those shown by the home-user product – disappointing, but steady in the RAP sets; better, but less even in the Response sets, and once again decent WildList coverage was marred by a single polymorphic sample being missed. Despite there being no false positives this time (suggesting that those noted before had been sparked by additional components not included or not active by default in the business product – or perhaps that the issues were spotted and fixed in the gap between running the two products), no VB100 award can thus be granted.

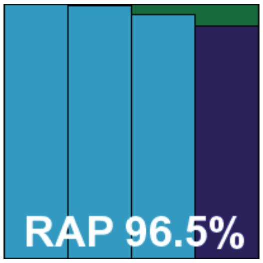
Our test history shows four passes and now a single fail from five entries in the last six tests; seven passes and three fails in the last two years. Testing stretched out to a little over three days, with no issues noted other than slow speeds over the infected sets.

## TrustPort Antivirus 2012

Main version: 12.0.0.4828

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

vb Dec 2011 100 VIRUS virusbtn.com



Another multi-engine product with a splendid record of high scores in our tests, *TrustPort*'s installer was surprisingly compact for the product type at 233MB, and the set-up involved no more than the usual set of steps, completing in good time with no need to reboot. Updating was not the fastest, as might be predicted, but was not too slow either, generally completing in 15 minutes.

The GUI is crisp and simple, providing an excellent range of fine-tuning options in a straightforward manner. Operation proved easy and reliable, with no problems under pressure, and testing progressed nicely. Scanning speeds were a little below average, but not outrageous, and on-access lags were likewise just a little heavy. Resource use was a little higher than most this month, but our set of tasks did not take too much longer than usual to complete.

Detection rates were superb, as always, with near-perfect scores throughout the Response tests and very high levels in the RAP sets, even the proactive week staying above 90%. The WildList was handled perfectly, and with no false alarms *TrustPort* comfortably earns a VB100 award this month.

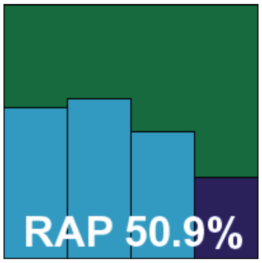
The vendor's recent record is very solid, with four passes from four entries in the last six tests; eight from eight in the last two years. No issues were noted in testing, which completed just within the allotted 48 hours of system time.

### UtilTool Antivirus

Main version: 14.1.7

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 99.60% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 99.13% |
| **False positives** | 0 | | |

Yet another branch from the *Preventon/VirusBuster* tree, *UtilTool* is one of the newer names on our ever-growing list. Once again, the 72MB installation package ran through quickly with minimal interaction and no reboot, and was all done within under a minute. Updates averaged less than four minutes over the three online runs. The GUI is fairly basic but clean and clear, providing a little more than the rudimentary options, but once again logging is a little problematic for us, defaulting to over-verbose records which are dumped after reaching a few MB.



Speed measures were not the fastest, and lag times a little high, with low-ish RAM use, high-ish CPU use and a decent time taken to complete our set of activities. Once again, scanning the RAP sets proved horribly problematic – even on-access runs over sets from which all known problem samples had been removed resulted in repeated crashing and freezing. The data was eventually gathered from multiple runs with much hard work put in to carry things on from previous checkpoints.

*UtilTool* showed considerably lower scores than those produced by similar products and those scores should thus be taken as unreliable; however, after devoting a great deal of time to nursing the product through the tests, these were the best figures that could be obtained. The Response tests proved much easier, and show much more respectable, if not hugely impressive scores. The clean set showed no problems, but in the standard WildList set a pair of samples seemed to go undetected on access on every run, despite full coverage on demand, thus denying *UtilTool* a VB100 award this month.

The vendor now has one pass and one fail in the two tests entered since its first appearance a few months ago; with enormous amounts of extra work required to gather the RAP data, and a few other freezes in the Response tests, the full set of measures took more than eight full days to harvest.

### VirusBuster Professional

Main version: 7.3.33

| | | | |
|---|---|---|---|
| **ItW Std** | 100.00% | **ItW Std (o/a)** | 100.00% |
| **ItW Extd** | 100.00% | **ItW Extd (o/a)** | 100.00% |
| **False positives** | 0 | | |

vb 100 VIRUS virusbtn.com Dec 2011

The penultimate entry in this month's report is the underlying source of many already discussed. *VirusBuster* was expected to give us some headaches.

The installer was an average-sized 70MB, with an additional 66MB of updates provided for offline use. Initial set-up was fairly fast and simple, with the usual step of hiding acceptance of a community feedback scheme on the EULA screen duly noted. No reboot was needed to complete. Online updates were a little tricky, repeatedly failing to do anything when manually fired off or even scheduled a few minutes into the future; in most cases, leaving the product alone for several hours seemed to be the only way to ensure successful updating, but once started the actual download and application of data seemed fairly speedy, taking less than 10 minutes on average.

The interface has undergone a bit of a facelift of late, but remains clunky and clumsy. Despite a good degree of fine-tuning the interface is hard to navigate and operate. In general it seemed stable, but the RAP sets threw up a wealth of problems with repeated freezes, and running on access brought on blue screens almost instantly. In the end, it was abandoned as a lost cause.

Other tests proved much simpler, with no issues in the Response sets, which showed some fairly respectable scores, dipping very sharply on the most recent day. Speeds were also decent, if unremarkable, with average overheads too. RAM and particularly CPU use were low, but our set of tasks took a fair while to complete. The core sets were handled well, and a VB100 award is duly earned.

The company has a very strong record of late, with six passes in the last six tests, 11 in the last two years, its last fail having been in February 2010. Fruitless re-running of the RAP sets took some extra time, as did getting the updates to apply, but overall, testing didn't run for too long, only hogging one of our test machines for around four full days.

### Webroot SecureAnywhere Complete

Main version: 8.0.1.20

| | | | |
|---|---|---|---|
| **ItW Std** | 81.07% | **ItW Std (o/a)** | 66.87% |
| **ItW Extd** | 79.01% | **ItW Extd (o/a)** | 47.17% |
| **False positives** | 2787 | | |

The last product in this month's test is also one of the most interesting: the only product on the final roster to operate solely from the cloud. *Webroot*'s acquisition of *PrevX* is the root source of this new solution, and we were looking forward to seeing how it performed. The package submitted was a tiny 600KB downloader, and running this proved very speedy indeed. A couple of clicks were followed by an initial scan, and the whole process completed without a reboot in just a couple of minutes. The product interface is clear and simple, and seems to provide a fairly decent level of control. Operation was extremely lightweight, with fast scan times, minimal on-access lags and use of resources barely registering; our set of tasks ran through in excellent time. These results are, of course, somewhat skewed by the absence of on-read scanning.

Detection tests were a little more difficult, with a number of crashes experienced when handling larger sets. We also saw one crash when simply exporting the log produced by a scan of the local system drive. On one occasion, the system could no longer be shut down properly.

Analysing the results was a little tricky, as the extremely verbose logs were hard to decipher, but with some help from the developers we soon figured things out. No RAP results were possible, but scores in the Response sets make for fairly dismal reading, with low numbers across the board. The WildList was not well handled either, with large numbers of samples missed in both sets, including all but one of our several thousand polymorphic samples.

The clean sets brought the biggest surprise though, with a huge number of alerts recorded. While our tables record only the number of unique files mislabelled as malicious, there were in fact many times more actual alerts – over 15,000 in total – with several files reported several times, for example in a *PowerPoint* slideshow where many XML sub-components were individually singled out for attention. Many of the alerts were on items with which we would not usually expect any problems, including plain text and image files, while many more were on various types of *Office* documents. Providers included *Microsoft*, *Adobe*, *Citrix*, *Sun*, *Nero*, *Asus* and *Belkin*, and as many of the files were documentation or help files provided with major packages, we would expect them to be seen on a large number of systems. It has been suggested that the product's previous encounters with our large sets of infected samples switched on some sort of 'outbreak mode', heightening the heuristics, which may well be the reason for this.

Clearly, no VB100 award can be awarded for this performance, and *Webroot* will have to make some serious improvements before it can qualify for certification with this product. This being its first appearance, it has no history in our records, but *Webroot*'s other, *Sophos*-based, offering has a decent record. Testing was fiddly but fairly speedy, and did not take more than three days to complete.

## CONCLUSIONS

So, we're finally at the end of our first test using the new methodology. It has been something of an epic struggle, these words being frantically scribbled down more than a month after what should have been our final deadline. As usual, things were somewhat hampered by the cramped conditions in the test lab, from which we hope to break free very soon to move into larger quarters.

We also suffered illness in the team, and important trips and holidays interrupted our testing schedules. These factors doubtless added to the extreme duration of the test, as did the additional work caused by what were some fairly ambitious expansions to the tests. However, none of these, alone or combined, should have seriously impacted our completion time. The main issue slowing things down was, as usual, the products under test. We suffered our complete standard catalogue of horrors, with products lingering for days on jobs which should take no more than a few hours; products crashing, freezing, hanging, blue-screening systems, in a couple of cases turning our test machines into unresponsive bricks; products failing to produce usable log data, dumping vital information, mangling and obfuscating logs where they should be readable by their users; and of course products simply not doing what they're told.

Additionally this month, we've delved into the new and surprisingly scary world of updating. Where we've looked at online updating systems in the past – in isolated cases, in small batches of products and in small numbers of runs – we have generally observed what you might expect from what is a fairly basic and fundamental part of these products: that updates for the most part seem to run rapidly and reliably. Here though, in trying to install and update large numbers of products multiple times, we've encountered some real horrors. Some update processes failed to initiate at all, or took hours to do so, while others ran for extraordinary lengths of time. Some updates ran to apparent completion, demanded a reboot, then expected to be allowed another complete update run. In some cases, updates completely failed, but also failed to adequately inform the user of their lack of efficacy. All of this has added a new headache to our already arduous testing programme. In the end, doubling the amount of time allotted to each product to complete the tests has proved insufficient in close to half of cases. With little space for further expansion, it seems that we may have to be a little more harsh with our rules and in how we apply them. There will be little room for leniency in future tests, especially given the time-sensitive nature of our new approach to the bulk of testing, and the near-impossibility of re-runs should problems emerge – we may have to start failing or excluding products at the first sign of a crash or other misbehaviour.

So far, the problems we have reported in these pages have failed to make much impact on some of the companies taking part; while most are eager to fix any issues we raise, some keep plodding on month after month with the exact same swathes of bugs and glitches. Sometimes it feels as though there are firms out there with no kind of internal testing or QA procedures at all, simply throwing out products at random and hoping external testers like ourselves will spot and diagnose all their problems for them, fixing those that seem simple enough to deal with. This is clearly not doing any favours for their customers, and if we can find a way of discouraging the widespread, slapdash approach to quality we've observed here, we will do all we can.

Enough of this moaning though. Moving on to the real meat of the test, the results, there are a number of surprises, and even a few shocks. The usual hard core of high performers continue to do well, with some excellent performances. It's always interesting to note that those products which have the best showing in our tables also tend to be those giving us the least grief in the test lab, running solidly, reliably and usually rapidly through our test suite. Quality will out, I suppose. In other cases we've seen handfuls of near misses, with a few good performances just missing out on certification for one reason or another. It feels like we have seen more than the usual number of false alarms this month, although this feeling could in part be biased by an epic, record-smashing score from one particular product. It's hard to tell if our new approach has had much influence on this; certainly in the past, it has been possible for vendors to be doubly cautious, performing extra false positive testing internally around the time of the submission deadline, whereas now there's no telling exactly when they'll be tested. This should give a more accurate reflection of how careful developers are in general, day to day, rather than at a fixed and pre-announced moment. So perhaps we're likely to see this sort of level becoming the norm for future tests. A worrying thought.

The expansion of the WildList has had some interesting effects. Perhaps surprisingly, given the level of outcry when we first announced our intention to make it a requirement for certification, coverage has been pretty solid. Only two products have been denied a reward solely on the basis of missing Extended WildList samples, and one of those managed to achieve full coverage in one of the three runs. A third product missed just a single sample in just one of the three tries, but also had a false positive. For the most part, those having problems with the Extended list had problems elsewhere too. We have made a few concessions for this first run, excluding a handful of samples which target less common platforms, and only demanding on-demand alerts rather than full detections in both modes – but this is something we hope to be able to change very soon. We'll be looking into those few cases where on-access scanners failed to detect, where on-demand scanners had no problems, and at some point will hopefully merge the sets, and the results, into a single united entity. As the Extended list matures, it seems certain to expand in both size and range, offering an ever tougher challenge to our participants.

The use of a live web connection for the WildList tests seems to have had minimal impact so far, although in a few cases we did observe changes in coverage from one run to the next. Indeed, this affected both of the products which failed on the Extended list only – where one product had full coverage in one run, the other missed in all three live runs but had full detection on the submission deadline, and once again shortly after the completion of the test. Some people have questioned the value of cloud solutions, pointing out that it has long been standard advice that the first thing a user should do when they suspect an infection is to pull out the network cable (or otherwise disable connections on which both the malware, and in some cases the anti-malware, rely). We considered including an offline run over the WildList as well, to show how well products can cope with this sort of emergency situation, but felt that the RAP test was an adequate measure of offline performance – an offline WildList run would mean excluding those products which cannot operate offline at all. One such product made it to the full report this month, although it performed disappointingly, while another was submitted but was ultimately found not to be fully testable under our procedures (a further three products were also submitted but excluded from the final report, as reliable test data could not be gathered – in most cases these products still took up a considerable amount of testing time before they were abandoned). We expect to see more cloud-only solutions taking part very soon.

On the wider detection front, our new Response test has proved an interesting first attempt. It's clear from comparison of these new figures with the RAP test results (at least, where RAP scores are available) which products are making good use of cloud look-up systems to cover the latest threats. For the most part, figures have conformed reasonably closely to the expected pattern of a gradual decrease from older to fresher samples, albeit with the occasional anomaly. Obviously some improvements are required; this initial run only included two sets of results per product, rather than the planned three, and our gathering processes were rather hampered by the loss of a vital system. Going forward we hope to improve the diversity of both sample types and source, and their freshness, to provide an even more accurate picture. Nevertheless, this first try has proved generally enlightening.

We're also looking at ways of presenting the Response data in more easily-readable format, although the figures are not as simple to place on a clear chart as the RAP data. This month's RAP quadrant chart shows once again a fairly clear clustering of products into three main groups: the mediocre, the good and the excellent. Looking at our other charts and graphs, the ever-growing numbers of competitors make these ever more cluttered, and we hope to find time to look at ways of simplifying them too. We're also looking at reporting more subjective or miscellaneous data, perhaps including some of the things currently covered only in the write-ups, presented in a way which allows simple comparison between products. If readers have any suggestions for the sort of data they'd like to see covered in more depth, we'd be happy to hear them, as of course we continue to listen to advice, ideas, criticisms and even occasional abuse.

The next test will be on *Linux* and thus should be considerably smaller than this month's behemoth, so hopefully there will be time for some background work before the looming juggernaut of the annual *XP* test. At the very least, there should be a few spare hours to mop our brows, steady our shaken nerves and generally recuperate from what has been a truly testing time.

**Technical details:**

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 7 Professional*, with Service Pack 1. For the full testing methodology see http://www.virusbtn.com/vb100/about/methodology.xml.

*Any developers interested in submitting products for VB's comparative reviews, or anyone with any comments or suggestions on the test methodology, should contact john.hawes@virusbtn.com. The current schedule for the publication of VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.*

## VIRUS BULLETIN

**Editor:** Helen Martin

**Technical Editor:** Morton Swimmer

**Test Team Director:** John Hawes

**Anti-Spam Test Director:** Martijn Grooten

**Security Test Engineer:** Simon Bates

**Sales Executive:** Allison Sketchley

**Web Developer:** Paul Hettler

**Consulting Editors:**

Nick FitzGerald, *Independent consultant, NZ*

Ian Whalley, *IBM Research, USA*

Richard Ford, *Florida Institute of Technology, US*

## 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.