FEBRUARY 2012

virus BULLETIN

Fighting malware and spam

# VB100 COMPARATIVE REVIEW ON RED HAT ENTERPRISE LINUX

## INTRODUCTION

The annual *Linux* test usually affords the *VB* lab team some respite from the non-stop VB100 test schedule – with a far smaller range of solutions on offer, and greater opportunities for automation of tests, the *Linux* comparative generally requires considerably less time and effort than the *Windows* tests that make up the bulk of the year's work. However, with some major changes to our testing procedures introduced in the last comparative, things were likely to take rather longer this year – and with a fairly full test bench, a relatively new and unfamiliar *Linux* distribution, and a late start thanks to the new year, there was little time to rest up.

## PLATFORM AND TEST SETS

The platform for this test was *Red Hat Enterprise Linux*. The latest version, 6.2, was released some months before the test began, but for several of the participants the fact that we would be using the latest version came as something of a surprise (perhaps not helped by a lack of specific information in the initial announcements). The platform itself was fairly simple to set up, with a pleasantly slick and efficient install process. However, this did seem to be lacking in some areas, notably the disk partitioning arrangements which were completely unable to cope with NTFS partitions on our test systems. Some of these were scrapped and replaced with the latest EXT4 file systems, while some spare partitions were left as they were, and thus remained invisible throughout the test. Defaults were used throughout the set-up, with some additional software selections including development tools that were likely to be needed for compiling some of the on-access components. Additional dependencies would be resolved as needed on a per-product basis, to allow us to monitor what extra items might be required. Previous experience with *Linux* tests has taught us to expect three main approaches to the on-access tests, with most products either protecting the entire system with the open-source *dazuko* file access hooking system, or only covering *Samba* shares using VFS objects, while a few would doubtless use their own proprietary approaches. An additional system was set up with *Windows XP SP3*, to use as a client for the on-access tests, and file shares on all the test servers were connected to this machine.

The test deadline was set for 5 January, which caused the usual problems for developers in countries where this date falls in the middle of a major national holiday, but submissions were dealt with smoothly. Most of the usual suspects were present, although two of the larger names in the industry chose not to submit their products, with little reason given for their absence. At the final count numbers were pleasingly manageable, and with a test bench full of seasoned regulars we looked forward to a smooth and straightforward test.

The test sets were put together using the November 2011 WildLists (Standard and Extended). These contained little of note, comprising mainly the usual worms, online gaming password stealers and the like, with a smattering of slightly more controversial items in the Extended list. Some changes to the Extended list were made at a very late stage (a handful of items had been adjudged to be 'grey' rather than truly malicious), the announcement from *The WildList Organization* coming just in time for us to incorporate the changes into the final publication of this report. We also made a few changes of our own, removing a handful of *Android* and similar items from the list as per our current policies. With no new polymorphic items to deal with, the test sets were rather smaller than usual and promised fewer issues for the vendors. The prospect of a clean sweep of passes loomed large.

The clean sets presented the only additional worry for the participants, and here we made the usual changes, removing older items and updating the set with a selection of new

ISSN 1749-7027

| Certification tests | On demand | | On access | | Clean sets | |
|---|---|---|---|---|---|---|
| | Standard WildList | Extended WildList | Standard WildList | Extended WildList | FP | Suspicious |
| Avast | 100.00% | 100.00% | 100.00% | 100.00% | | |
| AVG | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Avira | 100.00% | 100.00% | 100.00% | 100.00% | | |
| BitDefender | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Central Command | 100.00% | 100.00% | 100.00% | 100.00% | | |
| eScan | 100.00% | 100.00% | 100.00% | 100.00% | | |
| ESET | 100.00% | 100.00% | 100.00% | 100.00% | | 2 |
| Frisk | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Kaspersky AntiVirus | 100.00% | 100.00% | 100.00% | 100.00% | 1 | 3 |
| Kaspersky Endpoint Security | 100.00% | 100.00% | 100.00% | 100.00% | 1 | 3 |
| Norman | 100.00% | 100.00% | 100.00% | 100.00% | | |
| Sophos | 100.00% | 100.00% | 100.00% | 100.00% | | |
| VirusBuster | 100.00% | 100.00% | 100.00% | 100.00% | | |

*Please refer to text for full product names.*

items, focusing on business software to suit the corporate focus of this month's test. With the removals and additions more or less balancing out, the set remained much the same size at close to half a million unique files, 180GB total size.

The speed sets remained unchanged from the last test (before which they were refreshed considerably), and an additional set of *Linux* samples was added to measure scanning speed over these types of files – taken from the /bin, /sbin, /opt and /user areas on a basic install of the platform under test. Some adjustments to the speed scripts were required, including the removal of the activities tests which were not appropriate for this platform.

With everything ready in good time, testing proceeded rapidly with the new format of four test runs per product split into the RAP test (with updates frozen on the deadline day), and three runs through the certification components. These runs took place roughly a week apart throughout late January and early February, with testing completing just in time to repurpose the test network for the next comparative in mid-February.

## Avast Software avast! Linux/Unix Edition

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

vb Feb 2012 100 VIRUS virusbtn.com

RAP 90.9%

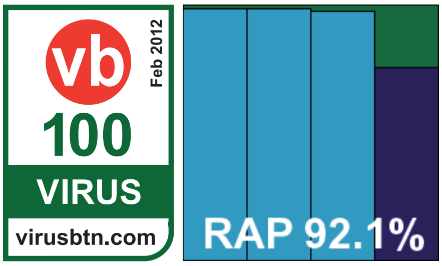
*Avast*'s *Linux* product was provided as a trio of RPM packages, totalling around 50MB. The set-up process was fairly simple, with the RPMs dropping everything neatly into place. Some simple instructions were provided for compiling and installing the *dazuko* modules, which ran smoothly too, and everything was ready to go in next to no time. The product operates in a standard manner, with a daemon controlled by normal init scripts, configuration files where one might expect to find them, and a simple and clear command line syntax. Man pages were provided to help work out how to use things, but were not really required after reading the basic instructions provided along with the submission.

Scanning was fairly quick for the most part, and tests ran through in good time, although a few suspect files in the RAP sets did cause scans to crash out with a segmentation fault error. Re-running things from where they had left off proved fairly simple though. On-access overheads were surprisingly high – notably over archived files which are inspected in depth by default – but the real-time component remained stable and solid under pressure. Updates were simple and reasonably quick, generally completing in just a few minutes.

Detection rates were very solid, with an excellent showing in the Response tests and good scores in the reactive part of the RAP test, dropping noticeably in the proactive week. The certification components were handled impeccably, with no issues in the WildList or clean sets, and a VB100 award is comfortably earned by *Avast*. After a slight blip in the last test, the vendor's history now shows five passes and one fail in the last six tests; 11 passes in the last two years.

## AVG Linux Server Edition

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



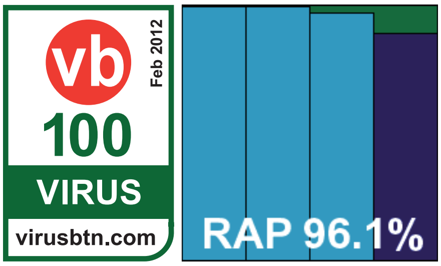
*AVG*'s submission came as a single RPM, and again some additional compilation and installation work was needed to add in the on-access component – in this case a combination of redirfs and avflt modules. The operation and layout was simple and followed standard practices, making it easy to work out without reference to the man pages, which were provided nevertheless. Everything ran smoothly and without problems, and again updates were simple and fairly zippy.

Speed tests showed good scan times on demand, which were slightly slower with archive scanning enabled, as expected. However, on-access overheads seemed rather heavy across the board. Detection rates were very good though, with another set of high scores in the Response sets and high catch rates in the reactive weeks of the RAP sets, again dropping off fairly sharply into the proactive week.

The WildList and clean sets were dealt with without problems, and a VB100 award is well earned, giving *AVG* five passes and one fail in the last six tests; 11 passes in the last two years.

## Avira AntiVir Server

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



*Avira*'s *Linux* product came as a simple archive containing an install script which sets everything up, running through a set of question-and-answer stages. This seemed to run OK up until the addition of the on-access module, which tried to install the *dazuko3* system but had some trouble (which we had been warned about by the developers). This proved fairly severe, locking up the test machine completely, and a hard reboot was needed to correct things. After cleaning off the machine and reinstalling the product, we opted instead to go with the simpler *dazuko2* approach. This seemed to work much better, although the installer warned that it was not officially supported.

With this hurdle overcome, tests proceeded without further issues. An absence of man pages was noted, but ample information was provided in PDF and text format documentation. With the software following standard approaches it proved simple to operate, with a number of scripts provided to perform standard tasks. Scanning speeds were pretty decent, and overheads fairly light, although archives again took some time to process – as did the set of *Linux* samples, which contained a number of archived files (many of them JAR archives included with the Java subsystem).

Detection rates were pretty splendid, with a superb showing in the Response tests, and excellent scores in the RAP tests too, dropping a little in the proactive week but remaining impressive even there. No problems were noted in the certification sets, and a VB100 award was easily earned, maintaining *Avira*'s clean sweep with 12 passes out of 12 in the last two years.

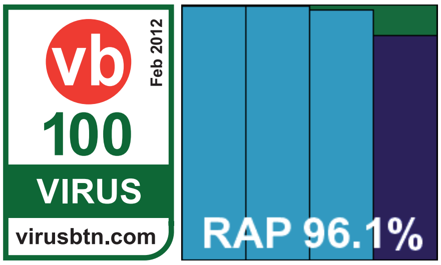
## BitDefender Security for Linux

| | | | |
|---|---|---|---|
| **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 *Linux* solution was provided as an RPM.run file which, once executed, ran through the set-up process swiftly and simply. Some additional manual work was required, including copying of VFS modules and making the appropriate changes to the *Samba* configuration file to provide on-access protection of shares, but this was fairly straightforward. Configuration is held in XML format

| File access lag time (s/GB) | Archive files | | | Binaries and system files | | | Linux 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 | Default (cold) | Default (warm) | All files |
| Avast | 313.46 | 311.42 | 313.46 | 143.21 | 139.24 | 143.21 | 251.56 | 240.77 | 251.56 | 128.74 | 124.95 | 128.74 | 152.05 | 147.96 | 152.05 |
| AVG | 179.99 | 184.31 | 179.99 | 210.03 | 208.65 | 210.03 | 184.10 | 187.68 | 184.10 | 189.25 | 186.99 | 189.25 | 198.62 | 198.62 | 198.62 |
| Avira | 177.37 | 179.14 | 177.37 | 19.52 | 20.15 | 19.52 | 257.10 | 258.82 | 257.10 | 19.79 | 19.49 | 19.79 | 77.12 | 77.72 | 77.12 |
| BitDefender | 220.25 | 216.50 | 220.25 | 94.38 | 102.32 | 94.38 | 213.99 | 218.20 | 213.99 | 118.41 | 114.11 | 118.41 | 209.81 | 215.04 | 209.81 |
| Central Command | 56.68 | 53.77 | NA | 89.02 | 84.86 | 89.02 | 43.88 | 43.75 | NA | 64.60 | 64.69 | 64.60 | 90.70 | 84.29 | 90.70 |
| eScan | 225.74 | 221.99 | 225.74 | 110.21 | 118.16 | 110.21 | 218.01 | 222.21 | 218.01 | 121.91 | 117.61 | 121.91 | 236.03 | 241.27 | 236.03 |
| ESET | 56.32 | 50.01 | NA | 55.57 | 62.12 | 55.57 | 50.61 | 54.87 | NA | 53.52 | 59.97 | 53.52 | 59.71 | 48.71 | 59.71 |
| Frisk | 142.74 | 141.18 | 142.74 | 101.02 | 103.20 | 101.02 | 76.52 | 79.64 | 76.52 | 81.39 | 91.95 | 81.39 | 119.29 | 131.77 | 119.29 |
| Kaspersky AV | 61.90 | 57.55 | 356.01 | 82.92 | 87.26 | 103.02 | 55.41 | 172.66 | 610.63 | 74.81 | 72.84 | 76.71 | 95.84 | 96.52 | 571.47 |
| Kaspersky ES | 60.42 | 56.37 | 356.90 | 79.31 | 83.58 | 103.49 | 53.93 | 56.41 | 621.93 | 71.65 | 65.18 | 74.08 | 87.88 | 92.48 | 178.46 |
| Norman | 64.00 | 66.67 | NA | 153.59 | 149.63 | 153.59 | 75.82 | 74.18 | NA | 105.32 | 108.18 | 105.32 | 236.97 | 229.72 | 236.97 |
| Sophos | 16.20 | 3.28 | NA | 39.39 | 38.18 | 93.68 | 4.72 | 4.41 | NA | 21.33 | 20.78 | 73.76 | 44.80 | 41.74 | 120.56 |
| VirusBuster | 60.48 | 51.23 | NA | 88.37 | 84.10 | 88.37 | 51.13 | 53.29 | NA | 65.23 | 69.51 | 65.23 | 87.24 | 81.58 | 87.24 |

*Please refer to text for full product names.*



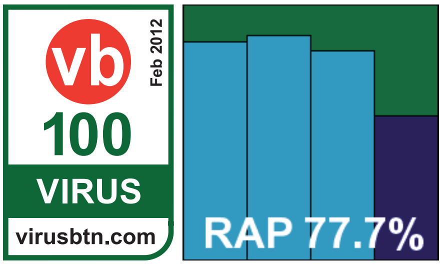
and modified using a control program. This proved a little more fiddly than hoped, but with a little practice it soon became simple to operate. A number of daemons are used, but these are all controlled from a single init script, so starting and stopping the program was also fairly simple.

Scanning speeds were fairly average on demand and notably slow over the archive-heavy *Linux* set. Overheads were a little high on access too, but detection rates were solid in the Response sets and splendid in the RAP sets.

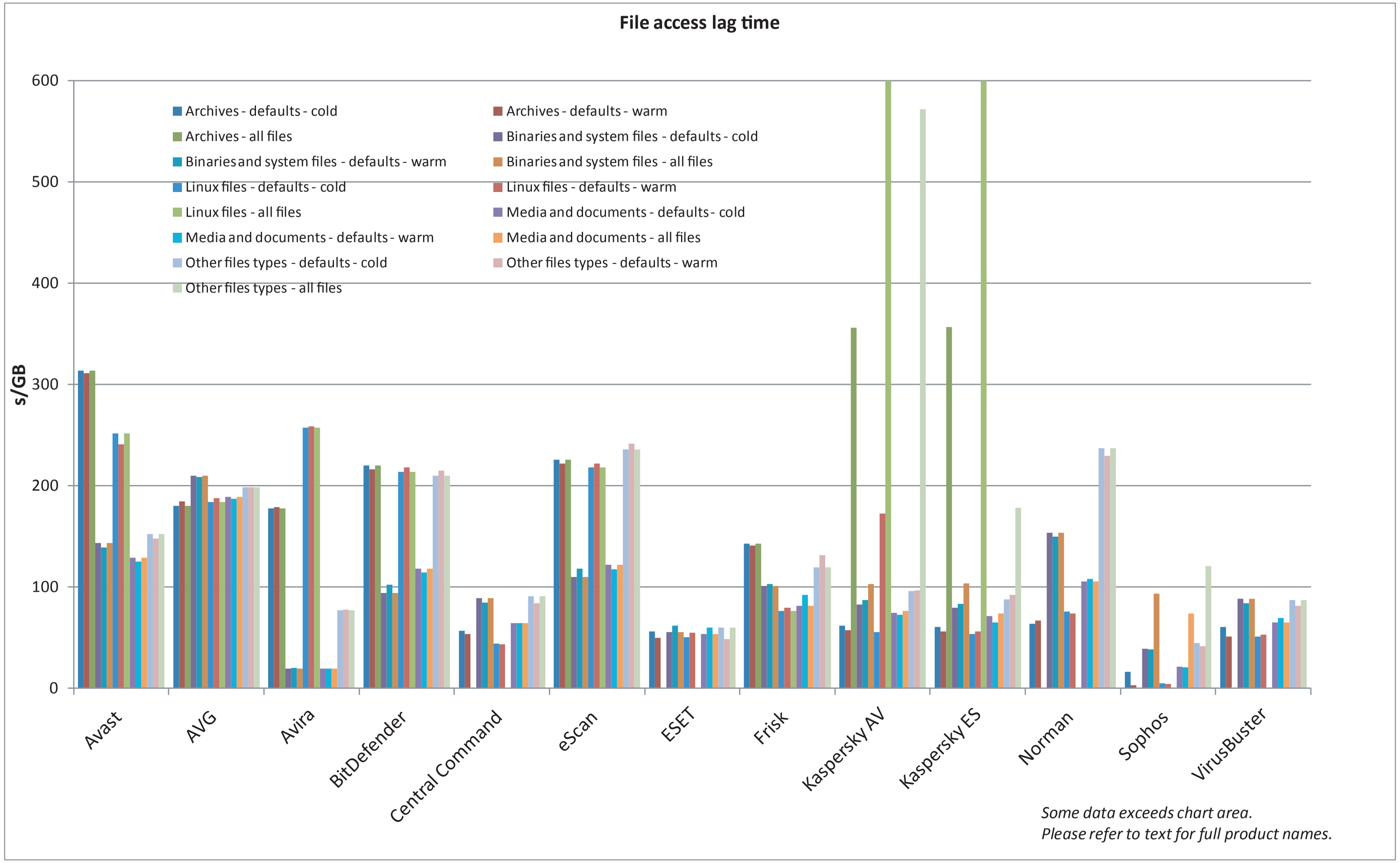
The WildList and clean sets presented no difficulties, and a VB100 award is duly granted, giving *BitDefender* six passes in the last six tests; ten passes, a single fail and one no-entry in the last two years.

## Central Command Vexira for Samba Servers

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



*Central Command* opted for the archive-containing-an-install-script approach, and set-up was fairly straightforward. Once again, some adjustments had to be made to the *Samba* configuration file to make it use a VFS object to check files before granting access to them. Configuration was fairly limited for the on-access component, with a basic configuration file providing minimal controls. No man page



File access lag time

*Some data exceeds chart area.*
*Please refer to text for full product names.*

| On-demand throughput (MB/s) | Archive files | | | Binaries and system files | | | Linux 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 | Default (cold) | Default (warm) | All files |
| Avast | 12.89 | 13.03 | 4.45 | 12.99 | 13.03 | 12.99 | 2.07 | 2.06 | 2.08 | 19.61 | 19.59 | 19.61 | 6.43 | 6.30 | 6.43 |
| AVG | 62.17 | 62.37 | 4.25 | 28.23 | 28.33 | 26.37 | 13.00 | 13.05 | 0.40 | 33.16 | 33.48 | 30.73 | 8.37 | 8.47 | 7.62 |
| Avira | 6.94 | 5.80 | 6.94 | 27.31 | 22.31 | 27.31 | 0.96 | 0.84 | 0.96 | 30.91 | 30.73 | 30.91 | 6.43 | 6.40 | 6.43 |
| BitDefender | 6.09 | 6.03 | 6.09 | 19.38 | 19.45 | 19.38 | 1.58 | 1.57 | 1.58 | 20.28 | 20.01 | 20.28 | 5.29 | 5.34 | 5.29 |
| Central Command | 5.91 | 5.95 | 5.90 | 16.69 | 16.69 | 16.59 | 1.03 | 1.02 | 1.02 | 17.53 | 17.34 | 16.05 | 7.14 | 7.11 | 5.96 |
| eScan | 5.74 | 5.60 | 5.74 | 22.97 | 23.13 | 22.97 | 1.49 | 1.51 | 1.49 | 28.97 | 29.14 | 28.97 | 7.80 | 8.01 | 7.80 |
| ESET | 9.10 | 9.12 | 9.10 | 13.85 | 13.67 | 13.85 | 1.82 | 1.81 | 1.82 | 87.88 | 89.00 | 87.88 | 8.52 | 8.53 | 8.52 |
| Frisk | 13.61 | 13.43 | 13.61 | 23.48 | 22.46 | 23.48 | 15.96 | 15.86 | 15.96 | 49.42 | 50.61 | 49.42 | 9.33 | 9.48 | 9.33 |
| Kaspersky AV | 3.22 | 3.22 | 3.22 | 8.56 | 8.60 | 8.56 | 0.46 | 0.46 | 0.46 | 31.23 | 31.37 | 31.23 | 0.81 | 0.80 | 0.81 |
| Kaspersky ES | 3.26 | 3.24 | 3.26 | 8.97 | 8.92 | 8.97 | 0.46 | 0.46 | 0.46 | 31.85 | 31.79 | 31.85 | 1.21 | 1.23 | 1.21 |
| Norman | 0.76 | 0.76 | 0.76 | 4.90 | 4.91 | 4.90 | 0.85 | 0.85 | 0.85 | 13.57 | 14.07 | 13.57 | 3.08 | 3.11 | 3.08 |
| Sophos | 108.93 | 166.27 | 1.68 | 20.15 | 20.09 | 11.96 | 52.57 | 51.95 | 0.14 | 117.09 | 112.28 | 18.88 | 91.75 | 92.65 | 4.39 |
| VirusBuster | 5.81 | 5.68 | 5.81 | 16.55 | 16.54 | 16.55 | 1.03 | 0.93 | 1.03 | 17.33 | 17.30 | 17.33 | 7.18 | 7.15 | 7.18 |

*Please refer to text for full product names.*

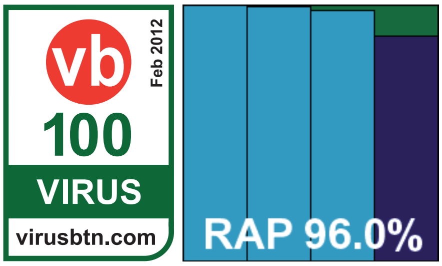
was provided for the on-demand scanner, but it proved fairly self-explanatory. The information on the on-access component was pretty rudimentary, but operation was stable and reliable.

Scanning speeds were fairly average on demand, but on-access overheads seemed on the light side. Detection rates were decent if unspectacular, with reasonable scores in the Response sets and the reactive weeks of the RAP sets, the proactive week dropping off fairly sharply. The certification sets were handled well though, and a VB100 award is duly earned. *Central Command* now has five passes and one fail in the last six tests; 11 passes in the last two years.

## eScan for Linux Servers

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

The *eScan* product incorporates the *BitDefender* engine, and on *Linux* also includes a *Clam* component controlled by a separate init script. The install process involves applying several RPMs, but is fairly simple. The on-access component is again provided via a *Samba* VFS object, which requires several lines to be added to the *Samba* configuration file. Operation was fairly simple and logical, with clear documentation.

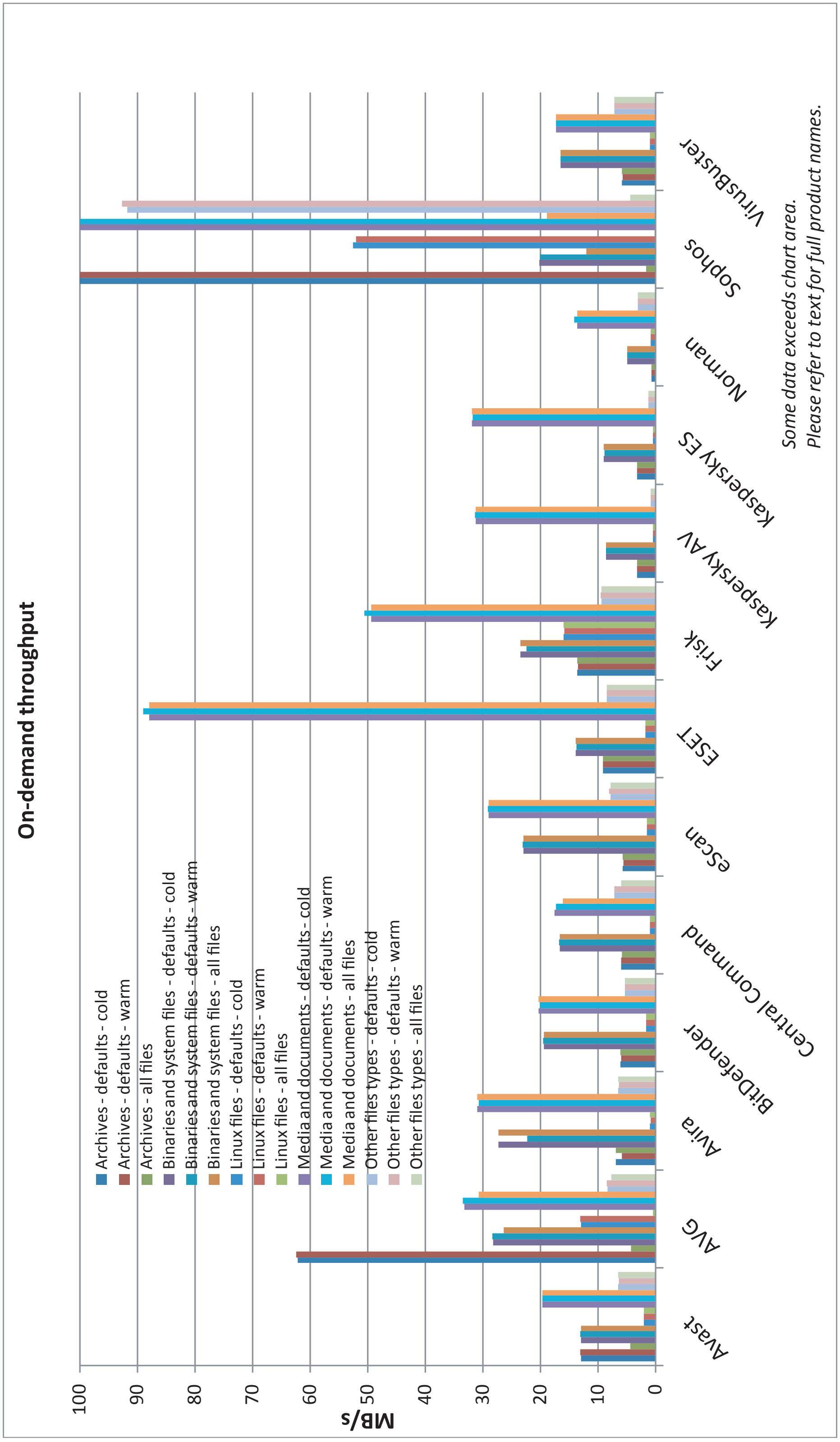


Scanning speeds were not bad on demand, a little heavy on access, but things seemed to operate stably under pressure. Detection scores were good, with the RAP sets particularly well handled. The WildList and clean sets threw up no surprises, and a VB100 award is comfortably earned, giving *eScan* six passes in the last six tests; things are a little rockier longer term, with ten passes and two fails in the last two years.

## ESET Security for Linux

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

*ESET*'s product came as a single RPM file, making initial set-up fairly straightforward, and a flexible system allows either *dazuko* or *Samba* VFS approaches to on-access

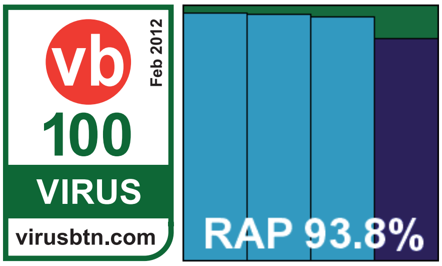


*Some data exceeds chart area.*
*Please refer to text for full product names.*

| Response tests | Day -7 | Day -6 | Day -5 | Day -4 | Day -3 | Day -2 | Day -1 | Average |
|---|---|---|---|---|---|---|---|---|
| Avast | 97.58% | 97.32% | 97.84% | 98.63% | 96.41% | 95.75% | 96.38% | 97.13% |
| AVG | 97.77% | 96.74% | 98.38% | 97.99% | 97.70% | 97.61% | 96.48% | 97.52% |
| Avira | 97.91% | 98.92% | 98.81% | 99.71% | 97.57% | 97.45% | 97.11% | 98.21% |
| BitDefender | 92.66% | 95.02% | 94.90% | 92.32% | 86.35% | 92.97% | 93.96% | 92.60% |
| Central Command | 80.27% | 68.68% | 80.44% | 75.14% | 65.15% | 78.08% | 74.01% | 74.54% |
| eScan | 93.13% | 93.31% | 94.21% | 87.80% | 88.60% | 94.25% | 91.72% | 91.86% |
| ESET | 96.76% | 96.98% | 97.13% | 98.29% | 95.47% | 93.77% | 94.39% | 96.11% |
| Frisk | 61.07% | 58.15% | 59.73% | 54.07% | 50.47% | 65.76% | 62.14% | 58.77% |
| Kaspersky AV | 93.63% | 96.15% | 95.36% | 94.36% | 92.99% | 94.44% | 94.45% | 94.48% |
| Kaspersky ES | 93.63% | 96.15% | 95.36% | 94.36% | 92.99% | 94.44% | 94.45% | 94.48% |
| Norman | 85.98% | 79.51% | 79.45% | 81.75% | 86.62% | 82.43% | 85.21% | 82.99% |
| Sophos | 80.18% | 79.97% | 73.20% | 70.71% | 76.27% | 75.74% | 83.54% | 77.09% |
| VirusBuster | 82.35% | 69.75% | 79.67% | 78.33% | 72.90% | 70.39% | 75.93% | 75.62% |

*Please refer to text for full product names.*

protection. At the suggestion of the developers we went for the *Samba* method, which involved adding a line to the *Samba* init script, thus covering all *Samba* shares rather than providing protection on a share-by-share basis as in previous products.



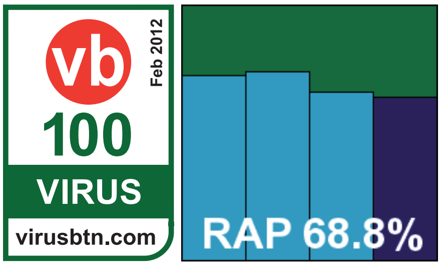
On-demand settings can be configured either by adjusting defaults in the configuration file or by passing in options on the command line; the latter method generally proved the simplest. The configuration file is lengthy and covers the full range of controls – including anti-spam protection – in a single, internally consistent file, making for simple operation. On-access controls included options to check archives fully, but these seemed to make no difference to the product's operation, and archives seemed to go unexamined regardless of the settings.

Scanning speeds were thus fairly impressive, with overheads very light indeed, and detection was impressive too, with great scores in the Response sets and solid levels in the RAP sets too, not dropping off too sharply in the proactive week. The WildLists were handled well, and with just a few hacker-esque items alerted on in the clean sets a VB100 award is duly earned. *ESET* maintains its impeccable record with every test entered and passed for close to a decade.

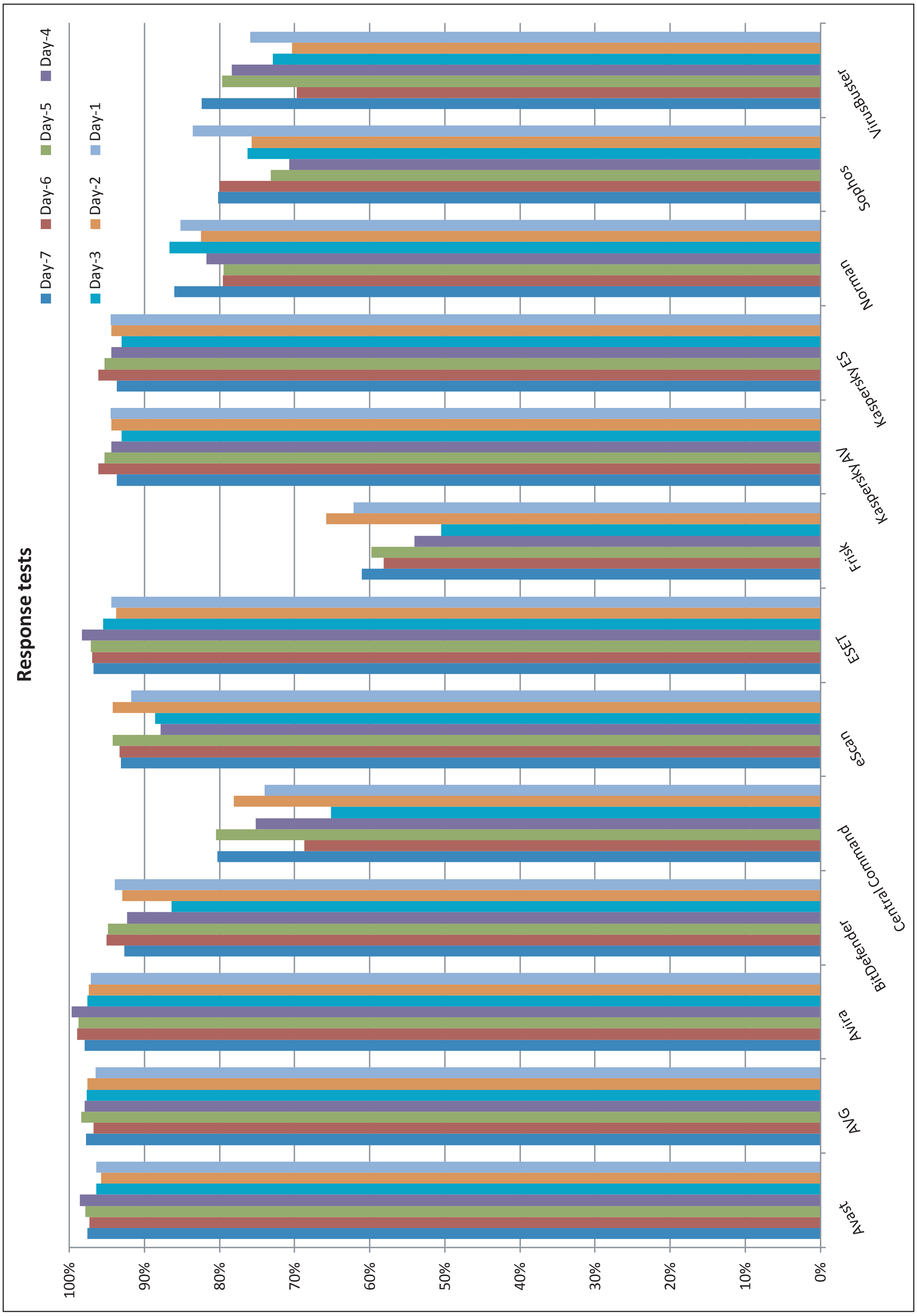
## Frisk F-PROT Antivirus for Linux

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

*Frisk*'s product was one of the most basic on the test bench this month, with a simple install script which simply links init and configuration scripts to the real components, allowing installation and operation from wherever the user wishes. The product is another which can use either *dazuko* or *Samba* methods, and again *Samba* was chosen as the simplest. The *Samba* init file is tweaked to provide protection of all shares. The layout and operation is straightforward and unsurprising, and everything ran smoothly and stably.



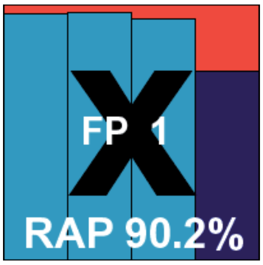
Scanning speeds were pretty good, and overheads fairly light, but detection rates were rather disappointing – barely rising above 50% on some days in the Response sets. Nevertheless, the certification sets were dealt with properly, and a VB100 award is duly earned. *Frisk*'s test history shows five passes and a single fail in the last six tests; four fails and eight passes in the last two years.



*Please refer to text for full product names.*

## Kaspersky AntiVirus 8.0 for Linux File Server

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



As usual, *Kaspersky* entered two products for the test, representing server and desktop offerings. The differences between them seemed fairly minimal though. Packages downloaded for the submission were supplemented by an offline update system which involved installing a downloader tool and setting it off to fetch data to build a local update repository. Setting up both the products was fairly simple, with install scripts performing a comprehensive set-up. Given the few differences between the two products, we opted to make the server version use *Samba* protection only, and it was one of few products to perform all the necessary changes automatically.

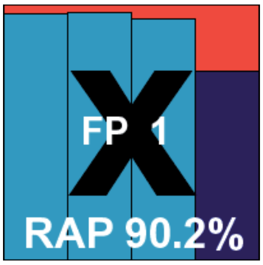
Once up and running, making changes and running tasks is a rather less straightforward process; a lengthy PDF manual had to be consulted in depth before the design of the product became clear. A master control program is provided, but the syntax of its commands is complex and esoteric in the extreme. The manual advises passing in huge multi-line commands to perform the simplest of tasks, with the traditional *Linux* approach of holding configuration in a simple, humanly readable test file eschewed for some reason. The easiest way we found of adjusting settings was to output the settings to a file, make changes there and read it back in again. We were baffled as to why the product couldn't simply have a normal configuration file. After much practice however, it became fairly usable.

Scanning was very slow, and frequently used up large amounts of disk space – presumably due to archives being unpacked into temporary folders. On-access overheads were high too, particularly once the settings had been adjusted to cover all file types. Detection rates were good though, with solid showings across the Response sets and good scores in the RAP sets, dropping off fairly steeply into the proactive week.

The WildList sets were dealt with well, but in the clean sets a single sample was alerted on – a driver file for a popular gaming controller which was labelled as a FakeAV trojan. This was enough to deny *Kaspersky* a VB100 award for this product, and to spoil our hopes of a comparative with a 100% pass rate. *Kaspersky*'s corporate line has three passes and two fails, with one no-entry, in the last six tests, and seven passes and four fails from 11 entries in the last two years.

## Kaspersky Endpoint Security 8.0 for Linux

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



As mentioned, the desktop version of *Kaspersky*'s product is fairly similar to the server version in approach. The most noticeable difference was a desktop alert system, which seemed clear and responsive throughout testing. Again, the installation process was thorough and efficient, with the company's own on-access system (based on the redirfs module) compiled and installed cleanly. Operation remains opaque and bizarre, with the control script hidden away and demanding lengthy and complex syntax. For non-*Linux* users, the approach is a little like having a *Windows* program that is run not by double-clicking an icon, but instead by right-clicking it and selecting the 'Sproing!' option, then pressing CTRL-ALT-F13 while licking the left side of the screen to access the controls.

Joking aside, the configuration system does become reasonably usable once it has been bullied into something approaching a normal set-up (by dumping the configuration to a file and adjusting it there), and things seemed generally stable and responsive. Scanning speeds were again sluggish, and overheads fairly heavy, with our set of media and documents the only area to be handled rapidly on demand. Detection was decent though, with a dependably high level throughout the Response sets and the earlier parts of the RAP sets, the proactive week dropping considerably. The WildList was dealt with without issues, but in the clean sets the same file was falsely accused, and *Kaspersky*'s desktop offering is also denied certification by a whisker. The desktop product's test history shows four passes and one fail from five entries in the last six tests; nine passes and two fails in the last two years.

## Norman Endpoint Protection for Linux

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

*Norman*'s product was unique in this month's line-up in being provided without any way to update offline. The

| **Archive scanning** | | ACE | CAB | EXE-RAR | EXE-ZIP | JAR | LZH | RAR | TGZ | ZIP | ZIPX | EXT* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Avast | OD | X/√ | X/√ | √ | √ | √ | X/√ | X/√ | √ | √ | √ | √ |
| | OA | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| AVG | OD | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| | OA | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Avira | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | X | √ |
| | OA | √ | √ | √ | √ | √ | √ | √ | √ | √ | X | √ |
| BitDefender | OD | √ | √ | 8 | 8 | √ | √ | √ | 8 | √ | √ | √ |
| | OA | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Central Command | OD | 2 | √ | √ | √ | √ | X | √ | √ | √ | X | X/√ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| eScan | OD | √ | √ | 8 | 8 | √ | √ | √ | 8 | √ | √ | √ |
| | OA | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| ESET | OD | √ | √ | √ | √ | √ | √ | √ | 5 | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| Frisk | OD | 5 | 5 | 5 | 5 | 5 | √ | 5 | 2 | 5 | 5 | √ |
| | OA | √ | √ | 5 | √ | √ | √ | √ | √ | √ | X | √ |
| Kaspersky AV | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X/√ | X/√ | 1√ | 1/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Kaspersky ES | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X/√ | X/√ | 1/√ | 1/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ |
| Norman | OD | X | √ | 8 | 1 | √ | √ | √ | 8 | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| Sophos | OD | X | X/5 | X/5 | X/5 | X/5 | X/5 | X/5 | X/5 | X/5 | X/5 | X/√ |
| | OA | X | X | X | X | X | X | X | X | X | X | √ |
| VirusBuster | OD | 2 | √ | √ | √ | √ | X | √ | √ | √ | X | X/√ |
| | 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

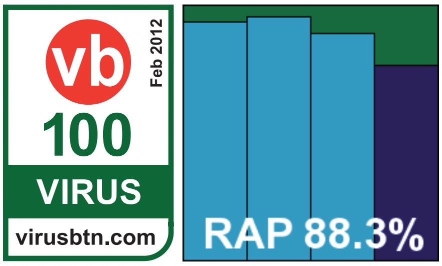
1-9 - Detection of EICAR test file up to specified nesting level

* Detection of EICAR test file with randomly chosen file extension

*Please refer to text for full product names.*

| **Reactive And Proactive (RAP) scores** | VB100 | Reactive | | | Reactive average | Proactive | Overall average |
|---|---|---|---|---|---|---|---|
| | | Week -3 | Week -2 | Week -1 | | Week +1 | |
| Avast | VIRUS 100 | 97.14% | 95.92% | 94.75% | 95.94% | 75.59% | 90.85% |
| AVG | VIRUS 100 | 98.18% | 98.22% | 97.04% | 97.82% | 75.03% | 92.12% |
| Avira | VIRUS 100 | 99.26% | 99.33% | 96.95% | 98.51% | 88.92% | 96.11% |
| BitDefender | VIRUS 100 | 99.50% | 99.12% | 97.74% | 98.79% | 87.98% | 96.08% |
| Central Command | VIRUS 100 | 85.47% | 87.52% | 81.68% | 84.89% | 56.14% | 77.70% |
| eScan | VIRUS 100 | 99.52% | 99.16% | 97.69% | 98.79% | 87.74% | 96.02% |
| ESET | VIRUS 100 | 96.86% | 96.04% | 95.36% | 96.09% | 86.89% | 93.79% |
| Frisk | VIRUS 100 | 72.09% | 73.90% | 65.62% | 70.54% | 63.53% | 68.78% |
| Kaspersky AV | | 96.32% | 96.56% | 94.17% | 95.68% | 73.88% | 90.23% |
| Kaspersky ES | | 96.32% | 96.56% | 94.17% | 95.68% | 73.88% | 90.23% |
| Norman | VIRUS 100 | 93.23% | 95.21% | 88.51% | 92.31% | 76.39% | 88.33% |
| Sophos | VIRUS 100 | 88.02% | 87.55% | 86.04% | 87.20% | 79.25% | 85.21% |
| VirusBuster | VIRUS 100 | 85.47% | 87.33% | 81.68% | 84.83% | 56.14% | 77.66% |

*Please refer to text for full product names.*



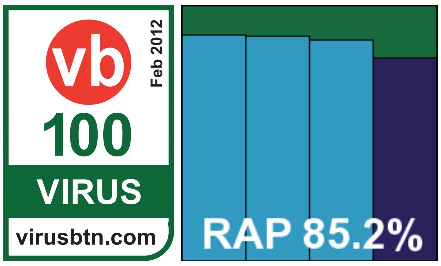
install and set-up process requires Internet access, and was thus run on the deadline day. It took some time, much of which was spent waiting for things to happen in the background – the script returns control with a warning that it won't actually be finished for several minutes, and the product's desktop interface (which seems to be the only way to monitor and control many of its activities) was unavailable for quite a while. When it finally reappeared, it continued to warn that updating and other tasks were ongoing.

Operating the on-demand scanner was at least fairly simple, but controls for the on-access component – which uses *Norman*'s own unique approach of mounting protected file systems in a special way – was limited and unreliable. As with the *Windows* products, we noted that despite setting the controls not to delete or remove infected items, some files disappeared after attempts to access them.

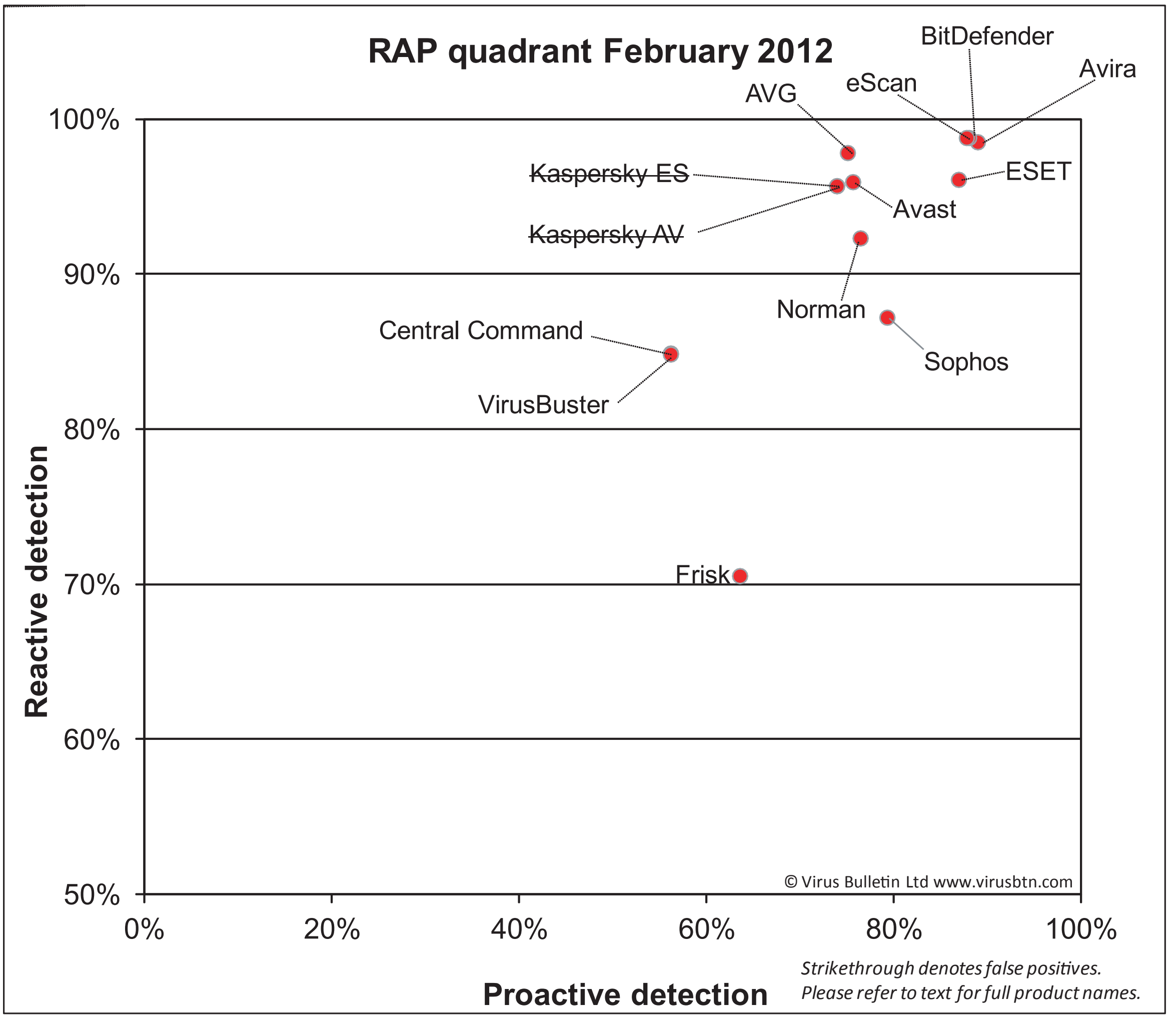
Scanning speeds were very slow, but overheads were not much worse than average, and detection rates were fairly reasonable – decent if not stellar in the Response sets and actually quite impressive in the earlier few weeks of the RAP sets. The WildList and clean sets were handled well, and *Norman* earns a VB100 award. The vendor's test history shows a strong recovery from a rocky period, with five passes and a single fail in the last six tests; eight passes and four fails in the last two years.

## Sophos Anti-Virus for Linux

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



The *Sophos Linux* product is apparently due to be connected to the company's cloud look-up system in the next few months, but for now remains locally based only. The set-up process was one of the simplest this month, with the installer script compiling and installing the company's proprietary



*Strikethrough denotes false positives.*
*Please refer to text for full product names.*

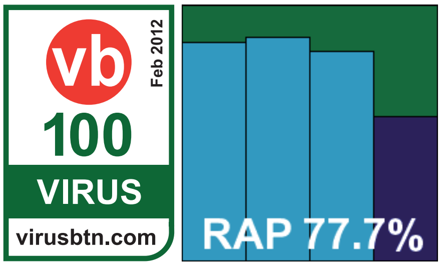
on-access system without complaint and with no need for manual intervention. Operation is a little less transparent than some, with no simple configuration file, and we could find no way of enabling archive scanning on access. Testing proceeded well though, with good stability throughout.

Scanning speeds were very good indeed, with overheads very light, even in the sets containing no archives – hinting that the on-access system is more efficient than most. Detection rates were a little disappointing in the Response sets, and it looks like the product's integration with the cloud is long overdue. Performance across the RAP sets was a little more impressive, with the older items handled noticeably better.

The core sets presented no surprises, and after a bad month last time *Sophos* returns to form, earning a VB100 award without trouble. *Sophos* now has five passes and one fail in the last six tests, and 11 passes in the last two years.

### VirusBuster for Samba Servers

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



Last up this month, *VirusBuster*'s product as usual provides few surprises thanks to its close similarity to the *Central Command* solution which is based on it. The set-up again revolves around an install script, and some simple tweaks to the

*Samba* configuration are required, but we got things up and running fairly quickly with minimal effort. Syntax is clear and simple, and operation generally proved straightforward.

Scanning speeds were not bad, and overheads fairly light, with scores a little below par in most areas but far from disastrous. The core sets were handled well, and another VB100 is duly earned, giving *VirusBuster* a solid record of six passes in the last six tests; 12 in the last two years.

## CONCLUSIONS

As we hoped, there were few major issues this month. The main surprise came in the speed sets, where sluggishness seemed to be the order of the day. This was not helped by our selection of samples for the *Linux* speed set, which contained many more complex archive files than we had expected and thus took considerably longer than hoped to get through. The use of only a single client system also slowed things down, as only one product could be put through the on-access tests at a time, and in most cases the test took longer than a full working day to complete.

In certification terms, only a single file prevented a clean sweep. The file affected two products from the same vendor, which can perhaps count itself rather unlucky on this occasion.

On the whole, products proved reasonably tractable, with some good, clear set-up processes and in general simple operating procedures. A few chose to break free from the standard *Linux* approach to software design, and in places this presented some serious issues, but most of these were overcome with careful reference to documentation. Whether busy server admins would be willing to spend time figuring out products which have wilfully ignored almost universal best practices is up for debate.

As we put the final touches to this report, the next comparative – on *Windows XP* – is already under way. It will be several times larger than this test and is likely to be a much more demanding task. Unfortunately, the unexpected long running time of this test has left little time for the maintenance work we had hoped to fit in, or the long-planned lab move, but we continue to welcome feedback, suggestions, comments and criticisms.

**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 *Red Hat Enterprise Linux 6.2*, *AMD64 Server Edition*. On-access tests were run from a client machine with the same hardware specification running *Microsoft Windows XP SP3 Professional Edition*, x86, connected via *Samba 3.5.10*. For the full test methodology see http://www.virusbtn.com/vb100/about/methodology.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.