Roundup

» Every month we compare tons of software so you don't have to!

LINUX FORMAT On the DVD
» ClamAV 0.95.3
» ClamTk 4.21
» KlamAV 0.46

Antivirus software

Hoping to stay healthy, **Nick Veitch** gets forensic on the available programs.

How we tested...

Although we advocate reading all the documentation and taking care with config files, for this test we've done as little tuning of the software as possible – the defaults should be good enough to keep a computer safe.

We employed the virus test suite, as developed by EICAR (**www.eicar.org/anti_virus_test_file.htm**), the European security organisation. There's nothing tricky here; effectively it's just a pseudo-viral text string that should be easy for all the scanners to pick up. It's provided in several formats, including plain text and Zip files. To complicate things further we included a few large RAW photos, plus the virus test files encoded in a tarball and hidden within an ISO image.

Our selection

- AVG Free p31
- Avira Antivir Pro p31
- ClamAV p32
- Sophos p32
- ClamTk p33
- Avast p33
- BitDefender p34

Pretty much every Linux user thinks they're immune to viruses, but they're wrong. Just recently, malware was found hidden inside an innocuous-looking Gnome theme from a reputable site. Users who installed the theme also got several scripts installed as root that were designed to attack internet targets, but it could easily have been much worse. You see, the problem with thinking that Linux is immune is that sooner or later, something like this happens, and you'll have no protection. Yes, 99% of the time you won't need it. Maybe even 99.9% of the time. But if a virus checker saves you just once a year, we think that's a good enough reason to install one.

Of course, there are other good reasons, not least that you don't want to be blamed in the flame-fest that would result if you accidentally forwarded a virus to your Windows-loving friends. For seconds, even if the virus doesn't affect you, wouldn't you at least like to know that it had somehow made its way on to your precious Linux box?

> "You don't want to be blamed for forwarding a virus to your friends."

For the most part, we expect virus checkers to run without us noticing that they're there, to consume no resources and just get on with things. Extra points are awarded to software that comes close to this ideal, while they're deducted for difficult installs, weak documentation and poor performance.

Many of the clients on test make use of *Dazuko*, which is a kernel module designed to give on-access notifications to userland software – so when you open a file, the module passes the details to any service that wants to know. Some of the checkers rely on an old version of *Dazuko*; we've made a note of these in the review text.

AVG Free

Long-established virus scanning provided free for Linux.

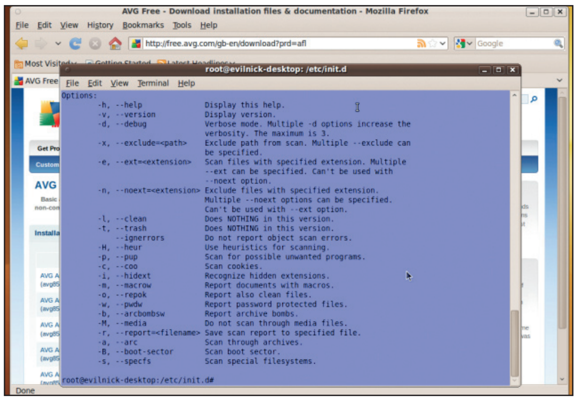
Products bearing the AVG name have a reasonable history in antivirus software, stretching back to 1992. Linux/Unix systems were only added to the lineup in version 7.5 and now lag behind the Windows version (at 9.0), having only had a few updates. Installing the free client is pretty straightforward, no matter what system you're using, because there are packages freely available in RPM, Deb and tarball formats. Installing the tarball might be a slight pain, but as it's binary, there's no need to worry about compiling this, that and the other.

Unlike many of the apps here, there's no GUI for this software. It's designed to be run as a system daemon to scan your files on schedule or on demand. There's an option for on-demand checking with the *Dazuko* kernel module. Starting the daemon is easy if you have some sysadmin skills, and it can be configured to run at boot.

In terms of speed, *AVG Free* did pretty well, but perhaps at the expense of being thorough. Surprisingly, the software failed to find the zipped versions of the virus test file. Since the test file has been around for years, this is pretty inexcusable – it shouldn't be at all hard to find. The only reasonable explanation is that perhaps the software is misconfigured. As part of our tests, we do the minimum amount of configuration to get the program to run. In a production environment, you might want to investigate the docs and the various settings, but even if you did, *AVG Free's* documentation is scantier than a minuscule bikini.

Because of the difficulty in making sure the system is configured and working, as well as the poor results in finding viruses, this wouldn't be one we could recommend for desktop use.

> **"In terms of speed, AVG did well, at the expense of being thorough."**


AVG Free - Download installation files & documentation - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://free.avg.com/gb-en/download?prd=afl
Google
Most Visited
AVG Free
root@evilnick-desktop: /etc/init.d
File Edit View Terminal Help
Done

```
Options:
        -h, --help              Display this help.
        -v, --version           Display version.
        -d, --debug             Verbose mode. Multiple -d options increase the
                                verbosity. The maximum is 3.
        -x, --exclude=<path>    Exclude path from scan. Multiple --exclude can
                                be specified.
        -e, --ext=<extension>   Scan files with specified extension. Multiple
                                --ext can be specified. Can't be used with
                                --noext option.
        -n, --noext=<extension> Exclude files with specified extension.
                                Multiple --noext options can be specified.
                                Can't be used with --ext option.
        -l, --clean             Does NOTHING in this version.
        -t, --trash             Does NOTHING in this version.
            --ignerrors         Do not report object scan errors.
        -H, --heur              Use heuristics for scanning.
        -p, --pup               Scan for possible unwanted programs.
        -c, --coo               Scan cookies.
        -i, --hidext            Recognize hidden extensions.
        -m, --macrow            Report documents with macros.
        -o, --repok             Report also clean files.
        -w, --pwdw              Report password protected files.
        -b, --arcbombsw         Report archive bombs.
        -M, --media             Do not scan through media files.
        -r, --report=<filename> Save scan report to specified file.
        -a, --arc               Scan through archives.
        -B, --boot-sector       Scan boot sector.
        -s, --specfs            Scan special filesystems.

root@evilnick-desktop:/etc/init.d#
```

› ***AVG Free* isn't well-documented or easy to set up, but it works, some of the time.**

LINUX FORMAT Verdict

AVG Free

Version: 8.5
Website: http://free.avg.com
Price: Free

» *It performs so poorly and comes with such minimal documentation that it's not worth it, even if it is free.*

Rating 2/10

Avira Antivir Professional

Command line scanner with a really low overhead.

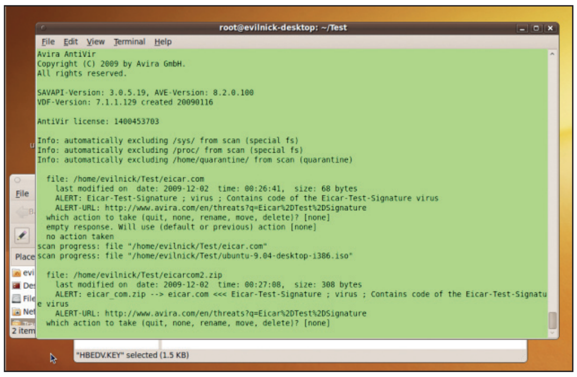
Avira Antivir, if you can get past the avoidably ugly name, lives in the shady realms of the command line, though it needs no real knowledge of *Bash* to install or use. Download the archive and run the install script within to set everything up. There follows a series of questions about which options are to be installed, whether to use the scan-on-access service (which requires *Dazuko*) and where you've put your keyfile. The latter was the only hitch on installing. For reasons still unclear, the website provided us with a trial key, but it didn't work. If you have the same problem, pretend you live in the USA...

Once we had it installed, we noticed the presence of a configuration file and daemons automatically being installed to run the software on startup. Running the test scan was surprising – the software seemed to be instantaneous, and barely took up any memory or CPU cycles at all. It would have been easy to believe that nothing had happened, but the scanner identified all of our infected files and offered to quarantine them.

The default settings seem good enough and the virus database is kept well up to date, so you needn't fear that you need to be extra vigilant in the configuration. It works impressively quickly – it's just a shame that the on-access scanning isn't available for modern kernels.

Avira does have free versions of its other antivirus software, but all the Linux versions come under the Professional department, so there's no dispensation if you're a non-business user. That said, the licensing structure doesn't make it expensive: £25 for a year-long single-user licence.

> **"The website provided us with a trial key, but it didn't work."**


root@evilnick-desktop: ~/Test
File Edit View Terminal Help
File
Places
"HBEDV.KEY" selected (1.5 KB)
2 items

```
Avira AntiVir
Copyright (C) 2009 by Avira GmbH.
All rights reserved.

SAVAPI-Version: 3.0.5.19, AVE-Version: 8.2.0.100
VDF-Version: 7.1.1.129 created 20090116

AntiVir license: 1400453703

Info: automatically excluding /sys/ from scan (special fs)
Info: automatically excluding /proc/ from scan (special fs)
Info: automatically excluding /home/quarantine/ from scan (quarantine)

  file: /home/evilnick/Test/eicar.com
    last modified on  date: 2009-12-02  time: 00:26:41,  size: 68 bytes
    ALERT: Eicar-Test-Signature ; virus ; Contains code of the Eicar-Test-Signature virus
    ALERT-URL: http://www.avira.com/en/threats?q=Eicar%2DTest%2DSignature
  which action to take (quit, none, rename, move, delete)? [none]
  empty response. Will use (default or previous) action [none]
  no action taken
scan progress: file "/home/evilnick/Test/eicar.com"
scan progress: file "/home/evilnick/Test/ubuntu-9.04-desktop-i386.iso"

  file: /home/evilnick/Test/eicarcom2.zip
    last modified on  date: 2009-12-02  time: 00:27:08,  size: 308 bytes
    ALERT: eicar_com.zip --> eicar.com <<< Eicar-Test-Signature ; virus ; Contains code of the Eicar-Test-Signatu
e virus
    ALERT-URL: http://www.avira.com/en/threats?q=Eicar%2DTest%2DSignature
  which action to take (quit, none, rename, move, delete)? [none]
```

› **It's impressive in speed and low resource use, but not really in the results stakes.**

LINUX FORMAT Verdict

Avira Antivir Professional

Version: 3.0.5
Website: www.avira.com
Price: £25

» *Pretty average all-round, and not worth paying for when there are better alternatives out there.*

Rating 5/10

»

ClamAV

Flying the flag for open source antivirus software.

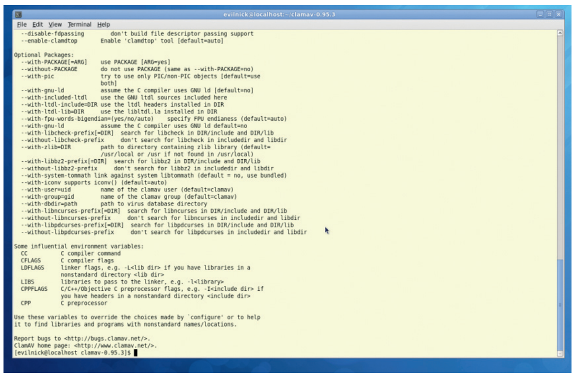
ClamAV was originally developed as a mail scanner, and there are plenty of configuration options and tools for integrating it into your local mailserver. For the same reason, it also supports a lot of archive formats that are commonly used for email attachments, though some of these may have been disabled if you installed *ClamAV* through a distro package.

It isn't complicated to compile, since the source is well documented, doesn't have a great deal of demands in terms of third-party libraries and gives you the opportunity to ensure the options you want are installed.

Once installed, *ClamAV* consists of two main parts. *Clamscan* is the command line tool to scan whatever you point it at. As with most commands, there's a host of switches to control behaviour and, among other things, this accounts for its versatility.

The second part to *ClamAV* is *clamd*, the daemon process that runs in the background and can be configured to scan at regular intervals or watch certain places. Like some of the other software included here, it can be configured to offer on-access scanning (including, thanks to it being open source, support for the latest version of *Dazuko*) and there's useful guidance on how to enable this on the *ClamAV* site.

The major disappointment with *ClamAV* was its failure to scan the ISO image file properly. This was a bit confusing, because the software did once support ISO file scanning, though a search through the documentation now reveals no clues. As we had a testing policy of using defaults, it would have been unfair on the other software to mess around too much. Suffice to say, there didn't seem to be a simple way of getting this to work.



```
evilnick@localhost:~/clamav-0.95.3
File  Edit  View  Terminal  Help
  --disable-fdpassing       don't build file descriptor passing support
  --enable-clamdtop       Enable 'clamdtop' tool [default=auto]

Optional Packages:
  --with-PACKAGE[=ARG]    use PACKAGE [ARG=yes]
  --without-PACKAGE       do not use PACKAGE (same as --with-PACKAGE=no)
  --with-pic              try to use only PIC/non-PIC objects [default=use
                          both]
  --with-gnu-ld           assume the C compiler uses GNU ld [default=no]
  --with-included-ltdl    use the GNU ltdl sources included here
  --with-ltdl-include=DIR use the ltdl headers installed in DIR
  --with-ltdl-lib=DIR     use the libltdl.la installed in DIR
  --with-fpu-words-bigendian=(yes/no/auto)    specify FPU endianess (default=auto)
  --with-gnu-ld           assume the C compiler uses GNU ld default=no
  --with-libcheck-prefix[=DIR]  search for libcheck in DIR/include and DIR/lib
  --without-libcheck-prefix     don't search for libcheck in includedir and libdir
  --with-zlib=DIR         path to directory containing zlib library (default=
                          /usr/local or /usr if not found in /usr/local)
  --with-libbz2-prefix[=DIR]  search for libbz2 in DIR/include and DIR/lib
  --without-libbz2-prefix     don't search for libbz2 in includedir and libdir
  --with-system-tommath link against system libtommath (default = no, use bundled)
  --with-iconv supports iconv() (default=auto)
  --with-user=uid         name of the clamav user (default=clamav)
  --with-group=gid        name of the clamav group (default=clamav)
  --with-dbdir=path       path to virus database directory
  --with-libncurses-prefix[=DIR]  search for libncurses in DIR/include and DIR/lib
  --without-libncurses-prefix     don't search for libncurses in includedir and libdir
  --with-libpdcurses-prefix[=DIR]  search for libpdcurses in DIR/include and DIR/lib
  --without-libpdcurses-prefix     don't search for libpdcurses in includedir and libdir

Some influential environment variables:
  CC          C compiler command
  CFLAGS      C compiler flags
  LDFLAGS     linker flags, e.g. -L<lib dir> if you have libraries in a
              nonstandard directory <lib dir>
  LIBS        libraries to pass to the linker, e.g. -l<library>
  CPPFLAGS    C/C++/Objective C preprocessor flags, e.g. -I<include dir> if
              you have headers in a nonstandard directory <include dir>
  CPP         C preprocessor

Use these variables to override the choices made by `configure' or to help
it to find libraries and programs with nonstandard names/locations.

Report bugs to <http://bugs.clamav.net/>.
ClamAV home page: <http://www.clamav.net/>.
[evilnick@localhost clamav-0.95.3]$ 
```

› **Compiling *ClamAV* yourself enables you to get the features you want.**

> **"The disappointment was its failure to scan the ISO image file."**

LINUX FORMAT Verdict

ClamAV

Version: 0.95.3
Website: www.clamav.net
Price: Free

» *This gets great kudos for being open source, but loses points for failing the ISO test.*

Rating 8/10

Sophos Anti-Virus

The antivirus heavyweights continue to support Linux – but is it worth it?

UK-based Sophos has come to be a recognisable name in the world of business-oriented antivirus software. Earlier versions of *Sophos* have appeared in the pages of **LXF** and fared well, so it's good to see that Sophos continues to support Linux.

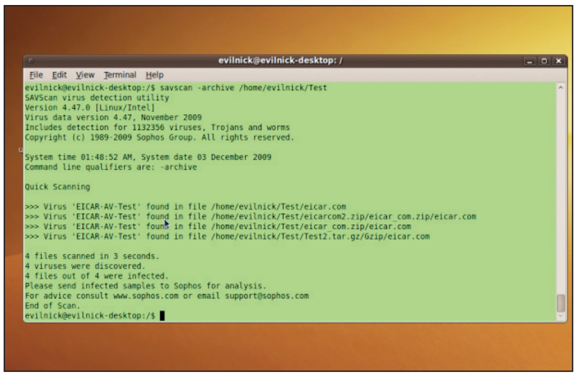
This software is commercial and there are no freebies for desktop users, but there's a trial version available.

Although the install script gamely suggests that it's trying to build the on-access support for the kernel, it's sadly trying to build an old 2.x module for *Dazuko*. It's hard in many repescts for the developers – they want to support the business and server distros, so they've opted for 2.x support. Unfortunately, 2.x won't work with the latest kernels, so eventually the software is going to need to support 3.x.

Sophos has an interesting collection of interfaces. Your scanning can be viewed and manipulated remotely over the web. As well as its own server interface for a simple lookup via HTTP, there's also a *Webmin* module for *Sophos*. *Webmin* is a web-based sysadmin tool, which for many years was a popular way of running remote machines and servers, so this adds some weight to *Sophos*'s claim of being an integrated and manageable solution.

Running scans from the shell is no problem and a shell client lends itself to being scriptable and run via a *Cron* job at an appropriate time of day.

Although not the fastest on test, it wasn't that slow or cumbersome either. Sadly, for something that seemed so large, *Sophos* also failed the virus test, with the usual flaw of not checking inside the ISO files – which is odd, because the scan took long enough.



```
evilnick@evilnick-desktop: /
File  Edit  View  Terminal  Help
evilnick@evilnick-desktop:/$ savscan -archive /home/evilnick/Test
SAVScan virus detection utility
Version 4.47.0 [Linux/Intel]
Virus data version 4.47, November 2009
Includes detection for 1132356 viruses, Trojans and worms
Copyright (c) 1989-2009 Sophos Group. All rights reserved.

System time 01:48:52 AM, System date 03 December 2009
Command line qualifiers are: -archive

Quick Scanning

>>> Virus 'EICAR-AV-Test' found in file /home/evilnick/Test/eicar.com
>>> Virus 'EICAR-AV-Test' found in file /home/evilnick/Test/eicarcom2.zip/eicar_com.zip/eicar.com
>>> Virus 'EICAR-AV-Test' found in file /home/evilnick/Test/eicar_com.zip/eicar.com
>>> Virus 'EICAR-AV-Test' found in file /home/evilnick/Test/Test2.tar.gz/Gzip/eicar.com

4 files scanned in 3 seconds.
4 viruses were discovered.
4 files out of 4 were infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com or email support@sophos.com
End of Scan.
evilnick@evilnick-desktop:/$ 
```

› **The *Sophos* client software is accessible via the command line only.**

> **"A shell client lends itself to being scriptable and run via a Cron job."**

LINUX FORMAT Verdict

Sophos Anti-Virus

Version: 4.47
Website: www.sophos.com
Price: £67

» *Corporate scanning, but it isn't as comprehensive as you might hope and again failed the ISO test.*

Rating 4/10

ClamTk

The one with GTK and Perl.

ClamTk is almost the default front-end to *clamscan*, in that even distros that prefer KDE to Gnome often install it, so it must have something going for it.

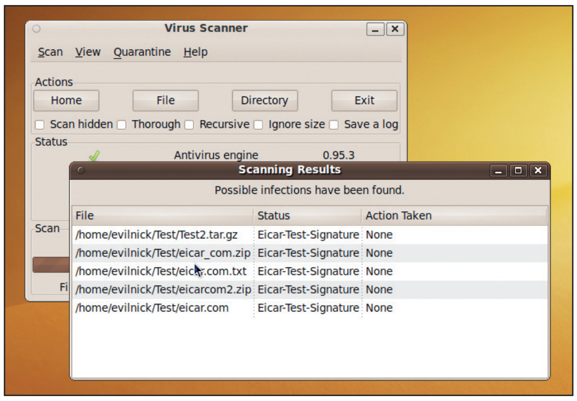
When it runs, this tool will check for the current version of itself, the *ClamAV* back-end and virus signature files, displaying the results in an easily-understood status table. Buttons along the top give quick access to the scanning functions, while various options can be turned on and off via the switches below. You may prefer to use the menu for some operations, but there isn't a lot that can go wrong with this simple client.

One feature worth noting is the searchable history log, which tracks any previous naughtiness and what files were involved, though it lacks some of the useful features of other front-ends such as *KlamAV*.

As the most popular front-end to *ClamAV*, you'll find up-to-date packages in almost every distro repository that carries *ClamAV*, though there's a quick note for Fedora users: for some reason the package currently showing for Fedora 12 is old and doesn't actually work, but you can get an RPM built by the developer at the *ClamTk* website. If you want to build it from source, you'll need little other than up-to-date Perl libraries and the standard *GTK* stuff.

A new feature is an option to restore files you might inadvertently have quarantined, but later want to let out again. It's hard to imagine this was top of the 'must have' list for users, but on the other hand, this small and simple GUI client isn't missing much at all.

Obviously, with either of the graphical clients running on top of *ClamAV*, the resource usage rises a little, but as *ClamTk* makes use of standard *GTK* libraries, it isn't really going to add much to the bill. There's a minimal amount of extra memory consumed and the difference in speed wasn't measurable, so Perl and *GTK* was obviously a good decision.


Virus Scanner
Scan View Quarantine Help
Actions
Home
File
Directory
Exit
□ Scan hidden □ Thorough □ Recursive □ Ignore size □ Save a log
Status
Scan
Fi

Antivirus engine 0.95.3

Scanning Results

Possible infections have been found.

File	Status	Action Taken
/home/evilnick/Test/Test2.tar.gz	Eicar-Test-Signature	None
/home/evilnick/Test/eicar_com.zip	Eicar-Test-Signature	None
/home/evilnick/Test/eicar.com.txt	Eicar-Test-Signature	None
/home/evilnick/Test/eicarcom2.zip	Eicar-Test-Signature	None
/home/evilnick/Test/eicar.com	Eicar-Test-Signature	None

› ***ClamTk* has a simple interface that enables straightforward virus scanning.**

LINUX FORMAT Verdict

ClamTk

Version: 4.2
Website: http://clamtk.sourceforge.net
Price: Free

» *Simple GTK interface makes scanning straightforward and easy, despite the lack of frills.*

Rating 8/10

Avast

Harrrr! Splice the mainbrace and stand by to repel boarders, me hearties!

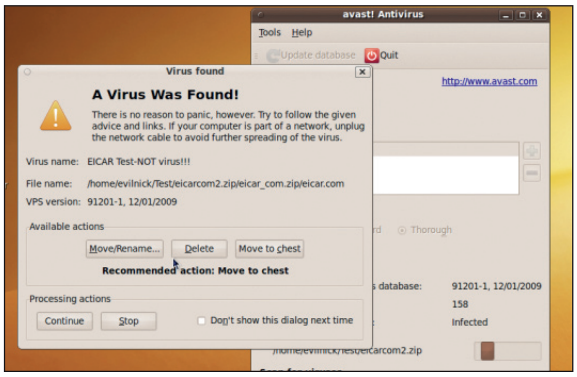
This nautically-themed gem may not be top of your list when you think about antivirus software, but the developer – Czech-based Alwil – has been creating antivirus tools since 1991, so there's a pedigree here. This version mirrors Alwil's Windows software in terms of features, and is available free of charge for personal use.

Downloads come from the website as RPM, Deb or binary archives for the Linux version and all are pretty easy to install. As you might expect with commercially-oriented software, there are few dependencies, but the GUI does make use of the *GTK* libraries, and the resulting app looks rather Gnome-like and not at all dissimilar to *ClamTk*.

Scanning manually using the graphical interface, you'll see a few extra buttons. Select the Thorough option – if you're not being thorough, you may as well not bother. Engaging this mode does pretty much double the time it takes to perform a test, but it pays dividends: *Avast* managed to find all of our hidden fake-viruses, even though it had to search through a Zip file embedded in an ISO image to complete the set. A curious follow-on to the Jolly-Jack-tar theme they have going on is that quarantined viruses are stored in what they call a chest, which is all very amusing once you get the hang of what's going on. Handily, you can also keep a list of commonly scanned locations for quick checking.

The command line tool is simple to use. Run it with no options to see the switches available. Unusually, this has fine control of the archive formats supported (like *ClamAV*) so if you want to do some very specific scanning, this may be the one to pick.

> **"Handily, you can keep a list of commonly scanned locations."**



A Virus Was Found!

There is no reason to panic, however. Try to follow the given advice and links. If your computer is part of a network, unplug the network cable to avoid further spreading of the virus.

Virus name: EICAR Test-NOT virus!!!
File name: /home/evilnick/Test/eicarcom2.zip/eicar_com.zip/eicar.com
VPS version: 91201-1, 12/01/2009

Recommended action: Move to chest

database: 91201-1, 12/01/2009
158
Infected
/home/evilnick/Test/eicarcom2.zip

› **We've caught something! Even though we did put it in there in the first place.**

LINUX FORMAT Verdict

Avast

Version: 1.3
Website: www.avast.com
Price: Free

» *A definite winner on talk-like-a-pirate day, and actually, it's pretty good the rest of the time too.*

Rating 9/10

»

BitDefender

Glitzy and glamorous, and it delivers the goods.

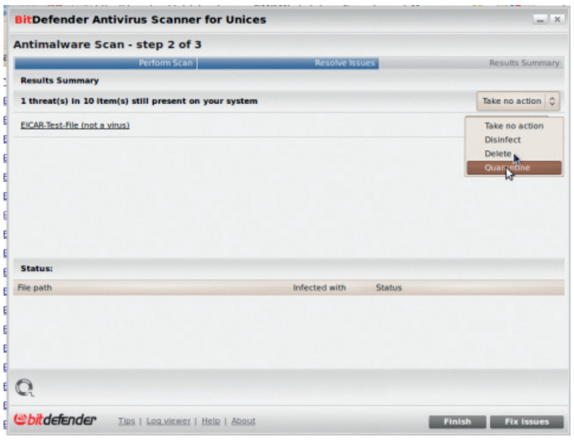
BitDefender is a reputable security company, and this antivirus solution sits within a giant cluster of antivirus software for different platforms. This version is provided free of charge for personal desktop users. You have to register first and get a trial key, which can then be turned into a proper keyfile if you're accepted. The real keyfile will last for about six months, at which point you can simply sign up and get another one.

Running the GUI is a slight surprise. It's built using custom widgets, so although it's essentially leveraging *GTK*, there is nothing very Gnome, KDE or even Linux-like about it. That said, it's easy to navigate and use. The initial run will download the latest definitions and check the software is up to date before you start scanning.

BitDefender gained top marks in the scanning test by finding all the suspect files (and correctly identifying them as the same 'threat', for a super-bonus gold star). Naughty files can be processed in a number of ways, including quarantining them or attempting to remove them, and you'll be reminded and warned about existing threats on your machine if you choose to take no action initially.

The settings screen is easy to follow, thanks to the proliferation of tooltips on every button and text-entry point, and they are also pretty concise. For example, the archive setting is just a simple toggle switch.

> "Running the GUI is a slight surprise: it's built using custom widgets. "



BitDefender Antivirus Scanner for Unices

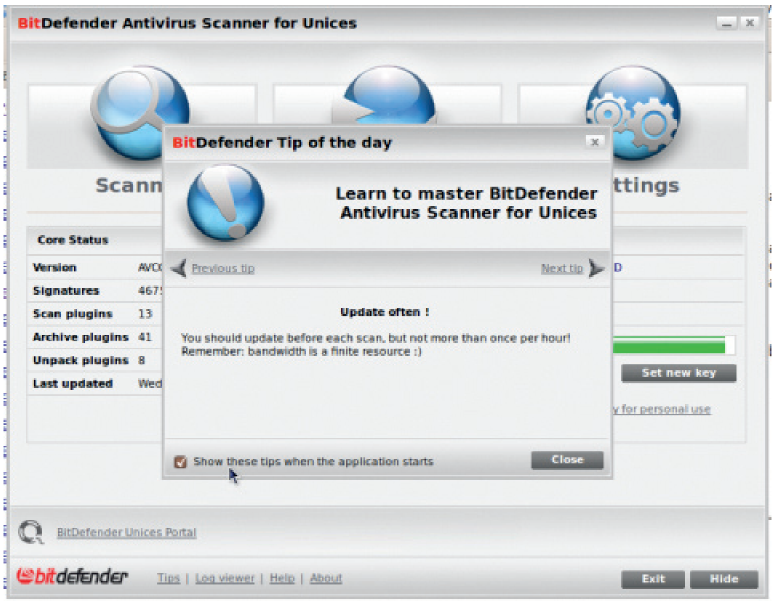
Antimalware Scan - step 2 of 3

Results Summary

1 threat(s) in 10 item(s) still present on your system — Take no action

EICAR-Test-File (not a virus)

› *BitDefender* asks you what you'd like to do with files on your system that are potentially harmful.



BitDefender Antivirus Scanner for Unices

BitDefender Tip of the day

Learn to master BitDefender Antivirus Scanner for Unices

Update often !

You should update before each scan, but not more than once per hour!
Remember: bandwidth is a finite resource :)

☑ Show these tips when the application starts

Core Status	
Version	AVC(
Signatures	467!
Scan plugins	13
Archive plugins	41
Unpack plugins	8
Last updated	Wed

› **A helpful tip of the day pops up over the UI's gigantic buttons.**

Thorough check

This might not give the fine-grain control that some people hanker after, but it seems like a sensible compromise – if you want to search through archives, you want to search through them all, not just ones of a specific type. The software warns that this will increase the resource overhead during scans, but neither the CPU cycles grabbed or the memory allocated seemed to be excessive compared with other software in the test. In fact, it put in the fastest performance of the scanners that found all the suspect files. *BitDefender*'s memory usage was higher than the other programs on test here, but that can partly be explained by the fact that it actually tested the files within the test ISO image, which some didn't.

There's a command line tool available for those who want to specify every available option, which also means that *BitDefender* can be scripted for other uses, such as checking mail or network shares if needed. It doesn't give quite as much control as, for example, *ClamAV*, when it comes to types of archive to include or patterns of files to avoid, but is manageable enough, and you could embed it in a more complicated script if your needs so demand.

BitDefender also includes an optional drop box for quick, one-off scans, which is a thoughtful addition, if somewhat un-Linuxy in execution – there's something strange about dropping files on to the red shredded logo device that floats in the corner of the screen, but it does work on Gnome and KDE desktops. About the only negative point to be found is that the GUI interface is perhaps a bit large and overdramatic. It takes up a considerable amount of screen real estate for what's essentially a one-click operation, which may be annoying if you use it regularly. The drop box may solve this in part, but perhaps a system tray widget would be better. Overall though, this put in an impressive and speedy performance that would be hard to beat.

LINUX FORMAT Verdict

BitDefender

Version: 2.1
Website: www.bitdefender.com
Price: Free

» *A great all-round performer. It's fast and easy to use, although the interface is a little bit in-your-face.*

Rating 9/10

Antivirus software

The verdict

BitDefender 9/10

Choosing an antivirus system to suit you depends on a number of factors, not least how much of a risk viruses are to you. If you're simply running a Linux desktop for personal use, there probably isn't an urgent need for you to spend time, money and the overhead of clock-cycles to check every file that comes near your system rigorously. If you use your Linux box to share files with Windows machines, then there's a bit more of a point. Also, as we've seen, sometimes it's better to use a command line tool, for example if you wish to build scripts or execute periodic checks through the *Cron* system.

We were impressed with the abilities of most of the packages included in the Roundup, but surprised that some of the commercial versions seemed less effective at finding viruses. The *AVG* software fared particularly badly at this.

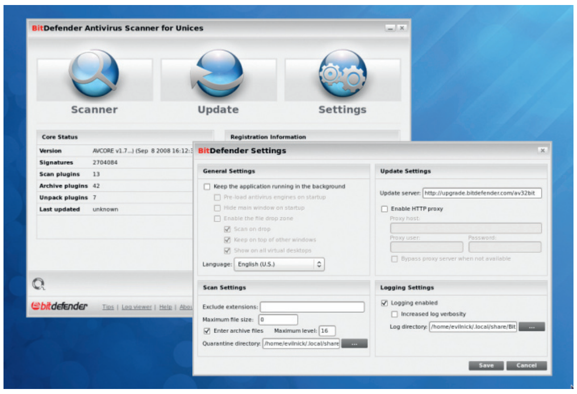
ClamAV will always be a favourite for Linux users because of its open source nature, choice of *GTK* or KDE GUIs and the way that it's kept up to date regularly. As the software development is supported by SourceFire (the company behind *Snort* and various intrusion detection systems) it can't be said to be just another temporary project that'll be here today and gone tomorrow. The *ClamAV* software is also popular running on the Windows platform too.

And the winner is...

Ultimately, *BitDefender* had the performance and accuracy needed to win. It wasn't the fastest on test, but neither was it the slowest. Changing the options makes a big difference to the performance, but we're of the opinion that if you want to run antivirus software, you should run it at the most paranoid level available. *BitDefender* competently found all the virus files, identified them and suggested appropriate action, so it's difficult to see what more it could do. It was simple to use and the updates to the virus database seem to be regular. The command line app is configurable and versatile too, so you can easily set up regular scans.

> "Ultimately, BitDefender had the performance and accuracy to win."

For those who baulk at the idea of running a virus scanner that takes up most of the screen, there's *Avast*. This software is a relative newcomer to the Linux scene, but performed as well as *BitDefender* in finding viruses. The interface was also simple to use and the command line tool is just as useful.


BitDefender Antivirus Scanner for Unices
Scanner
Update
Settings
bitdefender
Tips | Log viewer | Help | Abou

Core Status
Version AVCORE v1.7...) (Sep 8 2008 16:12:
Signatures 2704084
Scan plugins 13
Archive plugins 42
Unpack plugins 7
Last updated unknown

Registration Information

BitDefender Settings

General Settings
□ Keep the application running in the background
□ Pre-load antivirus engines on startup
□ Hide main window on startup
□ Enable the file drop zone
☑ Scan on drop
☑ Keep on top of other windows
☑ Show on all virtual desktops
Language: English (U.S.)

Update Settings
Update server: http://upgrade.bitdefender.com/av32bit
□ Enable HTTP proxy
Proxy host:
Proxy user: Password:
□ Bypass proxy server when not available

Scan Settings
Exclude extensions:
Maximum file size: 0
☑ Enter archive files Maximum level: 16
Quarantine directory: /home/evilnick/.local/share

Logging Settings
☑ Logging enabled
□ Increased log verbosity
Log directory: /home/evilnick/.local/share/Bit

Save Cancel

› ***BitDefender* provides reliable security and is easy to use.**

For die-hard free software fans, *ClamAV* is definitely good enough, but be careful how you configure it, or what you use it to check for. As long as you're aware of what files it's scanning and which ones might need further investigation, you should be safe.

We should close by saying that the number of Linux viruses that could possibly damage your system in any way is currently less than 10, so don't have any nightmares. LXF

Over to you

Do you think *ClamAV* should have won simply because it's open source? How concerned are you about viruses? Have you ever unwittingly transferred a Windows virus on to someone else? We'd love to hear from you – email your opinion of the Roundup to **lxf.letters@futurenet.co.uk**

Table of features

Name	Web	Version	Licence	Price	Trial version?	Toolkit	Memory usage	Disk usage	On access	Time to test	Test results
AVG Free	free.avg.com/us-en/download?prd=afl	8.5	Commercial	Free	n/a	Shell	95MB	75MB	via plugin	5.4s	2
Avira Antivir Professional	www.avira.com	3.0.5	Commercial	£25	✔	Shell	6MB	54MB	Dazuko 2	1s	4
Avast!	www.avast.com	1.3.0	Commercial	Free	n/a	GTK	82MB	32MB	✘	54s	6
BitDefender	www.bitdefender.com	7.6.4	Commercial	Free	n/a	wxWidgets	140MB	75MB	✘	16s	6
ClamAV	www.clamav.net	0.95.3	GPL	Free	n/a	Shell	25MB	28MB	Dazuko 2/3	11s	4
ClamTk	clamtk.sourceforge.net	4.2	GPL	Free	n/a	GTK	27MB	29MB	✘	12s	4
Sophos	www.sophos.com	4.47	Commercial	67	✔	Web	74MB	311MB	Dazuko 2	36s	4