



EXCERPTS FROM VIRUS BULLETIN COMPARATIVE REVIEWS JUNE – OCTOBER 2008

VIRUS BULLETIN VB100 TESTING

The basic requirements for a product to achieve VB100 certification status are that a product detects, both on demand and on access, in its default settings, all malware known to be 'In the Wild' at the time of the review, and generates no false positives when scanning a set of clean files.

Various other tests are also carried out as part of the comparative review process, including speed measurements. While the results of these secondary tests do not affect a product's qualification for VB100 certification, they are included to provide the reader with a better overall picture of product performance.

JUNE 2008: UBUNTU LINUX 8.04LTS SERVER EDITION

The June 2008 comparative review was performed on *Ubuntu Linux* – a relative newcomer to the scene compared to the likes of *SUSE* and *Red Hat*, the even more venerable *Slackware* and, of course, *Debian*, from which *Ubuntu* evolved. *Ubuntu*'s focus on friendly usability, stability and consistent updating has brought strong penetration of desktops – a poll held last summer found over 30% of respondents were using it, with its nearest rival, *OpenSUSE*, at 19% and *Debian* at 11%. At the server level fewer details are available, but the server edition seemed more appropriate to our purposes; of course this selection brought with it the likelihood of some compromises in usability, with any cuddly ease of use likely to have been stripped away in favour of efficiency, security and robustness.

The test sets for the June 2008 comparative review were aligned with the March 2008 WildList, which was released a few weeks prior to the test set and product submission deadlines. The latest WildList included a fairly large number of new additions, but these were concentrated in a few

families – most notably a large swathe of W32/OnlineGames trojans, showing further evolution of the WildList into the cybercrime-ridden modern world. Quite a few older items fell from the list, including several strains of W32/Mytob and W32/MyDoom, and also the veteran W32/Nimda.

Other test sets were expanded by a minimal amount for this test, with only a handful of items added to the clean and infected sets and the meagre set of *Linux* samples dusted off. The most significant addition was the insertion of a set of *Linux* files into the clean set, to form an extra part of the speed measurements.

ESET Security 3.0.3

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Linux	100.00%
Worms & bots	100.00%	Legacy	100.00%
File infectors	100.00%	False positives	0

The *ESET* installation process used the .deb package method, and proved both fast and efficient. On-access scanning could be implemented using either *dazuko* or the *Samba* VFS path, and the latter was adopted at the request of the developers. This proved simple to get working once I had navigated my way around the setup, and the command-line scanner was a joy to operate.

Scanning speeds were not as eye-watering as usual, but they seemed much quicker on the infected sets, suggesting that the clean items were being subjected to some thorough probing. With excellent detection and no false positive issues, *ESET* storms its way to a record 50th VB100 award.



**AUGUST 2008:
WINDOWS XP SERVICE PACK 3**

The August 2008 comparative review was performed on *Windows XP*. With the platform’s slicker, more advanced successor *Windows Vista* now well past its launch stage and settled in as the default operating system for new PCs, *Windows XP* has maintained its dominance as the platform of choice for the majority of PC users. Many businesses continue to run *XP* on their workers’ desktops, even where this entails removing *Vista* from new purchases. At this rate, *XP* looks set still to be the most widely used *Windows* version when the next new release, the successor to *Vista* currently going by the title ‘Windows 7’, hits the shelves – currently scheduled for around two years’ time.

The test sets for the August 2008 comparative review were frozen on 20 June, using the April WildList for the core certification set, with the product submissions taken on 24 June.

The false positive set saw expansion with new files and packages, and the other test sets were also extended, most notably the polymorphic set which saw several new items introduced in fairly limited numbers. The legacy set of older and more obscure items was left out of this test and in its place was a new set of trojans – a selection of several thousand samples gathered over the course of the previous six months or so.

ESET NOD32 Antivirus 3.0.667.0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.84%
Worms & bots	100.00%	File infectors	100.00%

False positives 0

ESET’s installer, these days adorned with the rather groovy robot that has become the company’s talisman, runs through a fairly standard set of options, with the whole thing running through from zero to protected in less than a minute and no reboot required.

With a splendid depth of options available in the advanced pages, more than plenty for the most demanding user, a few tweaks had everything just so and testing powered through in excellent time. A small issue appeared after scanning the full infected test sets in a single run on demand, in which the GUI appeared to hang and ceased to respond. Shutting it down with the task manager and restarting it soon put a stop to this however, and on-access scanning continued throughout this hiccup



without issues. Detection rates were near perfect, and false positives absent, thus another VB100 award is added to *ESET*’s record tally.

OCTOBER 2008: WINDOWS SERVER 2008

The October 2008 comparative review moved to an entirely new platform: the server version of *Microsoft*’s latest iteration of *Windows*. The *Server 2008* platform shares a code base with *Vista*, with many tweaks and improvements in a variety of areas, but sensibly avoiding the rather showy and resource-hungry cosmetic adjustments which most users will identify with the new breed of *Windows* systems.

The test sets for the October 2008 review saw some considerable evolution. Starting with the core of the VB100 sets, the WildList set was aligned with the July issue of the WildList, released about a week before the product submission deadline. The changes in the list from that used in the previous test included an impressive swathe of new arrivals, the vast majority of which were trojans that target online gamers and go by the fairly straightforward title of ‘W32/OnlineGames’. A few of the more interesting items on the list were removed, including several of the W32/Virut variants, but enough of these highly polymorphic viruses remained to provide a frisson of danger for those products which had previously had difficulties providing full coverage of these items.

Additions to the clean test set included a selection of drivers and system tools acquired as part of the process of enabling the test systems and the new platform to interact, as well as a collection of packages downloaded as freeware or trial installations, this month focusing on web development tools.

The combination of these changes to the test sets with the new platform seemed to provide a pretty tough challenge for those vendors striving for the glory of a VB100 award, but we also paid attention to the additional information provided for our readers. The zoo collections saw another round of development towards a more flexible and relevant set of challenges, with the dwindling test set of simple file-infecting viruses being retired to the legacy set for the time being. Replacing these was a substantial new selection of trojans, replacing entirely the set used in the last review with fresh samples gathered in the last two months. The set of worms and bots saw a smaller amount of updating.

ESET NOD32 Antivirus 3.0.672.0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	89.00%
Worms & bots	100.00%	False positives	0

ESET's highly regarded flagship product was subjected to a major overhaul not long ago, and the stylish new look remains impressive both visually and in usability terms. Tweaking the controls to fit our needs was as usual a delight, and testing zoomed along at its usual rapid pace. Scanning of the extremely large new test sets proved a little more sluggish, presumably as the product's strong heuristics kicked in, and on-access behaviour in the new trojan set was also a little odd, with many items not blocked on simple access but treated more severely when copying to the system or even browsing folders in *Explorer*.



Analysis of results showed the product's usual excellent detection rates and yet more splendid scanning speeds over the clean sets, and with nothing missed in the WildList set ESET adds a record 52nd VB100 award to its tally.



ESET, 610 West Ash St, Suite 1900,
San Diego, CA 92101, USA

Tel: +1 619 876 5400, Fax: +1 619 437 7045

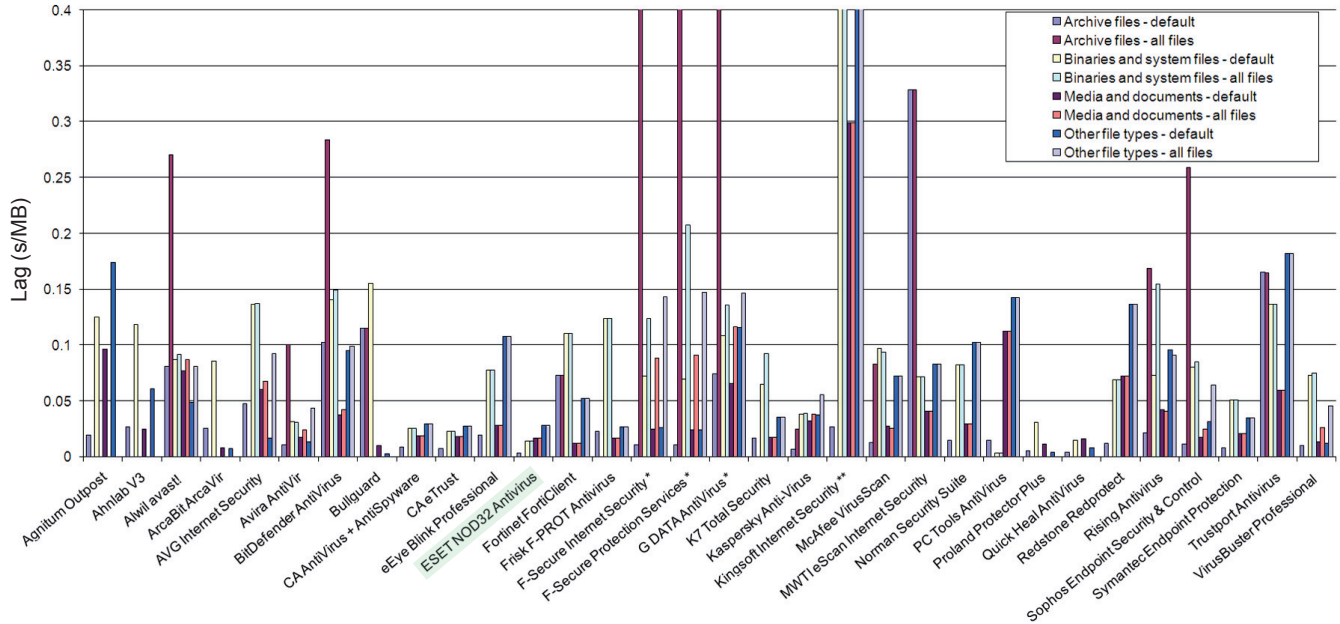
Email: sales@eset.com, Web: <http://www.eset.com/>.

June 2008 on-demand (OD) and on-access (OA) detection	WildList viruses		Worms & bots		File infector viruses		Polymorphic viruses		Linux samples		Legacy samples		Clean sets	
	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	FP OD OA	Susp. OD OA
Alwil avast!	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	319 319	87.13% 87.13%	2 2	96.67% 96.67%	1027 1027	97.02% 97.02%	2 2	
AVG Anti-Virus	0 0	100.00% 100.00%	1 1	99.94% 99.94%	7 7	98.43% 98.43%	691 691	73.89% 73.89%	3 6	88.33% 71.67%	710 710	95.83% 95.83%		
Avira AntiVir	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	6 2	66.67% 93.33%	0 0	100.00% 100.00%		
BitDefender Security	0 0	100.00% 100.00%	0 0	100.00% 100.00%	2 2	98.95% 98.95%	0 0	100.00% 100.00%	4 4	93.33% 93.33%	9 9	99.93% 99.93%		
Doctor Web Dr.Web	16 16	97.55% 97.55%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	3 3	12 12
ESET Security	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%		
Frisk F-PROT	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	
F-Secure Linux Security	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.88% 99.88%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	
Kaspersky Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.88% 99.88%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	
Microworld eScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.88% 99.88%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	3 3
Norman Virus Control	0 0	100.00% 100.00%	0 0	100.00% 100.00%	7 7	99.15% 99.15%	765 916	73.47% 66.94%	0 6	100.00% 66.67%	269 269	99.00% 99.00%		
Quick Heal	0 0	100.00% 100.00%	1 1	99.87% 99.87%	9 9	98.43% 98.43%	808 808	83.86% 83.86%	7 7	66.67% 66.67%	1127 1173	93.95% 93.00%	2 2	
Sophos Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	7 0	65.00% 100.00%	0 8	100.00% 99.95%		
Symantec AntiVirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%		
VirusBuster SambaShield	0 0	100.00% 100.00%	2 2	99.91% 99.91%	8 8	99.21% 99.21%	224 224	79.29% 79.29%	6 8	83.33% 70.00%	20 20	99.92% 99.92%		

August 2008 on-demand (OD) and on-access (OA) detection	WildList viruses		Worms & bots		File infector viruses		Polymorphic viruses		Trojans		Clean sets	
	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	FP OD OA	Susp. OD OA
Agnitum Outpost	0 0	100.00% 100.00%	2 2	99.91% 99.91%	8 8	99.21% 99.21%	317 317	77.32% 77.32%	347 347	84.22% 4.22%		
Ahnlab V3	2 N/A	99.99% N/A	3 N/A	99.81% N/A	8 N/A	97.64% N/A	526 N/A	92.86% N/A	345 N/A	84.34% N/A		
Alwil avast!	0 0	100.00% 100.00%	6 6	99.48% 99.48%	6 6	96.06% 96.06%	322 322	88.78% 88.78%	51 51	97.66% 97.66%		
ArcaBit ArcaVir	182 182	95.80% 95.80%	3 3	99.78% 99.78%	6 6	98.62% 98.62%	55 55	94.16% 94.16%	525 525	76.12% 76.12%	10 10	2 2
AVG Internet Security	0 0	100.00% 100.00%	1 1	99.94% 99.94%	1 1	99.21% 99.21%	52 52	89.95% 89.95%	34 58	98.47% 97.36%		
Avira AntiVir	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	38 38	98.27% 98.27%		
BitDefender AntiVirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	116 116	94.75% 94.75%	4 3	
Bullguard	0 2	100.00% 99.92%	0 12	100.00% 99.22%	2 2	98.95% 98.95%	0 0	100.00% 100.00%	96 96	95.62% 95.62%	4 2	
CA AntiVirus + AntiSpyware	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.84% 99.84%	96 96	95.37% 95.37%	1015 1015	53.86% 53.86%	1 1	
CA eTrust	0 0	100.00% 100.00%	0 0	100.00% 100.00%	1 1	99.84% 99.84%	96 96	95.37% 95.37%	1015 1015	53.86% 53.86%	1 1	
eEye Blink Professional	0 0	100.00% 100.00%	0 0	100.00% 100.00%	7 7	99.15% 99.15%	1005 1005	67.12% 67.12%	145 145	93.43% 93.43%		
ESET NOD32 Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	48 238	97.84% 89.20%		
Fortinet FortiClient	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	92 92	95.54% 95.54%	1854 1854	15.73% 15.73%		
Frisk F-PROT Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	90 90	95.65% 95.65%	230 250	89.53% 88.63%		
F-Secure Internet Security	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	30 30	98.55% 98.55%	117 129	94.66% 94.15%		
F-Secure Protection Services	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	30 30	98.55% 98.55%	117 129	94.66% 94.15%		
G DATA AntiVirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	5 21	99.76% 99.04%		
K7 Total Security	0 0	100.00% 100.00%	5 5	99.61% 99.61%	5 5	97.32% 97.32%	883 1072	68.95% 64.74%	455 455	79.33% 79.33%		
Kaspersky Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	30 30	98.55% 98.55%	72 137	96.73% 93.79%		
Kingsoft Internet Security	0 0	100.00% 100.00%	15 15	98.97% 98.97%	87 87	81.89% 81.89%	2009 2009	42.15% 42.15%	634 662	71.20% 69.91%	1 1	
McAfee VirusScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	341 341	84.52% 84.52%		
Microworld eScan Internet Security	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	90 90	95.65% 95.65%	106 106	95.17% 95.17%		
Norman Security Suite	0 0	100.00% 100.00%	0 0	100.00% 100.00%	7 7	99.15% 99.15%	767 1005	76.96% 67.12%	128 145	94.18% 93.43%		
NWI Virus Chaser	12 12	98.27% 98.29%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	90 90	95.65% 95.65%	93 93	95.77% 95.77%		2 2
PC Tools AntiVirus	0 0	100.00% 100.00%	2 2	99.91% 99.91%	8 8	99.21% 99.21%	313 313	77.70% 77.70%	381 381	82.69% 82.69%		
PC Tools Spyware Doctor	0 0	100.00% 100.00%	2 2	99.91% 99.91%	8 8	99.21% 99.21%	313 313	77.70% 77.70%	404 407	81.64% 81.52%		
Proland Protector Plus	6 162	99.99% 99.53%	5 5	99.48% 99.48%	56 59	92.76% 90.79%	1722 1722	46.38% 46.38%	1969 1973	10.48% 10.30%		
Quick Heal AntiVirus	0 0	100.00% 100.00%	53 53	93.15% 93.15%	10 10	98.03% 98.03%	908 908	81.51% 81.51%	1465 1465	33.40% 33.40%		
Redstone Redprotect	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	90 90	95.65% 95.65%	102 102	95.38% 95.38%		
Rising Antivirus	0 0	100.00% 100.00%	2 2	99.81% 99.81%	41 41	94.33% 94.33%	1302 1302	52.19% 52.19%	268 292	87.82% 86.74%		
Sophos Endpoint Security & Control	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	90 90	95.65% 95.65%	46 46	97.93% 97.93%		33 33
Symantec Endpoint Protection	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	90 90	95.65% 95.65%	38 38	98.29% 98.29%		
Trustport Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	561 561	87.72% 87.72%	40 40	98.20% 98.20%		
VirusBuster Professional	0 0	100.00% 100.00%	2 2	99.91% 99.91%	8 8	99.21% 99.21%	313 313	77.70% 77.70%	362 381	83.56% 82.69%		3 2
Webroot AntiVirus with AntiSpyware	0 0	100.00% 100.00%	4 4	99.48% 99.48%	0 0	100.00% 100.00%	107 107	95.06% 95.06%	48 50	97.81% 97.75%		

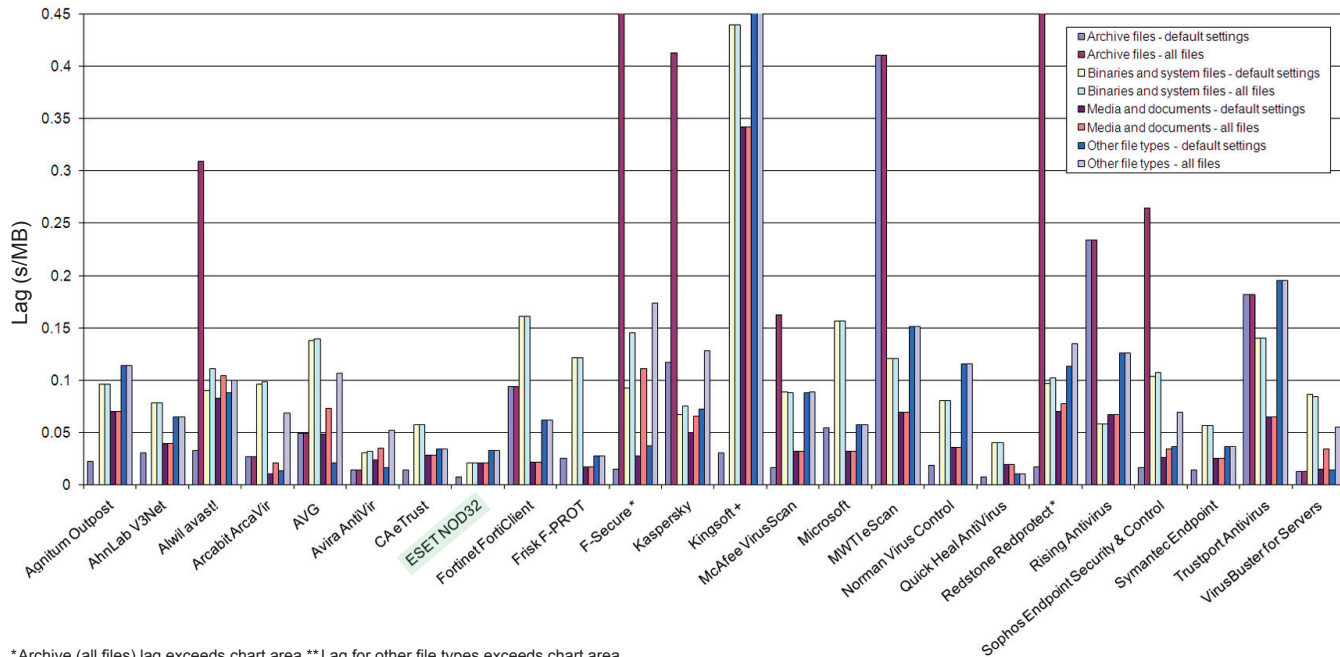
October 2008 on-demand (OD) and on-access (OA) detection rates	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	Missed OD OA	% OD OA	FP OD OA	Susp. OD OA
Agnitum Outpost	0 0	100.00% 100.00%	2 2	99.93% 99.93%	393 393	75.64% 75.64%	1242 1242	75.67% 75.67%		
AhnLab V3Net	0 0	100.00% 100.00%	3 3	99.84% 99.84%	703 703	79.40% 79.40%	1414 N/A	72.30% N/A		
Alwil avast!	0 0	100.00% 100.00%	3 3	99.78% 99.78%	290 290	92.25% 92.25%	296 447	94.20% 91.23%		
Arcabit ArcaVir	93 93	90.58% 90.58%	8 8	99.44% 99.44%	165 165	86.54% 86.54%	1711 1799	66.48% 64.76%	3 3	
AVG	0 0	100.00% 100.00%	1 1	99.95% 99.95%	52 52	90.75% 90.75%	257 478	94.96% 90.63%		
Avira AntiVir	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	36 82	99.29% 98.98%	1 1	
CA eTrust	1 1	99.998% 99.998%	0 0	100.00% 100.00%	172 172	91.82% 91.82%	3760 3476	26.35% 31.92%		
ESET NOD32	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	561 538	89.00% 89.46%		
Fortinet FortiClient	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	5000 5000	2.06% 2.06%		
Frisk F-PROT	0 0	100.00% 100.00%	0 0	100.00% 100.00%	125 125	95.66% 95.66%	746 924	85.39% 81.89%		
F-Secure Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	60 60	98.03% 98.03%	466 466	90.87% 90.87%	1 1	
Kaspersky Anti-Virus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	60 60	98.03% 98.03%	193 287	96.22% 94.38%	1 1	
Kingsoft AntiVirus	0 0	100.00% 100.00%	16 16	99.10% 99.10%	2119 2119	41.19% 41.19%	2605 2605	48.97% 48.97%		
McAfee VirusScan	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	216 216	95.77% 95.77%		
Microsoft Forefront	0 0	100.00% 100.00%	0 0	100.00% 100.00%	141 141	95.02% 95.02%	1054 1054	79.35% 79.35%		
Microworld eScan Internet Security	0 0	100.00% 100.00%	0 0	100.00% 100.00%	122 122	96.00% 96.00%	205 205	95.98% 95.98%	1 1	
Norman Virus Control	0 0	100.00% 100.00%	0 3	100.00% 99.78%	766 1037	78.86% 70.91%	649 788	87.29% 84.56%		
Quick Heal AntiVirus	0 0	100.00% 100.00%	45 45	95.16% 95.16%	977 977	79.25% 79.25%	3450 3477	32.42% 31.89%	1 0	
Redstone Redprotect	0 1	100.00% 99.89%	0 0	100.00% 100.00%	60 122	98.03% 96.15%	467 481	90.85% 90.58%	1 1	
Rising Antivirus	0 0	100.00% 100.00%	3 4	99.75% 99.64%	1333 1333	60.04% 60.04%	1801 2260	64.72% 55.73%		
Sophos Endpoint Security & Control	0 0	100.00% 100.00%	0 0	100.00% 100.00%	154 154	92.75% 92.75%	575 625	88.74% 87.76%		13 12
Symantec Endpoint Protection	0 0	100.00% 100.00%	0 0	100.00% 100.00%	0 0	100.00% 100.00%	357 395	93.01% 92.26%		
Trustport Antivirus	0 0	100.00% 100.00%	0 0	100.00% 100.00%	449 546	92.36% 92.06%	131 155	97.43% 96.96%		2 2
VirusBuster for Servers	0 0	100.00% 100.00%	2 2	99.93% 99.93%	392 392	75.77% 75.77%	1080 1281	78.84% 74.91%		

File access lag time – August 2008



* Archive (all files) lag exceeds chart area **Lag for several modes exceeds chart area

File access lag time – October 2008



* Archive (all files) lag exceeds chart area **Lag for other file types exceeds chart area