



## Why Select Kaspersky Lab Over Sophos

- KL consistently performs better than Sophos in a range of independent anti-virus tests, as shown below.
  - Since testing began in February 2004, KL has received more 'Advanced +' levels than any other vendor from AV-comparatives, including Sophos [see <http://www.av-comparatives.org>, refer to the Comparatives section and click the link in the section beginning 'to get an overview of the comparatives'].
  - Below is a summary of the results from the most recent on demand testing at <http://www.av-comparatives.org>, February 2007.

	KL	SOPHOS
DOS viruses	99.97	97.22
Windows viruses	99.91	90.13
Macro viruses	100	99.83
Script viruses	99.56	68.47
Worms	99.92	81.71
Backdoors	99.91	76.44
Trojans	99.78	55.63
Other malware	99.68	59.49
Other OS malware	88.18	75.49
ODS detection of dialers <sup>1</sup>	Excellent	High
<b>TOTAL</b>	<b>99.88</b>	<b>89.12</b>
Total without DOS & Other OS	99.9	78.4

<sup>1</sup> KEY: not present [0%-5%], low [6%-40%], mediocre [41%-70%], high [71%-95%], excellent [96%-100%].

[AV-comparatives](#) test summary, Kaspersky Lab and Sophos

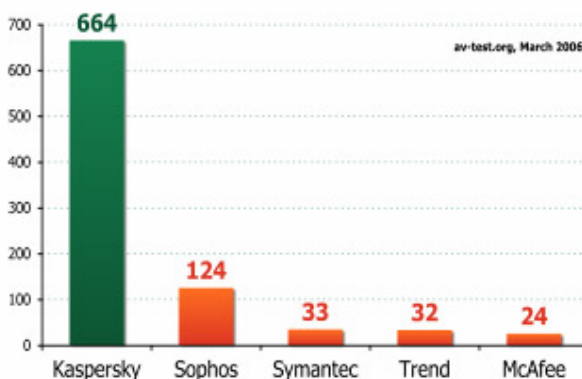
			Who detected more?
1	February 2004	On-demand comparative	KL
2	May 2004	Retrospective/proactive test	KL
3	August 2004	On-demand comparative	KL
4	November 2004	Retrospective/proactive test	KL
5	February 2005	On-demand comparative	KL
6	May 2005	Retrospective/proactive test	KL
7	August 2005	On-demand comparative	KL
8	November 2005	Retrospective/proactive test	Sophos not tested
9	February 2006	On-demand comparative	Sophos not tested
10	May 2006	Retrospective/proactive test	Sophos not tested
11	August 2006	On-demand comparative	Sophos not tested
12	November 2006	Retrospective/proactive test	Sophos not tested
13	February 2007	On-demand comparative	Sophos not tested

- KL has achieved more *Virus Bulletin* 'VB100%' awards than Sophos [see <http://www.virusbtn.com/>]. KL has received 38 VB100% awards, Sophos has received 37 [as of April 2007].

- ▶ KL out-performs Sophos in delivering proactive protection from new threats, as shown above. And KL proactive detection has been enhanced still further with the addition of the KAV 6.0 Proactive Defense Module [PDM].
- ▶ In June 2006, AV-comparatives tested the PDM. This module was tested in isolation, WITHOUT the detection capability normally provided by the KL anti-virus databases: i.e. standard signature scanning was disabled! The results speak for themselves:

	KL
Windows viruses	100
Script malware	93.5
Worms	99
Backdoors	99.9
Trojans	99.6

- Unlike other anti-virus scanners, KL Streaming Scan and Buffering Scan options offer scanning of web traffic is scanned in the stream, before files are written to the hard disk.
- KL has consistently responded faster to outbreaks than Sophos in tests conducted by AV Test GmbH [<http://www.av-test.org/>], including Zafi.d, Mydoom.bb and worms based on the MS05-039 vulnerability.
- New viruses, worms and Trojans appear all the time: KL adds around 450 new records to its databases every day. To protect against new threats as they appear, KL provides hourly, incremental [around 20KB] updates. The update mechanism for Sophos customers is far more cumbersome [see <http://www.sophos.com/support/knowledgebase/article/350.html>].
  1. Sophos Anti-Virus is upgraded monthly. This requires a new auto install of the full product once per month and this is forced once every three months or new IDE files will not work with the old engine version.
  2. Sophos also provides (a) Virus identity [IDE] files, to 'allow Sophos Anti-Virus to detect and disinfect the latest viruses and other malicious software' and (b) Daily Supplemental IDE files that 'provide protection against batches of low-profile threats that have not yet been in the wild.'
  3. However, Sophos makes it clear that 'IDE files are not a replacement for regular monthly updates'. They 'are not supplied for Sophos Anti-Virus versions more than three months old' and 'Sophos recommends that you upgrade Sophos Anti-Virus whenever there is a new release. Currently this is monthly'. This is because 'in any three-month period, Sophos will have analysed many hundreds of new viruses. Some of these will probably require updates to the scanning technology,...' That's why 'Sophos cannot offer technical support to customers who are not using an up-to-date version of Sophos Anti-Virus'.



- KL supports 3,200 different compression, archiving and packing utilities [March 2007]. This includes recursive scanning [e.g. a ZIP file within a ZIP] and *iCure*™ technology to clean commonly used archive utilities: ZIP, ARJ, LHA, RAR, CAB. The KL anti-virus engine also includes a smart algorithm to protect against 'archive bombs' that

can potentially sabotage the scanning process. Sophos, by contrast, handles just a small number of formats [see <http://www.sophos.com/readmes/readcli.txt>]. Sophos de-compresses archive files to the hard disk, rather than scanning them in memory [which is faster] and 'recommends that scanning inside archive files is set to off (the default), because scanning inside archive files can cause scanning to slow' [<http://www.sophos.com/support/knowledgebase/article/19.html>].

- Extensive QA testing ensures that KL customers do not experience false alarms problems of the sort faced by Sophos customers last year [see, for example, <http://isc.sans.org/diary.php?storyid=1139>]
- KL has included leading 'spyware' protection for many years, without the need for a stand-alone product. The quality of KL 'spyware' protection [from backdoor Trojans, keyloggers, adware, dialers and more] has been demonstrated in independent tests:
  - ▶ KL was placed FIRST in the *Computer Bild* 'spyware' test, July 2005.
  - ▶ KL holds West Coast Labs [<http://www.westcoastlabs.org/>] 'Checkmark' certification.
  - ▶ KL won the SC Magazine [<http://www.scmagazine.com/>] 'Best Anti-spyware' award 2006.
- In the February 2007 *Virus Bulletin* review, Kaspersky Lab achieved scan speeds of 12,118.91KB/s, compared to Sophos scan speeds of 6,337.41KB/s [default scanning of executable and system files under Microsoft® Windows Vista™].
- KL *iChecker*™ and *iSwift*™ technologies significantly reduce scan times by scanning new and modified files only.
- KL on-demand scans can be suspended when the processor is under heavy load, to minimize the performance overhead of the scan.
- KL includes a Rescue Disk facility that lets the user create a CD that can be used to boot clean during an emergency clean-up. In addition, KL is able to work with Intel® VPro™ Active Threat Management to enable remote clean-up of infected machines.
- Unlike other anti-virus scanners, KL Streaming Scan and Buffering Scan options offer scanning of web traffic is scanned in the stream, before files are written to the hard disk.

#### **About Kaspersky Lab – [www.kaspersky.com](http://www.kaspersky.com):**

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers. For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, visit [www.viruslist.com](http://www.viruslist.com).