Competitive Analysis: Kaspersky Lab & CA

Kaspersky Lab Key Features and Benefits:

- Fast response to new threats, provided by the 24/7 KL virus lab in Moscow and a team of experienced anti-virus researchers located across the globe.

- Automated hourly updates, plus additional emergency updates as required.

- Small, intelligent, incremental updates of around 45KB. Updates include new signatures plus, where required, updated engine components.

- Leading 'spyware' protection is included, delivering protection from backdoor Trojans, keyloggers, adware, dialers and more.[1]

- Leading detection rates, as shown in KL's consistent track record in independent certifications and tests.[2]

- Leading proactive detection technologies [heuristic, generic and behavioral] enable KL products to find new, unknown threats, even without the need for updated signatures.[3]

- Built-in anti-rootkit technology.

- Roll-back technology to undo the actions taken by malicious programs.

- Built-in support for 1,761 different compression, archiving and packing utilities[4], detecting the hidden threat that could lie within. This includes recursive scanning [e.g. a ZIP file within a ZIP, for example] and *iCure*™ technology to clean commonly used archive utilities: ZIP, ARJ, LHA, RAR, CAB. A smart algorithm also protects against 'archive bombs'.

- *iChecker*™ and *iSwift*™ technologies mean that KL products need to scan ONLY those files that have changed, NOT every file. Since most scanning is redundant, this delivers a huge performance benefit.

- Efficient use of system resources: the engine monitors system resources and suspends scanning if extra resources are needed by the user.

- Real-time e-mail scanning independent of the client application installed e.g. Outlook, Outlook Express, Eudora, etc.

- Real-time scanning of web traffic and browser-based scripts.

- Global 24/7 support, with experienced localized support.

- Broad platform and application support: includes Windows, Linux & Unix, NetWare, MS Exchange, Lotus Domino, Windows SMTP gateways, MS ISA Server, Windows Mobile, Symbian OS & Palm OS.

[1] KL placed FIRST in the *Computer Bild* spyware test, July 2005.
KL holds West Coast Labs. Checkmark 'Anti-Spyware' certification.
KL won SC Magazine 'Best Anti-spyware' award in 2006.

[2] This includes West Coast Labs. & ICSA Labs. certifications, together with the many independent test results referred to later in this document.

[3] The KAV 6.0 Proactive Detection Module scored 99% in AV-comparatives test, June 2006, WITHOUT the need for signatures.

[4] May 2006.

Recent Kaspersky Lab Awards:

- June 06 **SC Magazine Best Buy**: Kaspersky Business Optimal
  http://www.scmagazine.com/uk/grouptest/details/ab23b23f-f6b3-51ca-9609-26a657fc36b7/av+management+2006/

- May 06 **Computer Shopper Best Buy**: Kaspersky Anti-Virus
  http://www.pcpro.co.uk/shopper/labs/86685/kaspersky-antivirus-2006.html?searchString=kaspersky+review+kaspersky

- May 06 **West Coast Checkmark Certification**: Kaspersky Anti-Virus
  http://www.westcoastlabs.org/cm-av-products.asp?Comp_ID=15&Cat_ID=1

- April 06 **SC Magazine Reader Trust Award**: Best Anti-Worm
  http://www.scawards.com/winners/2006.asp#Europe

- April 06 **SC Magazine Reader Trust Award**: Best Anti-Spyware
  http://www.scawards.com/winners/2006.asp#Europe

- April 06 **SC Magazine Award Finalist**: Best Anti-Virus
  http://www.scawards.com/winners/2006.asp#Europe

- April 06 **SC Magazine Award Finalist**: Best Anti-Trojan
  http://www.scawards.com/winners/2006.asp#Europe

- April 04 **SC Magazine Global Awards Winner**: Best Anti-Virus
  http://www.scawards.com/winners/2004.asp

- 2005 **Techworld.com Network Awards**: Anti-Virus Product of the Year
  http://www.kaspersky.com/news?id=166240816
  http://techworld.com/networkawards/winners2005.cfm#cat6

Independent Test Results:

Detection[1] [2]

	KL
DOS viruses	99.96
Windows viruses	99.86
Macro viruses	100
Script viruses	97.69
Worms	99.32
Backdoors	99.87
Trojans	99.49
Other malware	99.79
Other OS malware	99.73
Dialers	99.19
TOTAL	**99.86**

Proactive detection[3] [2]

	KL
Proactive detection ALL samples	**53**

Detection[4] [2]

	KL
DOS viruses	99.97
Windows viruses	99.83
Macro viruses	100
Script viruses	98.45
Worms	99.82
Backdoors	99.49
Trojans	99.26
Other malware	100
Other OS malware	80.65
Dialers	100
TOTAL	**99.77**

Proactive detection[5] [2]

	KL
Proactive detection ITW samples	**25**
Proactive detection ZOO samples	**43**

[1] Based on figures published by AV-comparatives [February 2004].
[2] CA was not tested.
[3] Based on figures published by AV-comparatives [May 2004].
[4] Based on figures published by AV-comparatives [August 2004].
[5] Based on figures published by AV-comparatives [November 2004].

Detection[1] [2]

	KL
DOS viruses	99.95
Windows viruses	99.67
Macro viruses	100
Script viruses	97.90
Worms	99.63
Backdoors	99.64
Trojans	98.62
Other malware	99.02
Other OS malware	80.99
Dialers[4]	Excellent
TOTAL	**99.65**
Total without DOS & Other OS	99.40

Proactive detection[3] [2]

	KL
Proactive detection ITW samples	**35**
Proactive detection ZOO samples	**48**

Detection[5] [2]

	KL
DOS viruses	99.97
Windows viruses	99.91
Macro viruses	100
Script viruses	99.56
Worms	99.92
Backdoors	99.91
Trojans	99.78
Other malware	99.68
Other OS malware	88.18
Dialers[4]	Excellent
TOTAL	**99.88**
Total without DOS & Other OS	99.9

Proactive detection[6] [2]

	KL
Proactive detection ITW samples	**0**
Proactive detection ZOO samples	**32**

[1] Based on figures published by AV-comparatives [February 2005].

[2] CA was not tested.

[3] Based on figures published by AV-comparatives [May 2005].

[4] KEY: Not present [0%-5%], Low [6%-40%], Mediocre [41%-70%], High [71%-95%], Excellent [96%-100%].

[5] Based on figures published by AV-comparatives [August 2005].

[6] Based on figures published by AV-comparatives [November 2005].

Detection[1] [2]

	KL
DOS viruses	99.97
Windows viruses	99.84
Macro viruses	100
Script malware	99.15
Worms	99.56
Backdoors	99.76
Trojans	99.26
Other malware	97.90
Other OS malware	99.04
Dialers[4]	Excellent
Polymorphic malware	99.40
TOTAL	**99.57**
Total including DOS	99.77

Proactive detection[3] [2]

	KL
Proactive detection of NEW samples	**24**

Detection[5]

Sequence of product placement Windows 2000 anti-virus products		
3	KL	15 points
9	CA	8 points

Sequence of product placement Windows 2000 anti-malware products		
3	KL	19 points
9	CA	9 points

Sequence of product placement Windows XP anti-virus products		
3	KL	15 points
9	CA	8 points

Sequence of product placement Windows XP anti-malware products		
3	KL	19 points
9	CA	9 points

Sequence of product placement LINUX anti-virus products		
3	KL	15 points
7	CA	7 points

Sequence of product placement LINUX anti-malware products		
3	KL	19 points
	CA	

Virus Bulletin 'VB100%' awards[6]

	PASS	FAIL	NO ENTRY
KL	33	13	0
CA *e*Trust Antivirus	24	11	11
CA Vet Anti-Virus	25	13	8

[1] Based on figures published by AV-comparatives [February 2006].

[2] CA was not tested.

[3] Based on figures published by AV-comparatives [May 2006].

[4] KEY: Not present [0%-5%], Low [6%-40%], Mediocre [41%-70%], High [71%-95%], Excellent [96%-100%].

[5] Based on figures published by Virus Test Center, University of Hamburg [July 2004].

[6] Full results can be found on the *Virus Bulletin* web site [the above table is valid up to June 2006].

On its web site, CA makes the claim: 'CA has received the most Virus Bulletin 100% awards for detecting 100% of "in-the-wild" viruses of any antivirus vendor.' This is simply FALSE, as the table above shows.

Outbreak response[1]

	TIME
KL	2:34:28
InoculateIT-CA	10:35:00
InoculateIT-VET	15:08:34

Outbreak response[2]

	TIME
KL	Under 4 hours
CA *e*Trust INO	Under 12 hours
CA *e*Trust Vet	Under 16 hours

Outbreak response[3]

	TIME	THREAT IDENTIFICATION
Signature detection using regular updates		
KL	14 December 2004, 10:02	Email-Worm.Win32.Zafi.d
CA *e*Trust INO	14 December 2004, 16:50	Win32/Zafi.D.Worm
CA *e*Trust Vet	14 December 2004, 19:08	Win32.Zafi.D

Outbreak response[4]

	TIME	THREAT IDENTIFICATION
Proactive detection without the need for signature updates		
KL	Proactive detection[5]	Email-worm.Win32.Mydoom.m

Signature detection using regular updates		
CA *e*Trust Vet	17 February 2005, 05:31	Win32/Mydoom.AU!Worm
KL	17 February 2005, 12:18	Email-Worm.Win32.Mydoom.am

Signature detection using BETA updates		
CA *e*Trust INO [beta]	17 February 2005, 00:15	Win32/Mydoom.AU!Worm
CA *e*Trust Vet [beta]	17 February 2005, 01:19	Win32.Mydoom.AU

[1] From a survey measuring average response times to a series of outbreaks during Q1 2004. Full results can be found in *Unter Dauerbeschuss - Reaktionszeiten der Antivirenhersteller* by Patrick Brauch [based on analysis by AV-Test GmbH], c't 08/2004, page 168pp [5 pages].

[2] This data, measuring average response times to 45 outbreaks in 2004, is taken from the presentation *Antivirus outbreak response testing and impact*, presented at the *Virus Bulletin* 2004 Conference in Chicago by Andreas Marx [September 2004]. A paper containing these results can be found on the AV-Test GmbH web site.

[3] From a survey measuring response times to the outbreak of Zafi.d on 14 December 2004. Full results can be found in *Security Watch: Internet Bulletin Boards Join The Santy Generation*, by Larry J Seltzer [based on analysis by AV-Test GmbH], PC Magazine 12/2004.

[4] From a survey measuring response times to the outbreak of Mydoom.bb on 16 February 2005. Full results can be found in *Security Watch: MyDoom reappears – Anti-Virus Response Times to MyDoom.BB*, by Larry J Seltzer [based on analysis by AV-Test GmbH], PC Magazine 02/2005.

[5] Kaspersky Lab provided protection from 26 July 2004.

Outbreak response[1]

	TIME	THREAT IDENTIFICATION
Signature detection using regular updates		
KL	2 May 2005, 16:39	Email.Worm.Sober.p
CA *e*Trust INO	2 May 2005, 19:54	Win32/Sober.53554!Worm
CA *e*Trust Vet	2 May 2005, 23:15	Win32.Sober.N

Signature detection using BETA updates		
CA *e*Trust INO [beta]	2 May 2005, 18:17	Win32/Sober.53554!Worm
CA *e*Trust Vet [beta]	2 May 2005, 19:47	Win32.Sober.N

Outbreak response[2]

	TIME	THREAT IDENTIFICATION
Signature detection using regular updates		
KL	16 August 2005, 21:57	Net.Worm.Win32.Small.d
CA *e*Trust INO	16 August 2005, 23:51	Win32/MS05-039!exploit!Worm
KL	17 August 2005, 01:06	Net.Worm.Win32.Bozori.a
CA *e*Trust VET	17 August 2005, 01:53	Win32.MS05-039!exploit
CA *e*Trust INO	17 August 2005, 20:27	Win32/Zotob.E!Worm
CA *e*Trust VET	18 August 2005, 05:35	Win32.Tpbot.A

Signature detection using BETA updates		
CA *e*Trust INO [beta]	16 August 2005, 22:13	Win32/MS05-039!exploit!Worm
CA *e*Trust VET [beta]	16 August 2005, 23:16	Win32.MS05-039!exploit!
CA *e*Trust VET [beta]	17 August 2005, 02:20	W32.Peabot.A
CA *e*Trust VET [beta]	17 August 2005, 06:22	Win32.Tpbot.A
CA *e*Trust INO [beta]	17 August 2005, 19:00	Win32/Zotob.E!Worm

[1] From a survey measuring response times to the outbreak of Sober.p on 2 May 2005. Full results can be found in *Security Watch: Mac Users Alert! Major Security Update - Anti-Virus Vendor Response Times to Recent Sober Outbreak [Sober.p]*, by Larry J Seltzer [based on analysis by AV-Test GmbH], PC Magazine 05/2005.

[2] From a survey measuring response times to the MS05-039 worms in August 2005. Full results can be found on the AV-Test GmbH web site.

Detection[1]

	DETECTION
Detection on 1 January 2006	
*e*Trust-INO	73/73
*e*Trust-VET	73/73
KL	73/73
Detection on 4 January 2006	
CA *e*Trust-VET	206/206
CA *e*Trust-VET [beta]	206/206
KL	206/206
CA *e*Trust-INO	25/206
CA *e*Trust-INO [beta]	25/206

Outbreak response[2]

	TIME	THREAT IDENTIFICATION
Signature detection using regular updates		
KL	16 January 2006, 11:44	Email-Worm.Win32.VB.bi
CA *e*Trust VET	17 January 2006, 06:39	Win32/Blackmal.F
CA *e*Trust INO	17 January 2006, 16:52	Win32/Cabinet!Worm

[1] From a survey measuring detection of MS06-001 exploits ['Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution']. Results can be found in *Security Watch: Iniquitous Images Imperil the Internet!* [based on analysis by AV-Test GmbH], PC Magazine 01/2006.

[2] From a survey measuring response times to the Nyxem.e worm on 16 January 2006. Full results can be found in *Security Watch: Blackworm Blows Up on Friday – Anti-Virus Vendor Response Times to Blackworm* [based on analysis by AV-Test GmbH], PC Magazine 01/2006.