

Bagaimana cara dan metode memilih antivirus terbaik ?

Penulis : fajarnovriawan@gmail.com - Pemerhati Antivirus

Perkembangan teknologi informasi yang sangat pesat saat ini mendorong tingkat pertumbuhan virus yang signifikan. Banyaknya virus yang berkeliaran membuat pengguna komputer jengah. Apalagi sistem antivirus tidak seratus persen mampu melindungi komputer.

A. Apa antivirus itu?

Sebelum memilih antivirus ada baiknya kita mengetahui sedikit tentang antivirus. Antivirus yaitu software yang berfungsi untuk mendeteksi, menghapus, serta mengkarantina virus-virus dari sistem komputer. Disebut juga *Virus Protection Software*. Aplikasi ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi, atau ketika disimpan).

Dengan penjelasan tadi akan timbul pertanyaan bagaimana cara memilih antivirus terbaik? Disini saya coba merangkumkan barometer apa yang digunakan dalam memilih produk antivirus.

B. Apa yang menjadi Prioritas dalam menentukan kualitas sebuah produk antivirus ?

Dari hasil survey, maka didapatkan prioritas acuan dalam memilih antivirus :

1. Rate Detection Test

Adalah merupakan pengujian signature base antivirus terhadap ribuan bahkan jutaan sample virus, dan kemudian dilakukan perbandingan antivirus manakah yang terbanyak mendeteksi sample virus tersebut.

2. Heuristic/Prospective/Generic Test

Adalah merupakan pengujian virus/malware baru yang belum ada dalam database (signature file) akan tetapi memanfaatkan signature database tersebut sebagai acuan untuk mendeteksi virus/malware baru, apabila terdapat ciri-ciri virus/malware maka fungsi heuristic akan mendeteksinya.

Dalam hal ini seperti DNA pada manusia, sebagai contoh, Peter Parker adalah sebuah virus dan telah ada dalam signature database sebuah antivirus, sehingga dapat dideteksi bahwa ini adalah virus, tetapi apabila kemudian Peter Parker berubah wujud menjadi spiderman, maka secara dasar signature database antivirus tidak mengenali bahwa ini virus/malware, tetapi fungsi heuristic akan melihat bahwa DNA Peter Parker dan Spiderman adalah sama, maka antivirus juga akan mendeteksi bahwa ini adalah virus/malware.

Jadi dengan fungsi heuristic sangatlah penting setelah Signature Database.

3. Performance Test

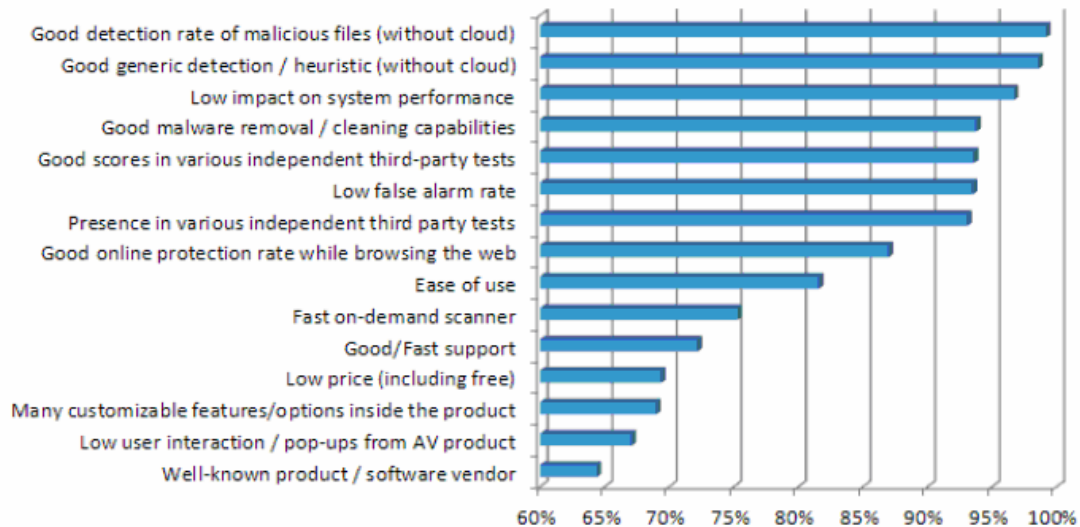
Penggunaan antivirus tentu saja akan memakan resource komputer, seperti CPU, Memory, disini peran kita adalah harus pintar dalam memilih produk antivirus yang memiliki pengaturan sumber daya yang baik, sehingga tidak mengganggu performansi komputer.

Saat ini, ada banyak antivirus yang menggunakan beberapa engine dalam produknya, ada yang menggunakan 2 (dua) engine, atau bahkan 7 (tujuh) engine, dimana hal ini akan berpengaruh dengan performansi komputer, resource / sumber daya komputer akan banyak digunakan dibandingkan dengan hanya 1 (satu) engine.

Tabel Survey

Sumber : av-comparatives.org (Security Survey March 2011)

What is important for you in a security product?



C. Organisasi/badan independen mana yang menjadi acuan dalam melakukan komparasi produk antivirus ?

Saat ini ada sekitar 22 badan/organisasi non profit yang membahas dan melakukan komparasi produk antivirus, akan tetapi hanya terdapat sekitar 5 organisasi terpercaya/independen berdasarkan survey, dimana dapat dipastikan tidak ada pesan sponsor di dalamnya, antara lain :

- AV-Comparatives
- Virus Bulletin / AV-Test
- ICSA Labs / West Coast Labs

AV-Comparatives sampai sejauh ini memiliki rating yang tertinggi sebagai badan independen yang melakukan komparasi produk antivirus, serta selalu mendapatkan respon yang sangat positif dari publik dari setiap ulasan yang publikasikan, VirusBulletin dan AV-Test dinilai sama pada urutan kedua, juga ICSALabs dan WestCoastLabs pada urutan ketiga, badan independen ini mensyaratkan kondisi dan minimum requirement dari vendor antivirus yang produknya akan di test.

Sebagai tambahan, disini tidak diikutsertakan analisis dari Gartner, mengingat gartner menganalisis banyak produk dan tidak spesifik ke antivirus saja.

Independensi AV-Comparatives dapat dilihat dari penilaian 4 (empat) tahun terakhir untuk kategori "Product of the Year" :

- Tahun 2007 : Eset NOD32
- Tahun 2008 : Avira
- Tahun 2009 : Symantec
- Tahun 2010 : F-Secure

Dimana tidak ada satu merk pun pernah menduduki peringkat "Product Of the Year" secara berturut-turut, sehingga pada artikel ini yang akan dibahas adalah pengujian dari AV-Comparatives.

D. Pengujian / testing oleh AV-Comparatives

Pengujian oleh AV-Comparatives secara periodik dilakukan per 3 (tiga) bulan sekali yang mencakup : *Restropective/ Proactive Test* dan *On Demand Comparative*, dimana kita tidak bisa berpedoman hanya dengan sekali pengujian, mengingat konsistensi suatu produk harus dilihat dalam jangka waktu tertentu.

Hasil pengujian AV-Comparatives dapat dilihat pada :

<http://www.av-comparatives.org/en/comparativesreviews/archive>

- May 2007 : <http://www.av-comparatives.org/images/stories/test/ondret/report14.pdf>
- Aug 2007 : <http://www.av-comparatives.org/images/stories/test/ondret/report15.pdf>
- Nov 2007 : <http://www.av-comparatives.org/images/stories/test/ondret/report16.pdf>
- Feb 2008 : <http://www.av-comparatives.org/images/stories/test/ondret/report17.pdf>
- May 2008 : <http://www.av-comparatives.org/images/stories/test/ondret/report18.pdf>
- Aug 2008 : <http://www.av-comparatives.org/images/stories/test/ondret/report19.pdf>
- Nov 2008 : <http://www.av-comparatives.org/images/stories/test/ondret/report20.pdf>

<http://www.av-comparatives.org/en/comparativesreviews/detection-test>

- Feb 2009 : http://www.av-comparatives.org/images/stories/test/ondret/avc_report21.pdf
- May 2009 : http://www.av-comparatives.org/images/stories/test/ondret/avc_report22.pdf
- Aug 2009 : http://www.av-comparatives.org/images/stories/test/ondret/avc_report23.pdf
- Nov 2009 : http://www.av-comparatives.org/images/stories/test/ondret/avc_report24.pdf
- Feb 2010 : http://www.av-comparatives.org/images/stories/test/ondret/avc_report25.pdf
- May 2010 : http://www.av-comparatives.org/images/stories/test/ondret/avc_report26.pdf
- Aug 2010 : http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2010.pdf
- Nov 2010 : http://www.av-comparatives.org/images/stories/test/ondret/avc_retro_nov2010.pdf
- Feb 2011 : http://www.av-comparatives.org/images/stories/test/ondret/avc_od_feb2011.pdf

Setiap hasil pengujian Detection Rate dapat dilihat pada halaman : **Summary Result**

Berikut hasil rekapitulasi AV-Comparatives periode Februari 2007 s/d November 2010, sampai artikel ini dibuat belum ada report testing baru.

RATE DETECTION & HEURISTIC TEST (RANK BY POINT)

REKAPITULASI AV-COMPARATIVES 2007-2011

Antivirus Brand	PERIODE TEST PER 3 BULAN & POINT (%)															SCORE	
	2007			2008				2009				2010				2011	RATA-RATA (Higher Better)
	May	Aug	Nov	Feb	May	Aug	Nov	Feb	May	Aug	Nov	Feb	May	Aug	Nov	Feb	
Avira Antivir	71,00	99,45	81,00	99,60	72,00	99,60	67,00	99,70	69,00	99,40	74,00	99,30	53,00	99,80	59,00	97,50	83,77
Eset NOD32	68,00	97,60	71,00	97,70	57,00	96,60	51,00	97,60	56,00	97,20	60,00	97,70	52,00	98,60	56,00	97,50	78,22
Trustport	58,00	99,64	56,00	99,80	64,00	98,70	49,00	97,10	42,00	97,60	49,00	99,10	63,00	99,80	58,00	99,20	76,87
Gdata (AVK)	31,00	99,31	39,00	99,50	29,00	99,50	59,00	99,80	60,00	99,80	66,00	99,60	61,00	99,90	62,00	99,80	75,26
Bitdefender	48,00	97,51	44,00	96,50	44,00	96,40	46,00	98,00	50,00	97,80	53,00	97,50	50,00	99,30	54,00	97,60	73,10
Kaspersky	9,00	98,46	40,00	98,30	21,00	97,60	60,00	97,10	50,00	94,70	64,00	97,10	59,00	98,30	59,00	97,00	71,29
Sophos	X	X	X	96,60	74,00	95,30	50,00	89,60	32,00	91,30	34,00	93,70	32,00	96,80	58,00	94,10	72,11
Microsoft	18,00	90,37	35,00	93,90	29,00	92,60	44,00	87,10	60,00	90,00	56,00	96,30	59,00	97,60	52,00	95,80	68,54
Avast	26,00	95,24	37,00	97,60	28,00	98,70	39,00	98,20	42,00	98,00	53,00	97,30	29,00	99,30	43,00	98,40	67,48
McAfee	24,00	93,15	34,00	94,90	32,00	99,00	29,00	99,10	25,00	98,70	47,00	98,90	38,00	99,40	X	96,80	67,26
Symantec	24,00	98,80	35,00	97,70	14,00	99,00	44,00	98,70	35,00	98,40	36,00	98,60	43,00	98,70	51,00	95,50	66,71
AVG	8,00	97,75	25,00	98,10	32,00	97,30	40,00	93,00	45,00	94,00	49,00	94,20	34,00	98,30	X	91,40	66,47
Escan	9,00	97,53	14,00	97,50	6,00	95,70	8,00	98,00	50,00	97,70	53,00	97,50	50,00	99,20	54,00	97,40	64,03
F-Secure	31,00	97,57	14,00	97,50	6,00	95,80	9,00	93,40	14,00	97,90	56,00	97,80	52,00	99,20	56,00	98,10	63,45
Norman	28,00	90,93	33,00	94,20	35,00	98,50	25,00	87,80	23,00	84,80	32,00	92,70	27,00	96,60	X	X	60,61
Panda	X	X	X	X	X	X	X	X	X	X	X	99,20	63,00	99,20	61,00	98,10	
K7	X	X	X	X	X	X	X	X	X	X	X	96,40	50,00	96,60	50,00	84,40	
PC Tools	X	X	X	X	X	X	X	X	X	X	X	98,70	17,00	98,10	37,00	92,80	
VBA32	X	X	X	87,70	25,00	86,50	26,00	X	X	X	X	X	X	X	X	X	
Kingsoft	X	X	X	X	X	X	X	84,90	19,00	86,40	32,00	81,80	11,00	80,10	X	X	
Trend Micro	X	X	X	X	X	X	X	X	X	X	X	90,70	26,00	90,30	X	94,40	

Note : - Data produk di komparasi hanya yang ikut minimal 14 kali pengujian

- Score : Total Rating dibagi Jumlah Pengujian

Source : <http://av-comparatives.org>

PERFORMANCE TEST (MB/s)
REKAPITULASI AV-COMPARATIVES 2007-2011

Antivirus Brand	PERIODE TEST PER 3 BULAN & POINT															SCORE (Higher Better)	
	2007			2008				2009				2010					2011
	May	Aug	Nov	Feb	May	Aug	Nov	Feb	May	Aug	Nov	Feb	May	Aug	Nov		Feb
Symantec		6,45		22,80		25,50	22,20		16,90		17,20		18,60		13,30	9,50	16,92
Avira Antivir		7,49		16,70		17,70	14,00		13,60		14,10		17,70		15,10	10,20	14,07
Avast		3,55		11,10		10,40	9,80		15,40		17,40		15,50		17,20	16,30	12,96
Eset NOD32		7,33		15,10		13,30			13,20		9,20		8,70		9,60	8,30	10,59
McAfee		6,32		11,80		14,30	14,70		10,40		7,50		6,60		12,30	11,20	10,57
AVG		2,25		12,20		12,30	16,50		6,80		6,80		13,10		13,00	9,90	10,32
Kaspersky		3,51		4,90		5,00	13,90		13,30		8,70		10,70		9,80	10,30	8,90
Bitdefender		1,96		11,30		9,40	11,10		5,30		7,20		5,40		12,10	9,70	8,16
Gdata (AVK)		1,86		4,80		5,30	10,80		11,20		9,30		10,60		10,30	8,50	8,07
Microsoft		6,11		10,20		8,20	8,80		8,10		6,60		5,80		5,90	6,60	7,37
Norman		3,58		9,40		9,70	11,40		5,80		6,30		6,10		4,40		7,09
F-Secure		1,48		3,80		4,10	7,60		3,70		6,70		5,90		11,90	9,40	6,06
Trustport		1,21		4,30		1,80	4,70		6,70		5,90		5,60		9,40	8,70	5,37
Escan		3,29		2,80		3,00	4,40		4,40		4,20		3,70		8,90	7,90	4,73
Sophos						7,80	17,10		11,70		9,50		15,20		10,60	10,60	
Kingsoft									24,00		14,50		12,90		11,60		
Panda													17,10		14,60	13,20	
K7													12,50		11,70	12,30	
Trend Micro													8,30		12,80	10,40	

Note : - Data produk di komparasi hanya yang ikut minimal 8 kali pengujian

Source : <http://av-comparatives.org>

- Score : Total Rating dibagi Jumlah Pengujian

Dari kesimpulan di atas, bahwa dalam menentukan kualitas produk antivirus yang terbaik berdasarkan prioritas adalah :

1. Rate Detection Test
2. Heuristic/ProActive/Prospective Test
3. Performance Test

Dan dalam penentuan kualitas produk antivirus terbaik harus dilihat dari beberapa kali pengujian, sehingga kita bisa melihat produk yang benar-benar konsisten dengan kualitasnya.

Semoga bermanfaat.

Wassalam
Fajar Novriawan