Visual-aid Slide Set to Accompany
An Updated Survey of Anti-Virus Software – from Published Test Results

compiled by Gary Patrick

Lexington, Massachusetts Senior Center Computer & Technology Club

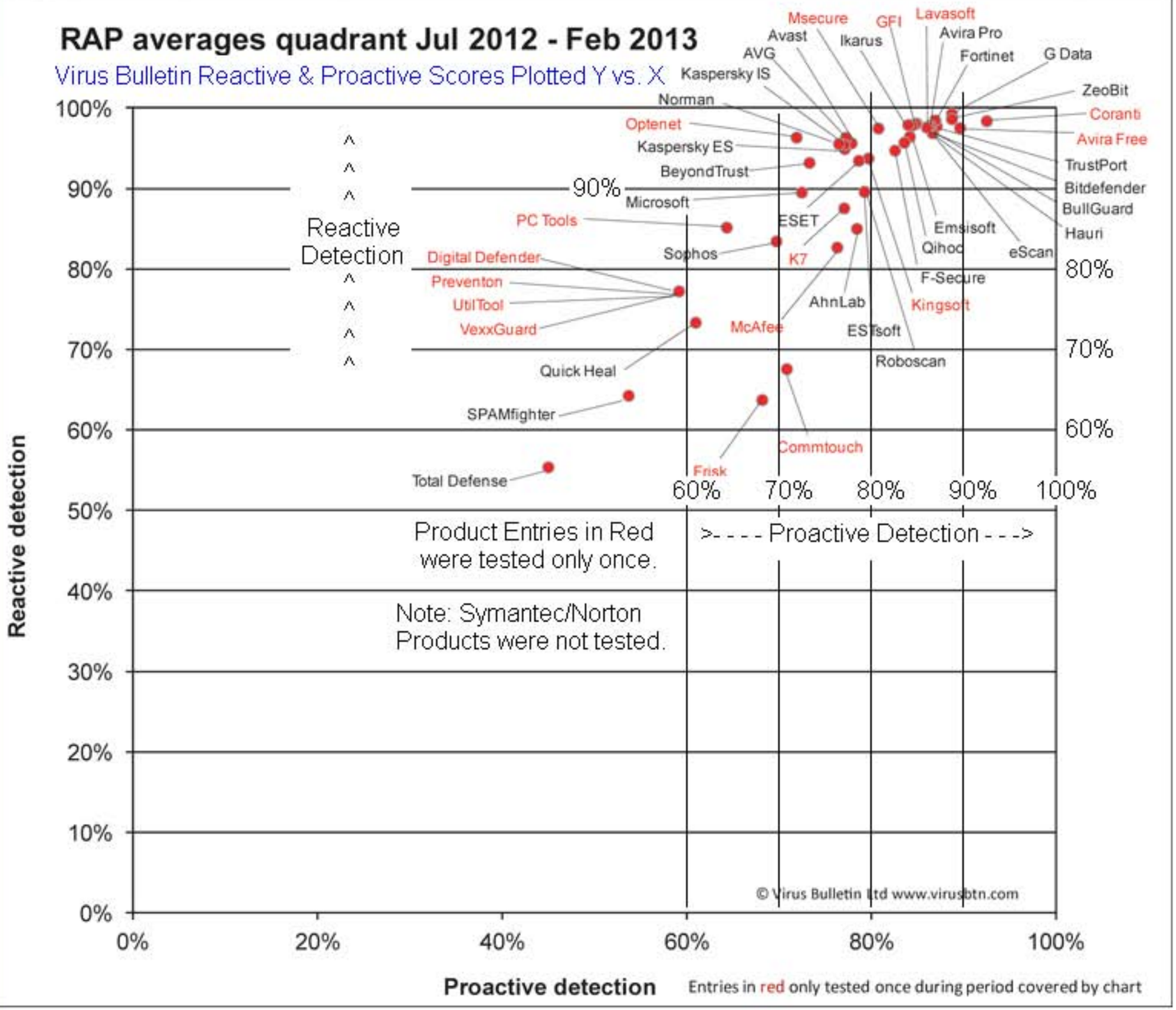
January 16, 2013

With updates, March 20, 2013;
more updates pending

Note: As last year, this survey is intended for users of Microsoft Windows personal computers. It does not address the question of Anti-Virus protection for Apple computers.

RAP averages quadrant Jul 2012 - Feb 2013

Virus Bulletin Reactive & Proactive Scores Plotted Y vs. X



Entries in red only tested once during period covered by chart

VirusBulletin RAP Plot Magnified

- Feb 2013

Upper-right = better anti-virus/anti-malware detection and protection.

Msecure
GFI
Lavasoft
Avast
Ikarus
Avira Pro
AVG
Fortinet
G Data
Kaspersky IS
ZeoBit
Norman
80%
100%
Coranti
Optenet
Avira Free
Kaspersky ES
TrustPort
BeyondTrust
Bitdefender
90%
Microsoft
90%
BullGuard
ESET
Emsisoft
Hauri
Tools
Qihoo
eScan
Sophos
K7
80%
F-Secure
70%
AhnLab
Kingsoft
Reactive Detection
McAfee
ESTsoft
Roboscan
Quick Heal
>- - - - Proactive Detection - - - ->
er
Commtouch

Beyond antivirus software: E | Virus Bulletin : VB100 results

www.virusbtn.com/vb100/archive/summary

Virus Bulletin Anti-virus Certification by Product and Operating System:	Windows XP April 2012	Windows Server 2008 R2 June 2012	Windows 7 Professional August 2012	Windows Server 2003 R2 October 2012	Windows 8 Professional December 2012
Agnitum (Outpost)	VIRUS 100	VIRUS 100	X	-	-
AhnLab	-	-	VIRUS 100	-	VIRUS 100
Auslogics Antivirus	-	-	VIRUS 100	-	-
avast!	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100
Avertive	VIRUS 100	-	-	-	-
AVG	VIRUS 100	X	VIRUS 100	VIRUS 100	VIRUS 100
Avira	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100	-
Avira Personal	VIRUS 100	-	VIRUS 100	-	-
BeyondTrust	VIRUS 100	VIRUS 100	X	VIRUS 100	X
Bitdefender	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100
Bkis BKAV Home	-	X	-	-	-
BullGuard	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100
Central Command (Vexira)	VIRUS 100	VIRUS 100	X	-	-
Check Point (ZoneAlarm)	VIRUS 100	-	-	-	-

Consumer Reports online
Ratings of Internet Security Software
(as of 3/15/2013)

Brand & Model	Price	Ratings and Test Results									
	Price ($/3 PCs)	Overall score (0 P F G VG E 100)	Threat blocking	Ease of use	Malware scan	Resource drain	Firewall	Updating	Anti-phishing	Response to threats
Free anti-malware security software											
Avast! Free Antivirus *	---	58								
Avira Free Antivirus *	---	55								
AVG AntiVirus Free 2013 *	---	49								
Microsoft Security Essentials *	---	43								
Pay security suites											
G Data Internet Security 2013	$45	67								
ESET Smart Security 6	$80	66								
F-Secure Internet Security 2013	$60	64								
Avira Internet Security 2013	$90	62								
Avast! Internet Security 7	$70	57								
BitDefender Internet Security 2013	$70	56								
Trend Micro Titanium Internet Security 2013	$80	54								
BullGuard Internet Security 2013	$60	53								
McAfee Internet Security 2013	$80	53								
AVG Internet Security 2013	$70	51								
Norton Internet Security 2013	$80	50								
Check Point ZoneAlarm Internet Security Suite 2013	$80	45								
Panda Internet Security 2013	$70	43								

Comparatives||tests - reviev | AV-TEST - The Independent | 2012's worst security exploit | Security Suite Endurance Te

www.av-test.org/en/tests/home-user/windows-7/sepoct-2012/

- Home User
  - Windows 8
  - Windows 7
    - Sep/Oct 2012
    - May/Jun 2012
    - Mar/Apr 2012
    - Nov/Dec 2011
    - Jul/Aug 2011
    - Quarter 1/2011
    - Quarter 2/2010
  - Windows Vista
  - Windows XP
- Corporate User
  - Windows 8
  - Windows 7
  - Windows XP
- Mobile Devices
  - Android

Home User Products

tested by AV-Test Labs, Magdeburg, Germany

Unfortunately, Microsoft Security Essentials 4.0 & 4.1 failed this certification test.

Windows 7

Testreport	Producer: Product	Certified	Protection	Repair	Usability	Platform	Date
123638	AhnLab: V3 Internet Security 8.0		3.0/6.0	4.5/6.0	3.5/6.0	Windows 7	10-2012
123615	Avast: Free AntiVirus 7.0		5.0/6.0	4.0/6.0	5.0/6.0	Windows 7	10-2012
123652	AVG: Anti-Virus Free Edition 2012 & 2013		4.5/6.0	3.5/6.0	4.5/6.0	Windows 7	10-2012
123684	AVG: Internet Security 2012 & 2013		4.5/6.0	4.5/6.0	4.5/6.0	Windows 7	10-2012
123617	Avira: Internet Security 2012 & 2013		4.0/6.0	4.0/6.0	4.0/6.0	Windows 7	10-2012
123671	Bitdefender: Internet Security 2013		6.0/6.0	6.0/6.0	5.0/6.0	Windows 7	10-2012
123661	BullGuard: Internet Security 12.0 & 13.0		5.0/6.0	3.5/6.0	4.5/6.0	Windows 7	10-2012
			5.5/6.0				

www.av-comparatives.org/images/docs/avc_sum_201212_en.pdf

AV-Comparatives' Test Results Summary, 2012 Report.

*=Standard level performance results; **=Advanced performance; ***=Advanced+ performance

	File Detection Test March 2012	Proactive Test March 2012	Performance Test (Suite) May 2012	Real-World Test (March-June 2012)	Anti-Phishing Test July 2012	File Detection Test September 2012	Performance Test (AV) October 2012	Malware Removal Test October 2012	Real-World Test (August-November 2012)
Product of the yr / Top-rated - - - Bitdefender	***	***	***	***	***	***	**	***	***
Kaspersky	***	***	***	***	***	***	**	***	***
F-Secure	***	***	***	***	***	***	**	**	**
AVIRA	***	***	***	**	**	***	**	**	**
BullGuard	***	***	**	**	***	***	*	**	***
ESET	***	***	***	**	*	**	***	**	**
G DATA	***	***	**	***	**	**	*	**	***
avast!	***	***	***	*	**	***	***	*	**
Panda	***	***	***	**		**	**	***	*
eScan	***	***	**	**	*	***	**		*
Sophos	***		***	*	***	**	**		*
Qihoo 360	*	*	***	***	*	tested	**		***
PC Tools	*	*	*	**	***	*	*	**	*
McAfee	**		**	*	***	***	**		tested
AVG	*	**	***	**	*	*	**	*	*
Trend Micro	*		**	*	***	***	*		**
Tencent QQ	**	**	***	*		***			**
Fortinet	**	*	*	tested	*	***	*	**	tested
GFI Vipre	*	*	**	*	*	**	*	**	tested
Webroot	*		***	tested	***	tested	***		tested
Microsoft	*	***				*	***		
AhnLab	tested	tested	**	tested		tested			tested

Although STANDARD is already a good score, tests in which a STANDARD award (or lower) was reached indicates areas which need further improvement compared to other products. ADVANCED indicates areas which may need some improvement, but are already very competent.

AV-Comparatives' Summary Report, 2012 [December, 2012, last revised January 5, 2013]
www.av-comparatives.org/images/docs/avc_sum_201212_en.pdf

Table of Contents

Sources of samples

(dated 2008)

AV-Comparatives have various sources from which it obtains samples. Like anti-virus vendors, we also use various **traps** and **honeypots** from all over the world, as well as samples downloaded from **malware downloaders** and **infected websites**. Furthermore, we get samples from the field which were collected by us or our partner companies (e.g. computer repair/cleaning services) on infected PC's belonging to home users and/or small/medium business companies. We also get samples from various **online scanning services** and (single and large) submissions from visitors[2] to our website, as well as **various organizations** that collect malware (internal and public security forums, honeypot projects, anti-malware initiatives, and so on). In order to have a test-set that is statistically valid and as large and representative as possible, AV-Comparatives also accepts samples from (security) **vendors**. Currently, samples submissions from about a dozen vendors are included in our tests and nearly dozen more vendors which are not included in our tests also contribute.

Any vendor is encouraged to send us samples they get from their customers, but no vendor is obliged to. While we are not going to disclose the names of the vendors which submit or do not submit their samples (partly because Non-Disclosure Agreements may apply), we can assure you that submitting samples to AV-Comparatives does not help a vendor to get a better score. As the test-set consists of samples from many various sources and vendors, a single vendor's contributions just make the test set more representative – in fact, there are some vendors who do not submit anything and score very highly, and some other vendors who submit a lot are at the bottom regarding detection rates. The reason for this may be that samples are usually shared between vendors anyway and most of the samples we get are usually already in some other collections, so it is impossible to tell how much is coming from which individual source and so on.

We also prefer not to disclose this information because of the possibility that some vendors may use it to mislead the public for PR reasons (this has happened several times in the past, for example when a vendor was unhappy with some test results or wanted to put pressure on a tester) or focus on specific sources. As we've said, any vendor is welcome to submit us their samples if they wish to. Last-minute submissions (especially "extraordinary" collections) from vendors are not accepted; this source of samples is usually frozen 2-3 weeks before the test starts, in order to avoid possible bias.

AV-Comparatives does not create, modify or repack any malware (for testing purposes or for any other purpose).

Currently (August 2008) the rules for the awards are as follow (as test-sets and methods change, also the award systems need to be updated from time to time):

Test report of February and August (overall detection rate tests):

To get ADVANCED+, over 97% of the whole test-set have to be detected during an on-demand scan with best possible settings.

over 97%	ADVANCED+
93-97%	ADVANCED
87-93%	STANDARD
under 87%	NO AWARD

An updated award system which will also consider the false alarm rate will be introduced and applied in the tests of 2009.

Test report of May and November (retrospective tests):

To get the Advanced+ award, a product must be able to detect at least 50% of new malware proactively and at the same time have only few false alarms.

	0-10%	10-25%	25-50%	50-100%
none - few	NO AWARD	STANDARD	ADVANCED	ADVANCED+
many	NO AWARD	NO AWARD	STANDARD	ADVANCED
very many	NO AWARD	NO AWARD	NO AWARD	NO AWARD

** proactive detection rate vs. amount of false alarms*

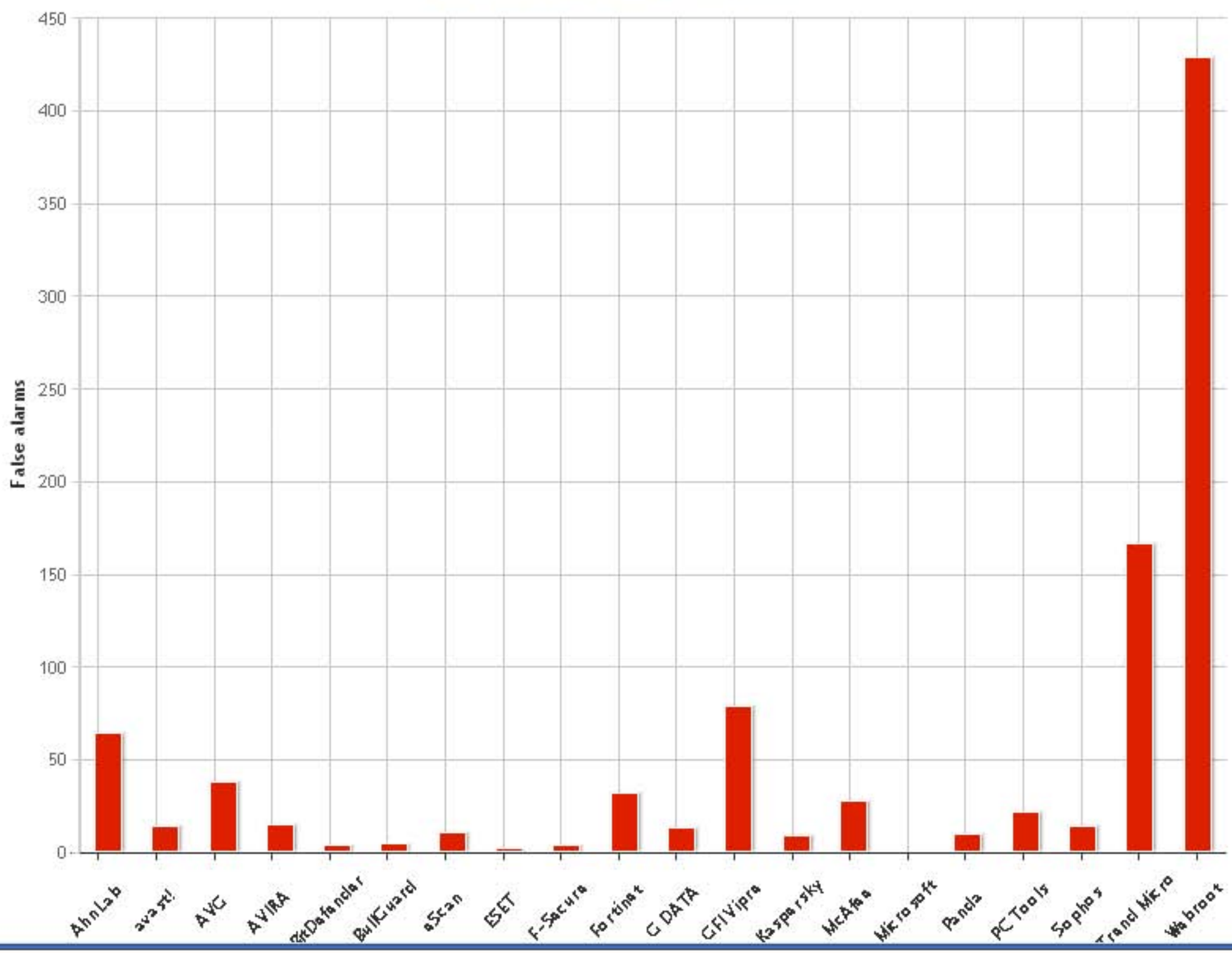
---

[3] http://www.av-comparatives.org/seiten/overview.html

Comparatives||tests - revie | AV-Comparatives - Indepen

chart.av-comparatives.org/chart1.php

Test: False Alarm Test | Year: 2012 | Month: Mar | Sort: by vendor | Zoom: 40 - 100%



Other test reports (e.g. performance tests, etc.) may also be awarded.

False alarms are an important issue and need to be taken into account when looking at detection rates. That's why e.g. in the retrospective tests false alarms lead to lower awards.

Currently (as of August 2008) the labels for the amount of false alarms are given as follows:

none or very few	0 - 3
few	4 - 15
many	16 - 100
very many	101 - 500
crazy many	over 500

At the end of each year, products are allocated an award in a summary test report, where products are nominated in various tested aspects (overall detection rate, proactive detection rate, false alarm rate, scanning speed, etc.[4]). To be designated product of the year, a product needs to get better scores than other products in most of the various tests done during the year. The label "Best product of the year" indicates only that the product was better than other products in most tests provided during the year[5]. More details about the summary awards will be given in the December report.

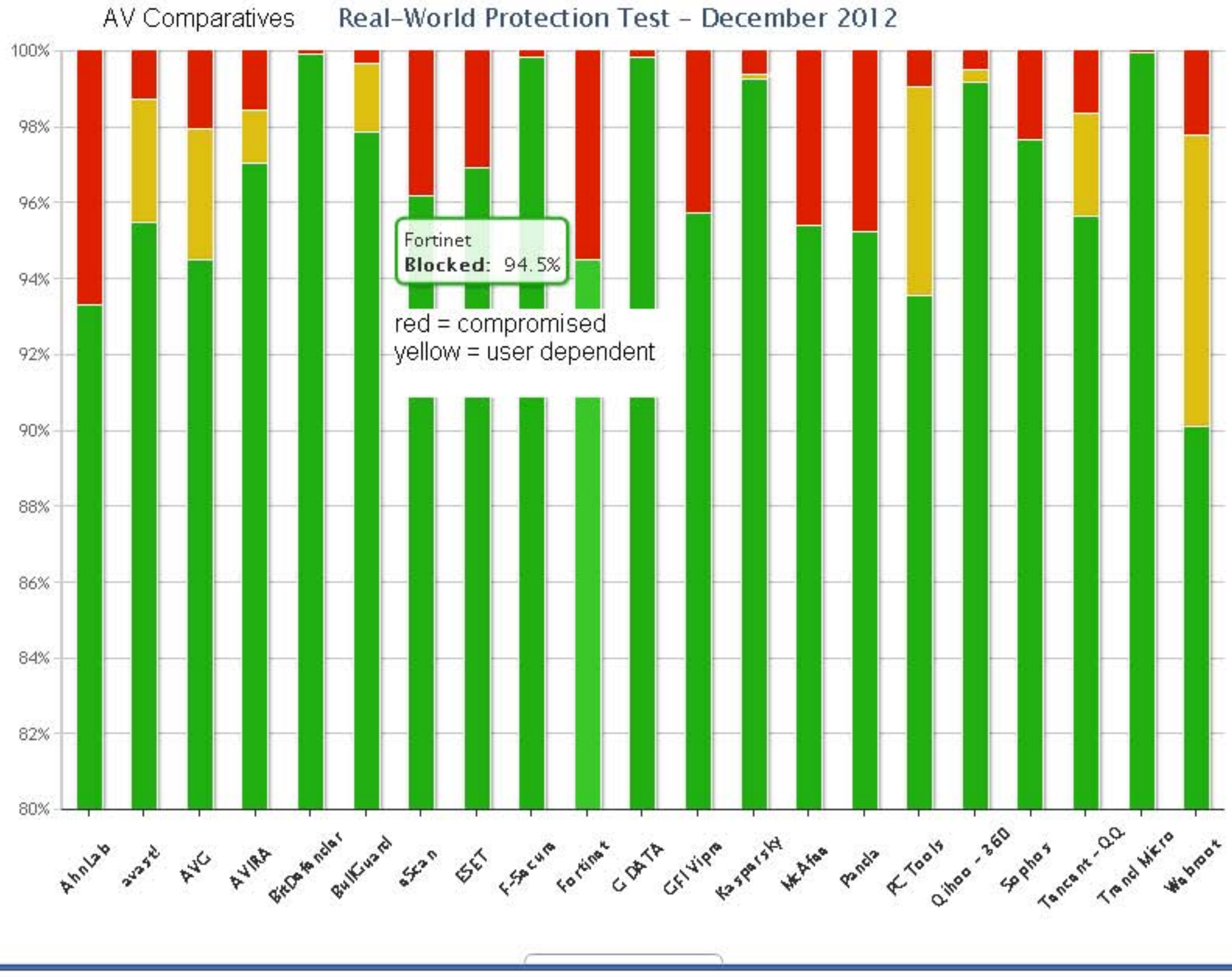
Since this year (2008), vendors of products receiving awards in the summary reports will get a certification plaque to display, for example, in corporate offices.

footnote (4): We plan to add performance tests, dynamic tests and some other tests in the future.
footnote (5) To know which product is best for you, try out the software on your own system. . . We [can only] tell you which products scored better than others in regard to some aspects of the software.

Comparatives||tests - reviev | Windows 8 approval | AV-Comparatives - Indepenc

chart.av-comparatives.org/chart1.php

Test: Real-World Protection Test | Year: 2012 | Month: Dec | Sort: by vendor | Zoom: 80 - 100%



Comparatives||tests - revie | AV-Comparatives - Indepen

chart.av-comparatives.org/chart1.php

Test: Heuristic Behavioural Test | Year: 2012 | Month: Jul | Sort: by vendor | Zoom: 40 - 100%

AV Comparatives — Heuristic Behavioural Test – July 2012

yellow = behavioral detection

Fortinet
Heuristic: 64.0
Heuristic + Behavioural Det.: 64.0

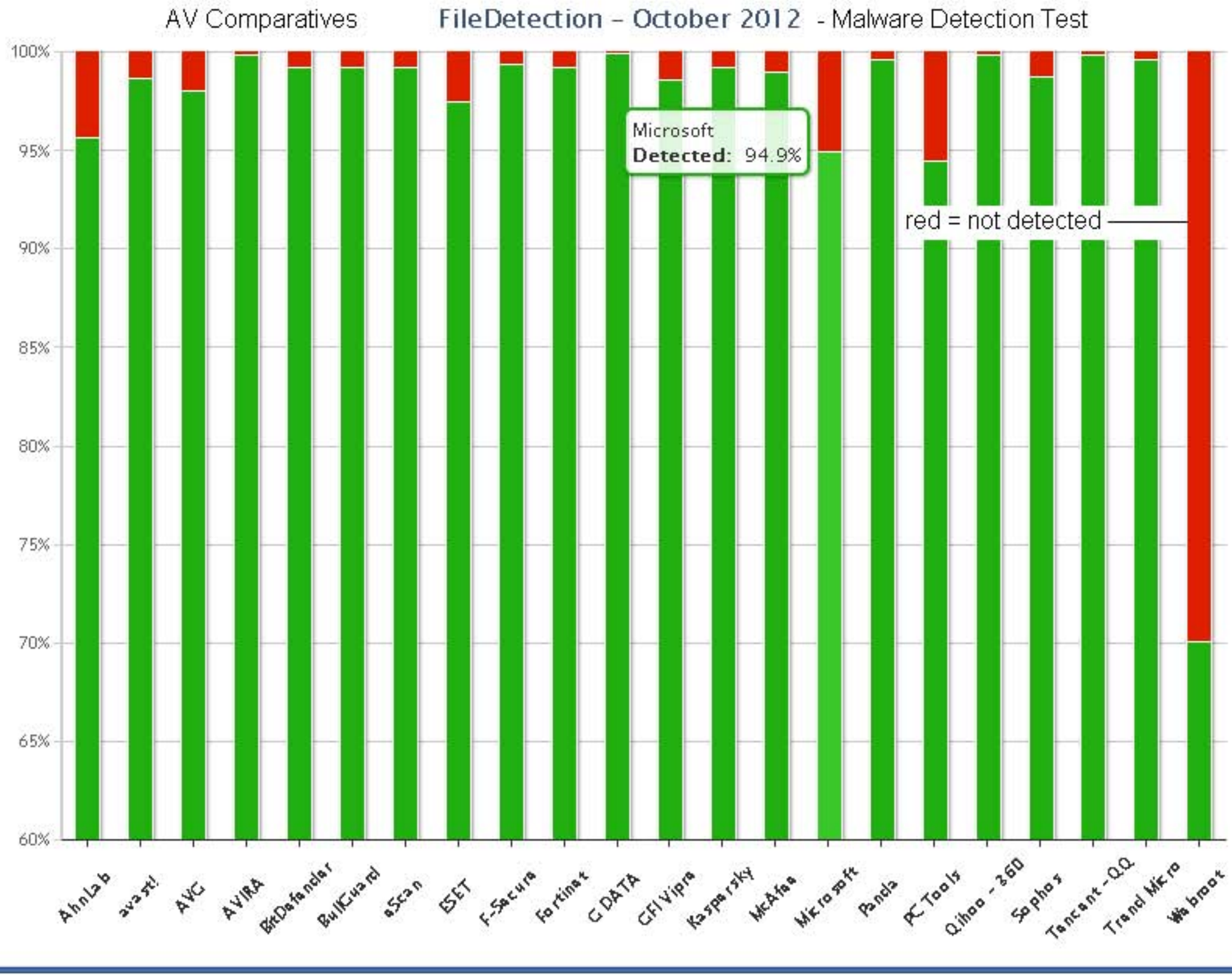
100% 90% 80% 70% 60% 50% 40%

AhnLab avast! AVG AVIRA BitDefender BullGuard eScan ESET F-Secure Fortinet G DATA GFI Vipre Kaspersky Microsoft Panda PC Tools Qihoo - 360 Tencent - QQ

Comparatives||tests - reviev | AV-Comparatives - Indepenc

chart.av-comparatives.org/chart1.php

Test: FileDetection | Year: 2012 | Month: Oct | Sort: by vendor | Zoom: 60 - 100%



Comparatives||tests - reviev | Windows 8 approval | AV-Comparatives - Indepenc

chart.av-comparatives.org/chart1.php

Test: Performance Test | Year: 2012 | Month: Oct | Sort: by vendor | Zoom: 0 - 100%

AV Comparatives

Performance Test – October 2012 - Burden on computer system

yellow = PC Mark Score

ESET
AVC Score: 88.0
Total Score: 187.7

Performance Test Scores

200
175
150
125
100
75
50
25
0

avast! | AVG | AVIRA | BitDefender | BullGuard | eScan | ESET | F-Secure | Fortinet | G DATA | GFI Vipre | Kaspersky | McAfee | Microsoft | Panda | PC Tools | Qihoo - 360 | Sophos | Trend Micro | Webroot