



Antivirus Comparative

2007 年度总结报告

成绩 优胜奖 评价

日期: 2007 年 12 月

最终修订: 2007 年 12 月 8 日

作者: Andreas Clementi

网站: <http://www.av-comparatives.org>

1. 前言

在每年年终时，AV-Comparatives 将会发布一份对各种防病毒产品的评测报告，并评出每项测试的优胜奖。请注意这份报告考虑的是**整个 2007 年的所有评测结果**，而不是最近某一单项的评测。注释和结论的依据是 AV-Comparatives 的各种评测报告，您可以在如下页面查看：

www.av-comparatives.org/seiten/comparatives.html

2. 2007 评测结果综述

反病毒产品只有拥有良好的检测率才有资格参加 AV-Comparatives 的各项正规测试。读者应该了解的非常重要的一点是：产品得到“STANDARD”评价也是一个好成绩，要达到这个标准，需要能检测到最低数量的恶意软件。许多不在 AV-Comparatives 列表中的产品远远达不到所需要的这个最低标准；因此凡是在 AV-Comparatives 评测列表中的产品都是经过挑选的优秀的反病毒软件。

下表是各种反病毒软件在 AV-Comparatives 2007 年主要评测中的成绩：

	February 2007 <i>On-demand test</i>	May 2007 <i>Retrospective test</i>	August 2007 <i>On-demand test</i>	November 2007 <i>Retrospective test</i>
Avast	ADVANCED	ADVANCED	ADVANCED	ADVANCED
AVG	ADVANCED		ADVANCED+	ADVANCED
AVIRA	ADVANCED+	STANDARD	ADVANCED+	STANDARD
BitDefender	ADVANCED	STANDARD	ADVANCED+	STANDARD
Dr.Web	STANDARD	STANDARD	STANDARD	STANDARD
eScan	ADVANCED+	STANDARD	ADVANCED+	STANDARD
F-Prot	ADVANCED	STANDARD	STANDARD	STANDARD
F-Secure	ADVANCED+	ADVANCED	ADVANCED+	STANDARD
Forinet	ADVANCED		STANDARD	
Gdata AVK	ADVANCED+	ADVANCED	ADVANCED+	ADVANCED
Kaspersky	ADVANCED+	STANDARD	ADVANCED+	ADVANCED+
McAfee	STANDARD	ADVANCED	ADVANCED	ADVANCED
Microsoft		STANDARD	STANDARD	ADVANCED
NOD32	ADVANCED	ADVANCED+	ADVANCED+	ADVANCED+
Norman	ADVANCED	ADVANCED	STANDARD	ADVANCED
Symantec	ADVANCED	ADVANCED	ADVANCED+	ADVANCED
TrustPort	ADVANCED+	STANDARD	ADVANCED+	STANDARD

注意：“灰色”意味着未达标。

3. “优胜奖”奖项

如果您计划购买一款反病毒软件，可以去厂家网站下载试用版本进行评估，它们通常会有一些附加的功能（如防火墙、恶意行为拦截、广告过滤器等）。您一般会考虑兼容性、图形用户界面、系统冲突、易管理性、语言、价格、许可证期限等诸多事项。由上可知，一款可以完美地满足所有用户需求的防病毒软件是不存在的。这决定了“优胜奖”的评选仅仅是考虑了客观测试数据，而没有考虑用户的特殊需要或喜好等其它因素。

a) 2007 年年度总冠军：

AV-Comparatives 选定 2007 年度最佳防病毒软件的条件是，需要具备高检测率，包括多复杂多态性病毒的检测率、高行为判断检测率、低误报（最好零误报）、扫描速度快、资源占用少、不引起系统崩溃或死机、没有恼人的 bug 等优势。2007 年中，以下产品均获得

三次以上的 ADVANCED+奖项：卡巴斯基和 ESET NOD32。以下产品在 2007 年度各项分类测试中综合成绩最佳：ESET NOD32 (11)、卡巴斯基 (10)、GDATA AVK (10)、赛门铁克 (9)、F-Secure (9)。其中 GDATA AVK 和 F-Secure 是多引擎产品，多引擎产品的劣势是扫描速度较慢，对系统资源的消耗相对较高，误报的可能性也相对更多一些。

综合各款防毒产品的性能和表现，2007 年度综合评比获胜者再次由 ESET NOD32 获得

b) 手动扫描测试优胜奖：

下列产品在 2007 年 2 月和 8 月的实时监控项目测试中都获得了 ADVANCED+ 的评价：eScan、F-Secure、GDATA AVK、Kaspersky and TrustPort。

下列产品在两次评测中的检测率都超过了 99%：AVIRA、GDATA AVK、TrustPort。

值得注意的是，手动扫描优胜者使用的引擎：

单引擎：**AVIRA**

多引擎：**GDATA AVK, TrustPort**

c) 主动防御按需扫描检测获胜者：

前瞻性测试能够很好地判断出按需扫描测试中，各款防毒产品的表现（使用按需扫描的方法，检测对新型、未知病毒的检测率）。测试要求在达到较高检测率的同时，将误报数量控制在最低水平。在 2007 年 5 月和 11 月的前瞻性测试中，以下产品均获得 ADVANCED+ 奖项：ESET NOD32。因此，主动防御按需扫描检测获胜者为：**ESET NOD32**。

d) 误报率测试优胜奖：

误报和真正的病毒警报一样让人心烦。因此，反病毒产品在正式发布前做严格的测试是非常重要的（为了避免误报）。

下列产品在 2007 年的评测中拥有最低的误报率：

Symantec (1), ESET NOD32 (2), eScan(2) and F-secure (2).

AV-Comparatives 2007 年误报率评测的优胜奖是零误报的测试产品：**Symantec**。

e) 手动扫描速度测试优胜奖：

下列产品拥有最高的扫描速度：

在 2007 年 5 月和 11 月两次测试中扫描速度最快的产品是：AVIRA，NOD32, Symantec 和 Fortinet。

最佳扫描设置是：**Fortinet, Symantec, AVIRA, ESET NOD32**

f) 变种病毒测试优胜奖：

下列产品在两次测试中可以 100% 检测到所有的变种病毒样本：Symantec, ESET NOD32。以 Kaspersky 作为引擎的产品（GDATA AVK, eScan, F-Secure, Kaspersky）只在最后一次测试中才能检测到所有的病毒样本。

变种病毒测试优胜奖是：**Symantec, ESET NOD32**

综上所述：

a) 总冠军/2007 最佳防病毒产品：**ESET NOD32**

其它候选者：Kaspersky, Symantec, F-Secure, GDATA AVK

- b) 手动扫描检测优胜奖（单引擎的产品）：**AVIRA**
其它候选者：Kaspersky
手动扫描检测优胜奖（多引擎的产品）：GDATA AVK, TrustPort
其它候选者：eScan, F-Secure
- c) 主动式智能扫描检测优胜奖：**ESET NOD32**
其它候选者：Kaspersky
- d) 最低误报率优胜奖：**Symantec**
其它候选者：ESET NOD32, eScan, F-Secure
- e) 最高手动扫描速度优胜奖：**Fortinet, Symantec, AVIRA, ESET NOD32**
其它候选者：McAfee, F-Port
- f) 变种病毒检测优胜奖：Symantec, ESET NOD32
其它候选者：Kaspersky, GDATA AVK, eScan, F-Secure

4. 总结

下面就 2007 年度各项测试中，各款参测防毒产品的测试结果、性能和未来发展趋势分别进行总结：

Avast (www.avast.com): 2007 年 Avast 共获得 4 项 ADVANCED 奖项，成绩较上一年度有所进步。Avast 病毒样本更新速度较快，脱壳引擎和广谱特征扫描技术也有所提高。可以预见，Avast 的检测率在下一年度将得到进一步提升。

AVG (www.grisoft.com): 2007 年我们检测了 AVG Anti-Malware，该防毒软件采用 Ewido 引擎，检测率较以往有一定提高，2007 年 8 月还获得一次 ADVANCED+ 奖项。AVG 是一款易用、占用资源较少的防毒产品，只是启发式分析技术还有待进一步提升。

AVIRA (www.avira.com): AVIRA 检测率很高（是单扫描引擎产品中检测率最高的一款），扫描速度快、主动防御检测率也较出众。唯一的不足仍然是误报过多（尽管略有改进），如果误报控制得较好的话（在不降低检测率的前提下），AVIRA 很有可能获得年度最佳防毒产品的称号。由于在启发式分析中，忽视大量误报的产品更容易取得较高的检测率，因此 AVIRA 目前还不能匹配这一称号。

BitDefender (www.bitdefender.com): 测试中，BitDefender 启发式检测率的表现再一次中规中矩，按需扫描整体检测率也较高，但不幸出现了一些误报。BitDefender 同样内置了行为分析启发式引擎，整合了个人信息防护功能，但后者只在恶意软件执行后才起作用。采用此类主动防御技术的防毒产品，一般在检测中都能获得出色的防护效果。

Dr. Web (www.drweb.com): Dr. Web (俗称大蜘蛛)是一款占用系统资源少、容易上手的防

毒产品，能够兼容较早的操作系统。Dr. Web 以其启发式技术而闻名(近来得到了改进，添加了恶意软件来源检测功能)，但不幸的是，误报仍然非常频繁。文件深入扫描能够提高检测率，但相对其他产品而言，也存在扫描速度较慢和稳定性方面的一些问题。在我们的测试中，程序不幸崩溃过一次，但给厂商反映后，迅速得以解决(包括误报的问题)。与其他产品比较而言，Dr. Web 添加新病毒特征的速度很慢，上一次测试中遗漏的病毒样本很少添加和修正。软件检测率虽然不高，但针对一些恶意软件的清除效果较为理想(根据其他检测结果³)。希望这些问题能够随着 Dr. Web v5 版本的推出得以解决。

eScan (www.mwti.com): eScan 是一款多引擎的防毒产品(使用卡巴斯基的引擎)，在我们的测试中，成绩非常接近 KAV v6 版本(KAV v7 采用了新的启发式技术，因此结果有一定差异)。在前瞻性测试中，eScan 的成绩不很理想，但按需扫描测试时，病毒库更新至最新版本后，检测还是很高的。

ESET NOD32 (www.eset.com): 由于在极低误报的基础上，保持了很高的主动防御检测率，ESET NOD32 防毒软件在历届前瞻性测试中总是无一例外地获得 ADVANCED+奖项。该防毒软件在按需扫描测试中也保持了优异的成绩，但还有改进的空间，如更快地添加当前无法检测的样本。ESET NOD32 扫描速度快，资源占用少，综合考察性能后，决定授予其 2007 年度参测防毒软件综合评比第一名的称号。

F-Prot (www.f-prot.com): 2007 年我们测试了 F-Prot 新推出的版本，F-Prot 是一款省资源、速度快、相对廉价的防毒软件产品，集成了启发式技术(但仍然造成了大量误报)。最近 F-Prot 又采用了一种新型启发式技术，想必在今后的测试中能够达到更高的检测率。

F-Secure (www.f-secure.com): F-Secure 防毒软件采用了多引擎的设计方案，其中之一就是 AVP 的引擎(使用卡巴斯基的特征库，但未采用其新型启发式技术)。这使得 F-Secure 在按需扫描测试中成绩优异，当然，同其他多引擎产品一样，扫描速度相对要明显慢一些。F-Secure 2007 版本在前瞻性测试中成绩平平，但该产品内置了主动防御技术 DeepGuard，可以防护系统免受新型、未知恶意软件的攻击(只在恶意软件执行后起作用，实时监控和按需扫描时无效)。以往的测试表明，此类主动防御技术往往能够提供较强的防护效果。

Fortinet (www.fortinet.com): 对 Fortinet 的首次测试是在 2007 年进行的。该软件扫描速度很快，但检测率不是很高。目前，Fortinet 正在努力提高检测率，迅速添加遗漏的病毒样本。其家庭版产品也采用了启发式技术，但由于随之而来的大量误报，建议用户不要开启此功能。最好 Fortinet 能够取消其家庭版产品(不包括邮件服务器版本)中现有的启发式功能，采用更加可靠的启发式方案取而代之，这样才能更容易获得个人用户的青睐。关闭启发式功能后，Fortinet 的主动防御检测率很低，因此 2008 年将不再测试 Fortinet 防毒产品。

GDATA (AVK) (www.gdata.de): AVK 2007 版本采用了双引擎的设计，一个是卡巴斯基 v6 版本引擎，另一个是 Avast 的引擎。双引擎的设计使得 AVK 2007 版本在二月和八月的按需扫描测试中脱颖而出，获得了 ADVANCED+奖项，并在前瞻性测试中获得 ADVANCED 奖项。由于将以前采用的 BitDefender 引擎更换为 Avast 引擎，主动防御检测率有所下降，但采用 Avast 引擎后速度有所提升(尽管整体来说仍然较慢)，系统资源的占用也有所改善。

卡巴斯基 (www.kaspersky.com): 卡巴斯基 2007 年共获得 3 项 ADVANCED+奖项，5 月

获得 STANDARD 认定(v6 版本), 按需扫描检测率很高, 启发式成绩优异(误报较少), 说明 v7 版有所改进。如果来年卡巴斯基采用新的引擎, 能够继续保持高检测率的成绩, 很有可能获得当年的最佳防毒产品称号。卡巴斯基内置了行为阻止功能, 能够在恶意软件执行时保护系统。检测结果表明, 其主动防御检测技术能够提供优秀的防护效果(并且可以还原恶意软件造成的系统破坏)。

麦克菲 (www.mcafee.com): 在 2007 年按需扫描测试中, 麦克菲分别获得 STANDARD 和 ADVANCED 奖项(随着 5200 引擎的推出有所提高)。采用新的引擎后, 前瞻性测试成绩也有所改进, 但误报数量较以往测试有所增加, 因此获得 ADVANCED 奖项。麦克菲产品的价格非常具有亲和力(包含反间谍、防火墙组件和一些 HIPS 功能的套装产品)。

微软 (onecare.live.com): 微软于 2006 年涉足防毒软件市场, 首次于 2007 年 2 月送样测试, 起初成绩很不理想。自那以后, 微软不断提高产品品质(按需扫描测试成绩从无奖项提升到 STANDARD, 前瞻性测试中从 STANDARD 提升至 ADVANCED)。OneCare 是一款安全套装产品, 易于个人用户掌握, 误报率也较低。微软目前正在努力提升其产品的检测率, 遗漏样本添加速度很快。如果微软能够坚持下去, 在今后的测试中一定会很快加入当前一流防毒软件的阵营。

Norman (www.norman.com): 2007 年中 Norman 继续完善其沙盘技术, 并且加快了样本的反应速度。在 AV-Comparatives 进行的前瞻性测试中, Norman 获得了 ADVANCED 奖项。Norman 采用了沙盘技术, 但只在恶意软件执行后才能发挥效力。以往的检测结果表明, 此类主动防御检测技术通常能够达到优秀的防护效果。

赛门铁克 (www.symantec.com): 赛门铁克(诺顿防毒软件)的品质在 2007 年继续有所提高, 按需扫描检测率有进一步提升, 极少出现误报的情况(能够迅速修正)。赛门铁克的最新版本在系统资源占用方面, 也比以往有很大的改善(取决于系统配置情况, 仍可能降低部分系统的效率)。扫描速度快, 能够检测出大量复杂的多态性病毒, 在主动防御检测方面, 也能达到一定的检测率, 但还有较大的提升空间。赛门铁克也在产品中内置了行为阻止功能(称为 SONAR)和主动防御系统, 能够阻止恶意软件的运行(例如偷渡式下载等)。以往的检测结果表明, 此类主动防御检测技术通常能够达到优秀的防护效果。根据其他测试结果显示, 赛门铁克对恶意软件的清除效果也相对较好。

TrustPort (www.aec.cz): TrustPort 内置了四套杀毒引擎: AVG、BitDefender、Ewido 和 Norman, 并且不久还会加入 Dr.Web 和 VBA32。由于采用多引擎设计, TrustPort 在按需扫描测试中整体成绩优异, 前瞻性测试成绩也很出色, 但是多引擎设计在取得一流检测率的同时, 也会带来扫描速度下降、系统资源占用过多和误报数量较高的问题, 对此 TrustPort 允许用户选择使用哪套引擎, 分别实现实时监控和按需扫描的功能, 所以比较适合于希望在计算机上安装多套防毒引擎的用户(如使用 AVG 引擎实时监控、BitDefender 引擎按需扫描等)。

6. 版权和免责声明

此出版物的版权归 AV-Comparatives 所有。任何对此出版物的全部或部分引用，在发表前必须得到 AV-Comparatives 的书面授权。AV-Comparatives 和其测试者不对此报告可能会引起的任何破坏或损失负责，不管它是书面的、链接或是其它任何形式。我们会尽力确保基础数据的正确性，但这并不表示 AV-Comparatives 会为测试结果的正确性负任何责任。我们不会对数据的正确性、完整性，或信息的任何内容在任何特定的时间适用于特殊目的而做出任何保证。没有人会因为涉及到创建、生成或发表测试结果而造成的任何间接地或特殊损害、或利润的损失而承担责任，也包括使用或者不能使用网站提供的服务、测试文档或任何相关数据而引起的或与此相关的任何事宜。

Andreas Clementi, AV-Comparatives (2007 年 12 月)