



# Antivirus Comparative 2006 年度总结报告

成绩 优胜奖 评价

日期: 2006 年 12 月

最终修订: 2006 年 12 月 8 日

作者: Andreas Clementi

网站: <http://www.av-comparatives.org>

## 1. 前言

从现在开始，在每年年终时，AV-Comparatives 都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 2006 年的所有评测结果，而不是最近某一项的评测。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：

<http://www.av-comparatives.org/seiten/comparatives.html>

## 2. 2006 年度评测结果综述

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 2006 年主要评测中的成绩：

	2006 年 2 月	2006 年 5 月	2006 年 8 月	2006 年 11 月
	手动扫描测试	主动智能扫描测试	手动扫描测试	主动智能扫描测试
Avast	ADVANCED	ADVANCED	ADVANCED	STANDARD
AVG	STANDARD	STANDARD	STANDARD	
AVIRA	ADVANCED+	ADVANCED	ADVANCED+	ADVANCED+
BitDefender	ADVANCED	ADVANCED+	ADVANCED	ADVANCED+
Dr.Web	STANDARD	ADVANCED	STANDARD	STANDARD
F-Prot	STANDARD	STANDARD	STANDARD	STANDARD
F-Secure	ADVANCED+	ADVANCED	ADVANCED+	STANDARD
Gdata AVK	ADVANCED+	ADVANCED+	ADVANCED+	ADVANCED+
Kaspersky	ADVANCED+	ADVANCED	ADVANCED+	STANDARD
McAfee	ADVANCED+	ADVANCED	ADVANCED	STANDARD
NOD32	ADVANCED+	ADVANCED+	ADVANCED+	ADVANCED+
Norman	STANDARD	ADVANCED	ADVANCED	ADVANCED
Symantec	ADVANCED+	STANDARD	ADVANCED+	STANDARD
TrustPort	ADVANCED+	ADVANCED+	ADVANCED+	ADVANCED+
VBA32		ADVANCED		STANDARD

注：“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) 2006 年年度总冠军：

下列产品在 2006 年全部四个主要的 AV-Comparatives 测试项目中都得到了 **ADVANCED+** 的评价：**AVK 2006**、**NOD32**、**TrustPort**（之所以是 **AVK 2006** 而不是 **AVK 2007**，是因为 **AVK 2007** 在最近的测试中有一项没有得到 **ADVANCED+** 评价）。

**AVK 2006** 和 **TrustPort** 都是多引擎产品（同时使用了诸如 **BitDefender**、**Kaspersky**、**Norman** 等引擎），只有 **NOD32** 是一个单引擎产品。多引擎产品的不利因素是会降低扫描速度，也会增加误报率。

因此，反病毒产品 2006 年度总冠军是：**NOD32**。

#### b) 手动扫描测试优胜奖：

下列产品在 2006 年 2 月和 8 月的实时监控项目测试中都获得了 **ADVANCED+** 的评价：**AVIRA**、**GDATA AVK**、**F-Secure**、**Kaspersky**、**NOD32**、**Symantec** 和 **TrustPort**。

下列产品在两次评测中的检测率都超过了 99%：**GDATA AVK**、**F-Secure**、**Kaspersky**。值得注意的是，它们都使用了 **Kaspersky** 引擎。

#### c) 主动式智能检测测试优胜奖：

主动式智能检测测试（retrospective tests）可以测试不同反病毒产品的主动式智能检测能力。可能一些主流产品像 **Kaspersky**、**McAfee** 和 **Symantec** 在此项测试中成绩不理想，这并不一定是因为它们的启发式/普通监测功能不如其它产品，而是因为一些恶意软件作者特别针对主流反病毒软件来编写自己的程序，以避免被它们检测到。因此，主流反病毒产品会面临比其它产品更多的风险。**Kaspersky**、**F-Secure**、**McAfee**、**Symantec** 等软件试图用其它监测技术来解决这个问题，但这些技术只有在恶意软件运行后才起作用，这是非常危险的事，也不适用于所有的情况，并且会比启发式技术产生更多的误报。

下列产品在 2006 年 5 月和 11 月的两次评测中都获得了 **ADVANCED+**

的评价：AVK 2006、BitDefender、NOD32 和 TrustPort；下列产品在每次评测中检测率都超过了 50%：NOD32。

主动式智能检测测试的优胜奖是：**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 2006 年的评测中拥有最低的误报率：Symantec(0 次)、McAfee(2 次)、AVG(4 次)和 Norman(6 次)。

AV-Comparatives 2006 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：AVIRA、NOD32、AVG、Symantec 和 McAfee。

在两次测试中扫描速度最快的产品是 AVIRA 和 NOD32，它们的速度可以超过 7 MB / 秒（使用最佳扫描设置）。在这两种产品之中，AVIRA 使用最佳扫描设置时速度略快于 NOD32，而使用默认设置扫描时 NOD32 的速度要快于 AVIRA。

手动扫描速度的优胜奖是：

**AVIRA**（最佳扫描设置）和 **NOD32**（默认扫描设置）。

#### 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。AVIRA 只是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**。

#### 总结：

a) 总冠军：**NOD32**

其它候选者：TrustPort, AVK 2006

b) 手动扫描检测优胜奖：KAV 引擎的产品：**AVK、F-Secure、Kaspersky**

其它候选者：AVIRA、NOD32、Symantec、TrustPort

c) 主动式智能扫描检测优胜奖: **NOD32**

其它候选者: BitDefender、TrustPort、AVK2006

d) 最低误报率优胜奖: **Symantec**

其它候选者: McAfee、AVG、Norman

e) 最高手动扫描速度优胜奖 (最佳设置): **AVIRA**

最高手动扫描速度优胜奖 (默认设置): **NOD32**

其它候选者: AVG、Symantec、McAfee

f) 变种病毒检测优胜奖: **Symantec**

其它候选者: AVIRA

#### 4. 评价

下面是关于各个参测产品在 2006 年连续测试中的成绩、性能和未来展望的一些评价:

**Avast** ([www.avast.com](http://www.avast.com)): Avast 在 2006 年的评测中赢得了三个 ADVANCED 评价和一个 STANDARD 评价。在 2006 年 8 月的手动扫描评测中, Avast 可以处理许多它以前未检测到的恶意软件。Avast 在 2007 年可能会进一步提高其检测率, 为了达到此目的, Avast 可能需要改进它们的启发式/普通扫描引擎。

**AVG** ([www.grisoft.com](http://www.grisoft.com)): AVG 拥有极快的扫描速度和很低的误报率。在 2006 年的各种测试中它的检测率不是很高 (STANDARD), 在主动式智能检测测试中的成绩也不太理想。这些状况在 2007 可能会得到改善, Grisoft 于 2006 年收购了 Ewido 公司后可能会联合 Ewido 的反恶意软件产品推出一款新产品。AV-Comparatives 将来的测试中会包括这个新的产品 (AVG AntiMalware), 它将会在预防病毒、恶意软件和间谍软件等方面提供更多的保护, 并且拥有一个改良的启发式智能扫描引擎。

**AVIRA** ([www.avira.com](http://www.avira.com)): AVIRA 是 2006 年进步最快的产品, 在 2006 年后半年的各种评测中超过了大多数其它参测产品。在第一次主动式智能检测测试

中 AVIRA 得到了很高的分数，但同时误报率也很高，这使它只获得了 ADVANCED 评价。在最后一次主动式智能检测测试时，AVIRA 在使用与 NOD32 (ADVANCED+) 相当的最佳检测设置下取得了最快的手动扫描速度，并且极少误报。AVIRA 的手动检测正确率也提高了很多 (ADVANCED+)。

如果 AVIRA 在 2007 年的全部评测中仍能保持这样的高水准，它将是明年年度总冠军的最有力竞争者。

**BitDefender ([www.bitdefender.com](http://www.bitdefender.com)):** BitDefender 在主动式智能检测测试中的成绩非常好 (ADVANCED+)，手动扫描检测率也很好 (ADVANCED)。最近几个月 BitDefender 在各方面都有进步，这将会在 2007 年评测中得以体现。BitDefender 的启发式扫描需要消耗不少系统资源并且速度不是特别快。BitDefender 内置恶意行为拦截功能 (B-Have)，它只有在恶意软件已经运行的情况下才能发挥威力。类似的主动智能检测技术测试表明它们通常能达到很好的防护效果。

**Dr.Web ([www.drweb.com](http://www.drweb.com)):** Dr.Web 以它的强力启发式扫描引擎而知名，但是很不幸，它同时导致了过高的误报率（一个产品如果误报率过高，那么它的主动式智能检测功能是不可靠的。因此，对 Dr.Web 在主动式智能检测测试中的成绩进行了扣分）。同时它的手动扫描速度也不算快，在 2006 年全部手动扫描测试中 Dr.Web 获得了 STANDARD 的评价。AV-Comparatives 认为 Dr.Web 有能力做得更好，但不清楚为什么它的进步非常缓慢。AV-Comparatives 联系了一位 Dr.Web 的代表，他承诺 Dr.Web 将会尽最大去提高检测率。

**ESET (NOD32) ([www.eset.com](http://www.eset.com)):** NOD32 在主动式智能检测测试中取得了最好的成绩 (ADVANCED+)，拥有极高的检测率和较低的误报率。NOD32 在所有的手动扫描测试中也得到了 ADVANCED+ 的评价，但仍有进一步改进的余地。再加上 NOD32 是最快的手动扫描器之一，因此，NOD32 取得了 2006 年年度总冠军的称号。

**F-Prot ([www.f-prot.com](http://www.f-prot.com)):** F-Prot 在 2006 年的各项测试中都取得了 STANDARD 的成绩。2007 年 F-Prot 推出 4.0 新版本后，测试成绩可能会有所提高。F-Prot v4 将会包括一个全新的启发式扫描引擎，在 AV-Comparatives 的内部评测中，它在主动式智能检测测试中得到了 ADVANCED+ 的评价，在 2006 年 8 月的手动扫描测试中得到了 ADVANCED 的评价。另外，F-Prot v4 也将可以很好地监测拨号程序。

**F-Secure ([www.f-secure.com](http://www.f-secure.com)):** F-Secure 在它的产品中使用了多种引擎，其中有 AVP 引擎（使用了 Kaspersky 的签名），这使 F-Secure 在全部的手动扫描测试中取得了很高的成绩（和 KAV 的成绩很相似）。像大多数多引擎产

品一样，多引擎技术的副作用是导致手动扫描的速度非常缓慢。F-Secure 2006 和 KAV 一样在主动式智能检测测试中成绩不很理想。新的 F-Secure 2007 除了改良间谍软件检测能力外，还包括主动智能检测技术 (DeepGuard)，用于防御新的/未知恶意软件 (它在恶意软件已经运行后才起作用)。类似的主动智能检测技术测试表明它们通常能达到很好的防护效果。

**GDATA (AVK) ([www.gdata.com](http://www.gdata.com)):** 本年度测试中使用的是 AVK 2006 版本。AVK 2006 在它的产品中使用了两套引擎: Kaspersky 引擎和 BitDefender 引擎。借助于这套双引擎技术 AVK 2006 很轻松地在 2006 年的四个测试项目中都得了 ADVANCED+ 的评价, 在手动扫描测试和主动式智能检测测试中都取得了很高的分数。一个产品中使用双引擎的副作用是手动扫描速度会变慢。最近 GDATA 用 Avast 引擎替换了 BitDefender 引擎, 这个改变带来的好处是稍微提高动手扫描率, 减少系统受感染的机率 (包括提高手动扫描速度)。但不幸的是, 因为去除了 BitDefender 引擎, AVK 2007 在主动式智能检测测试中的成绩比较差 (在 2006 年 11 月的评测中, 它只得到了 STANDARD 的评价, 而 AVK 2006 很轻松地就得到了 ADVANCED+ 的评价)。

**Kaspersky ([www.kaspersky.com](http://www.kaspersky.com)):** Kaspersky 拥有最高的动手扫描检测率 (像 AVK、F-Secure 等产品也使用 KAV 这套强力引擎)。在主动式智能检测测试中 KAV 没有取得很好的成绩, 但在 KAV 6.0 版本中包含恶意行为拦截功能 (PDM), 它将在恶意软件运行时保护系统。对这项主动智能检测技术的测试表明它能达到非常好的防护效果。

**McAfee ([www.mcafee.com](http://www.mcafee.com)):** 在 2006 下半年, McAfee 的检测率略有下降, 动手扫描测试的成绩由 ADVANCED+ 降为 ADVANCED, 主动式智能检测测试的成绩由 ADVANCED 降为 STANDARD。究其原因可能是 McAfee 为了减少误报, 把主要精力放在检测质量而不是检测数量上。McAfee 在 2006 年的测试中仅出现了一例误报, 这是非常不错的成绩。McAfee 新的扫描引擎在扫描速度上有所提高。2007 年 McAfee 新版的 VirusScan Plus 将会由反间谍软件、防火墙和一些其它工具捆绑而成。它还包括 SystemGuard 入侵检测组件, 用于拦截恶意行为。高级用户可能会发现 McAfee VirusScan Plus 2007 不像 SecurityCenter 那样提供丰富的设置选项。我们认为 McAfee 在 2007 年会通过改进普通/启发式扫描引擎的性能来达到它曾经拥有的水准。

**Norman ([www.norman.com](http://www.norman.com)):** 2006 年 Norman 一直在不断地进步, 最后赢得了两项 ADVANCED 测试评价。在最近八月份的手动扫描测试以来, Norman 可以检测到很多以前遗漏掉的恶意软件; 再加上它的“沙盒”启发式分析技术, 2007 年 Norman 应该会取得更好的成绩。在 AV-Comparatives 的主动式智能检测测试中 Norman 得到了 ADVANCED 的评价。Norman 的“沙盒”技术只有在恶意软件运行时才会发挥它的威力, 类似的主动智能检测技术测试表

明它们通常能达到很好的防护效果。Norman 不久将会发布产品的新版本。

**Symantec** ([www.symantec.com](http://www.symantec.com)): 凭着较快的手动扫描速度和我们的测试中唯一的无误报纪录这两项优势, Symantec (NAV) 成为 2006 年拥有最强检测变种病毒能力的防病毒产品。在手动扫描测试中 Symantec 取得了非常好的成绩 (ADVANCED+), 但在主动式智能检测测试中它只得到了 STANDARD 的评价。Symantec Norton Internet Security 2007 包含了主机入侵防御系统(HIPS), 它可以根据程序的行为来判断其是否为恶意软件并进行拦截。类似的主动智能检测技术测试表明它们通常能达到很好的防护效果。

**TrustPort** ([www.aec.cz](http://www.aec.cz)): TrustPort 在其产品中使用了两套引擎: BitDefender 引擎和 Norman 引擎。得益于它选择的引擎, TrustPort 的手动扫描检测率非常高, 它在主动式智能检测测试中成绩也很好, 在 2006 年的四项测试中它都取得了 ADVANCED+ 的评价。但由于同时使用了 BitDefender 和 Norman 引擎, 从而导致它的手动扫描速度较慢。

**VBA32** ([www.anti-virus.by](http://www.anti-virus.by)): VBA32 被证实拥有非常强劲的启发式扫描引擎, 但不幸地是它也导致了较高的误报率(一个产品如果误报率太高会影响用户做出最终选择。因此, 对 VBA32 在主动式智能检测测试中的成绩进行了扣分)。如果启用了它的深层分析模式, 它将消耗大量的时间进行扫描, 并且用户会收到如下警告信息: “注意: 额外的扫描会大大延长文件处理过程”。深层分析模式将会在 VBA32 的下个版本中进行改进, 但仍然会提供同样级别的保护。2007 年, VBA32 可能会内部测试另一个反病毒产品小组开发的产品。

## 5. 2007 年测试预计

在 2007 年, AV-Comparatives 将会改进和扩展更多的测试, 使用新的更强大的硬件来升级测试计算机, 以便有充足的时间完成测试。另外也会在 Windows Vista Ultimate 平台上进行测试(可能会在 2007 年后半年)。

越来越多的恶意软件采用了 Rootkits 技术, 反病毒产品正在展开对此类恶意软件的防护工作。对反病毒产品抵御 Rootkits 的能力测试预计在明年年内完成。

越来越多的反病毒厂家在它们的产品中添加了各种主动式检测技术, 如沙盒技术 (Sandbox)、主机入侵防御系统 (HIPS)、恶意行为拦截技术 (BehaviorBlocker) 等等, 其目的就是在其它的防护措施失效后能够抵御未知的新恶意软件。对此类技术的测试也将在 2007 年年内完成。

和 2006 年一样, 所有这些测试结果都可以在如下网页中查阅:

<http://www.av-comparatives.org/seiten/comparatives.html>

由于时间和人力物力的限制, 2007 年的评测可能只包含如下主流产品: Avast、AVG、AVIRA、AVK、BitDefender、Dr.Web、eScan、ESET NOD32、F-Prot、F-Secure、Fortinet、Kaspersky、McAfee、Microsoft、Norman、Symantec 和 TrustPort。

也可能也会追加一个附加评测（有限制），其它厂商有兴趣可以参与。现在有下列厂商很有可能会参与：**Comodo、Ikarus、K7、Rising、UNA、VBA32**。还有很多其它的厂商可以邀请，但是很显然他们没有兴趣参加明年的正式评测。

## 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 (2006 年 12 月)