



# Antivirus Comparative

## 2007 年度總結報告

成績 優勝獎 評價

日期: 2007 年 12 月

最終修訂: 2007 年 12 月 8 日

作者: Andreas Clementi

網站: <http://www.av-comparatives.org>

## 1. 前言

在每年年終時，AV-Comparatives 將會發佈一份對各種防病毒產品的評測報告，並評出每項測試的優勝獎。請注意這份報告考慮的是**整個 2007 年的所有評測結果**，而不是最近某一單項的評測。注釋和結論的依據是 AV-Comparatives 的各種評測報告，您可以在如下頁面查看：

[www.av-comparatives.org/seiten/comparatives.html](http://www.av-comparatives.org/seiten/comparatives.html)

## 2. 2007 評測結果綜述

反病毒產品只有擁有良好的檢測率才有資格參加 AV-Comparatives 的各項正規測試。讀者應該瞭解的非常重要的一點是：產品得到“STANDARD”評價也是一個好成績，要達到這個標準，需要能檢測到最低數量的惡意軟體。許多不在 AV-Comparatives 列表中的產品遠遠達不到所需要的這個最低標準；因此凡是在 AV-Comparatives 評測列表中的產品都是經過挑選的優秀的反病毒軟體。

下表是各種反病毒軟體在 AV-Comparatives 2007 年主要評測中的成績：

	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”意味著未達標。

## 3. “優勝獎”獎項

如果您計畫購買一款反病毒軟體，可以去廠家網站下載試用版本進行評估，它們通常會有一些附加的功能（如防火牆、惡意行為攔截、廣告篩檢程式等）。您一般會考慮相容性、圖形用戶介面、系統衝突、易管理性、語言、價格、許可證期限等諸多事項。由上可知，一款可以完美地滿足所有用戶需求的防病毒軟體是不存在的。這決定了“優勝獎”的評選僅僅是考慮了客觀測試資料，而沒有考慮用戶的特殊需要或喜好等其他因素。

### a) 2007 年年度總冠軍：

AV-Comparatives 選定 2007 年度最佳防病毒軟體的條件是，需要具備高檢測率，包括多複雜多態性病毒的檢測率、高行為判斷檢測率、低誤報（最好零誤報）、掃描速度快、資

源佔用少、不引起系統崩潰或死機、沒有惱人的 bug 等優勢。2007 年中，以下產品均獲得三次以上的 **ADVANCED+** 獎項：卡巴斯基和 **ESET NOD32**。以下產品在 2007 年度各項分類測試中綜合成績最佳：**ESET NOD32 (11)**、卡巴斯基 (10)、**GDATA AVK (10)**、賽門鐵克 (9)、**F-Secure (9)**。其中 **GDATA AVK** 和 **F-Secure** 是多引擎產品，多引擎產品的劣勢是掃描速度較慢，對系統資源的消耗相對較高，誤報的可能性也相對更多一些。

綜合各款防毒產品的性能和表現，2007 年度綜合評比獲勝者再次由 **ESET NOD32** 獲得

#### b) 手動掃描測試優勝獎：

下列產品在 2007 年 2 月和 8 月的即時監控項目測試中都獲得了 **ADVANCED+** 的評價：**eScan**、**F-Secure**、**GDATA AVK**、**Kaspersky and TrustPort**。

下列產品在兩次評測中的檢測率都超過了 99%：**AVIRA**、**GDATA AVK**、**TrustPort**。

值得注意的是，手動掃描優勝者使用的引擎：

單引擎：**AVIRA**

多引擎：**GDATA AVK**，**TrustPort**

#### c) 主動防禦按需掃描檢測獲勝者：

前瞻性測試能夠很好地判斷出按需掃描測試中，各款防毒產品的表現（使用按需掃描的方法，檢測對新型、未知病毒的檢測率）。測試要求在達到較高檢測率的同時，將誤報數量控制在最低水準。在 2007 年 5 月和 11 月的前瞻性測試中，以下產品均獲得 **ADVANCED+** 獎項：**ESET NOD32**。因此，主動防禦按需掃描檢測獲勝者為：**ESET NOD32**。

#### d) 誤報率測試優勝獎：

誤報和真正的病毒警報一樣讓人心煩。因此，反病毒產品在正式發佈前做嚴格的測試是非常重要的（為了避免誤報）。

下列產品在 2007 年的評測中擁有最低的誤報率：

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

AV-Comparatives 2007 年誤報率評測的優勝獎是零誤報的測試產品：**Symantec**。

#### e) 手動掃描速度測試優勝獎：

下列產品擁有最高的掃描速度：

在 2007 年 5 月和 11 月兩次測試中掃描速度最快的產品是：**AVIRA**，**NOD32**，**Symantec** 和 **Fortinet**。

最佳掃描設置是：**Fortinet**，**Symantec**，**AVIRA**，**ESET NOD32**

#### f) 變種病毒測試優勝獎：

下列產品在兩次測試中可以 100% 檢測到所有的變種病毒樣本：**Symantec**，**ESET NOD32**。以 **Kaspersky** 作為引擎的產品（**GDATA AVK**，**eScan**，**F-Secure**，**Kaspersky**）只在最後一次測試中才能檢測到所有的病毒樣本。

變種病毒測試優勝獎是：**Symantec**，**ESET NOD32**

#### 綜上：

- a) 總冠軍/2007 最佳防病毒產品：**ESET NOD32**  
其他候選者：Kaspersky，Symantec，F-Secure，GDATA AVK
- b) 手動掃描檢測優勝獎（單引擎的產品）：**AVIRA**  
其他候選者：Kaspersky  
手動掃描檢測優勝獎（多引擎的產品）：GDATA AVK，TrustPort  
其他候選者：eScan，F-Secure
- c) 主動式智慧掃描檢測優勝獎：**ESET NOD32**  
其他候選者：Kaspersky
- d) 最低誤報率優勝獎：**Symantec**  
其他候選者：ESET NOD32，eScan，F-Secure
- e) 最高手動掃描速度優勝獎：**Fortinet**，**Symantec**，**AVIRA**，**ESET NOD32**  
其他候選者：McAfee，F-Port
- f) 變種病毒檢測優勝獎：Symantec，ESET NOD32  
其他候選者：Kaspersky，GDATA AVK，eScan，F-Secure

## 4. 總結

下面就 2007 年度各項測試中，各款參測防毒產品的測試結果、性能和未來發展趨勢分別進行總結：

**Avast ([www.avast.com](http://www.avast.com)):** 2007 年 Avast 共獲得 4 項 ADVANCED 獎項，成績較上一年度有所進步。Avast 病毒樣本更新速度較快，脫殼引擎和廣譜特徵掃描技術也有所提高。可以預見，Avast 的檢測率在下一年度將得到進一步提升。

**AVG ([www.grisoft.com](http://www.grisoft.com)):** 2007 年我們檢測了 AVG Anti-Malware，該防毒軟體採用 Ewido 引擎，檢測率較以往有一定提高，2007 年 8 月還獲得一次 ADVANCED+ 獎項。AVG 是一款易用、佔用資源較少的防毒產品，只是啓發式分析技術還有待進一步提升。

**AVIRA ([www.avira.com](http://www.avira.com)):** AVIRA 檢測率很高（是單掃描引擎產品中檢測率最高的一款），掃描速度快、主動防禦檢測率也較出眾。唯一的不足仍然是誤報過多（儘管略有改進），如果誤報控制得較好的話（在不降低檢測率的前提下），AVIRA 很有可能獲得年度最佳防毒產品的稱號。由於在啓發式分析中，忽視大量誤報的產品更容易取得較高的檢測率，因此 AVIRA 目前還不能匹配這一稱號。

**BitDefender ([www.bitdefender.com](http://www.bitdefender.com)):** 測試中, BitDefender 啓發式檢測率的表現再一次中規中矩, 按需掃描整體檢測率也較高, 但不幸出現了一些誤報。BitDefender 同樣內置了行爲分析啓發式引擎, 整合了個人資訊防護功能, 但後者只在惡意軟體執行後才起作用。採用此類主動防禦技術的防毒產品, 一般在檢測中都能獲得出色的防護效果。

**Dr. Web ([www.drweb.com](http://www.drweb.com)):** Dr. Web (俗稱大蜘蛛) 是一款佔用系統資源少、容易上手的防毒產品, 能夠相容較早的作業系統。Dr. Web 以其啓發式技術而聞名(近來得到了改進, 添加了惡意軟體來源檢測功能), 但不幸的是, 誤報仍然非常頻繁。檔深入掃描能夠提高檢測率, 但相對其他產品而言, 也存在掃描速度較慢和穩定性方面的一些問題。在我們的測試中, 程式不幸崩潰過一次, 但給廠商反映後, 迅速得以解決(包括誤報的問題)。與其他產品比較而言, Dr. Web 添加新病毒特徵的速度很慢, 上一次測試中遺漏的病毒樣本很少添加和修正。軟體檢測率雖然不高, 但針對一些惡意軟體的清除效果較爲理想(根據其他檢測結果<sup>3</sup>)。希望這些問題能夠隨著 Dr. Web v5 版本的推出得以解決。

**eScan ([www.mwti.com](http://www.mwti.com)):** eScan 是一款多引擎的防毒產品(使用卡巴斯基的引擎), 在我們的測試中, 成績非常接近 KAV v6 版本(KAV v7 採用了新的啓發式技術, 因此結果有一定差異)。在前瞻性測試中, eScan 的成績不很理想, 但按需掃描測試時, 病毒庫更新至最新版本後, 檢測還是很高的。

**ESET NOD32 ([www.eset.com](http://www.eset.com)):** 由於在極低誤報的基礎上, 保持了很高的主動防禦檢測率, ESET NOD32 防毒軟體在歷屆前瞻性測試中總是無一例外地獲得 ADVANCED+ 獎項。該防毒軟體在按需掃描測試中也保持了優異的成績, 但還有改進的空間, 如更快地添加當前無法檢測的樣本。ESET NOD32 掃描速度快, 資源佔用少, 綜合考察性能後, 決定授予其 2007 年度參測防毒軟體綜合評比第一名的稱號。

**F-Prot ([www.f-prot.com](http://www.f-prot.com)):** 2007 年我們測試了 F-Prot 新推出的版本, F-Prot 是一款省資源、速度快、相對廉價的防毒軟體產品, 集成了啓發式技術(但仍然造成了大量誤報)。最近 F-Prot 又採用了一種新型啓發式技術, 想必在今後的測試中能夠達到更高的檢測率。

**F-Secure ([www.f-secure.com](http://www.f-secure.com)):** F-Secure 防毒軟體採用了多引擎的設計方案, 其中之一就是 AVP 的引擎(使用卡巴斯基的特徵庫, 但未採用其新型啓發式技術)。這使得 F-Secure 在按需掃描測試中成績優異, 當然, 同其他多引擎產品一樣, 掃描速度相對要明顯慢一些。F-Secure 2007 版本在前瞻性測試中成績平平, 但該產品內置了主動防禦技術 DeepGuard, 可以防護系統免受新型、未知惡意軟體的攻擊(只在惡意軟體執行後起作用, 即時監控和按需掃描時無效)。以往的測試表明, 此類主動防禦技術往往能夠提供較強的防護效果。

**Fortinet ([www.fortinet.com](http://www.fortinet.com)):** 對 Fortinet 的首次測試是在 2007 年進行的。該軟體掃描速度很快, 但檢測率不是很高。目前, Fortinet 正在努力提高檢測率, 迅速添加遺漏的病毒樣本。其家庭版產品也採用了啓發式技術, 但由於隨之而來的大量誤報, 建議用戶不要開啓此功能。最好 Fortinet 能夠取消其家庭版產品(不包括郵件伺服器版本)中現有的啓發式功能, 採用更加可靠的啓發式方案取而代之, 這樣才能更容易獲得個人用戶的青睞。關閉啓發式功能後, Fortinet 的主動防禦檢測率很低, 因此 2008 年將不再測試 Fortinet 防毒產品。

**GDATA (AVK) ([www.gdata.de](http://www.gdata.de)):** AVK 2007 版本採用了雙引擎的設計, 一個是卡巴斯基 v6

版本引擎，另一個是 Avast 的引擎。雙引擎的設計使得 AVK 2007 版本在二月和八月的按需掃描測試中脫穎而出，獲得了 ADVANCED+ 獎項，並在前瞻性測試中獲得 ADVANCED 獎項。由於將以前採用的 BitDefender 引擎更換為 Avast 引擎，主動防禦檢測率有所下降，但採用 Avast 引擎後速度有所提升（儘管整體來說仍然較慢），系統資源的佔用也有所改善。

卡巴斯基 ([www.kaspersky.com](http://www.kaspersky.com)): 卡巴斯基 2007 年共獲得 3 項 ADVANCED+ 獎項，5 月獲得 STANDARD 認定(v6 版本)，按需掃描檢測率很高，啓發式成績優異(誤報較少)，說明 v7 版有所改進。如果來年卡巴斯基採用新的引擎，能夠繼續保持高檢測率的成績，很有可能獲得當年的最佳防毒產品稱號。卡巴斯基內置了行爲阻止功能，能夠在惡意軟體執行時保護系統。檢測結果表明，其主動防禦檢測技術能夠提供優秀的防護效果（並且可以還原惡意軟體造成的系統破壞）。

麥克菲 ([www.mcafee.com](http://www.mcafee.com)): 在 2007 年按需掃描測試中，麥克菲分別獲得 STANDARD 和 ADVANCED 獎項(隨著 5200 引擎的推出有所提高)。採用新的引擎後，前瞻性測試成績也有所改進，但誤報數量較以往測試有所增加，因此獲得 ADVANCED 獎項。麥克菲產品的價格非常具有親和力(包含反間諜、防火牆元件和一些 HIPS 功能的套裝產品)。

微軟 ([onecare.live.com](http://onecare.live.com)): 微軟於 2006 年涉足防毒軟體市場，首次於 2007 年 2 月送樣測試，起初成績很不理想。自那以後，微軟不斷提高產品品質(按需掃描測試成績從無獎項提升到 STANDARD，前瞻性測試中從 STANDARD 提升至 ADVANCED)。OneCare 是一款安全套裝產品，易於個人用戶掌握，誤報率也較低。微軟目前正在努力提升其產品的檢測率，遺漏樣本添加速度很快。如果微軟能夠堅持下去，在今後的測試中一定會很快加入當前一流防毒軟體的陣營。

Norman ([www.norman.com](http://www.norman.com)): 2007 年中 Norman 繼續完善其沙盤技術，並且加快了樣本的反應速度。在 AV-Comparatives 進行的前瞻性測試中，Norman 獲得了 ADVANCED 獎項。Norman 採用了沙盤技術，但只在惡意軟體執行後才能發揮效力。以往的檢測結果表明，此類主動防禦檢測技術通常能夠達到優秀的防護效果。

賽門鐵克 ([www.symantec.com](http://www.symantec.com)): 賽門鐵克(諾頓防毒軟體)的品質在 2007 年繼續有所提高，按需掃描檢測率有進一步提升，極少出現誤報的情況(能夠迅速修正)。賽門鐵克的最新版本在系統資源佔用方面，也比以往有很大的改善(取決於系統配置情況，仍可能降低部分系統的效率)。掃描速度快，能夠檢測出大量複雜的多態性病毒，在主動防禦檢測方面，也能達到一定的檢測率，但還有較大的提升空間。賽門鐵克也在產品中內置了行爲阻止功能(稱爲 SONAR)和主動防禦系統，能夠阻止惡意軟體的運行(例如偷渡式下載等)。以往的檢測結果表明，此類主動防禦檢測技術通常能夠達到優秀的防護效果。根據其他測試結果顯示，賽門鐵克對惡意軟體的清除效果也相對較好。

TrustPort ([www.aec.cz](http://www.aec.cz)): TrustPort 內置了四套殺毒引擎：AVG、BitDefender、Ewido 和 Norman，並且不久還會加入 Dr.Web 和 VBA32。由於採用多引擎設計，TrustPort 在按需掃描測試中整體成績優異，前瞻性測試成績也很出色，但是多引擎設計在取得一流檢測率的同時，也會帶來掃描速度下降、系統資源佔用過多和誤報數量較高的問題，對此 TrustPort 允許用戶選擇使用哪套引擎，分別實現即時監控和按需掃描的功能，所以比較適合於希望在電腦上安裝多套防毒引擎的用戶(如使用 AVG 引擎即時監控、BitDefender 引擎按需掃描等)。

## 6. 版權和免責聲明

此出版物的版權歸 AV-Comparatives 所有。任何對此出版物的全部或部分引用，在發表前必須得到 AV-Comparatives 的書面授權。AV-Comparatives 和其測試者不對此報告可能會引起的任何破壞或損失負責，不管它是書面的、鏈結或是其他任何形式。我們會盡力確保基礎資料的正確性，但這並不表示 AV-Comparatives 會為測試結果的正確性負任何責任。我們不會對資料的正確性、完整性，或資訊的任何內容在任何特定的時間適用於特殊目的而做出任何保證。沒有人會因為涉及到創建、生成或發表測試結果而造成的任何間接地或特殊損害、或利潤的損失而承擔責任，也包括使用或者不能使用網站提供的服務、測試文檔或任何相關資料而引起的或與此相關的任何事宜。

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