

AV-Comparative



杀毒产品性能测试 (仅AV产品)

防病毒软件对系统性能的影响

语言: 中文

2013年4月

最后修订: 2013年5月6日

www.av-comparatives.org

目录



| | |
|----------------|----|
| 1. 简介 | 3 |
| 2. 参与测试的产品 | 3 |
| 3. 测试方法 | 4 |
| 4. 测试说明及注释 | 5 |
| 5. 测试案例 | 7 |
| 6. 测试结果 | 8 |
| 7. 本次测试产品取得的成绩 | 12 |
| 8. 版权及免责声明 | 13 |

简介

我们要明确的是：本报告所显示的结果，只是各种反病毒产品在此次特定的测试中对系统性能（主要是受实时/访问时扫描组件）的影响。我们鼓励用户在自己的电脑上试用软件，然后根据试用结果得出自己的意见。

参与测试的产品

在本次测试中，我们对以下产品¹进行了评估（使用各自的默认设置）：

| | |
|---------------------------------|--|
| Avast! Free Antivirus 8.0 | Kaspersky Anti-Virus 2013 |
| AVG Anti-Virus 2013 | 金山新毒霸 2013.SP2.5 |
| AVIRA Antivirus Premium 2013 | McAfee AntiVirus Plus 2013 |
| Bitdefender Antivirus Plus 2013 | Microsoft Security Essentials 4.2 |
| BullGuard Antivirus 2013 | Panda Cloud Antivirus Free 2.1.1 |
| Emsisoft Anti-Malware 7.0 | 奇虎360杀毒软件4.0 |
| eScan Anti-Virus 14.0 | Sophos Anti-Virus 10.2 |
| ESET NOD32 Antivirus 6.0 | Symantec Norton Anti-Virus 2013 ² |
| Fortinet FortiClient Lite 4.3.5 | ThreatTrack Vipre Antivirus 2013 |
| F-Secure Anti-Virus 2013 | Trend Micro Titanium Antivirus Plus 2013 |
| G DATA AntiVirus 2014 | |

请注意，本测试结果只适用于上面列出的产品/版本（例如，64位、产品版本等）。另外，提请读者注意的是，不同厂商的产品还提供不同类型（和不同数量的）的功能。

下列测试项目以及测试活动是在最新的Windows 7专业版SP1 64位操作系统下进行的：

- 复制文件
- 压缩/解压缩文件
- 编码/转码
- 安装/卸载应用程序
- 启动应用程序
- 下载文件
- PC Mark 7 专业测试集

¹ 测试时（2013年4月末），我们使用的产品版本都是最新的版本。

² 本次测试我们对赛门铁克诺顿做了测试，虽然他们并没有申请加入我们的年度测试。某杂志已承担赛门铁克的测试费。

我们更新了测试集和性能测试的步骤（例如，已重新更新过的测试文件、测试时间/测试周期和自动化脚本），以及测试使用的硬件。

测试方法

测试机采用英特尔酷睿i5-3330 CPU和4GB的内存。性能测试首先是在纯 Microsoft Windows 7 Professional SP1 64位（英文）系统上完成，然后在系统中安装了杀毒软件（采用各自默认的设置）。已经完成的测试还使用了有效的互联网连接，来模拟实际使用中云服务及功能对系统性能可能产生的影响。

在开始各项测试前，对硬盘已做过碎片处理，目的是要将各种可能影响测试结果和/或系统可比性的因素降到最低。某些产品采用的优化处理/指纹识别功能也被考虑在内——这意味着此结果能够体现安全产品对系统性能的影响，且受影响的系统已经被用户使用了一段时间。为取得平均值并剔除测量误差，我们（分别在使用和不使用指纹识别功能的情况下）对测试项目进行反复测试。每次运行完毕后，用于测试的工作站（机）都被整理和重新启动。我们模拟电脑用户可能执行的各种文件操作：从一处复制³不同类型的干净文件到另一处、压缩和解压缩文件、安装和卸载应用程序、转换⁴音频和视频文件、从网上下载文件、启动应用程序等等。我们还使用了业内公认的第三方性能测试集（PC Mark 7 Professional）来衡量现实生活中，使用各安全产品对系统的影响。我们请读者自己评估各款产品，看看这些产品是如何影响自己的系统的（如软件冲突/或用户的参数设置造成的影响，以及不同的系统配置，也可能导致不同的结果）。

防病毒产品需要在初期阶段加载到系统中，并从一开始就提供安全保障 - 这些加载在一定程度上对系统的启动时间存在某些影响。准确测量启动时间，是相当具有挑战性的。最显著的问题是确定系统完全启动的确切时间，因为很多操作环境在系统对用户已作出反应后，有时可能仍然继续执行启动。同样重要的还有，要考虑这些被测试的安全产品何时才算提供全面有效的保护时间，因为就安全解决方案而言，这可能是一种有用的启动完成衡量标准。此外，在启动时（用户可能已经注意到，系统经过一段时间加载后，有时系统速度变得很慢），一些安全产品加载服务很晚（有的甚至晚几分钟），所以，系统看起来像运行非常快，但实际上是稍后才加载服务，这样其实会使该系统变得不安全或极易受到攻击。由于我们不希望支持这类活动，所以，我们决定不检测启动时间。

为了验证我们的观点，我们对接受测试的各安全产品，对于存放在启动文件夹中的恶意软件被执行前，是否加载完各自全部的保护模块分别进行了检测。除了AVG、Bitdefender、eScan、金山、微软和Sophos几款产品外，其他产品都未加载完毕。其中，只有AVG和Sophos两款产品，在系统启动后，恶意软件被执行前（通过提前加载自身保护程序），检测到并阻止了恶意软件的执行，剩下的产品则是当恶意软件先被执行后，才由自己的防病毒程序检测到，但为时已晚。

³ 我们用于测试的各种类型的文件大约有3GB，（包括图片、视频、音频文件、各种MS Office 文档、PDF文件、应用程序/可执行文件、微软Windows 7系统文件、压缩文档等）。

⁴ 将MP3文件转换为WAV文件、将MPS文件转换为WMA和AVI到MP4文件

测试说明及注释

防病毒软件的访问时扫描/实时扫描程序组件，作为后台进程来检查所有被访问的文件，以持续保护系统免受恶意软件的威胁。例如，只要文件被访问，“访问时扫描”程序便扫描文件；同时行为拦截器又添加了一层不同的保护和监控，即当文件已经被执行或运行时监测文件动作。在后台运行的服务和进程来完成这些任务时也需要并使用系统资源。通常，套装产品对系统性能的影响要高于防病毒产品对系统性能的影响，因为套装产品中包含更多的服务/功能在后台运行。

防病毒产品需要积极的深入到系统中才能起到保护作用（例如执行扫描处理），并且为了识别 Rootkits 和其他的恶意软件，在系统启动过程中安全产品已处于激活的状态。那些步骤又占用了额外的时间，因此延迟了系统的开机/启动时间。

如果产品占用太多的系统资源，用户嫌烦，可能会禁用或卸载一些必要的防护功能（这将大大影响其系统的安全性）或更换到系统资源占用较低的安全软件。因此，对于防病毒软件来说重要的不仅是能够提供较高的检测率和良好的保护功能，免受恶意软件攻击，而且还需要它不会降低系统性能或使用户（使用时）感到麻烦。

虽然从这份报告中能看出各种防病毒产品对系统性能产生的影响，然而它并不能说明，安全软件需要为系统缓慢负主要责任。其他因素对系统性能也有影响，如果用户遵循一些简单的规则，系统性能可能会有显著的改善。接下来的部分针对其他因素可能产生的一些影响进行阐述。

在一些用户电脑上观察到的几个常见问题：

- 硬件陈旧：如果电脑的速度已经是超级慢，那么估计它的硬件已经是老的不能再老了，再配上现代的（反病毒）软件，会百分百让它吃不消。
 - o 如果条件允许，换一台新电脑，至少在配置上达到您要使用的软件的最低要求。最好是多核处理器。
 - o 增加内存也是不错的选择。如果您使用 Windows XP、Windows 7或 Windows 8，您应该最低使用2GB的内存（RAM）。如果您使用Vista，干脆换到Windows 7或Windows 8。最好使用64位操作系统，因为优化的软件在这样的系统中将会运行得更快。
 - o 请确保只使用一种反病毒实时保护方案。如果您的新电脑带有试用版的防病毒程序，请在安装其他不同的防病毒程序前删除它。
- 保持所有的软件为最新版本：即使您仍然可以更新病毒库，但2010年的防病毒软件所提供的保护，是无法与新版本提供的保护相提并论的。定期访问 <http://update.microsoft.com>，通过安装推荐的补丁让您的操作系统保持最新。任何软件都可能存在弱点和缺陷，所以让您电脑上安装的所有软件保持最新——这不但能够防止许多漏洞和缺陷，也能为您改善已推荐的其他应用程序。
- 清理您的硬盘内容

- 如果您的硬盘快满了，您的系统性能也将因此受到影响。至少留出 20% 的磁盘空间，然后将电影和其他经常访问的文件保存到另一个（外部）磁盘作为备份。如果钱不是问题，可以考虑买固态硬盘（SSD）。
 - 卸载不需要的软件。通常情况下，安装防病毒产品后，用户会发现电脑运行速度有变化，这是由于其他软件仍在电脑的后台运行造成的（即，由于软件冲突或其他巨大文件的访问程序，每次访问都需要杀毒扫描）。
 - 在程序菜单中，删除“自动启动/启动文件夹”中不必要的“项/快捷方式”。
 - 如果您的电脑已经被残留文件和在过去几年里安装和卸载的数百个遗留的应用程序注册表项搞砸了，那么请重做操作系统，只安装您真正需要使用的软件（安装的软件越少，潜在的漏洞和冲突就越少），例如图像/备份工具，以确保您未来不必手动重新安装一切。
- **定期整理您的硬盘：** 硬盘中的磁盘碎片可以对系统性能造成非常大的影响，它会大大延长您的系统启动时间。
- **指纹识别/优化：** 大部分防病毒产品使用各种技术来降低其对系统性能的影响。指纹识别就是这样一种技术，它对已扫描过的或已经记入白名单的文件，在一段时间内不再（或很少）重新扫描。这虽然大大提高了速度（特别是当个人电脑经过一段时间的使用后），但也增加了一些小的潜在风险，因为使用此技术，安全软件就不再重新扫描所有的文件。它取决于用户的选择。我们建议定期进行全系统扫描（以确保所有文件至少目前都是未受感染的，并进一步优化指纹识别技术）。
- **要有耐心：** 由于杀毒而额外拖延一点时间不应算是麻烦。但是，即使采纳了上述建议，在您已经安装了防病毒软件产品后，仍然还是有性能方面的困扰，那么应该考虑其他的防病毒产品试试。（如果在使用了防病毒产品很长一段时间后，只注意到系统运行速度下降，有可能背后还有其他原因）。不要通过禁用基本保护功能而降低了产品的安全保护设置，而是要为自己争取一个稍快的个人电脑。

测试项目案例

复制文件

一些防病毒产品不按设计/默认规则扫描所有类型的文件（在文件扩展名的基础上），或为了加快速度，跳过已扫描的文件（见第6页的注释），而使用指纹识别技术。我们复制了一套不同的常用文件类型，这套文件从一块物理硬盘被复制到另一块物理硬盘中。

压缩和解压缩文件

压缩文件通常是用于文件存储，而大多数用户关心的是，当建立新的压缩文件或从现有的压缩文件解压时，防病毒软件对这个过程的影响时间。我们压缩了一组被广泛使用于家庭和办公场所的不同的文件类型。测试结果已经考虑了防病毒产品的指纹识别/优化技术，因为通常情况下，大多数用户都在磁盘上压缩文件。

编码/转码

通常音乐文件都是在家庭系统存储并转换，转换这些文件也是非常占用系统资源的。因此，许多家庭用户可能有兴趣知道，当多媒体文件从一种格式转换到另一种格式时，防病毒产品是否也对他们的系统产生了影响。我们使用FFmpeg和HandBrakeCLI对一些多媒体文件进行了转换。

安装/卸载应用程序

我们使用静默安装模式安装了几款常用的应用程序，然后记录卸载这些程序所需的时间。因为通常情况下，一个应用程序只安装一次，所以（测试过程中）我们没有考虑指纹识别技术。

启动应用程序

Office 文件（Word、Excel、PowerPoint）和 PDF 文件都是常用的应用程序文件。我们用微软Office 文件打开了一些大型的文档（并关闭它），以及用Adobe Acrobat Reader打开一些大型的 PDF文件（并关闭它）。打开和关闭视图或编辑应用程序所需的时间也都做了计量。虽然我们列出了首次运行和后续运行的测试结果，但我们认为后续运行（的结果）更重要，因为通常此项操作已经被用户做过几次，并且防病毒产品的优化功能已开始发挥作用，其对系统的影响已降低到最小。

下载文件

使用允许在后台发送HTTP请求的，无图形界面浏览器，从本地服务器下载大型文件。此外，还从本地服务器经由wget获取一些热门网站的内容。

测试结果

这些特定的测试结果，显示了参与测试的上述几款防病毒产品同其它已测试过的防病毒安全套装相比，对系统产生的影响情况。报告中的数据只作为提示使用，并不一定适用于所有情况，因为还有太多的因素可能发挥另外的作用。

我们发现，使用百分比表示测试结果很容易被用户曲解（也容易被营销部门或媒体滥用），且当使用其他规格的硬件时，需要调整百分比。所以，我们通过聚类法为测试结果分组。在这些类别中，没有统计误差，也考虑了计量错误的影响。通过研究统计方法，诸如层次聚类法，我们对于类别进行了划分，以及从用户的角度考虑需注意的情况，或与其他产品相比，对性能的影响都考虑了进来。由于使用群集建立了单独的性能测试结果（第9页），如果有一些产品比其他产品较快/较慢，这都在测试结果中得到反映。因此，测试结果不能直接同之前的测试结果进行比较，只能在所在的测试中进行纵向比较。这意味着，如果您认为某个产品与去年同期相比（在某些方面）变得慢了，这是理解错误。需要纠正的是，这个结果表明，该产品的速度与（本次测试）排位较高的产品纵向对比的结果较慢。我们本次仅提供集群的平均值（百分比是指没有安装AV产品的系统）：

| | 慢 | 中速 | 快 | 非常快 |
|----------------------|---|--------------------|--------------------|---------------|
| 复制文件 (首次运行) | - | 本集群的平均值 超过100% | 本集群的平均值低 于100% | 本集群的平均值低于+50% |
| 复制文件 (后续运行) | - | - | 本集群的平均值超 过+35% | 本集群的平均值低于+35% |
| 压缩/解压缩文件 | - | - | 本集群的平均值超 过+10% | 本集群的平均值低于+10% |
| 安装/卸载应用程序 | - | 本集群的平均值 超过+80% | 本集群的平均值低 于+80% | 本集群的平均值低于+40% |
| 编码/转码 | - | - | - | 本集群的平均值低于2% |
| 打开Office文档（首 次运行） | - | 本集群的平均值 超过+120% | 本集群的平均值低 于+120% | 本集群的平均值低于+60% |
| 打开Office文档（后 续运行） | - | - | 本集群的平均值超 过+35% | 本集群的平均值低于+35% |
| 打开PDF文件（首次运 行） | - | 本集群的平均值 超过+60% | 本集群的平均值低 于+60% | 本集群的平均值低于+20% |
| 打开PDF文件（后续运 行） | - | - | 本集群的平均值超 过+10% | 本集群的平均值低于+10% |
| 下载文件 | - | 本集群的平均值 超过+120% | 本集群的平均值低 于+120% | 本集群的平均值低于+60% |

AV-C性能测试得分总览

| 厂商 | 复制文件 | | 压缩/解压缩文件 | 安装/卸载应用程序 | 文件编码/转码 | 启动应用程序 | | | | 下载文件 |
|-------------|------|------|----------|-----------|---------|------------|------|---------|------|------|
| | | | | | | 打开Office文档 | | 打开PDF文件 | | |
| | 首次运行 | 后续运行 | | | | 首次运行 | 后续运行 | 首次运行 | 后续运行 | |
| Avast | | | | | | | | | | |
| AVG | | | | | | | | | | |
| AVIRA | | | | | | | | | | |
| Bitdefender | | | | | | | | | | |
| BullGuard | | | | | | | | | | |
| Emsisoft | | | | | | | | | | |
| eScan | | | | | | | | | | |
| ESET | | | | | | | | | | |
| Fortinet | | | | | | | | | | |
| F-Secure | | | | | | | | | | |
| 歌德塔 | | | | | | | | | | |
| 卡巴斯基 | | | | | | | | | | |
| 金山 | | | | | | | | | | |
| 迈克菲 | | | | | | | | | | |
| 微软 | | | | | | | | | | |
| 熊猫 | | | | | | | | | | |
| 奇虎 | | | | | | | | | | |
| Sophos | | | | | | | | | | |
| Symantec | | | | | | | | | | |
| 趋势科技 | | | | | | | | | | |
| VIPRE | | | | | | | | | | |

关键字：
 慢 中速 快 非常快



PC Mark 测试

为了提供业界公认的性能测试，我们本次使用了 PC Mark 7 Professional Edition⁵ 测试集。用户使用 PC Mark 7 时，应注意尽量减少所有可能对测试套装产生影响的外部因素，并至少严格按照 PC Mark 说明书的考虑和建议去操作，以获得统一有效和有用的结果。此外，应反复多做几次测试来进行验证。更多的关于PC Mark的不同应用方案测试信息，请阅读其官网⁶公布的白皮书。

在使用PC Mark的测试中，对“未安装AV产品”采用的是100分的评分方法⁷。

| | PC Mark points |
|-------------------|----------------|
| <i>without AV</i> | 100 |
| F-Secure | 99,6 |
| Kaspersky | |
| Sophos | |
| ESET | 99,4 |
| Microsoft | |
| Avira | 98,9 |
| Avast | 98,7 |
| Panda | |
| Symantec | |
| AVG | 97,9 |
| Bitdefender | 97,6 |
| Emsisoft | |
| Fortinet | |
| McAfee | |
| Qihoo | |
| Vipre | 97,3 |
| G DATA | 96,8 |
| Trend Micro | |
| BullGuard | 96,3 |
| eScan | 92,5 |
| Kingsoft | 91,4 |

⁵ 更多信息，请进入 <http://www.pcmark.com/benchmarks/pcmark7/>

⁶ <http://www.pcmark.com/benchmarks/pcmark7/whitepaper/whitepaper.pdf> (PDF)

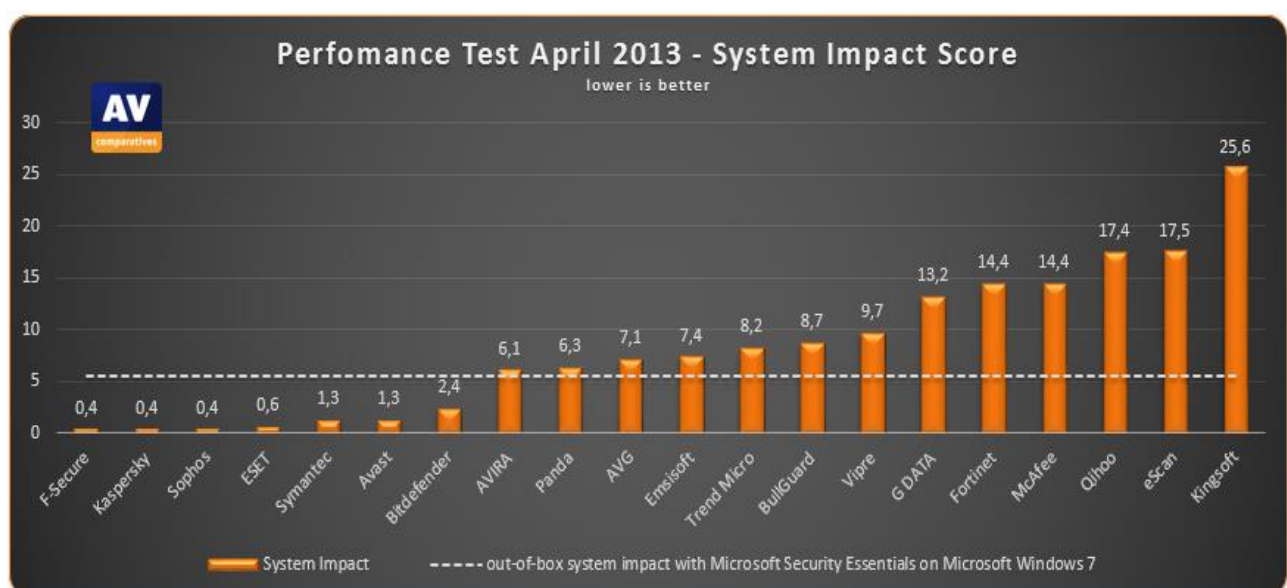
⁷ 基本评分方法：测试机使用英特尔酷睿i5-3330 4GB内存

总结

用户应根据需要权衡这些产品的其他分项测试。为总结各种测试结果，我们采用计分制。

“文件复制”以及“启动应用程序”（在后续运行时），我们采用平均值。与之前的性能测试一样，“非常快”我们给15分，“快”给10分，“中速”给5分，“慢”给零分。结果如下：

| | AV-C得分 | PC Mark 得分 | 总分 | 影响分 |
|----------------------|--------|------------|-------|------|
| F-Secure、卡巴斯基、Sophos | 90 | 99,6 | 189,6 | 0,4 |
| ESET | 90 | 99,4 | 189,4 | 0,6 |
| Avast、Symantec | 90 | 98,7 | 188,7 | 1,3 |
| Bitdefender | 90 | 97,6 | 187,6 | 2,4 |
| 微软 | 85 | 99,4 | 184,4 | 5,6 |
| AVIRA | 85 | 98,9 | 183,9 | 6,1 |
| 熊猫 | 85 | 98,7 | 183,7 | 6,3 |
| AVG | 85 | 97,9 | 182,9 | 7,1 |
| Emsisoft | 85 | 97,6 | 182,6 | 7,4 |
| 趋势科技 | 85 | 96,8 | 181,8 | 8,2 |
| BullGuard | 85 | 96,3 | 181,3 | 8,7 |
| VIPRE | 83 | 97,3 | 180,3 | 9,7 |
| G DATA | 80 | 96,8 | 176,8 | 13,2 |
| Fortinet、迈克菲 | 78 | 97,6 | 175,6 | 14,4 |
| 奇虎 | 75 | 97,6 | 172,6 | 17,4 |
| eScan | 80 | 92,5 | 172,5 | 17,5 |
| Kingsoft | 73 | 91,4 | 164,4 | 25,6 |



本次测试产品取得的成绩

以下评测成绩⁸仅适用于本次性能测试。请注意，性能测试仅告诉您一款杀毒产品同其他防病毒产品相比可能对您的系统产生的影响，它并不能证明各款产品所能提供的有效保护能力。

| 成绩 | 产品 ⁹ |
|---|--|
|  | <ul style="list-style-type: none"> ✓ F-Secure ✓ 卡巴斯基 ✓ Sophos ✓ ESET ✓ Avast ✓ 赛门铁克 ✓ Bitdefender |
|  | <ul style="list-style-type: none"> ✓ AVIRA ✓ 熊猫 ✓ AVG ✓ Emsisoft ✓ 趋势科技 ✓ BullGuard ✓ VIPRE |
|  | <ul style="list-style-type: none"> ✓ G DATA ✓ Fortinet ✓ 迈克菲 ✓ 奇虎 ✓ eScan |
|  | <ul style="list-style-type: none"> ✓ Kingsoft |

上述成绩是我们在Windows 7 Professional SP1 64 位操作系统中，使用各防病毒产品的默认设置测试后，并对影响结果进行综合评估基础上评出的。

⁸ 本次奖励不再包含微软安全产品，因为他们参与的是非奖励测试。

⁹ 对于同档成绩的产品，我们建议用户对这些产品给予同等考虑。

版权及免责声明

本报告的版权 © 2013 由 AV-Comparatives e.V. ®所有。任何出版物对本测试结果的使用, 无论是全部或部分, 都必须先得到AV-Comparatives管理部门明确的书面同意并允许。对使用本报告提供的信息, 可能会产生或导致的损害或损失, AV-Comparatives 和参与测试的人员, 不承担责任。我们竭尽全力可能, 确保基本数据的正确性, 但并不代表AV-Comparatives对测试结果的正确性需要承担义务。对报告的正确性, 完整性, 或者在任何特定的时间, 对报告提供的内容是否适合特殊目的的需求, 我们不做任何保证。对于在创建, 生成或发表测试结果过程中, 所涉及到的任何人, 对任何间接的, 特殊的损害或利益损失, 使用或不能使用该网站提供的服务, 测试文件或任何相关的数据引起的或与之相关的事宜, 均不承担任何责任。

AV - Comparatives是在奥地利注册的非盈利性组织。

AV-Comparatives e.V. (2013年5月)