

2011安全保护产品 调查报告



语言：中文

最后修订：2011年3月10日

www.av-comparatives.org

简介

为了从总体上改善我们的测试服务，我们对访问 AV-Comparatives 官网的访问者，做了一次主题关于防病毒软件测试和防病毒软件的问卷调查。调查的结果对我们非常有帮助。在此，我们对于肯花费时间完成我们的调查表的所有参与者表示感谢。

主要数据

调查持续时间： 2010 年 12 月 15 日 - 2011 年 1 月 15 日

收到的全部问卷： 1247 份

无效回复： 182 份（84 份无效，98 份回复来自有关的防病毒厂商）

有效回复： 1065 份

调查包含不少棘手的问题，需要我们检查并剔除那些无效的回复，以及试图扭曲结果或通过给出不可能或矛盾答案的问卷。因为我们主要对访问我们网站的普通用户的见解感兴趣，所以，这份公开的调查报告不考虑与防病毒厂商有关的参与者的回复。

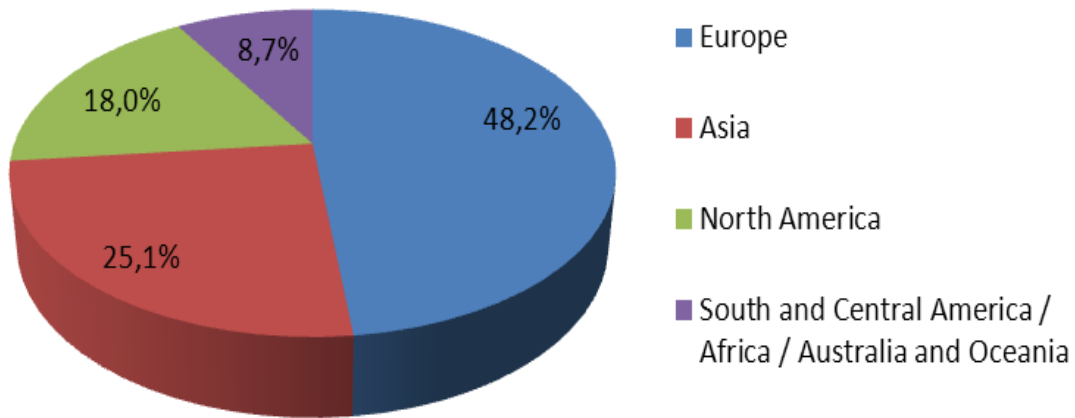
请注意：这些不厌其烦地填写我们冗长的调查表的参与者，仅是访问我们网站的用户的一部分。也请勿夸大此次调查的结果；这个结果只是在调查参与者回答的基础上形成的一个总结。还请阅读本调查报告的读者明白一点，那就是这份报告也包含了个人的评论和见解。

调查的结果对我们而言是弥足珍贵的；您将在这份报告中看到我们希望与您共同分享的一些问题的调查结果。

人口样本

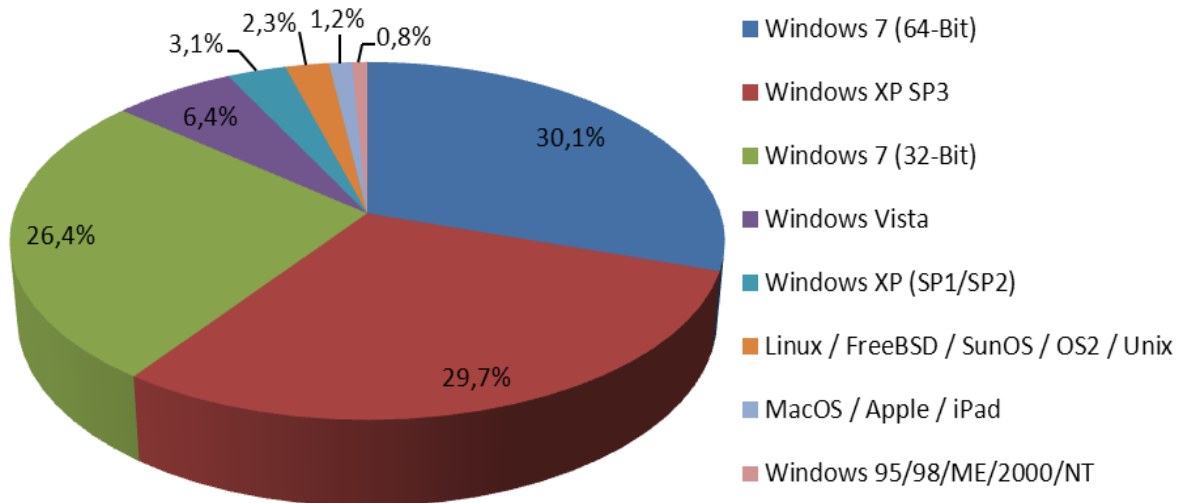
以下三个问题包括人口情况，以便我们同自己内部网站的统计数字进行对比，获得的信息让我们知道，用于调查的参与者的样本数量，是否足够代表我们网站的访问者。调查期间，问题的答案与我们网站的统计数字一致（这表示调查参与者的数量能够代表我们网站的访问者）。

1. 您来自哪里？



(饼图右侧文字说明<从上至下>：欧洲；亚洲；北美洲；南美和中美洲/非洲/澳洲和大洋洲)

2. 您主要使用哪个操作系统？



至少参与此次调查的家庭用户，现在都好像从 Windows XP 换成了 Windows 7 操作系统。在商业环境中 XP 也许仍在广泛使用，虽然在未来几年中将被淘汰。根据 Global Stats of Statcounter¹ 的统计，到目前为

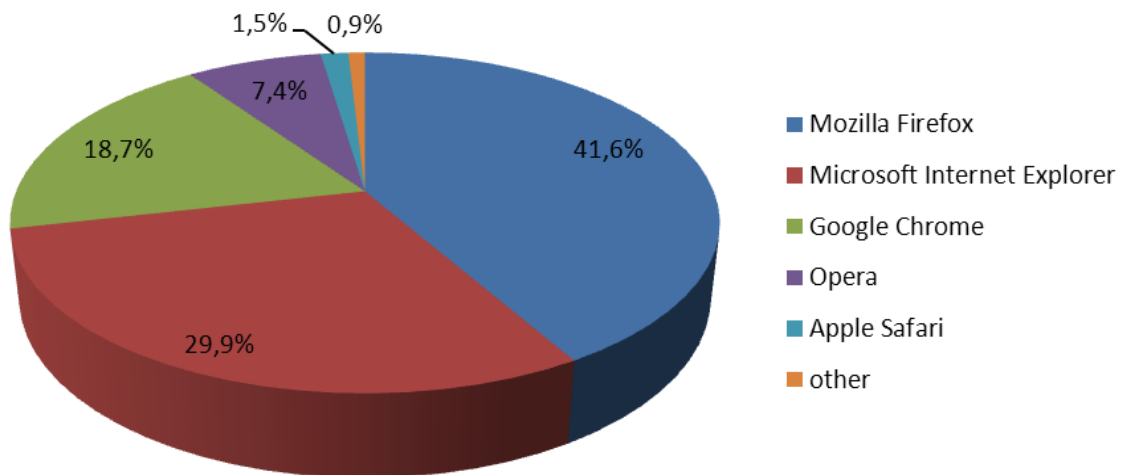
¹ <http://www.statcounter.com>

止，全球大约 48%的用户使用 Windows XP，而只有约 29% 使用 Windows 7。使用 64 位 Windows 7 的用户比 32 位的多，也许是因为大多数用户在 64 位下能使用超过 4 GB 内存的原因。

虽然使用不同的操作系统，但在检测率测试中几乎没有区别，性能表现上肯定是不同的，因为在 2010 年的性能测试中，当我们切换到 Windows 7 时得到了印证。2012 年，我们可能也会考虑将动态测试转换到 Windows 7 系统中执行；目前我们仍在 XP 下执行这项测试，由于我们主要想评价由安全产品提供的保护，而不是由某一特定的操作系统提供的保护（如果所有用户都使用最新和打过补丁的操作系统和安全软件，或许世界上就不会有那么多成功的黑客攻击）。

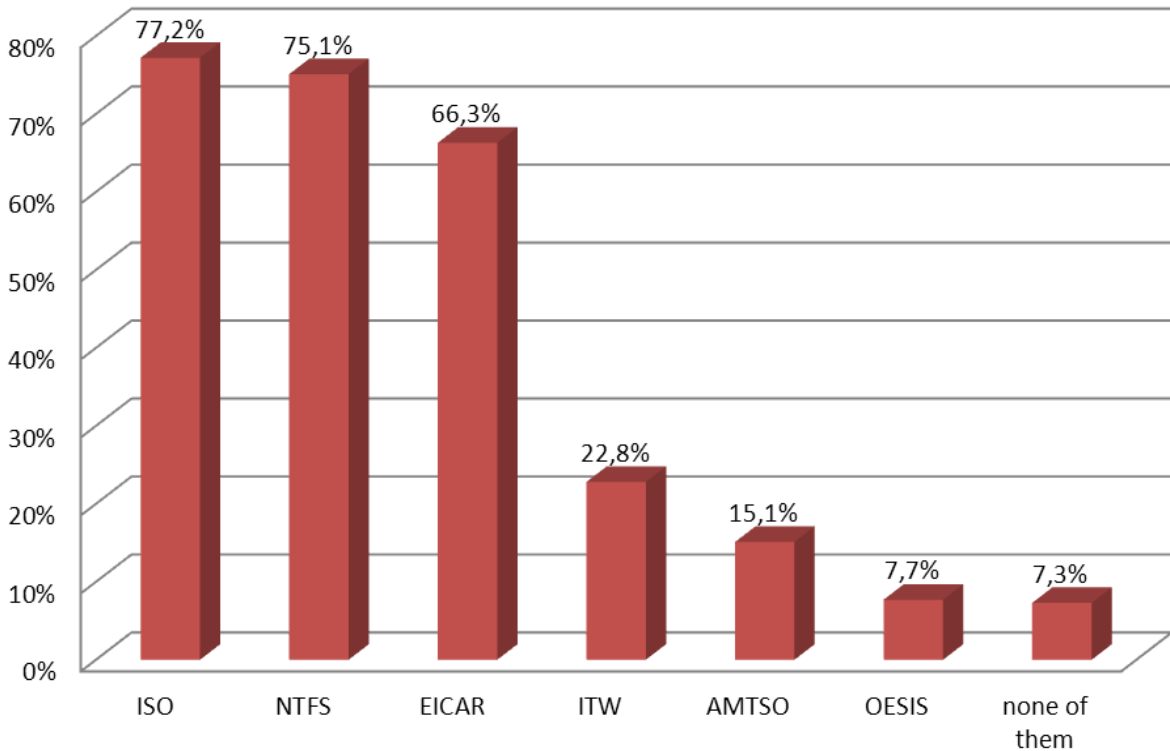
此外，由于我们的测试是为了迎合更多的普通用户，而不仅仅是为了我们网站的读者，所以，操作系统的选择考虑了操作系统使用的全球统计。

3. 您主要使用哪种浏览器？



根据市场研究公司 Global Stats of Statcounter 的统计，当前全世界大约 46%的用户，使用微软的 IE 浏览器，而只有大约 30%的用户使用 Mozilla Firefox（除了欧洲用户较倾向于 Mozilla Firefox 外）。

4. 您熟知哪些缩写?



5. 您目前主要使用哪款防病毒软件?

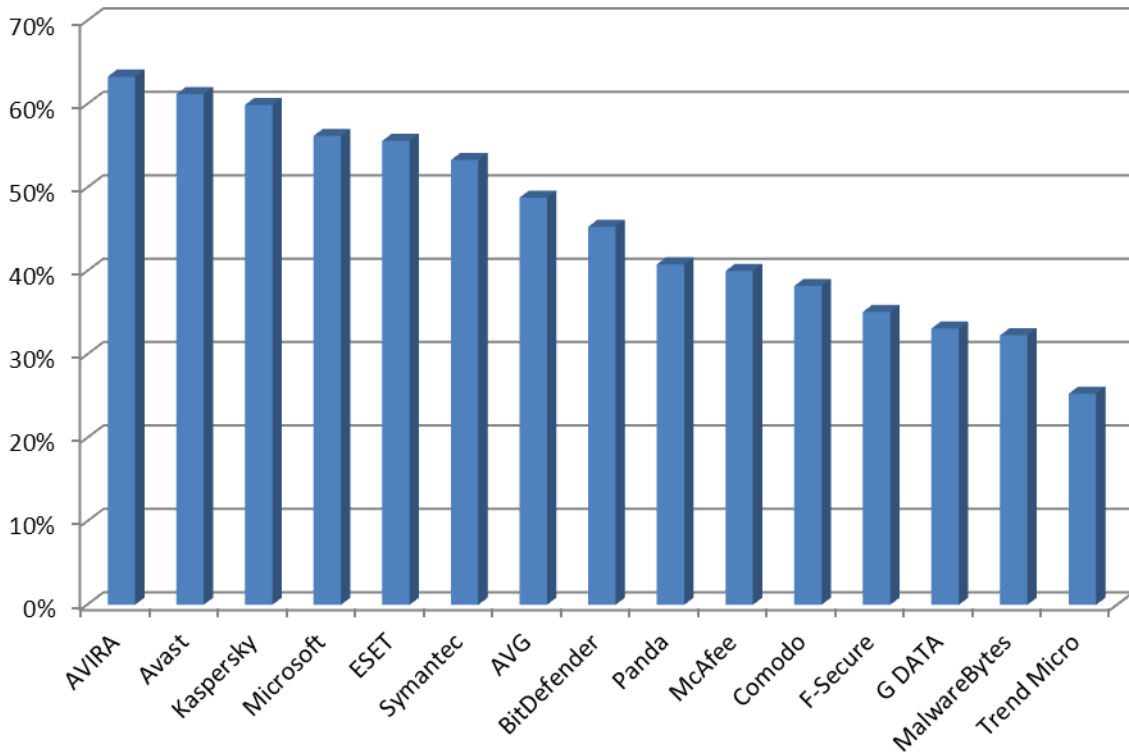
在使用最多的防病毒解决方案中，调查结果显示可用的免费软件版本占据上风，例如 Avast、AVIRA、Microsoft、AVG、Comodo 等等，紧随其后的是一些著名的商用解决方案，如 Symantec、Kaspersky、ESET、McAfee 等。

这个调查结果也使一种假设得到了确认：那就是一半的用户使用免费的防病毒解决方案。同 OPSWAT²的调查结果类似。

² <http://www.oesisok.com/news-resources/reports/worldwide-antivirus-market-share-report%202010>

6. 在我们的测试中，您希望看到哪款安全解决方案？

我们在此仅列出参与调查的用户投票超过 25% 的厂商：



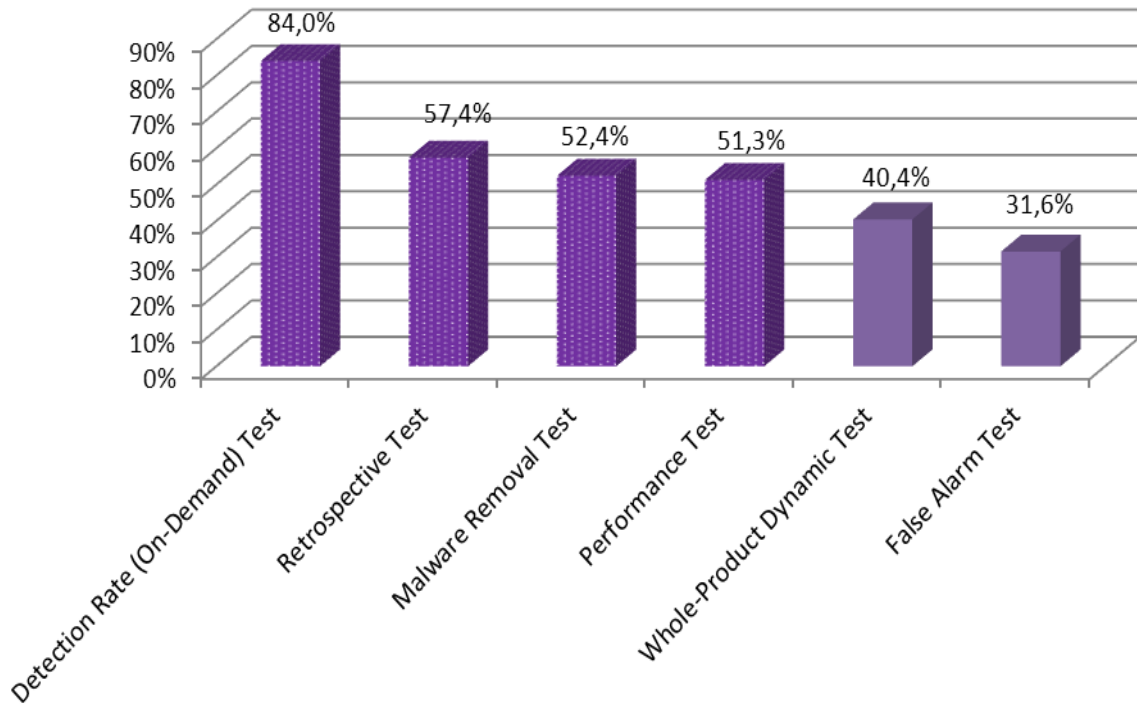
以上是前十五款投票选出的产品（列表共有 70 个著名的厂商）。

首先，MalwareBytes 并未打算成为防病毒产品或安全套装的替代品³，而是宁愿作为一种赠送的工具关注于较小的威胁并将其从已感染的系统中删除。因此，如果将它同我们通常检测的防病毒安全产品对比，势必会出错。

很遗憾，虽然 Comodo 的产品在本项调查中是用户呼声很高的产品，但 Comodo 并没有申请参与我们的 2011 测试系列，他们只同意参与产品单项（按需）测试。

³ <http://www.wilderssecurity.com/showpost.php?p=1826047&postcount=2>

7. 您对哪种测试更感兴趣？



(柱状图文字说明<从左至右>: 检测率(按需)测试; 回溯测试; 恶意软件移除测试; 性能测试; 整体产品动态测试; 误报测试)

根据答复的情况来看(用户必须从 12 种测试中选择 4 种最感兴趣的), 用户似乎对“反垃圾邮件测试”已不再有兴趣。对基于 Wildlist 和“防御可能有害的恶意程序”的测试, 反应似乎也很冷淡。

大多数用户对“按需恶意软件检测”明显关注, 以及对能够反映启发式等技术的“回溯测试”等感兴趣。对“恶意软件清除”以及“性能测试”也有较高期待。去年我们无法及时执行恶意软件移除测试, 但是考虑到如此多的用户关心此项测试, 所以, 今年我们将尽力恢复此项测试。

出乎意料的是, “整体产品动态测试”, 这一旨在模拟现实世界真实使用条件而执行的深层测试, 同时也被防病毒行业认为能反映产品能力的测试, 最后只勉强被用户排在了最希望的测试的第 5 位。我们期待, 随着时间的推移, 用户将会越来越欣赏此项测试。无论如何, 我们明白用户会一如既往的将兴趣停留在那些能够衡量按需检测率的“传统”测试上面。

8. 在您看来，以下测试实验室哪个是 ...

调查参与者需要通过下列三种选择为 22 个测试实验室定级：

- 可靠/可信赖/独立的
- 受厂商左右/不可靠
- 不清楚

根据参与者的调查显示，下列五个测试实验室最可信赖/可靠/独立的：

1. AV-Comparatives
2. VB / AV-Test
3. ICSA 实验室/西海岸实验室

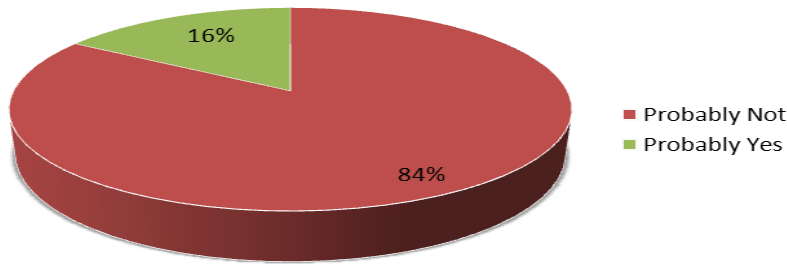
VB 和 AV-Test 被定为同一级，以及另外二个资深实验室 ICSALabs 和 WestCoastLabs（这也是我们将他们并行排列的原因）。AV-Comparatives 获得了极高的肯定而位列最先，但是由于此次调查是由我们所发起，并且调查参与者是我们网站的访问者，所以，这个结果也是在意料之中 - 然而在另外的与我们自己无关的网站的调查中，AV-Comparatives 也被评为最高（十分感谢！）。

本次调查还带来了五个不知名的实验室（以前从未听说过）：

1. TollyGroup
2. ENEX
3. JCSR
4. eKaitse
5. Cyveillance

为保证做到不“损害”某些指定的测试实验室或网站，我们将对在本次调查中，被参与者认为是最不可靠和受厂商左右的这些测试实验室或网站保守秘密。

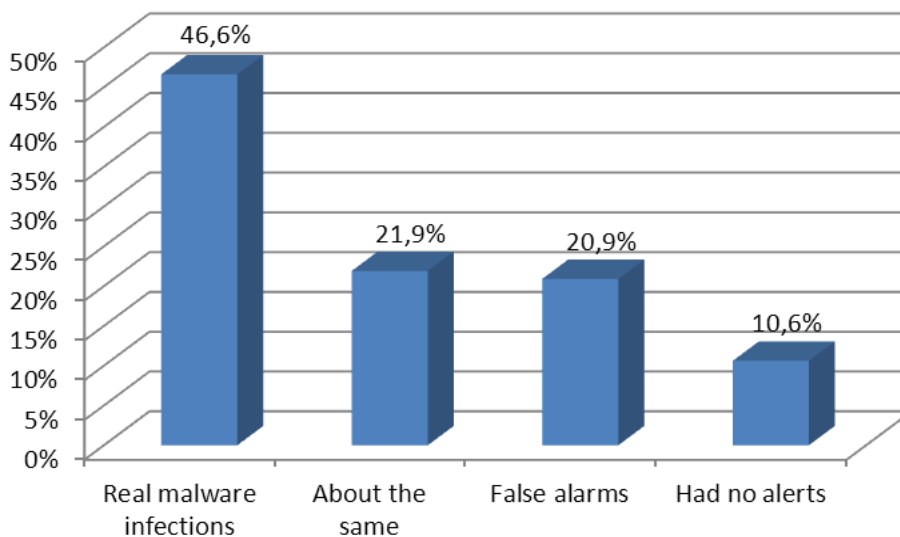
9. 您会使用一款不包括任何手动扫描功能的防病毒安全产品吗？



(饼图文字说明<从上至下按颜色>: 可能不会; 可能会)

提出上述问题的理由是，我们从一些防病毒厂商那里听到一种想法，就是在他们的产品中不想再继续提供手动扫描功能。而在我们看来，一些厂商同用户的需要和愿望脱节，所以我们想从参与调查的用户这里了解一下，他们是否也同我们一样认为移除这样的功能并不可取。

10. 在过去的 12 个月中，在您电脑中发出的任何恶意软件警告，在您看来多半是真的或者是误报？

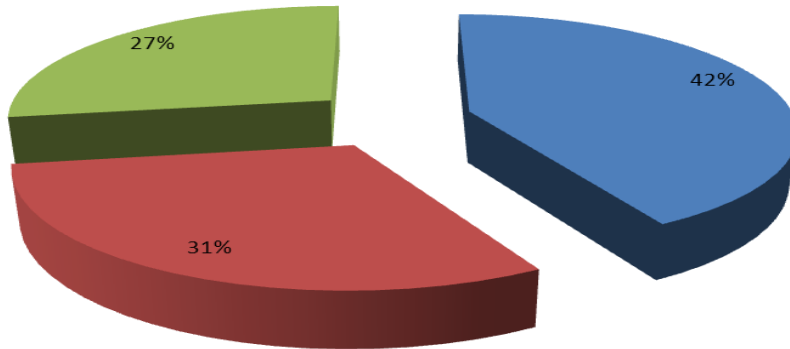


(柱状图文字说明<从左至右>: 真的病毒感染; 真假各半; 误报; 未出现警示)

可喜的是，大部分警报好象都是真的，但是发生的误报事件好象是被一些厂商低估而产生的问题。

11. 如果您的防病毒产品或操作系统问您，是否相信您特意从网上下载的文件时，您通常怎样回答？

- I execute the file and think that my security solution will in worse case protect me anyway.
- I trust the file and I am bothered about the pop-up.
- I do not longer trust the file and delete it.



(饼图文字说明<按颜色>：我仍然执行文件操作，我认为即使在不好的情况下，我的安全软件还会保护我的电脑。我对下载的文件很有信心，我讨厌弹出的窗口提示。我不再相信我下载的文件，然后删除。)

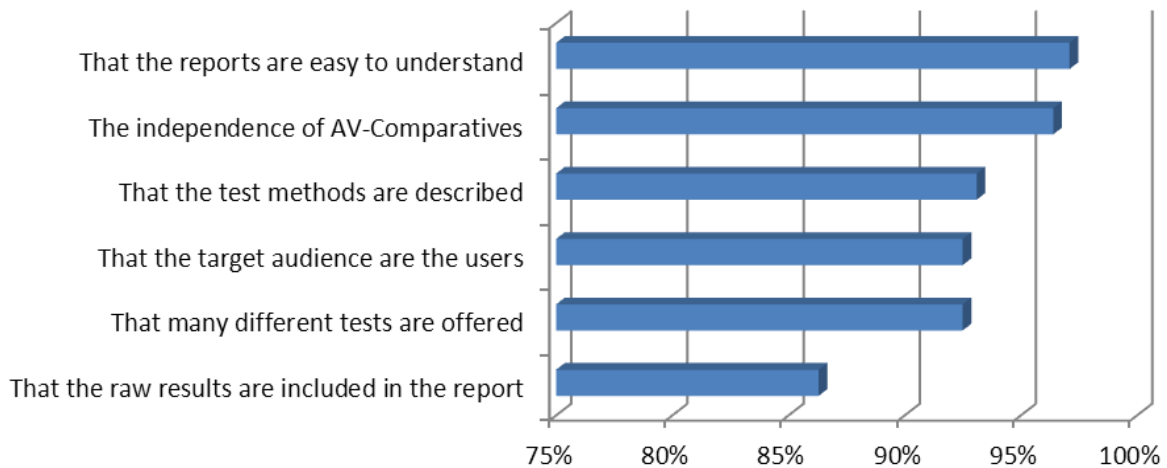
显然，好像不是每个人都能理解（我们承认问题是有些含糊），所以暂时先不去管结果如何。根据我们在客户方面的经验，我们相信，多数日常用户经常对操作系统或安全软件发出的问题和警告采取忽略的态度。

但是，有两种用户常遇到的安全通知应引起注意。Windows 在执行任何从网上下载的程序文件前，通常都要求用户予以确认，而从不根据文件的好坏做出任何假设。例如，运行一款真正的防病毒安装设置文件，通常这是安全文件中最安全的，却仍然带出一个 Windows 7 的 UAC（用户账户控制）提示，要求用户确认文件应该被运行。这完全取决于用户决定文件是好是坏；一直单击“否”可能意味着用户不能安装他/她从网上下载的任何合法软件。第二种类型的安全通知来自安全软件，例如防病毒程序或 Windows Defender（在此被看作是个别的应用程序，而非 Windows 的一部分）。安全程序可能警告说指定的文件可能是危险的，例如在行为或网页信誉的基础上。在此情况下，合理的选项是一直点击“否”来安装，因为合法的应用程序一般不会产生这样的警告。

我们对用户的建议是：如果您看到一个提示，询问您是否安装软件，或警告您小心安装，那么，在点击任何按键前，请暂时停下来想一想。

我们对防病毒安全软件厂商的建议是：请记住！很多普通用户在单击安全提示前，根本不去想那么多；他们期待自己所使用的产品将为他们的操作做出判断，如果危险会（主动）阻止。“狼来了”的故事在这里非常适用：太多的误报和用户干预会导致用户忽略真正的警告，这是人之天性。

12. 从 AV-Comparatives，您发现了哪些重要的信息？

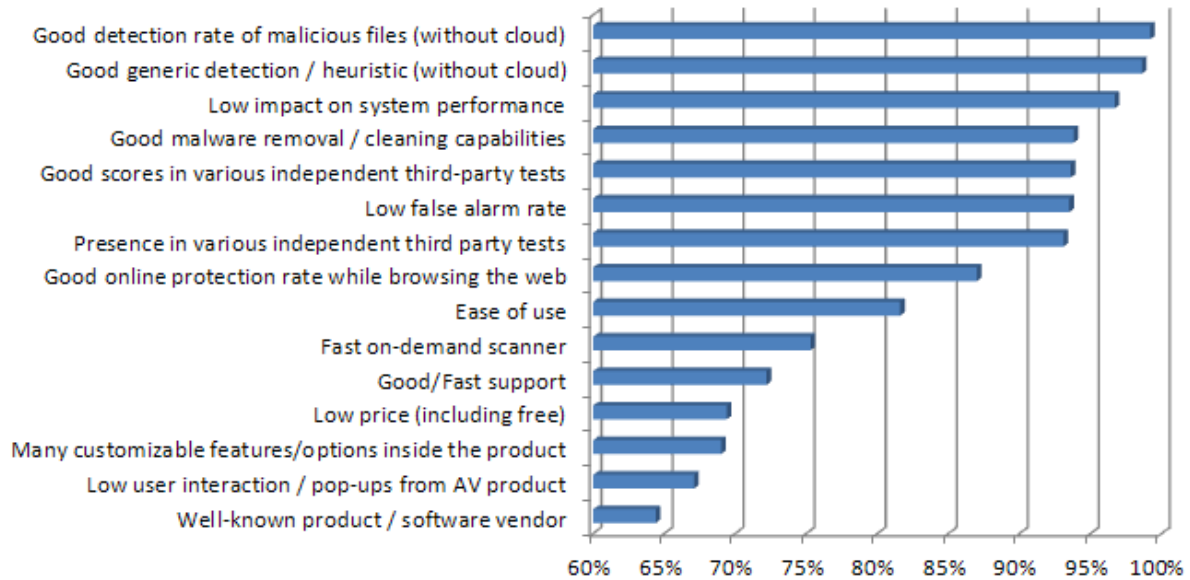


(柱状图文字说明<从上至下>：报告易懂；AV-Comparatives 的独立性；其所使用的测试方法；其读者群针对用户；提供的多种测试；未经修饰的测试结果)

此外，大约一半用户说，让他们感到欣慰的是，当他们想联系我们时，总能找到我们（测试人）。所以，我们已开始计划提供多语种的测试报告。

我们也注意到许多关于 AV-Comparatives 的善意评论，我们将尽力来满足一些用户的愿望。但是一些请求确实不太可能实现（例如还有的用户提出太多令我们难以获得的资源请求；我们毕竟不是 Google? ☺），同时，还有一些请求实际上在我们的网站或报告中已能找到，但是或许没有被用户注意到或读到。

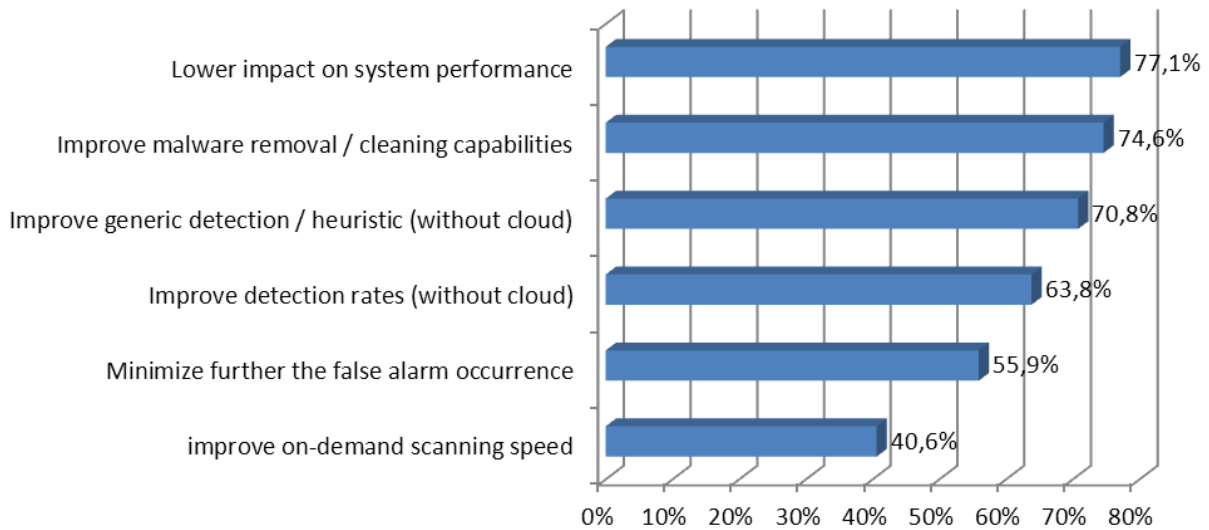
13. 在您看来，防病毒安全产品最重要的是什么？



(柱状图文字说明<从上至下>：良好的恶意文件检测率（无云技术）；良好的常规或启发式检测（无云技术）；系统影响低；良好的恶意软件移除或清理能力；在各种独立的第三方测试中良好的评分；低误报率；目前参与的在独立的第三方测试机构中的测试；浏览网址时良好的在线保护；易用性；快速手动扫描；良好和快速的支持；低价（包括免费版本）；产品中有较多的自定义功能或选项；较少用户干预或弹出提示；著名的产品或软件厂商）

注意：“没有云”意味着“无法依靠云或在线连接。”这已在调查报告中明确写明，因为我们清楚并预料到，多数用户仍然倾向于产品不应仅依赖云技术或在线连接来提供可靠的保护。

14. 就您看来，防病毒产品需要在哪些地方改善？



(柱状图说明<从上至下>：降低对系统性能的影响；提高恶意软件移除和清理能力；改进常规或启发式检测（无云技术）；提高检测率（无云技术）；进一步将误报降到最低；提高按需扫描速度）

用户需要从 6 个方面，就防病毒厂商的产品有待改进的地方进行选择。上图显示产品最需要改进的 6 个方面。这可能是用户认为的防病毒产品所表现的薄弱面。更有一些用户表达了他们的希望（不到 20%）：加强默认配置，商业键盘记录程序检测等等（无法检测是不信任防病毒产品的一个理由），不要过多依赖云技术/在线连接、更低的价格和更好的客户支持等等。

版权及免责声明

本报告的版权©2011 归 AV-Comparatives®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。

更多关于 AV - Comparatives 及测试方法，请访问我们的网站。

AV-Comparatives e.V. (2011 年 3 月)