

全方位思考选择适合您的反恶意软件 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/460/2021_2022__E5_85_A8_E6_96_B9_E4_BD_8D_E6_c100_460810.htm 如今正确选择的反恶意软件产品时，用户可能会感觉到更多的困惑。要想有效的对付恶意软件，你不得不在浩瀚的产品中苦苦寻找。杀毒软件产品、反间谍软件、IDS（入侵检测系统）以及其它一些发现并阻止恶意代码的产品等，各式各样摆字用户面前，该如何去选择呢？其实用户只需在选择产品时考虑如下几个问题，或许您会有正确的选择。到底需要什么样的反恶意软件产品？病毒、木马、蠕虫、恶意邮件以及间谍软件是几种主要的恶意软件范畴，你需要的产品必须要可以侦查和阻止这些威胁。一些产品将几种工具捆绑到一起，从而帮助企业有效的管理和对付恶意软件。怎样知道一种产品与其它形式的反恶意软件程序不发生冲突？因为你可能会选择多种安全产品，你肯定希望这些产品之间互相有良好的偕同工作。在购买产品之前，需要向厂商咨询可能存在的冲突名录。

Windows内置的反恶意软件产品能够提供有效的保护吗？

Windows XP及更早版本不能提供有效的保护。Windows Vista的防御者反间谍软件技术和其内置安全技术确实提高了操作系统的安全性能，但是不可能满足所有顾客对于安全的高要求。使用黑白名单机制有效吗？与使用黑名单机制阻止恶意程序的方法类似，白名单反恶意软件技术的工作原理就是只允许事先认可的应用程序的运行。许多企业认为使用这一机制就可以保证系统的安全，然而由于很多产品自身的缺陷仍然会被攻击者所利用。行为检测工具有效吗？一些反恶意软

件产品的行为阻断监控功能可以有效的防止执行含有恶意代码的软件的执行。一旦可疑的代码被发现，程序的运行就会被阻断。行为检测技术比起单纯的依靠病毒库识别的安全技术来说，智能化和复杂程度更高。这一技术在对付0-day攻击恶意程序时效果显著。智能分析管理技术可以有效的对付恶意软件的攻击吗？有些安全厂商使用了这一技术，Prevx公司在这方面尤为出色。这一技术就是使用多台电脑同时工作增强搜集病毒的能力，从而更好的对付病毒。每一台电脑都将程序，不管是恶意的还是未知的，统统发送到中央服务器进行自动分析。需要在网络层或是用户层面对付恶意软件吗？都需要。只要这一技术没有增加网络带宽消耗，降低设备的性能或是用户的工作效率的情况下。需要访问控制程序吗？访问控制程序会在用户准备运行未知程序的时候对其提出警告，这样就可以在早期对恶意软件感染做出预警。这一能力使得访问控制程序在对付恶意软件的时候相当有效。需要杀毒软件吗？随着越来越多的对付恶意软件的工具和技术在市面上的涌现，一些观察家宣称传统的杀毒软件将会被淘汰。显然这一说法夸大其词，实际上杀毒软件还是有效的。如果仅仅将其当作是一个二线的防御技术，杀毒软件的性价比还是很有竞争力的。最有效的防止反恶意软件误杀正常的IT程序的办法是什么？使用反恶意软件组合策略来提供安全覆盖。安装和使用防火墙。实时更新你的软件的补丁。培训员工和系统使用人员关于安全正确使用计算机的知识。相信做到以上几点，将会给您的企业计算机使用安全带来很大的帮助。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com