Windows7防毒理念之“ 纵深防御 ”Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Windows7_E9_98_c100_644260.htm Microsoft说Windows 7是有史以来最安全的Windows，但防毒厂商加以反驳，各说各话到底哪个才是真相？其实，真相未必存在，新闻有时只有 ”角度 ”问题 …… SophosLabs上周表示，他们在一台裸机上安装了Windows 7，并根据使用者帐号控制（UAC）的系统预设进行配置，但未安装杀毒软件，然后汇入10个病毒样本，发现有8个病毒能够攻击Windows 7的漏洞。 SophosLabs安全顾问Chester Wisniewski表示，UAC的确拦截了其中一个病毒样本，不论如何，如同他先前提出的警告，Windows 7的UAC预设配置无法保护个人电脑不受病毒威胁，Windows 7并没有微软宣称的那么安全。Wisniewski认为，Windows 7跟以前的操作系统一样令人失望。可是真的如此吗？ 是的，坏事是会发生的 首先，只要是 ”执行 ”都有危险，因此执行程序时一定要小心。虽然Microsoft的安全总监说： ”如果使用者在电脑上执行未知的程序，坏事就会发生。 ”但是这有个两难：我们买电脑就是要来执行程序的，就是要下载这个下载那个，就是要玩各种已知未知的各种有趣的东西，就是不想受限制不想被约制……若只要是未知的程序我们就不跑，那使用电脑还有什么乐趣？ 我的看法是：使用者可以 ”尽力 ”做些事情来改善这问题，像是 ”来路不明的程序不要乱跑它 ”， ”公司的电脑请按规定使用 ”， ”电脑都得装上杀毒软件 ”，多一分努力就多一分保障，就这样。目前的电脑世界就像是热带雨林，里面可是充满了毒蛇、箭蛙和食人鱼——与其抱

怨，不如自救。 Microsoft安全总监认为，用一台电脑硬是去执行病毒，然后说Windows 7不安全——这未免太武断了。关于这点，我得说，我真的见过使用者不分青红皂白的乱按、乱执行一通，管你有毒没毒有用没用，先点两下再说。所以，Shophos公司的这种测试——虽然简陋，稍嫌武断——但不是没有可能。但是，Microsoft安全总监也同意，Windows本来就需要杀毒软件，连Microsoft自己也提供了一个免费的给合解决方案供用户使用。 所以，不管他们吵什么，总之各位记得这结论就对了：跑Windows一定得装杀毒软件——不管它是不是更安全的Windows。不过，这也没什么好失望的，人生就是这样罗。 Windows 7的 ” 纵深防御 ” Microsoft安全总监提到了一个有趣的概念：纵深防御（defense-in-depth）理念，这是啥？ 这就是所谓的 ” 围城防御原理 ” 。你得从里到外，每个环节都加强防御，才能更有效的抵抗外敌。 要让国土能够保持安全，你得建立城墙、城池，城池外面再建立岗哨，派出巡逻队员，如果可能，最好有民众在城外屯垦、生活，倘若如此，就算有外敌入侵（外敌入侵是无法避免的），你的防线也不会一下就被攻破。Shophos公司认为Windows 7没有更安全，在我看来就像是 ” Windows 7还是有可能被病毒攻破 ” ，但这其实是合理的结论（哪一座城池是永远安全，永远不会被攻破？）。 而Microsoft公司的安全总监则说明，Windows 7被病毒攻破 ” 本来 ” 就是有可能的，所以Windows 7本来就需要杀毒软件。但是Windows 7确实在Windows的每一个环节都做了强化，设法让Windows 7 ” 不那么容易被攻破 ” 。他举了一些环节： ● UAC功能 ● Windows核心保护能力 ● 视窗服务（Windows Services）的强

化 ● 随机位址空间编排（ASLR） ● 资料执行防护（DEP）
这些东西很简单，就是 ” 由内而外设法让Windows更稳固 ” ，这就是 ” 纵深防御 ” 。Microsoft的安全总监要表达的是：有人说 Windows天下无敌吗？没有吧！所以Windows需要杀毒软件可说是天公地道啊！要是不装杀毒软件才恐怖吧！所以，就算是Microsoft，也提供杀毒软件给客户用啊！ 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