终端安全管理：守住网络安全最后的堡垒 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E7_BB_88_E7_AB_AF_E5_AE_89_E5_c101_142575.htm 互联网的迅猛发展，使信息时代的重要信息载体电脑，面临着越来越恶劣的应用环境，蠕虫、木马、冲击波等病毒层出不穷，时刻威胁着电脑安全，使得电脑出现运行缓慢、应用程序出错、系统崩溃等现象。而对于那些大量应用电脑的企业来说，电脑数量多、故障发生概率高也是一件棘手的事情，这些来自外部和内部的不利因素都成为了企业PC管理与维护需要面对的一大问题。如何确保PC拥有一个高效安全的运行环境、实施低成本的PC管理，已经成为企业亟待解决的重要课题。 近年来，随着信息安全建设的不断深入和安全形势的不断发展，终端安全问题开始凸现。传统的以组织边界和核心资产为保护对象的安全体系逐渐显示出严重的缺陷，无法有效应对终端安全管理中面临的诸多问题。这样终端安全体系建设问题就逐渐提到组织管理者和网络安全建设者的议事日程上来。虽然终端资产的重要性级别通常低于网络中的交换机、路由器等核心网络设备以及各种业务主机和服务器，但广大终端数量众多，并且是组织的日常办公和业务运行的载体，如果终端安全受到威胁，即使网络中的核心设备安然无恙，整个网络的业务运行也会受到严重影响甚至瘫痪，如同家庭是社会的细胞，终端也是组成网络的基本单元，他们的安全与否对网络自身的健康运行有着深远的影响。建设一个有效的终端安全管理体系，不仅能够保障终端安全，而且能够提升网络整体的安全防御能力。 终端:安全的起点和终点 终端安全管理

是一个复杂的问题，通常一个组织中的终端地理位置分散，用户水平参差不齐，承载业务不同，安全需求各异，这就决定了终端安全建设的复杂性和多元性，要根据终端用户的接入位置、所属部门、业务需要等条件来选择和执行适当的安全管理措施，既不能搞一刀切，也不能对用户放任自流，缺乏控管。 现在终端安全出现严重问题，包括:安全保护问题、系统管理问题和行为监控问题。 其中安全保护问题包括:病毒蠕虫大规模泛滥以及新的蠕虫不断出现给用户带来损失.来自内部和外部的入侵和攻击的问题.网络边界扩展带来的对于移动办公用户、第三方接入安全防范不足从而引入安全风险的问题。而系统管理问题则主要表现在对微软等操作系统不断出现漏洞的补丁措施的及时管理，以及网络中终端设备资产信息变化的精确统计管理问题。至于行为监控，则是企业主对于员工的安全监控预防和工作情况统计的措施。 如何应对当前终端安全面临的诸多困扰?显然局部的、简单的、被动的防护不足以解决问题，要想解决终端安全问题，一个好的思路是建设可信终端安全保障平台，全面管理终端安全。安全保障平台由资产管理中心、补丁管理中心、文件分发中心、安全策略中心、强制认证中心、行为监控中心、病毒防护中心、安全保护中心等模块组成，并且能够同其他保护网络边界和网络基础设施的网络安全产品和技术结合起来，共同组成信息安全保障体系，提升组织的信息安全保障能力，对抗来自内部和外部的威胁。 以下将以四大平台应用为例，看看终端安全未来全副武装的“ 面目 ”。 “ 疫苗 ”:单机恢复最高级安全 对于电信行业工作的小王来说，工作与电脑联系紧密，频受病毒木马之苦的他，最近有了一丝安全感。这是因为

单位最近为员工安装了个人电脑恢复解决系统。而该系统的特点就是，在遭遇病毒攻击或其他灾难，或者当操作系统崩溃时，及时有效地恢复和修理系统、设置和修复程序至已知的良好状况，且无需网管人员介入。 跟小王一样，信息社会中近60%的人将工作或者关键业务信息，保存在终端或客户机器上。正因为如此，保障业务连续性并提供持续服务仍然依赖于个人电脑的可用性。在当今的联网企业环境中，任何客户端PC都会受到攻击，如果得不到适当保护和管理，个人信息、企业知识产权和其它关键业务信息都可能遭受攻击。小王在应用Recover Pro个人电脑恢复软件后，对于非IT人员的小王来说的确简单多了。可以随时进行前一个阶段的修复，即使在Windows操作系统出现故障时，回复系统也仍能运行。它的预引导环境和受保护备份功能可以通过三个简单步骤来恢复系统，而无需备份光盘。 专业的安全机构凤凰科技副总裁Kort van Bronkhorst先生认为，安全和方便往往是一对矛盾，而尤其针对大多数非IT人员使用的安全设备，方便和直接简单应用，将是其真正意义所在。 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