



单位：北京大学

领域：

高等教育

信息中心负责人： 钱杰

网络现状

10000 点 windows2000\2003\XP\VISTA\2008

北大简介

北京大学创办于 1898 年，初名京师大学堂，是中国第一所国立综合性大学，也是当时中国最高教育行政机关。辛亥革命后，于 1912 年改为现名。

北京大学是一所以文理基础教学和研究为主的综合性大学，为国家培养了大批人才。据不完全统计，北京大学的校友和教师有 400 多位两院院士，中国人文社科界有影响的人士相当多也出自北京大学。改革开放以来，北京大学进入了一个前所未有的大发展、大建设的新时期，并成为国家“211 工程”重点建设的两所大学之一。

项目背景

北京大学校园网过去三年里使用的是赛门铁克防病毒软件企业版，由于服务即将到期，面临新一轮的选择，而且根据以往的经验 and 用户的反馈，我们打算在预算许可的条件下，至少购买两种防病毒软件供用户选择，所以对卡巴斯基软件和 NOD32 防病毒软件进行了试用，取得一些经验性的粗浅认识。

产品选型

1、Symantec 企业版

北京大学先后部署过 Symantec 企业版 8.0、9.0 和 10.1 版本，并在办公区取得了较好的效果，但在学生区使用的效果却并不理想，主要是办公区的用户行为较为单一，可以进行规范的管理，系统漏洞少，网络环境相对干净很多，但学生宿舍区则不同，网络应用复杂，用户行为不确定，难于规范管理，而且使用盗版软件的用户多，安全威胁隐患

非常高，是病毒大规模发作的重灾区。

Symantec 企业版是以防御为主，具备误判率低，稳定性好，系统资源占用较少，运行安静，简单易用等优点，优势体现在病毒样本库比较全面，引擎速度仍然够快，是传统特征码扫描技术的代表，缺点是病毒库的更新速度赶不上病毒变种的速度，主动防御能力差，启发式侦测能力弱决定了其对未知病毒、蠕虫、木马等威胁防御能力一般。

2、卡巴斯基网络版

虽然是网络版本，但客户端与单机个人版似乎没有本质区别，仍需要在每台系统上激活 KEY，对学校这种松散的管理模式，给部署带来极大的不方便，甚至防止 KEY 流失需要作为一项重要的任务来做。

卡巴斯基 6.0 具有主动防御功能，可对进程和注册表修改行为进行监控，但需用户共同参与完成，这就需要用户具备相当的安全基础知识。

卡巴斯基采用虚拟机技术来对变种或加密病毒进行脱壳，并拥有庞大的病毒库，但并没有给引擎带来太大的负担，其对已知或变种病毒优秀的防护和杀毒能力，得到了众多用户的认可，知名度很高。而且卡巴斯基对中国较为重视，对一些具有地域性的间谍程序或恶意脚本防护能力要强一些。

卡巴斯基启发式侦测能力也较弱，对暂时没有特征码的未知病毒、木马等威胁的事先预防能力一般，甚至会出现一些误报行为。普遍反映卡巴斯基的一些缺点是系统资源消耗较大，系统反应稍有迟滞。校园里用户主要是以动手能力强的学生为主。

3、ESET NOD32 防病毒软件企业版



ESET NOD32 是近几年来迅速崛起的防病毒软件，它注重病毒的早期侦测和防护，对安全威胁的判断不完全依赖于特征码，其启发式引擎采用了精简基因码，先进的虚拟机和代码分析等技术，对未知安全威胁进行主动侦测，不仅识别未知威胁的**准确率高**，而且**误报率又低**。具有病毒库规模小，**软件体积小**，**系统资源占用少**，**速度快、运行安静**，**简单易用**等特点，几乎**适合所有的用户使用**，而且鉴于其出色的性能，拥有许多爱好者。ESET NOD32 企业版具有**部署简单灵活**的特点，**很适合校园网松散管理模式的大规模部署**。

最终，北京大学信息中心选择了 ESET NOD32 防病毒软件企业版作为校园网安全的守护者。



单位:

南开大学

领域:

高等教育

信息中心主任:

张四海

网络现状:

5000 点 Windows 2000 , 2003, XP

安全隐患:

电子邮件, 网页服务, 网络行为, 连接到不可靠来源设备, 用户使用未经授权的软件。

用户需求:

防病毒的效率高; 对网络的影响小; 性价比合理

技术要求:

反病毒解决方案科学合理; 痕迹轻, 不降低系统性能; 自动升级; 集中管理简单易行; 对混合病毒威胁具有前瞻性的零小时保护(减少对签名升级的依赖); 安装和卸载简单易行

解决方案:

08 年 2 月在该大学举行的防病毒软件招标会上, ESET NOD32 防病毒软件一举夺魁。

地址:

天津市南开区

网址:

<http://60.28.145.113/>

大而生险

南开大学是一所历史悠久、享誉海内外的国内一流重点大学。她是敬爱的周恩来总理的母校。

目前她的在校生人数近 22000 人。南开大学

高等教育的信息中心管理着一个包括台式电脑和用户支持, 培训, 网页服务, 电子邮件, 文件存储, 打印, 应用布置与管理等等的庞大的异构 IT 环境。随着网络技术的进步, 网络环境变得日益复杂, 各种威胁越来越隐蔽, 造成的后果越来越严重。

台式电脑加上手提电脑, 再加上用户群体的多样性, 可谓大门洞开, IT 安全受到的威胁俯拾皆是。

大而行难

由于防病毒保护具有其特殊性, 在这方面的投资回报哪怕你想说出一个具体的数字都是一件非常困难的事, 因为在没有发生安全问题之前, 你就无法计算到安全工作给你挽回了多少损失。但有一点却不容置疑: 对于象南开大学这样支持着 22,000 名学生的信息传递和教学的系统来说, 无论任何威胁, 一旦将其系统瘫痪, 其代价都是高昂的。正是考虑到这一点, 南开大学一直在使用所能接触到的最好的防病毒软件。但是在使用的过程中, 总是出现一些令人意想不到的问题。首先是防病毒软件的性能不佳, 最主要的问题是它的滞后性, 总是做事后诸葛亮; 其次是随着病毒库的升级, 在网络资源上造成很大的负荷; 防不胜防的误杀是最令人头疼事; 将防病毒软件打包到一个大的软件包, 令它变成了一个大工具箱, 其中有很多是高校所不需要的, 也由此造成价格的不合理。基于以上考虑, 又值所用软件的使用权限已到, 于是该校信息中心趁此机会举办了一个招标会, 看一下市场上其它企业级的防病毒软件的情况, 然后综合比较选择目前业界最好的软件来使用。

机缘巧合

正值此时, ESET 公司的旗舰产品、国际著名的 ESET NOD32 防病毒软件登陆中国大陆, 使得国内广大用户有机会一睹业界领头羊的风采。凭借着卓越的性能和合理的价格, 在短短的一年多时间里, 取得了骄人的战绩。在南开大学举行的招标会上, ESET NOD32 防病毒软件傲视群雄, 一举夺魁。这里边包含了南开人对 ESET NOD32 防病毒软件的信任, 也是 ESET NOD32 防病毒软件实力的见证。



称砵虽小，可压千金

ESET NOD32 防病毒软件设计上与其它防病毒的软件最大的不同在于它是“引擎+病毒库”技术，在其在其心脏部位的是叫做“ThreatSense”的“零小时”及“探索式”核心技术。该项技术带有一个形成文件的跟踪记录，对于出现病毒警报和发行传统的病毒签名更新之间的关键时期出现的新病毒威胁，其预先侦测到的比例非常之高，大约 80% 的病毒都是由该引擎来拦截的。因此它的容量就比较小。而其它传统防病毒软件依靠病毒库升级来防病毒，随着病毒库文件的增多，导致它们的容量越来越大，而且这种被动式防毒，对新病毒没有任何防范。

轻若蝴蝶，迅捷如风

由于其它防病毒软件容量都太大了，以至于完成一次扫描太耗时，同时它们所占用的系统资源给用户的 IT 系统带来沉重的负担，导致用户经常会遇到系统性能下降的烦恼。令人庆幸的是，IT 用户们现在终于有了克敌制胜的杀手锏，它痕迹轻，占用资源少，扫描速度却远远领先于竞争对手，让你在不知不觉中就能完成对系统的监测。另一个关键的成功因素是 ESET NOD32 防病毒软件能够适应带宽资源紧张的环境，主要是由于其安装容量特别小，只占有 8 MB 及 50 KB 的文件更新容量。由于南开大学拥有不少远程用户，其中许多人使用拨号上网进入到南开大学的系统，所以在一个带宽资源有限的环境中可以对防病毒软件升级进行控制是非常重要的。传统软件的大容量的更新一直是个死穴。文件容量带宽上的负荷阻塞而导致更新过程不容易完成，增加用户更新的次数，使用户不情愿对软件进行更新，从而导致系统的漏洞。

安装方便，管理轻松

安装是另外一项重要考虑。如果一个系统加载了很多东西，这样的安装及配置肯定会出现问题。加载高的系统有时可以让电脑上的其它应用程序停止工作，另一个死穴就是在一大套软件中的单个软件有时会运行不正常。对于象南开大学这样一个有着庞大客户终端的网络系统而言，如果没有一个集中的配置和对其进行随时管理，要保护其系统的运行肯定要付出巨大的成本。但如果要南开大学的信息中心对其用户进行逐一进行指导，一则工作量太大，二则往往需要个人用户一些很个性的动作来配

合完成系统安装，IT 部门肯定承受不起。因此，配置只能是以终端用户完全看不见的方式进行。而

且，还要考虑软件的卸载问题。试想如果软件不能以一种企业级的方式来卸载，而需要逐台电脑手动卸载，这是个多大的麻烦。ESET NOD32 防病毒软件企业版使用应用配置工具，可以在很短的时间内完成大量用户的安装。为了方便管理，ESET NOD32 防病毒软件企业版为大型用户提供了一套压缩的管理和报告工具。它有一个中央镜像服务器，它可以令部份的系统管理自动化，比如说安装，它可以将所有客户预配置的设置进行复制，并管理 ESET NOD32 防病毒软件的更新升级。只要在信息中心设有一台中央控制台，通过中央控制台可以清楚地看到整个企业级客户的升级和侦测到病毒的情况。

支持教育，花开南开，香满中华

为了支持中国的教育事业，ESET 公司在 ESET NOD32 产品价格上做了很大的优惠，体现了 ESET 公司对教育事业的一份真情。落户南开大学开创了 ESET 公司和中国高校合作的新典范，相信这朵外来的奇葩一定能在南开大学生根开花，香满中华大地。





单位：西安体育学院

项目情况：3120 点

ESET NOD32 安全套装企业版

学院概况：

西安体育学院创建于 1954 年，坐落在古城西安小雁塔西侧，是新中国最早建立的六所体育院校之一。2001 年实行中央与地方共建，以地方管理为主，现为国家体育总局与陕西省共建院校。

建院初期，贺龙元帅亲自为学院圈选新校址并鼓励师生继承和发扬延安精神，艰苦创业，由此学院确立了“笃学重教、造就人才、服务体育、福佑人民”的办学宗旨。之后，国家体育总局历任主要领导人荣高棠、李梦华、伍绍祖、袁伟民、刘鹏等先后莅临学院指导工作，关怀和支持学院的建设与发展。经过几代西体人不懈努力和历史积淀，形成了“诚厚俭朴、勤奋刻苦、团结拼搏、求实创新、爱国荣校”的办学传统与特色，为国家培养造就了 3 万多名高素质体育人才。

网络现状：

3120 工作点 Windows 2000 , 2003, XP, Vista.
LINUX

安全隐患：

电子邮件，网页服务，网络行为，连接到不可靠来源设备，用户使用未经授权的软件。

用户需求：

进行文件扫描时，占用资源小，扫描速度快，不影响正常办公
防病毒的效率高；对网络的影响小；防御 ARP；性价比合理

学生机器数量大、分布广，因此要求安装部署简单方便；学生的好奇心及求知欲一般都很强烈，且校园一直是 IT 技术应用的前沿，比较容易发生病毒爆发及其他网络安全事件，需要防病毒厂商具有强大的应急处理能力及售后服务保障。

解决方案：

管理

将管理中心及控制台部署在服务器区域，管理员将通过其管理整个网络的防毒节点

西安体育学院病毒防护系统的组成：

根据西安体育学院的网络结构和对病毒来源的分析，西安体育学院病毒防护系统由以下几部分组成：

- 1、服务器和邮件病毒防护：对各种服务器进行病毒扫描和清除，集中报警；对 OA、数据分析系统、DHCP 服务器、DC 服务器、文件服务器、VOD 服务器和数据库（Oracle 和 MS SQL）进行病毒扫描和清除。
- 2、桌面病毒防护：针对各种桌面操作系统，进行病毒扫描和清除；
- 3、防病毒管理系统：在校园内部安装、建立防病毒软件管理系统，对所有客户端防病毒软件进行统一管理。

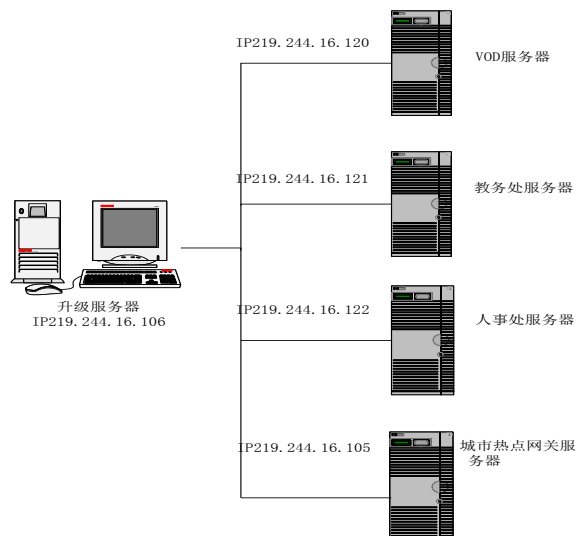
防病毒部署：

防病毒系统的部署按照网络节点的管理模式分为 2 级，核心节点网络→分支节点网络。两级模式包含升级、配置和管理工作的三个层次。病毒管理体系分为 2 个层次，核心节点网络→分支节点网络。核心节点网络和分支节点网络建立完整的管理平



台, 包含 NOD32 管理控制工具、升级服务器 (通过 WEB)。管理系统 NOD32 管理控制工具在核心节点网络和分支节点网络部署。核心节点网络负责建立核心节点网络的防病毒系统; 接收各分支节点网络的防病毒报告; 负责建立全校园的主升级服务器。对分支节点网络的管理服务器进行监控。各分支节点网络的 NOD32 管理控制工具负责管理直属于分支节点网络的联网 PC 和服务器。地市节点网络的病毒库更新、升级服务器与核心节点网络的病毒库更新、升级服务器作镜像。所有未联网的 PC 需使用光盘进行初始安装。病毒库更新由核心节点网络→分支节点网络进行同步。非主流操作系统 win3. x, DOS, OS/2, Netware, Unix 不纳入 NOD32 管理控制工具管理系统。小型办公室的 PC 作为单机处理。单机可设置为从最近的升级服务器 (WEB) 下载更新病毒库。

安装部署图:



服务器版 NOD32 防病毒将升级服务器设置在, IP 为 219.244.16.106 机器上, 通过此机器与互联网连接升级病毒库及模块. 其它服务器分别通过升级服务

器 (IP219.244.16.106) 更新病毒库和模块及时查杀各种病毒及危险程序, 防止病毒通过各种途径对服务器破坏.

收益

1. 大幅提升网络系统的安全性、稳定性

校园网通过 ESET NOD32 网络版病毒防护系统的建立, 西安体育学院校园网防毒的统一管理, 网络中存在得病毒威胁得以及时补救, 从而有效的遏制了病毒在校园网络中的传播, 使网络的安全性和稳定性得到了前所未有的提升。

2. 高效的管理、成本降低、创造价值

原先需要耗费大量人力、物力的病毒防护涉及的各项工, 现在只需通过 ESET NOD32 网络版的控制台发出策略指令和操作就可以实现。同时, 网络管理人员能够及时全面地掌握网络系统的相关信息, 为快速高效地应对病毒爆发提供了前提。安装之后, 校园全网都得到了很好的防护, 没有出现过因病毒大规模爆发而引起的网络故障。ESET NOD32 网络版出色的”轻/快/准狠”性能给学校留下了深刻的印象, 周到的服务也得到了校方一致好评。

校园网下载地址:

<http://www.xaipe.edu.cn/xwfb/nod32/index.html>



单位：广东技术师范学院天河学院

项目情况：2000 点

ESET NOD32 防病毒企业版

学校概况：

广东技术师范学院原名广东民族学院，是我省深具影响力的大学之一。广东技术师范学院天河学院是一所以工科办学为特色，着重强化动手能力培养、英语口语训练为优势的全日制普通高等院校，设有电气工程系、机电工程系、计算机系、建筑工程系、管理系、财经系、外语系、艺术系等 8 个教学系和基础课教学部，现有全日制在校学生近 10000 人，其中本科生近 2300 人。学院目前拥有专任教师 400 多名，其中教授、副教授以上职称 165 人，占专任教师的 36.9%；博士、硕士研究生 148 人，占专任教师的 35.5%；外籍教师 20 人；“双师型”教师占 40%。学院藏书丰富，各项配套设施完善，学术氛围浓厚，管理上实行专家办学，教授治校，民主管理。历年来，办学成绩突出，深受社会各界好评。

网络现状：

2000 工作点 Windows 2000 ， 2003, XP, Vista

安全隐患：

电子邮件，网页服务，游戏，下载，移动磁盘。

用户需求：

进行文件扫描时，占用资源小，扫描速度快。

很强的病毒查杀能力；性价比合理。

拥有强大的集中管理功能，集中更新。

用户安装简便，使用简单，自动杀毒。

解决方案：

将管理中心及控制台部署在学校网络中心管理员机器上，管理员将通过其管理整个学校网络的防毒节点。所有的客户端从管理员机器升级病毒库。

1. 集中控制

反病毒的关键在于防范，因此优秀的企业级杀毒软件必须具备集中管理的特性，从而才能对整个网络实施有效的反病毒策略。

在广东技术师范学院的远程管理员的机器上，区中心的管理员和县城管理员的机器上，安装 ESET NOD32 远程管理套件，统一管理本地所有客户端，控制客户端升级病毒库，定时查杀病毒等。

ESET NOD32 远程管理套件具有灵活高效的管理方式，客户端所有的配置项，都可以通过远程管理套件统一管理，分发的任务可以很快实施到客户端，实时生效。

2. 统一升级

广东技术师范学院部的所有工作站 PC，都通过管理员的机器升级病毒库，自动升级，无需人工操作。管理员的机器从外网更新病毒库。

ESET NOD32 会每小时定时检查是否有可用的更新，若有更新，会立即自动下载。客户端也会随之从网络管理员的机器上自动更新。

3. 灵活安装

ESET NOD32 拥有多种部署方式，Web 安装，推送安装，域环境下的登录脚本安装，自定义





安装包等,可以轻松方便地部署客户端,大大减少了网络管理人员的工作量,也使得 ESET NOD32 更容易部署. 广东技术师范学院的网络管理员采用的是通过WEB 按装的方法,将 ESET NOD32 部署到了所有的客户端.

目前, 广东技术师范学院的整个网络已经安装 ESET NOD32 防病毒软件,从 windows 平台的桌面机到移动电脑, ESET NOD32 都提供了完整的解决方案,能够有效抵御网络病毒, USB 病毒和 ARP 病毒等,保护服务器免遭病毒的破坏. 广东技术师范学院的网络管理人员在安装 ESET NOD32 后也感言, ESET NOD32 的确十分轻巧,不拖慢电脑,管理起来也十分灵活.