数字化医院如何突破网络安全管理难题？

——趋势科技 TDA 1000 提升无锡市锡山人民医院化解网络安全威胁管理标准

随着新医改的逐步推进，医疗卫生行业的信息化建设也迎来一个全新的发展阶段。如今许多的医疗机构使用的信息系统，都离不开终端、网络和服务器的安全运行，一旦这些系统遭遇病毒侵入，随时都可能会影响到数字化医院的正常运转。无锡市锡山人民医院（以下简称：锡山人民医院）在加大了医院信息化建设投入的同时，利用趋势科技提供的威胁发现设备 TDA（Threat Discovery Appliance），有效地提高网络安全维护的效率，并对一些医疗行业专用终端设备提供了 7×24 小时的安全监测，全面提升患者的就医体验。

数字医疗顺利推进网络安全维护难度加大

在我国制定的《十二五规划》中，医疗行业成为五大焦点行业之一，特别是新医改政策的推广实施对于医疗行业信息化的发展起到了关键的推动作用。“医改”无法一蹴而就，是一个长期不断推进的过程，同样，信息化安全也将是一个与之伴随的持久战。近年来，锡山人民医院加大了医院信息化建设的投入，引进了国际先进的医疗技术和设备，并筹建了国内一流的数字化就诊设备和各种与之配套的系统，在江苏省属于信息化程度较高的几所医院之一。锡山人民医院的网络结构由内部的千兆内网、连接各个社保中心的 VPN、统一的 Internet 出口组成，并且网络终端数量也超过了 400 台。

但网络从来就是一把“双刃剑”。据锡山人民医院信息科的王映涛科长介绍：“随着各种系统的上线以及终端数量的不断增加，网络安全维护的工作量开始成倍增长。尤其是各种医疗终端与网络连接之后，为一些高危蠕虫病毒和木马程序的查杀带来了难度。例如之前遇到的 DownAD Worm 家族系列的病毒，工程师很难发现真正的感染源头，因此用了两个月时间才基本上消除了这类病毒在内网的困扰。另外，虽然信息科的四位 IT 工程师对每台 Windows 终端都安装了防毒软件和最新的补丁程序，但一些装载英文操作系统、LINUX、UNIX 的终端也能存在病毒感染的机会。而这些终端多为 CT 机等患者病情采集设备连接，因此，我们需要随

时发现病毒感染事件，将隐患消除在第一时间的需求非常明显。因为只有这样，才能保证医院网络和各个系统随时都能为患者提供一流的服务。”

TDA 的“雷达”功能让病毒预警一目了然

网络环境因为医疗信息化覆盖范围的扩大变得越来越复杂，锡山人民医院信息科需要可以快速定位与了解内部威胁，这包括“在哪里发生、何时发生、影响是什么、进行事前的预警……”。在这些需求汇总之后，并考虑到原有趋势科技 OfficeScan 和 Server Protect 防毒墙版本升级后统一管理的特性，最终选择了趋势科技提供的威胁发现设备 TDA。

通过 TDA 独特的反向定位功能，锡山人民医院的网络安全管理效率提高了数倍。由于这项功能可以迅速找到隐藏于网络中的高风险节点，并根据趋势科技整合在 TDA 报告中的解决方案，在这些高危节点尚未造成大规模病毒爆发前就有效处理。比如,医院网络的 Windows 平台是传播病毒的最大终端隐患，但其它安装 LINUX、UNIX 医疗设备终端虽然不会与 Windows 平台交叉感染病毒且传播病毒的可能性也不大。但当这些客户端如果存在病毒，就很可能从网络发起攻击，病毒有可能通过此渠道进入 HIS 服务器区段，从而影响整个网络运行缓慢或者瘫痪。而在安装 TDA 之后，TDA 就像一台全天候工作的“雷达”，接收来自网络上所有的讯号进行智能的分析，这也包括了接入网络的每一台安装 LINUX 或 UNIX 系统医疗设备，从而真正意义上完成了每一个角落进行的全面监控

对此，王映涛科长表示：“趋势科技威胁发现设备可以在应用层对网络中流动的数据进行深度分析，能够看到整个内部网络深层次的安全问题，最大程度降低了恶意威胁可能对医院网络造成的影响。”

TDA 1000 充分考虑到中小网络用户的特性

近年来，医疗行业的信息化投资规模逐年增长的趋势非常明显，但这并不意味着医院就成了“有钱大户”。从医疗 IT 应用投资的结构来看，信息化投资向着更优化的结构转变。由于受资金规模的限制，一些医院的信息化建设，特别是信息安全建设很容易受到产品价格的影响，而忽略产品的质量和配套服务。王映涛科长表示：“其实，我们在 2010 年就对 TDA 产品进行过考察，但因为当时投资预算

等原因，未能及时将这款我们需要的产品进行采购。而今年趋势科技在 TDA 6000、TDA 3000 的产品线基础上，又推出了 TDA 1000 设备，这也是充分考虑到了像锡山人民医院这样的网络规模。同时，TDA 1000 的价格定位非常适合中小企业用户，而且对我们需求的把握也非常准确。”

据了解，锡山人民医院在与无锡市江阴人民医院等同行业用户的交流中，希望借鉴江阴人民医院的方法，在下一步的工作中，他们将结合微软活动目录与组策略安全管理的方法，对终端安全进行更加精细化、颗粒化的管理。同时，由于网络规模、业务系统、管理模式的相似性，其他友邻单位对于 TDA 安全产品的威胁定位功能也非常感兴趣，并且希望得到进一步试用的机会。

细说起来，医疗卫生行业与一些重要金融机构的 IT 系统一样，其实都是需要 7×24 小时的安全护航，尤其是在夜间急诊和周末医生值班时，每个系统地安全性依然要求很高。通过锡山人民医院在网络安全防护上的重视，以及将网络安全管理落地的措施，我们非常高兴“以病人为中心”的现代化医疗服务目标正在得以落实，从而带动整个医疗制度的变革，顺应《十二五规划》纲领。