



## 趋势科技成功案例



### 趋势科技 TDA “第一时间发现威胁” 担任杭州师范大学附属医院的“好助手”

随着医院信息系统的发展和大规模应用，系统的安全性越来越受到重视，一旦网络病毒或是木马在医护平台中出现，随时都可能会影响到患者就医，影响医院的服务质量。为了全面发现并消除终端病毒等安全隐患，杭州师范大学附属医院使用了全球服务器安全、虚拟化及云计算安全领导厂商趋势科技推出的威胁发现设备 TDA ( Threat Discovery Appliance )，为管理员提供了实时掌控网络风险的能力，在第一时间定位并快速处理安全隐患的基础上，全面提升了网络安全维护工作的效率。

#### 第一时间发现威胁，是实现安全管理的“最低要求”

杭州师范大学附属医院建于 1954 年，是一所融教学、医疗、科研、预防保健为一体的三级综合性医院。自医院开展信息化建设以来，院领导非常重视医院网络建设和管理工作，成立了信息化建设领导小组，并组织技术人员专门从事医院信息化建设工作，在人、财、物等多个方面给予全力保障。

近年来，随着信息化应用水平不断提升，数字化医院建设的步伐加快，整个网络规模和终端数量增长很快。其中，杭州师范大学附属医院的终端数量已经达到了 1000 台以上，而由数十台服务器承载的应用系统，如 HIS、LIS、 PACS、电子病历、协同办公系统等等，各种业务应用越来越紧密地与网络融合在一起。这种融合使得医院信息化工作不得不面对和解决一个非常重要的问题，那就是倍受关注的网络安全问题。

对此，杭州师范大学附属医院信息科的吴科长表示：当前的网络病毒感染的渠道越来越多，且病毒本身也越来越智能，不仅可以通过各种方式疯狂传播，而且可以对抗系统中的防毒软件，使用户的防毒软件不起作用或者丧失防护能力，我们之前用到的防毒系统就出现过这样的问题。但各大业务系统都离不开终端、网络和服务器的安全运行，而一旦这些系统遭遇病毒入侵，随时都可能会影响到患者就诊效率、医药处方处理等工作的正常运转。因此，在第一时间发现病毒威胁，将其隔离起来，这是保障医院各业务生产系统的稳定、安全、不间断运行的最低要求，也是符合上级单位要求的网络安全等级保护，实现合规性的基础。

## **第一时间发现威胁，是实现主动运维的“得力助手”**

为了完善并落实各项安全管理制度，尽可能将各类安全事故在萌芽阶段就能发现并处理，杭州师范大学附属医院对市场上的网络安全产品进行了较为全面的了解，并安排了测试工作。但这些 IDS、IPS 和内网防火墙产品都只能工作在网络层，并不能在应用层威胁进行事前防护，与医院倡导的主动运维管理、提升 IT 服务水平的高标准要求相差甚远。

机缘巧合，在寻找威胁发现产品的道路上，杭州师范大学附属医院最终与趋势科技推出的威胁发现设备 TDA 不期而遇。不但 TDA 功能中 HTTP 访问恶意代码检测、P2P 会话流量管理、蠕虫漏洞扫描等非法流量检测功能都能符合院方的技术要求，而且在“威胁”来源定位的效率，TDA 更做到了“秒”级预警。其次，TDA 还可通过“数据包”和“会话”视图对医院 1000 台终端的通讯数据进行自动关联分析，即从趋势科技的云安全数据库进行比较，自动将占用网络带宽的应用和造成网络通讯拥塞故障的信息建立威胁关联。

据了解，在 TDA3000 部署后，大大节省了以往人力查找威胁代码源头的工作量，避免了以往类似产品对网络造成的流量占用和其他风险，保障了传输网络效率。值得一提的是，通过 TDA 独特的反向定位功能，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。这些功能的整合应用，变被动运维为主动运维，使得管理员对医院网络中存在的风险能及时了解到全面的状况。

吴科长表示：TDA 3000 的部署确实给我们医院带了实惠，节省了很多人力成本，TDA 系统上导出的威胁分析报告，也给我们在今后信息安全规划方面起到了辅助和引导的作用。基于趋势科技在我院业务上的理解，以及虚拟化在医院数据中心的应用，下一步，我们将继续保持技术上的及时沟通并深入合作，让网络建设、安全管理与业务创新融合的更加紧密。

###



### 关于趋势科技 ( Trend Micro )

趋势科技是全球虚拟化及云计算安全的领导厂商,致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念,基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构,为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全,保障信息与财产的安全。同时,遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息,请访问:[www.trendmicro.com.cn](http://www.trendmicro.com.cn)。请访问 Trend Watch : [www.trendmicro.com/go/trendwatch](http://www.trendmicro.com/go/trendwatch) 查询最新的信息安全威胁的详细资讯。

#### 更多媒体垂询, 敬请联络:

趋势科技(中国)有限公司

刘婷婷

电话: 010-85252277

电子邮件: [angela\\_liu@trendmicro.com.cn](mailto:angela_liu@trendmicro.com.cn)

谋信传媒

那罡

电话: 010-67047822

电子邮件: [nagang@ctocio.com](mailto:nagang@ctocio.com)