趋势科技专家服务为上海华山医院信息化护航

复旦大学附属华山医院是一所综合性教学医院，具有90年的历史。该院于1992年首批通过国家三级甲等医院评审，目前已成为全国医疗、预防、教学、科研相结合的技术中心，融医、教、研为一体，在国内外享有较高的声誉。华山医院不仅拥有一大批专家教授和先进的医疗设备，而且还积极进行医院的信息化建设，为医疗和教研提供了现代化信息手段的支持。

医疗信息化，网络安全刻不容缓

医疗系统不同于其他行业，不间断的网络运营是最最重要的，而且由于医院涉及到人们的生命安全，对数据的安全性和一致性也要做到万无一失。随着医院信息化建设的不断探索和提升，医院信息化系统从以往单纯管理工作逐渐向医院的各个业务领域渗透。复旦大学附属华山医院先进、成熟的信息系统不仅成为该院医疗现代化、规范化的基础，更成为提升工作效率、扩展行业影响力的有效手段。趋势科技早在2003年便为华山医院的信息化建设提供业界领先的解决方案，保护其终端计算机、服务器以及应用安全，提供华山医院业务持续稳定运行所能依赖的坚实基础。

然而，越来越庞大的网络系统所面临的病毒、黑客威胁也与日俱增。随着网络安全形势日趋严峻，华山医院的信息化网络安全也受到极大的考验。病毒的泛滥、木马的威胁、以及间谍软件和黑客的骚扰，严重威胁着华山医院的信息安全。

作为全球网络安全的领导厂商，趋势科技一直关注网络安全问题的发展趋势。趋势科技先进的EOG专家值守服务在复旦大学附属华山医院的成功应用，成为医疗行业信息化安全应用的典范。面对日新月异的网络病毒，EOG专家值守服务整合了华山医院原有的防病毒体系，趋势科技相对应的提供了除产品之外EOG专家值守服务，丰富华山医院安全体系建设，真正做到：

- 通过产品，落实基础的安全架构框架；
- 透过服务，提升根本的安全管理水准。

通过应用该产品与服务内容相结合的解决方案，全院的400多个计算机节点的网络安全防范又得到了进一步的加强，取得了良好的防毒效果。

7×24专家在线支持，随时化解网络风险

EOG趋势科技专家值守服务不同于以往问题响应式的被动服务，通过实时监控的技术手段，能够为用户的网络提供7×24小时不间断的主动式远程代维服务。通过对网络中发生的所有安全事件进行整体汇总，控制病毒整体生命周期，做到早期预警、实时处理、全网病毒清除。

华山医院信息中心副主任黄虹表示，“使用了趋势科技EOG专家值守服务后，趋势科技后端的专家能细致地了解目前医院信息系统的整体安全状况，提供全面的安全指导，给我们提供了强大的技术支持；对于突发的安全事件，能及时地联系到我们，快速解决处理，并提供现场服务，解决了我们人员紧缺的问题。我们可以依赖一群网络安全专家来处理我们各式各样的网络安全威胁，这为我们医院网络的稳定运行提供了有力的保障。”

全方位报表分析，定期提升防毒能力

经过多年的防毒实践，华山医院信息中心的工作人员感觉到，尽管采取了多种措施，但是频繁爆发的安全问题还是让他们防不胜防，根本原因在于没有人和资源来7×24小时监控网络，随时应对可能爆发的安全问题。黄主任深刻体验到使用趋势科技EOG专家值守服务后带来的效果：“趋势科技提供的7×24不间断的病毒相关事件的接收、过滤、分析、通告，能够随时监测病毒和木马的侵袭，大大减轻了我们的工作压力。”

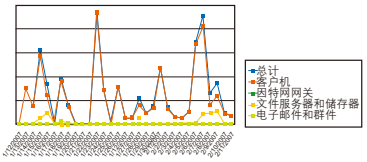
日趋复杂的网络应用使华山医院的网络安全压力与日俱增。黄虹表示，根据以前的经验，存在有引起病毒感染的漏洞的计算机或用户都只是很小的部分，但是由于缺乏好的分析手段而无法找出这些问题并解决，从而使病毒持续在这些计算机上泛滥并感染其它的计算机。

趋势科技的EOG专家值守服务能够提供每日检查分析公司防毒状况、每日防毒报表、病毒来源分析等信息，甚至能检视病毒是来自于网关、邮件服务器、档案服务器或是客户端计算机，这样在有效遏制病毒侵害的同时，也能根据报表的数据动态进行反病毒系统的安全设置，防患于未然。

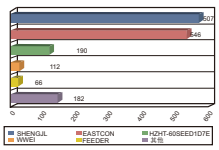
趋势科技EOG专家值守服务，为医疗系统保驾护航

如何在确保病毒风险可控的前提下，最大限度发挥信息网络的生产力，成为医疗系统IT管理人员必须面对的问题。一直以来，防病毒带来的业务中断及资产损失又需要耗费太多的精力，并且往往只能等待灾难降临时才仓促应对，信息中心人员似乎始终陷入在灾难处置工作当中。趋势科技EOG专家值守服务的推出改变了这一格局，能够在第一时间为信息系统提供最及时的安全防护，并构筑了从病毒监控、预防到处理、分析的全方位网络安全防护体系，全面满足了医院对信息安全的需要，有力地保障了医院的信息安全，必将成为医疗行业信息化安全的坚实后盾。

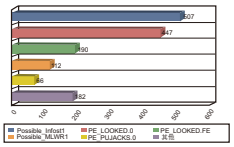
报表示例（该数据仅为演示用不代表华山医院实际情况）：



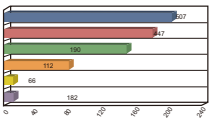
- 了解公司每天病毒数量分布情况
- 了解哪些产品感染病毒数量最多，便于重点着手解决



- 及时掌握每天公司感染病毒数量最多的5台电脑，可以：
  - 检查这些电脑的使用情况，是否存在漏洞或者其他安全隐患
  - 检查这些电脑使用者的使用习惯，是否在使用过程中存在严重违反安全策略的行为



- 及时了解公司每天病毒感染数量最多的5个病毒信息，通过分析这些病毒的传播方法和途径，可得出针对性的建议方案



- 每天及时掌握公司前5大病毒感染源，可以：
  - 查找这些电脑是否有系统漏洞以及不安全的共享
  - 加强对这些电脑的病毒检测和清除，以及加强对使用者的安全意识培训