

从 2001 年爆发的 CodeRed、Nimda，到去年的“冲击波”病毒，再到今年的震荡波、Phishing、witty 等等，蠕虫病毒带来的安全事件愈演愈烈，其危害不断升级，不仅攻击速度越来越快，而且攻击力越来越强大。与此同时，伴随着企业信息化进程的不断加快，更使信息暴露在网络攻击的面前。那么，面对这一严峻的形势，企业应该如何才能御毒千里呢？

打造主动防御的钢铁长城

——趋势科技 NVW 助力北京人民医院战胜蠕虫病魔

拿什么拯救网络？

伴随着网络的迅速发展，近年来，蠕虫病毒引发的安全事件此起彼伏，且有愈演愈烈之势。从 2001 年爆发的 CodeRed 蠕虫、Nimda 蠕虫，SQL 杀手病毒，到今年肆虐的震荡波、网络钓鱼、Witty 等蠕虫病毒，无不有蠕虫的影子，并且与病毒相结合愈发明显，如果不及时预防，它们就可能会在瞬间快速传播、大规模感染网络，对网络安全造成严重危害。

同时，各类蠕虫病毒各具特色，演绎了一场又一场长江后浪推前浪的安全事件。新病毒的攻击力变得越来越大，一旦爆发，其破坏力十分惊人，而且影响面相当大，它们无孔不入，不易清除。目前的安全解决方案，像防毒软件、防火墙、弱点评估、入侵侦测与预防系统，都无法有效阻挡这些病毒。据估计，“震荡波”造成的计算机损害要花 9.97 亿美元。

北京人民医院也曾饱受病毒之苦，其网络在改造前分为两部分：一是业务网络 HIS 系统，其中的客户机和服务器都加入 windows 域由网管员统一管理，而另一部分是以工作组形式出现的科研教学机器。由于全网机器没有安装统一的杀毒软件，特别是科研教学机器上单机版杀毒软件无法统一升级病毒库，网管人员也无法强制这些机器实时安装系统补丁。结果内网病毒泛滥，带宽被病毒数据包所占用，不仅上网速度慢，更会影响服务器的正常工作。

面对严峻的网络安全形势，北京人民医院原有的信息安全系统显得不堪一击。这正如北京人民医院一位负责人所说：“面对病毒，我们是那么的无助，不管是冲击波，还是震荡波都可以随意蹂躏我们辛辛苦苦建立起来的信息系统。更可怕的是，即便切断与外网的连接，内网里已经渗入的大量‘病毒’暗箭仍然防不胜防，长于对付真实病毒的我们，却无法将电脑中的病毒斩尽杀绝，以致我们不敢把重要的数据，放到信息系统里。”

因此，为了提高北京人民医院的核心竞争力，推进信息化的发展进程，必须结合网络病毒的发展趋势，在传统的防毒措施已经不能适应新的网络安全需求的情况下，寻求新的解决方案，并针对蠕虫病毒的特点，在网络层建立统一的全面的安全防护体系。

对症下药 药到病除

作为网络安全的全球领导厂商，趋势科技一直以来都致力于网络系统的安全防护研究，致力于建立一个更主动、更实时的智能化网络安全防护系统。针对网络安全的发展趋势，推出了具有全面病毒爆发防护、病毒爆发生命周期集中管理、抵御或减缓病毒发作等优势于一身的

Network VirusWall (网络病毒墙)。

在北京人民医院的安全防御系统的规划中，趋势科技针对网络病毒的发展趋势，以及北京人民医院的网络特点，为其量身定制了一套完整的解决方案，该方案采用 NVW1200 百兆和 NVW2500 千兆产品，不仅为北京人民医院构筑了从客户端到网关的网络安全解决方案，更在与外网的连接处布置了性能卓越的趋势科技病毒墙。

趋势科技病毒墙提供了自动隔离薄弱环节、智能网络疫情监测、预防网络疫情、网络扫描与侦测、自动清除损害、实现企业安全策略的实施，以及便于使用、管理与安全控制等功能，使北京人民医院的网络可以有效地防制 Internet 蠕虫之类的网络病毒的入侵，在爆发病毒疫情时隔绝高危险的网络脆弱环节，在网络层部署由趋势科技提供的安全防御策略，并能在缺乏防毒保护的设备等潜在感染源连接网络时，予以隔离和清除。不同于只监测安全威胁或提供信息的安全解决方案，Network VirusWall 协助企业采取准确、快速的安全措施，并且主动侦测、预防围堵与进行善后清理。

更为重要的是，趋势科技的病毒墙支持企业安全防护策略 (EPS)，并经由中央控管管理。主动预防技术对病毒的反击做到“先知先觉”，可以以最快的速度阻隔和消灭病毒攻击，把危害降到最低。而中央控管系统实现了在快速部署、积极防治的同时，主动遏止新病毒，这对于减少蠕虫病毒的危害以及降低技术支持成本均大有帮助。

总之，建成后的网络安全防御系统实现了将企业安全防护策略延伸到网络层次，避免因网络漏洞受到攻击及后续的病毒扩散，可以用来侦测和隔离网络资料串流内的病毒，协助安全管理人员透过通过经验式的分析监控网络活动，及早发现病毒爆发的征兆，确保了北京人民医院的网络安全。

实现最有效的防制

“采用趋势科技解决方案后，我们可以利用 NVW 的特性，强制全网计算机对本机进行漏洞评估，每台客户机只有在内部网站上下载更新系统补丁后，才能通过这一关，更妙的是全网计算机从此必须统一安装趋势科技客户机防病毒程序，才能正常上网，这样一来，以往网管员手工为每台机器打补丁和安装升级杀毒软件的庞大工作量，现在由每个网络使用者自己主动完成了，网络从此安全，我们也可以将精力更多投入其他方面的信息化建设。”对于趋势科技为其量身定做的网络安全防御系统，北京人民医院的 IT 主管说出了他的心里话。

无疑，当北京人民医院在网络部署 Network VirusWall 之后，效益非常明显，全网共查杀了 22 万多病毒，也不再有机发送病毒数据包占用网络资源了，而这是在疫情管理负担大大减轻的前提下实现的。

北京人民医院的成功也正凸现了趋势科技解决方案的优势。通过强制实施全网一致的防毒安全策略，并且准确清除网络上的感染源，可大幅降低安全风险。而一旦爆发病毒疫情时，隔离高危险的网络弱点，预防攻击或限制攻击发生的区域，以减少网络的停机时间。此外，可得

到来自趋势科技屡屡获奖的全球安全专家网络提供的特定病毒防治策略，这些防制策略可以方便、统一地部署到整个网络，有效地减轻疫情管理负担。

当然，网络安全是一个系统的、全局的工程，要最大限度地发挥病毒墙的效用，必须实现与其他产品优化组合。趋势科技通过各产品模块的组合构成了完善的防病毒架构，各产品模块可以互相集成，根据北京人民医院实际需求实现有针对性的保护策略，实现对企业网络内部资源的全面安全保护。同时通过集中管理平台，使管理员在集中的一点即可完成所有防病毒策略设定与分发。

趋势科技不仅提供防病毒产品，同时其提供的服务更值得称道，由趋势科技屡屡获奖的全球支持组织或是认证的渠道合作伙伴，提供最佳品质的支持服务。趋势科技的企业专属服务，通过专职的项目技术经理对企业用户进行点对点的技术支持，而等级服务协议做出的如果没有在规定时间内解决客户的问题将接受罚款的大胆承诺，更保证了客户价值的最大化。

我们知道，信息化作为未来社会发展的必然趋势，对医院的重要性也逐步显现。它的作用不仅仅是为了解决医院目前的生存问题，更是医院长期发展的基础。为此，面对纷繁复杂的网络环境，以及蠕虫病毒日益猖狂的今天，医院迫切需要全新的网络安全解决方案，以及积极主动的防御理念和中央控管的管理机制保证医院的网络安全，推进信息化建设，以提高医院的核心竞争力和服务水平。

+ + +

关于趋势科技

趋势科技—网络安全软件及服务领域的全球领导者，几年前就以卓越的前瞻和技术革新能力引领了从桌面防毒到网络服务器和网关防毒的潮流，现在又以独特的服务理念再次向业界证明了趋势科技的前瞻性和领导地位。总部位于日本东京和美国硅谷，目前在26个国家和地区设有分公司，员工总数近2000人。趋势科技分别在日本东京证券交易所和美国NASDAQ上市，并在2002年10月入选日经指数成分股，创造了日本证券史上的奇迹。

趋势科技在把创新思想成功转化为尖端科技方面享有盛誉，Gartner Group连续四年把趋势科技评定为最具创新能力的防毒管理供应商。IDC数据表明，趋势科技在全球服务器架构防毒解决方案居领导地位，在整体服务器防毒软件市场、群组防毒软件市场、网关防毒软件市场的占有率均高居全球第一位。

趋势科技2002年在全球推出了里程碑式的企业安全防护战略—EPS(Enterprise Protection Strategy)，采取主动性的预防措施，在病毒爆发的初期通过中央控管系统及时部署预代码，并对病毒进行生命周期的管理，从而使用户得到最大限度的安全保证。趋势科技一向注重服务品质，其企业专属咨询服务—PSP(Premium Support Program)自从推出以来，就受到了众多国际性大企业的青睐。去年，趋势科技在PSP的基础上又提出了服务等级协议—SLA(Service Level Agreement)，这又是一个伟大的创举，趋势科技做出了如果没有在规定时间内解决用户

的问题将接受罚款的大胆承诺，这在防毒业界是唯一的。