

再好的防病毒解决方案，如果使用不当也不会发挥出好的效果。同样的防病毒解决方案，在不同的用户那里会收到不同的效果。借用浙江移动负责网络及安全系统管理的负责人徐良的话说，在防病毒专家的指导下，有效的技术手段和管理制度，加上个性化的定制开发，就会收到事半功倍的防病毒效果。

全面实践防病毒理念 成为电信行业样本

-----浙江移动全面采用趋势科技的防病毒解决方案和服务

徐良的话是出自切身体验。近年来，由于与趋势科技加深合作，从客户端到服务器、从技术手段到管理手段，从薄弱点加固到个性化定制开发，浙江移动在防治病毒、蠕虫方面取得突出效果。病毒引发的安全事件大大减少了，每天采用人工查杀的机率已经降到了 15 台以下。由于安全规范和管理制度已经建立健全起来，IT 工作人员的工作状态也从以前的“风风火火”地赶往出事地点进行“灭火”，转变成“按部就班地进行例行检查”，浙江移动也因为防治病毒效果突出而成为样板，在电信行业中广泛推广。

曾经吃过苦头

浙江移动的防病毒之路，也不是一帆风顺的。这家隶属中国移动通信集团公司，是中国移动的全资内地运营子公司，在浙江全省拥有 11 个市分公司和 62 个县（市）分公司，移动电话客户总数已突破 1400 万户。就是这样一家网络规模和客户总数连续八年位居全国第二位的电信运营商，在病毒防治方面也曾经遇到许多波折。

徐良所在的浙江移动网络采用分布式的双星型结构，分为省中心和 11 地市，承载着内部办公，计费、审计、账务、客服、办公等职能，内部用户达 1.3 万之多。徐良所在的部门承担着系统开发管理维护与支持、公司内部信息安全建设等重任。可以想象，在这样庞大、异构的网络中，一旦发生病毒爆发，后果将是多么严重。

在采用趋势科技产品之前，浙江移动并没有大规模安装部署访问控制设备，只是在关键设备、核心位置以及内外网的连接处，部署了防火墙。当时，病毒是浙江移动面临的最大问题。由于病毒扩散严重，业务不能正常使用的情況时有发生，最严重的一次竟然导致一千多台终端受到影响。当时，浙江移动并没有统一购买网络版的防病毒解决方案，各个单位只是零星购买和使用着五花八门的单机版防病毒软件，如诺顿、金山、江民、瑞星等。这些防病毒软件既没有统一的升级，也没有统一有效的部署和管理。事后，徐良总结出两条教训：一是没有统一升级和管理的防病毒软件形同虚设；二是只有加强管理才能充分发挥防病毒方案的功效。

从 2002 年开始，浙江移动开始了与趋势科技的合作，并持续到今天。在近四年的合作中，浙江移动充分实践着趋势科技的防病毒技术理念：网关防毒、集中控管、控制蠕虫、安全策略的个性化定制.....,并一步步达到出神入化的防病毒境界。

经验一：网关控制病毒源头，NVW 围剿蠕虫

2002 年，浙江移动开始购买了趋势科技的 OfficeScan、ScanMail，并对趋势科技先进的防病毒技术和理念深信不疑。在实践中，徐良发现病毒来源主要是邮件和互联网。只要控制好这两个入口，就能把病毒源头控制住。而原来只是针对客户端的解决方案，只是治表不治本。于是浙江移动扩大的防病毒的产品线，陆续部署了趋势科技的网关防护。这样以来，占据邮件总量高达 2/3 的病毒垃圾邮件过滤掉了，大大节省了邮件服务器资源。

2003 年以来，攻击系统漏洞的蠕虫病毒出现的频率越来越高，对于那些利用系统漏洞传播的蠕虫病毒，传统的防病毒软件起不了太大作用。而趋势科技 NVW 设备适时地被研发出来并很快被浙江移动所采用，NVW 阻断网络病毒提供快速部署主动式网络病毒疫情防治解决方案，保护企业重要的网络交换设备、应用主机、网络性能以及分支机构的网络。在全球出现 Slammer、冲击波等几次

大的疫情时，很多电子邮件不能幸免，而浙江移动安然无恙，没有受到任何冲击。

经验二：TMCM 落实安全管理，安全管理与业务流程相结合

疏于管理是病毒防治的大敌。许多病毒事件是因为病毒代码库更新慢引起的。浙江移动又开始引用能够对防病毒系统进行统一升级，完成防病毒代码的统一分发和版本的统一升级的趋势科技 TMCM。

在部署了 TMCM 之后，浙江移动的防毒策略有了更强大的集中控管能力，可以从省中心来进行防病毒软件的统一管理、监控和部署，更有效地管理整个企业的防毒策略。TMCM 的设计旨在能够快速部署、积极防治，主动遏止新病毒，这对于浙江移动减少大量邮寄病毒的危害以及降低技术支持成本均大有帮助。在与趋势科技的共同努力下，浙江移动还开发了 TMCM 与安管中心的接口。这样第一时间知道多少台设备感染了病毒，了解病毒传播情况，实时获得相关信息，加强管理手段，

不仅如此，从 2004 年开始，浙江移动在趋势科技的帮助下，将病毒防治流程纳入到工作业务流程。在具体工作流程中，将安全责任到人，进行后续的手工清除，以保障对病毒的彻底清除。同时建立考核机制，并设立地方部门管理和省公司管理的两级管理机制，编写手册，加强对安全管理员防病知识方法的培训。

这里还有一个小插曲。为了确保防病毒具有持久效果，在全面部署趋势科技防病毒解决方案之前，浙江移动在趋势科技的建议下，对每一个结点的设备都进行了登记，记录下操作系统及防病毒的版本，用户名称等，确保安装防病毒软件之前，将病毒全部分清除，这为浙江移动日后的防病毒工作打下了坚实的基础。到目前为止，每天不能被防病毒软件查杀，需要通过人工查杀的，7 千多台不超过 15 台设备，网管员的工作量一下子锐减下来。

经验三：获得 PSP 专家支持服务，个性化定制开发

对于自己解决不了的问题，浙江移动的经验是赶紧求助趋势科技的技术专家。在 2005 年上半年，浙江移动购买了趋势科技的 PSP 服务，以快速解决突发

事件和可疑问题。

PSP 提供的服务内容包含产品技术支持、防病毒支持、病毒咨询百科，透过这套系统客户可以追踪目前所有产品或病毒未完成的案件，针对未能及时解决的案件，提供专门维护小组支持，最重要的是，趋势科技承诺在约定的时间内快速解决问题。

这里也有一个很好的小插曲。趋势科技在对浙江移动的日常检测中，发现了一些漏洞和后门，由于一些员工在下载陈桥五笔这种共享软件时，同时也将设置其中的后门漏洞下载下来，趋势科技在进行地址巡检时发现了并及时解决了这一问题。同样，趋势科技发现游戏也常常是病毒藏身的地方。对于发现的这些问题，趋势科技及时通报给浙江移动，并给出了专业建议，进一步弥补了病毒有可能侵害的漏洞。

高明的厂商与高明的用户结合在一起，产品肯定就会用活了。浙江移动与趋势科技的合作正在迈向更高层次——个性化定制开发。浙江移动正在与趋势科技及其他这一家 IDS 厂商一起，共同将 IDS 与防病毒系统互动，以充分发挥有效 IDS 的作用，使 IDS 也能跟踪病毒，掌控网络的感染情况有效监控，趋势科技对此给予积极响应。

浙江移动所取的防病毒效果是有目共睹的。徐良说这与趋势科技从产品到方案再到服务的全方位支撑是分不开的。徐良对趋势科技先进的防病毒理念表示充分肯定。由于病毒的生生不息，决定了病毒防治是一项长期工程，永无止境。对于这一点，浙江移动做好了充分准备并有很大信心，而趋势科技就是浙江移动信心的来源。