

消除病毒威胁刻不容缓 趋势科技全面保护“民生服务网络”

——趋势科技 OfficeScan 网络版防毒墙在青岛市人力资源和社会保障局防御效果显著

青岛市人力资源和社会保障局深化政务公开载体建设，借助信息化手段，已经建设完成了一流服务型政府网站和业务网络信息服务平台，全面提升政府民生保障和公共服务水平的措施，得到了领导和广大群众的认可。但伴随着互联网 Web 威胁的加剧，无孔不入的病毒和木马时刻都可能影响青岛市政务网络的稳定运行。

为了全面保护三大数据中心和大量下级单位的网络安全，青岛市人力资源和社会保障局信息中心携手国际领先的网络安全产品供应商和服务商——趋势科技，利用趋势科技 OfficeScan 网络版防毒墙，部署在 2000 余台终端层上，有效地抵御了内网病毒爆发等恶性事件的发生。

提供“例外”防护 有效避免“误杀”

近年来，青岛市人力资源和社会保障局高度重视信息化建设，在市政府的正确领导和大力支持下，加大资金技术投入，与实际应用紧密结合，本着以建设带动应用，以应用促进发展的原则，全面推进了人力资源和社会保障电子政务的建设。据了解，在信息化软件方面，包括养老待遇系统、医疗保险管理系统、劳动力就业系统、城镇居民医疗保险管理系统、劳动监察管理系统、劳动稽核管理系统等数十套业务系统。同时，在 IT 环境的网络安全项目建设中，也先后购置了防火墙、IDS、IPS、审计、隔离网闸、备份存储、网络准入控制等多套安全防护系统。但对于 5000 多台终端的防毒系统却一直未能统一，在 Web 环境日益恶化的今天，网络病毒的治理一直困扰着青岛市人力资源和社会保障局信息中心的工程师们。

据信息中心运行管理科负责人介绍：“青岛市人力资源和社会保障局在 IT 软件和硬件方面的维护人员共有 15 名，其中 6 人专门负责网络管理和信息安全工作。看似人手很多，但随着下联经办机构单位、医疗机构和区域劳动保障事业一体化、同城化的项目越来越多，网络安全运维的情况不容乐观。尤其是下联经办机构单位中，很多防毒系统都出现了对业务软件客户端‘误杀’的情况，这都让我们必须重新考虑安全、可靠、统一的终端防毒系统的建立。”据了解，几年前正是因为当时防毒软件误杀事件的不断扩大，运行管理科在近十种产品中反复评测和长期试用，最终选择趋势科技 OfficeScan 网络版防毒墙，并在绝大多数

的终端上成功部署。

“当时有很多厂商参与竞争，但信息中心不能接受‘拥有强力查杀，但误杀不断的解决方案’，因为一旦误杀事件出现，社会保障业务将可能面临着比病毒感染还要大的损失风险。换言之，对于病毒，即不可以漏判，也不可误判。”运行管理负责人说，而趋势科技 OfficeScan 由于可以启用云安全的文件信誉和定制的“例外列表”，在大幅降低最新木马病毒查杀延迟的同时，所有的业务系统也都可以在防毒墙的统一管理中心启用“例外”，达到了查杀与误杀的平衡。

随时随地统一管理 减少人力成本消耗

正如前面提到的统一和远程管理，这对于青岛市人力资源和社会保障局联入单位众多、缺乏专业安全人员，且地域分散的特点，非常有必要在防毒系统中体现。同时，由于数据涉及到参保人员的信息等等，业务应用系统网络和个人所用计算机上都有需要涉及个人隐私的信息，即使内部网络的一台机器安全受损（被攻击或者被病毒感染），就会影响在同一网络上的其它计算机，或是通过网络传播，还会影响到与本系统网络有连接的其他上一级网络，甚至还可能涉及安全敏感数据中心领域。

为了解决上述问题，青岛市人力资源和社会保障局根据国家对于政府行业计算机制定的国家三级等级保护要求，利用了趋势科技防毒墙控制管理中心（TMCM），为部署在网络中的 OfficeScan 和其他内容安全产品提供集中的管理和全网范围内的协调运行。运行管理负责人表示：“过去我们下联经办机构的终端用户如果感染了一些新病毒，尤其是变种病毒，管理人员就会充当‘救火员’的角色。但是由于这些单位离信息中心较远，终端用户计算机水平也参差不齐，无论是问题描述还是收取样本都很困难，使得很多新病毒的处理周期较长，给管理人员造成很大的压力。”

据了解，在使用 TMCM 之后，信息中心的工程师在第一时间，就能获得有关病毒事件或异常活动的准确信息，并能创建用于分析和监控的图形报告。通过 Web 管理界面，即使工程师不在现场，那么，只要是全网的任何一台终端都可以进行最新防御策略的调整。现在通过 TMCM 的统一管理，青岛市人力资源和社会保障局根据保护对象的重要程度，重新设计了安全保障体系，并制定了分级安全等一系列的管理措施，在病毒爆发周期的任何一个阶段都能做出快速响应。

虚拟化进程加速 独特防毒能力吸引眼球

青岛市人力资源和社会保障局在终端以及青岛同城生产数据中心一、生产数据中心二和备份中心都广泛开始部署虚拟化应用。经过在边缘服务器上测试趋势科技 Deep Security 之后，信息中心对 Deep Security 在 VMware 虚拟平台上的兼容情况非常满意，它不仅可以做到深度服务器安全防护，抵御病毒感染、非法入侵、数据泄露等恶性事件的威胁，同时也不因为虚拟化的安全需求而增加服务器的工作负载。

据了解，信息中心下一步将加速核心业务上启用虚拟化和私有云建设进程，而趋势科技的 Deep Security 将成为首选的安全防护产品。