[趋势科技成功案例]

趋势科技打造信息安全建设的“徽商典范”

——合肥百大集团零售业网络安全成功案例

随着时代变迁，零售行业的经营模式正在发生着质的变化，以信息化网络为核心的经营平台已经形成。近年来，合肥百货大楼集团股份有限公司（以下简称：百大集团）在信息化系统的支撑下，得到了快速发展，取得了骄人业绩，但随之而来的网络安全问题却为 IT 部门提出了各种难题。趋势科技作为全球服务器安全、虚拟化及云计算安全领导厂商，在对百大集团的供、销、存等应用系统以及网络架构的特性做了深入调研之后，为百大集团提供了一套适合零售业的整体安全解决方案。通过网络威胁主动防御体系的建立，帮助百大集团实现了从互联网到终端的多层次防护系统，标本兼治的效果得到了集团领导的高度认可。

到处救火网络安全成了“拖油瓶”

百大集团始建于 1959 年，连续多年入围中国企业 500 强，也是迄今为止安徽省唯一的零售行业的上市公司。近年来，随着门店的不断扩张，对财务管理、供应链管理、招商管理、门店管理、促销管理、会员管理、价格与促销管理、门店安全系统和协同办公等信息化系统的需求也大幅提升。作为安徽省零售行业的中流砥柱，百大集团的信息化建设虽然起步较早，但随着网络规模的不断扩大，终端和服务器的数量剧增，终端病毒爆发和 Web 恶意代码侵入的现象呈现出几何倍数增长的态势，这给正常业务的开展带来极大影响。

据百大集团信息部部长陈永斌介绍：“百大集团也曾经使用过多套防毒软件，并通过多种途径了解过友邻单位的几款终端杀毒软件的使用情况，但始终都是治标不治本。往往是中毒后再去查杀，而且交叉感染和反复中毒的现象十分严重，病毒感染严重影响了员工的工作效率。而近期测试过的几款软件，查杀率高的误杀率也高，功能全的资源开销又大，左右衡量之后都没有最佳的选择。现在的情况只能靠部门内的工程师亲身去现场解决，效果不好且人力成本极高，颇有消防队员到处救火的无奈。因此，我们对于网络威胁防护的期望也非常简明，形成主动防御，不再让安全问题成为企业高速发展的‘拖油瓶’。”

防御为先标本兼治的安全体系

百大集团对安全防护的期望，看似简单一句话，但真正要实现起来，却绝对不是桌面防毒软件“一招搞定”这么简单。为了避免再次出现“头痛医头、脚痛医脚”的方案，趋势科技的安全专家在全面分析百大集团的网络架构的基础上，比对被感染终端上提取的大量病毒样本。通过各类数据、样本和传播手法的分析，发现百大集团超过 7 成的病毒种类皆为木马病毒，且感染源来自互联网，再通过内网扩散传播。另外，终端用户的技术水平、使用习惯、安全意识的相对薄弱，也是病毒肆虐的重要因素之一。结合多方面的信息汇总，趋势科技安全专家，提出了“防御为先、标本兼治”的设计思路，这与陈部长的设想不谋而合。

既然找到了问题的根源，就应该从阻止感染源头着手。首先，在百大集团在互联网出口处部署了趋势科技 IWSA 互联网内容安全网关，针对包含恶意代码的网页浏览和文件下载进行实时的内容安全过滤。IWSA 使用了趋势科技独有的云安全技术，每天自动分析超过 46 亿条的海量 URL，并利用创新的 Web 信誉评估技术（WRT），自动过滤、分类各种网页，根据信誉评级阻挡恶意的 URL 进入到百大集团的网络中。

通过后台中网络威胁特征码的自动识别技术，以及无需更新的实时防护功能，将互联网威胁侦测的“速度”与“数量”的优势发挥到极致。据了解，百大集团现在可以将 90%的新威胁拦截在网关之外，极大地降低了内网终端与新型病毒的接触率，杜绝病毒不断入侵、反复感染的风险。其次，在终端防护这一层，百大集团还部署了趋势科技网络版 OfficeScan 安全防护软件，并利用趋势科技针对中国区病毒码，以及移动存储设备的权限管控技术，提高了终端病毒的查杀效率，以及移动设备交叉感染病毒的风险。

集中管理获认可安全产品发挥最大功效

在“IWSA + OfficeScan”双层威胁防御体系实施一段时间之后，趋势科技将一份阶段性分析报告呈现在百大集团 IT 人员面前，“总体病毒感染数量直线下降，新病毒入侵的问题被遏制，木马病毒感染的问题得到明显改善……”陈部长对实施结果和监控报告非常满意，他表示：“利用云安全技术，趋势科技提供的安全产品不仅具备了 Web 威胁数据库为依据的信誉评级技术，并且在终端 PC 的资源开销和稳定性都未受到影响的前提下，为日常管理提供了详细的安全报表和预警功能。同时，通过集中控管平台的中央控管技术，由安全管理员统一制定安全防护策略，避免了之前由于终端用户安全防护技术水平欠缺而无法将安全产品用好的尴尬。”

据介绍，百大集团的高层领导和普通用户对趋势科技实施的安全防护效果都十分满意。为了

进一步将安全威胁降低，陈部长主动表示，希望能与趋势科技进一步合作，着手考虑如何建立更加全面的风险预警平台。由此，趋势科技基于“智能关联分析”的企业威胁管理战略方案，也被提上议程。

此外，在百大集团的规划蓝图中电子商务将是集团业务发展的重点，百大集团未来的在线业务安全和数据中心将会向虚拟化和云计算中心方面迁移，届时趋势科技 Deep Security 可以完美地与百大集团的虚拟化环境实现无缝连接，提升虚拟化平台环境下的安全指数，令风险无处藏身。趋势科技将携手百大集团，共同打造成为信息安全建设的“徽商典范”。

###

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 1,200 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。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。