

趋势科技从客户端到网络层帮助文峰大世界阻击Web威胁

两年前，江苏文峰大世界连锁发展有限公司的信息中心主任王洪曾经面对企业内的600台PC头疼不已。在特洛伊木马、网络蠕虫不断地骚扰下，这600台PC就如同定时炸弹一般，说不定什么时候就会带来一场爆发式的病毒事件。王洪介绍：文峰大世界是一家商业连锁企业，旗下有百货商店、大型卖场、家电专卖店以及“文峰超市”等多种经营项目。但那时，公司还没有采取网络防病毒解决方案，仅仅依靠单机版杀毒软件。而随着网络威胁大规模肆虐，单机版防毒软件根本不能满足企业的安全需求。于是，文峰大世界不得不开始寻求新的网络安全解决方案。

趋势科技整体解决方案，从客户端到网络层打造立体防御

两年后的今天，文峰大世界的网络安全状况有了极大改观，王洪再也不用绞尽脑汁地想办法对付病毒了，而是把精力投入到了企业其他IT建设方面。带来这种效果的恰恰是趋势科技中型企业安全解决方案，包括趋势科技防毒墙客户机/服务器版（OfficeScan client/server version）与趋势科技专家值守服务（EOG），加上趋势科技控管中心（TMCM），以下简称TTD方案。除此以外，为了更严密地防护内网的各个网段，文峰大世界紧接着又部署了趋势科技网络病毒墙（NVWE），最终构成了整体全面的企业安全解决方案。

对于两年来部署趋势科技中型企业解决方案的感受，王洪谈道：“我们的信息部门只有十几个人，分管安全的就更少了。之前的单机版防病毒产品根本让我们对病毒无从下手。而趋势科技TTD方案除了能带来全网段的统一查杀和升级，详尽的报表功能和附加的专家服务以外，更便捷的管理操作平台让管理员从大量复杂的管理和行政工作中彻底解放。如今，我们对病毒情况了如指掌，做到了知己知彼，百战百胜。”据王洪介绍，正是因为有了趋势科技的TTD方案，文峰大世界才躲过了去年“熊猫烧香”的攻击。

趋势科技的TTD解决方案让文峰大世界解决了外患，但是对于内忧——已经流窜在局域网的病毒，也要想办法对付才行。所以，文峰大世界又选择了趋势科技网络病毒墙（NVWE）。NVWE可以保护不同网段和关键服务器群。通过NVWE控制台，管理员可以随意绑定网关，DNS，IP/MAC地址，制定详细的安全策略来过滤网络流量并组织特定文件传输。此外，NVWE还能对客户端设备的病毒状态进行检测。尤其是拦截经常爆发的局域网ARP攻击，NVWE更是一把好手。很多企业都有因为ARP攻击而阻断内外网通信的情况，而文峰大世界在部署NVWE后，一次ARP攻击也没出现过。

现在，TMCM可以对OfficeScan和NVWE进行统一管理，最终让TTD+NVWE的组合发挥出了最大效果。

专家服务+云安全技术 阻击Web威胁

文峰大世界之所以取得良好的病毒防范效果，除了OfficeScan和NVWE安全防护功能，趋势科技专家值守服务（EOG）也发挥了巨大作用。EOG彻底改变了中型企业缺乏妥善监控持续警觉性，遭遇病毒爆发匆忙着手解决现状，客观上解放了IT人员生产力，得以集中主要精力从事主要业务。EOG报表功能可以持续监控观察企业的信息安全健康度，随时掌握状况，最大程度上降低了企业因病毒爆发导致的数据丢失、被窃等风险。

现在，文峰大世界将网络全部交给了趋势科技的专家服务团队来监控，遇到一般状况，几个小时之内就可以得到解决方案。能得到如此快速的响应，王洪也感到很吃惊。随后他了解到，这是因为趋势科技在产品中采用了最新的“云安全”技术。在这套解决方案中的OfficeScan产品内含的Web信誉技术（WRT）就是云安全的核心技术之一。该项技术超越了拦截Web威胁的传统方法，从根本上将含有恶意威胁的网页阻挡在企业网络之外，在恶意信息侵入网络之前其进行阻止，从而达到零接触、零感染的防护价值。这种全新的方法降低了客户网络和端点的带宽消耗，提供了更快且更全面的及时保护。对于文峰大世界来说这也同样重要。

目前，趋势科技的“云安全”，在全球架设了3万4千多台服务器，拥有超过1000位的安全专家，在全球建立了5个数据中心，拥有99.9999%的可靠性。云安全可以支持平均每天50亿笔点击查询，每天收集分析2.5亿个样本，资料库第一次命中率就可以达到99%。借助云安全，趋势科技现在每天阻断的病毒感染最高达1000万次，这也是WRT的基础所在。

对于“云安全产品+专家服务”这种最新的反病毒模式，王洪说：“这种模式即让安全产品发挥出了最大价值，又让我们IT部门不用整天疲于应付病毒，将复杂问题交给更专业的人来处理。”王洪认为，最好的安全解决方案是让用户感受不到安全产品的存在。尤其是执行病毒扫描时，对带宽的占用不应该有明显的察觉。据了解，文峰大世界IT部门的下一步工作将是把重心放到了通过定期的报表研究防范病毒的重点，做到有的放矢，让自己的网络环境更加纯净。