为国际一流口岸构建智能安全的信息网络

——趋势科技 TDA 护航上海出入境检验检疫局信息网络

上海出入境检验检疫局（以下简称上海局）作为国家质量监督检验检疫总局设在上海口岸的直属机构，其较高的网络容量和负载形成了庞大而复杂的网络结构。为切实保证上海局信息化业务系统能够安全、持续、高效的运行，稳步推进和加强网络信息安全的保障力度，上海局自 2009 年底起开始启用趋势科技 TDA（威胁发现系统）产品，并在 2010 年中国上海世界博览会（以下简称上海世博会）期间利用 TDA 技术增强对内网终端漏洞与威胁的实时监管，完成原有系统的升级工作，最终确保了上海世博会的顺利召开。

蠕虫肆虐 阻塞数据通道

上海出入境检验检疫局是国家质量监督检验检疫总局设在上海口岸的直属机构。据了解，随着上海局信息化应用整体提升和业务系统融合，客户端和服务器的数量在近几年中大幅增长，目前整个 IT 环境已经拥有近 3000 台终端和由上百台服务器组成的数据中心。上海局所有的下属分支机构、办事处、口岸查验点等都通过专线的方式连接到上海局本部的数据中心。

上海世博会提出了打造“生态世博”、“绿色世博”的总体思路，而各国主题馆的设计或多或少均涉及引进植物等需求，甚至还有展示本国特色的动物。在履行检验检疫保障职能的同时，上海局需要全力以赴为上海世博会提供检验检疫优质服务和便利措施。

据上海局信息中心的技术人员介绍：“为不断提高网络系统的安全防护能力，抵御推陈出新的网络安全攻击，信息中心在所有网络专线的接入端增设了防火墙与 IPS 等安全控制设备。但由于网络故障往往是客户端病毒的交叉感染所致，加之部分员工的安全责任意识不到位，病毒很容易通过这些途径入侵内网，致使传统的安全设备无法全面确保网络的信息安全。尤其是 ARP 蠕虫病毒及其变种、ARP Spoofing（ARP 黑客攻击）等一并严重威胁着上海局及各分支机构网络安全，此类病毒感染源大多较为活跃且安全攻击行为较为分散，这不仅增加了上海局寻找和查杀病源的难度，而且严重影响了上海局业务的正常开展。

针对这些威胁，为避免突发事件可能造成的严重影响和巨大损失，进一步确保网络安全故障得到及时有效的处理，上海局更需要一个较为全面的网络安全检测产品，以便增强对相可疑威胁的检测能力，还希望能够通过病毒扫描分析可疑事件的内容，达到深层次的威胁检测，获得完备的安全防护解决方案。

云端联动　打造高效智能防护

当前，传统杀毒软件最大的问题就是“被动防护”。也就是说，杀毒软件的病毒库更新前，对于新的病毒或是病毒变种基本没有查杀能力。同时，也有很多网络版杀毒软件在发现病毒无法清除时，缺少相应的应急与防护能力。甚至一些用户本认为安装杀毒软件和升级病毒库就可以防止感染病毒和抵御攻击，但实际情况却并非如此。因此，抑制新病毒特别是蠕虫类病毒的爆发存在一定难度。

上海局专家在对网络安全市场上多个知名企业生产的 NIDS（Network Intrusion Detection System，即网络入侵检测系统）产品和防毒软件进行评估后认为：“安全设备的高防护性能是上海局的重要需求。以上海局的实际情况，产品的价格、性能等多项因素为评估标准，趋势科技的 TDA 和 OfficeScan 组合在实现与终端的防毒软件的动态联动，主动发现威胁并提前告警，快速调用和执行防毒软件的配置策略等方面具备一定的优势，使技术人员能够更有针对性的开展积极的防御工作。”

上海局信息中心技术人员还告诉记者，“从 2009 年底至今，通过使用趋势科技的 TDA 产品，已经逐步改善了部分网络应用的稳定性，由恶意软件所引发的困扰也有所降低。因此，上海局分别在世博办事处、外高桥局等下属分支机构的网络中部署了 TDA，用于对移动终端的威胁监测，及时升级系统漏洞补丁，为未安装防毒软件、防毒代码过期的设备进行更新。”

趋势科技的 TDA 产品在上海世博会期间发挥了实效，通过发现造成网络中断、消耗大量带宽或未经授权应用程序和服务程序，阻断了来自外网的病毒干扰，在满足世博大量业务安全保障需求的同时确保了世博物资检验检疫通关系统的运转效率。据进一步了解：“根据 TDA 提供的智能策略建议，通过与趋势科技云安全产品 OfficeScan 的联合使用，上海局的直属分支机构外高桥局在部署 TDA 的一个月里，日志报表中记录的网络高危行为和病毒数量统计由‘5 位数字’下降到了‘3 位数’以内。”

借助趋势科技灵活的安全策略，网络威胁达到了成倍降低的效果。这与 TDA 集成了趋势科技云安全中的“多协议关联分析技术”和 OfficeScan 集成了“云客户端文件信誉（Cloud-Client File Reputation，CCFR）”云安全技术密不可分。TDA 可全面检测网络中的 7 层恶意威胁，网络安全一旦受到病毒的侵犯，TDA 和 OfficeScan 就可以通过云端的 Smart Protection Network 形成统一的动态联动管理。尤其是对上海局这种大型网络，TDA 可自动形成反映全局安全形势的总体视图，通过集中管理界面帮助上海局信息中心应对紧急事件响应，并能在更详细的交互式报表中形成更加颗粒化的补救措施和改进建议。