[趋势科技成功案例]

江苏省移动将安全威胁阻断于源头
趋势科技 TDA 构建全方位威胁预警系统

在大型或者超大型网络中，必然存在着一些安全威胁让 IT 运维部门防不胜防，要在动态变化中找到这些威胁来源绝非易事，这就如同“大海捞针”。江苏省移动呼叫中心作为非常典型的电信行业大型网络用户，在全面提高用户体验感的同时，为全面消除异常流量和应用层漏洞，携手全球服务器安全、虚拟化及云安全领导厂商——趋势科技，并使用趋势科技威胁发现设备 TDA 6000，通过全网监控和定位 2~7 层的网络可疑活动，将威胁消灭在萌芽状态，大幅降低了日常安全管理的压力。

内部威胁“闹腾”不断 传统 IDS 力不从心

据了解，江苏省移动呼叫中心的网络终端数量大致在 1000~2000 台左右，服务器超过 200 台，为突出“稳定性”和“安全性”的需求，所有的链路、核心层、汇聚层设备都是双冗余设计。另外，针对病毒和内网交叉感染的问题，江苏省移动呼叫中心在客户端部署了防毒软件，并购置了 IDS 系统来保护办公网，但传统的 IDS 对于电信行业大型的网络来说， 明显力不从心。由于无法满足数据流量巨大、网络覆盖范围和结构复杂的需求， IDS 的误报和漏报问题开始显现出来。

据负责江苏省移动呼叫中心网络安全的王先生介绍：“由于网络庞大的客户端和服务器资源存在，网内高危漏洞监测的工作量极大，ERP、OCS、CRM、BSS、MSS 以及高清视讯等多域环境中随时都可能遭受到来自内部威胁的攻击。内网终端威胁日益变化，因此，传统的 IDS 厂商必须为不同业务平台开发不同的程序，那么就会给这些威胁充足的恶化时间。虽然构建了铜墙铁壁外围，但等内部威胁一旦升级到‘事故’，全副武装网络也架不住病毒和恶意代码的‘闹腾’。”

为确保业务平台稳定和数据保密性的要求，江苏省移动呼叫中心在呼叫中心的安全建设上投入巨大，不但采用双冗余设计、建立备份中心、为各个网络出入口处增加多级防火墙设备，还购买过多台 IDS 安全产品。但以上这些防护措施，并没有减轻 IT 运维人员的工作量，反而随着终端数量的不断增加，让人力成本节节攀升。

“串路”设备难挑重任 潜在威胁 TDA 法眼可辨

为了迅速消除网络中的安全隐患，防患于未然，江苏省移动呼叫中心邀请了数个网络安全厂商提供解决方案，并加入实地测试。在严格的测试环境中，一批“串”路的安全设备由于无法胜任如此大的通信量负载首先败下阵来，而在随后的实际环境试用中，很多厂商的产品由于无法做到第一时间预警最新的木马和变种病毒，并且无法构建江苏省移动呼叫中心的网络安全整体视图，纷纷被淘汰。最后，根据综合测试结果，江苏省移动呼叫中心认为：趋势科技推出的 TDA 集成了云安全技术、旁路设计、可检测应用层潜在威胁，为呼叫中心的业务发展提供充分的安全保障。

在试用过程中，王先生和趋势科技工程师一起，对于 TDA 功能中 HTTP 访问恶意代码检测、P2P 会话流量管理、蠕虫漏洞扫描等非法流量检测功能都作了模拟攻击测试，而对于这些“威胁”来源定位，TDA 基本上做到“秒”级的预警功能。其次，TDA 可通过“数据包”和“会话”视图对这些主机通讯的数据进行自动关联分析，即从云端数据库进行比较，自动将占用网络带宽的应用和造成网络通讯拥塞故障的信息建立威胁关联。王先生表示：“TDA 的严格控制功能也弥补了江苏省移动呼叫中心之前部署防毒软件的不足，这包括 Web 病毒、跨站木马、视频嵌入恶意软件、非法流量、DNS 劫持等尚未形成交叉感染的潜在威胁，现在利用 TDA 之后，我们可以从海量的数据流中迅速找到被防火墙放过来的漏网之鱼。”

威胁一目了然 云安全轻松化解两大难题

据了解，江苏省移动呼叫中心经过了几次重大的网络融合和升级工作，那么在较为复杂的网络结构和庞大的终端管理上，又应当如何简化管理，降低 IT 维护人员的工作量，从而进一步减少运营成本，提高资源使用效率呢？经过严格测试的 TDA 最终部署在了省移动呼叫中心核心交换机上执行全面覆盖，并在网络安全评估和主动安全运维两大方面解决用户安全管理中的两大难题。

第一：动态网络安全评估，将策略转化为行动

在部署 TDA 之前，江苏省移动呼叫中心已经对外网出口和各级网关设备进行了严格的安全评估工作，在使用 TDA 之后，内网的安全评估（主要是：威胁评估）完全交付给 TDA 去自动执行。由于 TDA 无须安装代理程序，便可自动对服务器和终端进行动态的监测，这大幅节省了运维人员需要每台终端需要安装代理端的工作。其次，TDA 可通过报表的形式显示客户端即时通讯（IM）、P2P 文件共享（BT）、流媒体，以及未授权服务如 SMTP 中继和 DNS 欺骗现象，这是其它 IPS 和 IDS 产品无法相比的。在日常工作中，TDA 为江苏省移动呼叫中心网络中形成“策略执行中心”，它不但能够及时的发现网络环境中的安全威胁，还能够将这些威胁转化为详细的处理措施并进行落实。

第二：安全运维主动出击，服务水平大幅提升

江苏省移动呼叫中心有十几位负责 IT 运维的工程师，但是要应付数千台客户端、200 多台服务器的运维需求，还是显得捉襟见肘。在部署 TDA 之前，IT 部门也都只能在用户电话或者邮件的通知后才能发现已经遭遇病毒的踪迹，IT 部门的服务总是处于亡羊补牢的阶段。Web 病毒、木马、邮件病毒、个人主机漏洞、移动设备交叉感染等等，时常搞得 IT 部门无从应对。而现在，江苏省移动呼叫中心将 TDA 预警和报表信息都纳入到 IT 服务流程中，一旦出现预警信息便会立即启动设计好的事件流程。因此，TDA 便起到了“关键岗位、关键人”的作用。如今，包括 TDA 在内所有安全产品都配合使用了趋势科技提供的 PSP 服务（专属咨询服务），一旦发现未能处理的信息和可疑的流量，都会得到趋势科技技术客户经理（TAM）的电话和现场支持，江苏省移动呼叫中心 IT 服务水平和应急能力也得到了进一步提升。

趋势科技 TDA 由于集成了趋势科技云安全中的“多协议关联分析技术”，因此可全面支持检测 2~7 层网络的恶意威胁。尤其是对电信企业这种大型网络而言，能自动形成映射全公司安全形势的总体视图，通过集中管理界面帮助企业应对紧急事件响应，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。

###

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 1,500 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。