概况

行业
运营商

网站
http://www.js.10086.cn/

简介

目标
江苏省移动呼叫中心希望在全力提高用户体验的同时，全面消除异常流量和应用层漏洞，防患于未然未然，为呼叫中心的业务发展提供充分的安全保障。

解决方案
在经过严格测试之后，江苏省移动呼叫中心将TDA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。

业务影响
- 动态网络安全评估，将策略转化为行动
- 安全运维主动出击，服务水平大幅提升

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

TDA 的严格控制功能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，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。

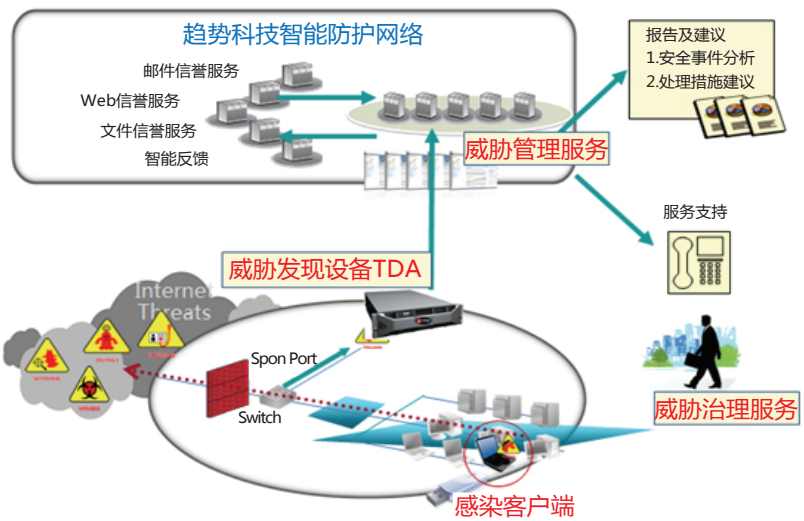
—— 王先生 江苏省移动呼叫中心网络安全负责人

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，在全力提高用户体验的同时，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TDA6000，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

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，为实现“稳定性”和“安全性”的目标，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对于电信行业的大型网络来说，明显力不从心。

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



趋势科技威胁发现系统TDA工作流程图

在数量庞大的客户端和服务器组成的网络中，ERP、OCS、CRM、BSS、MSS 以及高清视讯等多域环境随时都可能遭受到来自内部威胁的攻击，其高危漏洞监测的工作量极大。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提供了充足的恶化时间。虽然构建了铜墙铁壁外围，但等内部威胁一旦升级到‘事故’，全副武装的网络也架不住病毒和恶意代码的“闹腾”。

—— 王先生 江苏省移动
呼叫中心网络安全负责人

“串”路的安全设备由于无法承载如此大的通信量负荷，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，也被逐一淘汰。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等多项功能，可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中的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。另外，TDA还可通过“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，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

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为每台终端安装代理端的工作量。

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部门也只能在用户电话或者邮件通知后才能发现病毒的踪迹，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安全事件时常让IT部门无从应对。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，一旦出现预警便立即启动设计好的事件流程。

因此，TDA起到了“关键岗位、关键人”的作用。如今，包括TDA在内的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的IT服务水平和应急能力也得到了进一步提升。