概况

行业
制造

公司总部
苏州

网点
600多个

简介

目标
欣日兴需要从网络关口上防堵恶意的程序进入到企业的内网；此外，还需要确定相关事件的可疑威胁，利用病毒扫描引擎分析文件内容，达到深层次的威胁检测。

解决方案
欣日兴IT部门通过对网络安全产品的评估，最终部署了趋势科技TDA产品。TDA通过对每一台终端计算机和企业网络状况的整体分析，针对企业的一百多种协议进行深度关联分析，可以识别违反安全策略的终端，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，并提供完善的网络威胁日报、周报和月报信息。

业务影响
- 全面的显示威胁信息，防止病毒“乘虚而入”
- 提前将恶意访问在云端拦截，降低病毒威胁
- 提升了投资回报率

IT经理人如何评估安全产品的ROI？——趋势科技TDA揭开欣日兴迷雾

“TDA能够评估出安全产品投入到网络平台之后的ROI（投资回报率），通过‘（普通的终端使用者停滞工作的时间+网络管理员处理这项事件所用去的时间）×工时工资‘这一公式就可以得到单位时间内ROI的值，然后将这个值累计下来就可以得到这项安全产品的投资汇报率。通过趋势科技TDA，欣日兴已经对大部分的网络应用内部的安全弱点进行了改善，由恶意软件所造成IT部门的困扰情况也大大降低。”

——欣日兴IT部门负责人陈冠宇

对于绝大多数业务都依赖于信息系统的欣日兴精密电子（苏州）有限公司（以下简称欣日兴）来说，能否发现企业中已有的威胁、防止未知和潜在的威胁，将直接关系到企业能否正常运作。目前全球恶意程序已超过1600万个，而且每4秒钟就产生一个新病毒。虽然企业都安装有专门的防火墙或杀毒软件，但是要面对日新月异的网络威胁与黑客攻击手法，这样简单的防御无疑是远远不够的。

欣日兴自1995年起就已是世界上最大的笔记本转轴制造商。如今公司的业务大多靠IT技术平台支撑着，如果没有稳定的IT架构，各项应用系统（ER 、SCM、PLM等）也就无法正常运行。为此，在网络安全管理和建设方面，欣日兴的高层尤为重视。经过仔细的评估，欣日兴最终选择了趋势科技的威胁发现设备（Threat Discovery Appliance，简称TDA），主管IT部门的陈冠宇副经理表示:“TDA可以应用在各种复杂的异构网络环境中，让IT管理人员对企业的安全情况一目了然，让企业网络安全管理变得清晰可控。值得一提的是，TDA还能评估出安全产品投入到网络平台之后的ROI（投资回报率）。”

网络威胁无处不在

作为世界上最大的笔记本转轴制造商，欣日兴拥有600多个网点，服务器有40多台，包括Windows 、Linux和UNIX系统等。而在使用TDA之前，IT部门时常忙于应付各类病毒入侵、恶意代码的骚扰，经过实际排查与分析，发现网络安全故障往往是由于客户端病毒的交叉感染所致，IT部门主管开始考虑如何从网络层面防止这些恶意程序进入到企业的内网中。

随着欣日兴对企业网络安全防护不断投入和完善，使得网络的稳定性开始逐步增强，大范围的病毒感染已经非常少，通过划分VLAN等具体的技术部署，已经尽可能地缩小、降低感染的范围和速度。但如果出现安全事件，IT部门的人员只能充当着“消防员”的角色，依靠个人经验提出安全策略和补救措施。这种方式容易拖延补救时间，也不能确保处理的效果，根本无法形成反映全公司安全形势的总体视图，显示颗粒化的综合威胁信息，这阻碍了IT管理部门有针对性地开展主动防御工作。

“之前在其他公司工作，公司部署的网络防毒系统就是趋势的OfficeScan企业版。当时，亲历了IT部门对网络安全产品评估的全过程，趋势科技的产品在多项指标中脱颖而出，部署方便，使用简捷，整体防毒能力强等综合能力表现突出。经过多年的考验，欣日兴对趋势科技的产品更加信赖。”

——欣日兴IT部门负责人陈冠宇

欣日兴为了实现对企业信息安全威胁进行统一管理，让管理员能够轻松管理IT系统。经过对市场上的产品测试之后，发现拥有网络内容检测技术的趋势科技TDA产品最符合需求。TDA通过对每一台终端计算机和企业网络状况的整体分析，针对企业的一百多种协议进行深度关联分析，可以识别违反安全策略，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，并提供完善的网络威胁日报、周报和月报信息，企业管理员可根据TDA收集提供的反馈报告信息，制订相应的企业网络安全规划。

除此之外，趋势科技的“云安全”技术也成为欣日兴选择TDA产品的关键因素。云安全技术是趋势科技研发的具有跨时代意义的网络安全技术，云安全采用云计算技术将Web威胁采集出来，然后通过在云端的Web威胁信誉库，与用户的Web访问请求进行比对，一旦发现用户请求访问危险网页内容，可以提前将访问在云端拦截。

TDA价值与ROI评估

无论是一项投资还是一款产品，对于企业来说，最关心的都投资回报率ROI。同样，在企业的网络安产品投入中，ROI也是个核心且抽象的问题，往往使得一些企业的CTO和CIO都是很困惑。陈冠宇表示：“在使用TDA之前，一直存在这种困惑，网络可能造成威胁的信息和已经造成的事故是无法进行衡量，在购买安全产品后，并不知道自己的投资有没有带来相应的价值。” 在部署TDA之后,欣日兴的网络安全管理变得清晰可控, 他认为TDA的ROI价值主要表现在病毒的看见性、定位的准确性以及威胁可处理三方面。

可视性：TDA可部署在各个网络层次交换机上执行综合的全面覆盖，管理员通过监控使把网络中的可疑活动都看得一清二楚，从网络层至应用层的多种协议流量情况尽在眼中，TDA可以像“放大镜”一样帮助IT 部门发现网络中的已知、未知威胁和安全问题，从而构建了欣日兴的网络安全预警系统。

定位准：之前一直担心即使发现了威胁，但是无法抓到这些端点。如今，利用TDA基于云安全、智能行为分析和信誉评估技术，通过协议和应用的关联分析，快速定位高危节点和攻击形态。

可处理：TDA对于威胁的处置又分为两个方面。一是TDA在发现和定位之后，将安全威胁转化为详细的处理措施并进行落实。另一方面是趋势科技监控中心的专业服务工程师可对IT 部门“拿不准”的处理步骤，提供详细的处置建议，并根据服务协议提供远程或现场支持。

欣日兴在对TDA半年的实际部署测试过程中，对网络应用内部的大部分安全弱点进行了改善，由恶意软件所造成IT 部门应急响应也大大降低。而TDA的报表功能则将员工每个工时的价值和利用TDA防护到的安全威胁进行比对，假设没有使用TDA，这些威胁已经对系统造成了伤害，那么通过“（普通的终端使用者停滞工作的时间+网络管理员处理这项事件所用去的时间）×工时工资”这一公式就可以得到单位时间内ROI的值，然后将这个值累计下来就可以得到这项安全产品的投资汇报率。陈冠宇特别指出：“这里的ROI是把服务器受到威胁事件排除出去的情况，否则一次服务器的安全事件就可以使TDA的回报率成倍增长。”