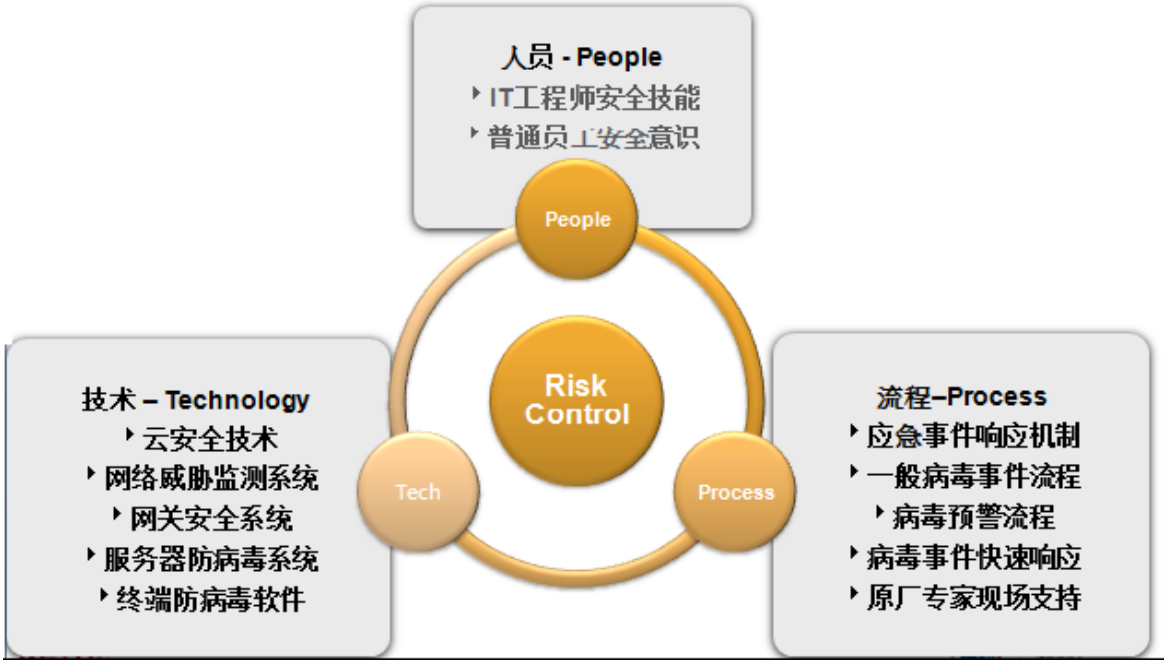
让病毒无处可藏-趋势科技为深圳发展银行构建全方位防病毒体系

深圳发展银行作为国内第一家上市的股份制商业银行，近年来，随着业务的不断扩展，陆续在国内多个城市开设了分支机构，随之而来的是信息化应用规模的不断扩大，日益复杂的网络结构，门类繁多的业务系统以及由此产生的巨大的信息交换量都为病毒的感染和传播提供了温床。如何有效地进行病毒防范，保障生产系统和办公系统的稳定性和可用性，保证总行和分支机构都能得到快速的响应与支持，并建立起更加行之有效的流程制度，成为深圳发展银行密切关注的问题。

趋势科技通过多年与深圳发展银行的合作，针对深圳发展银行自身的信息安全特点，提出了从人员、技术、流程三个方面来进行风险的控制。



打造立体式全方位的病毒防御体系

首先在技术层面上，深圳发展银行在服务器和终端上都部署了趋势科技Officescan企业版网络防病毒软件进行防护，并通过总行的趋势控管中心服务器TMCM对全行的防病毒系统进行管理，保证全行病毒码更新和策略设置的一致性；为了应对日益严重的互联网安全问题，阻止网站挂马和恶意URL地址威胁，在每个分行的网关出口处都部署了趋势科技的网关防病毒产品IWSA，确保用户访问互联网的安全性，减轻管理员在客户端的维护工作量。随着对信息化应用的增加和依赖，深圳发展银行信息科技部门也提出了要将以往被动式的防御模式转向主动式发现、预防潜在的恶意威胁，并在2011年开始引入了趋势科技主动式威胁发现系统TDA（Threat Discovery Appliance）。TDA采用了旁路的部署模式，数量超过20套，

对深圳发展银行总行和各分行网络核心交换机上的网络流量进行扫描监控。由于以前对于异常流量的监控主要依靠抓包工具和防病毒软件的日志进行分析，占用了大量的人力资源，而在采用了TDA后，可快速、高效的识别高危客户端和攻击形态，并通过趋势科技的云安全（Secure Cloud）技术进行智能分析，集中部署在总行总行的TMSP智能分析平台会定期为全行提供威胁评估报告，全面展现目前各分行和全行的网络整体安全状况和安全等级，并针对这些威胁提供安全解决建议。通过TDA的部署，使全行的安全策略得到有效的贯彻落实。

专家专人支持，减轻人员工作负担

有了一流的产品技术保障，还需要有人员的高效配合，在2010年初，趋势科技正式为深圳发展银行提供PSP企业专属服务，包括原厂的技术工程师驻场总行进行各项技术支持和管理维护，并配置专门的技术客户经理进行1对1的后援服务，保证7x24小时的快速响应和顾问服务，以及趋势科技公司在上海的病毒实验室提供2小时病毒应急响应。通过人员保障，一方面更高效地解决各类病毒相关的安全问题，另一方面也将趋势科技多年来在金融行业的成功经验导入到深圳发展银行的信息化运营体系中。

流程保障，降低风险

由于全国分行众多，如何保证在分行出现问题的时候能得到总行有效的支持和资源的合理调配一直是深圳发展银行在与趋势科技合作过程中反复强调的。在引进了趋势科技原厂企业专属服务后，趋势科技对深圳发展银行的服务支撑流程、企业文化、分行人员构成和技术水平进行了充分的调研，并不断与深圳发展银行进行探讨，结合其自身的特点及趋势科技在金融行业多年积累下来的成功经验，设计出对生产网的病毒码更新流程，常规病毒处理的流程，紧急事件响应流程，分行日常巡检流程等规范和制度，用于指导全行防病毒工作的开展。现在，每个岗位的人员都非常明晰自己的工作职责，一旦出现任何问题，也可根据流程规范去找到相应的资源进行解决。而每季度开展的全行防病毒巡检工作利用趋势科技全国的服务支持力量及时解决和发现分行存在的各类安全问题，并提出下一步的工作建议，一年来，原来一直困扰各分行的网络病毒已经得到了有效控制甚至或彻底消灭，而全行的各项防病毒KPI（关键业绩指标）也全面提升。

信息安全领域一直都有一个说法“三分技术，七分管理”，通过趋势科技全方位的产品技术保障，加上原厂服务对流程、人员和管理上的整合，使信息化安全建设体系不断完善，病毒在深圳发展银行的企业网络中得到有效遏制，整体病毒治理工作正朝可控可管方向迈步前进。