云安全智能平台“提前到位”

—— 南京证券携手趋势科技领跑金融安全

趋势科技在虚拟化、云计算安全领域的创新技术和产品，可以让我们脚踏实地，在不同发展阶段达成近期和长远目标。首先，Deep Security 具有出色的防毒能力，而它的无代理特性更可以全面降低服务器防毒系统对内存、磁盘、CPU 的负载消耗。其次，Deep Security 在为现有 VMware 虚拟化平台提供安全保障的同时，已经兼容了更广泛的虚拟化技术，这让我们在对各种虚拟化平台测试和数据中心升级时提供了保障，让安全提前到位。

—— 南京证券总工程师、电脑中心总经理 江念南

南京证券

行业
金融

注册资本金
17.71 亿元

分支机构
62 家

总资产
109 亿元

网站
http://www.njzq.com.cn/njzq/index_road.jsp

简介

目标
为了提高信息安全防护效果，南京证券将信息安全框架进行了调整和升级，并希望引入更加有效的防护套件和硬件产品，让网络、服务器、终端和应用不留“死角”。

解决方案
南京证券选用了趋势科技 OfficeScan 和 IWSA，在终端和网关上都加了一道锁。其结合趋势科技云安全智能防护网络，并通过 OfficeScan+TMCM 组合在病毒管理上实现了集中式管控。

业务影响
- 大大减轻了分支机构的病毒防范和运维工作的压力，人力成本逐步减少；
- 助力实现下一代数据中心运维管理和安全优化目标；
- 有效应对网络安全威胁。

在互联网金融时代，各大证券企业广泛运用以互联网为代表的信息技术，实现经营、管理和服务创新，但愈演愈烈的网络威胁成为了“搅局者”。为此，紧抓机遇、不畏挑战的南京证券选择了最佳的合作伙伴——趋势科技，利用云安全智能平台建起了集中化、立体化、智能化的网络防线。南京证券通过 OfficeScan 和 TMCM（趋势科技防毒墙控管中心）消除端点隐患、利用 TDA 构建威胁发现平台强健网络、部署 IWSA 封堵 Web 威胁入口、采用 Deep Security 独特的“无代理”底层防毒技术构建更安全的虚拟化数据中心，竖起了新一代金融网络安全建设的“风向标”。

网络安全架构全面升级，不留“安全死角”

作为全国创新类证券公司，南京证券是中国人民银行批准设立的江苏省第一家专业证券机构，截止 2013 年 12 月，总资产达到 109 亿元。南京证券以信息化为龙头，拓展了业务经营范围，带动了企业规模的增长，行业影响力不断提升。

在移动支付、云计算、大数据等全新应用环境下，愈演愈烈的网络威胁对证券行业的健康发展产生了负面影响。而对于这些“搅局者”的存在，南京证券总工程师，电脑中心总经理江念南认为：“承载这些业务系统的南京证券数据中心，服务器拥有量超过 500 台，营业部终端数量也至少在千台以上，而我们在严格遵守证监会各项网络风险管理要求的同时，克服了各种难题，采用了更加主动的网络防护方案。但由于证券行业对业务连续性管理的要求非常高，随着网络威胁不断进化，黑客释放的恶意代码也在寻找证券网络中极小的漏洞。对此，南京证券将信息安全框架进行了调整和升级，并希望引入更加有效的防护套件和硬件产品，让网络、服务器、终端和应用不留‘死角’。”

据介绍，信息安全系统建设历来是南京证券重点关注与确保的工作，公司成立了由总裁负责的信息安全领导小组，负责信息安全整体的规划与战略部署。而由总工程师负责的信息安全工作小组，针对核心安全问题不断加强和改造。

由于证券行业对业务连续性管理的要求非常高，随着网络威胁不断进化，黑客释放的恶意代码也在寻找证券网络中极小的漏洞。对此，南京证券将信息安全框架进行了调整和升级，并希望引入更加有效的防护套件和硬件产品，让网络、服务器、终端和应用不留“死角”。

—— 南京证券总工程师
电脑中心总经理 江念南

与趋势科技并肩“领跑”，严防 APT 攻击渗透网络

针对上述需求，南京证券选用了趋势科技 OfficeScan 和 IWSA，在终端和网关上都加了一道锁，其结合趋势科技云安全智能防护网络（Smart Protection Network，SPN）的防护效果令人满意。尤其是在采用 OfficeScan+TMCM 组合之后，南京证券在病毒管理上实现了集中式管控，总部可对分支机构的病毒防范维护、升级等工作统一维护，大大减轻了分支机构的病毒防范和运维工作的压力，人力成本逐步减少。

江念南表示：趋势科技在安全领域保持着高速发展，面对复杂的网络环境和不断发展的 IT 科技，趋势一直在跟进和领跑。另外，在金融和证券业，趋势科技有着丰富的成功案例，较为先进的部署和架构模式，产品线齐全，查杀效率高，系统占用与开销合理，策略灵活，有统一的管理平台，能够为安全管理人员生成详细的数据报表，这使得我们最终选择了趋势科技作为长期的合作伙伴，应对来自各个层面的新挑战。

近期，金融行业 APT 攻击事件屡有发生，而攻击者往往会持续不断地渗透并窃取金融企业的敏感数据，藏匿在内网的恶意程序潜伏周期甚至长达数年之久。为应对这种不易发现但危害巨大的威胁，南京证券对网络威胁管理能力进行了更深入的评估和应急演练。在关注 APT 攻击特点和变化的同时，也希望趋势科技提供更有针对性解决方案，力争做到威胁提前发现。

为帮助用户应对不断进化的安全威胁，趋势科技集成云安全技术，推出趋势科技云安全智能防护平台，平台涵盖了最终用户、服务器、网络三个层面的防护，其中趋势科技 TDA 正是满足上述需求，有效发现 APT 攻击的核心产品。

趋势科技 TDA 具备完善的启发式侦测能力与沙盒分析提示，当恶意程序在网络中传播感染其它用户时，它们就会被打上标记。南京证券将趋势科技 TDA 部署在核心内网，并分别对广域网、DMZ 区、业务外联区等交换机采用了端口映射的形式，成功实现了全网主动化的威胁管理。在进行产品功能测试阶段，TDA 便发现了网络内异常特殊的流量，成功定位出“飞客”蠕虫病毒的攻击源头，并协助管理员迅速做出隔离和查杀处理。

聚焦虚拟化安全，携手进入下一代数据中心

在业务蒸蒸日上的同时，南京证券的数据中心应用也进入新的变革时期，从最初的将分散数据合并集中，到后期的多业务整合、再造业务流程，从虚拟化技术实现资源整合，到关注软件定义（SDN）数据中心的发展引领创新。

江念南表示：在下一代数据中心运维管理和安全优化目标上，我们与趋势科技达成了一致，尤其是趋势科技在虚拟化、云计算安全领域的创新技术和产品，可以让我们脚踏实地，在不同发展阶段达成近期和长远目标。首先，Deep Security 具有出色的防毒能力，而它的无代理特性更可以全面降低服务器防毒系统对内存、磁盘、CPU 的负载消耗。其次，Deep Security 在为现有 VMware 虚拟化平台提供安全保障的同时，兼容了更广泛的虚拟化技术，这让我们可以为各种虚拟化平台测试和数据中心升级提供保障，让安全提前到位。