[趋势科技成功案例]

国海证券携手趋势科技共同抵御高级持续性威胁（APT）

趋势科技多层次、全方位安全加固方案助力证券企业业务快速发展

2012 年年初，国海证券携手全球服务器安全、虚拟化及云计算安全领导厂商——趋势科技，结合证监会颁发的国内证券业安全规范指引，对自身的安全防护体系进行安全加固。通过部署趋势科技提供的多层次、全方位安全加固解决方案，全面提升了国海证券包括网关、网络边界、业务服务器区等 3 个层次的安全级别，完全符合证监会对证券企业安全建设的要求。本次安全加固建设不仅有效加强了国海证券整体安全防护能力，保障了业务的快速发展，并且使得国海证券成为了安全运营管理的行业典范。

管理需求：全国性的网络规模，让管理员难以有效开展安全管理工作

国海证券前身为广西证券，1988 年经中国人民银行批准正式设立。是国内首批设立、唯一一家在广西区内注册的全国性综合类证券公司。2001 年增资扩股至 8 亿元并更名为国海证券有限责任公司。2011 年上市并更名为国海证券股份有限公司。目前，国海证券拥有 5 家分公司和 55 家营业部，超过千台营业终端分布在全国各地，这对于国海证券的安全管理员来讲，如何有效在全国各分支机构实时发现全网威胁，并快速给出针对性的应对方案进行处理是一个难题。另外，由于国海证券的办公网能够访问 Internet，大量的高级持续性威胁（Advanced Persistent Threat，简称 APT）威胁会通过 Internet 进入办公网，严重影响终端用户的正常办公及上网安全，而单纯的网络版防毒软件根本没法有效防御这些来自互联网的威胁，经常反复感染病毒让安全建设工作难以展开。

法规遵从需求：合规性是证券业 IT 安全建设的重点

在网络威胁不断翻新和 APT 越来越犀利的今天，证券企业由于其特殊的行业性质，已经成为各种黑客组织的首选攻击目标之一。为了正确指导各证券企业如何搭建内网安全体系，证监会在 2009 年中旬发布一份行业安全建设规范《证券期货业信息系统安全检查贯彻落实指引》。该指引明确规定各证券企业的安全体系建设必须具备“实时监控、边界防护、保留日

志、定期评估、定期整改。“的要求。

技术需求：传统安全防护方案难以抵御 APT 攻击

APT 是指拥有优秀技术、资金资源的黑客组织或集团，对某些特定的用户发起的有目的、长时间的攻击。由于其攻击前期的准备非常充足且攻击时间、次数相对于传统攻击更多，因此发起的攻击往往无法彻底防御。如中行惊魂 300 秒、某证券企业被发现 APT 潜伏超过 1 年的安全事件都充分反映了 APT 这种特殊攻击的特点。作为最早应用 IT 系统的行业之一，证券行业无论是在基础架构还是应用水平上都处在全球领先的水平。但伴随着网络与业务整合力度的不断加大，网络钓鱼、病毒、木马、黑客都将其攻击矛头指向了证券网络，以从中获取巨额的利益。如最近 2 年，在金融、证券行业发生的多起安全事件，充分证明网络安全已日益成为制约证券企业长足发展的瓶颈。

结合上述 3 点需求，国海证券决定对内网安全体系进行一次全面的加固。为此，国海证券与多家国内外知名的安全厂家进行了长时间的技术交流及产品测试。最后，趋势科技凭借其解决方案最为符合国海证券需求、能够符合国海证券在网络安全高效管理的要求、以及在证券行业有丰富安全服务经验的特点，成为本次安全加固项目的重要合作伙伴，为国海证券安全加固项目提供解决方案。

趋势科技全方位、多层次安全加固方案，协助国海证券抵御 APT 攻击

针对国海证券安全管理专责工程师提到的 3 点需求，结合国海证券现有的安全架构，趋势科技资深技术顾问杨嗣鹃提出以下的安全加固解决方案 :为了全面符合证监会对证券企业的安全建设要求及解决用户在安全管理工作上遇到的难题 ,建议在国海证券现有的安全防护体系下，建立一套从网关到网络的全方位、多层次的安全加固体系。整体安全加固体系如下：

1、 在办公网互联网出口部署趋势科技防病毒网关 IWSA3600，对进出的互联网数据进行安全检查。一旦发现数据中包含恶意代码，立刻阻断，以此解决办公终端用户的上网安全，提高办公效率，且能切断 APT 主要的入侵途径；

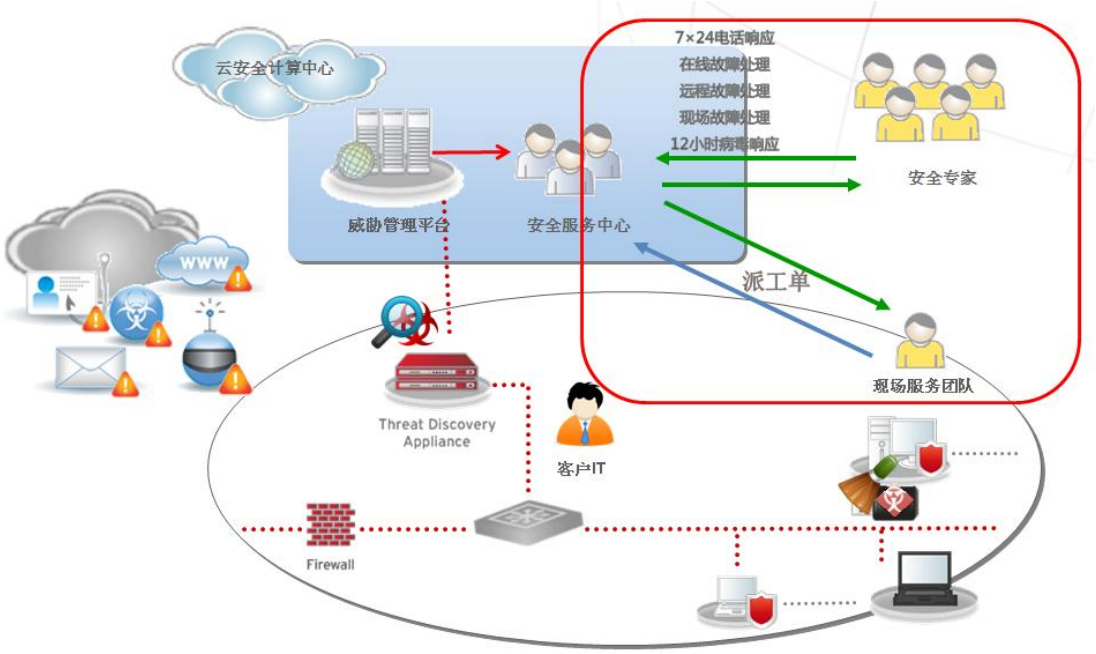
2、 在全网关键边界部署趋势科技威胁发现设备 TDA，对网络中流窜的数据进行深度分析，一旦发现威胁，立刻通过控制台为用户提供预警，并配合趋势科技 EOG 服务对分布在全国各地的威胁源头进行处理。以此解决了用户对于全网安全管理的难题，增加了国海证券的风险控制能力及对 APT 攻击的应对能力；
3、 另外，本次的安全加固方案在安全监控、边界防护、及日志审计方面完全符合证监会对证券企业在应对 APT 攻击方面的安全建设要求，为国海证券通过证监会安全考核提供了有力的保障。

据国海证券的安全管理专责工程师林工介绍："国海证券之所以选择趋势科技的安全加固方案，主要看重了趋势科技两方面的优势：一是趋势科技领先于业界的"云安全"技术，另一个则是趋势科技提供优质的原厂高级服务。趋势科技的"云安全"技术和网站信誉评估技术都是独有的，在方案调研过程中的产品测试阶段，就已经收到了良好的效果，能够快速、准确地发现来自外界的可疑 APT 攻击并提供简单直接的告警提示。再配合优质的原厂服务，更是快速地解决了任何时间点出现的 APT 威胁。

联手趋势科技共同抵御 APT 攻击为国海证券业务发展保驾护航

如今，通过使用趋势科技最新的全方位、多层次安全加固方案，国海证券能够实时发现全国范围内所有的 APT 威胁信息，并能够通过趋势科技提供的原厂高级服务，快速消除 APT 威胁对国海证券的影响。另外，针对互联网威胁的防护，趋势科技提供的防病毒网关 IWSA 凭借其独特的 Web 信誉评估技术，每天为用户拦截大量来自互联网的威胁，确保了终端办公用户的上网安全并提升了办公效率。

林工认为："针对证券行业的 APT 威胁已经被发现在国内部分证券企业内部中传播，目前简单的网络防病毒系统+防火墙方案，根本无法抵御这些 APT 的攻击。必须建立一套全方位、多层次的安全防护方案，才能保障证券企业的安全发展。而趋势科技的安全加固方案，能够为证券企业从网关到网络、服务器主机提供一整套的 APT 攻击防护体系，从而全方位地监控到 APT 威胁在证券企业内部的发展情况，进而有效协助证券企业抵御 APT 攻击，为证券企业的业务发展保驾护航！"



###

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 1,200 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。