趋势科技“云安全”护航渤海证券交易平台

-趋势科技配合渤海证券建立全方位立体防毒体系

证券交易安全关乎国计民生

渤海证券公司总部座落于天津，设有上海分公司和北京办事处。截至2010年12月31日，公司在全国重要省市和地区共有46个证券营业部，成为在全国举足轻重的大型证券公司。

公司秉承“诚信、和谐、高效、共赢”的经营理念、“团队拼搏，创新图强”的企业精神和“客户至上、服务领先”的基本原则，坚定不移地走市场化、专业化、规范化、特色化发展道路，在团结高效的经营团队带领下，坚持守法合规经营，严格控制各类风险，大力拓展各项业务，为客户提供专业化的金融服务。公司将努力把握中央关于加快滨海新区开发开放的历史性机遇，立足天津,面向全国,努力争取成为全国一流券商，以优良的经营业绩回报股东、回报社会。

证券信息系统是证券公司的基础建设，是证券业务正常进行的前提条件。满足基本的安全要求，是网络成功运行的必要条件，在此基础上提供强有力的安全保障，是证券网络系统安全的重要原则。

证券网络内部部署了众多的网络设备、服务器，保护这些设备的正常运行，维护主要业务系统的安全，这些是证券网络的基本安全需求。但网络安全事件频频威胁到证券信息系统的安全，对证券行业的正常运作造成了极大的威胁。无论是有意的攻击，还是无意的误操作，都将会给系统带来不可估量的损失。攻击者可以窃听网络上的信息，窃取用户的口令、数据库的信息；还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，攻击者可以删除数据库内容，摧毁网络节点，释放计算机病毒等等。由于内部工作人员能较多地接触内部信息，工作中的任何不小心都可能给信息安全带来危险。最重要的风险是网络系统风险——证券营业部的计算机系统是构建在一个内部网络平台之上的，利用网络平台使得证券营业部的计算机实现与服务器互连。网络服务器内装有证券营业部所有的交易资料，因此网络系统的安全性至关重要，一旦网络系统被黑客进入，那么证券营业部的交易资料将成为黑客攻击的对象。

面对计算机网络的种种安全威胁，必须采取有力的措施来保证安全。无论是在局域网还是在广域网中，网络的安全措施应是能全方位地针对各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

趋势科技 Officescan“稳”字当头 护航终端

“证券行业是一个实时性非常强的行业，而对于证券公司来说，公司的电脑设备是不允许感染计算机病毒的，一旦设备感染病毒将直接影响用户的实时交易，换句话说，证券交易和交易支持网络需要绝对的安全。”证券公司一般都会将交易网段和非交易网段进行物理隔离，保证没有一台电脑设备是同时横跨交易网段和非交易网段，以此来阻断来自非交易网段对于交易系统的无端干扰，而唯一在交易网段中载入数据的人为途径也会经由证券公司设置各种权限和制度进行遏制。为了避免各种危险，同时保证用户有效的实时性交易，证券公司必须保证公司网络的绝对安全，为此，渤海证券在多方考察下购买了趋势科技防毒墙网络版OfficeScan并成功防毒。

渤海证券公司在采购网络安全产品时首先是考虑安全技术的成熟性。趋势科技Officescan其应用上已经通过了时间的考验，拥有众多。渤海证券选择趋势科技OfficeScan之前，也做了许多选型，和市场上同类型的安全产品做了长期比对，最后觉得趋势科技的产品更适合自己。趋势科技的防病毒引擎以及功效上都比较符合渤海证券对于‘稳’的需求，比如软件的资源占用率比较小。安全产品的作用在于为其他交易设备的使用保驾护航，趋势科技OfficeScan可以满足渤海证券日常业务的安全保障需求，同时也不会影响到业务的进展。”

趋势科技WEB安全网关御毒于家门之外

凭借云安全架构下的WRT（Web信誉技术），趋势科技Web安全网关-IWSA可以在网关处协助渤海证券有效防范来自企业外部的Web威胁，通过分析和验证ActiveX&Java Applet 中含有的威胁，来阻止插件安装式攻击，并且通过URL过滤，避免员工访不良网站，降低法律风险，提高了生产效率。IWSA高性能的扫描方式最大限度地降低了资源占用，也不会对网络造成多少负担。IWSA采用的网络信誉评估技术（WRT）对网页进行实时安全级别分类，以拦截对恶意网站的访问，并凭借灵活的策略和完整的间谍软件数据库实施URL过滤，在网关处阻止间谍软件和其它Web威胁，实现安全访问。Web信誉技术（WRT）是趋势科技最新发布的云安全技术架构（Cloud-Client）的核心技术之一，借助全球最大的域信誉数据库之一，趋势科技的Web信誉技术按照恶意软件行为分析所发现的网站页面、历史位置变化和可疑活动迹象等因素来指定信誉分数，从而追踪网页的可信度。然后将通过该技术继续扫描网站并防止

用户访问被感染的网站。通过Web信誉技术，可以防范恶意程序源头，使用户进入网络前就能够获得良好的防护能力。

趋势科技TDA快速定位威胁，高效避免全方位攻击

渤海证券IT技术部针对上述需求，对网络安全产品市场和最新的技术动向都进行了深入的调研。在针对IDS、IPS和网关型防毒产品进行比对之后，技术部发现趋势科技企业威胁管理解决方案中的威胁发现设备（Threat Discovery Appliance,简称TDA）与这些产品有着本质上的区别。TDA实现了传统安全设备无法实现的多重协议侦测、直接预警分析、零日攻击、未知病毒检测、专门针对内部网络功能设计，以及最重要的根源分析功能等。由于证券公司的网络分为了互联网、办公网和交易网3大网段，为了更好的保障交易系统的稳定运行，IT技术部将TDA 6000放在交易网的核心交换的位置，并通过端口镜像的功能实现了透明接入。

据了解，由于高级持续性威胁（Advanced Persistent Threat，APT）的广泛出现，极可能造成证券企业数据中心业务数据泄露和交易系统的影响，因此越来越多的金融和证券企业开始对 APT 高度关注。证券公司及时对 TDA 的引入，有效地避免了员工和高级主管个人电脑被恶意代码植入的风险，在第一时间将这些威胁“扼杀在摇篮之中”，从而降低了交易网和数据中心的风险防御压力。

随着渤海证券在对自身安全体系不断加强的同时，IT 标准化运维的项目也在加紧实施过程中。在 IT 标准化运维中（如：ITIL、ITSM、BSM），安全服务等级、事件流程、控制台中都缺少不了预警和监控系统的支撑。由于 TDA 可以实现将预警和报表信息都纳入到证券公司的 IT 服务流程中，一旦出现预警信息便会立即启动设计好的事件流程。因此，TDA 就可起到了“关键岗位、关键人”的作用。同时，由于证券公司整体的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，在此基础上，渤海证券还可以得到趋势科技专业工程师的电话和现场支持，服务水平和应急能力也得到了进一步提升。

由于趋势科技大力推行本土化政策，并建立了相应的针对中国地区的病毒研发中心以及响应中心，大大提高了对于中国本土病毒的防范能力以及响应速度，在使用了一年多趋势科技安全产品后，渤海证券给出了高度评价：“趋势科技产品的病毒库更新速度很快，同时，技术人员的配置以及响应速度方面令人非常满意。由于渤海证券除了天津本地的网点外，其他营业部网络也需要售后服务方面的支持，异地网点发生安全隐患，趋势科技的技术人员也都能够及时的相应并解决问题。”