



趋势科技成功案例



趋势科技 Deep Security 让虚拟化“既稳又快” 助力中信证券实现业务连续性管理

作为提升信息化效率、降低成本的重要手段，虚拟化是每一个企业在信息化道路上所必需跨过的一道门槛。为了全面推进虚拟化进程，避免安全失控的风险，中信证券股份有限公司（以下简称：中信证券）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，采用无代理特性的趋势科技 Deep Security，全面化解虚拟机防毒扫描风暴（AV Storms）难题，在虚拟化安全统一管理平台上实现了更稳、更快的目标，让业务连续性管理（Business Continuity Management，简称 BCM）水平不断提升。

稳定第一，但不能放弃“性能”

作为一家知名的全国性综合类证券公司，中信证券在统一营业部系统、开通网上交易、实现广域网连接、数据中心虚拟化等方面，都在我国证券行业处于“旗标”位置。随着中信证券对虚拟化技术的深入探究，信息技术中心对自身的 IT 基础架构进行了虚拟化改造，在北京、深圳、青岛三大数据中心搭建了虚拟化平台，并将测试网中大部分服务器迁移到了 VMware 虚拟化平台。

在坚持守法合规经营、严格控制各类风险的规划目标下，中信证券对应用测试环境的部署效率，以及测试与生产环境一致性的要求变得越来越高。而在 40 多台 VMware ESX 服务器上，既要实现 1:50 的虚拟机密度，又要同时保护千余台虚拟机的安全运行，这让运维部门工作压力越来越重。

据中信证券信息技术中心的工程师介绍：稳定第一，但不是说我们会放弃性能。虚拟化系统在响应速度和性能方面的表现，将直接关系到最终用户在使用相关服务时的用户体验，这可以说是中信证券服务质量中最重要的一环。但由于传统防病毒软件不是针对虚拟化而设计，虚拟机上安装传统防病毒软件后，当所有的虚拟机进行预设扫描时，VMware 虚拟化平台的 CPU 利用率、I/O 读写等都变得非常高，访问延迟让人无法接受。因此，虚拟化安全已经变成了网络中的防护弱点，更是保障业务连续性不得不面对的挑战。

聚焦“无代理”特性，Deep Security 屡立战功

对中信证券来说，提前一步发现了虚拟化防毒可能带来的“性能锐减”问题，对全面推进、并最终在生产网络上实现虚拟化架构则是“一件好事”。这可以提前把虚拟化安全风险降至最低，让安全策略与防毒管理提前适应架构的变化。为此，中信证券对市场上所有防毒软件的功能进行了综合评估，同时也与 VMware 厂商的资深工程师对原有传统病毒防护软件“不适应性”进行了分析。最终，中信证券信息技术中心将目光锁定在基于无代理特性的趋势科技 Deep Security 身上。

首先，趋势科技 Deep Security 的无代理防病毒解决方案集成了 VMware 的 vShield Endpoint 技术接口，使 VMware 虚拟化平台上的所有虚拟机无需安装任何软件就能对病毒、间谍软件、木马等威胁进行查杀；其次，Deep Security 有效降低了虚拟机并发全盘扫描、病毒库更新时对 VMware 虚拟化平台产生的大量资源消耗，不存在防毒扫描风暴（AV Storms）的问题；最后，管理员不但可以利用 Deep Security 发现藏匿在虚拟网络中的恶意流量，同时还可以利用 VMware vShield 技术来保护处于运行状态和休眠状态的虚拟机。

据了解，中信证券为保障生产网万无一失，首先在测试网部署了 Deep Security，并对 Deep Security 的防护效果、性能、稳定性及兼容性进行测试评估，为虚拟化推至生产网络做好了准备。从 2012 年底至今，Deep Security 稳定运行并在测试网中屡次“杀毒立功”，而 Deep Security 进行杀毒时所占资源比使用传统防病毒软件有明显减低，随着虚拟机数量的增加，性能方面的优势则更加明显。

正因如此，中信证券信息技术中心对 Deep Security 的防毒效果给出了极高的评价：“Deep Security 为我们提供了防恶意软件、Web 信誉、防火墙、入侵阻止、完整性监控和日志检查，在简化安全操作的同时，大幅提升了虚拟化项目的投资回报率。这些都让我们可以彻底走出虚拟化的尝试阶段，可以最大限度的设计虚拟机密度。未来，中信证券将采用 Deep Security 的虚拟补丁功能，来解决防护间隙（Instant-On Gap）的难题，让更多的业务、更多的应用汇聚于新一代的虚拟化数据中心。”

###



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 1,500 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。