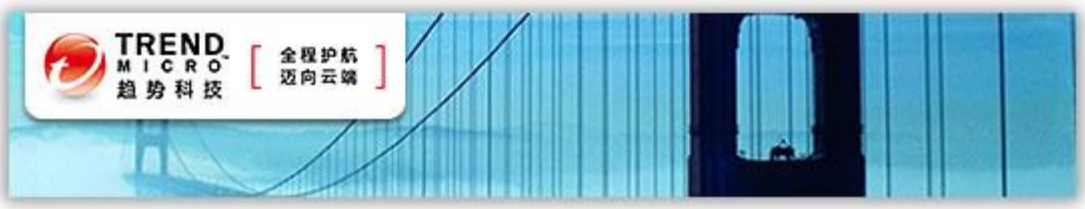

[趋势科技成功案例]

趋势科技助力湖南移动绿色 IT 之路
Deep Security 形成虚拟化平台“保护盾”

能耗问题已经成为中国移动头疼的一件事情，而虚拟化不但可以提高服务器工作效率，更能从根本上解决这个问题，这吸引着中国移动对其进行了多方试点应用。中国移动通信集团湖南有限公司（以下简称：湖南移动）作为虚拟化应用的先头部队，希望通过虚拟化技术降低整个数据中心的能耗，同时对服务器资源进行有效的整合。但是，在将该项技术大规模推广前，虚拟化新环境中的威胁防御与病毒管理成为了难题。

为了在虚拟化环境中保证安全，为中国移动云计算的整体战略提供有效支撑，湖南移动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，通过趋势科技服务器深度安全防护系统（Deep Security）冲破了虚拟化防毒性能瓶颈，为全面推动虚拟化平台应用系统整合，加速绿色 IT 建设做好了必要准备。

节能减排之路 虚拟化防毒出现“排斥”现象

湖南移动是湖南省第一家在香港和纽约上市的通信运营企业，在省内 14 个市州设有分公司。主要负责湖南省内移动通信网的规划、建设、运营管理和经营全省移动电话语音、数据业务。同时，湖南移动的信息化建设也一直以来充当着整个集团技术创新先锋兵的角色，早在 2008 年，湖南移动便率先建成了全国第一个统一信息平台。

为了响应国家节能减排，绿色 IT 的号召，同时充分利用现有服务器的资源。在 2011 年，湖南移动首先对内部 OA 等应用系统进行了虚拟化迁移。为了确保业务系统的正常运转、数据不被病毒入侵，削弱服务器可能被黑客攻击的潜在威胁，湖南移动首先谨慎的对市面上的所有防病毒和服务器保全系统进行了调查和试用。但意想不到的是，在测试过程中，发现这些基于物理主机上运行的传统防毒软件，到了虚拟化服务器上便出现了极为严重的“排斥反应”。

湖南移动公司负责网络安全的刘工表示：“使用虚拟化技术，将分散在不同服务器的应用系统整合，将服务器物理资源转化为资源池，可以确保我们的新业务对数据服务猛增的需求，并大幅减低空间占用和电力能耗，所以虚拟化是 IT 创新的必经之路。但由于传统的防毒系统不是针对虚拟化安全研制的，所以一旦其在虚拟服务器上运行，会同时扫描服务器或者系统，抢占 CPU、内存、I/O 三项主要资源。不但在测试平台，我们在已经迁移的 OA 系统中也已经开始发生了影响业务系统访问缓慢的问题，客户端访问会时常出现不稳定的‘延迟’现象。所以，必须要找到新的‘保护盾’，我们才能放心的把 BOSS 运营系统和 VAS 增值业务系统也迁移到虚拟化环境中。”

Deep Security 形成虚拟平台“保护盾” 安全防护永不中断

据了解，之前，湖南移动使用的病毒防护解决方案都是安装 Agent 代理程序到虚拟主机的操作系统中。但是服务器虚拟化的目的是整合资源，最大化的发挥服务器资源的利用率，而传统的防病毒技术需要在每个虚拟主机中安装程序，例如：一台服务器上跑 20 台虚机，传统方法需要安装 20 套 Agent，在扫描时就需要消耗虚拟主机的计算资源，没有达到节约计算资源的效果，反而增加了计算资源的消耗，并且在病毒库更新时带来更多的网络资源消耗。另外，现在操作系统和应用程序的安全补丁多得举不胜举，一旦安装完补丁程序就需要重新启动服务器，导致服务中断这让湖南移动的 IT 部门伤透了脑筋。

针对传统防毒软件产生的防毒扫描风暴（AV Storms）问题，以及安全补丁需要频繁启动服务器的困境，湖南移动的 IT 部门协同一些外聘的技术专家、VMware 厂商的资深工程师对原有传统病毒防护软件的缺点进行了分析，并重点圈定了专门针对虚拟化平台研发的产品。由此，趋势科技基于无代理特性的 Deep Security 被列为首选对象——作为全世界第一套专为虚拟化环境设计的恶意软件防护解决方案，趋势科技 Deep Security 在一台物理主机的底层实现多台虚拟主机的“保护盾”功能，虚拟机内无需安装 Agent 代理程序，就能在这个保护盾上运行起所有的威胁防护功能。

趋势科技与 VMware 公司在虚拟化产品上的深度合作和市场反馈消除了湖南移动在长期 IT 规划中对兼容性的顾虑。据介绍，在测试阶段，同等硬件配置的服务器上，采用趋势科技 Deep Security 的物理服务器在性能上要比安装传统防毒软件的服务器提升 3 倍以上，而且虚拟机密度也可大幅增加，真正起到了节能减排的设计。在正式部署 Deep Security 之后，利用了趋势科技云端为基础的自动化事件白名单功能，IT 部门可以根据实际情况设定可信赖的事件，极大地减轻了安全事件分析的工作压力。另一方面，一旦工程师发现可疑的漏洞和入侵攻击，Deep Security 能够自动屏蔽漏洞，还可以通过 Deep Security 提供的虚拟补丁（Virtual Patch）功能在几分钟内将防护策略推送至所有服务器上。与传统方式不同的

是，使用 Deep Security 虚拟补丁功能安装补丁，湖南移动不需重启虚拟机系统，保证技术应用的安全性和持续性共存，这完全符合湖南移动通信服务连贯不间断的特殊需求。

虚拟机密度大幅提升 绿色 IT 之路有保障

在 Deep Security 实施完毕后，湖南移动的 IT 部门将其与 VMware vCenter 进行了整合。并对 vSphere 虚拟机上的操作系统和应用系统进行了实时监控，与原有的 IT 运维系统一起构成了一体化的安全运维平台。

湖南移动的刘工表示："开始筹建虚拟化时，我们唯一担心的就是安全防护可能在虚拟化之后失去平衡。而通过与趋势科技的合作，我们完善的解决了这一问题。经过一段时间的应用，我们对于趋势科技的 Deep Security 安全产品的功能表现非常满意，它不仅可以在服务器上实现深度安全防护，抵御病毒感染、非法入侵、数据泄露等恶性事件的威胁，还可以让 IT 运维工作轻松自如的对接在虚拟化和云计算等新技环境之中。同时，由于大幅降低了服务器负载，虚拟机密度完全达到设计指标，让绿色 IT 的理念真正付诸于实践。"

###

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。

更多媒体垂询，敬请联络：

趋势科技（中国）有限公司
刘婷婷
电话：010-85252277
电子邮件：angela_liu@trendmicro.com.cn

北京谋信传习广告有限公司
那罡
电话：010-67047822
电子邮件：nagang@ctocio.com