



[趋势科技成功案例]

中国电信山东分公司

行业

电信

公司总部

北京

光缆总长度

50 万芯公里

下辖市分公司

17

网站

<http://sd.189.cn/>

简介

目标

山东电信希望通过部署安全解决方案，解决虚拟化和云计算平台中常见的“启动风暴、防毒风暴、升级风暴”三大难题。

解决方案

山东电信在先期转移到虚拟化平台上的测试平台中安装 Deep Security，并利用其独有的无代理技术来防范病毒。接下来，通过 Deep Security 提供的虚拟补丁（Virtual Patch）功能，为呼叫中心和营业厅桌面系统建成了统一的补丁部署架构。

业务影响

- 避免了防毒软件抢占 CPU、内存、存储 I/O 和网络拥堵的情况发生
- 建成了统一的补丁部署架构，在安全和效能上实现了最佳的平衡
- 避免了防护间隙的发生，使防毒性能获得最大化的提升

引语：

任何一项创新的技术都有着两面性，服务器和桌面虚拟化防毒遇到的性能瓶颈充分证明了这句话。在没有跨过这个阻碍之前，很多用户（包括使用 iPad 访问公文流转系统的领导）甚至因为虚拟桌面‘蜗牛一样的速度’决定放弃这个新应用，返回物理桌面。在这个关口上，我们通过部署趋势科技 Deep Security 成功化解了这个瓶颈，并走向一条成功之路。

——于先生 山东电信 IT 技术负责人

引语

由于 VDI 架构需要将映像文件放在刀片服务器上运行，如果在每一个映像中安装传统的防毒软件，几百台终端同时扫描病毒会造成服务器异常缓慢甚至瘫痪，这就与虚拟化的初衷背道而驰了。此外，传统的防毒软件在处在休眠状态下的虚拟机中无法进行病毒代码和补丁更

新。为了解决以上问题，同时不影响系统性能，我们必须寻找一种新的防毒解决方案，确保桌面终端虚拟化的项目能在所有的营业厅推进。

——于先生 山东电信 IT 技术负责人

## 山东电信破解虚拟化“三大风暴”有妙招 趋势科技 Deep Security 大幅特性云端性能

随着云数据中心、服务器虚拟化、桌面虚拟化等技术的发展，我国各大运营商都开始广泛吸收云计算和虚拟化技术带来的 IT 创新价值。其中，中国电信集团公司山东省电信分公司（以下简称：山东电信）在落地云桌面等项目中携手趋势科技、VMware 等国际领先的 IT 企业，在深入研究虚拟化产品特性和大量负载测试的基础上，通过趋势科技服务器深度安全防护系统（Deep Security）“无代理”防毒技术的部署，化解了虚拟化和云计算平台中常见的“启动风暴、防毒风暴、升级风暴”三大难题。

### 做好山东电信的中流砥柱 云和虚拟化带来创新良机

云计算在通信业界广受关注，但在运营商中实际落地、并取得优秀应用效果的案例并不多见。山东电信作为中国电信集团公司的直属分公司，已经搭建并完善了 BSS、OSS、MSS、EDA 等各领域系统，主要包括 CRM、在线/离线计费系统、综合结算系统、网上营业厅系统、综合资源管理系统、ODS 系统、经营分析系统、OA 及门户系统等，积累了可观的 IT 基础资源，而 IT 部门正是支撑这种庞大业务体系的中流砥柱。

山东电信 IT 技术负责人于先生表示：“面向纷繁复杂的业务需求，IT 部门需要具备快速开发、测试和响应的能力，并能将其尽快部署。而传统的方式都是在各应用中单独部署服务器，从业务部门提出需求到最终部署一台相应的业务应用服务器，这个过程有时候长达几个月，并且形成了一个孤岛式的‘应用烟囱’。再加上需要频繁在呼叫中心营业厅桌面系统上各种应用软件、补丁，这给 IT 管理人员的维护工作带来了前所未有的挑战。”

显然，传统上的这种服务器各自分立、桌面系统单点维护的 IT 基础架构已经不能适应山东电信的业务发展需求。为迎合国家和集团绿色 IT 建设的规划，同时在硬件性能和投资成本的限制下提升 IT 系统综合能力，山东电信开始逐步采用 VMware 虚拟化技术来升级原有的 IT 基础架构，整合现有的 IT 软硬件资源，以此提高资源利用率、改善 IT 系统性能和灵活性、降低运行维护成本。

## **虚拟化风暴来袭 从防毒入手破解难题**

在服务器方面,通过采用 VMware 云基础架构解决方案,山东电信实现了 IT 架构的全面优化升级,提高了 IT 资源的利用效率,降低了服务器管理和运行维护成本。例如:通过将物理机迁移至虚拟机平台,实现了快速的环境变换;利用 VMware vMotion 技术,实现了服务器资源的灵活调度和管理,提高了应用部署速度。

在桌面管理方面,为了提升营业厅、呼叫中心终端桌面管理的效率,山东电信开始尝试借助 VMware View 实现操作系统、应用和用户数据虚拟化,为终端用户提供新一代的桌面服务。但是,任何一项创新的技术都有着两面性,在服务器和桌面虚拟化技术提高兼容性并简化管理的同时,却遇到了安全、防毒管理的难题。

以虚拟桌面基础架构 (VDI) 为例,非常有代表性的“三大风暴”开始在试点营业厅和呼叫中心出现,它们分别是:启动风暴、防毒风暴、升级风暴。经过对网络和存储系统的重新规划之后,“启动风暴”得以解决,但防毒、升级风暴却依然存在。

山东电信的 IT 部门通过与 VMware 厂商的专家沟通,将目标聚焦在与 VMware vShield Endpoint 集成度最好的趋势科技服务器深度安全防护系统 (Deep Security) 上,并通过后续的实际应用,证明了 Deep Security 的无代理特性和虚拟补丁功能完全可以解决 AV 风暴和补丁管理难题。

## **虚拟化防毒性能问题迎刃而解 虚拟桌面前景无限**

Deep Security 提供了一种全方位服务器安全平台,这使山东电信可以自行量身定制安全方案,具体功能包括了防恶意软件、防火墙、IDS/IPS、Web 应用程序防护、完整性监控和日志检查在内的无代理防护和基于客户端的防护。作为一整套解决方案,其最大价值在于提升虚拟化和云项目投资收益率的同时简化安全操作,尤其是在不影响业务中断的环境下,以最低的成本使用紧急的虚拟补丁保护核心应用程序,并防止数据泄露事件的发生。

在没有使用 Deep Security 之前,为了防止病毒入侵和数据泄露的事件发生,山东电信的 IT 部门在每个虚机和镜像文件中都安装了防毒软件,而每台虚机中的防毒软件启动和扫描就要占去 40% 的内存限额。而在部署趋势科技 Deep Security 后,服务器威胁防御、桌面虚拟化管理效能都得到了提升,VMware 桌面虚拟化项目得以如期、顺利实施。

首先,山东电信在先期转移到虚拟化平台上的测试平台中安装 Deep Security,并利用其独有的无代理技术,以最低的资源消耗,成功的避免了防毒软件抢占 CPU、内存、存储 I/O

和网络拥堵的情况发生。接下来，通过 Deep Security 提供的虚拟补丁 ( Virtual Patch ) 功能，为呼叫中心和营业厅桌面系统建成了统一的补丁部署架构，在安全和效能上实现了最佳的平衡。

对于最新发现的漏洞，Deep Security 能够在第一时间提供修补程序，在无需重新启动系统的前提下，即可在数分钟内将这些规则应用到所有使用了 Deep Security 解决方案的虚拟桌面上。更重要的是，趋势科技 Deep Security 不但可以对物理服务器上的操作系统、应用程序和数据进行防护，还可以保护处于运行状态和休眠状态的虚拟机。据介绍，通过无代理技术的虚拟补丁功能，山东电信的虚拟化和安全管理人员完全避免了防护间隙 ( Instant-On Gap ) 发生，并在 Deep Security 集中式控管平台中获得最大化的性能提升，保证了操作的灵活性。

由于 Deep Security 无代理特性具有可完全释放云端服务器性能压力等优势，山东电信 IT 部门领导及其团队对于其给予了高度评价。未来，山东电信还计划进一步提高虚拟化的比例，整合 NOC、增值业务，统一建设 IAAS 云计算和资源池，基于现有平台构建云桌面系统，利用云计算技术提升呼叫中心、客服系统的服务效率。

###

### **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](http://www.trendmicro.com.cn)。请访问 Trend Watch：[www.trendmicro.com/go/trendwatch](http://www.trendmicro.com/go/trendwatch) 查询最新的信息安全威胁的详细资讯。