“无代理”防毒助力广东电信虚拟化全局拓展

—— 趋势科技Deep Security 9“多租户”支撑资源池管理

“使用趋势科技专门对虚拟化安全环境开发的Deep Security，并利用其独有的‘无代理’和‘多租户’安全防护方案，能够有效解决统一资源池安全管理上的三大难题，扫除了阻碍统一资源池发展的安全障碍，为广东电信统一资源池建设提供了有力的保障和强大的支持！”

—— 广东电信IT运维管理部门 梁先生

概况

行业
电信

公司总部
广州

下辖市分公司
21个

总资产
近**1000**亿元

网站
http://gd.189.cn/

简介

目标
广东电信希望应对服务器在虚拟化环境中不断涌现的安全挑战，在统一资源池建设后积极拓展云计算业务，开拓新的业务增长点。

解决方案
广东省电信通过支持最新“多租户”安全管理的趋势科技服务器深度安全防护系统（Deep Security），以及独有的“无代理”防毒技术部署，完成了安全可信的业务网统一资源池建设，发挥了**VMware ESX**平台虚拟化性能与成本优势。

业务影响
- 使统一资源池虚拟化密度提升**2.5**倍；
- 加快了统一资源池推广进程；
- 使统一资源池的安全合规性可以符合集团的安全规范

为了应对服务器在虚拟化环境中不断涌现的安全挑战，在统一资源池建设后积极拓展云计算业务，广东省电信公司（以下简称：广东电信）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，通过支持最新“多租户”安全管理的趋势科技服务器深度安全防护系统**Deep Security**，以及独有的“无代理”防毒技术部署，完成了安全可信的业务网统一资源池建设，真正发挥了**VMware ESX**平台虚拟化性能与成本优势。

难题一：传统安全域技术支撑无力

据了解，广东电信作为中国电信集团公司全国最大的省级公司，是最早按照集团技术规范要求进行统一虚拟化资源池建设的公司之一。目前业务网资源池已具备三个机房，共配置**3**个**VMware**云计算数据中心，共**5**个计算集群，**2000**台虚拟机，计划未来**3**年内扩展到**20000**台虚拟机。但在统一资源池建设初期，**IT**运维管理部门就发现一个必须要解决的安全问题。

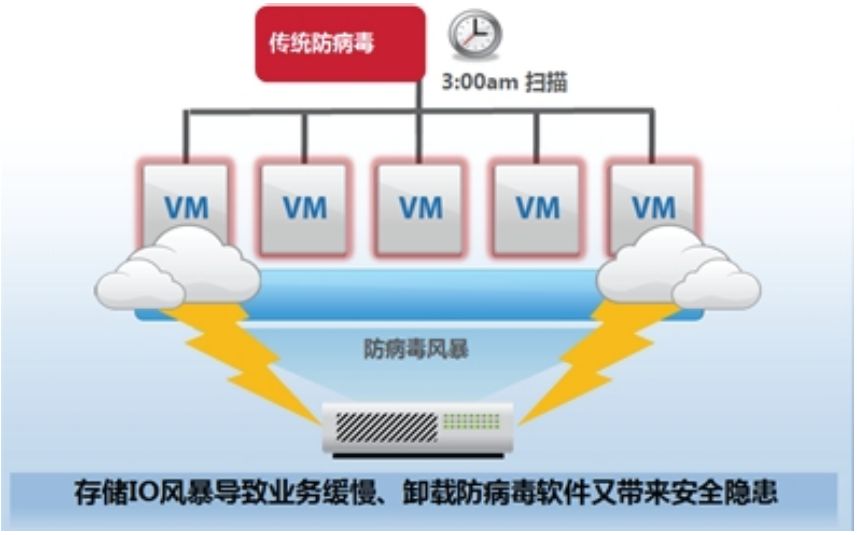
据广东电信**IT**运维管理部门的梁先生介绍，由于传统**IDC**环境采用边界分离、安全隔离的方式，可以建立安全域进行安全加固。而统一资源池使用了大量的虚拟化技术，虚拟网络层的交互数据直接在**VMwareESXi**主机内部完成。这种现象直接导致了原来部署的传统安全产品（如**IPS**、**IDS**等），无法实时监控到虚拟网络内部的潜在威胁，为全局应用下的安全运行带来了极大的风险。而由于缺少专门针对虚拟化防毒并消除安全威胁的配套方案，影响了统一资源池项目在广东电信乃至整个集团内部的推进步伐。

难题二：防毒扫描风暴致使ROI未达预期

广东电信数据中心利用**VMware**虚拟化技术建立统一的资源池，可以实现资源与项目分离，推进业务平台集中部署、集约运营，逐步实现资源整合。然而，原有服务器设备在迁移至云资源池后，其上部署的传统防毒防病毒方案（需要安装代理客户端）将产生“防毒扫描风暴**(AV Storms)**”。这是因为，传统防病毒方案与虚拟化底层兼容性极低，当虚拟机均采用这些技术时，会造成抢占**CPU**、内存、存储**I/O**和网络拥堵的现象，直接造成业务访问延迟或超时。对于这种情

由于传统IDC环境采用边界分离、安全隔离的方式，可以建立安全域进行安全加固。而统一资源池使用了大量的虚拟化技术，虚拟网络层的交互数据直接在VMwareESXi主机内部完成。这种现象直接导致了原来部署的传统安全产品（如IPS、IDS等），无法实时监控到虚拟网络内部的潜在威胁，为全局应用下的安全运行带来了极大的风险。而由于缺少专门针对虚拟化防毒并消除安全威胁的配套方案，影响了统一资源池项目在广东电信乃至整个集团内部的推进步伐。

—— 广东电信
IT运维管理部门 梁先生



【传统防毒系统在虚拟化环境中产生”防毒扫描风暴(AV Storms)”】

况，运营商只能通过降低虚拟化密度或卸载防病毒软件解决，但不管采用哪种方案，都会对资源池的ROI及安全带来负面的影响，致使预期收益不达标。

难题三：多用户管理不能“水中望月”

在数据中心未升级至虚拟化架构之前，各个业务部门的系统均拥有独立的运行环境，边界清晰，因而可以拥有独立自主的安全管理模式及系统，互不干扰。但当多个部门的系统均纳入统一资源池中运行时，各个业务系统之间的边界将变得模糊，传统安全方案无法支持各部门安全事务独立管理的模式，打乱了原有沿用多年的管理模式，极大的阻碍了统一资源池的推进。同时，由于未来统一资源池的规模会迅速扩张，如果把全省所有业务部门的安全事务集中交付给运维部门进行管理，必然会超出IT运维管理的承受极限。

因此，广东电信用户希望安全方案能够参考VMware的软件定义数据中心（vCloud SDDC）方案，将数据中心安全策略扩展到云端，在安全管理上实现“多租户”管理。

“无代理”防护获认可“多租户”承载云计算未来

为了确保公司的业务顺利迁移至资源池，广东电信开始广泛寻找最佳的解决方案。广东电信对多家厂商的虚拟化安全防护产品进行了全面评估及测试，但发现这些厂家的方案均是传统的、基于操作系统的解决方案，不能全面解决之前遇到的各种问题。而在一次与趋势科技的技术交流中，广东电信得知，有别于其它传统的安全解决方案，趋势科技Deep Security 9能够在VMWare ESXi平台下提供最新的无代理防护方案，直接把防护系统部署在ESXi虚拟化平台底层，有效地解决之前遇到的各种问题。

为了验证趋势科技Deep Security 9的技术可行性，广东电信邀请趋势科技参与虚拟化平台安全防护方案的测试。趋势科技利用以VMware vShield Endpoint及VMSAFE两套安全API为基础的虚拟化底层防护技术，有效解决了“安全管理多租户”等一系列虚拟化环境的安全问题。经过深入细致的测试，用户从以下

最新的**Deep Security 9**可以提供更完整的入侵防护和性能监控程序，并在一个无需安装代理程序的高性能平台上实现了动态的虚拟补丁功能，它大幅降低了数据中心和私有云环境的运维负荷。

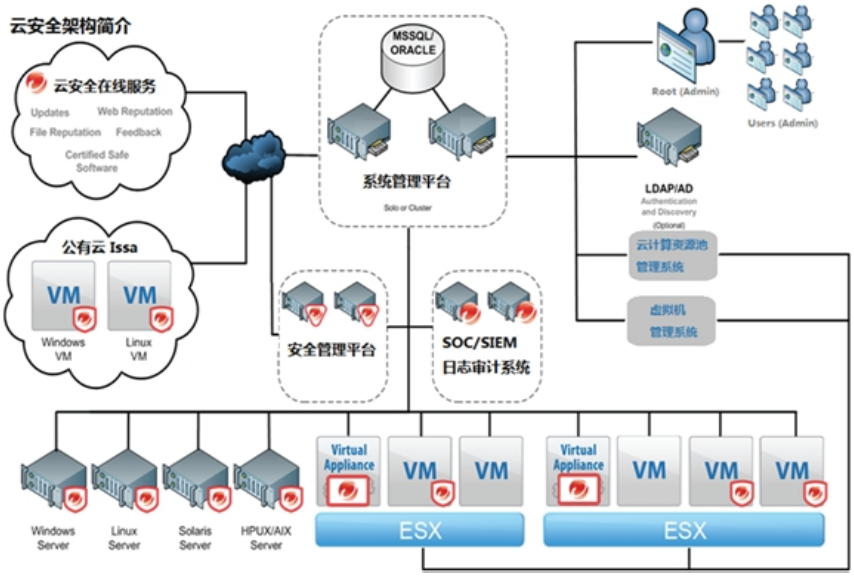
—— 广东电信
IT运维管理部门 梁先生

几方面了对趋势科技**Deep Security**无代理功能得到了充分认可，其中包括：

通过**DeepSecurity**的虚拟化底层防护技术，有效解决了**ESXi**环境下定时全盘杀毒的防毒扫描风暴问题，使统一资源池虚拟化密度提升**2.5**倍。

通过 **Deep Security 9**的多租户安全技术，有效解决了多业务部门安全管理分权的难题，加快了统一资源池推广进程。

通过**Deep Security**的虚拟化底层访问控制技术，有效解决了虚拟层无法划分安全域的难题，并使统一资源池的安全合规性符合集团的安全规范。



【趋势科技**Deep Security**有效解决了“安全管理多租户”等一系列虚拟化环境的安全问题】

资源池安全管理“三大难题”已解 云端业务蓄势待发

目前，广东电信还处在统一资源池建设的尝试阶段，一旦突破技术和管理上的难关，虚拟服务器数量将会呈爆炸式增长趋势，更多的业务、应用将直接汇聚于统一资源池中。而最新的**Deep Security 9**可以提供更完整的入侵防护和性能监控程序，并在一个无需安装代理程序的高性能平台上实现了动态的虚拟补丁功能，它大幅降低了数据中心和私有云环境的运维负荷。

广东电信在充分验证了趋势科技**Deep Security**的先进技术后，最终确定在现有虚拟化平台上全面部署了**Deep Security**无代理防护解决方案。广东电信的梁先生表示：“使用趋势科技专门对虚拟化安全环境开发的**Deep Security**，并利用其独有的‘无代理’和‘多租户’安全防护方案，能够有效解决统一资源池安全管理上的三大难题，扫除了阻碍统一资源池发展的安全障碍，为广东电信统一资源池建设提供了有力的保障和强大的支持！”