[趋势科技成功案例]

趋势科技助力深圳电网公司 迈向绿色 IT 之路

Deep Security“虚拟安全网关”技术提供最低能耗的底层防护

企业利用服务器虚拟化技术，结合自身情况对服务器资源重新优化配置，可以充分利用服务器资源，并有效控制随服务器数量快速增长带来的其他一系列问题。但是，当把这一技术付诸于实践之后，一些用户会发现，由于缺少专门针对虚拟化防毒和消除威胁的配套方案，这会直接影响虚拟化在企业内部的推进步伐。

为了应对服务器在虚拟化环境中不断涌现的安全挑战，深圳电网公司（以下简称：深圳电网）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）的“无代理”防毒技术的部署，真正发挥了 VMware ESXi 平台虚拟化性能与成本优势。在全面降低资源占用的基础上，低能耗、安全稳定的虚拟化平台为深圳电网把国家绿色减排的号召转变为最佳实践。

“脱离安全控制”传统防毒与虚拟化环境不兼容

深圳电网最高供电负荷（1367.5 万千瓦）位居全国第四、南方电网第一，同时也是全国供电负荷密度最大、供电可靠性领先的特大型城市电网。2012 年 建成 110 千伏及以上变电容量 346.2 万千伏安、线路长度 145.4 千米。然而，业务的全面增长，也为 IT 管理带来了的全新的挑战。无限的应用扩展，已经在能耗、机房空间为深圳电网公司带来巨大的压力，而虚拟化的出现，为深圳电网带来了新的选择。在国家绿色 IT 的指引下，深圳电网率先在公司内部开始推进服务器虚拟化进程。

作为全国最大的市级电网企业，为了确保在虚拟化平台上运行的业务系统、数据安全，深圳电网非常谨慎地对虚拟化平台上的各种安全解决方案进行测试、调研，并在虚拟化平台的小范围业务系统中进行试用。意想不到的是，在此次试用中，发现传统防病毒软件与虚拟化平台有着

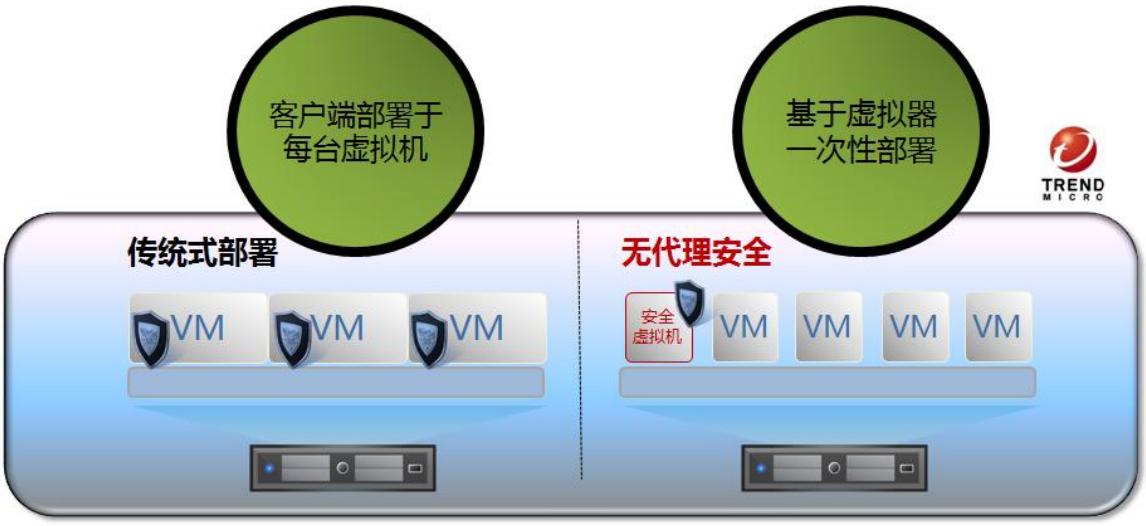
严重的兼容性问题。尤其是在虚拟系统上安装了传统防毒软件之后，但由于它们并不是专为虚拟化环境设计的，所以在运行全盘扫描时，会对虚拟化平台的硬件资源带来巨大的压力，轻者影响业务的正常运行，重者则会导致虚拟化环境崩溃。

深圳电网的黄工表示："使用虚拟化技术，能够将多个硬件资源整合成一个虚拟的统一资源池，供各个虚拟业务系统灵活调度，大大降低了业务系统膨胀带来的能耗、机房空间占用问题。但同时，由于在虚拟机上部署了传统的防病毒软件，不但降低了虚拟化技术在我公司的应用效率，还让虚拟机的安全管理脱离了我们原有的控制框架。"

那么，黄工所谈到的"脱离安全控制"主要是指什么呢？具他介绍：首先，在虚拟环境中，网络边界不再泾渭分明，传统安全设备（如入侵检测系统、入侵防御系统、防火墙等）无法监测到虚拟层的通信流，在虚拟层内部产生了安全"盲点"。其次，深圳电网使用虚拟化特有的动态资源分配技术（DRS），一旦 vCenter 发现某个主机资源不足以运行多台虚拟服务器时，能够动态把虚拟服务器迁移到其他主机上，保障业务不间断运行。这种虚拟机在主机间动态漂移的技术，虽然能够保障业务不间断运行，但同时管理员也没法掌握迁移到虚拟化平台的虚拟机是否具备最新组件的防护，为整个虚拟化平台的安全监控带来监控难度。很显然，面对以上在虚拟化推进工作中存在不利因素，传统的安全产品已经不能再适用深圳电网的需求。

无代理+虚拟层安全网关 "三大优势"得以验证

为了确保公司的业务连续性，避免病毒对数据、应用和网络带来威胁，深圳电网协同多位外聘安全专家、VMWare 原厂工程师对传统防病毒软件的问题进行分析。专家皆都认为在虚拟化平台上，必须使用专为虚拟化环境设计的安全软件，才能解决上述遇到的一系列问题。在后续通过 VMWare 官方网站的验证和第三方评测机构的推荐 ,深圳电网将目光聚焦在趋势科技的服务器深度安全防护系统上来。趋势科技 Deep Security 是第一款能够在 VMWare ESXi 平台下提供无代理防护方案的产品，它能把安全防护组件以虚拟层安全网关的方式部署在 ESXi 上，有效地解决了用户之前遇到的各种问题。



【趋势科技 Deep Security 有效解决了“防毒扫描风暴”等一系列虚拟化环境的安全问题】

为了验证趋势科技 Deep Security 的技术可行性，深圳电网邀请趋势科技参与了虚拟化平台安全防护方案的测试。经过深入细致的测试，深圳电网的 IT 部门对趋势科技 Deep Security 给出了极高的评价，并对无代理功能的优点进行了总结，其中包括以下三个方面：

- 第一，通过 Deep Security 的虚拟安全网关，能够在 ESX 底层即可对虚拟化环境的病毒进行查杀，解决了传统方案不能监测虚拟交换机内部风险的致命问题，并且查杀的效果更优于传统的客户端方式；
- 第三，通过 Deep Security 的无代理虚拟补丁技术，能够在 ESX 底层即可实现对所有虚拟机的补丁防护，并且通过非侵入式的部署方法，保障业务运行的不间断性；
- 第二，通过 Deep Security 的无代理杀毒技术，有效解决了 ESX 环境下定时全盘杀毒的资源风暴问题，这完全符合了第三方机构（Tolly）发布的测试结果。实际的测试结果是：采用趋势的 Deep Security 进行杀毒时所占资源，尽是传统方案的 10%（随着虚拟机数量的增加，效果更加明显）。

虚拟机密度提高 2 倍 绿色 IT 不再是梦

目前，深圳电网还处在虚拟化建设的尝试阶段，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、更多的应用将直接汇聚于数据中心中。因此，安全与性能的平衡，是当前深圳电网最为关注的要点。深圳电网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。

深圳电网的黄工表示：“当解决了安全系统对虚拟化平台带来的性能问题后，我们可以更加放心地把更多的业务系统迁移到虚拟化平台上。相对于原有的传统防病毒方案，采用趋势科技的 Deep Security 可以把虚拟化密度提高 2 倍以上，使我们能够更好地整合硬件资源，不再担心

机房因为业务膨胀而无限扩张，极为符合国家对电网公司的绿色 IT 要求。”

###

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。