

[趋势科技成功案例]

趋势科技助力广东电网公司 Deep Security “无代理” 技术推进虚拟化进程

虚拟化的出现，为终端用户带来了新的选择。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、私有云计算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，广东电网公司（以下简称：广东电网）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 ESX 平台虚拟化性能与成本优势。

传统防毒应对不暇 虚拟化进程受阻

作为全国最大的省级电网企业，广东电网在信息化创先战略的指引下，率先在公司内部开始了企业级信息系统建设，成为了国内电力行业第一家通过自主开发软件实现项目管理、物资管理、生产管理和财务管理四大业务高度融合的电网公司。而随着广东电网业务应用系统的不断增多，IT 部门面临着更为严峻的挑战，这包括提升资源利用、系统整合、降低运维成本以及绿色 IT 的需要。通过对原有服务器平均利用率的分析及测试，广东电网开始在小范围尝试虚拟化平台的推广，并着手建立私有云计算平台。但在此尝试中，也发现了一些问题传统安全防护体系不能解决的问题。

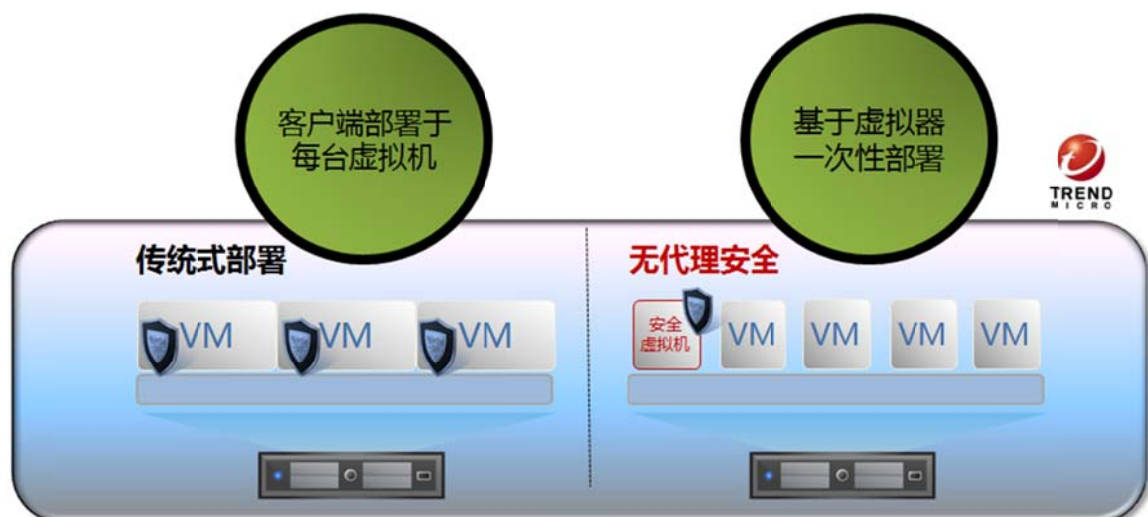
首先，在虚拟环境中，网络设备和服务器之间不再泾渭分明，传统网络安全设备（如 IDS、IPS、防火墙等）无法监测到虚拟机之间发送的通信流，在 ESXi 主机内部产生了风险“盲点”。其次，在虚拟化环境下用于快速恢复的快照技术，会产生很多安全策略过期已久的虚拟机，一旦启动，

必然会导致整个虚拟化环境出现薄弱环节。再者，由于虚拟化迁移技术（vMotion）能够随意把不同 ESX 平台上的虚拟机迁移到其他平台上，一旦 IT 人员没有检查到服务器补丁状态是否更新，都可以造成被黑客利用的情况发生，而主机的控制权一旦失控，很有可能让这种威胁在各个平台上蔓延。

面对以上在虚拟化推进工作中存在不利因素，广东电网 IT 工程师吴先生认为：“除了以上者三点之外，我们还在所有虚拟系统上安装了传统的防毒软件，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 CPU、磁盘、内存带来巨大的压力，并影响业务的正常运行，甚至导致虚拟化环境崩溃。显然，传统的安全产品已经不能再适用广东电网的需求。但经过多次的讨论之后，综合考虑虚拟化的优势、劣势，虚拟化仍然势在必行。为此，我们需要考虑借助专门在虚拟化平台上研发的安全解决方案，来改善上述遇到的安全问题，应对日新月异的威胁攻击。”

防毒创新获认可 “无代理” 功能解难题

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，广东电网开始广泛寻找最佳的解决方案。广东电网对多家厂商的虚拟化安全防护产品进行了交流及测试，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，尤其是在病毒扫描时，“防毒扫描风暴”会造成虚拟服务器极大地性能压力。而在一次与趋势科技的技术交流中得知，有别于其他传统的安全解决方案，趋势科技 Deep Security 能够在 VMWare ESX4.1 平台下提供目前最新的无代理防护方案，直接把防护客户端部署在虚拟化平台 ESX 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，广东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。而趋势科技也紧紧抓住了这个机会，利用趋势科技以 VMware vShield

Endpoint 安全 API 为基础的无代理防护技术，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。经过深入细致的测试，用户从以下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 Deep Security 的无代理防毒技术，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；
- 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；
- 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，实际的测试结果是：采用趋势的 Deep Security 进行杀毒时所占资源，仅是传统方案的 10%（随着虚拟机数量的增加，效果更加明显），这个也完全符合第三方机构（Tolly）发布的测试结果。

云计算建设信心十足 ROI 目标落地有声

目前，广东电网还处在私有云建设的尝试阶段，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的。而传统防毒方案，会让每台物理机能支撑的虚拟机数目（简称虚拟机密度）大幅降低，而这直接反映在总体拥有成本（TCO）得不到降低、投资回报率(ROI)无法达到预期目标，等等一系列的连锁反应。

广东电网在充分验证了趋势科技 Deep Security 的先进技术后，最终确定，并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。广东电网的吴先生表示：“当确定了虚拟化平台的安全性后，在 ROI 预期目标的落地方面做到了有设想、有规划、有保障，现在我们可以加速虚拟化平台的建设步伐。经过计算，以一台物理服务器能够同时运行 10 个应用服务为例，虚拟化建设可以为公司节省 80% 的服务器硬件投资成本。而在拥有了 Deep Security 服务器深度安全防护系统，可以使公司的业务运行在高效、低碳的基础之上，保障业务运行在安全的环境之中，对云时代的到来充满了信心。”