TREND MICRO

TREND MICRO 趋势科技

Deep Security 开启“无代理”防毒新纪元

—— 趋势科技为大理州人民医院医疗系统虚拟化安全护航

最初，我们在虚拟机上部署了传统客户端模式的防病毒软件，作为当时唯一的防毒手段，并没有发现异常状况。但经过一段时间的运行，虚拟机数量增加后，我们发现虚拟化平台在业务高峰期会出现严重的性能问题，而这就是后来深入分析后发现的防毒扫描风暴（AV Storm）。

—— 大理州人民医院安全工作负责人 李先生

大理白族自治州人民医院

行业
医疗

在职职工
900 余名

年门诊量
36 万余人次

开设床位
1000 张

网站
http://www.dlzrmyy.com/

简介

目标
大理州人民医院需要考虑借助专门在虚拟化平台上研发的安全解决方案，来改善医院遇到的虚拟化安全问题，使虚拟化技术得以在大理州人民医院推广。

解决方案
经过与趋势科技技术顾问的深入交流后，大理州人民医院最终决定使用趋势科技 Deep Security 作为其虚拟化平台的安全保障，以推动虚拟化的建设进程。

业务影响
- 有效解决了 ESXi 环境下的防毒扫描风暴问题，业务访问缓慢现象不再出现；
- 一线的医生和业务人员对业务系统的应用满意度大幅提升；
- 极大地加速了医疗系统虚拟化改造的进程。

众所周知，医疗行业信息化是提升医院生产力的重要手段，而虚拟化更是成为医疗行业信息化革命中最具爆发力的“英雄”，但由于缺少与之配套的安全防护软件，这让医疗行业的用户对其安全性心存忧虑。为了应对医疗系统在虚拟化环境中不断涌现的安全挑战，大理州人民医院携手全球服务器安全、虚拟化及“云安全”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”安全防护技术的部署，真正发挥了 VMware 虚拟化平台为医院信息化革新带来的性能与成本优势。

“防毒扫描风暴”始料未及 虚拟化不应因此受阻

据了解，大理州人民医院作为大理州最早获评的三甲医院，在信息化建设方面起步较早，先后实施了多个升级改造项目，保持着信息化的创新活力。目前，大理州人民医院的网络中包含了数十套大型医疗业务系统以及 1000 多台 PC 和智能终端，信息化系统已经成为保障医疗服务效率和水平的重要支撑。

与此同时，为了响应国家“十二五”规划所提倡的节能减排要求，大理州人民医院从降低服务器能耗及资源整合入手，对自身的医疗系统基础架构进行了虚拟化的改造，并把部分医疗系统迁移到虚拟化平台上。在第一阶段的迁移工作完成后，服务器硬件资源使用率得到了极大的提高，但随着虚拟化应用的深入，需要增加更多虚拟主机时，信息中心却发现一道始料未及的技术阻碍。

据大理州人民医院负责安全工作的李先生介绍：最初，我们在虚拟机上部署了传统客户端模式的防病毒软件，作为当时唯一的防毒手段，并没发现异常状况。但经过一段时间的运行，虚拟机数量增加后，发现虚拟化平台在业务高峰期出现严重的性能问题，而这就是后来深入分析后发现的防毒扫描风暴（AV Storm）。

通过对虚拟化技术资料的汇总分析，信息中心对防毒扫描风暴有了全面的了解。其产生的原因在于，由于传统防毒软件并不是专为虚拟化环境设计，当所有虚拟机的防毒软件开启实时防护时，会对虚拟化平台的 CPU、内存和磁盘 I/O 带来巨大的压力，并影响业务的正常运行。而当处于业务高峰期时，并发量增大，会导致虚拟化环境崩溃。

最初，我们在虚拟机上部署了传统客户端模式的防病毒软件，作为当时唯一的防毒手段，并没有发现异常状况。但经过一段时间的运行，虚拟机数量增加后，我们发现虚拟化平台在业务高峰期会出现严重的性能问题，而这就是后来深入分析后发现的防毒扫描风暴（AV Storm）。

—— 大理州人民医院安全工作负责人 李先生

寻找虚拟化安全“盲点” 传统防毒技术难以胜任

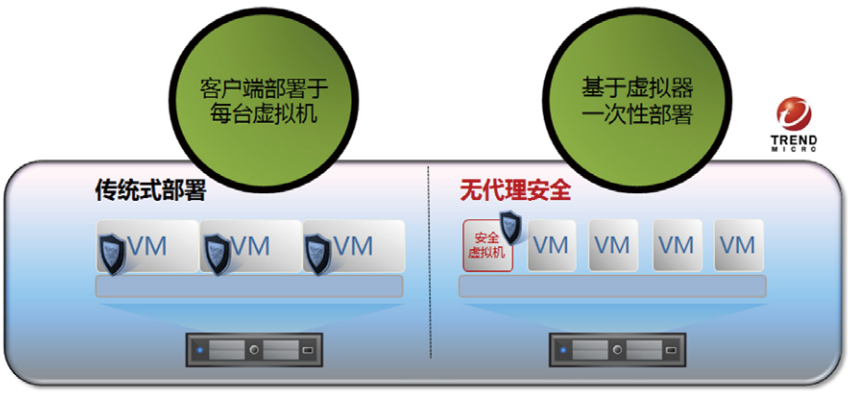
在绿色 IT 大潮下的虚拟化为医疗信息化带来了极大的成本和效率优势，但虚拟化进程中的新威胁和新挑战却需要及时发现和解决。除了防毒扫描风暴之外，信息中心还发现了更多传统防护系统无法与虚拟化相适应的监控“盲点”。

对此，李先生表示：我们还发现网络设备和主机之间不再泾渭分明，传统网络安全设备（如防火墙、IPS）无法监测到虚拟网络内部的数据流，在虚拟网络产生了风险“盲点”。另外，由于需要保障医疗信息化系统（如 HIS、LIS 等）不间断运行，我们使用虚拟化特有的动态资源分配技术（DRS），一旦 VMware vCenter 发现某个主机计算资源不足时，能够动态把虚拟机迁移到其他主机上，保障业务不间断运行。这种虚拟机漂移的技术，虽然能够保障业务不间断运行，但管理员却没法掌握漂移后的虚拟机是否具备最新组件的防护，增加了安全监控的难度。

显然，传统的防病毒软件已经不再适用大理州人民医院的需求，严重阻碍了虚拟化进程的推进，但经过多次的讨论之后，综合考虑虚拟化的优势、劣势，虚拟化建设仍然势在必行。为此，大理州人民医院需要考虑借助专门在虚拟化平台上研发的安全解决方案，来改善医院遇到的虚拟化安全问题，使虚拟化技术得以在大理州人民医院推广。

开创“无代理”防护新纪元 实地测试获用户认可

大理州人民医院开始广泛寻找最佳的解决方案，而在 VMware 官网上了解到的信息则为突破技术阻碍带来了新机会。这些信息包括 VMware 为了帮助用户节省系统资源、最大限度发挥性能价值而推出的“VMsafe”、“VMware vShield Endpoint”等 API，以及目前业界与 VMware 兼容度最佳的安全产品——趋势科技 Deep Security。经过与趋势科技技术顾问的深入交流后，大理州人民医院最终决定使用趋势科技 Deep Security 作为其虚拟化平台的安全保障，以推动虚拟化的建设进程。



【Deep Security 有效解决了“AV Storm”及“虚拟网络内部攻击”等安全问题】

趋势科技 Deep Security 能够利用 VMware 发布的 VMware vShield EndPoint 安全接口或最新的 NSX 架构上，为 VMware ESXi 平台上提供无代理防护方案。通过直接在 ESXi 上部署专用安全虚拟机（DSVA），能够有效地解决我们之前遇到的各种问题。

—— 大理州人民医院安全工作负责人 李先生

为了验证趋势科技 Deep Security 的技术可行性，大理州人民医院邀请趋势科技对虚拟化平台安全防护方案进行实地测试。而趋势科技也紧紧抓住了这个机会，利用特有的无代理防毒技术有效解决了防毒风暴及虚拟网络内部攻击等虚拟化环境的安全问题。其中包括：

- 通过 Deep Security 的无代理杀毒技术，有效解决了 ESXi 环境下的防毒风暴问题，实际的测试结果表明，采用趋势的 Deep Security 进行杀毒时所占资源，只是传统方案的 10%；
- 通过 Deep Security 的无代理防毒技术，能够在 ESXi 底层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网络内部风险的致命问题。

安全防护难题得以解决 医疗系统虚拟化改造随即加速

现在，在大理州人民医院的业务高峰期，传统防毒软件导致的业务访问缓慢现象已经完全消失，一线的医生和业务人员对业务系统的应用满意度大幅提升，这让希望虚拟化在全院推广的信息中心信心倍增。

李先生表示：“趋势科技 Deep Security 是目前少数能够支持虚拟机无代理防护技术的产品之一，在测试过程中，我们发现 Deep Security 与虚拟化平台的整合度是各个产品中最好的。在实施 Deep Security 后，我们在虚拟化建设时遇到的包括防毒扫描风暴和虚拟网络内部攻击等诸多安全问题得到了解决，这让我们更加安心地把重要的业务系统迁移至虚拟化平台，极大地加速了我院医疗系统虚拟化改造的进程。”