



趋势科技成功案例



趋势科技 Deep Security 有力支撑张掖市公安局虚拟化安全

在我国公安系统从传统警务向现代警务转变的过程中，信息化的作用不言而喻，而虚拟化以其低成本和高效利用资源的特点，已经成为了现代警务战略布局中的一颗关键棋子。甘肃省张掖市公安局在利用虚拟化技术成功“解围”服务器硬件瓶颈之后，与全球服务器安全、虚拟化及云计算安全领导厂商趋势科技展开合作，利用趋势科技服务器深度安全防护系统（Deep Security）将虚拟化层面的威胁一扫而光，此举为甘肃省 13 个市级公安系统虚拟化安全建设树立了新标杆。

虚拟化低成本优势明显 病毒防护如何齐头并进

张掖市公安局承担着确保全市安全稳定，预防、制止和侦查违法犯罪活动等警务工作。由于面临这些多任务的挑战，张掖公安迫切需要利用 IT 创新技术加速各大警用信息平台的建设速度，给警务工作提供后台支撑，然而，原有服务器的“不给力”直接限制了新业务的发展。同时，平台中各个系统不能根据实际需要和业务变化灵活、动态调整资源，系统的灵活性和扩展性较差，影响了公安业务部门管理和对外服务的能力。

此外，由于应用系统与底层硬件之间形成了“竖井”结构，要保障三大关键系统：户籍管理平台、警务综合管理平台和警用地理信息平台高效运转，就需要投入大笔经费购买数十台服务器。为此，张掖市公安局信息科决定引入虚拟化技术以降低成本。在经过严格测试之后，张掖市公安局最终采用了 VMware vSphere 5.1 服务器虚拟化解决方案，彻底解决了传统单一物理服务器部署应用方式所造成的弊端，在降低采购和应用成本的前提下大幅提升了服务器的利用率。

虚拟化技术的成功应用虽然让人欣喜，不过对于在系统安全性、可用性和可靠性方面要求更高的公安警务行业来说，虚拟化还是一个新鲜事物，如何保障其安全性成为新的挑战。张掖市公安局信息科的张科长表示：“虚拟化使得警用平台整个 IT 架构都发生了变化，在这种新的环境下，安全管理策略与工具需要紧跟这一架构变化，防毒系统也必须齐头并进，能够提前一步发现虚拟化防毒可能存在的问题，这包括是否会影响整个系统的效率、补丁管理是否能更轻松、针对虚拟机内部的数据流量是否能主动发现恶意代码等。为此，我们必须必须在市场

中选择一款能与 VMware vSphere 完全兼容的、成熟度最高的虚拟化安全管理软件。”

Deep Security 成熟度可以信赖 虚拟化加速前行

在听取了 VMware 虚拟化项目实施工程师建议后，张掖市公安局将目光聚焦在了虚拟化防毒领域内应用最多、成熟度最高、技术最新的趋势科技 Deep Security 上来。并在先期转移到虚拟化平台上的测试中安装了 Deep Security，利用其独有的无代理技术，实现了最低的资源消耗，成功地避免了防毒软件抢占 CPU、内存、网络的情况发生。据该虚拟化项目实施工程师熊晖先生介绍，由于趋势科技 Deep Security 8.0 与 VMware vSphere 5.1 的产品完全兼容，是通过底层应用接口实现虚拟化防护，所以不需要在任何一台虚拟操作系统中再安装防毒软件，整个部署过程非常迅速。

在接下来的测试阶段，张掖市公安局科技科对虚拟化安全应用状况进行了长期压力测试和访问效果跟踪。自安装 Deep Security 之后，VMware 虚拟化平台上的业务系统并未出现之前最担心的“延迟”现象。在正式迁移阶段，信息科将三大平台之一的“警用地理信息平台”率先迁移到虚拟化平台上，并通过使用 Deep Security 防火墙策略、虚拟补丁管理等一系列的创新设计，充分验证了该平台的易用性。对于最新发现的漏洞，Deep Security 能够在第一时间提供修补程序，无需重新启动系统，即可在数分钟内将这些规则应用到所有“警用地理信息平台”上的虚拟服务器中。

张掖市公安局对 Deep Security 的应用效果十分满意，据张科长介绍：“之前，我们担心虚拟化之后很多虚拟机产生的流量无法被监测到，这在公安系统的网络中是非常严重的问题。但在部署 Deep Security 之后，这一担心被证明是多余的。Deep Security 在虚拟化层面真正实现了双向状态防火墙，可以检查所有传入和传出虚机的通信，它可以使用细化过滤，针对虚拟交换机的底层对所有基于 IP 的应用进行检测。并且，我们通过其内部定制的服务器模板，在虚拟化之后仍然可以集中管理所有虚拟服务器的防火墙策略，为统一安全标准提供了最快捷的管理平台。”

据了解，张掖市公安局已经建立了虚拟化双机热备集群（HA Clusters），并陆续将 OA、邮件、财务系统迁移过来，确保三大平台和其它业务系统的业务连续性。由于张掖市公安局为突破虚拟化防毒瓶颈提供了有价值的经验，甘肃省其它市级公安系统都对虚拟化项目，以及下一阶段的安全防护核心工作充满了信心。

###

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。

更多媒体垂询，敬请联络：

趋势科技（中国）有限公司

刘婷婷

电话：010-85252277

电子邮件：angela_liu@trendmicro.com.cn

谋信传媒

那罡

电话：010-67047822

电子邮件：nagang@ctocio.com