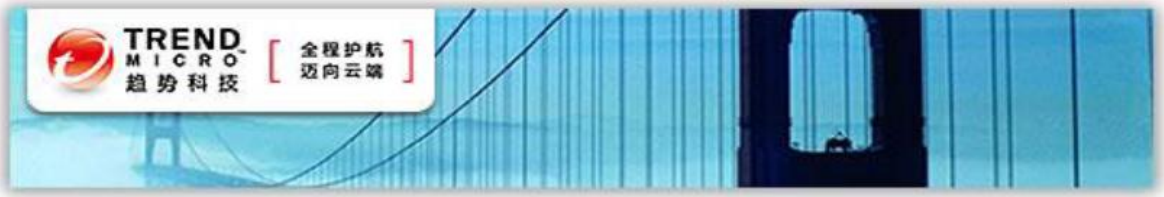

[趋势科技成功案例]

趋势科技Deep Security普陀区政府虚拟化安全案例-

虚拟化技术凭借其便捷性、灵活性、扩展性的特点，在各个行业中都发挥着积极的作用，它渗透到了数据中心的每个角度。但任何一项新技术都存在“两面性”，在大幅削减成本、驱动 IT 架构变革的同时，绝大多数用户在虚拟化安全领域的实践则刚刚开始。

上海市普陀区科学技术委员会响应国家绿色 IT 及虚拟化的号召，采用了 VMWare 提供的虚拟化技术成功完成了数十台服务器的迁移，但随之而来虚拟化防毒问题却让信息中心伤透了脑筋。经过充分的调研，以及严格的测试，趋势科技最新推出的服务器深度安全防护系统（Deep Security）在众多虚拟化安全解决方案中一举胜出。在部署后的半年周期内，Deep Security 充分发挥了独有的“云安全、无代理、虚拟补丁”的巨大优势，为普陀区电子政务虚拟化平台有效地抵御了病毒和黑客的攻击。

虚拟化实践逐步深入，安全隐患不断呈现

在国家信息化体系建设中，政府信息化又是整个信息化中的关键。“虚拟化在成本和管理方面的优势非常明显，但传统的防火墙、IPS等设备，无法对虚拟服务器之间进行很好的监测，虚拟化防毒、安全加固与补丁管理等工作更为重要。

服务器虚拟化的安全威胁超出了人们的预料，看似简单防病毒和安全策略部署经验在这里根本起不到任何作用，无法达到预期，甚至还会造成虚拟机资源被占用等非常严重的事件产生。当前大部分的黑客入侵、木马注入等威胁，多是基于操作系统及应用程序的安全漏洞进行攻击。因此，为服务器及时升级系统及应用程序补丁是防御新形态攻击、保障服务器安全的唯一途径。而各厂商每月发布的操作系统及应用程序的补丁程序数以百计，而安装补丁之后，管理员必须重新启动服务器才能使补丁生效。虚拟化“两面性”的矛盾积攒的越来越深，能否找到最佳的办法吗？

跳出思维定式 Deep Security 破冰虚拟化防毒难题

普陀区信息中心开始研究和测试各种针对虚拟化安全的解决方案，当测试趋势科技 Deep Security 时，“无代理防毒”的创新设计，终于让大家跳出传统防毒理念下的思维定势。作为全世界第一套专为虚拟化环境设计的恶意软件防护解决方案，趋势科技 Deep Security 在实际部署时可实现无代理安全防护，由一个安全虚拟设备负责为所有子虚拟机进行杀毒处理。经过严格测试，“无代理防毒”的功能完全可以破解虚拟防毒难题，它可避免反病毒风暴（AV Storms），可避

免防护间隙（Instant-On Gap），可避免重复性更新反病毒数据库。

“有了更好的工具，需要更快的行动。”在正式部署 Deep Security 之后，普陀区信息中心将其与 VMware 平台进行了整合，并对 VMware vSphere 虚拟机上的操作系统和应用系统进行了实时监控，有效的保证了之前设计的“虚拟机密度”达到了效能最佳状态。Deep Security 实现了真正的底层防护，现在普陀区电子政务平台每增加一台虚拟操作系统都无需再安装防毒软件。这样的结果，便为虚拟化平台随时启动和迁移提供了即装即防的实时防护，真正实现了虚拟化的便捷性优势。

在补丁管理方面，通过 Deep Security 与 VMware VMsafe API 的结合，通过虚拟补丁（Virtual Patch）的方式形成了更加快速的补丁部署架构，预先防止黑客利用最新漏洞发起的攻击。对于已知的漏洞，Deep Security 对普陀区电子政务平台网络内部运行的各种应用程序提供开箱即用的漏洞防护，使其免受了无数次的漏洞攻击。对于最新发现的漏洞，Deep Security 能够在第一时间提供修补程序，在无需重新启动系统的前提下，即可在数分钟内将这些规则应用到所有使用了 Deep Security 解决方案的服务器上。

普陀区科委王建平副主任表示：“趋势科技推出 Deep Security 这样的无代理防毒安全解决方案，为我们提供了全面完善虚拟平台的选择。虚拟补丁的设计又帮助我们有效解决了困扰多时的服务器补丁管理难题，是一套革新性的补丁管理方案。”通过趋势科的 Deep Security 进一步强化了我们的虚拟化安全架构，从而

提高了普陀区电子政务平台的敏捷性和可靠性。