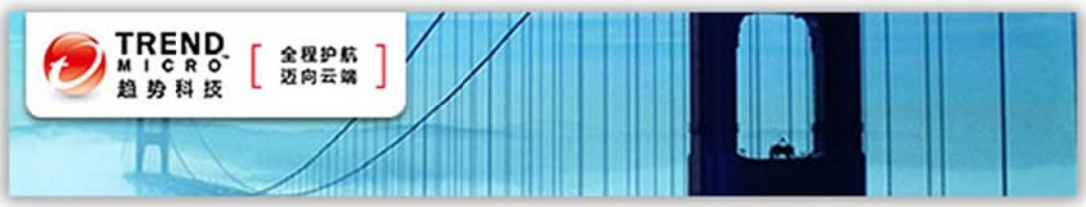

[趋势科技成功案例]

趋势科技与淄博矿业集团勠力同心
Deep Security 力保数据大集中安全无忧

云计算与虚拟化的日益普及直接影响了企业部署安全的方式，而企业的安全架构也必须具有持续优化和创新的能力，以适应业务需求不断的变化和因此带来的网络威胁。淄博矿业集团有限公司（以下简称：淄矿集团）通过与全球服务器安全、虚拟化及云计算安全领导厂商趋势科技的长期合作，利用趋势科技终端、网络、网关层产品形成卓有成效的防护体系，并在集团数据资源大集中的今天，通过趋势科技服务器深度安全防护系统（Deep Security）实现了安全无忧的虚拟化层面的威胁管理。

数据大集中 虚拟化安全需要“提前一步”

淄矿集团是一家具有上百年开采历史，多业并举的跨地区、跨行业、跨所有制的大型现代企业集团。作为全国企业 500 强之一，淄矿集团一直以来把信息化建设作为企业谋求新发展的战略核心要素之一，并利用信息化建设有效地发挥了管理创新的示范作用。据了解，淄矿集团与趋势科技一直以来保持着非常紧密的合作关系。为了应对日益恶化的互联网安全威胁，在长达“七年”的战略合作中，淄矿集团持续利用趋势科技的 OfficeScan 防毒墙网络版、网络防毒墙 NVWE、防毒墙控管中心 TMCM、网络威胁发现设备 TDA，以及 Web 安全网关 IWSA，在网关、网络接入、内网安全监控与终端防护上形成坚不可摧防护罩，层层排除隐患，为网络平稳运行提供了有效保障。

随着淄矿集团紧跟国家“十二五”信息化规划的如期启动，涉及矿采、机、掘、运、通、财、销等各个业务系统的数据中心正在全面升级，按照统一的数字化标准和规范实现的全集团综合信息集成平台的也进入到了数据大集中的攻坚阶段。为了更好的解决传统单一物理服务器部署、应用方式所带来的弊端，提升服务器的利用率，降低应用成本，淄矿集团在经过半年左右的测试和考察之后，引入了 VMware 服务器虚拟化架构解决方案。并决定按照 ITIL（Information Technology Infrastructure Library,信息技术基础架构库）中的 SLA（Service Level Agreement，服务水平协议）划分边缘与核心系统，并准备将邮件、财务、

OA、医保、瓦斯和通风检测、运销等三十多项业务系统逐级、逐批的迁移到虚拟化平台当中。

淄矿集团信息中心的杨主任介绍道："人无远虑，必有近忧；IT 创新，谋划在先。我们并不是国内第一个实施虚拟化项目的大型集团公司，但这也为我们瞄准同行业的领先发展水平，借鉴领先企业的经验和教训创造了条件。作为趋势科技长期的合作伙伴，我们在虚拟化项目刚刚立项时，正好赶上趋势科技举办的 2012 年 CIO 峰会，淄矿集团信息中心的同事与各行业的 CIO 进行了广泛接触，当然也不乏虚拟化安全管理中遇到问题的企业。他们在将传统防毒软件部署在虚拟化平台后遇到病毒扫描风暴、虚拟机之间通信无法监控、补丁管理任务繁重等诸多问题，都为我们敲响了警钟。最后，我们参考 VMware 的建议，并接受了 CSA 云安全联盟高层及趋势科技总部专家的推荐，最终选择了长期信赖的伙伴——趋势科技，以趋势科技的 Deep Security 安全产品来应对云计算、虚拟化带来的新威胁。"

"无代理"特性大幅降低资源消耗 虚拟机内部威胁轻松排除

在数据大集中时代，虚拟化使得企业整个 IT 架构都发生了变化，安全管理策略与工具也需要紧跟这一架构变化。由于提前一步发现了虚拟化防毒可能带来的资源消耗问题，淄矿集团在先期转移到虚拟化平台上的业务系统和测试平台中安装 Deep Security，利用 Deep Security 独有的无代理技术，以最低的资源消耗，成功的避免了防毒软件抢占 CPU、内存、网络的情况发生。经过信息中心 IT 运维工程师对客户端应用状况的长期跟踪，自安装 Deep Security 之后，这些应用在 VMware 虚拟化平台上的业务系统从未出现过"延迟"现象。

另一方面，淄矿集团庞大的网络结构和业务特性使得信息中心十分重视 IT 运维管理工作，而在项目实施之前，工程师也非常担心虚拟化之后监控管理工作，不想因为虚拟化而产生 IT 运维管理的"死角"。

应该说这份担心十分有必要，这是因为在虚拟化中，传统网络边界的防护手段将完全起不到作用。在非虚拟化的基础架构下，每一个层（数据库、应用程序和 Web 应用）都有所属的网络区段，可用防火墙、IPS/IDS、防毒软件分别为各自提供安全保护。比如，我们可以用防火墙来保护网路边界的安全，但现在不是所有的流量都来源于自互联网，当某个虚拟服务器与其它的虚机之间有流量沟通的时候，基于物理设备进行边界防护的手段就无法发现这些流量是否带有恶意的攻击特征。

据杨主任介绍："我们并不是把 Deep Security 看成是一款软件，而是把 DS 真正当成了虚拟化数据中心安全运维管理的平台。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，它可以使用细粒化过滤，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，在实施之后，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。这种在虚拟化平台上的完整性监控，完全打消了我们之前针对 IT 运维‘死角’的顾虑。”

Deep Security 安全再立新功 虚拟化大幅降低 TCO 成本

安全从来就没有终点 ,这就意味着要不停地发展并为新应用匹配最佳的防护手段。长久以来，趋势科技协助淄矿集团一次次对原有的网络安全架构进行升级 ,正是为了应对日益严峻的网络威胁，而之前建立起的多层次、全方位、系统化并易于管理的网络防病毒体系，已经取得了阶段性的成功。为了应对数据中心升级、虚拟化运维管理带来的挑战，此次淄矿集团依然使用趋势科技 Deep Security，无疑是为消除安全隐患、大幅降低总体拥有成本(TCO)起到了跨越式的支撑作用。

如今，通过 VMware 和趋势科技 Deep Security 的最佳实践，淄矿集团数据中心极大的提高了服务器整合的效率，控制和减少物理服务器的数量，明显提高了每个物理服务器及其 CPU 的资源利用率，从而降低了硬件、人力和能耗等多项成本。