[趋势科技成功案例]

趋势科技 Deep Security 高效推进青岛啤酒服务器虚拟化安全管理

青岛啤酒股份有限公司（以下简称青岛啤酒）这个百年品牌虽然历经沧桑，但依然充满着激情与活力，其 IT 信息化建设已成为企业做大、做强的有力推手。在虚拟化大潮的影响下，青岛啤酒通过与 VMware 虚拟化解决方案将多数物理服务器整合之后，在研发与测试环境中的病毒管理却遇到了棘手的问题。而在引入趋势科技 Deep Security 部署之后，通过与 VMware 虚拟机的无缝连接，构建出了高效的开发与测试环境，使得青岛啤酒虚拟化平台环境下的病毒也从此再无藏身之处。

虚拟化实践逐步深入“免罪金牌”不再适用

青岛啤酒是我国最早的啤酒生产企业，也是最早进入国际市场的中国品牌之一。作为我国最早一批上市企业中率先吹响了信息化建设号角的先头兵，在企业的不断发展壮大中，信息化成为青岛啤酒不容忽视的部分。

青岛啤酒在相继成立了营销中心、物流中心和制造中心之后，对应的 IT 数据中心逐步成为了承载这些业务高效运行的重要枢纽。从 IT 承载业务与软件生命周期管理的角度上看，青岛啤酒 IT 部门分管的数据中心主要分为研发测试和生产网络两大组成部分。在测试网络中，IT 部门承担了很多相关开发产品的测试工作，不仅任务繁重，而且测试环境的变化也十分频繁，这对测试环境的部署提出了非常高的要求。

据了解，为了解决测试环境的搭建与管理问题，青岛啤酒服务器虚拟化管理经历了如下四个发展阶段：

- 第一阶段，为了取得人力和资金成本的有效节省，青岛啤酒全面衡量了市场上的虚拟化产品，并果断的采用了流行的 VMware 服务器虚拟化解决方案，通过更好地对服务器进行整合，大幅削减了物理主机的数量。
- 第二阶段，当虚拟化走上舞台时，运维工程师根据开发部门的申请，大量的虚拟化测试服务器开始出现在数据中心，这一阶段基本解决了研发测试中遇到的所有环境搭建问题。

- 第三阶段，在虚拟机不断增加的过程中，虚拟化偶尔会获得“免罪金牌”，尤其是病毒和安全防护的管理方面。比如，不能统一安装防毒软件、防毒软件品牌不一、补丁程序和防毒代码得不到及时更新等等，这给虚拟化安全带来了许多实际发生过的病毒威胁。
- 第四阶段，通过虚拟化管理实践的总结，青岛啤酒已经制订了相应的审核流程，要求所有的虚拟服务器也需要与物理主机的管理一样严格有序，需要装防毒软件并设置统一的安全策略。

专门负责青岛啤酒虚拟化主机安全的王先生认为：“通过充分沟通，我们与开发人员在虚拟化安全方面取得了共识。尽管虚拟化技术本身并不容易受到攻击，但是程序开发人员和虚拟化服务器管理员之间的知识差异，导致了虚拟服务器配置的不安全性。之前，我们虽然保证了在每台主机上都安装防毒软件，但虚拟化防毒管理工作的后续难题开始逐渐浮出水面。”

Deep Security 有效避免“病毒扫描风暴”

之前提到的“虚拟化防毒管理工作的后续难题”是什么呢？据了解，首先是安装的问题，大量的虚拟机中安装和部署防毒软件的工作量让工程师应接不暇。其次，每台虚拟机的防毒软件都需要定时的更新和查看监控日志，管理的难度和复杂性出现了失控的状况。最后，由于将传统防毒软件直接转化在虚拟机中，研发和 IT 运维部门很快便发现传统防毒软件在虚拟环境产生的性能问题。由于每个虚拟机上都安装一套防毒软件，多个虚拟机同时启动病毒扫描，不但物理主机的磁盘的 I/O 将都会被占满，同时虚拟服务器也开始疯狂的抢占 CPU、内存、网络三项主要资源，客户端访问开始频繁出现“延迟”现象。

为了解决虚拟化资源抢占、统一安装、无法统一管理等一系列问题，青岛啤酒 IT 部门立即与 VMware 和趋势科技取得了联系，并通过部署 Deep Security 得到了满意的效果。据王先生介绍：“通过对趋势科技工程师的咨询和沟通，我们掌握了病毒扫描风暴产生的原因。由于这些传统的病毒解决方案不是专为虚拟环境设计的，它们会引起严重的运营问题，如，我们遇到的病毒扫描风暴、人力资源浪费、管理开支增加等等。另外，如果要防止最新的病毒入侵，就需要频繁地在每台虚拟机上更新防毒代码，以应对最新的病毒威胁。当然，许多传统的防毒方案也无疑能在病毒查杀上有所帮助，我们也可以通过时差的调整，采用分组扫描的办法。但是这些工作实际上还在采用手工的方式，且仍然是需要在每台虚拟服务器上安装客户端软件，在虚拟机数量达到了上百台之后，这些工作量确实让运维难上加难了。”

对症才能下药，由于 Deep Security 在子虚拟机上取消了安全防护代理程序，因此可以帮助底层宿主机大幅降低负载状况，同时利用云安全防护代码更新，这使得整个部署过程非常迅速简便。在正式部署 Deep Security 之后，青岛啤酒将其与 VMware vCenter 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。青岛啤酒对于趋势科技的 Deep Security 安全产品的功能表现非常满意，它不仅可以做到深度服务器安全防护，抵御病毒感染、非法入侵、数据泄露等恶性事件的威胁，同时可在不增加服务器负载的前提下达到了与物理服务器一样的安全管控标准。另外，针对不断变化的威胁攻击，目前的做法必须持续不断地管理、设定与修补代理程序。在别无他法的情况下，Deep Security 的无代理部署特性让虚拟机管理员在进一步保证性能的同时，将部署、设置，或更新代理程序通过集中的模式进行管理，这种做法真正的降低了管理工作的复杂性。

王先生还表示：“之前我们担心的就是安全防护可能在虚拟化之后失去平衡。而趋势科技推出 Deep Security 这样专门针对虚拟化系统的安全解决方案，为我们提供了全面完善虚拟平台的选择。通过简化虚拟化安全架构，我们已经可以创建更动态和灵活的数据中心，从而提高了业务敏捷性。而在下一步筹措的青岛啤酒私有云的建设中，我们对云安全的防护能力也更加有信心。相信，谈论啤酒品牌的时候，肯定少不了提到青岛啤酒，而我们谈到虚拟化病毒的防范，也肯定少不了 Deep Security 的身影。”

###

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 1,200 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。