概况

行业
制造

公司总部
青岛

品牌价值
805.85亿元

啤酒生产厂
59家

网站
http://www.tsingtao.com.cn/

简介

目标
青岛啤酒希望通过与VMware虚拟机的无缝连接，构建出了高效的开发与测试环境，使得病毒再无藏身之处。

解决方案
在正式部署Deep Security之后，青岛啤酒将其与VMwarevCenter进行了整合，并对VMwarevSphere虚拟机上的操作系统和应用系统进行了实时监控，确保了之前设计的“虚拟机密度”达到了最佳效能状态。

业务影响
- 抵御了病毒感染、非法入侵、数据泄露等恶性事件的威胁
- 确保了之前设计的“虚拟机密度”达到了最佳效能状态
- 通过简化虚拟化安全架构提高了业务敏捷性

青岛啤酒构建全面、完善、安全的虚拟化平台

—— 趋势科技推进青岛啤酒服务器虚拟化安全管理

趋势科技推出Deep Security这样针对虚拟化系统的安全解决方案，使我们搭建了全面、完善、安全的虚拟化平台。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建设中，我们对云安全的防护能力也更加有信心。我相信，当我们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防范的时候，也肯定少不了Deep Security的身影。

—— 王先生 青岛啤酒虚拟化主机安全负责人

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并部署之后，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，使得病毒再无藏身之处。

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。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，这对测试平台的部署效率提出了非常高的要求。

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 为了有效节省人力和资金成本，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，将大量的虚拟化测试服务器部署在数据中心，这一阶段基本解决了研发测试中遇到的环境搭建问题。

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

由于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，以应对最新的威胁。当然，许多传统的防毒方案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。

—— 王先生 青岛啤酒
虚拟化主机安全负责人

一、补丁程序和防毒代码得不到及时更新等，这给虚拟化带来了许多病毒威胁。

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与物理主机的管理一样严格有序，不但需要安装防毒软件，还需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：“通过充分的沟通，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？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，非常容易出现遗漏；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了传统防毒软件在虚拟环境中产生的性能问题。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I/O都会被占满，同时虚拟服务器也疯狂的抢占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、批量安装、统一管理等问题，青岛啤酒IT部门与VMware和趋势科技取得联系，并通过部署Deep Security得到了满意的效果。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VMwarev Sphere虚拟机上的操作系统和应用系统进行了实时监控，确保了之前设计的“虚拟机密度”达到最佳效能状态。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，实现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，目前的做法是持续不断地管理、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，这种做法从本质上降低了管理工作的复杂性。

王先生还表示：“之前我们最大的担心，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，使我们搭建了全面、完善、安全的虚拟化平台。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建设中，我们对云安全的防护能力也更加有信心。我相信，当我们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防范的时候，也肯定少不了Deep Security的身影。”