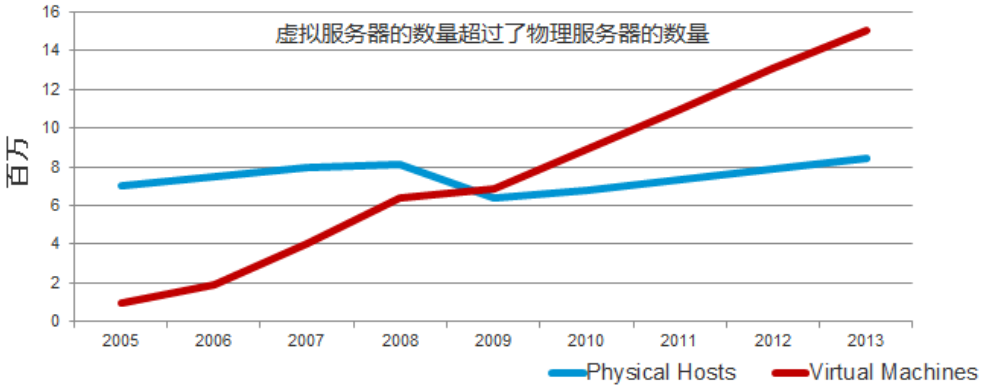
Deep Security 为企业虚拟化平台配备“安全气囊”

趋势科技服务器深度安全防护系统在江淮汽车部署案例

虚拟化技术早已不再是纸上谈兵的神话，据有关数据统计，在 2009 年时，全球虚拟化服务器的数量就已经超过了物理服务器的数量。虚拟化技术，凭借自身的低成本投入、灵活便捷的管理、强大的业务扩展能力，在 IT 架构中扮演着越来越重要的角色。

在国家“十二五规划”所提倡的“绿色 IT”指引下，江淮汽车也正在对 IT 基础架构进行着虚拟化洗礼，并且已经把部分应用系统和全部测试环境迁移至虚拟化平台。江淮汽车信息中心的邵科长表示，随着虚拟化技术在江淮的应用，极大的提高了服务器硬件资源的利用率，但是随着虚拟化程度的不断提高，在享受虚拟化带来的好处的同时，也带来了一些新的服务器管理复杂度和安全隐患的问题。作为信息中心负责人，邵科长急需一种专门针对虚拟化平台的行之有效的安全解决方案。

作为全球云安全和虚拟化安全技术的领导者，趋势科技在对江淮汽车虚拟化进程进行了详实的评估之后，为江淮汽车提供了一套专门针对虚拟化服务器环境的安全解决方案——Deep Security，帮助用户在提升虚拟环境安全性的同时，降低了管理成本，得到了客户的高度认可。



虚拟化安全管理出现“空缺”急需新途径弥补

江淮汽车是一家集商用车、乘用车及动力总成研发、制造、销售和服务于一体的综合型汽车厂商。据了解，江淮汽车在信息化建设方面走的比较早，从 1994 年开始进行信息化建设，

先后实施过 CAD、MRPII、ERP 等信息化项目，全面实现从产品开发到经营管理的信息化。随着最新的供应链管理 SCM 平台落地，为了进一步提高生产力，提升 IT 效率，江淮汽车很早就开始规划虚拟化架构，在国内汽车制造业中率先引入服务器虚拟化技术。随着江淮汽车的虚拟化项目全面进入第二阶段，应用服务器的虚拟化程度和虚拟机密度不断提升，随之而来的则是在虚拟化环境下崭新的安全管理难题，这给江淮汽车的 IT 部门带来了从未有过的挑战。

邵科长介绍说："在我们之前的虚拟化项目实施中，IT 管理员已经发现，要让每一台虚拟化服务器都能符合物理服务器同样的安全等级，就需要在每个虚机上单独安装一套防毒软件，大量的虚拟机中安装和部署防毒软件的工作量让工程师们应接不暇。并且，为了防止最新的病毒变种入侵，就需要频繁的在每台虚拟机上更新操作系统补丁和防毒代码，不但存在着兼容性隐患，而且每次更新状态之后的'重启'操作，都会严重的影响正常业务访问，管理成本也在随之成倍增长。"

在最新的二期工程中，除了上述问题依然存在之外，还会遭遇服务器安全审计，整体监控等定制化防护策略和统一管理的难题。并且，随着 Linux 和 UNIX 等更多的虚拟化服务器的加入，企业不但要额外购买和安装防毒软件，还要防止在同一台物理机上不同虚拟机之间的互相攻击，这些预算外的超支成本，让虚拟化原生的优势黯然淡去。

深入剖析虚拟化安全视角成为首选方案

针对上述问题，江淮汽车的 IT 部门协将安全产品采购的重点瞄准了专门针对虚拟化平台的安全防护软件上。据了解，鉴于江淮汽车的虚拟化环境架构在 VMware 的基础之上，趋势科技与 VMware 为全球战略合作伙伴，是全球最早、目前也是唯一可以基于 VMware 底层应用接口，实现虚拟化底层防护。就这样，趋势科技推出的 Deep Security 被列为首选对象。

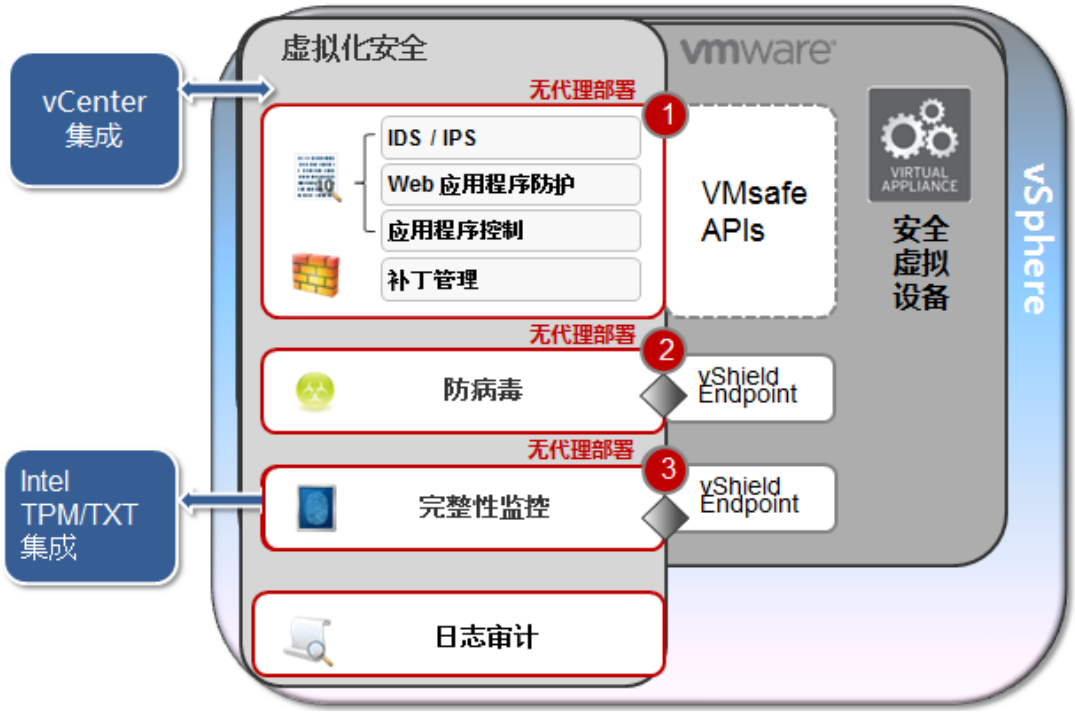
接下来，趋势科技与江淮汽车在"病毒扫描风暴"产生原因等一系列的技术难点和管理因素进行深入沟通，在真切了解到 IT 管理员的需求基础上，为江淮汽车规划了整体虚拟化应用的安全解决方案。

与多数加入虚拟化大家庭的企业一样，在虚拟化二期工程中江淮汽车也无法避免的遇到了

“病毒扫描风暴”等棘手问题。之前，由于每台物理主机上的虚拟化服务器数量还没有达到上限，而现在如果仍然使用传统的防毒软件直接转化在虚拟机中，很快就出现了虚拟安全管理中特殊的性能问题。正是因为，每个虚拟机上都安装一套防毒软件之后，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。

虚拟化安全提供全程护航受客户充分认可

Deep Security 的成功部署，为江淮汽车大幅提改良了之前虚拟化管理的复杂程度。邵科长介绍说，由于充分与江淮汽车部署的 VMware vShield Endpoint 相结合，Deep Security 实现了真正的底层防护，现在江淮汽车每增加一台虚拟操作系统都无需再安装防毒软件。由于每台物理机只需要在底层一次性安装防护软件，不但降低了物理服务器整体资源开销，又降低了管理安全策略的部署和管理成本。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。



同时，针对之前遇到虚拟化进程中的防毒软件兼容性、补丁和代码更新、服务器重启、交叉感染、相互攻击和服务器性能问题，Deep Security 凭借在虚拟化安全上的创新功能，难关被一一击破。通过与 VMware VMsafe API 的结合，Deep Security 通过虚拟补丁的方式，在无需要求服务器重启、且把兼容性隐患降到最低的前提下，为服务器弥补各类操作系统以及应用

程序的漏洞产生的风险。并且，由于 Deep Security 是基于 VMware 底层防护，直接在物理层进行管理，这样就可以在网络威胁经过 vSwitch（虚拟网络交换机）交互时进行过滤和拦截，最大程度缩小虚拟化平台的防护单位。针对 vSwitch 的安全检测，弥补之前江淮汽车使用传统硬件防火墙无法防护同一台虚拟服务器内部互相攻击的不足。

邵科长表示："趋势科技的 Deep Security 服务器深度防护系统让我们十分满意，并且已经起到了非常好的防护效果。现在，淮汽车现在虚拟化第二期工程正在顺利展开中，针对所有虚拟化服务要实现的统一监控方面的需求，通过 Deep Security 的日志审计和完整性监控功能，实现了所有虚拟化服务器的安全日志审计、分析，以及重要路径、文件、注册表键值的监控，进一步帮助我们完成了安全策略审查的目标。"

通过趋势科技的不懈努力，江淮汽车的虚拟化平台迁移工作进展顺利，并且用户对趋势科技的技术和服务非常认可，目前已经将原有桌面端某品牌的防护软件，全部替换成趋势科技 OfficeScan 防毒软件，并表示愿意在未来信息化安全建设中与趋势科技保持更全面、紧密的合作。

+++