趋势科技 Deep Security 全面支持电科华云 KVM 平台 虚拟化安全再度"泛化"

[趋势科技中国]– [2014 年 10 月 28 日] 在虚拟化生态圈中，各类层出不穷的创新产品支撑着数据中心架构的不断演进，其中一匹黑马便是 KVM（Kernel-based Virtual Machine，内核级虚拟化技术）。近日，全球服务器安全、虚拟化及云计算安全领导厂商趋势科技宣布，其服务器深度安全防护系统（Deep Security）已全面支持中国电子科技集团公司旗下中电科软件信息服务有限公司（以下简称：电科软信）自主研发的华云 KVM 虚拟化平台。通过采用业内独有的"无代理"技术，从底层防护入手，让趋势科技 Deep Security 实现了传统防毒技术无法触及的领域，而从最初支持 VMware 到电科软信华云 KVM，该产品已经成为全球支撑范围最广、防护能力最强的虚拟化安全平台。

据了解，电科软信凭借自主知识产权的虚拟化技术，拥有多项虚拟化核心技术专利，其完全自主开发的华云 KVM 系列产品具有了高效的虚拟化、广泛的平台支持、公有云多租户架构等一系列创新特色。而在市场方面，凭借本土化优势，电科软信能够为国内用户的虚拟化平台建设提供更加便捷的帮助，共同促进云计算应用落地。而在安全层面，趋势科技 Deep Security 将为电科软信的华云 KVM 平台提供最佳的防护配合，全面应对各种虚拟化威胁，充分发挥虚拟化的成本和管理优势。

在技术层面，虚拟化技术可以将软件和硬件分离出来，最终实现所有可用资源的池化，而这恰恰是实现云计算业务模式并迈向软件定义数据中心的关键一步。尽管虚拟化技术源于上世纪 60 年代，在今天也取得了重要的地位，可它的安全情况却令人担忧。

在 IDC 发布的企业云计算调查报告中显示，实施云计算战略的最大难题或障碍是安全性、遵从性与可用性，其中 67%用户担心虚拟化的安全问题会发生在自己的身上。另外，Gartner 评估分析数据也显示，在数据中心虚拟化最常见的安全风险中，"未在虚拟化项目的初期引入信息安全措施"被列为首位，虚拟化风险导致的上层应用危险和数据泄露将为云端建设项目留下"致命伤"。

而“为虚拟化而生”的趋势科技 Deep Security 则是帮助用户突破技术瓶颈，实现主动性防御的最佳工具。这是因为在使用传统防病毒解决方案构筑的虚拟化安全系统中，当管理服务器请求多台虚拟机运行按需扫描或更新病毒库时，触发了所有虚拟机同时执行功能，从而导致对物理资源的需求出现瞬间激增，造成 CPU、内存、存储 I/O 和网络拥堵的情况发生。“病毒扫描风暴”的产生不仅会让数据中心的弹性计算优势不在，更会让虚拟机设计密度大打折扣。为此，Deep Security 完全抛弃了传统防毒的概念，从虚拟化底层的防护入手，其在资源消耗方面的节省使得组织可以大幅提升虚拟机密度。

据了解，从率先利用 “VMsafe”、“VMware vShield Endpoint” 等 API 技术实现 VMware 平台对接，到近期能够为电科软信华云 KVM 虚拟化环境提供全面的安全解决方案，Deep Security 所支持的虚拟化产品种类不断扩容。趋势科技已经在 Citrix Xen Server, Huawei FusionSphere, Microsoft Hyper-V, 电科软信华云 KVM 平台上都成功研发了无代理安全技术，全面实现了虚拟化安全环境的泛化支撑。另外，最新的 Deep Security 可以支持多租户架构，使得拥有软件定义数据中心的企业或服务提供商可以通过它向其用户提供与众不同、安全的多租户云环境。

###

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 1,500 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。