



趋势科技新闻稿

[即时发布]

互联网+跨界融合加速 云安全为信息化基础设施保驾护航

【趋势科技中国】2015年7月13日-“互联网+”开启了一个风起“云”涌的新时代。以云计算为基础设施的应用已经渗透于各个领域，这项技术帮助人们在成本更低的环境下创造产品+服务，实时分享、高效敏捷的处理数据。云计算也同样在信息安全领域掀起了一场“革命”，它化解IT消费化过程中对数据安全的担忧，阻挡不断演化的高级威胁，保护信息化社会的云计算基础设施，为“互联网+”保驾护航。

云计算高速发展，安全防护是关键

在“互联网+”时代，互联网跨界融合的创新浪潮席卷了各行各业，推动互联网与传统行业的横向整合与纵向重塑，云计算成为这种融合浪潮的重要基础设施的。工信部电信研究所发布的《2014年云服务白皮书》报告显示，95.5%的企业对云服务有一定认知，38%的企业已采用云计算应用。而且，更多的企业用户已经从注重云技术发展变化本身，转向为注重服务提供商的综合实力，寻找一个能满足企业和行业特点的云环境。

数据表明，这与云计算起步阶段的情况截然不同。在2011年，趋势科技做过一份详细的云计算应用问题调查，报告显示：“由于用户存在对基础设施和数据安全等方面的担忧，云计算应用进程明显受到了影响，平均只有10%的企业正逐渐把虚拟化技术运用到关键业务应用当中。”那么，从10%到38%，除了宏观政策导向，以及硬件基础设施安全性等方面的进步之外，是什么因素促成这一巨大变化呢？

对此，趋势科技（中国区）业务发展总监童宁认为：“作为一种在云端整合信息防护资源的创新模式，云安全改变了传统的网络威胁防御方法，重塑了信息安全管理体系统。这包括两点：其一，企业用户运用云安全技术，通过智能感知和自动优化，可以保护以云数据中心为代表的信息基础设施；其二，云安全厂商可以利用大数据分析技术和智能威胁评估技术，替代以升级防毒代码为方式的杀毒模式，为企业用户和个人消费者提供可信赖的安全防护能力。”

IT 应用加速创新，威胁防御“三大趋势”

当前，IT 应用的创新变化集中在个人终端移动化、数据中心云化，而网络攻击技术也向更加高级的定向式攻击演化：

第一，PC 和移动设备构成了消费者信息终端的多样化，用户会面对日益增多、不断精进的恶意程序和黑客攻击手法，而传统防护系统陈旧的防护模式也会在新的安全威胁下显得“无力”。

第二，虚拟化为基础设施的云计算数据中心，即：云计算模式的服务器、网络和存储设备皆以准备完毕，它们会让数据中心变得更为灵活，更自动化，这让数据中心的防御环境出现了巨大的变化。

第三，高级持续性威胁（Advanced Persistent Threat，APT）呈增长之势，APT 攻击者采用定制化的手段、利用社会工程学，有计划、有组织的持续窥探目标的弱点，长期潜伏并窃取核心机密数据，这让各个行业的组织都处于危险境地。

信息安全厂商必须针对威胁的数量、变化和速度，寻找解决方案，以应对今日的威胁演进，这包括能够对任何设备、任何应用、任何地点，提供有效防护。而趋势科技应对方法是全面企业用户防护战略（Complete User Protection，CUP 战略）。

作为 CUP 战略的重要核心，趋势科技利用云计算技术搜集了大量的威胁相关信息，然后运用大数据分析来发掘、交叉关联、分析新的威胁。这让我们可以通过成熟的云端基础架构来提供即时的防护，确保网络威胁治理在数量、变化与速度上，都能获得有效而高效率的管理。

发挥云安全价值，打造零风险世界

在 IT 消费化风险管理上，趋势科技与其他厂商纠葛在防毒代码产品层面的威胁防护技术不同。从 2013 年开始，就在 PC-cillin 云安全软件中首家提供了多平台、跨设备的超强实时云防护能力，全面支持 Windows、Mac、Android、iOS 平台的安全防护。可以迅速而准确地收集和识别新型威胁，在恶意程序入侵设备之前就进行主动拦截，实现了“防患于未然”的防毒效果。

在云数据中心安全架构演进方面，趋势科技推出以“无代理”为核心技术的 Deep Security，与虚拟化底层结合的方式进行安全防护，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，从而降低了企业的资本支出（CAPEX）和运营支出（OPEX）。在 2014 年底，趋势科技

Deep Security 已经在国内的金融、政府、制造业和中小企业用户中广泛应用，总计超过 2000 个公有云、私有云和混合云架构的数据中心，40,000 颗以上 CPU 的虚拟化系统，在使用 Deep Security 无代理安全技术来进行防护。

在高级威胁防御领域的最前沿，趋势科技是业内第一个提出云安全概念的企业，即今天能够利用趋势科技云安全智能防护网络（TrendMicro Smart Protection Network，SPN），帮助用户共同治理高级威胁的起点。目前，SPN 可以持续利用遍布全球的沙箱（Sandnet）、反馈机制、Internet 地毯式搜索，每天处理 100TB 的数据，以分析新病毒、网站信誉和垃圾邮件信息，收集发现 C&C 服务器，并且识别 C&C 服务器的变种。另外，SPN 在全球部署和共享威胁信息的机制，由 1500 位资深专家监测保障，可实现每 15 分钟内同步一次。

在云安全技术创新方面，趋势科技“一路领跑”，致力于打造出一个交换数字信息“零风险”的世界。趋势科技保持着 80% 研发费用投入云安全的业内最高水准，通过在“3C 领域”的不懈努力，发挥 CUP 战略的技术优势，在“互联网+”时代携手用户无惧威胁。

###



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。