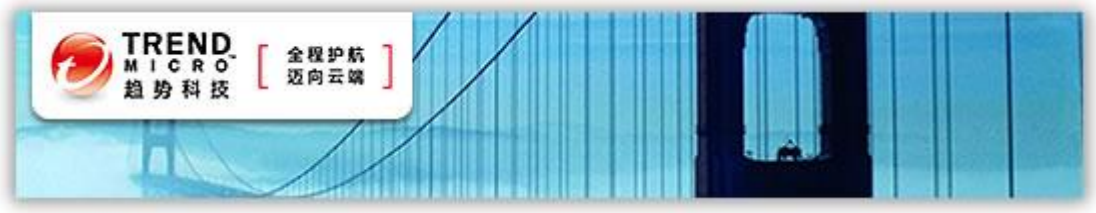

[趋势科技成功案例]

趋势科技为广西移动公司提供最佳的服务器漏洞攻击保护方案

创新管理全网运营服务器安全防御新组合保障业务安全运行

随着国内电信市场细化与用户认可度的广泛提高，移动通信公司的组织结构、业务特点都对自身的网络安全提出了更高的要求。为积极应对日益严峻的网络安全威胁，广西移动公司携手全球服务器安全、虚拟化及云计算安全领导厂商——趋势科技，在综合业务管理平台（简称：ISMP）的整体安全框架下，结合趋势科技服务器深度防御系统（Deep Security）和原厂专家服务（EOG），收到了良好的安全防御效果。

传统补丁管理方案无法支撑业务高速发展

随着广西移动数据业务的快速发展，服务器数量和网络规模不断扩大，加之与多种网络互联日益复杂，潜在网络威胁和风险都在逐步加大。据了解，目前广西移动数据业务系统尚未实施集中安全防护策略，业务系统和网络不但对外接口众多，同时又都各自为政，各业务平台安全防护水平参差不齐。而这些服务器所承载的核心包括了公司知识产权等诸多数据，必须依靠服务器的稳定运行，业务才能获得高速发展的动力。

据介绍，在广西移动制定的业务服务器运营制度中包含了一个非常重要的指标，这就是 7×24 小时不间断运行，但这个指标与“补丁重重”的现实环境却存在着巨大的矛盾。当前大部分的黑客入侵、木马注入等威胁，多是基于操作系统及应用程序的安全漏洞进行攻击。因此，为服务器及时升级系统及应用程序补丁是防御新形态攻击、保障服务器安全的唯一途径。各厂商发布的操作系统及应用程序每月会发布数以百计的补丁程序，而安装补丁之后，管理员必须重新启动服务器才能使补丁生效。另外，由于广西移动具备大量定制开发的业务，各厂商发布的安全补丁并不能保障能够与广西移动的业务兼容。一旦发生因为安装补丁而导致的业务访问中断问题，“回滚”的难度极大。

面对以上的困境，即使广西移动已经采用了包括补丁分发系统、软件防火墙、漏扫工具等系

统，却都不具备服务器在线修复的能力。因此，为了满足业务不中断的需求，就需要在找出一种创新性的漏洞攻击防护安全方案（无需重启动系统），不但要确保服务器安装到最新的系统及应用程序补丁，同时也不会对广西移动的业务带来任何的影响。

Deep Security 深度防御服务器补丁管理后顾无忧

在把市场上所有的服务器安全防御系统进行了充分评估之后，广西移动的 IT 技术部门与趋势科技运营商行业资深技术顾问杨嗣鹃经过反复交流后，最终决定使用趋势科技 Deep Security 的深度包检测技术作为全网运营服务器补丁管理方案，以此解决上述问题。

当前，所有基于漏洞进行的攻击，其数据包中必定包含特定的指令。当目标服务器具备某种特殊的应用并收到这种数据包时，就会因为执行了这些特定的指令而被获取管理员权限，进而被控制。基于这种攻击的原理，Deep Security 的深度包检测技术实现了这些攻击数据包达到服务器之前，就进行内容检查。通过漏洞攻击规则及智能规则对数据包包含的指令进行比对，一旦发现触发安全规则的数据包，就可以根据预定的策略进行监控、丢弃或阻断的动作，保障服务器的安全。

据了解，对于已知的漏洞，Deep Security 对广西移动公司内部运行的各种应用程序（包括数据库、Web、电子邮件和 FTP 服务器）提供开箱即用的漏洞防护，使其免受了无数次的漏洞攻击。对于最新发现的漏洞，Deep Security 能够在第一时间提供修补程序，在无需重新启动系统的前提下，即可在数分钟内将这些规则应用到数以千计的运营服务器上。同时，Deep Security 通过独有的技术，能够把监控到的漏洞攻击信息实时上传到移动内部的 ISMP 上，并通过工单系统把对应的攻击源头处理责任分派到对应的管理员，形成一套有效、快速的处

理机制，极大提高了广西移动公司对安全事件的响应效率。

广西移动安全专职工程师杨明表示： “趋势科技服务器深度防御系统，能够以非入侵式的方案对运营服务器提供漏洞防御能力，有效解决了困扰多年的服务器补丁管理难题，是一套革新性的补丁管理方案。在过去的 2011 年中，广西移动全网都没有发生因漏洞攻击造成的生产事故。最为关键的则是，多项技术的融合使得我们通过 Deep Security +ISMP 的方式，形成了新型网络威胁防御组合，这受到广西移动公司乃至集团总部的一致认可。

###

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。