概况

行业
运营商

公司总部
南宁

移动电话客户
2500多万户（2011年）

区域市场运营分公司
14个

网站
http://gx.10086.cn/

构建新型网络威胁防御组合 保障业务安全运行

—— 趋势科技为广西移动提供服务器漏洞防御方案

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。

—— 杨明 广西移动安全专职工程师

简介

目标
广西移动希望找出一种创新性的漏洞攻击防护安全方案，不但要确保服务器安装到最新的系统及应用程序补丁，同时也不会对公司的业务带来任何的影响。

解决方案
广西移动决定使用趋势科技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的核心，以此解决传统补丁方案存在的问题。

业务影响
- 修补补丁不会对业务产生任何影响
- 形成一套有效、快速的处理机制，提升了广西移动对安全事件的响应效率

随着国内电信市场的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，采用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，多种网络互联日益复杂，潜在网络威胁和风险都在逐步增多。但是，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，而且又都各自为政，各业务平台安全防护水平参差不齐。而这些服务器承载了公司知识产权等诸多机密数据，必须实现安全稳定运行，方可让业务获得高速发展的动力。

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。各厂商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其生效。另外，由于广西移动拥有大量定制开发的业务系统，各厂商发布的安全补丁并不能保障能够与广西移动的应用程序兼容。一旦服务器安装补丁后发生业务访问中断等问题，“回滚”的难度极大。

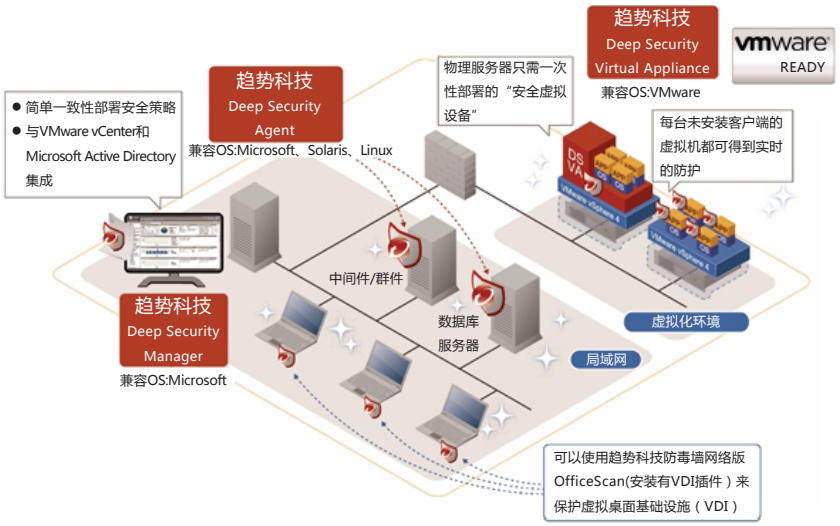
面对以上的困境，即使广西移动已经采用了包括补丁分发系统、软件防火墙、漏洞扫描工具等安全措施，却不具备服务器在线修复的能力。因此，为了满足业务不中断的需求，就需要找出一种创新性的漏洞攻击防护安全方案（无需重启动系统），不但要确保服务器安装到最新的系统及应用程序补丁，同时也不会对广西移动的业务带来任何的影响。

即使广西移动已经采用了包括补丁分发系统、软件防火墙、漏洞扫描工具等安全措施，却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影响。

—— 杨明
广西移动安全专职工程师

Deep Security深度防御让服务器补丁管理后顾无忧

在对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进行了反复交流，并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的核心，以此解决上述难题。



趋势科技Deep Security部署图

Deep Security的深度包检测技术实现了在攻击数据包达到服务器之前，就进行内容检查的目标。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。

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广西移动内部的ISMP上，并通过工单系统把对应的攻击源头处理任务分派到对应的管理员，形成了一套有效、快速的处理机制，提升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。“