



[趋势科技成功案例]

## **趋势科技为中国移动手机动漫基地撑起互联网“保护伞”**

### **高性能 IWSA 10000 构建园区网 Web 安全典范**

位于福建省中国移动手机动漫基地（以下简称：动漫基地）在准确把握市场机遇、业务高速增长的同时，遇到了内部多企业用户统一安全管理，Web 威胁防护产品效果差、性能低等一系列问题。为了实现全面提升用户网络应用效率和安全防护水平的目标，动漫基地携手全球服务器安全、虚拟化及云安全领导厂商——趋势科技，应用了基于趋势科技 Web 信誉评估技术的安全网关——IWSA 10000 利用云安全技术成功防范了来自互联网的 Web 威胁。

#### **Web 威胁滚滚而来，内忧外患如何应对**

2010 年 4 月，中国移动手机动漫基地正式落户厦门，基地旨在优秀动漫资源和手机客户的需求之间搭建起桥梁，为产业注入蓬勃活力。目前，动漫基地已云集近 400 家合作企业，动漫业务用户已超过 700 万。但是，在动漫基地用户高速增长的同时，为企业提供统一网络服务的 IT 部门却遇到了前所未有的挑战，这包括：外部互联网安全环境的进一步恶化、内部多企业用户统一安全管理复杂、用户安全意识薄弱、过度依赖终端防护、Web 威胁防护产品效果差、性能低等一系列的问题。

在外部，黑客攻击日渐猖獗，数据泄露威胁日益严重，严重影响了在线业务的发展。随着病毒黑色产业链不断发展，恶意 Web 地址链接、钓鱼网站及裹挟着社交工程学的黑客攻击不断增多，单一的基于终端防毒的防护架构，已经不能应对动态变化的威胁。利用“火焰”、“高斯”、“红色十月”病毒等实施的高级持续性威胁（Advanced Persistent Threat，简写 APT）活动频现。

在内部，入驻动漫基地的合作企业信息安全标准参差不齐、使用的安全产品也五花八门，频繁的病毒感染事件让运维工作超负荷运转。同时，由于动漫设计人员需要经常访问各类论坛、图片网站和各类国内外动漫网站，这容易导致其感染网站上的各类病毒木马和僵尸程序。由于对网络和计算机安全防护知识了解不深，许多终端的漏洞补丁未能及时安装部署，利用漏

洞进行攻击的蠕虫病毒在内网常出现交叉感染的情况。而一旦出现安全事件，就需要 IT 运维管理员手动病毒清理、重装系统，大大降低了工作效率。最令他们担心的是，一旦动漫设计资料的存储服务器受到病毒的攻击或破坏，将严重影响企业的运作。

有鉴于此，动漫基地考虑为其合作的 400 家企业撑起能够统一抵御互联网 Web 威胁的保护伞，在不改变设计人员工作模式的情况下，最大限度地降低访问互联网资源时接触各类恶意程序的概率。

### **突破网关性能瓶颈，唯有云安全技术**

Web 应用已经成为了众多企业核心业务开展的基石，但这也引发了网络攻击威胁的上移，传统的 2-4 层攻击已经越来越多地迁移到了应用层。因此，整体防御体系的建立不但需要功能丰富的安全产品，更需要主动性防毒架构来承载。显然，最佳的做法是在网关入口处过滤掉恶意代码，切断终端接触到的病毒源头。然而，当企业内部用户数量过多或是 Web 传输流量过大的时候，能够应对 Web 威胁的安全网关就会出现性能瓶颈，而且，这一瓶颈会随着园区的业务发展变得越来越严重。

据介绍，作为新兴高科技产业园区的典范，入驻动漫基地的企业数量已经达到了几百家，而这一数字还将随着移动互联时代的发展而迅速增长。即使每个企业当中的终端数量按照小型企业规模计算，相加后，也达到了上万台。大量的终端以及动漫企业利用网络传输超大图片、高清图材的应用特点，都给防毒网关产品提出了近乎苛刻的性能要求。据动漫基地的网络安全专家介绍，在产品选型期间，他们主要考虑以下 4 项权重最高的指标：

- 1、性能上能否支撑数百家企业，数万台计算机访问互联网的请求；
- 2、互联网恶意流量过滤的实时性和准确性；
- 3、互联网恶意站点信息搜集的全面性；
- 4、能否阻挡互联网 C&C 服务器对网内已经感染僵尸程序终端的控制命令。

带着这些指标，动漫基地与多家国内外知名的安全厂商进行了长时间的技术交流及产品测试，但这些产品或是因为功能所限、或是因为性能不达标，都无法同时满足以上 4 点需求。最终，趋势科技的 Web 安全网关——IWSA 10000 凭借“电信级”的处理性能和独有的“Web 信誉评估技术”，在多轮的严格测试中脱颖而出，解决了整个园区终端用户的 Web 威胁防御难题。

在整个测试期间，趋势科技利用其遍布全球的云安全监测平台，借助独有的 Web 信誉评估技术（WRT），可以将网页按照自身的 50 多种属性划分为不同的安全等级。在访问这些网

站时，用户都会得到是否安全的提示，并自行阻断对恶意网页的访问。WRT 是趋势科技“云安全”的关键组成部分，IWSA 10000 通过这项技术，彻底解决了动漫基地中一些终端没有安装防毒软件和防毒代码过期的问题。与此同时，因为可以将 70%威胁特征码放在云端，因此它能够减少用户层面 70%的核心内存占用，减轻了高带宽下的出口设备负载，这些都是传统防毒网关的病毒代码比对技术所无法比拟的。

### **切断恶意站点接触点，为动漫业务保驾护航**

在 IWSA 成功上线之后，及时拦截了恶意站点的 URL 访问，并成功阻断了木马、僵尸程序、病毒攻击的非法流量。对于网内客户端已经感染的木马僵尸程序，IWSA 成功阻止这类恶意代码对 C&C 服务器的回拨，阻断其从互联网下载恶意代码的更新程序，有效杜绝了各类恶意代码变种的产生。据介绍，通过一段时间的使用，动漫基地病毒事件的日志数量降低了 80%。另外，通过分析 IWSA 的报表统计可以发现，大量恶意站点的连接在形成文件传输之前就已经被 IWSA 成功拦截，真正实现了病毒安全事件的事前防御。

中国移动手机动漫基地的信息安全专家李先生表示：IWSA 符合云动漫基地的运营特点以及工作模式，真正起到了为业务保驾护航的作用。通过 IWSA 集成的云安全技术，能够实现在互联网的恶意代码进入网络之前进行主动拦截，有效保障了各动漫企业的工作环境，使设计人员能够畅通无忧地访问互联网。

###

### **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](http://www.trendmicro.com.cn)。请访问 Trend Watch：[www.trendmicro.com/go/trendwatch](http://www.trendmicro.com/go/trendwatch) 查询最新的信息安全威胁的详细资讯。