多层次安全防护架构，让病毒无所遁形

趋势科技为红云红河烟草集团生产系统保驾护航

作为引领全国烟草行业信息化建设的创新企业代表，红云红河烟草（集团）有限责任公司（以下简称：红云红河集团）携手全球服务器安全、虚拟化及云安全领导厂商——趋势科技，从终端、边界到网关处处防护，积极应对日益严峻的网络安全威胁。红云红河集团信息中心利用趋势科技 IWSA、NVWE、Server Protect 和 OfficeScan 建立了多层次、立体化安全防护架构，其良好的安全防御效果更受到了员工和集团各级领导的一致认可。

传统安全体系“不给力”，无法应对应用层威胁

红云红河集团成立于 2008 年 11 月 8 日，是以烟草为主业，跨地区经营的大型国有企业，下辖昆明卷烟厂、红河卷烟厂、曲靖卷烟厂、会泽卷烟厂、新疆卷烟厂、乌兰浩特卷烟厂六个生产厂，控股山西昆明烟草有限责任公司和内蒙古昆明卷烟有限责任公司。其核心品牌“云烟”、“红河”更是“中国驰名商标”和“中国名牌产品”。

红云红河集团非常重视企业的信息安全建设，早在上世纪 90 年代就投入大量资源，对内部的安全架构进行加固，包括防火墙、IPS 等，但这些网络层的传统安全设备对于随时翻新的应用层病毒攻击效果欠佳。另外，随着国内外高级持续性威胁（APT）事件不断增多，国务院在 2012 年出台了《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发[2012]23 号），以此督促国内重要企业在工业控制安全方面的建设。

据红云红河集团信息中心安全专员介绍：由于传统安全设备不能阻断应用层的攻击，红云红河集团对病毒攻击的唯一防御就是部署在终端系统的网络版防毒软件。但由于终端用户的安全意识往往非常薄弱，杀毒软件的防毒机理又相对落后，导致防护效果不佳，病毒感染事件屡屡发生，这给红云红河集团办公网络和生产系统带来巨大的影响。鉴于以上考虑，红云红河集团急需一套完整、高效的立体化安全防护架构，解决病毒带来各种影响生产系统稳定运行的问题。

从病毒进入源头入手，“三道防线”打造立体防御体系

针对安全架构与应用层威胁 ,红云红河集团信息中心的安全专员与趋势科技的众多技术顾问与进行多次的深入沟通,对病毒入侵的关口,以及现有安全防御体系中的薄弱环节进行了深入的分析。

首先,双方针对现有网络架构中的外部威胁和病毒入口进行了分析。由于红云红河集团及下属分支机构均具备独立的 Internet 出口，虽然中间有防火墙验证访问的合法性，但仍会受到来自互联网以 HTTP、FTP 等数据流为载体的潜在威胁。通过对原有防毒系统的日志分析得知,超过 80%的病毒都是通过 Web 应用进入红云红河集团内部网络的。因此，要做到入口安全，首先就是要对 Internet 边界访问提供一个能过滤最新病毒的关卡。

其次，针对内网安全管理现状分析后发现， 对十分重要的生产网络而言，Windows 终端平台和 U 盘等移动设备则是传播病毒的“沃土”。由于 Windows 终端用户安全意识参差不齐,导致部分终端经常出现没有部署防病毒软件,或者防病代码没有更新等状况。而黑客往往利用这个“人为”弱点,轻易地把已知病毒植入到终端计算机上。另外，U 盘等移动外设是红云红河集团生产网络病毒交叉感染的又一条主要通道。为了工作的方便，员工会把 U 盘作为办公网、生产网以及家庭 PC 的数据媒体。由于三者间的病毒情况根本无法确认，所以病毒就会通过这个途径迅速的扩散到其他终端上。

根据对网络隐患和终端环境分析结论是 :传统的安全防护体系并不能协助红云红河集团有效应对新形态病毒的攻击。只有从技术、服务、流程三方面同时加强，才能把红云红河集团的安全防护体系立体化加固。并最终确定了“端到端”的立体防护架构，而所有安全产品都通过集中控管中心，实现统一管理、集中配置，这包括：

- 第一道防线：在各个互联网边界部署防病毒网关 IWSA，提前拦截来自互联网的威胁，降低终端用户因为访问恶意站点感染病毒的机率；
- 第二道防线： 在关键网络边界部署网络防毒墙 NVWE，对所有接入网络的终端实施强制安全策略，提升全网安全级别；
- 第三道防线：在全网所有 Windows 终端上部署趋势科技网络版 OfficeScan，利用 OfficeScan 特有的 U 盘外设控制技术，解决内部 U 盘病毒扩散的风险。

终端+边界+网关“组合拳”出击，打击病毒入侵更有力

在互联网边界部署了防病毒网关 IWSA 后,由于启用了趋势科技独有的 Web 信誉评估技术（WRT),拦截了大量由内部用户发起的，对可疑高风险 URL 的访问。另外，通过 NVWE 在全网加载强制安全策略,使终端用户必须更新了病毒库及安全补丁后方能接入网络,大大加强了终端计算机的安全系数，避免了因终端使用者安全意识不强，导致的病毒入侵问题。

对于之前担心的 U 盘病毒扩散，通过在全网终端部署 OfficeScan 并启用了“高级外设控制功能”，这便能够在 U 盘接入电脑时，对包含在 U 盘中能够自动注入内存的病毒进行清除，有效提高了红云红河集团对 U 盘病毒的控制。

据红云红河集团信息中心的安全专员介绍：趋势科技提供的立体安全防护架构，从终端、边界到网关处处防护，相对于传统方案能更好地帮助集团解决病毒带来的问题，保障了集团生产系统的不间断运行。趋势科技立体化、层次化的防护架构完成之后，红云红河集团未曾发生过重大安全事故，并且病毒感染事件也下降了 80%，其防毒效果和网络体验受到红云红河集团信息中心及集团领导的一致认可。

###

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 1,500 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。