



趋势科技成功案例



趋势科技 OfficeScan 护航利丰汽车集团“5 年” 病毒爆发事件保持“0 记录”

当前，全球范围的恶意程序已经发现超过 1.4 亿个，每天新增恶意程序 20 万个，即每秒 2.3 个。而在网络威胁不断进化的大背景下，利丰汽车集团（以下简称：利丰汽车）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，在采用趋势科技防毒墙网络版 OfficeScan 长达 5 年的时间里，整个集团网络中未发生任何一起大规模病毒爆发事件，真正构建起了可以完全信赖、长期且有效的终端安全防护体系。

实现集团愿景 需要一个“无忧网络”

利丰汽车是中国汽车流通行业具影响力的汽车经销商企业之一，旗下拥有 18 个分支机构，代理经营 30 余个汽车品牌，拥有 200 多家汽车门店、数百家销售服务网点。作为心怀远大的企业，利丰汽车希望全面整合中国汽车产业价值链，成为最具竞争力的汽车生活综合服务厂商。而需要达成这一共同愿景，执行“以客户为中心”的经营理念，必然是利丰人需要思考的问题。

对此，利丰汽车信息技术部主任郭勇飞表示：“在汽车经销商行业，客户是我们的根本，客户服务是我们企业每个员工、每个部门都需要做到的，IT 部门也不例外。所以，为客户提供良好的 IT 服务是我们每个 IT 人员的责任，更不能因为网络安全影响整体应用效果。为此，利丰的信息化，从网络建设、业务系统、运维服务、威胁管理上都要给客户提供便捷而安全的无忧网络。”

据介绍，为了演好“开路先锋”的角色，利丰从 2008 年开始了一系列信息系统整合与升级工作。为了解决各个分公司网络中的信息孤岛，消除局域网内的 ARP 攻击和病毒爆发情况，实现手机和其他智能终端通过无线网访问业务系统、减少因会议沟通造成的高额差旅费问题，利丰汽车信息技术部启动了广域网、局域网、无线网建设项目。先后搭建了以呼和浩特为总部，辐射内蒙古全境分公司的 VPN 虚拟专用网络、BYOD 业务平台，从而使分散的分公司与总部构建成为一个大局域网，数据传输的更加高效、稳定、安全。同时，为了解决终端网络安全，公司在利用微软活动目录（AD）整合技术的基础上，需要为每一个端点配备最有效的防毒系统。

OfficeScan 发挥云安全特性 防毒效果前后对比明显

2008 年 9 月，鉴于局域网病毒感染与单机数据丢失的情况屡有发生，利丰汽车信息技术部决定采购可以支持集团统一管理的防毒软件。而在对比各大厂商防毒产品后，最终选择趋势科技与另外一家知名厂商的参与试用，通过自身 PC 机配置情况、结合技术、防毒效果、价格等多方面的对比，利丰汽车最终选择了趋势科技的 OfficeScan 产品，并在随后 5 年中经历了多次版本更新，彻底消除了大规模病毒爆发事件的发生。

据郭主任介绍：“在没有统一部署 OfficeScan 之前，零散的、不同厂商的防毒产品在集团内部虽有部署，但并没有发挥作用。两次大规模的病毒攻击，都是由外向内、交叉感染，直接造成局域网瘫痪，业务中断。而 IT 人员想要在众多的终端上，用最短的时间找到感染源也绝非易事。但在部署 OfficeScan 之后，利丰汽车借助趋势科技产品后台先进的云安全技术，使得防毒系统的资源占用率大幅下降，防毒效果也十分明显。ARP、木马攻击行为基本为零，受到恶意 URL 和钓鱼网站攻击的事件也明显降低。”

在部署方面，管理员通过微软活动目录的组策略配置，利用 OfficeScan 的 Client package 工具自动制作安装文档(MSI 格式)，对总部的终端进行自动部署。而对于分支机构，则通过 Web 形式，以更简便的方式对防毒墙网络版客户端进行部署或升级。

在管理方面，通过趋势科技防毒墙控管中心 TMCM，利丰汽车信息技术部对整个集团的所有分公司和 4S 店的客户端，都实现了更智能的统一管控。管理员可以实时获取上全网所有终端的健康状况，从而实现了 Web 病毒自动拦截、内网感染及时定位的防护预警机制。

合作步步深入 让安全“与时俱进”

据了解，在应急响应和配套服务方面，趋势科技原厂工程师的服务水准在长期合作中获得了利丰汽车的一致认可。在 OfficeScan 部署初期，针对应用问题，趋势科技的工程师实地考察，对不同配置和业务职能的终端采取了定制化的优化策略，让各类具体应用难题逐一化解。其中，某分支机构出现的一支最新的病毒，趋势科技了解情况后，第一时间到现场对病毒取样，并送交趋势南京研发中心开发了特定的防毒策略，而此策略下发到利丰汽车局域网内的趋势服务器后，病毒被及时查杀，而集团所有终端也自动形成了有效防护。

据介绍，为了帮助各级机构提升网络安全防护意识，利丰汽车整个集团利用趋势科技的产品，在绩效管理方面也发挥了作用。郭主任表示：通过设定，我们会将集团与各分公司的趋势杀毒服务器上的报表功能开启，制定邮件通知策略，将各个分支机构病毒周报、月报情况发送

给各自分公司的 IT 同事，由 IT 同事负责处理跟进。集团则收集所有分公司的病毒情况，制定不同计划并根据反馈情况，制定分公司 IT 考核方案。

在长达 5 年的合作中，不但双方的工程师在工作细节上已经达成了默契，趋势科技也在利用最新的产品、技术、服务，将这份合作步步深入，在网络威胁管理协助利丰汽车与时俱进。而正在试用和准备部署的产品包括：为应对 Windows XP 服务下线的虚拟补丁功能、针对外网防护的 IWSA 安全网关、洞察终端和网络层威胁的 TDA 等等。

###



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。