

# 西安地铁 (西安地下铁道有限公司)

## ——确保您的出行一路畅通

### 解决方案概览

用户: 西安地铁 (西安地下铁道有限公司)

国家/地区: 中国

行业: 交通运输

### 应用需求

西安地铁公司拥有大量的业务系统、服务器、PC和分子公司的IT管理公司, 希望有效地确保IT管理制度执行到位、高效率响应日益增多的客户端的系统维护任务、高效率地安装补丁分发软件、实时掌握公司设备资产。

由于各终端的安全配置及打补丁情况参差不齐——不但数量多, 而且分布非常分散, IT管理人员需要了解每一台机器上补丁更新的情况。而且新业务层出不穷, 终端上的应用也需要随着新业务的推出而不断变化, 西安地铁要及时对所有的终端进行升级, 更要避免在升级时出现病毒或者有威胁的程序通过光盘或其他维护工具、U盘带入。

### 解决方案

西安地铁选择了由LANDesk管理套件和LANDesk安全套件方案+防病毒组件组合而成的终端系统信息监测平台来满足西安地铁对终端系统的管理。

LANDesk终端系统信息监测平台提供了先进而实用的功能, 能够满足西安地铁终端的部署环境及应用系统要求, 进行资产管理、补丁管理以及常用程序的分发、终端应用管理、应用白名单管理、防病毒管理, 并提供各类自定义报表功能, 能够帮助用户高效率管理分布地域广的终端系统。LANDesk的可扩展性强, 除了基本的报表功能, 还可以为用户提供量身定制的终端报表系统的开发服务。

### 应用效益

借助LANDesk管理套件和安全套件, 西安地铁建设了一个统一的终端软件信息监测平台, 定期统计全行终端设备上安装的软件信息、防病毒软件更新, 建立操作系统补丁更新技术平台, 对终端上运行的软件情况进行监测, 及早发现不符合信息安全规范的行为并定期发布安全报告, 有助于提高西安地铁终端软件信息安全管理整体水平。

“虽然西安地铁应用LANDesk终端软件的时间不长, 但是已经取得了初步成效, 不但大大减轻了我们平时维护终端的工作量, 更使我们的安全管理工作从被动防御变为主动防御, 让我们对终端的信息安全更加放心。”

——西安地铁信息中心主管

### 企业概况

1994年, 西安市提出城市快速轨道交通线网规划, 由4条线组成, 线网总长度73.17公里, 并纳入1999年经国务院批复的《西安城市总体规划(1995—2010年)》。

2004年, 西安市重新编制了城市快速轨道交通线网规划, 其目标是形成以公共交通为主体, 轨道交通为骨干, 其它公交为辅助的多元化、快速、高效、环保的城市公共交通体系, 实现公共交通的可持续发展, 形成“棋盘加放射型”的城市快速轨道交通线网布局。轨道交通线网远期规划由6条线组成, 总长251.8公里。

地铁公司拥有大量的业务系统、服务器、PC和分子公司的IT管理, 为了更加科学有效地管理这些终端设备, 并且确保其信息安全, 西安地铁选择了LANDesk管理套件和安全套件对PC进行管理。借助系统的应用, 西安地铁通过一个集中的终端软件信息监测平台, 就能对众多终端PC进行软件合理升级、系统补丁检测, 阻止不合规软件的安装, 并且实时监控病毒防护情况, 对报警信息进行处理。

### 应用需求

终端的管理一直是IT管理的难点, 因为需要保证业务的连续性, 而且分布在不同地方的终端品牌可能各不相同, 应用的系统以及维护工具也各不相同。但是, 一旦这些终端因为中毒、主机硬盘空间不足等原因导致停机或者出错, 就会严重影响正常的业务运行, 还会影响政府的形象, 甚至带来不可估量的财产损失。

西安地铁同样面临这样的问题。西安地铁目前拥有300多台终端, 主要运行Windows操作系统。众所周知, Windows操作系统安装容易管理难, 如何更加合理地管理这些终端对西安地铁的IT管理部门来说, 是个很大的挑战: 一方面, 由于这些终端是由多个供应商提供的, 各终端的安全配置及打补丁情况参差不齐——终端不但数量多, 而且分布非常分散, IT管理人员不可能到每个终端上去操作, 过去西安地铁终端上的补丁往往都是由供应商直接去执行的, 是否每一台机器的补丁都得到更新却无从得知; 另一方面, 新业务层出不穷, 终端上的应用也需要随着新业务的推出而不断变化, 西安地铁要及时对所有的终端进行升级, 更要避免在升级时病毒或者有威胁的程序通过光盘或其他维护工具、U盘带入。

他们首先要解决的问题是如何收集并更新这些终端的基本信息, 如品牌、型号、具体安装位置、终端设备类型、业务柜员号, 同时还要了解终端安全性状态(如防病毒状态、主机硬盘使用空间、主机正常开机时间、内存占用情况、补丁更新情况), 然后还要增强终端日常维护时对现场操作员的管理, 特别是终端上运行的程序控制, 对型号不同、应用系统各不相同的终端进行补丁更新和程序控制, 建立终端厂商维护工具的认证流程和审批流程。

为了把IT信息安全做得更好, 西安地铁信息中心主任亲自主抓终端机的管理, 并且对很多相关的供应商进行考察, 希望能够在技术上有所突破。

## 解决之道

考虑到西安地铁终端数量庞大、地域分布散、应用复杂、终端控制难度较大的实际情况，项目实施要涵盖西安地铁300多台终端，项目实施不能过于复杂等多种因素，同时充分考虑了产品的可扩展性、在资产管理方面的专业性、灵活性、产品对特殊生产条件的适应性，以及对用户需求的匹配性，在对多个同类产品进行综合评估之后，西安地铁最后选择了由LANDesk管理套件和LANDesk安全套件方案+防病毒组件组合而成的终端系统信息监测平台来满足西安地铁对终端系统的管理。

LANDesk终端系统信息监测平台提供了先进而实用的功能，能够满足西安地铁终端的部署环境及应用系统要求，进行资产管理、补丁管理以及常用程序的分发、终端应用管理、应用白名单管理、防病毒管理，并提供各类自定义报表功能，能够帮助用户高效率管理分布地域广的终端系统。LANDesk的可扩展性强，除了基本的报表功能，还可以为用户提供量身定制的终端报表系统的开发服务。

值得一提的是，西安地铁之所以选择LANDesk，还有一个非常重要的原因，就是他们拥有基于学习模式的白名单技术。程序的白名单管理技术的好处在于：只有合法的软件才可以安装在终端上，而不合法的则不允许，这使西安地铁的安全管理从原来被动防御变成主动防御。但是白名单控制同样会带来管理上的复杂性，白名单源从何而来是个问题，并且如果设置了白名单，今后每发布一个系统补丁，升级一个应用都需要大量的人工操作去修改维护白名单，工作量太大，不具可操作性。经过详细的测试和论证，LANDesk在提供白名单技术的同时，还提供了自动学习以及信任签名的技术。

自动学习模式和信任签名技术方便了管理维护名单：白名单不需要人工输入，可自动从主机上获取，只需将主机的合法应用执行一次，系统会自动记录下执行过程关联的程序列表，自动加载清单；一些安全厂商的程序，比如微软的补丁、病毒定义程序，都不需要经过认证，因为程序已被微软和第三方软件公司做了数字签名，LANDesk可以识别来自不同厂商的签名，减少了名单的维护量。

## 应用效益

借助LANDesk管理套件和安全套件，西安地铁建设了一个统一的终端软件信息监测平台，定期统计全行终端设备上安装的软件信息、防病毒软件更新，建立操作系统补丁更新技术平台，对终端上运行的软件情况进行监测，及早发现不符合信息安全规范的行为并定期发布安全报告，有助于提高西安地铁终端软件信息安全管理整体水平。

## 安全管理层次提高

LANDesk管理套件是一个完全集成的、跨平台的模块化桌面管理解决方案，能够在单一的控制台上对管辖范围内的服务器和各种终端设备的桌面进行远程控制和管理，方便地对复杂而易变的终端设备资产进行高效跟踪和统计，远程安装和配置操作系统和应用程序，能够帮助西安地铁快速定位并解决问题。而LANDesk安全套件既是一个独立的解决方案，又能与LANDesk管理套件无缝集成，从而使得西安地铁能从一个统一的控制台——终端软件信息检测平台就能实现全面的安全管理，特别是通过白名单技术来控制终端信息安全，更是使得西安地铁的安全管理从被动防御提升为主动防御，安全管理提升了一个层次。

目前，在已经部署LANDesk解决方案的设备中，所有主机的防病毒状态都可以一目了然，帮助IT管理部门诊断防病毒的实际状况；能实时掌握所有主机的程序运行情况，是否存在非法程序，并且在第一时间邮件通知管理员以进行处理；能够提供定制的报表界面，以更加适合西安地铁IT管理人员的使用习惯，可以和西安地铁将来的业务考核进行结合；借助LANDesk解决方案，西安地铁基本形成了终端主机上程序的运行审批制度，非认证的程序无法执行，并且会报警，第一时间邮件通知管理员，主动地防御来自内部的安全威胁。

西安地铁信息中心主管高兴地说：“虽然西安地铁应用LANDesk终端软件的时间不长，但是已经取得了初步成效，不但大大减轻了我们平时维护终端的工作量，更使我们的安全管理工作从被动防御变为主动防御，让我们对终端的信息安全更加放心。”

## 一个平台管理所有的终端

近年来，随着信息化建设的不断深入，IT系统的复杂性也日益凸现，对IT管理系统的需求也随之增加。这种需求不仅体现在对复杂的大型机管理需求上，还包括桌面系统、移动设备、服务器的管理，同时，零散分布的终端系统的管理也变得越来越复杂。

西安地铁利用LANDesk解决方案，借助终端软件信息检测平台来集中管理数量庞大的终端的做法，无疑是给终端管理较为复杂的大中型企业的桌面管理提供了一个很好的借鉴。

据了解，在西安地铁的终端软件信息监测平台全部部署完毕以后，借助终端软件信息检测平台，西安地铁的IT管理部门可以集中掌握全公司终端防病毒软件的防护情况；可以集中查处终端设备上安装了哪些软件；可以控制终端上运行的程序，只有经过授权的程序才能在终端上运行；可以对终端厂商的维护工具进行报备、授权管理；并且对终端上异常的程序运行进行报警处理。