

上海浦发银行

——一个平台确保3500台ATM安全



解决方案概览

用户：上海浦东发展银行
国家/地区：中国
行业：银行

应用需求

银行的IT信息安全管理至关重要。分布很分散的ATM的安全防御非常复杂，是银行信息安全管理薄弱环节。针对ATM分布零散、不易管理的特点，浦发银行希望建设一个系统集中、管理分散的ATM软件信息监测平台，定期统计全行ATM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ATM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，从而提高浦发银行ATM软件信息安全管理整体水平。

解决方案

在充分考虑到产品的扩展性、在资产管理方面的专业性、产品对ATM特殊生产条件的适应性，以及和用户需求的匹配性，特别是基于学习模式的白名单技术，上海浦东发展银行最终选择了蓝代斯克管理套件和安全套件。浦发银行是我国银行业跨平台ATM管理中选择白名单技术的第一家。

应用效益

上海浦发银行在部署蓝代斯克管理解决方案之后，可以集中掌握分布在各地的防病毒软件的防护情况；集中查出ATM设备上多安装了哪些软件；限制ATM上运行的程序，只有经过授权的程序才能运行；对ATM厂商的维护工具进行报备，授权管理对ATM上异常的程序运行报警信息进行处理。

- 安装简便，高效部署
- 安全状态，一目了然
- 主动防御，堵塞漏洞
- 补丁管理，尽在掌控

“由于分布分散，却至关重要，对ATM系统的管理一直都是银行IT管理的一个难点。随着信息化建设的不断深入及业务的不断更新，ATM管理必须打破原有思路，选择合适、高效、稳定、兼容性良好的管理平台辅助管理非常必要。浦发银行应用蓝代斯克ATM软件信息监测平台的时间虽然不长，但是已经取得了初步成效，不但大大减轻了我们平时维护ATM的工作量，更是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ATM的信息安全更加放心。”

——浦发银行信息中心主管

用户概况

上海浦东发展银行是1992年8月28日经中国人民银行批准设立，于1993年1月9日正式开业的股份制商业银行，总行设在上海。截止到2008年底，全行总资产规模已达13094.25亿元人民币，实现税后利润125.16亿元人民币，并在全国范围开设了34家分行，机构网点总数超过491家。浦发分布在全国34个分行的ATM存取款设备大约3500台。一直以来，这些分布分散的ATM的管理，特别信息安全管理，是浦发银行IT管理的难点之一。为了更加科学有效地管理这些ATM，并且确保其信息安全，浦发银行选择了蓝代斯克管理套件和安全套件来对ATM进行管理。借助系统的应用，浦发银行通过一个集中的ATM软件信息监测平台，就能对3500台ATM进行终端软件的合理升级、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。

面临的问题

在银行业，ATM的管理一直是个难点——因为ATM不但分布分散，而且分布在不同地方的ATM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ATM因为中毒、主机硬盘空间不足等原因导致停机或者出错，就会严重影响银行正常的业务运行，还会影响银行的形象，甚至带来不可估量的财产损失。

浦发银行同样面临这样的问题。浦发银行拥有34个分行，一共拥有3500多台ATM，采用跨平台的管理模式，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ATM对浦发银行的IT管理部门来说，是个很大的挑战：一方面，由于这些ATM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——ATM不但数量多，而且分布非常分散，IT管理人员不可能到每个ATM上去操作，过去浦发银行ATM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，ATM上的应用也需要随着新业务的推出而不断变化，浦发银行要及时对所有的ATM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ATM的基本信息，如品牌、型号、具体安装位置、ATM设备类型、业务柜员号，同时还要了解ATM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ATM日常维护时对现场操作员的管理，特别是ATM上运行的程序控制，对型号不同、应用系统各不相同的ATM进行补丁更新和程序控制，建立ATM厂商维护工具的认证流程和审批流程。

为了把银行的IT信息安全做得更好，浦发银行信息中心主任信息中心主管亲自抓来加强ATM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

考虑到浦发银行ATM数量庞大、地域分布分散、应用复杂、终端控制难度较大的实际情况，项目实施要涵盖浦发银行全国34个分行3500多台ATM，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ATM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，浦发银行最后选择了由LANDesk管理套件和LANDesk安全套件方案组合而成的ATM系统信息监测平台来满足浦发银行对ATM系统的管理。

LANDesk银行ATM系统信息监测平台提供了先进而实用的功能，能够满足浦发银行ATM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、ATM应用管理、应用白名单管理，并提供各类自定义报表功能，能够帮助银行用户高效率管理分布地域广的ATM



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ATMSIM报表系统的开发服务。

值得一提的是，浦发银行之所以选择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ATM上，而不合法的则不允许，使得浦发银行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。当时浦发在选择ATMSIM的控制技术时曾经仔细考虑过这个问题。后来经过详细的测试，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、MCAFEE的病毒定义程序，都不需要经过认证，因为程序已被微软和MCAFEE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。

目前浦发银行也是我国银行业中首家在ATM管理上选择白名单技术来进行安全管理的银行。

借助LANDesk管理套件和安全套件，浦发银行建设了一个统一的ATM软件信息监测平台，定期统计全行ATM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ATM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，有助于提高浦发银行ATM软件信息安全管理整体水平。

批量快速部署

浦发银行ATM系统信息监测平台建设从2008年开始规划，到2009年3月开始部署，计划到2009年底部署结束。3500多个ATM分布在全国各地，对浦发银行的IT管理部门来说，选型虽然很重要，但是如何将管理软件部署在每个ATM上才是工作量大的地方。

针对浦发银行的3500多台ATM分布在全国各地的实际情况，项目组制定出详细的分步实施方案，先在小范围进行实施试验，然后在此基础上再分批实施。

浦发银行前期将上海、济南、深圳三地的分行作为试点，主要用于测试LANDesk的解决方案与ATM的兼容性，及早发现问题并解决问题，通过试点分行总结的部署经验，在2009年7月底，项目组进行第一轮的全局培训，约20家分行的IT管理员参与了这次培训。由于LANDesk解决方案的安装非常简单，这些参与培训的管理员在轻松掌握安装技巧后，就可以负责各分行的软件安装工作。借助他们的力量，浦发银行就可以形成软件部署的网状体系，从而快速部署每个ATM成为可能。2009年8月底，约10多家分行参与了第二轮全局培训。

截至2009年8月，浦发银行已经有900多个ATM已经成功部署了LANDesk管理套件和安全套件。可以预见，到2009年底可以将ATMSIM客户端全部部署完毕。

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，方便地对银行复杂而易变的ATM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，能够帮助浦发银行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，从而使得浦发银行能从一个统一的控制台——ATM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ATM信息安全，更是使得浦发银行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，在已经部署的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，以更加适合浦发银行IT管理人员的使用习惯，可以和浦发银行将来的业务考核进行结合；借助LANDesk的解决方案，浦发银行基本形成了ATM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。

浦发银行信息中心信息中心主管高兴地说：“浦发银行应用蓝代斯克ATM软件信息监测平台的时间虽然不长，但是已经取得了初步成效，不但大大减轻了我们平时维护ATM的工作量，更是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ATM的信息安全更加放心。”

一个平台管理3500多台ATM

近年来，随着信息化建设的不断深入，银行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，零散分布在各地的ATM系统的管理也变得越来越复杂。

浦发银行利用LANDesk的解决方案，借助ATM软件信息检测平台来集中管理数量庞大的终端的做法，无疑是给我国的金融银行业，乃至所有终端管理较为复杂的大型企业的桌面管理提供了一个很好的借鉴。

据了解，在2009年底浦发银行的ATM软件信息监测平台全部部署完毕以后，借助ATM软件信息检测平台，浦发银行的IT管理部门可以集中掌握全行3500多台ATM的防病毒软件的防护情况，可以集中查处ATM设备上安装的哪些软件；可以控制ATM上运行的程序，只有经过授权的程序才能在ATM上运行；可以对ATM厂商的维护工具进行报备、授权管理；并且对ATM上异常的程序运行报警行为进行处理。

如需获得最新的产品信息，请访问LANDesk网站：www.landesk.com.cn

本文中的所有信息与LANDesk®的产品相关，没有明确或暗示的知识产权被赋予此文档。LANDesk不保证此文档没有错误并保留随时更新、修正、更改此文档的权利，包括任何定义和产品描述。如需获得最新的产品信息，请访问<http://www.landesk.com.cn> 版权所有©2007 LANDesk 软件有限公司及其成员公司所有，保留所有权力。LANDesk, Peer Download 和 Targeted Multicast是注册商标以及LANDesk软件股份有限公司及其分支机构在北美及其他国家的商标。

客户的收益可能根据实际状况和具体情形而有所不同。

