

互联世界 · 满怀信心 Symantec

成功案例

广东移动通信有限公司

赛门铁克解决方案可将潜在数据泄露事件减少 80%

随着相关电信公司敏感客户数据的泄露，加上中国民众对个人信息意识不断增强，广东移动需要一款可防止数据泄露的解决方案。经过对若干解决方案的评估，该公司最终选择了赛门铁克的数据泄露防护解决方案。实施该解决方案后，该公司取得了显著的成效，包括公司和第三方人员发送关键数据的事件减少了 80%，以及数据审计时间缩短了 90%。

挑战：保护机密数据

众所周知，中国经济在过去10 年里取得了突飞猛进的发展。随着 13 亿居民的工作机会和可支配收入的增加，手机用户的数量呈现激增之势。目前，中国的手机用户数居全球之首，超过了 7 亿。为绝大数用户提供服务的是中国移动有限公司，这是一家全球规模最大的移动通信公司，拥有大约 5.4 亿名客户。

广东省从中国经济的蓬勃发展中受益匪浅。目前，该省已经发展成为全国人口最多的省份。由于大批流动务工人员渴望与家乡的亲人联系，这使得广东省在手机使用总量上可谓数一数二。

这种增长给中国移动及其分公司（广东移动通信有限公司 GMCC）带来了机遇，同时也带来了很多挑战，包括防止数据泄露。为了防止客户电话号码、地址、ID 号等敏感客户信息以及公司知识产权和运营信息泄露，GMCC 希望部署一种数据泄露防护解决方案。

企业简介

网站： www.gd.chinamobile.com

行业： 电信

总部： 中国广州

员工人数： 20,000

赛门铁克解决方案

Data Loss Prevention

为何选择赛门铁克解决方案?

- 让数据审计人员可以做出快速响应
- 可以监控多个数据元素
- 为员工提供有关敏感数据问题的培训

数据泄露日益受到关注

随着广东省手机用户量的增加，GMCC 的客户数据量也随之增长，达到了 35 TB。个人用户对于数据泄露问题的意识也逐渐增强。比如大家所熟知的 3 月 15 日消费者权益日的“3.15”事件，据新闻媒体披露，山东移动（中国移动分公司）以短信形式泄露了客户的敏感信息。

GMCC 安全技术经理彭林锋说，这起事件在全国公众中引起了强烈的反响。“一方面，中国大众现在知道电信记录可能会被泄露，因此，他们懂得保护敏感信息的重要性。另一方面，移动行业（所有公司及其人员）现在都清楚数据泄露防护的意义。”

为了解决数据泄露问题，中国政府对相关法律进行了修订。现在，凡泄露敏感客户信息的企业或员工都会受到相应的处罚。以前，GMCC 收到过客户关于数据泄露的投诉。因此，它希望与电信行业的其他公司联手，共同主动解决数据泄露问题。彭先生表示，“上到我们的母公司中国移动下到我们的管理人员和正式员工，我们都会非常认真地对待这一问题。我们已经斥巨资进行数据泄露防护。”

危急事件减少了 80%

针对其网络的几项关键要求，GMCC 将来自 赛门铁克和其他友商的解决方案进行了评估。彭先生表示，“首先，解决方案应该让我们可以监控和保护不同的数据格式，其中包括 ID 编号、地址和通信记录。其次，解决方案的部署必须灵活，不会给我们现有的系统造成影响。最后，解决方案必须稳定，不能破坏我们的网络。”

广东移动最终选择 Symantec™ Data Loss Prevention 的原因有二，一是该解决方案满足了其所有关键要求，二是赛门铁克提供了数据泄露防护专业技术。彭先生说，“我们还在公司的其他领域使用了赛门铁克解决方案，获得了良好的体验”。

为了便于部署 Symantec Data Loss Prevention，GMCC 采用了赛门铁克咨询服务。彭先生称，“我们与赛门铁克咨询团队交流，让他们了解我们面临的挑战，以及我们希望防止从公司泄露的信息类型。根据我们的要求，赛门铁克咨询团队为我们制定了 Symantec Data Loss Prevention 计划，同时还帮助我们降低了对现有系统的影响。”

解决方案概览

主要挑战

- 查询包含机密消息的文档
- 让公司数据审计人员做出精确而快速的响应
- 使管理层随时了解数据泄露防护的执行情况
- 对网络上的敏感客户数据进行监控
- 增进员工对公司数据安全计划的了解

赛门铁克产品

- Symantec™ Data Loss Prevention，带有
  - Network Discover

赛门铁克服务

- 赛门铁克咨询服务

技术环境

- 服务器平台：运行 IBM AIX 的 IBM P595x26 服务器
- 应用程序：计费和结算 B/OSS 系统、Microsoft Windows Server 2003 和 2008
- 数据库：Oracle Database 10g r2
- 存储：IBM System Storage DS4800、HPEVA 4000

业务成果和技术优势

- 公司人员发送敏感数据的事件减少 80%
- 数据审计时间减少 90%
- 审计流程不遵循事件从每月 10 起减少为零
- 提供详细的事件报告，实现了整个事件的恢复
- 提供了优化的数据保护功能，可提高客户忠诚度

“过去，由于人员发送关键信息导致的泄露事件据报道每周多达数十起。有了 Symantec Data Loss Prevention，现在每周报告的事件只有几起，减少了 80%。”

彭林锋
安全技术经理
广东移动通信有限公司

Symantec Data Loss Prevention 可以生成报告，提供有关公司人员在特定时间段所发送敏感数据的统计信息。彭先生表示，过去，由于人员发送关键信息导致的泄露事件据报道每周多达数十起。“有了 Symantec Data Loss Prevention，现在每周报告的事件只有几起，减少了 80%。”

更清楚地认识数据泄露

同其他电信服务提供商一样，GMCC 在其网络上使用业务运营和支持系统 (B/OSS)，该系统包括客户记录、账单和付款。第三方开发人员和制造商也能访问该系统。为了维护该系统的访问权限，GMCC 使用了应用程序管理系统 (AMS)。

要在监控客户数据的同时防止数据泄露，GMCC 需要一种方式来审计其 B/OSS 网络的访问者，因为公司文档有时包含可能会将敏感数据泄露给第三方的附件。另一个潜在的数据泄露途径是文件传输协议 (FTP) 服务器，即 B/OSS 用于发送数据的通道。

彭先生表示，“AMS 和 FTP 服务器是 B/OSS 系统中数据泄露的两个通道。我们的重点在于对这两个通道加以监控。”

GMCC 部署了 Symantec Data Loss Prevention Network Discover 这个附加产品，以便快速查找暴露的机密数据，无论这些数据存储在何处都是如此。Symantec Data Loss Prevention Network Discover 提供了范围广泛的企业数据存储库，它具有即装即用的扫描功能，可扫描文件服务器、数据库、文档和记录管理、电子邮件存储库以及 Web 内容和应用程序。

彭先生说，“借助 Symantec Data Loss Prevention Network Discover，我们可以设立不同的数据搜索标准，从而发现泄露的敏感信息。通过赛门铁克内部事件报告，我们可以了解这些事件的涉案人员、发生时间以及泄露的附件或文档类型。我们可以恢复整个事件，而不仅仅是部分数据。”

审计时间减少了 90%

事件报告后，GMCC 审计人员可以更深入地了解是否有敏感数据被泄露。Symantec Data Loss Prevention 可以帮助审计人员执行分析，做出决策，简化流程，将日常审计时间减少 90%。

GMCC 以及第三方公司员工的意识也得以提高，这也有助于防止数据泄露。最初部署 Symantec Data Loss Prevention 时，不遵从审计流程的事件每月平均有 10 起。彭先生称，“现在，由于员工现在知道他们的活动和行为受到 Symantec Data Loss Prevention 的监控，因此不遵从审计流程的事件减少到了零。通过 Symantec Data Loss Prevention，我们现在可以识别并报告这些事件，以便对它们进行审计。”

借助 Symantec Data Loss Prevention，GMCC 能够保护敏感数据，使客户相信他们的敏感信息一直是安全的，进而提高客户忠诚度。彭先生 认为，“赛门铁克的解决方案丰富了我们的数据保护方法。通过将 Symantec Data Loss Prevention 与公司的其他战略相结合，我们认为，我们可以提供良好的客户数据保护环境。”

“通过将 Symantec Data Loss Prevention 与公司的其他战略相结合，我们认为，我们可以提供良好的客户数据保护环境。”

彭林锋
安全技术经理
广东移动通信有限公司