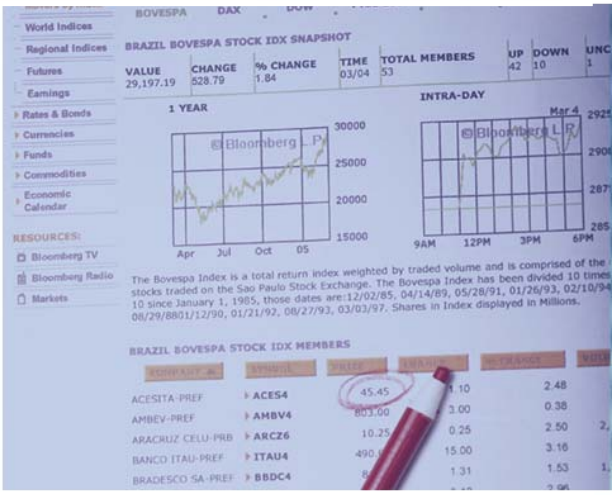
IBM Guardium 数据库安全、合规、审计、监控解决方案建议书

——IBM 企业数据管理综合解决方案



Information Management

目　录

第1章　数据库安全保护及审计工作必要性

1.1　您所面临数据库安全的挑战

如果有人问您：“谁在什么时候以什么方式访问过数据库里什么样的数据？”您能迅速的回答出来吗？甚至您可能不能回答这个问题，说明您目前也不能确保数据库的安全性。

数据，作为企业核心资产，越来越受到企业的关注，一旦发生非法访问、数据篡改、数据盗取，将给企业带来巨大损失。数据库作为数据的核心载体，其安全性就更加重要。

面对数据库的安全问题，企业常常遇到以下主要挑战：

- 数据库被恶意访问、攻击、甚至遭到数据偷窃，而您不能及时地发现这些恶意的操作；
- 不了解数据使用者对数据库的访问细节，从而不能保证您对数据安全的管理；

关键敏感的数据在什么地方？谁在使用这些数据？您并不知道类似“5W”—“谁（Who）用什么方法（What）在什么地方（Where），什么时间（When），对你的数据库做什么事情(How)。”的问题。

- 当数据库正在遭受恶意访问或攻击时，您不能及时地追踪并堵截这些恶意操作；
- 数据库遭受恶意攻击、访问后，您不能追踪到足够的证据；
- 来自内部的威胁，特权用户修改配置、改变或偷窃数据，没有明确的职责分工。

1.2　您所面临的合规/审计要求的挑战

信息安全同样会带来审计问题，当今全球对合规/ 审计要求越来越严格，由于不满足合规要求而导致处罚的事件屡见不鲜。美国《萨班斯法案》的强制性要求曾导致 2007 年 7 月 5 日中国第一家海外上市公司—华晨中国汽车控股有限公司从美国纽约证券交易所退市。

有关信息安全的合规/审计要求，中国政府也进行了大量的强化工作，例如，为了加强商业银行信息科技风险管理，银监会出台了《商业银行信息科技风险管理指引》规则，其中要求：“采取安全的方式处理保密信息的输入和输出，防止信息泄露或被盗取、篡改。”，“执行信息科技专项审计。信息科技专项审计，是指对信息科技安全事故进行的调查、分析和评估，或审计部门根据风险评估结果对认为必要的特殊事项进行的审计。”等等。

如今，中国政府——财政部、证监会、银监会、保监会及审计署等五部委会联合发布“中国版萨班尼斯－奥克斯利法案（以下简称‘C-SOX 法案’）”——《企业内部控制基本规范》（以下简称《基本规范》），宣布从 2009 年 7 月 1 日起将率先在上市公司范围内施行，旨在推动企业完善治理结构和内部约束机制，同时促进国内企业更好的同世界级管理接轨。 C-SOX 法案实施的三个主要目的：1，改变中国企业做事的方法，使其按规矩做事，减少感性认知，增加理性标准；

2，改变考虑问题的思维习惯，培养定量的管理习惯；3，通过审计，控制企业风险，从而提升企业管理的水平。企业如果不执行这个法案，可能带来严重后果。

以上信息反映了合规/审计要求越来越多，对数据库中的信息安全也越来越重视。合规/审计对于 IT 系统的核心要求在于对提供准确无误的数据、及时的数据处理，确保审计流程、提供符合审计要求的报表等。而传统的审计对于 IT 系统往往通过检查数据库/应用系统日志的方式进行。面对海量的日志数据，这种方法既耗费大量的人力，又不能准确、及时的处理这些日志信息，从而无法满足合规/审计的需求。

面对合规/审计要求，企业往往面临以下挑战：

- 不能做到持续性审计

用户审计目前主要是针对数据库、应用系统日志做审计，这些日志内容非常庞大，DBA（数据库管理员）和信息安全审计人员的审计工作就只能做事后分析，分析时间也长。不能做到持续性审计。

- 审计并不规范

用户目前审计的内容和表格主要是根据外部审计人员要求和内部安全管理要素来考虑，这些审计工作的好坏基本上取决于 DBA 和信息安全审计人员的经验和技能，这些不能有效成为公司规范和满足外部审计要求。

- 数据库管理员权责没有完全区分开，导致审计效果问题

现在的数据库管理和审计原始数据的收集实际上都是由 DBA 来做的，这就导致了 DBA 的权责不明确，DBA 没办法客观审计自己所做的工作，尽管用户设置了信息安全审计人员，但该角色的审计工作的部分证据建立在 DBA 初步审计基础上，因此审计效果与可靠性存问题。

- 审计并不完整

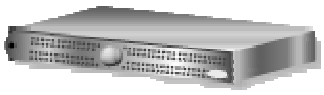
人工审计需要面对海量的日志，不可能对所有数据进行细致审计；审计报告就未必能满足100%可见性。

1.3 IBM Guardium 数据库安全、合规、审计、监控解决方案简介

为了满足企业的信息安全、合规、审计等需求，IBM公司推出了业界领先的“CARS”企业信息架构，该架构主要从“法规遵从”（Compliance）、“信息可用”(Availability)、“信息保留”(Retention)、“信息安全”(Security) 四个方面进行了全面的满足和保护。

不仅如此，IBM Guardium数据库安全、合规、审计、监控解决方案的推出，针对了“法规遵从”和“信息安全”进行了专项治理和加强。

这个被FORRESTER 公司评价为“绝对领导地位”的IBM Guardium数据库安全、合规、审计、监控解决方案，其以软硬件一



体服务器的方式，大大增强您的数据库安全性，满足并方便您的审计工作，提升性能，并简化了您的安装部署工作，其主要功能如下：

- 防止对数据库的破坏、恶意访问、偷窃数据，可帮助判断客户关键敏感的数据在什么地方；谁在使用这些数据；
- 控制对数据库中数据的访问，并可监控特权用户；
- 帮助企业强制执行安全规范；
- 检查薄弱环节、漏洞，防止对数据库配置的改动；
- 满足合规/审计的要求，并可简化内部和外部审计、合规的过程并使其自动化，增强运作效率；
- 管理安全的复杂性 。

1.4 该解决方案为您带来的价值

采用IBM Guardium数据库安全、合规、审计、监控解决方案，能为您带来以下价值：

- ✓ 保护您的数据库及核心数据；
- ✓ 提高对数据库访问的可控度；
- ✓ 帮助您满足合规/审计的要求；
- ✓ 简化您应对合规/审计的工作。

第2章　IBM Guardium 数据库安全、合规、审计、监控解决方案介绍

2.1　解决方案介绍

IBM Guardium是目前解决整个数据库的安全与合规/审计问题的唯一方案，其具有：

- 合适的数据库安全或合规/审计系统能通过网络数据的采集、分析、识别，实时监控网络中数据库的所有访问操作；
- 支持自定义内容关键字库，实现数据库操作的内容监测识别，发现各种违规数据库操作行为，及时报警响应、全过程操作还原；
- 实现安全事件的准确全程跟踪定位，全面保障数据库系统安全功能的产品。

该产品从四个方面满足了企业数据安全及审计的要求：

对于数据安全保护及审计数据库访问行为，IBM Guardium 产品系列已经得到广大业内分析师的认同，并赢得了众多大型企业客户。

Guardium 具有以下主要功能：

发现& 分类

自动寻找、分类和保护敏感信息

随着组织创建和需要维护的数字信息量不断扩增，寻找和分类这些敏感信息的难度也越来越大。

这一问题在某些组织中特别艰巨，因为他们经历过兼并和收购，或者原有系统早已过时。即使情况再乐观，新增业务也会要求他们不断改进应用程序和数据库结构，从而很容易导致一成不变的安全策略无效，导致敏感数据不被发现和疏于保护。

这些组织会发现尤其难以：

• 绘出所有包含敏感信息的数据库服务器和了解各个来源(营业线上的应用程序、批处理、即时查询、应用程序开发商、管理员等) 访问这些信息的方式；

• 在不了解已存信息的敏感性时保护信息和控制风险；

• 在不清楚哪些信息受到特定法规的条款约束时确保合规；

借助于 Guardium，您可以使用数据库自动搜寻和信息分类功能来识别机密数据的存储位置，然后使用定制的分类标签来自动执行适用于特定级别的敏感信息的安全策略。这些策略将确保只有授权用户才能浏览和/或更改敏感信息。同样，还可以将敏感信息搜寻设为定期执行，从而防止出现欺诈服务器，并确保不会“遗忘”任何关键信息。

评估& 加固

漏洞、配置和行为评估

Guardium 的数据库安全评估功能会扫描您的整个数据库架构，查找漏洞，并使用实时和历史数据提供持续的数据库安全状态评估。

它预先配置了一个综合测试库，建立在特定平台漏洞和业界最佳实践案例的基础之上，可以通过 Guardium 的订阅服务得到定期更新。您也可以自定义测试，以满足特定的要求。评估模块还会标记与合规相关的漏洞，如遵从 SOX 和 PCI-DSS 法规提供非法访问 Oracle EBS 和 SAP 数据表的行为。

评估分为两大类：

• 漏洞和配置测试可以检查各种漏洞，如缺少的补丁、权限配置错误和默认帐户问题。

• 行为测试通过实时监控所有数据库流量，根据数据库的访问和操作方式识别漏洞，如登录失败次数过多，普通客户端执行管理员命令，或在非规定时间登录。

除了凭借深度探查能力生成详细的报表之外，评估模块还能生成包含重要度量(基于最佳实践)的安全健康报表卡，并提出增强数据库安全的具体措施和规划建议。

配置锁定和变更追踪

当您实施了漏洞评估中推荐的措施后，便可以建立一个安全配置基线。使用 Guardium 的变更审计系统(CAS)，您可以监控基线的任何变更，以及确保所有变更符合您的授权变更控制策略和流程。

监控& 执行

监控和执行关于数据库安全和变更控制的各项策略 Guardium 通过定制细粒化的实时策略来防止特权用户进行非法或可疑的行为，同时抵挡欺诈用户或外来者的攻击。对于使用通用服务账号访问数据库的多层架构应用系统，例如 OracleEBS、PeopleSoft、Siebel、SAP 以及基于中间件 IBM

WebSphere、BEA WebLogic、Oracle AS 等自行开发的应用系统，您同样可以识别出非法篡改后台数据库的应用账号。该解决方案可由信息安全专员维护，而无需数据库管理员(DBA) 的参与。您还可以自定义细粒化的访问策略，根据登录操作系统、IP 或 MAC 地址、源程序、时间、网络协议和 SQL 指令类型来限制对特定数据表的访问行为。对所有数据库流量持续不断的语境分析 Guardium 对所有数据库操作进行持续不断的实时监控，并根据各个 SQL 查询的“人物、事件、地点、时间、地点和方式”等丰富的语境信息，使用语言分析方法(专利申请中) 检测非法行为。这种方法的独特性在于它不像传统方法那样只能查找预定义的模式或签名，而是提供了前所未有的控制水平，将肯定或否定的误判最小化。

设定检测异常行为和自动化策略定义的基线

通过创建基线，同时识别正常业务流程和表现异常的活动，该系统能自动提出策略建议，用以防御各种攻击，如 SQL 注入攻击。通过直观的下拉菜单还可以轻松添加自定义策略。

主动、实时安全

Guardium 提供了一整套实时监控，对非法或异常行为作出积极主动的回应。基于策略的措施包括实时安全告警(SMTP、SNMP、Syslog)；拦截(通过 TCP 重置或在线数据层防火墙技术)；完整记录；和自定义措施，如帐户自动锁定、VPN 端口关闭和 IDS/IPS 系统联动处理。

追踪和解决安全事件

组织遵守各项法规，就需要证明对所有事件都及时予以记录、分析和解决，并报告给管理层。Guardium 提供的商业用户界面和工作流自动化系统，可以处理安全事件，同时提供的图形化面板，可以追踪关键度量，如未处理事件数量、严重程度和事件未处理时长。

审计& 报表

捕获细粒化审计追踪

Guardium 创建一个覆盖所有数据库活动的连续、详细的追踪记录，并进行实时的语境分析和过滤，从而实现主动控制，生成审计员需要的具体信息。

生成的结果报表使所有数据库活动详细可见，如登录失败、权限升级、计划变更、在非规定时间或来自非法程序的访问、敏感数据表访问等，这些活动是否合规一览无余。例如，该系统能够监控所有的：

• 安全异常事件，如 SQL 错误和多次登录失败。

• DDL 指令，如新建/删除/修改数据表，这些数据表可能会改变数据库结构，在遵循 SOX 等数据管理法规时显得尤其重要。

• SELECT 查询，这在遵循 PCI 等数据隐私法规时显得尤其重要。

• DML 指令(插入、更新、删除)，包括约束变量。

• DCL 指令，这些指令控制帐户、角色和权限(授予、撤销)。

• 支持各种 DBMS (数据库管理系统) 平台的过程语言，如 PL/SQL (Oracle) 和 SQL/PL (IBM)。

• 由数据库执行的 XML。

业界最佳报表

Guardium 解决方案预置了 100 多项策略和报表，这些策略和报表来自我们与世界 1000 强企业、四大审计和评估事务所的合作经验及最佳实践案例。这些报表将帮助您满足 SOX、PCI 等法规的要求，遵守数据隐私条款，以及精简数据管理和数据隐私方案。

除了预定义的报表模板之外，Guardium 还提供了图形化的拖放界面，可以轻松制作新报表或修改现存报表。这些报表能够自动转换成 PDF 格式(附件) 或 HTML 页面链接，通过 E-mail 发送给用户。它们还可以通过网络控制台界面在线查阅，或以标准格式导出到 SIEM (安全信息与事件管理) 和其它系统。

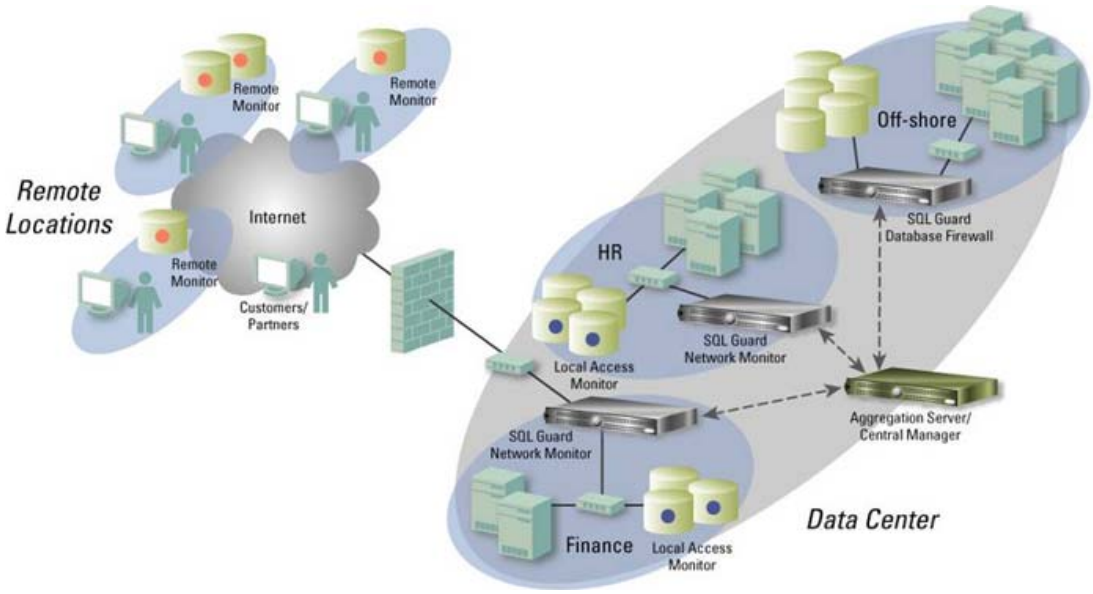
合规工作流自动化

Guardium 的合规工作流自动化在业内是独一无二的，它可以精简整个合规工作流程序，使生成审计报表、分发至重要管理层、电子签署和升级这一系列程序都自动完成。

2.2 Guardium 系统的部署

Guardium 的可扩展架构支持大大小小的操作环境，通过网络控制台实现企业范围内的审计数据的集中式汇集和规范，以及安全策略的集中式管理。S-TAP 探针是基于主机的轻量级探针，用于监控所有数据库流量，包括特权用户的本地访问，并依靠Guardium 收集器设备进行分析和生成报表。收集器设备通过S-TAP 探针及Z-TAP 探针(Z-TAP 探针是位于大型机上的探针) 和/或直接连接网络交换机的SPAN 端口来收集监控数据。汇集器自动从各个收集器设备汇集审计数据。为了实现最大化的扩展度和灵活性，您可以配置多个级别的汇集器。

如下示意图展示了企业内各种部署方式：



2.3 Guardium 兼容性列表

支持各类DBMS 平台

Guardium 的跨平台解决方案支持在各大操作系统(Windows、UNIX、Linux、z/OS) 中运行的所有主要 DBMS 平台和协议：

支持 S-TAP 探针的操作系统版本

Windows NT, 2000, 2003

Solaris - SPARC 6, 8, 9,10

Solaris - Intel/AMD 10

IBM AIX 5.1, 5.2, 5.3, 6.1

HP-UX 11.00, 11.11

11.23, 11.31 PA

11.23, 11.31 IA64

Red Hat Enterprise Linux 2, 3, 4, 5

SUSE Linux Enterprise 9, 10

Tru64 5.1A, 5.1B

支持平台支持版本

Oracle 8i, 9i, 10g, 11g

Microsoft SQL Server 2000, 2005, 2008

IBM DB2 UDB 8, 9

IBM DB2 for z/OS 7, 8

IBM Informix 7, 8, 10, 11

Sybase ASE 12, 15

Sybase IQ 12.6

My SQL 4, 5

Teradata 6

基于主机的监控

S-TAP 探针是一种轻量级的软件探针，在业内独一无二，它们可以在数据库服务器的操作系统层同时监控网络和本地数据库协议(共享内存、命名管道等)。S-TAP 探针不是在数据库中处理和存储日志数据，而是通过将所有流量分送到独立的 Guardium 设备进行实时分析和生成报表，因此对服务器性能的影响微乎其微。用户通常选用 S-TAP 探针，因为使用 S-TAP 探针，就不必再在远程站点或数据中心的 SPAN 端口配置专用硬件。

支持 S-TAP 探针的操作系统版本：

Windows NT, 2000, 2003

Solaris - SPARC 6, 8, 9,10

Solaris - Intel/AMD 10

IBM AIX 5.1, 5.2, 5.3, 6.1

HP-UX 11.00, 11.11

11.23, 11.31 PA

11.23, 11.31 IA64

Red Hat Enterprise Linux 2, 3, 4, 5

SUSE Linux Enterprise 9, 10

Tru64 5.1A, 5.1B

应用程序监控

企业部署的多层架构的应用系统，最终用户不是直接访问数据库，而是通过应用系统访问，Guardium 可以追踪到这些最终用户的访问记录，由此识别潜在的欺诈行为。这很有必要，因为这些应用系统通常使用名为“连接池”的优化机制。在共享环境中，所有用户的流量都汇集

在应用服务器上，只能通过服务帐号名来识别，因而屏蔽了最终用户的真实身份。Guardium 支持对各大主流应用系统的监控。而对其他应用系统(包括内部开发的应用系统) 的监控，则通

过对应用服务器层的活动监控来实现。

支持的企业应用程序

Oracle E-Business Suite

PeopleSoft

Siebel

JD Edwards

SAP

Business Objects Web Intelligence

支持的应用服务器平台

IBM WebSphere

BEA WebLogic

Oracle Application Server (AS)

Microsoft .NET

JBoss Enterprise Application Platform

第3章　为什么选择 IBM Guardium 数据库安全、合规、审计、监控解决方案

3.1 综合优势

- 可以实现从用户、应用服务器到数据库的全程跟踪即可记录，实现全方位准确监控（来自网络的访问和本地登录访问）；
- 对 SOX、PCI、DATA PRIVACY 等法律遵从性的良好支持，国际著名审计公司的认同、认可；第三方国际著名咨询评测机构的认可和赞赏，并具有多行业、众多客户成功应用案例的证明；
- 不依赖于数据库的日志，记录的日志不可更改，完全符合法律要求；
- 对数据库服务器性能影响极低（<5%），大大优于数据库本身的审计产品；
- 细粒度 5W 记录，监控记录的内容可定制，可自定义输出各种灵活的报表格式，并具备集中化管理、日志汇总、关联审计分析能力；
- 自学习能力模型，根据过去的访问习惯自动实现对异常访问的阻断，可自动完成内部审计流程、报表等工作，自动化程度高。

3.2 技术优势

- 可以同时支持监控管理多种数据库的各种版本，支持多种异构操作系统，支持多种企业级应用、应用服务器/中间件服务器；
- 部署容易简单，非入侵式部署，不影响网络、数据库服务器现有运行方式及状况，对用户、网络、服务器透明，不在数据库内安装，不需要数据库建立用户。具备分布式部署和分层架构能力，支持企业级不同地域、多种数据库的应用；
- 具有实时阻断非法访问，抵御攻击能力；
- 独特跟踪下钻（Drill Down）功能，追查问题可以一步步到最底层；
- 支持 IBM 大型机（Z-TAP，Z-GATE）；

3.3 成功案例简介

IBM Guardium 数据库安全、合规、审计、监控解决方案已经在世界各地拥有众多客户，概括如下：

- 金融: 世界五大银行、最大的信用卡公司、最大的共同基金公司
- 保险: 全球最大的五个保险公司中的三个
- 零售业: 全球三大零售商中的两个
- 制造业: 最大两个饮料食品集团、最大 PC 制造商之一和最大的汽车制造商
- 能源: 美国国家电网集团
- 电信: 15 个全球主要的电信运营商
- 交通: 主要铁路集团、航空公司和飞机场
- 政府: 美国和其它几个国家的政府机构
- 医疗卫生: 主要医疗服务机构之一
- 媒体: 美国主要媒体集团之一

第4章　IBM 中国公司简介

IBM，即国际商业机器公司，1911 年创立于美国，是全球最大的信息技术和业务解决方案公司，业务遍及 170 多个国家和地区。2008 年，IBM 公司的全球营业收入达到 1036 亿美元。

在过去的九十多年里，世界经济不断发展，现代科学日新月异，IBM 始终以超前的技术、出色的管理和独树一帜的产品领导着全球信息工业的发展，保证了世界范围内几乎所有行业用户对信息处理的全方位需求。

IBM 与中国的业务关系源远流长。早在 1934 年，IBM 公司就为北京协和医院安装了第一台商用处理机。80 年代中后期，IBM 先后在北京、上海设立了办事处。1992 年 IBM 在北京正式宣布成立国际商业机器中国有限公司。到目前为止，IBM 在中国的办事机构进一步扩展至 26 个城市。伴随着 IBM 在中国的发展，IBM 中国员工队伍不断壮大，目前已达到 14000 人。除此之外，IBM 还成立了 10 家合资和独资公司，分别负责制造、软件开发、服务和租赁的业务。

IBM 非常注重对技术研发的投入。1995 年，IBM 在中国成立了中国研究中心（2006 年更名为 IBM 中国研究院），是 IBM 全球八大研究中心之一，现有 200 多位中国的计算机专家。随后在 1999 年又率先在中国成立了软件开发中心，现有 3000 多位中国软件工程师。

二十多年来，IBM 的各类信息系统已成为中国金融、电信、冶金、石化、交通、商品流通、政府和教育等许多重要业务领域中最可靠的信息技术手段。IBM 的客户遍及中国经济的各条战线。 与此同时，IBM 在多个重要领域占据着领先的市场份额，包括：服务器、存储、服务、软件等。

对于 IBM 在中国的出色表现和突出贡献，媒体给予了 IBM 十分的肯定。IBM 先后被评为“中国最受尊敬企业”、“中国最受尊敬的外商投资企业”、“中国最具有价值的品牌”、“中国最佳雇主”等。2004 年，IBM 中国公司被《财富》杂志中文版评选为“中国最受赞赏的公司”，并荣居榜首。2005 至 2007 年，IBM 连续三次被中国社会工作协会企业公民工作委员会授予“中国优秀企业公民”荣誉称号。

2009年，IBM提出“智慧的地球”理念，倡导以智慧引领转变，从容应对金融危机、气候变暖、恐怖主义、能源紧张、环境污染等全球问题；同时，针对当今国际经济形势，分析中国企业的机遇与挑战。IBM从新锐洞察、智慧运作、动态架构、绿色未来等几个方面，分享建设“智慧的地球”的具体经验和方案，帮助您的企业抓住机遇，开启新的里程。我们相信以科技为助力，一定可以转危为"机"，共建智慧的企业，更有智慧的国家，甚至更有智慧的地球。