保护主机上的关键业务信息

IBM System z提供信息保护解决方案

目录

1 概述

1 IBM的全盘信息管理方法

2 运行z/OS的IBM数据服务器的安全性

3 运行z/OS的IBM数据服务器的审计功能

4 加密与数据迷惑

5 测试数据管理

7 数据生命周期管理和数据增长

8 结论

9 更多信息

概述

全球通信创造了地理透明性，允许更多的机构互动和共享信息，推动电子数据的收集、存储、使用、共享和处理快速增长。这种增长虽然给企业创造了开展新业务的机会，允许他们接触更多客户，但也给企业遵从日新月异的法律和法规增加了风险。

现在有许多规章制度都要求公司更长时间的保存数据。公司经常需要安全地保存生产和历史数据并且对数据访问实施严格控制。公司必须在数据的整个生命周期中始终对其实施保密控制——从开发和测试阶段、直到生产和归档阶段。数据必须是准确的，可接入的，以便审计人员和权威机构进行审查。数据违规将使企业受到严重的经济处罚、法律诉讼甚至锒铛入狱。

尽管如此，各大报纸曝光的数据违规事件仍然层出不穷：政府机构弄丢邮件中未经加密的数据；连锁超市在过卡期间遭劫；银行被盗用数百万美元；数据被员工偷窃后出售给犯罪集团；未加密的个人信息被用于离岸测试；利用员工和客户信息开展身份盗用活动等等。2008年，数据违规平均给公司带来了650万美元的损失，[1] 其中大多数都是内部所为。

本文将描述IBM针对数据犯罪做出的反应，尤其是在为保存在主机上的关键业务信息提供保护方面。

IBM的全盘信息管理方法

2004年，IBM成立了“IBM数据管理委员会”，即现在的“IBM信息管理委员会”，以便联合近50家其他的业界领先公司和组织来解决日益加剧的风险和数据暴露问题。委员会设计了数据管理框架来帮助企业了解数据管理的支持工具、核心原则与成功要素。他们还制作了成熟度模型来帮助企业评估自己的数据管理情况。

IBM认为企业需要利用全盘的端到端方法来管理信息。使用管理框架和成熟度模型，IBM开发出了各有侧重却又相互补充的解决方案，旨在帮助企业通过三个切入点来提高经营绩效——如管理业务风险、降低成本、为增加收入创造机会等。通过这些切入点，企业可以首先满足最迫切的需求，然后再采取措施构建全面的信息管理战略。这三个切入点是：

- 信息保护
- 信息质量
- 信息生命周期管理

本文将重点介绍“信息保护”切入点，也是企业开始信息管理的通用切入点。保护敏感数据是为了满足明确的业务需求，也是为了满足许多新政策的规定。但是，许多公司都选择自己构建解决方案，只是为了向审计人员和法律机构证明他们的系统在结构、运营和报告方面没有缺陷。此外，在法律法规和规章制度频繁变化的今天，公司还经常会低估维护循规框架的成本。

IBM SAFER的信息保护功能

IBM为IBM硬件平台提供全套的信息保护功能来帮助企业发现哪些数据需要保护、实现安全的数据访问、加密数据、并且确保在整个生命周期实施保密控制。此外，IBM还为企业提供强大灵活的分析、实时审计和报告工具。

图1: IBM为企业提供全面的信息保护功能

面向IBM System z的信息保护功能

在《财富》1000强公司中，预计约有95%的公司使用IBM System z® 保存业务数据。[2] 以业务为主的功能——高级业务连续性、安全性、事务处理完整性、可扩展性、工作负载动态均衡功能、及强大的数据访问控制和保护工具——使System z平台成为保存和处理关键业务信息的理想选择。

但是，为了证明自己是负责任的机构，企业必须要遵从行业、金融和政府指导原则，并且能够回答“谁在什么时间什么地点通过什么方式接入了哪些数据”。除了国家及地方政府的特定法律和法规外，企业还必须遵从国际法律。“萨班斯法案”（SOX）、“支付卡行业数据安全标准”（PCI DSS）、“联邦信息安全管理法案”（FISMA）、“健康保险可移植性和责任法案”（HIPAA ）、“Basel H”及“美国参议院 1396年法案”等，都是企业必须遵从的规章制度。调查显示，公司在履行企业经营管理责任方面给人留下的印象，会对公司股价及筹资成本产生影响。[3]

下面，我们来详细介绍System z平台的信息保护功能及其它是如何帮助公司满足这些法律要求的。

运行z/OS的IBM数据服务器的安全性

当用户试图使用运行IBM z/OS® 操作系统的IBM数据服务器提供的服务时，“鉴权”是他们需要接受的第一关安全考验。用户必须通过身份验证和鉴权才能获准使用任何这些服务。

运行z/OS的IBM数据服务器会将主要的身份验证和鉴权工作分配给安全子系统。在z/OS中，z/OS安全服务器——可能是IBM Remote Access Control Facility（RACF® ）或其他同等设备——将提供鉴权和授权服务来控制用户对数据库子系统的访问。这项技术可确保大量资源访问的一致性，无论这些资源是文件、打印机、还是通信设备或数据库。

在这次讨论中，我们假设RACF及其主要竞争产品CA-TopSecret和CA-ACF2都是安全产品，能够为虚拟化环境提供面向z/OS和IBM z/VM® 操作系统的访问控制和安全保护功能。能够为z/OS和z/VM（提供虚拟环境的操作系统）提供访问控制和安全保护功能。

RACF和DB2数据库

采用z/OS配置的IBM DB2® 数据库使用z/OS安全服务器（RACF或同等设备）实现以下目标：

- 控制与DB2子系统的连接
- 分配身份
- 保护基本的DB2数据库（可通过RACF数据集服务来保护DB2的基本数据集）

除了数据库服务器提供的基本安全保护外，您还可以使用数据库服务器的RACF访问控制模块通过RACF来控制用户对数据库对象、权限、命令和实用程序的访问。

RACF和IMS

IBM增强了信息管理系统（IMS™）以便利用RACF来控制对IMS资源的访问。您可以使用最初的IMS安全特性、全新的RACF特性，也可将二者结合使用。RACF提供比以往更加灵活的安全特性。您可使用RACF的标准特性来同时保护系统和数据库IMS数据集的安全。

使用IBM Tivoli产品来增强RACF

通过在RACF的基础上添加另一个用户友好层，IBM Tivoli® zSecure Admin为低级RACF管理员提供了全面易用的Interactive System Productivity Facility (ISPF) 界面。该产品能够基于窗口显示的信息生成RACF命令所需的句法，并且能够自动生成RACF命令，从而减少可能会导致安全信息暴露或系统故障停机的错误。zSecure Admin能够自动执行重复的RACF管理工作，从而将高级管理员解放出来，使他们集中精力开展高价值的工作。

IBM Tivoli zSecure Visual是面向RACF管理员的基于Microsoft® Windows® 的图形用户界面 (GUI)，允许管理员将RACF管理任务分配给初级安全管理员。zSecure Visual能够与运行z/OS UNIX® 的服务器进行通信，以便执行本机RACF命令，从而帮助zSecure Visual管理员摆脱本机RACF和TSO/ISPF的复杂性。

运行z/OS的IBM数据服务器的审计功能

RACF是面向z/OS的业界领先的安全产品，在保护数据服务器上的安全资产不被非法接入方面表现卓越。但在访问与活动报告领域差强人意。企业需要通过强大的审计机制针对面向z/OS的数据服务器中的活动收集信息和报告，但审计工具不会执行安全策略。因此，同时提供基于RACF的保护功能与审计支持功能的实施才能称得上是真正强大的安全环境。

审计是为了确保通过适当的控制来发现用户对生产数据的不当接入与使用。虽然审计工具不会执行接入模式策略或实施安全控制，但却能够提供适当的信息，用于在用户接入数据之后来分析用户活动。我们应该谨记审计解决方案不会对数据或其他的数据资源访问提供任何保护功能。

特权用户的问题

为确保所有数据库管理系统 (DBMS) 都能持续健康的运行，包括DB2和IMS on z/OS，系统和数据库管理员必须定期开展许多工作。这些工作虽然可通过RACF等外部安全流程得到良好控制，但它们的效力具有普遍深入性，执行时往往有悖于安全策略。

例如，DB2表格中保存着敏感数据，访问这个表格的应用— 如 IMS 或IBM CICS® ——受到RACF的合理保护。数据库管理员没有执行CICS应用的RACF权限，但是拥有管理该表格的数据库管理权限 (DBADM)。数据库管理员针对这个表格运行了UNLOAD实用程序，以便提取表中的全部数据。他或她随后可以通过任何机制将数据传输到外部实体 (FTP、Flash/USB、CSV及电子数据表等)。鉴于用户对该表拥有特殊权限，RACF将不会报告任何明显的安全违规问题。

相反，如果这个环境由审计解决方案提供保护的话，系统将会报告这个虽然合乎权限规定、但却存在特权使用问题的行为。对于审计数据的采集，公司可以选择监控特权用户对任何SQL或实用程序的访问。也可选择监控一个时段内的所有实用程序及/或SQL访问事件。因此，虽然数据库管理员在正常营业时间接入审计表是可以接受的，但公司应该就正常营业时间之外的非正常访问模式设置审计参数。

造成这个问题的症结在于：这些权限的性质允许特权用户在没有得到良好保护的应用环境中访问DB2和IMS资源及数据，从而能够绕过正常的事务处理级RACF保护，不受任何限制地访问数据。在DBMS环境中，企业在赋予特权用户权限时必须执行某些机制来跟踪并且记录这些特权用户开展的活动。

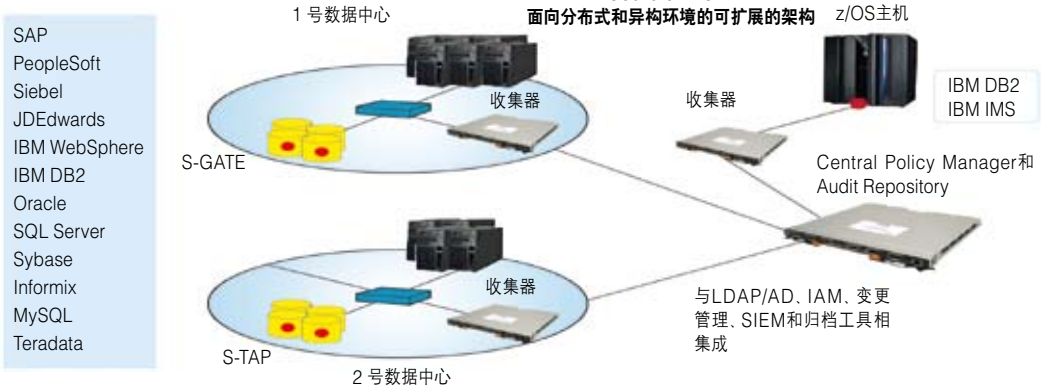

图2：Guardium能够跨越多个异构环境提供可扩展的审计、访问控制和监控功能

角色的分割

企业在针对可信用户设施任何活动审计机制时都必须确保防止特权用户干扰审计数据的采集工作或者破坏审计数据的来源。企业对z/OS数据服务器采用的审计机制必须确保必要的责任分割，以便保证审计数据的完整性和审计报告的准确性。这将允许数据库管理员开展自己的本职工作，并且允许审计人员独立处理数据库管理员的审计报告，实现更加轻松准确的审计。审计人员必须遵从现有的行业标准及外部审计标准，但不能依靠被监控人员提供帮助。

Guardium for z

使用Guardium for z的审计人员无需收集大量来源的数据，也不需要面向DB2或操作系统的用户ID。他们只需登录Guardium便可全面查看可以审计的全部对象。审计人员可以从一个中央存储库来显示全部DB2实例的审计数据，也可以只显示相关DB2实例的审计数据。

中央存储库是报告、控制和汇总数据的单一位置，包括针对审计异常事件提供高级趋势分析和细分功能（每次一个层次），还能提供由审计人员控制的强大的事件报告功能，无需数据库管理员参与。Guardium将安全的审计数据保存在被锁定的防篡改审计库中，不允许任何人以进行修改，包括数据库管理员和其他特权用户，从而满足责任分割要求，并且能够满足主要的审计要求。如果将审计数据保存在Guardium for z等加固的环境中，公司将能够更好地控制数据访问并且保护审计数据。

对许多企业来说，构建全面的审计环境远远不止是收集、保存和提供报告机制那样简单。现在，大多数客户都需要支持异构的DBMS环境，包括为不同的硬件、操作系统和数据库经理提供支持。有效的审计机制需要将这些独立环境提供的数据统统结合在单一视图中。

作为大规模异构解决方案的一部分，Guardium提供更多的支持功能来满足许多常见的审计和报告需求，并且还提供了更加强大的功能。

Guardium能够帮助企业满足大量的监控和报告需求——不会影响SLA和性能，也无需更改任何数据库或应用。

- 工作流自动化能够将循规报告自动分发给监管部门以便他们开展电子签名、上报或评论等活动，从而简化循规流程。
- 提供可扩展的多层架构，通过轻松增长来处理不断增加的工作负载及其他应用和数据中心。
- 防止非法更改数据库模式和数据。
- 将得到批准的变更申请与数据库管理员实际实施的变更进行比较，以便自动执行变更控制调节工作。
- 提供最佳业务实践库，内含几百个预配置的报告和策略，用于满足SOX、PCI及HIPAA等法律和规章制度的要求，并且提供易用的拖放式“构建器”，用于创建定制报告和策略。

加密与数据迷惑

加密静止数据是许多循规计划的基本单元。加密是将明文文本数据转变成惟密文本的过程。这个转变过程同时使用了名为加密算法的数学公式以及数据加密密钥来创建惟密文本。目前，有两种基本的加密算法被普遍认为是安全的：“三重数据加密标准”（TDES）和“高级加密标准”（AES）。密钥是由随机生成的字符组成的十六进制字符串，长度从128位到512位不等。总的来说，密钥越长，它所实施的加密越安全。

数据迷惑与数据加密不同，是通过转变敏感数据来生成全新数据值的过程，新生成的数据值与原始值具有相同的一般特征，但代表的是虚构数据值。一般情况下，数据迷惑采用的是因果逆向工程的方式，不是基于原始值衍生而来的。

基于IBM数据服务器和z/OS通信服务器的网络加密

虽然静止数据是主要加密对象，但是，强韧的加密环境中还应该包含适当的技术，以便在整个生命周期中对关键信息进行加密，包括加密通过网络连接进出企业的数据，如企业与外部业务伙伴共享的数据。

z/OS操作系统的固有功能，如z/OS通信服务器（z/OS Communications Server），能够帮助企业保护网络资源。z/OS通信服务器能够与DB2和IMS for z/OS互操作，并且其良好设计的架构允许企业利用不同类型的网络加密方法，如：

- 安全套接层（SSL），这个通信协议可通过开放通信网络提供安全通信。
- 互联网协议安全性（IPSec），旨在保护两个TCP/IP堆栈之间的流量，使它们具有应用透明性。
- 应用透明传输层安全性（AT-TLS），旨在保护特定客户端与服务器应用之间的流量，以及接收这些应用的TCP/IP堆栈之间的流量。以及绑定了应用的TCP/IP堆栈之间的流量。

IBM数据服务器与静止数据加密

您可通过多种方式来加密DB2和IMS中的数据。问题是“您希望保护哪些数据，希望禁止哪些人访问数据？”以及“您需要为此付出多大的努力？”，您需要回答这些问题才能决定使用什么技术以及数据的加密和解密位置。

对加密技术的选择需要您在功能、可用性和性能之间做出一些取舍。使用 DB2 for z/OS V8和更高版本的公司可以选择通过DB2的固有功能实施数据加密。但是，这些产品存在一些固有的问题，可能使企业无法灵活地构建强大的企业级解决方案。

IMS不支持DBMS加密实施，因此，企业需要考虑通过其他的机制来加密数据。

使用ICSF服务来管理密钥

Integrated Cryptographic Service Facility (ICSF) 是z/OS的组件，旨在透明地使用现成的加密功能来满足z/OS应用和子系统的数据加密需求，无论是CP Assist for Crypto-graphic Function（CPACF）还是Crypto Express[2]。

ICSF允许企业通过AES和TDES算法来确保数据的保密性。TDES（三重数据加密标准）最初于1999年颁布，现在仍然是普遍使用的行业标准。AES（高级加密标准）是国家标准与技术研究院于2001年颁布的，2002年作为联邦政府标准正式生效。AES是针对高度机密数据得到NAS批准的可以公开接入的第一个开放密码。更新后的算法提供更加强大的加密功能，是用于满足“静止数据加密”需求的推荐算法，支持128、192和256位密钥，具体取决于企业使用的System z处理器的类型。企业通过ICSF服务生成的密钥可供IBM Data Encryption for IMS and DB2 Data-bases工具使用。

企业可将加密硬件（又称协处理器）可提供给IBM Data Encryption for IMS and DB2 Databases使用，具体取决于处理器或服务器型号。z/OS ICSF支持IBM System z10® Enterprise Class和IBM System z10 Business Class处理器使用Crypto Express[3]功能。对于IBM System z9® 和 z10® 处理器，也可使用Crypto Ex-press[2]功能。

ICSF为密钥的生成、保存和使用提供安全的环境，比DB2 V8等产品提供的基于应用的密钥管理方法更受欢迎。

IBM Data Encryption for IMS and DB2 Databases

IBM Data Encryption for IMS and DB2 Databases通过单一产品同时为IMS和DB2 for z/OS 数据库提供数据加密功能，为IMS提供片段级敏感数据保护，为DB2提供表级敏感数据保护。

IBM Data Encryption for IMS and DB2 Databases是通过标准IMS出口及DB2 EDITPROC实施的。出口或EDITPROC代码可以调用System z加密硬件来加密需要存储的数据并且解密数据以便应用使用，从而保护驻留在各类存储介质中的敏感数据。System z硬件还增强了对加密指令和特性的支持，从而降低了加密对性能的影响。[4]

对于IMS和DB2来说，IBM Data Encryption for IMS and DB2 Databases生成的例行程序对于访问数据库的应用程序都是透明的，因此在实施时无需更改应用。您在为此类出口或应用编写和维护加密软件时，这个工具可以帮助您节省时间并且减轻工作负担。

实施系统生成的出口是一个简单过程。实施完成后，出口将由DBMS在适当时间驱动，根据需要进行加密或解密，具体取决于SQL或IMS语句的类型。

使用加密表，您也可以加密包含DB2恢复日志和DB2映像拷贝数据集的标准恢复数据。您可在EDITPROC启动后通过能够反射行式项目的日志映像来加密恢复日志记录。由于映像拷贝实用程序是页面级操作程序，因此，您需要加密DB2映像拷贝数据集。您在实施IMS之后，映像拷贝数据集也将得到加密。这对于将恢复资产运送到场外进行保存的公司来说非常重要；如果数据在运送期间丢失或被盗，由于已被加密，因此可防止非法使用，借此避免数据外泄。

测试数据管理

创建真实一致的应用开发与测试环境是企业交付可靠的应用、增强特性和升级包的第一步工作。但是，为了测试目的而复制大规模生产数据库会增加开展测试所需的时间。

企业可以选择不去复制大规模的生产数据库，而是更加有效地实施测试数据管理与子集设置功能，以便最大限度地降低存储需求，同时扩展测试覆盖范围。若只需测试能够准确体现生产数据的小规模真实子集，企业将能够大大加快测试速度，也不会给测试流程增加负担。

测试数据管理与子集设置功能可以帮助企业控制开发与测试环境的规模。消除需要测试的多余数据能够降低存储需求并且降低成本。您可以创建大小合适的任何数量的开发、测试和培训数据库来满足特定需求，既能扩展覆盖范围，又能提高准确性。简化后的测试数据库更加易于维护与管理，允许您加速迭代测试周期并且缩短部署全新应用功能所需的时间。

数据迷惑

大多数情况下，您都需要使用真实数据来测试应用功能并且确保准确性和可靠性。您通常只需复制生产数据库的拷贝即可创建测试环境。这意味着您可将敏感信息从安全的生产环境传送到易受攻击的非生产环境中。但是，虽然使用真实数据对于确保应用测试质量至关重要，但是，生产数据的身份去除 (deidentification) 或屏蔽功能才是保护敏感数据的最佳方法。

数据的身份去除是指系统地移除、屏蔽或转换数据单元，以防有人使用它们来识别数据身份的过程。数据身份去除功能允许开发人员、测试人员和培训讲师使用真实数据获得有效结果，同时仍然遵从数据保密规则。数据一旦被屏蔽，即使丢失或被盗也不会导致保密信息外泄。

数据屏蔽可能会非常复杂。从技术的角度看，这不是一次性过程，必须根据当时的开发、测试和培训需求酌情实施。理想的解决方案必须能够跨越多个应用、数据库、操作系统和硬件平台来确保数据满足保密要求。去除保密数据的身份是保护机密数据以及确保数据满足HIPAA及PCI DSS等规章制度和标准要求的一种最佳方式。

关系数据库和引用完整性

推动业务运营的大多数企业资源规划 (ERP)、客户关系管理 (CRM) 和定制应用都依赖于复杂的关系数据库技术。应用数据库中经常包含几十、几百甚至几千个数据库表及数据库中经常包含几十、几百甚至几千个数据库表及许多的数据关系。每当开发全新的应用增强特性或升级包时，数据库管理员都需要遍历数据库模式以确保数据的引用完整性。

您通过显式引用完整性在DBMS目录中完整定义数据关系智能的可能性极小。数据关系常存在于DBMS以外。您可通过应用逻辑来定义和执行真实世界的数据关系，但您必须了解并且维护它。

如果不能利用通用技术的话，您将无法轻松决定计划实施的应用数据库模式变化将对数据的引用完整性产生什么影响。您必须分析并且了解相关数据，以便在企业应用中更加有效地使用这些数据开展商业活动。这些问题解决之后，企业将能够提高数据准确性和可用性，并且能够更加轻松地实施企业数据管理战略，如数据库归档、测试数据管理及数据屏蔽等。

通过InfoSphere Discovery自动发现数据关系

使用专利功能，IBM InfoSphere™ Discovery能够识别并且记录数据、数据所在位置、以及数据在系统上的链接方式，智能地捕获数据关系并且决定适用的转换和业务规则。此外，该产品还能发现、记录、整理并且管理支持单一业务应用或整个企业应用环境的多组数据库表格与数据关系。这项功能现已被集成到Optim™ 解决方案中。IBM InfoSphere Discovery提供高级功能，允许您发现标量转换、条件逻辑、汇聚、算术等式及其他高级业务规则，如果仅凭手动检测，您几乎根本不可能发现这些规则。

IBM InfoSphere Discovery能够检查多个来源的数据值，以便决定可能会隐藏敏感内容的复杂规则和转换。IBM InfoSphere Discovery能够找到保存在大量字段中或者跨越多列的保密数据项目。

若与IBM Optim Data Privacy Solution结合使用，IBM InfoSphere Discovery将为您提供最有效的企业级方法，支持您跨越复杂的异构环境来定位和屏蔽敏感数据。

Optim Test Data Management Solution

IBM Optim Test Data Management Solution提供公认的技术来优化并且自动执行用于在非生产 (测试、开发和培训) 环境中创建和管理数据的流程。开发人员和质量保证 (QA) 测试人员可以创建大小合适的真实测试数据库，创建目标测试环境，保护数据的机密性，并且在测试前和测试后进行速度和准确性的比较。

一开始，解决方案会基于用户规定从生产系统或生产系统的复制品中提取所需的数据记录，然后将它们安全地拷贝到压缩文件中，再由IT人员将文件装载到目标开发、测试或QA环境中。

测试完成后，IT人员可将结果与基线数据进行比较，以便验证结果并且发现任何错误。他们只需再次插入提取文件便能更新数据库，从而确保一致性。

Optim能够为了测试而创建具有引用完整性的应用数据子集。子集设置功能能够准确捕获真实的应用测试数据并且降低多个测试环境的容量需求。

使用Optim Test Data Management Solution来定义子集选择标准，如同您为了开展特定测试而选择表、关系及其他功能标准一样简单。这个解决方案支持您在数据库中定义的数据关系，以及您通过应用逻辑执行的数据关系。子集选择标准确定之后，解决方案的处理功能可以识别并且提取精确的数据子集。插入和装载选项允许您高效准确地填充或更新测试数据集，不会对生产系统产生影响。

测试完成后，解决方案将对之前和之后的测试数据映像进行分析，自动检测出任何差异，并且通过简明的报告提供分析结果。您可以浏览突出显示的比较结果，以便轻松进行分析，从而节省无数的时间。

Optim Data Privacy Solution

IBM Optim Data Privacy Solution提供全面的功能来去除应用数据的身份，以便在非生产环境中有效使用这些数据。使用这个解决方案，开发人员和测试人员可以使用各项公认的数据转换技术，通过拥有准确上下文的虚构数据来替换保密数据，以便产生有效的结果。

Optim能够感知应用的屏蔽功能可确保姓名和街道地址等被屏蔽的数据与原始信息的外观相似。Optim既保护了数据完整性，又能生成可以体现应用逻辑的一致有效的结果。例如，您可通过不带有意义的文本字符串的随机姓氏来替代真实姓氏。

具有上下文感知能力的预包装的数据屏蔽子程序允许您轻松去除多类敏感信息的身份，如生日、银行账号和身份证等。屏蔽技术包括子串、算术表达式、随机数或序列号生成、及日期老化和串联等。

Optim的转换库子程序能够准确屏蔽复杂的数据单元，如社会安全号、信用卡号和电子邮件地址等。固有的查找表支持屏蔽姓名和地址。

截止到现在，我们描述的每种方法都能通过有效屏蔽数据来保护机密性。但是，关系数据库应用需要您将被屏蔽的数据单元传达给数据库中所有相关的表才能维护引用完整性。例如，如果电话号码等被屏蔽的数据单元是数据库表关系中的主键或外键，那么，系统必须要将这个新被屏蔽的数据值传达给数据库中所有相关的表或其他数据源。

键传达功能可以帮助您跨越多个应用、数据库和运行环境来确保被转换的数据应用的引用完整性。如果没有键传达功能，母表与子表之间的关系将变得非常紧张，令测试数据变得不准确。因此，应用测试将会生成不可靠的结果。Optim的永久性屏蔽功能能够跨越多个数据源一致准确地传达被屏蔽的替换值，从而生成准确的测试结果。

数据生命周期管理与数据增长

ERP、CRM和定制应用推动公司执行业务计划并且为公司创造了增收机会。处理更多的事务和收集更多的客户信息当然对公司有益，但是，由于不可管理的数据量增加，将对公司提供卓越服务与支持的能力产生负面影响，包括减慢应用性能、造成财务和技术资源紧张、导致关键业务流程无法实时完成等。

此外，各类安全计划和规章制度也在要求企业保存越来越多的数据。这些数据在最初收集和保存时可能与业务密切相关，但会逐渐失去商业价值。然而，为了满足未来可能出现的报告或审计要求，企业必须通过某种形式继续保存它们。这些“不活动”的数据虽然不再具有商业价值，但却不能被删除。

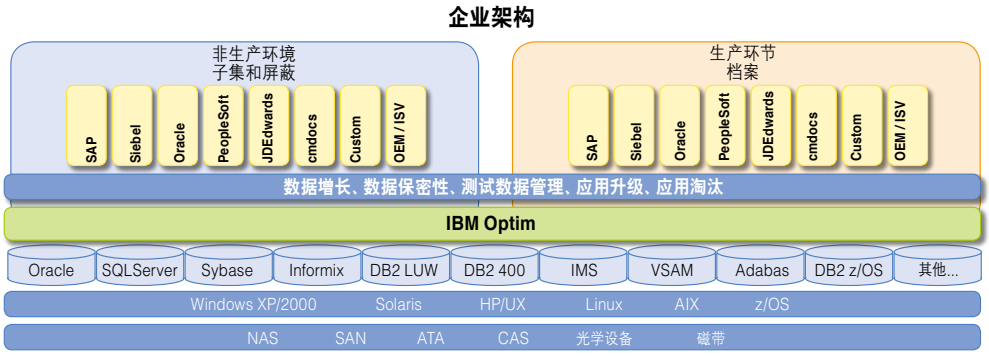

图3：IBM Optim作为一个可扩展的、可互操作的企业数据管理解决方案为您部署策略提供一个中央点，以便您在跨越从创建到删除的整个生命周期来提取、保存、转移和保护应用数据记录。

引进审计数据收集机制后，审计数据库会迅速成为企业中最大的数据库。与企业数据一样，这些审计数据也需要企业长期保存，但却很少被使用。

通过减少生产数据库中的信息量，您将能够减少面向应用数据的磁盘空间需求，从而降低存储成本。此外，由于减少了需要传输的信息量，您将能够加快应用流程的运行速度，提高运营效率，并且利用关键业务的企业应用及其数据创造最高的商业价值，从公司从中受益。

从安全性和循规性的角度看，在线事务处理 (OLTP) 运营数据库中保存的数据越少，因数据暴露而导致的违规风险越低，对数据的保护、加密和审计需求也就越低。

IBM Optim Data Growth Solution

IBM Optim提供数据管理解决方案来管理企业应用数据，以便解决与数据增长相关的问题。Optim提供公认的归档功能，允许用户将历史数据与最新数据分割开，并且将它们转移到安全的档案中，在这里经济高效的安全保存它们。这将能够帮助企业始终满足绩效目标，从而推动收入增长。

企业可根据需要提供这些信息，从而快速响应客户查询和法律要求。作为公认的最佳业务实践，数据库归档能够将不活动的应用数据与最新活动数据分割开。简化后的数据库将能够回收容量并且帮助您提高应用性能及可用性。

Optim的档案处理功能可管理事务级或业务对象级的应用数据（如凭单或分类账）。归档能够保护数据完整性并且保存关键的元数据，以便每个被归档的业务对象都能提供业务活动的历史参考快照。长期的系统化归档允许您将生产数据库与档案之间的事务分成多个级别，从而更加轻松地实现服务水平目标。

如果您需要访问历史业务数据来做出决策、制作报告、或者满足审计或电子发现要求，Optim允许您基于便利性和成本来选择最有效的接入方法。您可实施层级存储战略，基于应用数据的商业价值及访问需求的变化来管理它们。

如想进一步降低成本，您可将历史或参考数据离线保存在磁带或其他长期存储设备中。若将参考数据以不可更改的格式保存在安全的“一次写、多次读”(WORM) 设备中，您将能够保护已经归档的业务对象，从而满足循规要求。

Optim的通用接入方法允许您缩短制作历史信息报告的时间并且减轻工作负担——从基于应用的访问（通过现有界面）到独立于应用的访问，您都可利用业界标准的方法和工具。基于应用的访问方法可以通过现有的应用界面提供全新和历史数据的综合视图。此外，Optim还允许您使用ODBC/JDBC、XML或SQL以及IBM Cog-nos®、Crystal Reports及Oracle Discoverer或Busi-ness Objects等报告工具独立于应用去访问已归档的事务数据，不会影响OLTP性能。

使用适当的、安全的方法来淘汰数据能够防止信息资产成为您的负担。您可以自动保存数据来支持循规计划并且快速准确地响应审计和发现要求。Optim允许您在从创建到淘汰的整个生命周期中对数据进行控制。通过实施公认的企业数据管理战略，您可以跨越整个生命周期来控制关键业务数据，帮助整个企业实现可观成效。

结论

这个世界是扁平的，是任何公司都可以通过全球扩展来登台表演的竞技场。信息是拥有巨大威力的，是企业的生命线，能够决定公司损益表上的收入和收益率。鉴于此，想要利用数据安全薄弱环节来谋取经济利益或者盗取行业情报的大有人在。

修复安全问题的成本不仅远远高于实施安全措施的成本，并且还将公司的公众形象、股价和名誉产生负面影响。很多情况下，公司都是在事发多年之后因为数据违规而遭到经济处罚或者蒙受巨大损失才真正意识到当年犯下的错误。坦白说，公司现在再也没有任何借口可以为安全事件进行辩解。IBM面向z/OS的IBM Information Man-agement信息保护解决方案提供全面的端到端功能来帮助您管理业务风险并且降低数据违规和安全信息暴露风险——与数据的保存位置、使用人或使用时间无关。IBM可以帮助您重新获得控制权并且变得更加安全。

更多信息

如想了解面向z/OS的IBM Information Management信息保护解决方案如何帮助您避免数据违规和安全信息暴露风险，请与当地的IBM业务代表联系，或者访问：

ibm.com/software/data/db2imstools/solutions/ data-governance.html

作者简介

Ernie Mancill - 高级IT专家

Mark Simmonds - System z产品营销部信息管理产品组

Tom Vogel - System z产品营销部信息管理产品组

[1] Ponemon Institute, "Fourth Annual US Cost of Data Breach Study," 2009年1月：
www.ponemon.org/local/upload/fckjail/generalcontent/ 18/file/2008-2009%20US%20Cost%20of%20Data%20Breach% 20Report%20Final.pdf

[2] Moutsos, Kim. "IMS at 40: Stronger than Ever," IBM Data-base, 2008年10月：
www.dbmag.intelligententerprise.com/story/showArticle.jhtml?articleID=211300235

[3] O'Donovan, Gabrielle. "A Board Culture of Corporate Gov-ernance." Corporate Governance International Journal, Vol 6, Issue 3, 2003年7月：
http://findarticles.eom/p/articles/mLgo1494/is_200307/ai_n90

[4] ibm.com/servers/eserver/zseries/security/ cryptography.html网页上描述的IBM System z加密功能

IMW14299-USEN-01