信息管理
产品说明

IBM Information Management software

IBM InfoSphere Guardium

管理整个数据库安全性和遵从性生命周期

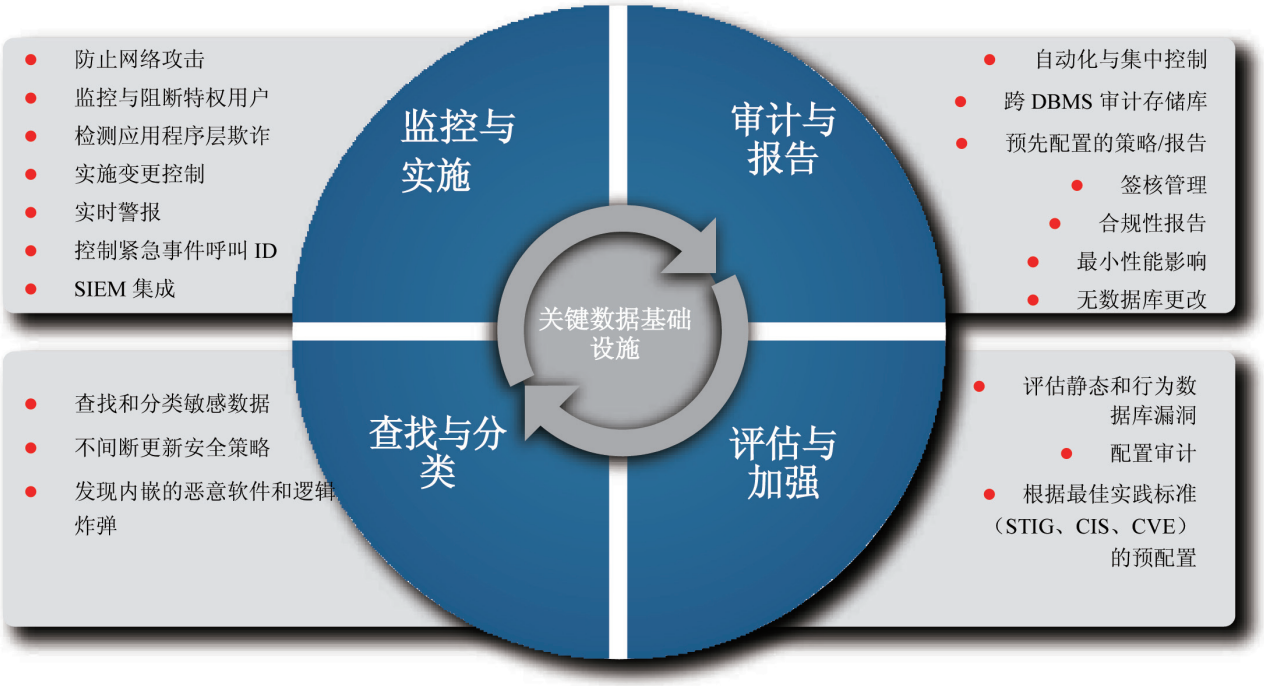
全球超过1000个组织信赖IBM，并请IBM而非其他技术供应商来保护其关键企业数据。实际上，我们提供了最简单、最有效的解决方案来保护财务和ERP信息、客户与持卡人数据和存储在企业系统内的信息资产。

我们的企业安全平台可防止拥有特权的内部人员或外部黑客进行未经授权或恶意的活动。该平台还能监控企业应用程序(例如Oracle E-Business Suite、PeopleSoft、SAP和自主开发系统)的最终用户可能存在的欺诈行为。

与此同时，我们的解决方案通过可拓展的多层架构来自动化和集中整个应用程序与数据库基础设施中的遵从性控制，从而提高运营效率。

该解决方案的功能引人注目，而它的性能指标同样值得关注。它对数据库服务器性能的影响很小，无需更改数据库，无需更改现有的网络拓扑，也不依赖于本地数据库日志或审计实用工具。

实时数据库安全与监控



统一的解决方案：InfoSphere Guardium基于一个统一的控制台和后端数据存储，提供了一系列集成化模块，用于管理整个数据库安全性和遵从性生命周期。

InfoSphere Guardium是唯一一种通过统一的Web控制台、后端数据存储和工作流自动化系统应对整个数据库完整性和遵从性生命周期的解决方案，它使您能够：

- 定位和分类企业数据库中的敏感信息。
- 评估数据库漏洞和配置缺陷。
- 确保在实现推荐更改后锁定配置。

- 凭借支持职责分离的安全、防篡改的审计跟踪，跨所有平台和协议提供所有数据库事务的**100%可见性和细粒度控制。**
- 跟踪主要文件共享平台上的活动，如Microsoft SharePoint。
- 监控和实施敏感数据访问、特权用户活动、变更控制、应用程序用户活动和安全例外(如登录失败)等策略。
- 自动化整个遵从性审计过程，包括将报告分发给监管团队、签核和上报——利用针对**SOX、PCI DSS和数据隐私的预配置报告。**
- 为企业级遵从性报告、性能优化、调研和辩论创建单一、集中的审计存储库。
- 轻松从保护单一数据库扩展到保护遍及全球的分布式数据中心内的数千个数据库。

查找与分类

自动定位、分类和保护敏感信息

组织创建和维护的数据信息量日益增加，他们发现定位和分类敏感信息也越来越困难。

对于经历过兼并和收购的组织以及原始开发人员已离开的遗留系统环境来说，这种挑战尤为艰巨。即便在最好的情况下，应用程序和数据库结构的不断更改(支持新业务需求所必须的更改)也会使静态安全策略失效，并使敏感数据处于不可知和无保护的状态。

组织发现以下任务尤为困难:

- 确定所有包含敏感信息的数据库服务器，并理解如何通过各种源进行访问(业务线应用程序、批处理、特别查询、应用程序开发人员、管理员等)。
- 在所存储信息的敏感程度未知时保护信息并控制风险。
- 在哪些信息应符合具体规范不明确的情况下确保遵从性。

利用InfoSphere Guardium，即可利用数据库自动发现和信息分类来确定将机密数据存储在何处，随后利用可自定义的分类标签来自动实施安全策略，将其应用于特定类别的敏感对象。这些策略可确保敏感信息仅可被授权用户查看和/或更改。

可以定期执行敏感数据发现任务，以防止引入恶意服务器，确保没有任何重要信息会“被遗忘”。

评估与加强

漏洞、配置和行为评估

InfoSphere Guardium的数据库安全性评估将扫描整个数据库基础设施，查找漏洞，并使用实时和历史数据提供对数据库安全状态的连续评估。

它提供了完整的预配置测试库，基于行业最佳实践(CVE、CIS、STIG)和特定于平台的漏洞(通过Guardium知识库服务定期更新)。您还可以定义与具体需求匹配的自定义测试。评估模块也会标记与遵从性相关的漏洞，例如未经授权地访问保留的Oracle EBS和SAP表，以便遵从SOX和PCI DSS。

评估可分为两大类别:

- 漏洞和配置测试检查漏洞，例如缺少补丁、特权和默认账户配置错误等。
- 行为测试实时监控所有数据库，根据访问和操纵数据库的方式来识别漏洞——例如登录失败次数过多、客户端执行管理命令或非工作时间的登录。

除了生成带有向下钻取功能的具体报告之外，评估模块还将生成一份安全性健康状况报告单，其中包含权重指标(基于最佳实践)、行业标准参考数字，并推荐可加强数据库安全性的具体行动计划。

配置锁定和变更跟踪

实现了漏洞评估所生成的建议行动之后，即可建立安全配置基准。利用InfoSphere Guardium的Configuration Audit System (CAS)，即可监控对此基准的任何更改，并确保不会在授权的变更控制策略和流程以外做出更改。

监控与实施

监控和实施数据库安全性与变更控制策略

InfoSphere Guardium提供了细粒度、实时的策略，防止特权账户执行未经授权或恶意操作或者来自恶意用户或外部用户的攻击。您还可以识别通过多层应用程序(这些多层应用程序通过通用服务账户访问数据库)对数据库进行未授权更改的应用程序用户，例如Oracle EBS、PeopleSoft、Siebel、SAP、Cognos和构建于IBM WebSphere、Oracle WebLogic和Oracle AS等应用服务器之上的自定义系统。

该解决方案可由信息安全人员管理，无需数据库管理员(DBA)的干预。您还可以定义细粒度访问策略，基于OS登录情况、IP或MAC地址、源应用程序、日时、网络协议和SQL命令的类型限制特定表的访问。

所有数据库流量的连续上下文分析

InfoSphere Guardium实时连续地监控所有数据库操作，利用正在申请专利的语言分析，根据各SQL事务的具体上下文信息(“谁、什么、哪里、何时和如何”)来检测未经授权的操作。

这种独特的方法可最小化假阳性和阴性现象，同时提供无与伦比的控制水平，不同于仅寻找预定义模板或签名的传统方法。

设定基准以检测异常行为并自动化策略定义

通过建立基准，并识别正常的业务流程和存在异常活动的业务流程，系统即自动推荐可用于防止SQL注入等攻击的策略。可通过直观的下拉菜单轻松添加自定义策略。

前瞻、实时的安全性

InfoSphere Guardium提供了丰富的实时控件，用于前瞻性地响应未经授权或异常的行为。基于策略的行动可包括实时安全警报(SMTP、SNMP、Syslog)、软件阻塞、启用完整日志记录、隔离用户和自定义操作，例如VPN端口关闭和与周边IDS/IPS系统协调一致。

跟踪和解决安全事件

遵从法规要求组织证明自己即时地记录、分析、解决了所有意外事件，并向管理者进行了报告。InfoSphere Guardium提供了业务用户界面和工作流自动化，用于应对安全事件，此外还提供了一个仪表板，用于跟踪关键指标，例如开放的意外事件、严重度级别和意外事件开放的时长。

审计与报告

配置细粒度审计跟踪记录

InfoSphere Guardium可创建所有数据库活动的连续、细粒度的跟踪记录，根据上下文实时分析和筛选以便实现前瞻性的控制并生成审计人员所需的特定信息。

所得到的报告提供对所有数据库活动(例如登录失败、特权升级、模式更改、非工作时间访问或未经授权的应用程序访问、敏感表访问)的可见性，并以此来体现遵从性。例如，系统监控以下全部内容:

- 安全异常，例如SQL错误和登录失败。
- 更改数据库结构的DDL命令，例如Create/Drop/Alter Tables，这对于SOX等数据治理规范尤为重要。
- SELECT查询，这对于PCI DSS等数据隐私规范尤为重要。
- 包含绑定变量的DML命令(Insert、Update、Delete)。
- 控制账户、角色和权限的DCL 命令(GRANT、REVOKE)。
- 各DBMS平台支持的过程语言，例如PL/SQL (Oracle)和SQL/PL (IBM)。
- 数据库执行的XML。
- SharePoint对象更改。

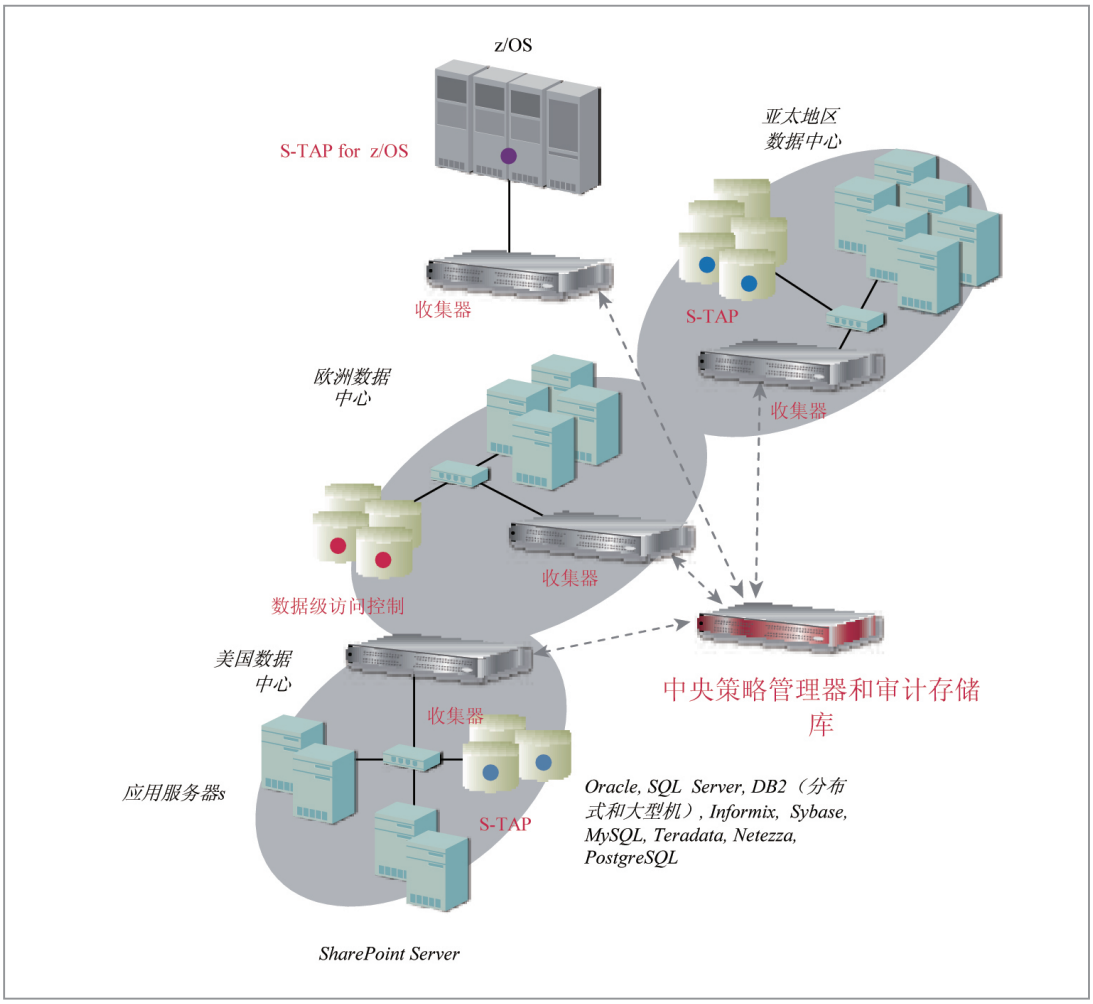
同类最佳的报告

InfoSphere Guardium解决方案以我们与全球1000家企业、四大会计师事务所审计人员和全球各地评估人员合作的经验与最佳实践为基础，包含超过150种预配置的策略和报告。这些报告可帮助满足法规要求，例如SOX、PCI DSS和数据隐私法，同时可简化数据治理和数据隐私计划。

除了预先打包的报告模板之外，InfoSphere Guardium还提供了拖放式的图形界面，使您可轻松创建新报告或修改现有报告。可采用PDF格式(作为电子邮件附件)或HTML页面的链接形式，通过电子邮件自动将报告发送给用户。还可通过Web控制台界面在线查看报告，或以标准格式导出到SIEM和其他系统。

为企业提供的特性功能

- **非侵入性**: 所有数据库事务的100%可见性——包括特权用户的本地访问，对性能的影响最小，无需数据库或应用程序更改。
- **独立于DBMS**: 跨平台解决方案，不依赖于本地日志记录或审计。
- **基于设备**: 模块化的软件套件，构建于加强的 Linux 内核之上，旨在通过"黑箱"设备快速部署(自包含的存储器、预先安装的应用程序、内置管理)。也可作为虚拟设备使用，支持硬件整合战略。
- **灵活的监控**: 利用基于轻量级主机的探测器、SPAN端口、网络TAP或任意组合。
- **基础设施就绪**: 支持SNMP、SMTP、Syslog、LDAP、Kerberos、RSA SecurID®、变更单系统，如BMC Remedy、CEF以及与所有主要SIEM平台的集成。
- **多层**: 业内唯一的 InfoSphere Guardium可自动在一个中央审计存储库内聚合和标准化来自多种数据库平台和位置的审计信息。
- **集中管理**: 通过Web控制台对跨DBMS的安全策略进行企业级管理。
- **可拓展**: 随着被监控的服务器数量或流量的增加，只需添加设备来处理新增负载。获得专利的智能存储算法提供的存储效率超出基于平面文件的传统方法百倍以上。
- **防篡改审计存储库**: 强力身份验证，无需root访问和加密存档。
- **基于角色**: 根据组织角色控制对模块和数据的访问。



可拓展的多层架构

InfoSphere Guardium的可拓展架构支持大型和小型环境，提供审计数据的集中聚合和标准化，并通过Web控制台提供企业级安全策略的集中管理。S-TAP是轻量级、基于主机的探测器，监控所有数据库流量，包括特权用户的本地访问在内，并将其转播至InfoSphere Guardium收集器设备用于分析和报告。收集器设备从S-TAP收集监控数据和/或通过直连网络交换机中的SPAN端口收集这些数据。聚合器自动聚合来自多个收集器设备的审计数据。为了实现最大程度的可拓展性和灵活性，您可配置多层聚合器。作为S-TAP扩展实现的InfoSphere Guardium数据级访问控制也可加强和实施职责分离，它可阻止DBA执行安全功能，例如创建新数据库账户或提升现有账户的特权。

遵从性工作流自动化

业内唯一的InfoSphere Guardium遵从性工作流自动化应用程序可简化整个遵从性工作流过程，帮助自动化生成审计报告、分发给关键参与者、电子签核和提交的过程。工作流过程是完全可由用户具体自定义的，支持通过签核单独发送和跟踪特定审计项。

异构环境的统一解决方案

广泛的平台支持

InfoSphere Guardium的跨平台解决方案支持所有主要操作系统(Windows、UNIX、Linux、z/OS)上运行的全部主要DBMS平台和协议以及Microsoft SharePoint和FTP环境:

支持的平台	支持的版本
Oracle Database	8i, 9i, 10g (r1, r2), 11g, 11gR2
Oracle Database (ASO, SSL)	9i, 10g (r1, r2), 11g
Microsoft SQL Server	2000, 2003, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.2, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	V5R2, V5R3, V5R4, V6R1
Sun MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
Netezza	4.5
PostgreSQL	8
Teradata	6.X, 12, 13
FTP	

基于主机的监控

业内唯一的S-TAP是轻量级的软件探测器，在数据库服务器的OS级别监控网络和本地数据库协议(共享内存、命名管道等)。S-TAP可将所有流量转播至独立的InfoSphere Guardium设备进行实时分析和报告，无需依赖数据库本身来处理和存储日志数据，因而可最小化对服务器性能的影响。S-TAP可消除对远程位置的专用硬件设备或数据中心内可用的SPAN端口的需求，因而往往更受欢迎。

OS 类型	版本	32 位和 64 位
AIX	5.1, 5.2, 5.3, 6.1	两者 64 位
HP-UX	11.00, 11.11, 11.23, 11.31	两者
Red Hat Enterprise Linux	3, 4, 5	两者
Red Hat Enterprise Linux for System z	5.4	
SUSE Enterprise Linux	9, 10, 11	两者
SUSE Enterprise Linux for System z	9, 10, 11	
Solaris - SPARC	8, 9, 10	两者
Solaris - Intel/AMD	10	两者
Tru64	5.1A, 5.1B	64 位
Windows	2000, 2003, 2008	两者
iSeries	i5/OS*	

* 通过Enterprise Integrator支持网络活动监控和本地活动支持

应用程序监控

InfoSphere Guardium可跟踪通过多层企业应用程序(而非直接访问数据库)访问关键表的最终用户的活动，识别潜在的欺诈行为。这种做法是必要的，因为企业应用程序通常使用称为“连接池”的优化机制。在池环境中，所有用户流量都聚集在少数数据库连接内，仅由通用应用程序 账户名称标识，因而可掩藏最终用户的身份。InfoSphere Guardium支持所有主要的现成企业应用程序的应用程序监控。在应用服务器级别监控事务可提供对其他应用程序(包括内部应用程序)的支持。

支持的企业应用程序	• Oracle E-Business Suite • PeopleSoft • Siebel • SAP • Cognos • Business Objects Web • Intelligence
支持的应用服务器平台	• IBM WebSphere • BEA WebLogic • Oracle Application Server (AS) • JBoss Enterprise Application • Platform

关于 IBM InfoSphere Guardium

Guardium是IBM InfoSphere的一部分，IBM InfoSphere是在系统内定义、集成、保护和管理可靠信息的集成化平台。InfoSphere平台提供了可靠信息的所有基本构造块，包括数据集成、数据仓库、主数据管理和信息治理，所有构造块均以共享元数据和模型为核心而集成。该产品组合是模块化的，允许您从任意位置开始，将InfoSphere软件构造块与其他厂商提供的组件随意混搭使用，或者选择同时部署多个构造块，以提高速度、增加价值。InfoSphere平台为信息密集型项目提供了企业级基础，提供了必要的性能、可拓展性、可靠性和加速能力，以便简化艰巨的挑战并交付可靠的信息，使您的业务更迅速地发展。

IBM Corporation
Route 100
Somers, NY 10589

在中国印制

2010年8月

IMD14286-CAEN-01