IBM

Information Management

数据库保护与合规

IBM InfoSphere Guardium

数据库安全及审计

目录

InfoSphere Guardium概述

InfoSphere Guardium为维护整个应用和数据库基础架构的安全性，提供了最简便、最强大的解决方案，它包括下列组件:

- 实时数据库活动监控(DAM)，主动识别未经授权的活动或可疑活动，从而防止攻击并阻止特权用户的非法访问
- 审计与合规解决方案，用以自动化和简化与PCI DSS、SOX、SAS70、ISO 27001/2、NIST 800-5及数据隐私法规相关的验证活动
- 变更控制解决方案，防止未经授权变更数据库、权限及配置
- 漏洞管理解决方案，识别并修复数据库漏洞，如丢失的补丁、权限配置错误及默认账户问题等
- 防欺诈解决方案，利用应用程序层监控来识别未经授权的应用程序用户(SAP、PeopleSoft、Oracle EBS、Cognos等)活动
- 数据库泄漏防护，定位敏感数据并防止数据中心破坏

目前全世界已有四百多位客户安装该解决方案，其中包括世界五大银行；全球最大的六家保险公司中的四家；高级政府机构；全球三大零售商中的两家；二十家全球主要的电信运营商；最大的两个饮料食品集团；最大的PC制造商之一；一家排名世界前三位的汽车制造商；一家排名世界前三位的航空公司；以及一家商业智能软件领先供应商。InfoSphere Guardium是首个解决核心数据安全漏洞的解决方案，它提供的可扩展企业平台，既可实时保护数据库，又实现了整个合规审计流程的自动化。

本文简要概述了InfoSphere Guardium的各种可选功能。要全面了解InfoSphere Guardium核心解决方案，请参见InfoSphere Guardium手册。

Guardium是IBM InfoSphere的一个组成部分；是一个定义、集成、保护及管理整个系统可靠信息的集成平台。InfoSphere平台可提供所有可信信息的基础构建块，包括数据集成、数据仓库、主数据管理及信息治理，所有构建块均围绕一个共享的元数据和模型核心进行集成。该产品是模块化的，您可以在任何位置启动，还可将InfoSphere软件构建块与其他厂商的组件混合与配对，或者将多个构建块部署在一起，以提高速度，增加价值。InfoSphere平台为信息密集型项目提供企业级基础，提供必要的性能、可扩展性、可靠性及加速度，化解难题，快速为企业提供可靠信息。

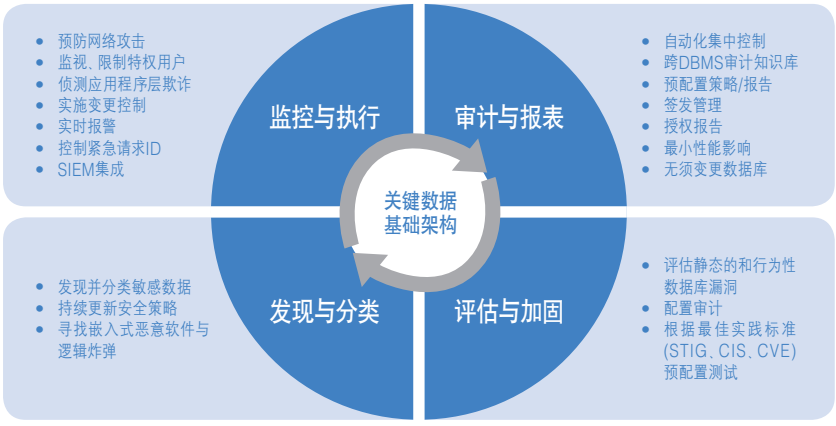


图1: 构建于一个统一的控制台和后端数据存储区上，InfoSphere Guardium可提供一系列集成模块，来管理整个数据库的安全性和合规生命周期。

先进的合规工作流自动化

自动化监督流程，降低运营成本

- 在企业范围内集中并自动执行监督流程，包括报告生成、分发、电子签发及逐级上报
- 通过指定您的独特的工作流程步骤、操作及用户组合，轻松创建自定义流程
- 支持按报表逐项自动执行监督流程，从而最大限度地提高流程效率，而不影响安全性
- 确保监督小组成员只能查看与其各自的角色相关的数据和任务
- 利用实时工具提高流程效率，集中进行流程管理
- 存储流程会产生安全的集中式知识库，以及供合规和法庭使用的具体审计数据

企业级监督流程管理

随着法规的日益增加和人们对数据隐私和安全性的重视，组织采用了各种流程，审核定期安排的监控活动结果，调查并补救违规事件。例如，组织会每日审查事件报告，同时每周进行数据库漏洞评估并审查数据库查询过程。

绝大多数企业都拥有数百至数万个数据库，这些数据库均由各种机构进行管理和监督，其中包括安全工作组及IT工作组。这些流程可能依次按照部门、地域、系统功能及其他因素进行组织。这种复杂性通常直接影响监督流程，因而需要执行各种不同的流程，每个流程均具有其各自独特的审查步骤、措施和参与者。

手动流程会增加运营成本和审计异常

过去，组织通过人工操作管理监督流程，依靠电子邮件和电子表格等工具记录事件、向有关方发布调查信息、表达补救措施和文档注释。由于流程复杂而多样，运营成本居高不下，由流程分解而导致的审计异常时有发生。按照法律需要检索历史结果同样困难，这是由于监督信息均以不同格式存储，并且有时存储于不同的物理空间内。

自动化监督流程以提高运营效率

先进的合规工作流自动化模块，可实现整个安全和合规工作流程的自动化，从而消除手动操作并确保及时完成监督活动。易于使用的图形用户界面允许创建各种流程，满足任务和参与人员的独特需求。可通过下列几个简单步骤创建新流程：

- 创建由个别事件状态和操作组成的自定义工作流(见图2)
- 为待执行的操作分配一个或多个人员或角色。操作可选择使用电子签发。允许并行操作，支持依照不同标准细分操作流程(例如，不同DBMS生成的异常审核可能由不同人员签发)

- 创建并安排审计流程，定期自动执行工作流程(见图3)
- 向审计流程中添加任意的任务组合。例如，可将每周使用相同的工作流程执行和审查的多份报告指派给同一审计任务。支持各种各样的审计任务，其中包括审查自动生成的漏洞评估、资产查询、数据分类、配置审计及数据库活动监控报告

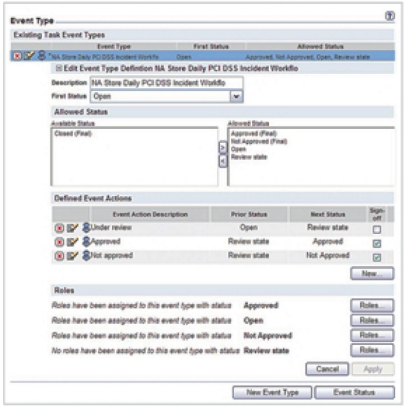


图2: InfoSphere Guardium先进的合规工作流自动化模块，可让用户通过简单的图形用户界面指定相关的操作、事件状态和角色，轻松地创建为其各自的独特流程定制的工作流。

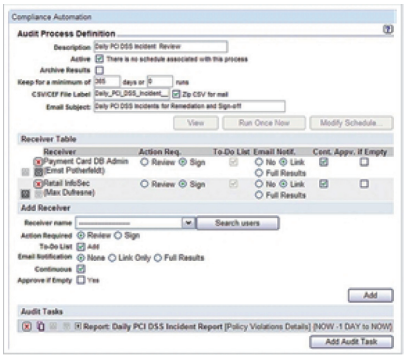


图3: 工作流定期自动启动，从而确保能够始终如一地执行和跟踪经常性任务，如日常事故审核和漏洞评估。

利用细粒度的工作流程控制措施提高安全性

通过自动发送电子邮件通知以及更新员工InfoSphere Guardium网络界面的“待办事项”列表，通知工作流中的相关人员执行特定操作，所有既定操作均在web上安全执行，包括审查结果、审批签发、评论及将操作逐级上报。

各项操作均逐项执行，从而能够快速而彻底地进行审核，并确保各流程不会受到有待研究的个别项目的阻碍。例如，一位收到日常PCI DSS异常报告的人员发现其中包含五项事件，其中四项均由已知问题引起，且已经得到解决。因此他可以迅速将这四个项目标记为已审核；而第五个项目待事件经过调查并解决后再行审核。已审核的四个项目立即进入工作流的下一步骤；第五个项目将随后进入这一步骤。还要向每一项添加注释，说明采取了哪些补救措施。

为了最大限度地提高安全性，支持职责分离，在工作流中工作的人员仅能查看与其具体职责相关的信息。职责分配体现在两个层次上。第一个层次与工作流上的职责相关，如上所述。根据工作流的定义，工作人员仅能查看与其具体职责相关的信息。

第二个层次涉及InfoSphere Guardium系统核心的访问控制机制，让管理员能够针对特定的数据库或系统向个人(或角色)分配职责，并实现分级管理。举一个简单的例子，便可以说明这种功能的好处。在一个旨在审核数据库漏洞定期评估结果的工作流中，第一步是“数据库管理员”组审核测试结果。数据库管理员组成员Martha被授权查看所有财务数据库，那么他仅可查看与财务数据库相关的测试结果，而Patrick，获得了支付卡数据库的管理权限，他仅可查看与此相关的结果。InfoSphere Guardium利用并行操作，定义了高效的工作流，既不会影响安全性，也不会让用户处理与其职责无关的信息。

通过企业级管理强化责任机制

工作流管理者可在整个企业范围内实时查看每项已定义的审计任务的状态视图，按责任方、当前操作状态和注释查看必要的操作。这个强大的界面，提供了跨越异构数据库基础架构和分布式团队妥善管理监督流程所需的必要信息，强化了责任机制，并最大限度地减少审计异常。

审计流程的结果存储于InfoSphere Guardium安全知识库中，与审计数据一同存放，从而使组织能够轻松地为审计员提供无可争议的审计线索，证明所有必要任务均一致执行。高级归档功能可自动安全地归档知识库，支持最严苛的记录保留要求，并可应审计或法庭调查要求轻松地进行恢复。

InfoSphere Guardium先进的合规工作流自动化功能使组织能够自动化并简化合规流程，从而降低运营成本，简化审计的筹备工作，适用于有独特操作要求的复杂环境。

数据库漏洞评估

基于最佳实践的全面自动化测试

- 扫描特定的数据库组
- 检查常见漏洞，如丢失的补丁、弱密码、权限配置错误及默认供应商账户
- 包含数百项基于互联网安全中心(CIS)和美国国防部(DoD)开发的最佳实践的预配置测试
- 生成安全状况记录卡，建议加强数据库安全性的具体操作计划
- 简化大型环境中的部署——可自动加载多个数据源(数据库名称、类型、服务器IP、端口、角色)，并通过脚本接口将数据源链接至评估

提高数据库安全性和合规性

保护数据库基础架构、遵从法规并通过审计最佳方式之一是定期执行数据库环境安全性评估。

安全性评估可评估数据库环境的安全强度，并将其与行业最佳实践进行比较。这些深度评估可检测补丁级别和数据库配置，突出环境漏洞——使您能够快速修复问题，并维护关键的企业数据，使其免受内部及外部威胁侵害。

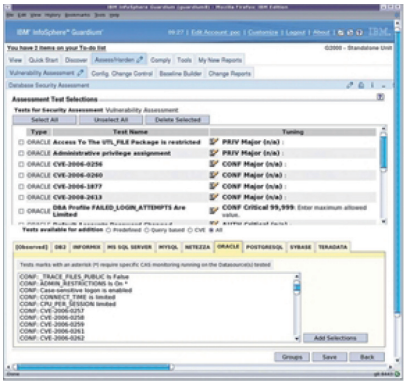


图4：InfoSphere Guardium的数据库漏洞评估模块可扫描数据库基础架构，搜寻丢失的补丁、权限配置错误及其他漏洞。它吸纳了包含数百项最佳实践的预配置测试库，并提供如何修复漏洞的相关建议，其中包括与外部资源相关联的标识符(例如CVE)。您也可以创建自定义测试和监督流程。

基于CIS与DoD最佳实践的预配置测试

InfoSphere Guardium的数据库漏洞评估(VA)模块可利用实时数据及历史数据，扫描数据库基础架构搜寻

漏洞，提供持续的安全状况评估。

InfoSphere Guardium VA包含基于美国国防部创建的计算机互联网安全(CIS)基准、数据库安全技术实施指南(STIG)等行业最佳实践的综合预配置测试库(见图4)。这些测试可检测丢失的补丁、弱密码、权限配置错误及默认账户问题等常见漏洞，以及每个DBMS平台的特有漏洞。

测试通过InfoSphere Guardium的知识库服务每季度更新一次。您还可以定义自定义测试(见图5)及安排自动审计任务，纳入扫描、报告分发、电子签发及逐级上报流程。

除利用向下钻取的功能(见图6)生成详细报告外，该评估模块还针对每项漏洞推荐具体的操作计划，增强安全性。例如，如果存在权限问题，系统将告知您究竟需要取消哪些权限，以便遵从最佳实践。测试结果还会引用 CVE 标识符等内容，以链接外部资源。

一旦漏洞得以修复，组织必须确保系统仅允许经过授权的变更。InfoSphere Guardium配置审计系统(CAS)可监控系统，检测安全配置基线建立后发生的任何变更。

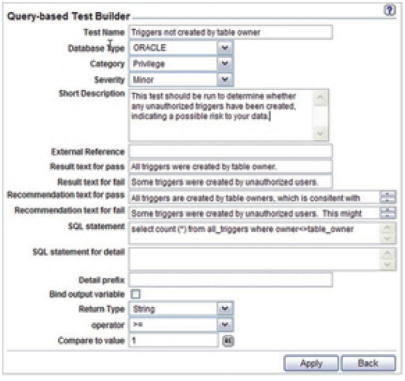


图5: 采用SQL查询的自定义测试可利用基于表单的测试生成器轻松创建。自定义测试也可通过OS脚本和Java类进行创建。

图6: InfoSphere Guardium数据库漏洞评估模块可生成整体安全状况的概要评估，并可下钻详细信息，提供具体的改进建议。

范围广泛的细粒度测试

评估可分为多种类别，包括:

- **权限:** 检查对象创建和使用权限、授予数据库管理员和用户的权限及系统级权限
- **验证:** 验证密码策略、默认供应商账户、非空密码、远程登录参数等
- **配置:** 检查特定于平台的变量，例如登录数据库管理员配置文件(Oracle)的最高尝试失败次数，禁止更新系统表(MS-SQL)，并确保SYSADM_GROUP已经定义(DB2)
- **版本:** 验证相应的版本号和补丁级别
- **行为:** 这些测试利用InfoSphere Guardium的实时活动监控功能，通过观察行为识别漏洞，例如在非规定时间登录、登录失败次数过多、特权命令执行及特权凭据共享等
- **文件权限:** 检查关键对象(如数据库主目录)、配置文件(如sqlnet.ora)及注册表/环境变量的权限

多项评估技术，不影响正常运行时间和性能

InfoSphere Guardium VA为行业中独一无二的产品，整合了三种基本侦测方法，全面覆盖各种漏洞和威胁:

- **扫描:** 系统通过使用只读凭据访问数据库，评估数据库漏洞
- **基于代理的扫描:** 每台数据库服务器上安装了轻量级代理，可识别远程无法确定的漏洞，如关键操作系统、数据库配置文件及脚本(需要CAS)的文件权限
- **被动网络监控:** 该系统通过实时观测所有数据库事务发现漏洞，如数据库错误过多(表明可能发生SQL注入攻击)、使用共享管理账户和服务ID，或使用默认供应商账户

最重要的是，InfoSphere Guardium的漏洞评估功能提供完整的平台覆盖范围(见图7)，而不会影响关键系统的性能和稳定性。该系统不运行因模仿攻击者行为而破坏系统的侵入式漏洞利用(intrusive exploits)，同时它也不依赖可能产生额外开支的传统数据库日志或本机审核功能。

数据库支持
Oracle
Microsoft SQL Server 2000、2005、2008
IBM DB2 (LUW和z/OS)
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

图7: InfoSphere Guardium可提供加固整个数据库基础架构的简单方法，从而为所有主要的DBMS平台提供漏洞评估功能。

超越简单的报告: 解决整个漏洞管理周期的问题

InfoSphere Guardium的数据库漏洞评估模块与平台中的其他模块紧密集成，让您能够利用统一的Web控制台、后端数据存储及工作流自动化系统，管理整个数据库安全与合规周期。

企业不仅能够生成漏洞报告，还能够解决端到端的漏洞管理流程中的问题，包括评估和降低业务风险、制定补救策略，及简化合规报告和监督流程。特别是，InfoSphere Guardium可让您迅速:

- **发现数据库漏洞:** 缺少补丁及配置错误的数据库会产生巨大风险。InfoSphere Guardium VA拥有大型评估测试库，融合了行业最佳实践，可以识别漏洞。每季度推出的知识库服务可确保评估测试经常更新
- 通过实时控制保护未打补丁的系统: 敏感系统可在三至六个月内生成补丁。InfoSphere Guardium可通过活动监控、基于签名的策略及预防性控制措施，在补丁生成期间保护数据库的安全

  这些策略和基线还能够防止应用程序漏洞，如SQL注入和缓冲区溢出。例如，您可以提醒和/或阻止在未打补丁的程序上执行来自非业务线应用程序的调用，说明可能会受到攻击
- **根据业务风险制定补救策略:** InfoSphere Guardium的Classifier模块可定位和分类公司数据库中的敏感数据(如信用卡号码)，同时其基线函数可对行为记录进行分析，弄清业务线应用程序在何时以何种方式访问敏感数据库。风险评估对于制定补救策略至关重要，因为绝大多数组织并不具备足够的资源，同时为所有敏感系统生成补丁

- **加固数据库:** 利用评估测试提供的建议修复敏感系统后，InfoSphere Guardium的CAS确保禁止在未经授权情况下变更配置，从而“加固”配置
- **记录并简化合规:** 审计员想了解各种事故是否及时地得到跟踪和解决。通过InfoSphere Guardium的事件管理和合规工作流自动化(见图8)模块，可以自动执行报告分发、电子签发及逐级上报，跟踪敏感系统的修复进程

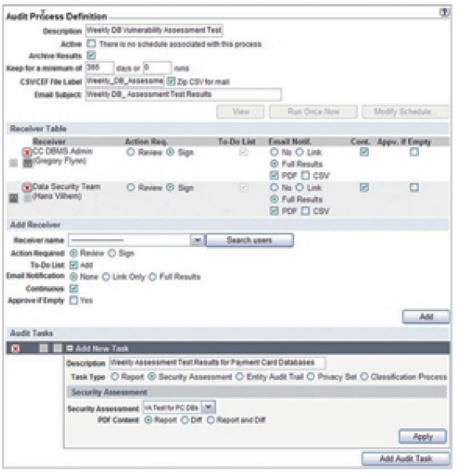


图8: 审计员要寻找证据证实组织确实采用了定义明确的流程，完全可以保护其关键数据。InfoSphere Guardium的工作流自动化模块，可让企业自行定制审计任务，同时利用报告分发、签发及逐级上报功能，自动执行预定的漏洞评估。

数据库保护知识库

定期内容更新使安全性与合规性最大化

- 利用有关数据库漏洞、最佳实践策略及企业应用的敏感表的最新相关信息，主动更新InfoSphere Guardium系统
- 利用有关数据库对象及软件包安全风险的最新信息，划分易受攻击的对象组，自动更新相关的防御性策略
- 识别常见企业应用(例如SAP、Oracle EBS)中需要保护的敏感表，如包含PCI DSS或财务(SOX)信息的表单，减少前期及持续劳动时间
- 对包含预定义漏洞评估测试的InfoSphere Guardium知识库进行更新，避免受到最新威胁的影响
- 对能够识别具有安全与合规要求的数据库和应用程序对象的组合评分，从而制定高级策略

在瞬息万变的环境中保护敏感数据

各行业中的组织都依靠数据库存储高价值信息，并结合企业应用来执行关键任务。因此，通常需要部署IBM的InfoSphere Guardium等数据库安全与合规解决方案。

为了最大限度地提高InfoSphere Guardium的保护功能，应定期更新群组、策略、测试等配置参数，以适应不断变化的数据库基础架构性质及相关威胁。例如，漏洞测试应显示最新漏洞利用和补丁级别，而策略应包含敏感对象的最新列表。

虽然管理员能够轻松地手动修改InfoSphere Guardium的配置参数来说明这种变更，但他们往往缺乏专业知识或时间来完成此操作。收集全面的漏洞信息需要具备与所保护系统有关的技术专长，还要具备从整个行业搜索和整合漏洞利用信息的能力。与企业中常见的多种数据库系统和企业应用保持同步，同样颇具挑战性。每种系统和应用程序都具有其各自独特的体系结构、文档和发布计划。然而无法做出更新反映所有这些参数的最新变更，可能会导致大量的安全与合规缺口。

利用IBM的专业技术和人才实现安全与合规最大化

IBM的InfoSphere Guardium数据库保护知识库是一项年度服务，以可消费的模式为客户提供与其数据库和应用相关的最新内容，实现安全性与合规性的最大化。提供的信息包括:

- 软件补丁级别
- 版本级别
- 易受攻击的对象

- 敏感对象(如带有SOX、PII或PCI数据的表格)
- 漏洞评估测试和标识符
- 存储程序
- 管理程序
- 命令、错误和用户角色

从多种来源中收集信息，包括IBM内部研究、与其他供应商的交流活动及跨行业的合作等等。信息被收集、封装、整合到相应的Guardium元素中(例如漏洞测试、分组等)，并在经过测试后，交付给InfoSphere Guardium客户。

易于管理

知识库的更新通常按季度发布，以配合DBMS供应商的季度发布时间表；不过，也会根据当前环境和风险状况做出调整。

只需单击鼠标，更新即可轻松实现(见图9)。InfoSphere Guardium内嵌的智能更新流程可适应用户的定制要求。如果用户已添加某个对象，系统将识别该操作并在更新过程中将其保留。例如，如果用户已经定制了某个企业应用，那么一个对象会添加至相关的PCI组，以确认该项定制已经生成。在下次更新时，InfoSphere Guardium将认出这个对象是后来添加的，并在更新过程中将其保留。

图9：只需单击鼠标，即可将数据库保护知识库服务定期提供的当前漏洞、审计及最佳实践库整合至InfoSphere Guardium。

IBM通过将打包的最新内容直接整合至InfoSphere Guardium，取消了手动内容更新操作，使管理成本最小化；与此同时，确保各项策略和测试都反映了最新的企业基础架构信息和威胁状况，使系统的数据保护和合规的优势最大化。

针对异构环境的全面保护

InfoSphere Guardium数据库保护知识库可针对所有主要平台更新交付内容(见图10)，从而提供一种简便的方法，确保安全策略始终都是最新的，而且同样适用于组织中常见的异构环境。根据平台的不同，交付的内容也不同(如上所述)，即广泛支持各种应用程序，包括：

- **测试以避免最新数据库漏洞的威胁**[1]：更新的漏洞评估(VA)测试可以确保定期执行安全性最佳实践要求的 VA 扫描，遵从各种法规，侦测各数据库基础架构平台的最新漏洞，包括丢失的补丁
- **合规性验证：**PCI、DSS及SOX等法规要求实施一些控制措施，以防止未经授权情况下修改和访问敏感数据。更新后的SAP和Oracle EBS最佳实践审计库，确保能够使用InfoSphere Guardium轻松地实施控制措施，无需花费时间持续研究这些应用以识别敏感表

[1] 需要漏洞评估模块

- **易受攻击对象的保护(虚拟补丁):** 在大多数组织中，在数据库补丁的发布和安装之间存在较长时间的延迟。希望在这段时间内降低暴露风险的组织，可对易受攻击对象组使用更新，轻松地实施规则，警示或阻止对该易受攻击对象的计划外访问，直至补丁安装成功

InfoSphere Guardium的数据库保护知识库还可执行多种其他应用程序，从敏感存储程序被使用时发出警报，到追踪特定类型的错误以期指示不当的活动。通过提供最新的群组信息，反映重要的安全与合规状况，InfoSphere Guardium在不增加运营开支的同时，实现了强有力的控制。

数据库支持
Oracle
Microsoft SQL Server 2000、2005、2008
IBM DB2 (LUW和z/OS)
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

图10: InfoSphere Guardium数据库保护知识库可提供多种更新内容，包括在所有主要数据库平台上的漏洞测试、敏感对象、易受攻击对象及当前补丁信息。

数据级访问控制

简化针对异构DBMS环境的预防性控制

- 阻止特权用户查看或变更敏感数据、创建新的用户账户或提升权限
- 不影响应用程序之间的通信
- 支持IT外包并节省相关费用——而不增加风险
- 实现SOX、PCI、Basel II、数据隐私法规的职责分离
- 通过对异构DBMS基础架构实施细粒度访问策略，简化安全与合规
- 以集中式自动化控制取代手动流程，提高运营效率

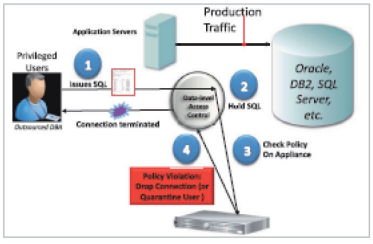
不断变化的控制需求

> *"Gartner咨询公司预测，2008年的金融危机将导致法规监管日趋严厉。因此，风险管理与合规性不容忽视。"*

事半功倍——管理风险时，在防范内部威胁的同时解决合规性问题，对于大多数组织而言越来越重要。

基于角色的访问及其他内置DBM控件旨在阻止最终用户访问敏感数据，但无法阻止可以自由访问所有SQL命令和数据库对象的特权用户的非法访问。

数据库活动监控(DAM)等新技术，可在侦测到异常活动或违反访问策略的行为时(包括特权用户违规)，生成详细的审计线索并发出实时安全警报，形成一个新的防护层。



Roles & Associated Policies	DDL	DML	SELECT	CREATE/ ALTER USER
PeopleSoft DBA	Allow	Allow	Block	Block
DBA access to other schemas	Block	Block	Block	Block
DBA working on DBA schema (sys, v$ tables, tuning)	Block	Allow	Allow	Allow or Block
Replication & Backups	Allow	Allow	Allow	Block
Developers	Block	Block	Block	Block

图11: InfoSphere Guardium数据级访问控制可利用一组细粒度策略简化企业安全性，实现跨越多个DBMS平台的职责分离—而不必中断应用程序访问或变更数据库配置。它是唯一能够限制特权用户(如数据库管理员、开发人员、外包人员等高级用户)的跨DBMS技术—防止他们查看或变更敏感数据。InfoSphere Guardium数据级访问控制可监控所有数据库连接，包括特权用户通过非TCP连接(如 Oracle BEQ、SHM、TLI、IPC等)进行本地访问。

虽然DAM是深度防护策略的重要因素，但在传统上一直仅限于提供侦测控制而非预防性控制，这是因为监控功能本身不能执行安全策略，阻止非法操作。

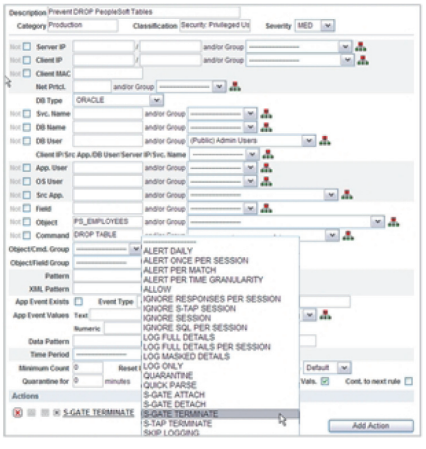
实时预防性控制；不会中断IT基础架构

作为基于主机的、包含细粒度的安全策略的(见图12)

轻量级软件代理(见图11)实现，InfoSphere Guardium数据级访问控制可提供自动化实时控制，防止特权用户执行下列非法操作:

- 执行敏感表查询
- 变更敏感数据值
- 在变更窗口外部添加或删除关键表(模式转变)
- 创建新的用户账户及修改权限

InfoSphere Guardium数据级访问控制完全是非侵入式的，且不需要数据库附加功能。因此，可以迅速执行，而无需中断关键业务应用程序，如Oracle E-Business Suite、PeopleSoft、Siebel、SAP、Business Objects及内部应用程序。



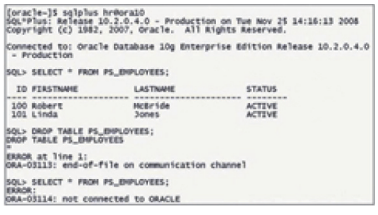


图12: InfoSphere Guardium平台可支持细粒度的决定性策略，主动识别违规操作(而不是依赖推断和猜测)。规则均以具体的会话属性为依据，如客户端IP地址、MAC地址、源应用程序、数据库用户、操作系统用户、应用程序用户、当日时间、SQL命令及表名称，往往通过预定义组进行定义，以简化日常管理。可针对策略违规调用范围广泛的策略操作，如实时警报(SMTP、SNMP、Syslog、CEF)、用户隔离及终止连接(如上所示)。

优于数据库驻留控制的特点

InfoSphere Guardium数据级访问控制拥有多项优于数据库驻留控制的特点，包括：

- **跨平台支持：** InfoSphere Guardium数据级访问控制可让组织针对它们的整体应用程序和数据库基础架构确定一套访问策略，而不是仅控制特定DBMS平台或版本访问。由于在数据库外部执行操作，InfoSphereGuardium数据级访问控制可支持所有主要的DBMS，平台：Oracle、Microsoft SQL Server、IBM DB2、IBMInformix、Sybase、Oracle MySQL、Teradata、Netezza及PostgreSQL
- **便于非数据库管理员使用：** 数据库驻留控制需要数据库管理员进行管理——产生了职责分离的问题。InfoSphere Guardium数据级访问控制可由IT安全性、合规性或风险团队进行管理，因为它使用英语语言，采用简明易懂的策略，可通过下拉式菜单进行定制，而无需掌握数据库命令和结构知识。此外，InfoSphere Guardium数据级访问控制还使用基于Linux的加固的网络设备管理访问策略，从而防止特权用户禁用或修改策略，并进一步加强职责分离
- **使用单一解决方案进行策略实施和审计：** 遵从性法规要求存储所有特权用户操作的完整审计线索，以便记录合规并协助法庭调查。DBMS供应商通常提供细粒度的审计，并将审计库作为独立的附加件。InfoSphere Guardium可在一项解决方案中同时提供策略实施和细粒度的审计，从而进一步削减成本，降低复杂性
- **审查查询结果的策略不仅针对即将生成的查询：** 数据库驻留控制仅限于控制对特定的对象执行特定的SQL命令。虽然同样是审查查询结果，但InfoSphere Guardium数据级访问控制却更进一步(见图13)。例如，当突然发现不合法的脚本或应用程序正在从数据库中提取PII时，连接立即断开，或者在调查期间将其隔离，而合法应用程序提取PII数据将不会受到影响
- **无中断执行：** 在执行某些日常维护任务时(如备份和修补)，某些数据库驻留控制必须关闭。在这些维护运行期间，特权用户可以利用控制被禁用的机会执行非法操作。InfoSphere Guardium数据级访问控制可持续执行访问策略，因为它不需要禁用数据库内部的特定特权账户

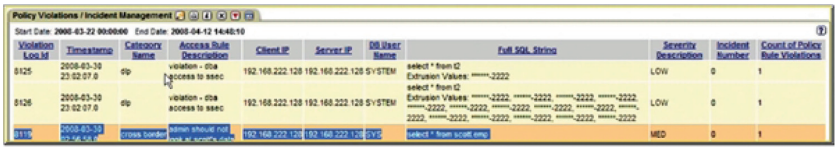


图13：挤压规则检查返回的数据(而不是入站SQL命令)，搜寻16位信用卡号码或9位社会保险号码。挤出的数据通常在作为审计线索(在上方以星号显示)的一部分存储于InfoSphere Guardium设备之前被遮罩。您可以定义名为“S-TAP TERMINATE”的策略操作，在查询结果中侦测到敏感数据后终止连接，从而限制数据泄漏(通常为数十条记录)。相比之下，“S-TAP TERMINATE”甚至会在DBMS对特定的数据库对象执行SQL命令之前终止连接。

InfoSphere Guardium基于主机的软件监视程序的扩展

数据级访问控制是InfoSphere Guardium基于主机的轻量级监视程序S-TAP™（“software tap”）的扩展。S-TAP业界独特的非侵入式软件监视程序，在数据库服务器的操作系统级别监控网络数据流，其中包括特权用户网络访问和本地访问(通过共享内存、命名管道、Oracle Bequeath等)。

S-TAP对服务器性能的影响极小，因为它们将所有流量中继到单独的InfoSphere Guardium设备，以进行策略评估、分析、报告及在线安全存储审计线索。

已经采用S-TAP的客户能够轻松地升级至InfoSphere Guardium数据级访问控制，开始执行细粒度级别访问——而不中断他们的应用环境。

授权报告

简化异构数据库环境的用户权限管理

- 提供了收集和了解整个数据库基础架构的授权信息的简便途径
- 来自八家供应商的、支持所有主要操作系统的、开箱即用的数据库平台支持
- 针对常用视图的预定义报告
- 与包括合规工作流自动化在内的其他InfoSphere Guardium模块完全集成，以降低运营成本
- 消除人工劳动，利用OX、PCI DSS及数据隐私法规等主要法规，提高数据安全性并简化合规性验证

数据库用户权限管理的挑战

近年来，组织都在努力应对不断增长的数据库信息量。随之而来的另一个挑战是实现有效的数据保护措施。

传统上，数据库管理员(DBA)主要依靠DBMS本机授权功能保护数据；努力最小化用户与其工作需求相关的对象和系统的特权(权限)。鉴于可用的特权种类繁多、用户账户和对象不断增加，以及级联角色的管理十分复杂，因而需要付出大量劳动。

数据库支持
Oracle
Microsoft SQL Server 2000、2005、2008
IBM DB2
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

图14：InfoSphere Guardium授权报告提供了收集和了解异构数据库基础架构用户权限信息的简便途径。

然而，业务环境的变化加剧了用户权限管理面临的挑战。越来越多的充满活力的组织异常频繁地变更角色和职责。兼并和收购形成了分布式的多供应商数据库基础架构，数据库管理员必须应对多样化的供应商授权模式和许多不同的系统。因此，确保将数据库权限控制在一定范围内，保证敏感对象和系统不受威胁，是极其困难的。这不仅带来了数据保护的问题，也产生了合规性的问题。

按照主要法规验证合规性的审计员需要进行定期审查(有时称作数据库用户权限鉴证报告)，确保定期调整用户权限，以符合人事、职责及实际使用状况的变动。

自动集中收集授权信息

InfoSphere Guardium授权报告提供了收集和了解整个组织的数据库授权信息的简便途径。系统还配置了可选的软件模块，以便定期扫描基础架构中所有选定的数据库，自动收集用户权限信息，包括通过角色和组成员资格赋予的用户权限。这省去了检查每个数据库的时间，并逐个跟踪级联角色(一个角色为另一个角色授权)，了解授权的真实状况。它还支持系统经常收集此类信息，无需使用稀缺的技术资源，从而提供及时、准确的信息，加强了安全性，满足了审计要求，同时降低了运营成本。

范围广泛的预配置报告

授权报告选项专为各种流行DBMS的授权系统而设计(见图14)，使其能够检索、了解并提交信息，这些信息是通过限定的权限以只读的方式访问整个异构环境收集的[1]。多样化的预定义报告(见图15和16)可提供不同的授权数据视图，使组织能够快速便捷地识别安全风险，如对象的不合理暴露、用户权限过多，及未经授权的管理操作。多种预定义报告的示例如下:

- 具有系统权限的账户
- 所有的系统和管理员权限; 同时按用户和角色显示
- 按用户显示的对象权限
- 所有可公开访问的对象
- 按对象显示的用户权限
- 为用户和角色授予的职责
- 权限的授予和撤销
- 按程序显示的执行权限

ORA Accnts with BECOME USER

Start Date: 2010-07-02 11:50:00 End Date: 2010-07-09 11:50:00
Aliases: ON

Grantee	Privilege	Admin Option	Datasource Name
BANKAPP	BECOME USER	NO	OCEAN ORACLE DB
JBROWN	BECOME USER	YES	OCEAN ORACLE DB
DBA	BECOME USER	YES	OCEAN ORACLE DB

图15: 利用InfoSphere Guardium授权报告模块可轻松识别权限不当的用户。在这份报告中，JBROWN拥有强大的Oracle "BECOME USER"的系统权限。此权限可能会被滥用，以获取未经授权的信息，或危害重要的应用程序。

mssql2005/8 Accnt Of db_owner db_securityadmin Role

Start Date: 2010-07-02 15:13:14 End Date: 2010-07-09 15:13:14
Aliases: OFF

Granted_Role	Grantee	SqlGuard Timestamp	Datasource Name	DB Name
db_owner	dbo	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial
db_owner	dbo	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	tempdb
db_owner	JBrown	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial
db_securityadmin	JBrown	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial

图16: InfoSphere Guardium可跨越八个DBMS平台(包括SQL Server、Oracle及DB2)聚合并展示授权信息。它简化了识别授权不当角色的过程，例如，JBrown同时被授予财务数据库db_owner和db_security管理员角色。

安全性与合规性的自动验证活动

从数据库基础架构中收集的所有授权信息，将与所有数据库审计信息一起存储在InfoSphere Guardium合法的、防篡改的存储库中，供所有系统模块(包括报表生成器、策略生成器及合规工作流自动化应用)使用。可

通过直观的拖放界面轻松构建自定义报告，从而显示在预定义报告中没有的特定视图。合规工作流自动化允许自动生成这些需要定期审核的报告，并将它们分发至相应的监督小组。它还可以电子捕捉评论、报送和审批，并将它们存储于库中，供审计员使用。

InfoSphere Guardium的策略监督和实现功能，还可利用从授权报告模块中捕获的信息。授权信息可在自动填充的策略组(automatically populating policy groups)等应用中使用。一个典型用例是，在用户尝试非法访问高级会员(VIP)的客户记录时，自动更新一个生成警报的策略。涉嫌泄露VIP记录而正在接受调查的员工，在受调查期间，他们的访问权限通常被撤销，并在下一期更新的“授权用户”组中有所反映。如果该员工尝试访问VIP记录，将会生成警报和事件记录，以供调查。

降低运营成本并改进数据保护

InfoSphere Guardium授权报告提供了收集、了解和使用用户权限信息的简便途径，最大限度地保护了敏感数据、并将运营成本降至最低，确保了审计的成功。它消除了耗时且容易出错的手动收集流程，在降低运营成本的同时分析用户权限信息，快速识别重要的安全缺口。合规工作流和策略管理的整合进一步降低了运营成本，同时展示了前瞻性控制措施的实施，满足敏锐的审计员的要求。

[1] 登录数据库收集授权信息，是通过IBM提供的脚本完成的，该脚本的运行要求具备限定的(只读)的权限；客户可检查此脚本，确定权限是否与其公司策略相符。

数据库服务器的配置审核系统

侦测影响数据库安全性的配置变更

- 跟踪数据库引擎范围外可能影响数据库安全性的所有变更
- 与InfoSphere Guardium数据库活动监控模块相辅相成，提供全面的数据库监控
- 跟踪可能影响数据库安全状况的数据库配置文件及其他外部对象变更，如
  - 环境/注册表变量
  - 配置文件(例如SQLNET.ORA、NAMES.ORA)
  - 外壳脚本
  - 操作系统文件
  - Java程序等可执行文件
- 实现所有治理及风险管理的必备模块
- 无需管理员参与即可实施最佳安全实践

保障数据库环境的安全

绝大多数数据库环境的变更均通过数据库引擎发生。对于大多数数据库类型，数据库控制和配置均通过特定的SQL命令，或者由数据库管理员或(数据库)安全管理员执行的存储程序来完成。

可使用InfoSphere Guardium的数据库活动监控功能来轻松地进行保护这些活动，这种功能使您能够监控并审计所有数据库活动——包括特权用户操作——并可执行访问控制策略，而不影响性能，也不依赖DBMS驻留日志或审计功能。

此外，InfoSphere Guardium的漏洞评估产品还可评估数据库的安全强度，突出强调一些问题，如参数配置错误、默认账户问题、需要应用补丁的漏洞，及需要撤销的特权。

综上所述，数据库是一项在操作系统级别上安装的程序，并且依赖操作系统的服务。许多配置元素均驻留在操作系统结构内，而不是位于数据中。

这样的例子包括文件、注册表值及环境变量。这些文件和值大多能控制某些最为重要的数据库安全性方面。数据库身份验证的方法就是一个很好的例子。在几乎所有的数据平台中，管理员均可以通过变动一个这样的值(要么与SQL一同使用，要么替代SQL)来变更数据库验证用户身份的方式，显然，如果管理员修改和使用较弱的身份验证方法则可能会出现严重的安全漏洞。因此，必须监控和警惕这种状况的出现。

InfoSphere Guardium数据库服务器配置审核系统(CAS)可跟踪数据库各级别的变更，并将这些变更报告至基于Web的中央控制台。有了CAS，安全管理员可以绕过数据库SQL引擎，了解是否有影响安全性的变更发生。

结合InfoSphere Guardium的数据库活动监控功能，此系统便可提供业界唯一的全面的数据库监控、审计和控制解决方案。

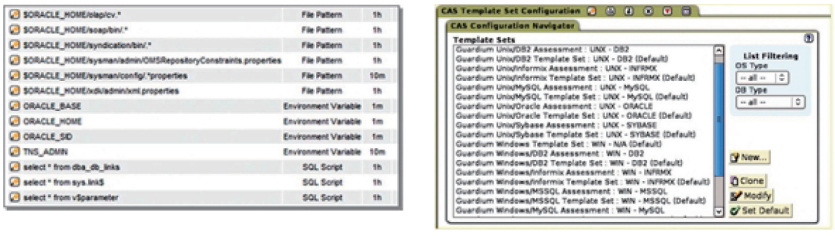


图17: InfoSphere Guardium的数据库服务器配置审核系统(CAS)模块，可跟踪可能影响数据库安全的所有外部数据库对象变更—如配置文件、环境、注册表变量、脚本及可执行文件。为了加速部署，CAS整合了最佳实践资料库，其中包含数百套针对所有主要操作系统和DBMS组合的预配置知识模板。

CAS具有哪些功能

CAS是轻量级代理，可在安装有数据库实例的服务器上运行。CAS可监控对各种结构做出的所有变更，包括文件变更、文件所有权、权限定义、注册表值、环境变量及数据库结构。

然后它将会根据用户定义的一系列时段轮询这些结构，如有任何变更，将会通知InfoSphere Guardium服务器究竟哪项元素发生变更，新值(与旧值相比较)如何等等。

CAS从定义监控内容的模板开展工作。InfoSphere Guardium系统包含一系列预定义模板，定义了各种最佳实践，可供在Oracle、DB2、Sybase、SQLServer、Informix、MySQL、Netezza、Teradata或PostgreSQL环境下进行监控(见图17)。用户通过选择模板和主机将这些模板部署到服务器，由CAS完成，其余的操作。

部署完成后，CAS可将此模板扩展至实际的实例元素。例如，安全性的最佳实践通常会要求您确保不会对数据库可执行文件做出任何变更。一套数据库安装装置拥有数十份可执行文件，攻击者可利用其中的任何

一份文件攻击环境。例如，攻击者可以用某个版本替换其中一份可执行文件，该版本除执行日常工作外，还会将用户名和密码存储在文件中，供攻击者进行读取。确保此类文件没有发生变更是任何审核(外部或内部)的组成部分。

CAS还可以跟踪其他值。例如，SQL Server允许使用SSL对数据库通信进行加密。此值可在各种SQL Server工具内进行设置。在一天结束时，会将此值存储在标准Windows注册表(见图18)中。Windows管理员可通过简单的修改，轻松地关闭数据传输数据加密功能，智慧至极。CAS模板可监控这些值，用来进一步确保数据库安全的稳定性。

除文件和注册表值的变更外，CAS能够监控的其他变更有:

- 环境变量变更
- 文件权限变更。CAS还能够验证文件权限设置是否在限定范围内
- 文件所有权变更。CAS还能够验证是否仅将文件所有权设置为某些确定的值
- 能够查询的任何数据库元素变更
- 能够查询的任何操作系统值变更

CAS提供可由安全管理员控制的其他参数。例如，虽然每个模板元素均具有默认轮询间隔，但管理员仍能够设置不同的轮询间隔(见图19)。管理员可以指定CAS确定变更是否发生的方式。一种方式是使用时间戳，另一种方式是使用MD5校验和值。后者更趋向于资源密集型计算，但更加强劲稳固。

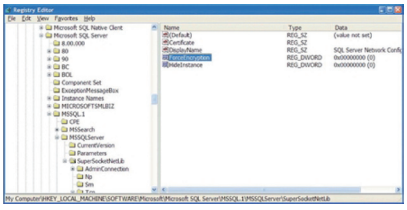


图18: CAS可简化跟踪关键注册表值的流程，如SQL Server的“强制协议加密”注册表值。

图19: CAS可让您定义跟踪变更轮询周期；启用MD5 (还是时间戳)跟踪变更；以及CAS是否还要“让数据”跟踪“从前的”值。

此外，每种元素还可指定CAS是仅仅报告变更的值，还是要将之前和之后的值一起返回。如果是后者，将提供报告，显示旧值与新值之间的差异(见图20)。

CAS安装和操作

CAS可作为S-TAP安装的一部分安装，也可以单独安装。

CAS作为Java程序运行，因此需要在主机上安装Java 1.4或更高级的配置。Java是一项必备条件，CAS安装程序要求提供Java安装位置。右表概括了CAS的存储需求。

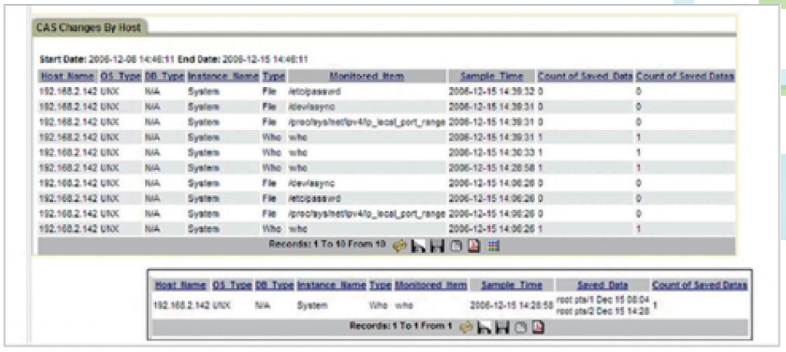


图20：如果需要的话，CAS可选择保留之前的值和之后的值(见上方“Saved Data”)

定制CAS

除预建模板和跟踪元素外，CAS还可让安全管理员构建仍旧需要进行跟踪的新目标。这意味着不仅可以定义待监视的新文件或元素，您还可以定义新数据库脚本和新操作系统脚本由CAS进行管理，也可以用它们来补充CAS提供的广泛的内置功能。

操作系统	需要的磁盘空间
AIX	350MB
HP-UX	650MB
Linux	450MB
Solaris	400MB
Tru64	350MB
Windows	300MB

利用自动签发与报送功能记录合规性

审计员想要了解有待及时跟踪和解决的事件。利用InfoSphere Guardium事件管理和合规工作流模块(见图21)，您可以实现报告分发、电子签发、评论及报送的自动化，同时跟踪变更事件的补救进程。

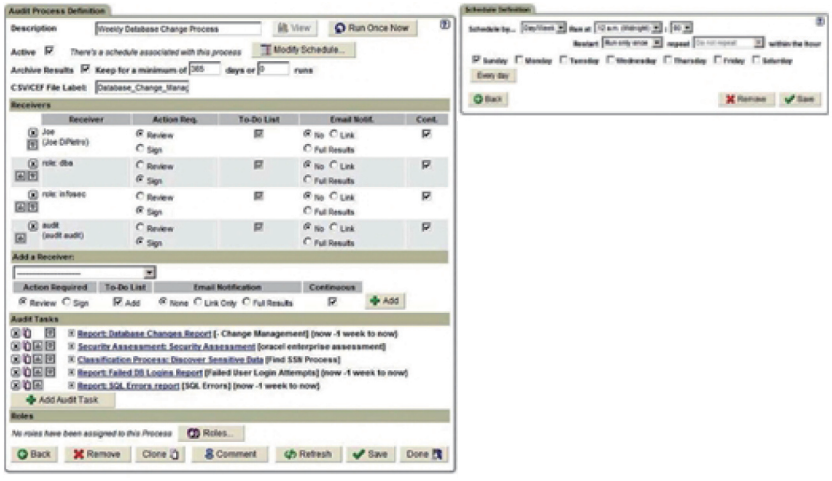


图21：审计员寻找证据证明组织具备定义完善的流程，以保护他们的关键数据不受威胁。InfoSphere Guardium的工作流自动化模块，可让您定制审计任务，自动执行预定的变更审计报告、报告分发、签发及报送。

应用程序最终用户识别器

通过监控应用程序用户活动实时侦测欺诈

- 保护主要企业应用程序免受欺诈、外部或内部攻击、权限滥用及数据泄漏的威胁
- 报告应用程序用户执行了那些非法操作，尽管应用程序采用通用服务账户访问数据库
- 采用确定性方法积极识别应用程序用户，而不是像其他系统一样依靠近似法，如统计抽样和流量匹配，这些方法不能用于审计及法庭之目的
- 满足审计员的要求，监控任何来源的敏感信息访问
- 降低运营成本，并根据内部与外部审计要求简化法规，包括SOX、PCI DSS、ISO 27001、NIST 800-53及SAS70

企业应用程序环境的安全性与合规性

许多组织依靠企业应用程序执行核心业务流程，管理大量关键任务和高度敏感数据。财务数据、人事数据及客户数据均是SAP、PeopleSoft及Oracle EBS等应用程序内部管理的资产示例。因此，许多合规性要求和审计涉及到由企业应用程序管理的数据，因而需要IT安全组织确保这些数据的安全性。

InfoSphere Guardium应用程序最终用户识别器提供了一个预封装的解决方案，满足主要企业应用程序管理的数据的安全性及合规性需求——而无需变更现有的业务流程或应用的源代码。

应用程序层监控的主要目的在于，侦测通过企业应用程序产生的欺诈。这种级别的监控往往需要遵循SOX、ISO 270001、SAS 70及NIST 800-53控制等数据治理要求。

保护多层企业应用程序

多层企业应用程序往往最难以进行保护，因为它们高度分散，并且允许内部人员和外部人员(如客户、供应商及合作伙伴)通过网络进行访问。此外，多层企业应用程序通常采用一种称作“连接池”的优化机制，在数据库事务处理级别掩饰了最终用户的身份。

连接池用一个通用的服务账户名称标识所有事务，因此难以将具体的数据库事务与特定的应用程序最终用户相关联。如果您依赖于仅能根据用户数据库登录账户监控和识别用户的传统数据库记录工具，这一点就更加明显了。

由于企业应用程序数据驻留在关系数据库中，因此也可以通过直接数据库连接(例如，通过SQL *Plus等开

发工具)或通过应用程序本身进行访问。IBM可提供独一无二的全面解决方案，解决这两种访问路径上的问题。它能够主动识别与特定数据库事务相关的应用程序用户(见图22、26和27)，识别特权用户非法访问对象。例如，在图24中，通过SQL *Plus尝试选择数据这一操作，已经违反了用户仅可通过Oracle应用程序访问EBS数据的策略。这种违规会自动触发指定的操作。本例中指定的操作是：终止SQL *Plus会话，记录违规细节和生成警报。

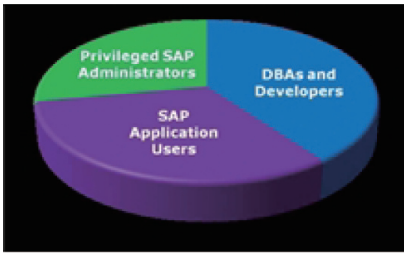


图22: InfoSphere Guardium应用程序最终用户识别器可授权IT安全机构，快速识别欺诈及其他违反企业策略的操作，如非法变更具有池连接的企业应用程序环境敏感数据(注意，所有事务的数据库用户名均是APPS)。Oracle EBS环境也可用于监视在EBS中定义用户时指派给用户的职责。在上图中，Bob的AX General Ledger Supervisor (AX总帐主管)角色，是组织策略中活动监控的一部分，目的是简化报告审核工作。我们还可以看到，John还担任两个角色；一个角色是AX Receivables User (AX应收账款用户)，另一个是System Administrator (系统管理员)，负责识别潜在的不合理授权。

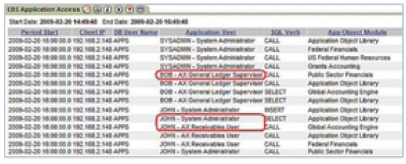


图23: InfoSphere Guardium可保护企业应用程序环境，使其免受所有主要风险源的威胁。

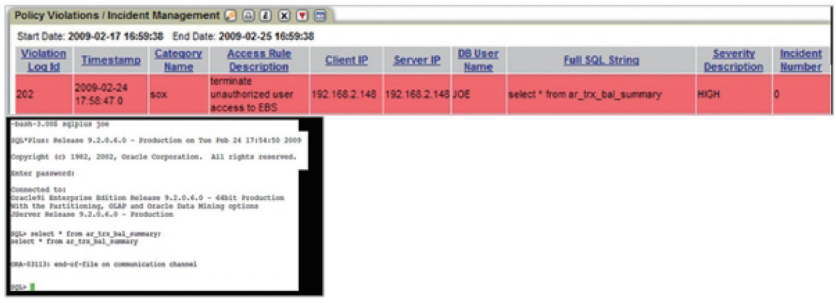


图24: 策略违规(如利用SQL *Plus等工具绕过EBS直接访问数据)可被侦测并被有选择的阻断(左图)。支持记录详细信息，并通过工作流自动化自动派遣人员进行调查(上图)。

可扩展的企业安全平台

应用程序最终用户识别器模块，在业界领先的InfoSphere Guardium数据库活动监控(DAM)和漏洞评估(VA)技术基础上构建，通过特定于应用程序的策略、审计报告及跟踪组，为主流企业平台强化这些核心模块的功能。

DAM技术可实时监控所有数据库访问活动，而不依赖本机数据库日志，不会影响性能也无需进行数据库变更。InfoSphere Guardium业界独特的多层体系结构可自动将多个DBMS系统和位置的审计信息聚合至一个中央存储库，并可实现审计信息标准化，从而支持企业级合规报告，实现相关、合法、先进的数据库分析。

图形化的Web控制台可集中管理策略、报告定义、合规工作流及设备设置(如归档时间表)。这种可扩展的多层架构能够轻松地进行扩展，通过添加在联邦模式下协同工作的各种设备，来满足任何吞吐量和审计策略组合的需求。

InfoSphere Guardium的漏洞评估模块还提供了自动化测试的最佳实践库，可以识别丢失的补丁、权限配置错误、默认账户问题及弱密码等漏洞。该模块配有知识库服务支持，可定期更新SAP和Oracle EBS漏洞测试、敏感对象以及预配置组。通过不断更新对象列表及组，IBM简化了对于重要表单的访问和更改的监控。

基于策略的全面监控和审计

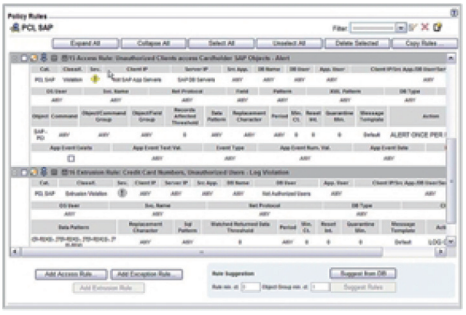


图25: InfoSphere Guardium提供了针对SAP和Oracle EBS应用程序的粒度预配置策略，快速识别可疑活动或非法活动，如敏感对象变更或多次登录失败等。对于需要复杂的研究才能确定的敏感对象，可通过知识库服务进行识别，以促进自定义策略开发。实时SNMP警报等一系列操作，均可配置为当策略被违反时触发。

InfoSphere Guardium可提供:

- 专为SOX和PCI环境(这些环境内通常包含企业应用程序)开发的内置预配置报告
- 针对Oracle EBS和SAP的内置SOX及PCI DSS策略(见图25)
- 对存储应用程序数据的底层数据库引擎的全面评估
- 全面的活动和数据审计，显示所执行的直接和间接活动及数据访问
- 用户执行活动的审计线索，在应用程序级别显示用户使用用户ID访问数据库的情况(见图22、26和27)。审计记录会显示执行访问的用户ID及客户端主机

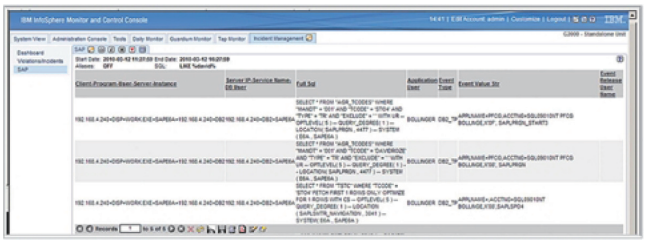
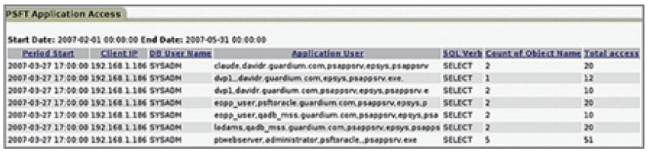


图26: InfoSphere Guardium应用程序最终用户识别器能够监控SAP与DB2和Oracle等丰富的数据库环境之间的所有事务。


PSFT Application Access

Start Date: 2007-02-01 00:00:00 End Date: 2007-05-31 00:00:00

Period Start	Client IP	DB User Name	Application User	SQL Verb	Count of Object Name	Total access
2007-03-27 17:00:00	192.168.1.186	SYSADM	claude.davidr.guardium.com,psappsrv,epsys,psappsrv	SELECT	2	20
2007-03-27 17:00:00	192.168.1.186	SYSADM	dup1..davidr.guardium.com,epsys,psappsrv,exe.	SELECT	1	12
2007-03-27 17:00:00	192.168.1.186	SYSADM	dup1.davidr.guardium.com,psappsrv,epsys,psappsrv.e	SELECT	2	10
2007-03-27 17:00:00	192.168.1.186	SYSADM	eopp_user,psftoracle.guardium.com,psappsrv,epsys,p	SELECT	2	20
2007-03-27 17:00:00	192.168.1.186	SYSADM	eopp_user,qadb_mss.guardium.com,psappsrv,epsys,psa	SELECT	2	10
2007-03-27 17:00:00	192.168.1.186	SYSADM	ladams,qadb_mss.guardium.com,psappsrv,epsys,psappa	SELECT	2	20
2007-03-27 17:00:00	192.168.1.186	SYSADM	ptwebserver.administrator,psftoracle..psappsrv.exe	SELECT	5	51

图27: 最终用户标识符模块可识别与PeopleSoft池连接环境中的特定事务相关的用户(应用程序用户), 在这些环境中, 依赖本机数据库审核信息的传统工具, 将仅显示通用标识符(SYSADM)。

广泛的异构应用程序支持

InfoSphere Guardium可支持针对所有主要应用程序和应用程序服务器的应用程序层监控, 而无需进行应用程序变更。这些应用程序包括:

- Oracle E-Business Suite
- SAP ERP和NetWeaver BW
- PeopleSoft
- Cognos
- Siebel
- Business Objects Web Intelligence

InfoSphere Guardium还可识别在下列标准应用程序服务器平台上构建的自定义及打包应用程序的应用程序用户ID:

- IBM WebSphere
- BEA WebLogic
- Oracle应用程序服务器
- JBoss企业应用程序平台

Enterprise Integrator

提高运营和安全效益的数据集成

- 轻松地连接至多个关系型数据库或文本文件，检索数据并将其集成至InfoSphere Guardium知识库，以实现审计完整性
- 创建统一的审计报告，包括加强安全性及提高运营效率的外部信息
- 导入描述性信息，如与用户名相关联的全名及电话号码，以简化异常的调查
- 集成角色及部门等信息，实现更加细化的安全策略部署
- 通过从IBM iSeries和Progress数据库等环境整合日记信息，为所有数据库安全与合规数据创建单一管理平台
- 充分利用现有的Tivoli和Centera基础架构，简化InfoSphere Guardium审计数据及任务结果的自动归档过程

管理复杂、快速变化的环境

数据库安全与合规管理变得越来越具有挑战性。不仅网络攻击持续增加，而且需要管理的环境也日趋复杂。

在瞬息万变的商业背景下(包括兼并、外包、劳动力调整及不断加速的业务自动化进程)的推动下，及时获取所需的信息，从而有效制定、管理并报告安全策略也日趋困难。数据库跨越了地理和组织的边界不断建立，管理及授权信息分散于各个系统，人事和系统数据不断变化，同时审计信息期望也稳步增加。

传统上，企业一直依赖手动流程收集所需的信息，确保数据库安全性策略和报告包含准确和有意义的数据。鉴于当前的环境资源有限、管理的环境日趋复杂及工作量不断增加，目前各组织正寻求途径，提高数据库安全与合规运营的自动化程度。

自动执行安全性数据的采集、集成和归档

InfoSphere Guardium的Enterprise Integrator是一个可选的软件模块，可简化并自动将外部数据库或文本文件中的数据集成至InfoSphere Guardium知识库，以及确保充分利用现有的企业存储基础架构进行归档。其强大性能支持多种功能，从自动化的变更控制调和(reconciliation)之类的新型应用程序，到消除昂贵的手动操作的流程和策略改进功能。

集成外部信息需要几个简单的步骤(见图28)。首先创建自定义表存储数据。表定义可通过为InfoSphere Guardium提供从源数据库检索元数据所需的信息来创建，也可使用更加具体的图形化用户界面手动输入

表定义。然后上载目标数据，利用InfoSphere Guardium BMC的Remedy和HP的Peregrine等供的工具检查模式兼容性，并在上载后执行任何所需的DML。上载可以是一次性事件，也可以定期执行，从而无需手动干预即可使库与不断变化的主要数据源保持同步。

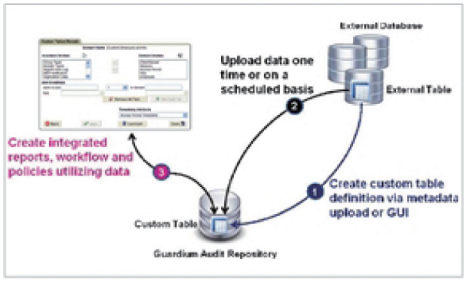


图28: Enterprise Integrator可提供一种简单的途径，集成外部来源的重要安全信息。自动或手动提供各种工具：1)为InfoSphere Guardium审计库中导入的数据创建自定义表定义；2)上载外部来源数据；3)创建数据链接，以便所有InfoSphere Guardium工具都能够无缝地使用导入的数据。

在将数据存储于库中后，便可以使用各种InfoSphere Guardium的策略、分析、报告及工作流工具了。例如，可以从独特环境(如IBM iSeries)导入日记信息，从而使自动化的报告、工作流及签发工具能够应用于数据之上，确保策略的一致性，提高运营效率。上载的数据也可能链接至库中现有的数据。这样便可将重要的描述性信息添加至报告和策略(见图29)，进而消除手工查找，提供关键数据，以便识别特定的策略违规行为。

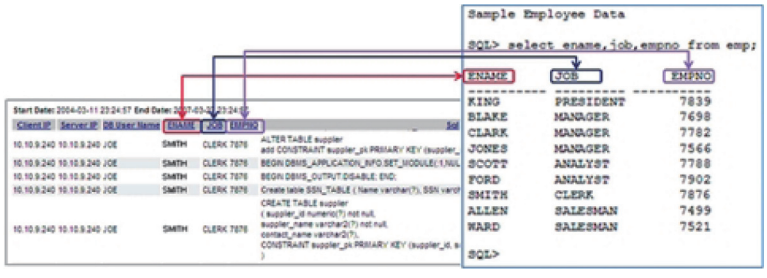


图29: Enterprise Integator使用户能够创建包含外部信息的统一审计报告，因此可增强安全性并提高运营效率。例如，可以轻松地集成存储在远程员工数据库中的真实工作人员姓名(ENAME)和编号(EMPNO)，从而不必手动研究与特定数据库用户名对应的员工，即可对异常报告进行调查。导入员工的工作类别(JOB)便可识别潜在的不合法活动，如职员(CLERK)修改数据库表的行为。

自动化的协同变更控制

绝大多数组织具有正式的变更控制策略及流程，用以监管做出生产数据库变更的方式及时间。但提的系统，因而在大多数情况下无法侦测非法变更。如果没有执行机制，变更控制策略将无法发挥效用。然而，通常可以利用的唯一选择(利用本机审计日志手工进行)极其耗费人力。

通过将企业集成与核心InfoSphere Guardium系统共同使用，便不必耗费大量人力，即可轻松地执行变更控制策略。企业集成可从将要检索并整合至InfoSphere Guardium系统的变更管理系统，启用经过批准的变是，由于变更管理应用程序和生产数据库是不同更请求。在商业系统中，请求均包含业务级摘要描述。通过票证ID将变更描述链接至InfoSphere Guardium观察到的实际变更，实现调节流程自动化(见图30)。审查员能够轻松地将摘要描述与执行的SQL命令进行比较，以确保做出适当的变更。工作流程自动化可确保所有变更都经过了审核和审批，问题被标记出来以便进行后续的补救。如果在不具备有效票证ID、超出授权的变更期限，或利用非法用户ID的情况下做出变更，则会自动侦测。各种响应活动都可能发生，从发出实时警报到阻止操作。

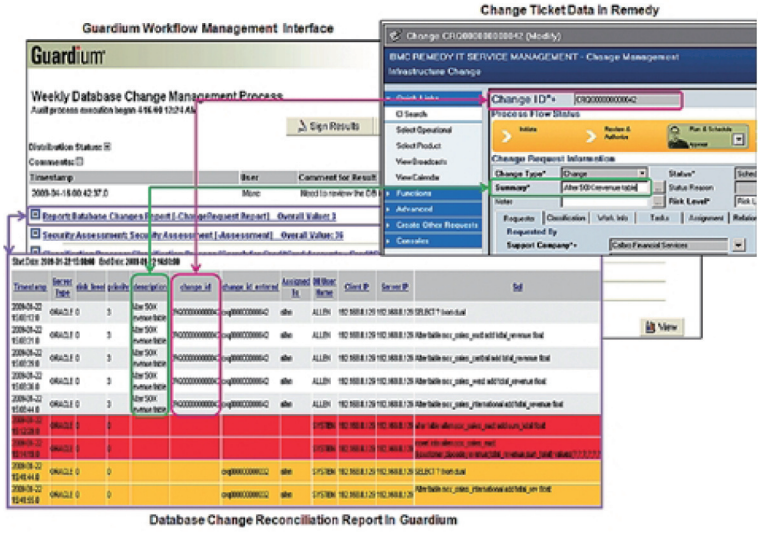


图30: Enterprise Integrator技术可用来从BMC的Remedy或HP的Peregrine等自定义或商用系统导入变更管理信息。在本例中，Change ID和Summary描述均包含在每周数据库变更报告内，这种报告采用InfoSphere Guardium的工作流功能进行分发和管理。此报告已被结构化，以便所有非法变更均以红色突出显示。以黄色显示的变更表示输入了无效的变更号码。系统显示了授权变更的补救概要(Remedy Summary)和实际执行的SQL命令，使报告接收人能够验证变更是否符合授权。

自动化的变更控制调和功能，可保护重要数据，展示前摄性控制，满足敏锐的审计员的要求。

通过自动更新策略信息消除安全漏洞

尽管InfoSphere Guardium最初可能用于保护极为重要的资产，但随着时间的推移，应用范围通常会扩展，最后包括了企业的所有敏感数据库。随着系统扩展，组的使用变得非常重要。一个组就是共享相同属性的一系列元素。分组简化了策略与报告的开发和维护流程。例如，组织可能拥有30个独立的对象，它们都包含敏感的财务数据。无需分别为这些对象创建策略和报告，SOX组的定义就包含了所有的成员。因此，旨在监控和报告SOX对象访问的策略和报告将变得更加简单。

Enterprise Integrator 支持	
数据源	Oracle、DB2、Sybase、Microsoft SQL Server、Informix、mySQL、Teradata、Netezza及PostgreSQL数据源的开箱即用支持
连接	连接至CSV文本文件数据源的HTTP、HTTPS、FTP、SAMBA及IBM iSeries的开箱即用支持

组的功能可用于简化多种其他对象的管理，例如多种服务器(如含有SOX、PCI、PII数据的服务器)及用户(如特权用户、授权访问SOX对象的用户，或负责审查服务器组异常的业务合作伙伴)。通常组中包含的数据均来源于网络数据库，并在网络数据库中进行维护。通过采用Enterprise Integrator技术检索此类数据及填充组，可减少劳动并消除错误。更重要的是，随着对象变更(源于职责、基础架构变更)，可通过安排Enterprise Integrator定期上载内容，自动更新组的成员，而不必对InfoSphere Guardium组或策略做出任何变更。这同样也能够减少工作量，并避免由于组的成员数据过时而引入安全漏洞。

自动归档以降低合规成本

在绝大多数组织中，合规性法规和内部策略需要以报告和法庭使用为目的归档所有InfoSphere Guardium数据，包括审计数据和审计任务结果。为了支持这一需求，解决方案须具备自动归档和恢复功能。

Enterprise Integrator包含Tivoli Storage Manager和EMC Centera开箱即用的连接器，能够轻松地将这些主要企业归档解决方案与InfoSphere Guardium归档功能配合使用。用户只需输入池连接字符串及密码等配置信息，即可启用InfoSphere Guardium连接这些系统。利用Enterprise Integrator，用户便能够利用现有的企业归档解决方案，而无需开发自定义的集成工具。

IBM InfoSphere Guardium for z/OS

采用成熟的z/OS技术实现审计可视化

- 通过特权用户、大型机驻留应用程序及网络客户端，监控并审计z/OS上的所有数据库活动
- 在精细级别查看关键操作，包括SELECT、DDL、DML、访问授权与撤销
- 所有审计数据分析、报告及存储均在安全环境下脱离大型机执行
- 与企业级Guardium架构集成，为大型机和分布式数据库环境提供统一的安全与合规解决方案
- 采用可靠的IBM z/OS技术，最大限度地提高可靠性和效率

不断增长的DB2安全与合规需求

许多组织在大型机数据库上托管大量敏感和关键任务数据。财务、人事及客户记录均可在这些环境中找到。

因此，大型机数据自始自终都是合规性法规约束的对象。明智的组织会实施新型控制措施，确保其DB2数据不会遭到非法访问以及内部和外部操作的影响，并且审计员能够轻松获取验证控制措施有效性的详细审计线索。

IBM的InfoSphere Guardium解决方案可提供简单而强大的途径，来保护整个企业的关键性数据。它可以依据策略快速侦测违反企业策略的异常活动，通过警报、可审计的工作流进行实时响应，确保适当地解决异常情况，连同自动报告功能一起，简化SOX、PCI DSS及数据隐私等法规的合规性验证过程。

InfoSphere Guardium for z/OS可针对z/OS上的DB2提供这些功能。该解决方案可针对大型机环境单独使用，也可以与企业的其他Guardium数据库安全和监控组件集成(见图31)，提供集中的安全审计库和管理平台。

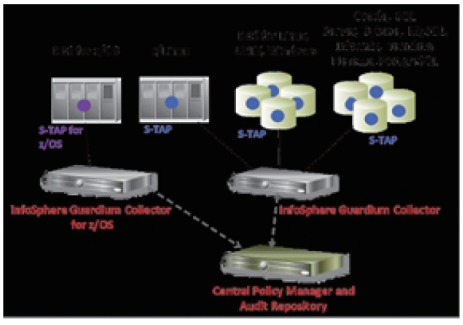


图31: Guardium 采用名为 S-TAP for z/OS 的轻量级软件监视程序，捕捉特权用户、大型机驻留应用程序及 z/OS 网络客户端执行的关键数据库活动。大型机和分布式环境均可从单一控制台进行监控；此外，所有审计数据均会自动聚合并归到一个中央存储库，供企业合规性报告、分析及法庭使用。

避免传统解决方案中的安全和成本问题

历史上，致力于监控和保护z/OS上的DB2敏感数据的组织，都采用了基于跟踪或事务日志等记录工具开发的解决方案。这些解决方案，以及在这些解决方案的基础上构建的其他解决方案，均受到各种限制的影响，例如:

- 依赖大型机数据库管理员(DBA) 进行管理，无法实现审计员要求的职责分离(SOD)
- 无法捕捉审计员要求的所有关键活动(如使用记录功能时的读取操作，或使用跟踪功能时的SQL语句)
- 缺乏精细的分析和警报功能，从而消除了立即侦测重要类别的非法活动(如非法更新授权用户访问的数据)的可能性
- 需要大量技能纯熟的员工维护自定义软件，或分析报告以侦测策略违规

InfoSphere Guardium for z/OS可消除这些局限性，同时提供重要的新功能，如合规工作流自动化、报告，及在企业范围内查看数据库安全性和合规性状态。

可扩展的企业级数据库安全与合规平台

InfoSphere Guardium for z/OS采用名为S-TAP for z/OS的轻量级软件监视程序，捕捉特权用户、大型机驻留应用程序及z/OS网络客户端执行的关键数据库活动，包括通过JDBC或DB2 Connect等服务执行的连接。可靠的IBM DB2/z事件捕捉技术，确保捕捉SELECT、DML、DDL及访问授权等关键性操作，而不必使用DB2第四类和第五类审计跟踪。

S-TAP for z/OS会根据用户定义的审计策略(见图32)将指定的信息发送至InfoSphere Guardium Collector for z/OS设备。这样可确保大型机不必受制于增量存储或处理要求、网络流量限制，费力地满足安全存储完整审计线索的需求。S-TAP事件捕捉技术还能够通过IBM Query Monitor共享，从而为使用两种产品的客户提供进一步的性能提升。

InfoSphere Guardium在业界独一无二，其多层体系结构(见图 31)可跨越数据库平台、应用程序和位置，聚合审计信息并将其归到单一的中央存储库。这样便可提供全面的企业合规性报告以及相关的、合法的数据库分析。一开始便在大型机上实现的用户，只需添加适当的S-TAP、收集器和聚合器，使它们在联邦模式下协同工作，便能够轻松地进行扩展，支持任何数据库和系统的组合。

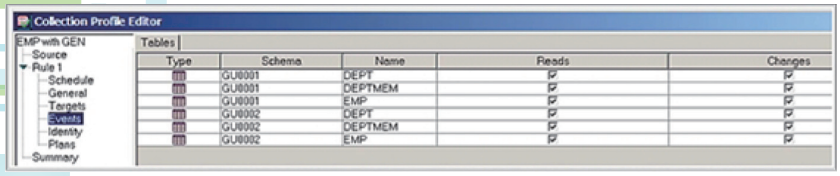


图32: 用户可以轻松地使用基于Windows的审计策略编辑器构建审计策略，定义需要捕捉的DB2事务。

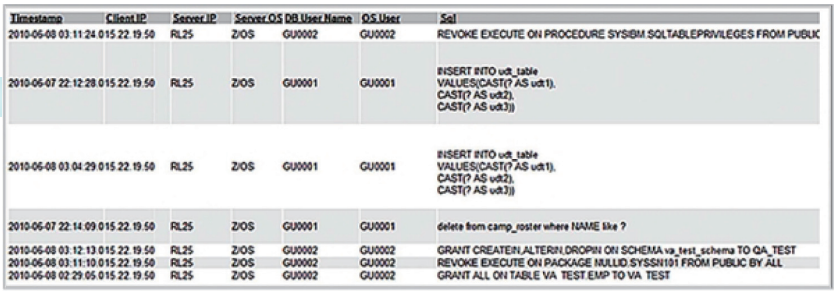


图33: Guardium可全面可视化在z/OS上使用的DB2数据，捕捉大型机和网络访问，并可获取操作系统用户名、客户端IP、数据库用户名及执行的SQL语句等主要细节。

基于策略的监控和审计简化了合规性验证

InfoSphere Guardium Web控制台无需数据管理员参与，即可集中管理警报、报告定义、合规工作流及设置(如归档时间表)，从而提供审计员要求的职责分离，简化合规性活动，并可跨越整个数据库基础架构执行各种管理操作，包括:

- 使用针对您的特定环境的风险指示器定义具体的访问策略，包括数据对象、SQL命令类型、用户ID、客户端IP地址、操作系统用户名、源应用程序或每日时间
- 自动创建正常业务活动的基线，提出侦测SQL注入攻击等异常活动的策略
- 定义响应策略违规的操作，如生成警报及记录完整的事件细节
- 自动执行日常活动的合规工作流及事件响应，包括签发、注释及升级等步骤
- 运行数以百计的开箱即用的报告，包括SOX、PCI DSS及数据隐私法规所需的报告，创建自定义报告

利用InfoSphere Guardium，用户可以完全可视化DB2环境，实时识别并应对数据篡改或数据攻击等非法活动。实现整个安全与合规周期的自动化，降低劳动力成本，促进整个组织的交流，简化审计的准备工作。

IBM环境的全面支持

InfoSphere Guardium解决方案还支持其他各种流行的IBM平台，包括:

- IBM DB2 for Linux、UNIX及Windows
- IBM Informix
- IBM DB2 for iSeries
- System z Red Hat Enterprise Linux及SUSE

- Linux Enterprise Server for System z，支持在IBMz/虚拟机管理程序中运行的所有主要DBMS平台(Oracle、MySQL等)
- Cognos 8，其中InfoSphere Guardium可通过应用程序层监控识别欺诈及其他非法活动。Guardium还支持其他企业应用程序，如针对IBM WebSphere应用程序服务器及其他中间件平台开发的SAP、PeopleSoft和SOA应用程序

IBM InfoSphere Guardium for z/OS	
支持DB2版本	DB2 for z/OS V7或V8或V9
支持z/OS版本	z/OS V1.6或更高版本