IBM银行业数据安全治理方案

行业特点:

面对数据库的安全问题，银行业常常遇到以下主要挑战: 安全制度存在但得不到有效的技术手段得以实现；企业内部几十种应用系统，各系统数据库又不同，难以统一管理；数据库内嵌的日志审计方式难以满足系统性能要求；其他IT安全方案与数据安全方案的集成和协同；数据安全方案的切入点和而后拓展性；数据安全方案对企业组织机构的影响等。

解决方案概述:

1. 解决方案需求背景:

IBM在其2009年11月25日发布的对上市公司IT需求的研究报告指出:

"以上市(中)企业作为一个群体的长远发展来看，IT需求主要是集中在财务控制、流程控制、信息安全和管理ERP、生产渠道等。国家在法规政策上会继续采取规范化管理的趋势，另外，国家在法规政策上会继续采取规范化管理的趋势。

数据作为企业核心资产，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。全球各大媒体2010年3月11日纷纷报道: 汇丰银行因内部IT员工盗窃客户资料，损失重大。在受到侵害的2.4万客户中，已有9千名白金资格以上的客户离开了汇丰银行。

发生如此严重事件的原因是其对信息安全的举措尚未得到全面落实，但非个例。全球独立的ORACLE用户组织(IOUG)在2010年对其430个成员的数据安全调查报告发现:

- 3/4的成员不清楚特权用户对数据库进行过何种操作
- 2/3的成员不能有效防止特权用户对数据库的非授权访问
- 85%的成员将真实数据不加防范地交与开发、测试人员或第三方组织
- 将近一半的成员对其非特权用户访问敏感数据毫无措施
- 大多数成员都未能及时采取防范SQL注入的攻击

面对以上数据安全现状，银行业为提升自身数据安全防范意识、管理手段与技术手段，常常遇到以下主要挑战:

- 安全制度存在但得不到有效的技术手段得以实现
- 企业内部几十种应用系统，各系统数据库又不同，难以统一管理
- 数据库内嵌的日志审计方式难以满足系统性能要求
- 其他IT安全方案与数据安全方案的集成和协同
- 数据安全方案的切入点和而后拓展性
- 数据安全方案对企业组织机构的影响等

2. IBM Guardium数据库审计监控解决方案:

IBM Guardium是解决生产环境中数据库安全与合规/审计需求的全面方案，已经得到广大业内分析师的认同，并赢得了众多大型企业

IBM银行业数据安全治理方案

客户。IBM Guardium在2011年被FORRESTER评价为“绝对领导地位”的数据库安全、合规、审计、监控解决方案，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，其主要作用如下:

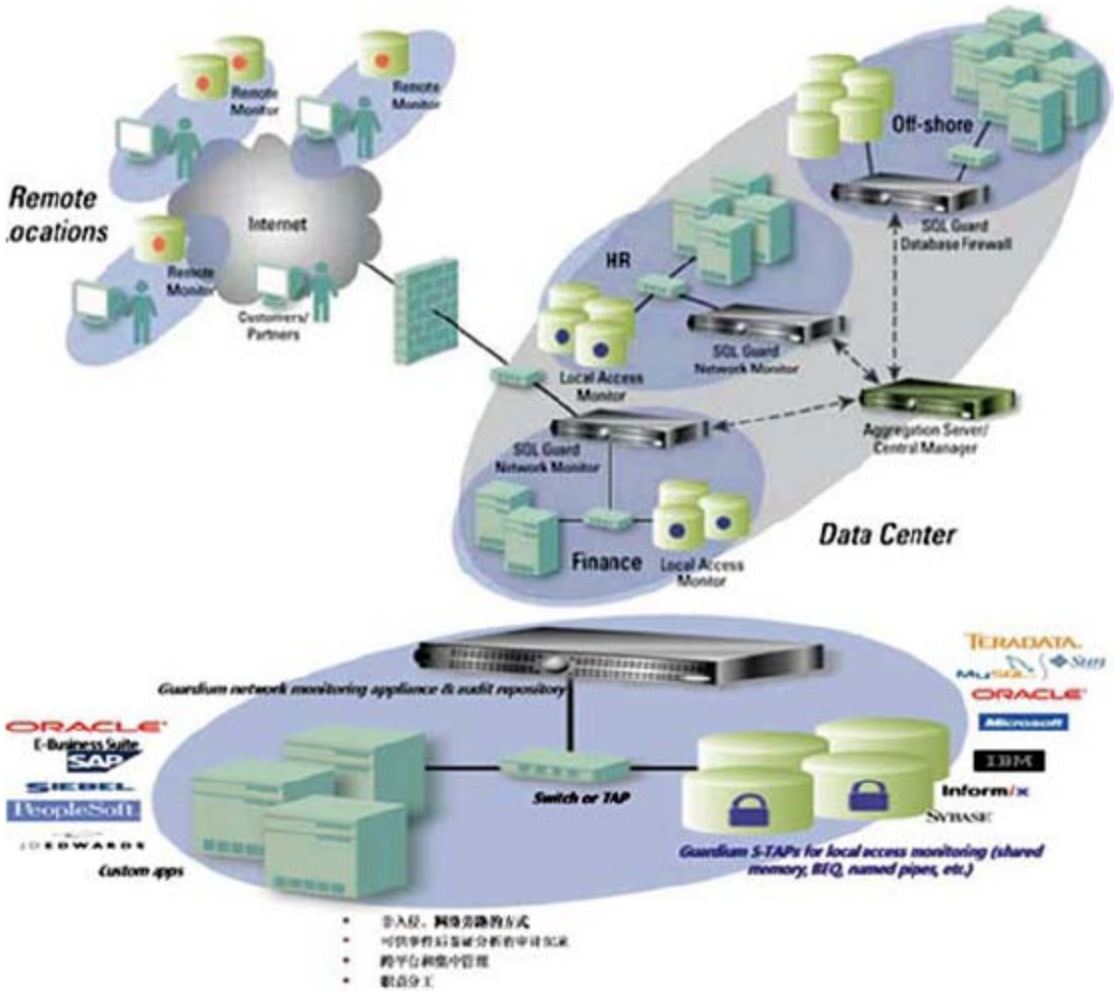
- 防止对数据库的破坏、恶意访问、偷窃数据，可帮助判断客户关键敏感的数据在什么地方；谁在使用这些数据；
- 控制对数据库中数据的访问，并可监控特权用户；
- 帮助企业强制执行安全规范；
- 检查薄弱环节、漏洞，防止对数据库配置的改动；
- 满足合规/审计的要求，并可简化内部和外部审计、合规的过程并使其自动化，增强运作效率；
- 降低数据安全管理的复杂性。

IBM Guardium从四个方面满足企业数据安全及审计的要求:

解决方案价值主张:

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。

IBM银行业数据安全治理方案



综述: 流量是数据库活动的载体，在流量中捕获相关的数据库操作，并加工整理成正交化可视信息，用以适时保留、实时报警、事件跟踪、及数据库安全隐患分析等。因为是旁路方式捕获数据库操作，所以对系统性能没有影响。

用途: 根据安全治理原则，数据库安全是由检测、解析、监控、和设计等过程共同完成的。无论数据库操作源于哪种渠道，网络或本机，安全方案都要求对正在发生的和因安全漏洞而可能发生的操作进行有效的控制和操作审计。数据库操作包括: 查询敏感数据、改变表定义(DDL)、数据操作(DML)、例外操作(Failed logins,SQL errors,etc.)、授权变更(DCL)。

IBM银行业数据安全治理方案

IBM Guardium解决方案的综合优势:

- 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。
- 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；
- 独特的审计记录跟踪下钻(Drill Down)功能，追查问题可以一步步到最底层；
- 国内已有多家大型商业银行、股份制银行、城市商业银行以及农信社的成功案例。

IBM产品:

- IBM Guardium