IBM

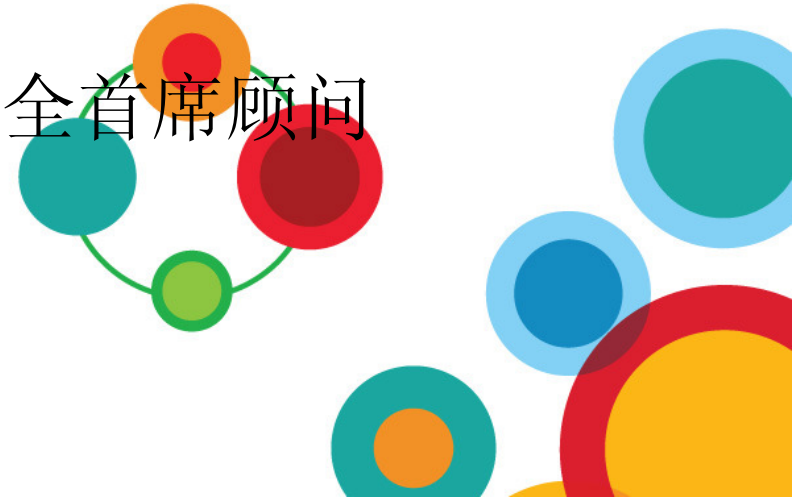
您的信息 您的智慧

2011 IBM 信息管理与业务分析论坛

企业数据安全的终极保镖
-企业级数据库安全审计(Guardium)

邱建, jayqui@cn.ibm.com

IBM软件集团大中华区数据安全首席顾问



信息安全是12.5信息规划三大目标之一

第十三章　全面提高信息化水平(国民经济和社会发展十二五规划纲要 - 2011-3-17新华社)

加快建设宽带、融合、安全、泛在的下一代国家信息基础设施，推动信息化和工业化深度融合，推进经济社会各领域信息化。

第一节　构建下一代信息基础设施

...建立健全法律法规和标准，实现电信网、广电网、互联网三网融合，促 进网络互联互通和业务融合。

第二节　加快经济社会信息化

推动经济社会各领域信息化。积极发展电子商务，完善面向中小企业的电子商务服务，推动面向全社会的信用 服务、网上支付、物流配送等支撑体系建设。大力推进国家电子政务建设，推动重要政务信息系统互联互通、信息共享和业务协同，建设和完善网络行政审批、信息 公开、网上信访、电子监察和审计体系。加强市场监管、社会保障、医疗卫生等重要信息系统建设，完善地理、人口、法人、金融、税收、统计等基础信息资源体 系，强化信息资源的整合，规范采集和发布，加强社会化综合开发利用。

第三节　加强网络与信息安全保障

健全网络与信息安全法律法规，完善信息安全标准体系和认证认可体系，实施信息安全等级保护、风险评 估等制度。加快推进安全可控关键软硬件应用试点示范和推广，加强信息网络监测、管控能力建设，确保基础信息网络和重点信息系统安全。推进信息安全保密基础 设施建设，构建信息安全保密防护体系。加强互联网管理，确保国家网络与信息安全。

12.5信息规划前瞻性地指出了企业面临的日益严峻的信息安全状况

- 继去年公安部破获11.30跨国电信诈骗案后,该案使国内银行客户损失了1.4亿人民币.近日又破获“3·10”特大跨境电信诈骗案,其中单体个案金额最大的达到400万元以上.这些案例值得各行业深思
- 索尼4月26日宣布，PSN网络遭遇黑客攻击，黑客窃取了约7700名用户的姓名、家庭住址、电子邮件、生日、用户名和登录密码等信息，甚至包括用户信用卡的详细信息。索尼CFO加藤优(Masaru Kato)周一称，上述种种成本，以及相关的法律费用，此次攻击事件预计将给索尼带来140亿日元(约合1.7亿美元)的损失。加藤优同时指出：“到目前为止，还没有发现用户个人信息被滥用的事件。” 2011年05月23日 新浪科技
- LulzSec窃取了索尼逾100万个用户的个人信息, 2011年6月3日 新浪科技
- IBM信息安全年度报告披露:2010新增IT漏洞达8,562,意味着IT系统需要更多的保护。SQL注入成为增长幅度最大的攻击方式

According to the X-Force database tracking, 2010 had the largest number of vulnerability disclosures in history—8,562. This is a 27 percent increase over 2009, and this increase has had a significant operational impact for anyone managing large IT infrastructures. More vulnerability disclosures can mean more time patching and remediating vulnerable systems.

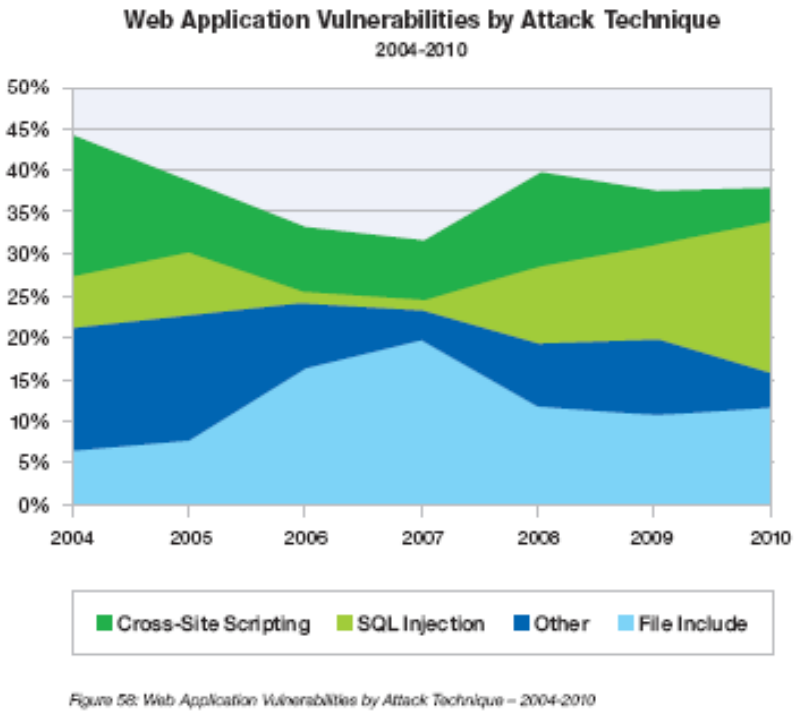
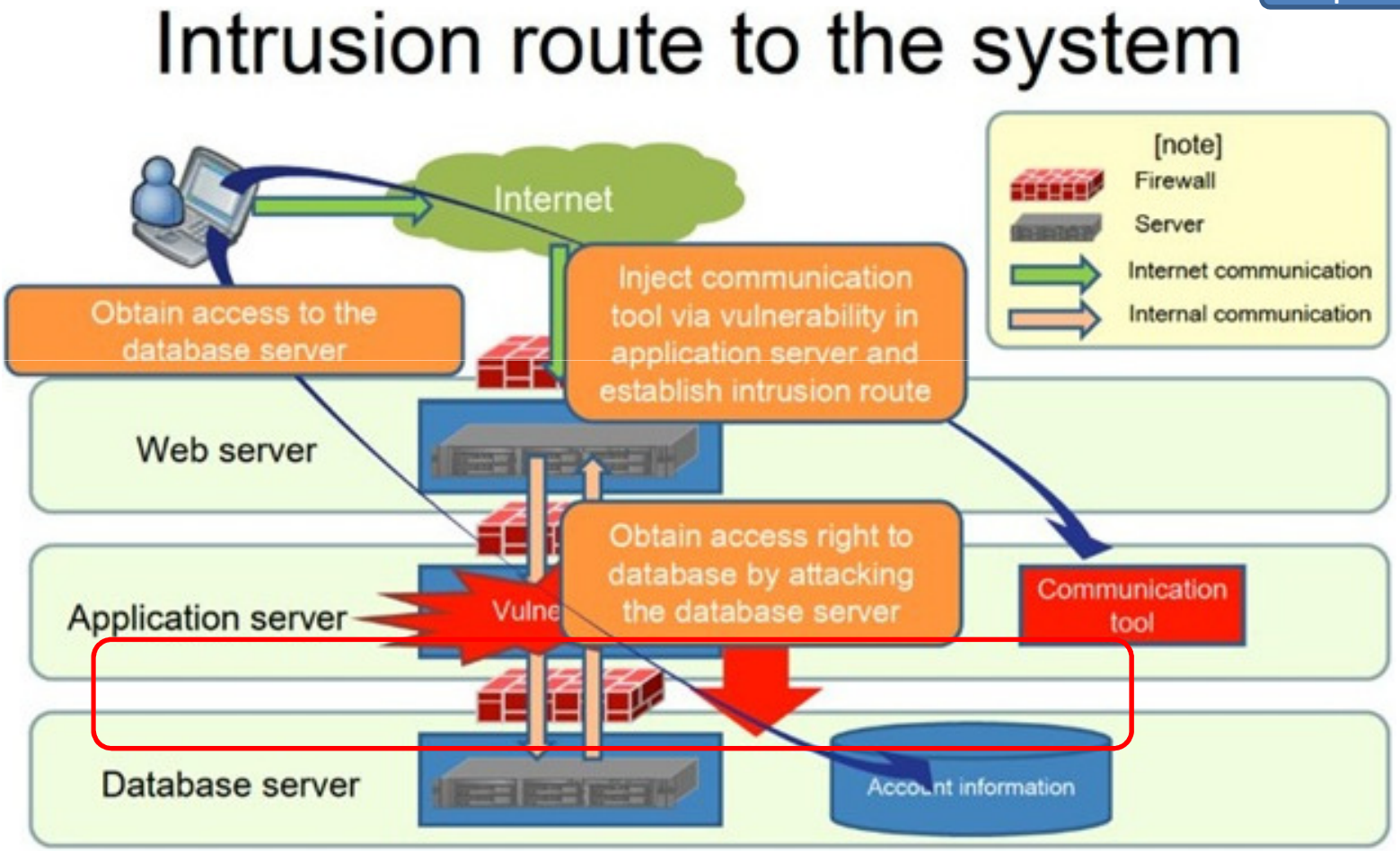


Figure 58: Web Application Vulnerabilities by Attack Technique – 2004-2010

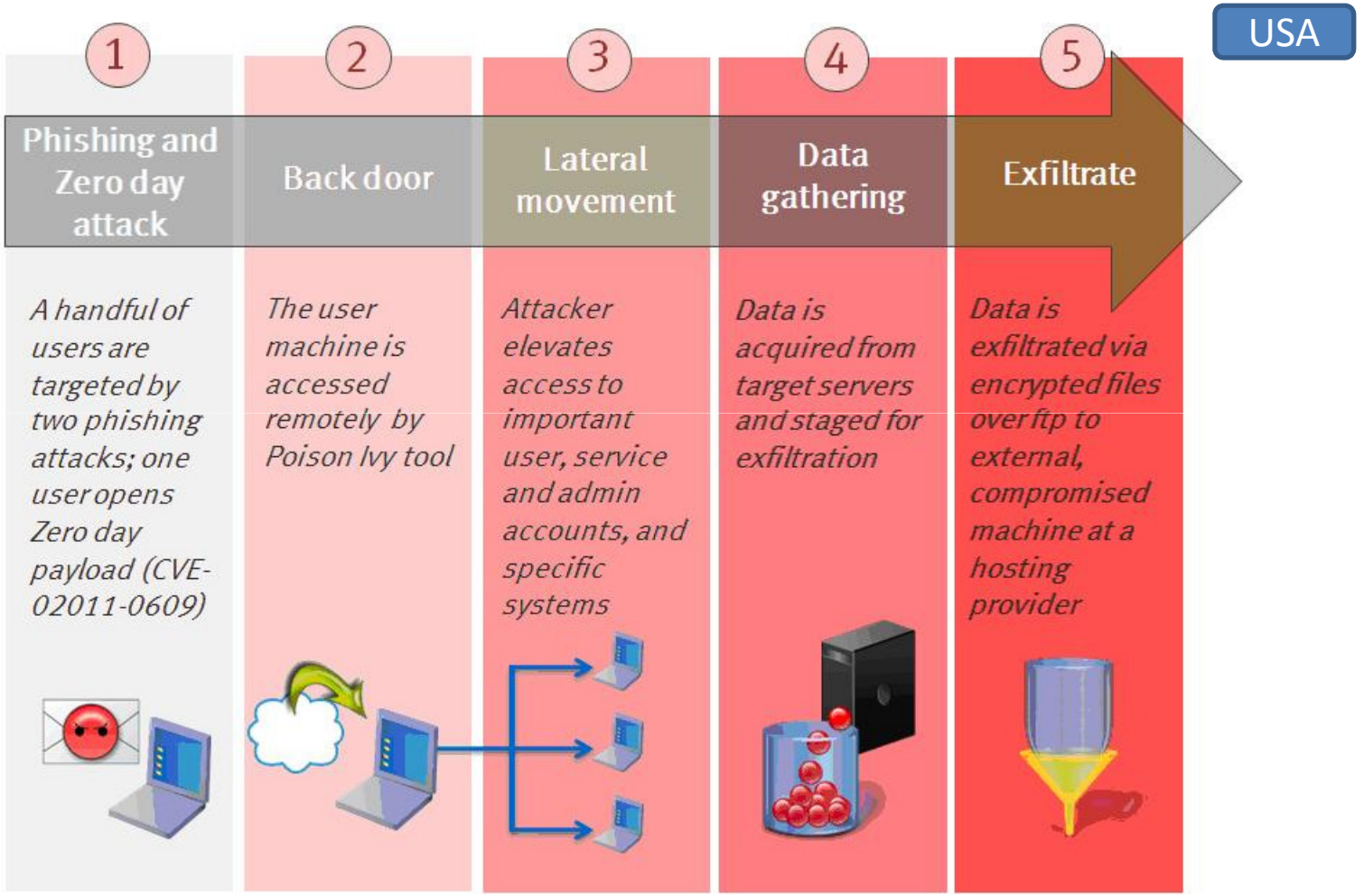
数据泄露案例分析(Sony)

Japan



https://threatpost.com/en_us/blogs/what-sony-playstation-network-attack-can-teach-us-about-database-security-051211

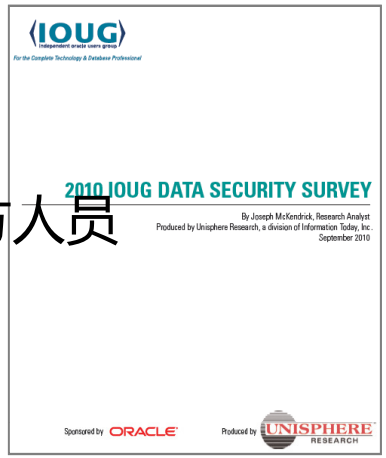
数据泄露案例分析(RSA)



http://blogs.rsa.com/rivner/anatomy-of-an-attack/

分析结论:信息安全的防范重点在数据库

- 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人员或第三方人员
- 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



✓ *Source: 2010 Independent Oracle User Group (IOUG) Data Security Survey, based on survey of 430 members.*
http://www.oracle.com/dm/offers/fy11/50651_2010_report_ioug_data_security_survey.pdf

- 随着企业业务对IT系统的依赖程度越来越高，IT风险对业务风险的影响也越来越大。尽管IT技术出现漏洞的状况有上升趋势，今天的企业已经不可能脱离IT系统仍能够有效地管理和运营，数据安全正是企业赖以生存和发展的核心资产。因此，有效地掌控企业数据库的操作状态，对企业的安全运营至关重要。

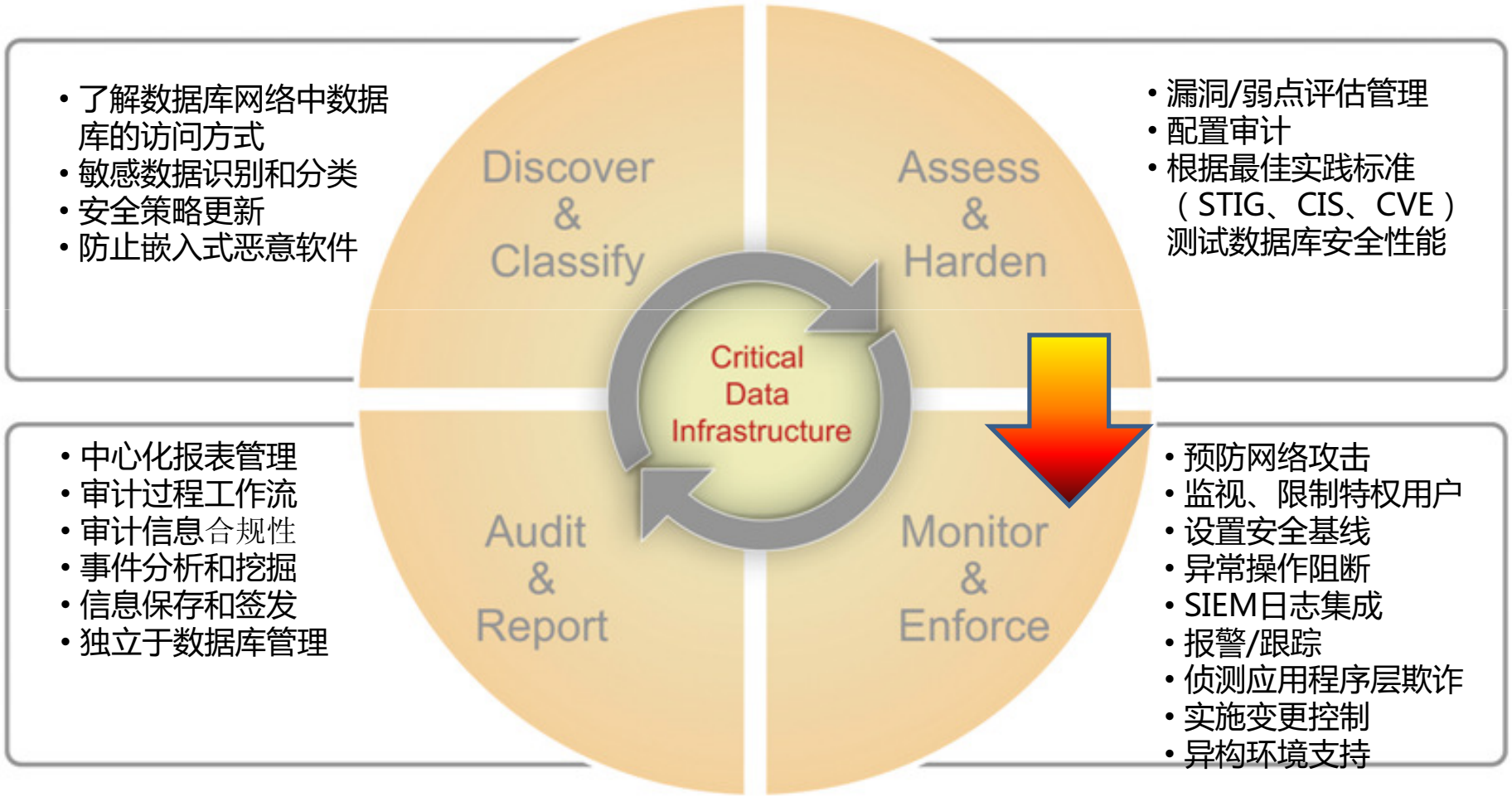
如何掌控？根据国家信息安全等级保护条例了解信息是否遭到非授权修改、泄漏或无法使用是关键

安全等级	等级名称	基本描述	安全保护要求
第一级	自主保护级	适用于一般信息系统。若系统所存储、传输和处理的信息遭到非授权修改、泄漏或无法使用，或者系统中断、损坏，导致系统承载的业务无法正常进行，会对公民、法人和其他组织的合法权益产生损害，但不损害国家安全、社会秩序和公共利益。	参照公司标准自主进行保护。
第二级	指导保护级	适用于一般的信息系统，若系统所存储、传输和处理的信息遭到非授权修改、泄漏或无法使用，或者系统中断、损坏，导致系统承载的业务无法正常进行，会对公民、法人和其他组织的合法权益产生严重损害或对社会秩序和公共利益造成损害，但不损害国家安全。	在国家主管部门的指导下，按照国家和公司标准自主进行保护。
第三级	监督保护级	适用于涉及国家安全、社会秩序和公共利益的重要信息系统。若系统所存储、传输和处理的信息遭到非授权修改、泄漏或无法使用，或者系统中断、损坏，导致系统承载的业务无法正常进行，会对社会秩序和公共利益造成严重损害，或对国家安全造成损害。	在国家主管部门的监督下，按国家和公司标准严格落实各项保护措施进行保护。
第四级	强制保护级	适用于涉及国家安全、社会秩序和公共利益的重要信息系统。若系统所存储、传输和处理的信息遭到非授权修改、泄漏或无法使用，或者系统中断、损坏，导致系统承载的业务无法正常进行，会对社会秩序和公共利益造成特别严重损害，或对国家安全造成严重损害。	在国家主管部门的强制监督和检查下，按国家标准严格落实各项措施进行保护。
第五级	专控保护级	适用于涉及国家安全、社会秩序和公共利益的极端重要信息系统。若系统所存储、传输和处理的信息遭到非授权修改、泄漏或无法使用，或者系统中断、损坏，导致系统承载的业务无法正常进行会对国家安全造成特别严重损害。	根据安全需求，由国家主管部门和运营单位对信息系统进行专门控制和保护。

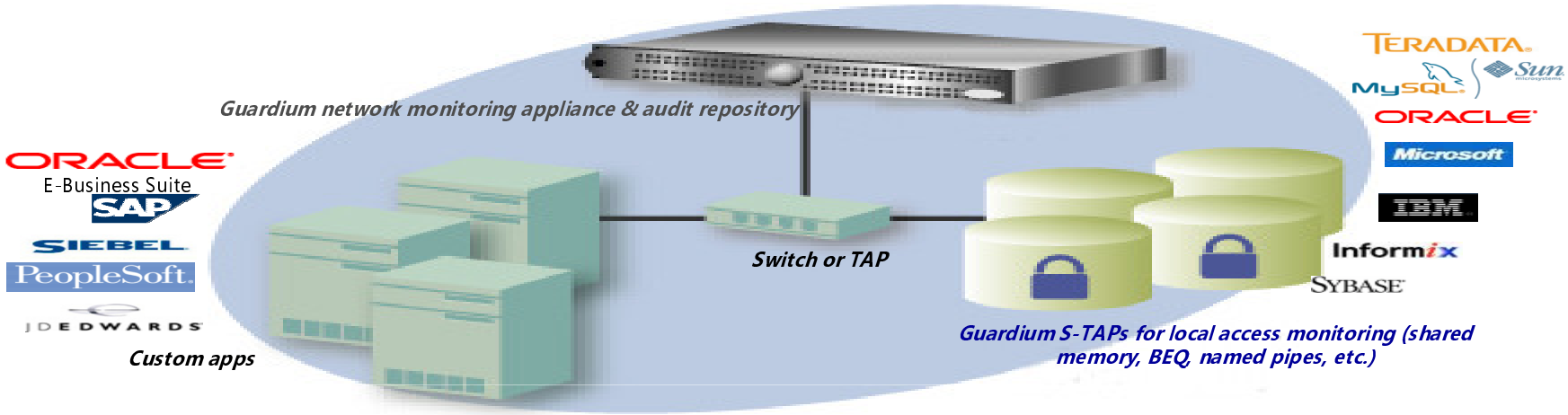
具体到数据安全就是要了解以下数据库操作状况

- 谁在修改、删除数据？(Who is changing database schemas or dropping tables?)
- 何时发生过非法数据访问、篡改? (When are there any unauthorized source programs changing data?)
- DBA或其他外部人员正在对数据库做什么操作?(What are DBAs or outsourced staff doing to the databases?)
- 某段时间内发生过多少次失败的数据库登录? (How many failed login attempts have occurred?)
- 谁在读取书库中的信用卡数据? (Who is extracting credit card data?)
- 敏感数据正在被哪个网络节点访问? (What data is being accessed from which network node?)
- 哪些敏感数据正在被哪些应用程序访问?(What data is being accessed by which application?)
- 敏感数据正在被以何种方式访问? (How is data being accessed?)
- 每天的各个时间段内，数据都在以什么样的访问模式被访问着?(What are the access patterns based on time of day?)
- 数据库正在产生什么样的错误?(What database errors are being generated?)
- SQL注入式攻击在何时由谁发起?(When is someone attempting an SQL injection attack?)

实施步骤：从数据库操作监控入手，进而拓展到安全审计、信息分布及被使用状况、和系统综合评估



Guardium简介：
非入侵式数据库活动监控(DAM)架构



- 非入侵、网络旁路的方式
- 可供事件后鉴证分析的审计纪录
- 跨平台和集中管理
- 职责分工

- 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，数据库安全是由监测、解析、控制、和审计等过程共同完成的。无论数据库操作源于那种渠道，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)。

GUARDIUM数据库操作流量导向方式

- 镜像导入(SPAN):在端口A和端口B之间建立镜像关系，通过端口A传输的数据将同时复制到端口B，以便于在端口B上连接监控设备
- S-TAP:软件分路器,工作原理同上。灵活性、可拓展性更高，且对网络拓扑和数据库设置无影响

Guardium技术要点说明

数据安全需求	描述
100%的监控能力	无监控死角，完全监控源自网络、数据库服务器、或堡垒机的各种操作
应用系统用户的监控	监控颗粒度能做到通过连接池操作的用户ID
与SIEM(SOC)系统集成	SYSLOG通道实时集成其他监控系统
审计流程自动化	工作流引擎提升审计效率
异常操作阻断	阻断可使数据泄漏风险降至最低
对生产系统影响小	无须变更网络拓扑、数据库配置、及过量系统存储
审计凭证性	审计监控数据按数据库格式提供，能被更改的数据不能做为审计凭证
企业级无缝拓展能力	无论项目实施范围是1台或数千台数据库，企业均可统一管理部署各环节。例如：策略、报告、和传输加密

Guardium在全球（包括中国）拥有超过500家客户

金融: 世界十大金融公司中的七家
保险: 全球最大的六个保险公司中的五个
零售业: 全球三大零售商中的两个
制造业: 最大饮料食品集团、PC制造商之一和最大的汽车制造商
能源: 美国某大型电网集团
电信: 25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

国内客户使用GUARDIUM一览

客户	项目名称	简介
某保险公司	内部数据安全审计	大量的数据校对使已有的审计手段难以满足日益频繁的审计要求及信息可靠性的要求，GUARDIUM兼顾监控和信息审计凭证两方面需求。
某农信银行	客户数据保护	实施GUARDIUM以实现行业合规和客户信息保护
某政府财政厅	财务数据审计	GUARDIUM采集的操作信息可追踪到每个用户，即财务审计的关键
某报社	敏感数据保护	大量敏感数据存在于不同厂商的数据库中，GUARDIUM提供跨平台的数据保护
某住房公积金	大额交易审计	超百亿的基金流向必须严加掌控，GUARDIUM可做到100%访问监控
某行业协会	数据库监控	Guardium满足协会对特权用户和敏感信息保护的要求
某石油公司	系统扩容	数据安全在系统扩容时已是必须满足的要求
某航空公司	敏感信息访问控制	GUARDIUM不仅能实现敏感信息保护同时能阻断非正常数据操作
某医院	统方治理	GUARDIUM帮助该医院实现了统方治理

GUARDIUM近期培训

Guardium Beijing Aug 9 – 12

https://www.ibm.com/developerworks/wikis/display/im/InfoSphere+Guardium+Bootcamp

Thank you