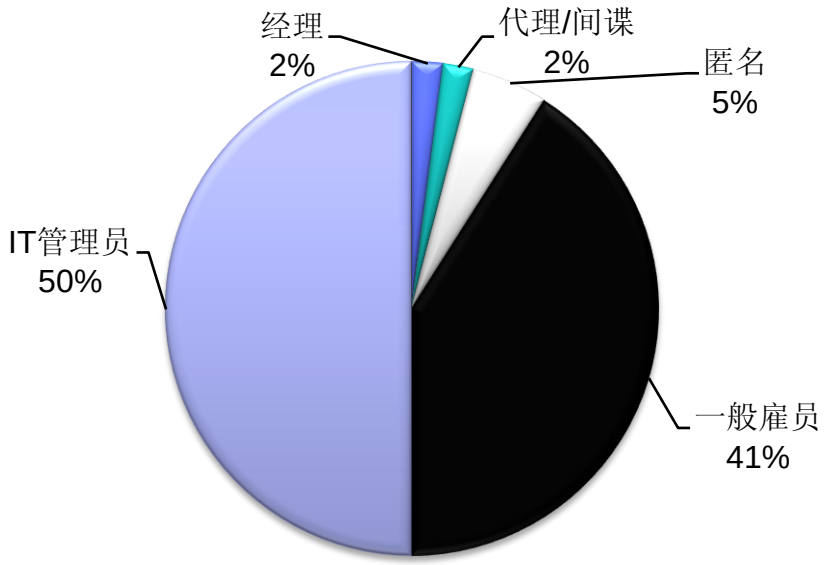
数据综合管理与数据安全

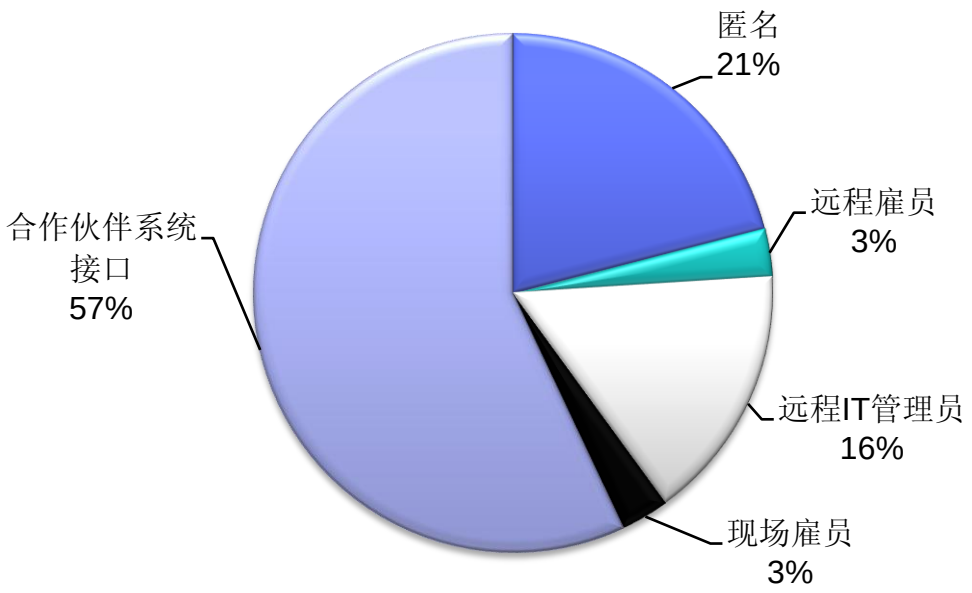
邱建,技术咨询顾问
jayqui@cn.ibm.com
IBM IDM Tiger Team

目录

数据安全风险实实在在



内部风险来源分布



合作伙伴风险来源分布

- 2008 Data Breach Investigations Report
- 深入分析2004至2007年间全球 500+ 的数据安全案件

verizon business

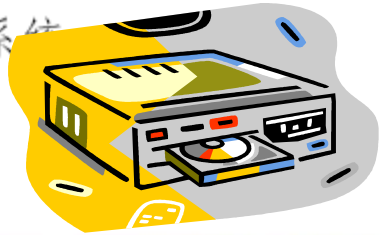
国家/企业自身的法规遵从的要求逐年加强

企业内部控制应用指引第18号-信息系统第6条…

企业在系统开发过程中，应当按照不同业务的控制要求，通过信息系统中的权限管理功能控制用户的操作权限，避免将不相容职责的处理权限授予同一用户。

企业应当针对不同数据的输入方式，考虑对进入系统数据的检查和校验功能。对于必需的后台操作，应当加强管理，建立规范的流程制度，对操作情况进行监控或者审计。

企业应当在信息系统中设置操作日志功能，确保操作的可审计性。对异常的或者违背内部控制要求的交易和数据，应当设计由系统自动报告并设置跟踪处理机制。



数据安全直接关系到企业的实际利益!!!

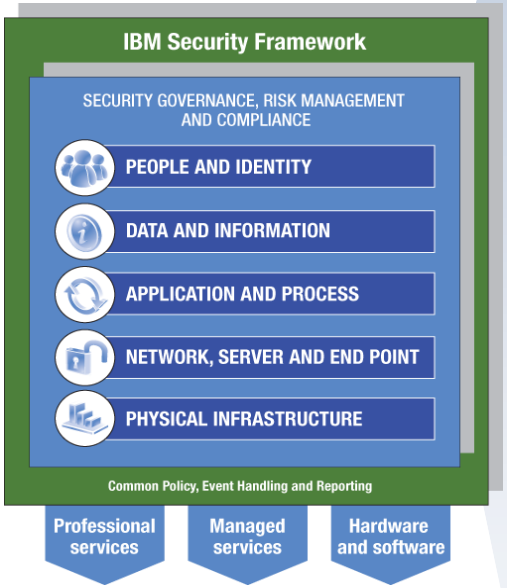
- 某电信运营商用两周时间查出员工接受一千元出售市长通话记录给私人侦探
- 可口可乐泄密案,力拓门泄密案件
- 中国海军潜艇科研项目的军工科研所发生重大泄密事件(2010年2月,彭某的电脑中违规下载了大量军工科研项目的资料)
- 全球各大媒体(包括CCTV)2010年3月11日纷纷报道:”汇丰银行因内部IT员工盗窃客户资料,损失重大.在受到侵害的2.4万客户中,已有9千名离开了汇丰银行
- 2008年17个国家的43家大型公司丢失的4200条到113000条客户记录中,每条记录平均损失202美元中，有139美元（占69%）是指丢失业务
- 在Fortune排名前100家的公司中，每次电子文档泄漏的平均损失是50万美元
- 有数据显示，我国每年因网络泄密导致的经济损失高达上百亿!

企业IT安全治理全景图

= Professional Services

= Cloud-based & Managed Services

= Products



GRC

Security Governance, Risk and Compliance

SIEM and Log Management

Identity and Access Management

Identity Management

Access Management

Data Security

数据保护

加密和密钥

Messaging Security

E-mail Security

数据库活动监控(DAM)

隐私化

Application Security

App Vulnerability Scanning

Web Application Firewall

App Source Code Scanning

Web / URL Filtering

Access and Entitlement Management

SOA Security

Infrastructure Security

Vulnerability Assessment

Mainframe Security

Threat Assessment

Web/URL Filtering

Intrusion Prevention System

Firewall, IDS/IPS, MFS Mgmt.

Security Event Management

Virtual System Security

Physical Security

DAM数据安全的核心领域 -Gartner 2010年4月

Figure 1. Applicable Use Cases for Use in the Evaluation and Selection Process

		DAM	DLP	SIEM	NIDS	DB Scanner	CCM	Fraud	IAM
Privileged Users	Access or changes to data	●	◐	○	○	○	○	◐	○
	Access via inappropriate or unapproved channels	●	◐	●	◐	○	○	◐	○
	Schema modifications	●	○	◐	○	◐	●	○	○
	Addition or modification of accounts	●	○	◐	◐	◐	○	◐	◐
End Users	Access to excessive or unneeded data	●	◐	◐	◐	○	○	●	◐
	Data access outside standard hours	●	●	◐	●	○	○	●	◐
	Access via inappropriate or nonapproved channels	◐	◐	◐	●	○	○	●	◐
Developers Sys. Admins Analysts	Access to live production systems	◐	◐	◐	●	○	○	◐	◐
IT Ops	Nonapproved changes to databases or applications	◐	○	◐	○	●	●	○	○
	Out-of-cycle patching of production systems	◐	○	◐	◐	●	●	○	○

Legend

Database Activity Monitoring	DAM	Database Vulnerability Scanner	DB Scanner
Data Loss Prevention	DLP	Change and Configuration Management	CCM
Security Information and Event Management	SIEM	Fraud Monitoring and Detection	Fraud
Network Intrusion Detection/Prevention	NIDS	Access Management	IAM

Value/Applicability

- ● High
- ◐ Good
- ○ Poor or not applicable

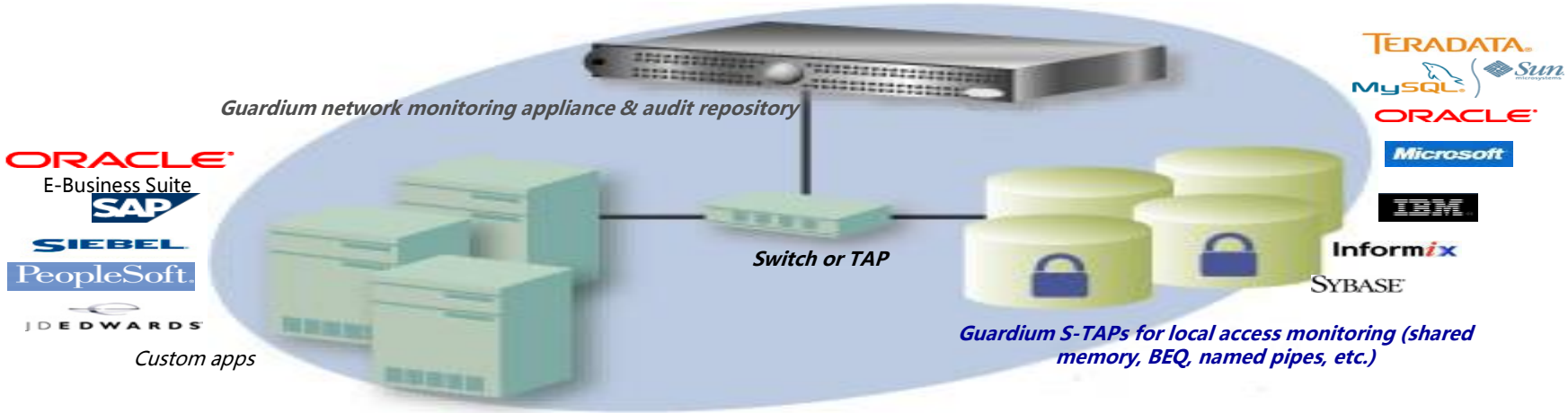
Source: Gartner (April 2010)

目录

企业数据安全管理需求

- 企业信息安全规范需要技术手段得以强化
- 需要记录关键数据流各环节的操作
- 对异常或违背内控规范的操作实时报警
- 数据库活动监控要支持工作流机制
- 监控方案可拓展
- 对现有生产系统性能无负面影响
- 简化数据安全管理的复杂度
- 法规遵从、降低成本、提升企业整体抗风险能力

Guardium架构示图



- 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

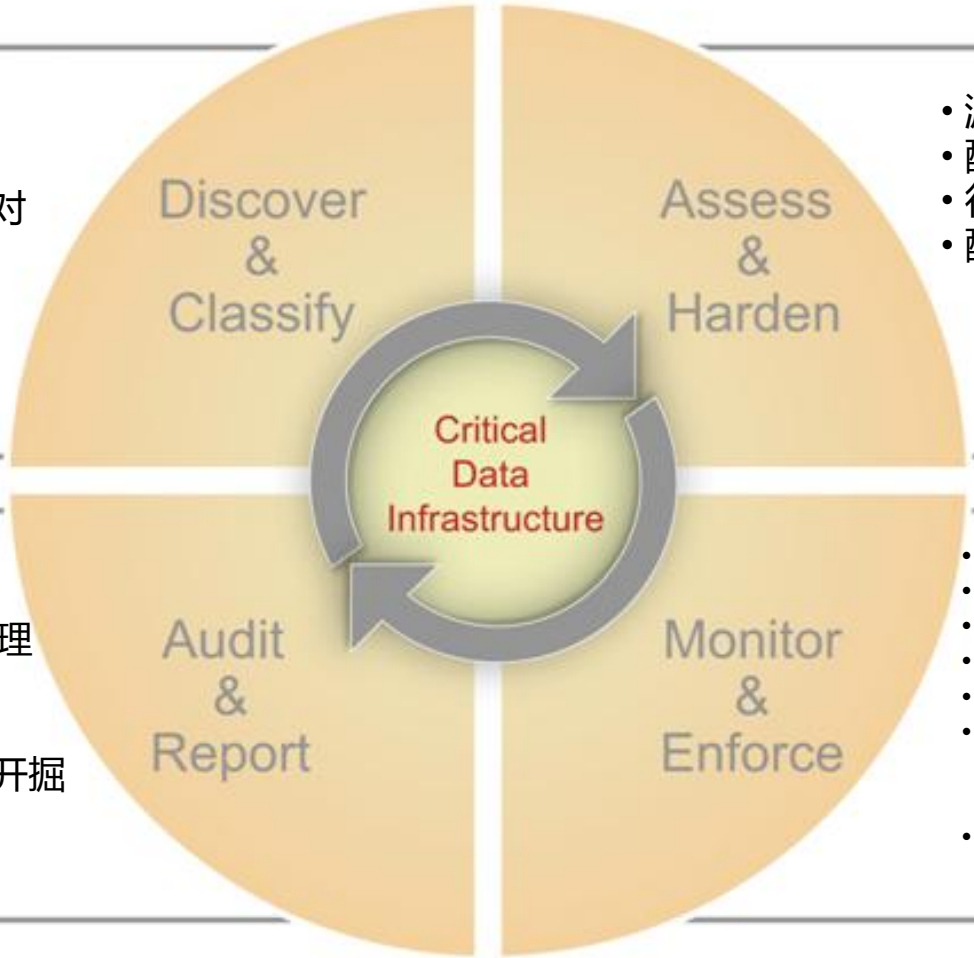
- 综述:网络是数据库活动流量的载体，Guardium结合企业信息安全规范捕获网络中相关的数据库操作，经过加工整理提供实时报警、跟踪报告、及数据库安全隐患分析等。Guardium采用的是网络旁路方式捕获数据库操作的，因此对系统性能影响很小。
- 用途:根据数据治理原理，信息安全是由隐私化和审计两领域共同完成的。隐私化（如：Optim Redaction)在最大限度保障信息泄密，而Guardium的监控可对正在发生的和可能会发生违反企业安全规范的数据操作进行有效的控制。这些操作包括：查询敏感数据、改变表定义 (DDL) 、数据操作 (DML)、例外操作(Failed logins, SQL errors, 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，且对网络拓扑无影响

GUARDIUM四大功能

- 识别发现所有数据库、应用系统和客户端
- 识别关键敏感数据并对其分类

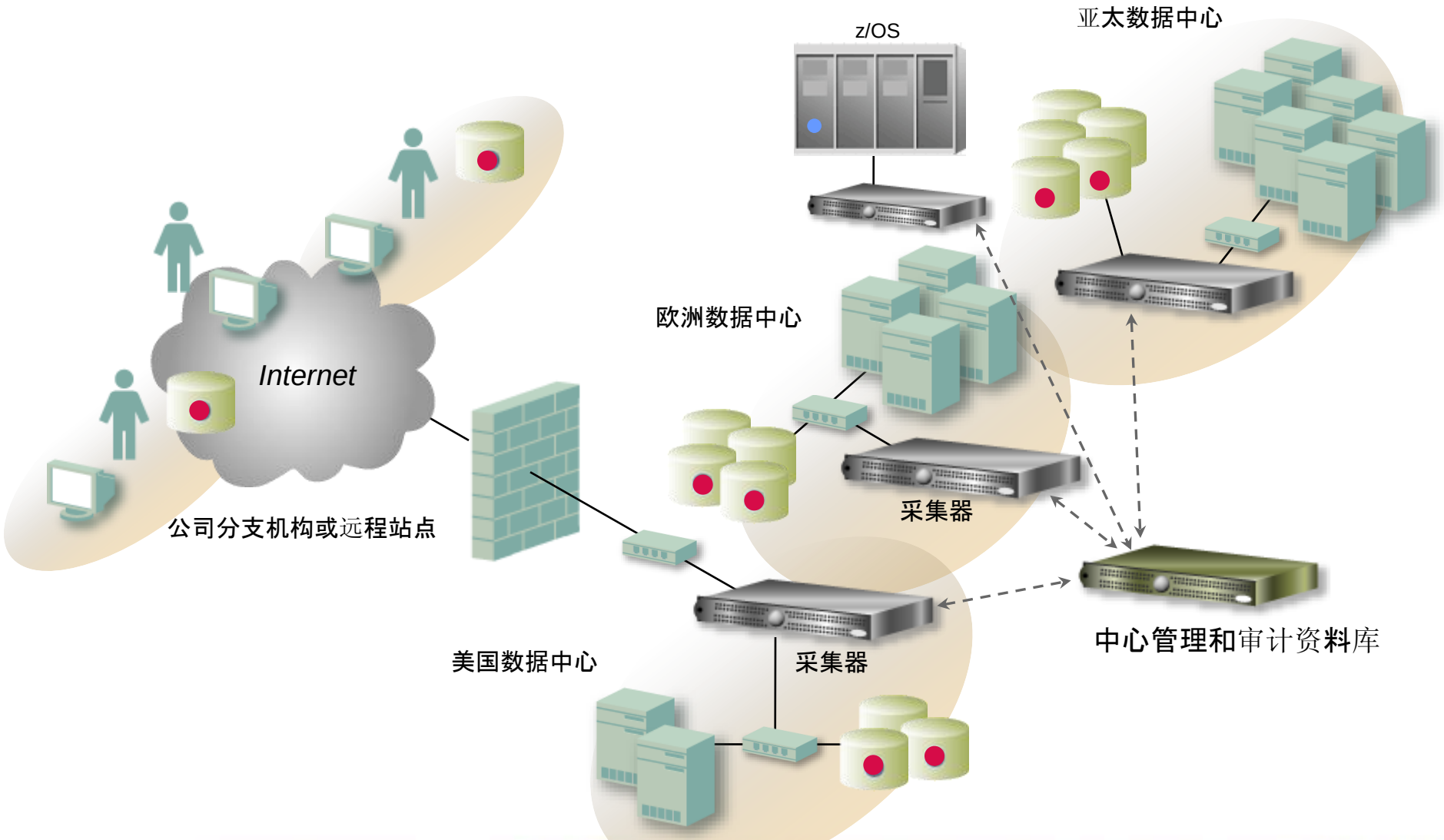


- 漏洞/弱点评估管理
- 配置评估
- 行为评估
- 配置锁定和跟踪变化

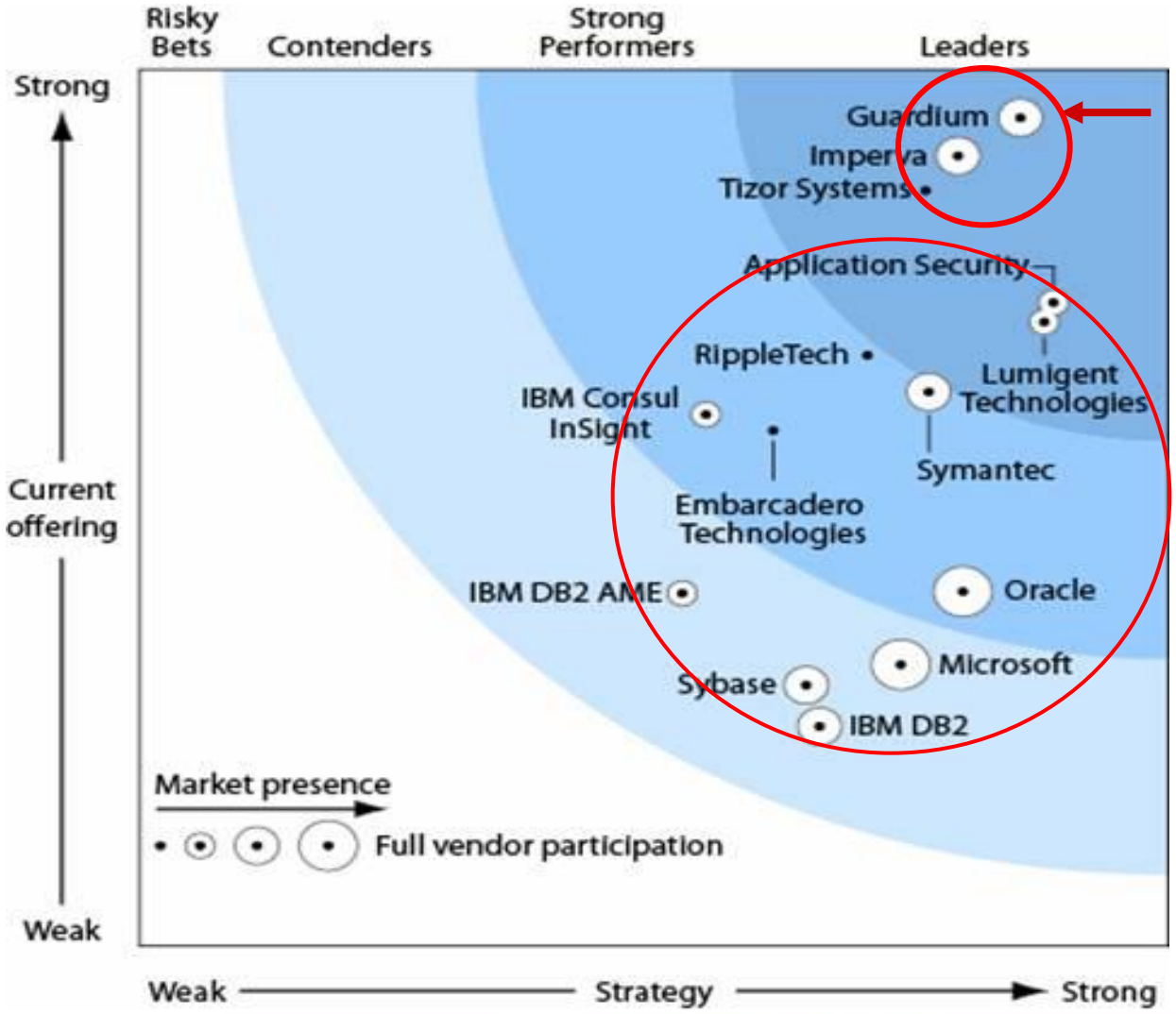
- 中心化管治报表
- 签发（Sign-off ）管理
- 自动化问题升级
- 安全审计库
- 用于事件分析的数据开掘
- 长期保存

- 100%的可视性
- 基于规范的行动
- 对异常情况的识别
- 细微的访问存取控制
- SIEM 整合
- 监测 内部访问存取和加密连接 (Oracle ASO, SSL, ...)
- 监测大型机 mainframe 连接 (CICS, MQ, IMSTM, TSO, CAF, ...)

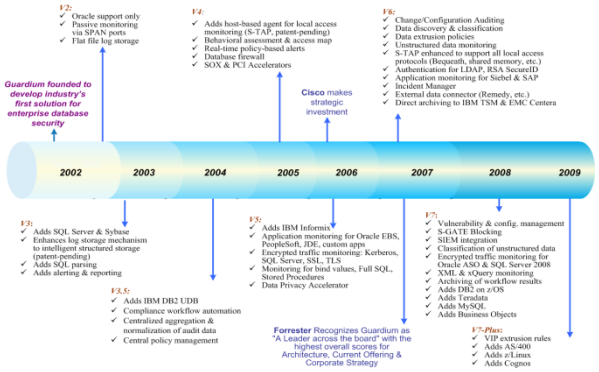
GUARDIUM实施案例



GUARDIUM引领数据安全管理的发展方向



- 数据库平台支持
- 生产系统性能
- 责权分离
- 监控实时性
- 管理复杂度
- 可拓展性



Guardium客户

金融：世界五大银行、最大的信用卡公司、最大的共同基金公司

保险：全球最大的五个保险公司中的三个

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：美国国家电网集团

电信：15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

目录

数据库安全--8步最佳实践

8.加密-使用加密技术呈现敏感数据，阻止攻击者从数据传输过程中获取信息

7.认证、访问控制及权限管理-确保每个用户拥有权限赋予访问范畴，并通过管理特权来限制对数据的访问

6.审计-针对合规要求,如:SOX,预先配置报告，自动化整个遵从性审计流程，包括向监督团队分发报告、报告签署和上报

5.数据库活动监控-监控敏感数据访问、特权用户行为、变更控制、应用用户活动和安全性异常（比如登录失败），并实施对应安全策略,如实时报警

数据库安全

1.发现-定位和分类企业数据库中的敏感信息

2.弱点和配置评估
评估数据库漏洞和配置缺陷

3.加固
执行安全建议,如:安全补丁

4.变更审计-设置'黄金'安全防护基线，对偏离基线的事件提供全面可视性

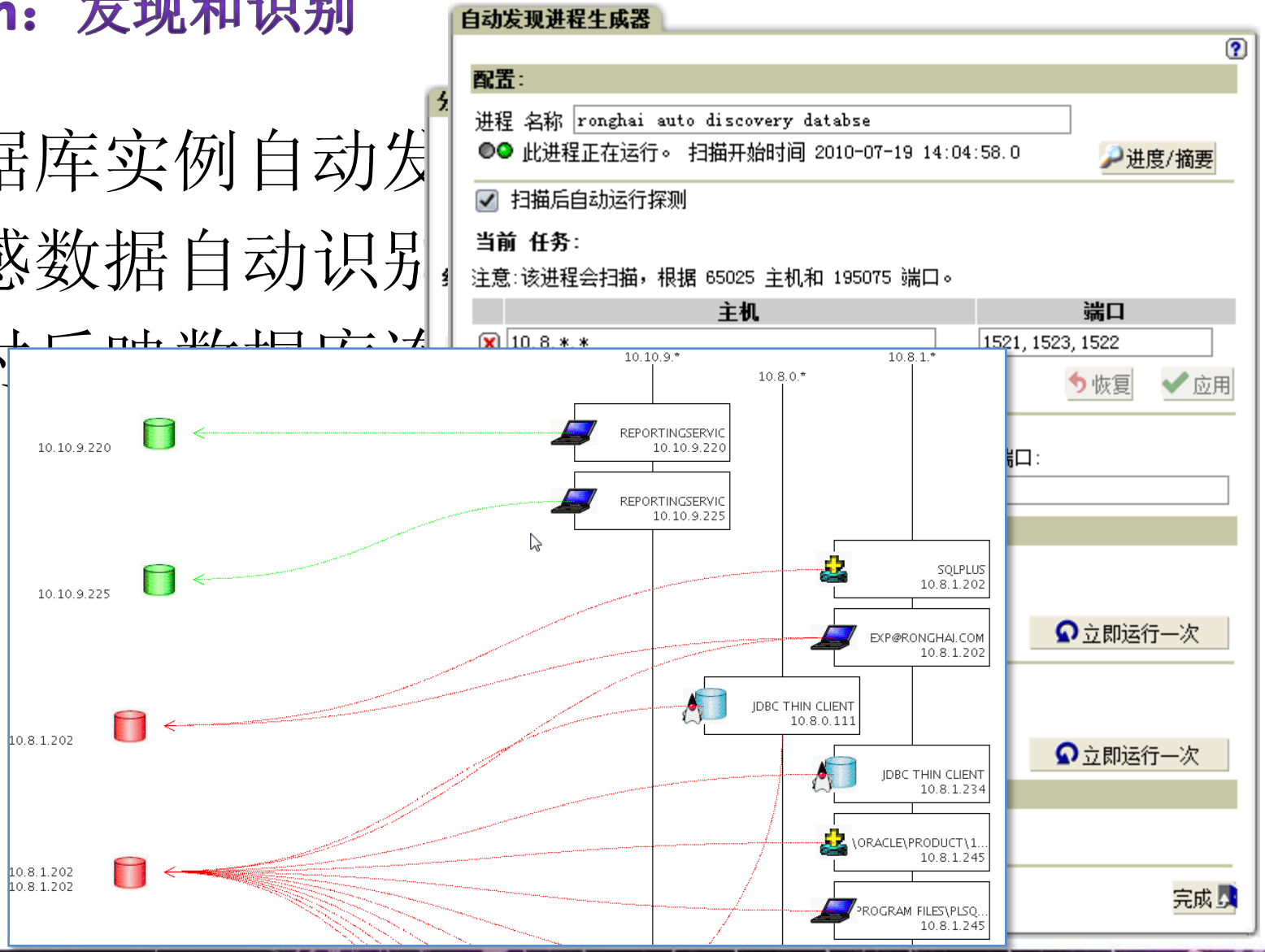
By Ron Ben Natan, Ph.D., CTO, Guardium , an IBM Company

第一步：发现

- **你不能保护你不知道的东西！**
- 你必须要对敏感的信息资产有很好的了解：
  - 数据库实例
  - 对数据库的访问连接
  - 数据库中的数据
- 要有自动化的发现机制：
  - 应用的变化很可能导致敏感数据存储的变更

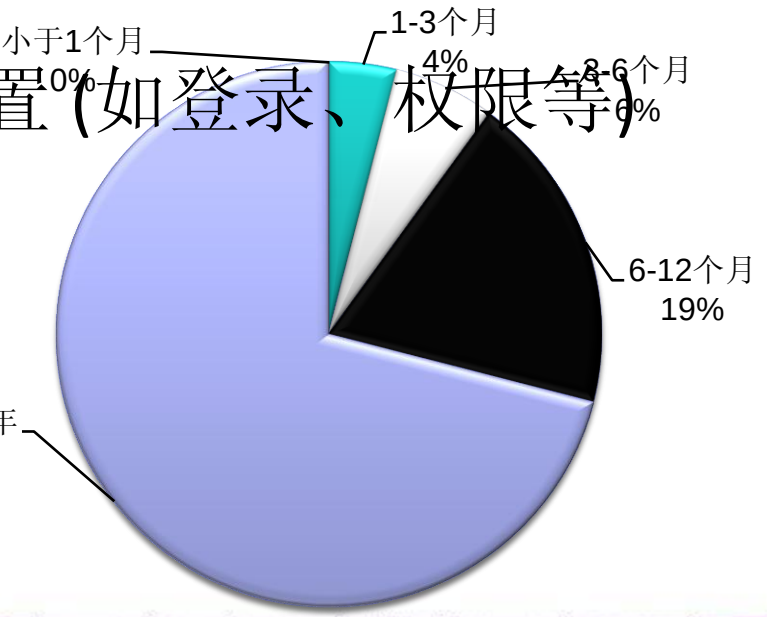
Guardium：发现和识别

- 数据库实例自动发
- 敏感数据自动识别
- 实时



第二步：弱点和配置评估

- 对数据库的配置进行评估，以避免明显的漏洞
  - 数据库安装文件的安全性 (如，配置文件的权限以及可执行属性)
  - 数据库内部的安全性配置 (如登录、权限等)
  - 数据库补丁
- 定期进行
  - 以了解安全性的变化



Guardium：识别出没有打Patch的风险点

Guardium Data Protection Service (DPS), Oracle Database Risk Matrix

Vuln#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS VERSION 2.0 RISK			
					Base Score	Access Vector	Access Complexity	Authentication
CVE-2009-0979	Resource Manager	Oracle Net	ALTER_SYSTEM	No	8.5	Network	Medium	Single
CVE-2009-0985	Core RDBMS	Oracle Net	IMP_FULL_DATABASE role	No	7.1	Network	High	Single
CVE-2009-0972	Workspace Manager	Oracle Net	Create Session	No	6.5	Network	Low	Single
CVE-2009-0977	Advanced Queuing	Oracle Net	Execute on DBMS_AQIN	No	5.5	Network	Low	Single
CVE-2009-0992	Advanced Queuing	Oracle Net	Execute on DBMS_AQIN	No	5.5	Network	Low	Single
CVE-2009-0984	Database Vault	Oracle Net	Execute on DBMS_SYS_SQL	No	5.5	Network	Low	Single
CVE-2009-0980	SQLX Functions	Oracle Net	Execute on AGGXQIMP	No	5.5	Network	Low	Single

Manage Members for Selected Group

Group Name: **Vulnerable Objects (with wildcards)**

Group Type: **OBJECTS**

Group Members:

%DBMS_AQADM.%
%DBMS_AQADM_SYS.%
%DBMS_AQELM.%
%DBMS_AQIN
%DBMS_AQJMS_INTERNAL.%
%DBMS_AQ_INV.%
%DBMS_CAPTURE_ADM_INTERNAL.%
%DBMS_CDC_DPUTIL.VALID_TABLE
%DBMS_CDC_IMPDP.%
%DBMS_CDC_IMPDP.IMPORT_CHANGE_COLUMN
%DBMS_CDC_IMPDP.VALIDATE_IMPORT
%DBMS_CDC_IMPDP.VALIDATE_SUBSCRIPTION
%DBMS_CDC_IPUBLISH%
%DBMS_CDC_IPUBLISH.%
%DBMS_CDC_ISUBSCRIBE.EXTEND_WINDOW_LIST

第三步：数据库加固

- 评估的结果作为数据库加固的指导建议
- Database STIG(Database Security Technical Implementation Guide)
  - DISA(Defense Information Systems Agency)为DOD(Department of Defense) 设计的安全指导
  - http://iase.disa.mil/stigs/index.html
- *举例*
  - *删除或锁住不使用的预定义帐户，不使用预定义的密码；*
  - *删除不使用的预定义角色；*
  - *删除不使用的数据库组件；*
  - *删除不使用的数据库选项或属性；*
  - *删除PUBLIC权限*

第四步：变更审计

- 数据库配置文件以及权限的调整不仅可能引起**故障**，也往往预示着数据**风险**！
- 需要利用配置变更控制工具持续地对配置信息进行跟踪审计
- 一旦有变化，应立即报警！

Guardium：变更审计

- Guardium的CAS(Change Audit System)功能可以：
  - 监控数据库关键的配置文件、脚本的内容及权限的变化
  - 监控数据库环境变量或注册表的变化
  - 监控操作系统关键配置文件及权限的变化

CAS 变化详细信息

开始日期: 2010-07-12 16:11:39 结束日期: 2010-07-19 16:11:39

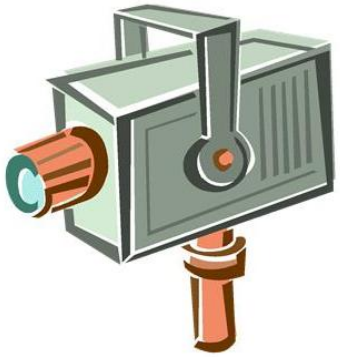
主机名	监视的项	OS 类型	DB 类型	实例名	类型	所有者	上次修改时间	示例时间	权限	已保存数据计数	主机配置计数
10.8.1.244	/etc/passwd	UNX	N/A	System	File	root	2010-05-28 09:16:57.0	2010-07-19 16:01:11.0	-rw-r--r--	0	1
10.8.1.244	/etc/passwd-	UNX	N/A	System	File	root	2009-08-06 15:26:51.0	2010-07-19 16:00:24.0	-rw-r--r--	0	1

记录: 1 结束时间 2 关闭 2

别名: 关闭

第五步：数据库活动监控(DAM)

- **100%、实时**地数据库活动监控：
  - 及时发现入侵和误用行为
    - 如，SQL注入、非法修改财务数据或权限、通过SQL进行配置调整
  - 对特权用户(SOX)以及敏感信息(PCI DSS)的活动进行监控
  - 在静态评估的基础上，进行动态的“弱点评估”
    - 如，是否有登录失败不设限的情况
  - 应该提供对应用级用户的识别，以便更好地识别风险



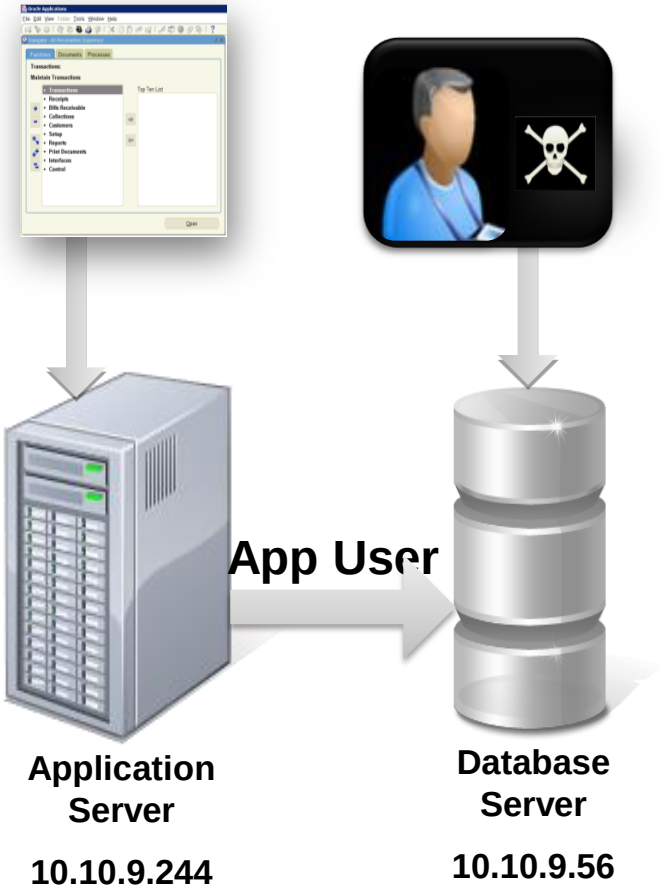
Guardium：记录 SELECT 语句对性能没有任何影响 (PCI)

Timestamp	Server Type	Server IP	Client IP	Network Protocol	DB User Name	Sql
2007-02-08 11:35:14.0	ORACLE	10.10.9.55	10.10.9.55	BEQUEATH	BENJI	SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER(?) LIKE UPPER(PRODUCT)) AND (UPPER(USER) LIKE USERID)
2007-02-08 11:35:14.0	ORACLE	10.10.9.55	10.10.9.55	BEQUEATH	BENJI	SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER(?) LIKE UPPER(PRODUCT)) AND ((UPPER(USER) LIKE USERID) OR (USERID = ?)) AND (UPPER(ATTRIBUTE) = ?)
2007-02-08 11:35:14.0	ORACLE	10.10.9.55	10.10.9.55	BEQUEATH	BENJI	SELECT DECODE(?,?,?,?) FROM DUAL
2007-01-24 14:10:35.0	ORACLE	10.10.9.55	10.10.9.240	TCP	BENJI	SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER(?) LIKE UPPER(PRODUCT)) AND ((UPPER(USER) LIKE USERID) OR (USERID = ?)) AND (UPPER(ATTRIBUTE) = ?)
2007-01-24 14:10:35.0	ORACLE	10.10.9.55	10.10.9.240	TCP	BENJI	SELECT DECODE(?,?,?,?) FROM DUAL
2007-01-24 14:10:34.0	ORACLE	10.10.9.55	10.10.9.240	TCP	BENJI	SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER(?) LIKE UPPER(PRODUCT)) AND (UPPER(USER) LIKE USERID)
2007-01-24 14:09:24.0	SYBASE	10.10.9.55	10.10.9.240	TCP	SA	select name, dbid from master.dbo.sysdatabases order by name
2007-01-24 14:09:14.0	SYBASE	10.10.9.55	10.10.9.240	TCP	SA	select o.name, o.language, o.dbname from master.dbo.syslogins o where o.name = ?
2007-01-24 14:09:14.0	SYBASE	10.10.9.55	10.10.9.240	TCP	SA	select substring (@@version, ?, charindex(?,@@version)-?)
2007-01-24 14:09:11.0	SYBASE	10.10.9.55	10.10.9.240	TCP	SA	select substring (@@version, ?, charindex(?,@@version)-?)

Records: 2496 to 2505 of 2537

GUARDIUM已压缩/加密的方式保留数据库的监控信息,其信息颗粒度是可控的.

Guardium：细粒度的策略制定，实时告警



Rule #1 Description: non-App Source AppUser Connection

Category: Security | Classification: Breach | Severity: MED

Not ☐ Server IP / and/or Group: Production Servers

Not ☑ Client IP / and/or Group: Authorized Client IPs

Not ☐ Client MAC | Net. Protocol | and/or Group

DB Type | Not ☐ Service Name | and/or Group

Not ☐ DB Name | and/or Group

Not ☐ DB User: APPUSER | and/or Group

Min. Ct.: 0 | Reset Interval (minutes): 0

Continue to next Rule ☐ | Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

☒ Notification Type MAIL Mail User marc_ga

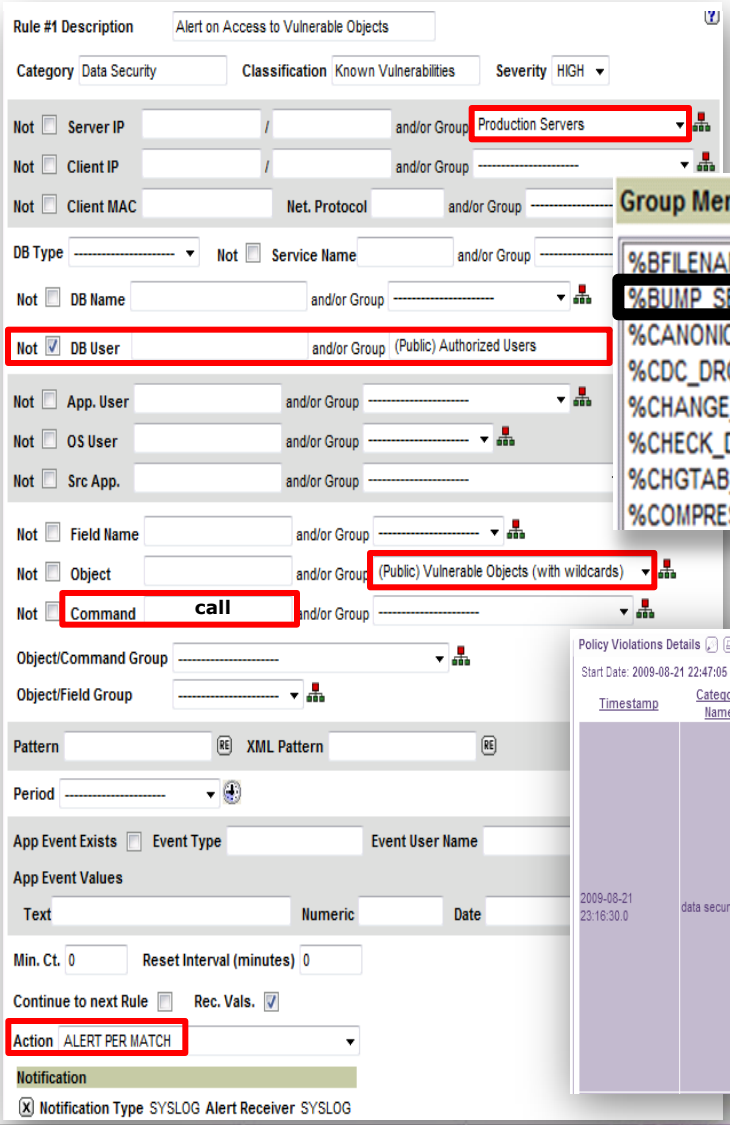
From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:00 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

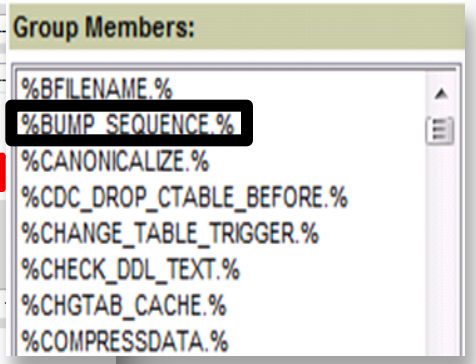
Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
Category: security Classification: Breach Severity MED
Rule # 20267 [non-App Source AppUser Connection]
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: TNS DB Protocol Version: 3.8 DB User: APPUSER
Application User Name
Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable

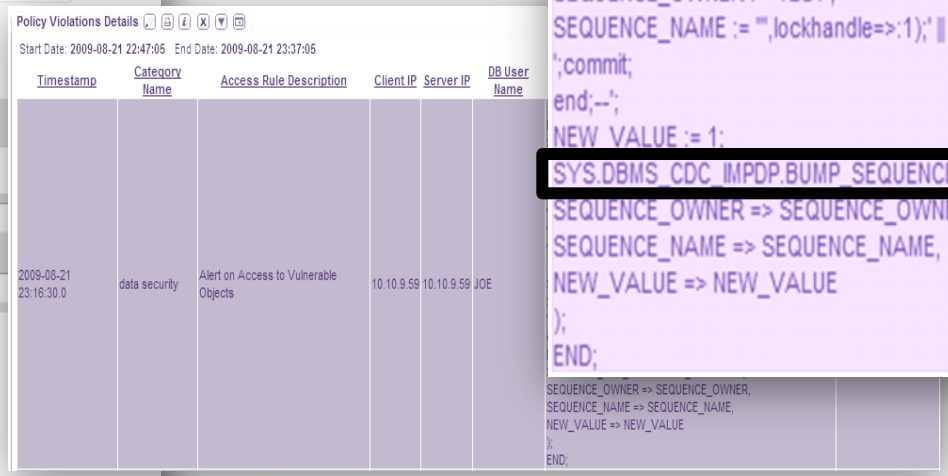
Alert! 有人从应用服务器以外的地方使用专用口令访问数据库！

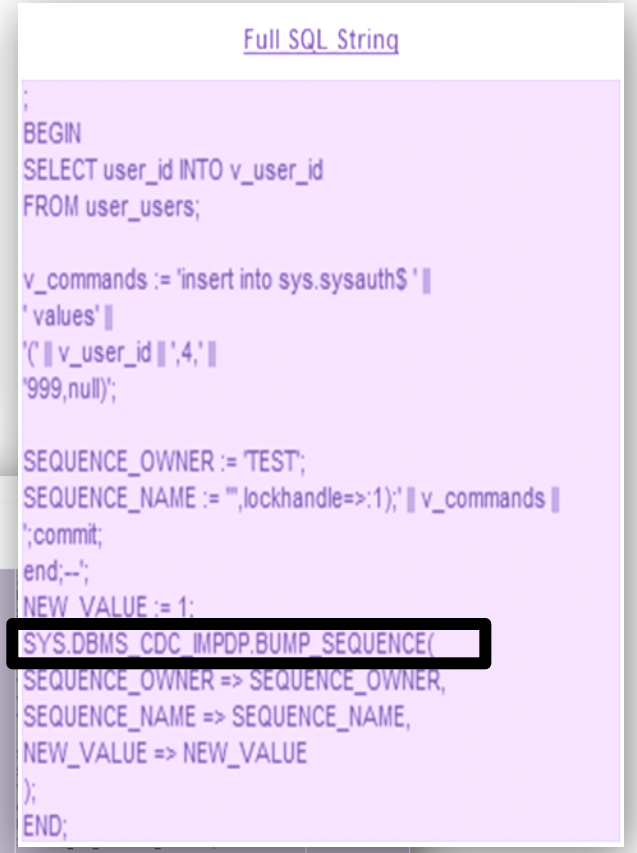
Guardium：细粒度的策略制定，实时告警

- 针对敏感对象制定策略







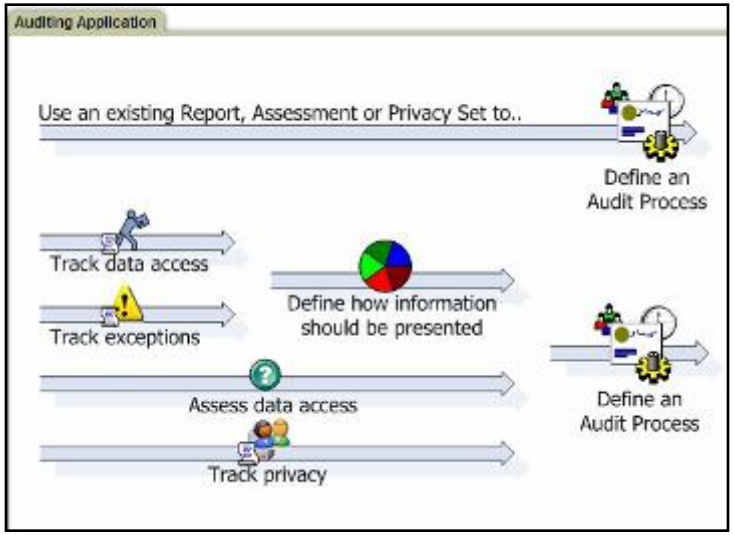


第六步：审计

- 审计是方法/过程，不是目的！
- 形式审计与实质审计
  - 审计不应该成为一个安全的漏洞！
- 合理的审计方案应该：
  - 提高审计效率（vs Native Log，手工分析）
  - 对生产系统没有或很少的性能影响
  - 减少对存储的需求
  - 最好是跨平台的数据库审计
  - 职责分享（DoS）

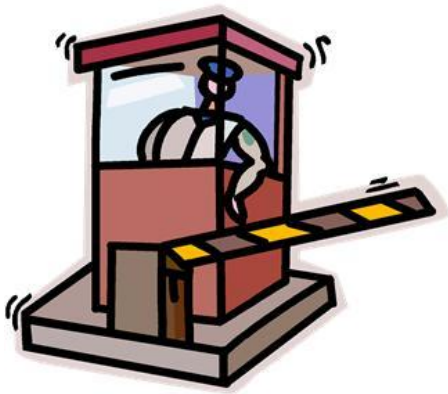
Guardium：审计工作流程自动化

- 事先安排好的和自动化的任务Scheduled & automated tasks
- 在敏感数据由于不断的变化而更换地方的情况下及时加以发现
  - 先按模式、表格名称等加以发现识别，然后:
  - 加以分类， 设置报警，将其加到某一数据组等 (基于规范的）
  - 定时操作以使安全规范得以更新
- 合规报表
  - 自动生成报表
  - 将报表分发给监管团队
  - 跟踪电子签发（ sign-offs）
  - 需要时自动将问题升级
  - 安全地储存程序trail
  - 向审计部门显示监管程序



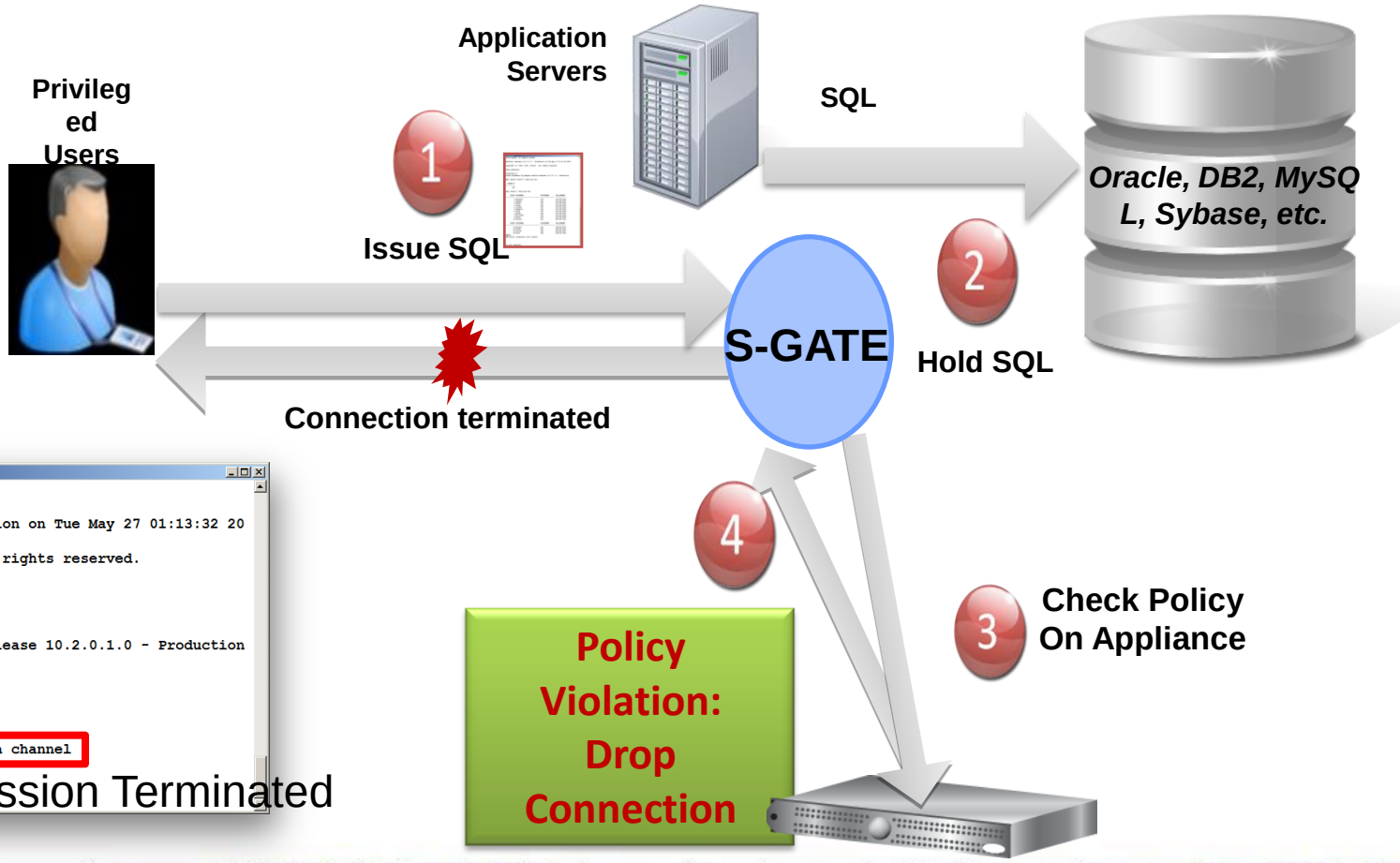
第七步：认证、访问控制及权限管理

- 每个用户对每个数据的访问当然会有不同的权限！
  - 用户认证/**身份识别**
  - 每个用户的可识别性
  - 对数据访问的权限控制
- 定期对用户权限进行审计
  - 权限配置文件
  - 权限调整SQL
- 对应用级用户的识别



Guardium S-GATE: 在 Cross-DBMS 环境中实施阻断策略

“DBMS 软件本身对于管理员是不设防的, 今天DBAs 可以轻松地查看并拿走数据库中的敏感数据。” Noel Yuhanna, Forrester, “Database Security: Market Overview,” Feb. 09

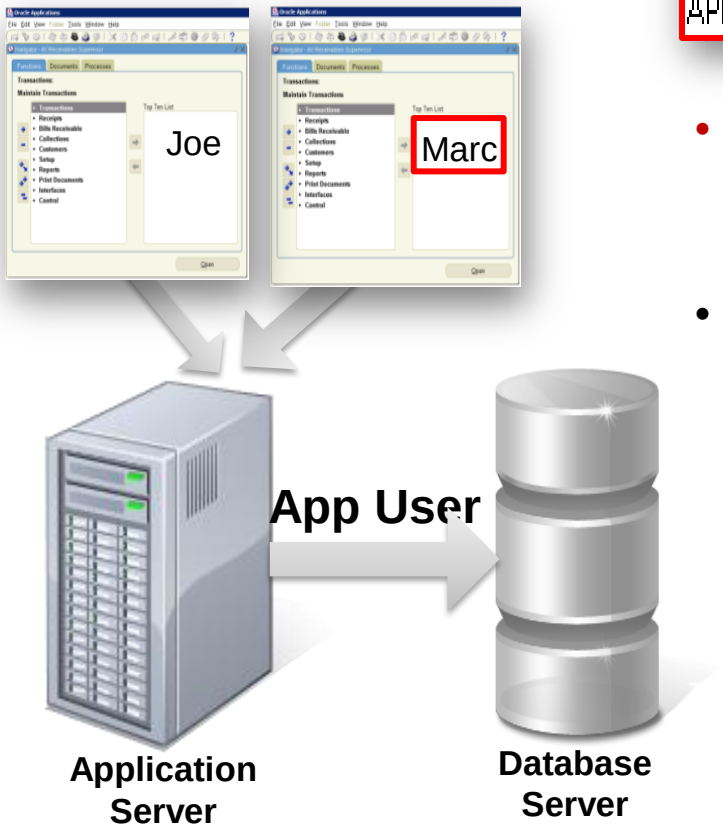



```
root@osprey:~
[root@osprey ~]# sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

SQL>
```

Session Terminated

Guardium：应用级用户-识别在连接池应用中的欺骗行为

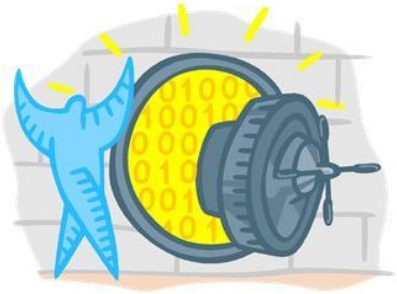
DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)



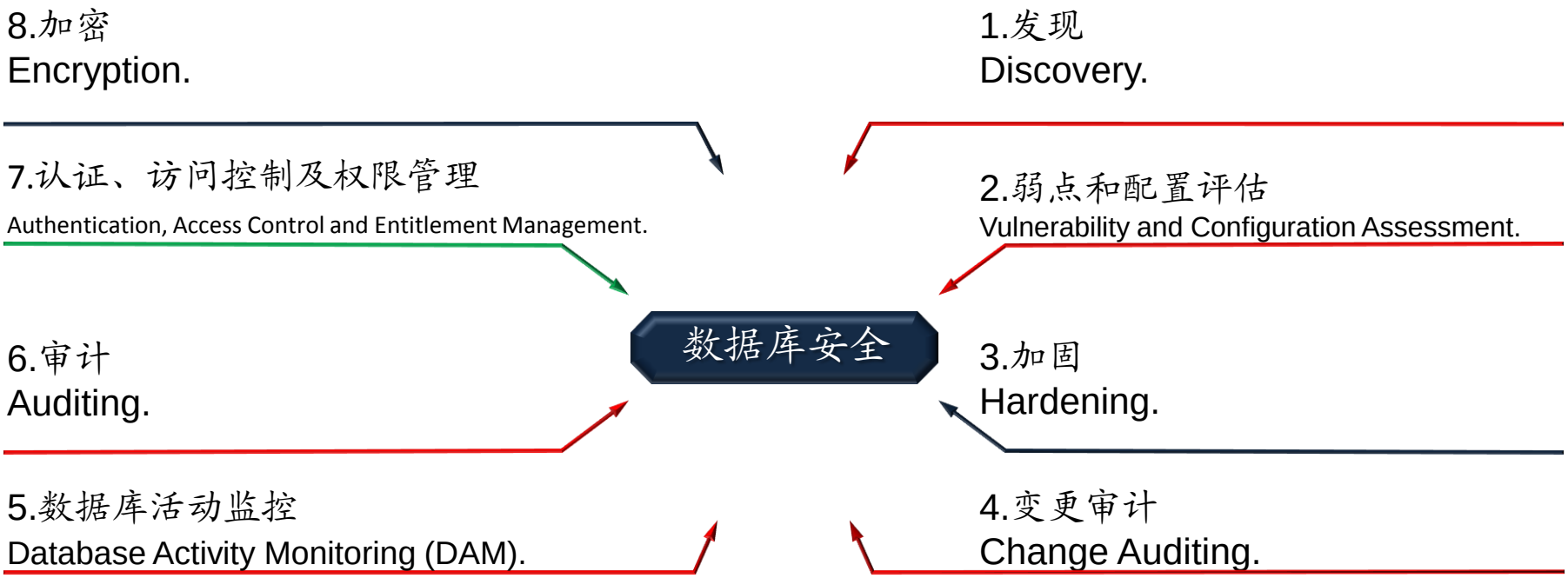
- *问题: A应用服务器一般使用一个能用的服务帐号来访问数据库 – 这样就不能识别出究竟是 WHO 发起的交易 (连接池的应用环境中)*
- *解决*: 跟踪与SQL命令相关的实际应用用户
  - Deterministic identification vs. time-based “best guess”
  - 直接支持所有主流的企业级应用 (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos, etc.)
  - 直接支持主流的中间件平台应用 (WebLogic, WebSphere, Oracle AS, etc.)
  - 提供简单的API

第八步：加密

- 传输中加密
  - 防止在网络传输中泄露
  - 可能会造成传输性能的下降，eg.SQL Server 可能下降35%
  - 方法：
    - 数据库自身的安全传输（e.g. Oracle Advanced Security）
    - 安全传输协议（e.g. SSL）
    - 安全通道（e.g. SSH通道）
    - 操作系统安全机制（e.g. IPSec）
- 存储中加密
  - 无法解读窃取的信息
  - 防止DBA了解敏感信息
  - 方法：在应用或数据库层面
- Key Management is Key !

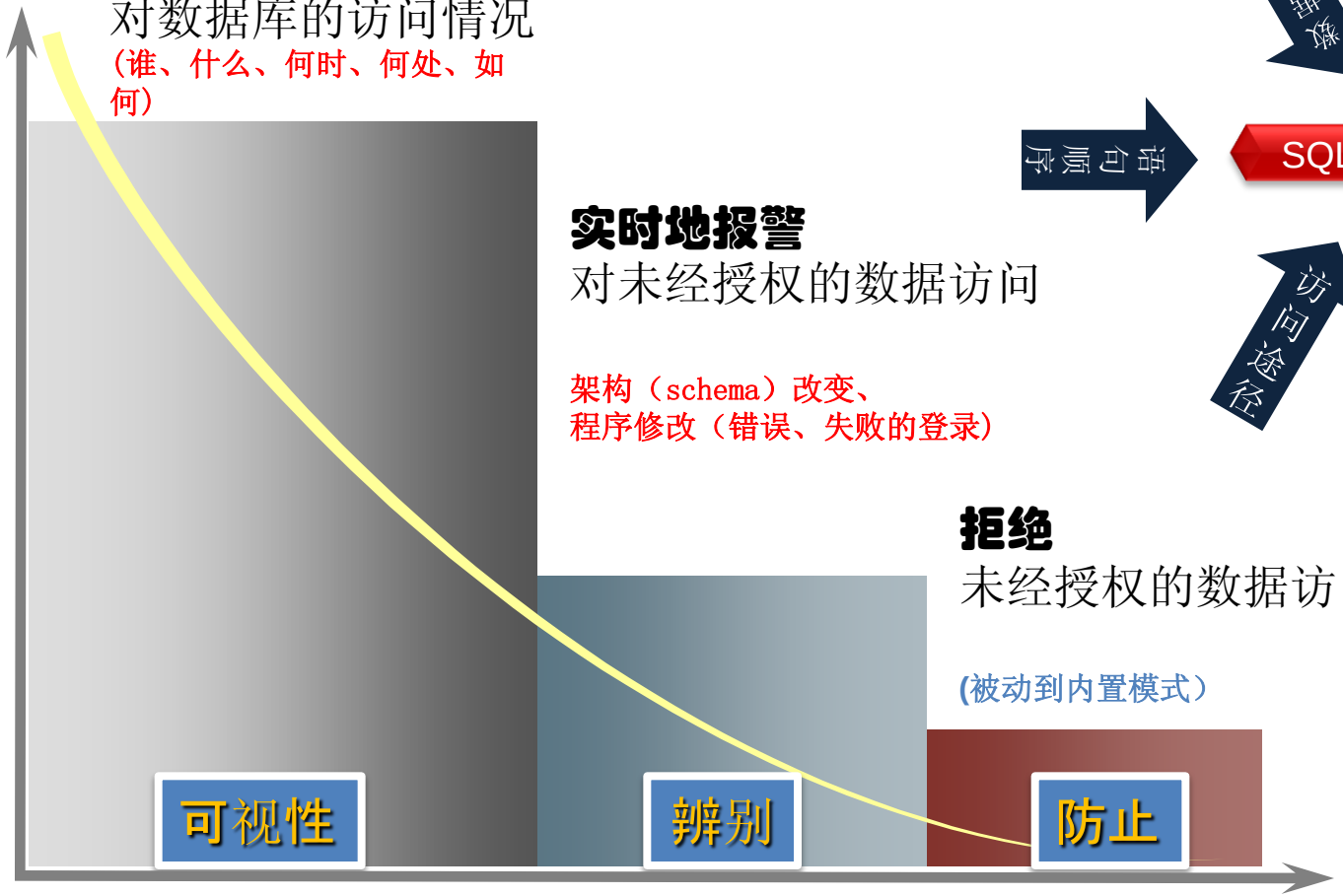


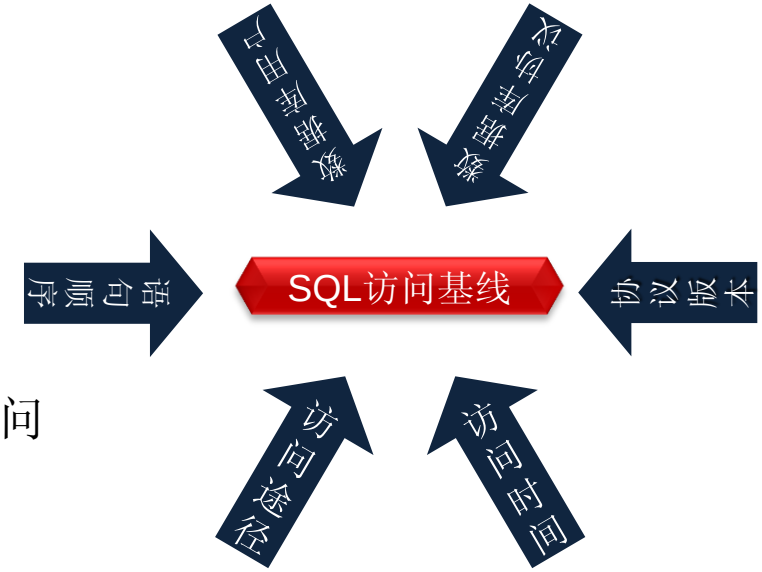
数据库安全--8步最佳实践



Guardium

数据库审计方法：建立基线、持续改进



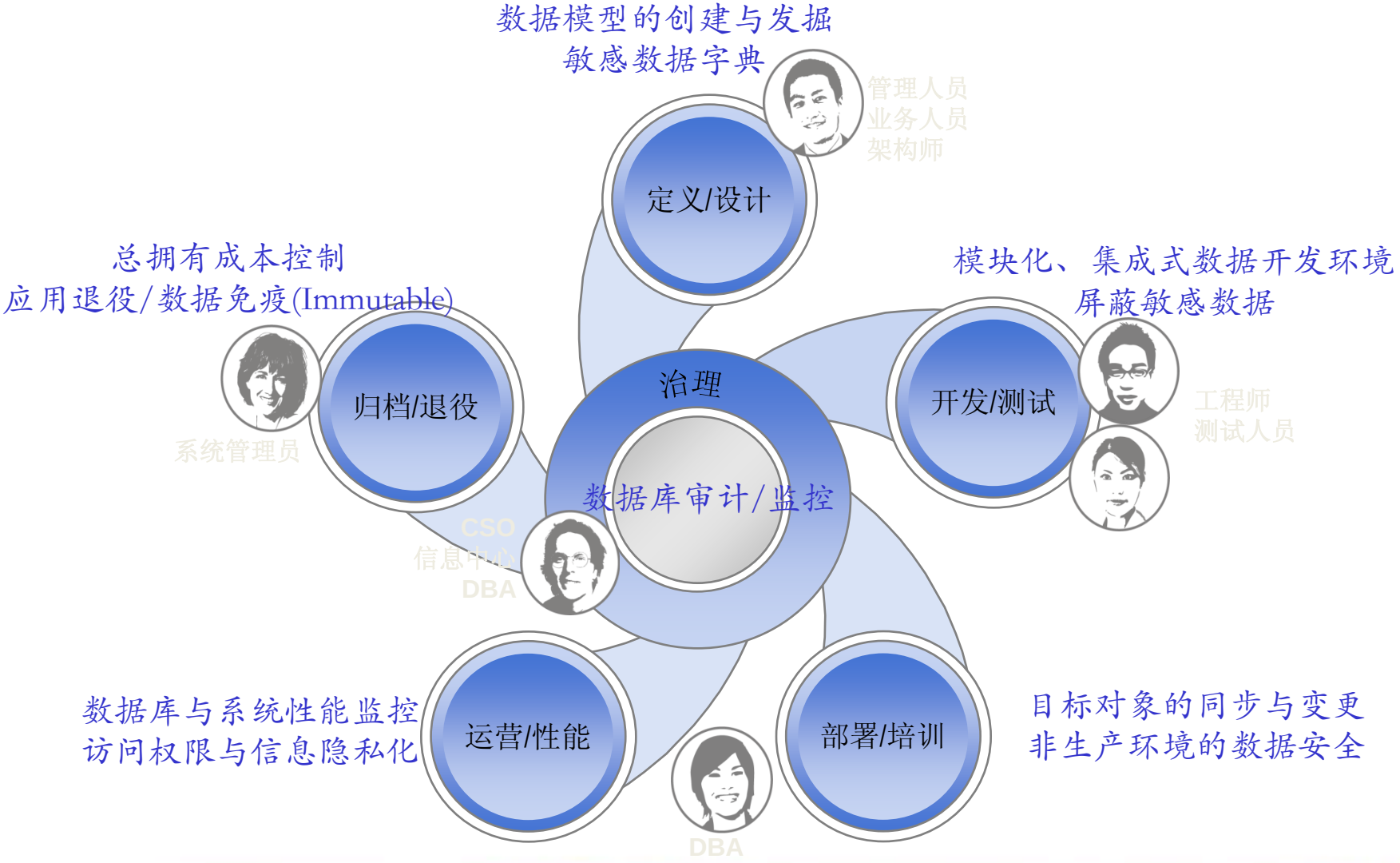


常用的数据库活动审计

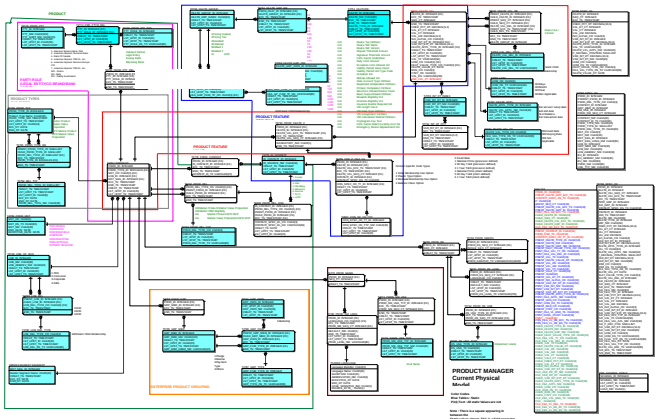
	特权用户	最终用户	开发及应用维护人员
数据库的登入/登出活动	✓	✓	✓
异常的数据库登入/登出	✓	✓	✓
数据库访问渠道		✓	
正常工作时间外的活动	✓	✓	✓
所有的DDL活动	✓		✓
存储过程和触发器的变化	✓		✓
权限及用户管理	✓		✓
数据库的链接和复制	✓		✓
重要数据的修改(DML)	✓	✓	✓
敏感数据的查询(SELECT)	✓	✓	✓
配置变更记录	✓		
审计系统本身的变化	✓		

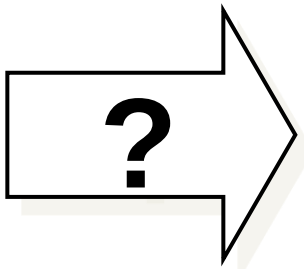
目录

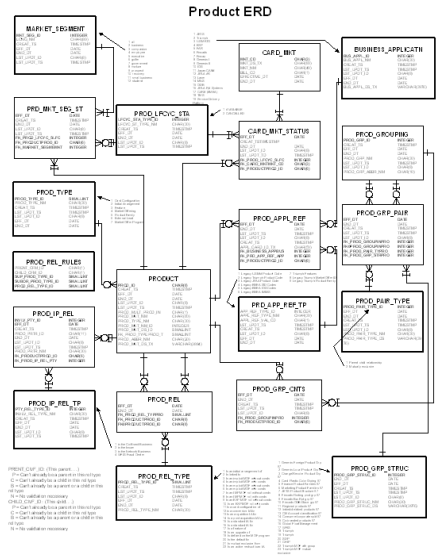
在生命周期的动态环境中解决数据治理课题



InfoSphere Discovery(模型发掘)

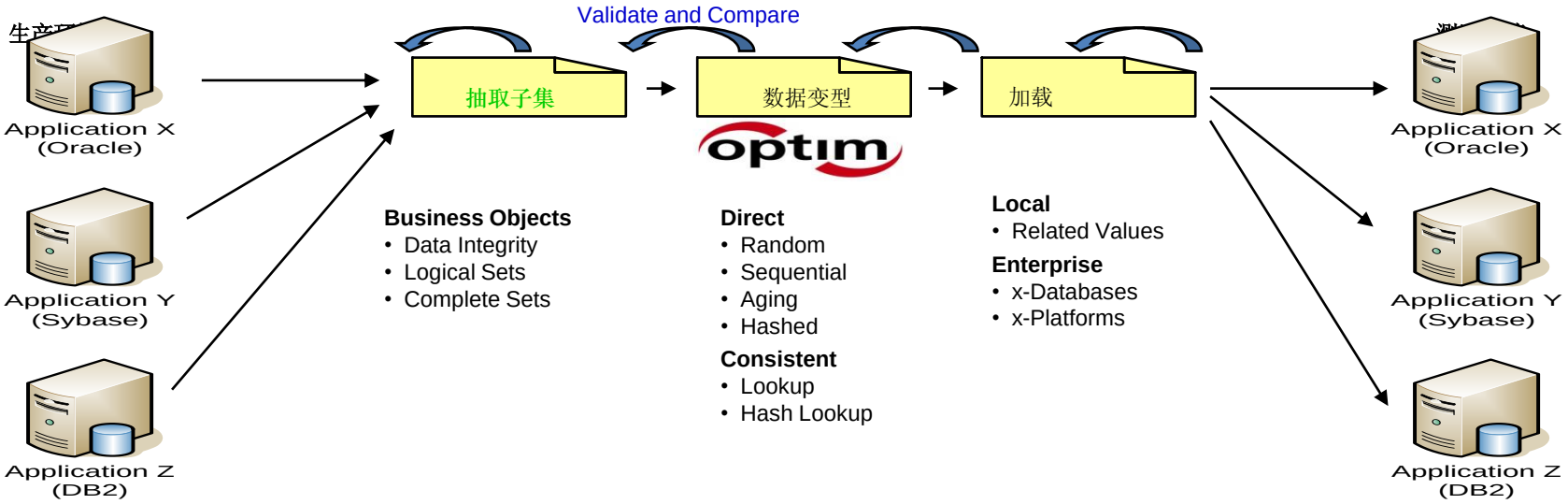






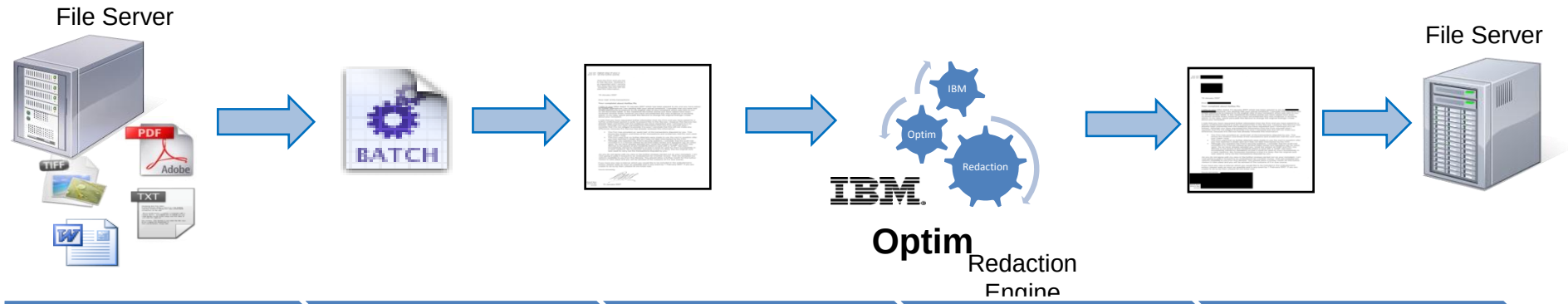
- 综述:适用于分析数据库中数值的内在联系找出数据模型的定义,特别是对数据关系逻辑是由应用层来维护的情况.例如,某两表间的关系是有数据转变的情况发生,表A与表B的关系是在A中记录字段”河北”时,A记录”冀”这种较复杂的关联.该方案的输出是数据关系模型.
- 用途:模型发掘往往占据数据项目实施70%的时间,如,BI、EAI、系统合并/升级等.完整的数据模型有利于定义敏感数据字典、信息隐私化、元数据管理、以至企业信息安全意义重大

Optim TDM(测试数据管理)



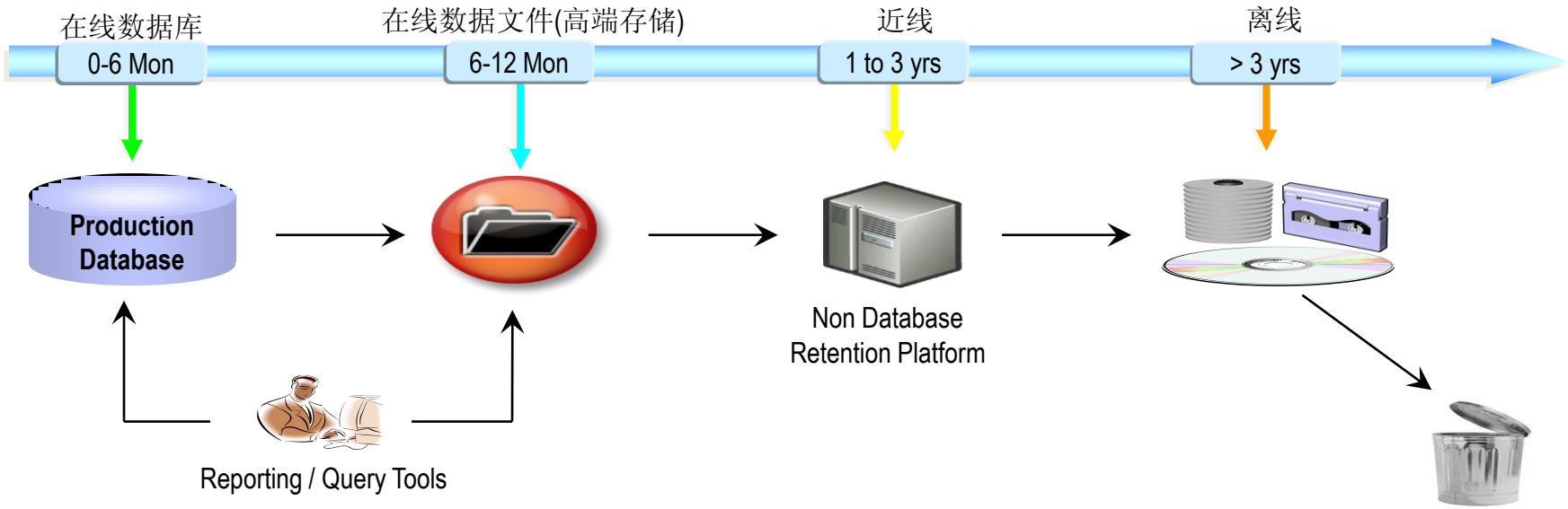
- 综述:应用系统升级换代过程中需要大量数据进行各种测试,通过生产数据全复制给管理带来许多困难.如数据再利用率低、测试过程相互干扰、测试前与测试后数据无法跟踪、甚至出现数据泄密等. Optim TDM提供了从数据抽取、子集生成、数据变形、加载、及测试数据前后比较等一系列完整的功能.
- 用途:系统测试是保障新应用按计划上线的关键步骤,测试数据管理在企业IT进程中是必须的,尤其是在企业系统融合的过程.在这一过程中新应用将取代旧应用的一或多个应用,无论如何新应用的测试数据都需要与现有应用不同的数据进行测试.无疑,测试数据管理是企业IT管理平台要面对的课题,而非仅仅各项目组能够解决的.

Optim Redaction(在线信息隐私化)



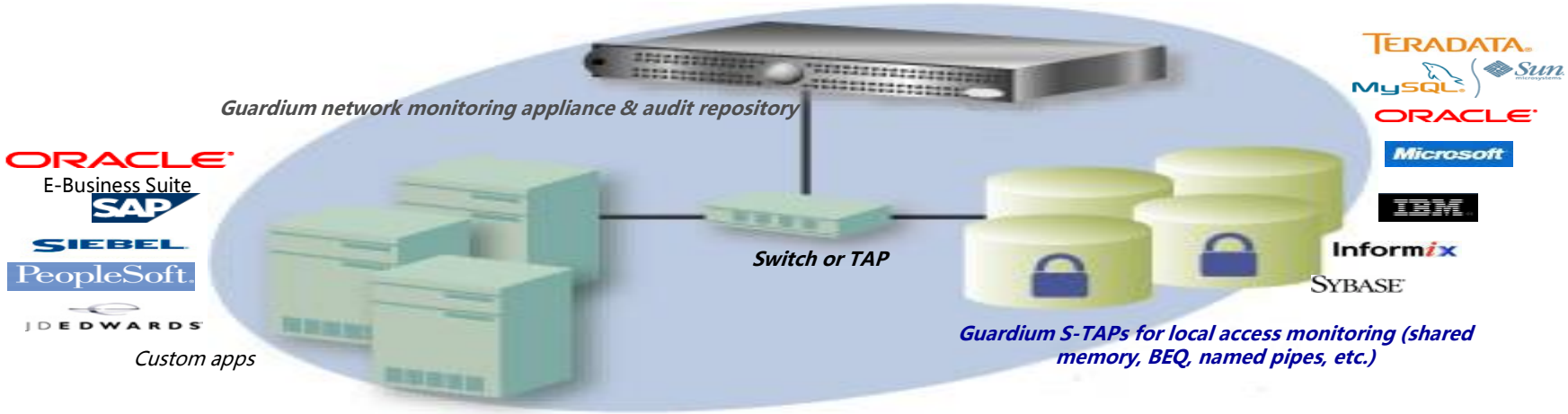
- 综述:Optim Redaction为企业提供了信息安全的有效手段.该方案提供的功能有:在数据迁移的过程中进行隐私化处理、对数据库中的所有或部分数据进行变形处理、及对文档资料中的敏感数据进行隐私化处理。
- 用途:对生产数据进行加密是保证企业信息安全手段之一,然而在实际应用中却并非切实可行。如；对生产数据加密虽然能够防止信息泄密，但因要对许多应用进行改造而无法实施。在现有应用访问权限和设立必要的信息安全规则的情况下，Optim Redaction为企业的信息安全提供了强有力的保障和切实可行的方案。

Optim Archive(数据归档)



- 综述:通过对数据实体（如：订单由10张数据表构成）的定义，Optim Archive是目前市场上唯一提供数据归档的方案。该方案不仅将历史数据有效的分离出生产系统，同时保证归档数据可查询。经过压缩后还可节约大量存储空间。更为重要的该方案提供数据免疫功能，即归档数据不可再改动，为审计真实性提供有利保障。当需要将归档数据恢复时， Optim Archive可将数据恢复至甚至是不同的数据库中。
- 用途:数据归档是信息生命周期管理的最佳实践。把数据转化为可查询文件数据库后，企业能够将归档数据连同其它文件形式一起，集成分级存储管理软件最大限度控制信息生命周期管理的总拥有成本。

Guardium(数据库活动监控)



- 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:网络是数据库活动流量的载体，Guardium结合企业信息安全规范捕获网络中相关的数据库操作，经过加工整理提供实时报警、跟踪报告、及数据库安全隐患分析等。Guardium采用的是网络旁路方式捕获数据库操作的，因此对系统性能影响很小。
- 用途:根据数据治理原理，信息安全是由隐私化和审计两领域共同完成的。隐私化（如：Optim Redaction)在最大限度保障信息泄密，而Guardium的监控可对正在发生的和可能会发生违反企业安全规范的数据操作进行有效的控制。这些操作包括：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)。


Thank
You