

# Oracle 数据库高级安全特性

许您一个安全的未来

公益讲座11: 00准时开始, 请大家先浏览云技术微信公众号技术文章。资料会在各群同步发布, 已入群客户请勿重复入群!



20-20

数据库和云讲座群



甲骨文云技术公众号



B站专家系列课程



# 基于 Oracle 数据库 免费企业数据健康检查

- 及时了解数据库健康状况，发现并解决潜在问题
- 维护数据库系统良好状态，保护数据资产的安全
- 提升数据库性能、稳定性和安全性，降低业务风险

免费咨询热线：

**400-699-8888**

\* 活动最终解释权归甲骨文公司所有

# Oracle 数据库高级安全特性， 许您一个安全的未来

甲骨文技术公益课 - 数据库专场

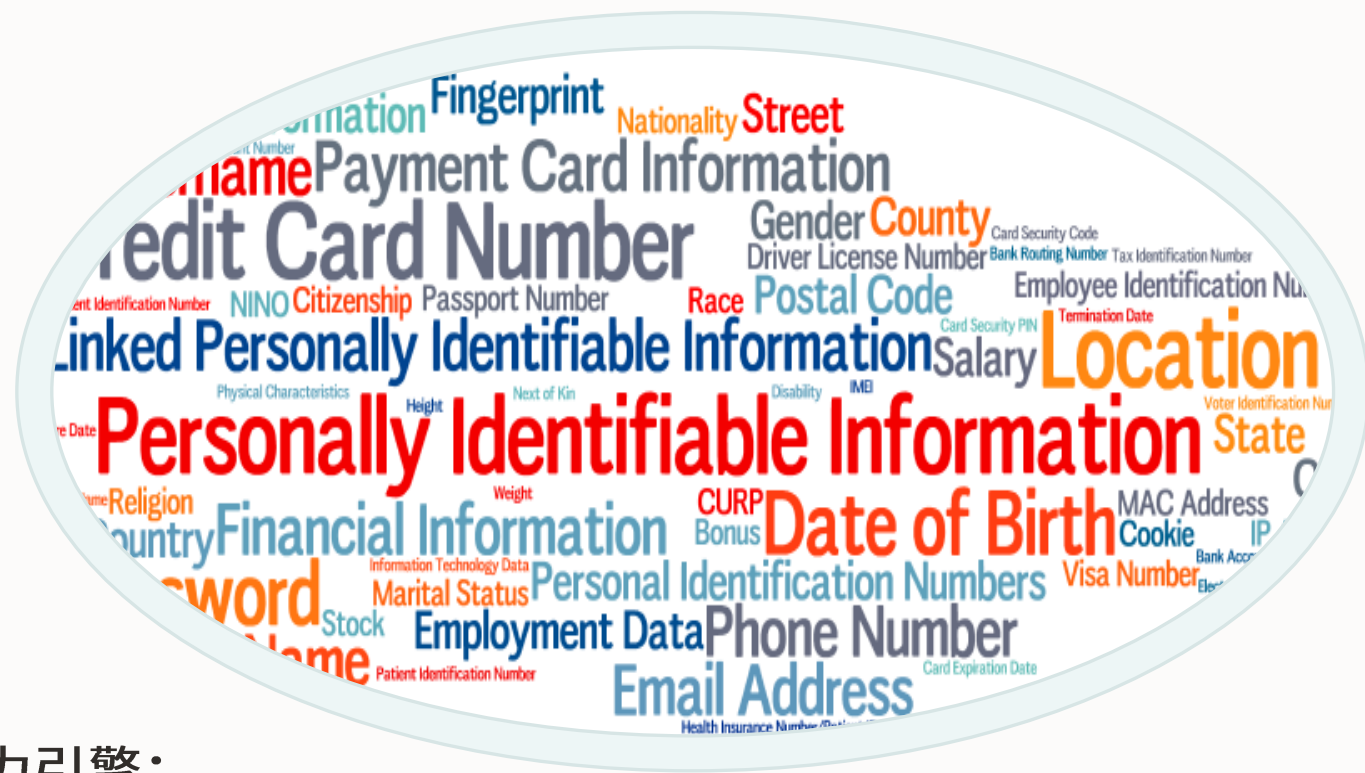
2023 年 4 月 7 日 11:00

线上直播

# 数据是我们非常宝贵的资产

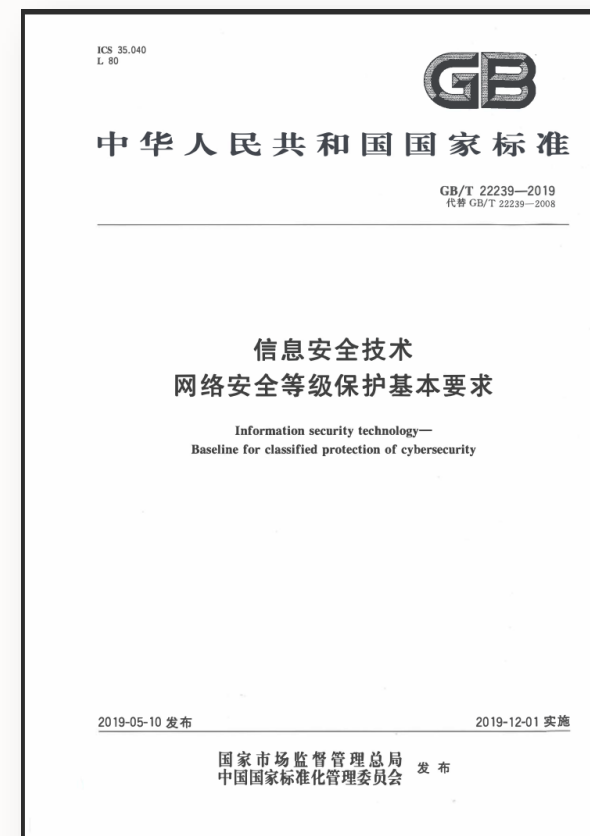
- 数据产生自任何人，但是有很多人对它感兴趣
- 数据只需生成一次，就可以轻松无休止地进行读取/复制
- 数据合并后变得更加有价值
- 数据价值由时间和目标决定
- 数据被篡改（或伪造）可能导致错误的决策

数据库是企业数据资产的主要载体和动力引擎；保护数据安全、为重要信息提供安全防护成为全球任何组织都需要面对的问题。



# 信息安全与等保2.0

- 2017年6月1日，《网络安全法》正式实施。
  - 《网络安全法》第21条明确“国家实行网络安全等级保护制度”。
  - 《网络安全法》第31条明确“国家对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。
  - 信息系统**安全**保护已上升到**法律**高度。
- 2019年12月1日，《信息安全技术网络安全等级保护基本要求》GB/T22239-2019 正式实施，开启**等保2.0**时代。



## 等保2.0 中关于**数据加密**的解读

《网络安全法》— 第三章-第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

(4) 采取数据分类、重要数据备份和**加密**等措施；

《网络安全法》— 第四章-第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

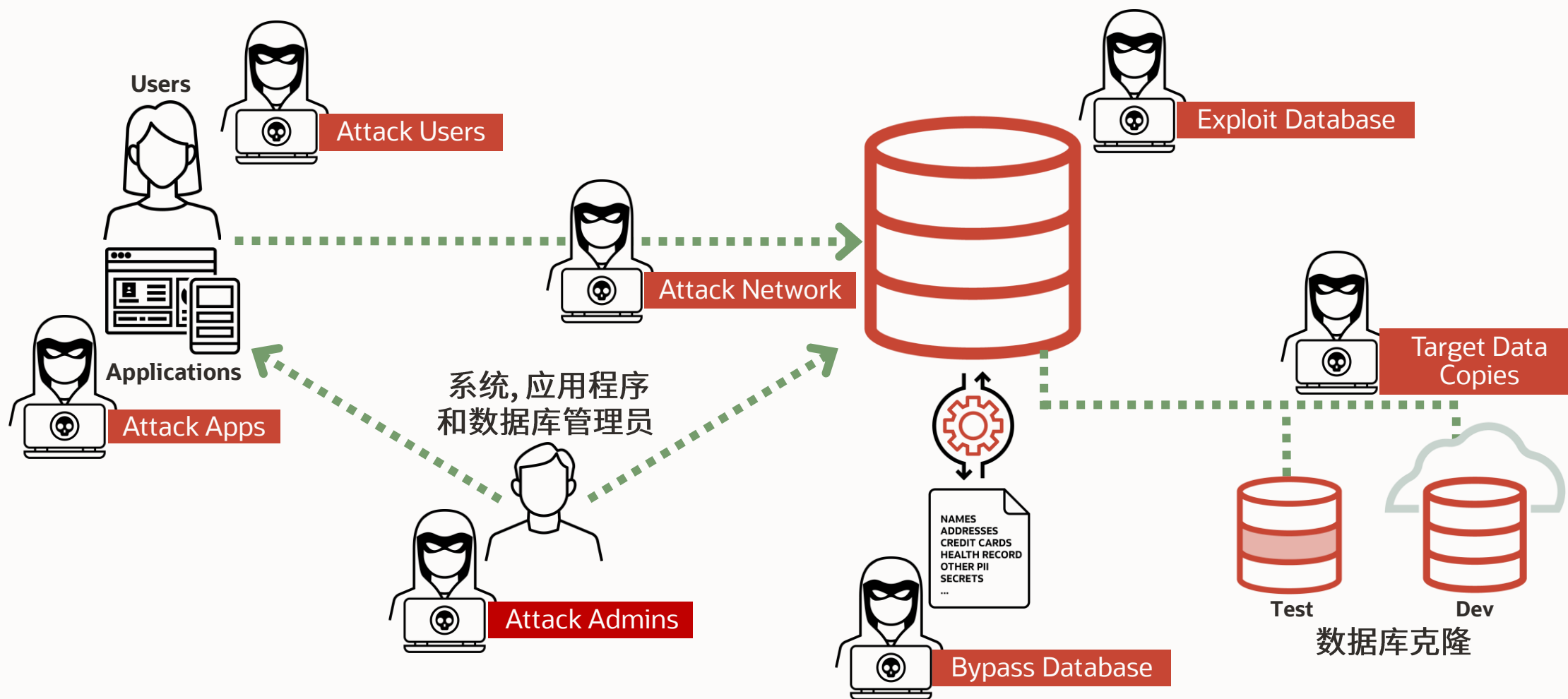
《信息安全技术网络安全等级保护基本要求》GB/T22239-2019 中8.1.4.7节和9.1.4.7节对三级和四级安全的数据完整性要求 —

- a) 应采用**密码技术**保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
- b) 应采用**密码技术**保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

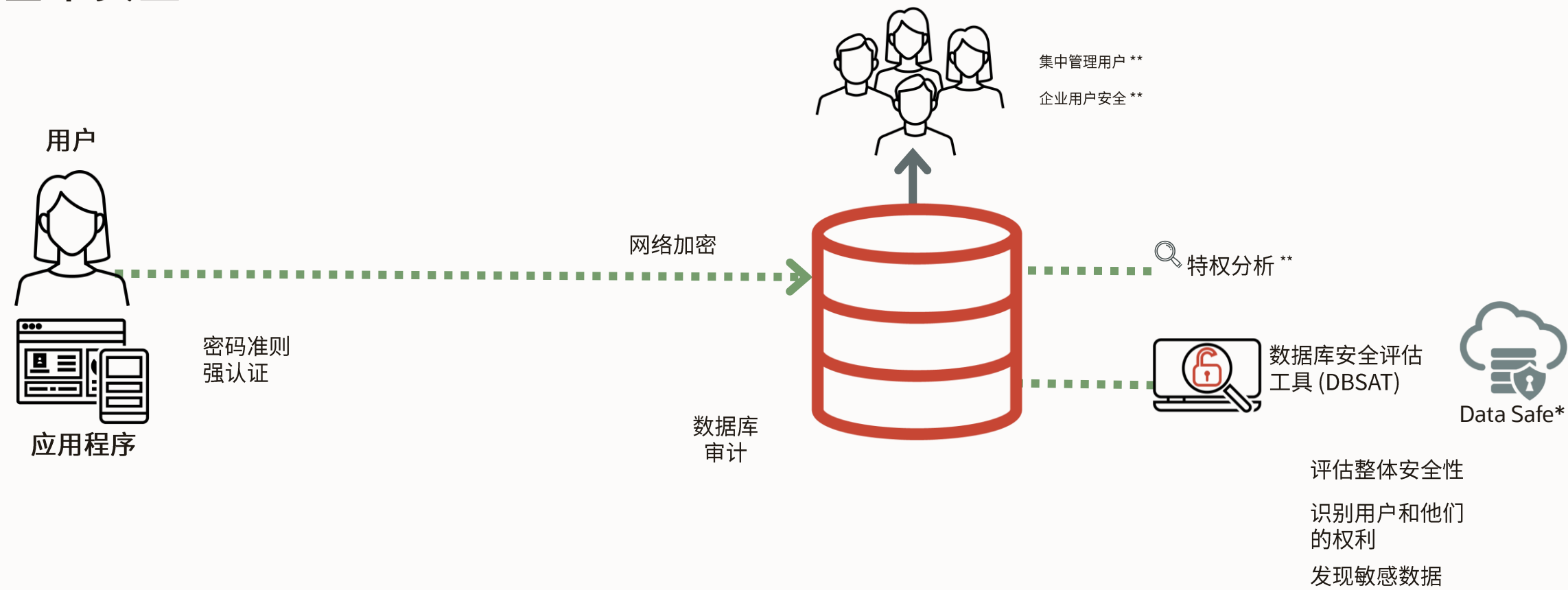
《信息安全技术网络安全等级保护基本要求》GB/T22239-2019 中8.1.4.8节和9.1.4.8节对三级和四级安全的数据保密性要求 —

- a) 应采用**密码技术**保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
- b) 应采用**密码技术**保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

# 黑客如何攻击数据库？



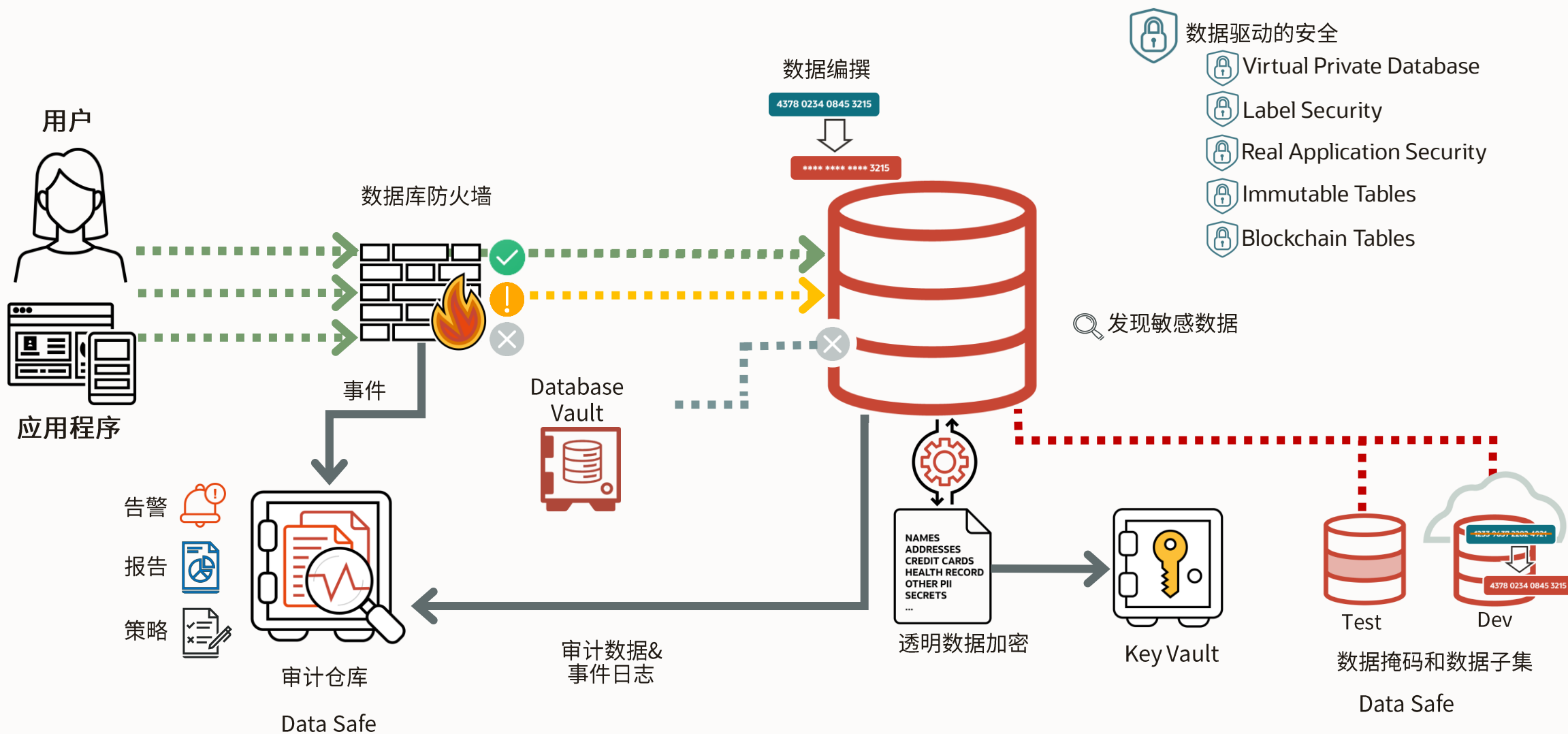
# 基本安全



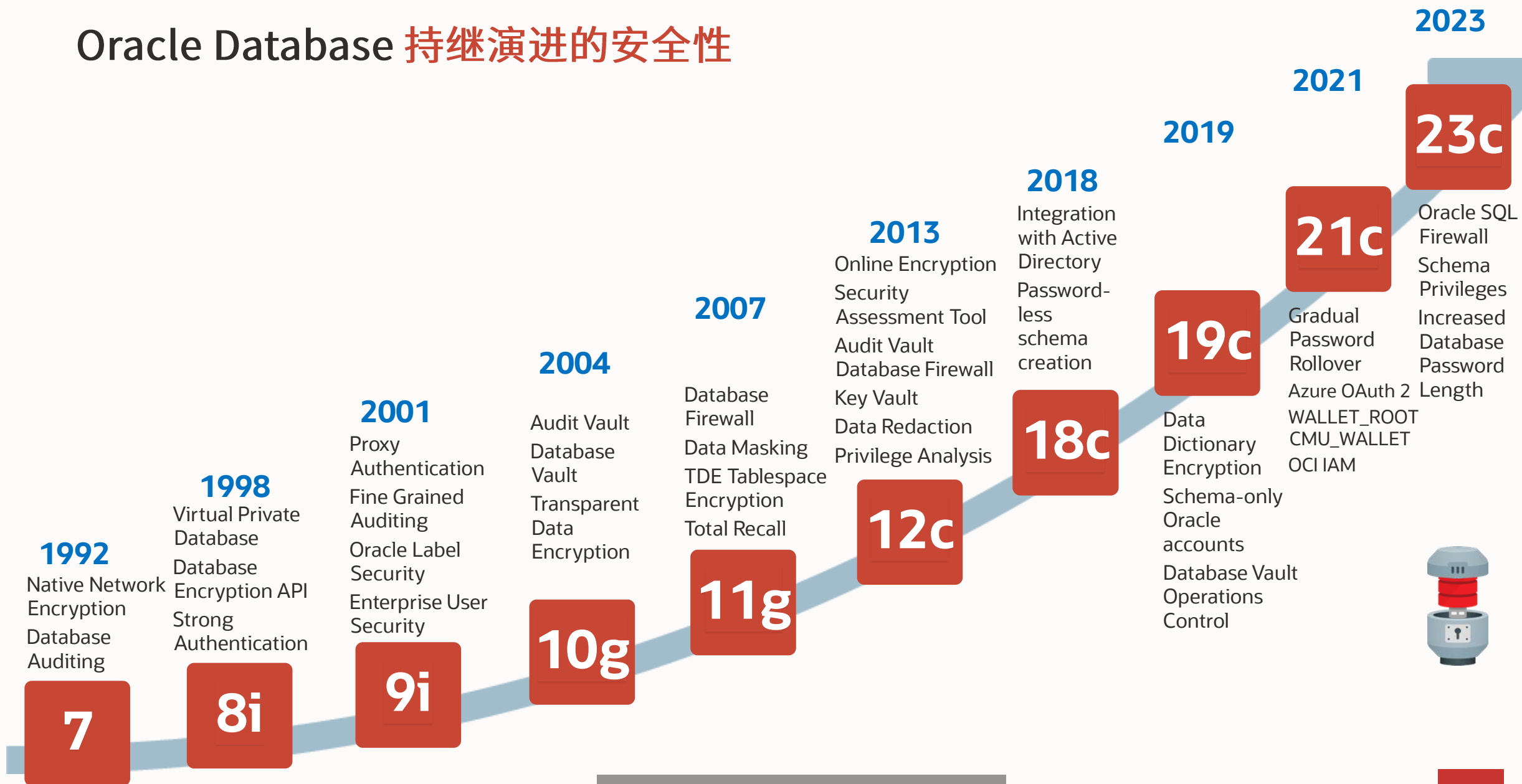
\* Included with Database Cloud, additional cost on-premises  
\*\* Only available with Enterprise Edition



# 高安全架构



# Oracle Database 持续演进的安全性



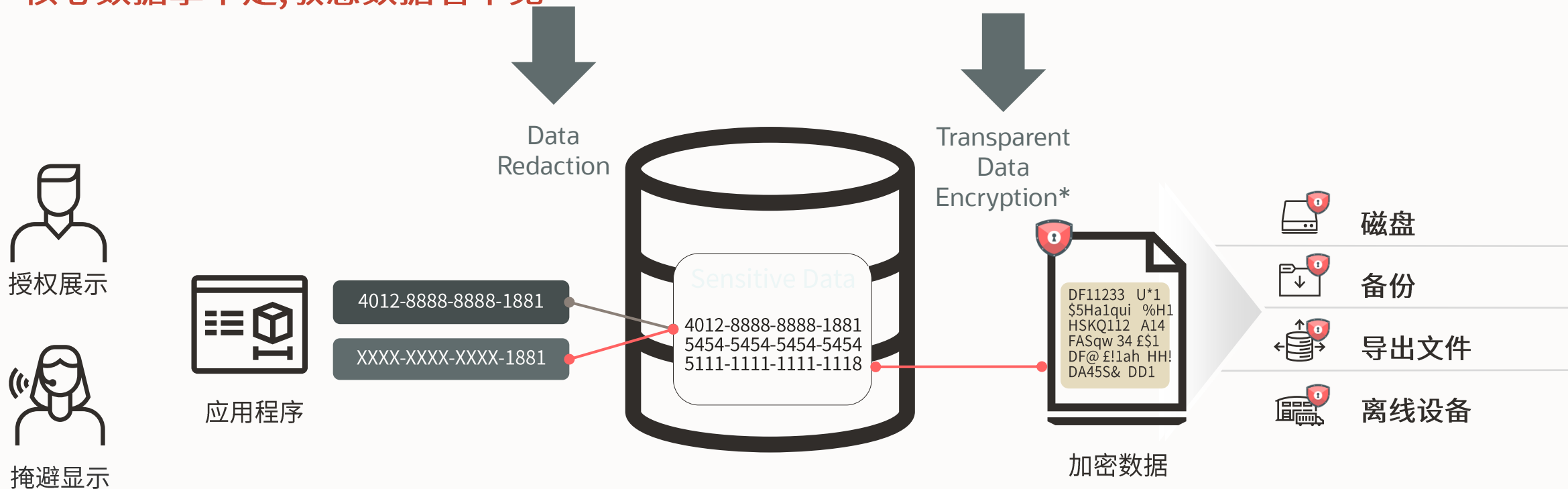
# Oracle 19c提供更强的安全性，满足等保2.0的要求

- Oracle 数据字典加密(SYSTEM, SYSAUX, TEMP, UNDO)
- 以AES192, AES256, ARIA, 3DES 加密离线表空间
- 更新 FIPS 加密库
- Database Vault 操作控制防止云DBA访问PDB数据
- 审计 top-level 用户行为
- Schema-Only Accounts
- 跨主备库单一登录失败计数



# 高级安全特性

核心数据拿不走,敏感数据看不见

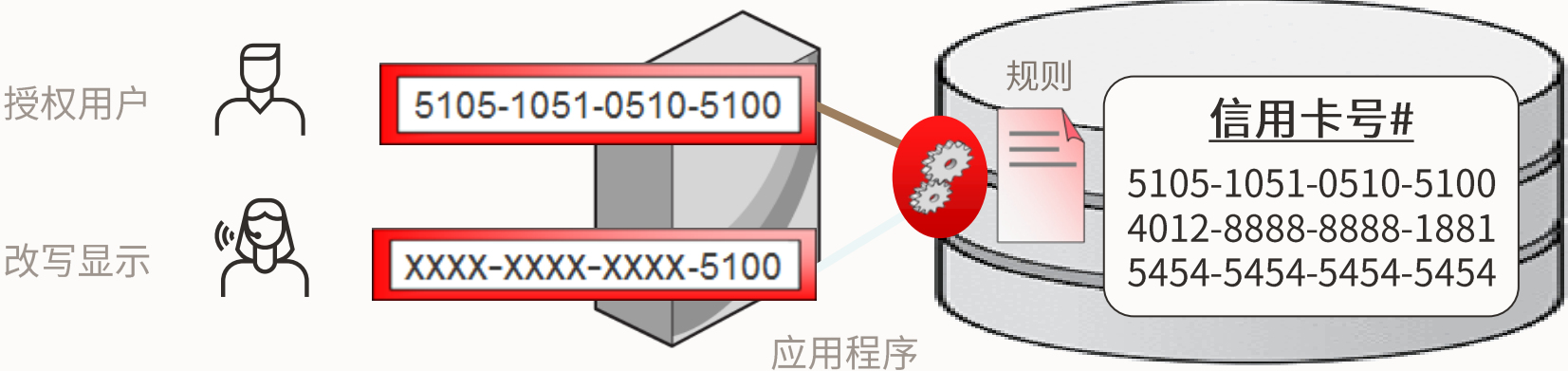


- 防范数据泄露的主动性防御数据库加固选件
- 功能上实现两种类型加密
  - 透明加密 (TDE)
  - 面向展现层的编纂加密 (Redaction)
- 性能高、部署配置简单

\* TDE在默认情况下可用于所有Oracle云数据库

# 高级安全 – 实时编纂 (Redaction) 加密敏感数据

为应用实时改写敏感数据

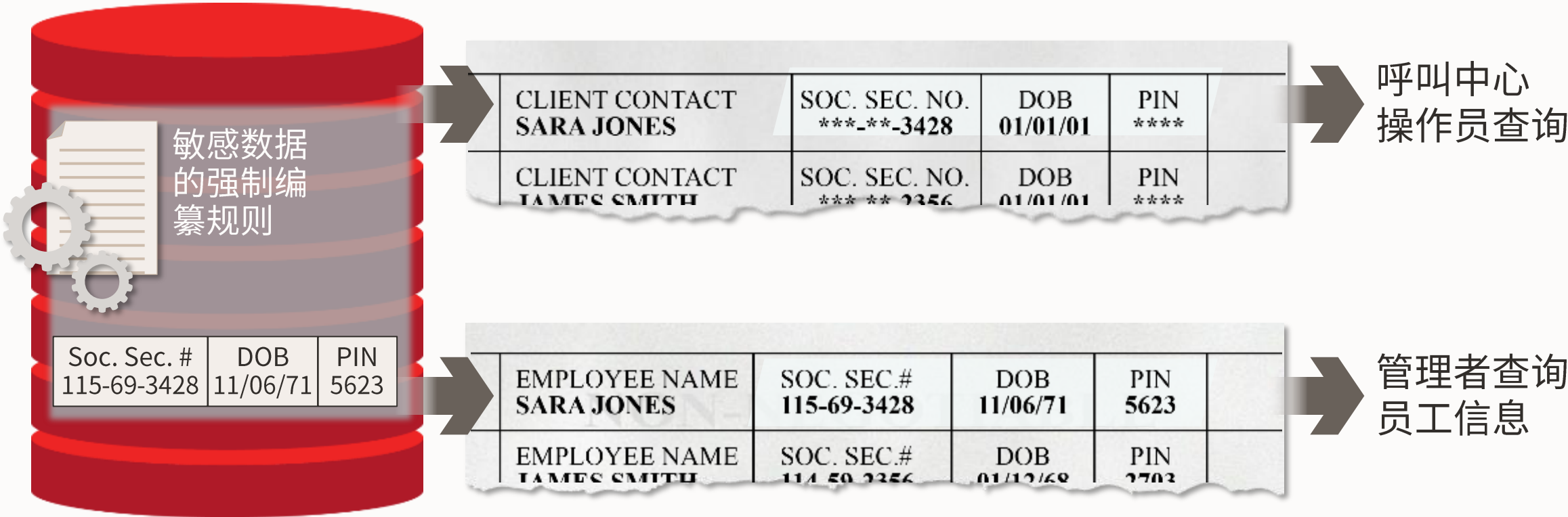


- 根据用户名、IP地址、应用程序上下文,和其他因素即时改写
- 跨应用高度透明的实施和使用
- 对生产负载影响可忽略

呼叫中心  
决策支持系统  
HCM 应用



# Data Redaction (12c以上版本)

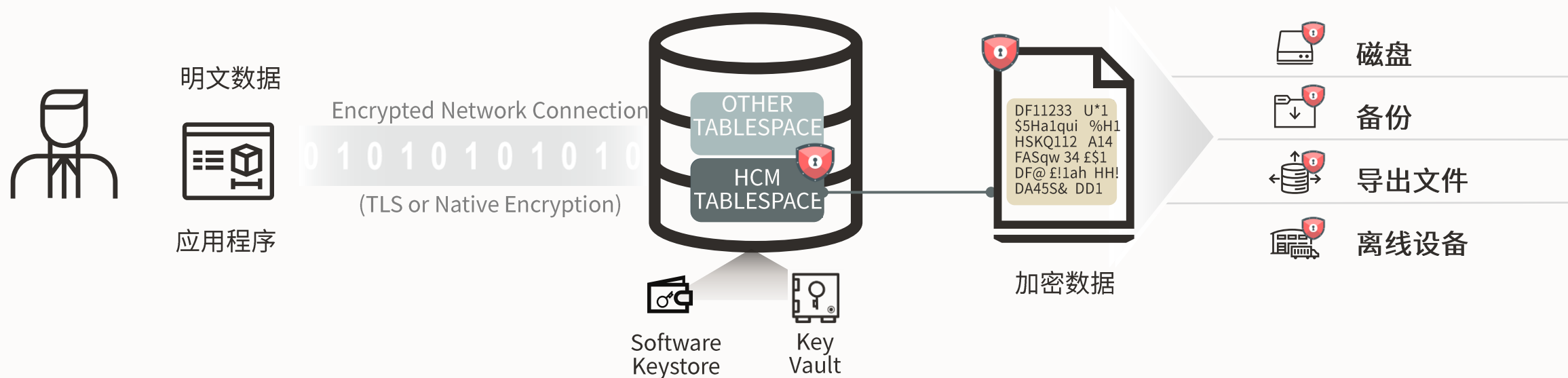


- 依据法律法规要求，保护客户与员工的个人隐私等敏感数据在非授权下的显示泄露
- 在应用、查询和报表中的实时编辑数据
- 避免改变应用程序、查询和报表



# 高级安全 - 透明数据加密 (TDE)

## 预防控制数据存储泄密



加密整个应用程序表空间或应用程序列  
保护磁盘上和备份中的数据库文件  
无需更改应用程序  
与Oracle技术栈相集成  
内置密钥管理

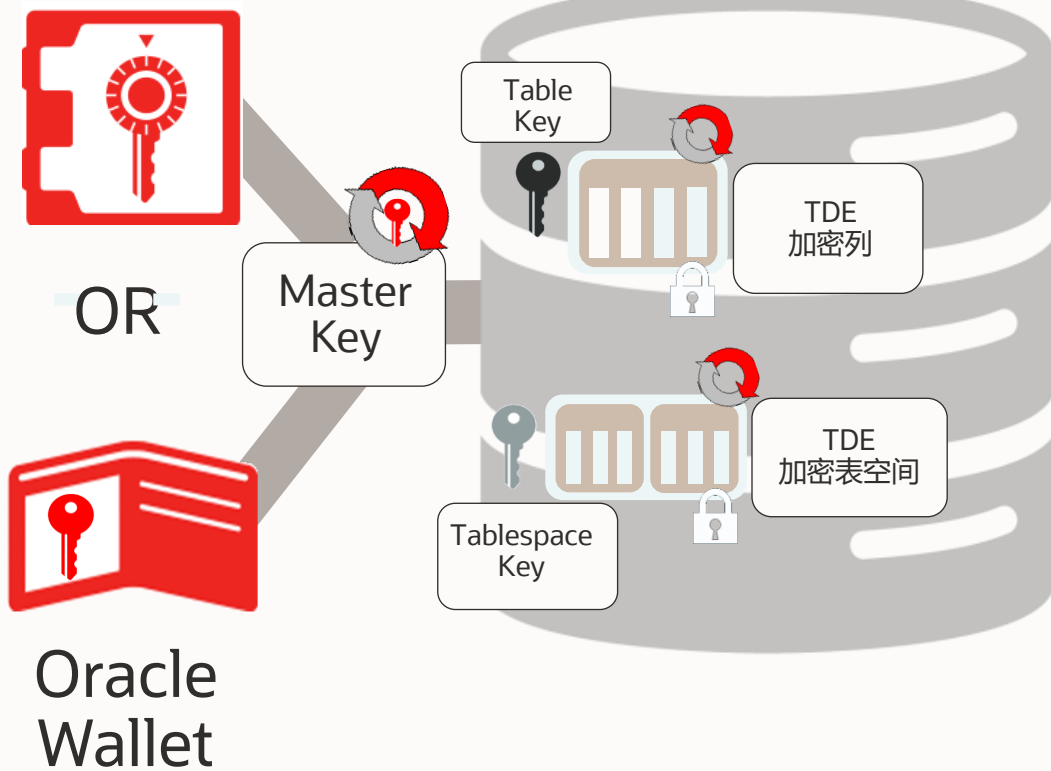
## 技术概念说明：透明数据加密

- TDE 既可以对像信用卡号和社会保险号这样的个别应用程序表列进行加密，也可以加密整个表空间，在存储介质或数据文件被盗的情况下也**不会泄露敏感数据**。
- 存储在加密表空间中的所有数据都将自动加密，**性能高效**。
- 备份数据库时，加密的文件在介质上仍保持其**加密**状态，即使**备份介质**丢失或被盗仍然能保护的信息不会外泄。
- TDE 表空间加密可以无缝地与 Oracle Streams、Oracle Compression 和 Oracle Exadata Smart Scans 协同工作。
- 由于压缩而实现的存储节省将维持不变，因为压缩过程完成后才对数据进行加密。
- 安全文件/LOBs的透明加密 (11g以上)
- 硬件安全模块(HSM)整合 (11g以上)
- 包括数据字典在内的**所有Oracle表空间** (19c)
- 内置密钥管理，**应用透明**，易于实施
- 帮助用户解决与安全性相关的**法规遵从**问题

# Oracle TDE 关键架构

- 数据的加密密钥（Key）由TDE自动创建和管理
- 主密钥（master encryption key）加密数据的加密密钥（data encryption keys）
- 主密钥（master encryption key）通常存储在 Oracle Wallet 或 Oracle 密钥库中

## Oracle Key Vault



# TDE与Oracle数据库技术栈相集成

| 数据库技术                | 集成点示例                                                          | TDE 支持 |
|----------------------|----------------------------------------------------------------|--------|
| High Availability    | Real Application Clusters, Sharding, (Active) Data Guard       | ✓      |
| Backup and Restore   | Oracle RMAN, Oracle Secure Backup                              | ✓      |
| Import and Export    | Oracle Data Pump                                               | ✓      |
| Database Replication | Oracle GoldenGate                                              | ✓      |
| Pluggable Databases  | Oracle Multitenant Option                                      | ✓      |
| Engineered Systems   | Oracle Exadata Smart Scan                                      | ✓      |
| Storage Management   | Oracle ACFS                                                    | ✓      |
| Data Compression     | Oracle Standard, Advanced, Exadata Hybrid Columnar Compression | ✓      |



# 表空间与列加密

TDE可以加密单个表列和表空间

加密表空间的优点：

- 无需跟踪要加密的列和列特性（如索引和约束）
- 不干扰Exadata混合列压缩（EHCC）或智能扫描技术
- 使用Intel（AES-NI）和SPARC CPU中的特殊指令加快加密操作，速度非常快

# 如何使用TDE

- 使用TDE不需要额外的安装
- 部署和配置TDE
  - 1) 设置一个keystore 并创建一个初始的master key
  - 2) 在数据库创建新的加密表空间或者将非加密表空间转换为加密表空间（12cR2以上支持在线迁移）、也可以在数据库中创建含有加密列的新表或者在原有表中启用加密列
- 所有步骤可以使用SQL命令或者通过Oracle Enterprise Manager 图形化界面完成
- 所有加入这些加密表空间的数据自动被加密存储；列加密可以应用在新表或已经存在的表中

# 示例：快速设置 TDE

1. 设置静态参数WALLET\_ROOT 为 wallet的存储目录，设置 TDE\_CONFIGURATION参数指定 keystore 的类型. (login as SYSDBA)

```
ALTER SYSTEM SET WALLET_ROOT = '$ORACLE_BASE/ADMIN/ORCL/WALLET' SCOPE =  
SPFILE SID = '*';  
ALTER SYSTEM SET TDE_CONFIGURATION="KEYSTORE_CONFIGURATION=FILE" SCOPE =  
BOTH SID = '*';
```

2. 创建 keystore (login as SYSKM)

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE IDENTIFIED BY password;
```

3. 打开wallet (keystore) (login as SYSKM)

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY password;
```

4. 设置主密钥 (login as SYSKM)

```
ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY password WITH BACKUP;
```

5. 开始使用TDE创建加密对象

## 示例：加密列值和表空间

- 对现有表中的列值进行加密

```
alter table credit_rating modify (person_id encrypt);
```

- 创建使用列加密的新表

```
create table orders (  
  order_id      number(12),  
  customer_id   number(12),  
  credit_card   varchar2(16) encrypt using 'AES256');
```

- 创建加密存储的表空间

```
CREATE TABLESPACE securespace_1  
DATAFILE '/home/user/oradata/secure01.dbf'  
SIZE 150M  
ENCRYPTION USING 'AES192' ENCRYPT;
```

# Oracle Wallet中管理Master Key注意事项

- 关键: 牢记wallet密码
- 关键: 不要删除wallet。即使采用自动登录，也一定要保存好基于密码的wallet备份。
- 关键: 不要让多个数据库共享相同的wallet
- 设置一个强wallet密码：使用数字、大小写、长度大于等于12个字符……
- 大约每6个月轮换一次master encryption key 和 wallet 密码
- 初始创建wallet后立即备份
- 每次key轮换操作之前和之后备份wallet
- 自动打开的Wallet备份和加密数据的备份要分开保存
- 限制wallet目录和文件的访问权限
- 保持wallet只读，设置不可变位
- 对于RAC, wallet存储于ACFS (DB 11gR2) 或ASM (DB 12c以上版本)
- 对于DB 12c以上版本, 使用SYSKM角色分离职责

## 对现有数据部署TDE

- 在线表空间转换(12.2以上)
- 离线表空间转换（11gR2以上）
- 维护期间离线迁移
  - Oracle DataPump Export / Import
  - Alter table move + alter index rebuild
  - Dbms\_metadata.get\_ddl + insert as select
  - Create table as select (CTAS)
- 接近零停机的在线迁移
  - Oracle Online Table Redefinition (DBMS\_REDEFINITION)
  - 对于 Oracle Database 11gR2 和12cR1，结合Data Pump 和 Data Guard

White Papers  
Available on OTN





## 演示——在线加密表空间



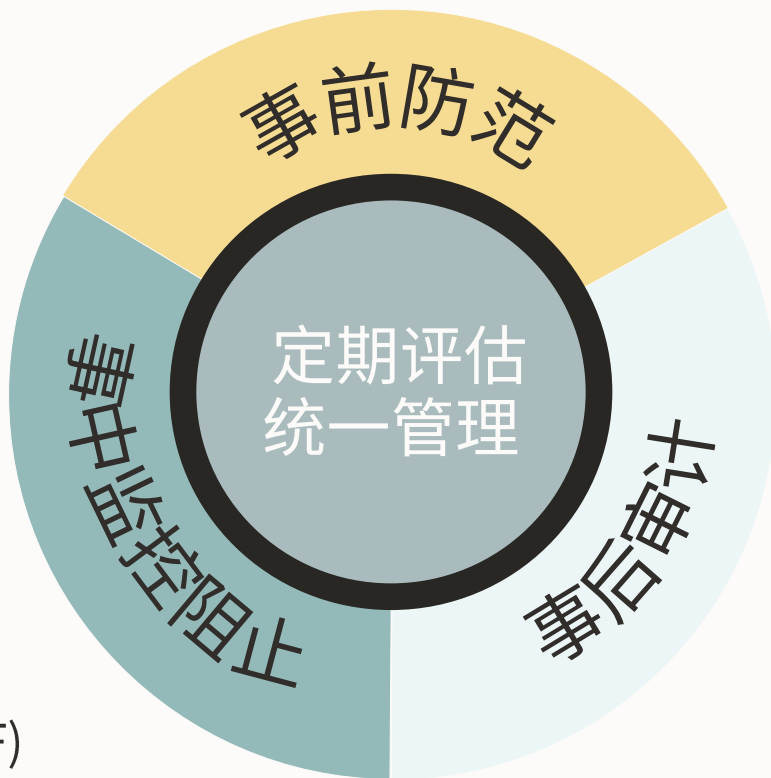
# Oracle数据库安全方案

## 事前防范

透明数据加密 (TDE)  
实时数据编纂 (Data Redaction)  
数据脱敏 (DM & Subsetting)  
特权分析 (PA)  
安全备份 (Secure Backup)

## 事中监控阻止

数据库保险库(DV)  
审计数据仓库与数据库防火墙(AVDF)



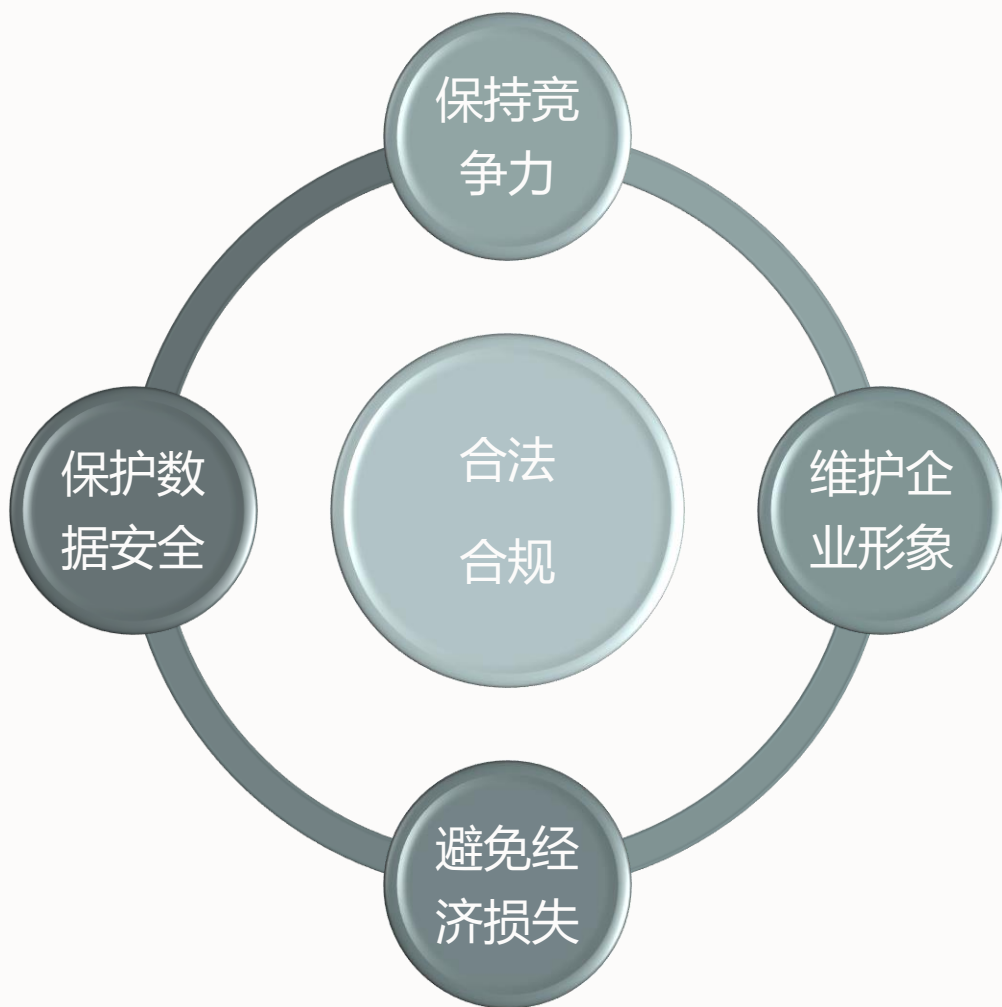
## 事后审计

审计数据仓库与数据库防火墙  
(AVDF)

## 定期评估/统一管理

数据库安全评估工具(DBSAT)  
数据库生命周期管理(DBLM)  
密钥保险库(Key Vault)





## Oracle数据库安全方案 保护您高价值的数据资产

## 更多资源

免费动手实验，帮助您学习如何使用不同的安全功能和选项



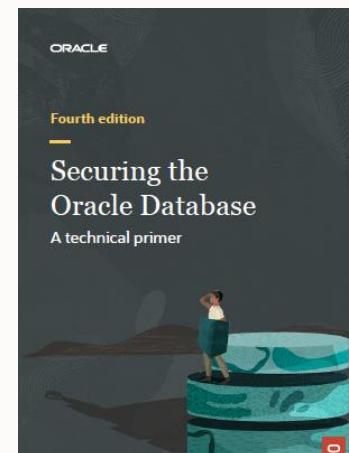
[bit.ly/golivelabsdbsec](https://bit.ly/golivelabsdbsec)

Database Security office hours –每月第二个星期三



[bit.ly/asktomdbsec](https://bit.ly/asktomdbsec)

《保护Oracle数据库-技术入门指南（第四版）》



[oracle.com/securingthedatabase](https://oracle.com/securingthedatabase)



ORACLE

Our mission is to help people see  
data in new ways, discover insights,  
unlock endless possibilities.



ORACLE  
甲骨文

# Oracle 19c新特性-ADG DML 重定向，应用双活新概念



范宏伟

- 资深解决方案工程师
- 电信行业机构师
- 15年以上数据相关工作经验

## 内容简介

- ADG对于业务连续性保障的价值
- Data Guard的技术演进及重要特性
- ADG DML重定向



Zoom直播

直播时间：4月14日 11:00 - 12:00

扫描二维码进入直播

Zoom ID: 976 6962 5763

密码: 98039717



微信扫一扫预约



20-20

数据库和云讲座群



甲骨文云技术公众号



技术专家1V1深入交流

