

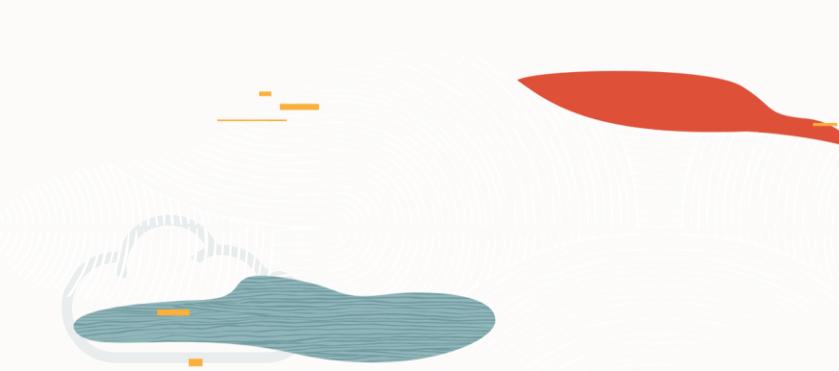
# 许你一个安全的未来：Oracle DB最高安全架构 之 高级安全特性

2020年4月10日上午11:00

李炜玉 甲骨文资深技术顾问

公益讲座11点准时开始，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！

扫码加入：  
19c新特性讲座群



欢迎关注：  
甲骨文云技术公众号





# 许你一个安全的未来： Oracle Database 最高安全架构 之 高级安全特性

---

**李炜玉**

资深技术顾问

甲骨文中国

April 10, 2020

## Safe harbor statement

---

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

# 议程

---

- 1 信息安全的重要性
- 2 Oracle数据库最高安全架构概览
- 3 19c数据库增强的安全特性
- 4 利用高级安全特性透明地加密数据
- 5 总结

# 数据是我们最宝贵的资产

... 而敏感数据就意味着￥

- 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“安全”事故不时发生.....

时间：2018年6月

泄露数据量：10亿

2018年6月19日，一位广泛关注，据称，这些信息。

根据消息显示，本次验证，发现在所购“单

当时暗网对外泄数据用户信息，而10亿条

重蹈覆辙，顺丰快递

时间：2018年7月

波及用户：约3亿

快递行业的数据泄露真  
据为顺丰的快递信息，

作为快递行业口碑最差  
条用户信息的打包价为2个比特币，当时市值约10万人民币。

华住集团5亿用户数据泄露

时间：2018年8月

泄露数据量：约5亿

2018年8月，根据曝  
美爵、禧玥、漫心、  
下酒店均有

Facebook 数据泄

时间:2018年3月

泄露数据量：约81

NATION-WORLD

## Capital One data breach: 100 million affected in the US

Capital One says the Social Security numbers for about 140,000 of its

### 数据泄露变得越来越大、越来越大胆

**新的目标：**数据收集者、财务会计公司、调查人员、安全公司、政府以及任何拥有敏感数据的人

**新目标类型：**数据库（主要来源）、设备、云.....

### 数据泄露对受害者、品牌和企业造成不可逆转的损害

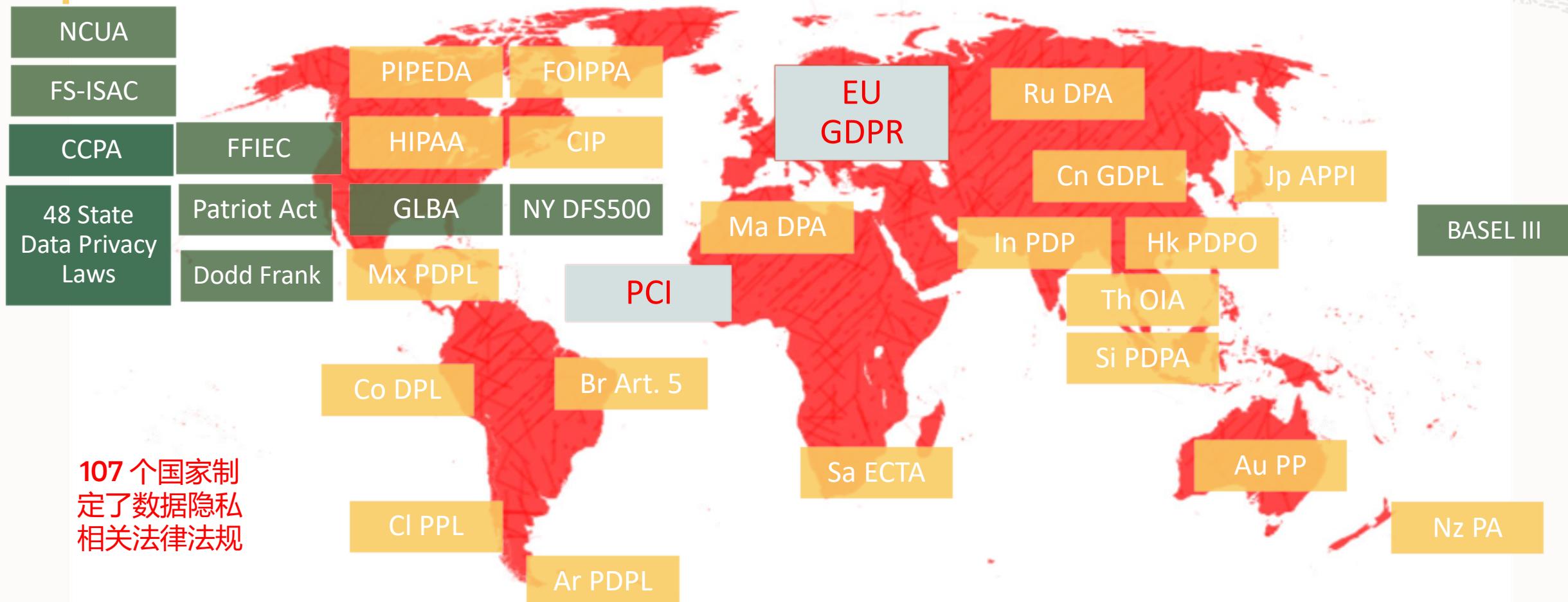
万豪集团步华住集团后尘

时间：2018年11月

泄露数据量：约5亿

指出，约有14万信用卡用户的社  
会安全号（SSN）被泄露，此外，有8万个与信用卡关联的  
银行账号（bank account numbers）也遭到了泄露！案件规模之大令人震惊，《今日美  
国》报道更指，这起事件已经成为了美国史上最大的10起信息泄露事件之一。

# 全球数据安全和隐私保护法律法规猛增



# 我国对数据安全和隐私保护越来越重视

名称	日期	部门
《网络安全法》	2017年6月1日起施行	人大
《网络安全等级保护条例（征求意见稿）》	2018年6月27日-2018年7月27日征求意见	公安部
《网络安全等级保护基本要求》等保2.0 GB/T22239-2019	2019年12月1日起实施	国家标准化管理委员会
《数据安全管理办办法（征求意见稿）》	2019年5月28日-2019年6月28日征求意见	国家互联网信息办公室
《个人信息安全规范（征求意见稿）》	2018年5月生效。2019年4月22日修改版	全国信息安全标准化技术委员会
《个人信息出境安全评估办法（征求意见稿）》	2019年6月13日-2019年7月13日征求意见	国家互联网信息办公室
《网络关键设备和网络安全专用产品相关国家标准要求（征求意见稿）》	2017年6月1日第一批目录生效。 2019年5月16日-2019年6月15日征求意见	全国信息安全标准化技术委员会
《关键信息基础设施安全保护条例（征求意见稿）》	2017年7月10日	国家互联网信息办公室

## 网络安全法获高票通过 明确加强个人信息保护

十二届全国人大常委会第二十四次会议11月7日上午经表决通过了《中华人民共和国网络安全法》



网络安全法的出台先后经过了全国人大常委会的三次审议

网络安全法共有7章79条  
内容上有6方面突出亮点

- ① 明确了网络空间主权的原则
- ② 明确了网络产品和服务提供者的安全义务
- ③ 明确了网络运营者的安全义务
- ④ 进一步完善了个人信息保护规则
- ⑤ 建立了关键信息基础设施安全保护制度
- ⑥ 确立了关键信息基础设施重要数据跨境传输的规则

该法自2017年6月1日起施行

新华社发（大果制图）

# 等保2.0的特点

- **二个全面覆盖**: 个人及家庭自建自用的网络除外
- 根据“**谁主管、谁运营，谁负责**”的原则，网络**运营者**成为等级保护的责任主体。**企业**需要对其建设、掌管、运营的各类系统的等保负责。
- 由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行**收集、存储、传输、交换、处理**的系统，被称为等级保护的对象。

一是覆盖各地区、各单位、各部门、各企业、各机构，  
即是覆盖全社会。

二是覆盖所有保护对象，包括网络、信息系统、信息，  
以及云平台、物联网、工控系统、大数据、移动互联等  
各类新技术应用。



## 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。

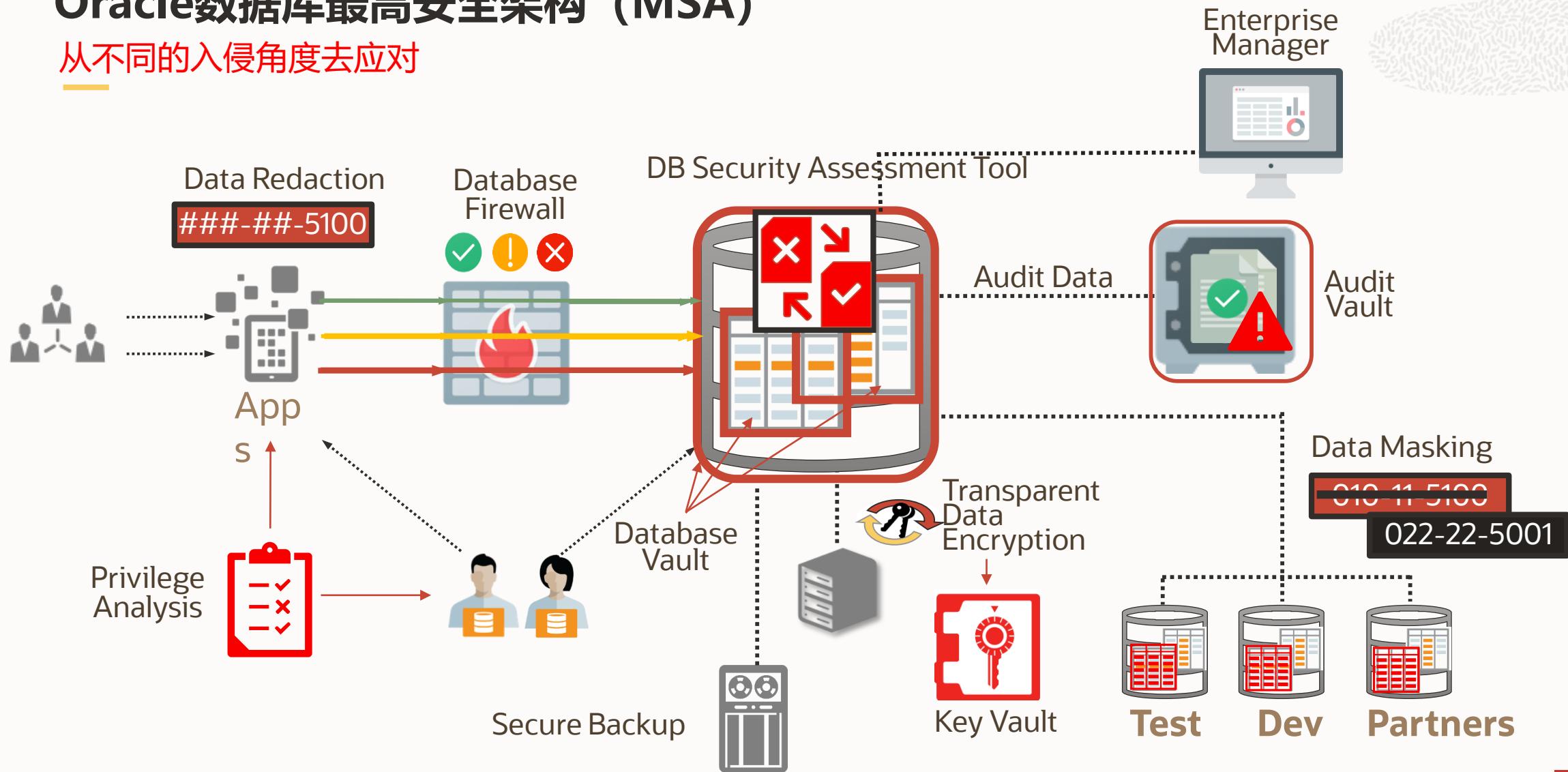
《网络安全等级保护条例（征求意见稿）》-第三章-第二十条【一般安全保护义务】网络运营者应当依法履行下列安全保护义务，保障网络和信息安全：（六）落实数据分类、重要数据备份和**加密**等措施；（七）依法收集、使用、处理个人信息，并落实个人信息保护措施，**防止个人信息泄露、损毁、篡改、窃取、丢失和滥用**；

《网络安全等级保护条例（征求意见稿）》-第三章-第三十一条【数据和信息安全保护】网络运营者应当建立并落实重要数据和个人信息安全保护制度；采取保护措施，**保障数据和信息在收集、存储、传输、使用、提供、销毁过程中的安全**；建立异地备份恢复等技术措施，保障重要数据的完整性、**保密性**和可用性。未经允许或授权，网络运营者不得收集与其提供的服务无关的数据和个人信息；不得违反法律、行政法规规定和双方约定收集、使用和处理数据和个人信息；**不得泄露、篡改、损毁其收集的数据和个人信息**；不得非授权访问、使用、提供数据和个人信息。

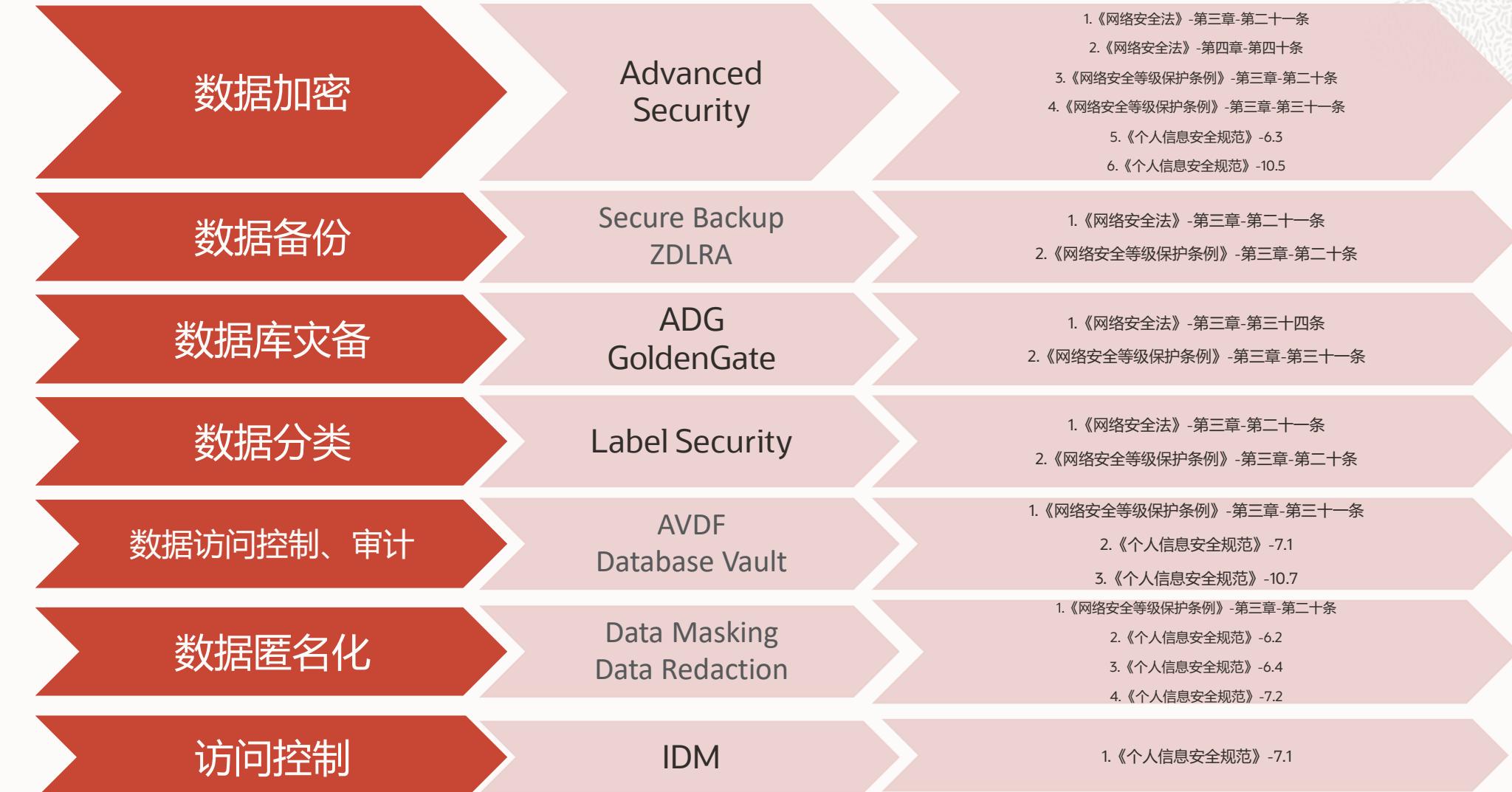


# Oracle数据库最高安全架构 (MSA)

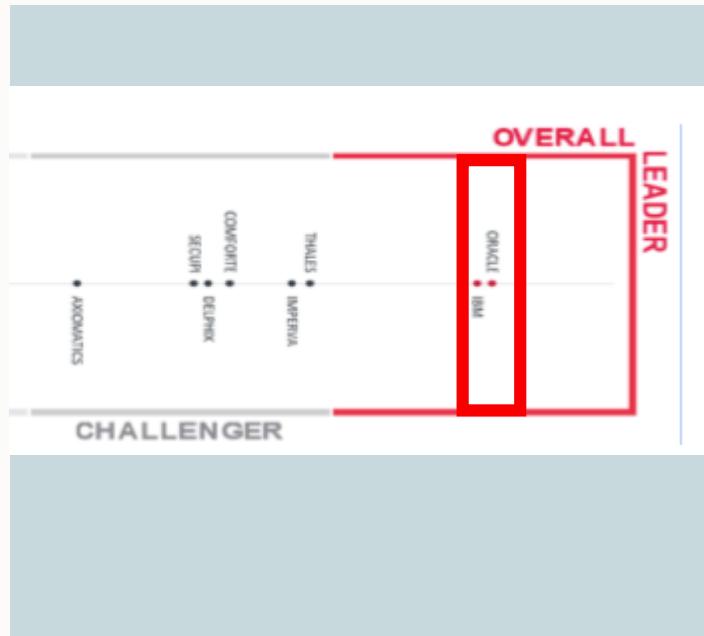
从不同的入侵角度去应对



# Oracle 数据安全解决方案助力网安法及等保2.0落地



# Oracle #1 最安全的数据库



KuppingerCole: *Database+Big Data Security Leadership Compass*, Jun '19

**Oracle #1** overall for Database & Big Data security



Forrester: *Database-as-a-Service Wave*, June 2019

**Oracle #1** “security” criterion (4.5/5)

<https://reprints.forrester.com/%23/assets/2/132/RES144407/reports>

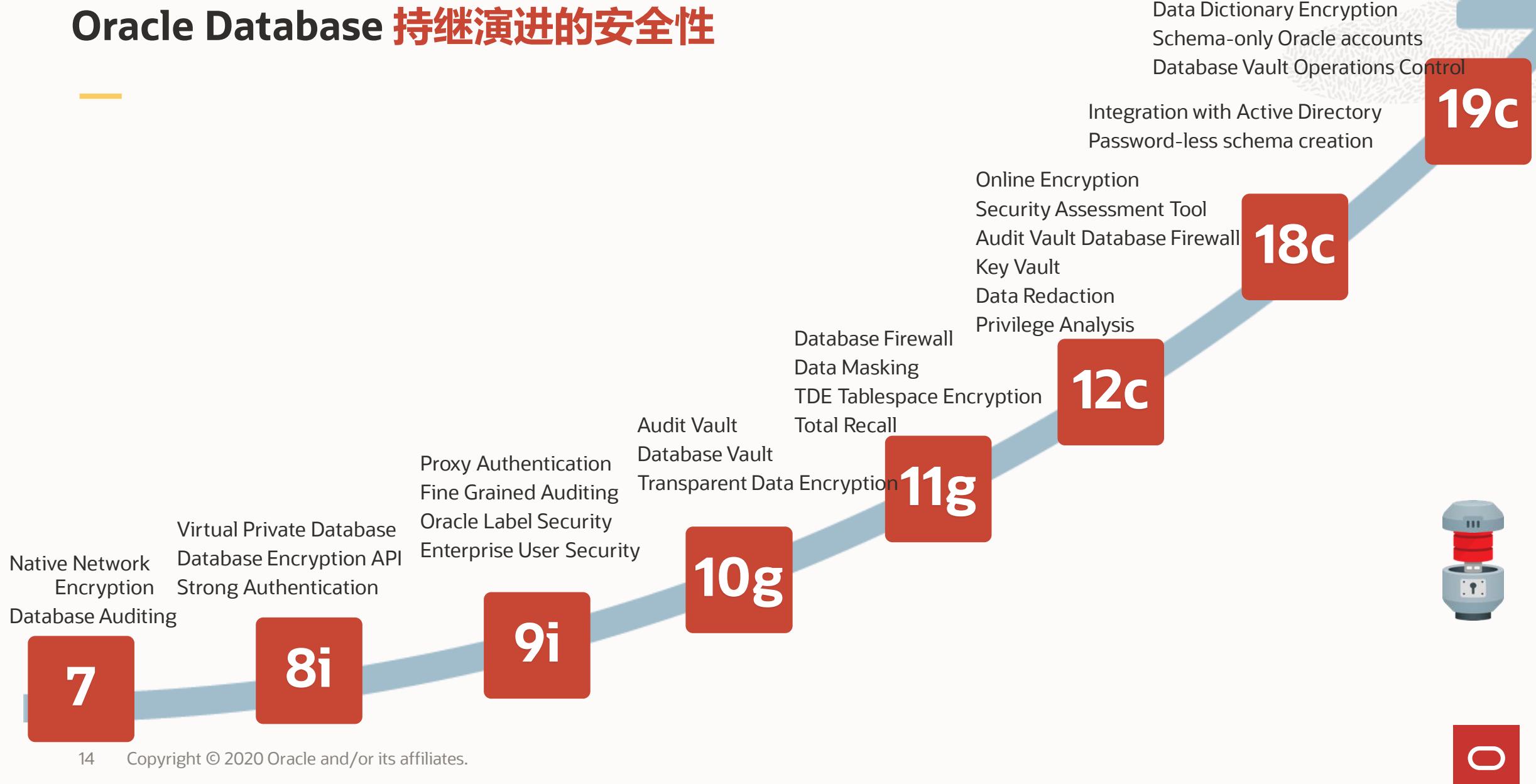
Critical Capabilities	AWS (Amazon + Dynatrace)	Google (Cloud Spanner)	IBM (DB2 + DB4)	Microsoft (SQL + Server)	Oracle (Oracle Database)
High Availability	5.0	5.0	4.0	4.5	5.0
High-Speed, High-Volume Processing	5.0	3.5	4.5	4.0	4.5
Cloud/Hybrid Deployment	2.0	2.0	2.0	4.5	4.5
Administration and Management	3.0	3.0	4.0	4.5	4.5
Security	3.0	2.5	3.5	4.5	4.5
Consistency	2.5	3.0	2.0	4.0	4.0
Multiple Data Types/Structures	4.0	1.0	3.5	4.5	4.0
Automated Data Distribution	4.0	5.0	3.0	3.5	4.0
Programmability for ITAP	2.0	2.0	4.0	4.0	4.0

Gartner: *Operational DBMS Critical Capabilities*, Oct. 2018

**Oracle #1** “security” criterion (4.5/5)

<https://www.gartner.com/doc/reprints?id=1-5LPN68L&ct=181015&st=sb>

# Oracle Database 持续演进的安全性



# Oracle Database 19c中的安全增强

- Oracle 数据字典加密(SYSTEM, SYSAUX, TEMP, UNDO)
- 以AES192, AES256, ARIA, GOST, 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



# Schema Only Accounts

## 问题

- 数据库用户帐户附带密码身份验证，无论是否将其用作登录帐户
- 有些帐户将永远不会用于登录，但是仍然需要维护密码

## 解决

- 从这些帐户中删除密码（和所有身份验证）
- CREATE USER auxapp NO AUTHENTICATION;
- 使用 ALTER USER 增加/删除身份验证

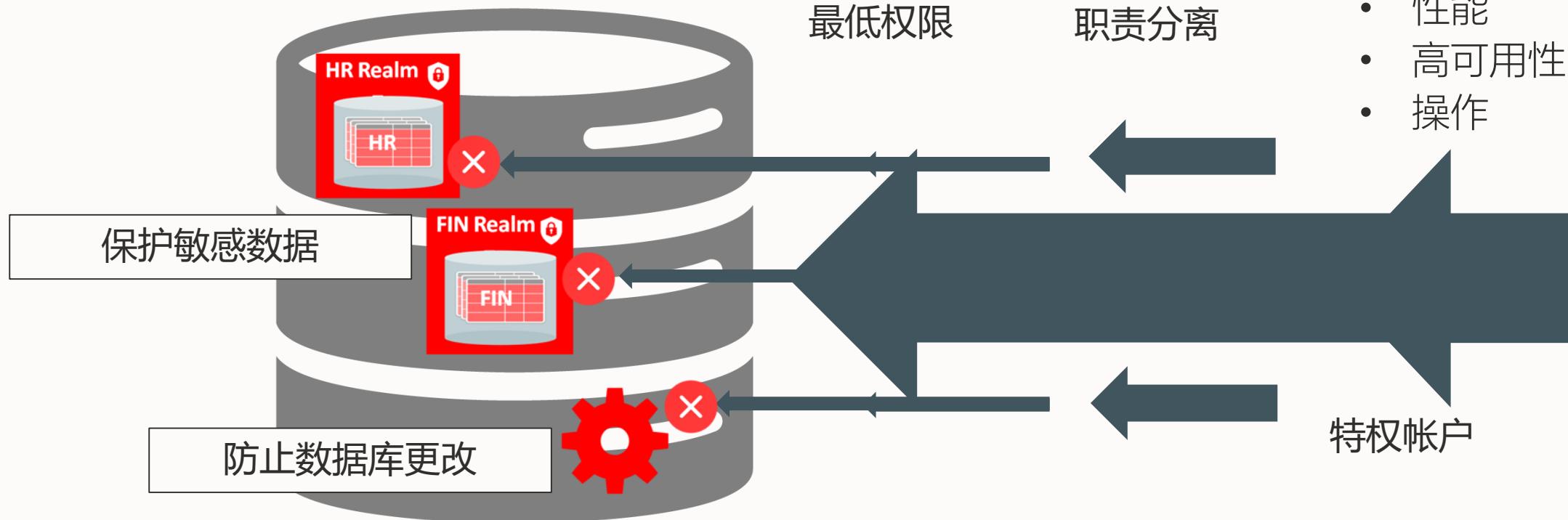
## 19c 新增

- 从19c开始，大部分Oracle自带的schema，除了SYS, SYSTEM以及Sample Schema User Accounts（比如HR）外，都是Schema Only Account。管理员无需周期性的维护这些密码，同时也降低了攻击者使用默认密码侵入这些帐户的安全风险。
- 当我们确实有需要的时候，可以为这些帐户分配密码，但是为了更好的安全性，Oracle建议您使用完毕后将它们再设置为Schema Only Account。



# Oracle Database Vault

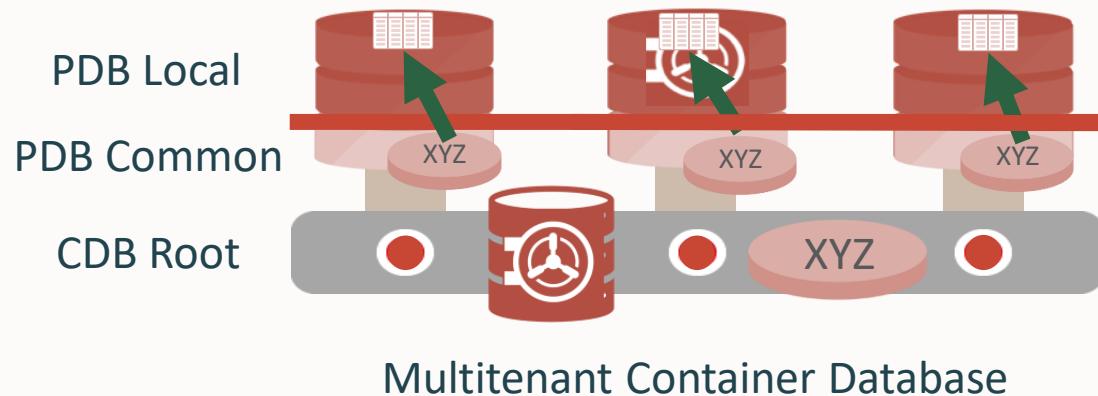
## 减少来自恶意用户的风险



### 最小的影响:

- 应用程序
- 性能
- 高可用性
- 操作

# Database Vault Operations Control



- 多租户数据库面临的挑战
  - 客户的IT部门人员可以管理数据库基础架构，但无需查看PDB中的业务部门敏感数据
  - 云的运营人员不应看到客户PDB中的数据
- 操作控制
  - 对PDB用户透明地阻止common user访问PDB本地数据
  - CDB root中激活DV, 由DV Admin激活DV Operations Control
  - 默认情况下，禁止CDB root common用户访问PDB本地数据—对PDB客户透明
  - 通过PDB lockdown profile的补充保护，可防止PDB用户影响其他PDB和数据库

# Oracle Database中加密特性的增强

- 以最少的停机时间将未加密表空间数据迁移为加密数据
  - 在线加密、增量存储最少、无停机 (12cR2)；支持表空间数据的实时重新加密
  - 快速离线数据加密 (12cR2、12c, 11gR2)；使用Data Guard减少停机时间
- 使用RMAN将明文数据迁移到云时自动加密
- BYOK - Bring Your Own TDE master encryption Key into the database (18c)
  - 支持AES256, ARIA256, SEED128, GOST256
- 每个PDB可选的管理自己的密钥库keystore (isolated mode) (18c)
- Oracle 数据字典加密(19c)
  - TDE 能够加密包括数据字典在内的所有Oracle表空间
  - Oracle Database能够被完全加密



# 如何实现数据加密：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（存储加密、备份加密、导出文档加密）
  - 面向展现层的编纂加密（redaction）
- 技术特点突出，性能高、部署配置简单

# 高级安全 - 透明数据加密 (TDE) 预防控控制数据存储泄密



文明数据

Encrypted Network Connection  
0 1 0 1 0 1 0 1 0  
(TLS or Native Encryption)



加密数据



- 加密某些敏感列或整个表空间
- 保护存储在磁盘或备份中的数据文件
- 不需要修改应用
- 与Oracle技术栈相集成(REDO/TEMP Logs, RAC, Multi-Tenant, GoldenGate, Active Data Guard, Exadata)
- 内置秘钥管理

## 技术概念说明：透明数据加密

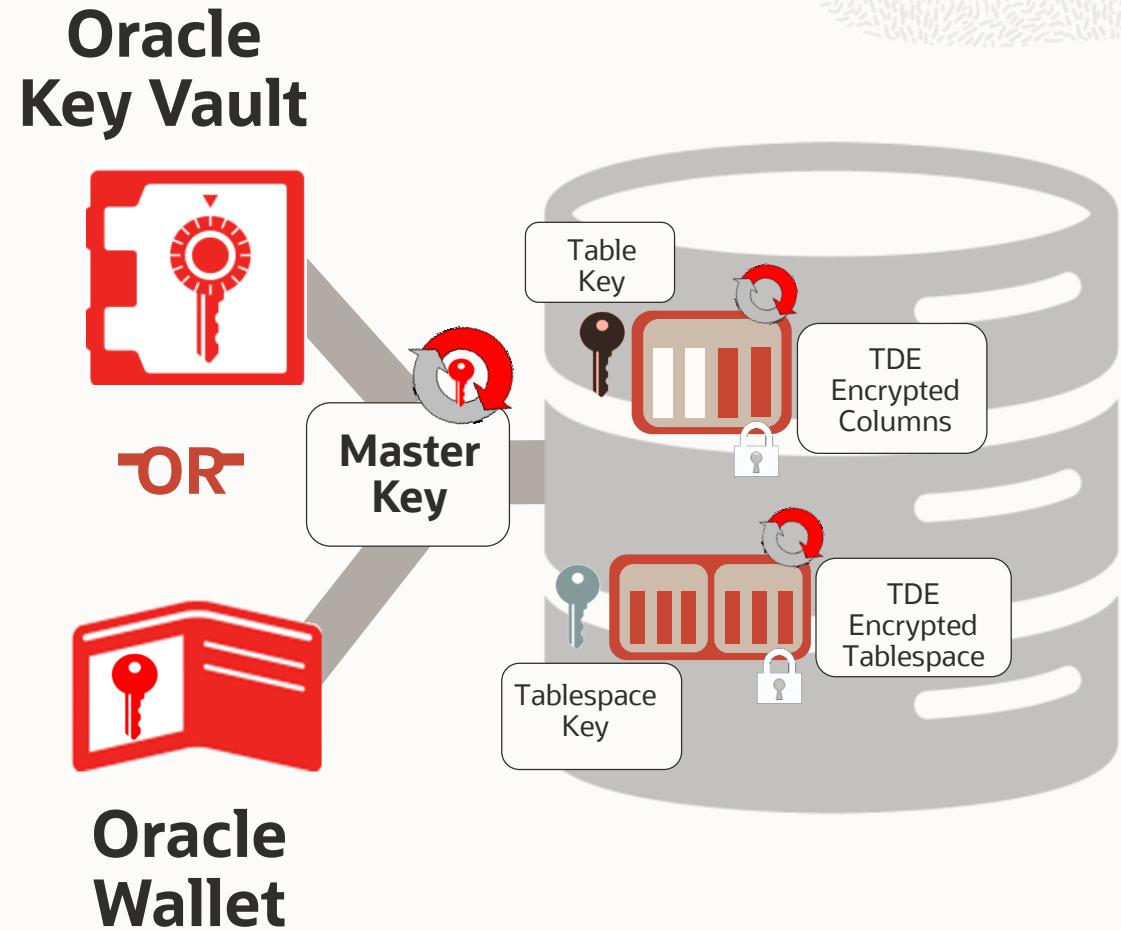
- TDE 既可以对像信用卡号和社会保险号这样的个别应用程序表列进行加密，也可以加密整个表空间，在存储介质或数据文件被盗的情况下也不会泄露敏感数据。
- 存储在被加密表空间中的所有数据都将自动加密，性能高效。
- 备份数据库时，加密的文件在介质上仍保持其加密状态，即使备份介质丢失或被盗仍然能保护的信息不会外泄。
- TDE 表空间加密可以无缝地与 Oracle Streams、Oracle Compression 和 Oracle Exadata Smart Scans 协同工作。
- 由于压缩而实现的存储节省将维持不变，因为压缩过程完成后才对数据进行加密。
- 安全文件/LOBS的透明加密 (11g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 Key 架构

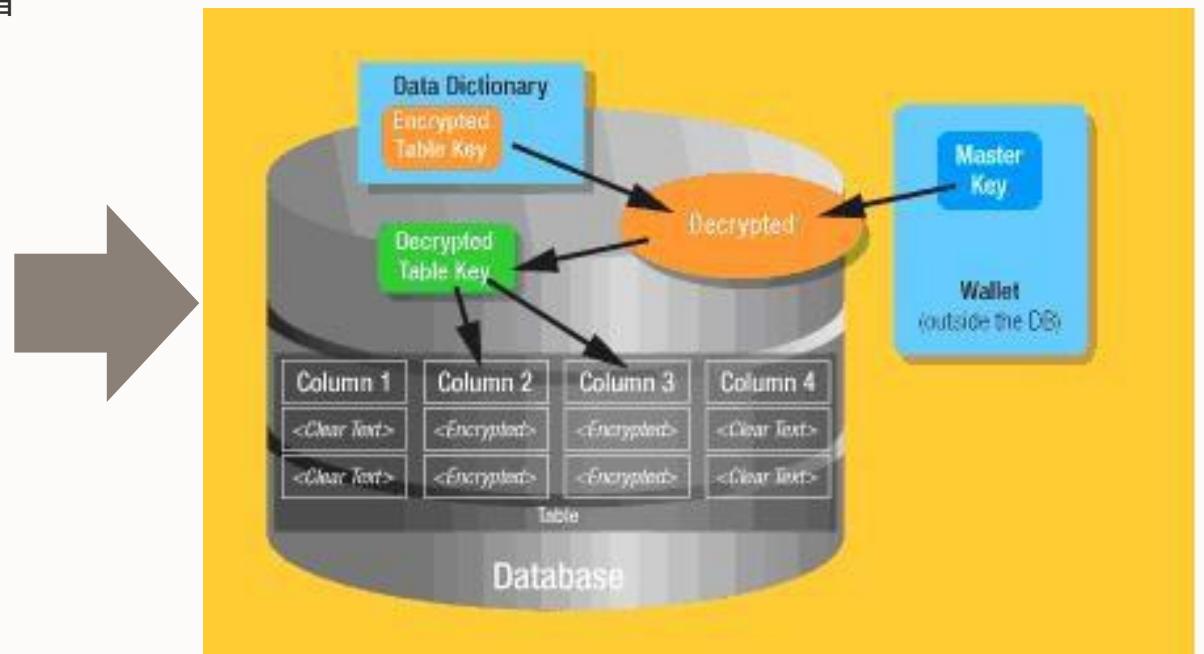
## 两级架构

- 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) 存储在 Oracle Wallet 或 Oracle Key Vault 中



# 技术概念说明：Wallet 简介

- 什么是Oracle wallet
  - 通常称为oracle钱夹，是一种用于存储验证和签名身份证明的安全软件容器，它是用口令加密的PKCS#12文件，存储包括TDE万能密钥、PKI私钥、许可证和SSL需要的信托证书
  - 可以简化依赖口令身份证明连接到数据库的大型部署
- Wallet分为以下两种：
  - 手动打开的wallet (数据库启动后需要手动打开wallet)
  - 启动打开的wallet (数据库启动后会自动打开)
- Wallet和TDE的关系：
  - Oracle从钱夹中获取master密钥，用master密钥解密数据字典中的表密钥或加密表空间的密钥进行表字段的解密



# TDE 支持的算法和Key长度

算法	Key长度	参数名称
Advanced Encryption Standard (AES)	<ul style="list-style-type: none"><li>• 128 bits (default for tablespace encryption)</li><li>• 192 bits (default for column encryption)</li><li>• 256 bits</li></ul>	<ul style="list-style-type: none"><li>• AES128</li><li>• AES192</li><li>• AES256</li></ul>
ARIA (18c 以上)	<ul style="list-style-type: none"><li>• 128 bits</li><li>• 192 bits</li><li>• 256 bits</li></ul>	<ul style="list-style-type: none"><li>• ARIA128</li><li>• ARIA192</li><li>• ARIA256</li></ul>
GOST (18c 以上)	256 bits	GOST256
SEED (18c 以上)	128 bits	SEED128
Triple Encryption Standard (DES)	168 bits	3DES168



# 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）、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. 在sqlnet.ora 文件中加入wallet的存储位置

```
ENCRYPTION_WALLET_LOCATION=
(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/u01/app/wallet)))
```

2. 创建Oracle wallet (kesytore) (login as SYSKM)

```
SQL>ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/u01/app/wallet' IDENTIFIED BY Welcome;
```

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

```
SQL>ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY Welcome;
```

4. 设置主秘钥 (login as SYSKM)

```
SQL>ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY Welcome 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 securitespace_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

Oracle Maximum Availability Architecture

Converting to Transparent Data Encryption Using Data Guard Transient Logical Standby

Oracle Database 11g Release 2

ORACLE WHITE PAPER | MAY 2015

Oracle Maximum Availability Architecture

Converting to Transparent Data Encryption Using Active Data Guard (DBMS\_ROLLING)

Oracle Database 12c

ORACLE WHITE PAPER | MAY 2015



# TDE 与 Oracle 数据库技术相集成

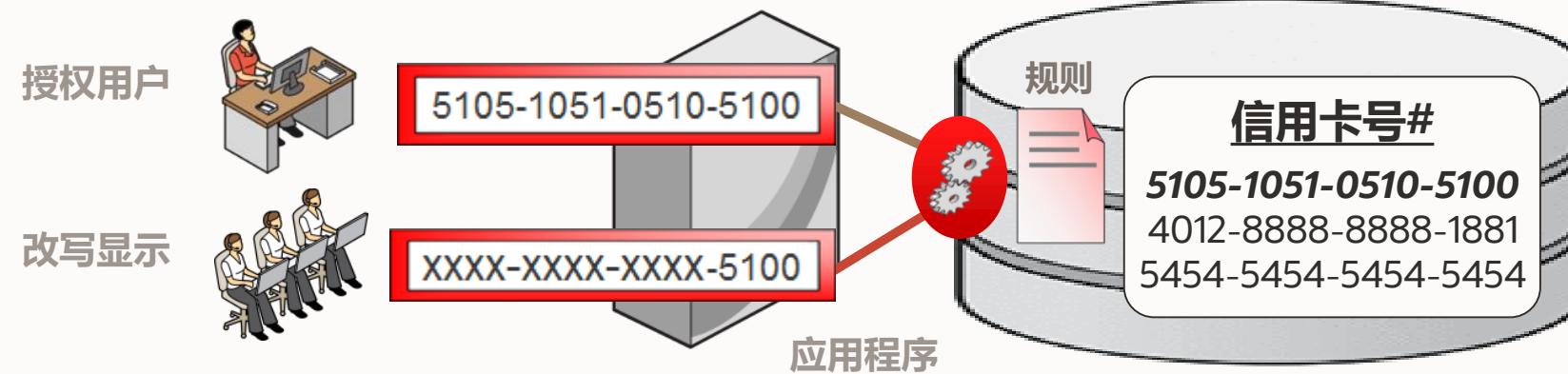
Database Technologies	Example Points of Integration	TDE Support
High-Availability Clusters	Oracle Real Application Clusters (RAC), Data Guard, Active Data Guard	✓
Backup and Restore	Oracle Recovery Manager (RMAN), Oracle Secure Backup	✓
Export and Import	Oracle Data Pump Export and Import	✓
Database Replication	Oracle Golden Gate	✓
Pluggable Databases	Oracle Multitenant Option	✓
Engineered Systems	Oracle Exadata Smart Scans	✓
Storage Management	Oracle Automatic Storage Management (ASM)	✓
Data Compression	Oracle Standard, Advanced , and Hybrid Columnar Compression	✓



## 演示——在线加密表空间

---

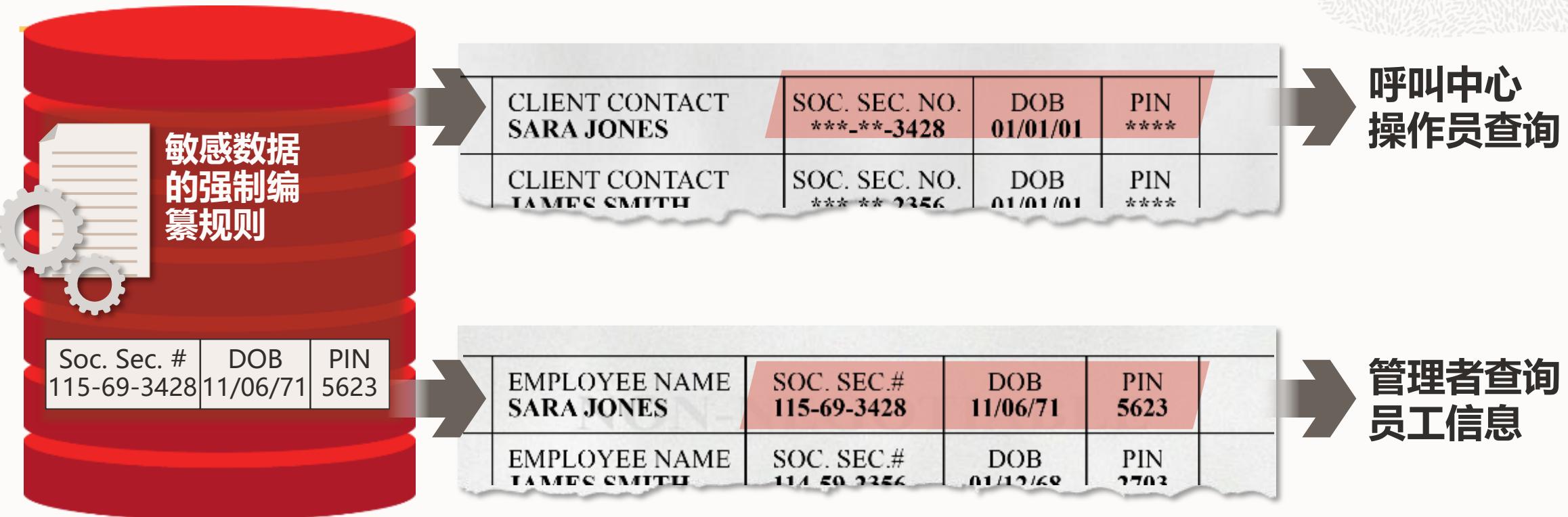
# 高级安全 – 实时编纂 (Redaction) 加密敏感数据 为应用改写敏感数据



- 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
- 最小的生产负载影响



# 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

# OEM中的安全管理界面

Enterprise Targets Favorites History

Search Target Name DBSec-OW-13.us.

dbsec01.us.oracle.com Oracle Database Performance Availability Security Schema Administration

Page Refreshed Aug 26, 2013 3:12:12 PM Auto Refresh Off

**Summary**

**Status**

- Up Time 4 days, 2 hrs
- Version 12.1.0.1.0
- Load 0.00 average active sessions
- Total Sessions 57
- Last Backup N/A
- Available Space 0.10 GB
- Used Space 2.34 GB
- Total SGA 597.31 MB

**Diagnostics**

- ADDM Findings 0
- Incidents - 0, X 1, ! 0, P 0

**Compliance Summary**

**Compliance Standards**

- View Trends
- Name Average Score

Services

SYS\$BACKGROUND  
SYS\$USERS  
dbsec01XDB  
dbsec01.us.oracle.com  
CPU Cores

Data Masking

Data Redaction

Transparent Data Encryption

Database Vault

Privilege Analysis

Label Security

Virtual Private Database

Application Contexts

Enterprise User Security

Duration	SQL ID	Session ID	Parallel	Database Time
23.00 s	7gbccvcns5fmg	77		48.31 s
5.00 s	7wgks43wrjtrz	68		6.21 s
19.00 s	8szmwam7fyasa3	68		19.36 s

# 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)  
秘钥保险库(Key Vault)



# 价值体现



# 保护Oracle数据库安全

技术入门电子书

第三版

<https://oracle.com/securingthedatabase>

- 数据库身份验证和授权
- 强制执行职责分离
- 数据加密和密钥管理
- 敏感数据脱敏
- 审计数据库活动
- 数据库防火墙监控数据库活动
- 数据驱动的应用程序授权
- 安全态势评估
- 欧盟GDPR和数据库安全
- 保护云中的数据库



# Database Security 更多资源

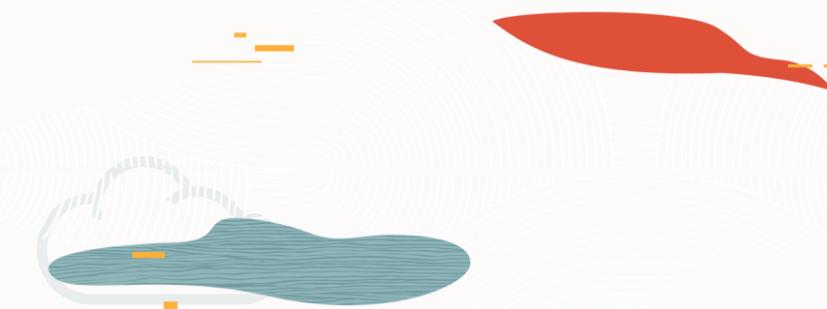
- 了解Oracle数据库安全  
<http://oracle.com/database/security>
- Blog:<https://blogs.oracle.com/cloudsecurity/db-security>
- 免费数据库安全评估工具**Database Security Assessment Tool** [MOS ID: 2138254.1](#)
- 数据安全和GDPR白皮书  
<https://go.oracle.com/LP=54366>
- AskTOM数据库安全专题办公时间
  - 每月第二个星期四9:00-20:00(UTC)
  - 检索：“AskTom Database Security”



A screenshot of the Oracle Technology Network website showing the DBSAT tool. The page has a red header with the Oracle logo. The main content area features a title "Oracle Database Security Assessment Tool" with a magnifying glass icon over a padlock. Below the title is a paragraph of text explaining the tool's purpose. At the bottom, there are two download links with "Download" buttons: "Presentation: Oracle Database Security Assessment Tool overview" and "FAQ: Oracle Database Security Assessment Tool".

扫码加入:

19c新特性讲座微信群



欢迎关注:

甲骨文云技术公众号  
纯技术分享无广告

