ORACLE

ORACLE

Seguridad en la Base de Datos Oracle:

La seguridad de su base de datos Oracle no es negociable

Alfonso Chavez Coronilla
José Vazquez
Francisco Alvarez
Juan Carlos Díaz

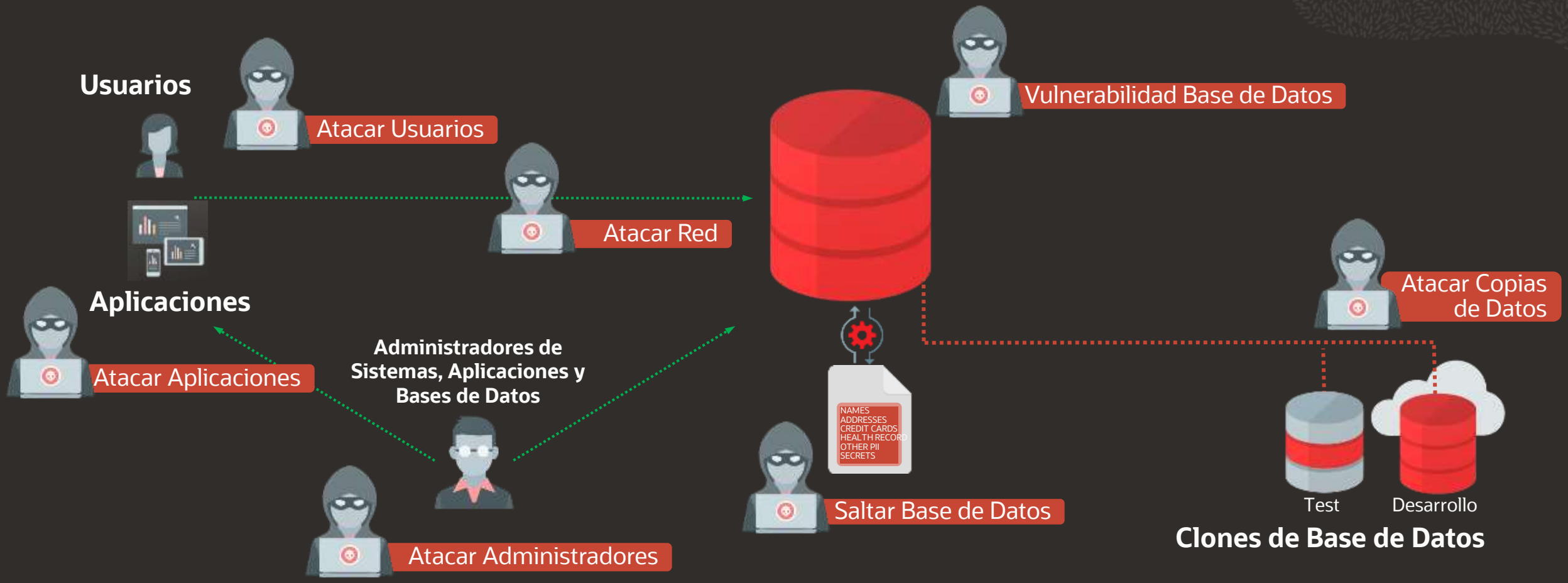
Client Engineers
Febrero 2022

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.

¿Cómo intenta atacar la base de datos un hacker?



Seguridad Básica

Seguridad Básica

Controles de Seguridad de Base de Datos

Evaluar Prevenir Detectar

Seguridad Básica

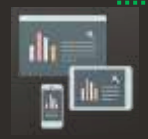
- Evaluación general de seguridad

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

Seguridad Básica

Usuarios



Aplicaciones

Database Security Assessment Tool (DBSAT)

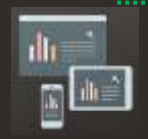
- Evaluación general de seguridad

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

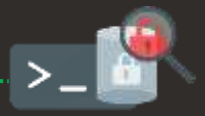
Seguridad Básica

Usuarios



Aplicaciones

Passwords seguras
Autenticación fuerte



Database Security Assessment Tool (DBSAT)

Evaluación general de seguridad

Controles de Seguridad de Base de Datos

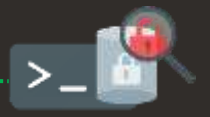
Evaluar **Prevenir** **Detectar**

Seguridad Básica

Usuarios

Aplicaciones

- Passwords seguras
- Autenticación fuerte



Database Security Assessment Tool (DBSAT)

- Evaluación general de seguridad
- Identificar usuarios y permisos

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

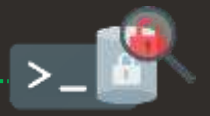
Seguridad Básica

Usuarios

Aplicaciones

Passwords seguras
Autenticación fuerte

- Análisis de privilegios *



- Evaluación general de seguridad
- Identificar usuarios y permisos

Database Security Assessment Tool (DBSAT)

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

Seguridad Básica

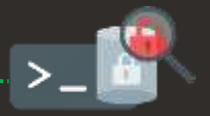
Usuarios

Aplicaciones

Passwords seguras
Autenticación fuerte

Cifrado de red

Análisis de privilegios *



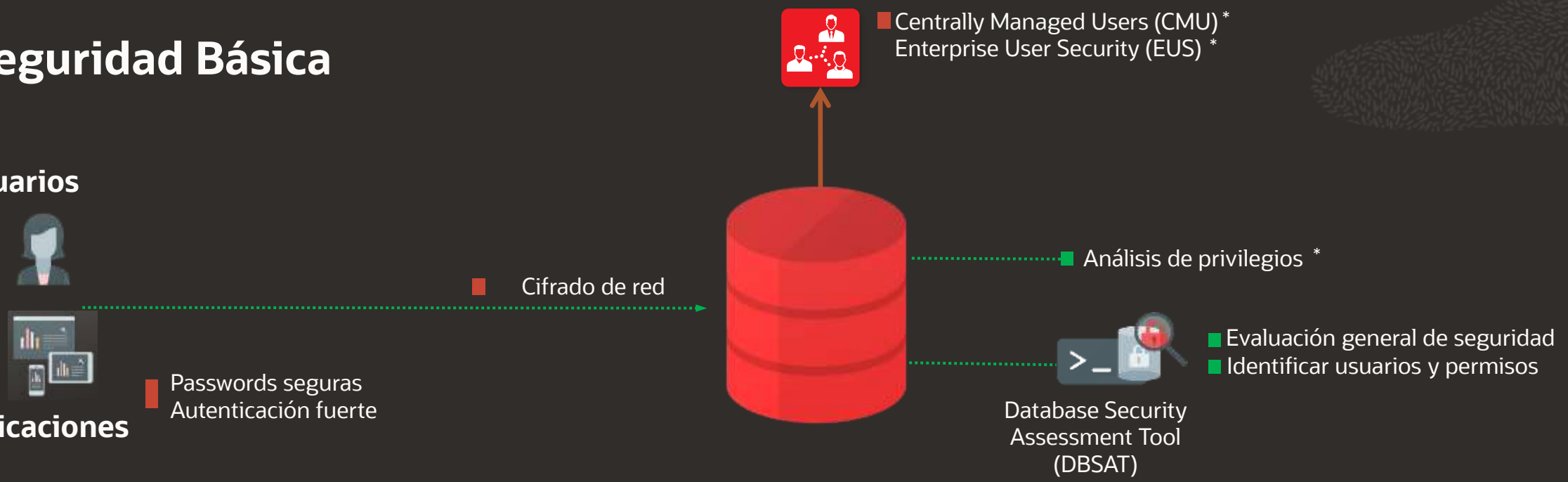
Evaluación general de seguridad
Identificar usuarios y permisos

Database Security Assessment Tool (DBSAT)

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

Seguridad Básica

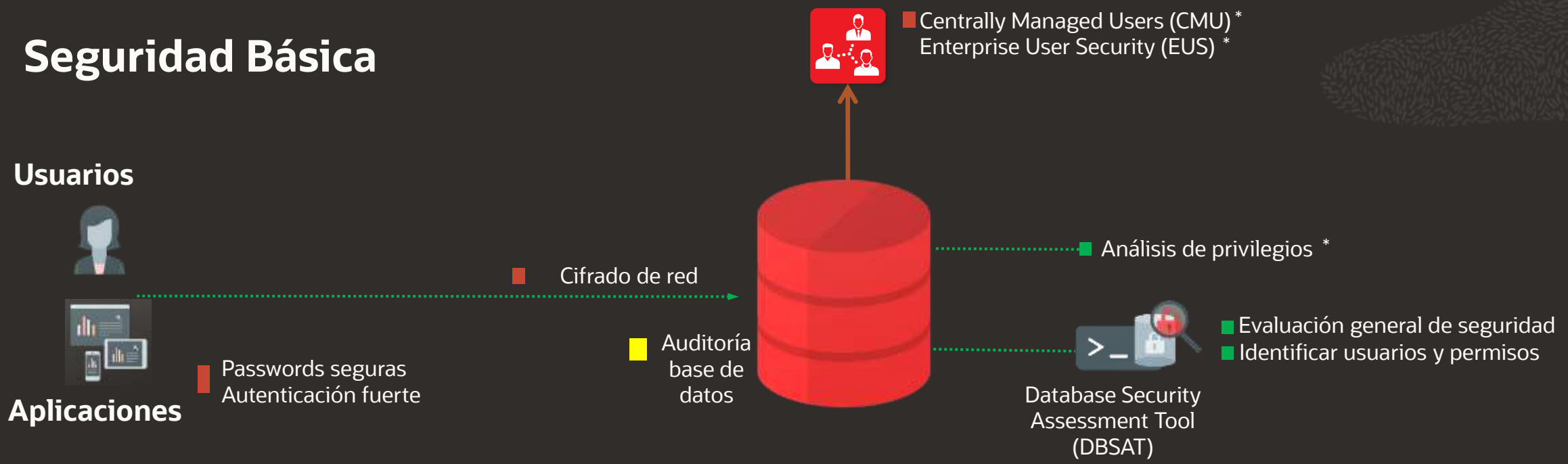


* Solo disponible en Enterprise Edition

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

Seguridad Básica

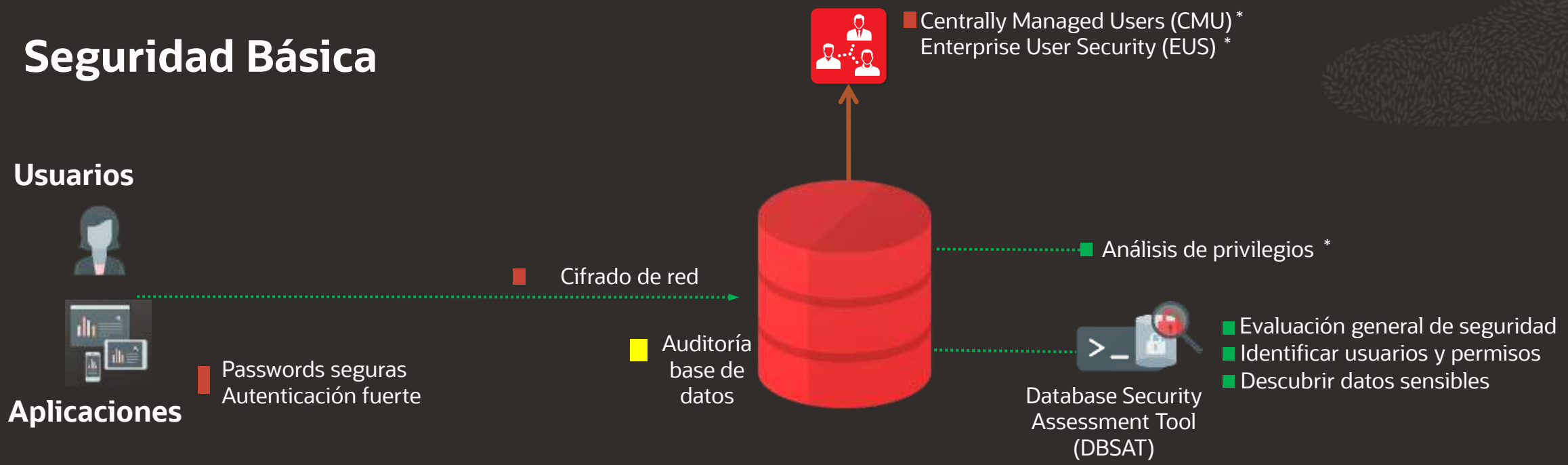


* Solo disponible en Enterprise Edition

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

Seguridad Básica

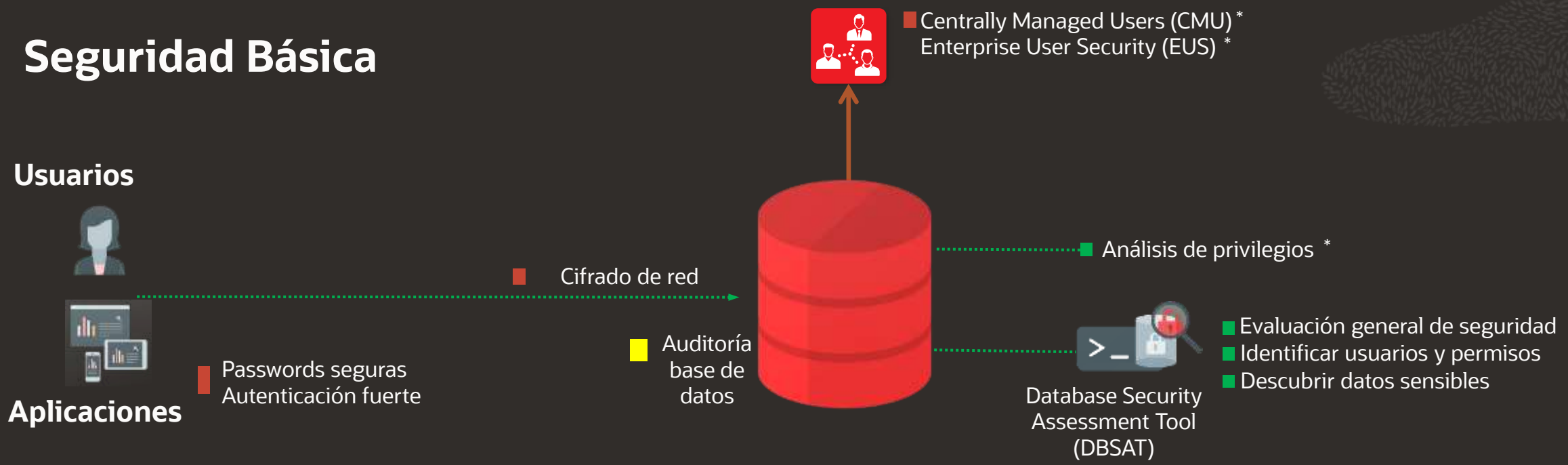


* Solo disponible en Enterprise Edition

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

Seguridad Básica

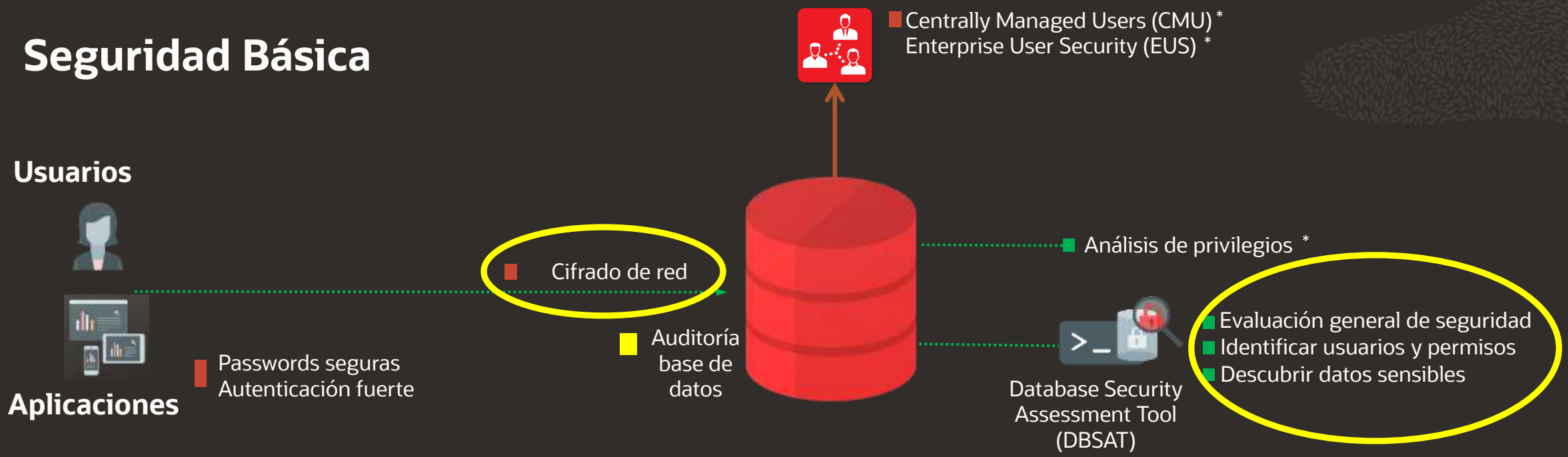


* Solo disponible en Enterprise Edition

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

Seguridad Básica



* Solo disponible en Enterprise Edition

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

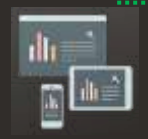
Usuarios

Aplicaciones

Controles de Seguridad de Base de Datos

Evaluar Prevenir Detectar

Usuarios



Aplicaciones

Transparent
Data Encryption

Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**

Usuarios

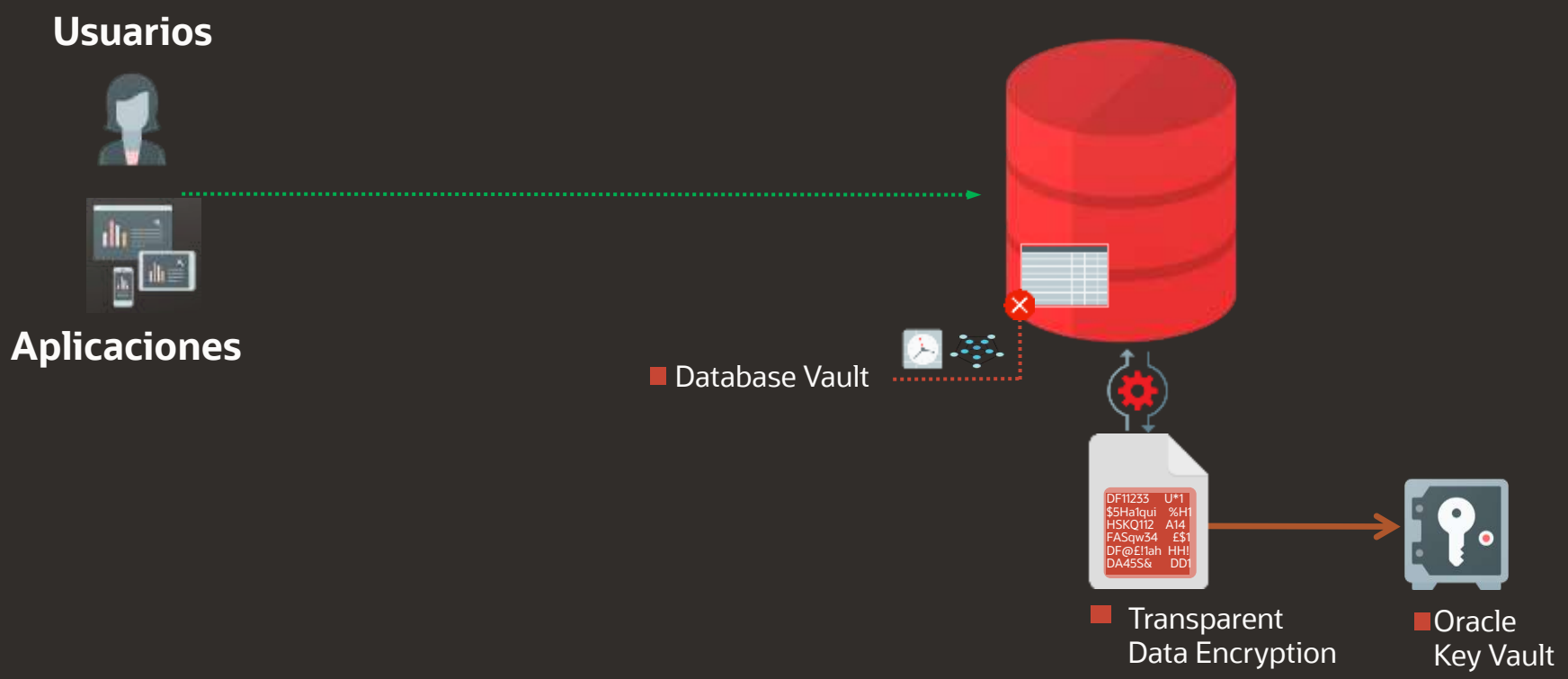
Aplicaciones

Transparent Data Encryption

Oracle Key Vault

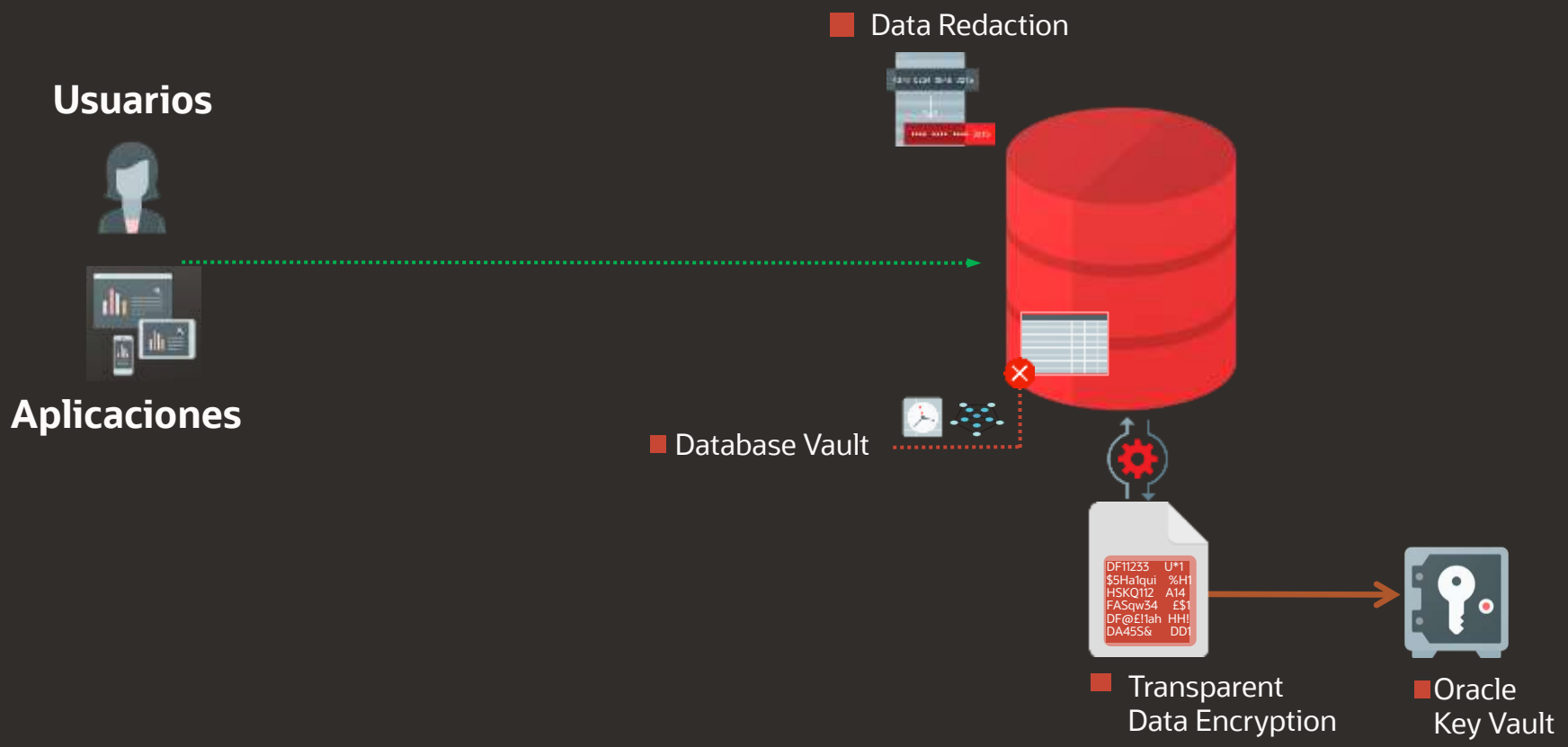
Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**



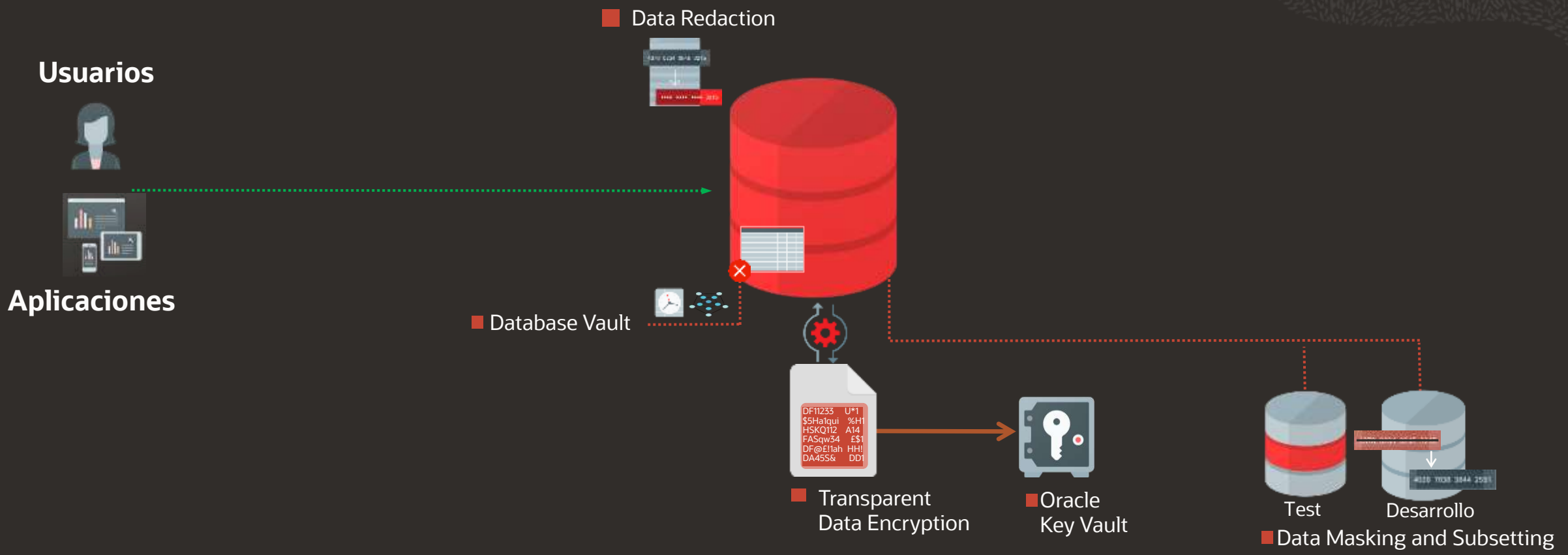
Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**



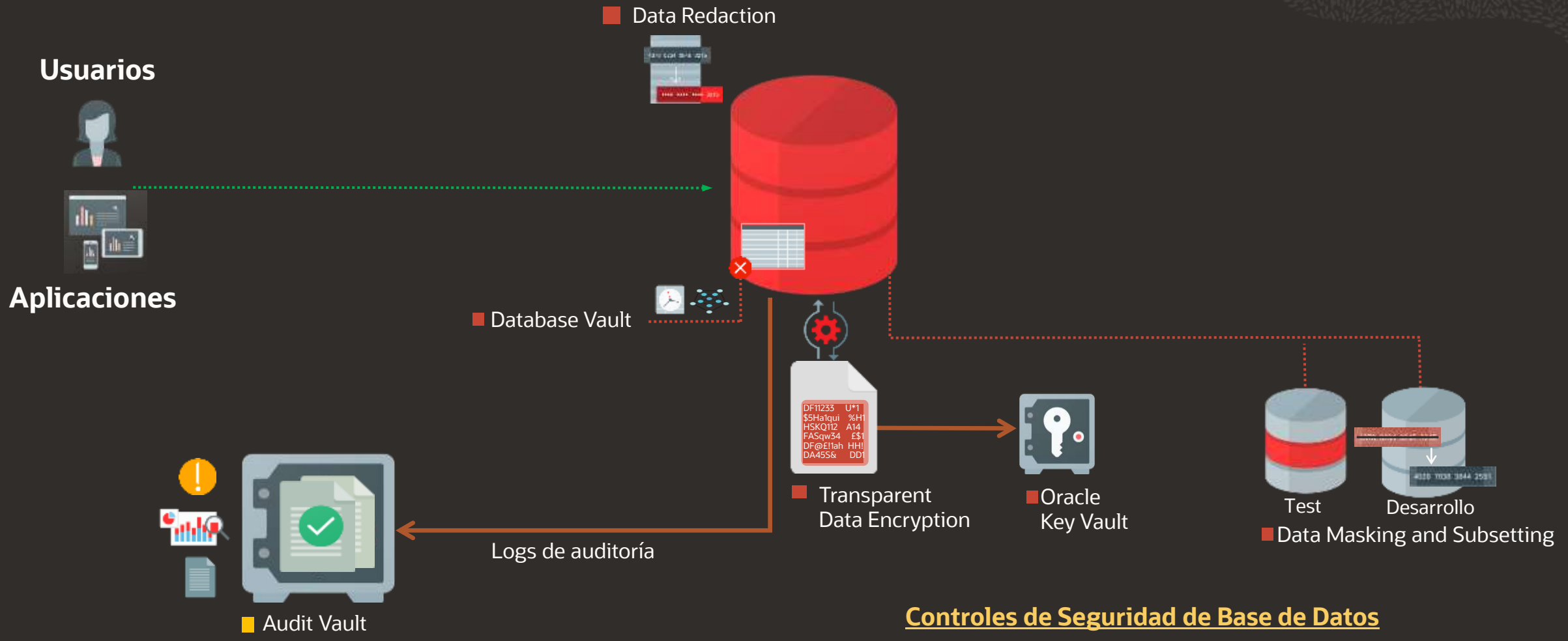
Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**



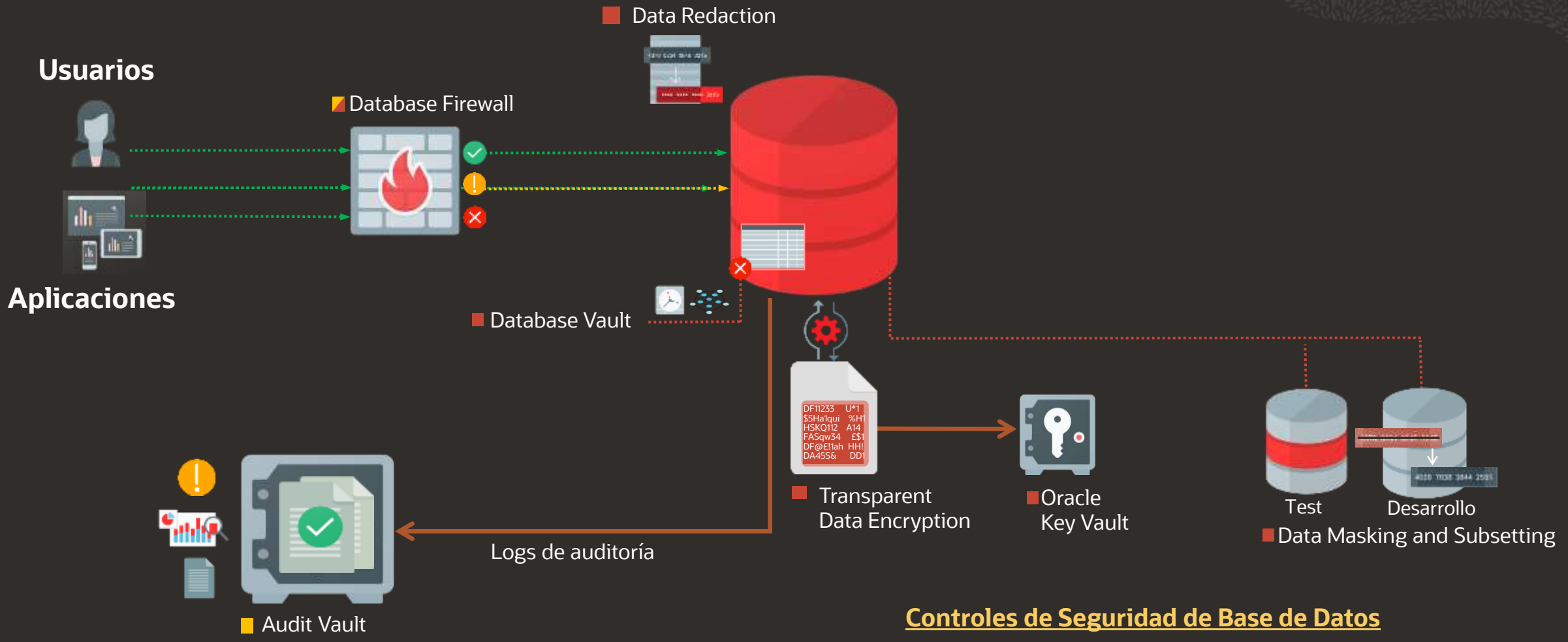
Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**



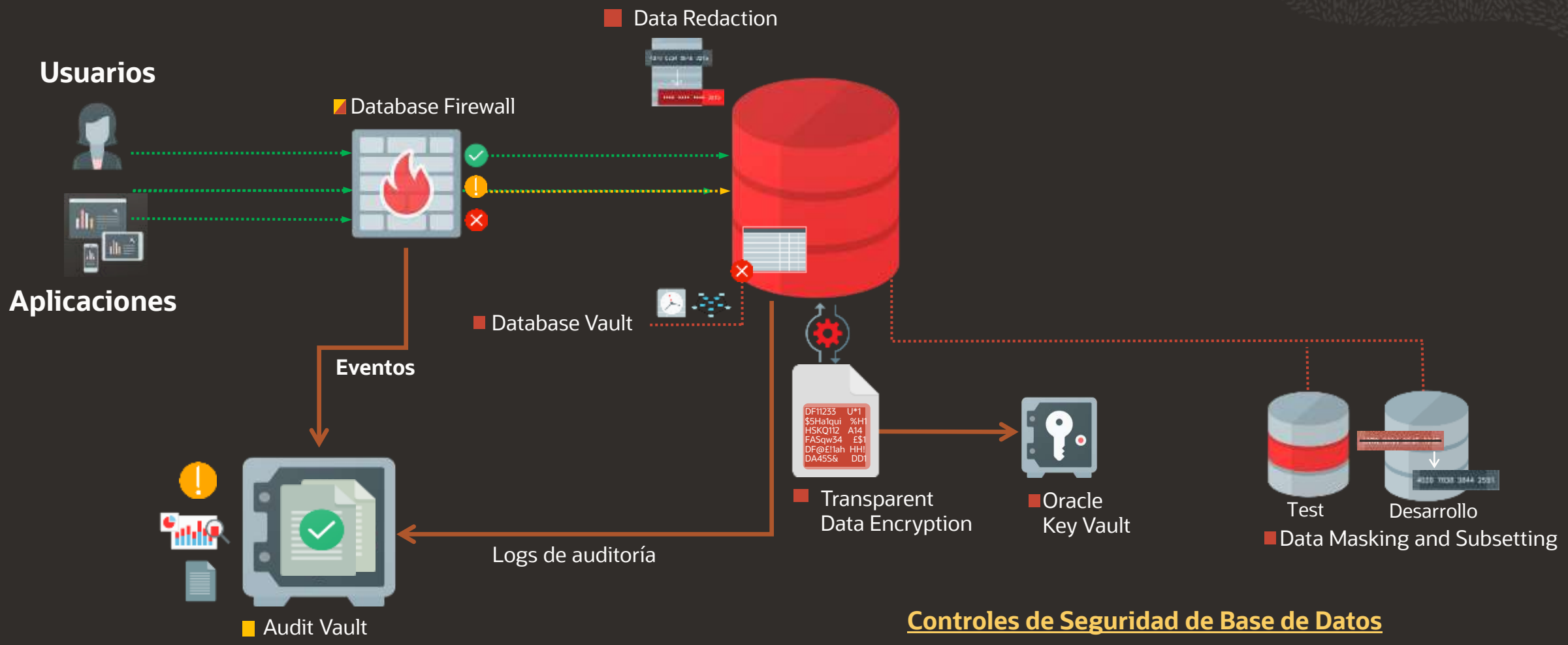
Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**



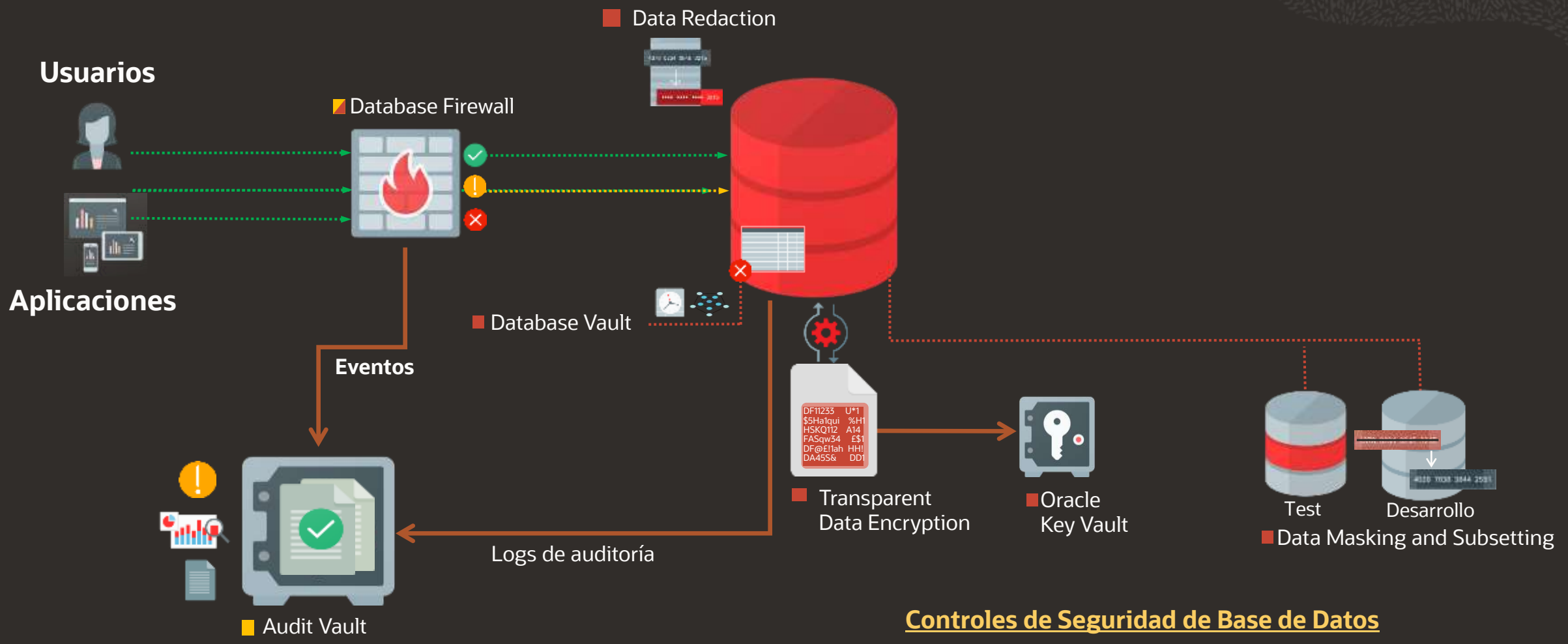
Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**



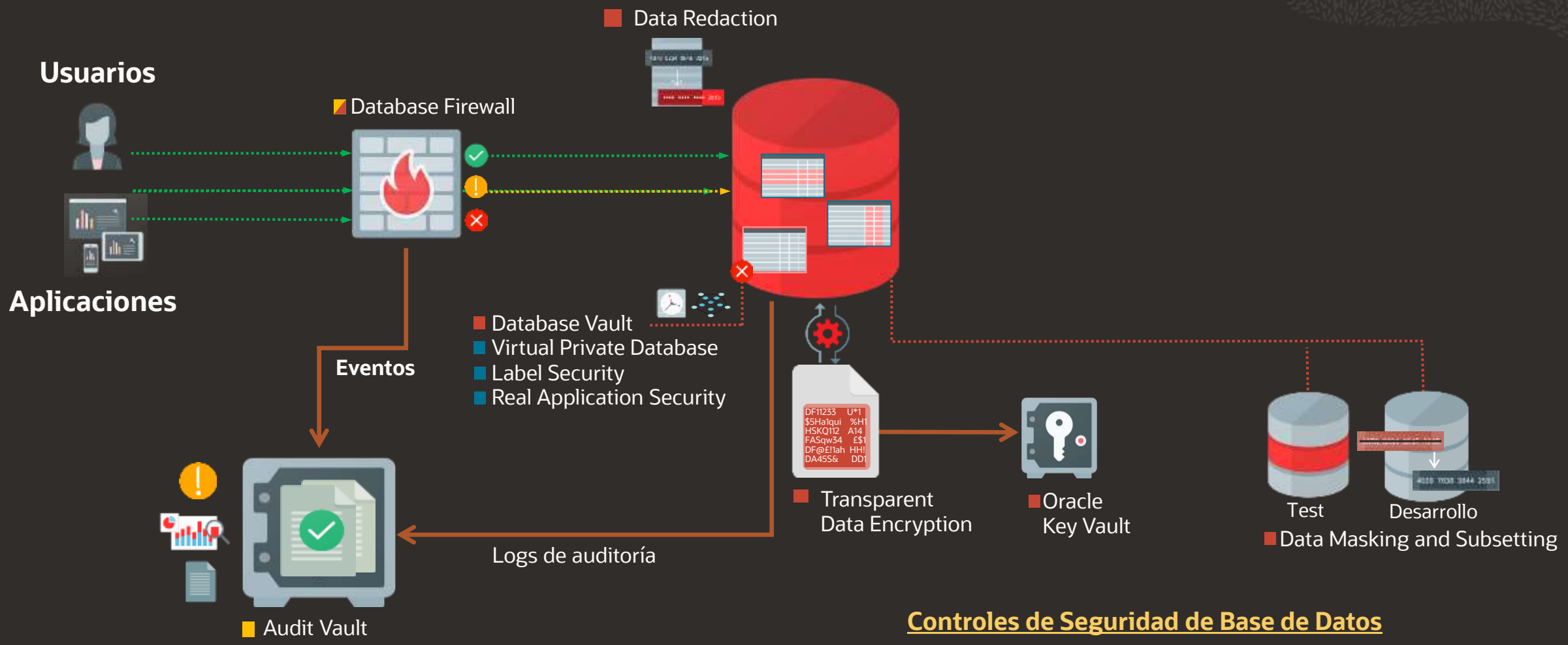
Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar**



Controles de Seguridad de Base de Datos

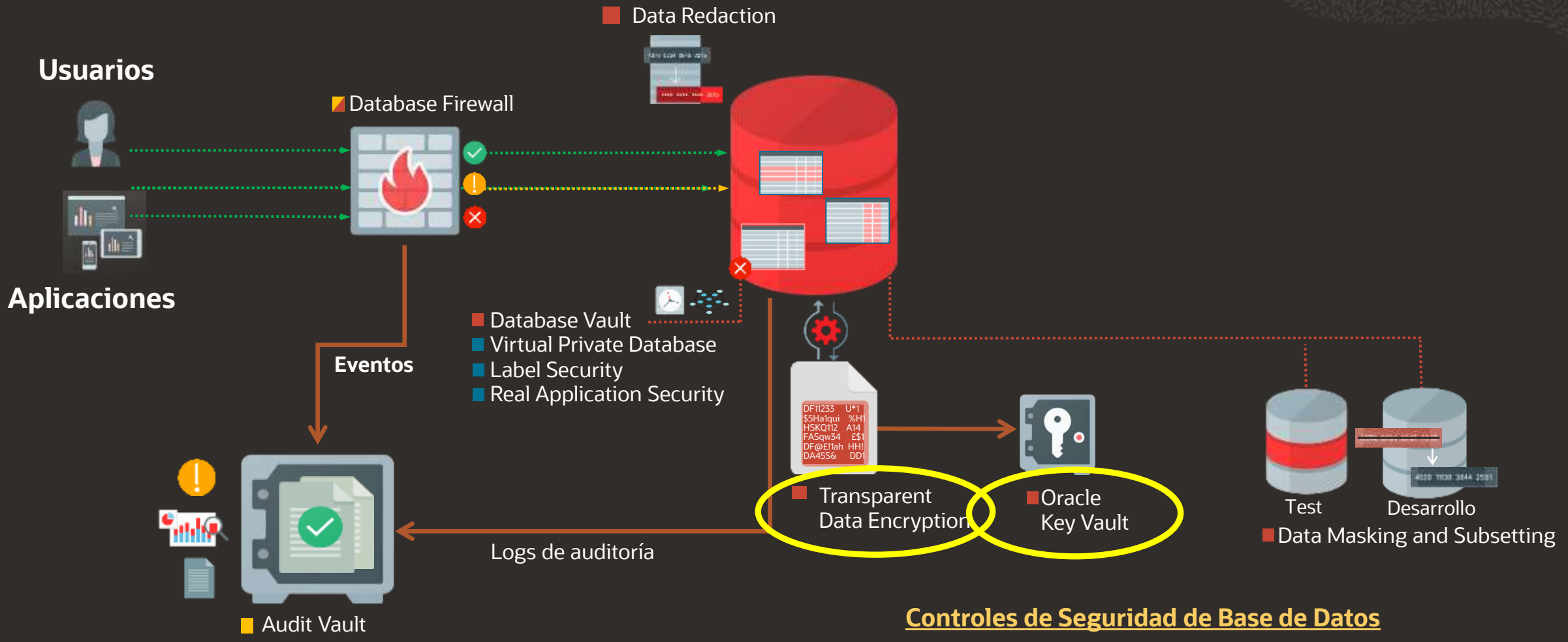
Evaluar **Prevenir** **Detectar** **Seguridad dirigida por datos**



Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar** **Seguridad dirigida por datos**

Arquitectura de máxima seguridad



Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar** **Seguridad dirigida por datos**

Opciones Base de Datos Oracle

Producto	Funcionalidades
Oracle Advanced Security Option	• Cifrado transparente de datos, en reposo, en copia de seguridad y en exportaciones • Seudonimización (ofuscación “al vuelo”)
Oracle Key Vault	• Archivado de wallets y keystores para retención a largo plazo • Fácil recuperación cuando estos ficheros son requeridos • Gestión centralizada de claves para las claves maestras de TDE
Oracle Data Masking and Subsetting Pack	• Descubrimiento de datos sensibles • Anonimización de datos • Muestreo de datos
Oracle Database Vault	• Control y protección de super-usuarios de BBDD (DBAs) • Limitación de acceso a datos y de acciones por contexto • Segregación de funciones
Oracle Audit Vault and Database Firewall	• Auditoría, monitorización, alertas e informes centralizados (seguridad reactiva) • Firewall de BBDD y bloqueo de inyección SQL (seguridad preventiva)

Agenda

Sesión 1: martes 15 de febrero – “Evaluación de seguridad y Cifrado”

10:00 - 10:45
Presentación del entorno y casos de uso: guía de trabajo

10:30 - 12:45
Laboratorios “Cifrado y gestión de claves”
- Acceso y conocimiento del entorno
- Herramienta de análisis DBSAT
- Cifrado de comunicaciones
- Cifrado transparente de tablespaces
- Cifrado en tiempo real sin paradas de servicio
- Administración de centralizada de claves y wallet

Sesión 2: miércoles 16 de febrero – “Análisis de privilegios y Segregación de Funciones”

10:00 - 10:30
Presentación Oracle Database Vault

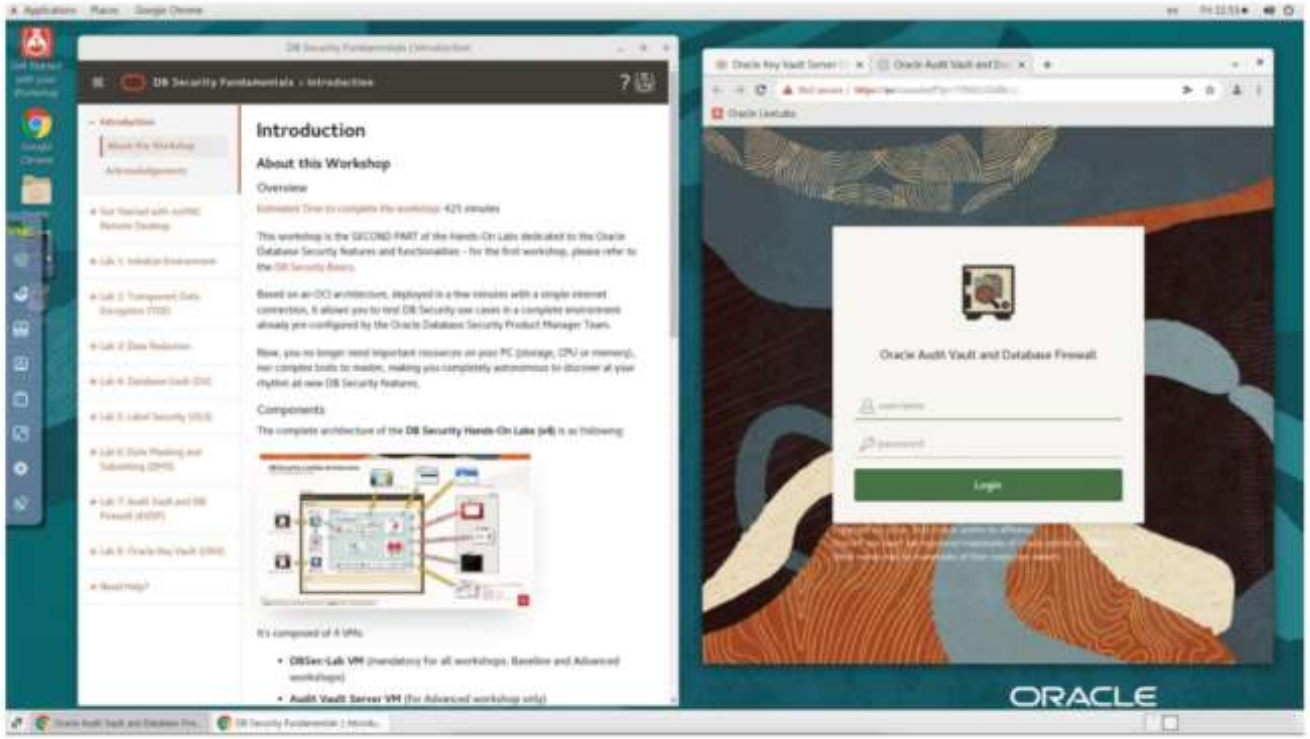
10:30 – 12:45
Laboratorio “Segregación de funciones”
- Análisis de uso de privilegios de usuarios
- Creación reglas acceso
- Reglas de acceso en modo simulado
- Control de acceso por ruta de aplicación

Sesión 3: jueves 17 de febrero – “Enmascaramiento dinámico - Anonimización de datos”

10:00 - 10:30
Presentación Oracle Data Redaction – Data Masking & Subsetting

10:30 – 12:45
Laboratorio “Enmascaramiento de datos”
- Políticas de censura de datos on-line
- Creación de modelo de enmascaramiento
- Descubrimiento de datos sensibles
- Aplicación de máscaras
- Conclusión y cierre

Día	Guía	Ejercicio
15	***DB Security Basics***	Lab 1: Initialize Environment
15	***DB Security Basics***	Lab 2: Database Security Assessment Tool (DBSAT)
15	***DB Security Basics***	Lab 3: Native Network Encryption (NNE)
15	***DB Security Fundamentals***	Lab 2: Transparent Data Encryption (TDE)
15	***DB Security Fundamentals***	Lab 8: Oracle Key Vault (OKV)
16	***DB Security Basics***	Lab 4: Privilege Analysis
16	***DB Security Fundamentals***	Lab 4: Database Vault (DV)
17	***DB Security Fundamentals***	Lab 3: Data Redaction
17	***DB Security Fundamentals***	Lab 6: Data Masking and Subsetting (DMS)



- La documentación de los laboratorios, con la guía paso a paso, es accesible en estos dos enlaces:

DB Security Basics
https://oracle.github.io/learning-library/security-library/database/baseline/workshops/desktop/

DB Security Fundamentals
https://oracle.github.io/learning-library/security-library/database/advanced/workshops/desktop/

Oracle Advanced Security Option (ASO)

Oracle Advanced Security

Protección avanzada para bases de datos Oracle

Transparent Data Encryption (TDE)

- **Cifra de forma transparente los datos en disco de la base de datos y gestiona de forma segura las claves de cifrado**
- **Protege frente a perdida o robo de discos o backups**
- **Impide a usuarios de OS inspeccionar los ficheros BD**

Nuevo

Data Redaction

- Censura “on line” de datos sensibles de las aplicaciones
- Políticas declarativas gestionadas de forma central en la base de datos
- Decisiones tomadas en función del contexto
- Multiples transformaciones para elegir

Oracle Advanced Security

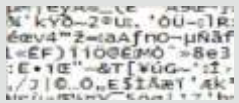
Proteger datos sensibles de usuarios no autorizados

INSERT
Nombre: Juan Nadie
DNI: 12345678A

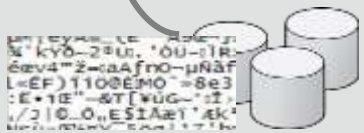
ORACLE JDEDWARDS SIEBEL SAP PeopleSoft

Oracle Advanced Security
Reescritura del dato

SELECT
Nombre: Juan Nadie
DNI: 12345678A



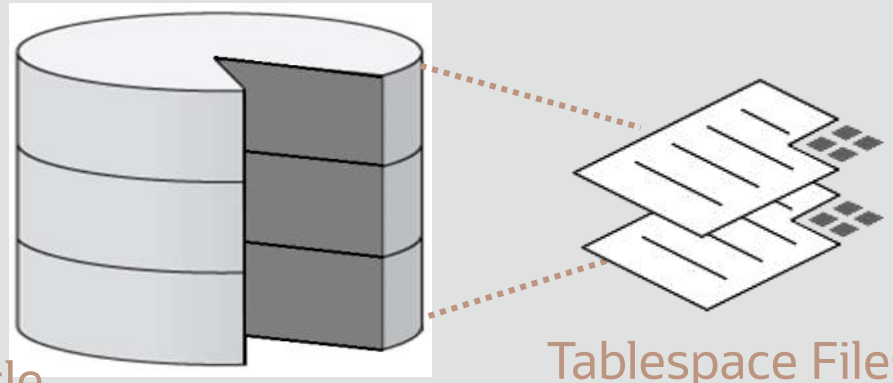
Los datos escritos a disco son cifrados automáticamente



Los datos se descifran de forma transparente y se devuelven en claro

Oracle Advanced Security
Cifrado de los datos en disco

Lectura datos en claro de Tablespace Files



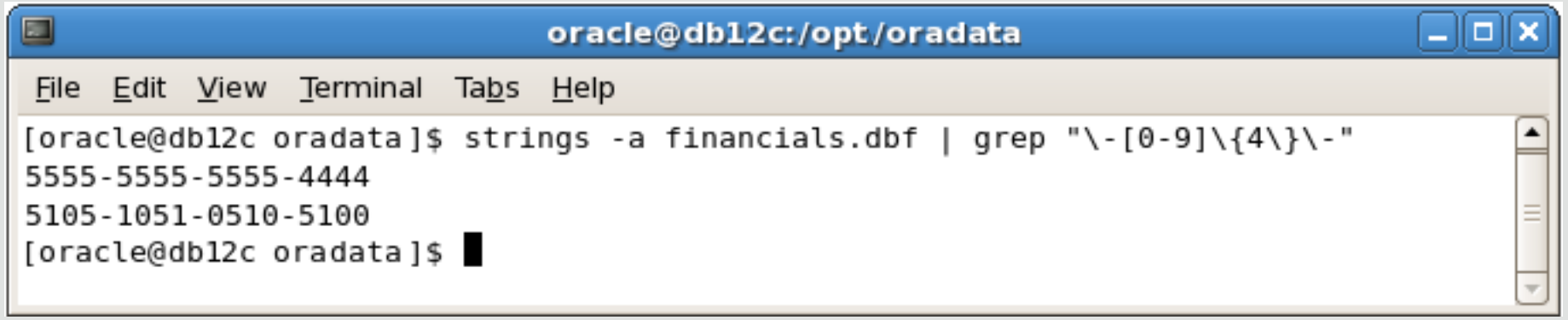
Oracle Database

Tablespace Files (financials.dbf)

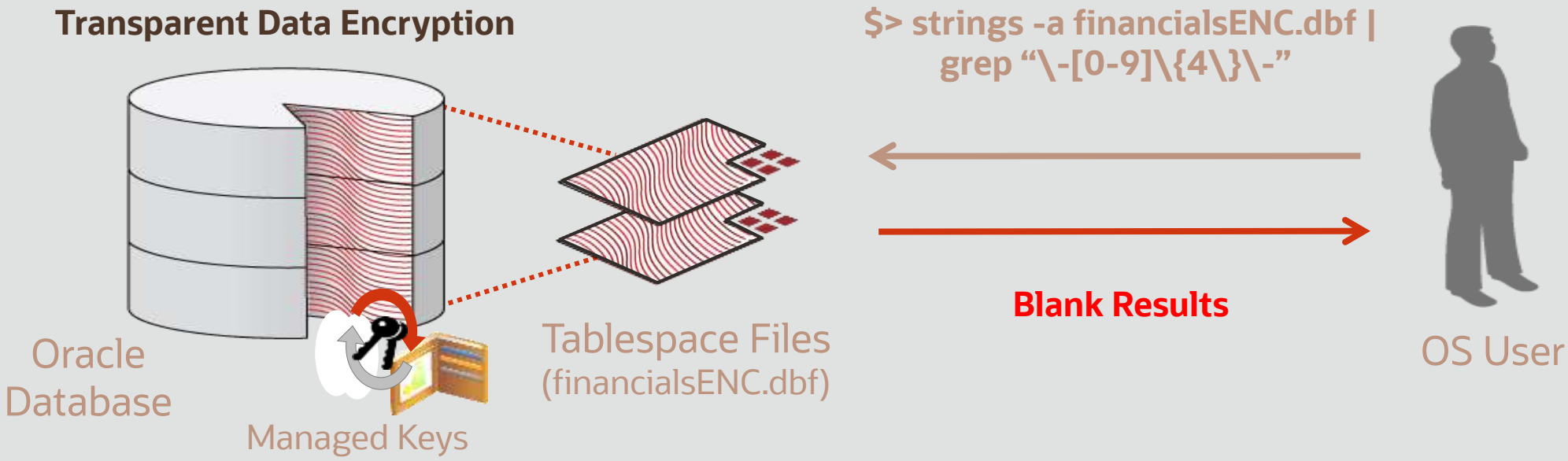
$> strings -a financials.dbf | grep “\-[0-9]\{4\}\-”

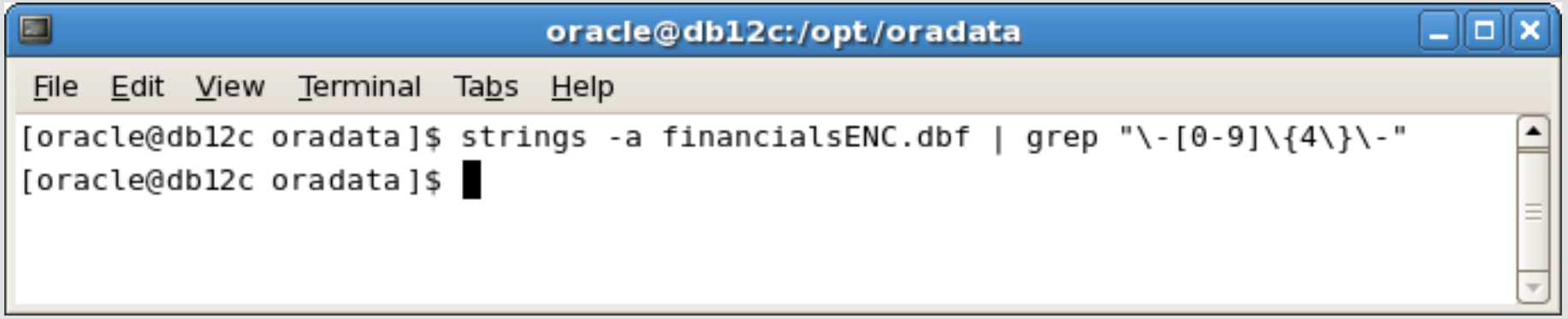
5555-5555-5555-4444
5105-1051-0510-5100

OS User



Intento lectura datos de Tablespace Files cifrado





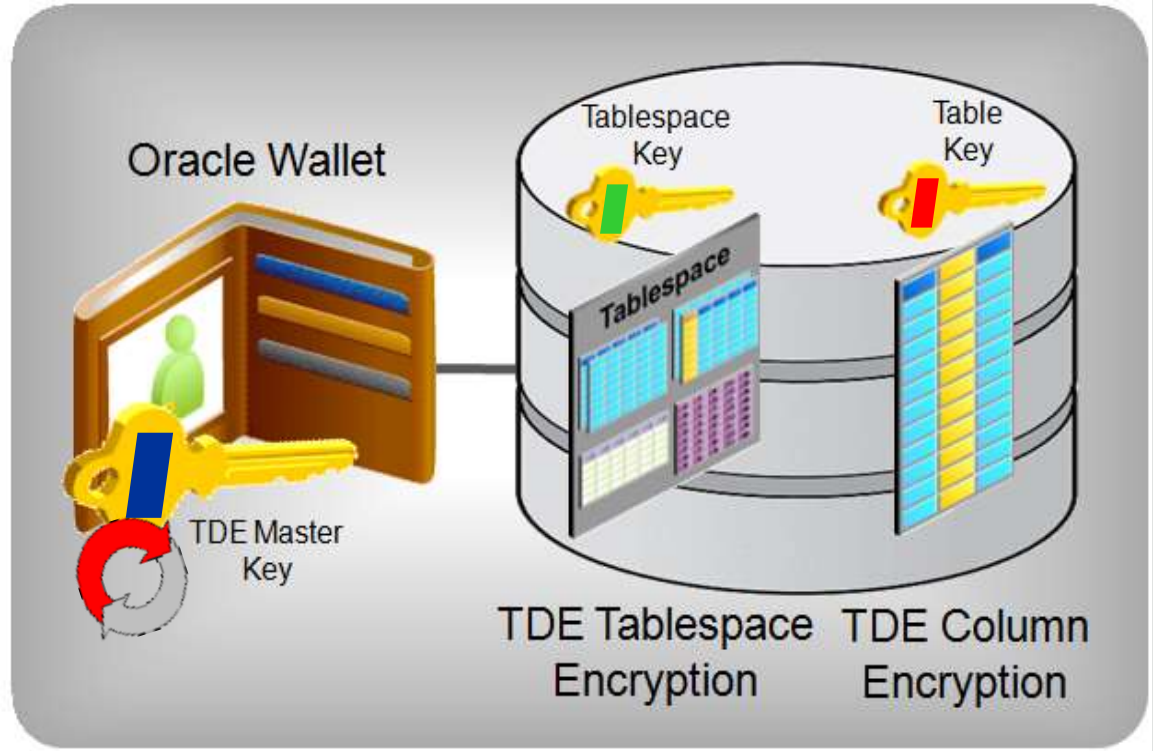
TDE Arquitectura de Claves

Claves de cifrado de datos se crean y gestionan automáticamente por TDE.

Una master encryption key cifra las claves de cifrado de datos.

La master encryption key se crea por la bbdd y se gestiona directamente por un usuario.

La master encryption key suele almacenarse en Oracle Wallet.



Transparent Data Encryption

Cifrado de Tablespaces

Disponible desde Oracle Database 11g R1

Cifra *tablespaces* completos de aplicaciones

No hay que identificar columnas concretas

Permite cifrar cualquier tipo de dato (incl. LOBs)

Permite aplicar cualquier tipo de índice, búsquedas por rangos y/o claves ajenas índices

Gestión de claves

- Una clave por cada *tablespace* cifrado
- La clave de cada *tablespace* se cifra utilizando la clave maestra de TDE

Transparent Data Encryption

Cifrado de Tablespaces. Sintaxis y consideraciones

Creando un nuevo *tablespace*

```
SQL> create tablespace SECURE datafile '/opt/enc_tbs.dbf' size
100M encryption using 'AES256' default storage(encrypt);
```

No hay incremento en el tamaño de almacenamiento

Opciones en el algoritmo de cifrado

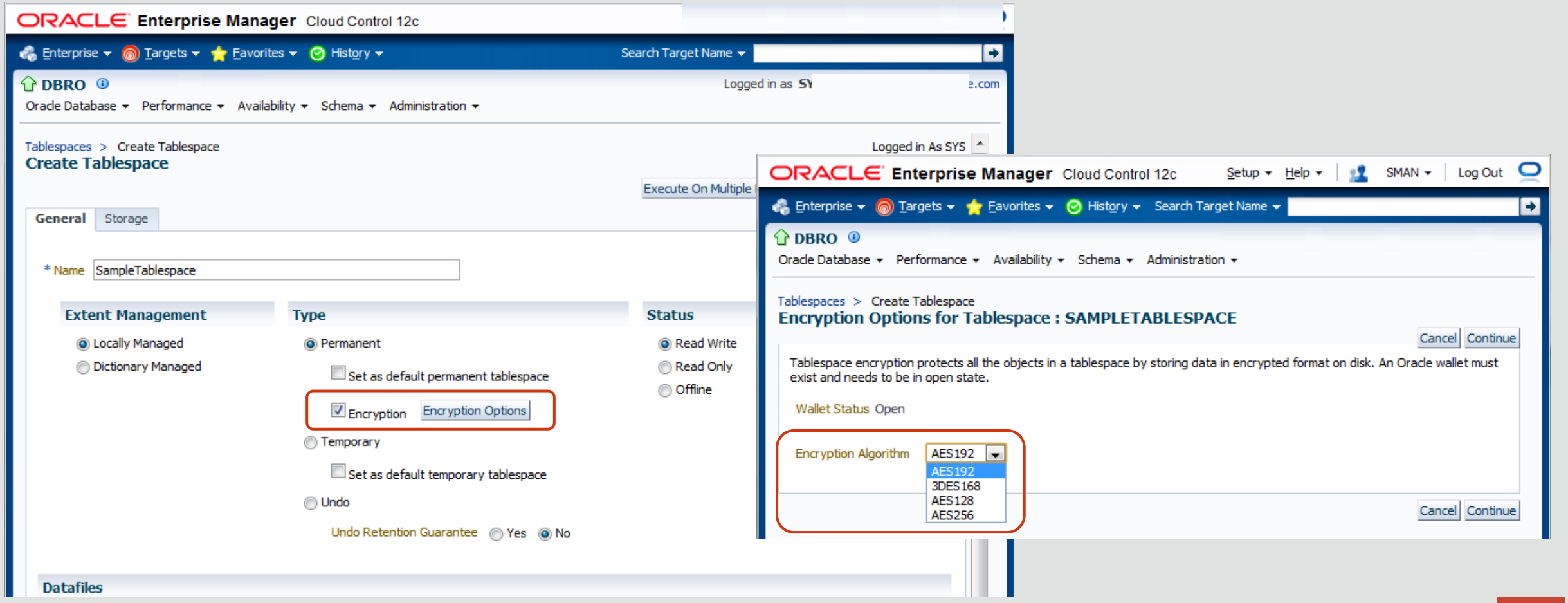
- AES256, AES192, AES128 (default) and 3DES168

Se estima una pérdida de rendimiento de 1-2%. El cifrado/descifrado se realiza en la capa de IO de Oracle

Certificado con Advanced Compression. Los bloques son comprimidos antes de ser cifrados

TDE integrado con Oracle Enterprise Manager

Creación de Tablespace cifrado



Transparent Data Encryption

Gestión de claves

Gestión del ciclo de vida de las claves

- Genera, almacena, rota y destruye claves maestras de encriptación
- Oracle Wallet (almacén software PKCS#12) o almacén HSM

Hardware Security Module (HSM):

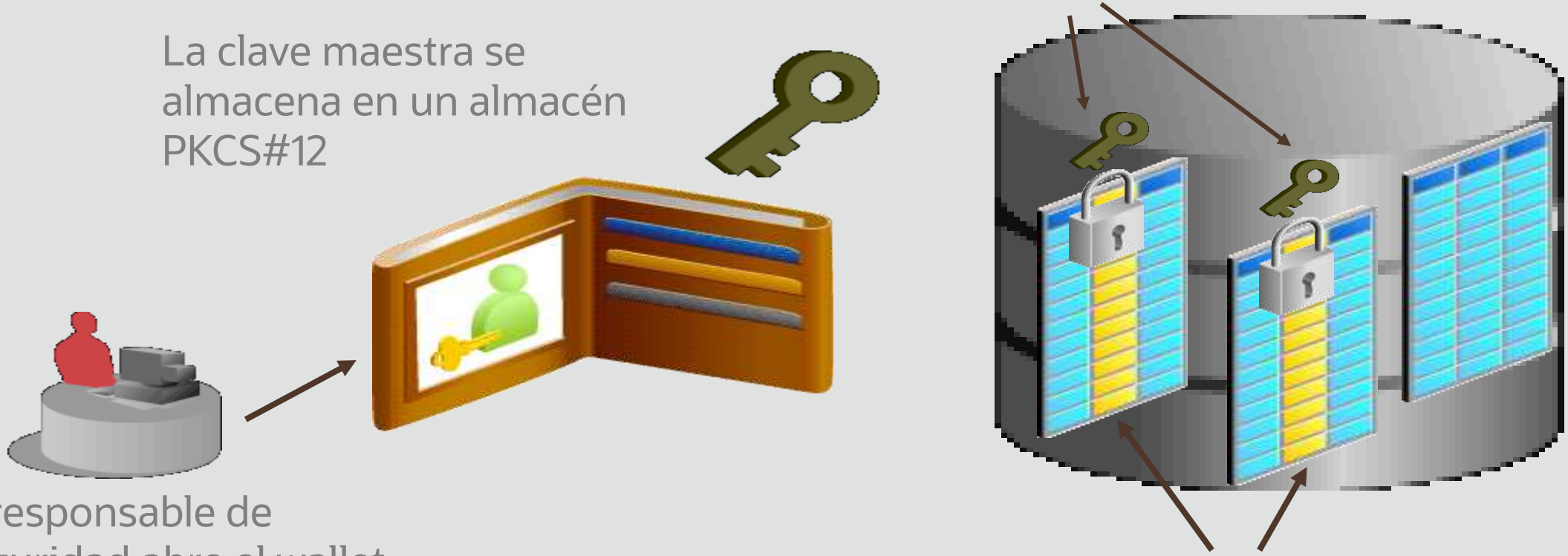
- Hardware específico para almacenar claves digitales
- Interfaz de comunicación PKCS#11 que permite a los clientes Oracle utilizar una amplia variedad de dispositivos HSM

Transparent Data Encryption

Gestión de claves

Las claves de tablas/tablespaces son cifradas con la clave maestra

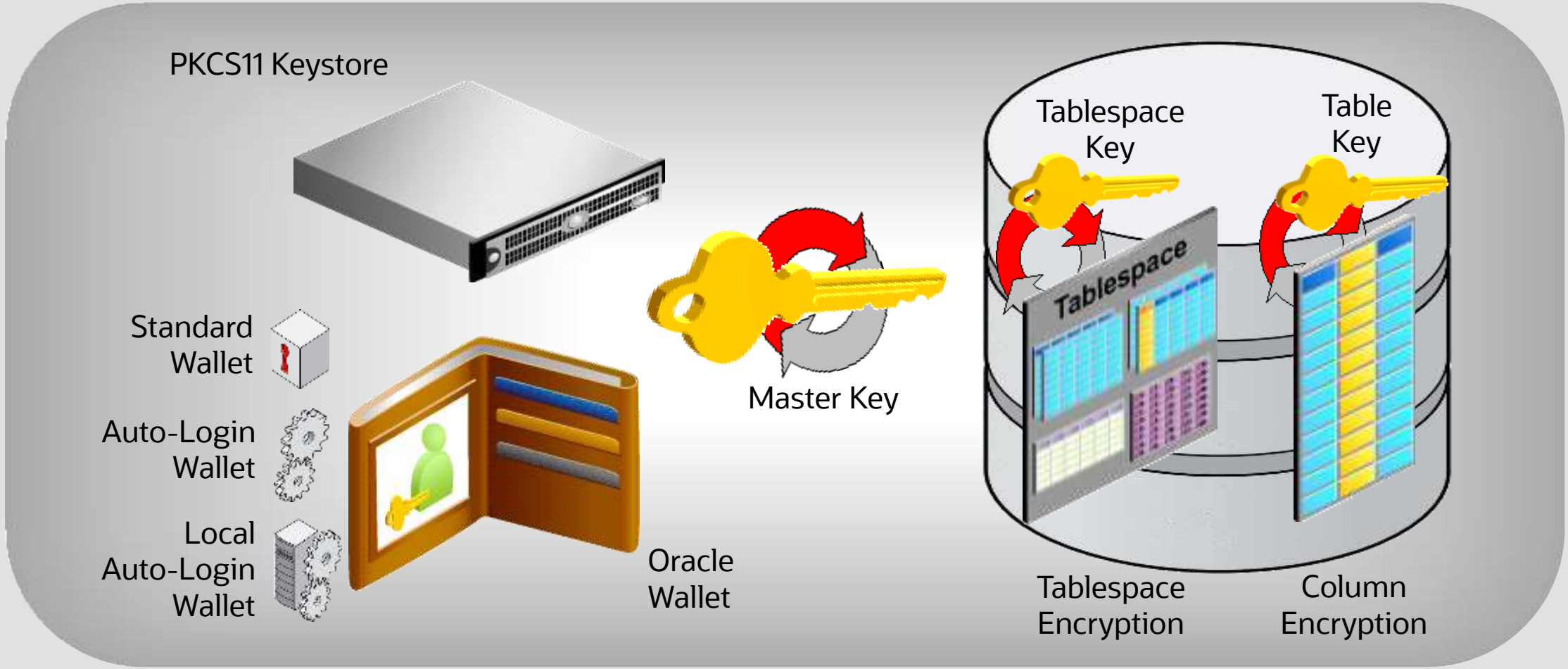
La clave maestra se almacena en un almacén PKCS#12



El responsable de seguridad abre el wallet

Las columnas se cifran con las claves de tablas

Arquitectura de claves de cifrado



Transparent Data Encryption

Backup con Data Pump y RMAN

Oracle Data Pump

- Exportación/importación masivos a ficheros planos

Oracle RMAN

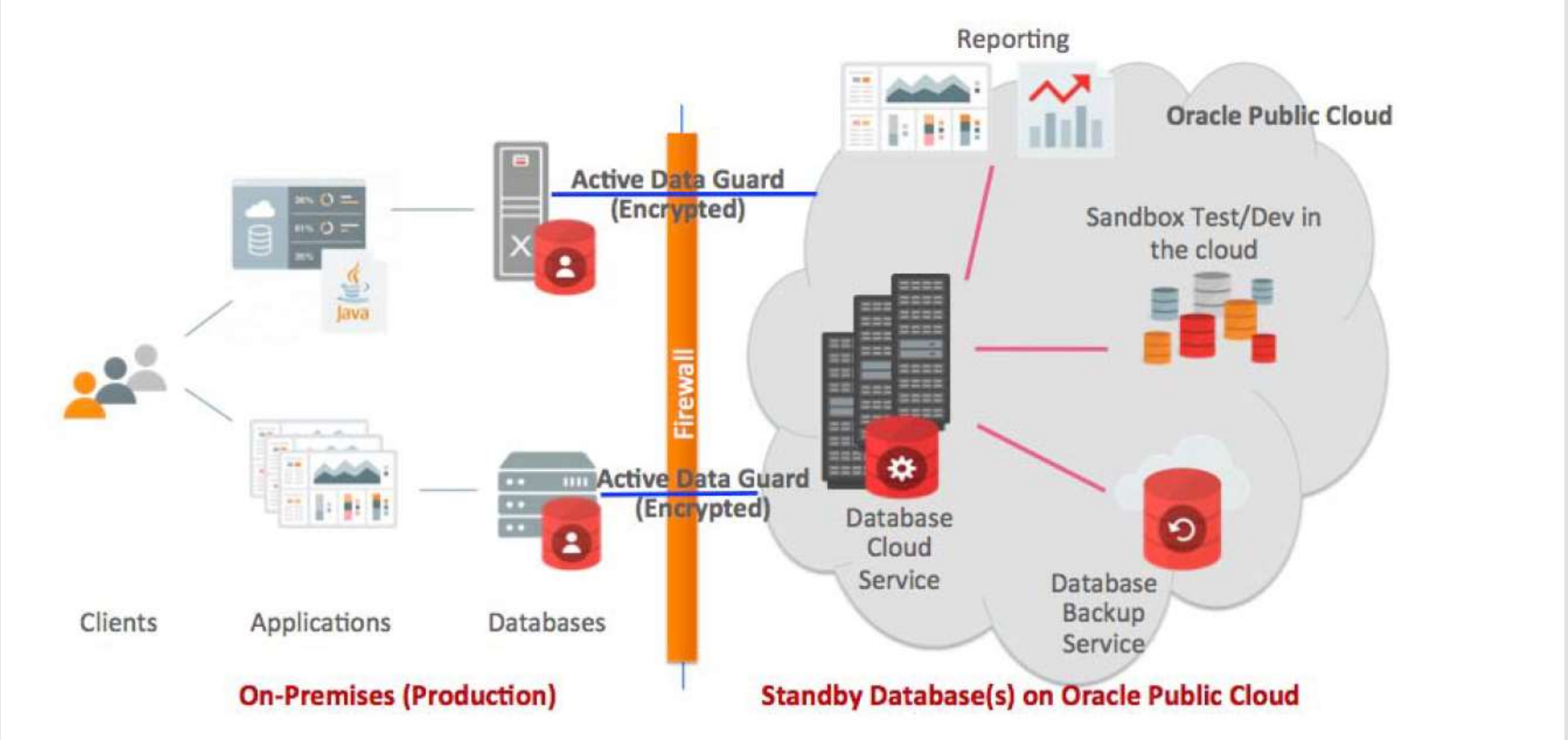
- *Backup & recovery* de BB.DD.

Utiliza las claves para cifrar el archivo de exportación o de copia de seguridad

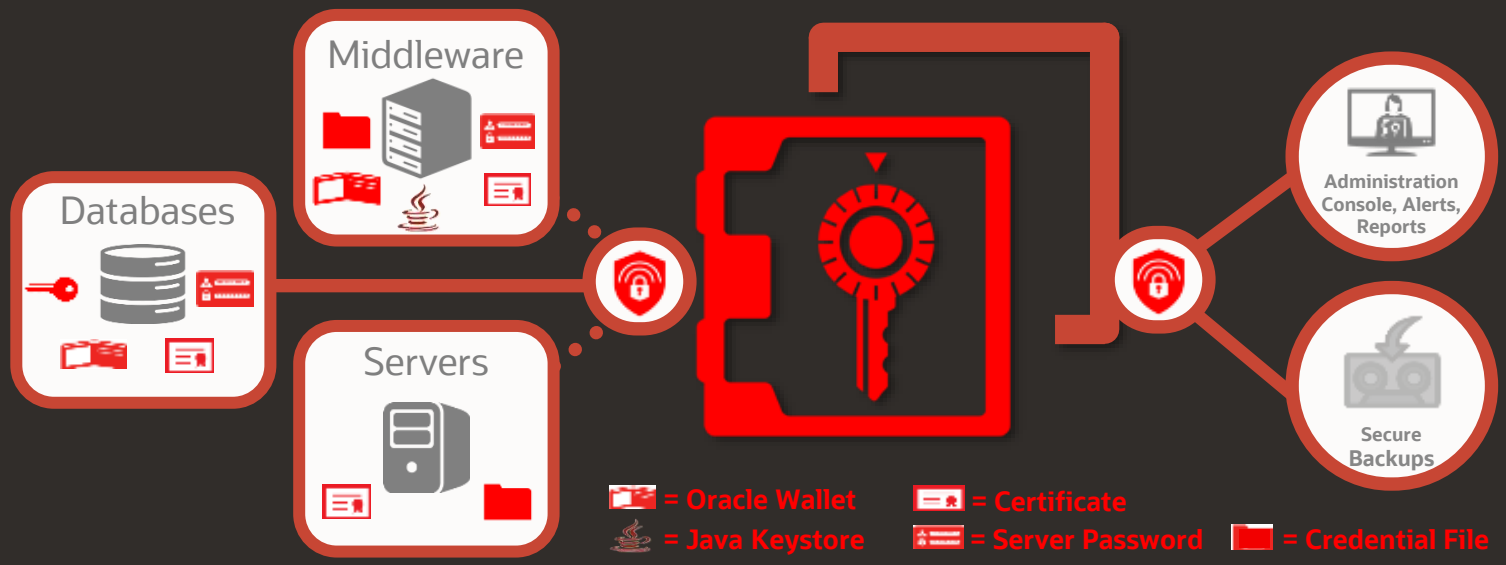
Completamente integrado en Oracle Database

Soporte TDE	Funcionalidad	Ejemplo de puntos de integración
✓	Compression	Oracle Advanced Compression, Exadata Hybrid Columnar Compression (EHCC)
✓	Backup and Restore	Oracle Recovery Manager (RMAN), Oracle Secure Backup (OSB)
✓	Export and Import	Oracle Data Pump Export and Import
✓	High-Availability Clusters	Oracle Real Application Clusters (RAC), Oracle Data Guard, Oracle Active Data Guard
✓	Replication	Oracle GoldenGate

Secure Desaster Recovery:
Data Guard Híbrido con Cifrado Transparente



Oracle Key Vault: Gestión centralizada de claves



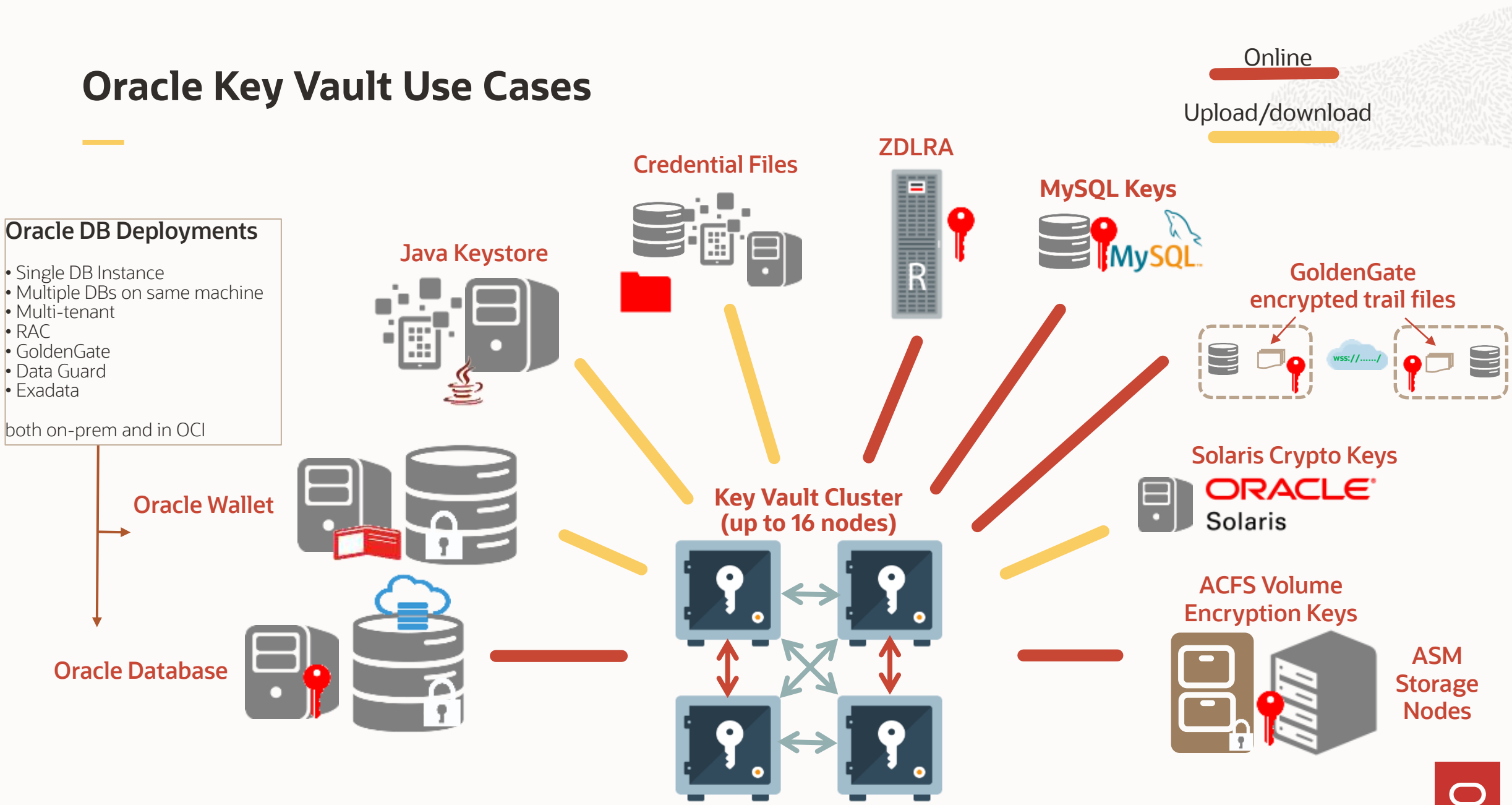
Archivado de wallets y keystore para retención a largo plazo

Fácil recuperación cuando estos ficheros son requeridos

Gestión centralizada de claves para las claves maestras de TDE

- Gestión del ciclo de vida de las claves
- Prevención de pérdida de claves
- Auditoría
- Distribución de claves

Oracle Key Vault Use Cases

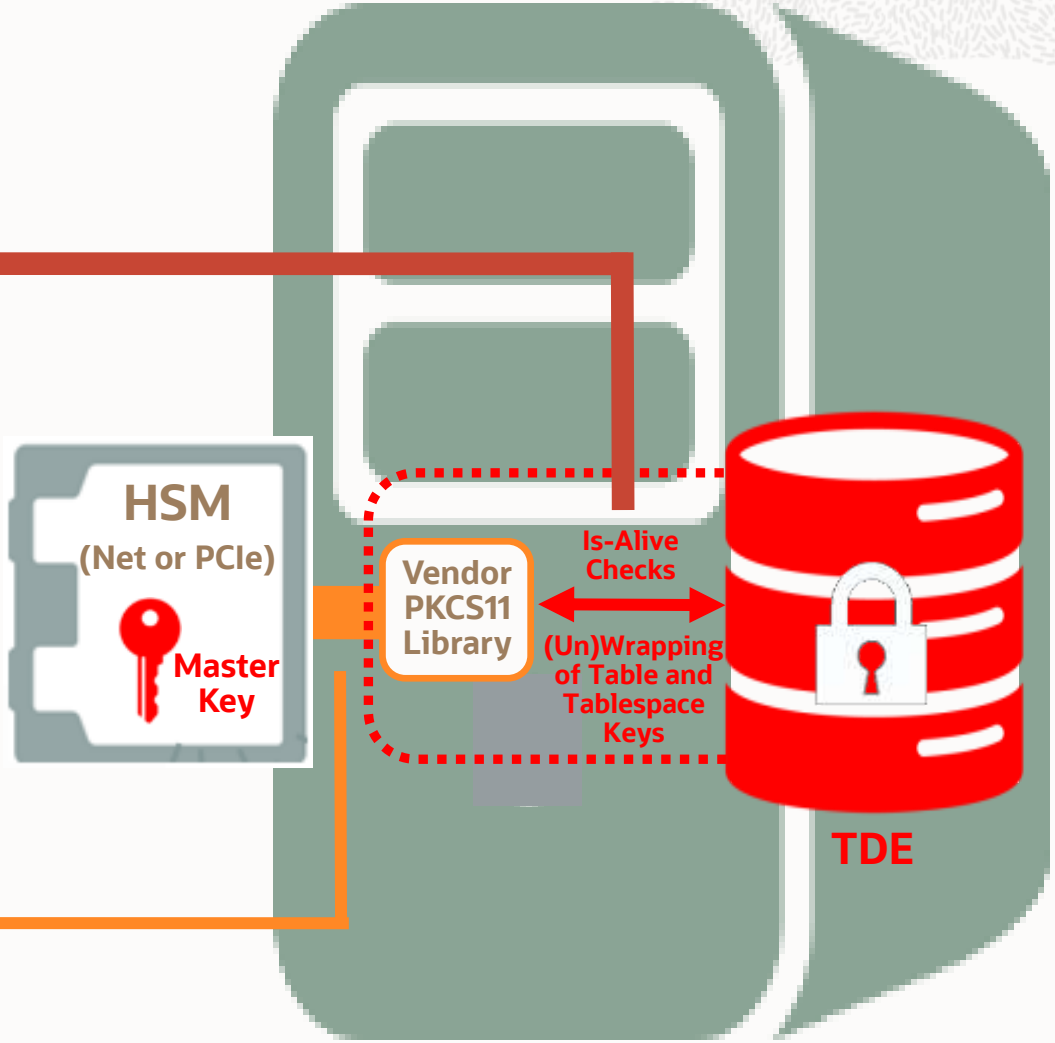


TDE and Hardware Security Modules (HSM) Interactions

1. DB loads PKCS11 client library
2. DB checks if HSM is alive
3. DB sends TDE table keys and tablespace keys

HSM Vendor Responsibility:

1. PKCS#11 library
2. Secure communication between PKCS11 client and HSM
3. Auditing and logging
4. HA redundancy and failover
5. Device backup and restore
6. Validation in real-life Oracle Database deployments



HSM Performance and Scalability Concerns

Database opens the connection to the HSM every time it needs to decrypt a tablespace or table key, as well as every three seconds to ensure the HSM is still available.

Some operations that require the key are:

- Every three seconds (a heartbeat to ensure the key store is available)
- Every time a new process opens an encrypted asset
- Database startup
- Encrypted datafiles brought online or new encrypted datafile
- Initial access to an encrypted column
- Direct-path imports/exports
- Redo log switch (each redo process, typically one per log file in the log group, makes its own call to the HSM)
- Direct-path parallel query operations (each server process/parallel query process makes its own call to the HSM)
- Golden Gate & Data Guard

Conclusion: A single production, enterprise-class database can make very high demands on an HSM

Credit: Russ Lowenthal

HSM Integration

HSM as root-of-trust

- SafeNet Luna 7000
- Thales nShield 6000+

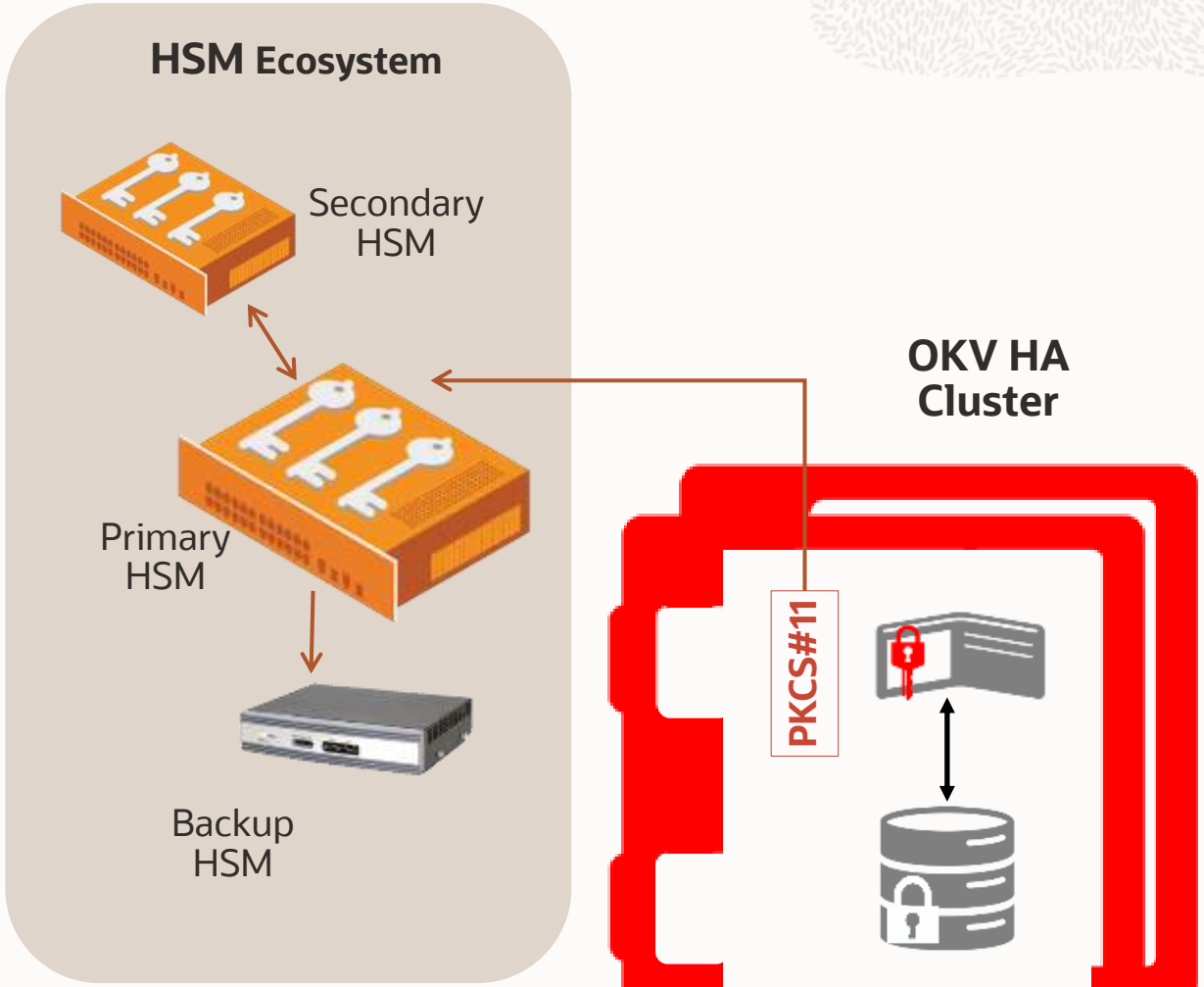
Root-of-trust remains in HSM

- Three tier hierarchy
- HSM root of trust protects wallet password which protects TDE master key

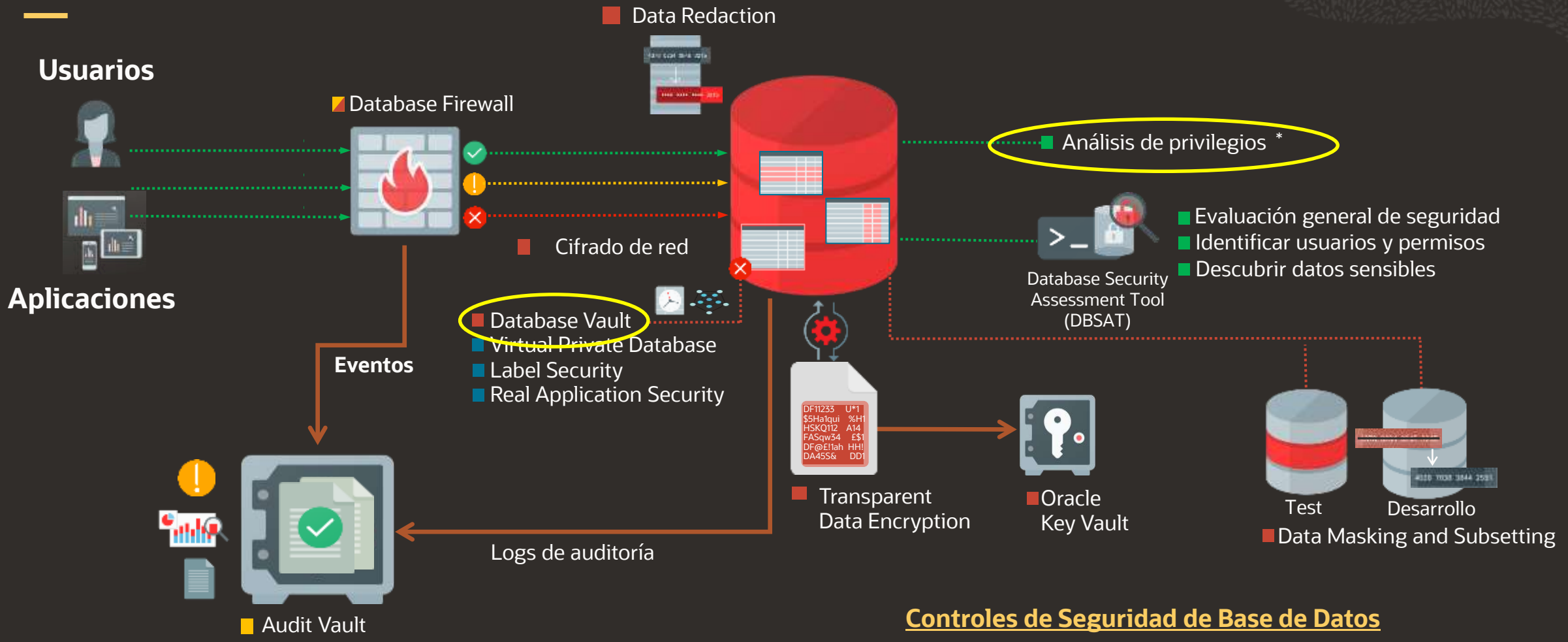
HSMs should also be deployed in HA configuration

- OKV 18.2 will ping the HSM regularly and alert if connection is lost
- OKV continues to function after HSM disconnected until next restart

HSM does not store customer keys



Arquitectura de máxima seguridad



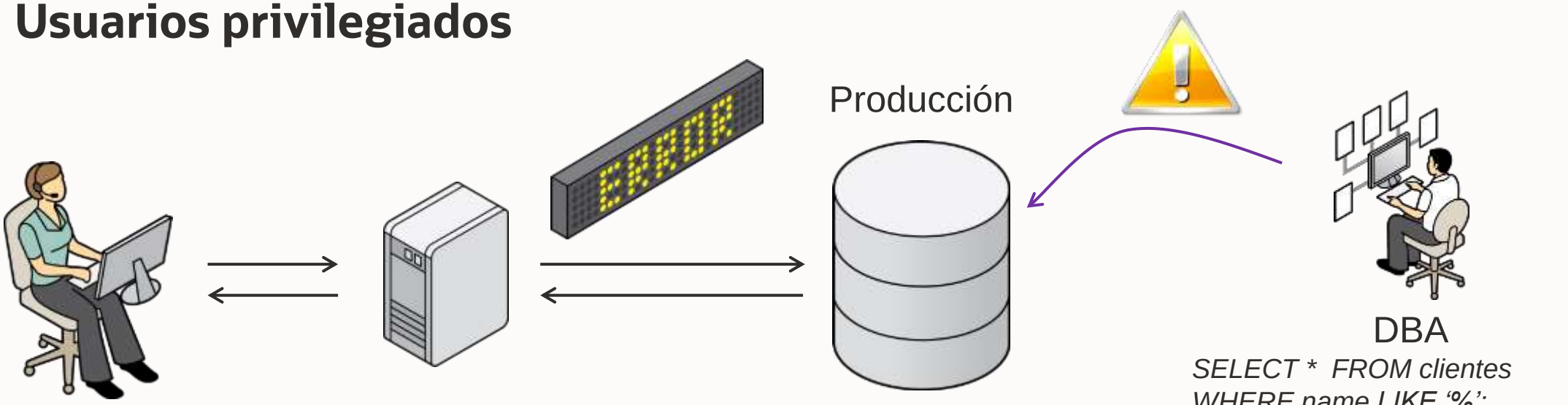
Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar** **Seguridad dirigida por datos**

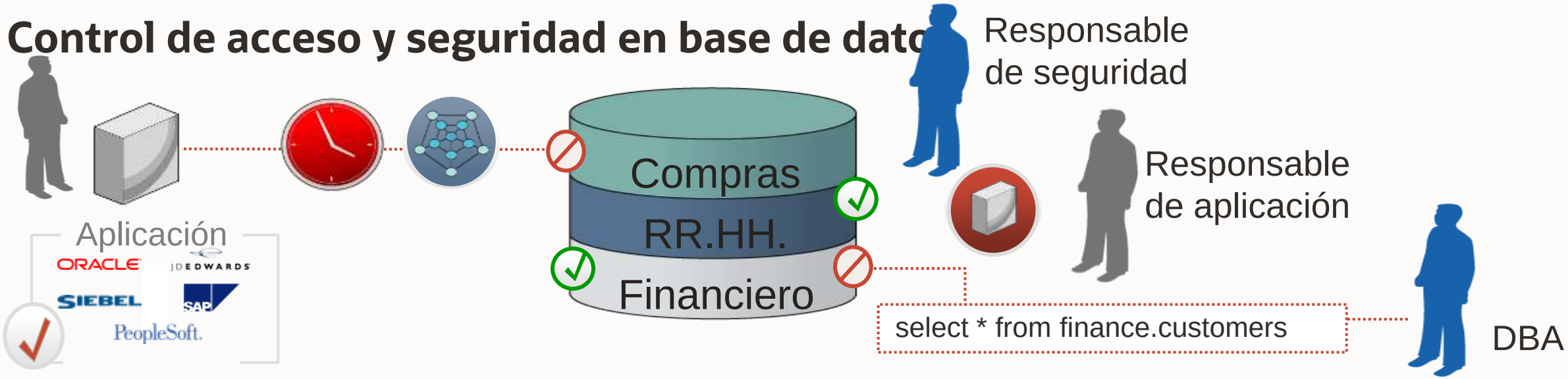
Oracle Database Vault

Problemáticas típicas

Usuarios privilegiados



Oracle Database Vault



- Segregación de funciones y cotos de seguridad
- Asegura quién, dónde, cuándo y cómo accede a la base de datos
  - Asegura los mínimos privilegios a los usuarios privilegiados
  - Evita el “puenteo” de las aplicaciones y asegura el gobierno de los datos
- Permite consolidar de forma segura los datos de aplicaciones multicompañía

Oracle Database Vault

Funcionalidades

Protege la Base de Datos con Separación de Funciones por Aplicación/Usuario/Objeto

Permite implementar controles de lectura/escritura de los datos de aplicación

Permite limitar a los DBA's y súper usuarios el acceso a los Datos Sensibles

Permite administrar los Objetos, aún cuando se limite el acceso a los datos

Proporciona un conjunto de Informes de seguridad para control y seguimiento de las medidas implementadas

La protección se implementa con carácter Selectivo para Usuarios y Objetos concretos

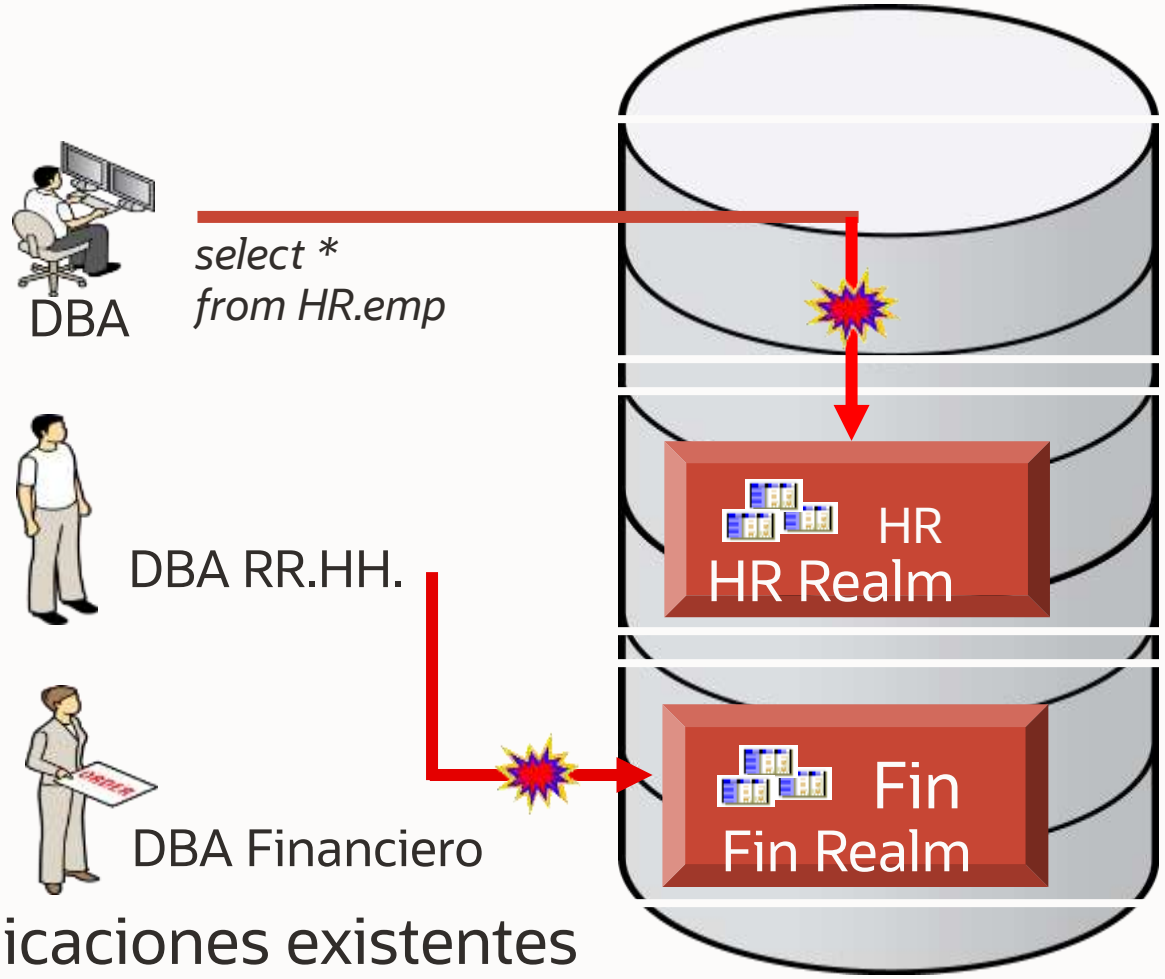
Oracle Database Vault

- DBA ve datos de RRHH

  Protección contra accesos

- DBA de RRHH ve Finan.

  Eliminando riesgos de seguridad por consolidación de servidores

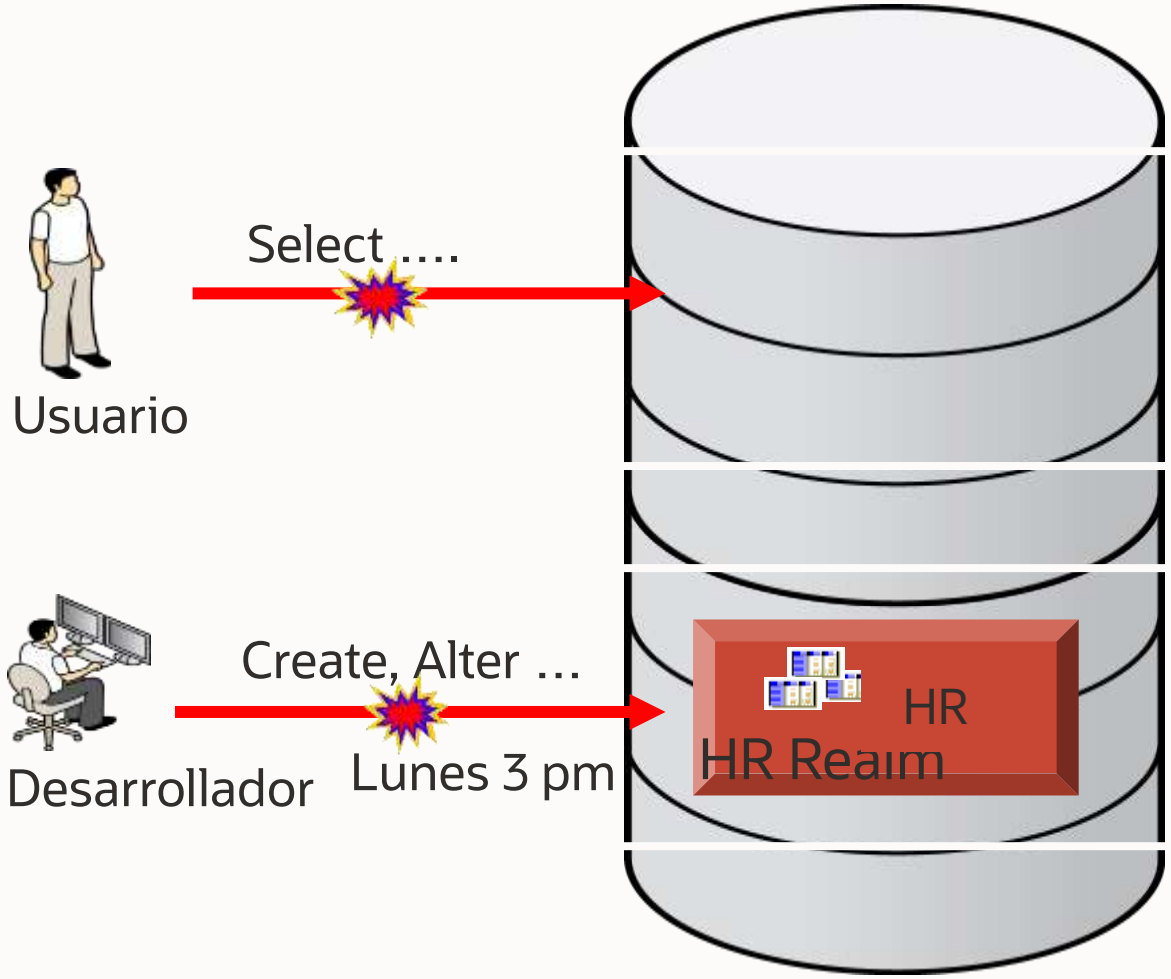


Pueden ser fácilmente aplicados a aplicaciones existentes con mínimo impacto en el rendimiento

Oracle Database Vault

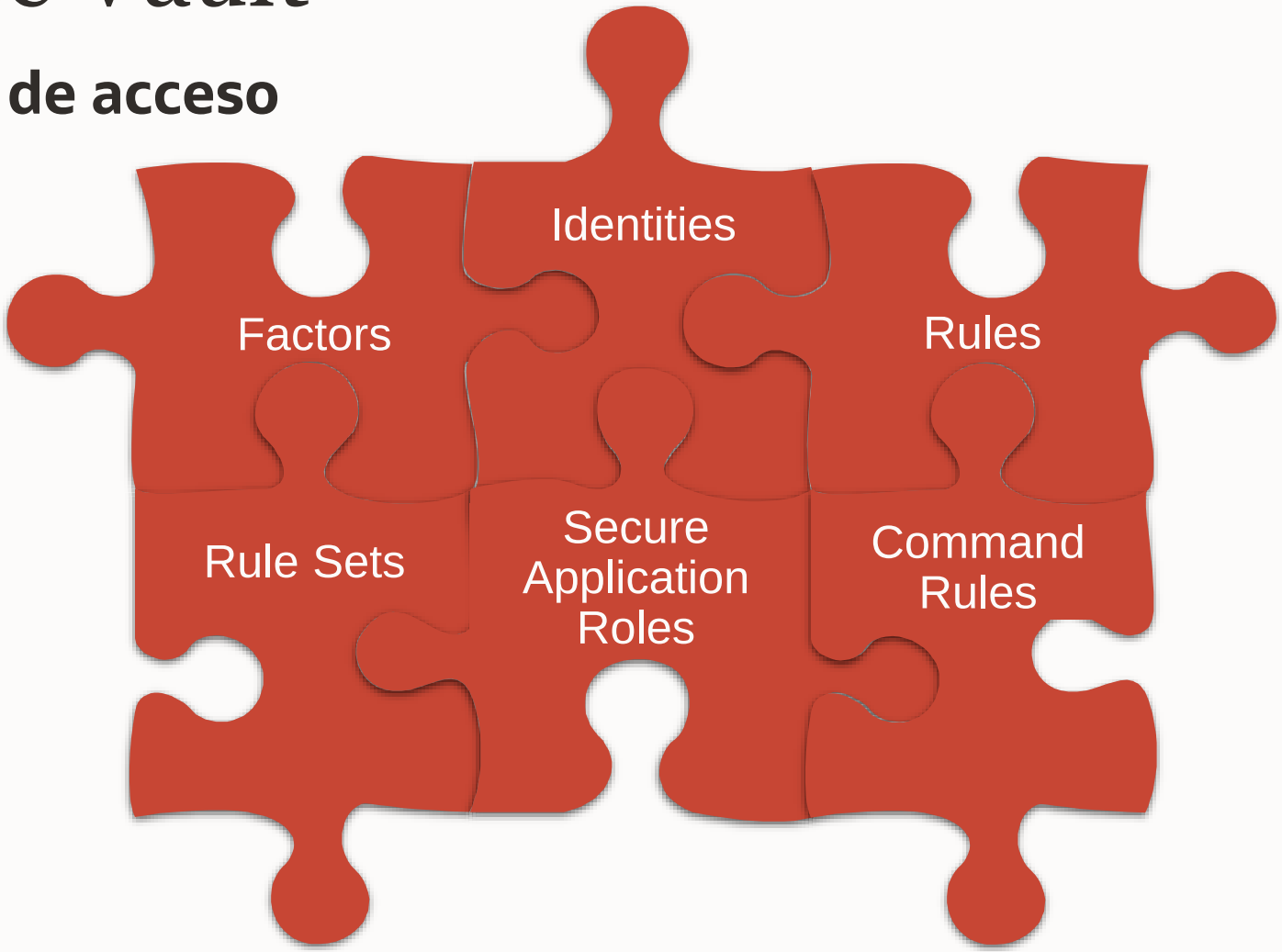
Políticas de control de acceso

- El usuario intenta acceder desde una IP no autorizada
  Regla basada en IP bloquea la acción
- El usuario realiza una tarea no autorizada en hora productiva
  Regla basada en fecha y hora bloquea la acción



Oracle Database Vault

Componentes de control de acceso



Oracle Database Vault

Un “Factor”

Es un parámetro de entorno (atributo de una sesión de BD)

Puede usarse individualmente o en combinación con otros factores (multi-factor authorization)

factores predefinidos

factores personalizables

Factores predefinidos (Ejemplos)

- Client_IP
- Database_Instance
- Domain
- Database_Name
- Session_User
- Machine
- Authentication_Method
- Program

Oracle Database Vault

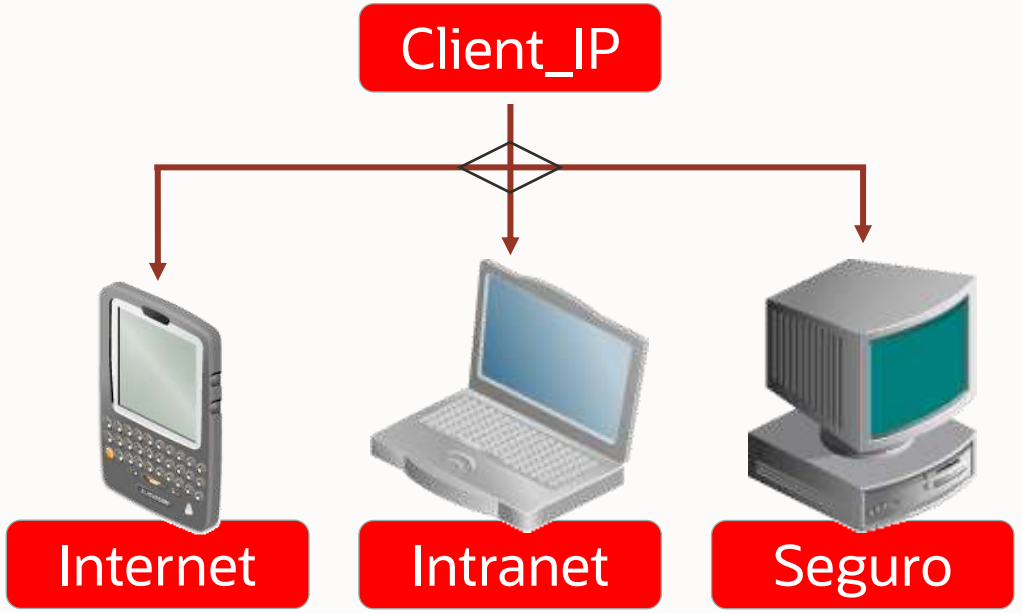
Una “identidad”

es el valor real de una variable de tipo factor

puede ser conocido o desconocido por anticipado

puede tener un nivel de confianza asociado

Ejemplo de nivel de confianza



Oracle Database Vault

Un "Rule Set"

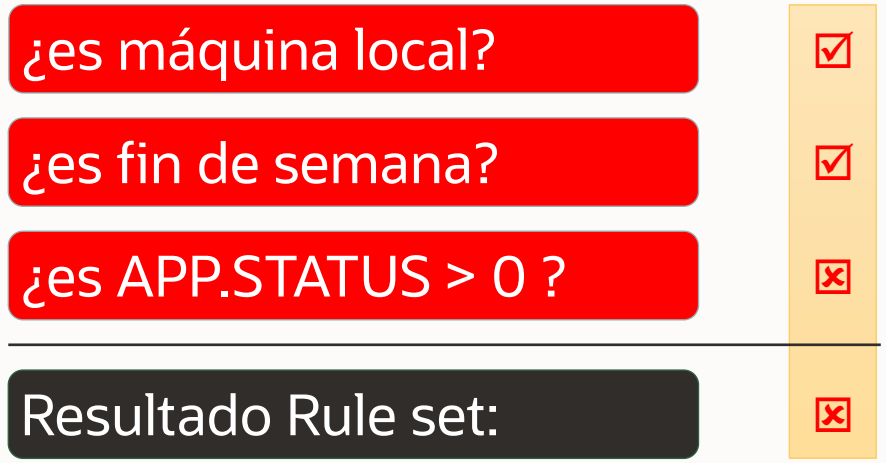
Es una colección de una o más reglas

Se evalua a Verdadero o Falso según la evaluación del contenido de cada regla

Tipos de evaluación

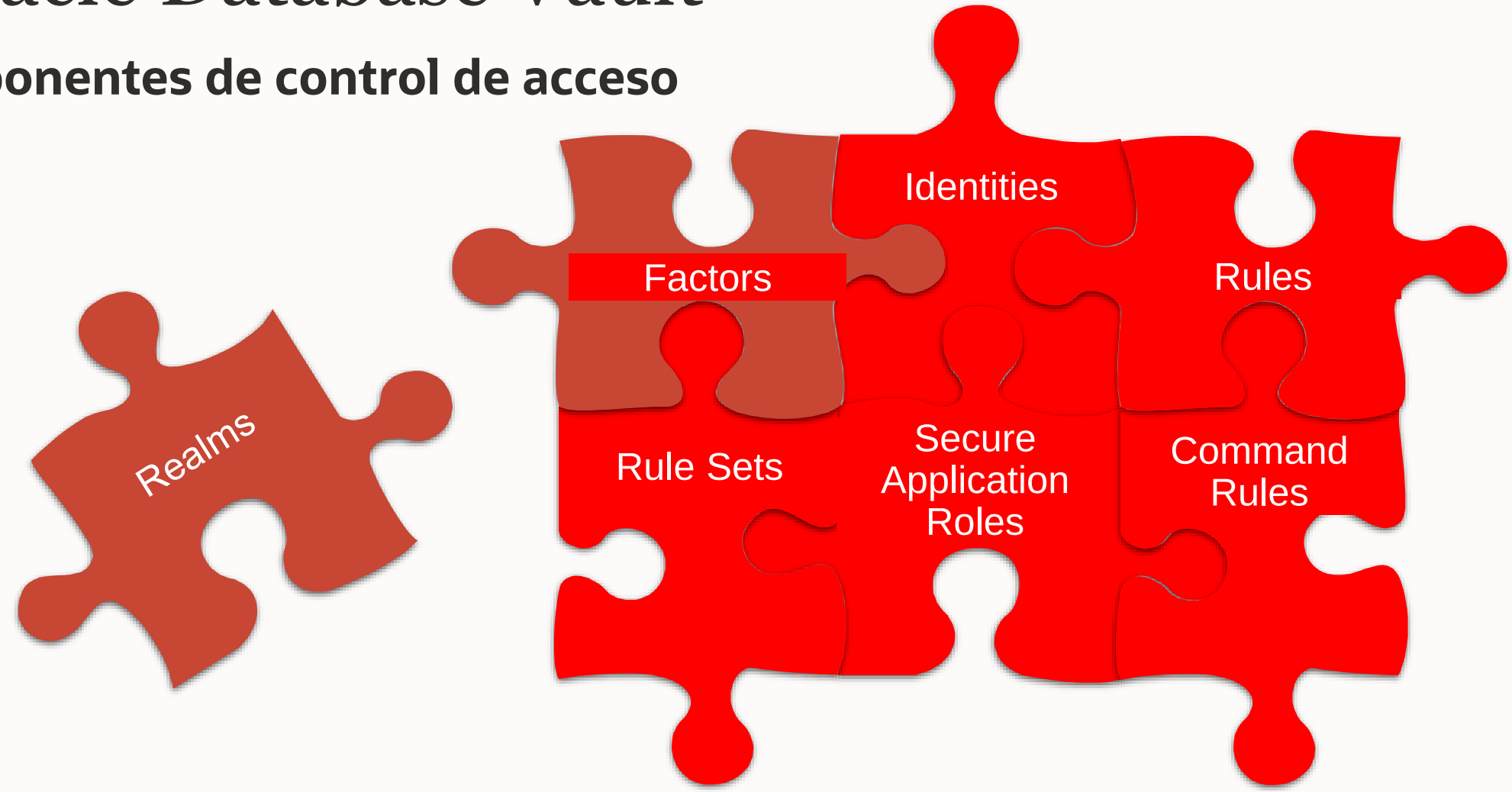
- Todos Verdad
- Alguno Verdad

Ejemplo de evaluación de Rule Set "Todos Verdad"



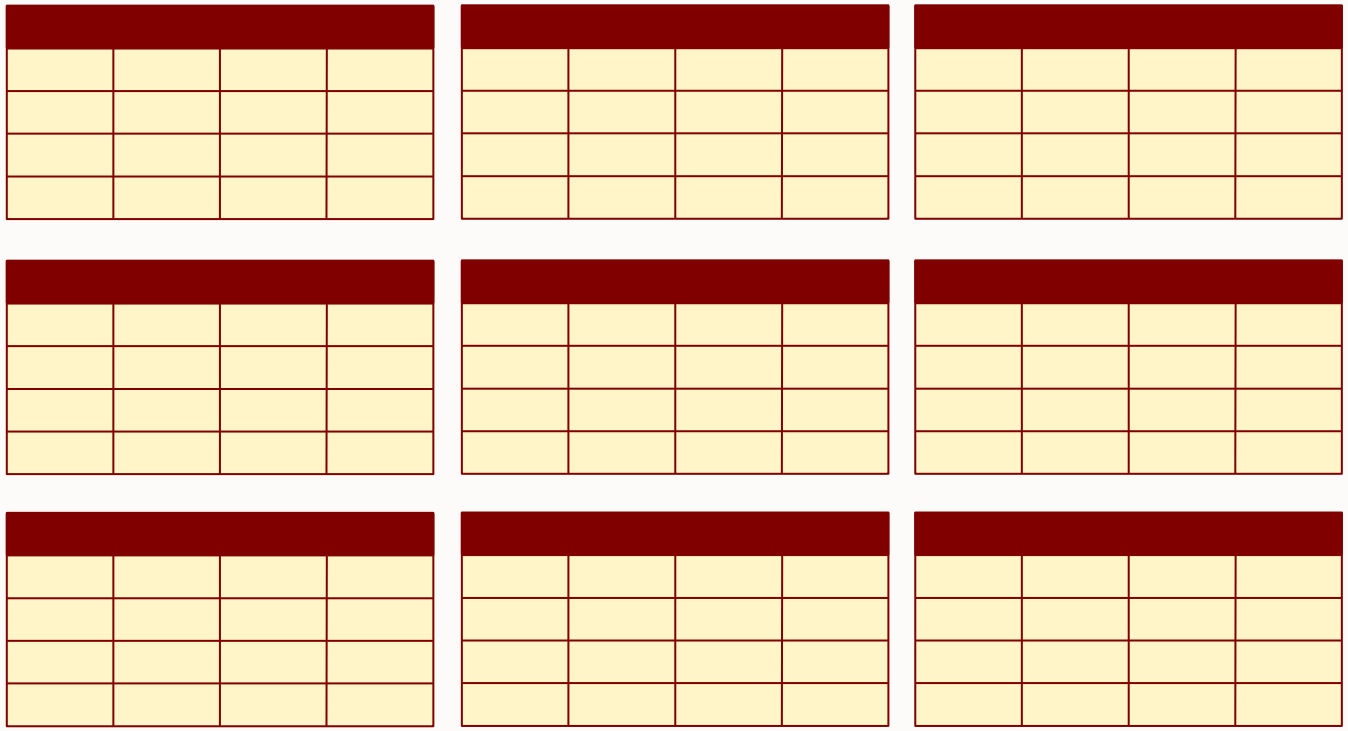
Oracle Database Vault

Componentes de control de acceso



Oracle Database Vault

Realms

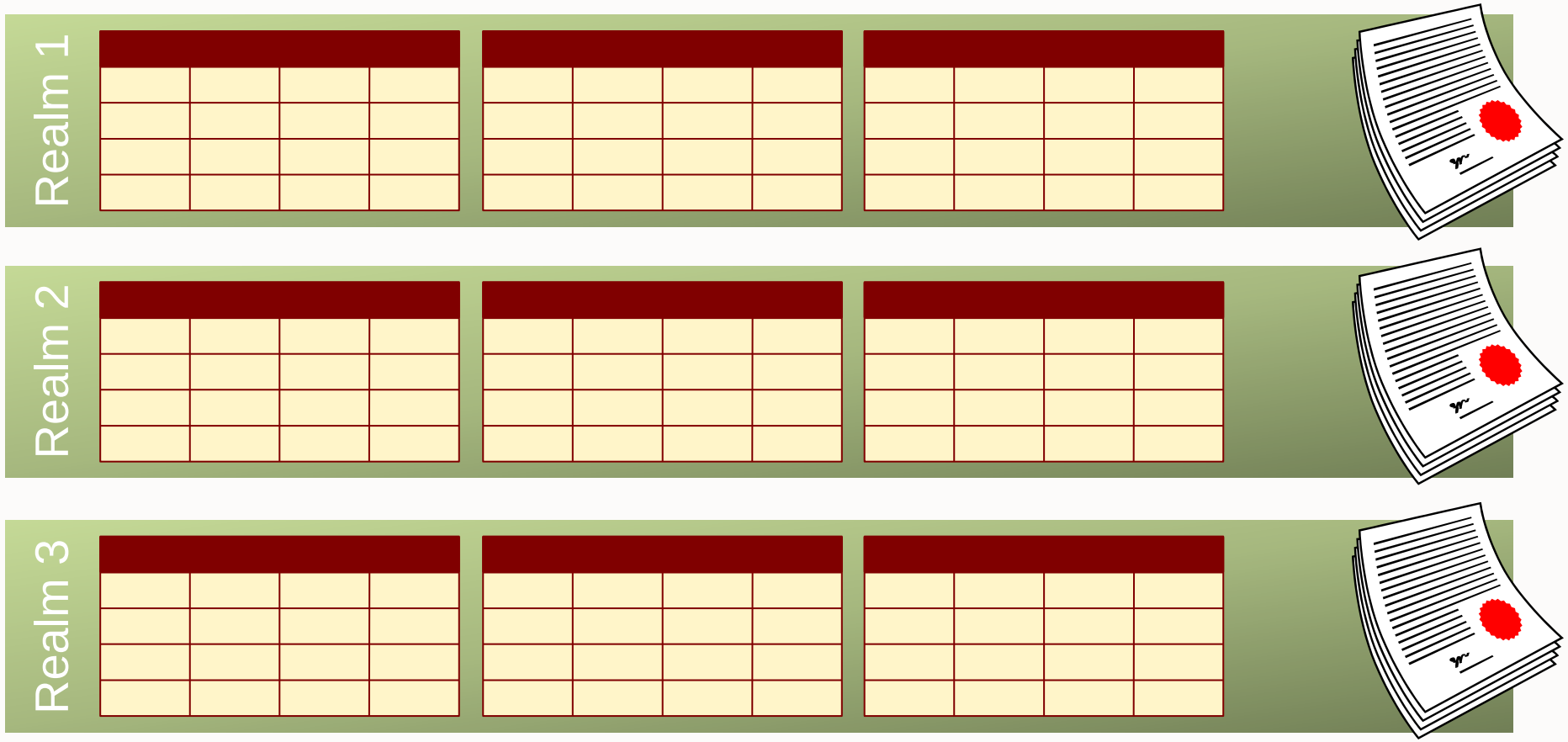


¿Cómo aplicar una política de control de acceso a decenas de miles de tablas?

- Las políticas pueden ser complejas
- Pueden ser diferentes para distintos grupos de tablas

Oracle Database Vault

Realms



Oracle Database Vault

Conceptos: Realm

Agrupación de esquemas, roles que deben estar seguros en un entorno de aplicación o base de datos

Los *Realms* son agrupaciones lógicas de objetos de base de datos, como tablas, vistas, paquetes, privilegios, ...

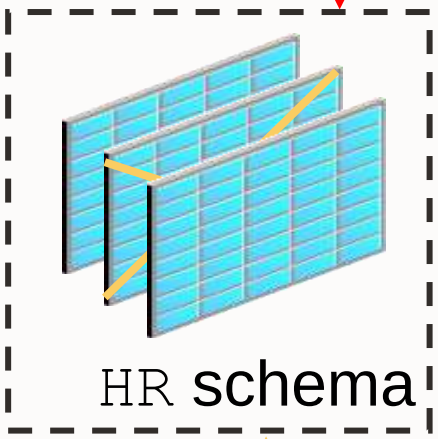
Los *Realms* pueden contener *Rule Sets* para un mayor filtro de acceso.

Oracle Database Vault

Ejemplo: Segregación de funciones

1 *SALES_DBA* posee el role *DBA* y puede borrar tablas de *HR*:

```
SQL> CONNECT sales_dba/password
SQL> DROP TABLE hr.bonus_it;
Table dropped.
```



2 El administrador de DV rea un realm para asegurar las tablas *HR*:

Realm Secured Objects

Create | Edit | Remove

Select	Owner	Object Type	Object Name
◉	HR	TABLE	%

Edit | Remove

3 *SALES_DBA* intenta borrar la tabla restaurada *bonus_it*:

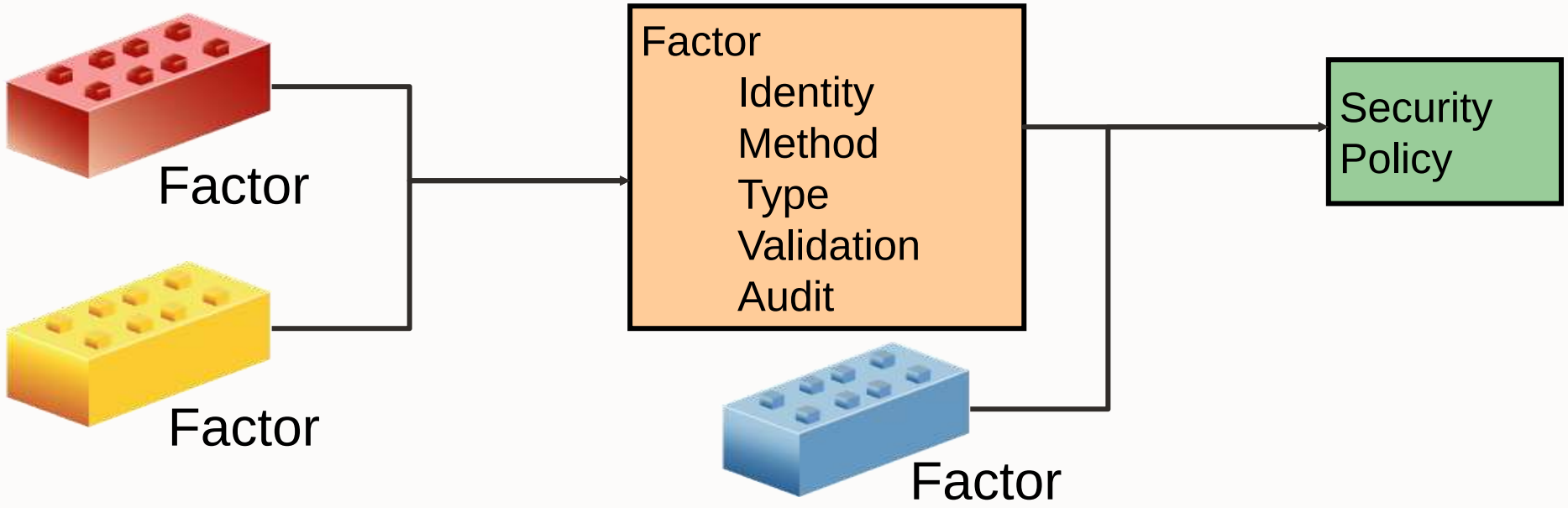
```
SQL> DROP TABLE hr.bonus_it;
ORA-20401: Realm Violation for drop table on
    HR.BONUS_IT
```

Oracle Database Vault

Conceptos: Factores

Son variables o atributos construidos para la configuración de políticas de seguridad y dotar de filtros de acceso a los datos y usuarios.

Tiene un valor asignado llamado identidad. Ejemplo Intranet/Internet



Oracle Database Vault

Conceptos: Factores

Externo

Domain = INTERNET

```
SELECT * FROM hr.employees
```

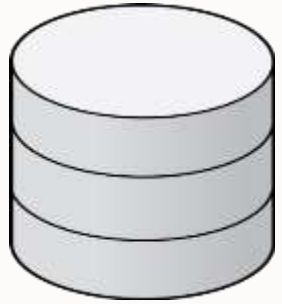
RR.HH.

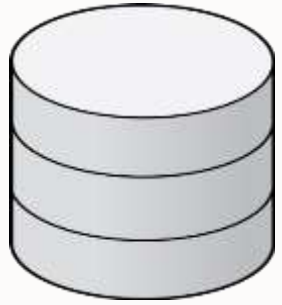
WorkHours = FINdeSEMANA

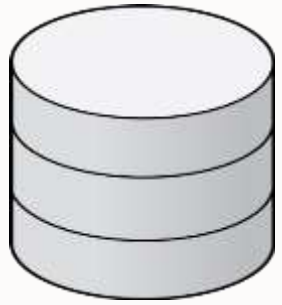
```
UPDATE hr.employees
```

Domain = SEGURO

```
INSERT … INTO sh.sales
```







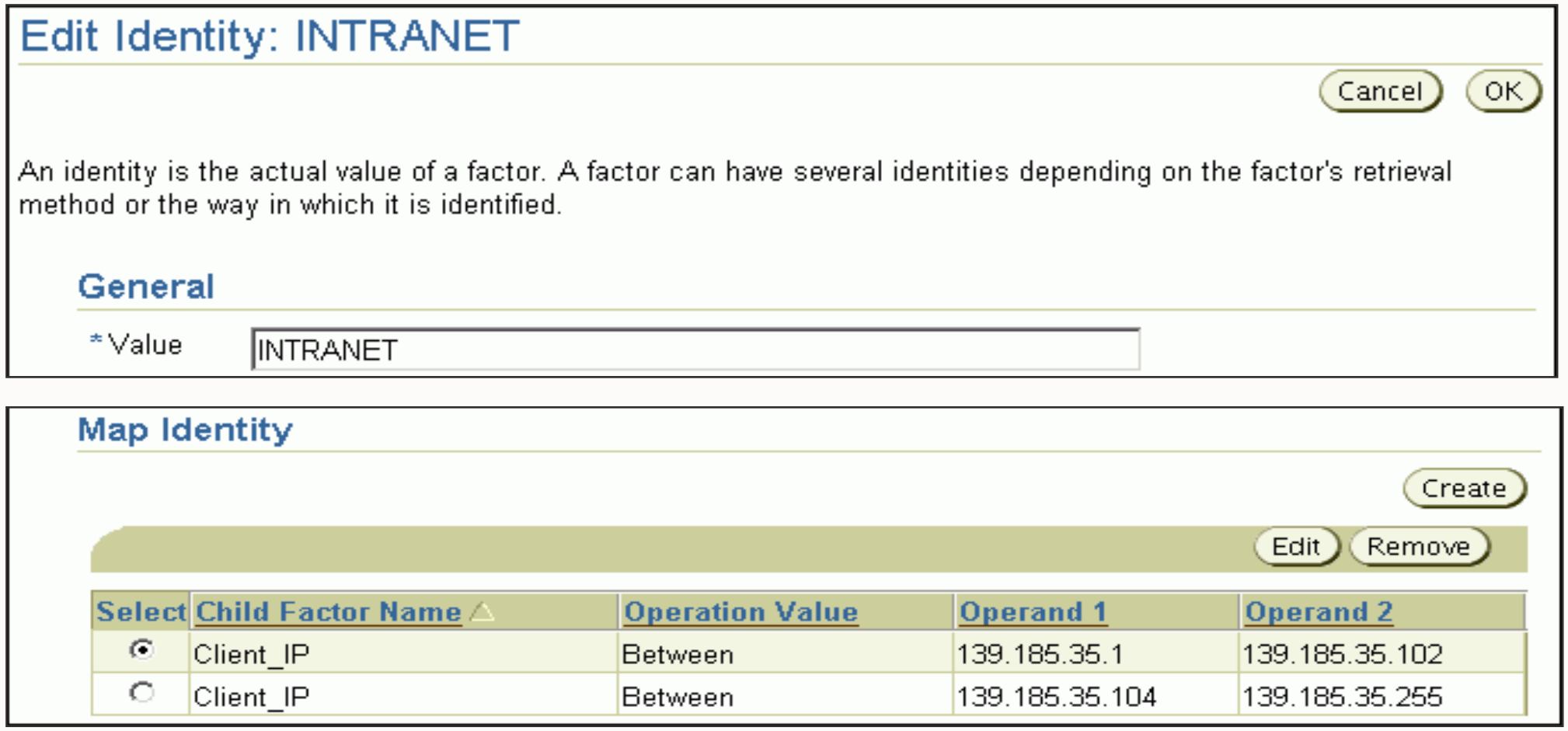
Oracle Database Vault

Conceptos: Rule Set

Rule Set es una colección de una o más reglas que se pueden asociar a un *Realm* o *Command rule*.
El *Rule Set* evalúa “true” o “false” según el contenido de la expresión (función) de cada regla.
Se utiliza para dotar de mayor restricción al *Realm*.
Los *Rule Sets* pueden contener *Factors* para un mayor filtro de acceso.

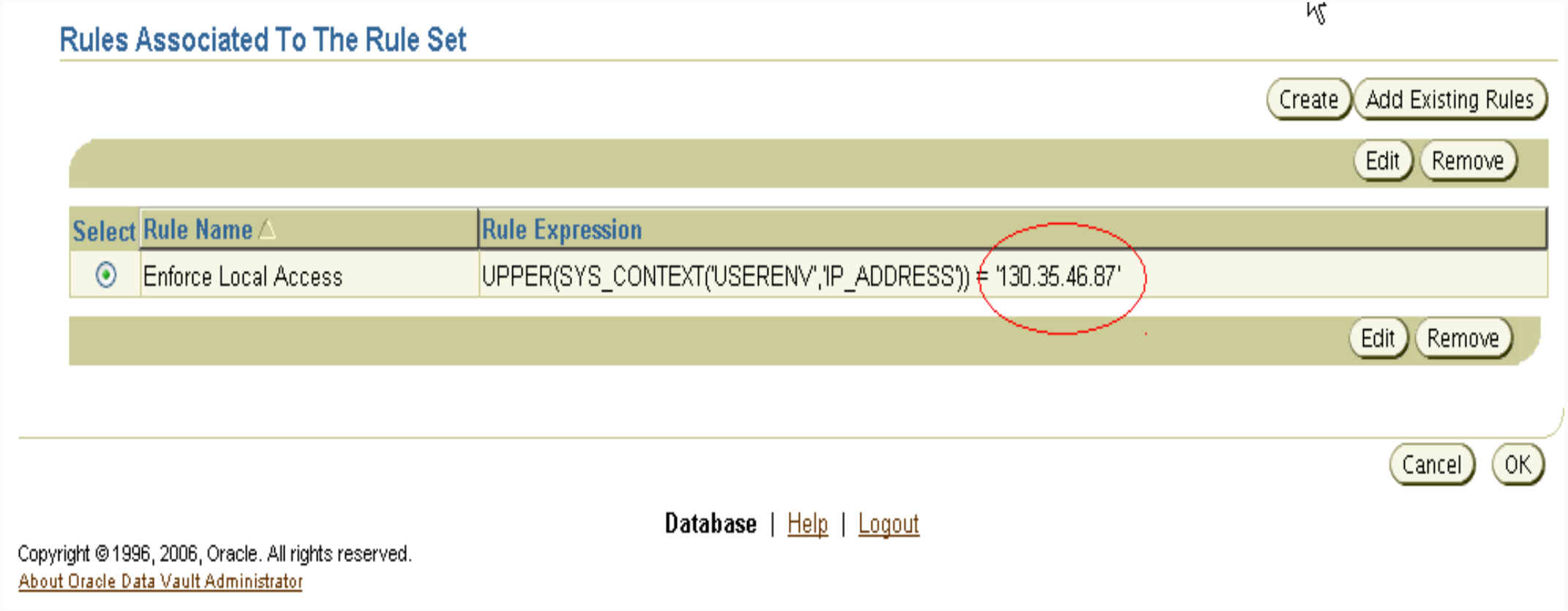
Oracle Database Vault

Conceptos: Factores



Oracle Database Vault

Ejemplo: Regla basada en IP



Oracle Database Vault

Conceptos: Command Rule

Command Rule es una regla global que se crea para controlar el uso de sentencias y operaciones (select, alter system, dml o ddl) disponibles en la base de datos.

Las *Command Rules* pueden contener *Rule Sets* para un mayor filtro de acceso.

Oracle Database Vault

Ejemplo: Command Rule

1 El usuario *OE* altera la tabla *OE.ORDERS*:

```
SQL> ALTER TABLE oe.orders ADD (my_code VARCHAR2(10));
Table altered.
```

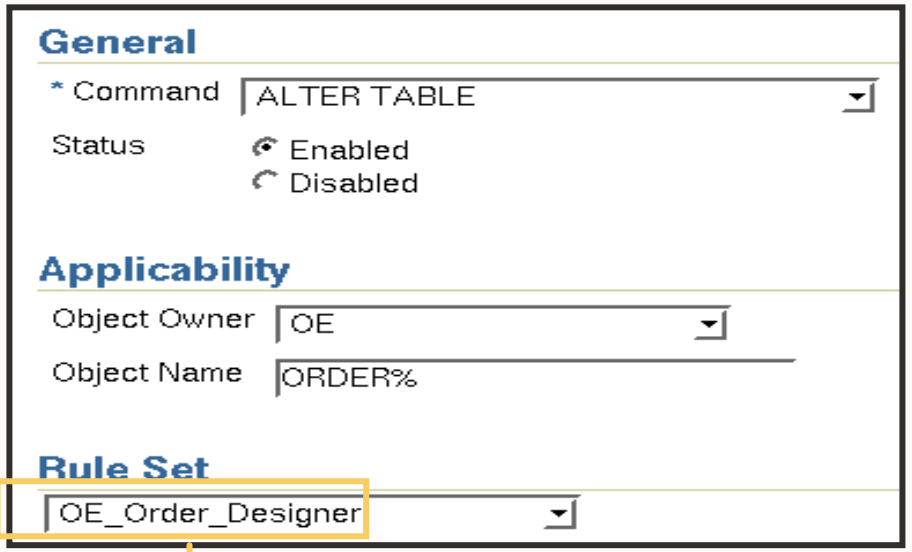
2 El usuario *OE_ORDERS_DBA* no estaba notificado

3 *OE_ORDERS_DBA* tiene un role creado y se concede grant a si mismo:

```
SQL> CREATE ROLE ORDER_APP_DBA;
SQL> GRANT order_app_dba TO OE_ORDERS_DBA;
```

Oracle Database Vault

Ejemplo: Command Rule

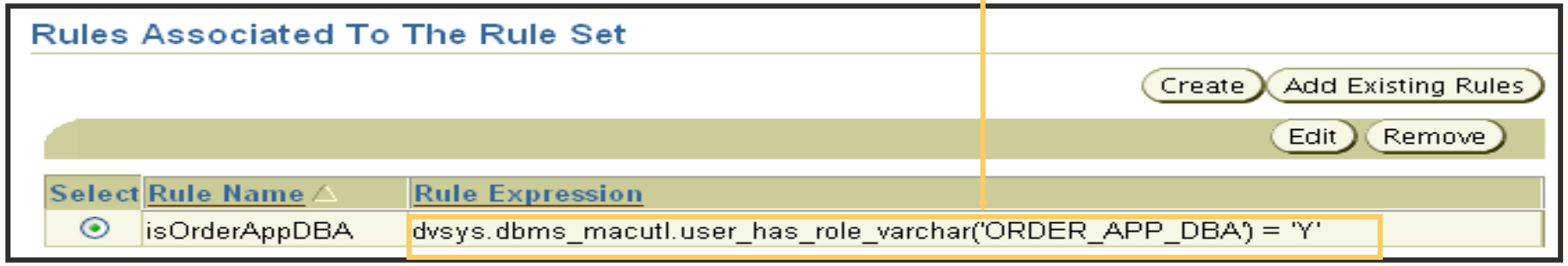


4

El usuario administrador de Database Vault crea un command rule para prevenir alterar las tablas *ORDER%*.

Usuario debe tener el role `ORDER_APP_DBA`

`OE_Order_Designer` rule set:



Oracle Database Vault

Ejemplo: Command Rule

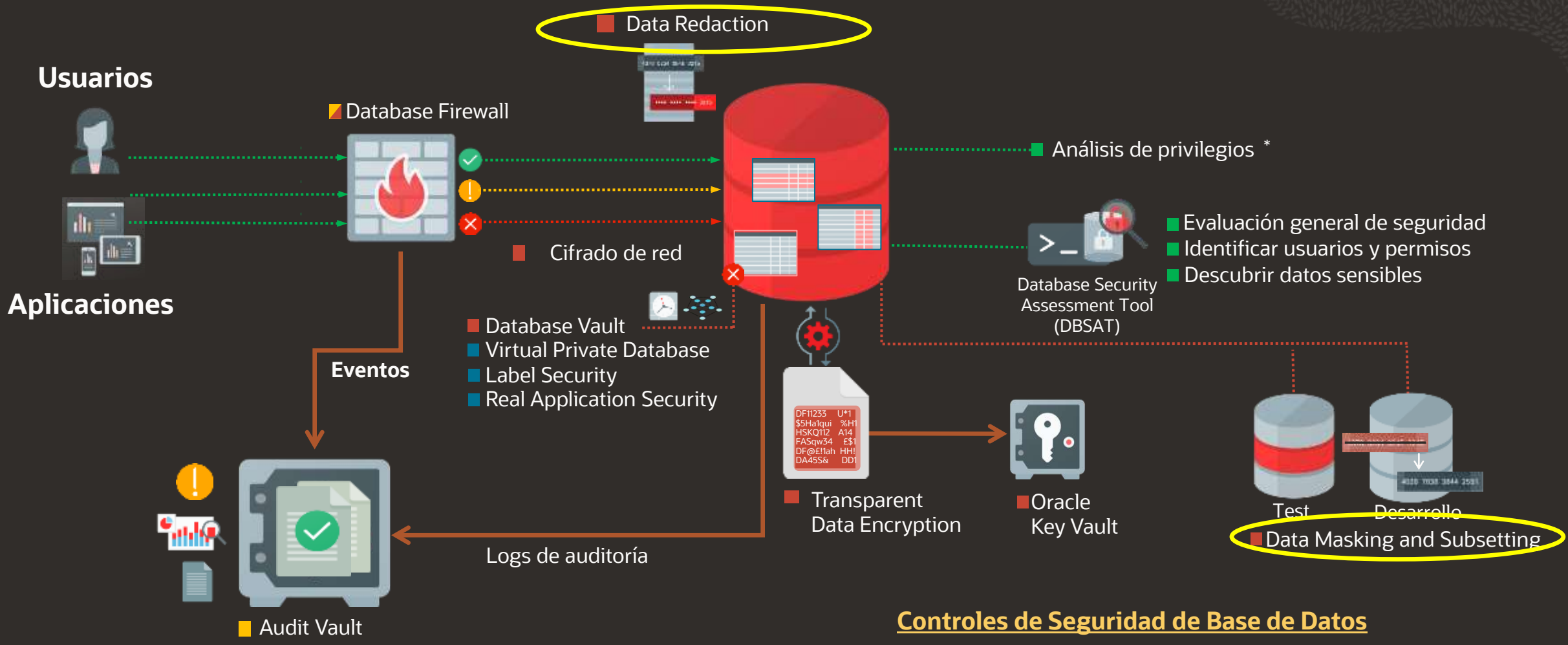
5 Ahora cuando *OE* intenta alterar las tabla *ORDER*, se produce una violación de regla:

```
SQL> ALTER TABLE oe.orders ADD (my_code NUMBER);
ORA-47400: Command Rule Violation for alter table on OE.ORDERS
```

6 Incluso cuando *OE* intenta alterar una tabla diferente,
se produce una violación de regla:

```
SQL> ALTER TABLE oe.order_items ADD (my_code NUMBER);
ORA-47400: Command Rule Violation for alter table on
    OE.ORDER_ITEMS
```

Arquitectura de máxima seguridad



Controles de Seguridad de Base de Datos

Evaluar **Prevenir** **Detectar** **Seguridad dirigida por datos**

Oracle Data Redaction (incluido en ASO)

Oracle Advanced Security

Protección avanzada para bases de datos Oracle

Transparent Data Encryption (TDE)

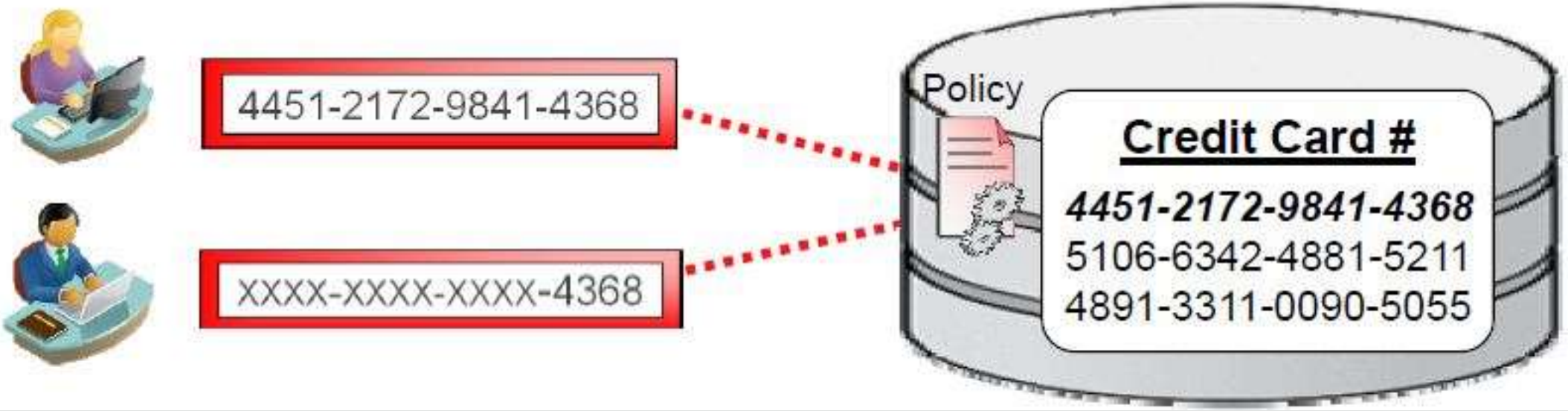
- Cifra de forma transparente los datos en disco de la base de datos y gestiona de forma segura las claves de cifrado
- Protege frente a perdida o robo de discos o backups
- Impide a usuarios de OS inspeccionar los ficheros BD

Data Redaction

- **Censura “on line” de datos sensibles de las aplicaciones**
- **Políticas declarativas gestionadas de forma central en la base de datos**
- **Decisiones tomadas en función del contexto**
- **Multiples transformaciones para elegir**

Oracle Advanced Security

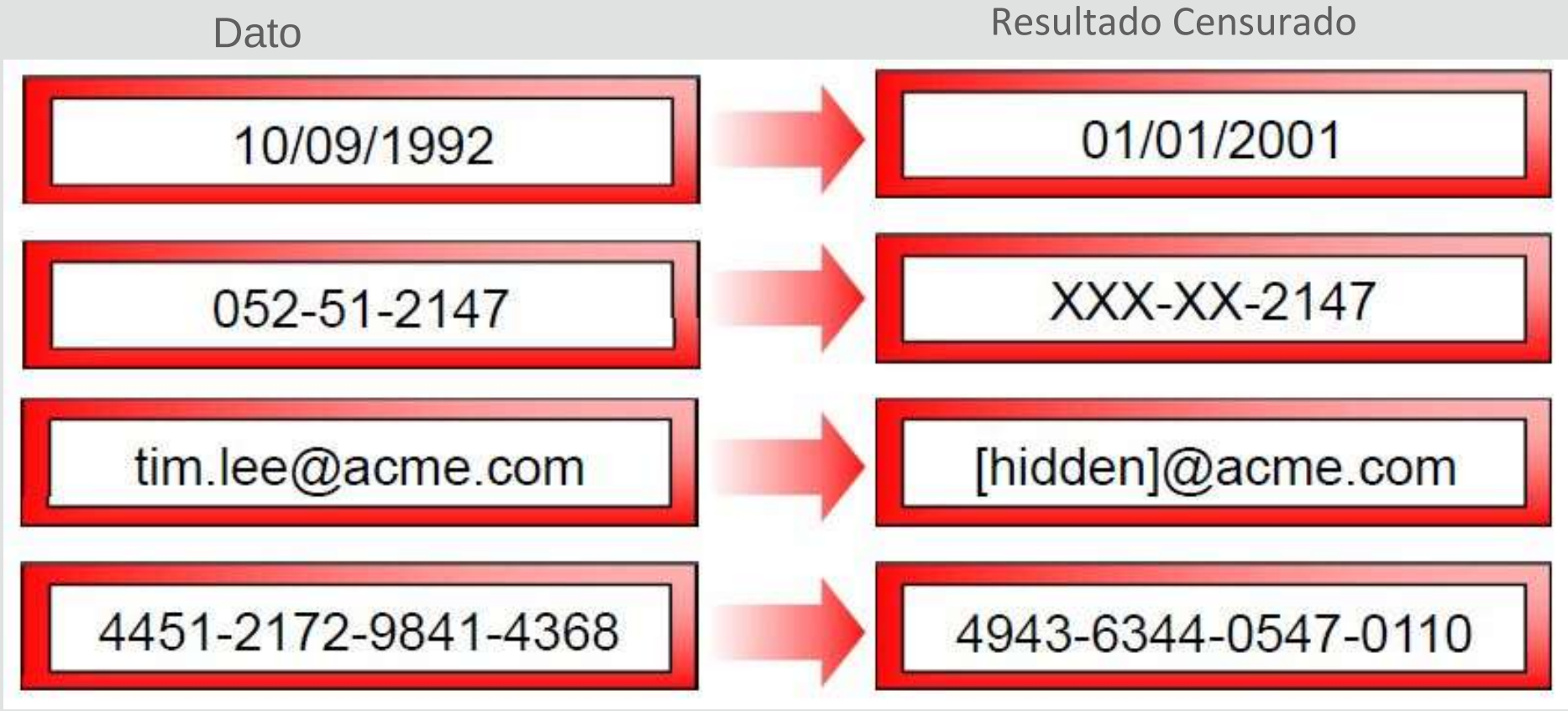
Data Redaction



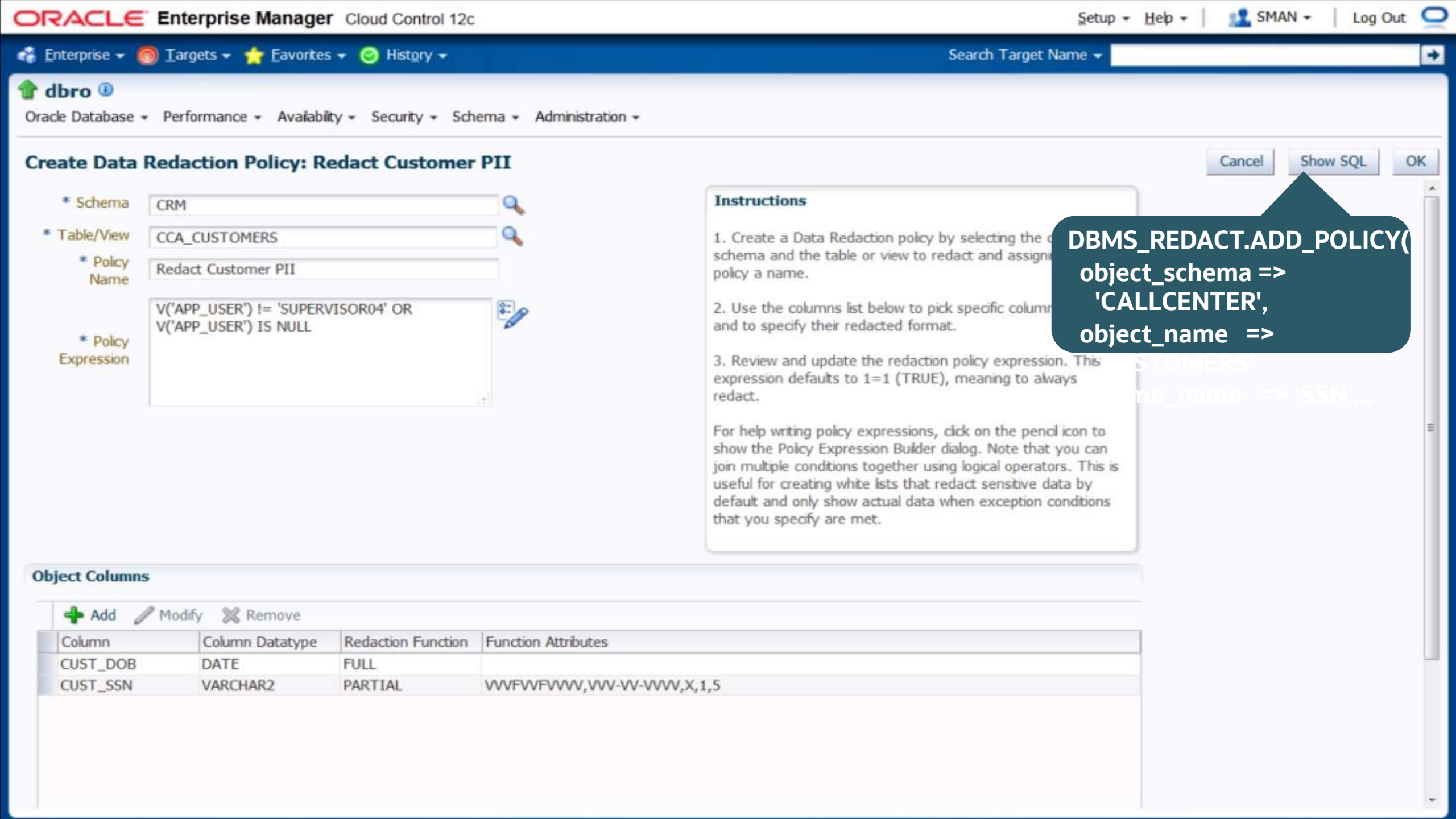
Censura de datos on-line basada en usuario, IP, contexto de aplicación u otros factores

Transparente. Impacto mínimo en cargas de producción

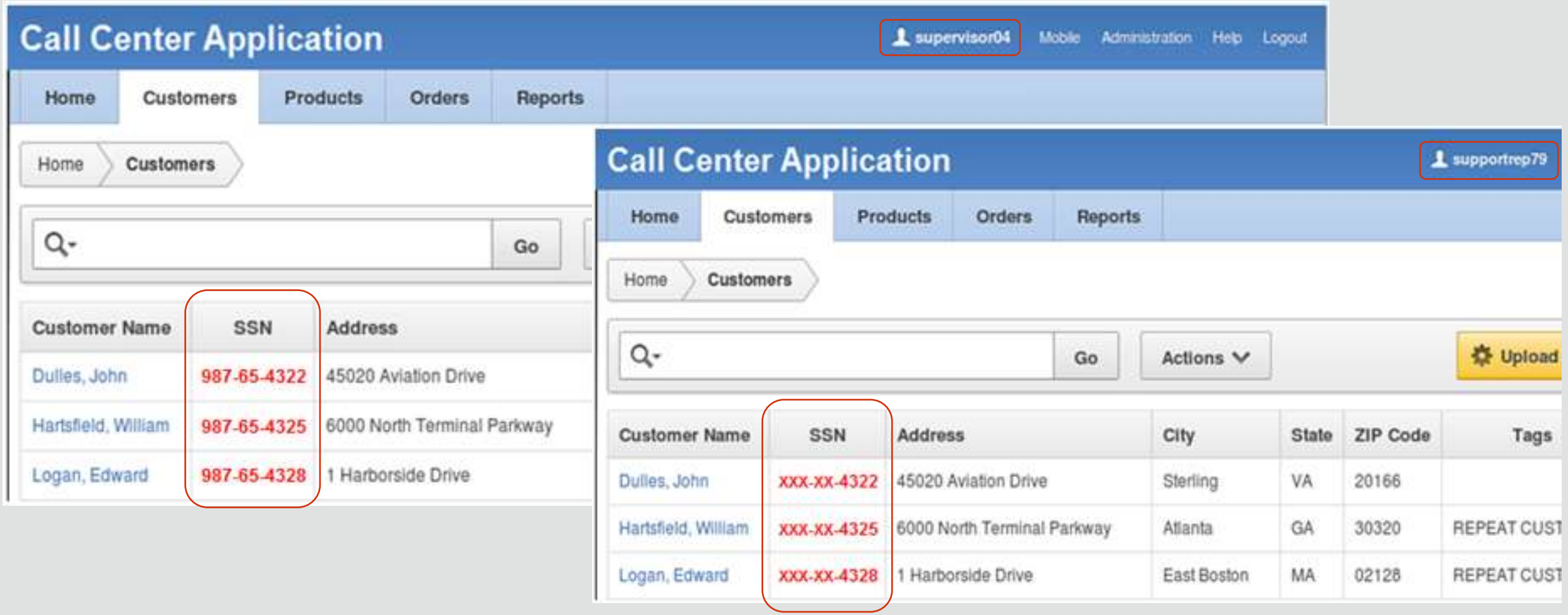
Oracle Data Redaction



- Incluye librería de formatos para datos comunes de PCI y PII
- Gestionable con Enterprise Manager ó API de línea de comando


ORACLE Enterprise Manager Cloud Control 12c
Setup
Help
SMAN
Log Out
Enterprise
Targets
Favorites
History
Search Target Name
dbro
Oracle Database
Performance
Availability
Security
Schema
Administration
Create Data Redaction Policy: Redact Customer PII
Cancel
Show SQL
OK
* Schema
CRM
* Table/View
CCA_CUSTOMERS
* Policy Name
Redact Customer PII
* Policy Expression
V('APP_USER') != 'SUPERVISOR04' OR
V('APP_USER') IS NULL
Instructions
1. Create a Data Redaction policy by selecting the
schema and the table or view to redact and assign
policy a name.
2. Use the columns list below to pick specific colum
and to specify their redacted format.
3. Review and update the redaction policy expression. This expression defaults to 1=1 (TRUE), meaning to always redact.
For help writing policy expressions, click on the pencil icon to show the Policy Expression Builder dialog. Note that you can join multiple conditions together using logical operators. This is useful for creating white lists that redact sensitive data by default and only show actual data when exception conditions that you specify are met.
DBMS_REDACT.ADD_POLICY(
object_schema =>
'CALLCENTER',
object_name =>
Object Columns
Add
Modify
Remove
Column
Column Datatype
Redaction Function
Function Attributes
CUST_DOB
DATE
FULL
CUST_SSN
VARCHAR2
PARTIAL
VVVFVVFVVVV,VVV-VV-VVVV,X,1,5

Antes y después de Redaction



Oracle Data Redaction Target Use Cases

Application screens with **read-only static pages** such as dashboard and reports	
Application screens with **read-only static pages** such as dashboard and reports Using **GROUP BY** and **ORDER BY** operators	
Application screens with **actives pages** such as forms which can post redacted data back to the database	
Privileged DB users (e.g. DBA) who can bypass applications and access redacted fields using **backend SQLs**	
Any DB user who can write **exhaustive and ad-hoc SQLs** to access redacted data . e.g. Multi-layered SQLs with several sub-queries; multiple joins using set operators such as UNION ALL; in-line views; and no-merge hint;	
As an alternative to VPD, OLS, Database Vault, and Data Masking(in test/dev)	

Please refer to the product documentation for known Data Redaction limitations

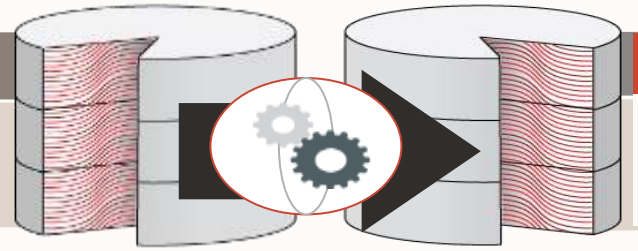
Oracle Data Masking & Subsetting

Oracle Data Masking and Subsetting

Enmascaramiento irreversible de datos en entornos no productivos

Producción

NOMBRE	DNI	SALARIO
ANA PÉREZ	12345678-A	30,000
PEDRO SÁNCHEZ	48765432-Z	25,000



Desarrollo

NOMBRE	DNI	SALARIO
JUAN CHACÓN	81331100-J	25,000
MARTA RODRÍGUEZ	87766348-S	30,000

Transfiere datos de aplicación de forma segura a entornos no productivos

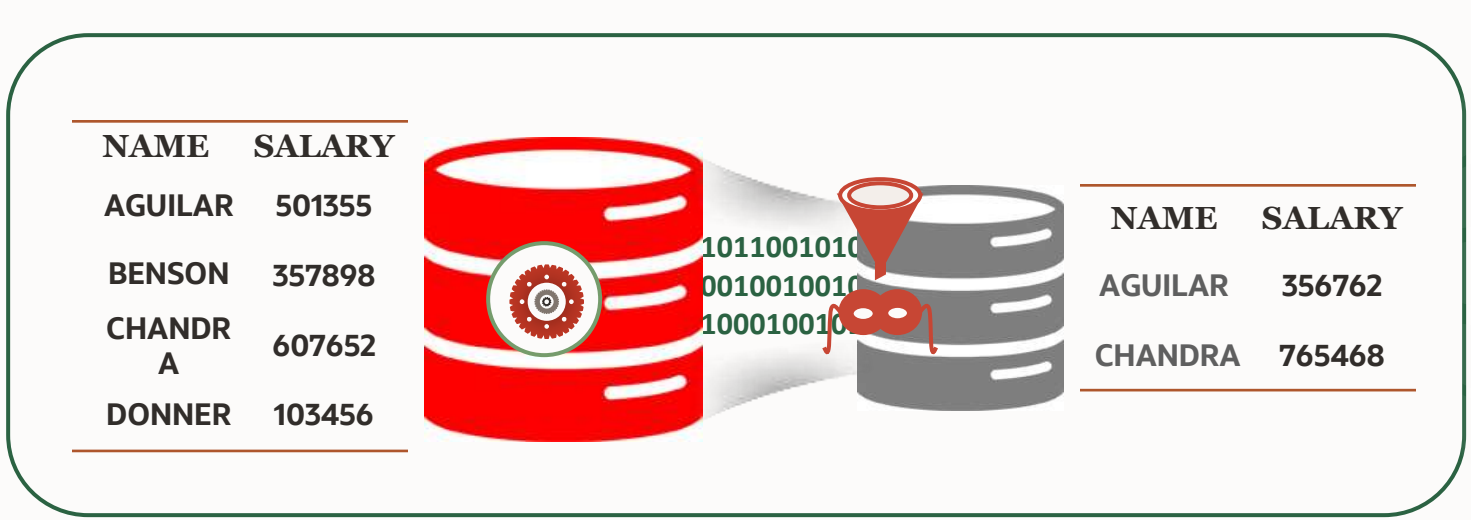
Evita que desarrolladores de aplicaciones accedan a datos reales de producción

Librerías y políticas extensibles para la automatización del enmascaramiento de datos

Se preserva la integridad referencial por lo que las aplicaciones continúan funcionando correctamente

Oracle Data Masking and Subsetting Pack

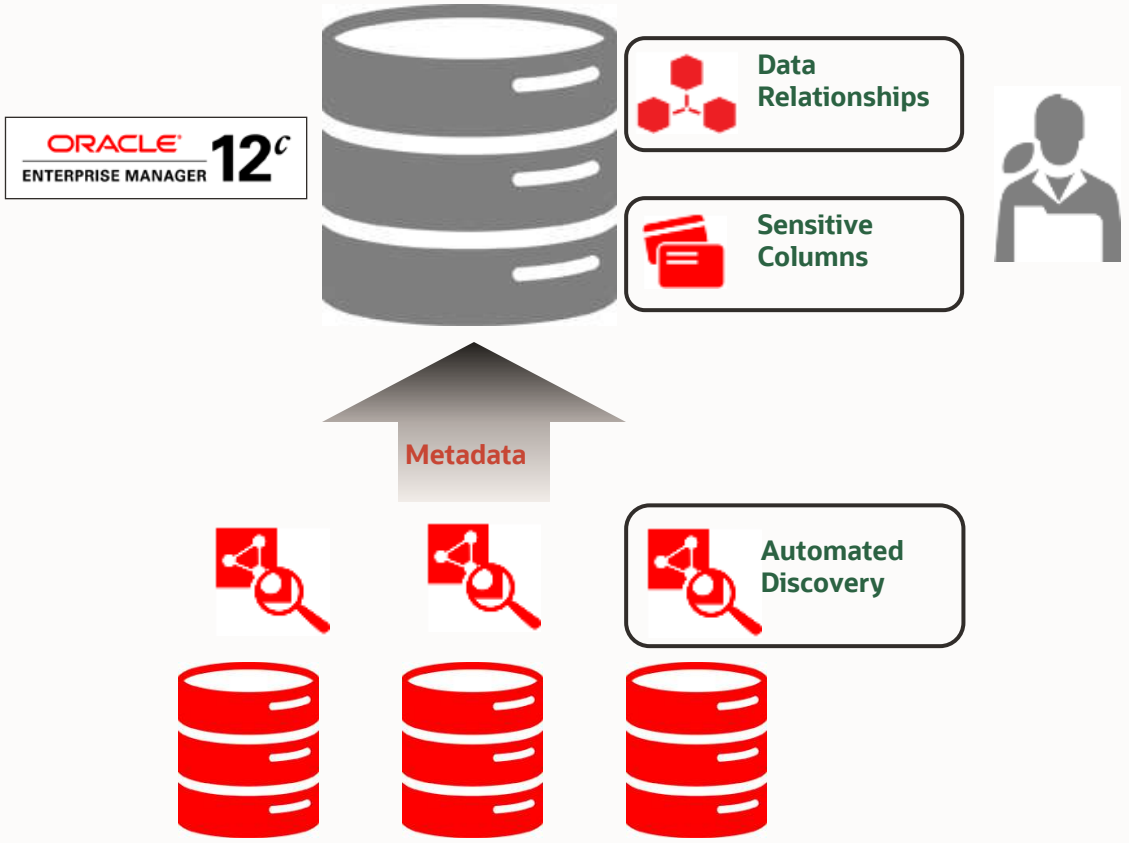
Reduce riesgos alterando o eliminando datos sensibles

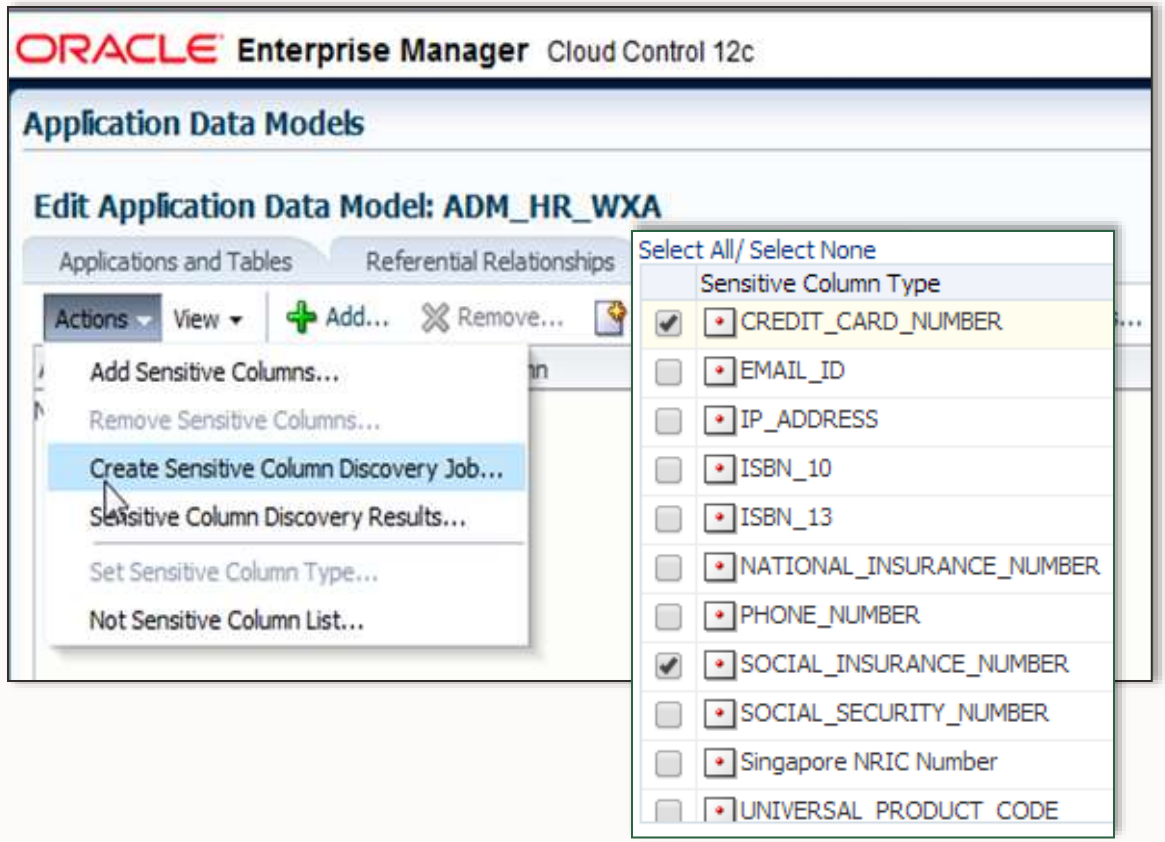


- Descubrimiento de datos sensibles
- Masking con librería de formatos
- Subconjunto según meta/condición
- Mantiene integridad aplicación
- Mask/Subset en Export o Staging

Application Data Modeling

Descubrimiento de datos sensibles

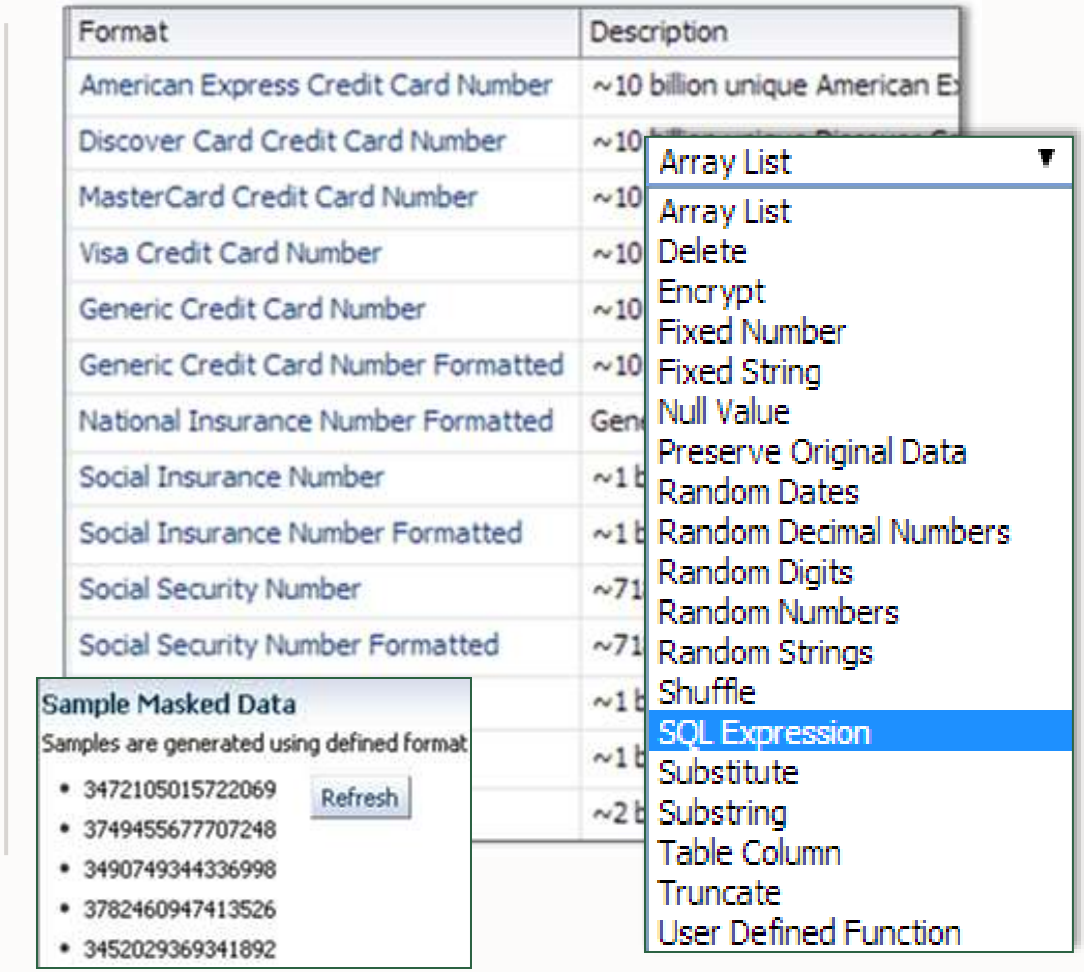




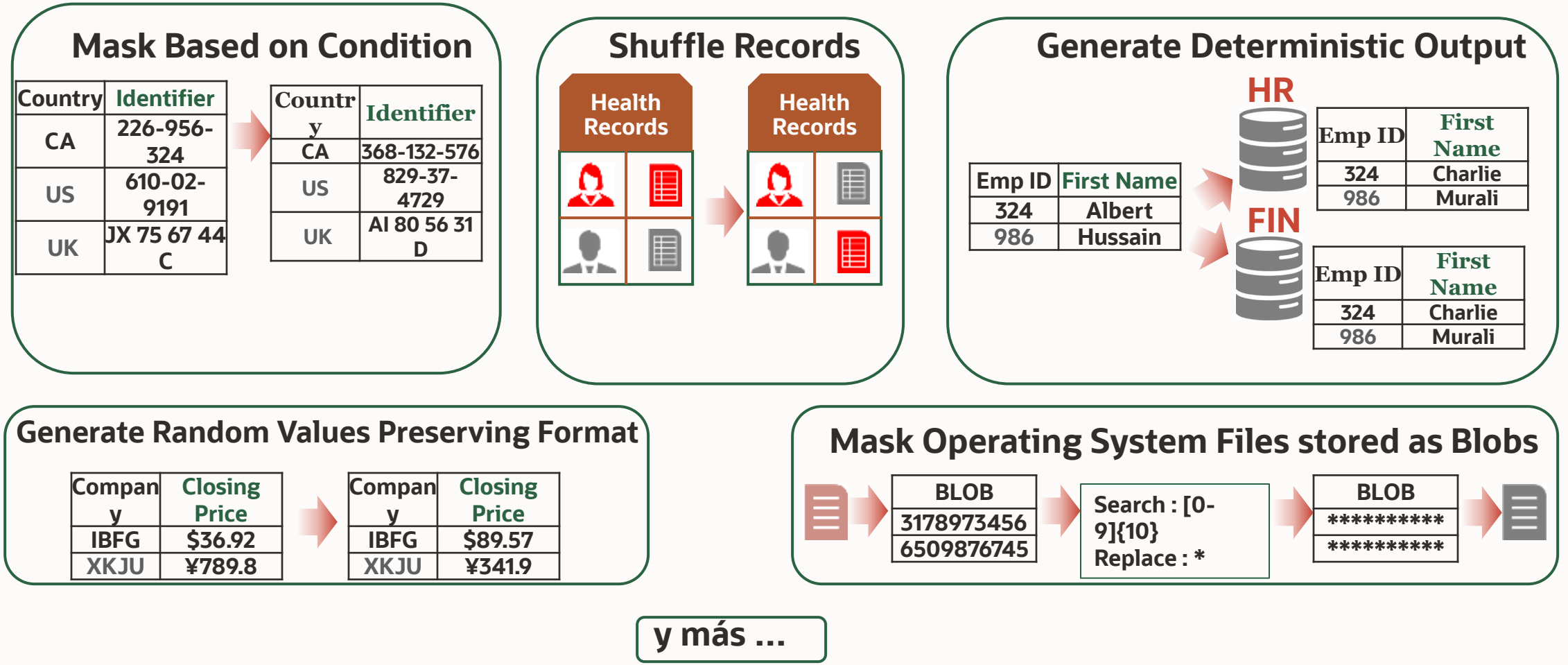
Amplia librería de formatos de enmascaramiento

- Formatos de máscara comunes
- Soporta formatos a medida
  - Números aleatorios/strings/fechas
  - Substitución
  - Función PL/SQL definida por el usuario

    … y más
- Genera muestras de valores enmascarados
- Plantillas para versiones específicas de E-Business Suite y aplicaciones Fusion



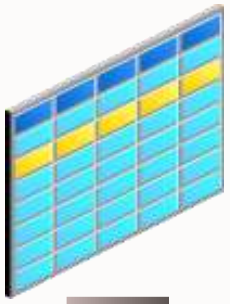
Ejemplos de enmascaramiento

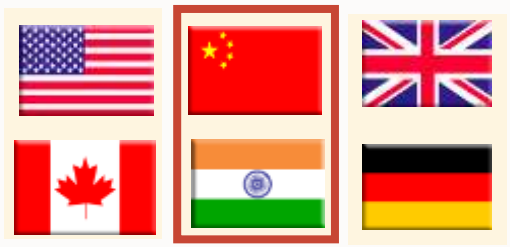


	Masking Format	Supported Data Types	Inputs	Combinable	Uniqueness	Reversible	Deterministic
1	Deterministic Encryption	• Character • Numeric • Date	• Regular Expression • Seed Value OR • Start Date • End Date • Seed Value			✓	✓
2	Deterministic Substitution	• All	• Schema Name • Table Name • Column Name • Seed Value				✓
3	Fixed Number	• Character • Numeric	• Fixed Number	✓			
4	Fixed String	• Character	• Fixed String	✓			
5	Group Shuffle	• All	• Grouping Columns				
6	Post Processing Function	• All	• Post Processing Function	✓			
7	Random Date	• Date	• Start Date • End Date	✓			
8	Random Decimal Number	• Character • Numeric	• Start Value • End Value	✓			
9	Random Digits	• Character • Numeric	• Start Length • End Length	✓			
10	Random List	• Character • Numeric • Date	• Random List	✓			
11	Random Number	• Character • Numeric	• Start Value • End Value	✓			
12	Random String	• Character	• Start Length • End Length	✓			
13	Random Substitution	• All	• Schema Name • Table Name • Column Name				
14	Regular Expression	• Character • LOB	• Regular Expression • Replace With				
15	SQL Expression	• All	• SQL Expression				✓
16	Substring	• Character	• Start Position • Length	✓			
17	User Defined Function	• Character	• User Defined Function	✓			✓

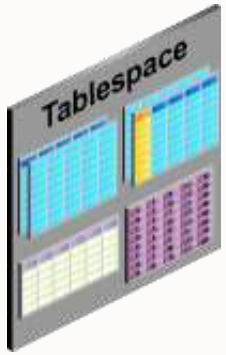
Extracción de subconjuntos de datos (*)

Fecha:
(año 2011)

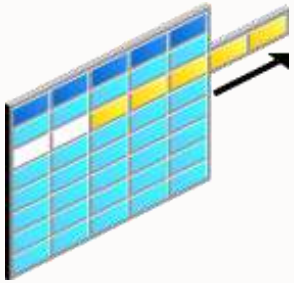




Dimensión
(Región: Asia)



Espacio
(tamaño:10%)



Selección de tablas

- Se seleccionan automáticamente las tablas necesarias para se incluidas en el subconjunto

Criterios de extracción

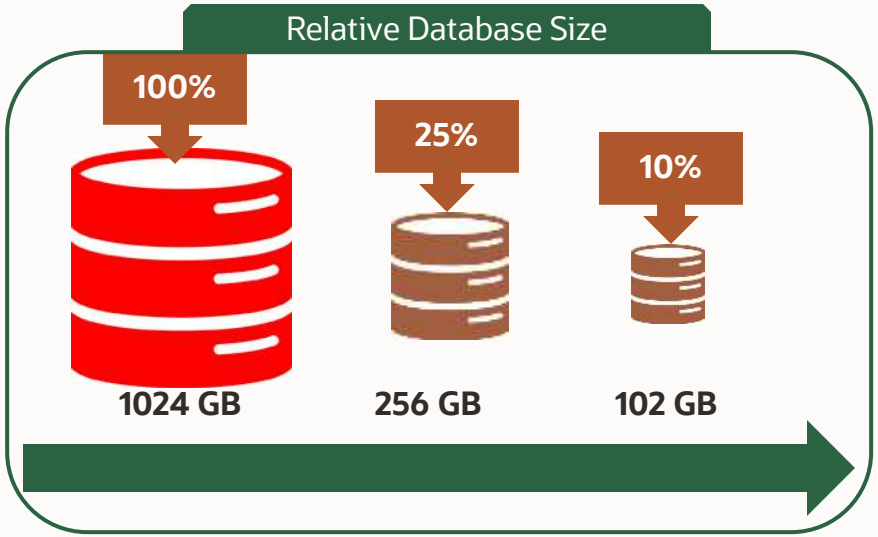
- Se recorre la jerarquía relacional para identificar las filas a extraer

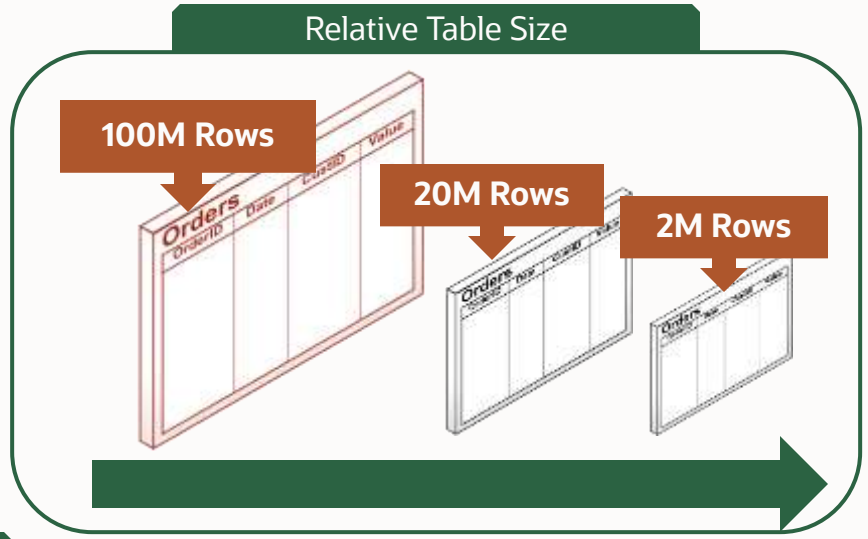
Parámetros de subconjunto

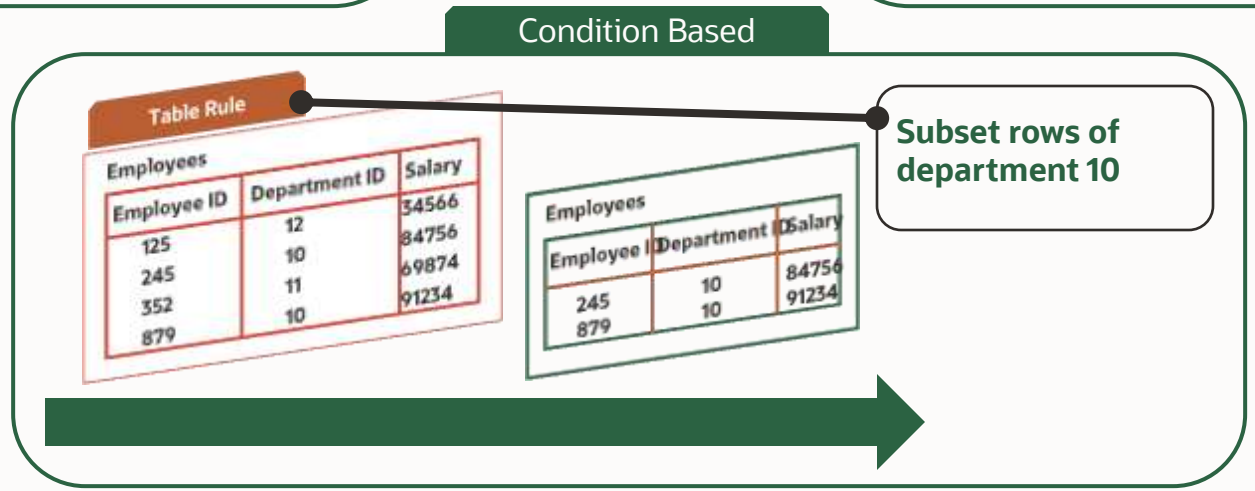
- Analiza las estadísticas de las tablas para estimar el tamaño de los datos generados

(*) Disponible a partir de EM CC 12c

Subsetting basado en meta o condición



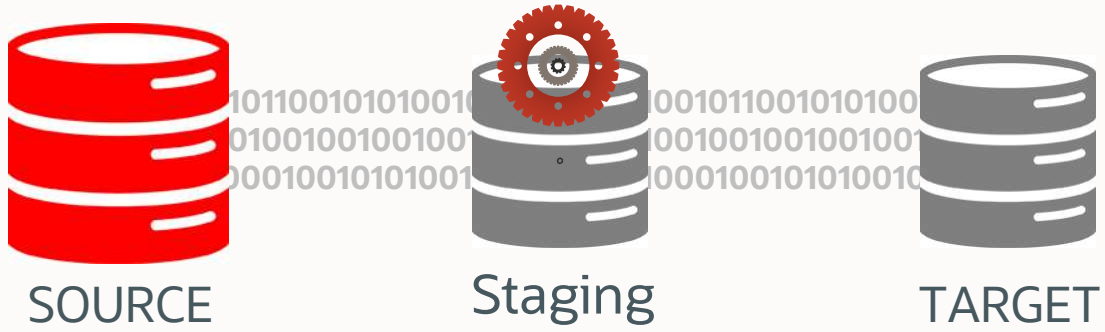




Oracle Data Masking and Subsetting

Opciones de despliegue

In-Database



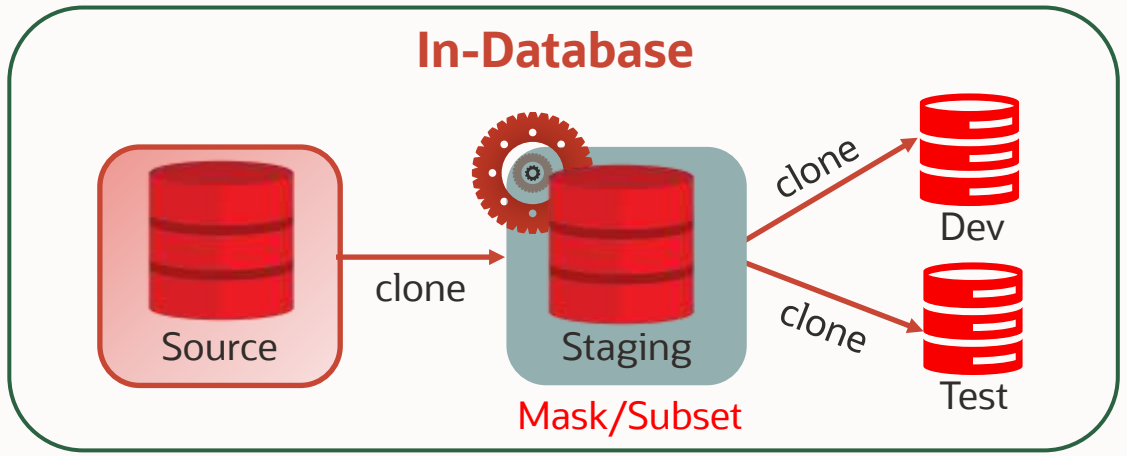
Impacto mínimo
en el origen

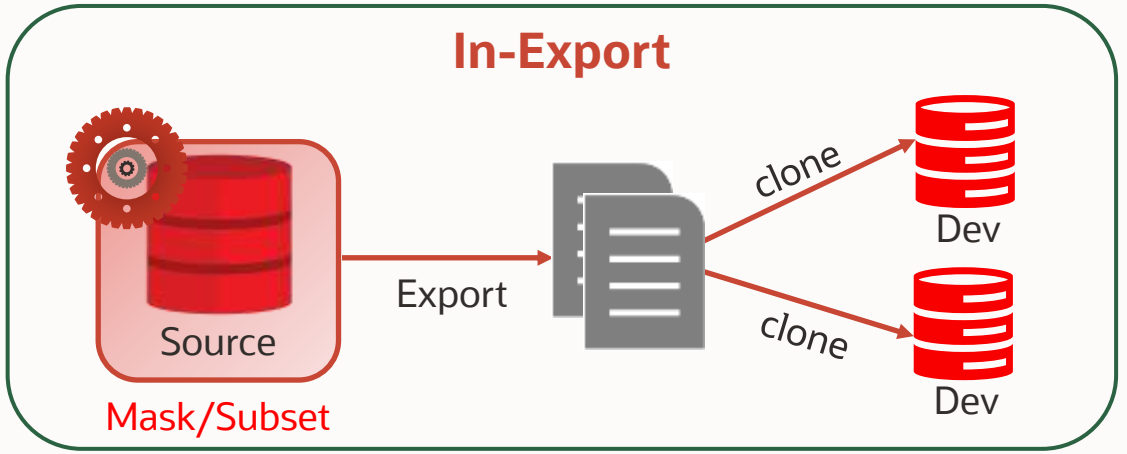
In-Export

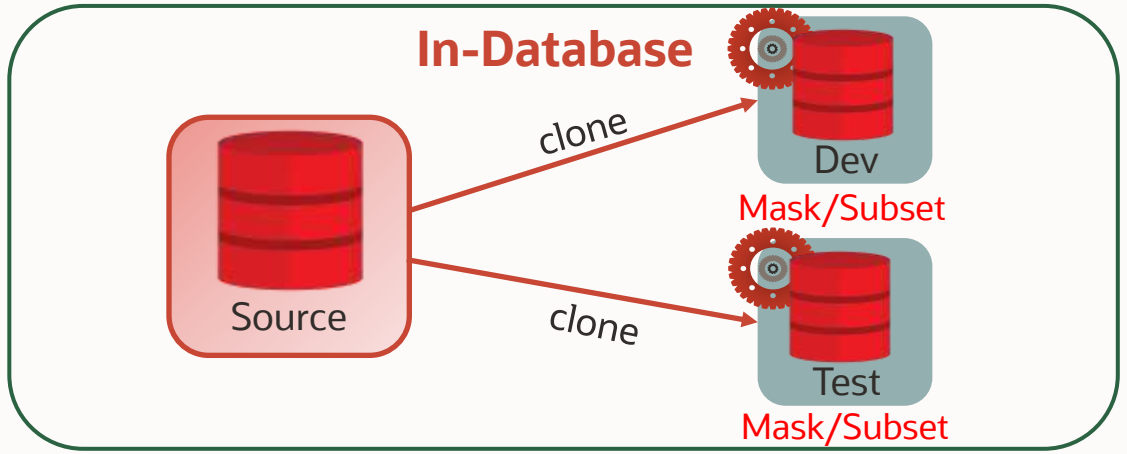
Los datos sensibles
no salen de producción

Oracle Data Masking and Subsetting

Modelo de licenciamiento para bases de datos Oracle

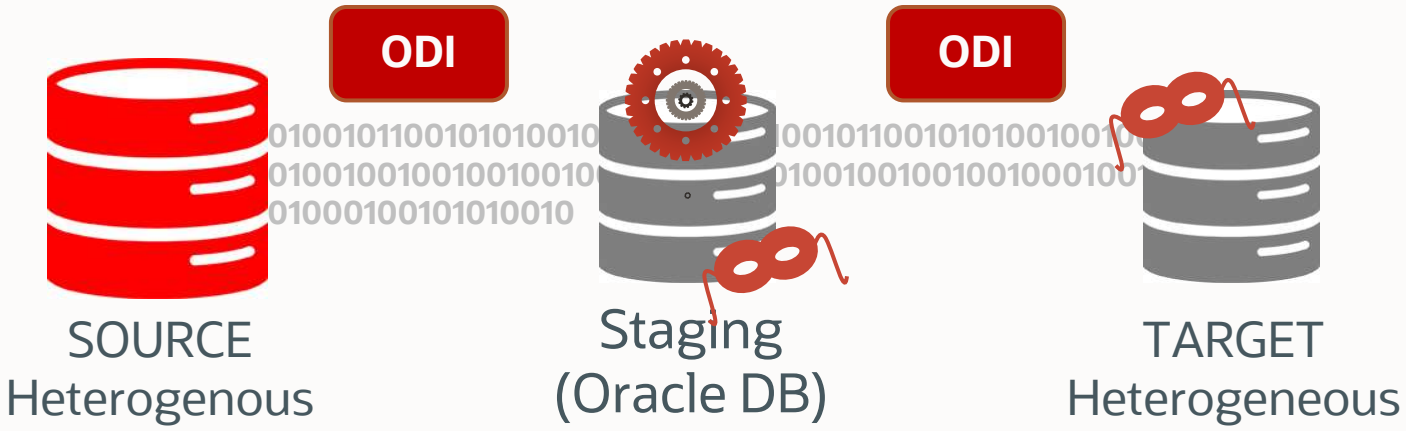






Oracle Data Masking and Subsetting

With Oracle Data Integrator (ODI)

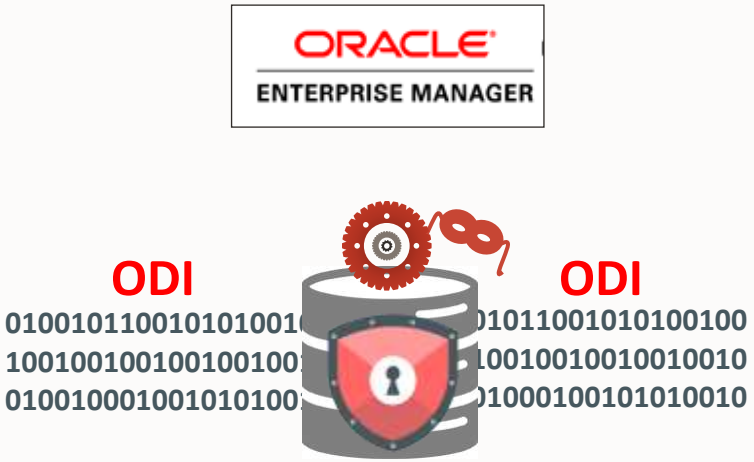


Oracle Data Masking Factory (DMF)

Concept

ANY SOURCES

On-Prem / Cloud



DMF Oracle DB

(Staging)

ANY TARGETS

On-Prem / Cloud

Oracle Data Masking Factory (DMF)

ODI supported technologies - Based on JDBC Drivers

RDBMS

IBM DB2 LUW
Informix
Ingres
MS SQL Server
MySQL
Netezza
Oracle
PostgreSQL
Progress
Sybase ASA
Sybase ASE
Sybase ASIQ
Teradata
TimesTen
Universe

MAINFRAME - MINI

DB2 z/OS
DB2 AS/400

BIG DATA

Hive
MongoDB

FILES & BUS

File
Complex File
XML
JMS Queue
JMS Q. XML
JMS Topic
JMS Topic XML

OTHERS

Hyperion Essbase
Hyperion Fin Mngt
Hyperion Planning
Salesforce.com
SAP ABAP
SAP HANA
SAP Java Connector

LiveLabs | Search Workshops... | Feedback | Sign In

Home | Available Workshops | My Reservations | Have an Event Code? | FAQ

DB Security Advanced Workshop

Explore how to use Oracle Database Security advanced products and solutions.

Workshop length: 6 hours

Share Workshop Link

Other LiveLabs you might like

Database 19c - Hybrid Partitioning

DB Security Basics

Boost Analytics Performance with Oracle Database In-Memory

Ways to run this workshop

Choose how you want to run this workshop.

Launch **Free Trial** Workshop

*More about **Free Trial***

Run On Your **Tenancy**

*More about using Oracle Universal Credits you've purchased: **Using your credits** | **Services available***

Reserve Workshop on **LiveLabs**

*You need an Oracle account to run on the free LiveLabs tenancy: **Oracle account help** | **Oracle account signup***

Workshop Outline

Workshop Details

ORACLE

ENCUESTA

Workshop Virtual Seguridad en Base de Datos

¡Tu opinión es muy importante!

Escanea el QR para responder o entra aquí:

https://bit.ly/3uU49eR

Gracias