
ORACLE®

ORACLE®

Seguridad: Protección de la Información en la Empresa

José Villalón
Senior Sales Consultant

Consideraciones en la Seguridad de las Bases de Datos

- Amenaza externa
  - Discos reemplazados que no son adecuadamente desechados
  - Cintas de respaldo perdidas o robadas durante el transporte
- Amenaza interna
  - DBAs con acceso a datos de aplicaciones, incluyendo registros financieros o de R.R.H.H.
  - Modificaciones no autorizadas a las aplicaciones o bases de datos
- Conformidad normativa
  - Sarbanes-Oxley y Graham-Leach Bliley, y Basel II requieren **Fuertes Controles Internos** y **Separación de Deberes**
  - Quién estuvo accediendo a información clasificada, cuándo, dónde, y cómo?

Los clientes están preguntando por…

- “Privacidad / Conformidad normativa”
- “Protección de los datos en las cintas de respaldo”
- “Protección adicional contra el sistema operativo / robo de archivos de datos”
- “Robo de dispositivos / reemplazo de discos”
- “Dejar que la base de datos maneje todos los aspectos de encriptación, no la aplicación”
- “Hacerlo fácil y seguro”

“Encryption isn’t “buy and forget” security, understand its limits and when it is appropriate”

-Gartner: When and How to Use Enterprise Data Encryption

Oracle – Seguro desde el inicio

Oracle Audit Vault
Oracle Database Vault
Database CC Security Eval #18 (10g R1)
Transparent Data Encryption
VPD Column Sec Policies
Fine Grained Auditing (9i)
1st Database Common Criteria (EAL4)
Oracle Label Security (2000 8.1.7)
Virtual Private Database (1998)
Enterprise User Security (8i)
Database Encryption API
Kerberos Support (8i)
Support for PKI
Radius Authentication
Network Encryption (Oracle7)
Oracle Advanced Security introduced
First Orange Book B1 evaluation (1993)
Trusted Oracle7 MLS DB
Government customer

30 Años de Liderazgo en Seguridad de Base de Datos

ORACLE

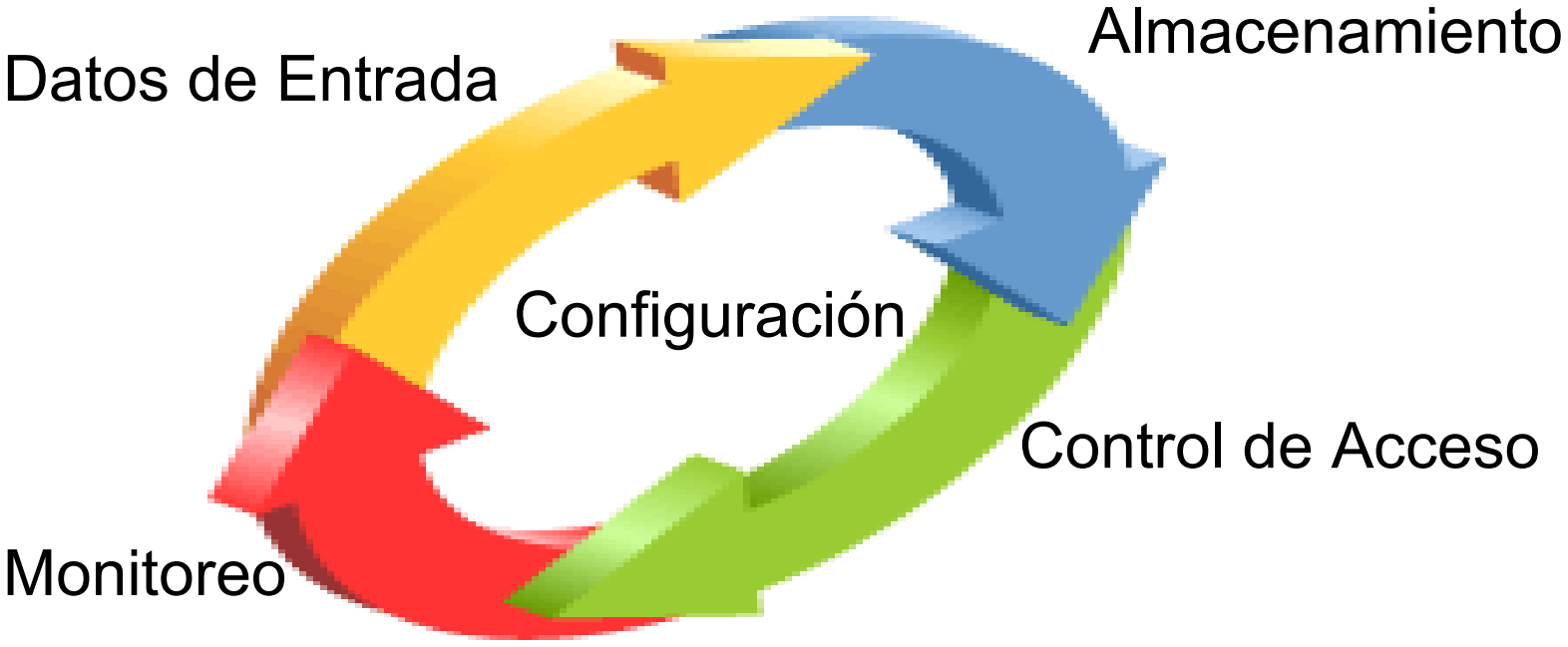
1977

2007

Evaluaciones Independientes de Seguridad

Security Evaluations	Oracle	DB2	SQLServer
US TCSEC, Level B1	1	-	-
US TCSEC, Level C2	1	-	1
UK ITSEC, Levels E3/F-C2	3	-	-
UK ITSEC, Levels E3/F-B1	3	-	-
ISO Common Criteria, EAL-4	8	1	-
Russian Criteria, Levels III, IV	2	-	-
US FIPS 140-1, Level 2	1	-	-
TOTAL	19	1	1

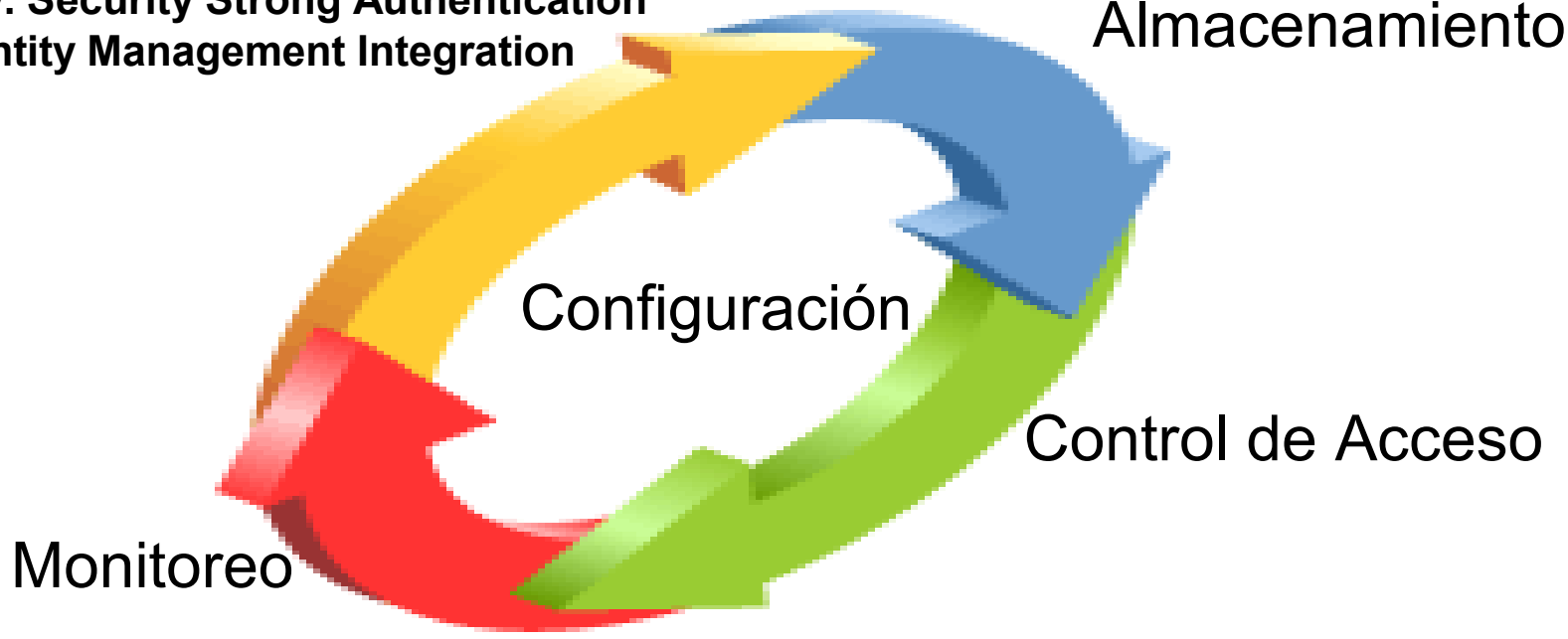
Ciclo de Vida de la Seguridad de los Datos



Ciclo de Vida de la Seguridad de los Datos

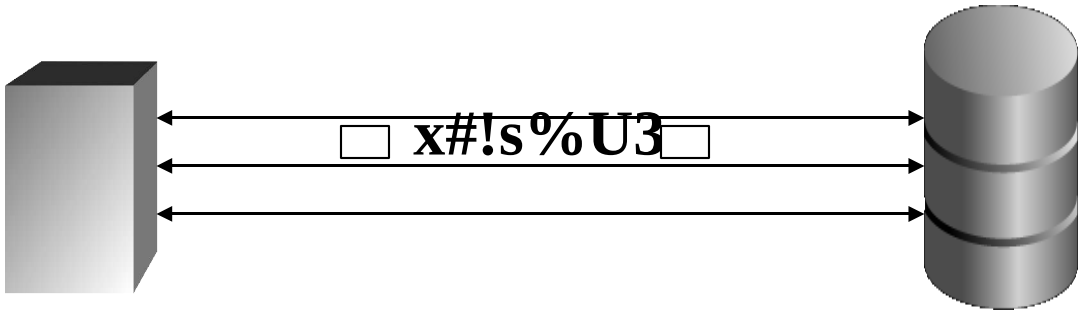
Datos de Entrada

- Adv. Security Network Encryption
- Adv. Security Strong Authentication
- Identity Management Integration



Network Security

- Encriptando la Información en Tránsito



Problema de Seguridad

- La encriptación debe ser utilizada no solo para tráfico Internet sino además para tráfico Intranet
- Configurar la encriptación de la red en la Intranet puede tomar mucho tiempo

Seguridad de la Red

- Encriptación de la Red es ofrecida por Oracle por casi una década
- Fácil configuración con o sin certificados
- Encripta todas las comunicaciones con la base de datos
  - AES
  - RSA RC4 (40-, 56-, 128-, 256-bit keys)
  - DES (40-, 56-bit) and 3DES (2- and 3-key)
  - Diffie-Hellman key exchange
- Integridad de datos con Checksums
  - SHA-1 y MD5
  - Automáticamente detecta modificaciones, repeticiones, paquetes faltantes

Strong Authentication

Oracle Strong Authentication

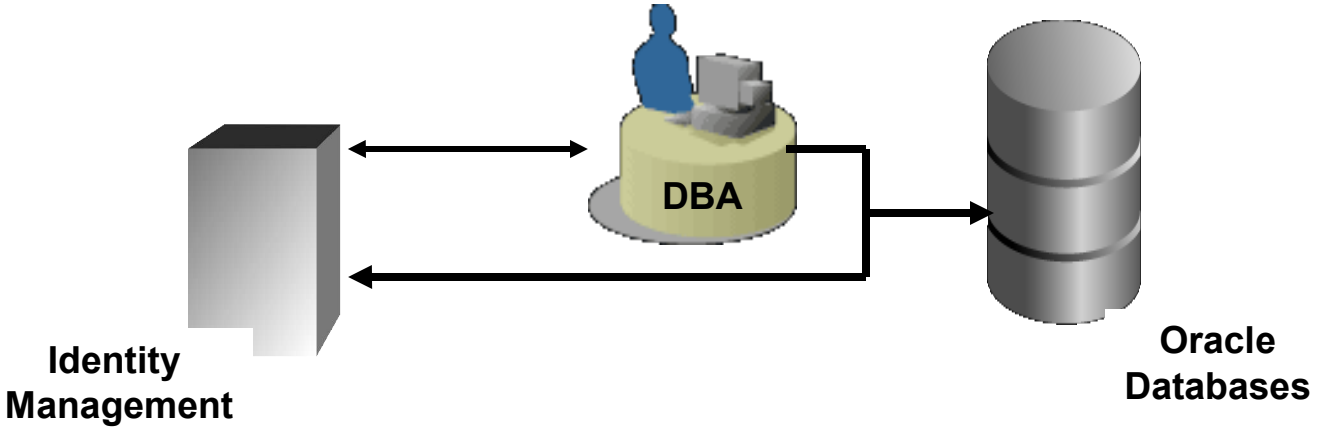
- PKI
  - A través de Certificados X.509V3
- Kerberos
  - Rabaja con Microsoft Kerberos Server
- Radius
  - Se integra con soluciones compatibles Radius de terceros

Strong Authentication Beneficios

- Resuelve los problemas inherentes con la autenticación basada en passwords
  - Passwords débiles
  - Pobre gestión de passwords
- Conformidad con las Regulaciones
- Amenazas Internas

User Management

- Enterprise User Security



Problema de Seguridad

- Cuentas de usuario individuales en múltiples bases de datos
- Un cambio de empleado requiere borrar / deshabilitar las cuentas dejadas
- Gestión de autorización de usuarios descentralizada

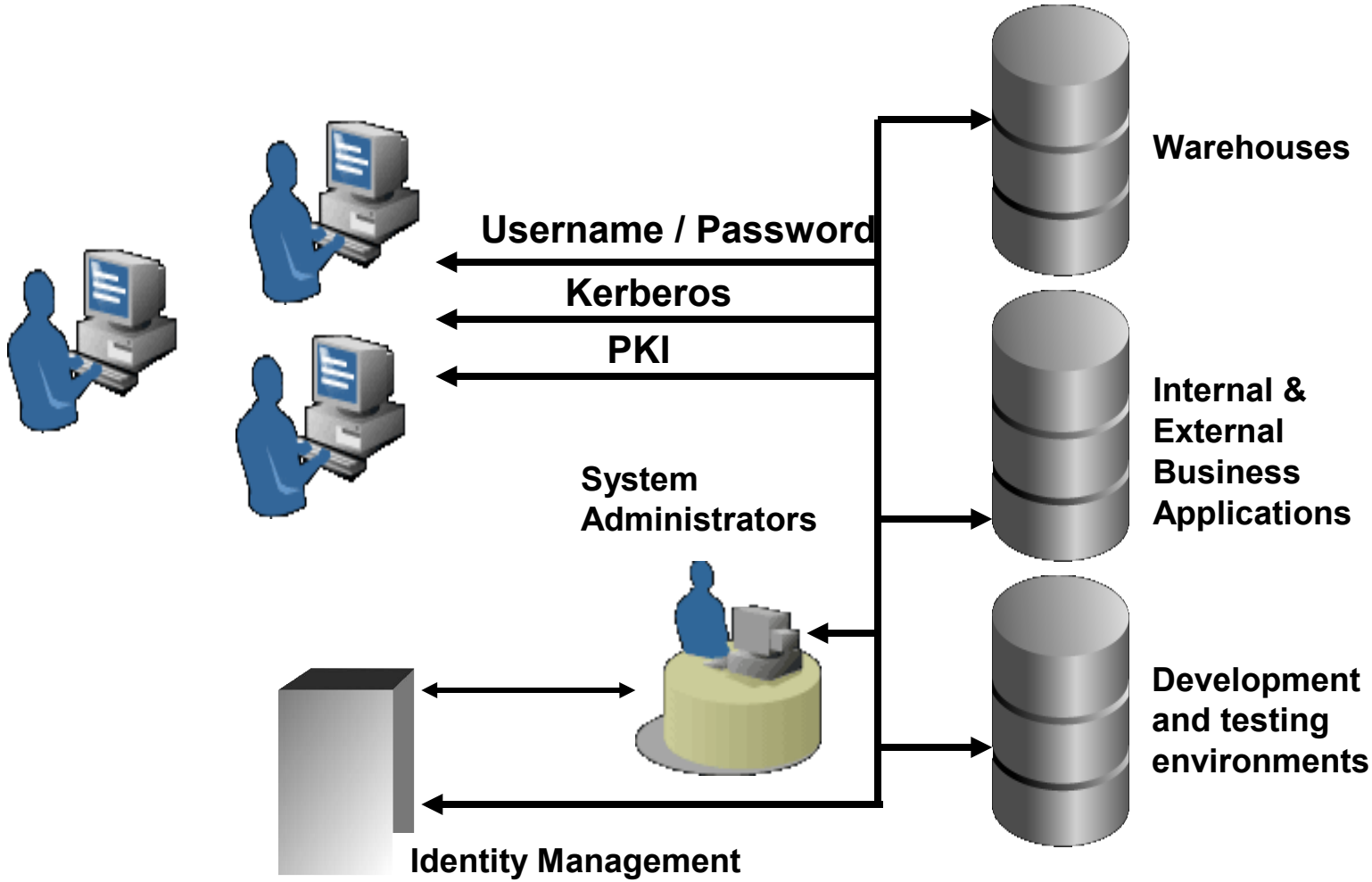
User Management
Enterprise User Security

- Introducido en Oracle8i
- Simplifica la gestión de usuarios, reduce costos
  - Las credenciales y autorizaciones de usuarios (acceso a roles de base de datos) son almacenadas centralizadamente en el directorio de la infraestructura de Oracle Identity Management (OID)
  - Muy útil para grandes comunidades de usuarios acediendo a múltiples aplicaciones / bases de datos
- Mejora la seguridad
  - Gestión de usuarios/roles centralizada

User Management
Enterprise User Security

- Simplifica el login
  - Certificados X509v3 sobre SSL (8i)
  - Permite un único password para los usuarios (9i)
  - Kerberos tickets (10g)
- Multiples usuarios pueden compartir un schema
  - Menos schemas que administrar
  - No hay necesidad de crear usuarios en cada base de datos
- Administración de Passwords
  - Las políticas de complejidad de passwords son definidas y controladas en el directorio de Identity Management
  - La base de datos toma el estado de las cuentas de usuario en OID (10gR2)

User Management
Enterprise User Security

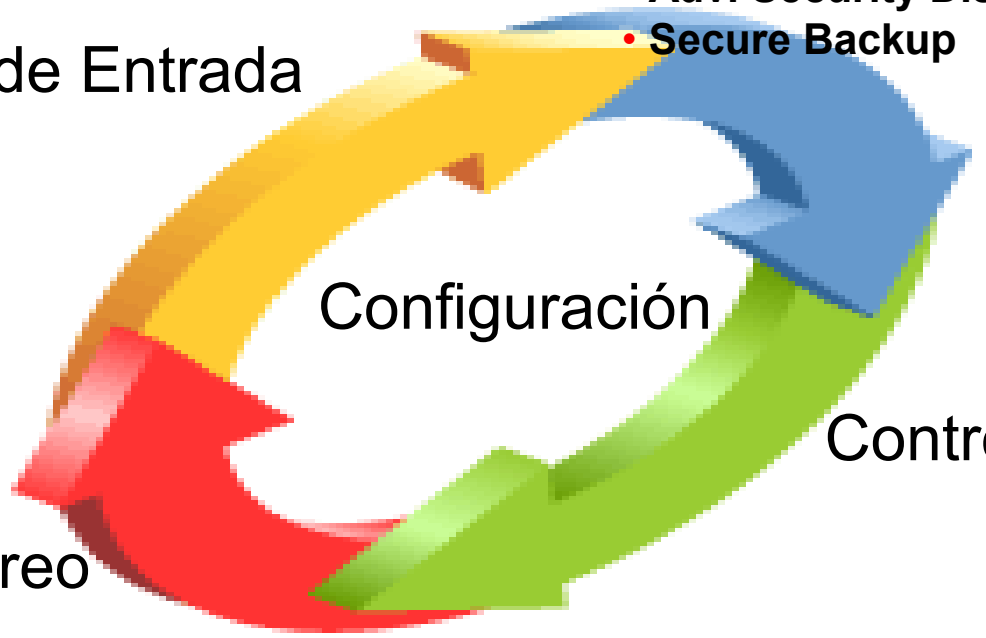


Ciclo de Vida de la Seguridad de los Datos

Almacenamiento

- **Database Encryption APIs**
- **Adv. Security Transparent Data Encryption**
- **Adv. Security Disk Backup Encryption**
- **Secure Backup**

Datos de Entrada



Configuración

Control de Acceso

Monitoreo

Noticias: El Robo de Información

- General Electric, Sep. ‘06: lost laptop
- Chase Card Systems, Sep. ’06: tape thrown in trash
- Wells Fargo, Sep. ‘06: stolen laptop
- CA Dept. of Mental Health, Aug. ‘06: missing tape
- Sovereign Bank, Aug. ’06: stolen laptop
- Chevron, Aug. ’06: stolen laptop
- US Dept. of Transportation, Aug. ’06: stolen laptop
- Cablevision, Jul. ’06: lost tape
- US Dept. of Veterans Affairs, Jun. ’06: lost computer
- Nelnet Inc./UPS, Jul. ’06: lost tape
- Your Company, ‘??

Encriptación

- DBMS_CRYPTO
- TRANSPARENT DATA ENCRYPTION
- SECURE BACKUP

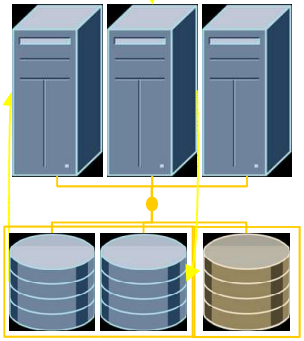
Es DBMS_CRYPTO Para mi?

- Para clientes quienes:
  - Desean programar manualmente la encriptación/desencriptación dentro de aplicaciones existentes.
- Desafíos
  - Minimizar el impacto del rendimiento encriptando solo data sensitiva
  - Mantener la encriptación transparente a las aplicaciones.
  - Que sea fácil y seguro

Transparent Data Encryption

Application

ASO
Network
Encryption



Data
Decrypted
Through
SQL Interface

Data
Written
To Disk
Encrypted

Data Encrypted
On Backup Files

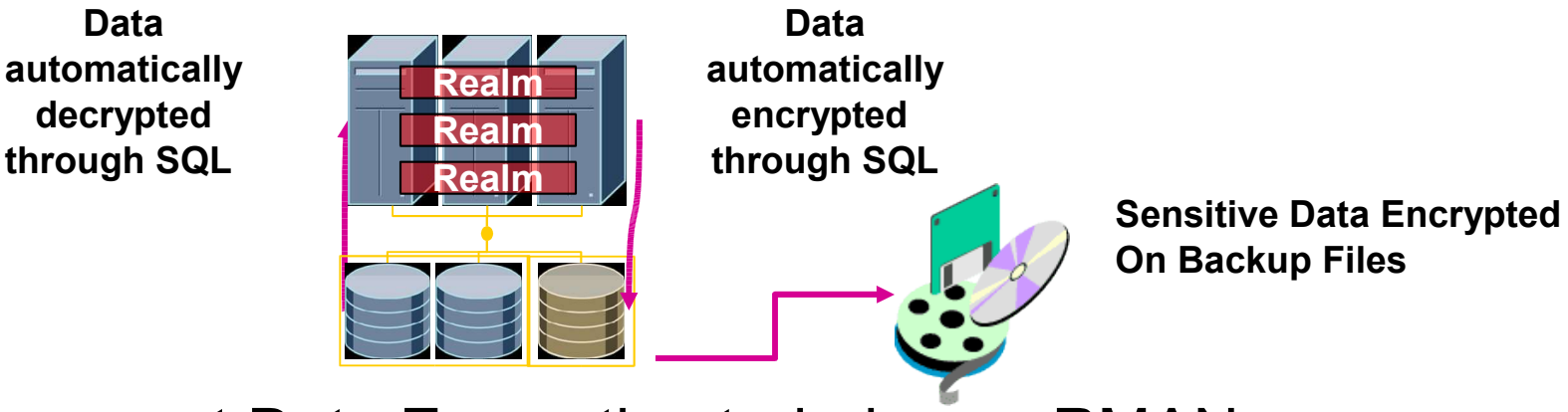
- Transparent Data Encryption
  - Incluye gestión de claves
  - Transparente para las aplicaciones
  - Ayuda a cumplir con políticas de seguridad

Algoritmos y Modos Soportados

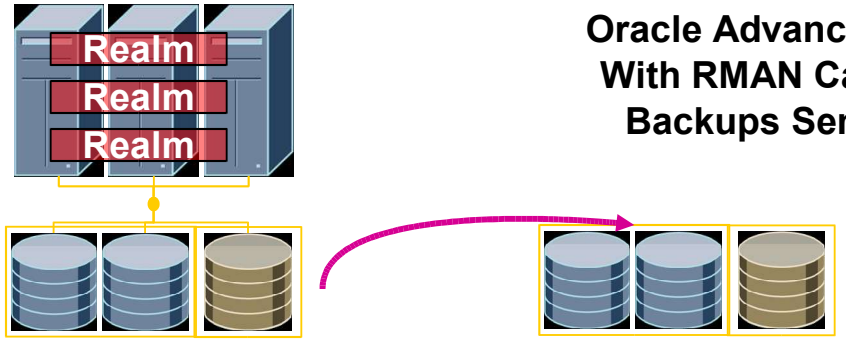
- Encryption
  - AES (128, 192, 256)
  - Triple DES (168)
- Salt
- SHA1
- Cipher Block Chaining (CBC)

Media Protection

- Realms trabajan transparentemente con Transparent Data Encryption



- Transparent Data Encryption trabaja con RMAN para encriptar los backups escritos a disco



Separación de Deberes

Wallet password es separado del password de System o DBA

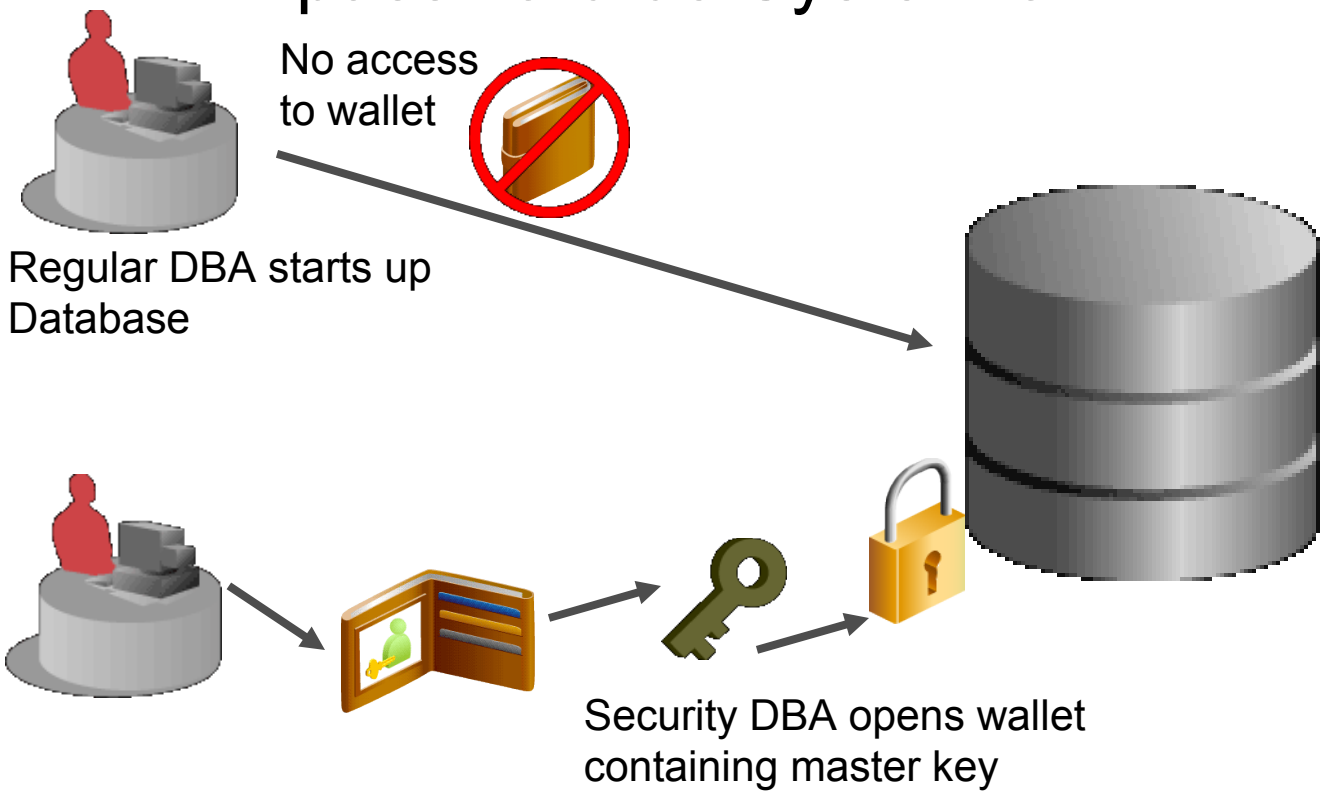
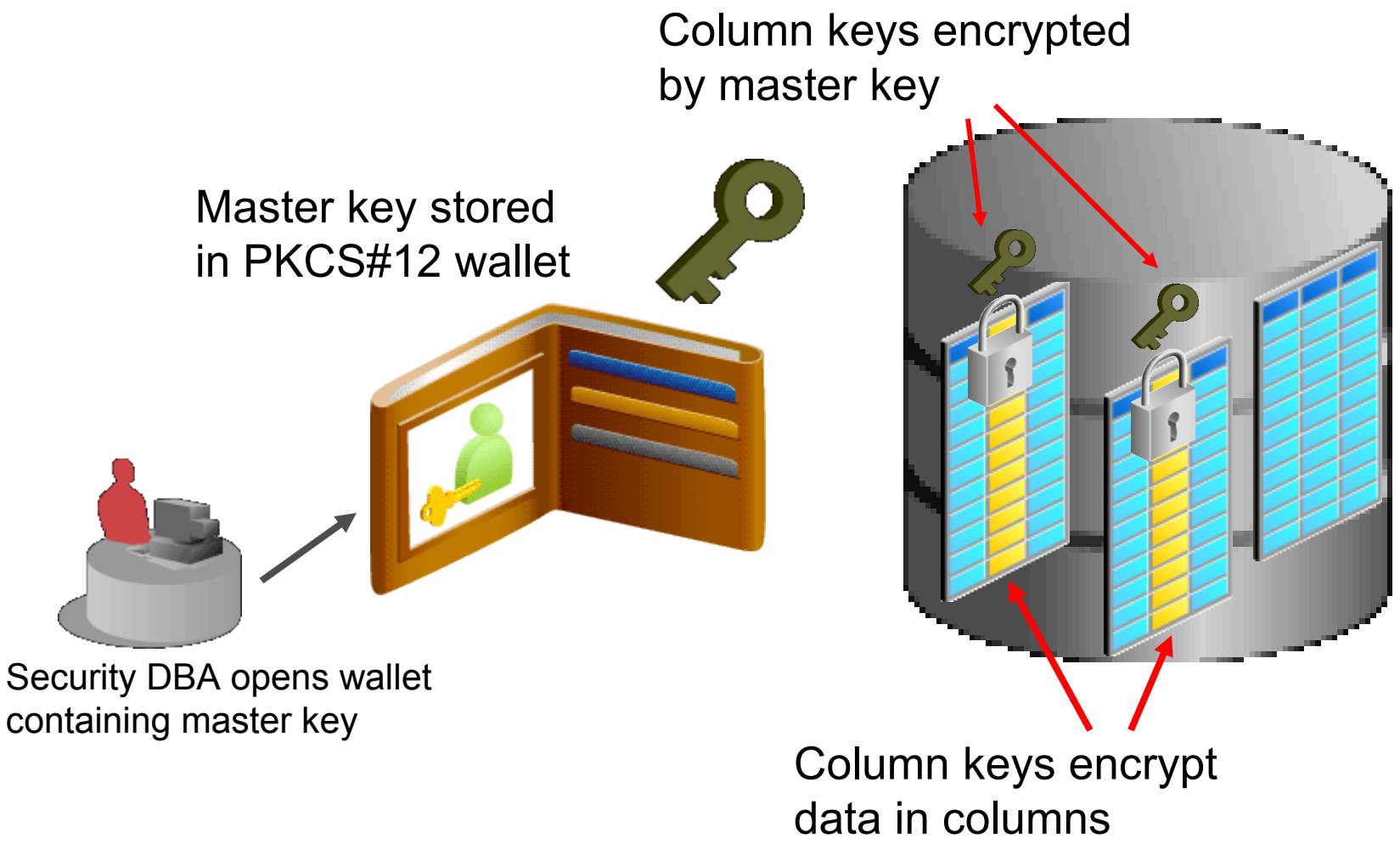


Table Specific Column Keys



Preparando la Base de Datos para TDE

- Creando un Wallet y generando el Master Key
  - `alter system set key identified by "e3car61"`
- Abrir el Wallet
  - `alter system set wallet open identified by "e3car61"`

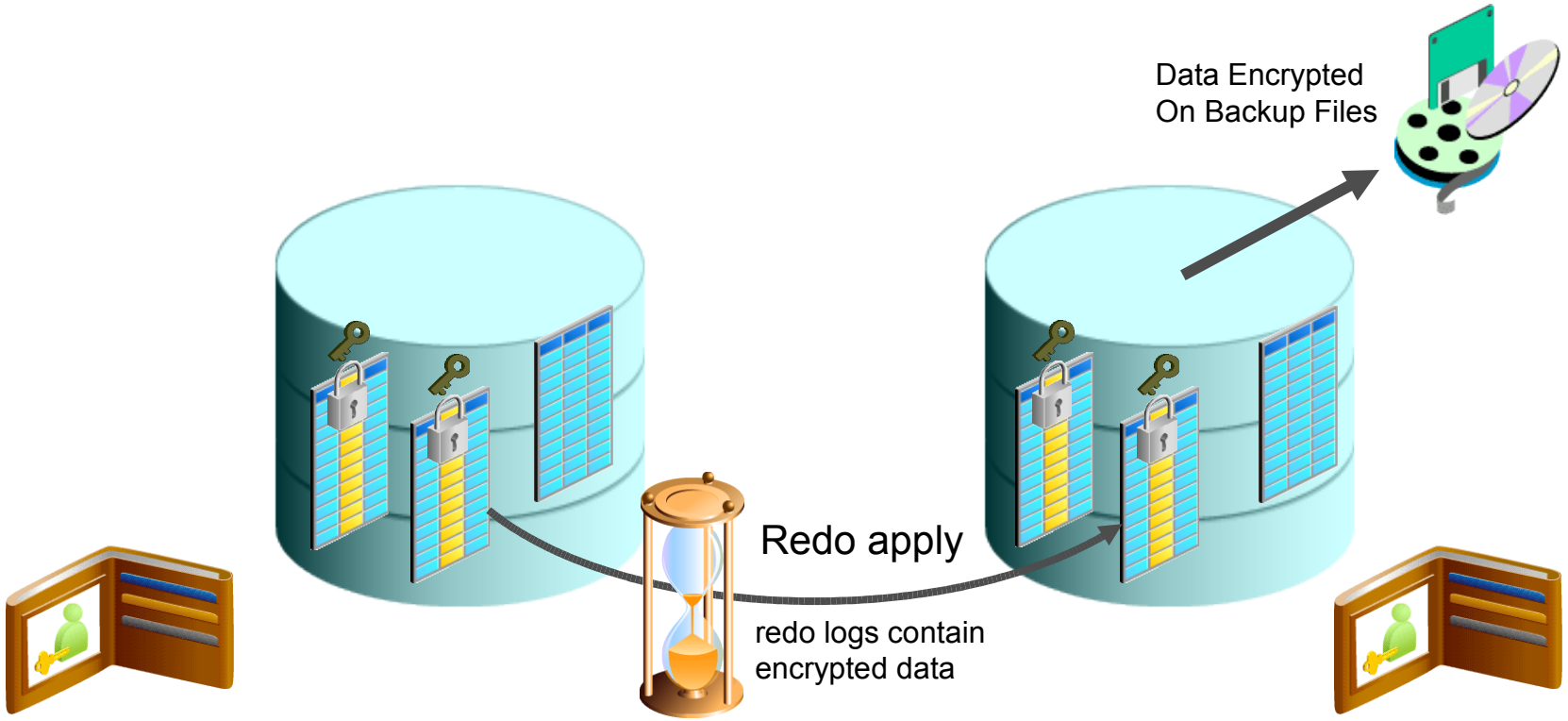
Encriptando las Columnas

- Encriptando una columna en una tabla existente
  - `alter table credit_rating modify (person_id encrypt)`
- Creando una nueva tabla con una columna encriptada

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

TDE y Data Guard

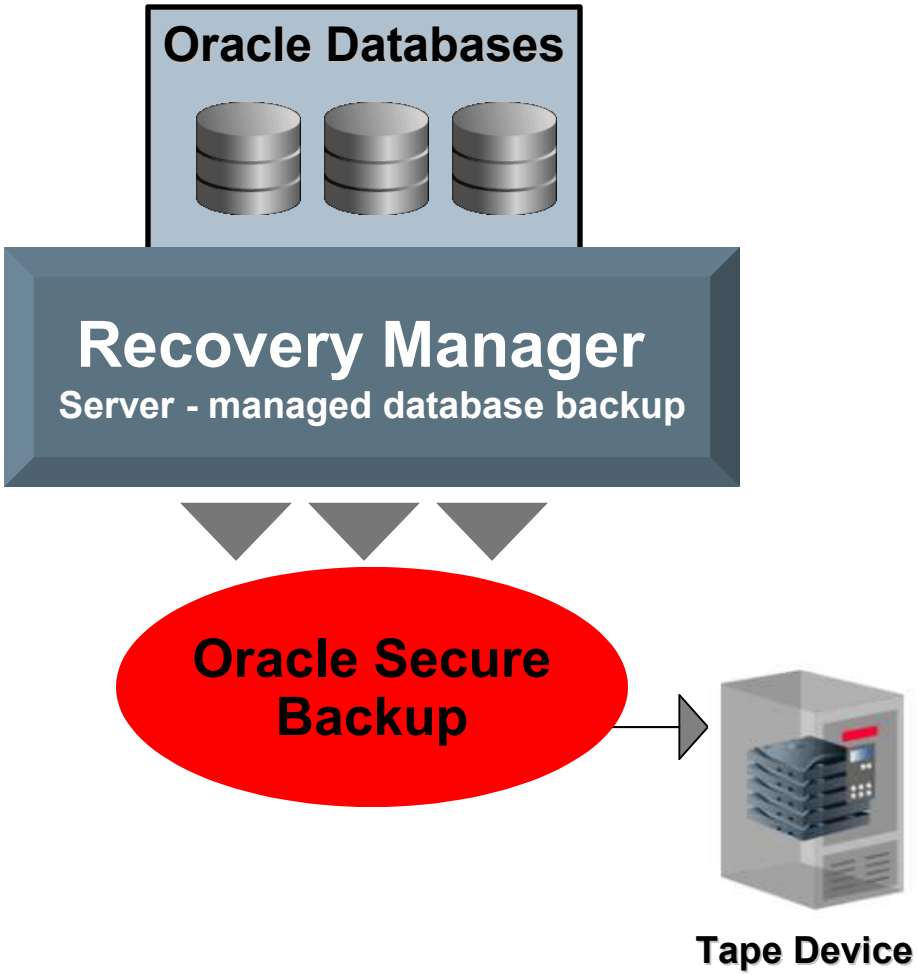
- Production Database
- Physical Standby



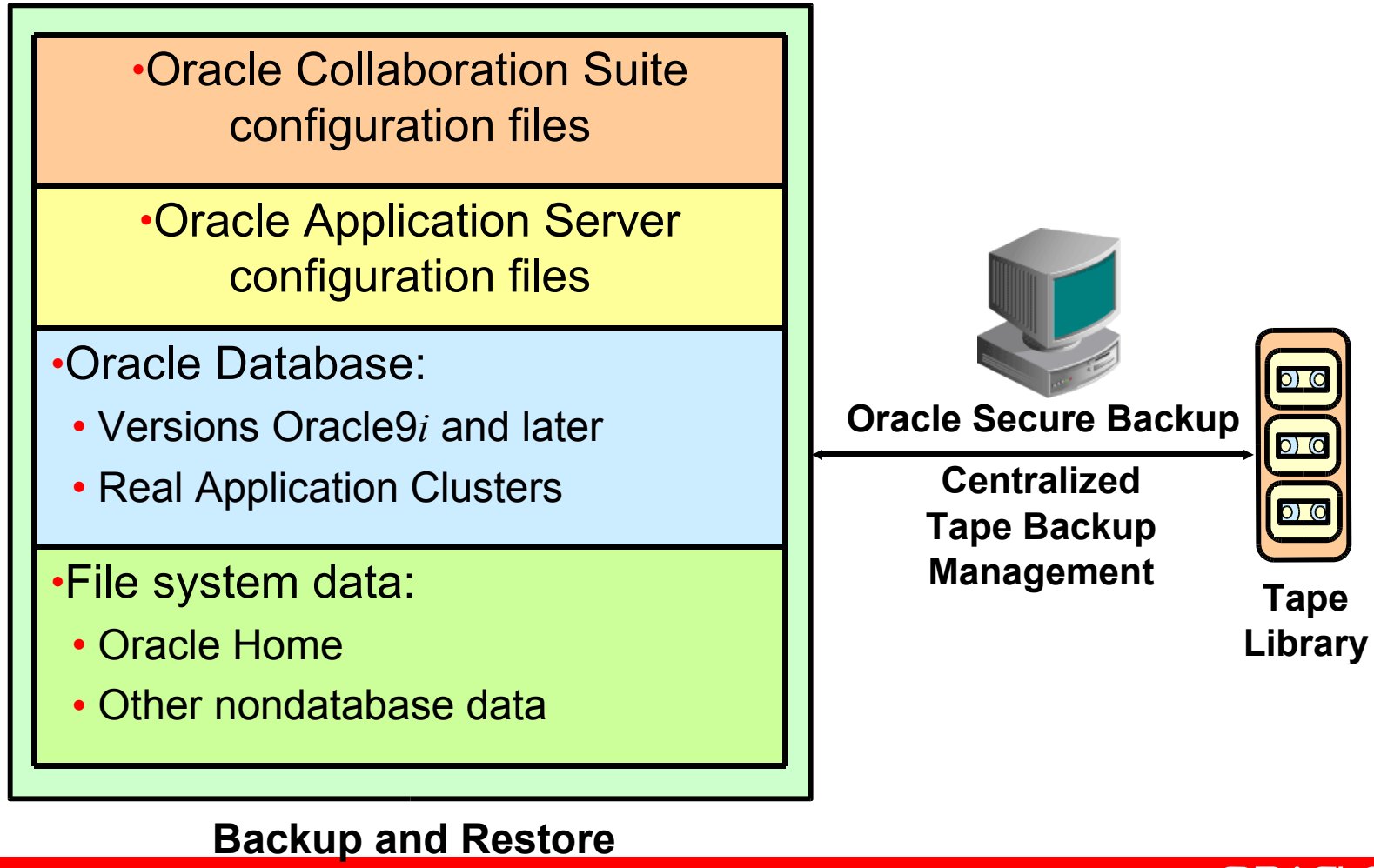
Oracle Secure Backup

Protección de los Datos de Respaldo

- RMAN
  - Online, full, incremental database backups to disk
  - Requires media mgmt software for tape backup
- Oracle Secure Backup
  - Media mgmt software
  - Up to 256 bit AES
  - Encryption modes
    - PKI
    - Password
  - Encrypt at the database or tablespace level
- Integrated solution



Protección de Datos a Cinta para todo el Stack



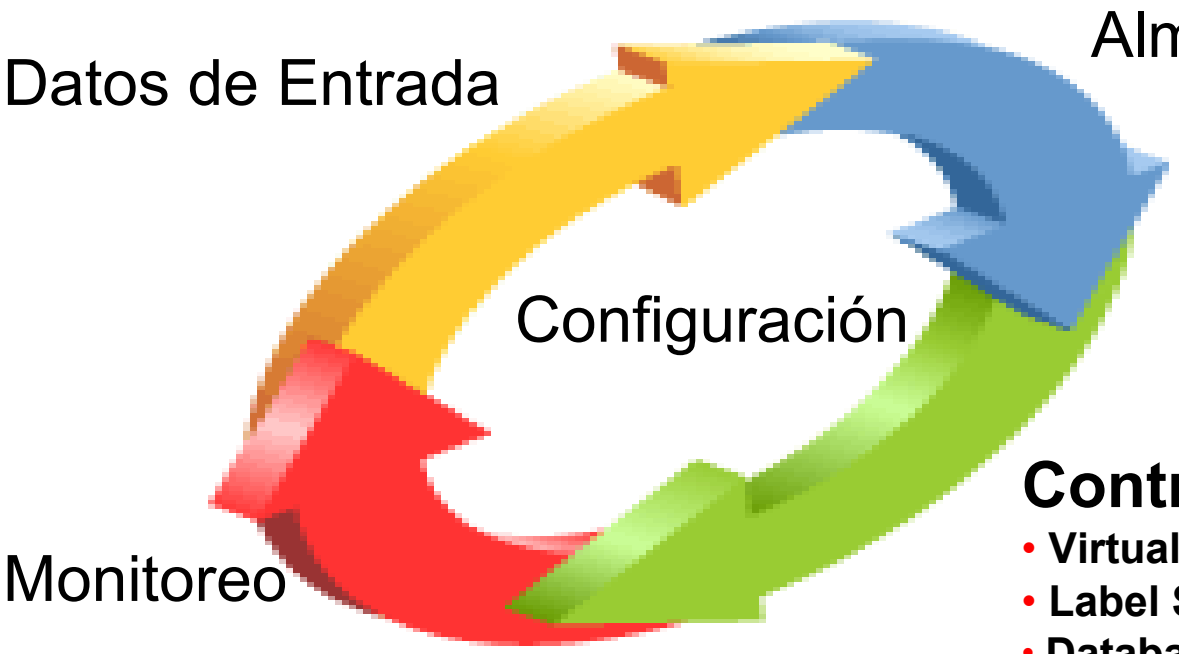
Oracle Secure Backup
La Ventaja de la Integración

- **La integración con RMAN ofrece beneficios en el rendimiento de los backups**
  - Menor consumo de cinta dado que sólo los bloques utilizados son respaldados resultando en backups al menos 15% más rápidos
  - Backups de base de datos a cinta más confiables con validación de bloques de RMAN
  - Soporta bases de datos Oracle9i en adelante
- **La exclusiva integración con Oracle Enterprise Manager significa facilidad de uso**
  - Ofrece una interfaz familiar para clientes Oracle reduciendo curvas de aprendizaje asociadas a otros productos
  - Administra todo el respaldo y recuperación de la base de datos Oracle desde disco (Flash Recovery Area) a cinta utilizando EM
- **Soporte de un único fabricante acelera la resolución de problemas**

Soporte a los Principales Dispositivos de Cinta

Intelligent Storage™

Ciclo de Vida de la Seguridad de los Datos



Control de Acceso

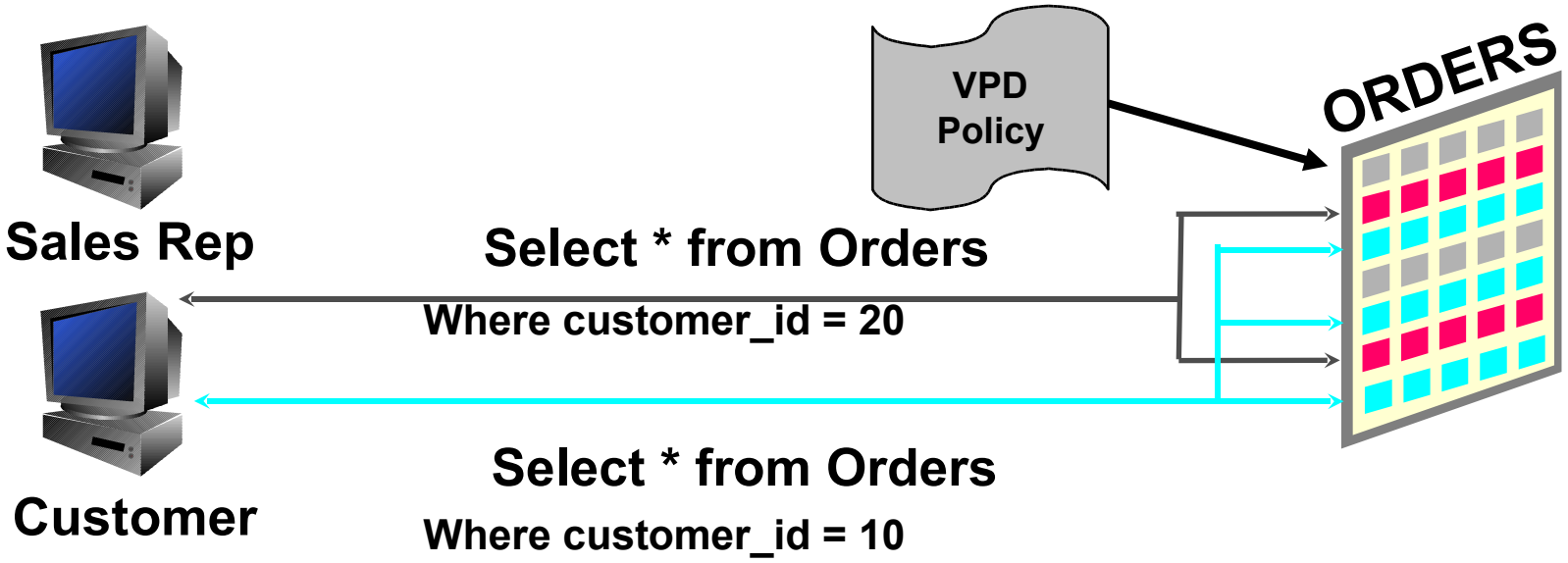
- **Virtual Private Database**
- **Label Security**
- **Database Vault**

Row Level Security Controls

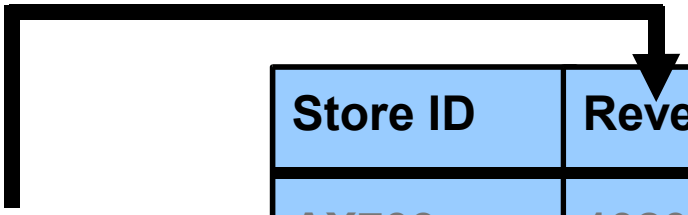
- Virtual Private Database

Row Level Security Controls

- Virtual Private Database
- Introducido en Oracle8i
- Extiende la seguridad más alla de los privilegios de los objetos



Row Level & Column Controls

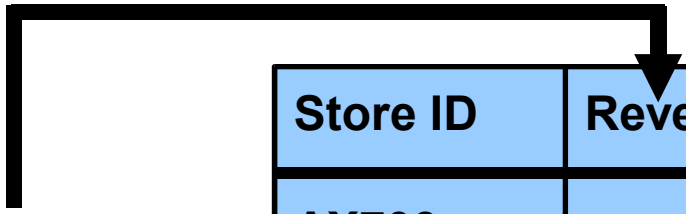


Select store_id, revenue…
(enforce)

Store ID	Revenue	Department	
AX703	10200.34	Finance	X
B789C	18020.34	Engineering	OK
JFS845	12341.34	Legal	X
SF78SD	13243.34	HR	X

VPD Policy is invoked ONLY if the revenue column is referenced In the SQL statement

Row Level & Column Controls



Select store_id, revenue…
(enforce)

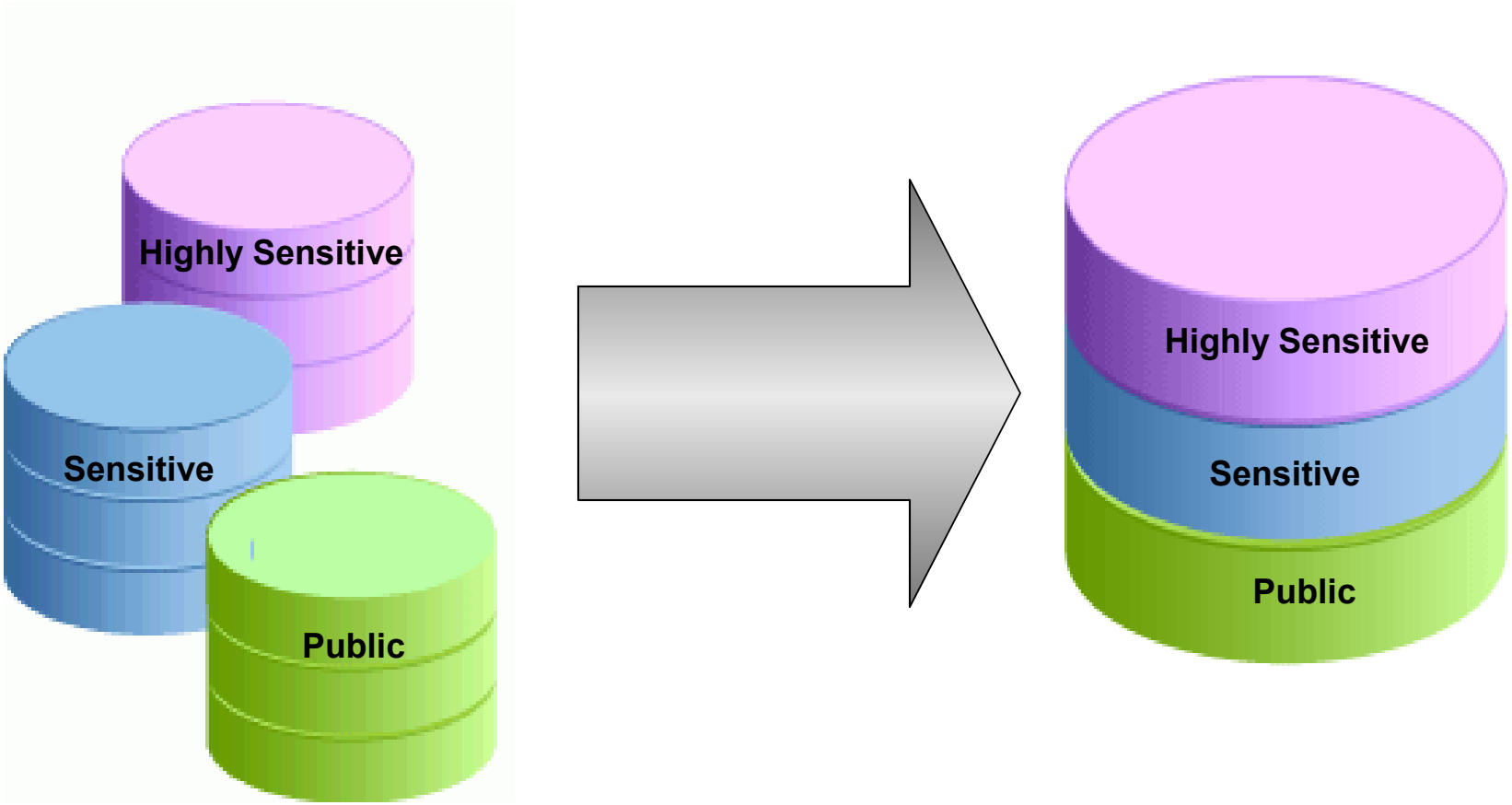
Store ID	Revenue	Department	
AX703		Finance	OK
B789C	18020.34	Engineering	OK
JFS845		Legal	OK
SF78SD		HR	OK

VPD Policy is invoked ONLY if the revenue column is referenced In the SQL statement, BUT All rows are returned with columns NULLED out in rows which didn't pass VPD policy

Multi-level Security
and
Data Classification

Label
Security

Oracle Label Security
Consolidated Sensitive Data



Controles de Acceso Fuertes y Flexibles

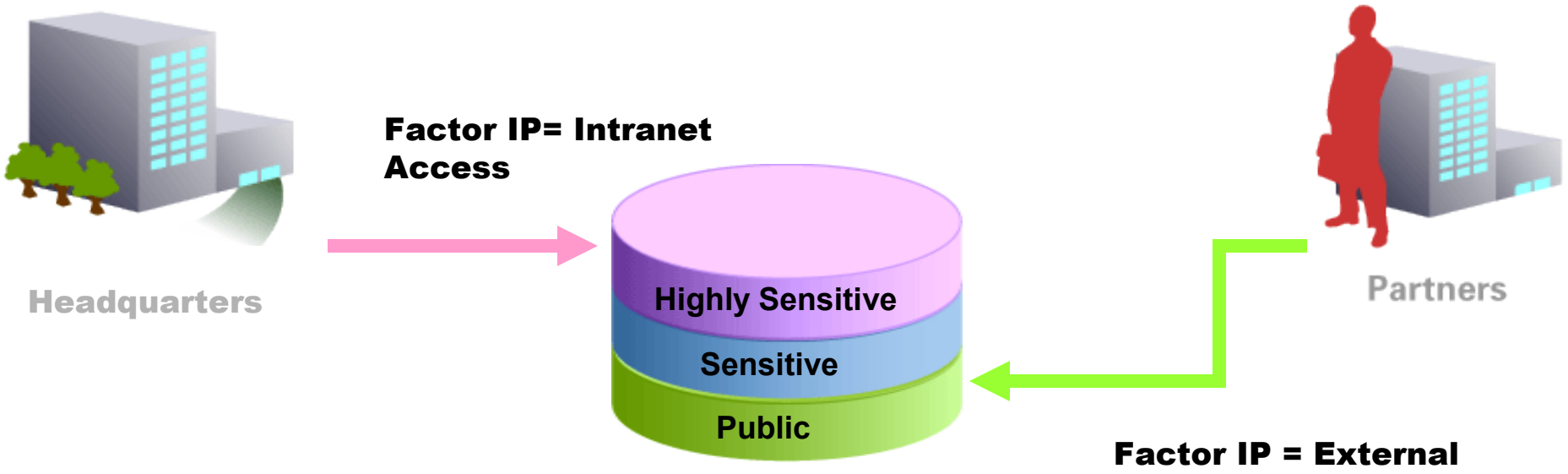
Oracle Label Security

User Sensitivity Level = **Sensitive**

Application Table

Store ID	Revenue	Department	Sensitivity Label
AX703	10200.34	Finance	Sensitive
B789C	18020.34	Engineering	Highly Sensitive
JFS845	15045.23	Legal	Confidential
SF78SD	21004.45	HR	Public

Oracle Label Security Database Vault Integration



Oracle Label Security Restricts Access To Labeled Data Based On Database Vault Factors

Oracle Database Vault

Problemas de Seguridad Comunes

- Tengo requerimientos por SOX acerca de cómo puedo prevenir que mi DBA mire datos de la aplicación, incluyendo información como Tarjetas de Crédito?
- Cómo puedo reforzar el acceso a los datos a través de la aplicación?
- Cómo puedo prevenir las modificaciones no autorizadas a mi aplicación y base de datos?

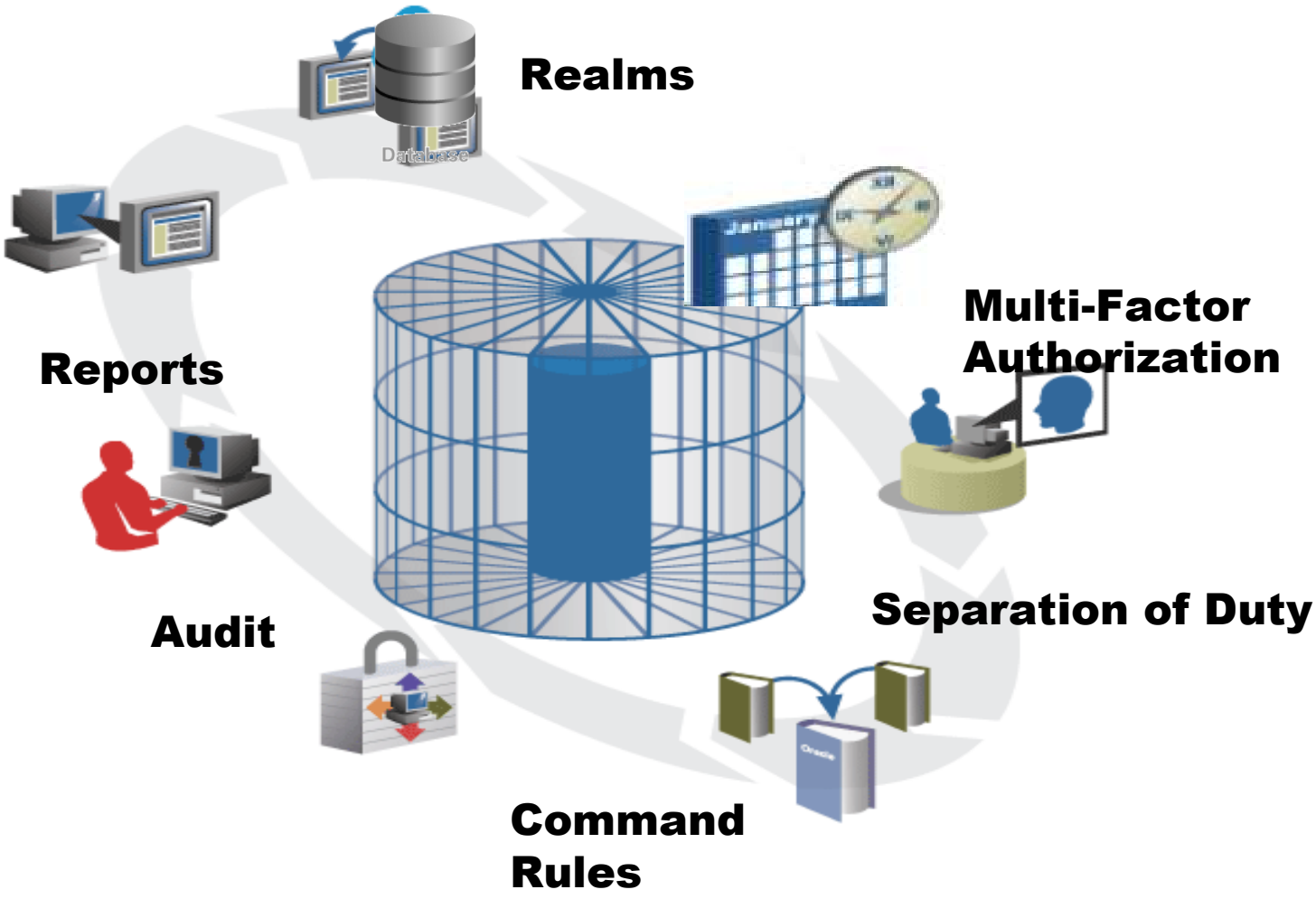
Ad-Hoc Query
On Financial Data

Applications

Ad-Hoc Query
Tool

Remote DBA
Services

Database Vault Security



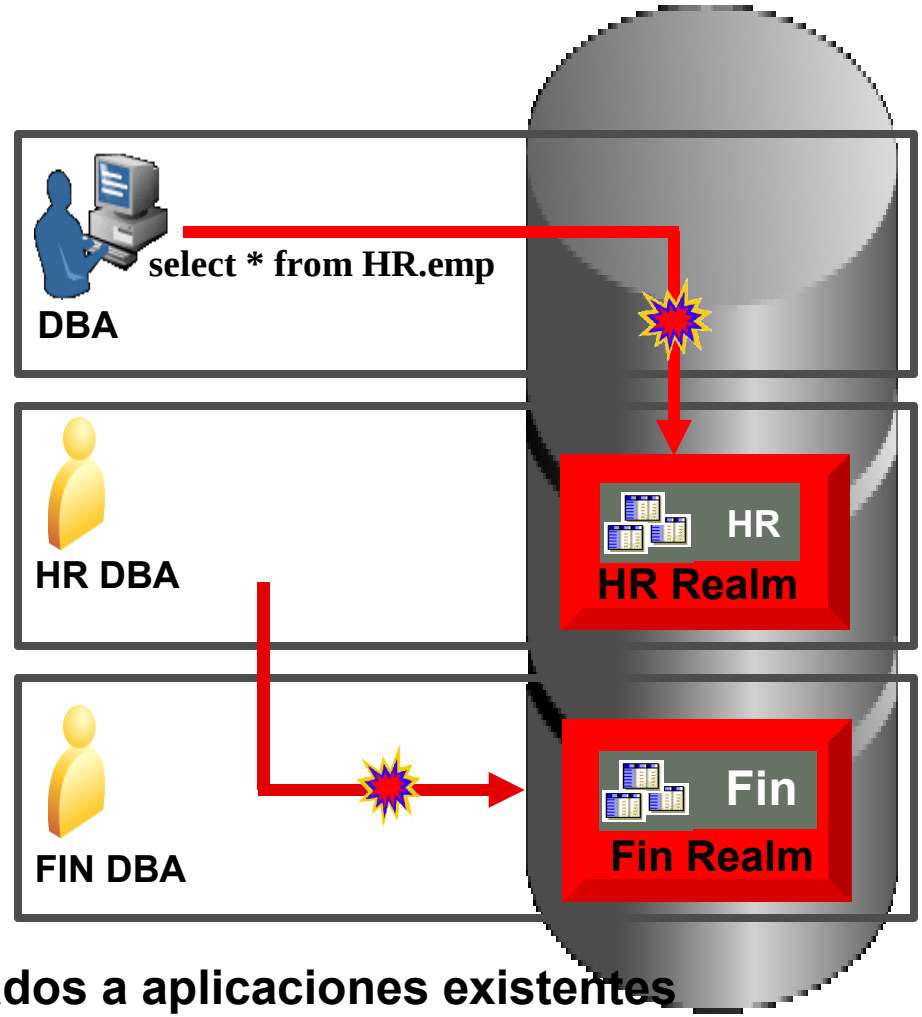
Oracle Database Vault Realms

- DBA de la Base de Datos ve datos de HR

  Conformidad normativa y protección de “insiders”

- DBA de HR ve datos de Fin

  Elimina los riesgos de seguridad por consolidación de servidores



Realms pueden ser fácilmente aplicados a aplicaciones existentes con mínimo impacto en rendimiento

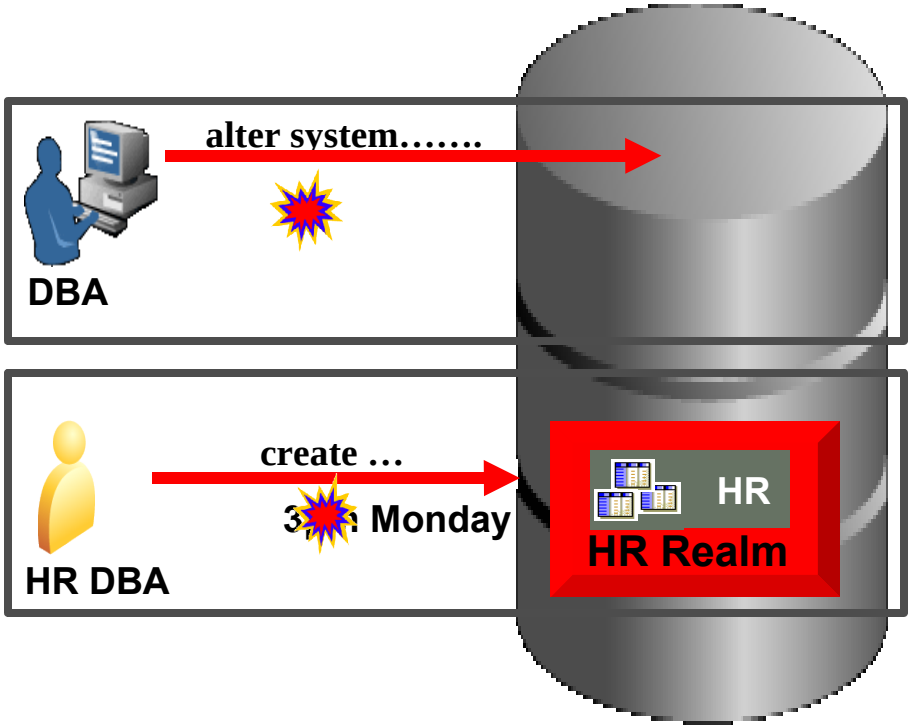
Oracle Database Vault
Rules & Multi-factor Authorization

- DBA intenta un "*alter system*" remoto

  Regla basada en la dirección IP bloquea la acción

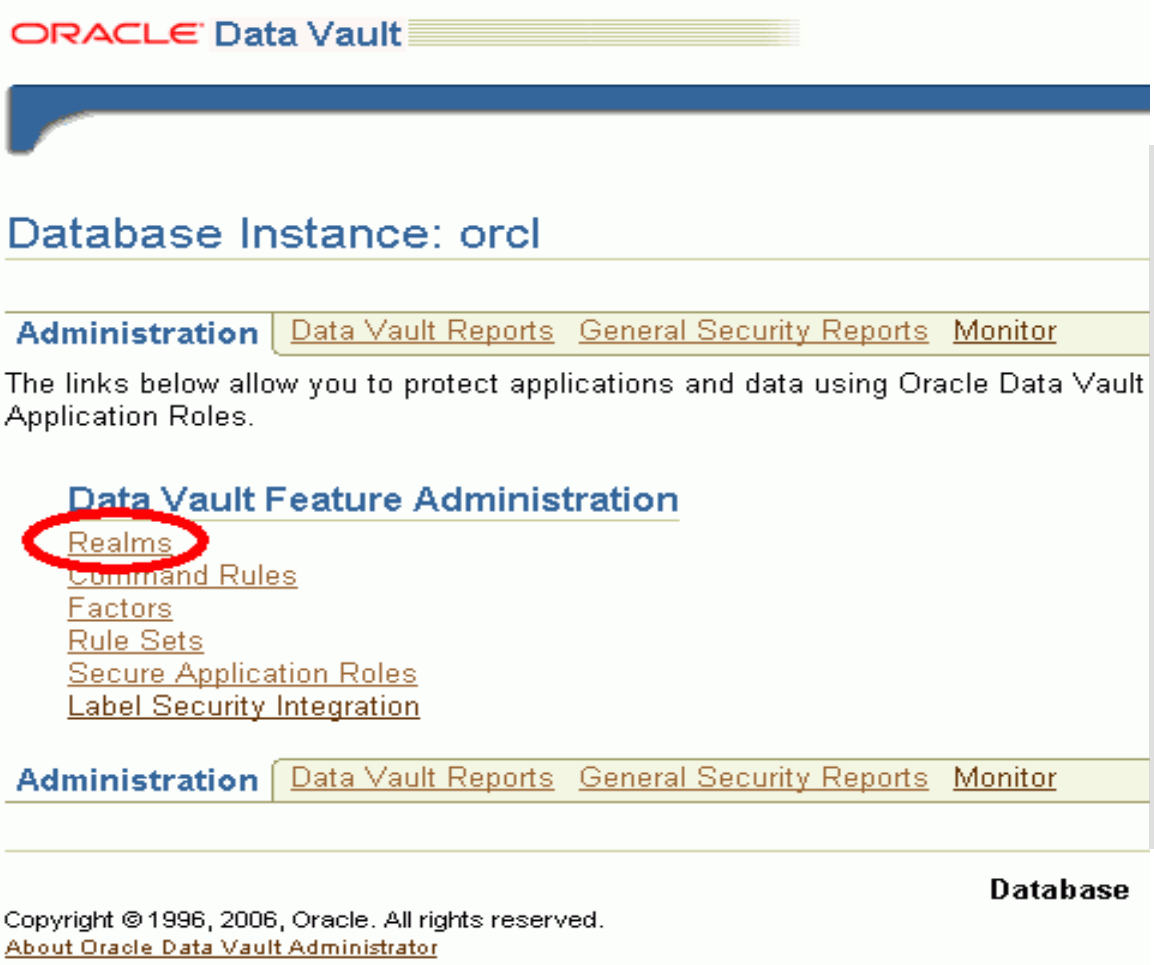
- DBA de HR realiza acciones no autorizadas durante producción

  Regla basada en Fecha y Hora bloquea la acción



Los Factores y Reglas de Comando ofrecen controles de seguridad flexibles y adaptables

Interfase Administrativa Web

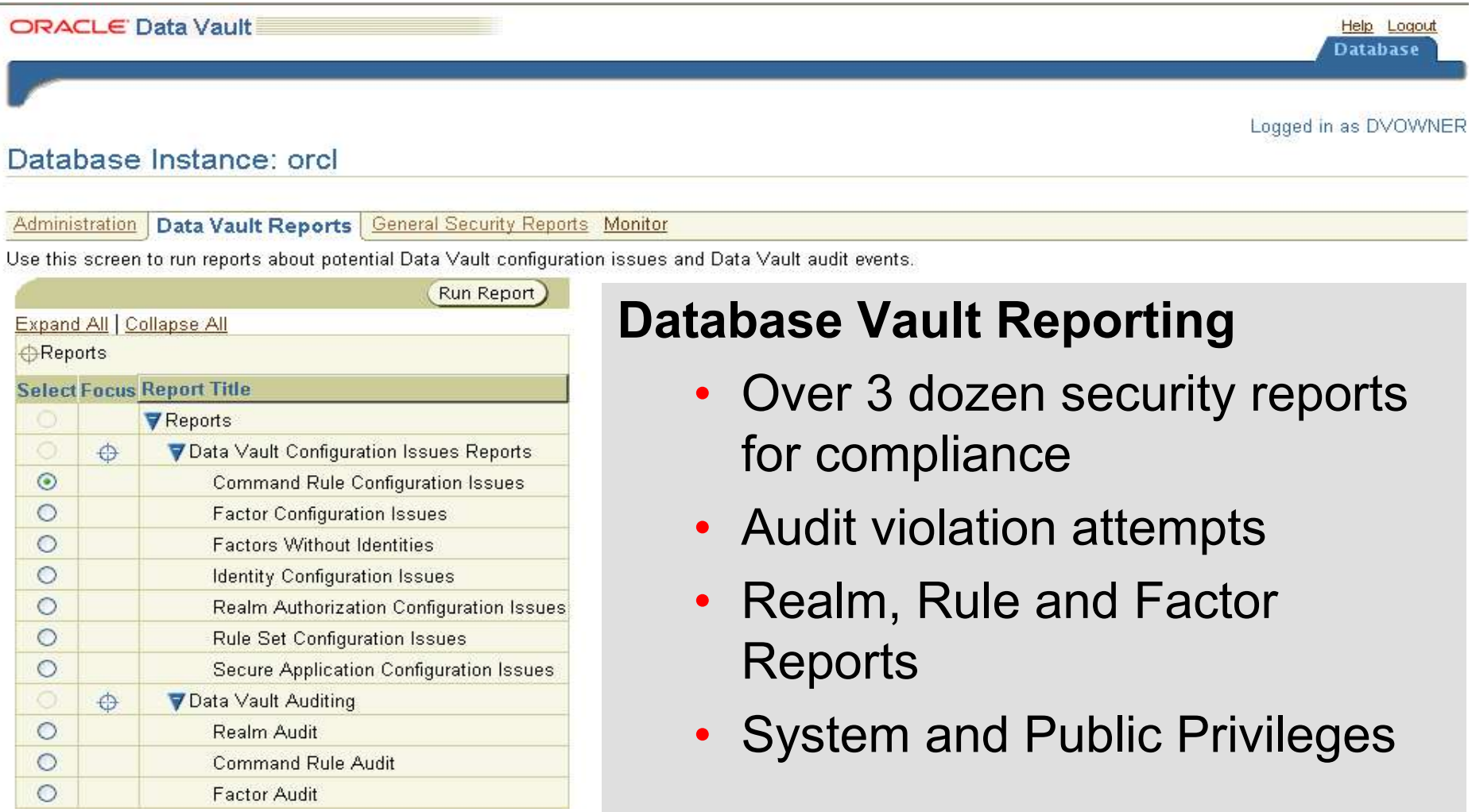


Web Based Management

- Realms
- Rules
- Factors
- Reports
- Dashboard

Back to Platform Diagram

Reportes Oracle Database Vault



Database Vault Reporting

- Over 3 dozen security reports for compliance
- Audit violation attempts
- Realm, Rule and Factor Reports
- System and Public Privileges

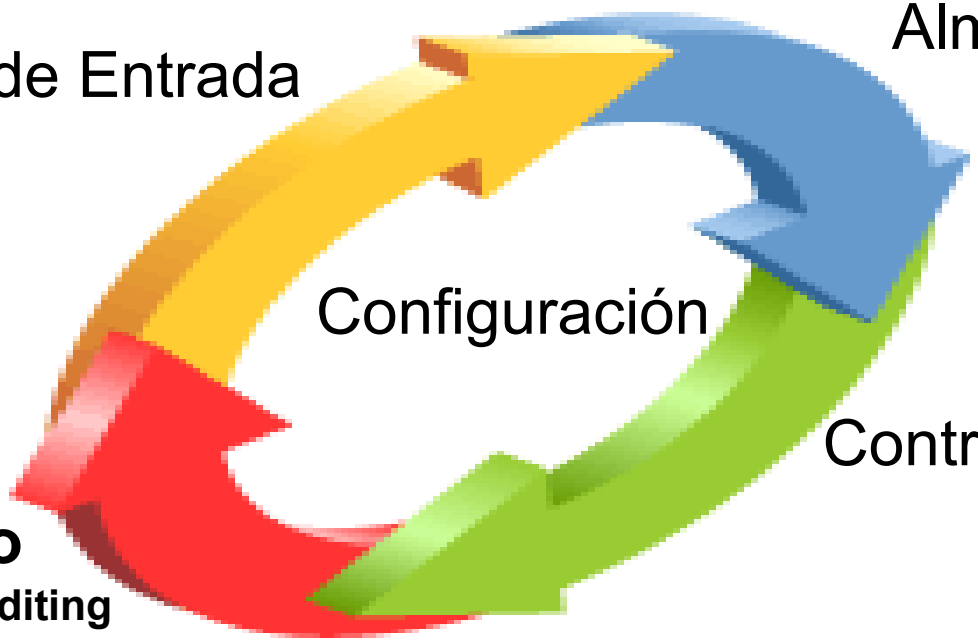
Back to Platform Diagram

"Microsoft, IBM and Sybase don't have anything like this”

"Enterprises want their administrators to manage their databases, not data“

- *Noel Yuhanna, Forrester Research*

Ciclo de Vida de la Seguridad de los Datos



Monitoreo

- **Database Auditing**
- **Audit Vault***

Auditoría Corporativa

Confía pero Verifica (Control)

- Motivadores principales
  - Conformidad con las regulaciones
    - Demostrar controles para la utilización, configuración, roles, políticas
    - Rastro de auditoría verificable
  - Amenaza interna
    - Detectar mal uso de los datos
    - Alertas y acciones correctivas

- Los rastros de auditoría muestran quién hizo qué, cuándo, dónde y cómo
- Requerimientos
  - Recolectar y administrar grandes volúmenes de datos auditados
  - Proteger datos de auditoría y compliance
  - Fuertes capacidades analíticas y de reportes

Oracle Database Audit

Auditoría Robusta, Flexible, y de Alta Fidelidad

- Auditoría Mandatoria
  - Eventos críticos incluyendo startup y shutdown
- Auditoría SYS
  - Acciones de SYSDBA y SYSOPER
- Auditoría Estándar
  - Sentencias (DML, DDL)
  - Privilegios, Objetos, Usuarios
  - Falla o Exito
- Fine Grained Auditing (FGA)
  - Basado en cualquier condición
  - Manejador de evento para notificación
- Almacenamiento de auditoría: Database, OS files

- Quién
  - Database username, OS username, clientid, userguid…
- Dónde
  - Userhost, terminal#, process#, ecid…
- Cuándo
  - Timestamp, System Change Number(SCN), logofftime…
- Qué
  - DML, DDL
  - SQL-Text
  - SQL-Bind…

Database Auditing

- Fine Grained Auditing introducido en Oracle9i
  - Desarrollado a petición de un cliente de gobierno
  - Las políticas de auditoría son almacenadas en la base de datos, asociadas con tablas
  - La política es invocada cuando la tabla es accedida; puede auditar cuando una columna específica es accedida

Enforce Audit Policy in Database
...
Where Salary > 500000
AUDIT COLUMN = Salary

Audit Record Shows...

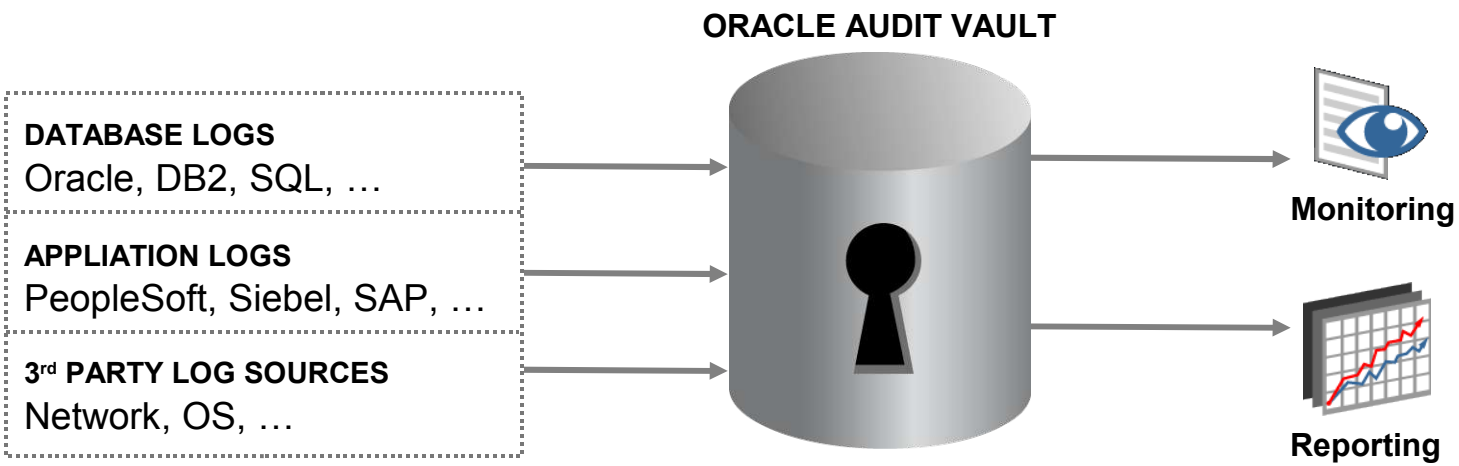
Select name, salary
from emp
where name = 'KING',
<timestamp>,
<username>

Oracle Audit Vault

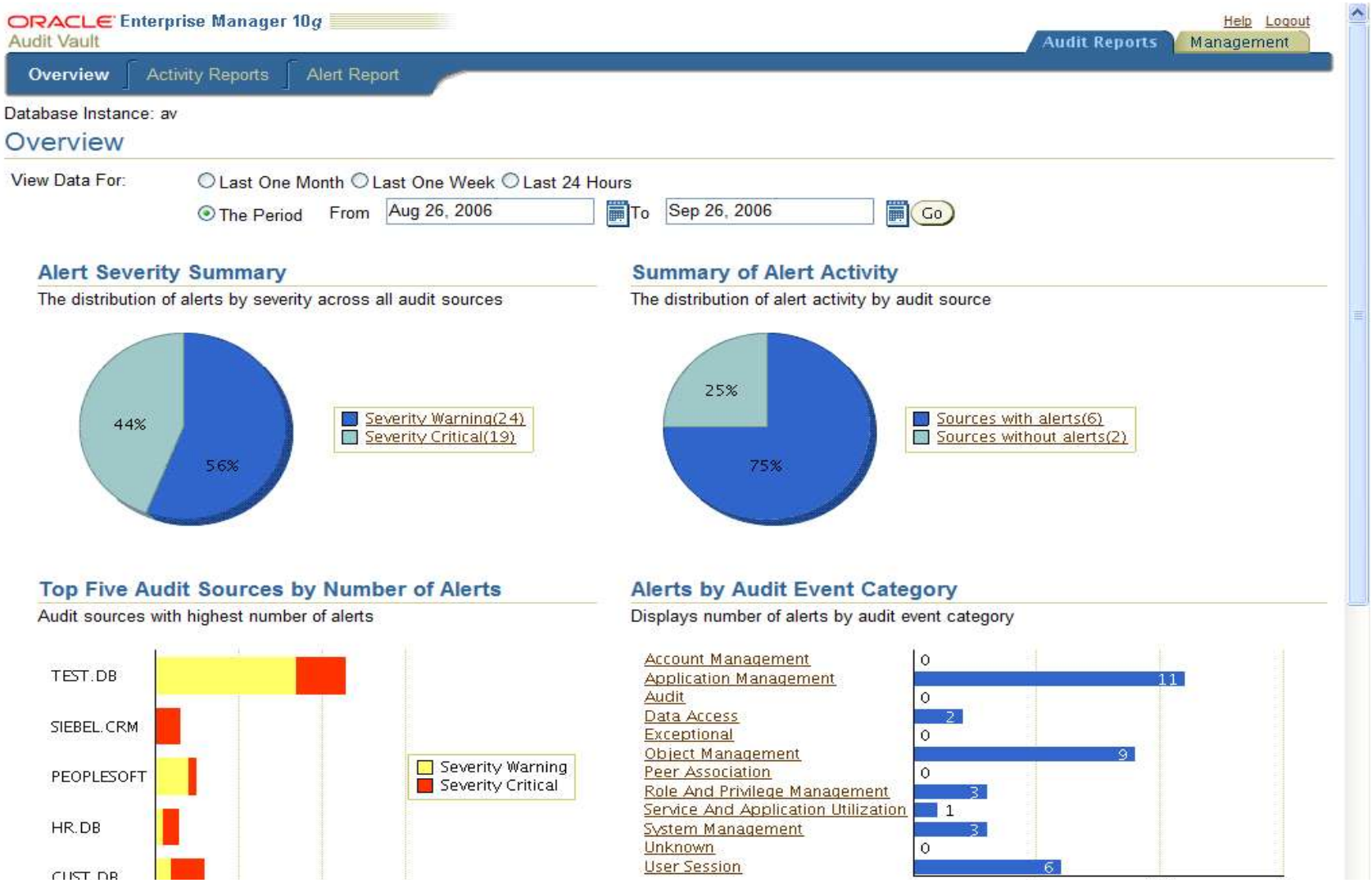
Asegurando la prueba de conformidad

Coming Soon!

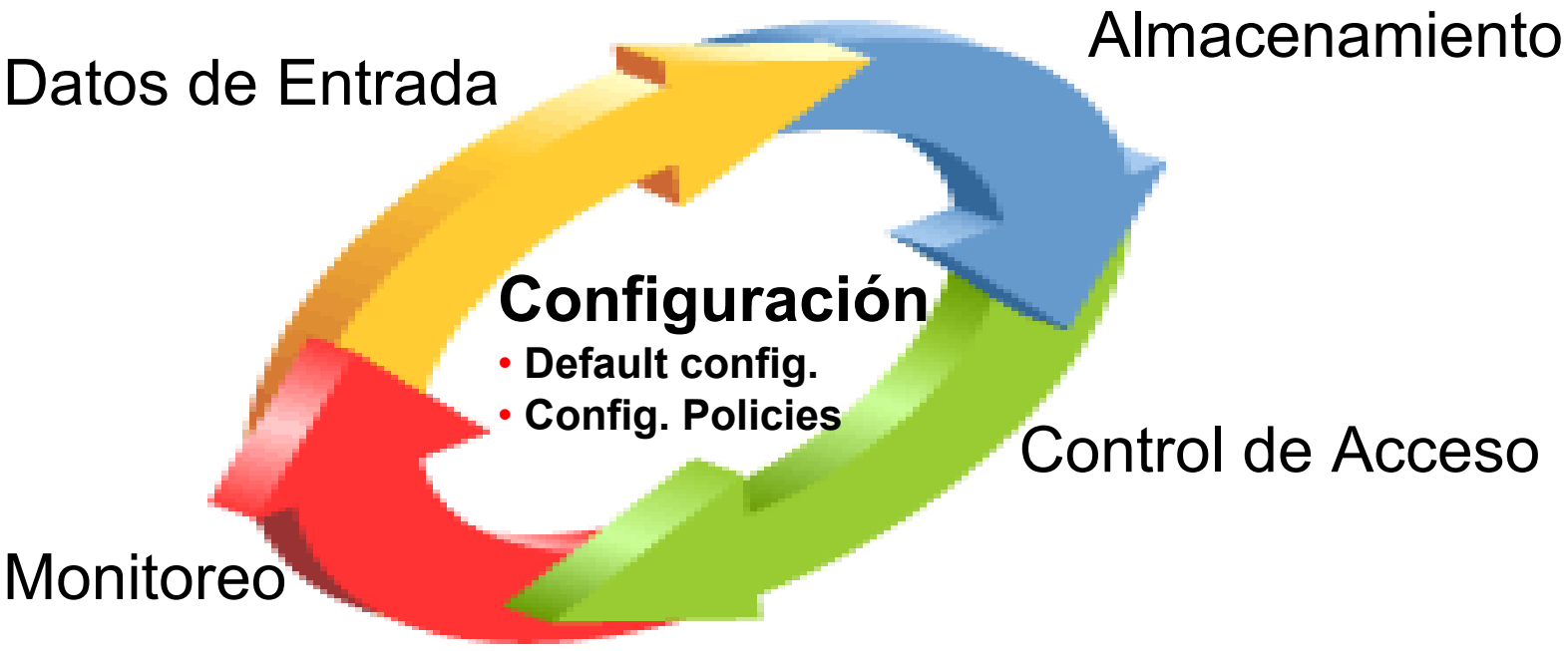
- Asegura la integridad de los datos de auditoría.
- Oracle Audit Vault – warehouse especializado para data de auditoría.
  - **Agrega** los datos de auditoría – fuentes Oracle y no Oracle
  - **Asegura** datos de auditoría valiosos
  - **Monitorea** cambios asociados con usuarios privilegiados
  - **Reportes** para la conformidad



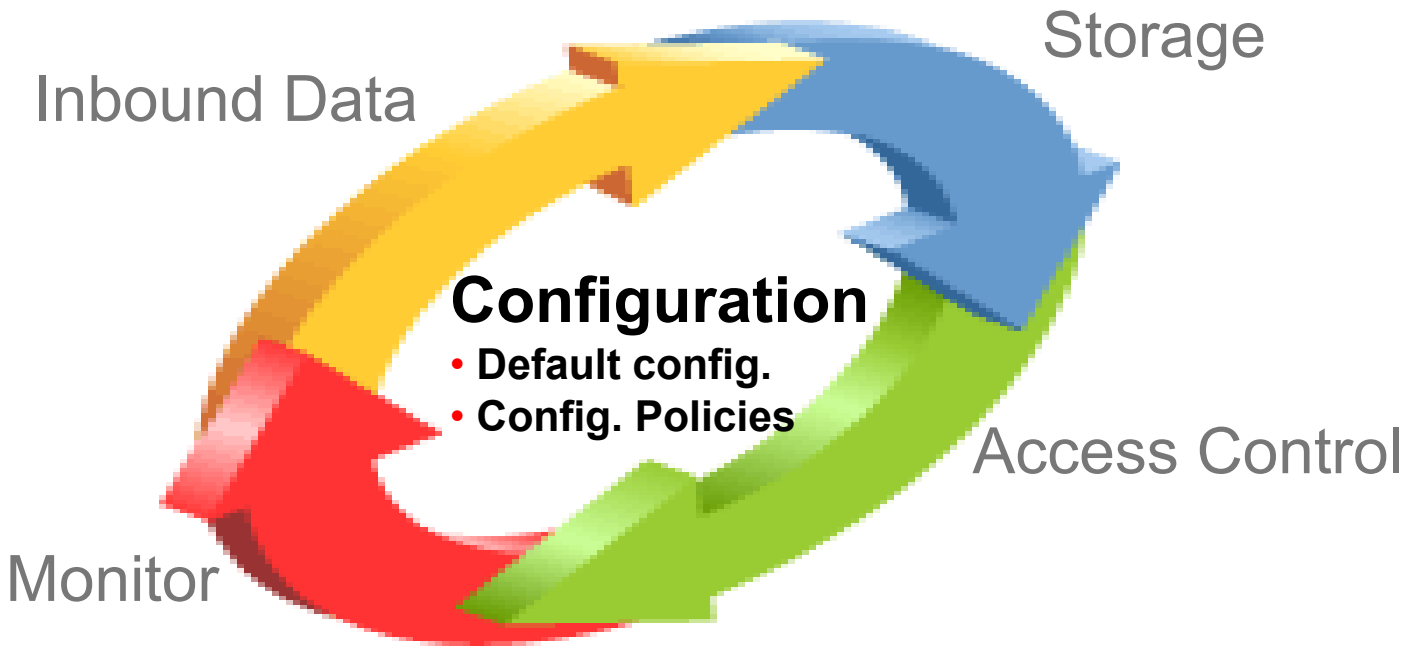
Audit Vault Dashboard



Ciclo de Vida de la Seguridad de los Datos



Data Security Lifecycle



EM Configuration Management

- Foco en la gestion y auditoría de las Configuraciones
  - Quién cambió la configuración, cuándo y por qué
  - Automatiza la evaluación del sistema y reporta desviaciones
  - Mantene los sistemas alineados con la “configuración dorada”
  - Registra el progreso de la conformidad en el tiempo
- Ciclo completo de corrección
  - Acciones correctivas guiadas
  - Integración con soluciones de registro de problemas
- Configuraciones recomendadas
- Soporta Oracle 8*i* y versiones posteriores
- Soporta los Estándares de la Industria: ITIL, COBIT, CIS

Ejemplos de Reglas de Políticas de Seguridad

All Oracle Software

- Security alerts
- Critical security patches

ost

etect open ports

etect insecure services

nsure NTFS file system type

pplication Server

TTPD has minimal privileges

se HTTP/S

Database Services

nable listener logging

assword-protect listeners

isallow default listener name

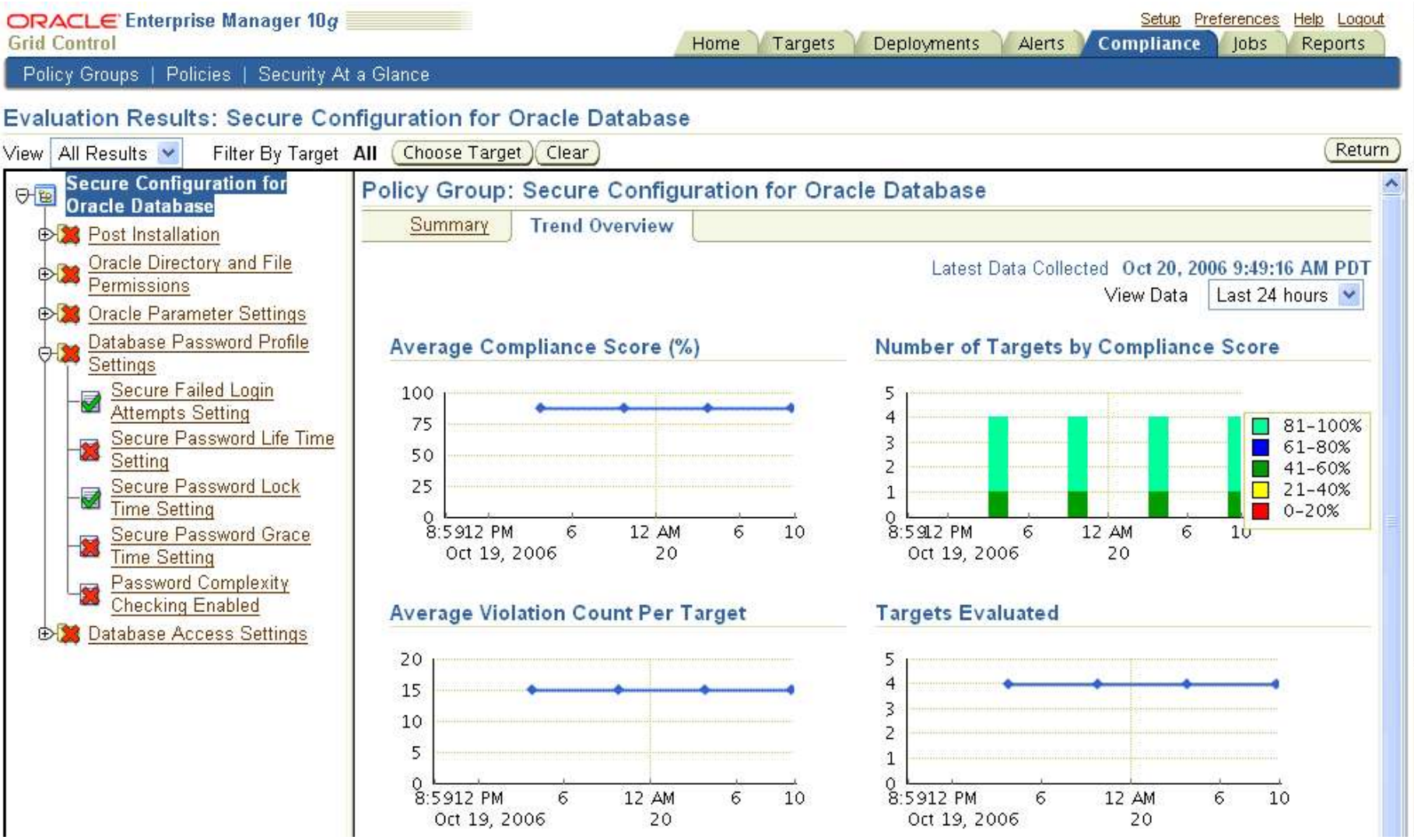
Database File Permissions

- Init.ora with restricted file permission
- Files in $OH/bin owned by Oracle
- …

Database Profile/Configuration

- Disallow object access by fixed user link
- Set password_grace_time
- Limit or deny access to DBMS_LOB
- Avoid using utl_file_dir parameter
- …

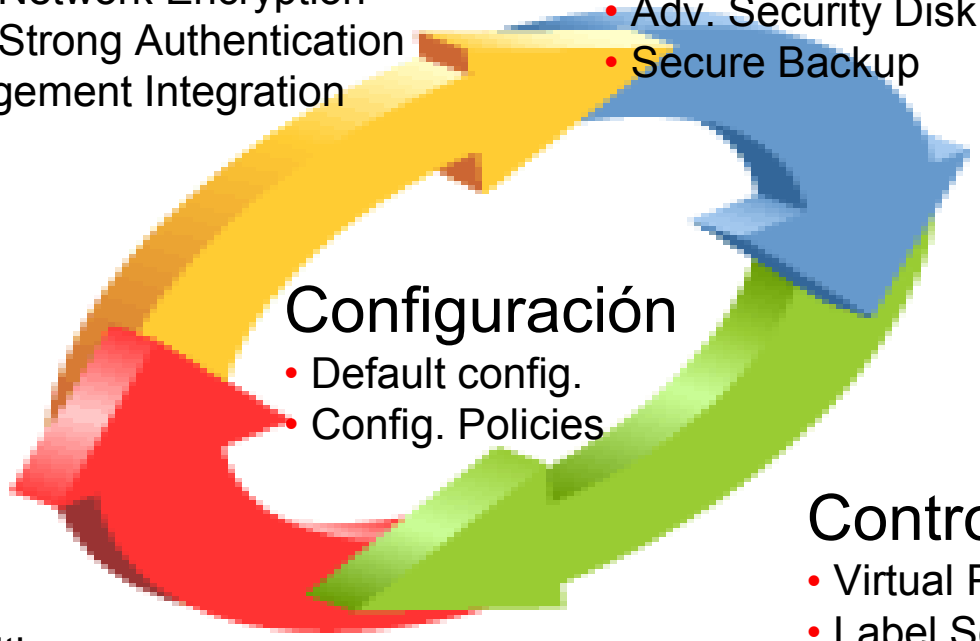
Compliance Trend Analysis: 10gR3



Ciclo de Vida de la Seguridad de los Datos

Datos de Entrada
- Adv. Security Network Encryption
- Adv. Security Strong Authentication
- Identity Management Integration

Almacenamiento
- Database Encryption APIs
- Adv. Security Transparent Data Encryption
- Adv. Security Disk Backup Encryption
- Secure Backup



Configuración
- Default config.
- Config. Policies

Monitoreo
- Database Auditing
- Audit Vault*

Control de Acceso
- Virtual Private Database
- Label Security
- Database Vault

Coming up….

27 a 29 de Marzo, 2007

Transamerica Expo Center

São Paulo – Brasil

www.oracle.com/goto/openworld-la

ORACLE IS THE INFORMATION COMPANY