
redPartner®

Soluciones para Seguridad Riesgo y Cumplimiento (GRC) Portafolio Oracle para optimizar el cumplimiento de normas y la eliminación del Riesgo

MSc. Lina Forero
Gerente de Consultoría
Junio 2010

La Seguridad no es un producto Puntual

Ataques son más comunes de lo que queremos creer ...

| Security Fix Live: Web Chats | E-Mail Brian Krebs

Network Solutions Hack Compromises 573,000 Credit, Debit Accounts

Hackers have broken into Web servers owned by domain hosting provider **Network Solutions**, planting rogue coc in the compromise of more than 573,000 debit and credit over the past three months, **Security Fix** has learned.

Bahamas Share Print Email RSS

IDs of 50,000 Bahamas resort guests stolen

1:20PM Monday Jan 09, 2006

January 3, 2006 5:02 AM PST

Marriott loses data on 200,000 customers

ies of more than 50,000 customers of major
en exposed to possible identity fraud

By Ingrid Marson

Related Stories

Hackers steal customer data from gaming company
December 19, 2005

Stolen PC holds sensitive consumer data

Hotel chain Ma
containing dat
company offic

The data, whicl
Vacation Club I
card details, Sc
customers.

July 22, 2005 5:27 PM PDT

University of Colorado servers hacked

By Joris Evers
Staff Writer, CNET News

The University of Colorado has become the latest educational institution to fall prey to hackers. The school is warning about 43,000 people that they may be at risk of having their identities stolen after two of its servers were attacked, it said Thursday. One server, at the school's health center, contained the names, Social Security numbers, student ID numbers, addresses and dates of birth of about 42,000 people, the university said. Also stored on the server were the results of about 2,000 laboratory tests, the university said. The break-in was discovered on July 14. Initial investigation has found no evidence that personal data was extracted or abused, according to the university.

ISO 9001 : 2000
Sistema de Gestión de Calidad Certificado

contacto@red-partner.com

Ataques son más comunes de lo que queremos creer ....

"Wells Fargo Bank reports computer stolen containing private data"

*"Lexis Nexis database hacked containing **310,000** customers"*

*"Bank of America looses back tapes containing **1.2 million** federal emp"*

Y la lista sigue . . . 50 millones de clientes afectados!! *

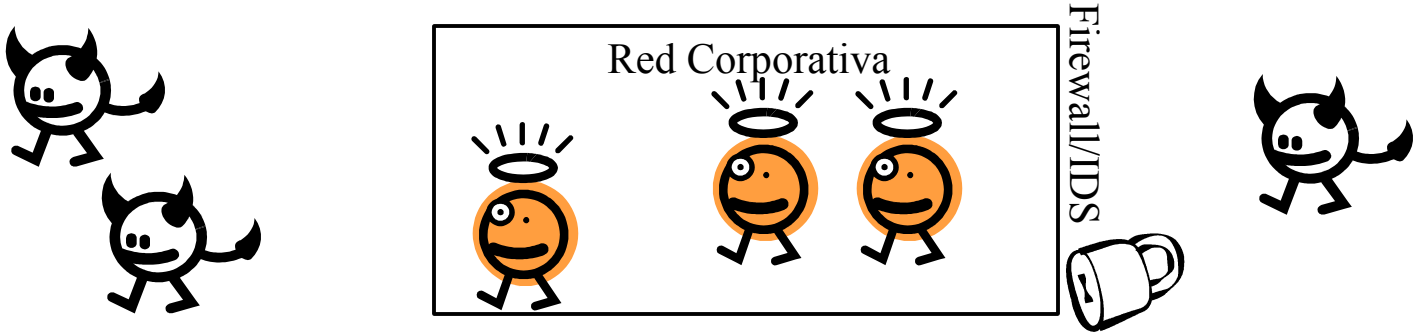
- Por qué fueron atacadas estas bases de datos ?
- Podría haberse evitado ?
- Y que hay de los ataques que no se reportan ?

* Fuente: Forrester db security report 2006

Tipos de amenazas a las bases de datos

- SQL Injection, passwords robados, ataques de fuerza bruta
- Passwords débiles
- Alteración y fabricación de datos y logs de auditoria
- Vulnerabilidades en la arquitectura de la aplicación
- Cintas de respaldo perdidas, o robadas

- Amenazas internas una gran preocupación debido a la facilidad que representa tener información privilegiada para causar daño.



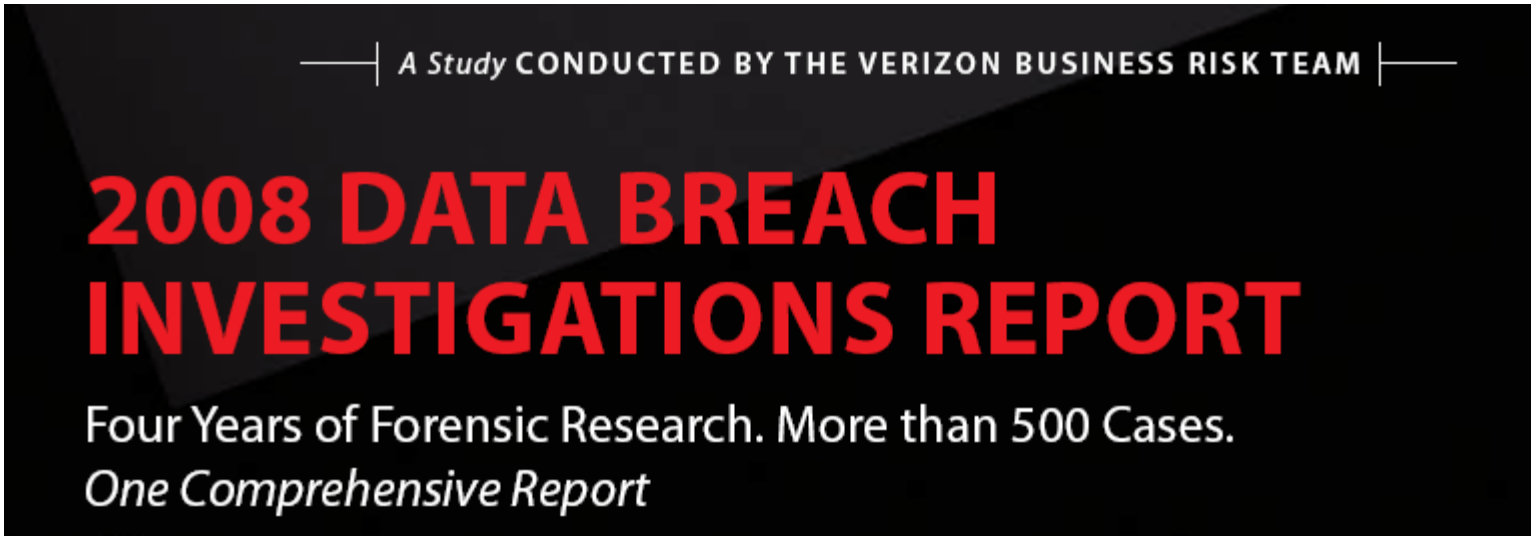
Pilares de la Seguridad de la Información

Confidencialidad	Prevención del acceso no autorizado a la información;
Integridad	Prevención de la modificación no autorizada de la información;
Disponibilidad	Prevención de la falta de acceso a la información cuando esta es necesaria, bien sea por motivos lógicos o físicos.

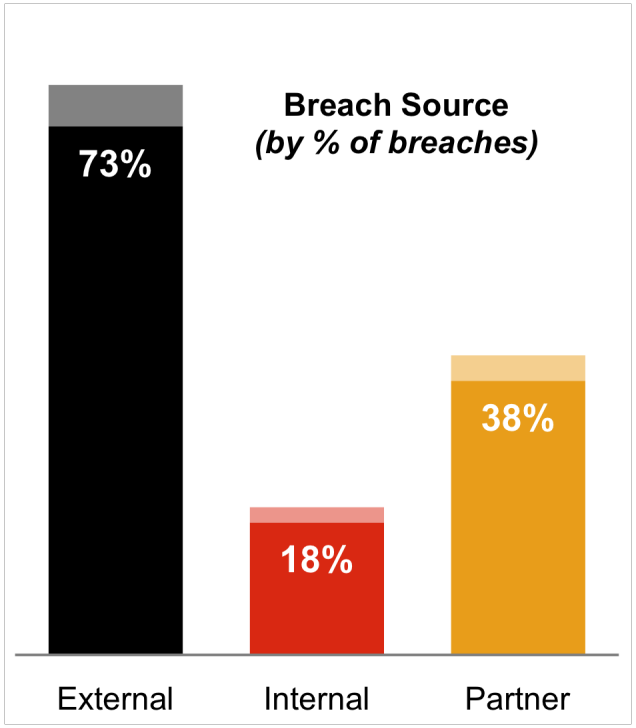
Information Technology Security Evaluation Criteria (ITSEC)

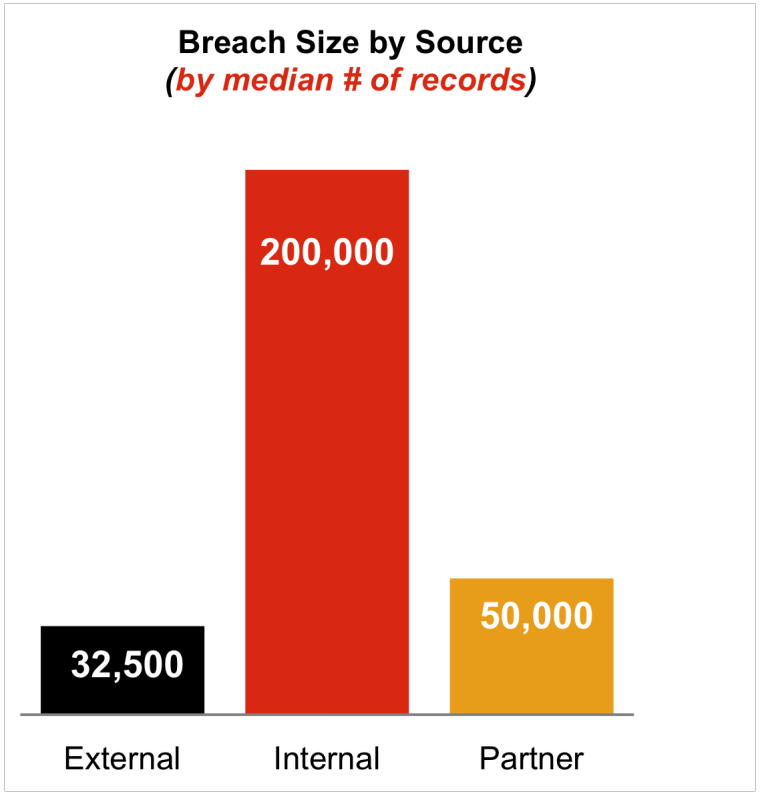
Anatomía de un ataque – Robo de Información

- 2008 Data Breach Investigation Report
- Más de 500 casos documentados, durante un período de 4 años



Anatomía de un ataque – Robo de Información





Cómo ocurren los ataques a la información?

62% Fueron consecuencia directa o indirecta de un error

59% Como resultado de hacking e intrusiones

31% Incorporando código malicioso

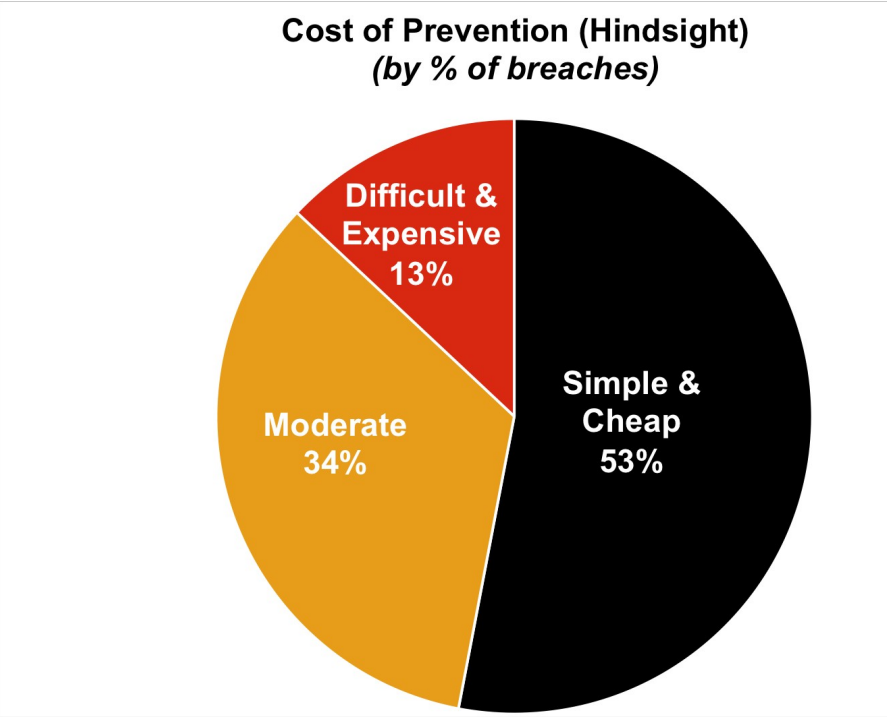
22% Explotaba alguna vulnerabilidad

15% Debido a amenazas físicas

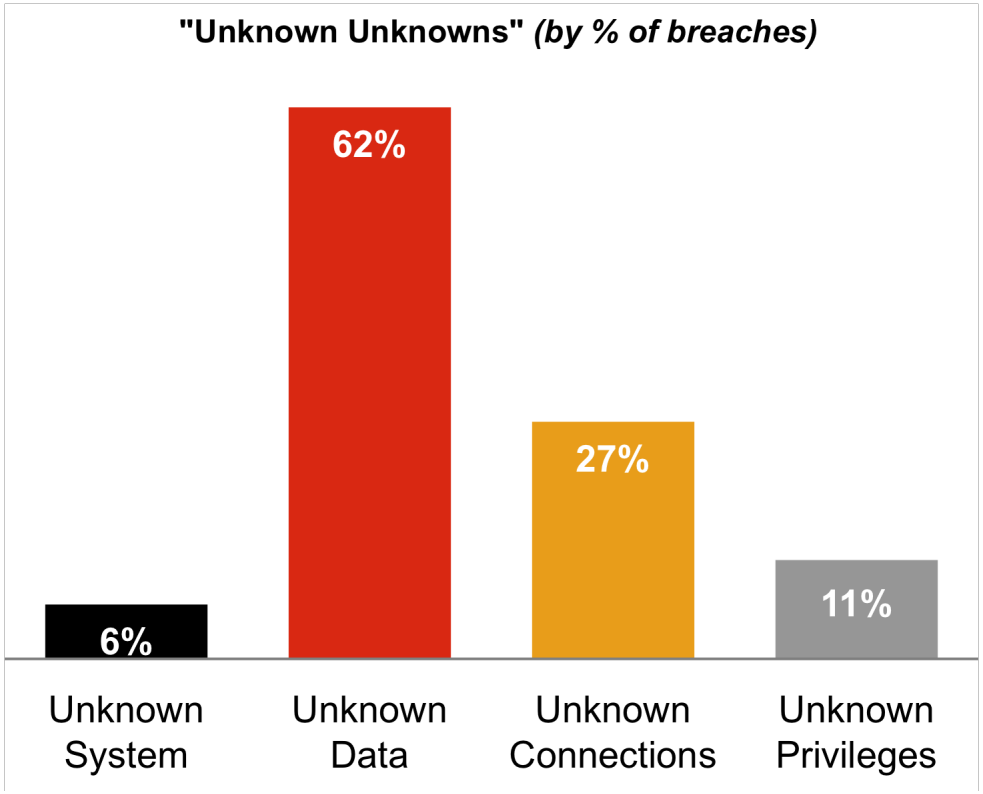
90% de las vulnerabilidades conocidas explotadas por ataques, tenían parches disponibles **al menos 6 meses antes** del *ataque*

Qué tienen en común estos ataques?

- Falta de procedimientos de validación y aseguramiento
- Costo de la prevención órdenes de magnitud menores que el impacto
- Demasiada atención a cosas que no suceden
- Poca atención a las cosas que si ocurren



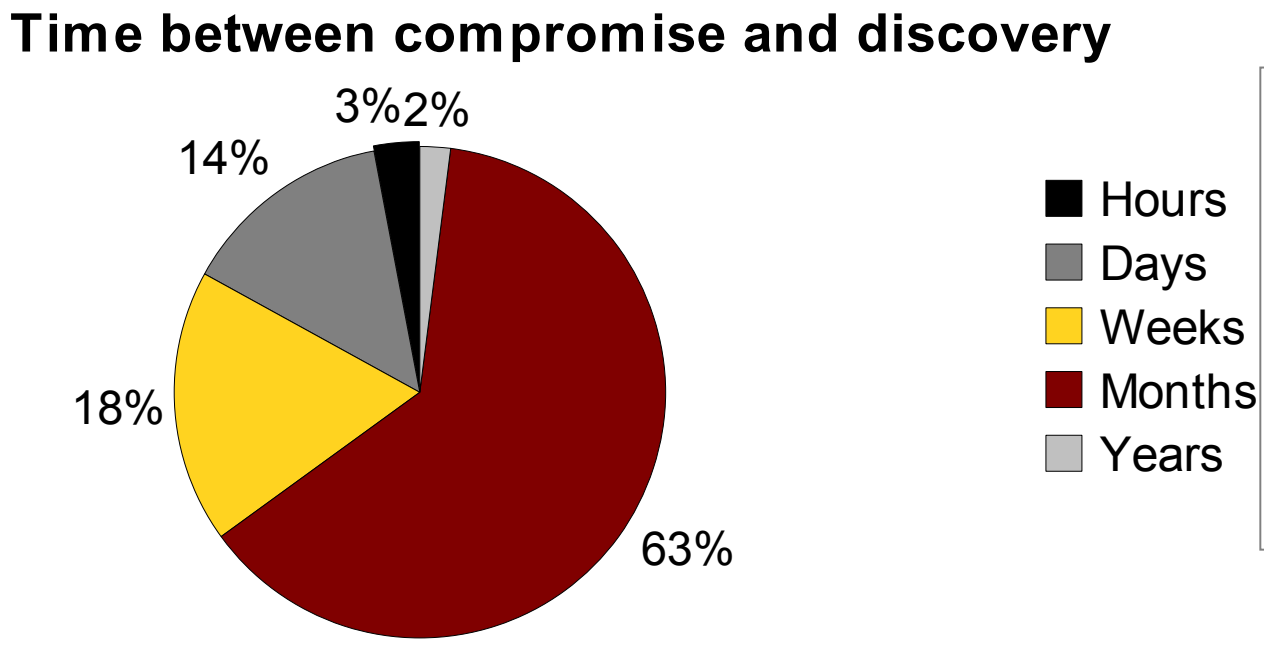
Qué tienen en común estos ataques?



66%

Comprometieron datos que la víctima no sabía que existían en el sistema

Qué tienen en común estos ataques?



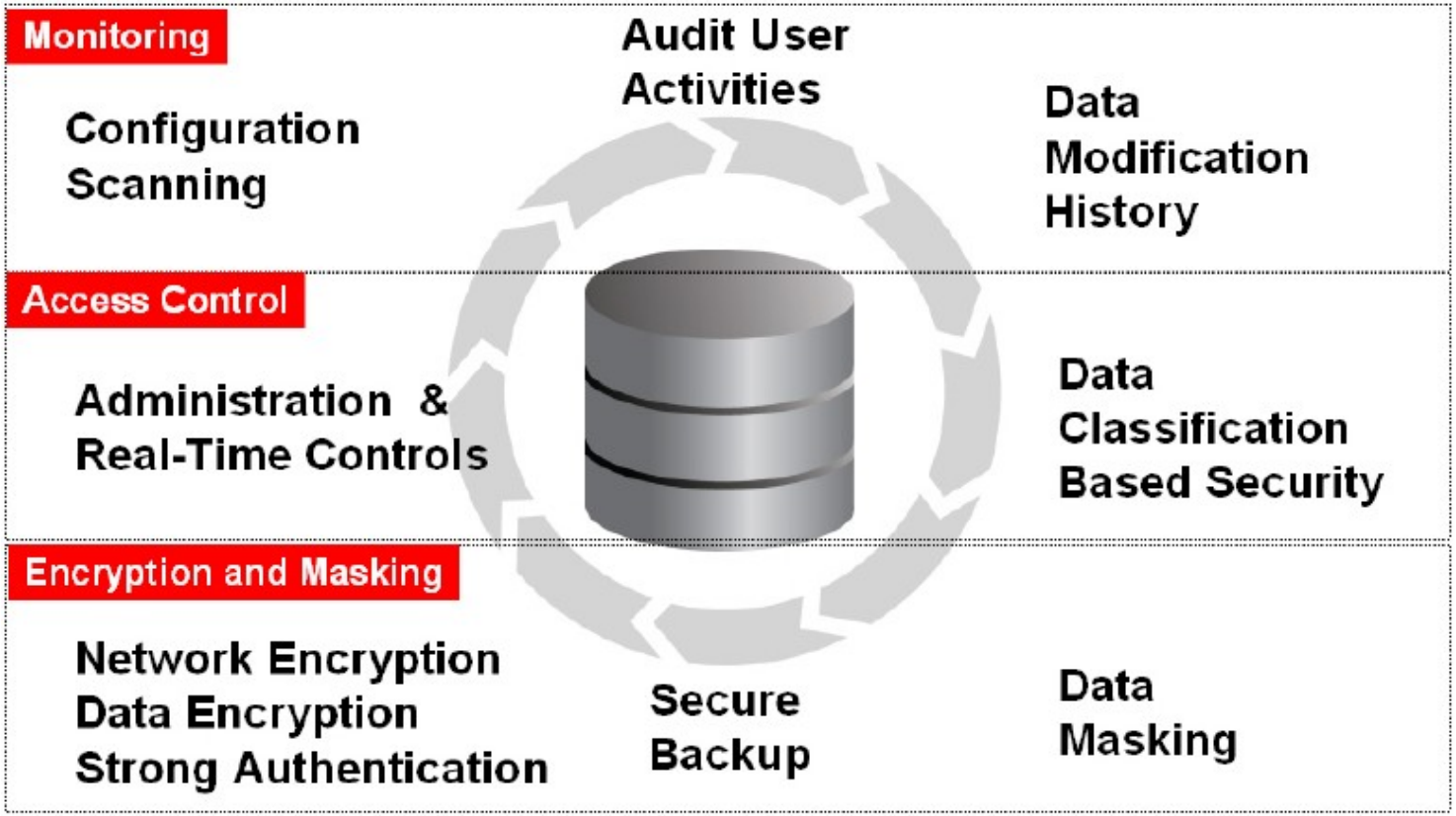
!!!

Existe una gran deficiencia en Monitoreo y Auditoría!

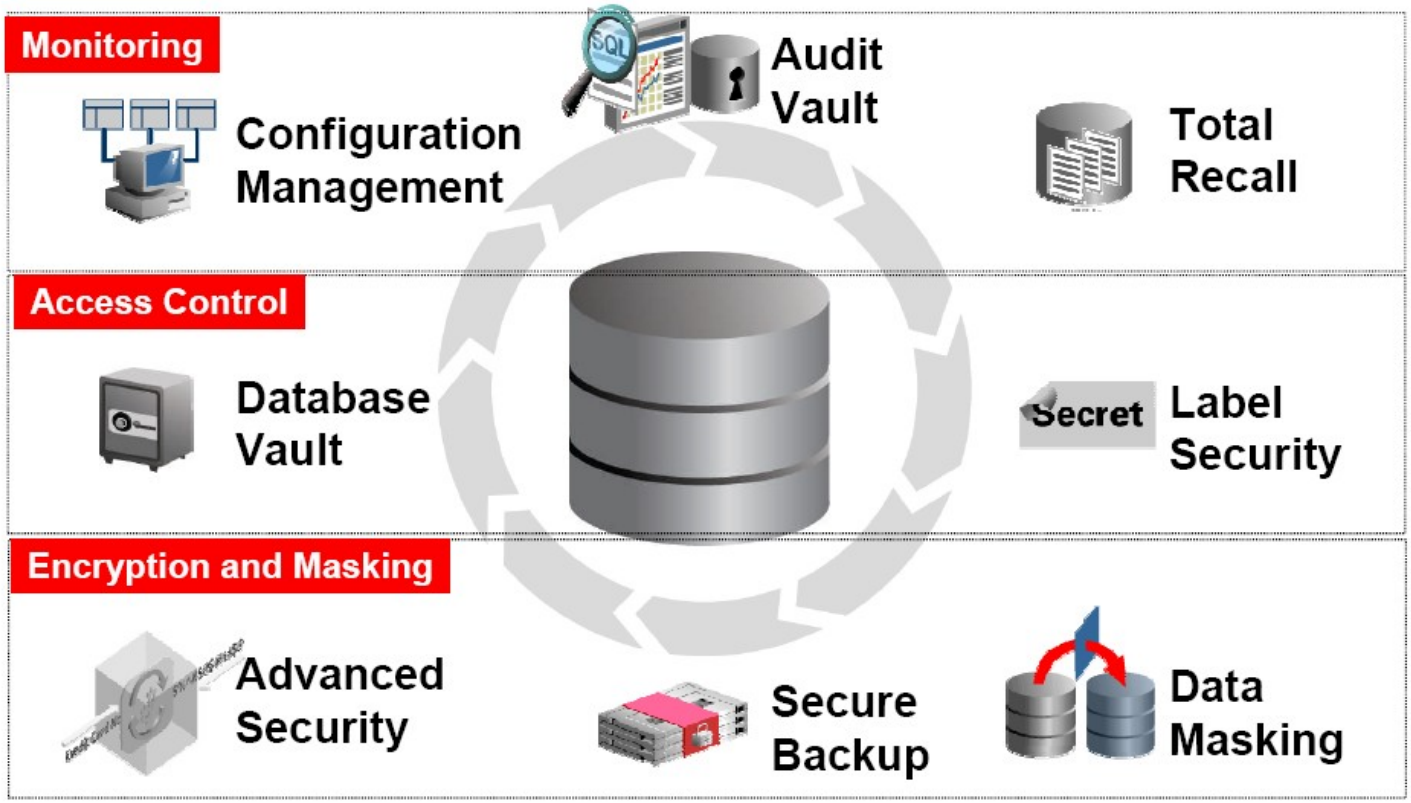
Grandes Objetivos

- Obtener una Base de Datos Segura
- Almacenar los datos valiosos/críticos de forma Segura.
- De acuerdo a IDC , Protección y Control de la Información (IPC).

Productos de Seguridad de Oracle

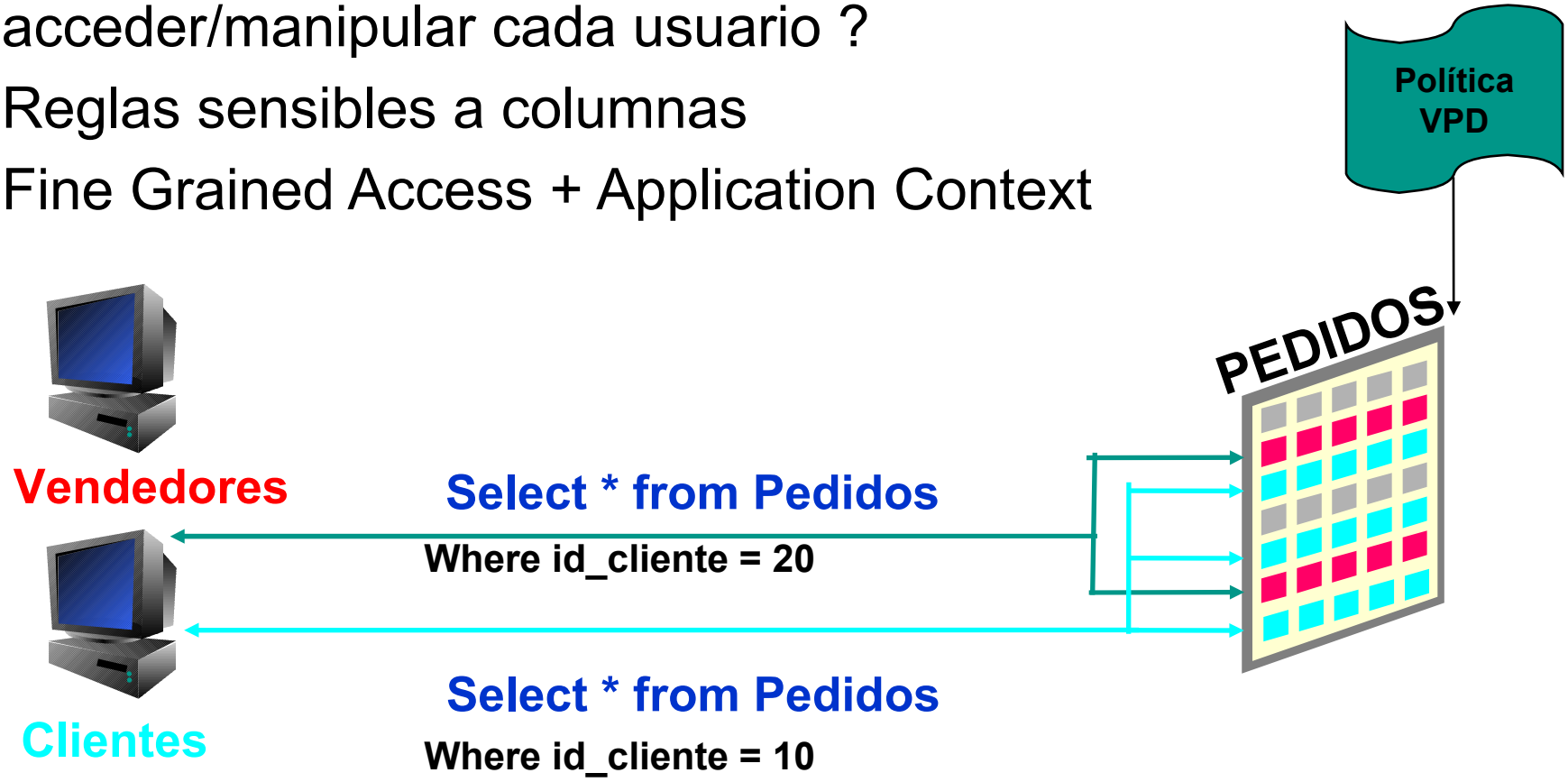


Productos de Seguridad de Oracle



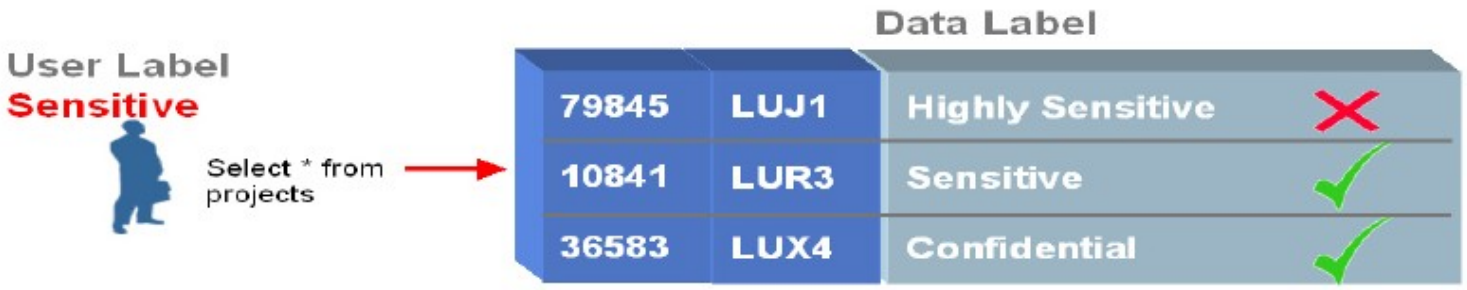
Control de Acceso – Virtual Private Database

- Seguridad horizontal : Qué filas puede acceder/manipular cada usuario ?
- Reglas sensibles a columnas
- Fine Grained Access + Application Context



Control de Acceso – Oracle Label Security

- Control de Acceso a nivel de fila utilizando etiquetas o 'labels'
- Seguridad multi-nivel para organizaciones gubernamentales y militares.
- Refuerza la política de 'need-to-know' con base en las etiquetas de los usuarios
- Particiona los datos de acuerdo a las etiquetas

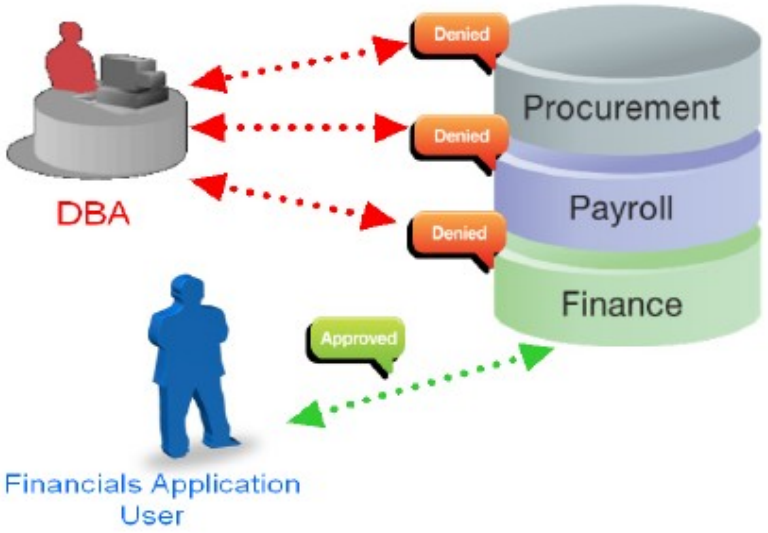


Oracle Label Security- Demostración

- Restricción de acceso a la tabla Locations mediante una etiqueta de Sensibilidad.
- Se requiere dar acceso a los usuarios a los registros de la tabla de acuerdo a su nivel de sensibilidad.
- Niveles: Publico , Confidencial y Sensible
- Usuarios: JPATEL,KPARTNER,PKESTNER

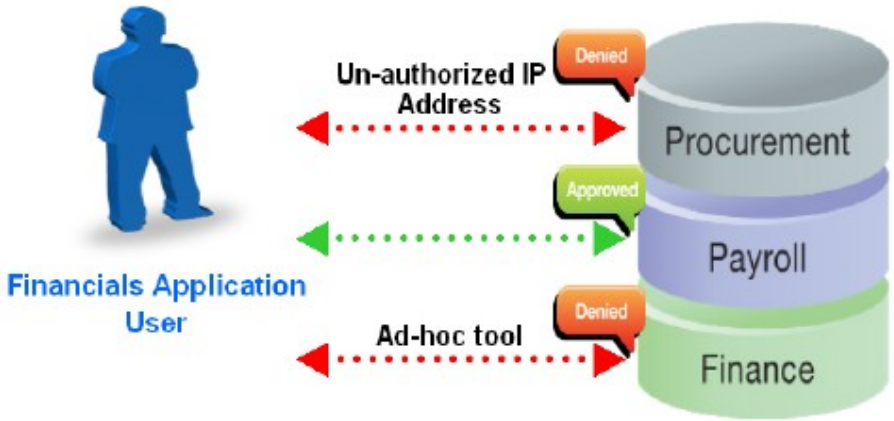
Control de Acceso – Oracle Database Vault

- Controles sobre usuarios Privilegiados
  - Restringe el acceso de usuarios privilegiados, a los datos de su aplicación.
  - Proporciona Separación de Responsabilidades



Control de Acceso – Oracle Database Vault

- Controles de acceso en tiempo real
- Controla quién,cómo, cuándo, dónde y cómo se accede a los datos
- Tome decisiones basadas en dirección IP, tiempo, autorización....



Oracle Database Vault - Regulaciones

Oracle Database Vault (DBV)		
Regulatory Legislation	**Regulation Requirement**	**Does DBV Mitigate This Risk?**
Sarbanes-Oxley Section 302	Unauthorized changes to data	Yes
Sarbanes-Oxley Section 404	Modification to data, Unauthorized access	Yes
Sarbanes-Oxley Section 409	Denial of service, Unauthorized access	Yes
Gramm-Leach-Bliley	Unauthorized access, modification and/or disclosure	Yes
HIPAA 164.306	Unauthorized access to data	Yes
HIPAA 164.312	Unauthorized access to data	Yes
Basel II – Internal Risk Management	Unauthorized access to data	Yes
CFR Part 11	Unauthorized access to data	Yes
Japan Privacy Law	Unauthorized access to data	Yes
PCI – Requirement 7	Restrict access to cardholder data by business need-to-know	Yes
PCI – Requirement 8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed	Yes
PCI – Compensating Controls for Requirement 3.4	Provide ability to restrict access to cardholder data or databases based on the following criteria: • IP address/Mac address • Application/service • User accounts/groups	Yes
PCI - Requirement A.1: Hosting providers protect cardholder data environment	Ensure that each entity only has access to own cardholder data environment	Yes

Oracle Database Vault - Demostración

- Proteccion de los datos de Recursos Humanos , previniendo el acceso al DBA, mediante la definición de un Realm (Dominio de Protección).
- Separación de Responsabilidades entre el DBA de HR y el DBA de OE.
- Crear un Rule set que evite que el usuario HR_DBA_JR

ejecute un TRUNCATE de una tabla excepto cuando se cumplan las siguientes condiciones:

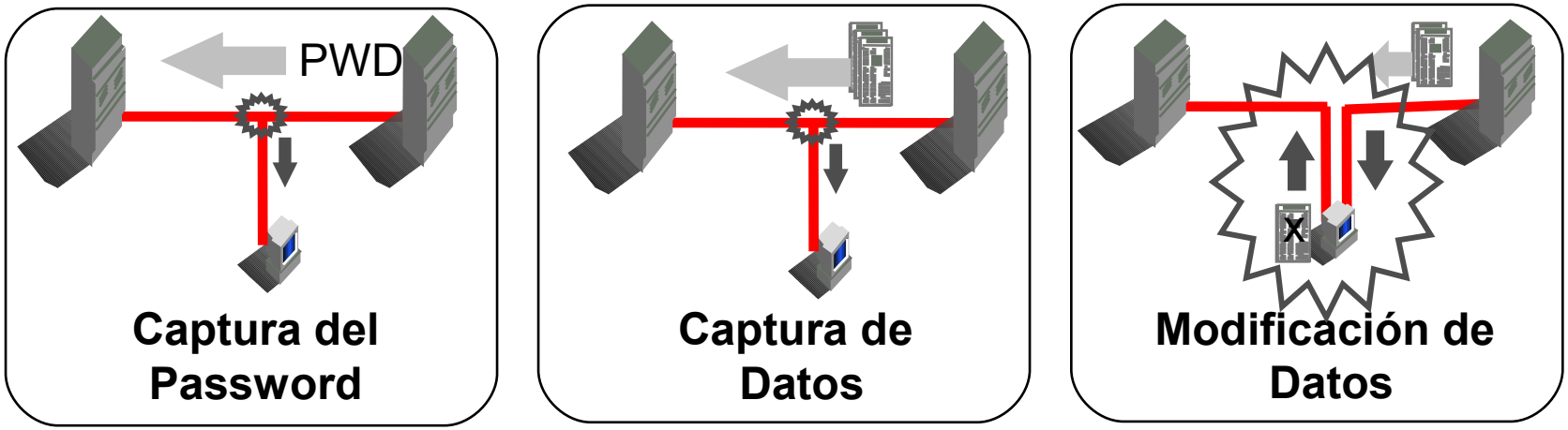
  - La hora y fecha debe ser de 8-5, Lunes a Viernes
  - Debe estar conectado a la base de datos localmente

Protección de Datos – Oracle Advanced Security

- Encripta transparentemente números de tarjeta de crédito, cédulas, y otra información privada.
- Encripta tablas completas.
- Protege los backups de la base de datos con encriptación.
- Encripta transparentemente el tráfico en la red.
- Habilita autenticación fuerte (Kerberos,PKI, RADIUS)
- Criptografía fuerte

Protección de Datos – Oracle Advanced Security

- Garantía de Confidencialidad
- Garantía de Integridad



Para ataques externos, data en tránsito

Oracle Advanced Security - Demostración

- En nuestra compañía ficticia, CashBank Trust, se están evaluando tecnologías de encriptación para su ambiente de base de datos. Ellos requieren satisfacer los requerimientos de PCI, que bajo la sección 3 y 4 establece que ciertos datos estén encriptados en el disco y mientras viajan a través de la red.

Requirement 3: Protect stored cardholder data

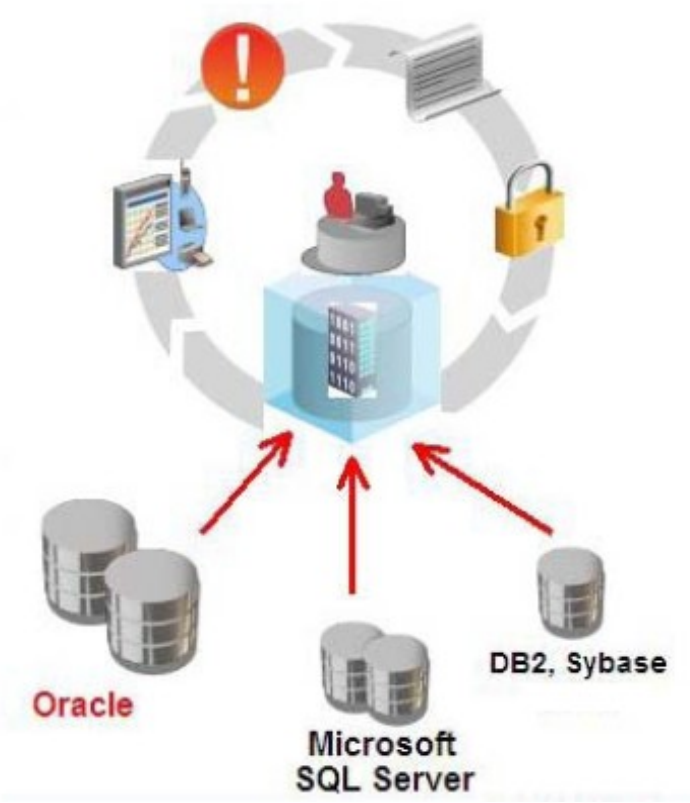
Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.

Monitoreo y Control – Desafíos de la Auditoría

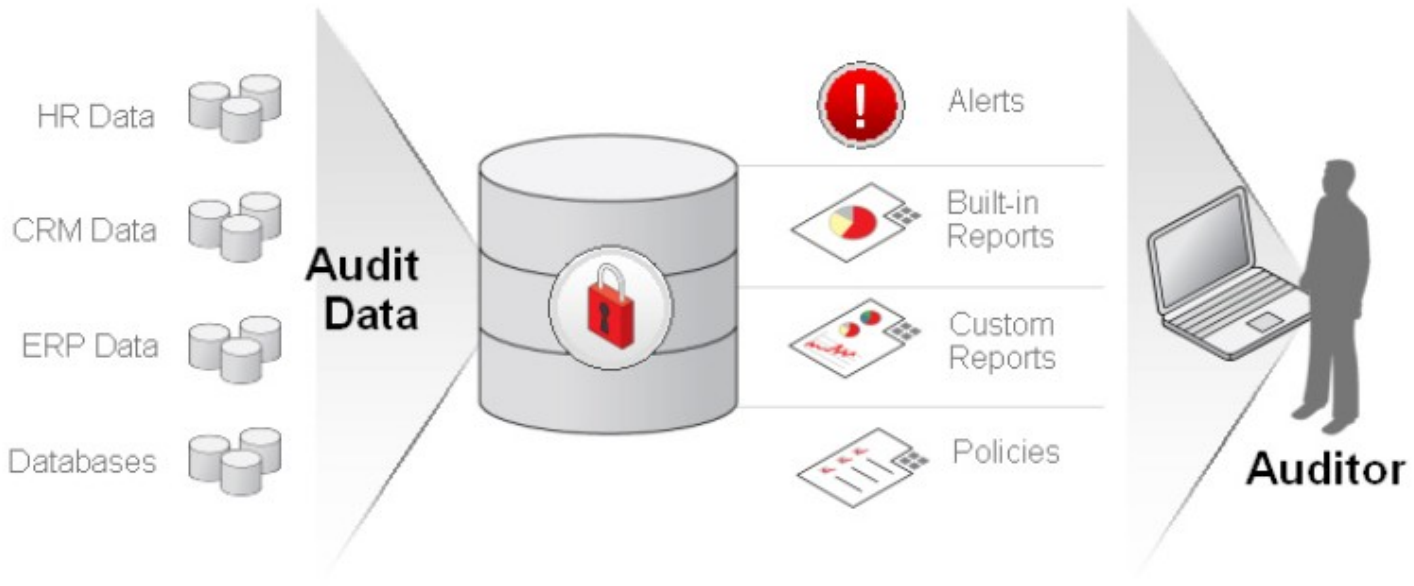
- Qué se debe auditar ?
- Datos modificados:
  - Quien realizó ?
  - Qué realizó ?
- Consulta de datos sensibles:
  - Quién consultó ?
  - Qué tanto consultó ?
- Auditoria x Tecnología
  - Como auditar las actividades de la bd, sin impactar el performance?

Monitoreo y Control – Oracle Audit Vault

- Consolidar los rastros de auditoría , inclusive de bases de datos heterogéneas.
- Construcción de reportes personalizados para monitoreo y control.
- Configuración de alertas de actividad sospechosa.
- Captura de valores antes/después de los logs de las transacciones.
- Administrar políticas de auditoría en las bases de datos Oracle.



Monitoreo y Control – Oracle Audit Vault

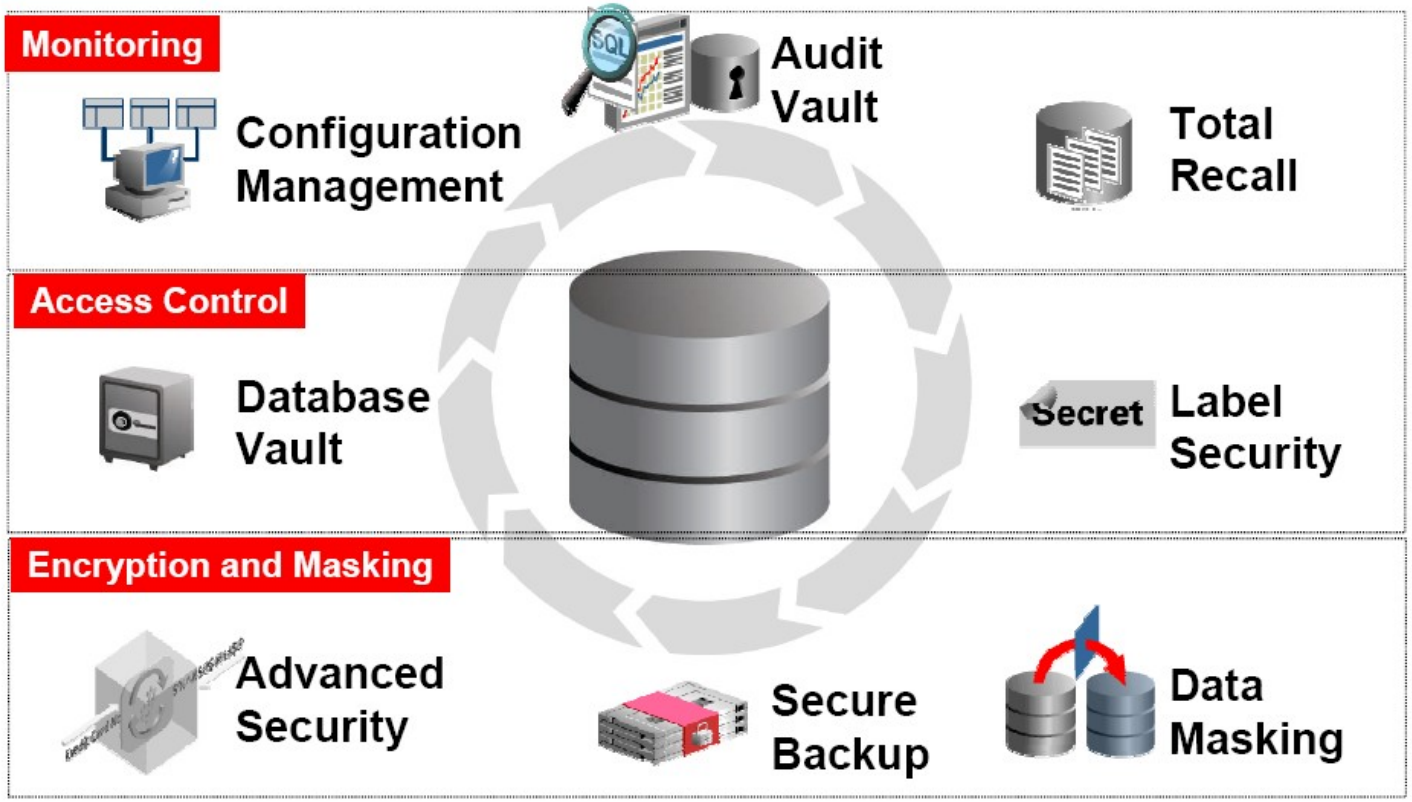


Productos de Seguridad de Oracle

Detección

Prevención

Prevención




Q&A

lina.forero@red-partner.com