

# ORACLE DATABASE VAULT

## KEY BENEFITS



- Protect application data from DBA
- Protect database from powerful application owners
- Control access to the application with flexible security controls
- Protect against database changes
- Enforce separation of duty
- Oracle Database 10g Release 2 Enterprise Edition Security Option



*Oracle Database Vault provides a solution to help customers address the most difficult security problems remaining today - protecting against the insider threat, meeting regulatory compliance requirements and enforcing separation of duty. Oracle Database Vault keeps the DBA from viewing application data, a top concern for customers who must protect sensitive business information or privacy data related to partners, employees and customers. Oracle Database Vault keeps the powerful application DBAs from accessing other applications and from performing tasks outside their authorized responsibilities. Oracle Database Vault can protect existing applications quickly and easily without interfering with the application functionality.*

### What is Oracle Database Vault?

Oracle Database Vault addresses some of the most common security problems and internal threats by:

- Restricting the DBA and other privileged users from accessing application data
- Preventing the Application DBA from manipulating the database and accessing other applications
- Providing better controls over who, when and where an application can be accessed.

In addition, compliance regulations such as the US Sarbanes-Oxley (SOX), US Healthcare Insurance Portability and Accountability Act (HIPAA), Japan Privacy Law, EU Privacy Directive, and the US California Senate Bill 1386 require tighter internal controls to prevent unauthorized disclosure or modification of sensitive information which could lead to identity theft and financial irregularities.

Historically, the Database DBA or Application DBA have had full access to the database including the application data and the data dictionary to simplify the application design, development and rollout. In fact, it is difficult and perhaps impossible to specify additional access control policies based upon the customer environment without significant knowledge of the underlying application design.

Oracle Database Vault introduces several new and powerful security features such as Realms, Factors, and Rules to restrict access inside the database even from users with powerful roles such as the DBA role, or powerful privileges such as "SELECT ANY". These features can be used in a flexible and adaptable manner to enforce security requirements, without changing the existing applications.

### Protect Application Data from DBA and Privileged Users

Authoritative security studies have documented that more than 70% of information system data losses and attacks have been perpetrated by 'insiders' — those authorized with some level of access to the system and its data. Oracle Database Vault can be used to prevent a DBA from viewing application data using their DBA privileges by simply defining a Realm around sensitive schemas and objects.

**ORACLE DATABASE VAULT**

## RELATED PRODUCTS:

The following products provide additional security to help meet security, privacy and regulatory requirements:

- Oracle Database 10g Release 2 - Oracle Label Security
  - Multi-level Security
  - Protect sensitive data
  - Manage User Security Clearances
  - Integrated with Oracle Identity Management
  - Common Criteria Evaluation at EAL4
- Oracle Database 10g Release 2 - Oracle Advanced Security
  - Transparent Data Encryption with no modification to existing application SQL code
  - Strong Authentication
  - Network Encryption
- Oracle Secure Backup
  - Protection for backup data on tape
  - File system support, backup Oracle Home and Applications
  - Integrated with Oracle Recovery Manager (RMAN) and supports up to 256 bit AES
  - EM interface for ease of use

Once a Realm and associated rules are defined, a DBA can continue to perform database management tasks, but they can no longer view or change application data as shown below.

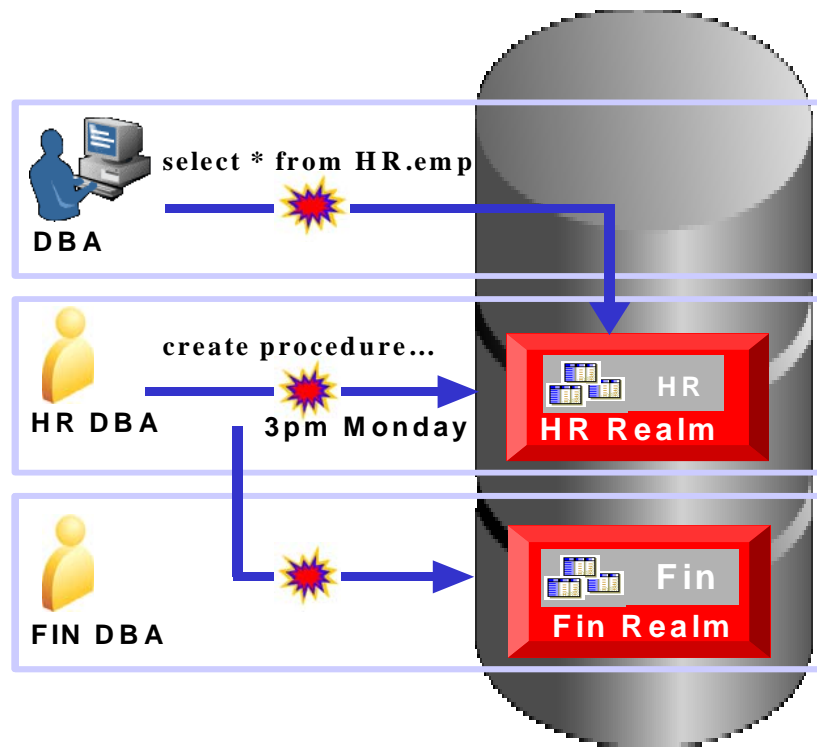


Fig 1. Oracle Database 10g Release 2 with Database Vault Option

**Control Access to Applications**

Oracle Database Vault Rules and Factors can be used to significantly tighten application security by limiting who, when, where and how an application is accessed. These features can be used in a flexible and adaptable manner to enforce authorization requirements, without requiring changes to the existing applications. Factors such as time of day, database client's location on a network, or custom factors specific to the enterprise can be used independently or in combination to implement multi-factor authorization and control the ability to access the application. For example, access to the database could be restricted to a specific middle tier or batch jobs running on the database server. Database Vault multi-factor authorization significantly strengthens security.

**Protect Against Database Changes**

Oracle Database Vault provides powerful separation of duty controls and protects the database from unauthorized changes. Oracle Database Vault will block a DBA with the *CREATE USER* privilege from creating a new user if the DBA doesn't have the proper user administration role. In addition, command rules can be defined for all SQL commands to provide control over the command execution.

**Administrative Interface and Reporting**

Oracle Database Vault provides an administrative user interface and out-of-the-box security related reports that enable the Security administrator to understand security relevant events and protect the database and the applications.