

ORACLE DATABASE VAULT

KEY BENEFITS

ORACLE
DATABASE **11g**

- Prevent access to sensitive application data by highly privileged users
- Control access to the applications, databases and data with flexible security controls
- Enable Separation of duty
- Available for both Oracle Database 10g Release 2, Oracle Database 9i Release 2, and Oracle Database 11g Release 1
- Validated with Oracle PeopleSoft Applications



Oracle Database Vault provides strong internal controls for regulatory compliance and protection against insider threats. Oracle Database Vault not only prevents highly privileged users from viewing sensitive application data, it also enforces policies on who, when, where and how applications, databases and data can be accessed. Oracle Database Vault transparently protects database applications without requiring any changes to the existing application.

Oracle Database Vault

Regulations such as Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI), and the Healthcare Insurance Portability and Accountability Act (HIPAA) require strong internal controls to protect sensitive information such as financial, healthcare and credit cards records from unauthorized access and modification. Oracle Database Vault provides a powerful and easy-to-use security solution inside the Oracle Database, enabling enterprises with new and existing applications to easily comply with these and future regulations. Insider threats are an increasing concern for customers worldwide. The CSI/FBI 2005 Computer Crime and Security study documented that more than 70% of information system data losses and attacks have been perpetrated by insiders, that is, by those authorized at least some level of access to the system and its data.

Complying with regulations and protecting against the insider threats requires two primary enhancements to existing environments:

- Preventive controls to restrict unauthorized access to sensitive data by highly privileged users
- Flexible and adaptable controls over who, when, where and how applications, databases and data can be accessed

Oracle Database Vault Realms, Factors, and Rules (described below) work together inside the database to restrict access from even the most powerful users without interfering with the normal day-to-day database administration. These features can be used in a flexible and adaptable manner to enforce security requirements, without changing the existing applications.

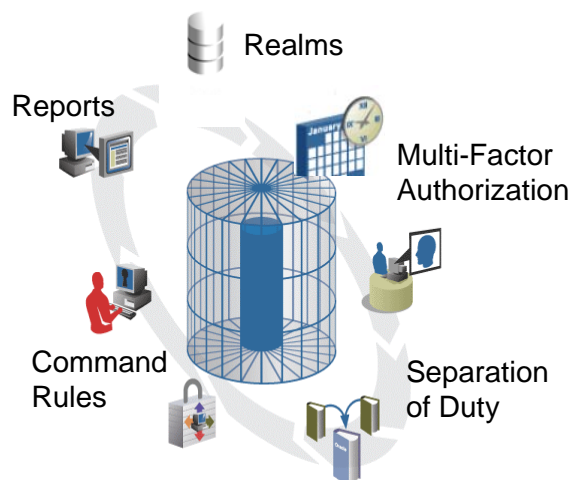


Fig 1. Oracle Database Vault Overview

Oracle Database Vault

RELATED SECURITY PRODUCTS:

- Oracle Audit Vault
 - Transparently consolidate audit data from multiple databases
 - Simplify compliance reporting with built-in reports
 - Detect threats early with alerts
 - Manage audit policies across databases
 - Scale with robust Oracle Database technology
 - Build custom reports against an open warehouse schema
- Oracle Advanced Security
 - Transparent Data Encryption with no modification to application SQL code
 - Supports AES 256
 - Strong Authentication
 - Network Encryption
- Oracle Label Security
 - Label based access control
 - Multi-level Security
 - Protect sensitive data
 - Integrated with Oracle Database Vault through label factors
 - Common Criteria Evaluation at EAL4
- Oracle Secure Backup
 - Encrypt database and file system data during tape backup
 - Integrated with Oracle Recovery Manager (RMAN) and supports up to 256 bit AES

Highly Privileged User Controls

IT administrators, database administrators, and application administrators fill highly trusted positions within the enterprise. However, regulatory compliance, outsourcing, application consolidation and increasing concerns over insider threats have resulted in an almost mandatory requirement for strong controls on access to sensitive application data. Retrofitting existing application code with new access controls can be costly and time consuming, and not an option for many enterprises. With Oracle Database Vault Realms, enterprises can restrict highly privileged users, even the powerful DBA, from accessing application data. Realms are easily defined and can be placed around an entire application or set of tables quickly and easily.

Flexible and Adaptable

Oracle Database Vault Rules and Factors significantly tighten application security by limiting who, when, where and how databases, data and an applications can be accessed. Multiple factors such as IP address and authentication method can be used in a flexible and adaptable manner to enforce authorization requirements, without requiring changes to the existing applications. For example, access to the database could be restricted to a specific middle tier. Command rules can be defined for all SQL commands to provide additional control.

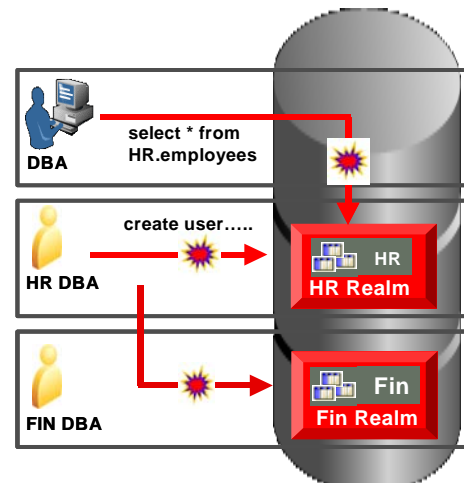


Fig 2. Oracle Database Vault Realms, Rules and Factors

Separation of Duty

Oracle Database Vault provides powerful separation of duty controls and protects the database from unauthorized changes. Oracle Database Vault provides three distinct responsibilities out-of-the-box for security administration, account management, and resource management. For example, Oracle Database Vault blocks a DBA with the *create user* privilege from creating a new user if the DBA doesn't have the proper responsibility. You can further subdivide the resource administration responsibility into backup, performance and patching responsibilities. Optionally, responsibilities can be consolidated.

Application Validation

Oracle has validated Oracle Database Vault with PeopleSoft applications. Easy to use setup scripts and step-by-step instructions can be downloaded from the Oracle Technology Network. Validation with the E-Business Suite and Siebel are currently underway and are expected to complete this calendar year.

Copyright 2007, Oracle. All Rights Reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor is it subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.