

# Oracle Database Vault

*An Oracle White Paper*  
*September 2008*

## **INTRODUCTION**

Strengthening internal controls for regulations, enforcing industry best practices, and guarding against insider threats are just a few of the challenges facing organizations in today's global economy. While problems such as the insider threat are certainly not new, the concern over unauthorized access to sensitive information has never been greater. The cost of data theft from both a financial and public relations standpoint can be significant. At the same time, remaining competitive in a global economy requires the flexibility to deploy IT systems in a cost effective manner while still adhering to industry best practices and regulatory mandates such as PCI, Sarbanes-Oxley and Basel II. Transparent security controls are critical when bringing existing applications and IT operations into compliance with existing and newly emerging regulations as well as industry best practices. Modifying existing application can be a time consuming and costly exercise. As a result, new security products must protect transparently, without modification to existing applications. Oracle Database Vault provides a transparent solution for mitigating the risk of insider threats and complying with regulatory requirements.

## **ORACLE DATABASE VAULT**

Over the past two decades many applications have been developed to perform business critical functions such as financial processing and human resources management. In addition, many custom applications have been developed to address unique business requirements. Historically applications have been designed to deliver massive scalability and high availability. These two issues were the driving force behind many technological advanced, including Oracle Real Application Clusters. Today, however, security has become an equally important part of day-to-day IT operations. Regulations and best practices require that strong controls be put in place to prevent privileged user access to sensitive business data and eliminate ad-hoc access using off-the-shelf reporting tools. Oracle Database Vault addresses these challenges using powerful technology enforced deep within the Oracle Database server. Whether it's traditional client server applications or web based applications, Oracle Database Vault provides flexible, transparent and highly adaptable security controls that require no application changes. Privileged users can be prevented from access application data and separation-of-duty can be enforced across existing database administrators without a costly and time

consuming least privilege exercise. Oracle Database Vault uses a number of technical real time access controls to achieve these protections.

- Realms - Prevent highly privileged users from accessing application data
- Multi-Factor Authorization – Create trusted paths to data, defining who, when, where and how applications, data and databases are accessed
- Command Rules- Enforce operational policies based on IT Security and internal or external auditor recommendations
- Separation of Duty - Control administrative actions within the database to prevent actions that may violate regulations and best practices
- Reports - Run security related reports on attempted realm violations and other Database Vault enforcement controls

Regulations such as Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Basel II, and PCI have common themes that include internal controls, separation of duty and strong access controls to sensitive information. While many requirements found in regulations such as SOX and HIPAA are procedural in nature, technical solutions are required to mitigate the risks associated with items such as unauthorized modification of data and unauthorized access.

<b>Oracle Database Vault (DBV) and Regulations</b>		
<b>Regulation</b>	<b>Requirement</b>	<b>Does DBV Mitigate This Risk?</b>
<b>Sarbanes-Oxley Section 302</b>	Unauthorized changes to data	<b>Yes</b>
<b>Sarbanes-Oxley Section 404</b>	Modification to data, Unauthorized access	<b>Yes</b>
<b>Sarbanes-Oxley Section 409</b>	Denial of service, Unauthorized access	<b>Yes</b>
<b>Gramm-Leach-Bliley</b>	Unauthorized access, modification and/or disclosure	<b>Yes</b>
<b>HIPAA 164.306</b>	Unauthorized access to data	<b>Yes</b>
<b>HIPAA 164.312</b>	Unauthorized access to data	<b>Yes</b>
<b>Basel II – Internal Risk Management</b>	Unauthorized access to data	<b>Yes</b>
<b>CFR Part 11</b>	Unauthorized access to data	<b>Yes</b>
<b>Japan Privacy Law</b>	Unauthorized access to data	<b>Yes</b>
<b>PCI – Requirement 7</b>	Restrict access to cardholder data by business need-to-know	<b>Yes</b>
<b>PCI – Requirement 8.5.6</b>	Enable accounts used by vendors for remote maintenance only during the time period needed	<b>Yes</b>
<b>PCI – Compensating Controls for Requirement 3.4</b>	Provide ability to restrict access to cardholder data or databases based on the following criteria:	<b>Yes</b>

	<ul style="list-style-type: none"> <li>• IP address/Mac address</li> <li>• Application/service</li> <li>• User accounts/groups</li> </ul>	
<b>PCI - Requirement A.1: Hosting providers protect cardholder data environment</b>	Ensure that each entity only has access to own cardholder data environment	<b>Yes</b>

**Table 1. Oracle Database Vault and Regulations Overview**

## ORACLE DATABASE VAULT REALMS

Database administrators and other privileged users play a critical role in maintaining the database. Backup and recovery, performance tuning, and high availability are all part of the DBA job description. However, the ability to prevent privileged users within the database from viewing sensitive application data has become an increasingly important requirement. In addition, application consolidation requires strong boundaries between sensitive business data such as that found in financial and human resource applications.

Oracle Database Vault realms prevent DBAs, application owners, and other privileged users from viewing application data using their powerful privileges. Database Vault realms put in place preventive controls, helping reduce the potential impact when a data breach does occur, and enabling the DBA to perform his or her job more effectively. Oracle Database Vault realms can be used to protect an entire application or a specific set of tables within an application, providing highly flexible and adaptable security enforcement.

## ORACLE DATABASE VAULT COMMAND RULES AND FACTORS

The proliferation of regulations and privacy laws around the globe requires flexible and highly adaptable security policies that can be easily modified to meet existing and newly emerging access control requirements. In addition, right sourcing and on-demand application environments introduce additional access control requirements. Oracle Database Vault introduces powerful capabilities that are uniquely suited to address these and future access control requirements.

Oracle Database Vault command rules enable multi-factor authorization controls that extend beyond the traditional database roles. Using command rules and multi-factor authorization, access to databases can be restricted to a specific subnet or application server, creating a virtual *trusted path* for data access. Limiting data access to approved applications can be achieved using Oracle Database Vault factors in combination with Oracle Database Vault command rules. Oracle Database Vault provides a number of built-in factors, such as IP address, that can be used individually or together in combination with other security rules to significantly raise the level of security for an existing application. In addition to the built-in Factors provided by Database Vault, you can add your own custom factors to meet your own business requirements.

Oracle Database Vault command rules provide the ability to easily attach security policies to virtually any database operation. Command rules allow you to strengthen internal controls and enforce industry best practices and secure configuration policies. Command rules can be used to enforce strong protections on critical business data. For example, a command rule can be used to prevent any user, even the DBA, from dropping application tables in your production environment. Command rules can be easily managed through the Database Vault GUI or on the command line using the API.

## ORACLE DATABASE VAULT SEPARATION OF DUTY

Oracle Database Vault separation of duty enables a systematic approach to security that strengthens internal controls within the database. Out-of-the-box, Oracle Database Vault creates three distinct responsibilities within the database.

Responsibility	Description
Account Management	A user with the account management responsibility can create, drop, or modify database users. Existing highly privileged users will be prevented from performing account management activities.
Security Administrator	The security administration responsibility is designed to enable a user to become a security administrator (Database Vault Owner) of the database. A security administrator can setup Database Vault Realms, Command Rules, authorize other users to use them, and execute various Database Vault specific security reports. The security administrator is prevented from self-authorizing access to secured business data.
Database Administration	The database administration responsibility enables a user with the DBA privileges to continue performing normal management and maintenance associated with the database such as backup and recovery, patching, and performance tuning.

**Table 2. Oracle Database Vault Separation of Duty**

Oracle Database Vault extensibility allows separation of duty to be customized to your specific business requirements. For example, you can further subdivide the database administration responsibility into backup, performance and patching responsibilities. If you have a small company you can consolidate responsibilities, or assign different named login accounts for each responsibility, enabling more granular accountability and auditing.

Oracle Database Vault provides numerous out-of-the-box reports that give you the ability to report on such things as attempted data access requests blocked by realms. For example, if a DBA attempts to access data from an application table protected by a realm, Database Vault will create an audit record in a specially protected table inside the Database Vault. Oracle Database Vault includes a realm violation report that makes it easy to view these audit records.

### **ORACLE DATABASE VAULT AND APPLICATIONS**

As part of Oracle's commitment to helping customers comply with regulations and insider threat concerns, Oracle Database Vault has been certified with numerous applications. The certification process includes out-of-the-box security policies including realm and command rule definitions that work with each of the applications.

<b>APPLICATION</b>	<b>CERTIFICATION AND OUT-OF-THE-BOX POLICIES</b>
ORACLE E-BUSINESS SUITE 11/R12	DONE
PEOPLESOFT APPLICATIONS	DONE
SIEBEL	DONE
I-FLEX CUBE	DONE
ORACLE CONTENT DB	DONE
ORACLE INTERNET DIRECTORY	DONE

**Table 3. Oracle Database Vault and Applications**

## CUSTOMER CASE STUDY

Virtually all industries can benefit from Oracle Database Vault. Whether it's sensitive intellectual property, personally identifiable information, credit card information, or financial results, sensitive data needs strong protection against increasingly sophisticated threats.

<b>Financial Services Customer</b>	
<b>Customer Requirement</b>	<b>Oracle Database Vault Solution</b>
Restrict privileged user access to sensitive data.	Defined a Realm around his application data and authorized only the application owner to access the data, preventing highly privileged users, such as the DBA, from accessing application data.
Enforce application access through middle tier processes and from the middle tier servers.	Defined command rules to restrict access to the database to specific middle tier applications on specific servers
Protect database structures from intentional or accidental harmful changes.	Defined additional command rules to protect from dangerous operations such dropping or wiping out business data structures accidentally or intentionally.
Enforce patching and backup to specific maintenance periods and monitor the patching process.	Defined command rules to enforce maintenance periods, thus restricting database maintenance DBA's login to specific days and times. Additionally, the customer used multi-factor authorization to enforce a two person rules during maintenance periods.

**Table 4. Oracle Database Vault Case Study**

## **CONCLUSION**

Oracle Database Vault is the industry's leading database security solution for addressing regulatory requirements and reducing the risk of insider threats. Oracle Database Vault helps address access control requirements associated with regulations such as PCI and Sarbanes-Oxley and is available for Oracle9i Release 2 databases and higher. Oracle Database Vault has been certified with Oracle E-Business Suite, PeopleSoft, Siebel, and I-Flex Cube. Validation with additional applications, including JD Edwards and SAP are currently underway. Using Oracle Database Vault, privileged database users can be prevented from accessing application data. In addition, access to applications, databases and data can be tightly controlled based on such variables as time of day, IP address or subnet. In summary, Oracle Database Vault provides the flexible, transparent and highly adaptable security controls required in today's global economy.

Oracle Database Vault

September 2008

Author:

Contributing Authors:

Oracle Corporation

World Headquarters

500 Oracle Parkway

Redwood Shores, CA 94065

U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

[oracle.com](http://oracle.com)

Copyright © 2008, 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 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.