Oracle Database Vault

An Oracle White Paper
June 2007

ORACLE

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 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. Insider security breaches can be much more costly than attacks from outside the enterprise. 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.

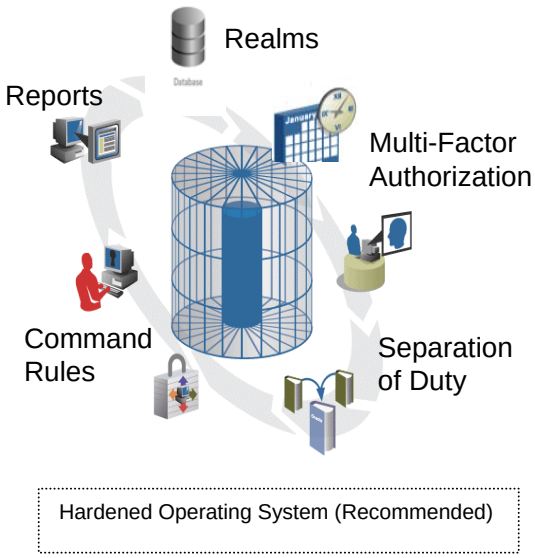
Transparent security controls are critical when bringing existing applications and IT operations into compliance with existing and newly emerging regulations as well as industry best practices. Modifying existing application can be a time consuming and costly exercise. As a result, new security products must protect transparently, without modification to existing applications.

ORACLE DATABASE VAULT

Controlling access to databases, applications and data requires sophisticated access controls that are enforced from within the database. Oracle Database Vault is the industry's leading solution for protecting business data. Whether it's traditional client server applications or web based applications, Oracle Database Vault provides flexible, transparent and highly adaptable security controls with no application changes. Oracle Database Vault recently won the 2007 Global Excellence in Database Security Award from the Info Security Products Guide.

Over the past several decades, thousands of applications have been developed. Some of these applications have broad usage such as HR or financial processing, while others are custom applications, designed to address an industry specific business problem. Today, the highly privileged user can be found in many application environments. Today, regulations and best practices require that strong controls be put in place to address highly privileged users and prevent access to data using off the shelf reporting tools. Oracle Database Vault is designed to

address these challenges using highly privileged user controls and custom security policies. Oracle Database Vault has been backported to Oracle Database 9i Release 2, enabling customers that have not yet upgraded to Oracle Database 10g to leverage Oracle Database Vault. In addition, Oracle Database Vault was recently validated with the Oracle PeopleSoft Applications.



Highly Privileged User Controls

Realms
- **Prevent highly privileged users from accessing application data**

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 Realms and other Database Vault enforcements**

Flexible and Adaptable Custom Security Policies

Multi-Factor Authorization
- **Created 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**

Figure 1. Oracle Database Vault Overview

Oracle Database Vault and Regulations

Oracle Database Vault realms, separation of duty, command rules and factors are applicable to reducing the overall risk associated with specific provisions of regulations worldwide. Regulations such as Sarbanes-Oxley (SOX), Healthcare Insurance Portability and Accountability Act (HIPAA), Basel II, and PCI have common themes that include internal controls, separation of duty and strong access controls on access 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.

Oracle Database Vault (DBV) and Regulations		
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**

Table 1. Oracle Database Vault and Regulations Overview

Highly Privileged User Controls

Database administrators and other highly privileged users play a critical role in maintaining the database. Backup and recovery, performance turning, and high availability are all part of the DBA job description. However, the ability to prevent highly 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

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 causes when a data breach does occur, 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 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 others 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.
Resource Administration	The resource administration responsibility enables a user with the DBA privileges to continue performing normal management and maintenance associated with the database such 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 resource administration responsibility into backup, performance and patching responsibilities. If you have a small company you can consolidate responsibilities, or assign different 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.

Flexible and Extensible Access Controls

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. Further complicating access control requirements are issues such as out-sourcing and hosted or on-demand based applications. Oracle Database Vault introduces powerful capabilities that are uniquely suited to address these and future access control requirements.

Oracle Database Vault Multi-Factor Authorization

Oracle Database Vault Multi-Factor Authorization extends access controls beyond the traditional role based and even more sophisticated label based access control found in the Oracle Database. Using 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 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

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 AND APPLICATIONS

As part of Oracle's commitment to helping customers comply with regulations and address insider threat concerns, Oracle has validated Oracle Database Vault with PeopleSoft Applications. Oracle has created an easy to use guide that shows how Oracle Database Vault can be used in a PeopleSoft Application environment to prevent highly privileged users from accessing application data. The guide also includes additional examples on how multi-factor authorization and command rules can be used to enforce more sophisticated policies. 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. Oracle is also working with 3rd party application providers. Oracle Partners can validate their application with Oracle Database Vault and receive free technical assistance from the Oracle Partner Technical Services.

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.

Financial Services Customer	
Customer Requirement	**Oracle Database Vault Solution**
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 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.
Enforce patching and backup to specific maintenance periods and monitor the patching process.	Defined additional command rules to protect from dangerous operations such dropping or wiping out business data structures accidentally or intentionally.

Table 3. Oracle Database Vault Case Study

CONCLUSION

Oracle Database Vault is the industry's leading database security solution for addressing regulatory compliance and concerns over the insider threat. Oracle Database Vault helps address access control requirements associated with regulations such as PCI and Sarbanes-Oxley. In addition, Oracle Database Vault has been back ported to Oracle Database 9i Release 2 and validated with Oracle PeopleSoft Applications, enabling customers to take advantage of Oracle Database Vault without upgrading to Oracle Database 10g. Validation with additional applications will take place during this calendar year. Using Oracle Database Vault, highly 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
June 2007
Author: Kamal Tbeileh, Paul Needham
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