An Oracle White Paper
September 2009

Oracle Database Vault with Oracle Database 11g Release 2

ORACLE

Introduction

Regulatory compliance, industrial espionage and insider threats are just few of the challenges facing organizations in today's global economy. At the same time, remaining competitive requires the flexibility to deploy IT systems in a cost effective manner through consolidation and off shoring. While problems such as insider threats 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 compliance with regulations such as Sarbanes-Oxley (SOX), European Union Data Protection Directive, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and numerous breach disclosure laws requires strong controls on access to sensitive data. Oracle Database Vault provides a powerful and transparent security solution that helps organizations comply with regulations, deploy systems in a cost efficient manner, and prevent unauthorized access to sensitive data.

Oracle Database Vault

Historically performance and high availability have been two of the key drivers behind IT decision making. Over the past decade, however, security has become a critical component in that list. Oracle Database Vault is a security option for the Oracle Database and provides flexible and highly adaptable security controls that can be transparently applied to existing application environments. Oracle Database Vault security controls include realms, command rules, factors, separation of duty, and reporting. Together these controls transparently increase security around existing applications without requiring changes to the application code. Realms act like a firewall inside the Oracle database enabling preventive controls on privileged user access to application data. Command rules and factors provide controls over who, when, where and how databases,

data and applications are accessed. Command rules can use factors such as IP address, authentication method, and program name to enforce rules on common database commands, thereby strengthening security around existing applications. Oracle Database Vault separation of duty controls enforce a least privilege model on existing databases, separating account management from traditional database administration activities and Oracle Database Vault security administration.

TABLE 1. ORACLE DATABASE VAULT FEATURES

FEATURE	DESCRIPTION
Realms	Boundaries within the Oracle database that act like a firewall to prevent privileged users from using their special privileges to access application data
Command Rules	Security rules that control the execution of database commands
Factors	Environmental parameters (IP address, Authentication method) that can be used with Database Vault command rules and realms to create trusted paths to data, defining who, when, where and how applications, data and databases are accessed
Separation-of-Duty	Out-of-the-box least privilege controls within the database that separate out key administrative actions (account management, security administration, and database administration)
Reports	Out-of-the-box security related reports that provide details on attempted realm violations and other Database Vault enforcement controls

Oracle Database Vault is available for Oracle9i Database Release 2, Oracle Database 10g Release 2 and Oracle Database 11g.

Oracle Database Vault and Regulations

Many regulations have common themes that require strong and demonstrable controls on access to sensitive data as well as separation of duty. While many regulatory requirements are procedural in nature, technical solutions are required to mitigate the risks associated with items such as unauthorized access and modification of data.

TABLE 2. ORACLE DATABASE VAULT AND REGULATIONS (SAMPLE LIST)

REGULATION	REQUIREMENT	IS DATABASE VAULT APPLICABLE?
Sarbanes-Oxley Section 302	Prevent unauthorized changes to data	Yes
Sarbanes-Oxley Section 404	Prevent modification to data and unauthorized access	Yes
Sarbanes-Oxley Section 409	Prevent denial of service and unauthorized access	Yes
Gramm-Leach-Bliley	Prevent unauthorized access and unauthorized modification	Yes
HIPAA 164.306, 164.312	Prevent unauthorized access to data	Yes
Basel II – Internal Risk Management	Prevent unauthorized access to data	Yes
CFR Part 11 (FDA)	Prevent unauthorized access to data	Yes
Japan Privacy Law	Prevent 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 Realms

Database administrators and other privileged users play a critical role in maintaining the database. Backup and recovery, performance turning, and high availability are just a few of the day-to-day tasks that privileged users perform. However, the ability to prevent privileged database users from viewing sensitive application data has become increasingly important. Application consolidation and right sourcing / off shoring require strong controls on access to sensitive data found in financial, human resource, healthcare, retail applications, and other applications.

Oracle Database Vault realms prevent privileged users from viewing application data using their powerful privileges. 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

Oracle Database Vault command rules enable multi-factor authorization controls that extend beyond 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 trusted path for data access. 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 factors to significantly raise the level of security for an existing application. In addition, custom factors can be defined to meet your own business requirements.

Oracle Database Vault command rules provide the ability to easily attach security policies to commonly used database commands. 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 or the application owner, from dropping application tables in your production environment. Command rules can be easily managed through the Oracle Database Vault administrative console or using the Oracle Database Vault command line interface.

Oracle Database Vault Separation-of-Duty

Oracle Database Vault separation of duty enables a systematic approach to security that strengthens controls within the database and helps satisfy requirements found in many regulations. Out-of-the-box, Oracle Database Vault creates three distinct separate responsibilities within the database.

TABLE 3. ORACLE DATABASE VAULT SEPARATION OF DUTY

RESPONSIBILITY	DESCRIPTION
Account Management	A user with the account management responsibility can create, drop, or modify database users. Existing privileged users will be prevented from performing account management activities.
Security Administration	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 manage realms, command rules, factors, and run 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 without having access to secured business data.

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 Reports

Oracle Database Vault provides numerous out-of-the-box reports that give you the ability to report on such things as data access attempts blocked by realms. For example, if a DBA attempts to access data in an application table protected by a realm, Oracle Database Vault will prevent that access and create an audit record that can be easily viewed using the realm violation report.

Oracle Database Vault Manageability

Oracle Database Vault provides an administrative console for managing realms, command rules and rule sets. The Oracle Database vault reports can also be viewed through the console. For enterprise wide management, Oracle Database Vault has been integrated with Oracle Enterprise Manager Grid Control. Oracle Enterprise Manager Grid Control provides the ability to monitor Oracle Database Vault and clone Oracle Database Vault security settings between databases. For example, the Oracle Database Vault realm and command rule definitions can be easily replicated from a central pre-configured and tested Oracle Database Vault enabled database to another Oracle Database Vault enabled database without any coding.

Oracle Database Vault and Applications

Oracle Database Vault has been certified with numerous Oracle applications as well as partner applications. The certification includes out-of-the-box security policies specific for each application. It includes definitions for realms and command rules that work with each of the applications.

TABLE 4. ORACLE DATABASE VAULT CERTIFICATION WITH APPLICATIONS

APPLICATION	CERTIFIED	APPLICATION-SPECIFIC PROTECTION POLICIES AVAILABLE?
Oracle E-Business Suite (releases 11iand 12)	Yes	Yes
Oracle PeopleSoft	Yes	Yes
Oracle JD Edwards EnterpriseOne	Yes	Yes
Oracle Siebel	Yes	Yes
Oracle Internet Directory	Yes	Yes
SAP	Yes	Yes

Customer Case Study

Whether it is controlling access to intellectual property, personally identifiable information, credit card information, or financial data, virtually all industries can benefit from Oracle Database Vault. Oracle Database Vault provides powerful preventive controls to help organizations comply with regulations and to protect against increasingly sophisticated threats.

TABLE 4. CUSTOMER CASE STUDY

CUSTOMER REQUIREMENT	ORACLE DATABASE VAULT SOLUTION
Restrict privileged user access to sensitive data.	Defined a Realm around the customer application data and authorized only the application owner to access the data, thus preventing privileged users, such as DBAs, 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 running on specific servers
Protect database structures from intentional or accidental harmful changes.	Defined additional command rules to protect from dangerous operations such dropping or deleting 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 logins to specific days and times. Additionally, the customer used multi-factor authorization to enforce a two person rule during maintenance periods.

Satisfying these requirements allowed the customer to out-source backend operations while still protecting sensitive data and complying with regulations.

Conclusion

Oracle Database Vault is the industry's leading access control solution for addressing regulatory requirements and reducing the risk of insider threats. Oracle Database Vault transparent security controls address common requirements found in regulations such as SOX, HIPAA and PCI-DSS. Oracle Database Vault is available for Oracle9i Release 2, Oracle 10g Release 2, and Oracle Database 11g. Oracle Database Vault has been certified with Oracle E-Business Suite, Oracle PeopleSoft, Oracle Siebel, Oracle JD Edwards EnterpriseOne, and SAP applications. Using Oracle Database Vault, preventive controls can be easily and transparently applied to existing applications to help comply with regulatory requirements, reduce the risk of unauthorized access to data, and enable cost saving strategies such as data consolidation and out sourcing.

Oracle Database Vault with
Oracle Database 11g Release 2
September 2009
Author: Kamal Tbeileh
Contributing Authors: Paul Needham

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

Oracle is committed to developing practices and products that help protect the environment

0109