

Transparent Solutions for Privacy and Compliance with Oracle Database 11g

*An Oracle White Paper
September 2008*

Transparent Solutions for Privacy and Compliance with Oracle Database 11g

INTRODUCTION

Over the past decade numerous regulations have emerged that mandate strong internal controls and protection of personally identifiable information (PII). Examples of such regulations include Sarbanes-Oxley (SOX), PCI, HIPAA, Financial Instruments and Exchange Law, Basel II and the EU Directive on Privacy and Electronic Communications in Europe. The continued emergence of new regulations worldwide combined with the increasingly sophisticated nature of information theft requires strong data security.



AMERICAS

- Sarbanes-Oxley (SOX)
- Healthcare Insurance Portability and Accountability Act (HIPAA)
- CA SB 1386 and other State Privacy Laws
- Payment Card Industry Data Security Act
- FDA CFR 21 Part 11
- FISMA (Federal Info Security Mgmt Act)

EMEA

- EU Privacy Directives
- UK Companies Act of 2006

APAC

- Financial Instruments and Exchange Law (J-SOX)
- CLERP 9: Audit Reform and Corporate Disclosure Act (Australia)

GLOBAL

- International Accounting Standards
- Basel II (Global Banking)
- OECD Guidelines on Corporate Governance

Table 1 - Compliance & Privacy Challenges

While the Internet accelerated the development of new applications for all aspects of business processing, regulations now require much stronger controls on sensitive financial and privacy related information. Transparent security solutions are necessary to deploy stronger controls because most applications rely on application level security to restrict access to sensitive data. Security concepts such as *least privilege* and *need-to-know* were considered less important than scalability and high availability. Oracle Database Security products compliment application level

security, enabling organizations to minimize the costs associated with regulatory compliance and the deployment of strong internal controls.

ORACLE DATABASE 11G DEFENSE-IN-DEPTH

Oracle Database 11g provides comprehensive defense-in-depth security protections. Oracle Database security includes data encryption and masking, strong access controls, centralized user and role management, high fidelity auditing and reporting, enterprise configuration scanning, and data change forensics.

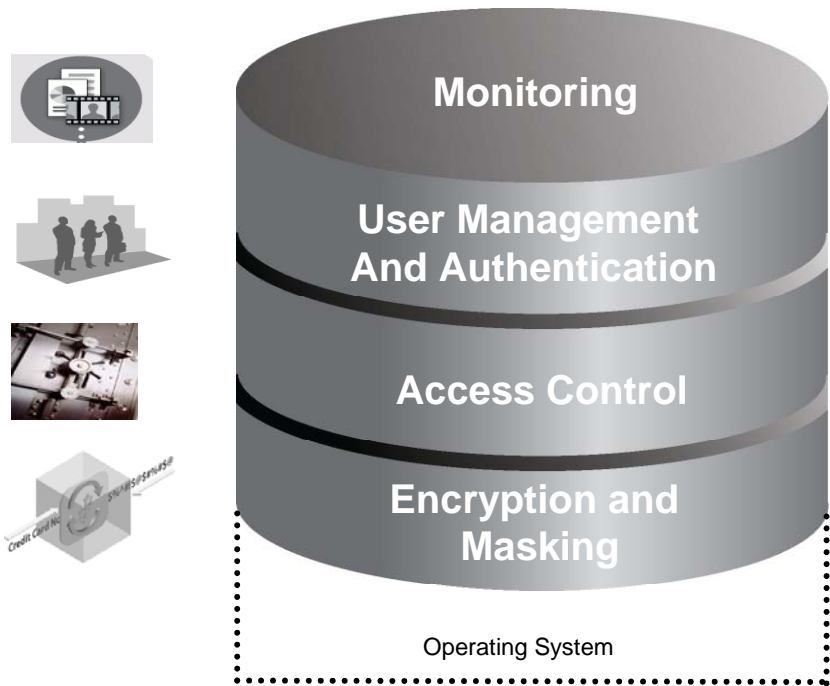


Table 2 – Oracle Database 11g Defense-in-Depth

ORACLE DATABASE 11G ENCRYPTION AND MASKING

Encryption is one of the oldest security technologies in the market place. However, in the last 5 years the need for encryption has increased due to issues such as identity theft and lost media. Theft of social security numbers, credit card numbers, and intellectual property is a serious issue and the need to protect privacy related information spans from higher education to retail to virtually every business around the globe. While the Oracle database provides the industry's strongest protections for data inside the database. Once data leave the database on disk, tape or across the network, the only solution is encryption.

Oracle Advanced Security

Oracle Advanced Security helps customers address regulatory compliance requirements by protecting sensitive data from unauthorized media access, lost,

misplaced or stolen backup media, and network sniffing. Oracle Advanced Security Transparent Data Encryption provides the industry's most advanced encryption capabilities for protecting sensitive information.

Transparent Data Encryption

Unlike most database encryption solutions, TDE is completely transparent to existing applications with no triggers, views, or other application changes required. TDE provides robust encryption to safeguard sensitive data against unauthorized access at the operating system level or through theft of hardware or backup media. TDE helps address privacy and PCI requirements by protecting personally identifiable information such as social security numbers and credit card numbers. Data is transparently encrypted when written to disk and transparently decrypted after an application user has successfully authenticated, and passed all authorization checks. Authorization checks include verifying the user has the necessary *select* and *update* privileges on the application table and checking Database Vault, Label Security and Virtual Private Database enforcement policies. Existing database backup routines will continue to work, with the data remaining encrypted in the backup. For encryption of entire database backups, TDE can be used in combination with Oracle RMAN.

Oracle Database 11g TDE provides exciting new support for complete tablespace encryption. When a tablespace is created through Enterprise Manager or on the command line, an option now exists to specify that the entire data file be encrypted on the file system. When new tables are created in the new tablespace all of the associated data will be transparently encrypted. When the database reads data blocks from the encrypted tablespace it will transparently decrypt the data blocks with single digit minimal performance overhead.

Hardware Security Modules

TDE has been enhanced in Oracle Database 11g to support storing the TDE master encryption key externally on a hardware security module (HSM) device. This provides an even higher level of assurance for protecting the TDE master key. Oracle Database 11g communicates with the HSM device using the PKCS#11 interface. The existing wallet based storage mechanism for the master key will continue to be supported.

Strong Protection For Data In Transit

Oracle Advanced Security provides an easy-to-deploy and comprehensive solution for protecting all communication to and from the Oracle Database, providing both native network encryption and SSL based encryption. SSL based encryption and authentication is available for businesses that have deployed Public Key Infrastructure. Support for the TLS 1.0 protocol (including AES cipher suites) was introduced with Oracle Database 10g. The Oracle Database can be configured to reject connections from clients with encryption turned off, or optionally allow unencrypted connections for deployment flexibility. Configuration of network

security is simplified using the Oracle Network Configuration administration tool, allowing businesses to easily deploy network encryption, as there are no changes required in the application.

Oracle Advanced Security and applications

As part of Oracle’s commitment to helping customers comply with regulations and insider threat concerns, Oracle Advanced Security Transparent Data Encryption has been certified with numerous applications.

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

Table 3 – Oracle Advanced Security and Applications

Oracle Data Masking

Oracle Data Masking pack for Enterprise Manager, part of Oracle's comprehensive portfolio of database security solutions and helps organizations comply with data privacy and protection mandates such as Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPAA), as well as numerous laws that restrict the use of actual customer data. With Oracle Data Masking, sensitive information such as credit card or social security numbers can be replaced with realistic values, allowing production data to be safely used for development, testing, or sharing with out-source or off-shore partners for other non-production purposes. Oracle Data Masking uses a library of templates and format rules, consistently transforming data in order to maintain referential integrity for applications.

The benefits of Oracle Data Masking include:

- Using production data freely in non-production environments without violating data privacy regulations or risking sensitive data leaks.
- Security administrators define the masking rules once, which are then automatically applied every time the database administrator masks the database.
- De-identifying sensitive data is increasingly being called out as critical technology in data privacy protection laws globally.

ORACLE DATABASE 11G ACCESS CONTROL

The Oracle database provides the industry's most advanced access controls. Over the past 30 years Oracle has introduced powerful access control features such as Virtual Private Database and Oracle Label Security. Complying with the stringent internal control requirements found in regulations requires controlling access to databases, applications, and data from within the database, complimenting existing enforcement at the application level.

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.

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 4 – 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.

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

Table 5 – Oracle Database Vault and Applications

Oracle Label Security

Oracle Label Security (OLS) is the industry's most advanced label based access control (LBAC) product. Available for Oracle9i and higher databases, OLS is used within government organizations for protecting classified information and enforcing multi-level security requirements. Within commercial organizations OLS is used for a wide range of business requirements ranging from data consolidation to hosting to controlling access to regulatory data and enforcing need-to-know.

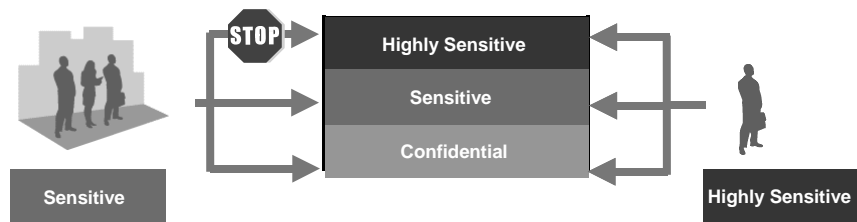


Table 6 – Oracle Label Security Access Mediation

Data labels are comprised of multiple components including a hierarchical level, one or more optional compartments and one or more optional groups. Policy based administration provides a highly flexible and adaptable model enabling OLS to be applied to a wide variety of use cases. Table 5 shows three example OLS

policies with unique data label components. Integration with Oracle Identity Management provides enterprise wide management of user labels across multiple databases.

Used in combination with Oracle Database Vault, user labels become powerful factors for use in multi-factor authorization, helping address regulatory compliance requirements. For example, user label authorizations can be used in Oracle Database Vault command rules to control access to the database, SQL commands, and application tables. This powerful capability extends Label Security concepts beyond traditional row level access controls to mediation at the database and application levels.

Label Industry	Levels	Compartments	Groups
Human Resources	Confidential Sensitive Highly Sensitive	Privacy Data Investigation	HR Rep Senior HR Rep
Law Enforcement	Level 1 Level 2 Level 3	Internal Affairs Gang Task Force	Local Jurisdiction FBI Justice Department
Government and Defense	Confidential Secret Top Secret	Desert Storm Border Protection	NATO Homeland Security

Table 7 – Example OLS Policies and Label Components

Oracle Database 11g User Management

Efficient provisioning and de-provisioning of database users is an important part of the overall enterprise security architecture. Oracle Database enterprise user security allows administrators to manage database users in Oracle Identity Management or their existing corporate directory using Oracle Virtual Directory. Enterprise user security enables thousands of users to be centrally managed in an existing corporate directory. Users can individually authenticate using a password, Kerberos or PKI credential and share a single database account, thus simplifying user management and increasing security. For example, a single database account called '*Org A*' could be defined in the Oracle database and users in *Business Unit A* could be mapped to the new account. The need for individual accounts in the database is reduced. New in Oracle Database 11g Release 1, global roles can be created for SYSDBA and SYSOPER in Oracle Identity Management. Organizations with large numbers of databases can centrally manage SYSDBA and SYSOPER access to various enterprise databases. New in Oracle Database 11g Release 1, enterprise user security manageability has been integrated with Enterprise Manager Database Control. In addition, Oracle recently completed testing of enterprise user security with Oracle Virtual Directory. Oracle Virtual Directory enables Oracle Database

enterprise user security to work with existing corporate directories such as Microsoft Active Directory, dramatically simplifying management of Oracle database users.

ORACLE DATABASE 11G MONITORING

The Oracle database provides robust audit capabilities including both standard and fine-grained auditing. Auditing has never been more important than it is today. Auditing has become a key security resource for helping expedite regulatory compliance reporting and proactively detecting suspicious activity. The increasingly sophisticated nature of security threats requires a defense-in-depth approach to security that includes comprehensive monitoring of your enterprise.

Oracle Audit Vault

Oracle Audit Vault reduces the cost and complexity of compliance and the risk of insider threats by automating the collection and consolidation of audit data. It provides a secure and highly scalable audit warehouse, enabling simplified reporting, analysis, and threat detection on audit data. In addition, database audit settings are centrally managed and monitored from within Audit Vault, reducing IT security cost.

Oracle Audit Vault transparently collects and consolidates audit data, providing valuable insight into *who* did *what* to *which* data *when* – including privileged users who have direct access to the database. With Oracle Audit Vault reports, alert notifications, and centralized audit policy management, the internal threat risk and the cost of compliance are greatly reduced. Oracle Audit Vault leverages Oracle's industry leading database security and data warehousing technology for managing, analyzing, storing, and archiving large volumes of audit data.

Simplified Compliance Reporting

Oracle Audit Vault provides standard audit assessment reports covering privileged users, account management, roles and privileges, object management and system management across the enterprise. Parameter driven reports can be defined showing user login activity across multiple systems and within specific time periods, such as weekends. Oracle Audit Vault provides an open audit warehouse schema that can be accessed from Oracle BI Publisher, Oracle Application Express, or any 3rd party reporting tools.

Proactive Threat Detection with Alerting

Oracle Audit Vault event alerts help mitigate risk and protect from the insider threats by providing proactive notification of suspicious activity across the enterprise. Oracle Audit Vault continuously monitors the inbound audit data, evaluating audit data against alert conditions. Alerts can be associated with any auditable database event including system events such as changes to application

tables, role grants, and privileged user creation on sensitive systems. Oracle Audit Vault provides graphical summaries of activities causing alerts.

Security and Scalability

Protecting audit data is critical to the security and internal controls processes. Oracle Audit Vault protects audit data by using sophisticated controls including Oracle Database Vault and Oracle Advanced Security. Access to the audit data within Oracle Audit Vault is strictly controlled. Privileged DBA users cannot view or modify the audit data and even auditors are prevented from modifying the audit data. Oracle Audit Vault leverages Oracle's proven data warehousing and partitioning capabilities to achieve massive scalability, a key requirement for any auditing solution. Oracle Audit Vault can optionally be deployed with Oracle Real Application Clusters (RAC), enabling scalability, high availability, and flexibility.

Lowers IT Costs with Oracle Audit Vault Policies

IT security personnel work with auditors to define audit settings on databases and other systems across the enterprise to meet both compliance requirements and internal security policies. Oracle Audit Vault provides the ability to provision and review audit settings in multiple databases from a central console, reducing the cost and complexity of managing audit settings across the enterprise.

Oracle Enterprise Manager Configuration Management Pack

Oracle Enterprise Manager Configuration Management Pack provides a rich policy-based vulnerability detection solution. It provides automated assessments for secure configurations through XML-based policy solutions for security checklists, configuration benchmarks, automated compliance testing, and compliance scoring. Oracle Enterprise Manager Configuration Management Pack ships with more than 240 “best practices” policies in the areas of security, configuration, and storage. Policies help in continuous security assessment by automated detection of critical security vulnerabilities.

Policies are effective in managing configuration drift (through installation of patches, adding files and directories, changing settings and ports, editing its dependencies, etc) by continually auditing against prescribed configurations. This “drift” is tracked so that administrators know when they are happening, what changes are acceptable, and what changes must be corrected. This level of security and compliance, through proactive auditing and enforcement, is necessary to keep control in the continual flux that defines most of today’s data centers. Policies can be scheduled and applied across targets.

Increasing regulatory compliance demands that IT systems are secure and have not been compromised. Ensuring that IT systems are behaving in-line with security best practices is critical for any IT shop. Policy Groups (a collection of security and configuration policies that map to a best practice or regulatory standard) enable administrators and CIOs to get at-a-glance view on how their systems are

complying with security best practices specified in their environment. The evaluation results are converted into compliance scores (based on a weighted average) and the overall scores can be presented in a compliance dashboard. The dashboard presents summaries of key indicators, with ability to drilldown to details, allowing users to continuously monitor and verify their compliance posture. Support for trend analysis provides the ability to track progress towards compliance over time for the entire IT environment. Exceptions and violations can be addressed to bring systems back into compliance with policy groups.

SUMMARY

Transparent security solutions are critical in today's global business economy. Addressing regulatory compliance and reducing the risk of insider threats requires strong security on application data. Modifying existing application code can be a complex and costly process. Oracle Database Security products are designed to work transparently, minimizing any impact on existing applications while addressing mandatory requirements found in many regulations.

Oracle Database Vault transparently addresses the strong internal control requirements found in SOX, PCI, HIPAA, and many other regulations. Oracle Database Vault realms prevent even the DBA from accessing sensitive financial or privacy related information found in applications. Oracle Label Security sensitivity labels provide a wealth of new factors to use in Oracle Database Vault multi-factor authorization decisions. Oracle Advanced Security transparent data encryption provides an elegant solution for PCI encryption and key management requirements and continues to lead the encryption industry with table space and LOB encryption in Oracle Database 11g. Oracle Audit Vault turns audit data into a key security resource, transparently consolidating and securing vital audit information associated with database activity. Oracle Audit Vault reports, alerts, and policies expedite the job of audit compliance personnel and security officers. Oracle Enterprise Manager configuration management pack continuously monitors hosts and databases for violations of security and configuration best practices, greatly simplifying the job of the security administrator.

Transparent Solutions for Privacy and Compliance with Oracle Database 11g

September 2008

Author: Paul Needham

Contributing Authors: Kamal Tbeileh

**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

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.