Oracle Database 11g Release 1 Transparent Solutions for Security and Compliance

An Oracle White Paper
June 2007

ORACLE

INTRODUCTION

Over the past ten years 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. The

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**

Fig 1. Compliance & Privacy Challenges

CSI/FBI 2005 Computer Crime and Security studies have 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. Transparent security solutions are critical in today's global business economy. Oracle Database 11g Release 1 provides the industry's most advanced data security capabilities with security solutions that work transparently with existing applications while addressing mandatory requirements found in regulations.

TRANSPARENT SECURITY SOLUTIONS

Transparent security solutions are critical because historically most applications have relied 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 rapid deployment of new applications. The Internet accelerated the development of new applications for all aspects of business processing, resulting in better accessibility, tremendous cost saving and increases in productivity. However regulations worldwide now require much stricter controls on sensitive financial and privacy related information. Oracle Database Security products simplify the transition from application level security to database enforced security, enabling organizations to minimize the costs associated with regulatory compliance and the deployment of strong internal controls. Oracle database security provides application transparent security solutions in the critical areas of user management, access control, data protection and monitoring.

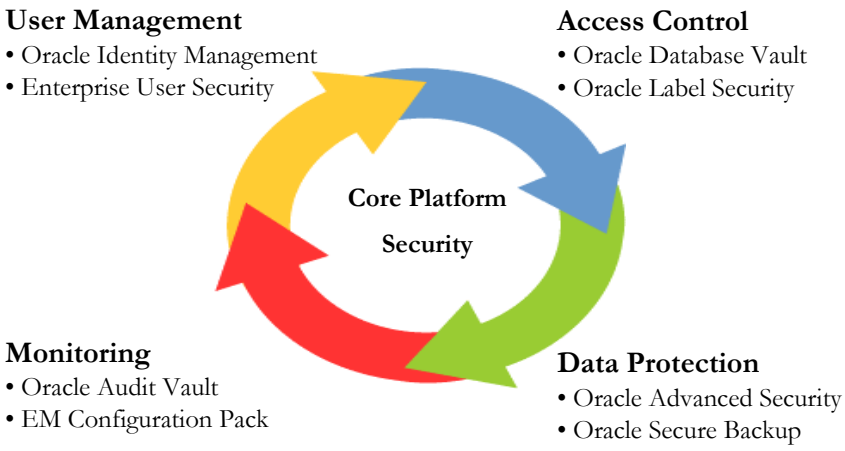


Fig 2. Oracle Data Security Products

ORACLE DATABASE 11G RELEASE 1 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

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.

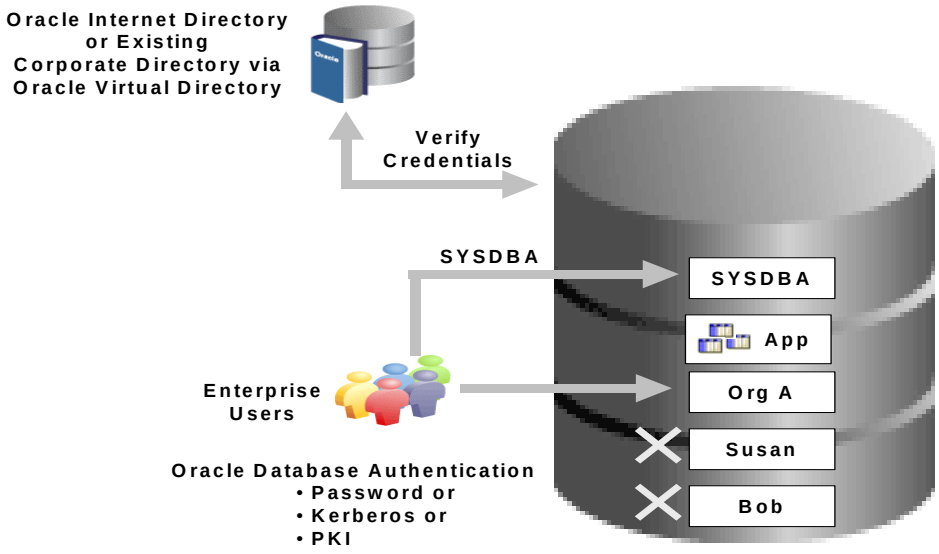


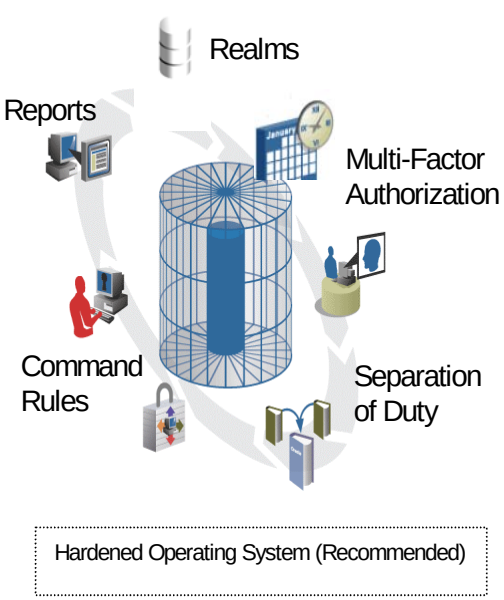
Fig 3. Oracle Database Enterprise User Security with Oracle Identity Management

ORACLE DATABASE 11G RELEASE 1 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 and reducing enforcement at the application level.

Oracle Database Vault

Oracle Database Vault is the latest industry's leading security solution from oracle designed specifically for protecting business data for regulatory compliance and reducing the risk associated with the insider threat. Whether it's traditional client server 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. Oracle Database Vault is available for Oracle Database 9i Release 2, Oracle Database 10g Release 2, and Oracle Database 11g Release 1. In addition, Oracle Database Vault has been validated with Oracle PeopleSoft Applications. Validation with additional applications, including Oracle E-Business Suite and Siebel, is currently underway.



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**

Fig 4. Oracle Database Vault Overview

Oracle Database Vault Realms

Oracle Database Vault Realms prevent DBAs, application owners, and other privileged users from viewing application data using their powerful privileges. Oracle Database Vault Realms put in place preventive controls, helping reduce the potential impact 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.

- Account administration
- Security administration
- Resource administration

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 of security for an existing application. In addition to the built-in Factors provided by Oracle 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 Oracle Database Vault console or on the command line using the API.

Oracle Label Security

Oracle Label Security enables transparent row level access control in the Oracle database using sensitivity labels. Used in combination with Oracle Database Vault, sensitivity labels become powerful factors for use in multi-factor authorization, helping address regulatory compliance requirements. Highly flexible and adaptable, Oracle Label Security is the industry's most advanced label based access control product. Policy based administration simplifies the management of sensitivity labels and user label authorizations.

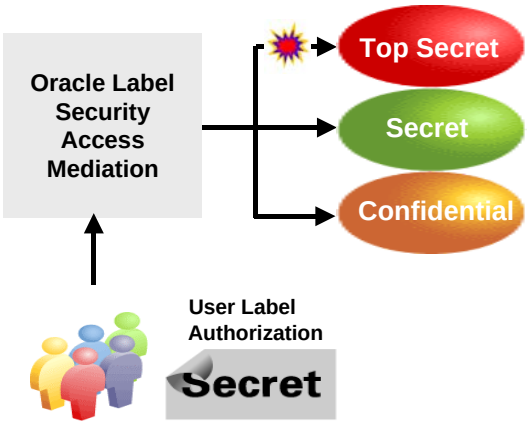


Fig. 5 Oracle Label Security Overview

Protect Sensitive Data

Oracle Label Security transparently controls access to application data by comparing data sensitivity labels with user label authorizations. Using Oracle Enterprise Manager, security administrators can define data sensitivity labels and assign label authorizations to users, including the maximum sensitivity label an individual user is allowed to access. Security administrators can then apply Label Security policies to one or more application tables. Once applied, Label Security will transparently mediate access to application data by comparing the user label authorization with the sensitivity label assigned to the data. Only if the user label authorization is equal to or greater than the data sensitivity level, will access to the data be allowed. Data sensitivity labels can be comprised of three components.

- Mandatory, hierarchical level *plus*
- Zero or more horizontal compartments *plus*
- Zero or more parent child groups.

For example, the sensitivity label *Secret:ProjectAthens:ExecOnly* is comprised of the level *Secret*, the compartment *ProjectAthens* and the group *ExecOnly*. Many organizations may choose to only use the level component.

Integrated With Oracle Database Vault

Used in combination with Oracle Database Vault, sensitivity 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 new capability extends Label Security concepts beyond traditional row level access controls to mediation at the database and application level. Oracle Database Vault separation of duty can

be extended. For example, database administration activities could be based on the label authorization of the administrator.

Flexible and adaptable

Oracle Label Security provides multiple enforcement options for access control at the row level. Policies can be applied for read operations only, update operations only, or both. User label authorizations include a maximum read label, default write label and default session label. The maximum read label specifies the maximum data sensitivity label a user is allowed access to, the default write label is the default data sensitivity label assigned to data the user inserts and the default session label is the default sensitivity label a user has when connecting to the database. This must be equal to or less than the maximum read label. Special authorizations allowing access to all data for either read or update operations regardless of the users label authorizations can be granted to users and stored procedures. Special authorizations are useful for patching and maintenance purposes. Proxy capability for the one big user application model is provided through the Label Security profile access authorization, allowing the primary application user to assume the label authorizations of an application user. SQL predicates or 'where' clauses can optionally be added to any Label Security policy, extending access control beyond the sensitivity label. Note that label authorizations can be assigned to application users.

Simplified Manageability

Oracle Label Security provides an easy to use policy based administration model. Policies are the logical containers of sensitivity labels, label authorizations and optionally protected objects. Multiple polices can exist in the same database. Optional integration with Oracle Identity Management provides centralized management of policies and user label authorizations. In addition to the Enterprise Manager Label Security console, a comprehensive Label Security API is provided.

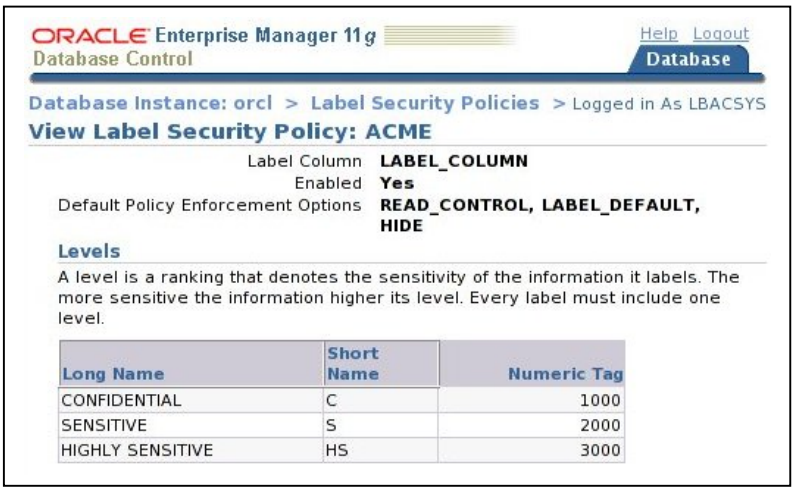


Fig 6. Oracle Label Security Manageability

ORACLE DATABASE 11G RELEASE 1 DATA PROTECTION

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 on the network, on backup media or within the database, from unauthorized disclosure. Oracle Advanced Security Transparent Data Encryption provides the industry's most advanced encryption capabilities for protecting sensitive information without requiring any changes to the existing application.

Transparent Data Encryption

Oracle Advanced Security transparent data encryption (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. With a simple *alter table* command an administrator can encrypt sensitive data within an existing application table.

```
SQL> alter table customers modify (credit_card_number encrypt)
```

Unlike most database encryption solutions, TDE is completely transparent to existing applications with no triggers, views, or other application changes required. 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

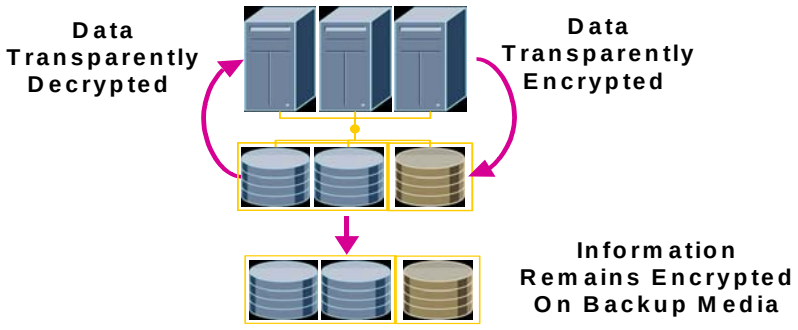


Fig 7. Transparent Data Encryption Overview

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.

Tablespace Encryption

Oracle Advanced Security in Oracle Database 11g Release 1 includes support for tablespace encryption. When a tablespace is created through Enterprise Manager or on the command line, an option now exists to specify that the file be encrypted on the file system. When new data is added to the new tablespace using the *insert* command or datapump, entire tables will be transparently encrypted. When the database reads data blocks from the encrypted tablespace it will transparently decrypt the data blocks.

Hardware Security Modules

TDE has been enhanced in Oracle Database 11g Release 1 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 Release 1 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 Release 1. 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 DATABASE 11G RELEASE 1 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.

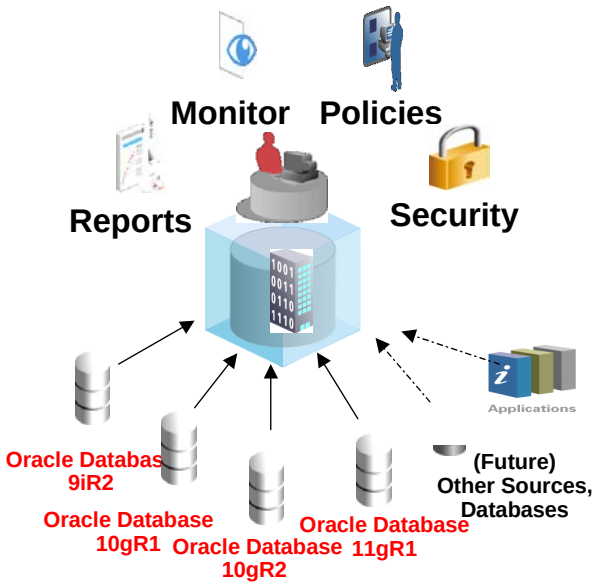


Fig 8. Oracle Audit Vault Overview

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.

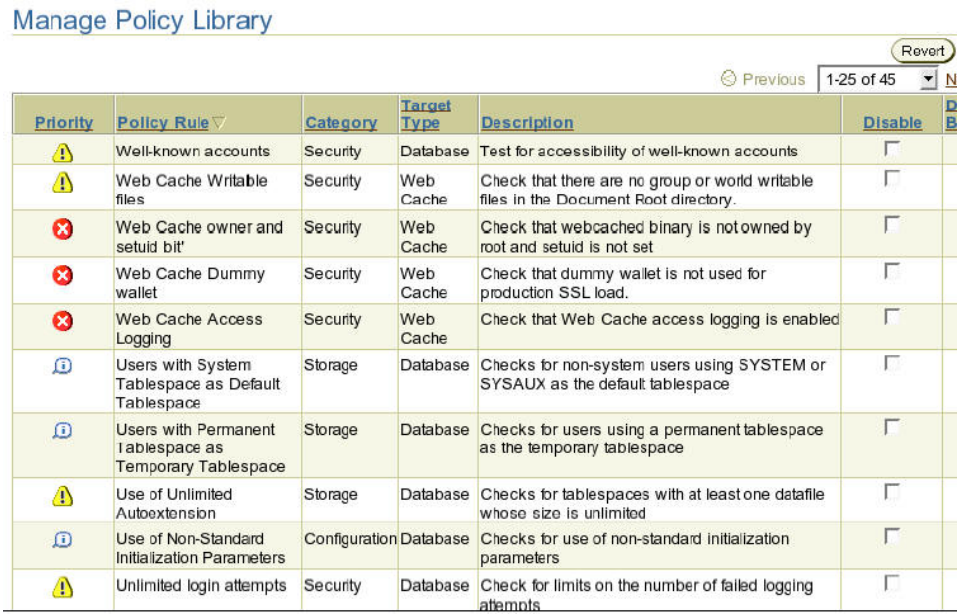
Oracle Enterprise Manager Configuration Management Pack

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 remidiated to bring systems back into compliance with policy groups.



Priority	Policy Rule	Category	Target Type	Description	Disable
⚠	Well-known accounts	Security	Database	Test for accessibility of well-known accounts	☐
⚠	Web Cache Writable files	Security	Web Cache	Check that there are no group or world writable files in the Document Root directory.	☐
✖	Web Cache owner and setuid bit'	Security	Web Cache	Check that webcached binary is not owned by root and setuid is not set	☐
✖	Web Cache Dummy wallet	Security	Web Cache	Check that dummy wallet is not used for production SSL load.	☐
✖	Web Cache Access Logging	Security	Web Cache	Check that Web Cache access logging is enabled	☐
ⓘ	Users with System Tablespace as Default Tablespace	Storage	Database	Checks for non-system users using SYSTEM or SYSAUX as the default tablespace	☐
ⓘ	Users with Permanent Tablespace as Temporary Tablespace	Storage	Database	Checks for users using a permanent tablespace as the temporary tablespace	☐
⚠	Use of Unlimited Autoextension	Storage	Database	Checks for tablespaces with at least one datafile whose size is unlimited	☐
ⓘ	Use of Non-Standard Initialization Parameters	Configuration	Database	Checks for use of non-standard initialization parameters	☐
⚠	Unlimited login attempts	Security	Database	Check for limits on the number of failed logging attempts	☐

Fig 9. Enterprise Manage Configuration Management Pack Secure Configuration Policies

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 tablespace 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.

Oracle Database 11g Release 1 Transparent Solutions for Security and Compliance
June 2007
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