

An Oracle White Paper
August 2010

Cost Effective Security and Compliance with Oracle Database 11g Release 2

Introduction	2
Oracle’s Defense-in-Depth Security Solution.....	2
Encryption and Masking	3
Access Control	3
Auditing, Monitoring and Blocking.....	3
Encryption and Masking	3
Oracle Advanced Security	4
Oracle Secure Backup.....	5
Oracle Data Masking	5
Access Control	5
Oracle Database Vault.....	6
Oracle Label Security	7
Auditing, Monitoring and Blocking.....	7
Oracle Database Firewall	7
Oracle Audit Vault.....	8
Oracle Configuration Management Pack	9
Oracle Total Recall	9
Application Certification	10
Oracle Exadata Database Machine	10
Conclusion	10

Introduction

Consolidation, outsourcing, information sharing, and cloud computing are just a few of the business initiatives that present increased information security challenges. While most organizations have web facing firewalls deployed, strengthening security controls around data in a cost effective and efficient manner has become a top priority. The recently published 2010 Data Breach Investigations Report published by the Verizon Risk Team showed that 98% of data breached came from servers¹. Oracle provides a defense-in-depth security architecture that enables organizations to systematically and transparently increase security controls around data and applications. By leveraging these controls, organizations can safeguard data, help ensure regulatory compliance, and achieve business goals while still maintaining scalability, performance and availability.

Oracle's Defense-in-Depth Security Solution

Defense-in-depth data security means looking at data security holistically. To do that, one needs to look at the entire life cycle of the data, where the data resides, what applications access the data, who is accessing the data and under what conditions, and ensuring that the systems have been properly configured. Built upon 30 years of security experience, Oracle's defense-in-depth security architecture includes encryption and masking, access control, auditing and monitoring solutions.

¹ *2010 Data Breach Investigations Report* (Verizon Business)

Encryption and Masking

- Oracle Advanced Security Transparent Data Encryption (TDE) is Oracle's solution for transparently encrypting Oracle database data before writing it to disk, protecting sensitive application data from direct access at the operating system level and on backup media.
- Oracle Secure Backup is Oracle's backup solution that transparently encrypts data during the backup process to tape media, protecting the data in the event the tapes are lost or stolen.
- Oracle Data Masking is Oracle's off-line data de-identification solution that substitutes production data with anonymous data values, protecting sensitive data from unnecessary exposure in development and test environments.

Access Control

- Oracle Database Vault is Oracle's solution for enforcing strong operational security controls inside the Oracle database, preventing ad-hoc access to application data, changes to application structures, and access to application data by privileged users.
- Oracle Label Security is Oracle's solution for enforcing data classification based access control at the row level and multi-level security for government and defense organizations.

Auditing, Monitoring and Blocking

- Oracle Database Firewall is Oracle's solution for monitoring network SQL traffic before it reaches Oracle and non-Oracle databases, helping provide a first line of defense against SQL*Injection and other unauthorized SQL.
- Oracle Audit Vault is Oracle's solution for reporting and alerting on audit data from Oracle and non-Oracle databases, enforcing the trust-but-verify principle and helping organizations simplify and reduce the cost of compliance reporting.
- Oracle Enterprise Manager Configuration Management Pack is Oracle's solution for maintaining a secure configuration for Oracle installations, periodically scanning for security related configuration settings.
- Oracle Total Recall is Oracle's solution for providing a history of changes to sensitive data for forensic analysis.

Encryption and Masking

Encryption and masking are important for protecting data outside the access controls of the database and application. Preventing direct, unimpeded access to sensitive data at the operating system layer is critical for protecting personally identifiable information (PII), credit card data and other sensitive information. In addition, movement of production data to other departments

for testing and development purposes unnecessarily exposes sensitive data and increases the risk of data loss.

Oracle Advanced Security

Oracle Advanced Security Transparent Data Encryption (TDE) helps address security requirements found in PCI-DSS, HIPAA and the Massachusetts data protection law 201 CMR 17.00 by encrypting sensitive information. TDE can be used to encrypt specific sensitive columns or entire Oracle tablespaces. TDE is transparent to existing applications and does not require any triggers, views or other application changes.

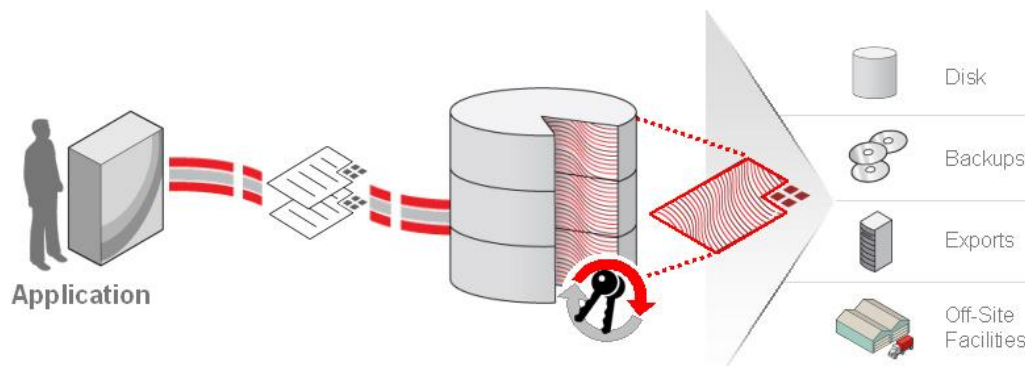


Figure 1. Oracle Advanced Security

TDE transparently encrypts data before writing it to disk and transparently decrypts it after an application user has successfully authenticated, and passed all access control checks at the application and database level. Existing database backup routines continue to work, with the data remaining encrypted on the backup media. For encryption of entire database backups, TDE can be used in combination with Oracle RMAN. TDE can also be used with Oracle Data Pump to encrypt database exports. TDE provides built-in key management with a two tier key architecture consisting of a single master encryption key stored outside the database and one or more encryption keys stored inside the Oracle database. The master encryption key is used to encrypt and protect the encryption keys stored inside the Oracle database. The master encryption key can be stored in an Oracle Wallet or a hardware security module (HSM) provided by vendors such as Thales and Safenet. TDE also interoperates with the RSA key management solution.

Oracle Advanced Security provides an easy-to-deploy solution for protecting all communication to and from the Oracle Database with SSL/TLS based encryption. Oracle Advanced Security also provides a native network encryption capability for enterprises without a PKI infrastructure. Oracle Advanced Security can be configured to reject connections from clients that do not

encrypt data, or optionally allow unencrypted connections for deployment flexibility. For an alternative to password based authentication, Oracle Advanced Security supports PKI, Kerberos and RADIUS authentication to the Oracle database.

Oracle Secure Backup

Backup tapes containing sensitive data can be protected using encryption. Oracle Secure Backup encrypts backups and provides centralized tape backup management for the entire Oracle environment, including the Oracle database, and the associated UNIX, Linux, Windows and Network Attached Storage (NAS) file system data. Oracle Secure Backup integrates with the Oracle database through Recovery Manager (RMAN) supporting versions Oracle Database 9i to Oracle Database 11g and higher. With its optimized integration, it achieves faster backups than comparable media management utilities with less CPU utilization.

Oracle Data Masking

Oracle Data Masking helps organizations comply with data privacy and protection mandates. With Oracle Data Masking, sensitive information such as credit card or social security numbers can be replaced with realistic but non-factual 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.



Figure 2. Oracle Data Masking

Access Control

Access controls at the data layer are becoming increasingly important as organizations move toward data consolidation, off-shoring and cloud computing. Most modern applications enforce security at the application level using application specific authorizations. Today, however, regulations and privacy laws require limited access to application data, even by privileged users who maintain the database on an on-going basis. Controls at the database layer provide added protection against privilege misuse either by an insider or by someone posing as an insider using stolen credentials.

Oracle Database Vault

Oracle Database Vault creates a highly secure environment for applications by enforcing strong operational controls inside the Oracle database. Oracle Database Vault realms prevent ad-hoc access to application data by privileged users. Oracle Database Vault realms are essentially firewalls inside the Oracle database, blocking all encompassing DBA like privileges from being used to access application data. Oracle Database Vault realms are transparent to existing applications, enabling significantly stronger security controls to be achieved without changing the existing application code or performing a tedious least privilege exercise.

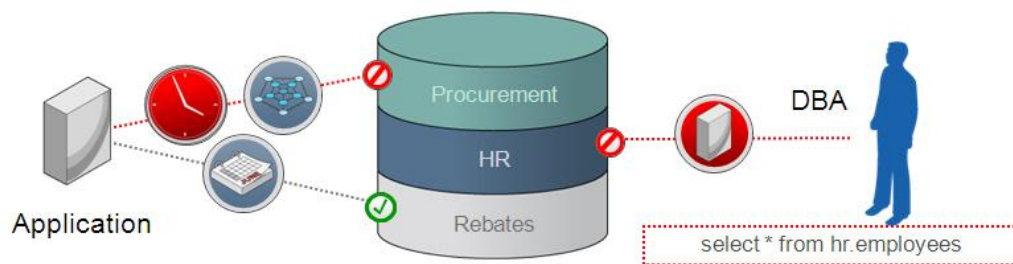


Figure 3. Oracle Database Vault

Oracle Database Vault command rules significantly tighten security by limiting who, when, where and how databases, data and applications can be accessed. Multiple factors such as IP address, time of day and authentication method can be used in a flexible and adaptable manner to enforce access controls regardless of whether the connection is local or remote and without making changes to the application. For example, access can be restricted to a specific middle tier, creating a “trusted-path” to the application data and preventing use of ad-hoc tools local or remote to the Oracle database. Policies can be associated with many SQL commands including data definition language (DDL) commands such as *create*, *drop* and *truncate* table.

Oracle Database Vault enforces separation of duty by providing three distinct responsibilities out-of-the-box for security, account management, and day-to-day database administration activities. For example, Oracle Database Vault blocks a DBA from creating a new user in the database even though the DBA has the *create user* privilege granted through the DBA role. This capability locks down and prevents unauthorized changes that may result in unexpected audit findings as well as potential security vulnerabilities such as creating an un-authorized DBA account in the database.

Oracle Label Security

Oracle Label Security protects sensitive data by assigning a data label or data classification to each row in an application table. Oracle Label Security mediates access by comparing the data label against the label authorization of the user requesting access. This mediation check is in addition to any application level access control checks as well as the traditional discretionary access controls (*select, insert, update, delete*) checks performed by the database. For application transparency, the data label can be appended to an existing application table using a *hidden* column. Based on the policy of the organization, data labels can be defined to enforce a combination of hierarchical, compartmental and group access controls. High security organizations use Oracle Label Security to enforce multi-level security (MLS) requirements. Commercial organizations can similarly use Oracle Label Security to control access to sensitive data, compartmentalize data for multi-tenancy, software-as-a-service and other business requirements. Oracle Label Security is commonly applied to a subset of application tables. Oracle Label Security label authorizations can be assigned to traditional database users as well as application users that do not have database accounts.

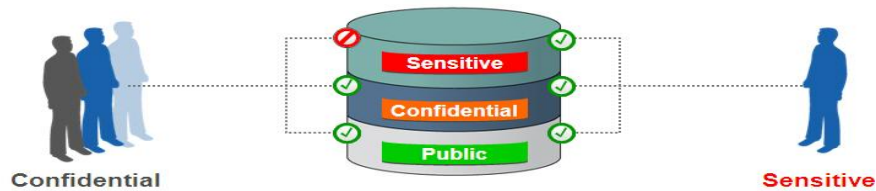


Figure 5. Oracle Label Security

Auditing, Monitoring and Blocking

While Oracle Advanced Security encryption and Oracle Database Vault access controls are key components to protecting data outside and inside the Oracle database, defense-in-depth security requires enforcing the *trust-but-verify* principle by monitoring events taking place inside the database as well as inbound SQL activity, helping protect against unauthorized SQL commands and SQL injection attacks.

Oracle Database Firewall

Oracle Database Firewall acts as the first line of defense for databases, helping prevent internal and external attacks from reaching the database. Highly accurate SQL grammar-based technology monitors and blocks unauthorized SQL traffic on the network before it reaches the database. Oracle Database Firewall is easy to deploy and requires no changes to existing applications.

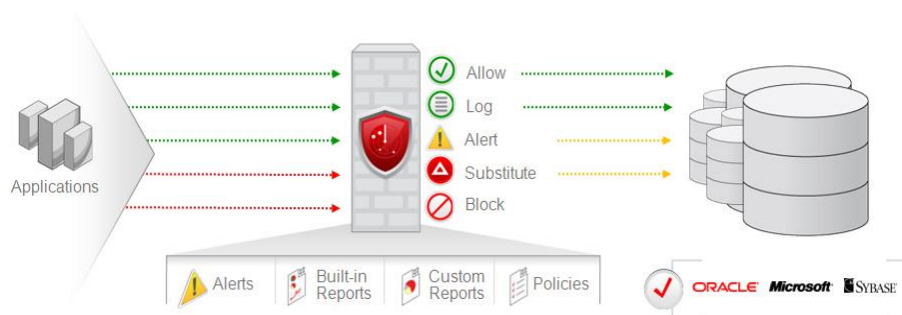


Figure 6. Oracle Database Firewall

Oracle Database Firewall supports white list, black list, and exception list based policies. A white list is simply the set of approved SQL statements that the firewall expects to see. These can be learned over time or imported. A black list includes schemas, tables, users, and SQL statements that are not permitted to be sent to the database. Exception list based policies provide additional deployment flexibility that can be used to override the white list or black list policies. Policies can be enforced based upon attributes including SQL category, time of day, application, user, and IP address. Oracle Database Firewall can log and alert, block or substitute the incoming SQL statement with a harmless SQL statement. This flexibility, combined with advanced SQL grammar analysis, provides organizations graceful application handling of unauthorized requests. Oracle Database Firewall can be used to monitor Oracle, SQL Server and Sybase databases.

Oracle Audit Vault

Oracle Audit Vault reduces the cost and complexity of compliance and helps detect suspicious activity by transparently collecting and consolidating the audit data from Oracle and non-Oracle databases, 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 risks from internal threats 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.

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 such as 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, or 3rd party reporting tools. Oracle Audit Vault consolidates audit data from Oracle, SQL Server, Sybase and IBM DB2 databases.

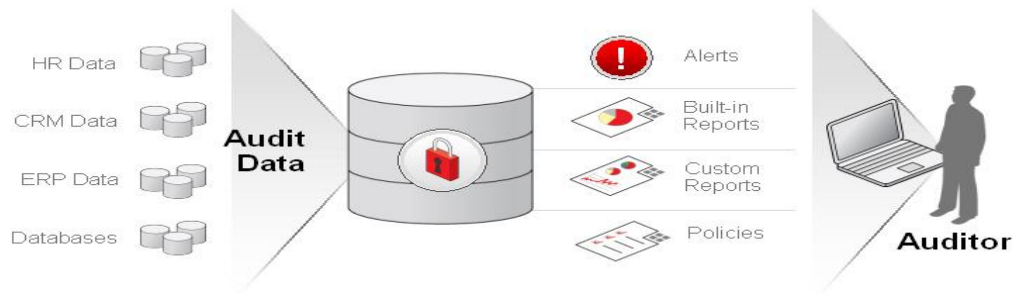


Figure 7. Oracle Audit Vault

Oracle Configuration Management Pack

Configuration management is a critical component in day-to-day IT operations. Oracle Configuration Management Pack forms the centerpiece of Oracle Enterprise Manager's ability to manage configurations and automate IT processes. A key component of this solution is Configuration Change Console, which reduces cost and mitigates risk by automatically detecting, validating and reporting on authorized and unauthorized configuration changes. Oracle Configuration Management Pack ships with over 200 built-in policy checks and the capability for administrator's to define their own custom policies.

Oracle Configuration Management Pack tracks violations of these policies in a similar manner as performance metrics. Notification rules can be applied and corrective actions can be assigned to violations. For example, if a well-known username/password is present in a database, or if an open port is detected in the Application Server, a corrective action could be defined to automatically disable the account and close that port.

Oracle Total Recall

Regulatory and compliance regulations such as SOX, HIPAA and BASEL-II require retention of historical data. Additionally, businesses are increasingly realizing the immense value historical data can provide in terms of helping them understand market trends, customer behavior and forensic analysis.

Organizations need an efficient mechanism to retain data for longer duration that doesn't involve application rewrites, 3rd party or handcrafted software solutions, and additional administrative overheads. Oracle Total Recall in Oracle Database 11g addresses these challenges by ensuring complete, secure retention and management of all your historic data. Oracle Total Recall with the underlying technology, Oracle Flashback Data Archive transparently tracks changes to database tables data in a highly secure and efficient manner without requiring use of special interfaces or application changes.

Application Certification

To help customers protect sensitive data and applications, Oracle has pre-certified Oracle database security solutions such as Oracle Database Vault and Oracle Advanced Security with numerous applications including Oracle E-business Suite, Oracle PeopleSoft, Oracle JD Edwards EnterpriseOne, and Oracle Siebel. SAP recently completed certification with both Oracle Database Vault and Oracle Advanced Security. Oracle Database Vault and Oracle Advanced Security provide critical safeguards to protect data from ad-hoc access by privileged users both inside and outside the database. For monitoring, Oracle Audit Vault and Oracle Database Firewall can be deployed to monitor activity inside the Oracle database as well as inbound SQL traffic on the network. Please refer to application specific support notes for the most up-to-date certification information.

Oracle Exadata Database Machine

Oracle Advanced Security and Oracle Database Vault are fully certified with the Oracle Exadata Database Machine. Both Oracle Advanced Security and Oracle Database Vault provide critical safeguards for Oracle Exadata Database Machine deployments, encrypting data at rest and enforcing strong operational controls. Large data repositories are increasingly the target of choice for hackers and organized crime, making defense-in-depth security especially important for the Oracle Exadata Database Machine.

Conclusion

Oracle provides a comprehensive and transparent defense-in-depth security architecture to help address the complex security and regulatory challenges found in today's global economy. Oracle Advanced Security and Oracle Data Masking provide encryption and de-identification solutions for sensitive data, protecting data at rest from unauthorized access and reducing risk of data exposure in non-production environments. Oracle Database Vault enforces strong operational controls in the Oracle database, providing a highly secure environment for applications and helping address security issues associated with data consolidation and outsourcing. Oracle Audit Vault securely consolidates and monitors database audit data from Oracle and non-Oracle databases. Oracle Database Firewall monitors inbound SQL traffic to Oracle and non-Oracle databases, helping prevent unauthorized SQL and SQL injection attacks.



Cost Effective Security and Compliance with
Oracle Database 11g Release 2
August 2010
Author: Oracle

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

Copyright © 2009, Oracle and/or its affiliates. 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.