ORACLE 11g DATABASE

An Oracle White Paper
March 2011

Defense In-Depth Security for Oracle E-Business Suite Applications

ORACLE

Executive Overview

Applications play a critical role in the day to day operations of nearly every organization worldwide. For that reason organizations have historically focused on the high availability and scalability aspects of applications for business continuity. Today, however, safeguards must be deployed that help protect against information security threats. These threats directly impact such business initiatives as application consolidation and outsourcing. Oracle database security solutions are focused on protecting sensitive data through a defense-in-depth architecture. This means securing the application roles and protecting the application data and structure through database-enforced change controls, providing preventive controls on privileged user access to application data, encrypting sensitive data, and permanently masking sensitive data when moved from production to test environment. To help Oracle E-Business Suite customers protect their sensitive data and applications, Oracle has pre certified Oracle database security solutions such as Oracle Database Vault and Oracle Advanced Security with Oracle E-Business Suite.

Oracle Advanced Security with Oracle E-Business Suite

Industry directives such as the Payment Card Industry Data Security Standard (PCI-DSS) and numerous state privacy breach notification laws require the use of encryption for sensitive data. Oracle Advanced Security provides a transparent and scalable encryption solution for encrypting sensitive Oracle E-Business Suite application data in the database, on the network, and on disk backup. As the definition of sensitive data continues to expand far beyond credit card and social security numbers, Oracle Advanced Security provides the flexibility to encrypt individual columns or the entire application data.

Transparent Data Encryption with Oracle E-Business Suite

Oracle Advanced Security transparent data encryption (TDE) automatically encrypts Oracle E-Business Suite application data when written to database files and transparently decrypts the data when accessed inside the database, without requiring any application code changes. Traditional access controls still apply, so data will not be decrypted until an application or database user has authenticated to the Oracle database and passed all access control checks including those enforced by Oracle

Database Vault. Encrypted data remains secure in the event of unauthorized access to files at the operating system level, discarded disk drives and off-site disk backup. TDE column encryption can be used to protect individual columns in application tables containing credit card numbers or other personally identifiable information (PII). Encryption of credit card numbers stored in Oracle E-Business Suite applications helps organizations comply with section 3.6 of the PCI Data Security Standard (PCI-DSS). Customers running on Oracle Database 11g can use TDE tablespace encryption to protect all the application tablespaces.

Supported Oracle E-Business Suite Releases

Oracle E-Business Suite application releases 11.5.9 and higher running on Oracle Database 10g Release 2 are supported with TDE column encryption. Oracle E-Business Suite application releases 11.5.10 and higher running on Oracle Database 11g are supported with TDE column encryption and TDE tablespace encryption.

For more information
Current E-Business Suite Technology Stack Certifications[1]
Using TDE Tablespace Encryption with Oracle E-Business Suite Release 12 [2](Note 828229.1)
Using TDE Column Encryption with Oracle E-Business Suite Release 11i [3](Note 403294.1)
Using TDE Tablespace Encryption with Oracle E-Business Suite Release 11i [4](Note 828223.1)
Transparent Data Encryption best practices [5]

To learn more about Oracle E-Business customers' success stories with Oracle Transparent Data Encryption, visit the links below:

CMC markets[6]

Oracle Database Vault with Oracle E-Business Suite

[1] https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=828229.1
[2] https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=828229.1
[3] https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=403294.1
[4] https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=828223.1
[5] http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf
[6] http://www.oracle.com/customers/snapshots/cmc-markets-database-snapshot.pdf

Oracle Database Vault enforces strong operational controls inside the Oracle database creating a highly secure environment for Oracle E-Business Suite applications. 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 Oracle E-Business Suite 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.

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 Database Vault security controls address common requirements found in regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and the Health Insurance Portability and Accountability Act (HIPAA). These regulations require strong internal controls to protect sensitive data such as financial, healthcare, and credit card information. Outsourcing and off-shoring,

"Deploying Oracle Database Vault and Oracle Audit Vault allows us to achieve most of our audit requirements without making changes to our applications," says Gharu. "It allows us to harden our database environment so that the applications continue to work, but direct access to the application data requires that privileged users meet a defined set of criteria."

— Akash Gharu, Global Database Services Manager, CMC Markets

application consolidation, and increasing concerns over insider threats have resulted in an almost mandatory requirement for strong controls on access to sensitive application data. Oracle Database Vault enforces real-time preventive controls in the Oracle Database supporting the Oracle E-Business Suite applications.

Oracle Database Vault protections for Oracle E-Business Suite enables customers to restrict privileged users' access to application data, enforce separation-of-duty, and provide tighter access control with multi-factor authorization.

Supported Oracle E-Business Suite Releases

E-Business Suite release 11.5.10 and 12.0.4 and higher are certified with Oracle Database Vault release 10.2.0.4 and higher. All Oracle Database Vault released platforms are supported with this certification. Oracle Support provides best practices on common E-Business Suite specific maintenance tasks in the Oracle Database Vault environment.

For more information:

Integrating Oracle E-Business Suite Release 11i with Oracle Database Vault 11.2[7] (Note 1091086.1)

Integrating Oracle E-Business Suite Release 12 with Oracle Database Vault 11.2[8] (Note 1091083.1)

Integrating Oracle E-Business Suite Release 11i with Oracle Database Vault 11.1.0.7[9] (Note 859399.1)

Integrating Oracle E-Business Suite Release 12 with Oracle Database Vault 11.1.0.7[10] (Note 859397.1)

Integrating Oracle E-Business Suite Release 12 with Oracle Database Vault 10.2.0.5[11] (Note 1139798.1)

Integrating Oracle E-Business Suite Release 11i with Oracle Database Vault 10.2.0.5[12] (Note 1139844.1)

To learn more about Oracle E-Business Suite customers' success stories with Oracle Database Vault, visit the links below:

- CMC[13]
- ABSA Group[14]

Oracle Data Masking for Oracle E-Business Suite Applications

Enterprises have always shared data within and outside their organizations for various business purposes. Database administrators (DBAs) in these enterprises copy production data into staging or test environments to allow in-house developers or offshore testers to perform application development and application testing. The problem with data sharing is that copies of production data often contain

[7] https://support.oracle.com/CSP/main/article?cmd=show&id=1091086.1&type=NOT
[8] https://support.oracle.com/CSP/main/article?cmd=show&id=1091083.1&type=NOT
[9] https://support.oracle.com/CSP/main/article?cmd=show&id=859399.1&type=NOT
[10] https://support.oracle.com/CSP/main/article?cmd=show&id=859397.1&type=NOT
[11] https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1139798.1
[12] https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1139844.1
[13] http://www.oracle.com/us/corporate/customers/cmc-database-snapshot-081133.pdf
[14] http://www.oracle.com/newsletters/information-indepth/database-insider/apr-10/absa.html

company confidential, sensitive or personally identifiable information, access to which is restricted by government regulations. Therefore, these enterprises run the risk of exposing sensitive information when sharing production data with application developers or software quality testers.

Oracle Data Masking Pack helps Oracle E-Business Suite customers achieve security and compliance by permanently obfuscating sensitive data in the production databases before they move to test and development environments. Oracle Data Masking Pack helps reduce security risks by irreversibly replacing the original Oracle E-Business Suite sensitive data with fictitious data so that it can be shared safely with IT developers or offshore business partners. Oracle Data Masking Pack helps maintain the integrity of the Oracle E-Business Suite applications while masking data.

To learn more about Oracle E-Business Suite customers' success stories with Oracle Data Masking, visit the links below:

CISCO[15]

Conclusion

Applications play a critical role in the day to day business operations and protecting those applications from information security threats has never been more important. While Oracle E-Business Suite application level security ensures application users have access to the appropriate roles and responsibilities within the Oracle E-Business Suite applications, threats today will attempt to bypass application controls to get to valuable data in the database. Oracle database security solutions are focused on protecting sensitive data through defense in-depth architecture. This means securing the application roles and protecting the application data and structure through database-enforced change controls, preventive controls on administrative access to application data, encryption of sensitive data, and masking sensitive application data.

[15] http://www.oracle.com/technetwork/oem/app-quality-mgmt/s317297-heterogeneous-data-masking-181640.pdf

Defense In-Depth Security for Oracle E-Business Suite Applications
March 2011
Author: Anna Leyderman
Contributing Authors: Kamal Tbeileh, Peter Wahl

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

Hardware and Software, Engineered to Work Together