An Oracle White Paper
March 2011

Defense In-Depth Security for Oracle PeopleSoft 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 PeopleSoft 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 PeopleSoft.

Oracle Advanced Security with Oracle PeopleSoft

Industry directives such as the Payment Card Industry Data Security Standard (PCI-DSS) and numerous 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 PeopleSoft Enterprise 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 PeopleSoft

"Even though we evaluated other options, we chose Oracle Advanced Security because it's important to us to make sure we get the right level of protection for our Oracle systems. By using the Transparent Data Encryption capabilities, even the personal data on our backups that are shipped to off-site locations is protected because it's encrypted."

— Brad Peiffer, IT director at ETS

Oracle Advanced Security transparent data encryption (TDE) automatically encrypts sensitive Oracle PeopleSoft Enterprise 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 PeopleSoft Enterprise 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 or some application tablespaces.

Supported Oracle PeopleSoft Releases

All Oracle PeopleSoft application modules and all PeopleSoft application releases running on PeopleTools release 8.46 and higher are supported with Oracle Database 10g Release 2 TDE column encryption. Oracle PeopleSoft applications running on PeopleTools release 8.48 and higher are supported with Oracle Database 11g TDE tablespace encryption and TDE column encryption. To migrate a PeopleSoft application from clear text to encrypted tablespaces without downtime and transparent to applications and users, use this migration guide and script. [1]

For more information see the Red Paper: "Oracle Advanced Security TDE Tablespace Encryption for PeopleTools 8.48 and higher"[2].

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

Ross Stores Improves Information Security with Oracle Database Security Solutions [3]
Oracle Magazine Sept./Oct. 2010 "Secure in the Knowledge" [4]
Transparent Data Encryption best practices [5]

[1] http://www.oracle.com/technetwork/database/security/tde-tabsp-enc-for-psft-131732.zip

[2] http://www.oracle.com/technetwork/database/security/rp-tse-ptools-8-134112.pdf

[3] http://streaming.oracle.com/ebn/podcasts/media/8762531_Ross_060310.mp3

[4] http://www.oracle.com/technetwork/issue-archive/2010/10-sep/o50security-165447.html

[5] http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf

"With Oracle Database Vault and the Transparent Data Encryption feature provided by Oracle Advanced Security, our highly sensitive personal and medical data is now protected against unauthorized access. We therefore were able to integrate our national health information system with healthcare providers' local information systems."

— Madis Tiik, Member of Management Board, Estonian eHealth Foundation

Oracle Database Vault with Oracle PeopleSoft

Oracle Database Vault enforces strong operational controls inside the Oracle database creating a highly secure environment for Oracle PeopleSoft 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 PeopleSoft 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, 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 PeopleSoft applications.

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

Supported Oracle PeopleSoft Releases

Oracle Database Vault has been certified with Oracle PeopleSoft applications. The certification includes out-of-the-box security policies specific for Oracle PeopleSoft applications. All Oracle PeopleSoft application modules and all Oracle PeopleSoft application releases running on PeopleTools release 8.46 and higher or PeopleTools release 8.22 are supported with Oracle Database Vault.

Oracle Database Vault security policies for Oracle PeopleSoft are available for download on the Oracle Technology Network[6]. For more information, see the Red Paper "Oracle Database Vault for Enterprise Tools 8.46 and higher And Enterprise Tools 8.22[7]".

To learn more about Oracle PeopleSoft customers' success stories with Oracle Database Vault, visit the links below:

Security - Ross Stores and Database Vault [8]

Oracle Data Masking for Oracle PeopleSoft 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 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 PeopleSoft applications customers to achieve security and compliance objectives by obfuscating sensitive data in the production databases so they can be leveraged in the test environments. Oracle Data Masking Pack helps reduce security risks by

[6] http://www.oracle.com/technetwork/database/options/database-vault/psft-dbvault-sec-policies-130324.zip

[7] http://www.oracle.com/technetwork/database/security/rp-tse-ptools-8-134112.pdf

[8]http://streaming.oracle.com/ebn/podcasts/media/8762531_Ross_060310.mp3

irreversibly replacing the original Oracle PeopleSoft 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 PeopleSoft applications while masking data.

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 PeopleSoft application level security ensures application users have access to the appropriate roles and responsibilities within the Oracle PeopleSoft 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.

Defense In-Depth Security for Oracle PeopleSoft 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