18c ORACLE Database

Oracle Database Vault with Oracle Database

ORACLE WHITE PAPER | FEBRUARY 2018

Table of Contents

Introduction

Regulations, industry directives and numerous breach disclosure laws require stronger security controls including separation of duty. Privacy and regulatory challenges are becoming increasingly complicated as access to data must be controlled based on laws spanning multiple countries. In parallel, attacks on databases are becoming increasingly common as hackers and even insiders target large data repositories to steal data, disrupt business, or gain economic advantage through industrial espionage. Data breaches resulting from unauthorized privileged users access or abuse of these accounts has accounted for a large percentage of the overall number of data breaches over the past few years. Protecting the database has become paramount and requires a defense in depth, multi-layered approach that encompasses preventive, detective, and administrative controls. Oracle Database 18c strengthens Oracle's industry leading database security solution by providing important security controls in each of these areas.

Oracle Database Vault with Oracle Database 18c provides the industry's most comprehensive access control capabilities for the Oracle Database. Oracle Database Vault provides essential safeguards against common threats, including:

- Threats that exploit stolen credentials obtained from social engineering, key-loggers, and other mechanisms to get access to privileged accounts in your database
- Threats from insiders that misuse privileged accounts to access sensitive data, or to create new accounts, and grant additional roles and privileges for future exploits
- Threats from insiders who bypass the organization's usage policies (including IP address, date, and time of usage), or from unintended mistakes from junior DBAs who might use unauthorized SQL commands that change the database configuration and put the database in a vulnerable state
- Threats to sensitive data during maintenance window from the application administrators
- Threats that exploit weaknesses in the application to escalate privileges and attack other applications on the same database

Oracle Database Vault with Oracle Database 18c includes a powerful runtime privilege analysis capability that allows administrators to identify unused privileges and roles for applications and users. This information can then be used to tighten privilege and role grants and increase the security of the overall application. Oracle Database Vault with Oracle Database 18c is installed by default, enabling efficient setup, configuration and deployment.

Controls for Privileged Accounts

Privileged user accounts are common place in all databases and are used by DBAs for daily tasks such as user management, performance tuning, replication, patching, backup and recovery, space management, startup and shutdown. Many Oracle predefined system users such as SYSTEM and roles such as DBA role can access any application data in the database. Due to their wide ranging access, most organizations enforce strict processes and internal rules on who can be granted privileged access or DBA access to the databases. These accounts and roles, however, have also been a prime target of hackers because of their unimpeded access inside the database. They have also been misused by insiders to gain access to confidential information.

Privilege User Access Controls on Application Data with Realms

Increasing controls on privileged and DBA accounts is vital to improving security. Oracle Database Vault creates a highly restricted application environment ("Realm") inside the Oracle database that prevents access to application data from privileged accounts while continuing to allow the regular authorized administrative activities on the database. Realms can be placed around all or specific application tables and schemas to protect them from unauthorized access while continuing to allow access to owners of those tables and schemas, including those who have been granted direct access to those objects.

Figure 1 below shows how an Oracle Database Vault Realm blocks a DBA or someone masquerading as a DBA. It also shows how applications with powerful system-wide privileges can also be blocked from looking at other application data inside the database. System-wide privileges include SELECT ANY TABLE, frequently granted not only to database administrators but also found in many application environments.

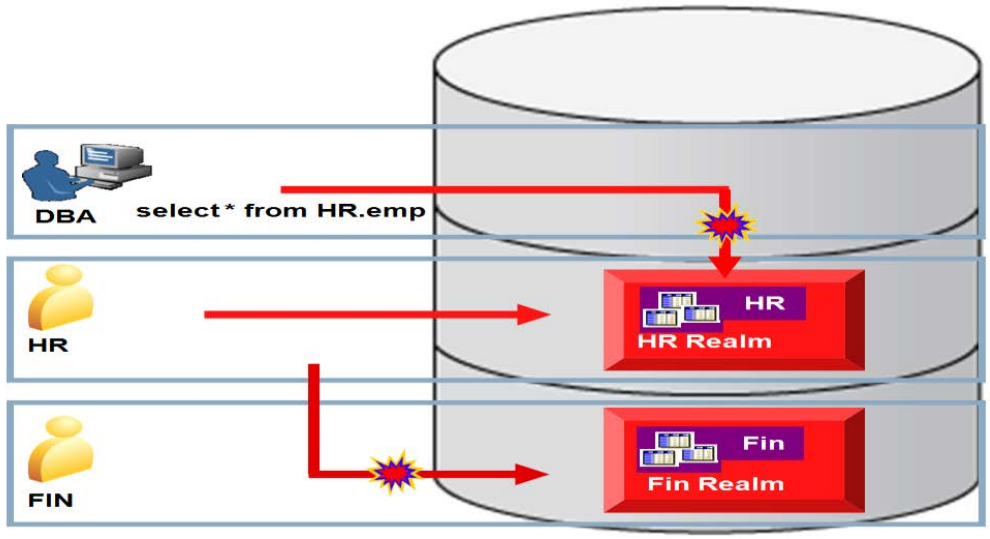

Figure 1. Oracle Database Vault Control for Privileged Accounts

TABLE 1. ORACLE DATABASE VAULT REALMS USE CASES

Use Case	Description
Prevent unauthorized DBA access to application data	Realms help customers comply with data access regulations and protect from insider threats as well as outsider attacks exploiting compromised DBA accounts.
Enable secure consolidation	Realms allow customers to consolidate multiple applications into a single database while preventing highly privileged application accounts from accessing each other's data. This helps customers secure their consolidated applications in their private clouds and helps cloud providers maintain higher level of security assurance for their customers.
Enable secure outsourcing /off-shoring	By controlling access to sensitive data even by administrative staff, Realms allow customers to take advantage of the cost benefits of outsourcing/off-shoring of backend operations.

Oracle Database Vault Realms also place controls on powerful system privileges, roles, and account management. In addition, Oracle Database Vault Realms restrict access to security related packages commonly used by applications, such as the Virtual Private Database (VPD) package. For example, Oracle Database Vault limits who can manage VPD policies, increasing the overall security of the application.

Controls for Maintenance with Mandatory Realms

Periodic access to production environments by IT support staff or application DBAs is a common requirement and is typically associated with patching activity or diagnosing a performance issue. This task may typically involve recreating indexes and triggers, patching PL/SQL packages, or adding new tables, views, and other objects. During such maintenance windows, organizations need the ability to seal off access to tables and views containing highly sensitive data, even to those with direct object grants or the application owner. This is an increasingly common security need driven by data governance requirements and multi-country regulations.

Oracle Database Vault with Oracle Database 18c includes "Mandatory Realms" that effectively seal off application tables, views, or other objects from all access, including the object owner and privileged users, unless access has been specifically granted. Mandatory Realms can be pre-configured and then enabled during maintenance operations. Mandatory Realms can also be used as an additional line of defense to protect applications. In this case, they would not only prevent privileged user access, just like regular realms, but also provide an additional check on all users who have access to the application including those with direct object grants and the application owner. These users can be authorized to the Mandatory Realm and additional checks can be performed before gaining access to application data. Figure 2 shows how Oracle Database Vault Mandatory Realm enforces additional authorization check on the application owner before allowing access to application data.

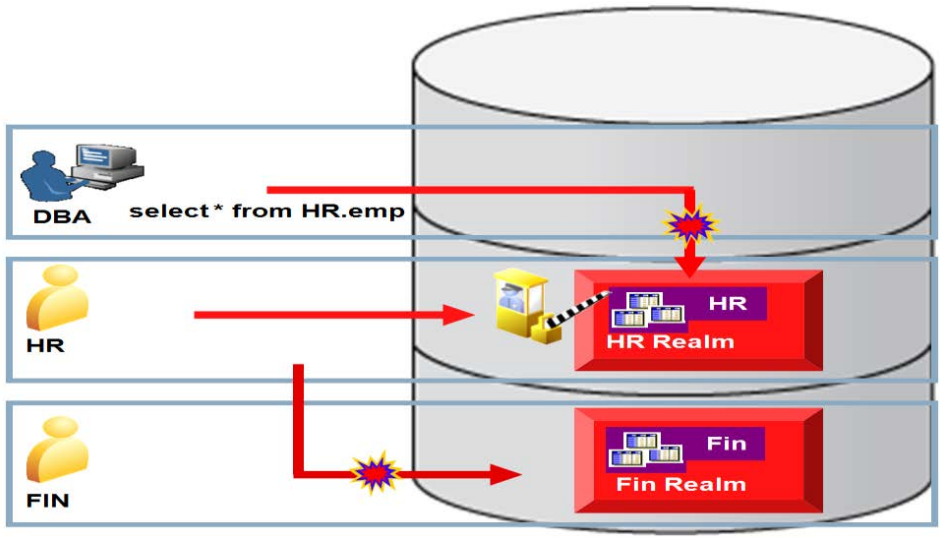

Figure 2. Oracle Database Vault Mandatory Realm for Maintenance

TABLE 2. MANDATORY REALMS USE CASES

Use Case	Description
Support and Development Access	Mandatory Realms can be placed around all or specific application tables, blocking both the application owner as well as those with direct object grants from accessing the data. For patching and support access, stored procedures and application meta data can still be accessed and patched, but application sensitive data will be protected by the Mandatory Realm.
Entitlement Controls	Mandatory Realms freeze the entitlements granted to a database role so that no privileged user can change them. Only authorized users will be able to grant these roles and change their entitlements.
Application Protection	Mandatory Realms can be used to protect applications just like regular realms. In this case, all users who rely on direct grants for access should be added to realm authorizations. This makes it easier for auditors to identify all who have access to data and verify compliance.
Incident Response	In the event of a breach or other failure, data may need to be sealed off by Mandatory Realms irrespective of the direct grants and ownership until authorities can analyze the situation.
Threat Response	If an organization becomes aware of a threat, Mandatory Realms can be turned on quickly to stop all access until the threat has been evaluated.

Controls for Database Configuration

Technical controls can prevent changes that could lead to an insecure database configuration, prevent configuration drift, reduce the possibility of audit findings, and improve compliance. Changes to database structures such as application tables and roles, privileged role grants, and ad hoc creation of new database accounts are just a few examples of configuration drift that can have serious consequences. To prevent these audit findings and to comply with regulations, customers need to put in place strong operational controls inside the database. Oracle Database Vault allows customers to prevent configuration drift by controlling the use of commands such as ALTER SYSTEM, ALTER USER, CREATE USER, DROP USER, etc.

SQL Command Controls with Oracle Database Vault

Oracle Database Vault can be used to control SQL commands that can impact the security and availability of the application and the database. Oracle Database Vault Command Controls introduce an additional layer of rules and checks before any SQL command is executed including CONNECT to the database, DROP TABLE, TRUNCATE TABLE, and DROP TABLESPACE, to name a few. The Command Controls can be used to restrict access to databases to a specific subnet, application server, and program, creating a trusted path from the application to the database. Built-in factors such as IP address, host name, and session user name can be used to enforce SQL Command Controls inside the database. Oracle Label Security factors can also be used to control activity based on the security clearance of the database session. In addition, Oracle APEX applications' native functions and factors can be used with Oracle Database Vault Command Controls to determine whether to allow access to specific DML or DDL statements.

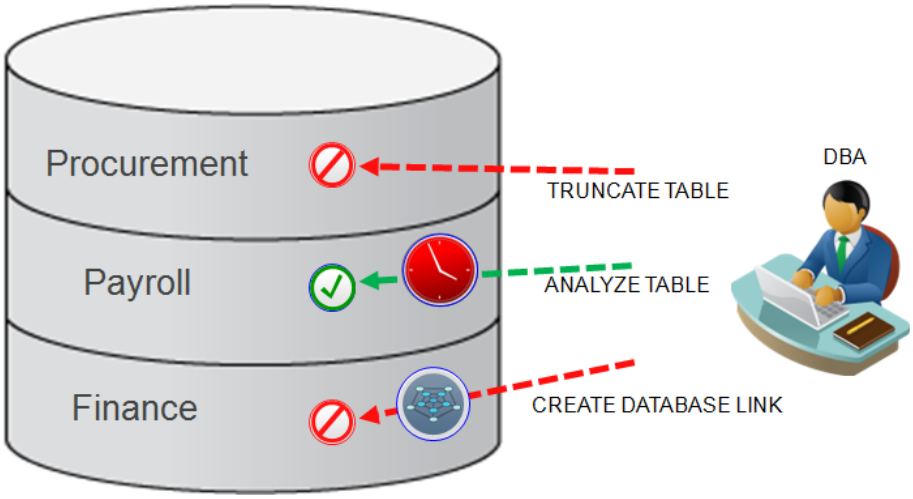

Figure 3. Oracle Database Vault SQL Command Controls

Account Management Controls with Oracle Database Vault

Oracle Database Vault places controls over who can create and manage database accounts and roles inside the database. By default, the ability to create database accounts is removed from existing DBAs and assigned to a new "Database Account Manager" role. This makes it possible to implement separation of duty (SOD) between regular database operations and account management, this increases security for operations such as create user, change password, and alter user. This SOD enforcement control serves as an important safeguard against misuse and the proliferation of powerful database privileges and roles whether granted to users or applications. Organizations can provision the database account management role at their discretion. However, Oracle recommends trusted paths be used to increase security on account management by looking at factors such as IP address, program name and time. In addition, account management activity can be audited and alerted on, if needed.

Database Role Controls with Oracle Database Vault

As roles aggregate privileges and other roles, there are two ways in which they can be misused: granting or revoking roles without authorization, or changing the contents of role itself. Regular Realms protect database roles from being granted by privileged but unauthorized users. Thus only the realm owner can grant the protected roles to other users or roles.

In addition, the new Mandatory Realm feature allows customers to freeze the settings of database roles by preventing any privilege grant or revoke from roles. This ensures that there is no drift in the roles and entitlements configurations inside the database.

Run-time Privilege Analysis with Oracle Database Vault

Oracle Database Vault with Oracle Database 18c includes a feature called Privilege Analysis to further harden the application by identifying unused privileges and roles based upon the actual usage of the roles and privileges by the user or from within the application. Understanding the set of unused roles and privileges is important because it helps identify the least number of privileges the application needs to run there by making the application more secure.

This feature extends the capabilities of Database Vault to include least privilege analysis for existing applications and a continuous analysis of privileges used during new application development. Privilege Analysis allows customers to:

- Report on actual privileges and roles used in the database
- Identify unused privileges and roles by users and applications
- Reduce risk by helping enforce least privilege for users and applications

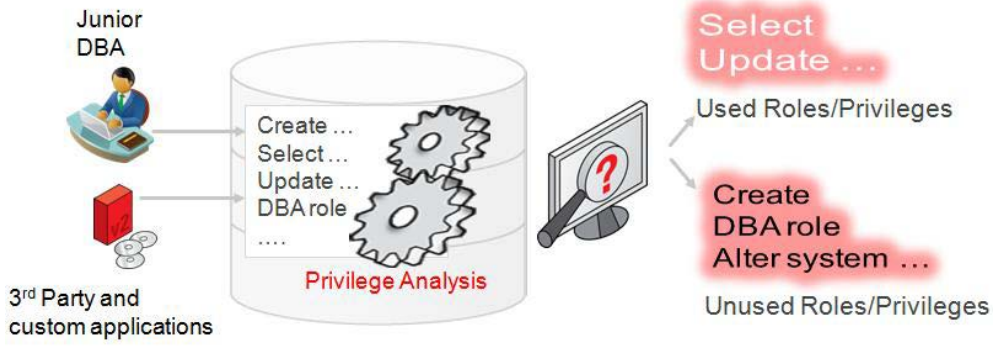

Figure 4. Oracle Database Vault Privilege Analysis

Using the new Privilege Analysis feature, the set of run-time roles and privileges required for specific job functions or application can be determined and then encapsulated within a new database role to be then protected with a Mandatory Realm. Privilege Analysis can also be used as part of the application development process to track privilege use and achieve least privilege for both the application and the users. Unused privileges can be audited to track their use before revoking them from users or roles. Privilege Analysis allows organizations to increase security of existing applications as well as monitor privileges required during the application development process.

Controls for Consolidation and Cloud Environments

Consolidation and cloud environments provide numerous cost and operational efficiencies but also dramatically increase the potential impact of a data breach due to the massive amount of data, applications, and users on the same database. Consolidation intrinsically brings new risks that were not present in single application databases. To keep such consolidated systems up and running 24x7, there may be multiple teams of administrators to manage the system, database, and the application, requiring almost unimpeded access by many privileged users managing the

environment. In addition, a simple administrative error on a single vulnerable application may bring down the entire system, or jeopardize the security of all applications and accounts on that server.

Oracle Database Vault can systematically defend such high value targets through defense-in-depth approach by controlling database commands, restricting account management, and protecting the sensitive application data. Oracle Database Vault Command Controls prevent SQL operations that may modify the database dictionary and configuration, and thus open the database to security vulnerabilities. The Separation of Duty provided by Oracle Database Vault Account Management Controls enforces the roles and responsibilities of the different administrative teams, and minimizes internal threats. In addition to restricting the team of privileged users from accessing sensitive application data, Oracle Database Vault Realms can be placed around an application, preventing other applications within the same database and operating with DBA-like privileges from having the ability to access the application data.

All Oracle Database Vault Controls can be configured and deployed transparently on the Oracle Exadata Database Machine, including the pre-configured out-of-the-box control policies for Oracle and non-Oracle enterprise applications. Oracle Database Vault can be used and deployed with Oracle Advanced Security, and Oracle Audit Vault and Database Firewall to enable a Maximum Security Architecture for the Oracle Exadata Database Machine.

Controls for Oracle Multitenant

Oracle Database Vault secures pluggable databases (PDBs) by allowing customers to create realms around all applications data inside a PDB which prevents access to their sensitive data by the common DBA in the multitenant container database (CDB), the local PDB DBA, and by other PDBs DBAs residing within the same CDB. Oracle Database Vault Command Controls can enforce inside a PDB from where and how the PDB is accessed as well as what operations can be performed within that PDB.

Application Protection Policies

The process of creating Oracle Database Vault policies for custom or commercial applications is a straight forward process. Oracle Enterprise Manager Cloud Control can be used to create a realm around the full application schema or around specific tables with sensitive data. Alternately, a set of PL/SQL packages can also be used to create Realms and Command Rules.

Oracle Database Vault has been certified with numerous Oracle and partner applications. The certification includes out-of-the-box security policies specific for each application taking into consideration their install, run-time, and maintenance requirements. These security policies protect application data from unauthorized privileged users, and provide real-time preventive controls that prevent ad hoc changes to application's data structures.

TABLE 3. ORACLE DATABASE VAULT PROTECTION FOR ENTERPRISE APPLICATIONS

Application	Application-Specific Protection Policy Available?
Oracle Fusion Applications	Yes
Oracle E-Business Suite	Yes
Oracle Peoplesoft	Yes
Oracle JD Edwards Enterprise One	Yes
Oracle Siebel	Yes
Oracle Retail Applications	Yes
Oracle Financial Services	Yes
Oracle Utilities Applications	Yes
Oracle Primavera	Yes
Oracle Enterprise Taxation Management	Yes
SAP Applications running Netweaver 7.0 and higher (ERP, CRM, PLM, SCM, SRM, BW, etc)	Yes
Finacle from Infosys	Yes

Policies for Oracle Applications are available through Oracle Support, or through the Oracle Technology Network and the partner support portals. The policies can also be used as blueprints for designing policies to protect custom applications. The Oracle Database Security team continues to work with Oracle Application groups as well as with partners to provide out of the box policies for additional applications.

Monitoring Oracle Database Vault

Oracle Database Vault Reports can show SQL statements blocked by Oracle Database Vault, and any security policy changes made by an Oracle Database Vault administrator. For example, if a DBA attempts to access data in an application table protected by a realm, Oracle Database Vault prevents that access and creates an audit record for the incident that can be viewed using the Realm Audit Report. Oracle Database Vault reports can also be used to track security administrators' actions and show any changes to Oracle Database Vault configuration.

For Privilege Analysis, out of the box views provide an overview of the runtime analysis and provide insight to the used and un-used privileged and roles. Oracle Database Vault specific reports are available out-of-the-box through Oracle Enterprise Manager Cloud Control, or through Oracle Audit Vault and Database Firewall. In addition to aggregating and reporting on Oracle Database Vault audit events, Oracle Audit Vault and Database Firewall provides a comprehensive overview of activity that includes SQL statements on the network, as well as audit data generated by Oracle and non-Oracle databases, operating systems, and directories.

Deployment and Operational Simplicity

Oracle Database Vault comes installed by default with Oracle Database 18c and can be enabled on the command line. Once enabled, the Oracle database simply needs to be restarted for Oracle Database Vault controls to be in effect. No installation of additional software or re-linking of the Oracle database executable is needed.

Oracle Database Vault enforcement remains with the database even when the database files are exported or restored to a different Oracle home environment. Oracle Database Vault can be deployed with Oracle's Maximum Availability Architecture, including Oracle RAC and Oracle Data Guard.

Oracle Database Vault protects applications data while keeping the DBA fully operational. DBAs can do their regular duties like tuning, backup and recovery as usual. However, Oracle Database Vault does enforce discipline when it comes to administering protected sensitive data. DBAs need authorization before they can export, import or move protected sensitive data. For more details, please refer to the white paper "DBA Administrative Best Practices with Oracle Database Vault" available from the Oracle Database Vault page on the Oracle Technology Network website.

Oracle Database Vault is enforced inside the Oracle Database kernel, providing unparalleled security and very low performance overhead, providing transparency to the performance profile of existing applications. Production customers running Oracle Database Vault on major applications have reported no change in their application response time.

Simulation Mode, introduced with Oracle Database 12cR2 reduces risk when enabling new Database Vault controls in the production environment. Instead of enabling the controls, the controls are put into simulation mode to capture command rule and realm violations in a simulation log instead of blocking the SQL statement. This can be used to more quickly certify an application with new Database Vault controls since the application will be able to complete its regression test without being blocked. New applications can also use simulation mode to identify authorized users, trusted paths and command rules to deploy with the application into production.

Conclusion

Oracle Database Vault creates a robust foundation for secure database operations and application deployment. It protects against internal and external threats targeting intellectual property, privacy related data, and application data. Controls can be pre-configured and enabled to meet increased security requirements. Oracle Database Vault provides support for consolidation and cloud computing, and can be deployed seamlessly with Oracle Exadata and the Oracle Multitenant Database option. Oracle Database Vault preventive controls are designed to be transparent to existing applications and adaptive to existing database administration processes.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

White Paper Title
February 2018
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]