

Oracle Database Vault



KEY FEATURES AND BENEFITS

- Preventive controls to block privileged users and DBAs from accessing sensitive data in the databases
- Enforce operational controls inside the database, lock down the configuration, and prevent audit findings
- Seal off highly sensitive application objects during maintenance periods and in response to cyber threats
- Increase security controls for consolidation, cloud environments, and outsourcing and help comply with regulations from multiple countries
- Identify used and unused privileges and roles with Privilege Analysis
- Application-specific protection policies for enterprise applications including Fusion Applications, E-Business Suite, PeopleSoft, Siebel, and SAP

Oracle Database Vault provides powerful security controls to help protect application data from unauthorized access, and comply with privacy and regulatory requirements. Controls can be deployed to block privileged account access to application data and control sensitive operations inside the database using multi-factor authorization. Security of existing applications can be increased through analysis of privileges and roles. Oracle Database Vault secures existing database environments transparently, eliminating costly and time consuming application changes.

Controls for Privileged Accounts

Privileged database accounts are one of the most commonly used pathways for gaining access to sensitive applications data in the database. While their broad and unrestricted access facilitates database maintenance, the same access also creates a point of attack for gaining access to large amounts of data. Oracle Database Vault Realms around application schemas, sensitive tables and stored procedures provide controls to prevent privileged accounts from being exploited by hackers and insiders to access sensitive application data.

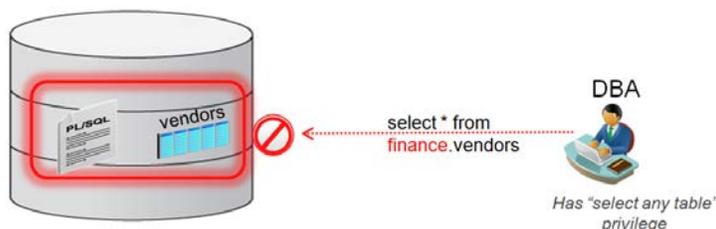


Figure 1. Oracle Database Vault Realms block access from privileged accounts

Controls for Database Configuration

Among the more common audit findings are unauthorized changes to database entitlements, including grants of the DBA role, as well as new accounts and database objects. Preventing unauthorized changes to production environments is important not only for security, but also for compliance as such changes can weaken security and open doors to hackers, violating privacy and compliance regulations. Oracle Database Vault SQL Command Controls allow customers to control operations inside the database, including commands such as create table, truncate table, and create user. Various out-of-the-box factors such as IP address, authentication method, and program name help implement multi-factor authorization to deter attacks leveraging stolen passwords. These controls prevent accidental configuration changes and also prevent hackers and malicious insiders from tampering with applications.

Oracle Database Vault with Oracle Database 12c introduces new Mandatory Realm controls that allow customers to seal off access to application objects, even to those with direct object grants, including the object owner. This is useful when Support must access the application schema directly as the application owner. Mandatory Realms can be enabled at runtime and used in response to a

RELATED PRODUCTS

Oracle Database 12c Defense-in-Depth Security Solutions:

- Oracle Advanced Security
- Oracle Data Masking
- Oracle Label Security
- Oracle Key Vault
- Oracle Audit Vault and Database Firewall

cyber threat, preventing all access until the threat has been analyzed.

Controls for Consolidation and Cloud Environments

Consolidation and cloud environments reduce cost but potentially expose large amounts of sensitive application data to those without a true need-to-know. Data from one country may be hosted in an entirely different country, but access to that data must be restricted based on regulations of the country to which the data belongs. Oracle Database Vault controls provide increased security for these environments by preventing database administrators from accessing the applications data. In addition, controls can be used to help block application bypass and enforce a trusted-path from the application tier to the application data.

Oracle Database Vault provides three distinct separation of duty controls out-of-the-box for security administration, account management, and day-to-day database administration activities. Oracle Database Vault separation of duty controls can be customized and organizations with limited resources can assign multiple Oracle Database Vault responsibilities to the same administrator.

Oracle Database Vault can be used with Oracle Multitenant to provide increased security for consolidation. It can prevent privileged user access inside a pluggable database (PDB) and between the PDB and the common privileged user at the container database.

Run-time Privilege Analysis for Users and Applications

Oracle Database Vault with Oracle Database 12c introduces a new feature called Privilege Analysis which helps increase the security of applications by identifying the actual privileges and roles used at run-time. The additional unused roles and privileges can then be audited or revoked by the security administrators to reduce the attack surface and implement least privilege model. Privilege analysis can also be used on administrators to help limit the roles and privileges they are granted to fulfill their responsibilities.

Enterprise Applications Protection Policies

Application-specific Oracle Database Vault protection policies are available for major enterprise applications including Oracle Fusion Applications, Oracle E-Business Suite, Oracle PeopleSoft, Oracle Siebel, Oracle Financial Services (i-Flex), Oracle Primavera, SAP, and Finacle from Infosys.

Manageability

Oracle Database Vault with Oracle Database 12c comes pre-installed by default and can be enabled easily. Oracle Database Vault administration is fully integrated with Oracle Enterprise Manager Cloud Control, providing Security Administrators with a streamlined and centralized interface to manage Oracle Database Vault.



CONTACT US

For more information about Oracle Database Vault, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

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

Hardware and Software, Engineered to Work Together

Copyright © 2015, 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0115



Oracle is committed to developing practices and products that help protect the environment