ORACLE

Oracle Database Vault

Built into the Oracle Database, Database Vault provides controls to limit unauthorized privileged users from accessing sensitive data, limit unauthorized database changes, and help customers meet industry, regulatory, and corporate security standards.

April, 2025, Version 23ai

ORACLE

Purpose

This document provides an overview of the features and capabilities of Database Vault for Oracle Database. It is intended solely to help you assess the business benefits of upgrading to Database Vault for Oracle Database and planning for the implementation and upgrade of the product features described.

Introduction

Regulations, industry directives, and numerous breach disclosure laws require stronger security controls, including the separation of duties. Privacy and regulatory challenges are becoming increasingly complicated as access to data is controlled based on laws spanning multiple countries. In parallel, database attacks 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 have 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 encompassing preventive, detective, and administrative controls. Database Vault strengthens Oracle's industry-leading database security solution by providing essential security controls.

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

- Threats that exploit stolen credentials obtained from social engineering, keyloggers, and other mechanisms to get access to privileged accounts in your database.
- Threats from insiders who misuse privileged accounts to access sensitive data or 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 day.
- Threats from unintended mistakes from unauthorized SQL commands that change the database configuration and put the database in a vulnerable state.
- Threats to sensitive data during maintenance windows from the application administrators.
- Threats that exploit weaknesses in the application to escalate privileges and attack other applications on the same database.

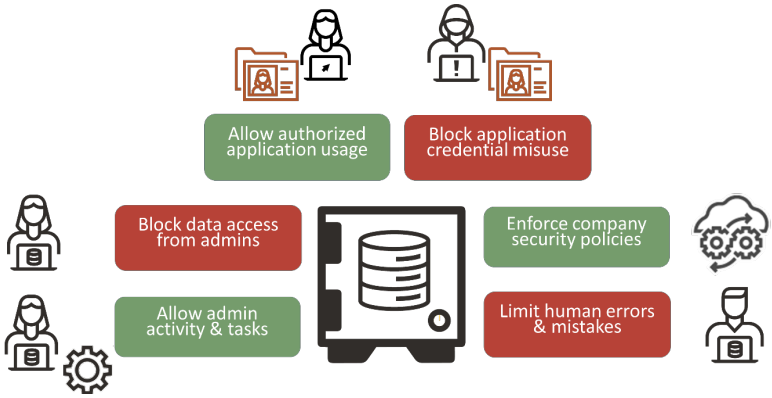

Figure 1 - Database Vault common use-cases

Deployment and operational simplicity

Database Vault is built into the kernel of the Oracle Database and can be enabled using the command line. Once enabled, the Oracle Database must be restarted for Database Vault controls to be in effect. No additional software installation or re-linking of the Oracle database executable is needed.

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

Database Vault protects application data while keeping the DBA fully operational. DBAs can perform their regular duties, such as tuning, diagnostics, backup, and recovery. However, Database Vault does enforce discipline when administering or accessing protected sensitive data.

DBAs need authorization before they can export, import, or move protected sensitive data. Database Vault policies are enforced inside the Oracle Database kernel, providing unparalleled security, minimal overhead, and transparency to existing applications' performance profiles.

Simulation Mode 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 rules and realm violations in a simulation log instead of blocking the SQL statement. This allows users to 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.

Controls for privileged accounts

Privileged database user accounts are commonplace 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 predefined database users and roles can access any application data in the database. Due to their wide-ranging access, most organizations enforce strict processes and internal rules regarding who can be granted privileged access to the database. These accounts and roles, however, have also been a prime target of hackers because of their unimpeded access inside the database. Privileged access can also be misused by insiders to gain access to confidential information.

Privilege user access controls with realms

Increasing controls on privileged and DBA accounts is vital to improving security. Database Vault creates a highly restricted application environment ("realm") inside the Oracle Database that prevents access to application data from privileged accounts while allowing authorized administrative activities on the database. Realms can be placed around all or specific application objects, such as tables or entire schemas, to protect them from unauthorized access while allowing authorized users to access those tables and schemas. Database Vault realms can enable access to those who have been granted direct access to the protected objects or limit access to only those who have been granted specific authorization through the realm.

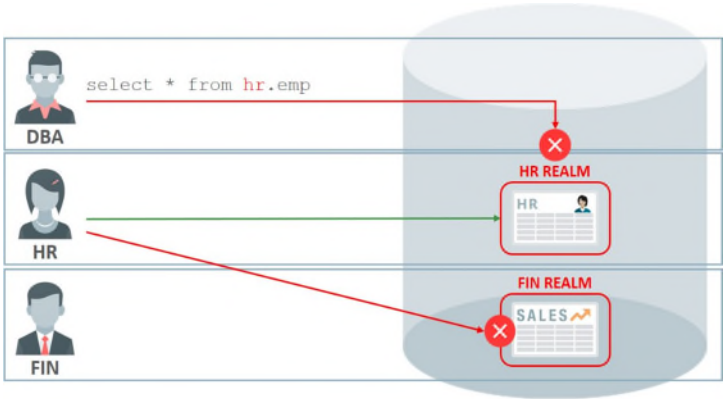

Figure 2 - Oracle Database Vault separation of duties and realm protection

USE CASE	DESCRIPTION
Prevent unauthorized access to application data	Realms help customers comply with data access regulations and protect from outsider attacks exploiting compromised DBA accounts and insider threats.
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 a higher level of security assurance for their customers.
Enable secure outsourcing	Controlling access to sensitive data, even by administrative staff, allows customers to take advantage of the cost benefits of outsourcing backend operations.
Reduce risks caused by accidents or mistakes	SQL command rules can disable destructive operations that might be accidentally executed against a production database or run at inopportune times, such as during business hours. They can also prevent even the application database user account from running commands such as TRUNCATE TABLE, DROP TABLE, DROP INDEX, or ALTER INDEX.

Database Vault realms also control powerful system privileges, roles, and account management. In addition, they restrict access to security-related packages commonly used by applications, such as the Virtual Private Database (VPD) and Oracle Label Security (OLS) packages. For example, Database Vault limits who can manage VPD and Label Security policies, increasing the overall security of applications that use these features.

Stronger authorization controls with mandatory realms

While regular Database Vault realms protect access to sensitive data from broad system privileges like SELECT ANY TABLE, a Database Vault mandatory realm also protects against direct object privileges. When using a Database Vault mandatory realm, even schema owners would be blocked from accessing their objects unless authorized to the mandatory realm. This simplifies finding the list of users who are authorized to access the realm-protected data, so the security officer doesn't have to worry about schema owners and others with direct object privileges from granting these same privileges to other users.

Further, you can enhance the security controls of a Database Vault mandatory realm by adding a Database Vault rule set to a user's authorization. You can create rules that identify where, and how, an application schema accesses its objects or data and limit it to only that connection path – a trusted application path. For example, several administrators or developers might know the password to the HR database schema account, but they should not use this password to access or modify objects or data. You can use a Database Vault mandatory realm to limit HR to only be able to access its objects from a list of application server hostnames, IP addresses, or a CIDR block. This can help protect your application credentials from being misused or abused, even if the password is known.

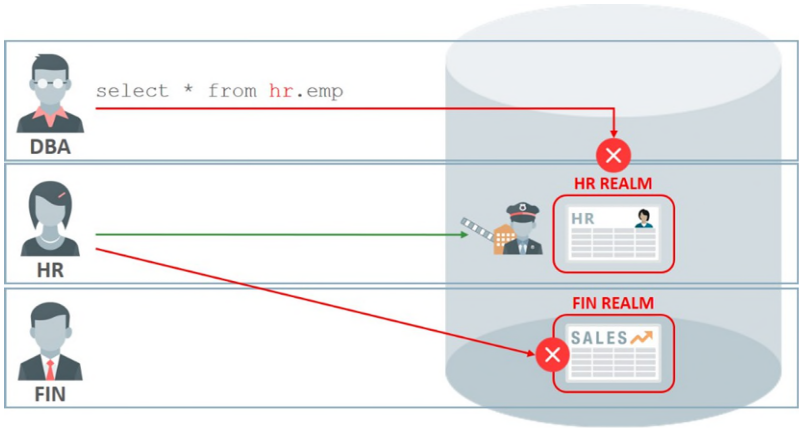

Figure 3 - Limit how, when, or where the HR database account can authenticate.

Controls for database configuration

Changes to database configuration may lead to insecure database configuration, configuration drift, or the possibility of audit findings. 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 or auditable events that can have serious consequences. To limit such change, customers should put in place strong operational controls inside the database. Database Vault allows customers to prevent configuration drift by controlling commands such as ALTER SYSTEM, ALTER USER, CREATE USER, DROP USER, etc.

SQL command controls with Database Vault

Database Vault can control SQL commands that can impact the security and availability of the application and the database. Database Vault command rules 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 rules can restrict database access 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, hostname, and session username 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 user's session. In addition, Oracle APEX includes native functions and factors that can be used with Database Vault command rules to determine whether to allow access to specific DML or DDL statements.

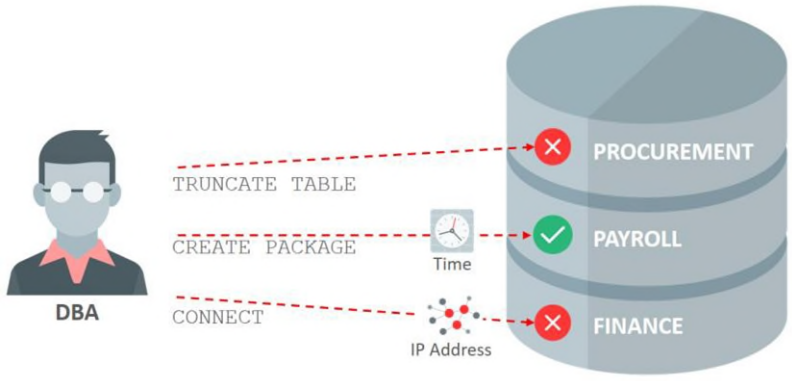

Figure 4 - Oracle Database Vault command rules & trusted paths

Account management controls with Database Vault

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 managers who are responsible for operations such as creating or altering users and changing user passwords. This SOD enforcement control serves as an essential 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 should be audited and may be alerted on, if needed.

Database role controls with Database Vault

Roles aggregate privileges, which can be misused in two ways: granting or revoking roles without authorization or changing their contents. Realms protect database roles from being granted by privileged but unauthorized users. If a realm protects a role, only the realm owner can grant the protected role to other users or roles.

In addition, realms allow customers to freeze the settings of database roles by preventing any privilege granted or revoked from roles. This ensures that the roles and entitlements configurations inside the database do not drift.

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 manage such consolidated systems, there may be multiple teams of administrators to manage the system, database, and application, requiring almost unimpeded access by many privileged users managing the environment. In addition, a simple administrative error on a single application may bring down the entire system or jeopardize the security of all applications and accounts on that server.

Database Vault can defend such high-value targets through a defense-in-depth approach by controlling database commands, restricting account management, and protecting sensitive application data. All Database

Vault controls can be configured and deployed transparently, including the pre-configured out-of-the-box control policies for Oracle and non-Oracle enterprise applications. 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, Autonomous Database, Oracle Base Database Services, Exadata Cloud@Customer, Exadata Cloud Services, and Oracle Database in multicloud environments.

Controls for Oracle Multitenant

Database Vault secures pluggable databases (PDBs) by allowing customers to create realms around the sensitive application 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. Database Vault command rules can be enforced from within a PDB from where and how the PDB is accessed as well as what operations can be performed within that PDB.

Operations Control, introduced in Database Vault 23ai, transparently prevents common user access to local PDB data without having to configure and enable Database Vault in every PDB. This control is suited for cloud operations and consolidated customer multitenant databases where an infrastructure DBA team manages the fleet of PDBs from the CDB using common user accounts.

This allows sensitive local PDB data to be protected without the PDB administrator having to enable Database Vault in the PDB and configure realms to protect local data.

Controls for Oracle Cloud and multicloud environments

As Database Vault is built into the kernel of the Oracle Database, it is available anywhere you can run Oracle Database Enterprise Edition, including Oracle Exadata, Autonomous Database, Oracle Base Database Services, Exadata Database Service, and Oracle Database in multicloud environments. In Oracle Autonomous Database, Database Vault is enabled in the container database by default, allowing customers to enable it on the ADB environment to protect their data from their privileged users, administrators, and cloud administrators.

Database kernel-resident SQL Firewall

SQL Firewall is a new capability in Oracle Database 23ai. SQL Firewall is built into the Oracle Database kernel, operating closer to where data resides, eliminating the possibility of bypassing the control. SQL Firewall inspects all incoming SQL statements and helps ensure the database executes only explicitly authorized SQLs coming from trusted database connection paths. It can examine all SQL statements - whether local or over the network, encrypted or clear text. Unlike regular expression-based pattern-matching protection mechanisms, SQL Firewall cannot be bypassed by encoding the SQL statement, referencing synonyms, or using dynamically generated object names.

SQL Firewall and Database Vault pair well together. With Database Vault, you can secure data from privileged users and create allowed lists of known-good SQL statements with SQL Firewall. Database Vault limits who can manage SQL Firewall operations, such as applying or modifying policies. For more information on SQL Firewall, please see the Oracle SQL Firewall User's Guide at https://docs.oracle.com.

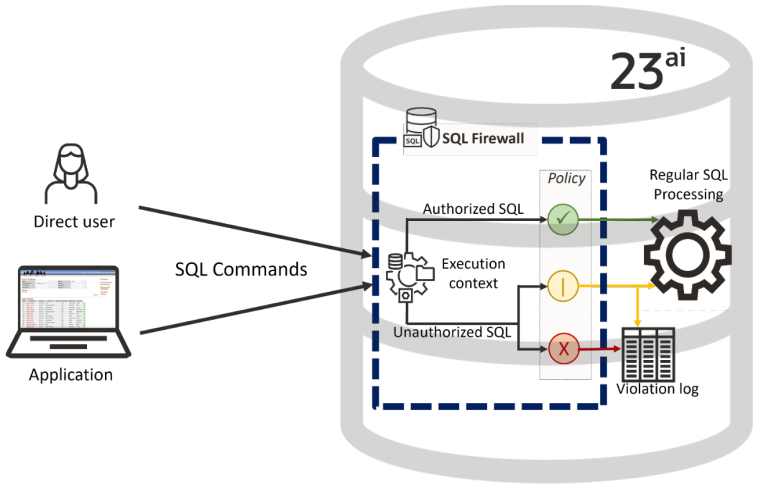

Figure 5 - Oracle SQL Firewall is built into Oracle Database 23ai

Application protection policies

Creating Database Vault controls for custom or commercial applications is straightforward. Oracle Enterprise Manager Cloud Control can be used to create a Database Vault realm around the full application schema or around specific tables with sensitive data based on your security and application design. Alternately, a set of PL/SQL packages can also be used to create realms and command rules.

Database Vault has been certified or supported with numerous Oracle and partner applications. Certifications include out-of-the-box security policies specific to applications, taking into consideration their installation, 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 the application's data structures.

Enterprise Applications supporting Database Vault include, but are not limited to:

- Oracle Fusion Applications
- Oracle E-Business Suite
- Oracle PeopleSoft
- Oracle JD Edwards Enterprise One
- Oracle Siebel
- Oracle Retail Applications
- Oracle Financial Services
- Oracle Utilities Applications
- Oracle Primavera
- Oracle Enterprise Taxation Management
- SAP Applications
- Infosys Finacle

Many policies and guidelines for Oracle applications are available through Oracle Support 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 and partners to provide policies and guidelines for additional applications.

Monitoring Database Vault

Database Vault audit records show SQL statements blocked by Database Vault realms or command rules, and any security policy changes made by a Database Vault administrator. For example, if a DBA attempts to access data in an application table protected by a realm or command rule, Database Vault prevents that access and creates an audit record for the incident that can be viewed using the realm audit report. Database Vault reports can also be used to track security administrators' actions and show any changes to Database Vault configuration. In Oracle Database 23ai, the unified audit trail is protected by Database Vault, and access to view audit records, or create or manage audit policies, can be strictly limited to only database users with Database Vault audit viewer or audit admin authorization.

Database Vault-specific reports are available out-of-the-box through Oracle Enterprise Manager Cloud Control, Oracle Audit Vault and Database Firewall, and Oracle Data Safe.

Conclusion

Database Vault creates a robust foundation for secure database operations and application deployment. It protects sensitive data like intellectual property, privacy data, and application data from external attackers and insider threats. Controls can be pre-configured and enabled to meet increased security requirements. Database Vault provides support for consolidation and cloud computing and can be deployed seamlessly with Oralce Database on-premises, Oracle Exadata, Autonomous Database, Oracle Base Database Services, Exadata Cloud Services, and Oracle Database in multicloud environments. Database Vault preventive controls are designed to be transparent to existing applications and adaptive to existing database administration processes.

For more details, please refer to the *Oracle Database Vault Administrator's Guide* or the *Oracle Database Vault Getting Started Guide* at https://docs.oracle.com.