ORACLE

ORACLE Database 23ai

Oracle Database Vault

Oracle Database Vault provides robust security controls to protect sensitive data from unauthorized access and enables separation of duties between database administrators and data owners to help address privacy and regulatory requirements. Database Vault controls block privileged accounts from accessing application data, and command rules restrict when administrative users can perform sensitive operations inside the database. A trusted path limits client connections based on the originating IP address, client application, OS user, or other factors. Oracle Database Vault secures existing database environments transparently, eliminating costly and time-consuming application changes.

Key Business Benefits

- Enables segregation of duties, helps users protect sensitive data, and provides an easy, cost-efficient route for addressing requirements associated with regulations such as PCI-DSS, HIPAA, and EU GDPR.
- Compatible with enterprise business applications such as Oracle E-Business Suite, Oracle PeopleSoft, Oracle Siebel, SAP, and more.
- Adds additional security to existing privileges and roles, allowing you to restrict access based on IP address, subnet, hostname, client program name, and much more.
- Limits the use of application credentials to specific contexts, such as client IP address, IP subnet, or hostnames, reducing the risk stolen credentials pose to your sensitive data.
- Restricts privileged users from using their privileges on application data through Database Vault realms or command rules.
- Helps minimize outages and data loss due to human error by allowing you to restrict the use of almost any database command, such as potentially destructive DDL commands (DROP TABLE, DROP INDEX, DROP USER, etc.).
- Improves governance by enforcing policies and procedures as technical controls in the Oracle Database.
- Enables secure data isolation in Oracle Multitenant environments by separating container database administrators from data in an Oracle pluggable database.
- Application-specific protection policies and guidelines are available for Oracle E-Business Suite and SAP.

Controls for database configuration

Among the most common audit findings are changes to database entitlements, including grants of the DBA role and unauthorized accounts and database objects. Preventing unauthorized changes to production environments is essential for security and compliance, as these changes can weaken security and open doors to hackers, violating privacy and compliance regulations.

Separation of duties

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

Minimize human mistakes

In many cases, unauthorized changes aren't malicious but result from human error. Whether intentional or accidental, unauthorized changes can cause production database outages or damage production data. Oracle Database Vault command rules allow customers to control operations inside the database, including commands such as `alter database`, `alter system`, `drop table`, `truncate table`, and `drop user`. These controls prevent hackers, malicious insiders, and human errors from tampering with or making application changes.

Validate controls with simulation mode

Before implementing Database Vault security controls, customers can swiftly validate them with their applications using simulation mode. Simulation mode captures security violations instead of blocking them, allowing a single regression test to capture the required security changes without blocking legitimate production activity. Simulation mode lets customers quickly deploy new security controls into production without compromising operations.

Operations control

Database consolidation on Oracle Multitenant benefits from increased security with Database Vault operations control. Operations control transparently prevents container database administrators from accessing application data in pluggable databases. Oracle Database Vault operations control even applies to pluggable databases that do not have Database Vault configured or installed. When used with PDB lockdown profiles that prevent PDB users from impacting other PDBs, customers have the critical controls they need to help protect their application data in a managed, multitenant environment.

Manageability

Oracle Database Vault is built into the database kernel of all supported Oracle Database versions and can be enabled easily. Oracle Database Vault administration integrates with Oracle Enterprise Manager Cloud Control, providing security administrators a streamlined and centralized interface to manage Oracle Database VaultSecurity management can be delegated to domain security experts for expertise and to meet requirements for separation of duties.

Related products

Oracle Database 23ai defense-in-depth solutions

- Oracle Key Vault
- Oracle Database Vault
- Oracle Label Security
- Oracle Data Masking and Subsetting Pack
- Oracle Audit Vault and Database Firewall
- Oracle Data Safe

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

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