ORACLE DATABASE 12c

Oracle Database 12c Release 2 Security and Compliance

Defense-in-Depth Database Security for On-Premises and Cloud Databases

ORACLE WHITE PAPER | APRIL 2017

ORACLE

Table of Contents

Introduction

The need to secure data is driven by an expanding privacy and regulatory environment coupled with an increasingly dangerous world of hackers, insider threats, organized crime, and other groups intent on stealing valuable data. The security picture is complicated even more by the rapid expansion of access to sensitive data via the Internet, an unprecedented understanding of technology, increasing economic competition, and the push to achieve greater efficiencies through consolidation and cloud computing. Information targeted for attack has included citizen data, intellectual property, credit card data, financial information, government data, and competitive bids. Attack methodologies include hacking of privileged user accounts, exploitation of application vulnerabilities, media theft, and other sophisticated attacks collectively known as advanced persistent threats or APT. In response to the increasing threat to data, regulations have been put in place that include the numerous U.S. State privacy laws, Payment Card Industry Data Security Standard (PCI-DSS), the U.K Data Protection Act, the European Union's General Data Protection Regulation (GDPR), and the Korean Act on Protection of Personal Data, to name a few.

To better understand the importance of database security one needs to consider the potential sources of vulnerability.

- Threats that target the operating system can circumvent the database by accessing raw data files, bypassing application security, access controls inside the database, network security, and encrypted drives.
- Proliferation of production data beyond the controls of the production environment expand the scope of compliance and increase the risk to data.
- Privacy related information can be exposed to individuals without a true need-to-know due to an oversight in the development process or the complexity of modifying legacy applications.
- Privileged user accounts and over privileged applications may become targets for highly specialized attacks or the source of insider threats.
- Ad-hoc access to application data by privileged accounts may violate internal policies, regulatory mandates, service level agreements, as well as expose data to external attacks.
- Application bypass through SQL injection can expose large amounts of sensitive data to attackers or unauthorized users.
- Configuration drift or changes that create deviation from internal deployment standards and security best practices can result in audit findings, impact business continuity, and increase security risks.

Oracle Database 12c Security

Security and compliance requires a defense-in-depth, multi-layered, security model that includes preventive, detective, and administrative controls. Controls should be aligned with the sensitivity of the data, its location, its environment, and applicable regulations. Additional consideration should be given to the business impact should the data be lost, stolen, or used for unauthorized purposes. Oracle Database 12c Release 2 (12.2), the latest generation of the world's most popular database, is available for deployment on premises and in the Oracle Cloud. With Oracle Database 12c Release 2, Oracle continues to lead the industry with the most complete solution set for securing business-critical data throughout the data lifecycle.

Oracle Database 12c security, combined with the Oracle Audit Vault and Database Firewall and Oracle Key Vault solutions, provide unprecedented capabilities to protect data and defend against cyber threats. Deploying and managing Oracle Database 12c security is easy with simplified setup and configuration as well as a new security menu in Oracle Enterprise Manager 12c. Oracle Database 12c introduces a wealth of security enhancements and new features including conditional auditing, privilege analysis, data redaction, enhanced encryption key management, real application security, mandatory realms, and performance optimizations to name a few. Fully integrated with Oracle Multitenant, security controls can be customized for individual pluggable databases.

Oracle Database 12c security enables four pillars of security controls to meet the need for a multilayered defense-in-depth data security strategy. These pillars enable customers to

- **Evaluate** the security posture and potential risks to their applications
- **Prevent** on authorized access to data
- **Detect** the various activities which can be indicative of data breach
- Leverage **Data-Driven Security** to secure data at the source

The remainder of this paper will examine the Oracle Database 12c features which enable these security pillars for data security.

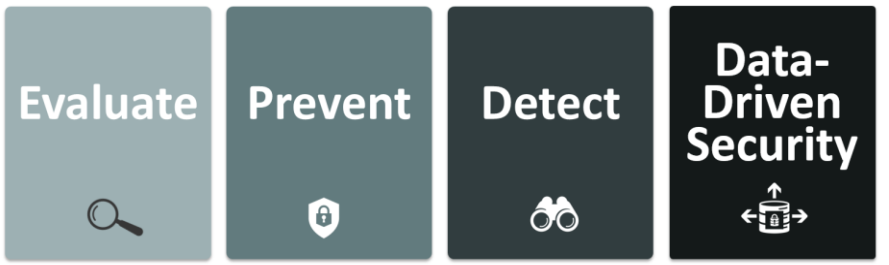

Figure 1. Security controls available for Oracle Databases can be organized into four pillars.

Evaluating Security Risks

To implement a database security strategy, you first need a thorough understanding of the risks associated with the data assets in your organization. Factors which influence these risks include:

- Sensitivity of the data under management in various databases
- Threats to the data from a variety of potential sources

» Possible vulnerabilities to databases due to improper deployment, configuration, user rights administration or maintenance

Features in the "Evaluate" pillar enable administrators to implement a risk-based approach to security. These kinds of controls can catch security miss configurations, inadvertent privilege escalations, and potential misuse by over privileged accounts.

Knowing Where Sensitive Data Resides with Sensitive Data Discovery

Knowing where your sensitive data resides is an important first step in deploying a defense-in-depth security model. Identifying sensitive databases based on the types of applications they support is a common method used to classify databases. However, it is also valuable to understand the level of sensitivity of the data under management in various applications. Knowing where specific types of data reside can be challenging due to the complexity and size of large applications.

Oracle Enterprise Manager Data Discovery and Modeling and Sensitive Data Discovery (SDD) can be used to automate the process of locating sensitive data within an application schema. This information can provide organizations with a better understanding of which data assets require higher levels of security controls. In addition, the results from an SDD analysis can be used with Oracle Data Masking and Subsetting and other database security solutions to identify and protect sensitive data.

Oracle has created Application Accelerators for Oracle Fusion Applications and Oracle E-Business Suite to reduce the time it takes to implement data masking solutions. Application Accelerators list the sensitive data for each of the applications. Oracle Data Masking and Subsetting uses the Application Accelerators to facilitate masking of data from production databases to test and development environments. In addition, the new Oracle Database 12c feature Transparent Sensitive Data Protection (TSDP) can leverage information from Oracle Enterprise Manager Data Discovery and Modeling to apply security controls such as Oracle Advanced Security Data Redaction.

Reducing the Attack Surface with Role and Privilege Analysis

Over privileged user accounts is a common vulnerability that hackers can seek to exploit. To prevent this, implementers should apply a least privilege model to all user accounts, providing users with only the rights they require to run their applications and get their jobs done. One challenge with applying this principle to database applications, however, is in understanding exactly which rights are required by complex enterprise applications. As a result, implementers often default to granting broad data access rights to application users.

Oracle Database Vault with Oracle Database 12c introduces the capability to perform user privilege analysis. Oracle Database Vault privilege analysis helps increase the security of applications by identifying the actual privileges in use by a database user at run-time. Privileges identified as unused can be evaluated for potential revocation, helping reduce the attack surface and achieve a least privilege model. Privilege analysis can be integrated into the application development process, helping create more secure applications. It can also be used to analyze entitlement requirements for common database administration tasks.

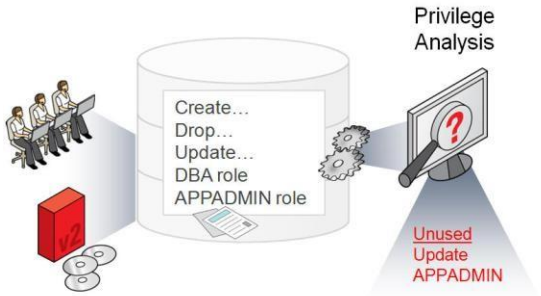

Figure 2. Oracle Database Vault privilege analysis identifies the privileges required by database users at run-time.

Oracle Database Vault with Oracle Database 12c comes pre-installed by default and can be easily enabled. In addition, Oracle Database Vault administration is fully integrated with Oracle Enterprise Manager Cloud Control, providing Security Administrators with streamlined and centralized management across their hybrid cloud datacenter.

Evaluating the Database Security Posture with Database Security Assessment

In order to provide a secure repository for data, databases must be deployed and configured appropriately. Database vulnerabilities can arise from misconfigured or inactive user account, unencrypted data, insufficient access controls, lack of audit policies and incorrect OS-level file permissions to name a few. These risks are compounded in environments that implement replication for high-availability, consolidate data from a variety of applications into a single database, or support legacy applications.

The Oracle Database Security Assessment Tool (DBSAT) is an application which automatically checks a number of database configurations. These include information regarding user accounts privileges and roles, authorization controls, data encryption, fine-grained access control, auditing policy, database configuration, listener configuration, and OS file permissions. DBSAT incorporates 71 security rules in total spanning various aspects of database configuration. The tool runs against the Oracle database and collects information regarding configurations into a configuration file. The DBSAT reporter then generates a report for analysts and administrators summarizing a number of security findings. The output from DBSAT includes a summary of scores for each of the rules, as well as an indication of the relative degree of risk found with the configuration as well as suggestions for areas where configuration security can be improved.

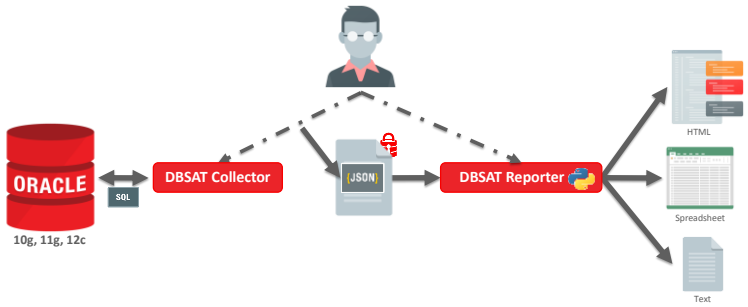

Figure 3. The Database Security Assessment Tool (DBSAT) incorporates a collector which gathers findings, as well as a reporter which presents the findings to the user.

Monitoring the Database Configurations with Enterprise Manager

Preventing and detecting configuration drift increases business continuity, high availability, and security. Oracle Enterprise Manager Database Lifecycle Management Pack can be used to scan databases for numerous security related settings, including checks for account default passwords, account status, and account profiles. Over 100 out-of-the-box policy checks can be easily run against existing databases. In addition, custom configuration checks can be defined to supplement those provided by Oracle.

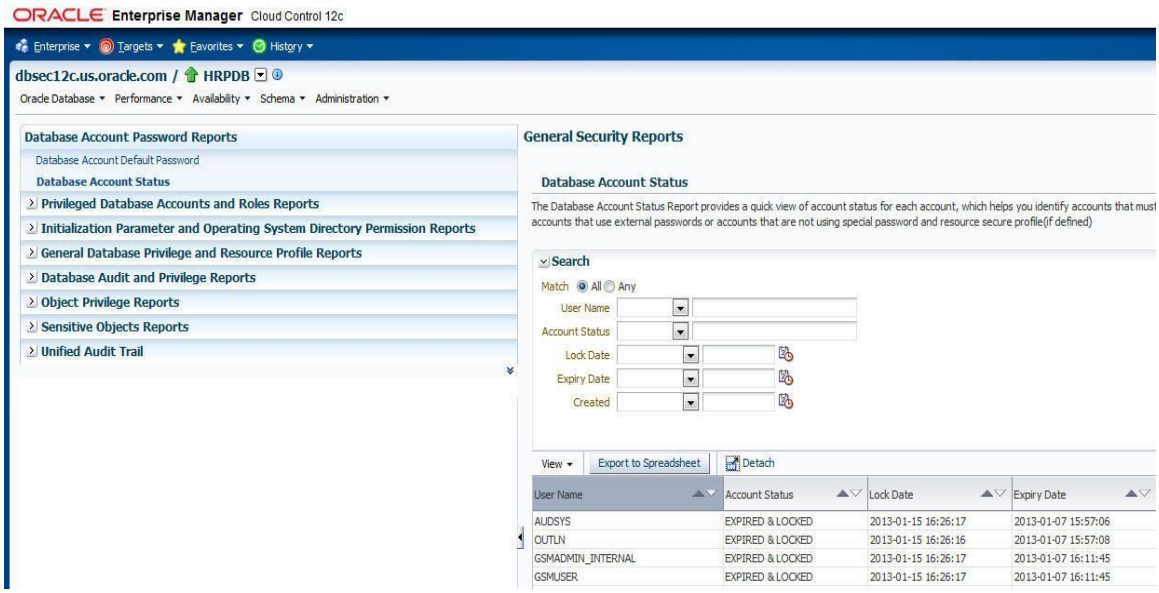

Figure 4. Oracle Enterprise Manager Security Configuration Reports can help compliance reporting and maintain database security hygiene.

Preventing Unauthorized Access to Data

As part of the evaluation phase, customers have identified sensitive data. Now customers need to apply security controls to prevent damage to databases from attacks.

The prevent pillar aims to prevent the loss of data even in the event of an attack or breach. Many of the potential threats mitigated by the prevent pillar include OS level attacks and temp files, misuse of stolen privileged accounts, risks of data support exposure to customer service, support and other users, potential threats against test, development, and staging systems and risk of exposure of data to development or test.

Preventing Database Bypass with Transparent Data Encryption

Database bypass threats target operating system files and backup media. Targeting these locations simplifies the job of the attacker. No database access is required, fewer audit records, if any, are generated, and any associated database as well application access controls are completely bypassed. One of the most widely used technologies used to protect against database bypass threats is encryption. A key driver in the widespread recognition of encryption technologies came in 2003 with the passage of California Senate Bill 1386 (SB1386). SB1386 introduced the topic of encryption to a broad audience by including a provision that removed the notification requirement if the breached data was encrypted. Today the need to protect privacy-related information is a global issue as companies expand their operations and businesses. In addition to privacy laws, the payment card industry data security standard (PCI-DSS), first introduced in 2006, has raised awareness across the board for security and the need to render cardholder data unreadable where it is stored and transmitted.

While encryption of backup media and proper disposal of media are probably the two most well understood security controls, increasingly sophisticated attacks have focused on attacking the servers themselves and gaining access to the raw data files that hold sensitive information. Oracle Advanced Security with Oracle Database 12c delivers industry leading encryption with transparent data encryption (TDE) and data redaction capabilities, vital to protecting sensitive application data. TDE helps prevent unauthorized access to sensitive information via direct access to the operating system, backup media, or database exports. Sensitive data such as credit card information or social security numbers can be automatically encrypted in storage.

TDE safeguards sensitive data against unauthorized access from outside of the database environment by encrypting data at rest. It prevents privileged and unauthorized operating system users from directly accessing sensitive information in database files. TDE also protects against theft, loss, or improper decommissioning of database storage media and backups.

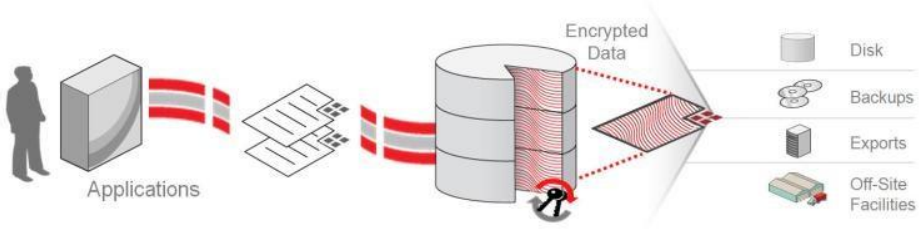

Figure 5. Oracle Advanced Security Transparent Data Encryption (TDE) prevents data loss through application bypass and provides data confidentially control throughout the data lifecycle.

The solution is transparent to applications because data is encrypted automatically when written to storage and decrypted when read from storage. Access controls that are enforced at the database and application layers remain in effect. SQL queries are never altered, and no application code or configuration changes are required. The encryption and decryption process is extremely fast because TDE leverages Oracle Database caching optimizations. In addition, TDE utilizes CPU-based hardware acceleration in Intel® AES-NI and Oracle SPARC T-Series platforms, including Oracle Exadata and SPARC SuperCluster. TDE further benefits from Exadata Smart Scans, rapidly decrypting data in parallel on multiple storage cells, and from Exadata Hybrid Columnar Compression, reducing the total number of cryptographic operations performed.

TDE provides a two-tier encryption key management architecture consisting of data encryption keys and master encryption keys. The master keys are stored outside of the database in an Oracle Wallet. Built-in key management functionality provides assisted key rotation without re-encrypting all of the data and management of keys across their lifecycle. TDE can be deployed easily and is installed by default as part of the database installation. Existing data can be encrypted with zero downtime on production systems using Oracle Online Table Redefinition or encrypted offline during a maintenance period. Additionally, TDE works out of the box with Oracle Automatic Storage Management.

Scaling Transparent Data Encryption with Oracle Key Vault

Oracle Key Vault (OKV) enables customers to quickly deploy encryption and other security solutions by centrally managing encryption keys, Oracle wallets, Java keystores, and credential files. It is optimized for managing Oracle Advanced Security TDE master keys. The full-stack, security-hardened software appliance uses Oracle Linux and Oracle Database technology for security, availability, and scalability. A browser-based management console makes it easy to administer OKV, provision server endpoints, securely manage key groups, and report on access to keys. Administrator roles can be divided into key, system, and audit management functions for separation of duties. Additional users with operation responsibilities for server endpoints can be granted access to their keys and wallets for ease of management.

Figure 6. Overview of Oracle Key Vault

Limiting Privileged User Access with Database Vault

A common characteristic of many cyber-attacks and data breaches has been the use of privileged user credentials and their far-reaching access inside the database. Some of these data breaches were perpetrated by insiders, while others were executed by hackers. Privileged user accounts inside the database and their unimpeded 24/7 access to application data create prime targets for hackers and exploitation by insiders. Protecting against attacks requires a defense-in-depth approach. The depth of the security controls required will depend on the application and sensitivity of the data. For example, while privileged user controls may be vital on production systems, they most likely are

less applicable on test and development systems where sensitive data has been masked or swapped out with production “like” data. At the same time, multiple preventive controls may be applicable on highly sensitive systems, while a subset may be applicable on less sensitive systems.

Oracle Database Vault SQL Command Controls allow customers to control operations inside the database, preventing unauthorized changes to production environments that may impact both the security posture and compliance. Unauthorized changes can significantly weaken database security, result in audit findings, compliance violations, and result in data breaches. SQL command controls allow potentially dangerous operations to be blocked altogether or allow verification checks such out-of-the-box factors such as IP address, authentication method, and program name. SQL command controls can be configured for commands such as database connect, create table, truncate table, create directory, create database link, and create user, to name a few. These controls prevent accidental configuration changes and also prevent hackers and malicious insiders from tampering with applications.

Oracle Database Vault helps prevent data breaches and increase the security of the database overall using privileged user controls, configuration controls, and separation of duty controls. These powerful controls can be configured to create a highly secure database environment, helping defend against attacks from both inside and outside the organization and prevent unauthorized changes that may lead to audit findings or open doors to hackers.

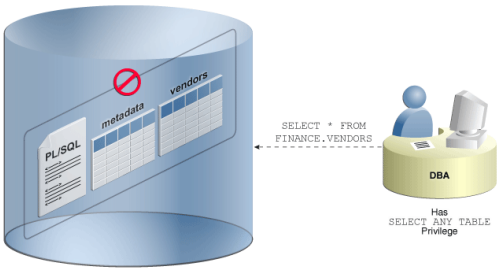

Figure 5. Oracle Database Vault Realms block access from privileged accounts

Oracle Database Vault realms prevent ad hoc access to application data by privileged accounts. Enforced inside the Oracle database kernel, attempts to access realm protected data are blocked and audited. Monitoring these Database Vault audit records can provide an important early indicator of potential malicious activity. Oracle Database Vault with Oracle Database 12c introduces even more powerful controls that can be used to seal off access to application objects and lock down privileged granted to roles. Known as a Mandatory Realm, this powerful security capability can be used as an additional gate check prior to allowing access by both privileged as well as traditional users, including the object owner. Mandatory realms can also be used to protect sensitive information when direct access to the application schema is required for maintenance operations or as a temporary lockdown in response to an active cyber threat. Mandatory realms, like traditional realms, can be pre-configured and enabled with a single command by the database security administrator.

Consolidation and cloud environments reduce cost but potentially expose large amounts of sensitive application data to those without a true need-to-know. Oracle Database Vault controls provide increased security for these environments. 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 while retaining the security restrictions on access to application data.

Protecting sensitive data in applications with data redaction

Limiting the distribution of and access to sensitive data is a well understood security principle. What has changed, however, is the realization that much tighter controls can be put in place on access to sensitive data without adversely impacting business operations. The goal being to reduce the attack surface by stopping the unnecessary proliferation of sensitive data beyond the boundaries of the consolidated database. The proliferation could be in the form of poorly designed applications that display sensitive data, copies of production data transferred to test and development environments, or shared with business partners. Regardless of the proliferation path, over exposure of sensitive data makes it easier for data breaches and other access violations to take place and go undetected.

Oracle Advanced Security data redaction provides selective, on-the-fly redaction of sensitive data in query results prior to display by applications. Redaction is the process of scrubbing out data. Imagine a paper document with certain fields scratched out with a black marker. Oracle Advanced Security data redaction works similarly but on application data stored in the database. Because it is enforced inside the database, it is possible to consistently redact database columns across different application modules accessing the same data. Data redaction minimizes changes to applications because it does not alter actual data in internal database buffers, caches, or storage, and it preserves the original data type and formatting when transformed data is returned to the application. Data redaction has no impact on database operational activities such as backup and restore, upgrade and patch, and high availability clusters.

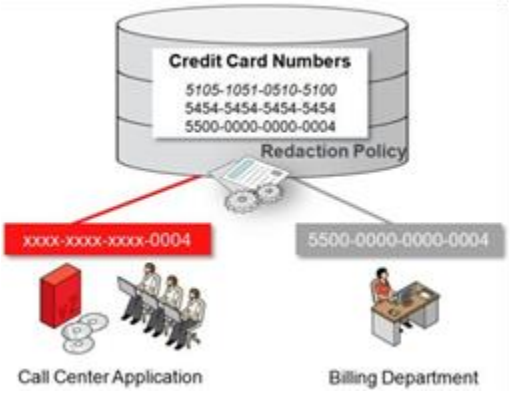

Figure 3. Oracle Advanced Security Data Redaction

Unlike historical approaches that relied on application changes and new software components, Oracle Advanced Security data redaction policies are enforced directly in the database kernel. This application agnostic approach greatly reduces the time and cost of addressing business requirements, especially important given the constantly evolving regulatory landscape. Declarative policies can apply different data transformations such as partial, random, and full redaction. Redaction can be conditional, based on different factors that are tracked by the database or passed to the database by applications such as user identifiers, application identifiers, or client IP addresses. A redaction format library provides pre-configured column templates to choose from for common types of sensitive information such as credit card numbers and national identification numbers. Once enabled, polices are enforced

immediately, even for active sessions. Oracle Advanced Security data redaction is also available on Oracle Database 11g Release 2 (11.2.0.4). Oracle Advanced Security fully supports Oracle Multitenant option. Both TDE and data redaction remain in place when pluggable databases are moved to new multitenant container databases, and they protect pluggable databases while in transit.

Minimizing sensitive data exposure with data sub setting and masking

The need for realistic data sets for development and test environments has resulted in the proliferation of data beyond the boundaries of production applications. This movement of production data dramatically increases the risk to data and increases the overall cost of security and compliance. Masking of data before it is moved from production eliminates the risk of data breaches in non-production environments by irreversibly replacing the original sensitive data with fictitious data so that data can be safely shared with IT developers or business partners.

Oracle Data Masking and Subsetting enables entire copies or subsets of application data to be extracted from the database, obfuscated, and shared with partners inside and outside of the business. Most importantly, during the obfuscation process, application integrity is preserved by maintaining data relationships across application tables. Oracle Data Masking and Subsetting improves security by reducing the scope of data exposed to partner organizations. Compliance costs are lowered by narrowing the compliance boundary for test and development groups.

Figure 4. Oracle Data Masking and Subsetting Pack

Oracle Data Masking and Subsetting provides end to end automation for provisioning test databases from production in compliance with regulations. Sensitive information such as credit card or social security numbers can be replaced and used for development and testing without expanding the security perimeter. This reduces the number of database systems that need to be monitored for compliance and security.

Important considerations in masking include the ability to maintain referential relationships between application tables after the masking process has taken place. Application records that span application tables and are linked by a given column need to have those values consistently replaced across the related tables. Oracle Data Masking and Subsetting discovers these relationships and masks all related data elements automatically while preserving referential relationships. The combination of sensitive data columns and the associated primary key-foreign key relationships are stored in an Application Data Model in the Oracle Enterprise Manager repository.

Oracle Data Masking and Subsetting provides a centralized library with out-of-the-box mask formats for common types of sensitive data, such as credit card numbers, phone numbers, national identifiers (social security number for U.S., national insurance number for U.K.). By leveraging the Format Library in Data Masking, enterprises can apply data privacy rules to sensitive data across enterprise-wide databases from a single source and thus, ensure consistent compliance with regulations. Enterprises can also extend this library with their own mask formats to meet their specific data privacy and application requirements.

Once the work of associating masking definitions with application attributes is complete, the formats and data associations can be saved in the Application Data Model and re-executed when test, development or partners need a refresh of data. Oracle Data Masking and Subsetting Pack can support masking of data in heterogeneous databases, such as IBM DB2 and Microsoft SQLServer, through the use of Oracle Database Gateways.

Detecting Access Attempts and Abuse

Satisfying compliance regulations and reducing the risk of security breaches are among the top security challenges businesses face today. Traditional perimeter firewalls play an important role in protecting data centers from unauthorized, external access, but attacks have grown increasingly sophisticated, bypassing perimeter security, taking advantage of trusted middle tiers, and even masquerading as privileged insiders. Examination of numerous security incidents has shown that timely examination of audit data could have helped detect unauthorized activity early and reduced the resulting financial impact. Various studies and surveys have concluded that a sizeable percentage of data breaches have been perpetrated using insider credentials, typically one with elevated access to systems and its data.

Auditing Database Activity with Universal and Conditional Audit

To provide more effective auditing inside the database, Oracle Database 12c introduces policy based conditional auditing for simplified configuration and management. Audit policies encapsulate audit settings and audit conditions allow auditing to be accelerated based on conditions associated with the database session. For example, an audit policy can be defined that audits all actions outside a specific IP address and username. Out-of-policy connections can be fully audited while no audit data will be generated for others, enabling highly selective and effective auditing.

Figure 7. Oracle Database 12c Conditional Auditing

In addition to the audit policies and conditions, new roles have been introduced for managing audit data and audit policies. Audit data integrity is further protected by restricting management of audit data to the built-in audit data management package. Three default audit policies are configured and shipped out of the box. The traditional audit commands available in previous releases continue to be supported in Oracle Database 12c.

Managing Audit Data with Audit Vault

The Audit Vault component of Oracle Audit Vault and Database Firewall helps enforce the trust but verify principle by consolidating and monitoring audit data from Oracle databases, Non-Oracle databases, Microsoft Active Directory, Microsoft Windows, Oracle Solaris, Oracle Linux, and Oracle ASM Cluster File System. A plug-in architecture consolidates custom audit data from application tables and other sources. Native audit data provides a complete view of database activity along with full execution context irrespective of whether the statement was executed directly, through dynamic SQL, or through stored procedures.

Audit data from databases is automatically purged after it has been moved to the Audit Vault Server. Audit Vault Server supports data retention policies spanning days, weeks, or years on a per source basis, making it possible to meet internal or external compliance requirements.

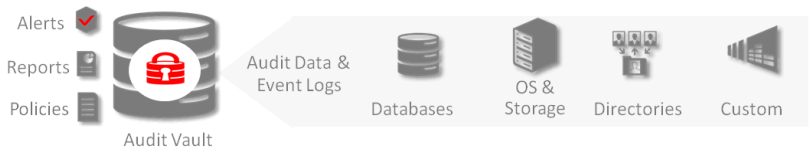

Figure 8. Oracle Audit Vault and Database Firewall

Dozens of out-of-the-box reports provide easy, customized reporting for regulations such as SOX, PCI DSS, and HIPAA. The reports aggregate both the network events and audit data from the monitored systems. Report data can be easily filtered, enabling quick analysis of specific systems or events. Security Managers can define threshold based alert conditions on activities that may indicate attempts to gain unauthorized access and/or abuse system privileges. Fine grained authorizations enable the Security Manager to restrict auditors and other users to information from specific sources, allowing a single repository to be deployed for an entire enterprise spanning multiple organizations.

Monitoring SQL Activity with Database Firewall

The concept of trust but verify applies equally well to applications. The Database Firewall component of Audit Vault and Database Firewall provides an optimized solution for monitoring SQL sent from the application to the database. A highly accurate SQL grammar-based analysis engine applies the trust but verify principle, monitoring and blocking unauthorized SQL traffic before it reaches the database. The Database Firewall SQL grammar analysis engine inspects SQL statements going to the database and determines with high accuracy whether to allow, log, alert, substitute, or block the SQL. Database Firewall supports white list, black list, and exception list based polices. A white list is simply the set of approved SQL statements that the database firewall expects to see. These can be learned over time or developed in a test environment. A black list includes SQL statements from specific users, IP addresses, or specific types that are not permitted for the database. Exception list-based policies provide additional deployment flexibility to override the white list or black list policies. Policies can be enforced based upon attributes, including SQL category, time of day, application, user, and IP address.

Figure 9. Oracle Audit Vault and Database Firewall

This flexibility, combined with highly accurate SQL grammar analysis, enables organizations to minimize false alerts, and only collect data that is important. Database Firewall events are logged to the Audit Vault Server enabling reports to span information observed on the network alongside audit data.

The Database Firewall can be deployed in-line, out-of-band, or in proxy mode to work with the available network configurations. For monitoring remote servers, an agent on the database server can forward the network traffic to the Database Firewall for inspection. Both the Audit Vault Server and Database Firewall components are delivered as software appliances. Both Audit Vault Server and the Database Firewall can be configured in high availability mode for fault tolerance.

Protecting Application Data with Data-Driven Security

Most applications developed over the past 20 years use 3-tier architectures and connect as one big application user to the database. This shift in security models was driven by the Internet, the resulting ability to make applications easily accessible, and the need to scale to thousands of users. At the same time, however, security requirements such as identity propagation, fine grained security, and auditing have become important security controls. In addition, compliance and privacy regulations continue to emerge and threats to data continue to evolve. In fact the number, size, and frequency of data breaches seem to be accelerating. Oracle has pioneered the development of advanced database security features to help address emerging requirements, with technologies such as Oracle Virtual Private Database and Oracle Label Security. Oracle Database 12c introduces Real Application Security, Oracle's next generation database authorization framework and the industry's most advanced solution for developing secure applications.

Implementing Fine-Grained security with Virtual Private database

Oracle Virtual Private Database (VPD), introduced in Oracle8i, is widely used today to enforce fine grained access control within applications. It allows application developers to associate a stored PL/SQL program unit with an application table, view, or synonym. The program unit fires when the application object is accessed via SQL. The program unit computes a predicate or 'where clause' that is appended to the original SQL statement. In many cases, the program module will query specific meta data tables containing information on user roles and privileges as nearly every application today has its own unique set of security tables. Another common approach used with VPD is to initialize an Oracle application context when a new application user is initialized within the application.

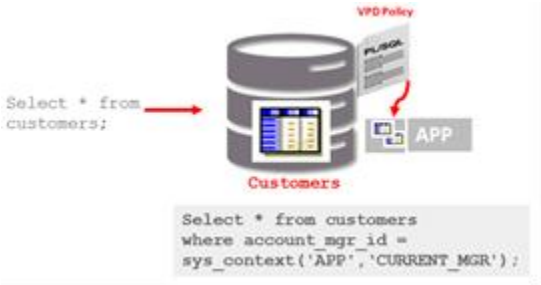

Figure 10. Oracle Virtual Private Database

Implementing Multi-Level Security with Oracle Label security

Controlling access to data based on classification is a common requirement found in government and defense environments. Commonly known as multilevel security, access to business objects is controlled based on the data classification label assigned to the object and the label authorization assigned to the user. Data classification enables information of varying sensitivity to reside in the same application table. In addition to multilevel security, classification labels can also be used to strip or virtually partition information in the same table, eliminating the need for custom built views.

Oracle Label Security assigns a data label or data classification to application data and enforces access control by comparing the data label with the label authorization or security clearance of the user requesting access. Data labels can be attached as hidden columns to existing tables, providing transparency to existing applications by mediating access based on the data label but not returning the actual data label in the SQL statement.

2014 Jabberwocky Rd	Southlake	PUBLIC
2011 Interiors Blvd	South San Francisco	HIGHLY_SENSITIVE::UNITED_STATES
2007 Zagora St	South Brunswick	PUBLIC
2004 Charade Rd	Seattle	HIGHLY_SENSITIVE::UNITED_STATES
147 Spadina Ave	Toronto	PUBLIC
6092 Boxwood St	Whitehorse	PUBLIC
40-5-12 Laogianggen	Beijing	SENSITIVE::ASIA
1298 Vileparle (E)	Bombay	PUBLIC
12-98 Victoria Street	Sydney	PUBLIC
198 Clementi North	Singapore	SENSITIVE::ASIA
8204 Arthur St	London	PUBLIC

Figure 11. Oracle Label Security Protected Table Showing Data Labels

Enforcing Application Data Controls with Real Application Security

Most applications today have specific security and authorization models, the strength of which depends completely on the application. As the access control policy is embedded within the application logic, and each application comes with its own infrastructure, it becomes difficult to maintain and extend the policies. IT security teams struggle to verify application security policies and how they impact enterprise-wide data access policies as each application has its own custom-built security policy constructs and enforcement mechanisms. As the database does not know about end-users, it cannot natively audit end-user activities, leading to weaker accountability.

Unlike the basic Oracle Virtual Private Database (VPD), Oracle Database 12c Real Application Security (RAS) provides a robust declarative model that allows developers to define the data security policy based on application users, roles and privileges within the Oracle Database. The new Oracle Database 12c RAS technology is more secure, scalable, and cost effective than the traditional Oracle VPD technology.

Real application security provides a declarative interface that allows developers to define the data security policy, application roles, and application users without requiring application developers to create and maintain PL/SQL stored procedures. The data security policies are defined inside the database kernel using the Oracle Database 12c RAS API. The permissions associated with business objects are stored in Access Control Lists (ACLs).

Figure 12: Components of Oracle RAS Data Security Policy

ACLs are a key component of RAS and store the privileges assigned to principals and control the type of operations select, insert, update and delete that can be performed on the objects.

Name	ID	SSN	Salary	Manager	Phone Num
Steven	SKING	100-51-4567	24000	-	515.123.4567
Neena	NKOCHHAR	101-51-4568	17000	Steven	515.123.4568
Nancy	NGREENBE	108-51-4569	12008	Neena	515.124.4569
Luis	LPOPP		6900	Nancy	515.124.1111
John	JCHEN		8200	Nancy	515.124.1111

Figure 13: Data Realm and Column Authorization using ACLs

Oracle Database 12c with Real Application Security provides the next generation authorization architecture for applications:

» **Uniform Data Security:** The RAS Security model allows uniform specification and enforcement of access control policies on business objects irrespective of the access path. It overcomes the limitation of custom- built approaches that only work when an object is accessed via the specific code path that has access control logic embedded into it.

» **Secure End User Identity Propagation:** Application sessions allow the end user identity and associated attributes to be conveyed securely to the database allowing the database to use the information for end-user access control and auditing.

» **Declarative and Fine Grained Access Control:** RAS policy components encapsulate the access control requirements of the application in the form of declarative policy on data for application users, application roles, and application privileges. With column security, RAS model extends authorization to the column level to protect sensitive data such as SSN. With support for master-detail, parameterized, delegation, and exception based declarative policies, RAS meets the real-life deployment requirements of applications.

» **Security without Performance Trade-off:** In most current systems, security is either coded into the applications or it is externalized but requires multiple round-trips impacting performance. Unlike these cases, RAS is natively implemented in the database and provides a security solution without trading-off performance.

Oracle can be used regardless of whether the application is a 3 tier or traditional 2 tier applications, including stand-alone client-server applications. Using RAS, applications do not have to develop their own access control policy

infrastructure within the database. Administration of access control policies is separated from the actual program code, enabling flexibility and extensible.

Oracle Real Application Security unifies database and application-specific access control models by making it possible to define and use application-specific privileges, users, and roles within the database. In addition, it provides the much needed application authorization functionalities in the database and a uniform administration model for access control policies on data.

Conclusion

Oracle Database 12c Release 2 delivers the industry's most advanced security capabilities spanning protective, detective, and administrative controls. In addition to the features described above, Oracle Database 12c includes features to help ensure deployments are secure by default.

Many Oracle Database customers in the government, banking, and healthcare sectors are familiar with the requirements of U.S. Federal Information Processing Standard #140 version 2, or FIPS 140-2. Oracle Database 12c includes an embedded FIPS 140 certified software module. Once set, Oracle Advanced Security TDE, network encryption, and the DBMS_CRYPTO toolkit will leverage the new module. In addition to FIPS 140, Oracle Database 12c also introduced full support for SHA-512, a more modern algorithm for securely hashing data required by various industry and government standards.

Configuration drift and unauthorized configuration changes can result in a failed audit and, even worse, data breaches. For many years the Oracle Enterprise Manager Database Lifecycle Management Pack has shipped hundreds of out-of-the-box configuration checks. Scans can be scheduled and alerts created on failed checks. One of the most common standardized configuration checks used by Oracle Database customers in the United States public sector is known as the Secure Technical Implementation Guide, or STIG. The latest release of Oracle Enterprise Manager ships the STIG for Oracle Databases out of the box, making it easy for customers who want to use the STIG as their baseline to quickly assess their compliance status.

In summary, Oracle Database 12c Release 2 continues to set the standard for securing data. Conditional audit polices simplify audit configuration, increasing the value of audit information for both auditors and security personnel. The risk of sensitive data exposure in applications and elsewhere can be reduced with Oracle Advanced Security data redaction and Oracle Data Masking and Subsetting. Credit card data, date of birth, and other personally identifiable information can be automatically redacted before being returned to applications. Data Shared with partners inside and outside the organization can be masked, reducing the compliance boundary and cost of data breaches. Management of encryption keys is simplified with a new key management interface for Transparent Data Encryption (TDE) and Oracle Key Vault accelerates encryption deployments by centrally managing encryption keys, Oracle Wallets, Java Keystores, and credential files from across the enterprise. Application bypass controls have been increased with enhancements to Oracle Database Vault realms, enabling a powerful, additional security boundary for applications and highly sensitive application objects. The new privilege analysis capability within Oracle Database Vault provides insight on the actual database privileges and roles used within an application, helping existing and new applications adhere to the principle of least privilege and reduce their attack surface. And Oracle Database 12c Real Application Security introduces a powerful new authorization framework for supporting application security requirements, enabling application users, roles and privileges to be defined within the database. In combination, these capabilities provide a defense-in-depth solution for protecting any organization's most critical data assets.

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

ORACLE DATABASE 12C RELEASE 2 SECURITY AND COMPLIANCE
April 2017

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