Security and Compliance with Oracle Database 12c
Introduction .................................................................................................................. 2
Oracle Database 12c Security ......................................................................................... 3
Protecting Against Database Bypass Threats ............................................................... 3
Limiting Sensitive Data Exposure in Applications ....................................................... 4
Preventing and Detecting Common Threats ................................................................. 5
Data Classification.......................................................................................................... 10
Protecting Data in Non-Production Environments ..................................................... 11
Locating and Cataloging Your Sensitive Data .............................................................. 12
Monitoring the Configuration of Sensitive Databases .............................................. 12
Auditing Database Activity ......................................................................................... 13
Building More Secure Applications ........................................................................... 14
Oracle Database 12c Secure By Default .................................................................... 14
Oracle Database Security and Applications .............................................................. 15
Conclusion ................................................................................................................... 16
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 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, 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 Security combined with Oracle Audit Vault and Database Firewall provides 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 delivers 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.

Protecting Against Database Bypass Threats

Database bypass threats include attacks that target backup media, discarded media, and the physical storage where the production data resides. One of the most widely used technologies used to protect against database bypass threats is encryption. A key driver in the widespread recognition of encrypt technologies came in 2003 with the passage of California Senate Bill 1386 (SB1386). SB1386 introduced the topic of encryption to a broad audience and since then many other states have passed their own privacy-related laws. 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 at the application layer, in the operating system, on backup media, and within 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.
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.

Limiting Sensitive Data Exposure in Applications

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.
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, policies 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.

**Preventing and Detecting Common Threats**

A common characteristic of many 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. SQL injection has been another common attack vector used to gain unauthorized access to vast amounts of information. Protecting against these types of 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 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.

![Oracle Database Vault Realms block access from privileged accounts](Image)

**Figure 3.** Oracle Database Vault Realms block access from privileged accounts

Figure 3 shows a Database Vault realm blocking a DBA from accessing an application schema. 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 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. Command controls can reference out-of-the-box factors such as IP address, authentication method, and program name to control the usage of commands such as `create table as select from`, `create database link`, and `create user`. 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 controls that seal off access to application objects, even to those with direct object grants, including the object owner. Known as a Mandatory Realm, this powerful security capability can be used as an additional gate check.
prior to allowing even the application owner access to the data. Mandatory realms can also be used to protect sensitive information when direct access to the application schema is required for maintenance operations.

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.

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.

Oracle Database Vault with Oracle Database 12c introduces privilege analysis. Oracle Database Vault privilege analysis helps increase the security of applications by identifying the actual privileges used 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.

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

Perimeter firewalls play an important role in protecting data centers from unauthorized, external access, but database attacks have grown increasingly sophisticated, bypassing perimeter security, taking advantage of trusted middle tiers, and even masquerading as privileged insiders. As a result, database activity monitoring and enforcing security controls in and around the database have become critical. Effective monitoring and auditing can alert and block attempted policy violations, as well as provide comprehensive reports for compliance.

Oracle Audit Vault and Database Firewall provides a first line of defense for Oracle and non-Oracle databases and consolidates audit data from databases, operating systems, and directories. A highly accurate SQL grammar-based analysis engine monitors and blocks unauthorized SQL traffic before it reaches the database. Database activity data from the network is combined with detailed audit data for easy compliance reporting and alerting. With Oracle Audit Vault and Database Firewall, auditing and monitoring controls can be easily tailored to meet enterprise security requirements.

![Diagram of Oracle Audit Vault and Database Firewall](image)

**Figure 5.** Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall consolidates database activity monitoring events and audit logs. Policies enforce expected application behavior, helping prevent SQL injection, application bypass, and other malicious activities from reaching the database while also monitoring and auditing privileged users, and other activities, inside the database. Oracle Audit Vault and Database Firewall can also consolidate audit data from 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.
Oracle Database Firewall provides a sophisticated next-generation SQL grammar analysis engine that inspects SQL statements going to the database and determines with high accuracy whether to allow, log, alert, substitute, or block the SQL. Oracle Database Firewall supports white list, black list, and exception list based policies. 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. 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.

**Enterprise Audit Data Consolidation and Lifecycle Management**

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. In addition to consolidating audit data from databases, operating systems, and directories, the Audit Collection Plugin can be used to collect audit data from application tables or XML files, and transfer them to the Audit Vault Server. 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.

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.

Security controls can be customized with in-line monitoring and blocking on some databases and monitoring only on other databases. 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, the Audit Vault Agent on the database server can forward the network traffic to the Database Firewall. Delivered as a soft appliance, a single Audit Vault Server can consolidate audit logs and firewall events from thousands of databases. Both Audit Vault Server and the Database Firewall can be configured in a HA mode for fault tolerance.
Data Classification

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 authorization can also be used as factors with solutions such as Oracle Advanced Security Redaction and Oracle Database Vault command rules. For example, the decision to redact data could be based on the label authorization of the user.

Oracle Label Security data labels can be comprised of three components. The first component is a mandatory hierarchical level. Examples of levels include public, confidential, and highly sensitive. The second component is optional and is known as a compartment. Multiple compartments can be assigned to a data label and are used to enforce additional special access requirements. For example a compartment might correspond to a special project. The third and final component of a label is optional and is known as a group. Multiple groups can be assigned to a label and typically correspond to ownership hierarchies, territories, or jurisdictions.

Oracle Label Security authorizations can be assigned to database as well as application users. The basic user label authorizations consist of a minimum and maximum level, default compartments, and groups. Once authorized, Oracle Label Security will compare the data label
of the business object to the label authorization of the user and determine access. Oracle Label Security authorizations are in addition to any required privileges on the database object itself, including select, insert, update, and delete. When using in an Oracle Advanced Security Redaction condition or Oracle Database Vault command rule, the Oracle Label Security function ols_dominates can be used to create a simple policy expression.

Protecting Data in Non-Production Environments

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 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 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 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 Pack can support masking of data in heterogeneous databases, such as IBM DB2 and Microsoft SQLServer, through the use of Oracle Database Gateways.
Locating and Cataloging Your Sensitive Data

Knowing where your sensitive data resides is an important first step in deploying a defense in depth security model. Identifying sensitive data based on the type of application running is a common method used to classify databases. In some cases, more granular controls on data within a given application may be desired. Knowing where specific data resides 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 facilitate the process of locating sensitive data within an application and applying security controls on that data. SDD can be used with Oracle Data Masking and other database security solutions to identify and protect sensitive data.

Oracle has created Application Accelerators for both Oracle Fusion Applications and Oracle E-Business Suite. The Application Accelerators list the sensitive data for each of the applications. Oracle Data Masking 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 load sensitive information from Oracle Enterprise Manager Data Discovery and Modeling into the Oracle database and apply security controls such as Oracle Advanced Security Data Redaction.

Monitoring the Configuration of Sensitive Databases

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.
Auditing Database Activity

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.

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.
Building More Secure Applications

Most applications today use 3-tier architectures, connecting as one big application user to the database. This model typically results in the application connection having wide ranging and powerful privileges within the database. Understanding these privileges, how and if they are used, is a complex task. In addition, application users, roles, and privileges are commonly all managed in custom application tables and are unknown to the underlying database. This model, while widely used, relies on the application for all security enforcement. Direct connections to the database generally result in unimpeded access to all application data.

Code Based Access Control

Oracle Database 12c Code Based Access Control enables database roles to be granted to stored procedures, functions, and packages. This new security feature enables limited privilege elevation within the stored program unit. Applications that rely on definers or invokers rights procedures can use this new feature to grant roles to the stored program unit. When the stored program unit is invoked, the privileges associated with the granted role will be available in the runtime context of the stored program unit.

Real Application Security

Oracle Database 12c introduces the next generation authorization framework to support application security requirements. Unlike the traditional Oracle virtual private database (VPD), Oracle Database 12c Real Application Security (RAS) provides a declarative model that allows developers to define the data security policy based on application users, roles and privileges within the Oracle Database. This new RAS based paradigm 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). ACLs are a key component of RAS and store the privileges assigned to principals and control the type operations select, insert, update and delete that can be performed on the objects.

Oracle Database 12c Secure By Default

Oracle Database 12c has numerous enhancements that provided increased configuration security by default. Included in these enhancements are reduced dependency on SYSDBA, stronger security on sensitive data dictionary tables, display of last login time after authentication in tools such as SQL*Plus, removal of the UNLIMITED TABLESPACE privilege from the RESOURCE role, support for multiple forms of authentication within the same database, and
support for network encryption and strong authentication in the SE and EE editions of the
database. Oracle Database 12c introduces new roles for separation of duty, including SYSDG
(Data Guard), SYSBACKUP (RMAN), and SYSKM (Advanced Security Key Management),
enabling more secure management of the database by reducing the frequency and conditions
under which the SYSDBA role needs to be used. In addition, two new roles, AUDIT_ADMIN
and AUDIT_VIEWER, have been introduced for audit management inside the database.

Oracle Database Security and Applications

Oracle Advanced Security TDE and Oracle Database Vault have been certified with many
applications include Oracle E-Business Suite, Oracle Siebel Applications, Oracle PeopleSoft
Applications, Oracle JDEdwards EnterpriseOne, Oracle Primavera, and Oracle Retek. Third
party certifications include SAP and Finacle. Oracle Audit Vault and Database Firewall can be
used for monitoring SQL traffic being sent to the database or consolidating audit data from the
underlying operating system and directories supporting the application. Oracle Audit Vault and
Database Firewall can also be used to consolidate audit data from application specific tables.
Conclusion

Oracle Database 12c delivers the industry’s most advanced security capabilities spanning protective, detective, and administrative controls. Designed to help prevent and detect common and advanced attack vectors, Oracle Database 12c advancements include conditional auditing, data redaction, real application security, privilege analysis, stronger application bypass controls, and new administrative roles for common tasks, to name a few. Fully integrated with Oracle Multitenant, security controls can be customized per pluggable database.

Oracle Database 12c conditional audit policies simplify audit configuration, increasing the value of audit information for both auditors and security personnel. The risk of sensitive data exposure in applications can be reduced with data redaction. Credit card data, date of birth, and other personally identifiable information can be automatically redacted before being returned to applications. Management of encryption keys is simplified with a new key management interface for Transparent Data Encryption (TDE). In addition, a new role provides increased security and separation of duty for management of encryption keys. Application bypass controls have been increased with mandatory realms, enabling an additional security boundary for applications and highly sensitive application objects. New privilege analysis provides insight on the actual database privileges used within an application, helping existing and new applications adhere to the principle of least privilege and reduce their attack surface. 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.