

# ORACLE LABEL SECURITY



## KEY FEATURES AND BENEFITS

**ORACLE** **11g**  
DATABASE

- Transparently enforces row level access control using data labels
- Provides multi-level security capabilities for government and defense organizations
- Enforce need-to-know policies based on user labels
- Partition data based on its data label
- Flexible policy based administration model
- Extends Oracle Database Vault factors
- Oracle Label Security 10g Release 2 has been successfully evaluated for Common Criteria EAL4+

*Oracle Label Security enables powerful row level access controls in the Oracle Database using data sensitivity labels. Policy based administration provides flexibility for a wide range of use cases from healthcare to law enforcement. Oracle Label Security extends database security authorizations beyond traditional roles, enabling powerful factors for use in Oracle Database Vault and other security products.*

### Protect Sensitive Data

Traditional privileges such as *Select*, *Insert*, *Update* and *Delete* stop at the object level. For example, a user can be granted *Select* on the *Customer* table but not on a subset of rows within the *Customer* table. Historically this type of access control was achieved using database views. Views, however, can be cumbersome and may need to be modified as the security requirements change. In addition, view based access control is subject to bypass by the application table owner. Label Security protects data by assigning a physical data label to each row. High security organizations use Label Security to compartmentalize access to *Sensitive* and

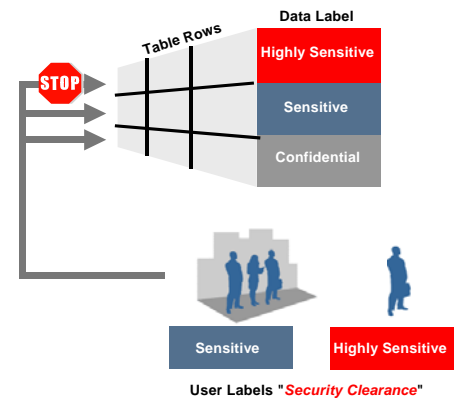


Fig 1.0 Oracle Label Security Access Mediation

*Highly Sensitive* data stored in the same application table, commonly referred to as multi-level security (MLS). Commercial organizations can use data labels to compartmentalize data for multi-tenancy, hosting, software-as-a-service and other security requirements.

### User and Data Labels

User labels are an important part of Label Security and determine whether a user has access to a particular data row. The example in Figure 1 shows two groups of users. The first group has access to data labeled *Sensitive* and *lower*. The second group has access to data labeled *Highly Sensitive* and *lower*. Labels are comprised of three components, a level, one or more optional compartments plus one or more optional groups. Levels show the overall sensitivity of the data. For example, data labeled *Highly Sensitive* is more critical than data labeled *Sensitive*. Compartments, also known as categories, compartmentalize data horizontally. Groups are commonly used to map organizational access controls. To access a row protected by a data label with levels, compartments and groups, a user must be authorized to a level equal to or higher than the data level, all compartments and at least one group. In other words, a user must have the appropriate *level* a superset of the *Compartments* and at least one *Group*. Groups might be used to represent companies in a

RELATED PRODUCTS:

The following products provide additional security to help meet privacy and regulatory requirements:

- Oracle Database Vault
  - Protect application data from privileged users
  - Customizable separation-of-duty
  - Real time preventive controls
  - Out-of-the-box policies available for Oracle E-Business Suite, Siebel, and PeopleSoft Applications
- Oracle Advanced Security
  - Provides Transparent Data Encryption for Oracle Databases at the tablespace or column level
  - Supports 3DES, AES 192, 256
  - Network Encryption
  - Strong authentication using Kerberos and PKI
- Oracle Audit Vault
  - Secure and consolidate audit data from Oracle 9i and higher databases
  - Secure and consolidate audit data from SQL Server 2000 and 2005 databases
  - Built-in reports for compliance and privileged user activity
  - Pro-actively alert on suspicious activity
  - Centrally manage audit policies for Oracle Databases.
- Oracle Data Masking
  - De-identify privacy related application data for development and test environments
  - Create masking policies for easy management

hosted environment and can have also have a parent-child relationship. Compartments might be used to restrict access to a subset of customers handled by a specialized team. User labels can be managed centrally in Oracle Identity Management or locally in each database.

**Flexible and Adaptable**

Label Security provides an easy-to-use policy based administration model. Policies act as the logical containers of label components, data labels, user labels, enforcement settings and protected objects. Policy based administration allows you to create policies specific to your environment. Moreover, multiple policies can reside in the same database, making it easy to create policies for different applications in a consolidated environment.

Oracle Label Security Data Label Components	Human Resources	Law Enforcement	Government
<b>Levels</b>	Confidential Sensitive Highly Sensitive	Level 1 Level 2 Level 3	Confidential Secret Top Secret
<b>Compartments</b>	PII Data Investigation	Internal Affairs Drug Enforcement	Desert Storm Border Protection
<b>Groups</b>	HR	DOJ FBI	NATO Homeland Security

Table 1.0 Oracle Label Security Policy Examples

Data labels can be attached as *hidden* columns to application tables enabling existing *update* and *insert* statements to continue working without modification. Label Security provides numerous enforcement options such as enforcing access control on *Select* operations, *Update* operations, or both and works with common application user models.

**Integrated with Oracle Database Security Products and Features**

User labels can be used as factors within Oracle Database Vault command rules. This powerful capability extends Label Security concepts beyond traditional row level access controls to mediation at the database and application level. For example, separation-of-duty can be customized by looking at an administrator’s user label within a Database Vault command rule. Security administrators can leverage the Oracle Label Security policy model to manage simple virtual private database (VPD) security checks without having to maintain a separate VPD PL/SQL security package. Please refer to the Database Security page on the Oracle Technology Network for complete examples of using Oracle Label Security with both Database Vault and VPD. Oracle Label Security can be used with Oracle E-Business Suite and other applications. Please refer to Oracle Meta Link for more information.

Copyright 2008, Oracle. All Rights Reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor is it subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.