

# SECURITY INSID=OUT

Complete Protection for Your Database,  
Middleware, and Applications

**ORACLE<sup>®</sup>**

## **Oracle Database Vault Technical Overview**

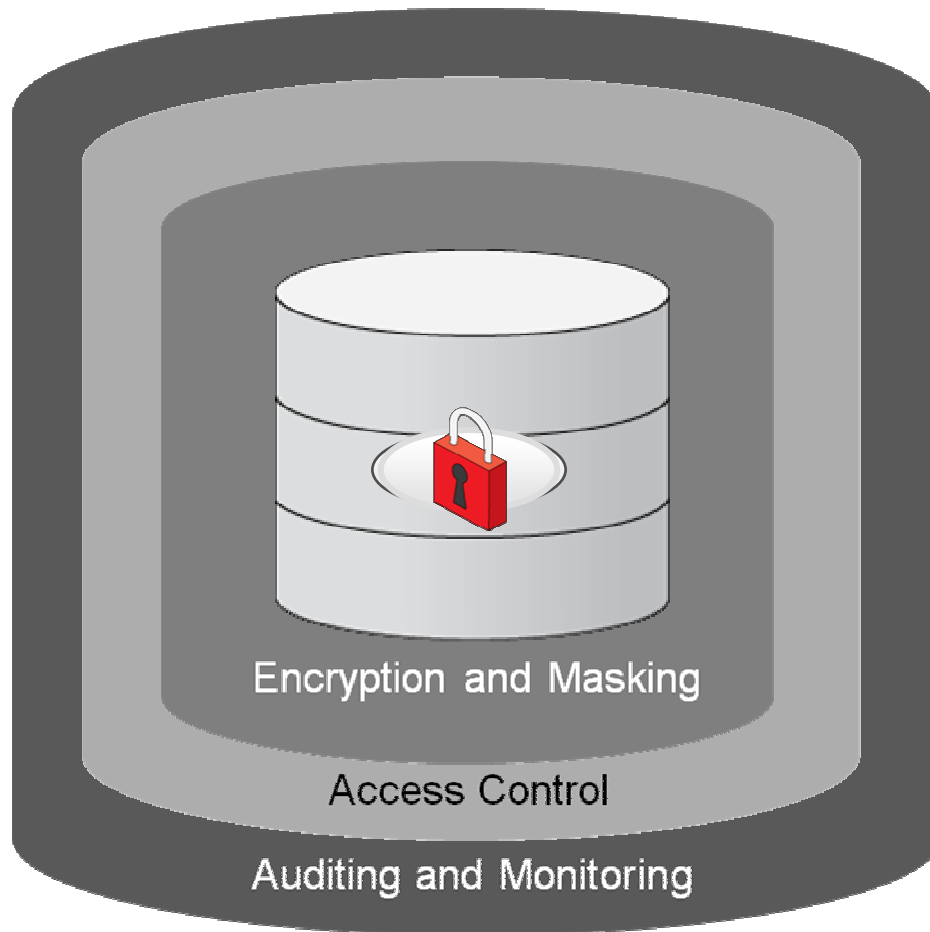
Mazhar Zoaib Ali  
Head, Technology Sales Consulting  
Pakistan & SAGE - West



# Agenda

- Oracle Database Security – Defense-in-Depth
- Business drivers
- Technology introduction
- Look inside – how it works
- Demo #1 Preventive controls using Realms
- Demo #2 Trusted paths using command rules and multi-factor authorization
- Customers
- Summary
- Q&A

# Database Defense-in-Depth



## Encryption and Masking

- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

## Access Control

- Oracle Database Vault
- Oracle Label Security

## Auditing and Monitoring

- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall



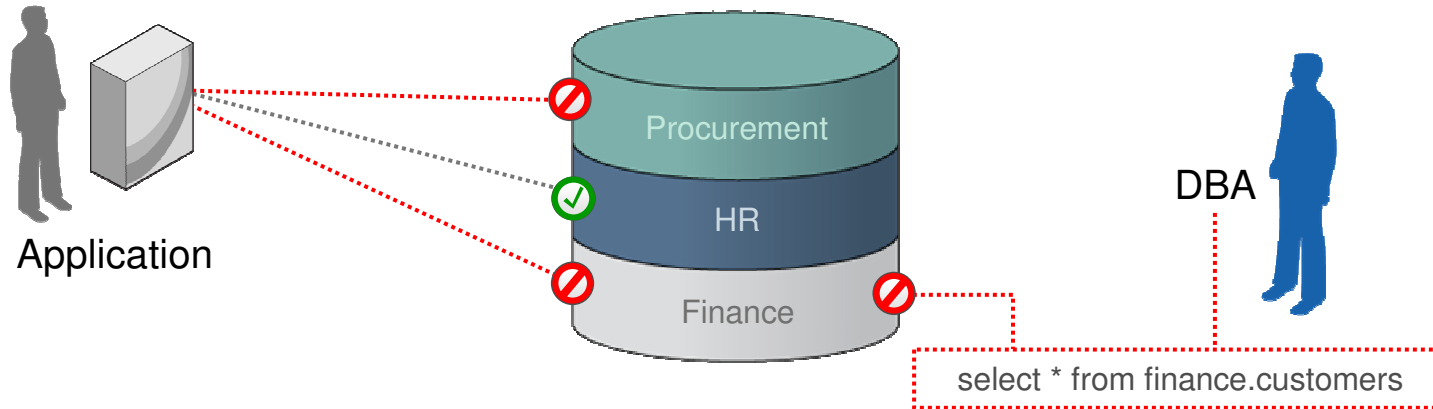
# Oracle Database Vault

## Business Drivers

- Outsourcing / Database Consolidation
  - Reduce costs without sacrificing security
  - Enforce separation of duty controls inside the database
- Simplify Privacy and Compliance
  - Prevent audit findings
  - Prevent unauthorized database changes
  - Enforce operational controls inside the database
  - Prevent unauthorized access to sensitive application data

# Oracle Database Vault

## Separation of Duties & Privileged User Controls

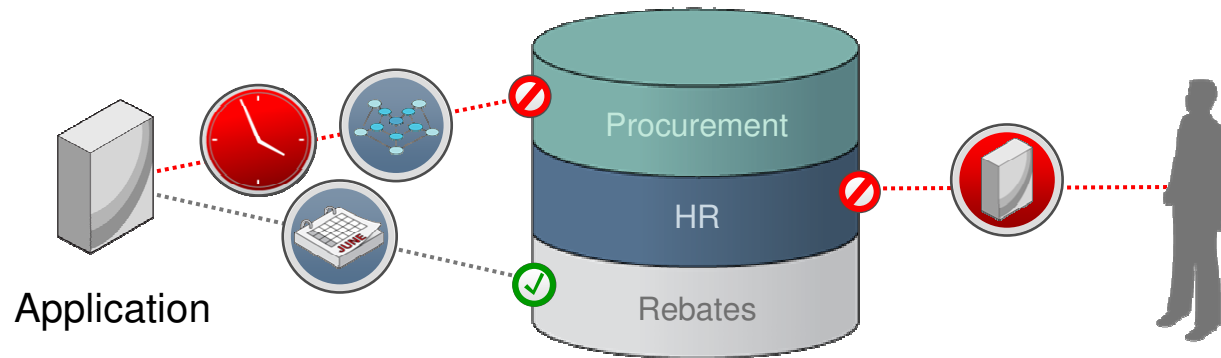


- DBA separation of duties
- Limit powers of privileged users
- Securely consolidate application data
- No application changes required
- Works with Oracle Exadata V2 Database Machine



# Oracle Database Vault

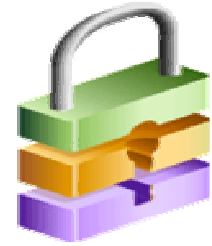
## Multi-Factor Access Control Policy Enforcement



- Protect application data and prevent application by-pass
- Enforce who, where, when, and how using rules and factors
- Out-of-the box policies for Oracle applications, customizable

# Oracle Database Vault

## Built-In Factors



- User Factors
  - Name
  - Authentication type
  - Session User
  - Proxy Enterprise Identity
- Network Factors
  - Machine name
  - Client IP
  - Network Protocols
- Extensible
  - Define custom factors
- Database Factors
  - Database IP
  - Database Instance
  - Database Hostname
  - Database SID
- Runtime Factors
  - Language
  - Date
  - Time



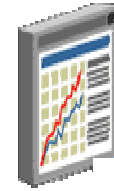
# Oracle Database Vault

## Command Rules

- Alter table
- Alter trigger
- Alter package
- Alter tablespace
- Connect / login
- Create table
- Create index
- Create view
- Drop table
- Drop user
- Drop index
- Truncate table
- ....
- ....
- ....

# Oracle Database Vault

## Reports



- Built-in Auditing and Reporting
  - Realm violation audit report built-in shows attempts to access Realm protected data
  - Privileges reports such as who has the DBA role
- Other reports
  - 2 dozen other Database Vault and security reports
- Easy to administer
  - Web interface and API

# Oracle Database Vault

## Out-of-the-Box Protections For Applications

- Prevent DBA from accessing application data
- Pre-built policies include realms and command rules
- Complements application security
- Transparent to existing applications
- Customizable

Oracle E-Business Suite  
11i / R12



PeopleSoft Applications



Siebel, i-Flex



JD Edwards Enterprise One



SAP

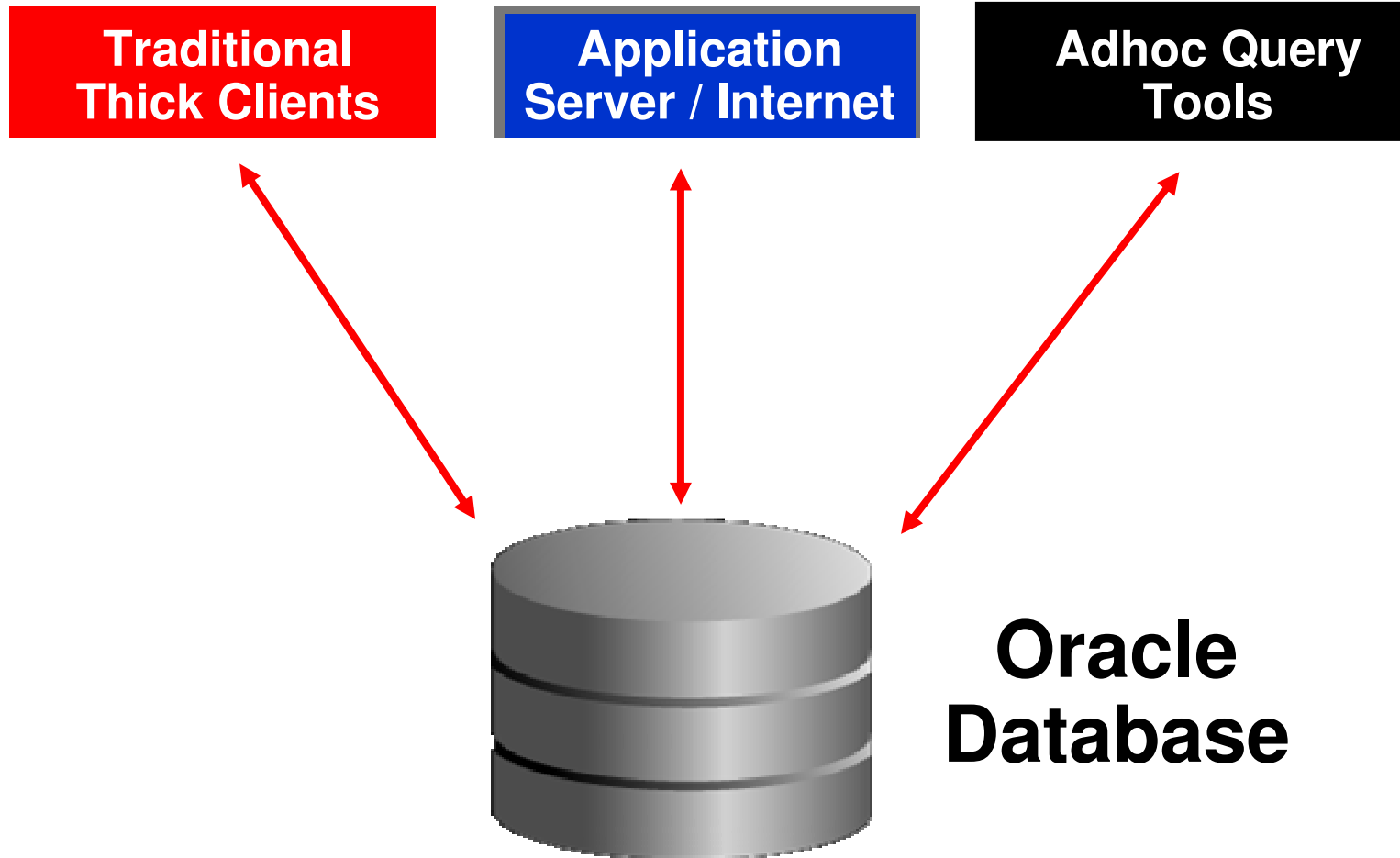


Infosys Finacle



# Oracle Database

## Common Data Center Architectures

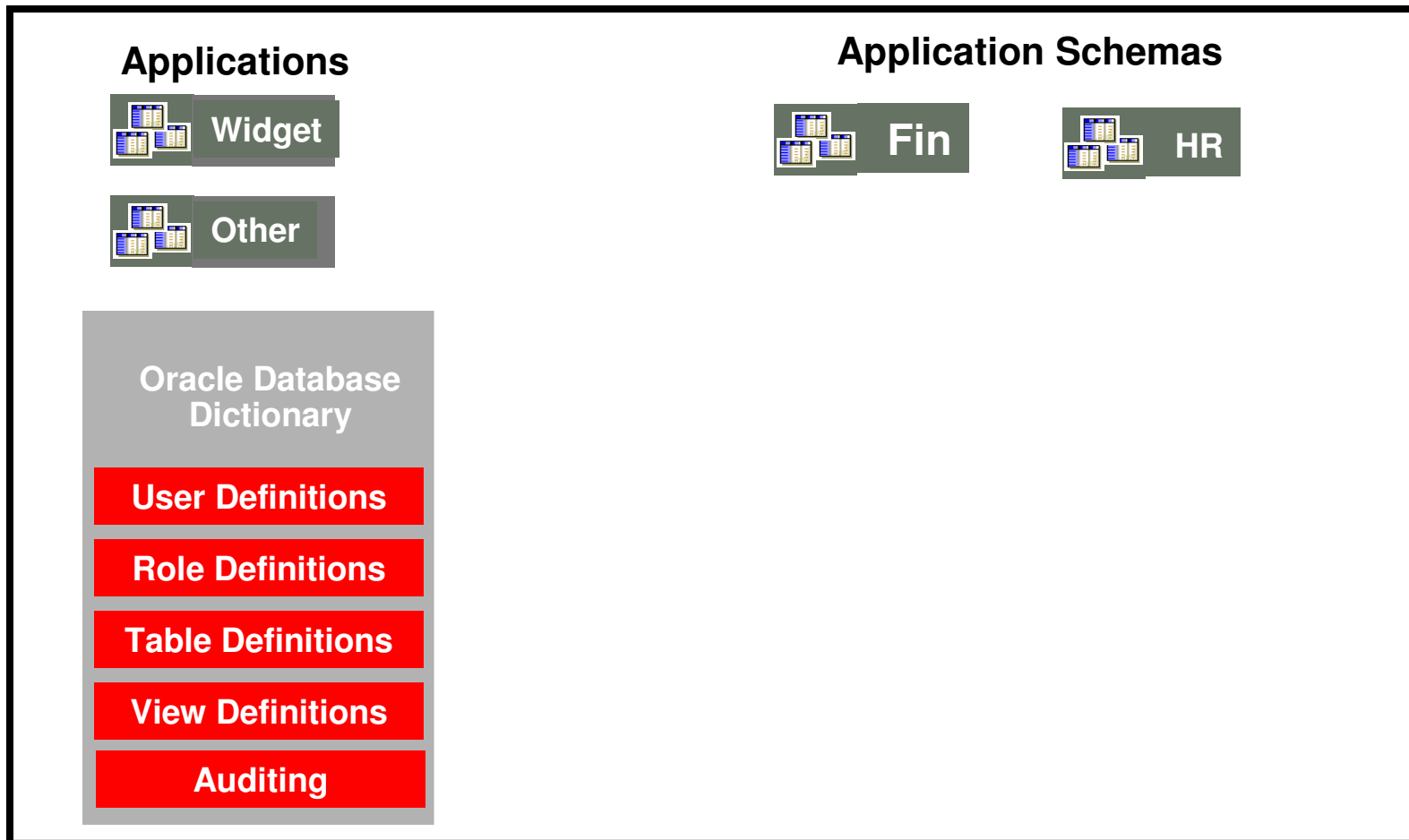


# Oracle Database Without Database Vault

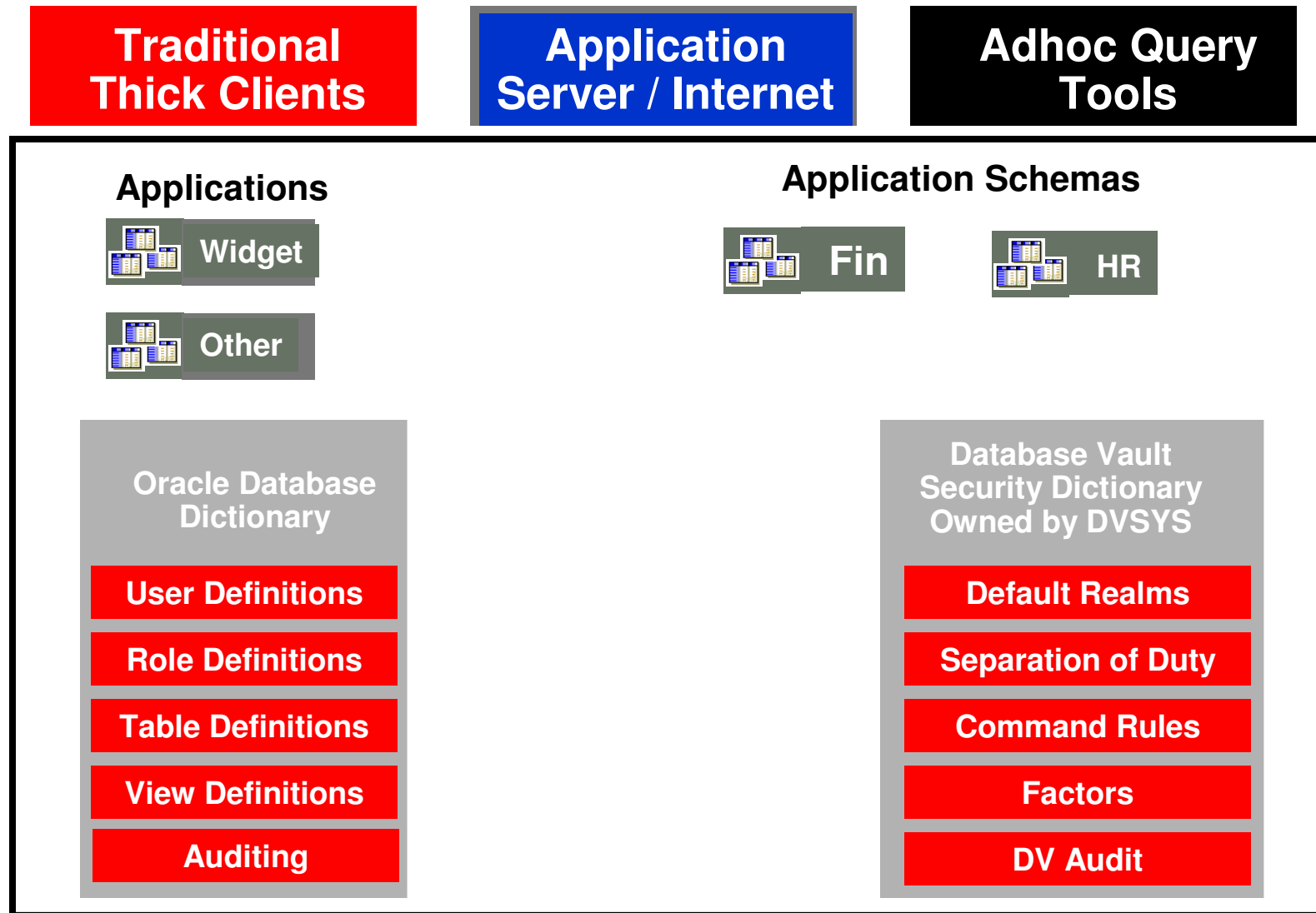
**Traditional  
Thick Clients**

**Application  
Server / Internet**

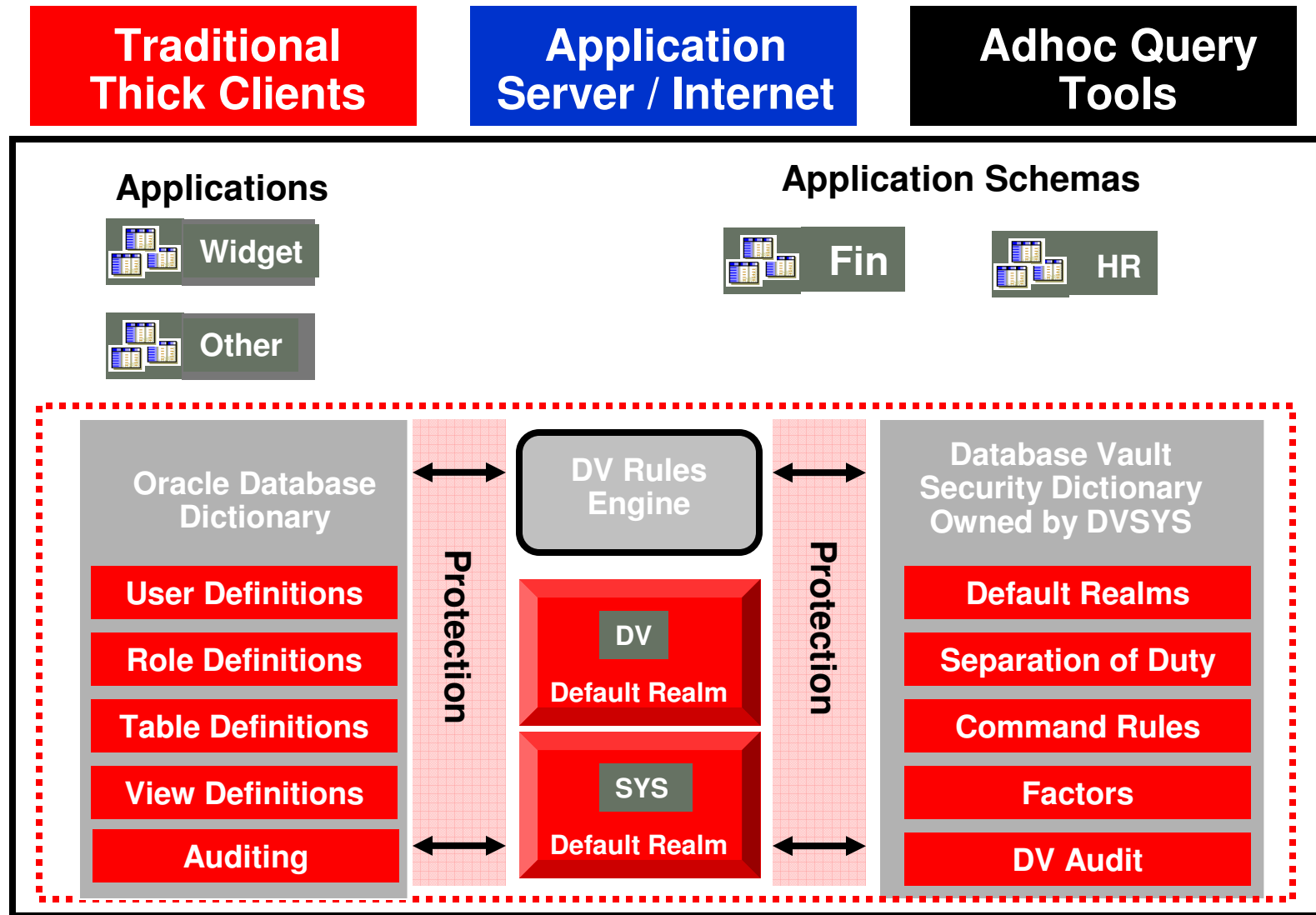
**Adhoc Query  
Tools**



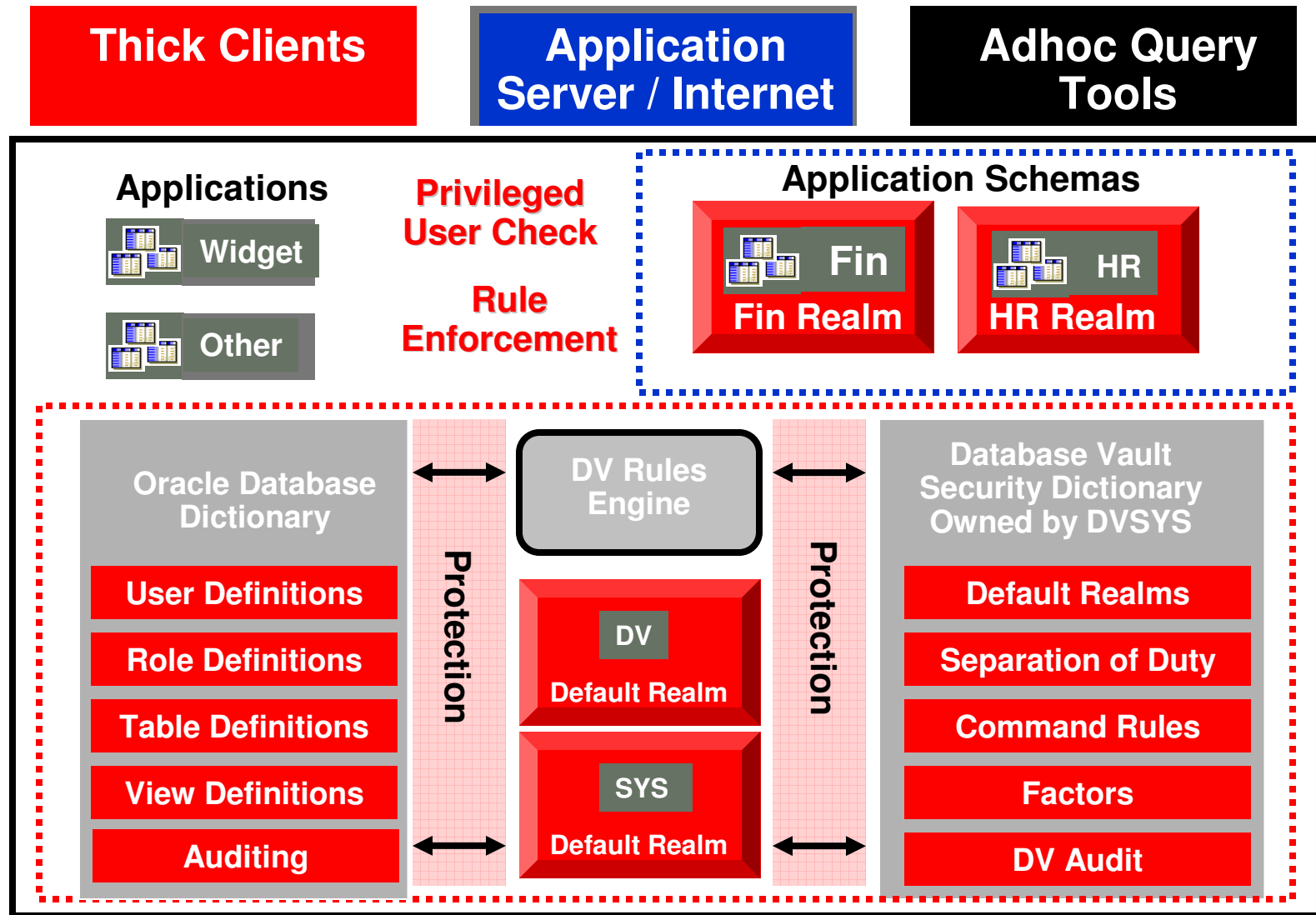
# Oracle Database Vault Architecture

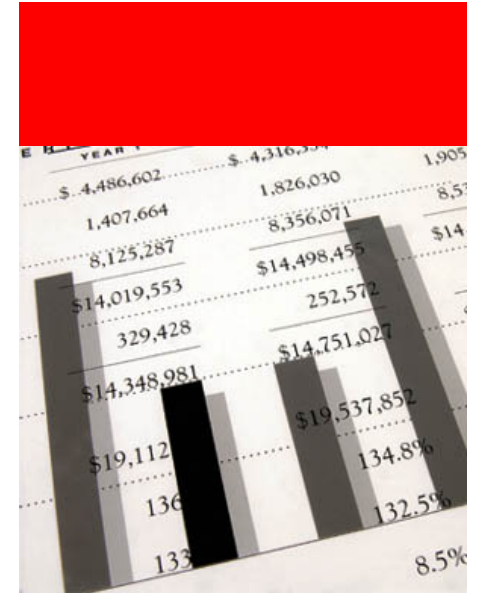


# Oracle Database Vault Architecture



# Oracle Database Vault Architecture





## Demo #1:

Protecting application data from privileged users using Realms

Oracle SQL Developer : DBA - JSMITH

File Edit View Navigate Run Debug Source Tools Help

Connections Reports

DBA - JSMITH 0.026 seconds DBA - JSMITH Snippets

Enter SQL Statement:

```
select * from sysadm.t_ps_acct_1n;
```

Results Script Output Explain DBMS Output OWA Output

Results:

All Rows Fetched: 0 | Line 1 Column 35 | Insert | Unix: LF | Editing

The screenshot displays the Oracle SQL Developer application window. The title bar reads "Oracle SQL Developer : DBA - JSMITH". The menu bar includes "File", "Edit", "View", "Navigate", "Run", "Debug", "Source", "Tools", and "Help". Below the menu bar is a toolbar with icons for file operations and execution. The main interface is divided into several panes. On the left is the "Connections" pane, which shows a tree view of database objects for the "DBA - JSMITH" connection, including Tables, Views, Indexes, Packages, Procedures, Functions, Triggers, Types, Sequences, Materialized Views, Materialized View Logs, Synonyms, Public Synonyms, Database Links, Directories, Recycle Bin, Other Users, and Financials - DBA. The central pane is the SQL editor, titled "DBA - JSMITH", which shows the SQL statement "select \* from sysadm.t\_ps\_acct\_1n;". Above the editor, the execution time is shown as "0.026 seconds". Below the editor is a toolbar with buttons for "Results", "Script Output", "Explain", "DBMS Output", and "OWA Output". The "Results" pane is currently empty. At the bottom of the window, a status bar displays "All Rows Fetched: 0", "Line 1 Column 35", "Insert", "Unix: LF", and "Editing".

Oracle SQL Developer : DBA - JSMITH

File Edit View Navigate Run Debug Source Tools Help

Connections Reports

DBA - JSMITH 0.065 seconds DBA - JSMITH

Enter SQL Statement:

```
select * from sysadm.t_ps_acct_1n;
```

Results Script Output Explain DBMS Output OWA Output

Results:

	PURCHASE_PRICE	BUSINESS_UNIT	FISCAL_YEAR	PRODUCT	TRANSACTION_ID
1	13354.00	AJ123	2006	C22	T9837JR867
2	786221.00	FJ33	2006	S22	T991856123
3	81954.00	LX82	2006	Z83	T97856842
4	98174.00	LX82	2006	Z83	T918356834
5	76985.00	LX82	2006	Z83	T98568234
6	87675.00	AJ123	2006	C22	T978892384
7	27579.00	FJ33	2006	S22	T995928345
8	38692.00	ST385	2006	L11	T97384956
9	78963.00	ST385	2006	L11	T903984856
10	19877.00	ST385	2006	L11	T97728356
11	76785.00	FJ33	2006	S22	T938682934
12	45636.00	LX82	2006	Z83	T998868283
13	17733.00	AK123	2006	C22	T988612571

All Rows Fetched: 13

Line 1 Column 35 | Insert | Unix: LF | Editing

# Database Vault Administration Page

ORACLE Database Vault [Help](#) [Logout](#)

Database

Logged in as DBV\_OWNER

Database Instance: un102232

**Administration** [Database Vault Reports](#) [General Security Reports](#) [Monitor](#)

The links below allow you to protect applications and data using Oracle Database Vault features that include: Realms, Command Rules, Rule Sets, Factors, and Secure Application Roles.

**Database Vault Feature Administration**

- [Realms](#)
- [Command Rules](#)
- [Factors](#)
- [Rule Sets](#)
- [Secure Application Roles](#)
- [Label Security Integration](#)

**Administration** [Database Vault Reports](#) [General Security Reports](#) [Monitor](#)

Database | [Help](#) | [Logout](#)

# Step 1. Defining a Realm

ORACLE Database Vault [Help](#) [Logout](#)

Database Instance: un102232 > [Realm](#) > Create Realm Logged in as DBV\_OWNER

## Create Realm

[Cancel](#) [OK](#)

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

### General

\* Name

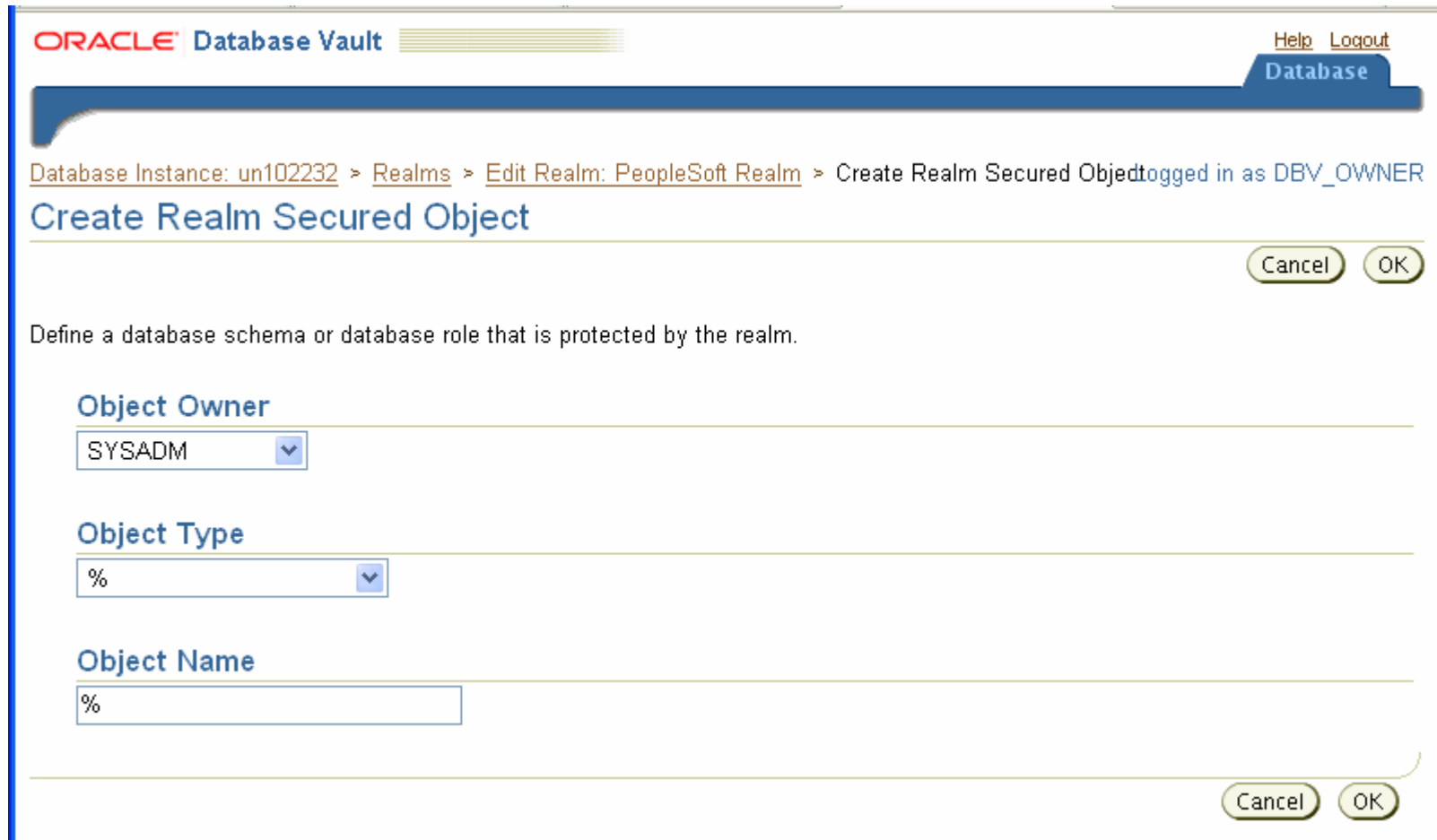
Description

Status  Enabled  
 Disabled

### Audit Options

Audit Disabled  
 Audit On Failure  
 Audit On Success or Failure

## Step 2. Adding Protected Schema



The screenshot shows the Oracle Database Vault interface for creating a secured object. The page title is "ORACLE Database Vault" and the breadcrumb trail is "Database Instance: un102232 > Realms > Edit Realm: PeopleSoft Realm > Create Realm Secured Object logged in as DBV\_OWNER". The main heading is "Create Realm Secured Object". Below the heading are "Cancel" and "OK" buttons. The instruction reads: "Define a database schema or database role that is protected by the realm." There are three input fields: "Object Owner" with a dropdown menu showing "SYSADM", "Object Type" with a dropdown menu showing "%", and "Object Name" with a text input field containing "%". At the bottom right, there are "Cancel" and "OK" buttons.

ORACLE Database Vault [Help](#) [Logout](#)  
Database

Database Instance: un102232 > Realms > Edit Realm: PeopleSoft Realm > Create Realm Secured Object logged in as DBV\_OWNER

### Create Realm Secured Object

[Cancel](#) [OK](#)

Define a database schema or database role that is protected by the realm.

**Object Owner**  
SYSADM

**Object Type**  
%

**Object Name**  
%

[Cancel](#) [OK](#)

Oracle SQL Developer : DBA - JSMITH

File Edit View Navigate Run Debug Source Tools Help

Connections Reports

DBA - JSMITH 0.026 seconds DBA - JSMITH Snippets

Enter SQL Statement:

```
select * from sysadm.t_ps_acct_1n;
```

Results Script Output Explain DBMS Output OWA Output

Results:

All Rows Fetched: 0 | Line 1 Column 35 | Insert | Unix: LF | Editing

The screenshot displays the Oracle SQL Developer application window. The title bar reads "Oracle SQL Developer : DBA - JSMITH". The menu bar includes "File", "Edit", "View", "Navigate", "Run", "Debug", "Source", "Tools", and "Help". Below the menu bar is a toolbar with icons for file operations and execution. The main workspace is divided into three panes. The left pane, titled "Connections", shows a tree view of database objects for the "DBA - JSMITH" connection, including Tables, Views, Indexes, Packages, Procedures, Functions, Triggers, Types, Sequences, Materialized Views, Materialized View Logs, Synonyms, Public Synonyms, Database Links, Directories, Recycle Bin, Other Users, and Financials - DBA. A mouse cursor is hovering over the "Views" folder. The middle pane, titled "DBA - JSMITH", shows the execution of a SQL statement: "select \* from sysadm.t\_ps\_acct\_1n;". The execution time is 0.026 seconds. The right pane, titled "Results", shows the output of the query, which is currently empty. The status bar at the bottom indicates "All Rows Fetched: 0", "Line 1 Column 35", "Insert" mode, "Unix: LF", and "Editing".

Oracle SQL Developer : DBA - JSMITH

File Edit View Navigate Run Debug Source Tools Help

Connections Reports DBA - JSMITH 0.026 seconds DBA - JSMITH Snippets

Enter SQL Statement:

```
select * from sysadm.t_ps_acct_1n;
```

**ORA-01031: insufficient privileges**

An error was encountered performing the requested operation:

ORA-01031: insufficient privileges

Error at line:1 Column:21

OK

Connections

- DBA - JSMITH
  - Tables
  - Views
  - Indexes
  - Packages
  - Procedures
  - Functions
  - Triggers
  - Types
  - Sequences
  - Materialized Views
  - Materialized View Logs
  - Synonyms
  - Public Synonyms
  - Database Links
  - Directories
  - Recycle Bin
  - Other Users
  - Financials - DBA

All Rows Fetched: 0

Line 1 Column 35 | Insert | Unix: LF | Editing



## **Demo #2:**

**Creating a Trusted Path - Limiting connection from non-application server IP addresses using Command Rules**

# Limit Access to Specific IP Addresses

## Creating a Command Rule

ORACLE Database Vault Help Logout

Database

Database Instance: un102232 > Command > Create Command Rule Logged in as DBV\_OWNER

### Create Command Rule

This page allows you to create or edit a command that can be authorized based on the evaluation of a Database Vault rule set.

#### General

\* Command

Status  Enabled  Disabled

#### Applicability

Object Owner

Object Name

#### Rule Set

# List of Allowed IP Addresses

**General**

\* Name

Description

Status  Enabled  
 Disabled

Evaluation Options  All True  
 Any True

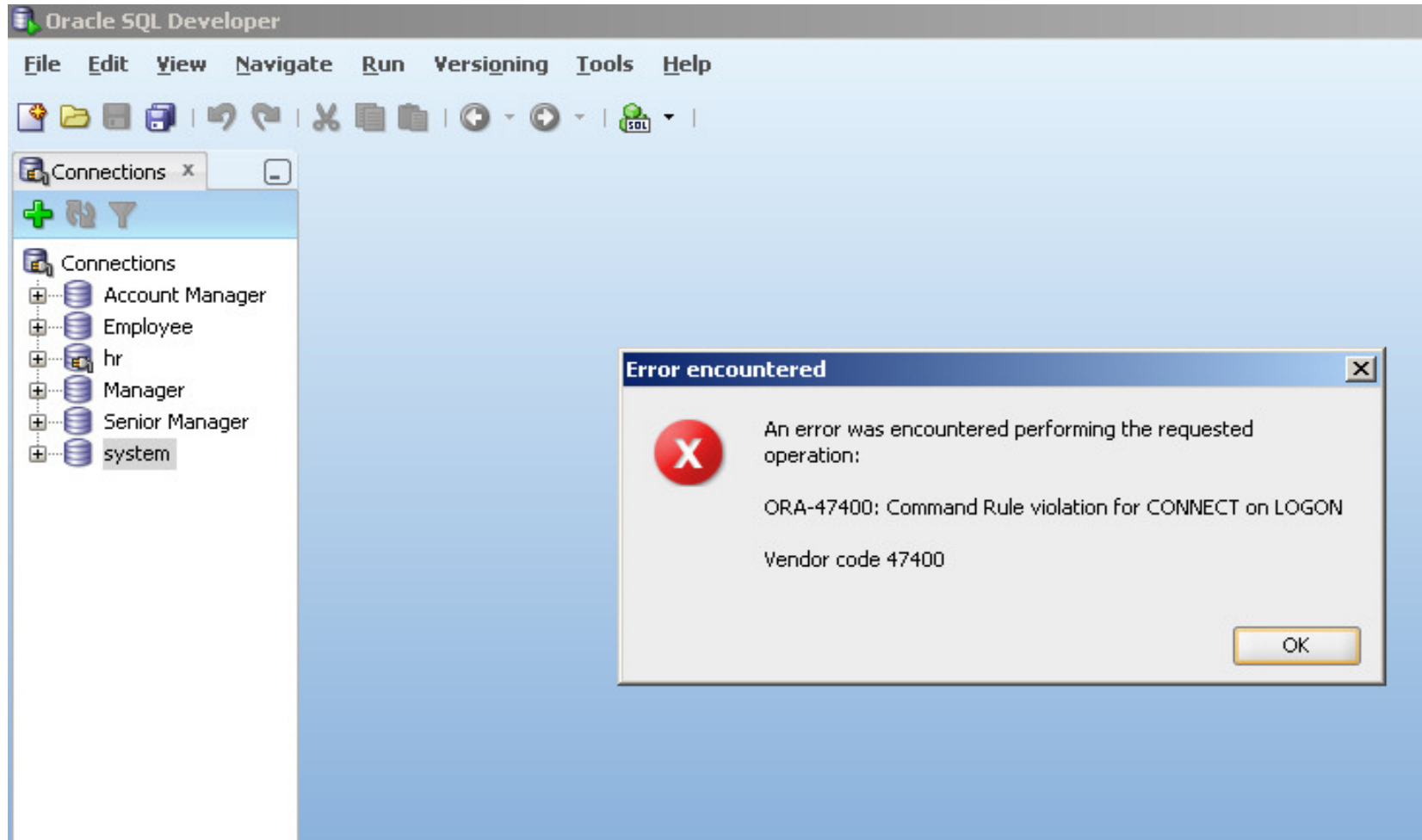
**Audit Options**

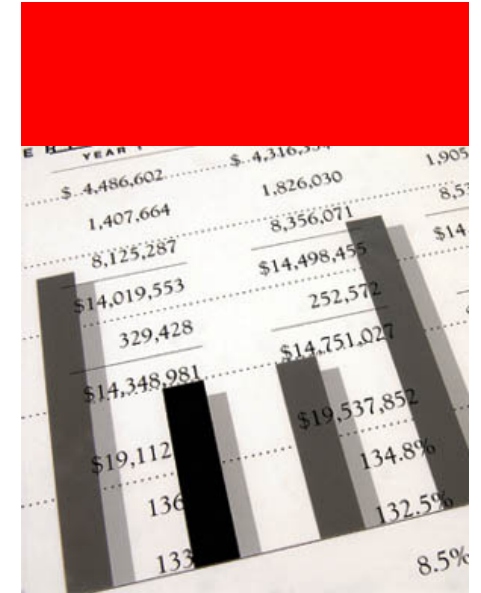
Audit Disabled  
 Audit On Failure  
 Audit On Success or Failure

**Rules Associated To The Rule Set**

Select	Rule Name <small>▲</small>	Rule Expression
<input checked="" type="radio"/>	Verify Local IP	SYS_CONTEXT('USERENV','IP_ADDRESS') IN ('130.35.46.19','130.35.49.27','130.35.56.12')

# Connection Blocked from Other IP Addresses





# Oracle Database Vault Customers

# Absa Group Limited

The screenshot shows a web browser window with the URL [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=29021&O=E&E=renee@emergingmedia.co.za](http://www.itweb.co.za/index.php?option=com_content&view=article&id=29021&O=E&E=renee@emergingmedia.co.za). The page features a navigation bar with links for 'FREE NEWSLETTERS', 'IT DIRECTORY', 'NEWS ALERTS', 'RSS', 'NEWS TIP-OFFS', and 'ADD TO FAVOURITES'. The main header includes the 'iWeb INDUSTRYSOLUTIONS' logo and a secondary navigation menu with categories like 'HOME', 'COLUMNISTS', 'IN DEPTH', 'INDUSTRY VIEWS', 'SURVEYS', 'JOBS', 'EVENTS', 'SERVICES', and 'PUBLICATIONS'. The article title is 'Absa steps up compliance with Oracle', dated 5 Jan 2010, and includes an Oracle logo. Below the title, there are tags for 'Read in this story' such as 'A need for compliance', 'A solid audit trail', 'Consistent configuration throughout Absa', and 'The road ahead'. The article text begins with: 'One of South Africa's largest financial services groups, the Absa Group Limited (Absa), has been a prominent innovator in the financial services industry and offers a complete range of banking, bank assurance and wealth management products and services.'

Premlin Pillay, Head of Group Information Services at Absa:

"Oracle Database Vault provides a security solution inside the Oracle Database, which enables our existing applications to comply with these and possibly future regulations without much customisation, ..."

# Financial Customer



## Customer Profile

- Annual revenue €39.283 Billion
- Over 2000 employees
- Located in Dusseldorf, Germany

## Challenge

- Meet internal and external compliance requirements
- Streamline data management, consolidate applications
- Protect the privacy and security of very sensitive data

## Solution

- **Oracle Database Vault**
  - Separation of Duties
  - Realms and Command Rules to restrict DBAs access to data
  - Consolidate multiple applications into one DB

## Results

“With this new solution provided by Oracle our highly sensitive personal data is now protected against unauthorized access. We therefore were able, to integrate our hr applications into our centralized IT and save cost.”  
Detlev Althaus, Deutsche Apotheker



## Customer Profile

- Annual revenue \$312 million
- Over 1000 employees
- Located in London, United Kingdom

## Challenge

- Meet internal and external compliance requirements
- Streamline data management, consolidate applications
- Protect the privacy and security of very sensitive data

## Solution

- **Oracle Database Vault**
  - Separation of Duties
  - Realms and Command Rules to restrict DBAs access to data
  - Consolidate multiple applications into one DB

## Results

“Our aim is to have the most secure database systems in our industry which protect our client data and our business from internal and external threats. The Oracle security components underpinning our standard Oracle security configuration bring a new level of assurance to our senior management and audit teams.”

Akash Gharu, Global Database Services Manager



대우증권



DAEWOO  
SECURITIES

Financial Customer



### Customer Profile

- Investment banking and brokerage service
- Over 3000 employees
- Located in Seoul, Korea

### Challenge

- Meet internal and external compliance requirements
- Prevent privileged user access to sensitive data
- Enhance security without rebuilding the application code

### Solution


- **Oracle Database Vault and Oracle Advanced Security**
  - Separation of Duties
  - Realms and Command Rules to restrict DBAs access to data
  - Use Transparent Data Encryption for encryption

### Results

“We used Oracle’s database security solutions to resolve internal security issues, a common challenge for financial institutions. Oracle Database Vault offers internal controls that help secure human resources data, while Oracle Advanced Security has automated encryption functions that further protects sensitive information.” – Jung HakSoo, Deputy Manager, Infrastructure Development Department, Daewoo Securities

ORACLE®

# SAP Utility Customer – Hydro One

	<p>“Oracle Database Vault is helping Hydro One to further address regulatory compliance,” said Norman Crook, Director IT Service Delivery, Hydro One Networks Inc. “With Oracle Database Vault, Hydro One is positioned to complete the final stages of the SAP security roadmap, further strengthening the security policies safeguarding our data.”</p>
<b>Challenge</b>	<ul style="list-style-type: none"><li>• Meet internal and external compliance requirements - NERC</li><li>• Protect the privacy and security of SAP sensitive data</li><li>• Prevent any tampering of data by privileged users</li></ul>
<b>Solution</b>	<ul style="list-style-type: none"><li>• <b>Oracle Database Vault</b><ul style="list-style-type: none"><li>– Apply Database Vault Protections for SAP</li><li>– Realms and Command Rules to restrict DBAs access to sensitive data</li><li>– Multi-Factor authorization to further enhance data security</li></ul></li></ul>
<b>Results</b>	<ul style="list-style-type: none"><li>• Ensure compliance with regulations – NERC Regulations</li><li>• Reduce the risk of data breaches and impropriety</li><li>• Enhance SAP Application Availability by gaining confidence that no user can change database objects without the Security Administrator’s approval</li></ul>

## Oracle Database Vault (DBV)

Regulatory Legislation	Regulation Requirement	Does DBV Mitigate This Risk?
Sarbanes-Oxley Section 302	Unauthorized changes to data	Yes
Sarbanes-Oxley Section 404	Modification to data, Unauthorized access	Yes
Sarbanes-Oxley Section 409	Denial of service, Unauthorized access	Yes
Gramm-Leach-Bliley	Unauthorized access, modification and/or disclosure	Yes
HIPAA 164.306	Unauthorized access to data	Yes
HIPAA 164.312	Unauthorized access to data	Yes
Basel II – Internal Risk Management	Unauthorized access to data	Yes
CFR Part 11	Unauthorized access to data	Yes
Japan Privacy Law	Unauthorized access to data	Yes
PCI – Requirement 7	Restrict access to cardholder data by business need-to-know	Yes
PCI – Requirement 8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed	Yes
PCI – Compensating Controls for Requirement 3.4	Provide ability to restrict access to cardholder data or databases based on the following criteria: <ul style="list-style-type: none"> <li>▪ IP address/Mac address</li> <li>▪ Application/service</li> <li>▪ User accounts/groups</li> </ul>	Yes
PCI - Requirement A.1: Hosting providers protect cardholder data environment	Ensure that each entity only has access to own cardholder data environment	Yes



# Summary

- Restrict full access of privileged users
  - Restrict access to application data stored in the database
  - Enforce Separation of duty controls
- Easily implement environment based access control
  - User parameters
  - Network parameters
  - Database parameters
- Applying on existing applications
  - Highly transparent
- Minimal performance impact
  - Less than 5%



# For More Information

search.oracle.com

Search for:  In the section:   [Refine Search](#)

[oracle.com/database/security](https://oracle.com/database/security)



Q&A



**ORACLE IS THE INFORMATION COMPANY**