




**ORACLE®**

## **Oracle Database Vault**

Kamal Tbeileh

Senior Principal Product Manager, Database Security



The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

# Agenda

- Regulatory Compliance and Application Security
- Oracle Database Vault Overview
- Oracle Database Vault Protection for Applications
  - PeopleSoft, E-Business Suite, Siebel, ... and more
- Where to go for more information
- Q&A

# Application Data Security & Compliance

## Business Drivers

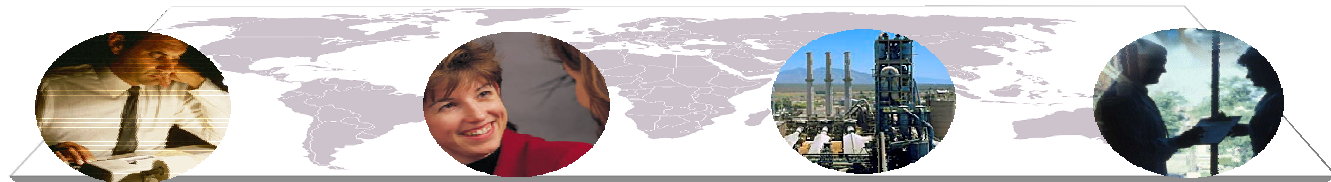
Security  
Threats

Industrial Espionage

Identity Theft

Insider Threats

Data Consolidation  
Globalization  
Right Sourcing



Compliance  
Mandates

SOX

HIPAA

PCI

EU  
Directives

JSOX

Basel II

GLBA

SB1386

# Application Data Security & Compliance

## Continuous Innovation

Oracle Database 11g

Data Masking

TDE Tablespace Encryption

Oracle Total Recall

Oracle Audit Vault

Oracle Database 10g

Oracle Database Vault

Transparent Data Encryption (TDE)

Real Time Masking

Oracle Database 9i

Secure Config Scanning

Fine Grained Auditing

Oracle Label Security

Oracle8i

Enterprise User Security

Virtual Private Database (VPD)

Database Encryption API

Strong Authentication

Oracle7

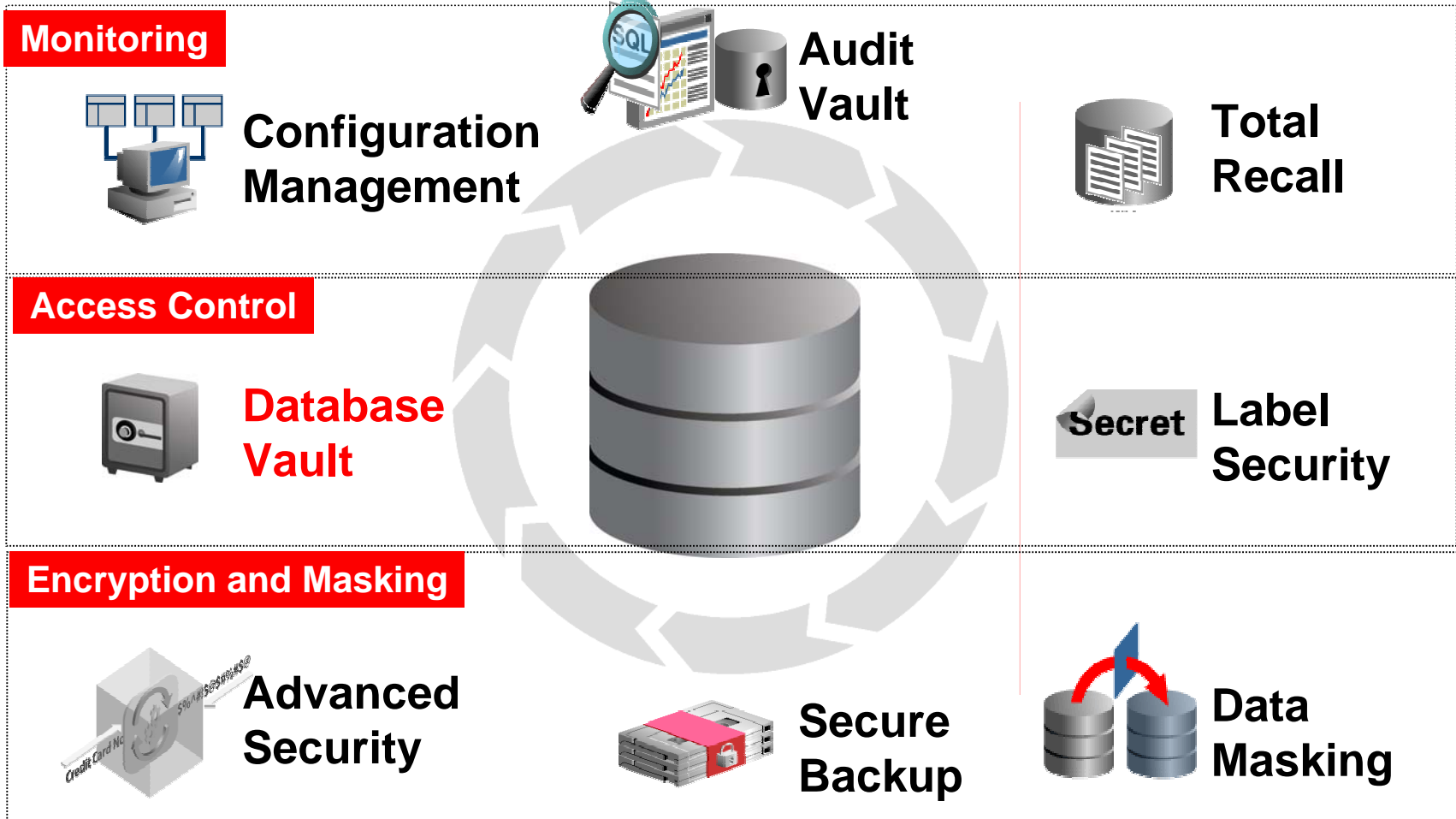
Native Network Encryption

Database Auditing

Government customer

# Application Data Security & Compliance

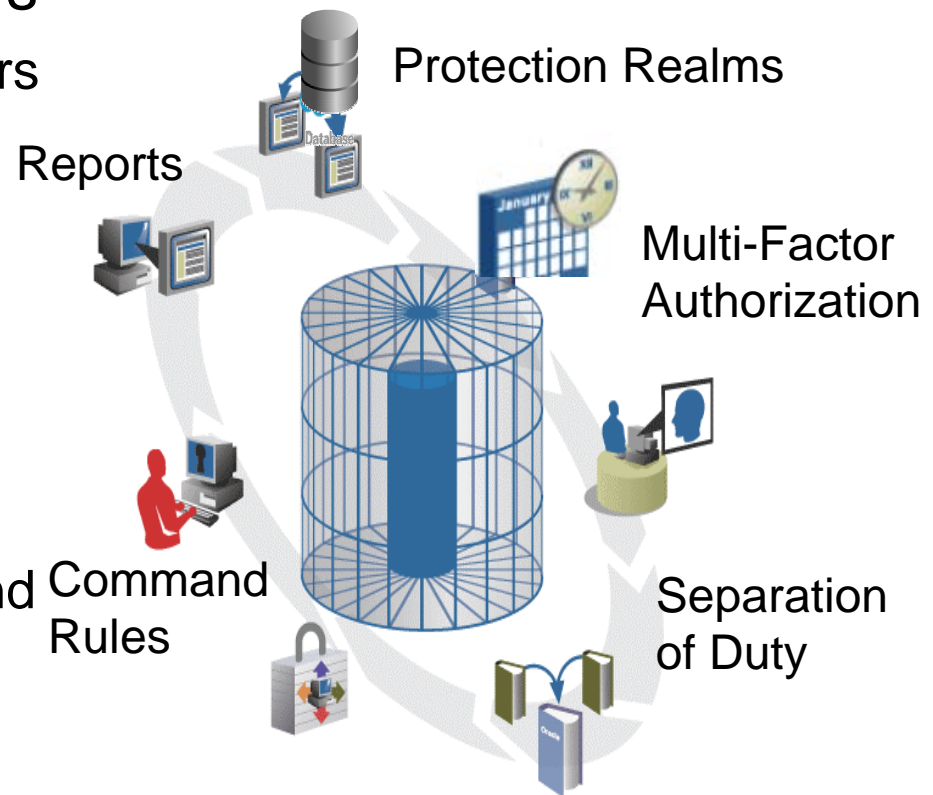
## Defense-in-Depth



# Application Data Security & Compliance

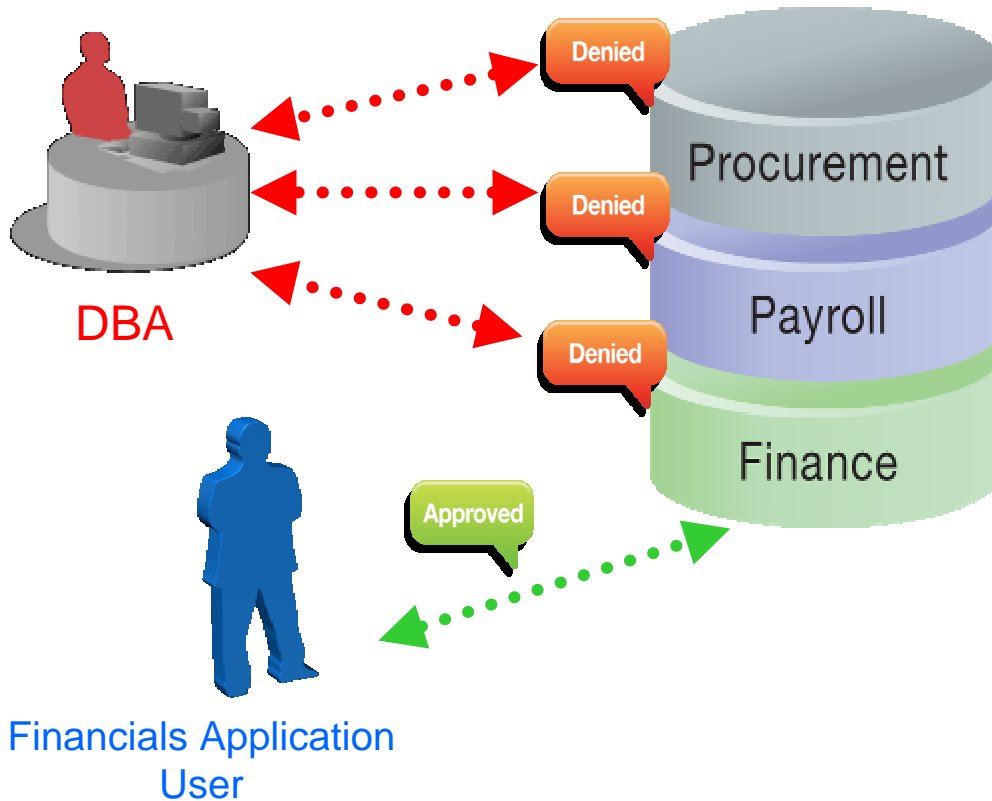
## Oracle Database Vault

- Controls on privileged users
  - Restrict highly privileged users from application data
  - Provide Separation of Duty
  - Security for database and information consolidation
- Real time access controls
  - Control who, when, where and how data is accessed
  - Make decision based on IP address, time, auth...



# Oracle Database Vault

## Control Access to Application Data



### Benefits

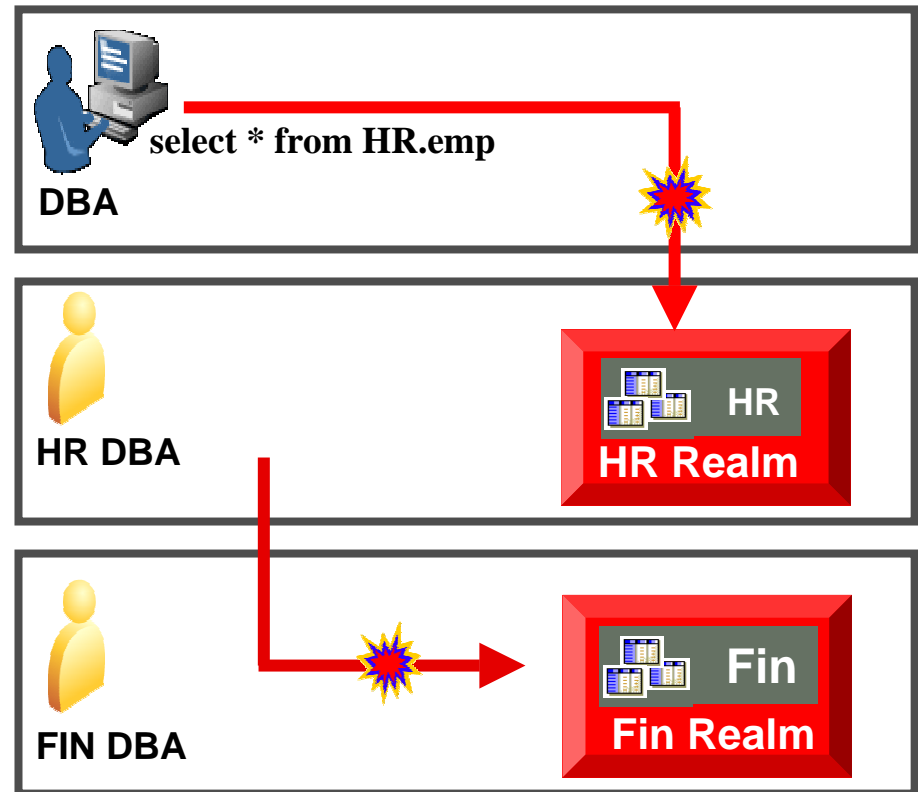
- ✓ Transparently prevent admin access to application data with “Realms”
- ✓ Control SQL commands and other database operations
- ✓ Enforce whom, how, where, and when with multi-factor authorization
- ✓ Get Separation-of-duty
- ✓ Securely consolidate databases
- ✓ No application changes required



# Oracle Database Vault

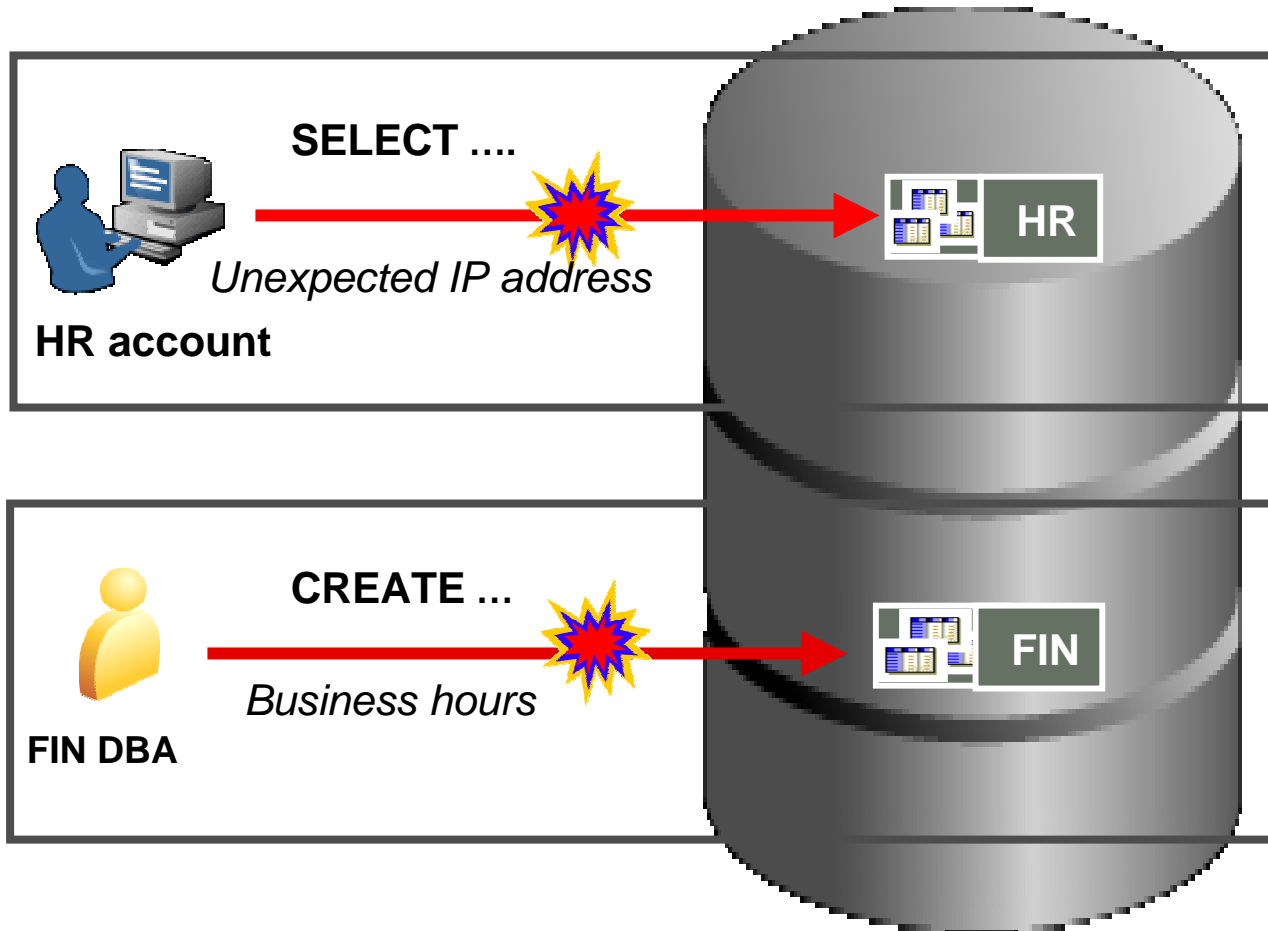
## Protection Realms

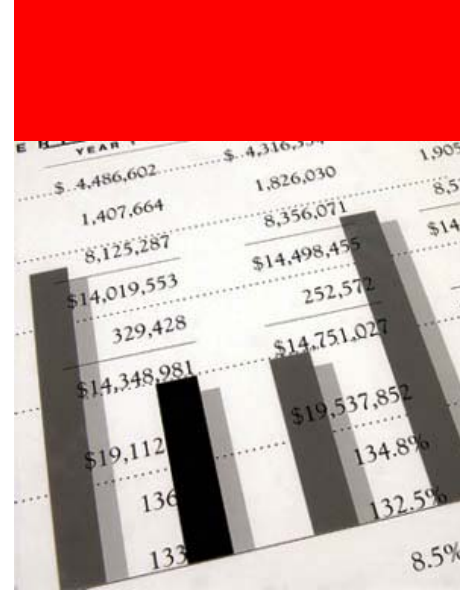
- Database DBA views HR data  
**Compliance and protection from insiders**
- HR DBA views Fin. data  
**Eliminates security risks from server consolidation**



# Oracle Database Vault

## Transparent Multi-factor Authorization





**Example:**

**Protecting application data from  
Database privileged users**

Connections

Reports

DBA - JSMITH

0.026 seconds

DBA - JSMITH

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

Enter SQL Statement:

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

Results

Script Output

Explain

DBMS Output

OWA Output

Results:



Connections Reports



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

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

# 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

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

## Create Realm

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. At the top left is the 'ORACLE Database Vault' logo. At the top right are 'Help' and 'Logout' links, and a 'Database' tab. Below the header is a breadcrumb trail: 'Database Instance: un102232 > Realms > Edit Realm: PeopleSoft Realm > Create Realm Secured Object logged in as DBV\_OWNER'. The main title is 'Create Realm Secured Object'. There are 'Cancel' and 'OK' buttons at the top right. 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



Connections

Reports

DBA - JSMITH

0.026 seconds

DBA - JSMITH

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

Enter SQL Statement:

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

Results

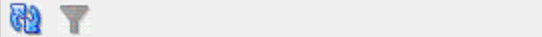
Script Output

Explain

DBMS Output

OWA Output

Results:



- 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

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

SQL Output



**Example:**

**Limiting connection from non-application  
server IP addresses**

# 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

iSQL\*Plus



Error

ERROR - ORA-47400: Command Rule Violation for CONNECT on LOGON

## Login

Unauthorized use of this site is prohibited and may be subject to civil and criminal prosecution.

\* Indicates required field

* Username	<input type="text" value="sysadm"/>
* Password	<input type="password"/>
Connect Identifier	<input type="text" value="un102232"/>
	<input type="button" value="Login"/>



# Application Data Security & Compliance

## Oracle Database Vault & Grid Control

# Enterprise Manager Grid Control

## Database Vault Target

ORACLE Enterprise Manager 10g  
Grid Control

[Setup](#) [Preferences](#) [Help](#) [Logout](#)

[Home](#) [Targets](#) [Deployments](#) [Alerts](#) [Compliance](#) [Jobs](#) [Reports](#)

[Hosts](#) | [Databases](#) | [Web Applications](#) | [Services](#) | [Systems](#) | [Groups](#) | [All Targets](#)

Database Instance: **dv10205**

[Home](#) [Performance](#) [Availability](#) [Server](#) [Schema](#) [Data Movement](#) [Software and Support](#)

Page Refreshed Jan 16, 2009 3:23:57 PM PST [Refresh](#) View Data [Automatically \(60 sec\)](#) ▼

General

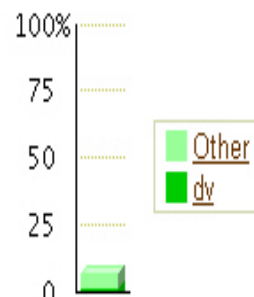


[Shutdown](#) [Black Out](#)

Status [Up](#)  
Up Since **Dec 16, 2008 10:28:11 PM PST**  
Instance Name **dv**  
Version **10.2.0.5.0**  
**Database Vault Enabled**  
Host [stadk38.us.oracle.com](#)  
Listener

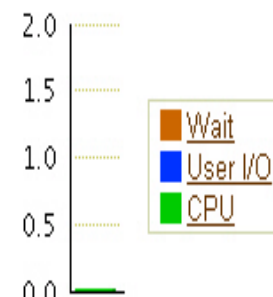
[View All Properties](#)

Host CPU



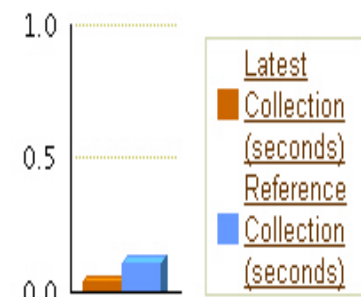
Load [1.59](#) Paging [0.03](#)

Active Sessions



Core Count **2**

SQL Response Time



SQL Response Time (%) [35.29](#)

[Edit Reference Collection](#)



# Enterprise Manager Grid Control

## Database Vault Generated Alerts

### Alerts

Category All  Critical **X** 4 Warning **!** 2

Severity	Category	Name	Message	Alert Triggered
<b>X</b>	Database Vault Policy Changes	Database Vault Policy Changes Count	<u>Rules have Policy Changes.</u>	Jan 16, 2009 8:45:49 AM
<b>X</b>	Database Vault Policy Changes	Database Vault Policy Changes Count	<u>Realms have Policy Changes.</u>	Jan 16, 2009 8:45:49 AM
<b>X</b>	Database Vault Policy Changes	Database Vault Policy Changes Count	<u>Factors have Policy Changes.</u>	Jan 16, 2009 8:45:49 AM
<b>X</b>	Database Vault Policy Changes	Database Vault Policy Changes Count	<u>Command Rules have Policy Changes.</u>	Jan 16, 2009 8:45:49 AM
<b>!</b>	Invalid Objects by Schema	Owner's Invalid Object Count	<u>9 object(s) are invalid in the WMSYS schema.</u>	Jan 16, 2009 9:01:11 AM
<b>!</b>	Invalid Objects by Schema	Owner's Invalid Object Count	<u>22 object(s) are invalid in the SYS schema.</u>	Jan 16, 2009 9:01:11 AM



# Application Data Security & Compliance

## Oracle Database Vault & PeopleSoft

# Application Data Security & Compliance

## PeopleSoft Protection with Oracle Database Vault

- All PeopleSoft modules are protected
  - Realm that protects PeopleSoft (SYSADM schema)
  - A CONNECT Command Rule that ensures
    - Access through middle tier
    - Access from trusted IP addresses
  - A SELECT Command Rule restricts Application DBA access
- Separation of Duty
  - Database Account Manager
  - Security Administrator
  - Application DBA
- Extensible
  - Customer can create additional realms and command rules

# Application Data Security & Compliance

## PeopleSoft supported versions with Database Vault

- PeopleSoft apps less than 8.4 (e.g.. 8.0, 8.1, 8.3)
  - Must be on PeopleTools 8.22
- PeopleSoft apps 8.4 or greater (e.g.. 8.4, 8.8, 8.9, 9.0 and higher)
  - Must be on PeopleTools 8.46 or greater
- Oracle Database versions:
  - Oracle Database 10.2.0.3 or 10.2.0.4 (recommended)
  - Oracle Database 9.2.0.8
  - Oracle Database 11g release

<i>Authorized with Rule Set</i> <i>Protection Type</i>	SYSADM	PSFTDBA	SYSTEM	DBA
PeopleSoft Realm	OWNER	OWNER	No Access	No Access
Select Command Rule	Not Restricted	Limit PSFTDB Rule Set	No Access	No Access
Connect Command Rule	PeopleSoft Access Rule Set	Not Restricted	Not Restricted	Not Restricted
Drop Tablespace Command Rule	Disabled Rule Set	Disabled Rule Set	Disabled Rule Set	Disabled Rule Set

# Pharmaceutical Services Customer



## Customer Profile

- Over 11K employees, with revenue over \$500 Million
- 15 databases
- Solaris Platform

## Challenge

- Meet internal and external compliance requirements
- Streamline data management, optimizing a lean IT staff
- 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 PeopleSoft
  - Multi-factor authorization to prevent application by-pass

## Results

- Ensure compliance with regulation such as Sarbanes-Oxley
- Reduce the risk of data breaches and impropriety by limiting access to sensitive information with preventive controls
- Save time and money by implementing The Oracle-provided PeopleSoft-specific Database Vault protection policies



# Application Data Security & Compliance

## Oracle Database Vault & E-Business Suite

# Application Data Security & Compliance

## E-Business Suite Protection with Database Vault

- E-Business Suite data protected
  - Oracle Database Vault **pre-seeded Realms** prevent access by unauthorized privileged users to E-Business Suite application data
  - All E-Business Suite modules are **Protected**
  - Oracle Database Vault **Separation of Duty** prevents new account creation or ad hoc changing of passwords
- Extensible
  - Define custom command rules to **restrict ad-hoc access** to specific Factors such as IP addresses or subnets
  - Define **custom realms** for E-Business Suite custom schemas



# Application Data Security & Compliance

## EBS with Database Vault best practices

- Treat the SYSTEM account the same way as APPS account
  - SYSTEM account is required to run the AD utilities
- Monitoring
  - Audit using database auditing during patching for SYSTEM and APPS
  - Mitigate the risk of accessing data during patching
- Manage accounts passwords when not doing patching
  - Security Administrator should own the passwords for these accounts

# Application Data Security & Compliance

## EBS with Database Vault supported versions

- Certified Configurations
  - E-Business Suite Release 11.5.10.CU2 or 12.0 and higher
  - Oracle Database 10.2.0.4
  - Oracle Database 11.1.0.7 will be certified soon
- Documentation
  - Integrating Oracle E-Business Suite Release 12 with Oracle Database Vault 10gR2 (Note 566841.1)
  - Integrating Oracle E-Business Suite Release 11i with Oracle Database Vault 10gR2 (Note 428503.1)

# Oracle Database Vault

## E-Business Suite Application Protection Matrix

Realm Name	What is Protected?	Who is authorized to access?
EBS Realm	All tables in Oracle E-Business Suite 11i Product Schemas	All Oracle E-Business Suite 11i Product Schemas and APPS, APPLSYS, SYSTEM, CTXSYS
EBS Realm - Applsyst Schema	Most tables in the APPLSYS Schema	APPS, APPLSYS, SYSTEM and CTXSYS
EBS Realm - Apps Schema	All objects in the APPS Schema (except the views)	APPS, APPLSYS, SYSTEM, CTXSYS and All product schemas, that uses intermedia indexes
EBS Realm - Applsystpub Schema	Objects required for EBS authorization	APPS, APPLSYS, SYSTEM, APPLSYSPUB and CTXSYS
EBS Realm - MSC Schema	Tables in the MSC Schema - except those, which require partitions to be exchanged (see script for full details)	APPS, APPLSYS, SYSTEM, CTXSYS and MSC
CTXSYS Data Dictionary	Objects in the CTXSYS Schema	All Oracle E-Business Suite 11i Product Schemas and APPS, APPLSYS, SYSTEM

# Global Financial Services Customer



## Customer Profile

- Over 100K employees, with revenue over \$50 Billion
- Over 800 databases
- Solaris, Linux x86-64, and AIX Platforms

## Challenge

- Meet internal and external compliance requirements
- Streamline data management, optimizing a lean IT staff
- Protect the privacy and security of very sensitive client data

## Solution

- **Oracle Database Vault**
  - Separation of Duties
  - Realms and Command Rules to restrict DBAs access to sensitive data
  - Multi-factor authorization to prevent application by-pass

## Results

- Ensure compliance with regulation such as Sarbanes-Oxley
- Reduce the risk of data breaches and impropriety by limiting access to sensitive information with preventive controls
- Save over \$15 mil a year by outsourcing/off-shoring backend operations while still be compliant with regulations



# Application Data Security & Compliance

## Oracle Database Vault & Siebel

# Application Data Security & Compliance

## Siebel Protection with Oracle Database Vault

- All Siebel modules are protected
  - Siebel Realm protects the Siebel database schema
  - CONNECT Command Rule that ensures
    - Access through middle tier
    - Access from trusted IP addresses
  - SELECT Command Rule restricts SIEBELDBA data access
- Separation of Duty
  - Database Account Manager
  - Security Administrator
  - Application DBA: SIEBELDBA user
- Extensible
  - Customer can create additional realms and command rules

# Application Data Security & Compliance

## Siebel Supported Versions

- All Siebel modules are supported
  - Service, Sales, Marketing, ...etc
- Siebel 7.7 and above versions are supported
  - 7.7
  - 7.8
  - 8.x
- Oracle DB Versions:
  - Oracle Database 10.2.0.4
  - Oracle Database 11.1.0.7

# Global Telecom Services Customer



## Customer Profile

- Over 80K employees, with revenue over \$30 Billion
- Over 200 databases
- Solaris, Linux x86-64, and HPUX Platforms

## Challenge

- Meet internal and European compliance requirements
- Prevent any tampering or deletion of database objects
- Protect the privacy and security of very sensitive client data

## Solution

- **Oracle Database Vault**
  - Separation of Duties
  - Realms and Command Rules to restrict DBAs access to sensitive data
  - Command Rules to prevent any tampering of database objects

## Results

- Ensure compliance with regulations - European privacy laws
- Reduce the risk of data breaches and impropriety
- Enhance Application Availability by gaining confidence that no user can change database objects without the Security Administrator's approval



<b>Authorized with Rule Set</b> <b>Protection Type</b>	<b>SIEBEL</b>	<b>SIEBELDBA</b>	<b>SADMIN</b>	<b>DBA And SYSTEM</b>
<b>Siebel Realm</b>	OWNER	OWNER	Access through middle tier	No Access
<b>Select Command Rule</b>	Not Restricted	Restrict Select Rule Set	Not Restricted	No Access
<b>Connect Command Rule</b>	Siebel Access Rule Set	Not Restricted	Siebel Access Rule Set	Not Restricted
<b>Drop Tablespace Command Rule</b>	Disabled Rule Set	Disabled Rule Set	Disabled Rule Set	Disabled Rule Set

# Application Data Security & Compliance

## Application Protection Summary with Database Vault

### Application / Product

- PeopleSoft Applications
- E-Business Suite Applications
- Oracle Siebel Applications
- JDE Applications
- Partner applications (SAP)
- Oracle Content DB
- Oracle Internet Directory

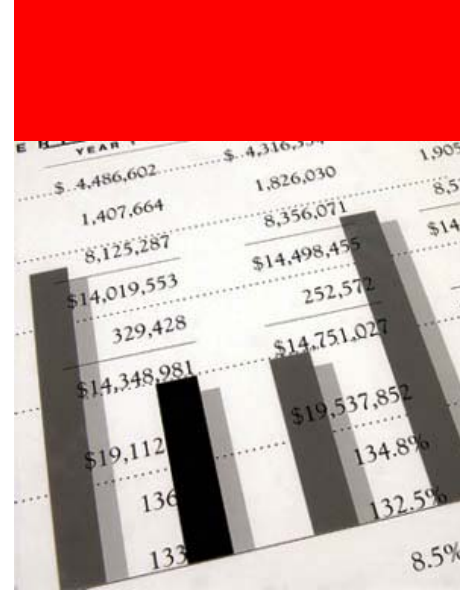
### Protection Status



(In progress)

(In progress)





# Application Data Security & Compliance

## Summary

# Application Data Security & Compliance

## Oracle Database Vault - Summary



- Enforce Separation of Duty for the Database
- Prevent DBA access to sensitive data
- Protect applications using Protection templates available for download for:
  - PeopleSoft, EBS, and Siebel
- Use Enterprise Manager Grid Control integration
- Apply on all of your existing Database releases:
  - Oracle Database Releases 11g, 10g, and even 9i
- Achieve Better JSOX compliance for the Database

# Learn More



## Database Vault technical details

- <http://www.oracle.com/technology/deploy/security/database-security/database-vault/index.html>



## Steven Chan blog

- <http://blogs.oracle.com/schan>



## PeopleSoft's Database Vault Protection templates:

- [http://www.oracle.com/technology/software/products/database\\_vault/index.html](http://www.oracle.com/technology/software/products/database_vault/index.html)



## Siebel's Database Vault protection templates

- [http://www.oracle.com/technology/software/products/database\\_vault/index.html](http://www.oracle.com/technology/software/products/database_vault/index.html)



Q&A



**ORACLE IS THE INFORMATION COMPANY**