The 10 Principles of Security in Modern Cloud Applications

Nigel King, Vice President, Oracle

In-Depth Seminars – D11

Safe Harbor Statement

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.

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

The Context for Applications

The Enterprise

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Functional Footprint – Role Based Access Control

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Functional Footprint – Role Based Access Control

ORACLE

Fusion Procurement

INTERNAL USERS

- Buyer
- Category Manager
- Procurement Manager
- Procurement Contracts Administrator
- Procurement Catalog Administrator
- Procurement Applications Administrator
- Supplier Administrator
- Sourcing Project Collaborator

EXTERNAL USERS

- Supplier Bidder
- Supplier Accounts Receivable Specialist
- Supplier Customer Service Representative
- Supplier Demand Planner
- Supplier Sales Representative
- Supplier Self Service Administrator
- Supplier Self Service Clerk

190 Seeded Job Roles across over 83 Applications

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

BENEFITS OF FUSION SECURITY

USABILITY

- Clean Access Model
- Seamless Transition to IDM

PRODUCTIVITY

- Faster On boarding
- SSO
- Management Approval Workflows
- Easier Regulatory Compliance

RISK

- Secure Out of The Box
- Across Tools
- Across the Info Lifecycle
- SOD

ADMINISTRATIVE COSTS

- Role Provisioning
- Transparent Policies
- Standards Based

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

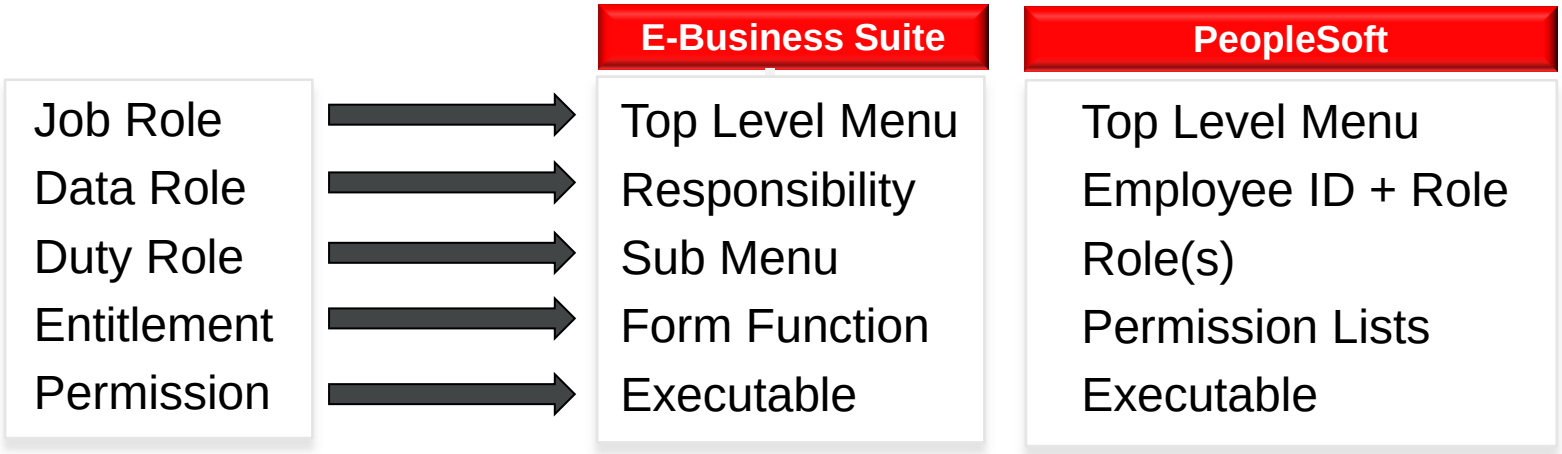
The 10 Principles

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

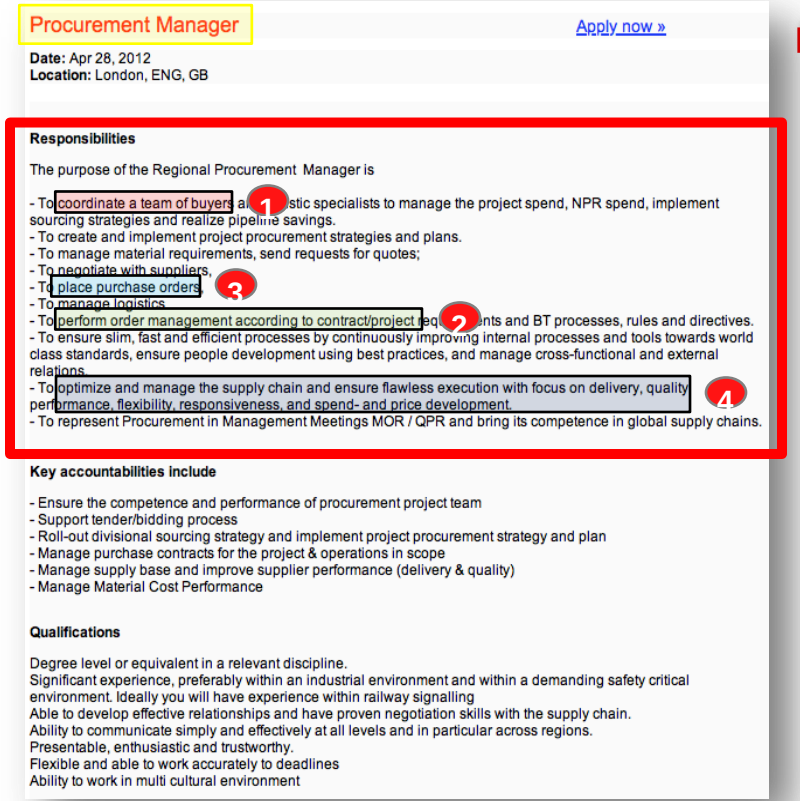
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Fusion Applications Security



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

A Role is a Job Description



Procurement Manager

Apply now »

Date: Apr 28, 2012
Location: London, ENG, GB

Responsibilities

The purpose of the Regional Procurement Manager is

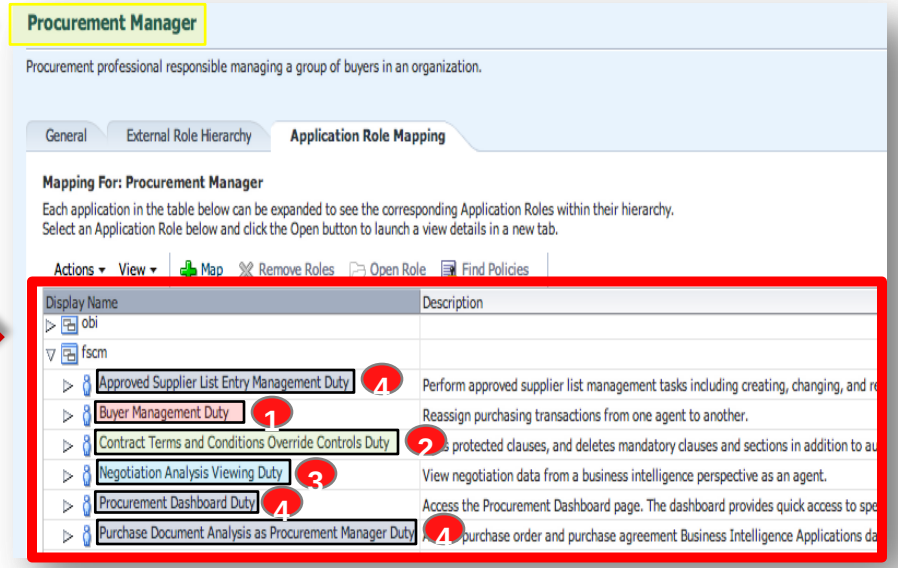
- To coordinate a team of buyers a[illegible]stic specialists to manage the project spend, NPR spend, implement sourcing strategies and realize pipeline savings.
- To create and implement project procurement strategies and plans.
- To manage material requirements, send requests for quotes;
- To negotiate with suppliers,
- To place purchase orders;
- To manage logistics
- To perform order management according to contract/project req[illegible]nts and BT processes, rules and directives.
- To ensure slim, fast and efficient processes by continuously improving internal processes and tools towards world class standards, ensure people development using best practices, and manage cross-functional and external relations.
- To optimize and manage the supply chain and ensure flawless execution with focus on delivery, quality performance, flexibility, responsiveness, and spend- and price development.
- To represent Procurement in Management Meetings MOR / QPR and bring its competence in global supply chains.

Key accountabilities include

- Ensure the competence and performance of procurement project team
- Support tender/bidding process
- Roll-out divisional sourcing strategy and implement project procurement strategy and plan
- Manage purchase contracts for the project & operations in scope
- Manage supply base and improve supplier performance (delivery & quality)
- Manage Material Cost Performance

Qualifications

Degree level or equivalent in a relevant discipline.
Significant experience, preferably within an industrial environment and within a demanding safety critical environment. Ideally you will have experience within railway signalling
Able to develop effective relationships and have proven negotiation skills with the supply chain.
Ability to communicate simply and effectively at all levels and in particular across regions.
Presentable, enthusiastic and trustworthy.
Flexible and able to work accurately to deadlines
Ability to work in multi cultural environment



Procurement Manager

Procurement professional responsible managing a group of buyers in an organization.

General | External Role Hierarchy | Application Role Mapping

Mapping For: Procurement Manager

Each application in the table below can be expanded to see the corresponding Application Roles within their hierarchy.
Select an Application Role below and click the Open button to launch a view details in a new tab.

Actions ▾ View ▾ Map Remove Roles Open Role Find Policies

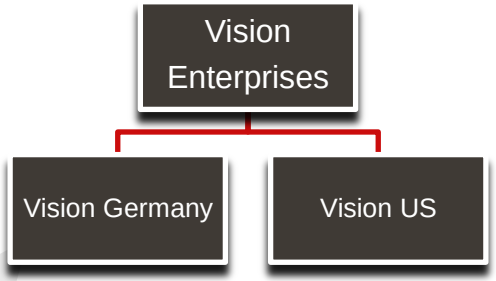
Display Name	Description
obi	
fscm	
Approved Supplier List Entry Management Duty	Perform approved supplier list management tasks including creating, changing, and re
Buyer Management Duty	Reassign purchasing transactions from one agent to another.
Contract Terms and Conditions Override Controls Duty	s protected clauses, and deletes mandatory clauses and sections in addition to au
Negotiation Analysis Viewing Duty	View negotiation data from a business intelligence perspective as an agent.
Procurement Dashboard Duty	Access the Procurement Dashboard page. The dashboard provides quick access to spe
Purchase Document Analysis as Procurement Manager Duty	purchase order and purchase agreement Business Intelligence Applications da

A Duty is what you do in that Role.

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

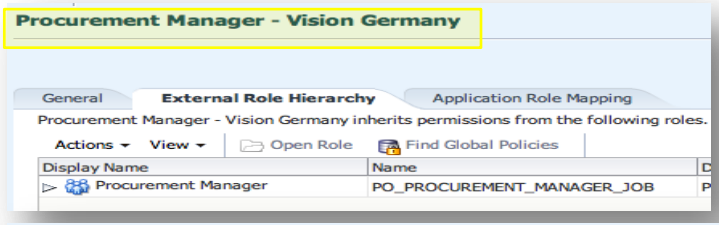
Once a New Employee is inducted, You grant them a Role

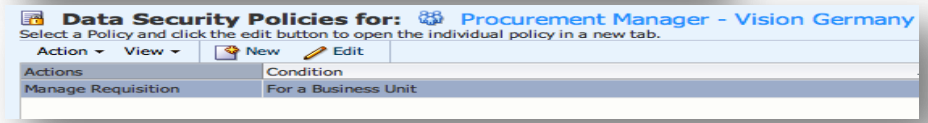
Employee Joins As Purchasing Manager of Vision Germany



Roles not tied to Job but to Employee, such as
- Employee (ERs)
- Purchase Requisitioner

We call these roles:
Abstract Roles





Employee is Granted the Purchasing Manager Role with Data Secured by Vision Germany. We call these roles: Data Roles

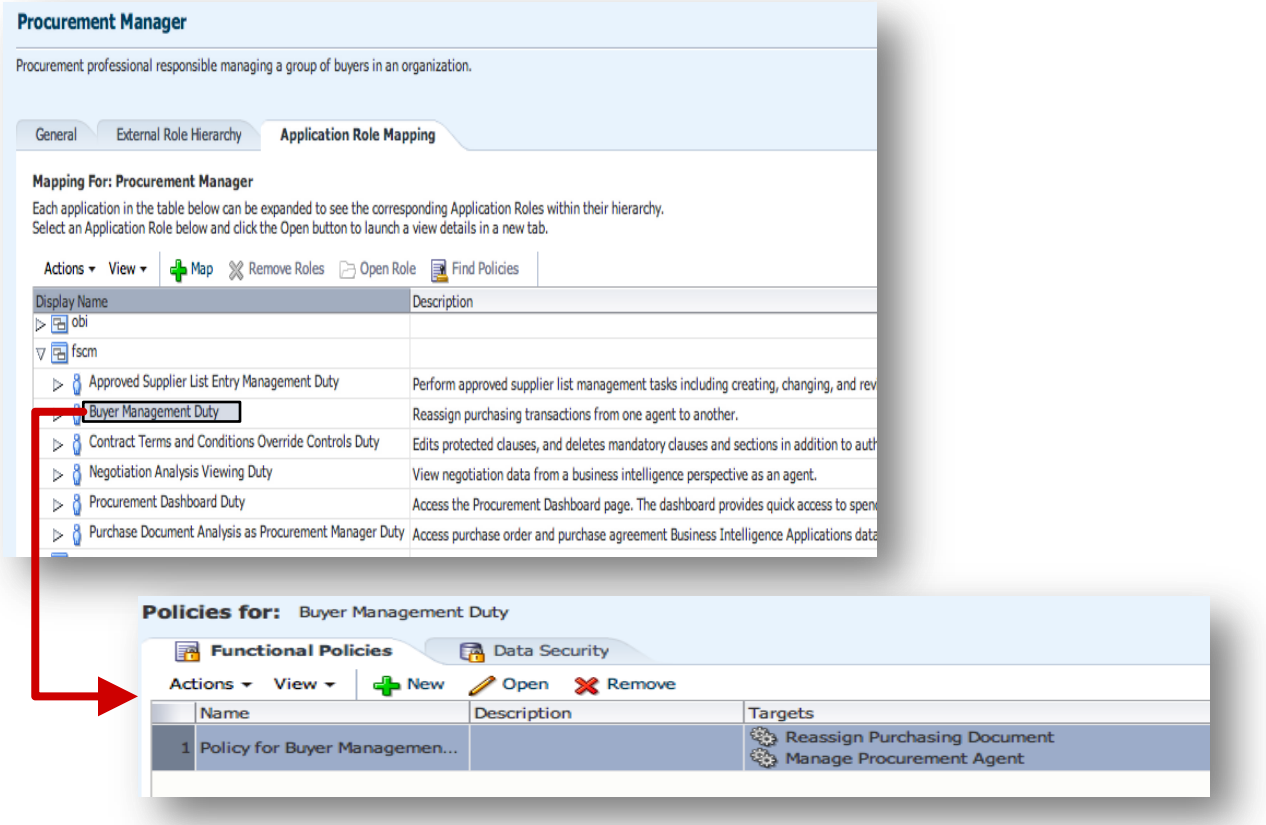
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

What can the new Employee Do and View ?

Based on their Role assignment the Employee has duties.

Each of these duties provides access to functionality in Fusion Apps.

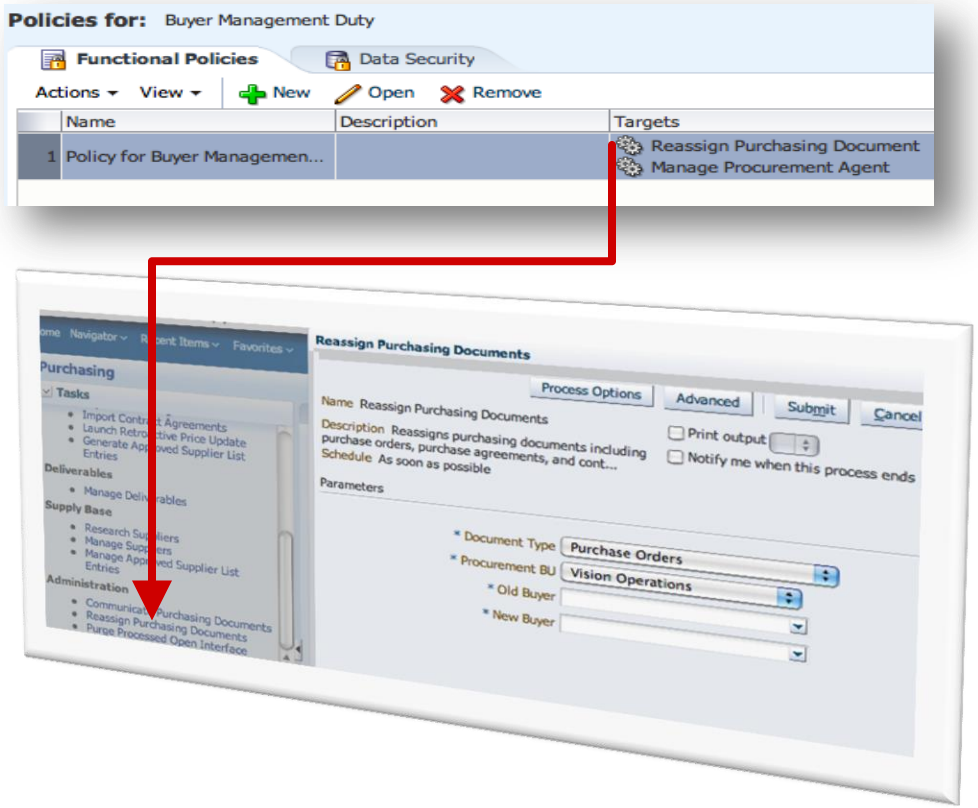
This Access to Functionality is what we call Entitlements



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

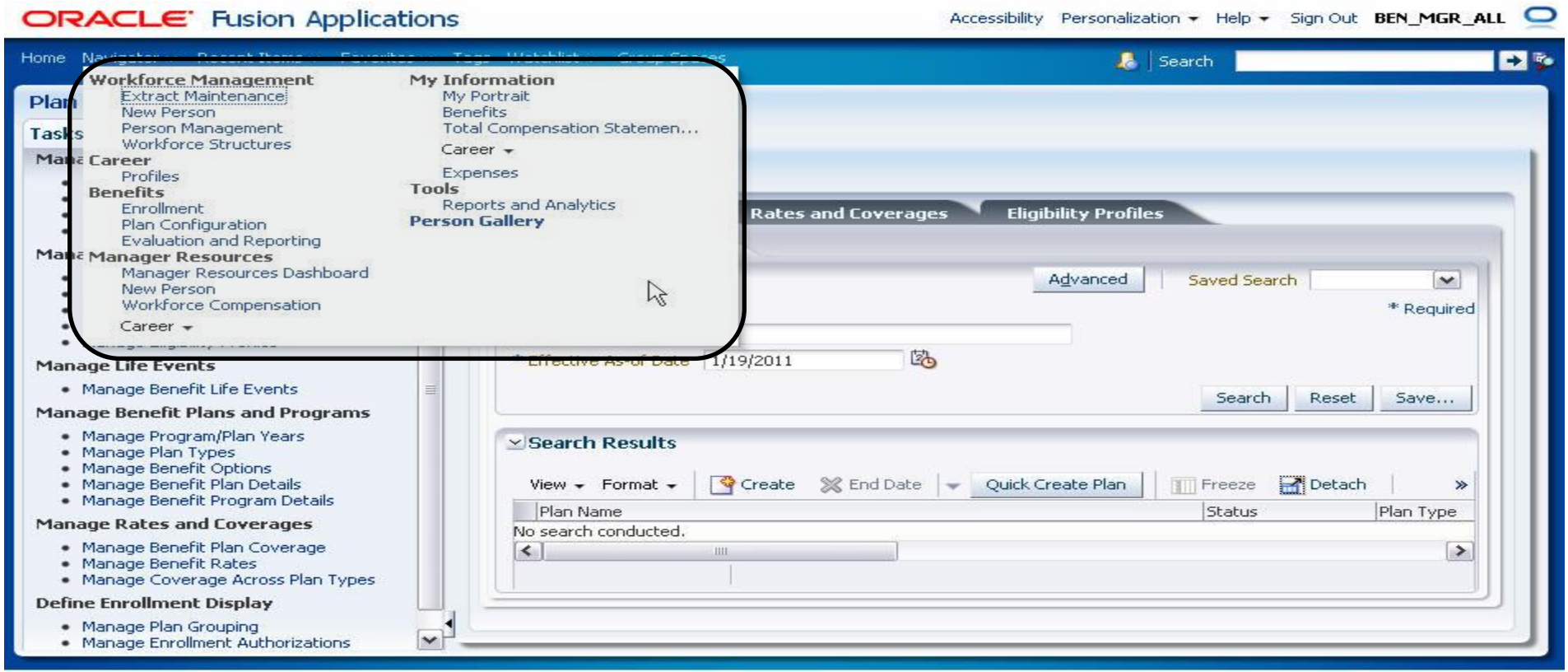
Now the New Employee Starts Using the System

When the Employee starts using Fusion Apps She will be able to access the Menu Tasks she is entitled to.



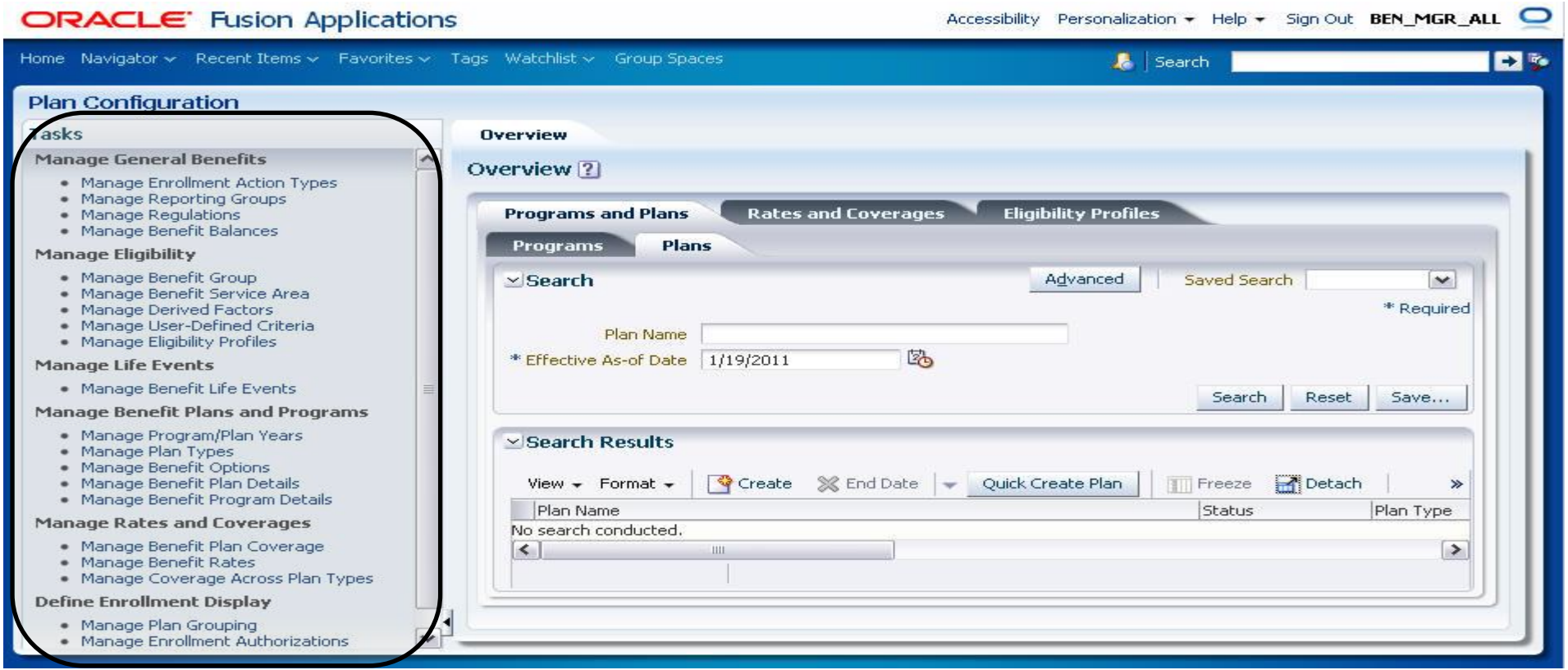
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Menu Items



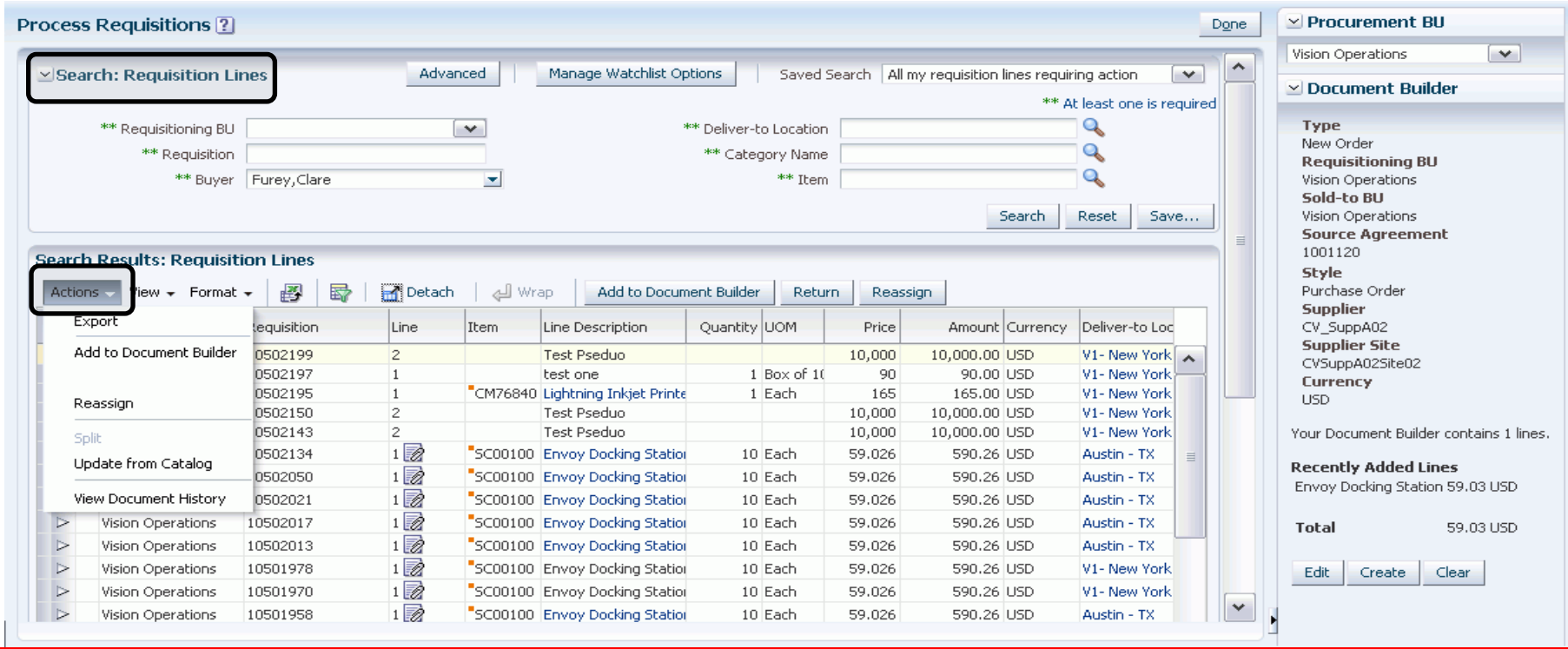
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Tasks



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Buttons, Regions and Actions



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

	A	B	C	D	E
1	RESPONSIBILITY_NAME	MENU_NAME	MAIN_MENU	SUB_MENU	CHILD_SUB_MENU
1219	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Import	Run
1220	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Generate	Recurring
1221	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Schedule	Allocation
1222	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Schedule	Recurring
1223	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Reconciliation	Reconcile
1224	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Journals	Reconciliation	Reverse
1225	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Jou		
1226	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Jou		
1227	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Bud		
1228	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Bud		
1229	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Bud		
1230	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Budgets	Enter	Journals
1231	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Row Set
1232	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Column Se
1233	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Content Set
1234	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Order
1235	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Report
1236	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Request	Financial
1237	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Display
1238	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Define	Report Set
1239	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Reports	Request	Standard
1240	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Other	Report	Set
1241	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Other	Report	View
1242	XXXX GL Supervisor - Industrial	XXXX GL Supervisor Menu	Other	Report	Run
1243	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Import	Run
1244	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Define	Recurring
1245	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Import	Correct
1246	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Generate	Allocation
1247	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Reconciliation	Reverse
1248	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Schedule	Allocation
1249	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Schedule	Recurring
1250	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Reconciliation	Reconcile
1251	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Journals	Generate	Recurring
1252	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Budgets	Enter	Amounts
1253	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Budgets	Enter	Journals
1254	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Budgets	Enter	Upload
1255	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Budgets	Enter	Transfer
1256	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Reports	Request	Financial
1257	XXXX GL Supervisor - LEOD	XXXX GL Supervisor Menu	Reports	Request	Standard

Manual Process
-No Auto Provisioning

Sheet 1

Ready

Count: 3617

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Account and Role Provisioning Events & Workflows

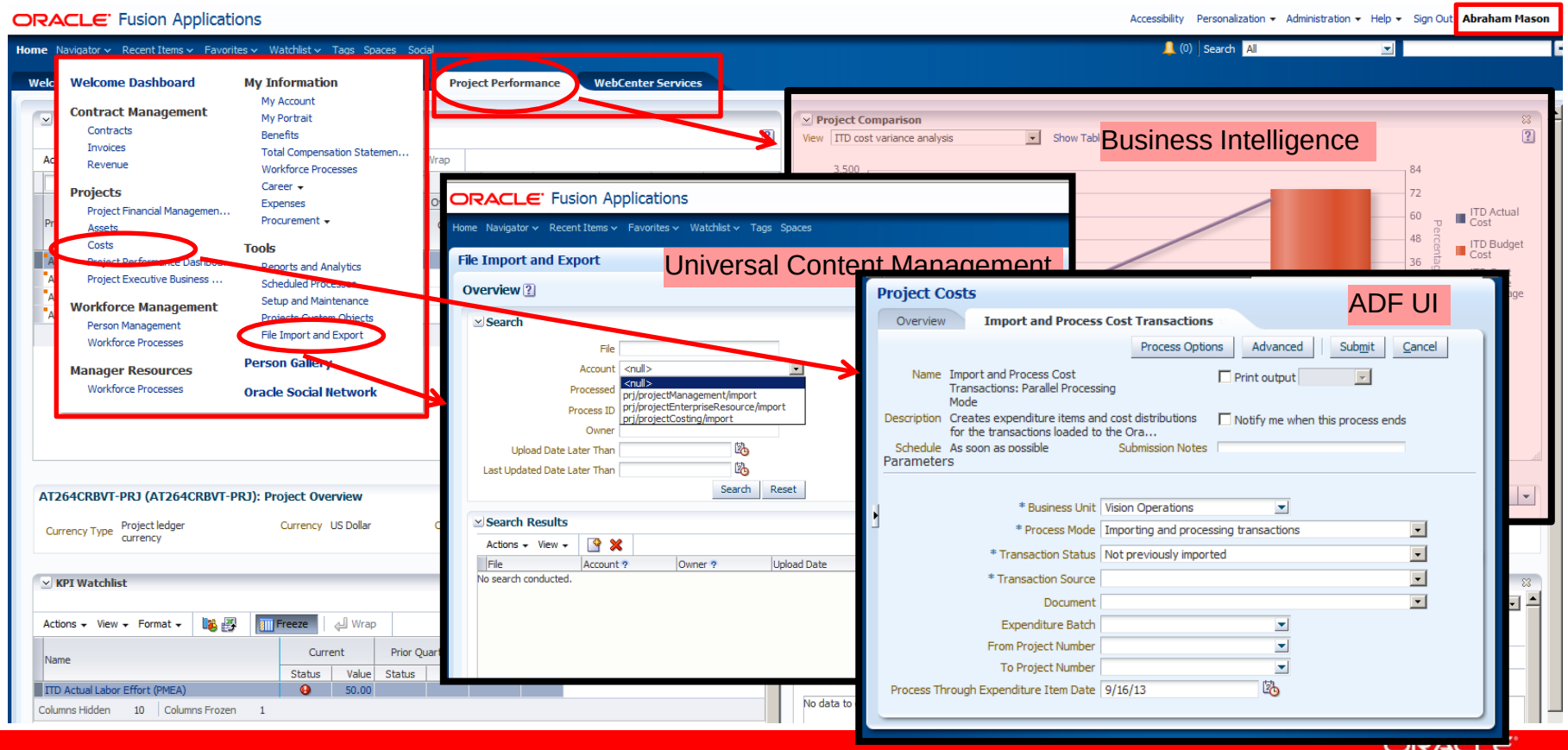
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Secure Out of the Box

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

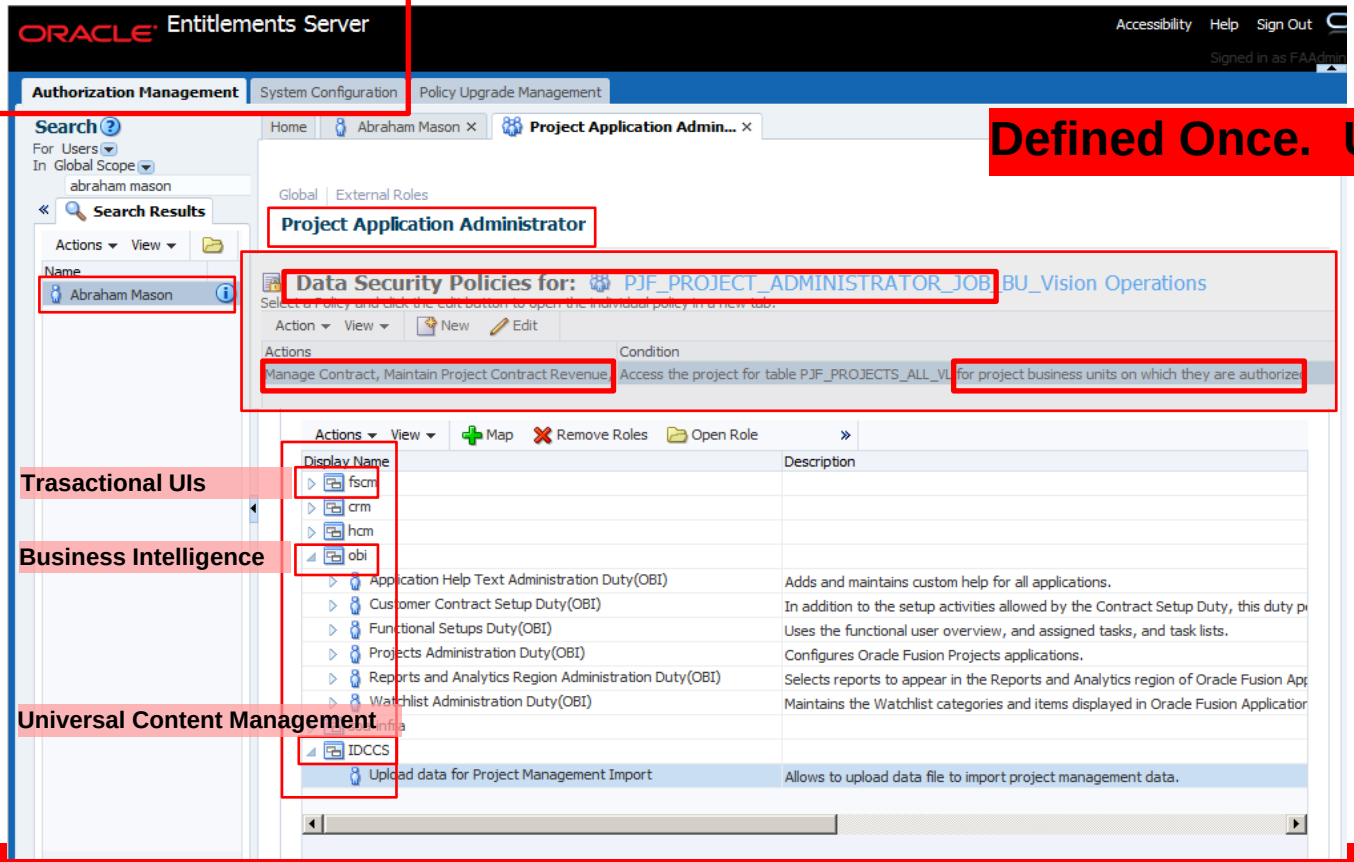
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Secure OOTB: Enforcement Across Tools



Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Secure OOTB: Enforcement Across Tools



Defined Once. Used Everywhere !

- ADF
- Enterprise Search
- Business Intelligence
- Reporting
- Mobile
- Web Services
- Content Management

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

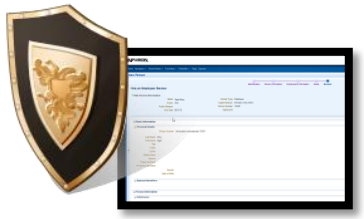
Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Secure OOTB: Pervasive Privacy Protections

- Fusion Applications protect personally identifiable information (PII)
- PII = any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.
  - Social Security Number (SSN)
  - Driver's license number
  - State or National Identifier (Identification Card number)
  - Passport Number
  - Account number, credit card number (CCN) or debit card number
  - Home or Physical address (e.g street address)
  - Email address
  - Telephone number



Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Secure OOTB: Pervasive Privacy Protections

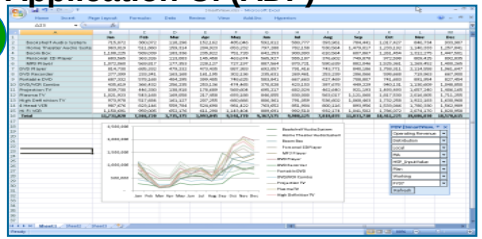
RBAC

Defined once ..

A **Supplier Manager** can **maintain** supplier **tax identifier** for the **business units** in which they are authorized

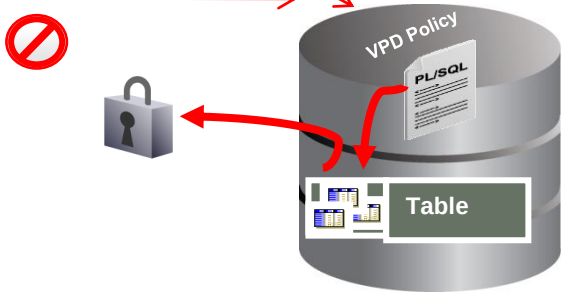
Used in UI

Application UI (ADF)



Bypasses UI and gets direct access to database

Used in VPD policy



Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Fusion Applications Security

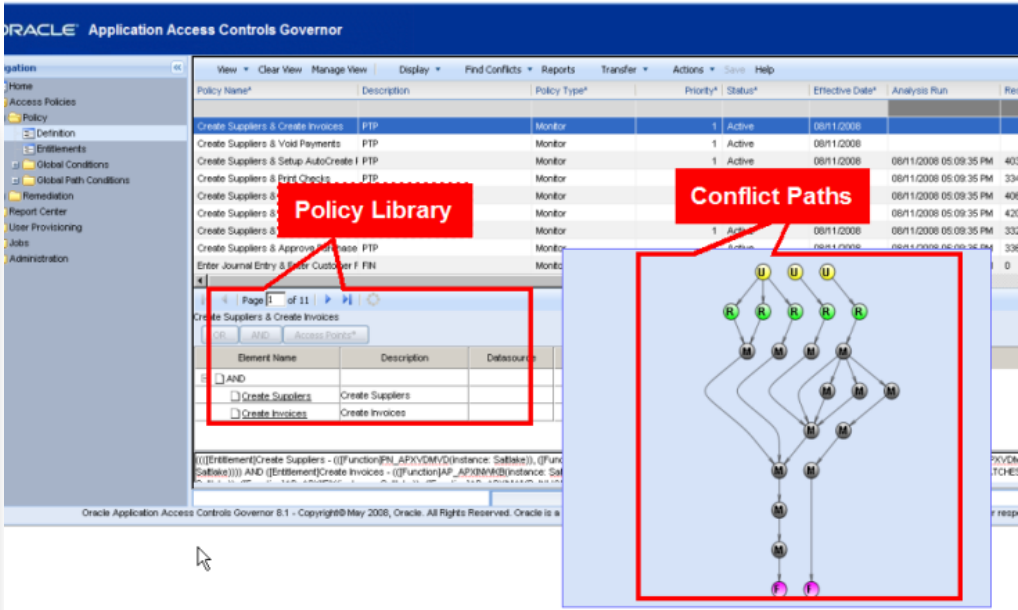
1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Manage Access & Segregation of Duties

Solution

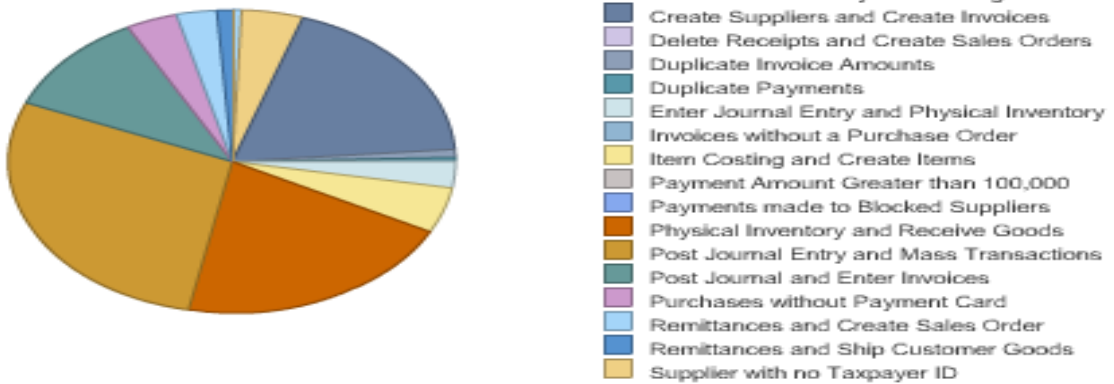
- Preventive AND Detective Access Controls
- Simulation for Role Design
- Preventive Provisioning
- Pre-built Content and Reports



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Preventive Provisioning

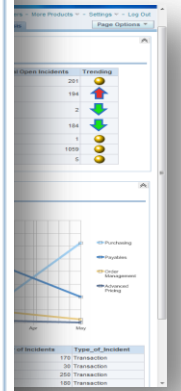
Incidents By Control



Control_Name	Control_Type	Number_of_Incidents	Last_Run_Date	Control_Owner
Control Budgets and Create Invoices	Access	76	01-APR-2011	KBROWN
Create Customer and Release Sales Order	Access	0	01-APR-2011	ASMITH
Create Items and Cycle Counting	Access	512	01-MAR-2011	ASMITH

cement
ype

Required



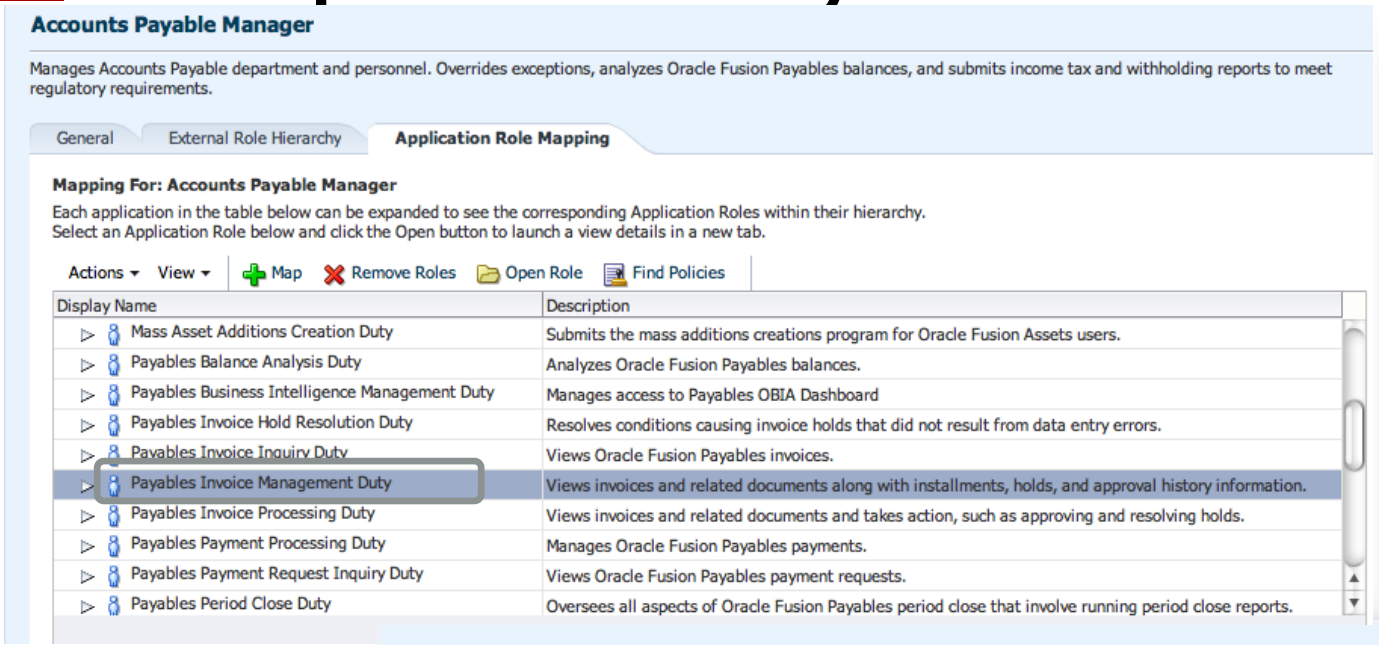
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

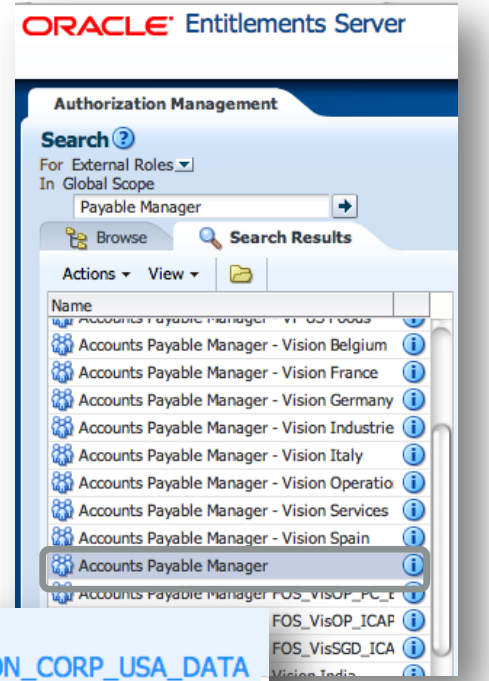
Fusion Applications Security

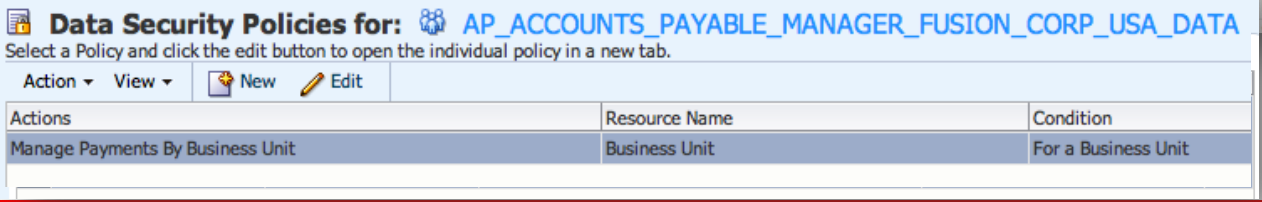
1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Transparent Security Policies







Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

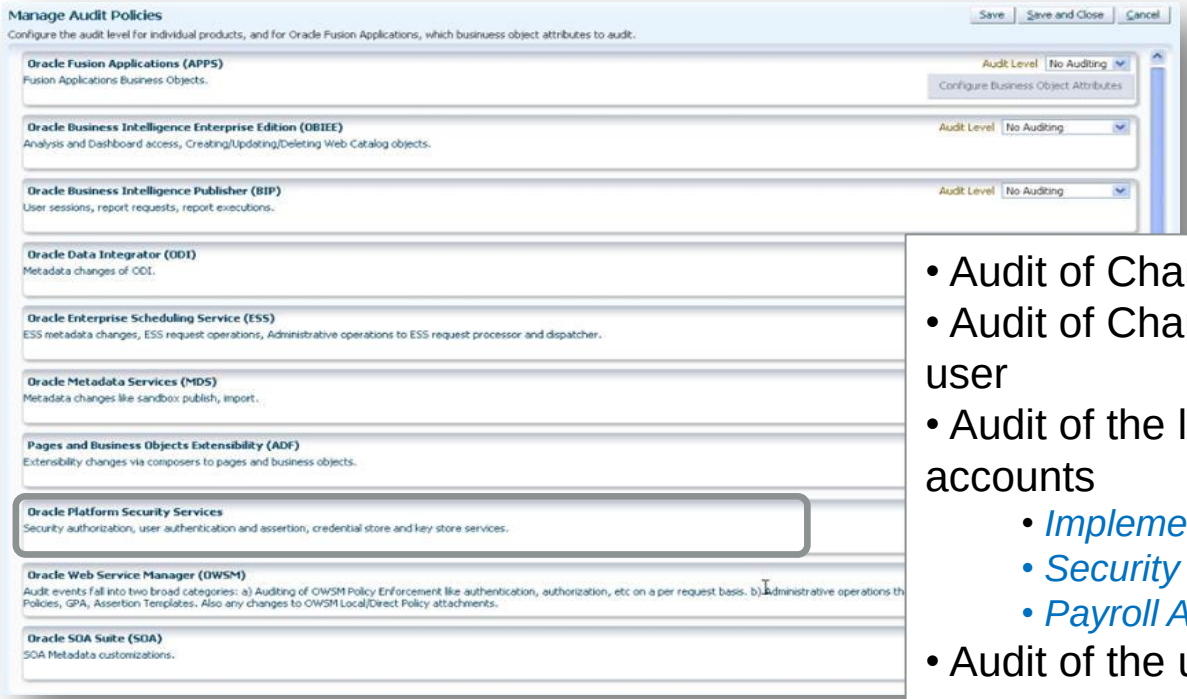
Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Audit of Security Changes

Who made what changes, and when

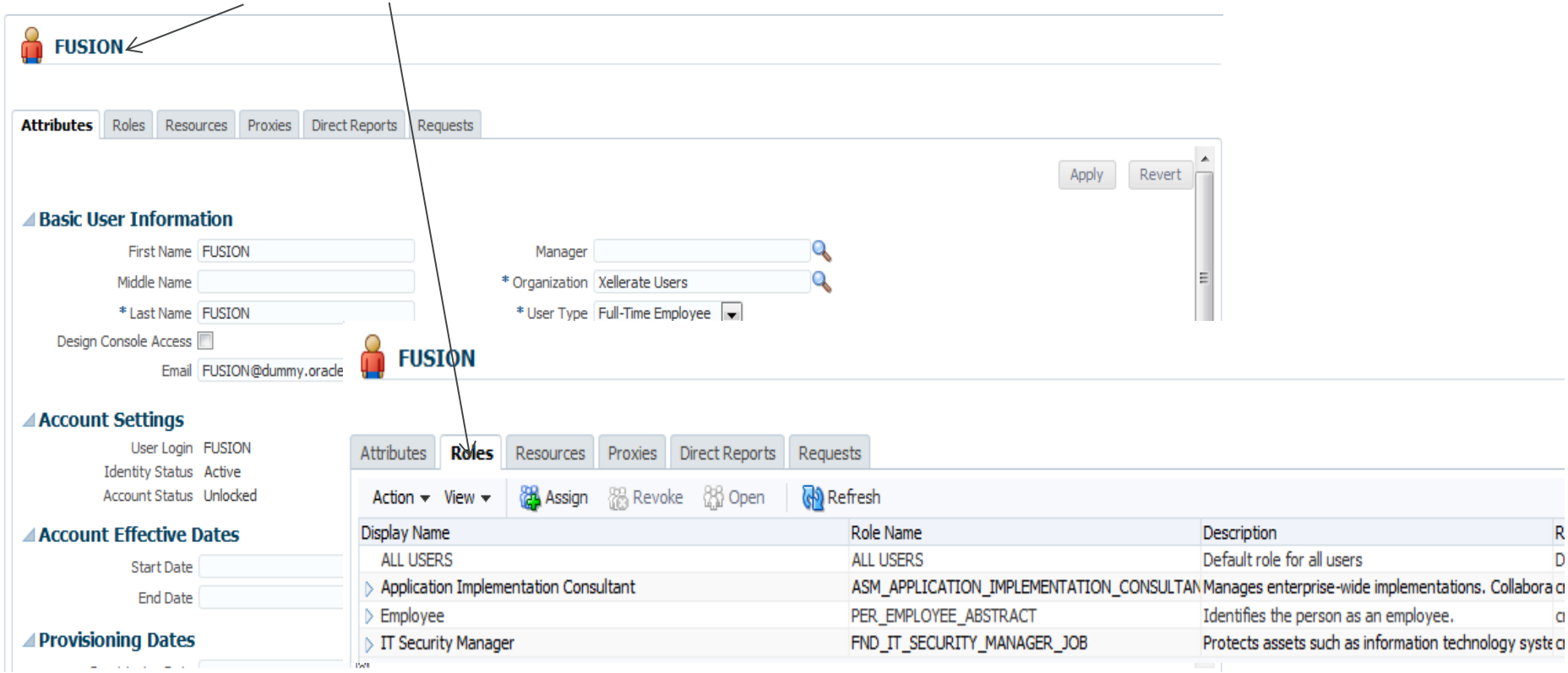


- Audit of Changes in the definition of a role
- Audit of Changes to the roles assigned to a user
- Audit of the logins of highly privileged accounts
  - *Implementation Consultant*
  - *Security Manager*
  - *Payroll Administrator*
- Audit of the use of a highly privileged function
  - *Voiding of a Check*

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

IT Audit - Security

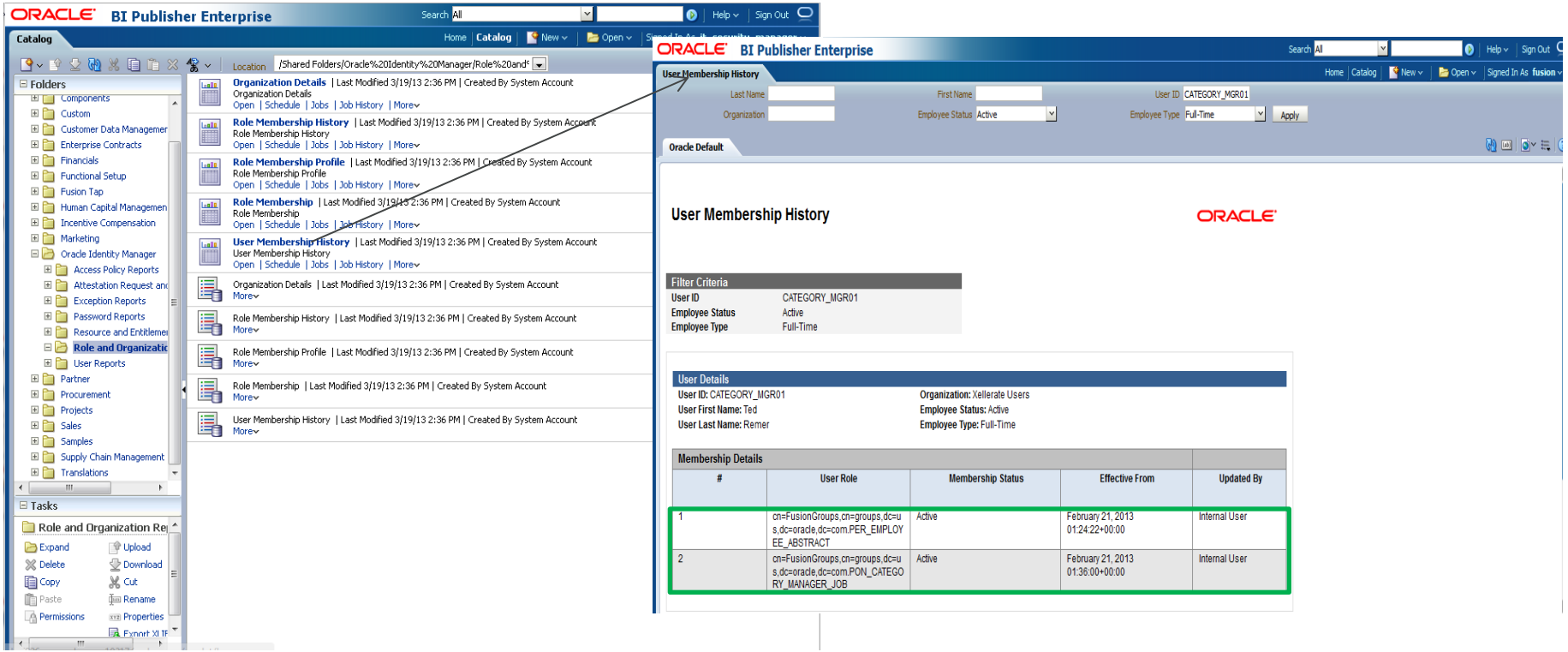
Show User and Roles from Oracle Identity Manager (OIM)



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

IT Audit - Security

Show User and Role Change Reporting



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Secure OOTB: Secure Across Info Lifecycle

- Sensitive data in file system and backups (data-at-rest) protected using Transparent Data Encryption
- Sensitive data in cloned, non-production databases protected using Oracle Data Masking
- Sensitive data protected from database administrators and other privileged users using Oracle Database Vault

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

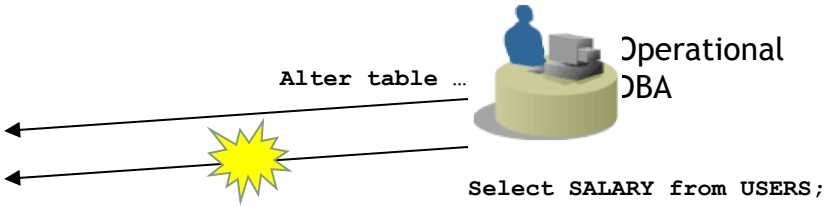
Secure OOTB: Secure Across Info Lifecycle

Protect Data in Motion with Network Encryption using *Advanced Security Option*

Protect Data from View and Alteration as well as Insider Threat using *Database Vault*

Database Vault	Operational DBA	Data DBA / Manager
`Select SALARY from users;`	X	✓
`Alter system. Alter table..`	✓	X

* Example roles and privs



Protect User and Sensitive Data at Rest by Encrypting Database Columns using *Transparent Data Encryption*

LNAME	SSN	SALARY
KING		
SCOTT		
SMITH		

Sensitive Data in cloned instance protected by *Data Masking*

LNAME	SSN	SALARY
KING	111-11-1111	$99,000
SCOTT	222-22-2222	$888,000
SMITH	333-33-3333	$77,000

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Fusion Applications Security

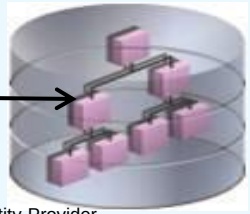
1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Secure OOTB: Co-existing with your current Security Infrastructure

Allows a user to log in once & access all applications…

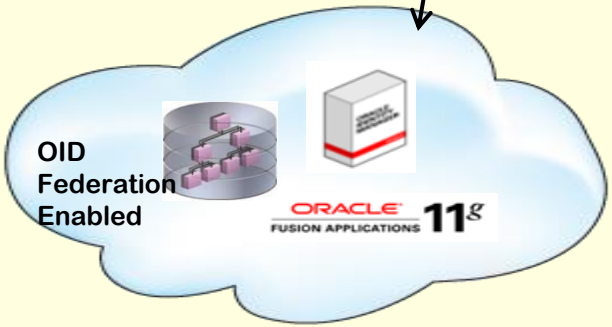
authentication

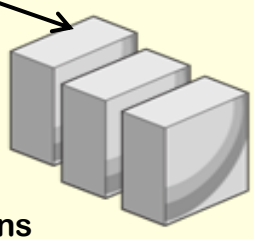


Identity Provider

Existing Identity Management Infrastructure

Service access





Custom Applications

Service Providers

Applications Unlimited

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Fusion Applications Security

1. Role Based Access
2. Account and Role Provisioning Events & Workflows
3. Enforcement Across Tools and Transformations
4. Pervasive Privacy Protections
5. Integration with Governance Risk and Compliance
6. Transparent Security Policies
7. Complete Audit of Security Changes
8. Secure Across the Information Lifecycle
9. Co-existing with your current Security Infrastructure
10. Comprehensive Extensible Reference Implementation

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Secure OOTB: Reference Implementation

ORACLE

FUSION APPLICATIONS

OOTB

- ✓ roles you will recognize as jobs
- ✓ hierarchy of duties
- ✓ data security policies
- ✓ SOD Policies
- ✓ Provisioning Events

To extend

Security Console

- ✓ new jobs
- ✓ new duties

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

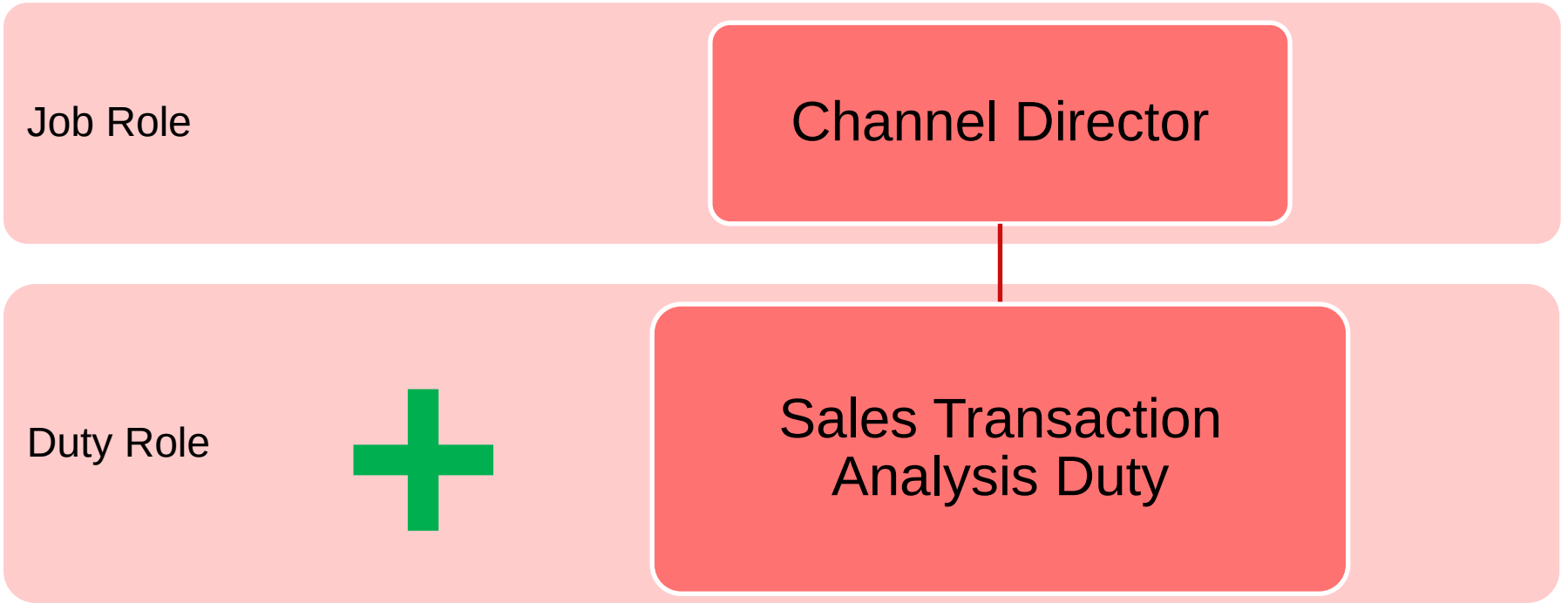
Configuration Flexibility

"What if I want to expand what reports the channel directors can see?"

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Configuration Flexibility

Add a Duty Role



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

ORACLE
Search
IT_SECURITY_MANAGER
Social
Hiring
Notifications
Learning
Navigator
Getting Started
Analytics
Security Console
Security Console
Create Role
Compare Roles
Search
Channel Sales Director
Refine
Search Results (1)
Channel Sales Director
Code
ZPM_ CHANNEL_ SALES_ DIRECTOR_ JOB
Description
Supervises channel roles to support partner relationships and transactions.
Visualization
Expand paths toward:
Privileges
Users
CRMRead
Business Intelligence Worker
Upload data for Customer Import
Upload data for Resource Team Import
Upload data for Customer Hierarchy Member...
Marketing Approver
Partner Channel Transaction Analysis Duty
Channel Sales Director Duty
Channel Sales Director
Upload data for Consumer Import
Business Intelligence Applications Worker
Expand All
Collapse
Compare Roles
Copy Role
Edit Role
Set as Focus
Simulate Navigator

ORACLE

IT_SECURITY_MANAGER

Security Console

Edit Role : Role Hierarchy

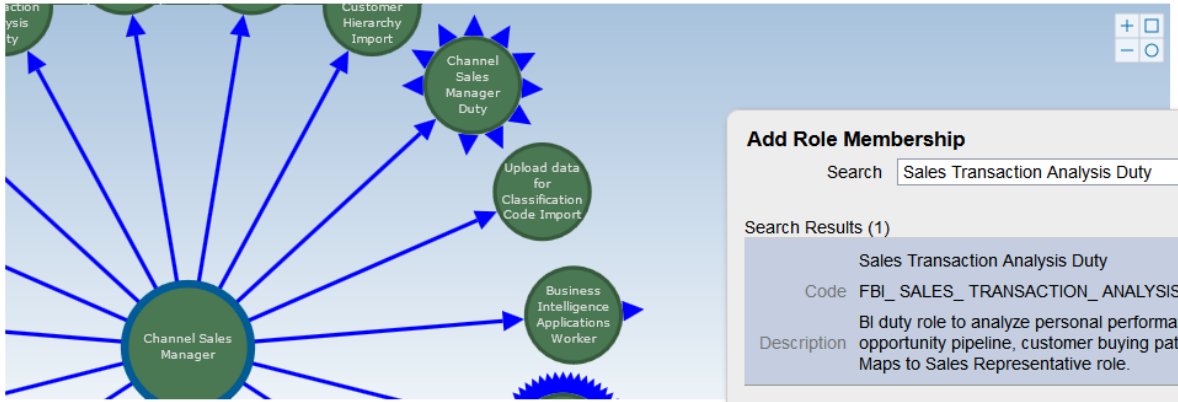
Back | Next | Cancel

Channel Sales Manager

Basic Information | Functional Security Policies | Data Security Policies | Role Hierarchy | Users | Summary and Impact Report

Below is a visualization of this role.

Add Role



Add Role Membership

Search: Sales Transaction Analysis Duty | Refine

Search Results (1)

Sales Transaction Analysis Duty

Code: FBI_ SALES_ TRANSACTION_ ANALYSIS_ DUTY

Description: BI duty role to analyze personal performance against quota and also opportunity pipeline, customer buying patterns, to better cross sell and up sell. Maps to Sales Representative role.

Add Role Membership | Cancel

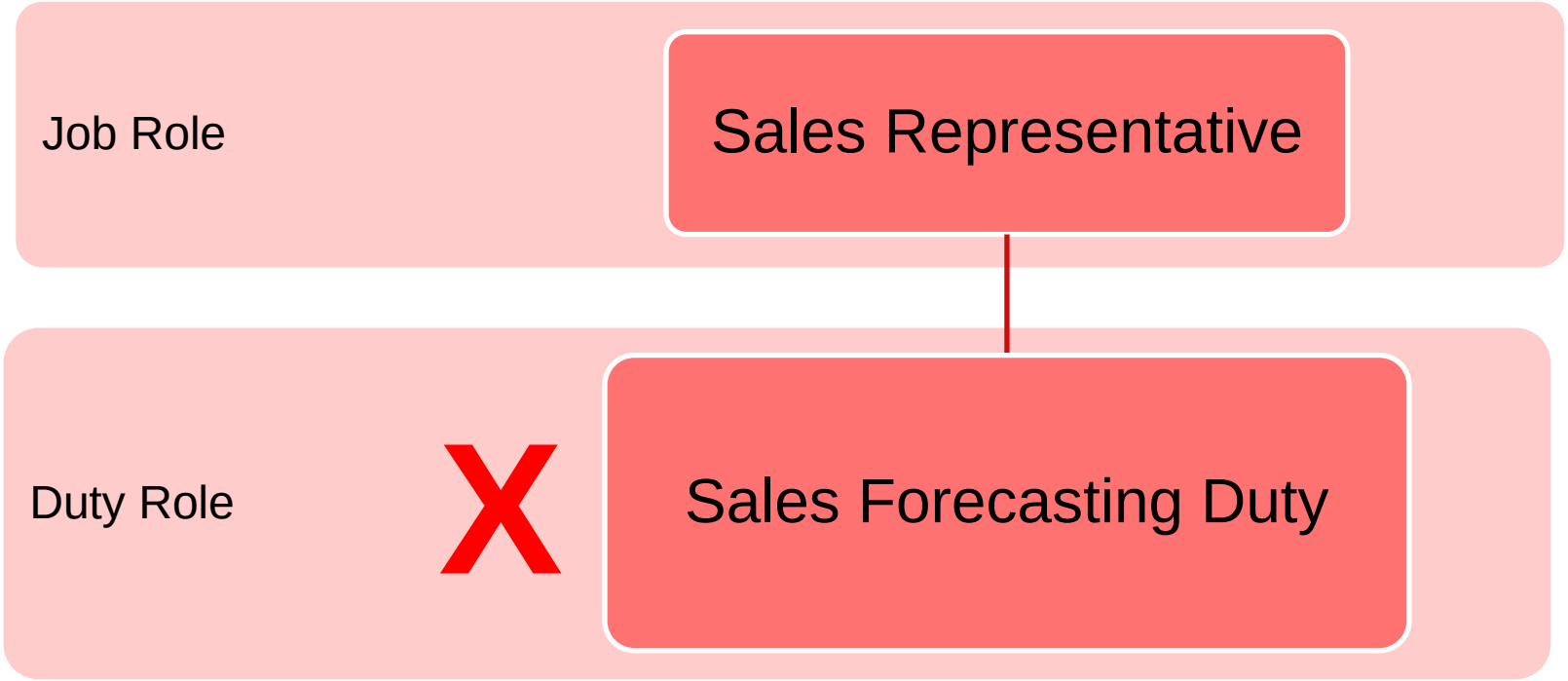
Configuration Flexibility

"Most business groups have their sales reps do forecasting, but I know of one where the sales managers do that, not the sales reps. What should I do?"

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Configuration Flexibility

Remove a Duty Role



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

ORACLE

IT_SECURITY_MANAGER

Security Console

Edit Role : Role Hierarchy

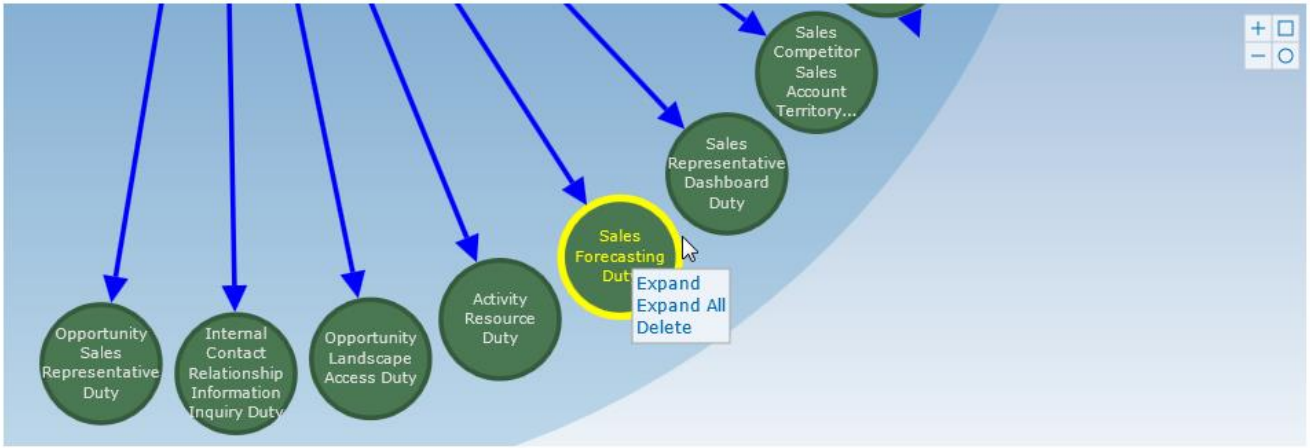
Back | Next | Cancel

Sales Representative

Basic Information | Functional Security Policies | Data Security Policies | Role Hierarchy | Users | Summary and Impact Report

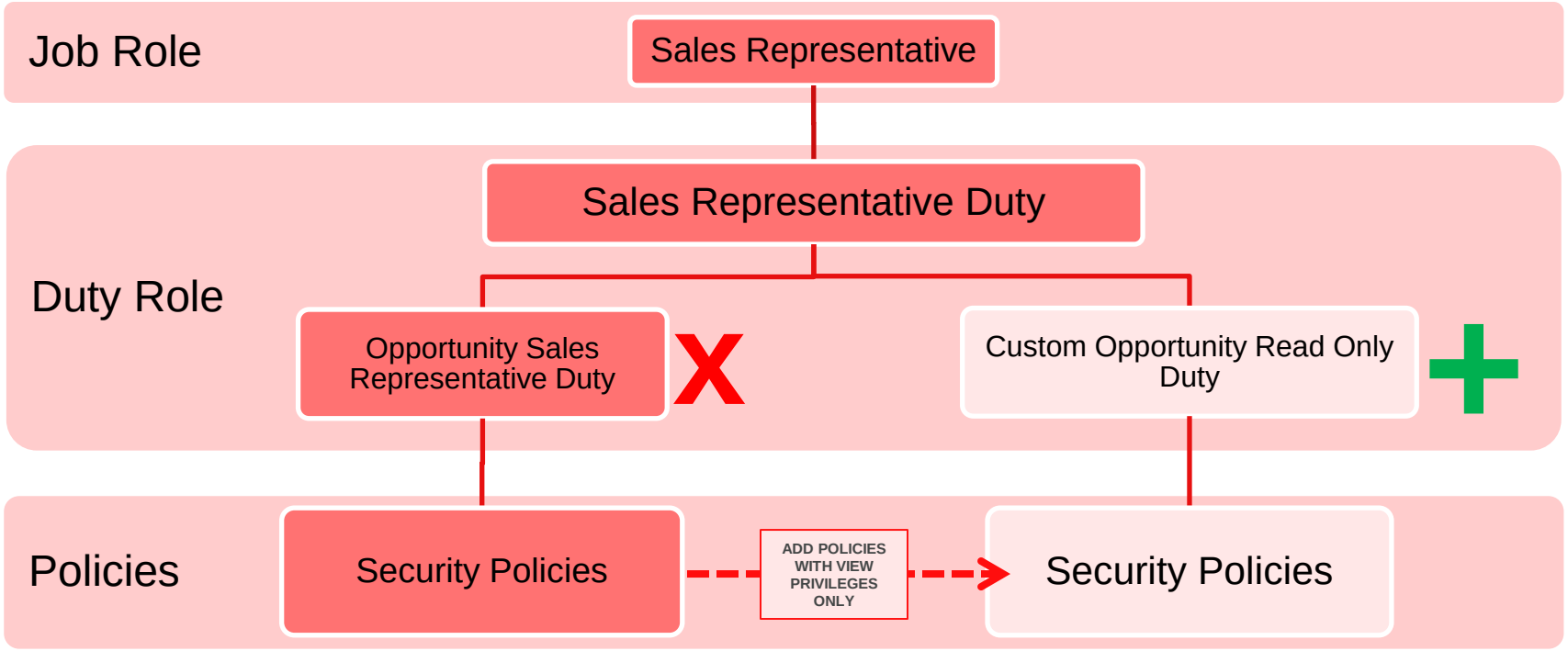
Below is a visualization of this role.

Add Role

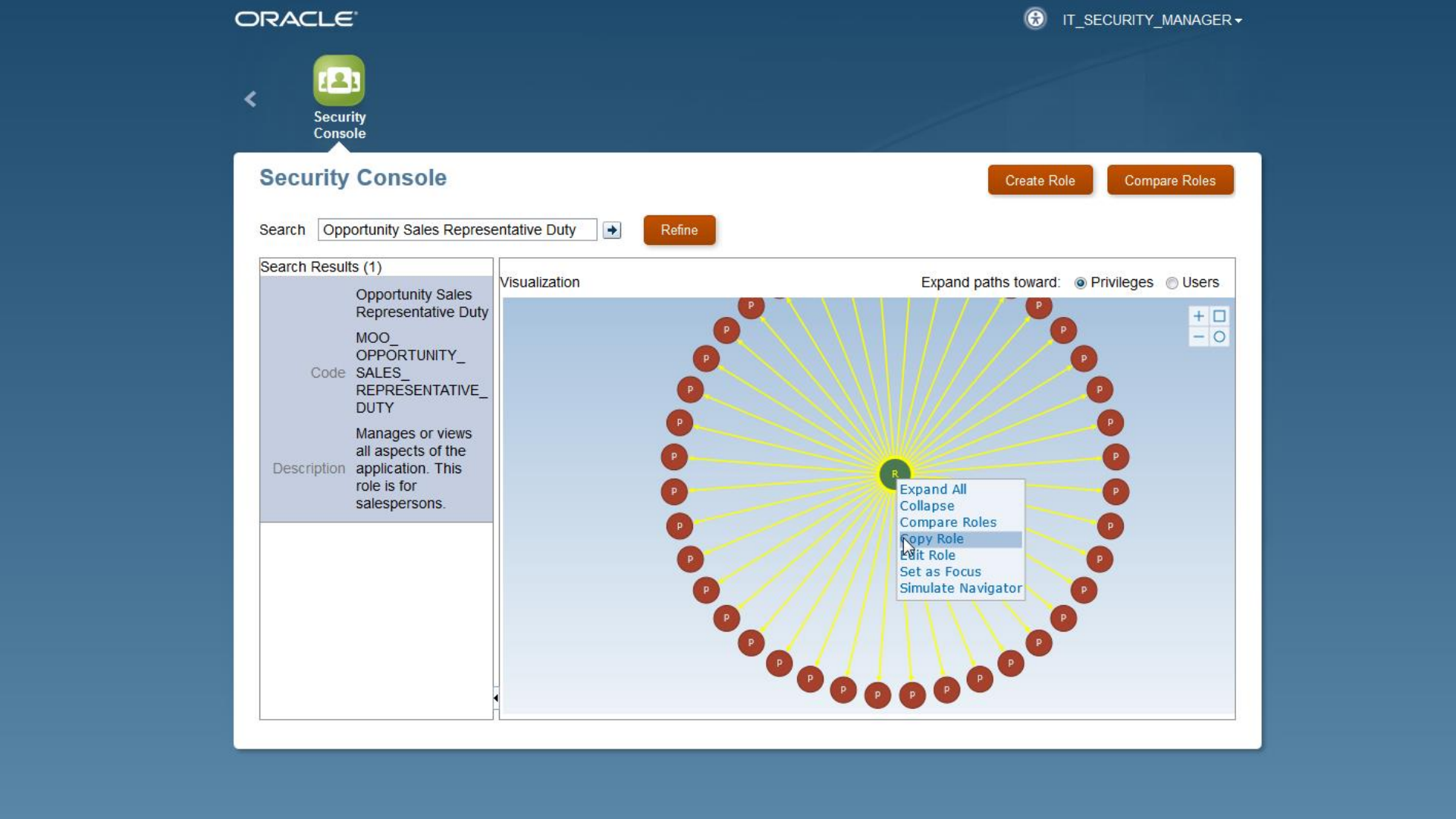


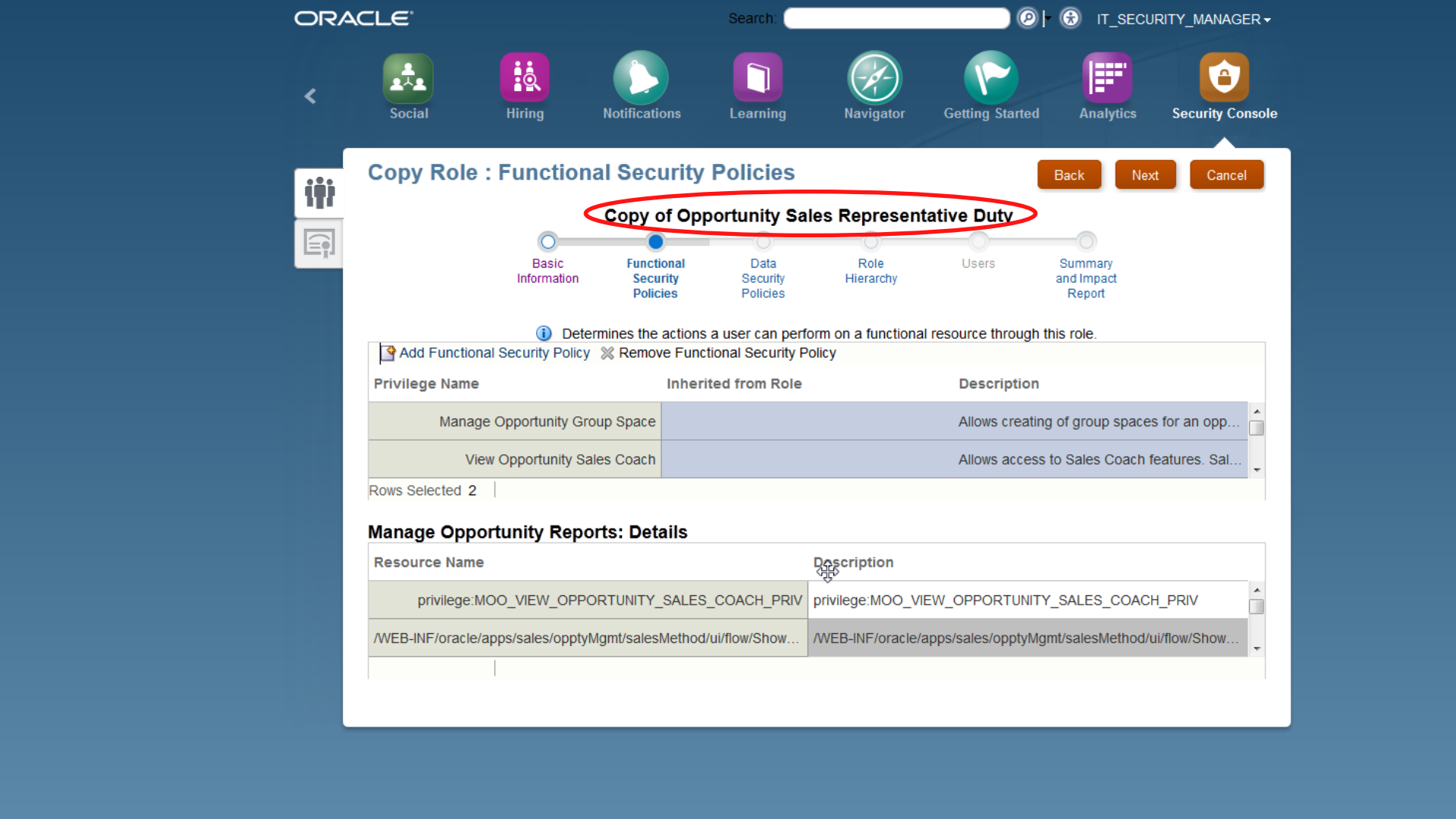
Configuration Flexibility

Remove Duty Role and Add Custom Duty Role



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.


ORACLE
IT_SECURITY_MANAGER
Security Console
Security Console
Create Role
Compare Roles
Search
Opportunity Sales Representative Duty
Refine
Search Results (1)
Opportunity Sales Representative Duty
Code
MOO_OPPORTUNITY_SALES_REPRESENTATIVE_DUTY
Description
Manages or views all aspects of the application. This role is for salespersons.
Visualization
Expand paths toward:
Privileges
Users
Expand All
Collapse
Compare Roles
Copy Role
Edit Role
Set as Focus
Simulate Navigator


ORACLE
Search:
IT_SECURITY_MANAGER
Social
Hiring
Notifications
Learning
Navigator
Getting Started
Analytics
Security Console
Copy Role : Functional Security Policies
Back
Next
Cancel
Copy of Opportunity Sales Representative Duty
Basic Information
Functional Security Policies
Data Security Policies
Role Hierarchy
Users
Summary and Impact Report
Determines the actions a user can perform on a functional resource through this role.
Add Functional Security Policy
Remove Functional Security Policy
Privilege Name
Inherited from Role
Description
Manage Opportunity Group Space
Allows creating of group spaces for an opp...
View Opportunity Sales Coach
Allows access to Sales Coach features. Sal...
Rows Selected 2
Manage Opportunity Reports: Details
Resource Name
Description
privilege:MOO_VIEW_OPPORTUNITY_SALES_COACH_PRIV
privilege:MOO_VIEW_OPPORTUNITY_SALES_COACH_PRIV
/WEB-INF/oracle/apps/sales/opptyMgmt/salesMethod/ui/flow/Show...
/WEB-INF/oracle/apps/sales/opptyMgmt/salesMethod/ui/flow/Show...

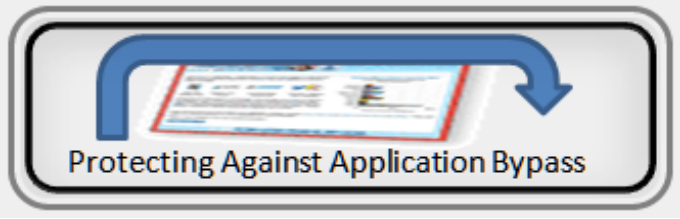
Securing the Database

MEGA BREACHES ON THE RISE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Considerations for Maximum Security

Preventive and Detective Controls



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption & Redaction	Activity Monitoring	Key Management
Masking & Subsetting	Database Firewall	Privilege & Data Discovery
Privileged User Controls	Auditing & Reporting	Configuration Management

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Oracle Database Security Innovations

Privilege Analysis

Data Redaction

Real Application Security

Conditional and Unified Auditing

SQL Grammar based Database Firewall

Privileged User Controls

SQL Command Controls

At-source Data Masking

Sensitive Data Discovery

Transparent Data Encryption

Label-based Access Control

Virtual Private Database

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption & Redaction	Activity Monitoring	Key Management
Masking & Subsetting	Database Firewall	Privilege & Data Discovery
Privileged User Controls	Auditing & Reporting	Configuration Management

ORACLE

ORACLE

ORACLE

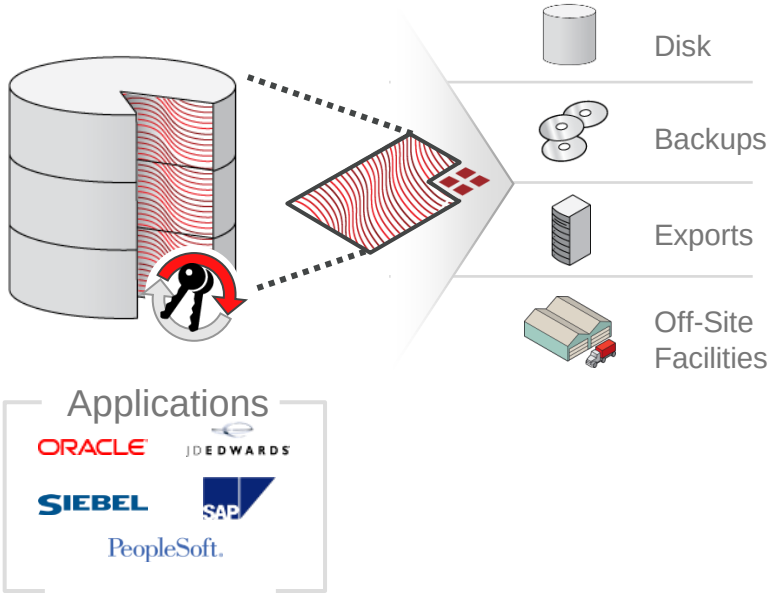
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Encryption is the Foundation

Preventive Control for Oracle Databases

Advanced Security

- Transparent data encryption
- Prevents access to data at rest
- Requires no application changes
- Built-in two-tier key management
- “Near Zero” overhead with hardware
- Integrations with Oracle technologies
  - e.g. Exadata, Advanced Compression, ASM, GoldenGate, DataPump, etc.



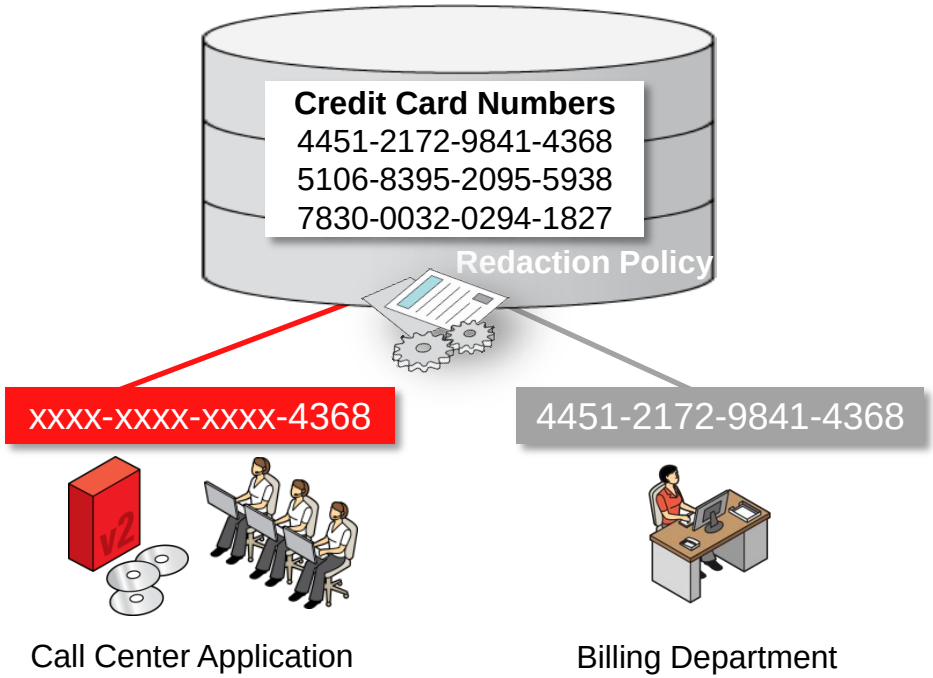
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Redaction of Sensitive Data Displayed

Preventive Control for Oracle Database 12c and 11g (11.2.0.4)

Advanced Security

- Real-time redaction based upon user, IP, app context, session factors, …
- Applies to columns on tables/views
- Full/partial, random/fixed redaction
- No impact on operational activities



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

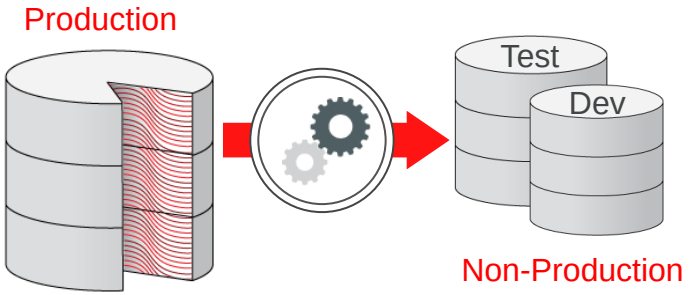
Masking Data for Non-Production Use

Preventive Control for Oracle Databases

Data Masking

- Replace sensitive application data
- Referential integrity detected/preserved
- Extensible template library and formats
- Application templates available
- Support for masking data in non-Oracle databases

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000



LAST_NAME	SSN	SALARY
ANSKEKSL	323—23-1111	60,000
BKJHHEIEDK	252-34-1345	40,000

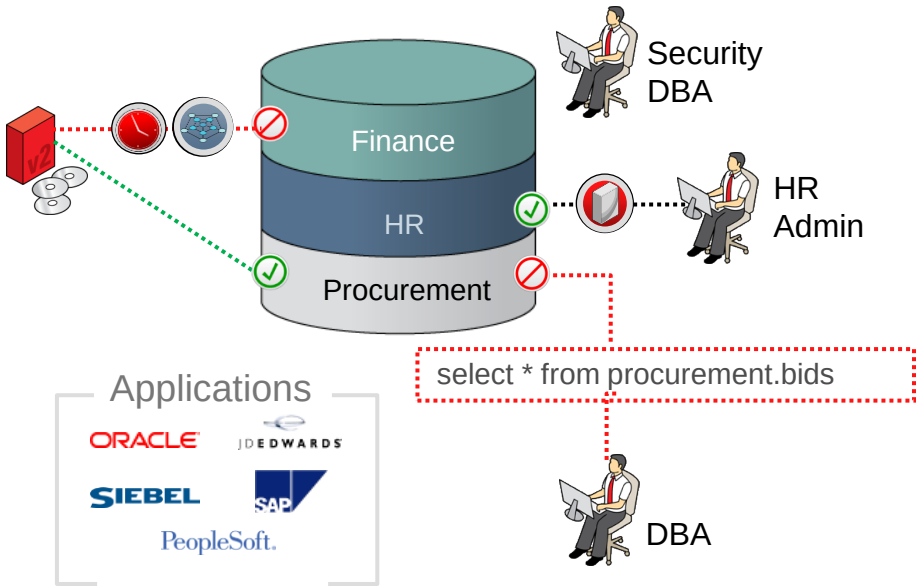
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Preventive Controls Inside the Oracle Database

Preventive Control for Oracle Databases

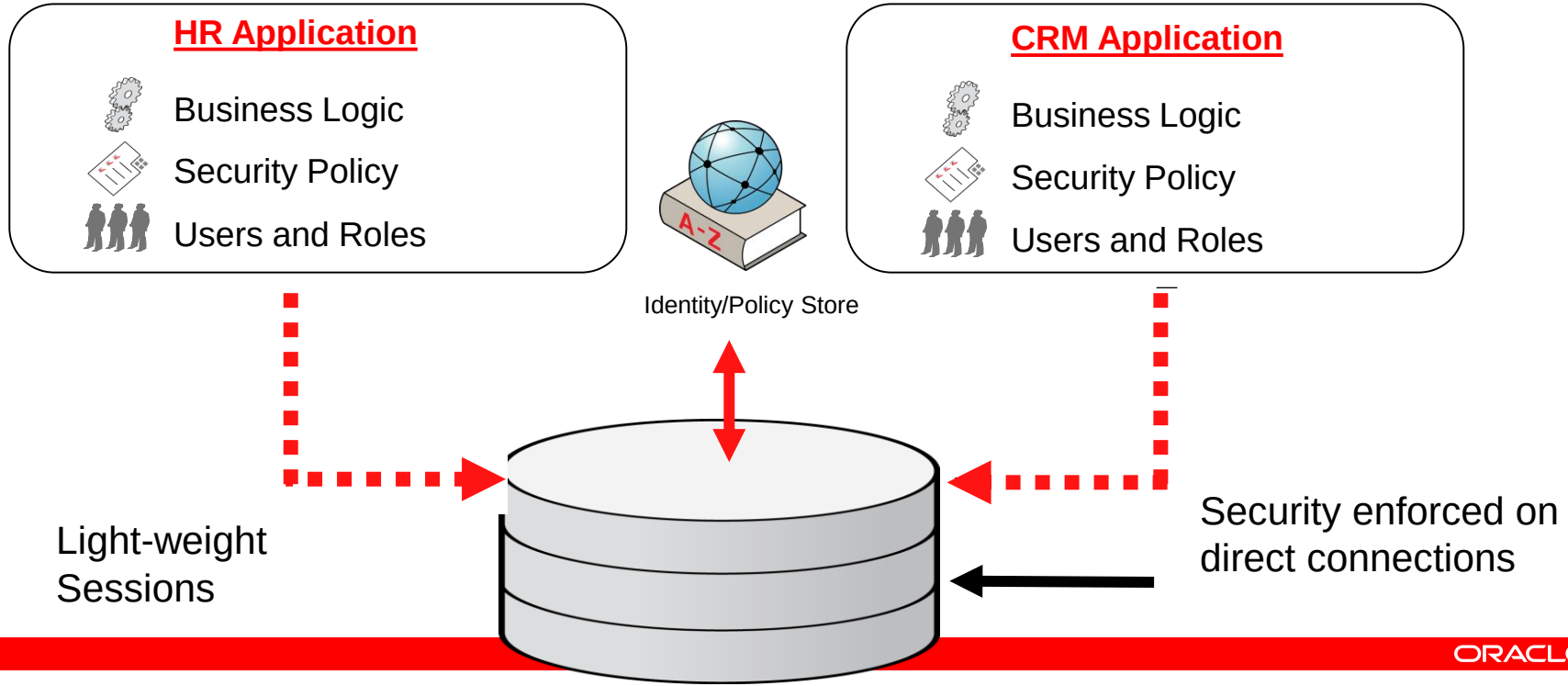
Database Vault

- Realms around sensitive schemas or objects
- Restrict DBA access to realm data
- Support multi-factor SQL command rules
- Enforce separation of duties
- Block threats targeting privileged DB accounts
- Restrict all access unless explicitly authorized with Mandatory Realms (New)



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Real Application Security



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption & Redaction	Activity Monitoring	Key Management
Masking & Subsetting	Database Firewall	Privilege & Data Discovery
Privileged User Controls	Auditing & Reporting	Configuration Management

ORACLE

ORACLE

ORACLE

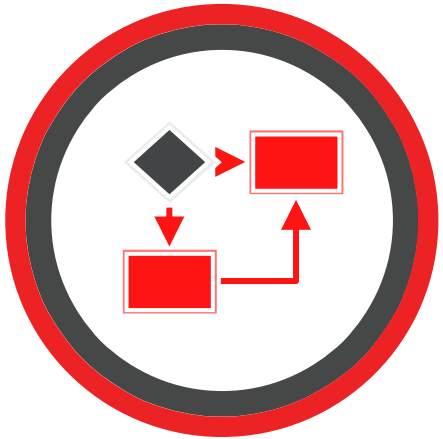
 Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

New Conditional Auditing Framework

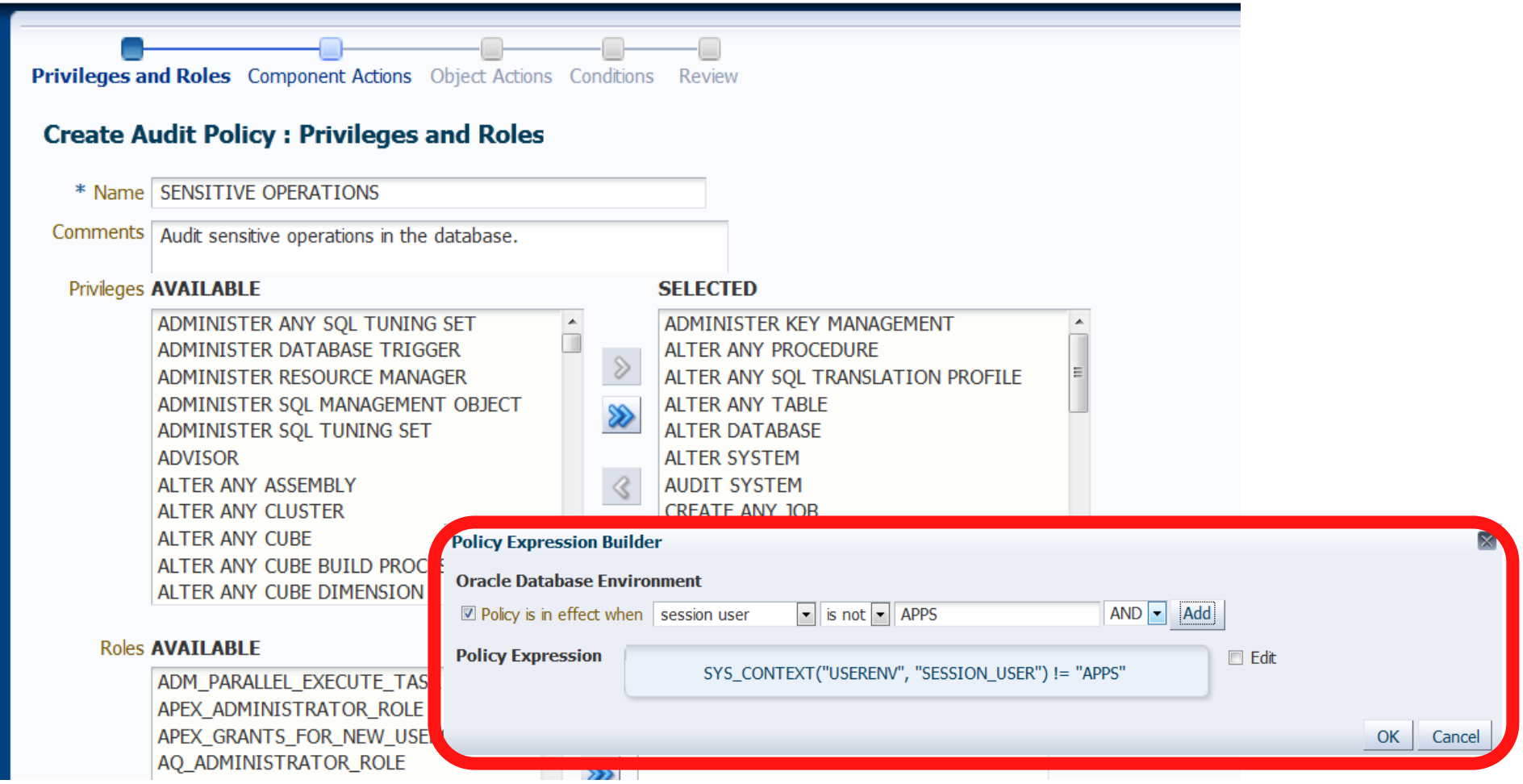
Detective Control for Oracle Database 12c

Database Auditing

- New policy and condition-based syntax
  - What: CREATE, ALTER, ALL, …
  - Where: Set of Privileges, Roles, objects
  - When: IP_ADDRESS !=“10.288.241.88”
  - Exceptions: Except HR
- Group audit settings for manageability
- New roles: Audit Viewer and Audit Admin
- Out-of-box audit policies
- Single unified database audit trail



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.



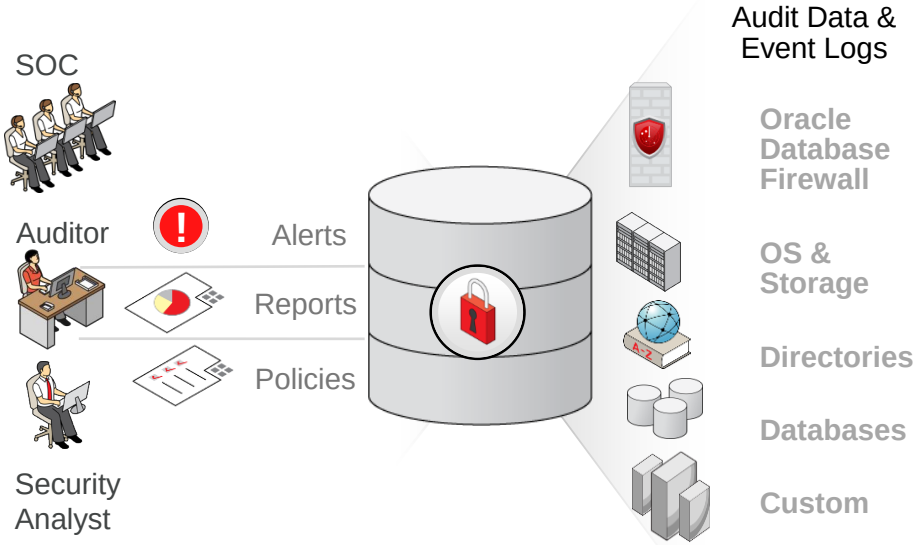
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Audit, Report, and Alert in Real-Time

Detective Control for Oracle and non-Oracle Databases

Audit Vault and Database Firewall

- Collect and Analyze audit/event data
- Centralized secure audit repository
- Consolidated multi-source reporting
- Out-of-the box and custom reports
- Conditional real-time alerts
- Fine-grain separation of duties
- Secure, scalable software appliance



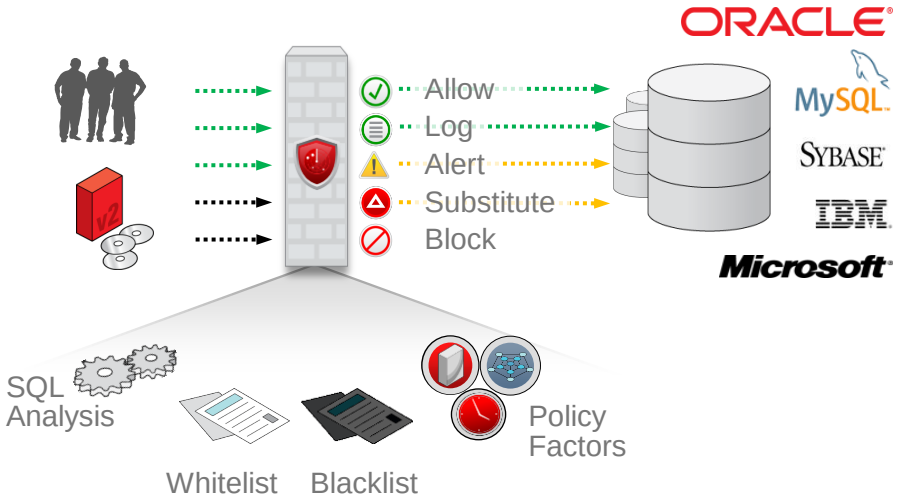
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Database Activity Monitoring and Firewall

Detective Control for Oracle and non-Oracle Databases

Audit Vault and Database Firewall

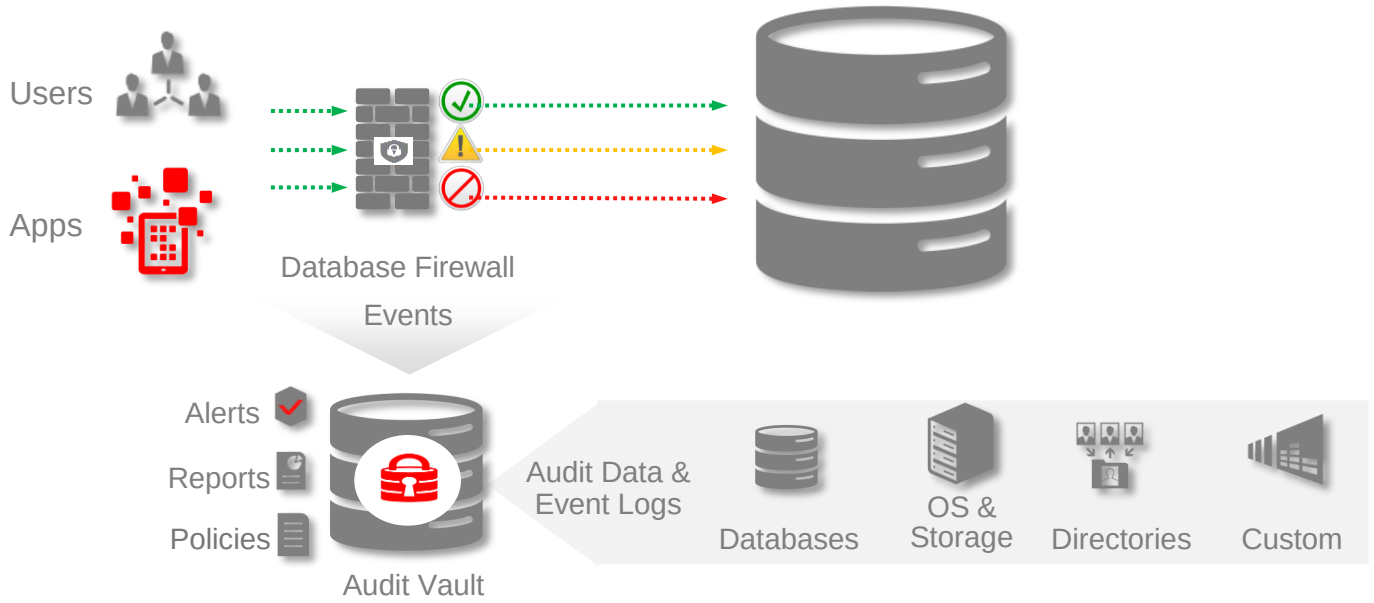
- Monitor network traffic, detect and block unauthorized database activity
- Detect/stop SQL injection attacks
- Highly accurate SQL grammar analysis
- Whitelist approach to enforce activity
- Blacklists for managing high risk activity
- Scalable secure software appliance



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Oracle Audit Vault and Database Firewall

Detective Controls



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption & Redaction	Activity Monitoring	Key Management
Masking & Subsetting	Database Firewall	Privilege & Data Discovery
Privileged User Controls	Auditing & Reporting	Configuration Management

ORACLE

ORACLE

ORACLE

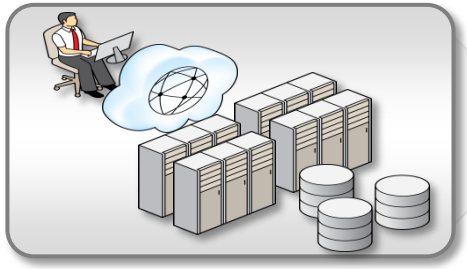
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Configuration Management

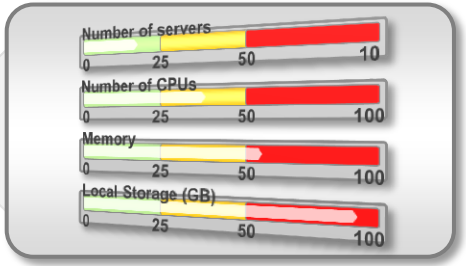
Administrative Control for Oracle Databases

Database Lifecycle Management

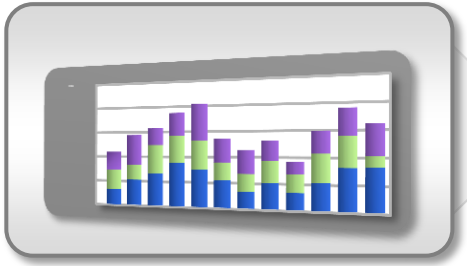
- Discover and classify databases
- Scan for best practices, standards
- Detect unauthorized changes
- Patching and provisioning



Discover



Scan & Monitor



Patch

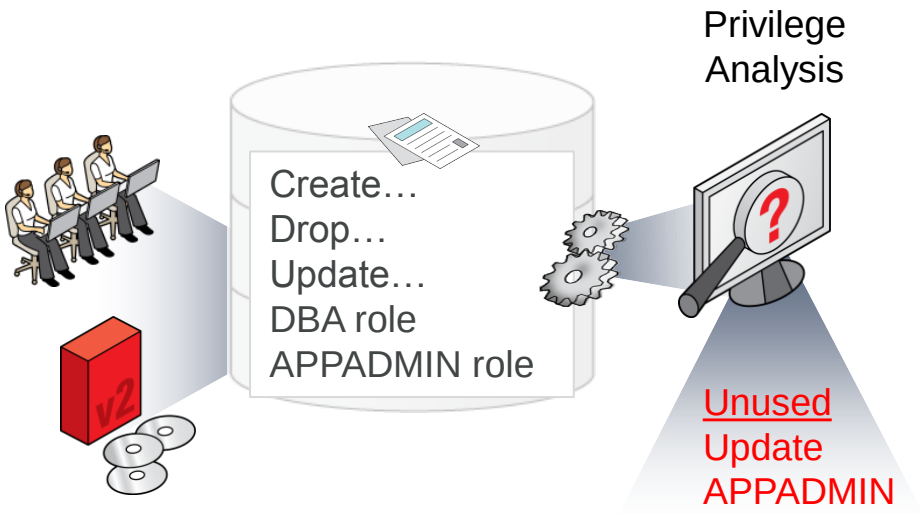
Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Discover Use of Privileges and Roles

Administrative Control for Oracle Database 12*c*

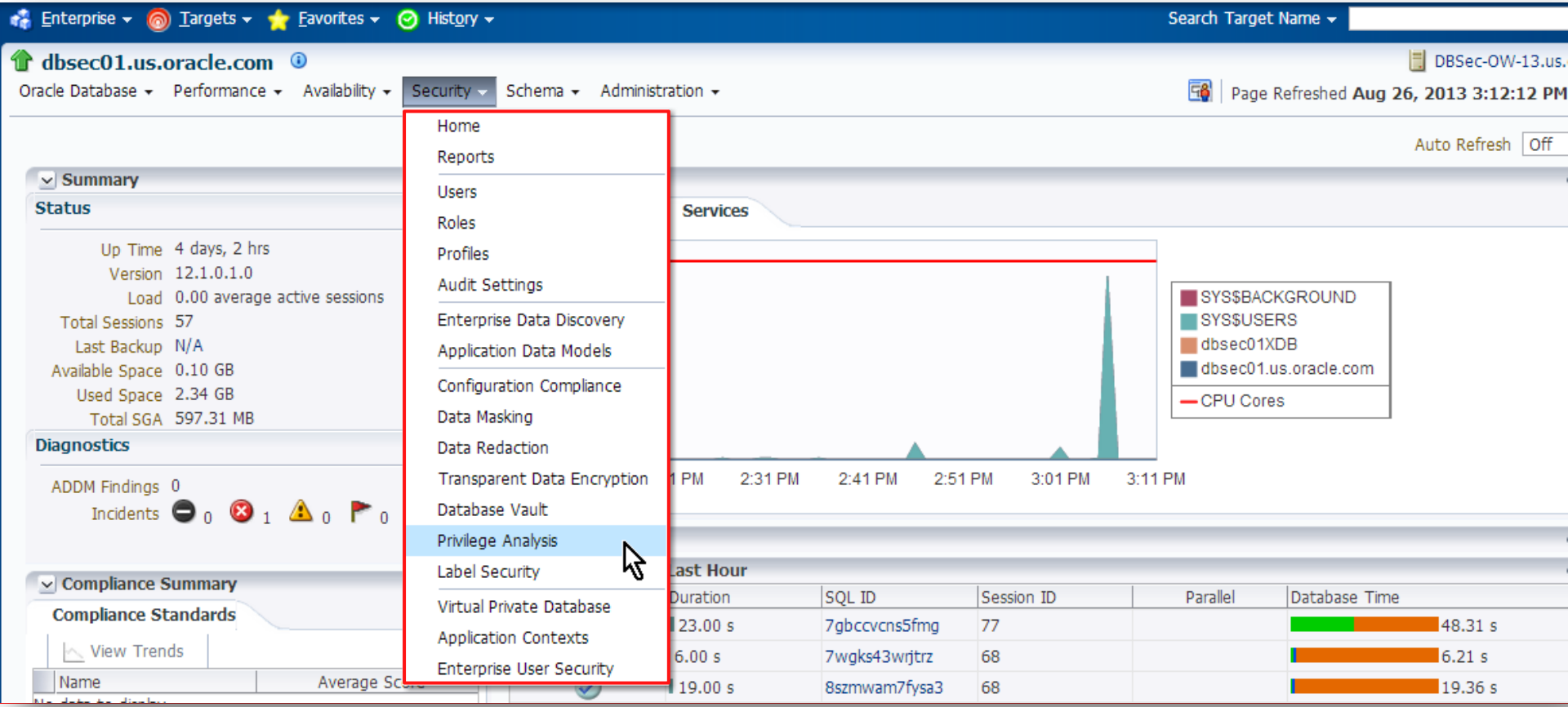
Database Vault

- Capture privileges used per session, across sessions, per specific context, or full database
- Report on privileges/roles used/unused
- Help revoke unnecessary privileges
- Enforce least privilege and reduce risks
- Increase security without disruption



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

New Oracle Enterprise Manager Security Menu



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption & Redaction	Activity Monitoring	Key Management
Masking & Subsetting	Database Firewall	Privilege & Data Discovery
Privileged User Controls	Auditing & Reporting	Configuration Management

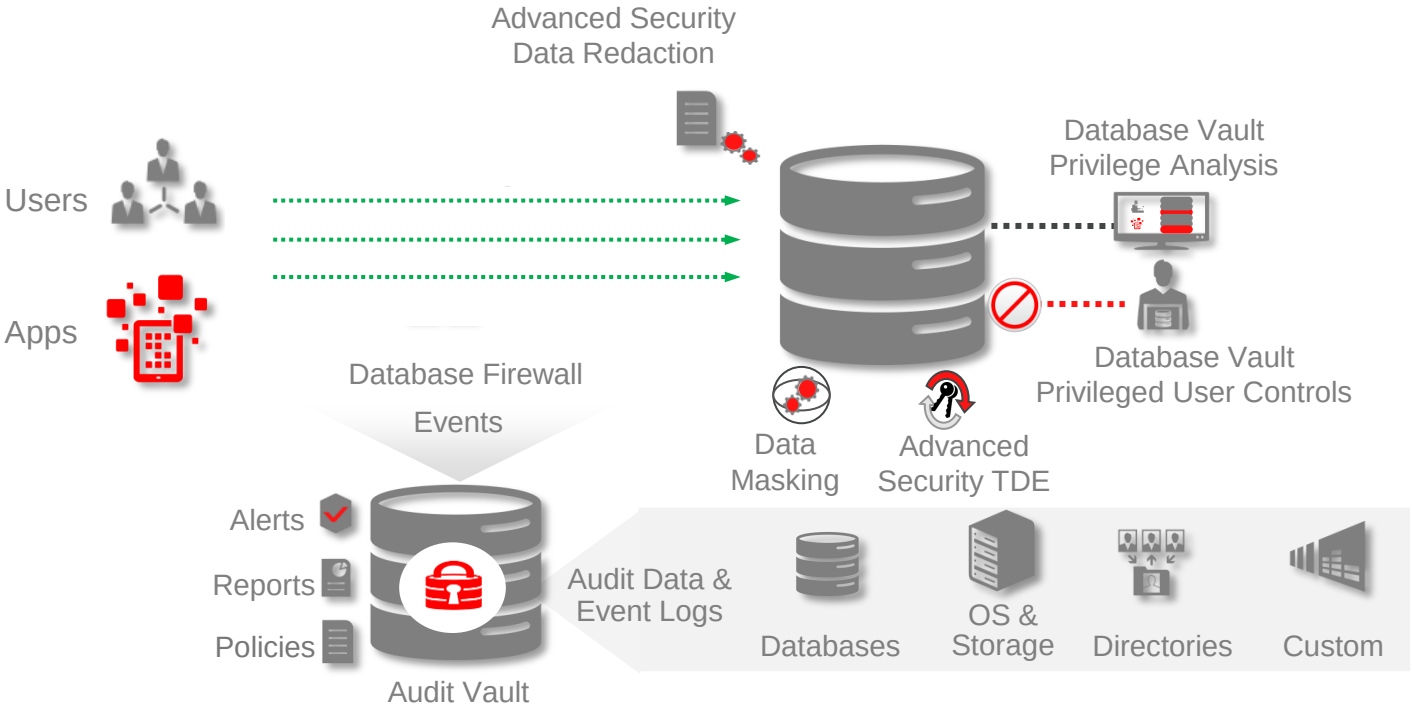
ORACLE

ORACLE

ORACLE

 Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Oracle Database Maximum Security Architecture



Copyright © 2013, Oracle and/or its affiliates. All rights reserved.