ORACLE®

Building Secure Database Applications

ORACLE OPEN WORLD

October 1–5, 2017
SAN FRANCISCO, CA

Scott Rotondo
Oracle Database Security
October 4, 2017

ORACLE

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.

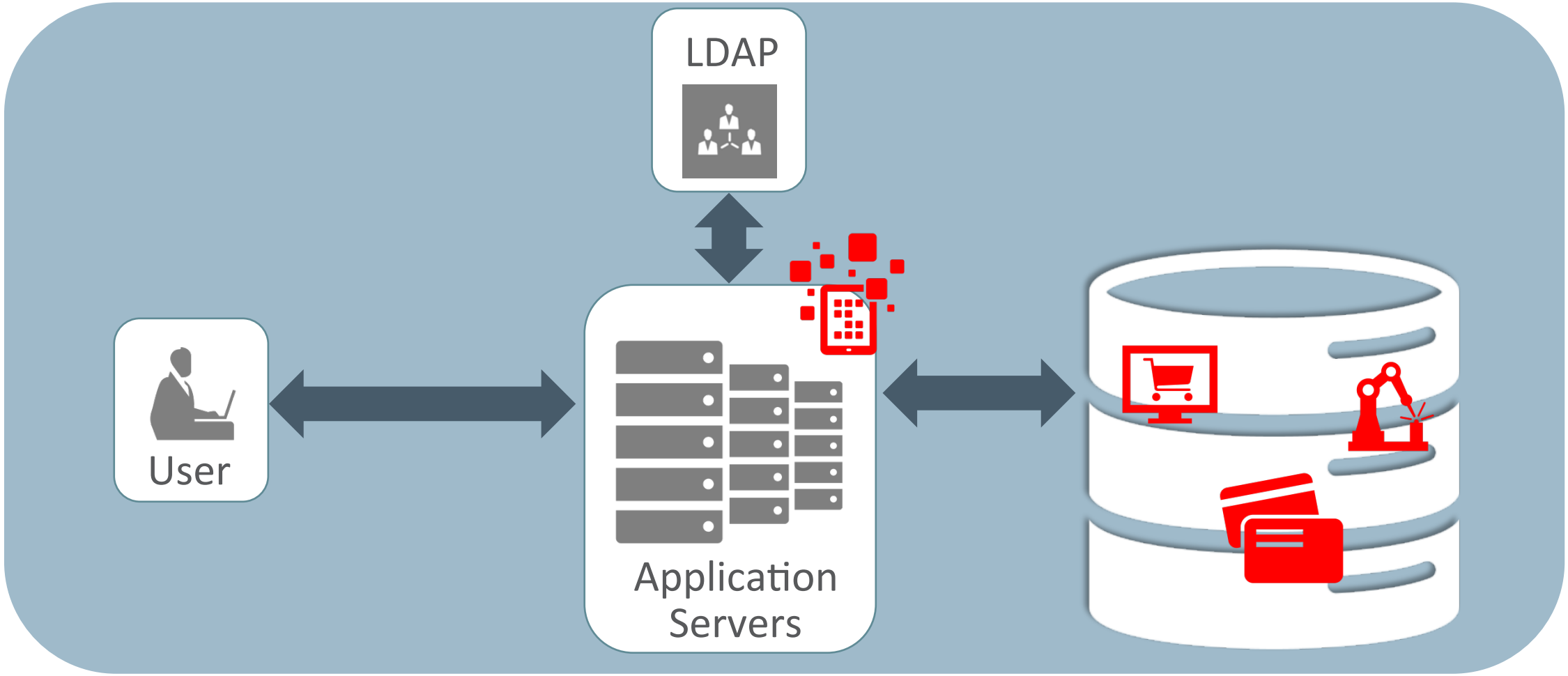
ORACLE

Defense-in-Depth Security for Databases

EVALUATE	PREVENT	DETECT	DATA DRIVEN SECURITY
Privilege Analysis	DBA & Operation Controls	Database / SQL Firewall	Label based Security
Security Configuration	Data Masking and Subsetting	Centralized Monitoring	Real Application Security
Security Assessment	Key Management	Alerting & Reporting	Row Level Security
Sensitive Data Discovery	Data Redaction	Database Auditing	Crypto Toolkit for Applications
	Data Encryption		

ORACLE

Typical Application Architecture



Problems with Typical Implementations

- All data is treated the same
  - Regardless of sensitivity or importance
- Application always runs with all the privileges it will ever need
  - Independent of end-user or operation being performed
- Database security protections don't match the application
  - Need richer, application-specific policies
- Insufficient auditing
  - To monitor application users and those who bypass it

ORACLE

Five Areas to Consider

1. Sensitive Data
2. Least Privilege
3. Basic Access Control
4. Application-Specific Protection
5. Auditing

ORACLE

Five Areas to Consider

1. Sensitive Data
2. Least Privilege
3. Basic Access Control
4. Application-Specific Protection
5. Auditing

ORACLE

Dealing with Sensitive Data

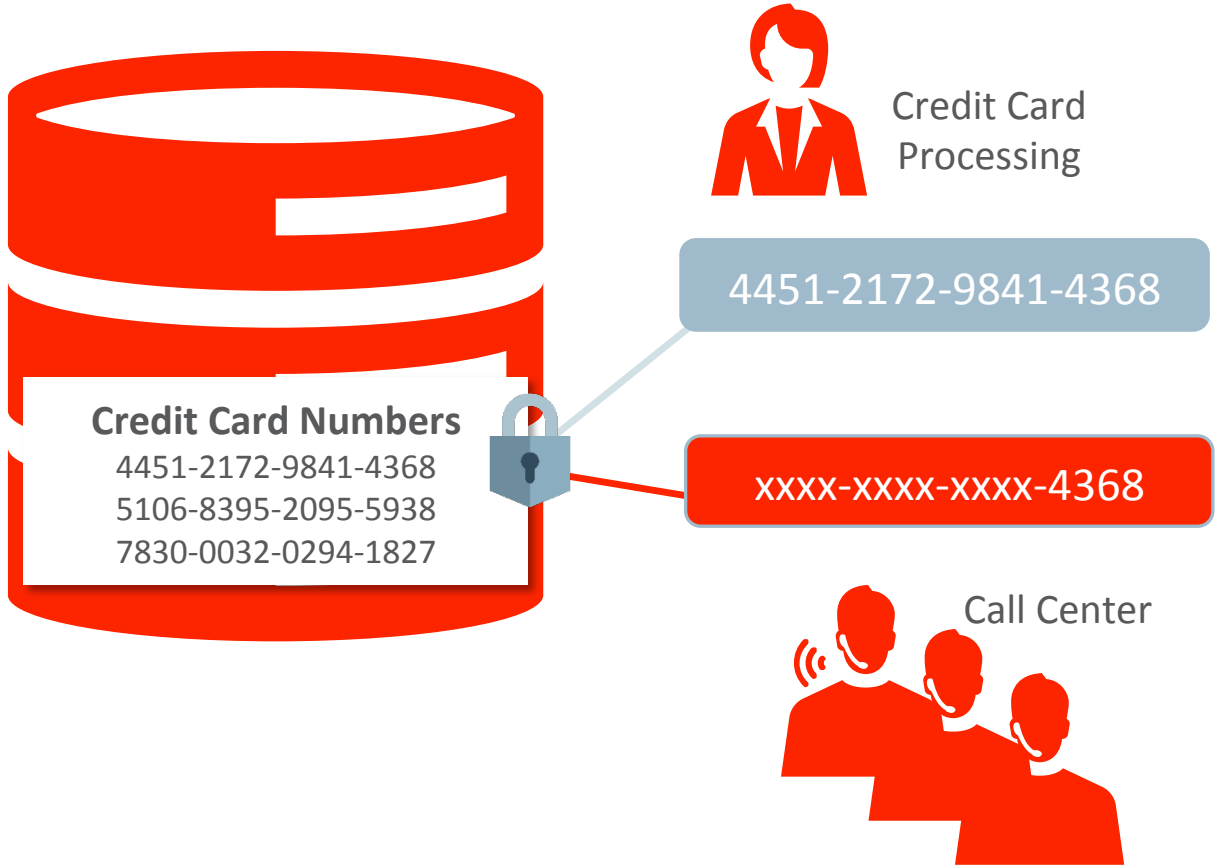
- Examples of sensitive data
  - Personally identifiable information (e.g. name, phone, national id)
  - Private records (e.g. medical, academic)
  - High-value information (e.g. corporate financials, intellectual property)
- Key issues
  - Discovering which information in the database is sensitive
  - Exposing sensitive data only in controlled ways

ORACLE

Discovering Sensitive Data

- Identify and catalog sensitive data
  - Enterprise Manager
  - DB Security Assessment Tool (DBSAT)
- Application Data Model describes sensitive types and relationships

Oracle Data Redaction



Real-time redaction of sensitive data based on context

Transparent to applications. No code changes required

Consistent enforcement within the database

No changes in regular database operations

Supported Transformations

	Stored Data	Redacted Results
Full	10/09/1992	01/01/2001
Partial	052-51-2147	XXX-XX-2147
Reg Exp	tim.lee@acme.com	[hidden]@acme.com
Random	4451-2172-9841-4368	4943-6344-0547-0110

ORACLE

Five Areas to Consider

1. Sensitive Data
2. Least Privilege
3. Basic Access Control
4. Application-Specific Protection
5. Auditing

ORACLE

Principle of Least Privilege

- Run each program with the minimum privileges needed to perform its intended function
- Limits possible damage if
  - The program contains a bug
  - A vulnerability is exploited by an attacker
- Sounds obvious, but this principle is violated all the time

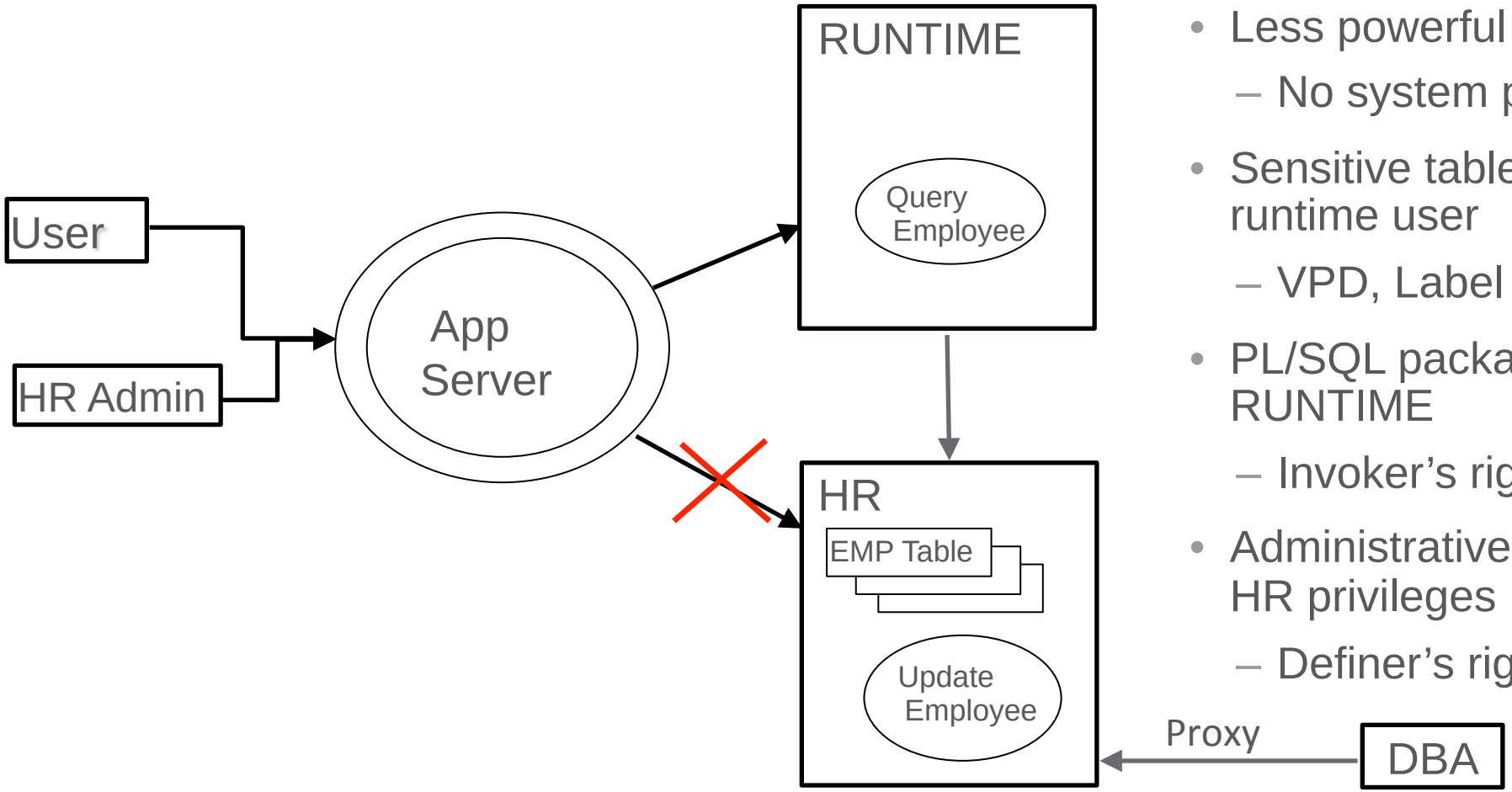
ORACLE

Review of Database Privileges and Roles

- The Oracle database supports two types of privilege
- Object privileges allow an operation on a specific object
  - grant SELECT on HR.EMPLOYEES to SCOTT
- System privileges apply to any object or to the database as a whole
  - grant DROP ANY TABLE to SCOTT
  - grant ALTER DATABASE to SCOTT
- Can assign privileges directly to users or indirectly via roles
- PL/SQL code can use either owner's or caller's privileges
  - Definer's vs. invoker's rights

ORACLE

Schema Separation



- Less powerful runtime account
  - No system privileges or DDL
- Sensitive tables protected from runtime user
  - VPD, Label Security, RAS
- PL/SQL packages called by RUNTIME
  - Invoker's rights
- Administrative packages run with HR privileges
  - Definer's rights

Code-Based Access Control

- Starting with Oracle 12c, a way to associate privileges with code instead of users
- Grant roles to a PL/SQL procedure or function
  - Privileges are active only while executing this block of code
- Similar in effect to definer's rights, except
  - Normal DR procedure uses only privileges directly granted to owner, not roles
  - Different procedures with the same owner can have different roles
  - Works with both definer's and invoker's rights procedures

ORACLE

Which Privileges Do I Need?

- We want to grant specific privileges to each user or schema
- But how do we know which privileges to grant?
- Start with analysis of the program, but …
  - Want to confirm that analysis empirically
  - What about existing programs?

ORACLE

Database Vault Privilege Analysis

- Capture and report on database privilege usage at runtime
  - For users, sessions, and roles (incl. PUBLIC)
  - Show used System, Object, and Public privileges
  - Show how the user got the privilege
- Show unused system and object privileges
- Administrator can modify privilege grants based on results

ORACLE

Unused Privileges Report

S/N	Policy	Grantee	Grantee Type	System Privileges	Grant Path
1	HR Analysis Policy	APPS	USER	DROP ANY TABLE	APPS
2	HR Analysis Policy	APPS	USER	ALTER ANY TABLE	APPS
3	HR Analysis Policy	APPS	USER	CREATE TABLE	APPS
4	HR Analysis Policy	APPS	USER	UNLIMITED TABLESPACE	APPS
5	HR Analysis Policy	APPS	USER	DROP ANY PROCEDURE	APPS,APPS_PATCHING
6	HR Analysis Policy	APPS	USER	CREATE PROCEDURE	APPS,APPS_PATCHING

Used Privileges Report

S/N	Policy	User Name	Used Role	System Privileges	Object			Grant Path
					Owner	Name	Type	
1	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	DEPARTMENTS	TABLE	APPS
2	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	JOB_HISTORY	TABLE	APPS
3	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	COUNTRIES	TABLE	APPS
4	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	EMPLOYEES	TABLE	APPS
5	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	LOCATIONS	TABLE	APPS
6	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	REGIONS	TABLE	APPS
7	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	JOBS	TABLE	APPS
8	HR Analysis Policy	APPS	APPS	CREATE SESSION			(null)	APPS
9	HR Analysis Policy	APPS	PUBLIC	(null)	SYS	DBMS_APPLICATI...	PACKAGE	PUBLIC
10	HR Analysis Policy	APPS	PUBLIC	(null)	SYSTEM	PRODUCT_PRIVS	VIEW	PUBLIC
11	HR Analysis Policy	APPS	PUBLIC	(null)	SYS	DUAL	TABLE	PUBLIC

ORACLE

Five Areas to Consider

1. Sensitive Data
2. Least Privilege
3. Basic Access Control
4. Application-Specific Protection
5. Auditing

Virtual Private Database

Database Enforced Row Level Security

Sales Rep

US Region

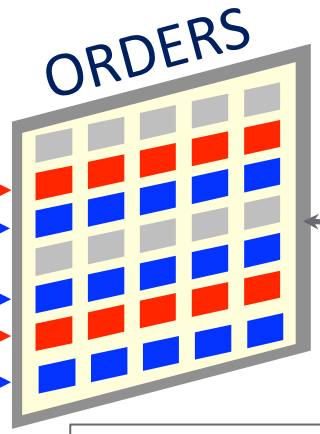
Select * from Orders

Where Region= 'US'

EU Region

Select * from Orders

Where Region = 'EU'



- Restrict access to subset of data
  - Row filtering
  - Column masking
- Customizable policies
  - Application context value
  - Current system state
  - Current and foreign tables

Oracle Label Security

Label Based Access Control

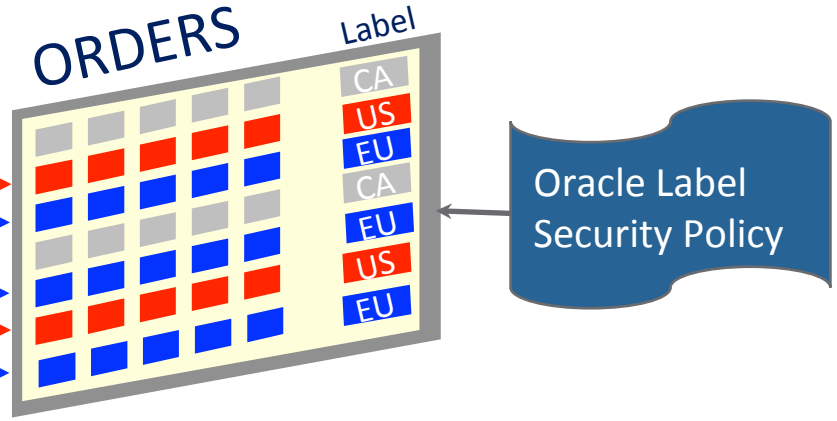
Sales Rep

US Region

Select * from Orders

EU Region

Select * from Orders



- Classify data based on application
- Level, Compartment, Group
- Authorizations to application or database users
- Authorizations can be managed in directory

Who Is Trying to Access Data?

Access Control Requires Authentication

- End user identity must be known to the database
  - Database can manage users for client-server applications
  - Three-tier application must propagate user identity to database
    - Allows database to enforce access control based on user identity
    - Allows auditing to track who actually performed the operation

ORACLE

Application Context

USERENV Fixed Attributes

- Information about current session
- Most predefined attributes cannot be modified

USERENV Modifiable Attributes

- Set by DBMS_APPLICATION_INFO, JDBC, OCI
- Recorded in audit trail

Application Namespace

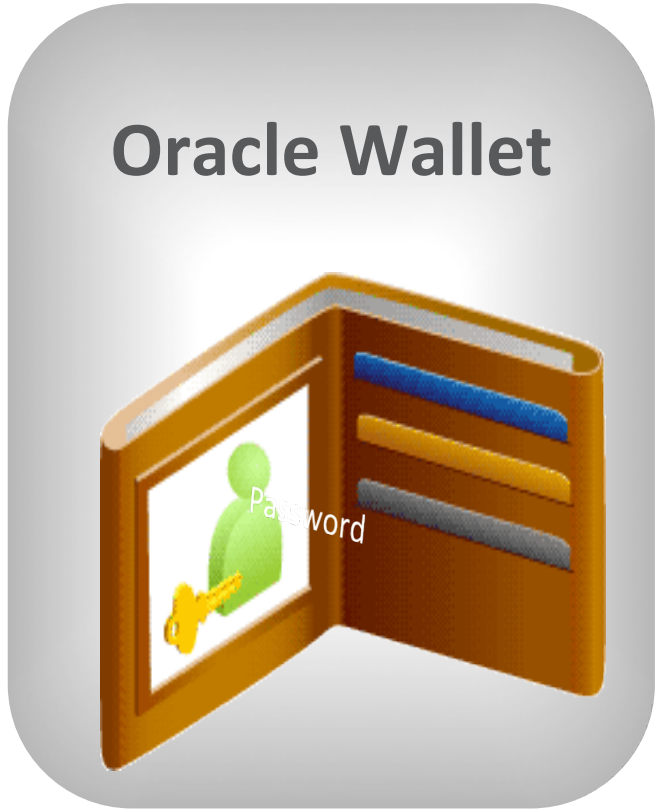
- Key-value pairs set by designated PL/SQL package
- Each application has its own namespace

ORACLE

Authenticating the Application

Secure External Password Store

- Secure database-external location to store application and user passwords
  - Leverages the Oracle Wallet
  - Passwords never in the clear on file system
  - Accessible from OCI, SQL*Plus, JDBC
- Supports using different password credentials for different databases



Five Areas to Consider

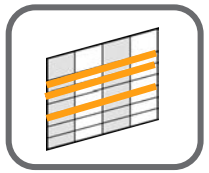
1. Sensitive Data
2. Least Privilege
3. Basic Access Control
4. Application-Specific Protection
5. Auditing

ORACLE

Oracle Real Application Security (RAS)

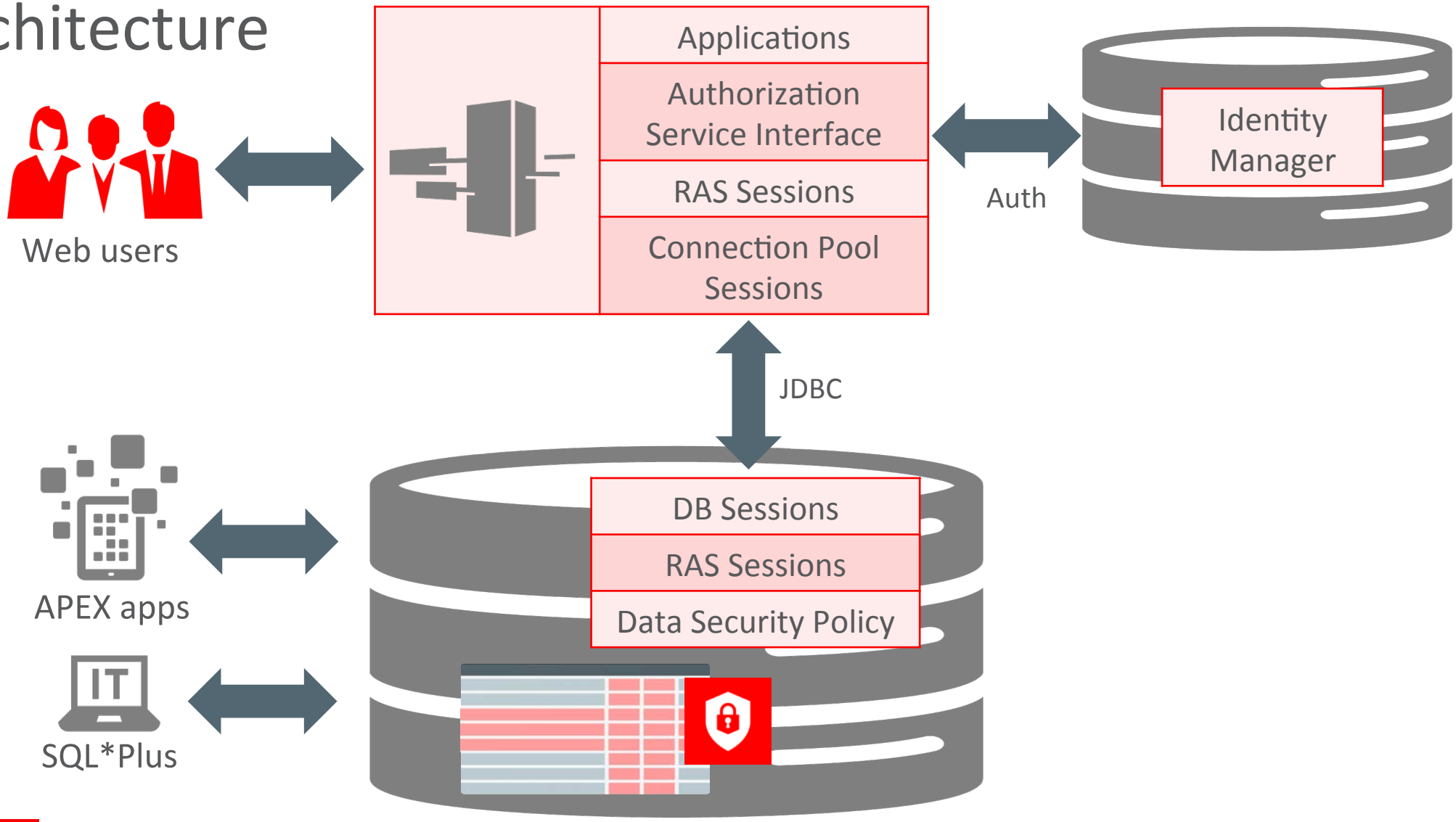
- Support Application Users and Sessions
  - Schema-less user, Security and application context in DB

- Support Application Privileges and Roles
  - E.g., *ViewSalary, RequestLeave, ApproveLeave* privileges
  - E.g., *Manager*, *HR_Rep*, *Approver* roles



- Support fine-grained data access control on rows and columns
  - Based on user operation execution context
  - Enforce security close to data

RAS Architecture



Example: Access Control Requirements

- Employees can view public information
- An employee can view own record, update contact information
- Manager can view salary of his/her reports

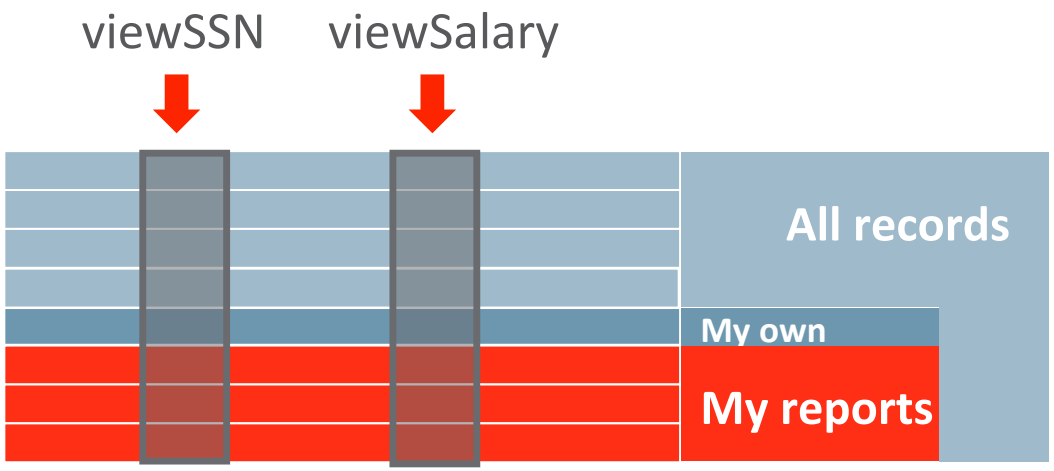
Name	Manager	SSN	Salary	Phone Number
Adam	Steven			515.123.4567
Neena	Steven			515.123.4568
Nancy	**Neena**	**108-51-4569**	**12030**	**650.111.3300**
Luis	Nancy		6900	515.124.4567
John	Nancy		8200	515.124.4269
Daniel	Nancy		9000	515.124.4469

ORACLE

Real Application Security Concepts

Data Realms

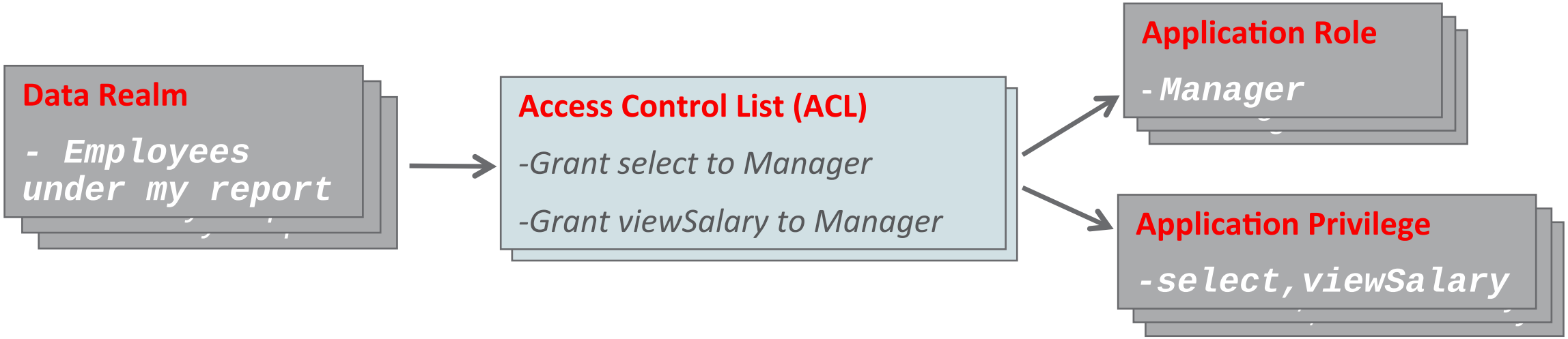
- A group of rows representing a business object
  - All employees
  - My own employee record
  - All employees reporting to me
- Assign privileges to columns
  - *viewSSN* for SSN column
  - *viewSalary* for Salary column



EMPLOYEE table

Real Application Security

Data Security Policy Components



- Each Data Realm has an associated ACL with grants
- Data Security policy is a collection of Data Realms and ACLs

RAS APEX HR Application

Manager

Can view salaries of my reports

Employee | Org Chart

Employee

Go | Rows 15 | Actions

	Name	Manager	SSN	Salary	Phone Number	Email Id
	Diana Lorentz	Alexander Hunold	-	-	590.423.5567	DLORENTZ
	Valli Pataballa	Alexander Hunold	-	-	590.423.4560	VPATABAL
	Daniel Faviet	Nancy Greenberg	-	9000	515.124.4169	DFAVIET
	Ismael Sciarra	Nancy Greenberg	-	7700	515.124.4369	ISCIARRA
	John Chen	Nancy Greenberg	-	8200	515.124.4269	JCHEN
	Jose Manuel Urman	Nancy Greenberg	-	7800	515.124.4469	JMURMAN
	Luis Popp	Nancy Greenberg	-	6900	515.124.4567	LPOPP
	Nancy Greenberg	Neena Kochhar	108-51-4569	12008	515.124.4564	NGREENBE
	Den Raphaely	Steven King	-	-	515.127.4561	DRAPHEAL

Org Hierarchy

- Steven King
  - Neena Kochhar
    - Nancy Greenberg
      - Daniel Faviet
      - John Chen
      - Ismael Sciarra
      - Jose Manuel Urman
      - Luis Popp
    - Jennifer Whalen
    - Hermann Baer
    - Shelley Higgins
      - William Gietz
    - Susan Mavris
  - Lex De Haan

Oracle Real Application Security

Uniform Authorization on All Access Paths

Manager 'Nancy'

Direct connect to DB with SQLPLUS

```
$ sqlplus ngreenbe

......

NGREENBE> select NAME, EMAIL, SSN, SALARY, OFFPH  from HRSCHEMA.EMPLOYEE;

NAME                 EMAIL                SSN             SALARY OFFPH
-------------------- -------------------- ----------- --------- ---------------
Steven King          SKING                                      515.123.4567
Neena Kochhar        NKOCHHAR                                   515.123.4568
Lex De Haan          LDEHAAN                                    515.123.4569
Alexander Hunold     AHUNOLD                                    590.423.4567
Bruce Ernst          BERNST                                     590.423.4568
David Austin         DAUSTIN                                    590.423.4569
Valli Pataballa      VPATABAL                                   590.423.4560
Diana Lorentz        DLORENTZ                                   590.423.5567
Nancy Greenberg      NGREENBE             108-51-4569     12008 515.124.4569
Daniel Faviet        DFAVIET                               9000 515.124.4169
John Chen            JCHEN                                 8200 515.124.4269
Ismael Sciarra       ISCIARRA                              7700 515.124.4369
Jose Manuel Urman    JMURMAN                               7800 515.124.4469
Luis Popp            LPOPP                                 6900 515.124.0000
Den Raphaely         DRAPHEAL                                   515.127.4561
Alexander Khoo       AKHOO                                      515.127.4562
Shelli Baida         SBAIDA                                     515.127.4563
Siqal Tobias         STOBIAS                                    515.127.4564
```

RAS Administration Tool

Home | Policies | Privileges | Namespaces | Users | Roles | Settings

Home > Policies > Policy Definition

Policy — Cancel | Delete | Apply Changes

Policy Name * HRM.EMPLOYEE_POLICY

Description: Policy for Employee Records

Protected Objects: HRM.EMPLOYEES +

Data Realm Authorization — Delete | Add

Realm Description	SQL Predicate	ACL	Reorder
ALL_RECORDS	1=1	HRM.ALL_EMP_ACL	
MY_RECORD	EMPLOYEE_ID IN (SELECT EMPLOYEE_ID FROM HRM.USER_PROFILE WHERE LOGON_NAME = XS_SYS_CONTEXT('XS$SESSION','USERNAME'))	HRM.MY_EMP_ACL	
MY_REPORTS	EMPLOYEE_ID IN (SELECT EMPLOYEE_ID FROM (SELECT EMPLOYEE_ID, level lvl FROM HRM.MANAGERS M START WITH M.EMPLOYEE_ID IN (SELECT ...	HRM.MY_REPORT_ACL	

1 - 3

Column Authorization — Delete | Add

Column	Privilege	Description
SALARY	VIEW_SALARY	To view Salary column
SSN	VIEW_SSN	To view SSN column

1 - 2

Employees Table

1. All records
2. My record
3. My reports

Restricted Salary & SSN Columns

Privilege Grants

Data Security Patterns

Session attribute based	• VP can view employee salaries of his organization
Master/Detail	• An Employee record and its Job History line items are protected as a single logical record
Parameterized Grant	• Managers in each region, e.g., East and West, access employee records, striped based on region
Conditionally related	• HR representative can change job designation, if the employee is assigned to him
Exceptions	• A contract worker needs temporary access to certain employee records

ORACLE

Five Areas to Consider

1. Sensitive Data
2. Least Privilege
3. Basic Access Control
4. Application-Specific Protection
5. Auditing

ORACLE

What Actually Happened?

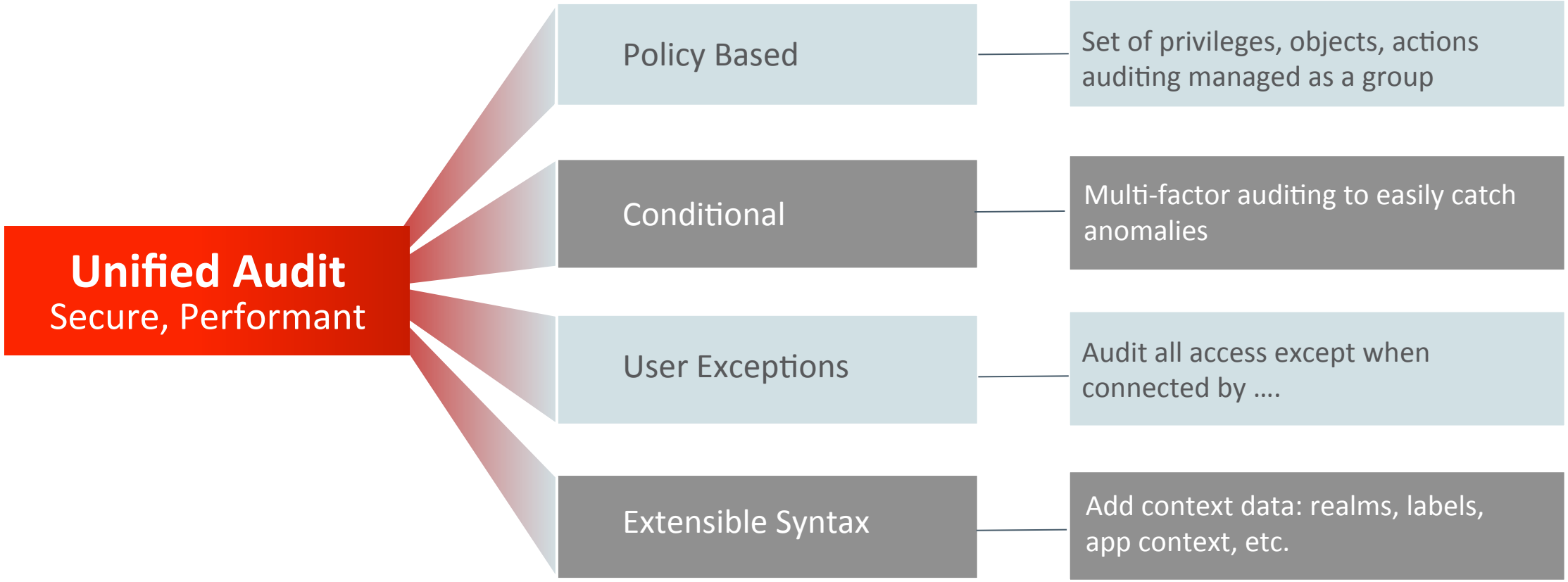
Auditing the Application from the Database

- Monitor privileged user accounts for non-compliant activity
  - Audit non-application access to sensitive data (credit card, financial data, personally identifiable information, etc.)
- Verify that no one is trying to bypass the application controls/security
- Audit application activity selectively
  - Perhaps audit changes to the most sensitive data even from within the application

ORACLE

Oracle Database Auditing

Catch Anomalies with Conditional Auditing



Audit Policy Example

Audit Accesses that Bypass Application Code

- CREATE AUDIT POLICY hr_app_policy

  ACTIONS ALL ON HR.EMPLOYEES

  WHEN 'UPPER(SYS_CONTEXT (''USERENV'', ''MODULE'')) != ''HR_APP'')' EVALUATE PER SESSION;
- AUDIT POLICY hr_app_policy EXCEPT hr;

Bringing it all together…

ORACLE

Summary

- Think security from the beginning
- Identify and catalog sensitive data
- Minimize privilege based on user and action
- Use Database Security to control access to data
  - Consistent enforcement
  - Easy to extend and adapt
  - Close to data and not bypassable
- Audit changes to application and data

ORACLE

Visit Us in the Oracle Database Security Demo Grounds

Demo Booth Title	Featured Solutions
Authentication & Authorization	Centrally Managed Users, Database Vault, Real Application Security, Label Security
Encryption & Key Management	Transparent Data Encryption, Key Vault, Data Redaction
Auditing and Activity Monitoring	Database Auditing, Audit Vault and Database Firewall, Data Security Cloud Service - Auditing
Database Security for Application Developers	Database Security Assessment Tool, Data Masking and Subsetting, Data Discovery and Data Security Cloud Service - Masking

ORACLE

Integrated Cloud

Applications & Platform Services

ORACLE

ORACLE®