
ORACLE®

Building Secure Database Applications Quickly in the Cloud Era

TIP4104

Alan Williams, Senior Principal Product Manager
Oracle Database Security
October 2018

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

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		

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Application Data Security

1. Application Data Security
2. Virtual Private Database
3. Real Application Security
4. Oracle Label Security
5. Comparison

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

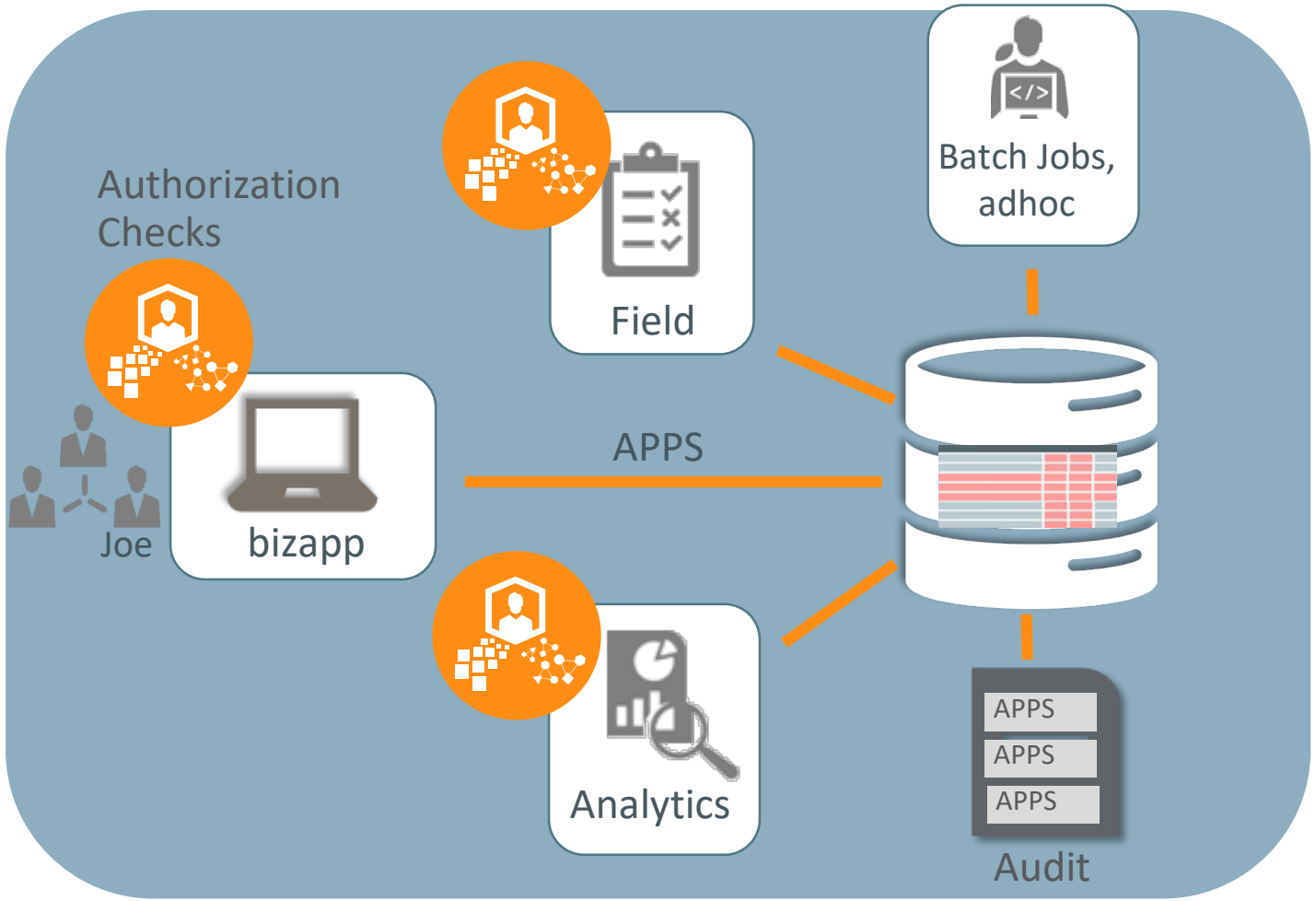
Example Application Security Requirements: HR

- 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

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Challenges with Application Data Security

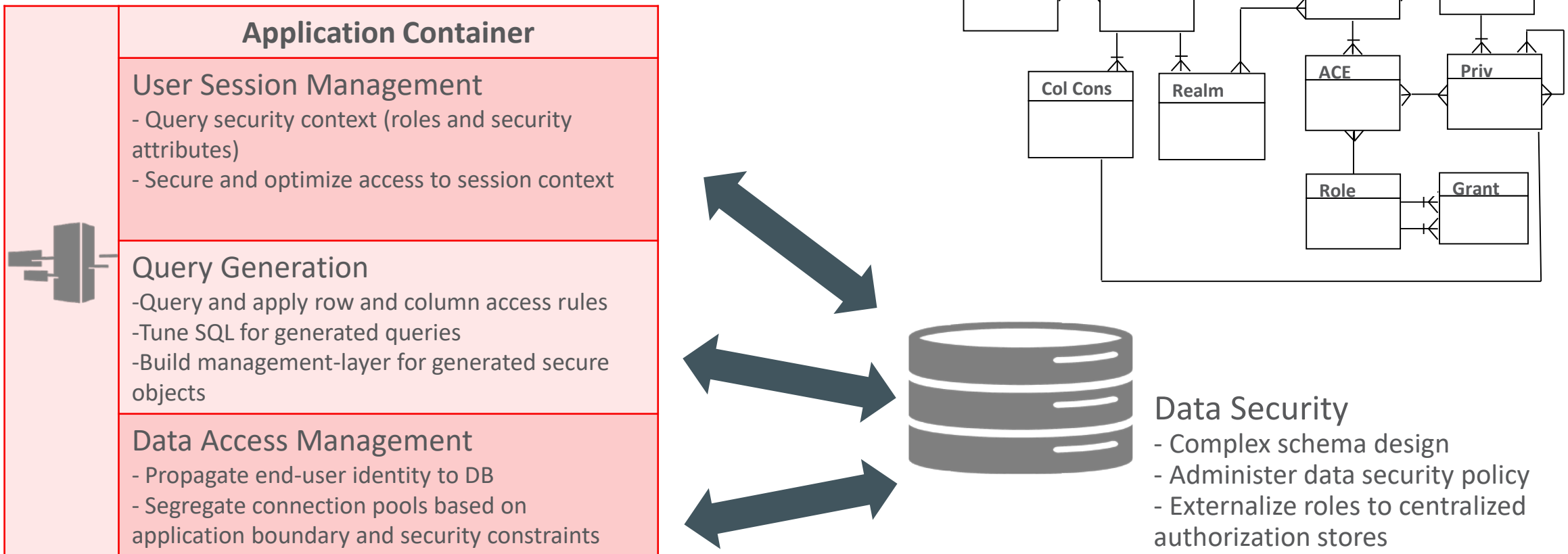


Highlights

- Security checks embedded in application logic
- High risks with big-user connection
- Fragmented security
- Data not protected from direct connection
- No application user audit
- Complex development and maintenance

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

How Enterprise Data Access Control is Typically Done



Data Security

- Complex schema design
- Administer data security policy
- Externalize roles to centralized authorization stores
- Secure direct access to data using separate policy and mechanism

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Oracle Data Driven Security

Virtual Private Database (DBMS_RLS)

Fine-grain access control (row/column)

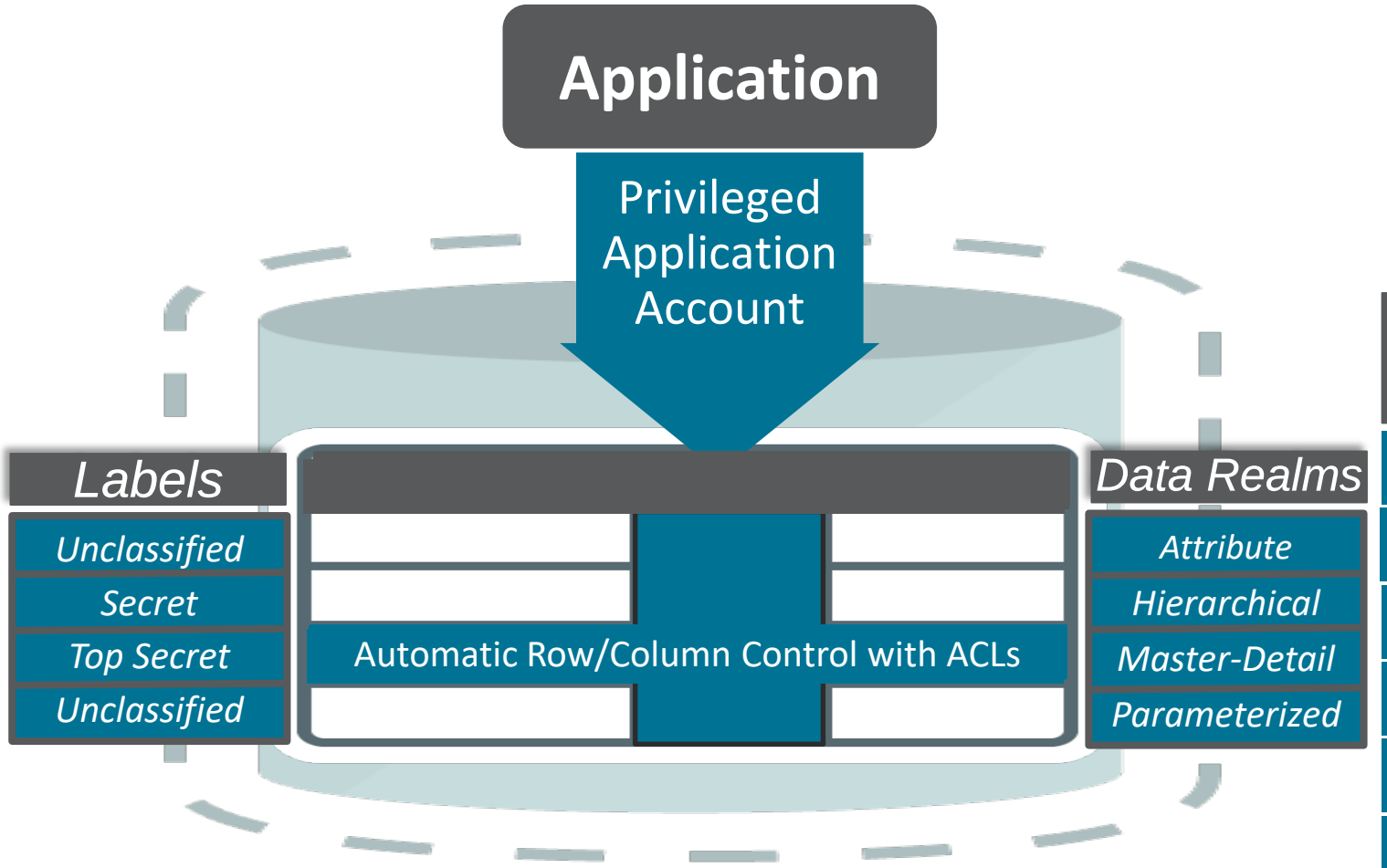
Predicate-based : User/Role, System / Application context, …

Oracle Label Security

Label based Access Control Platform

Declarative

User & Data Labels



Real Application Security

Rich Policy Model

Real Users & Roles

Audit Real User

APEX/FMW conn

Declarative

End-to-End

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Virtual Private Database (VPD)

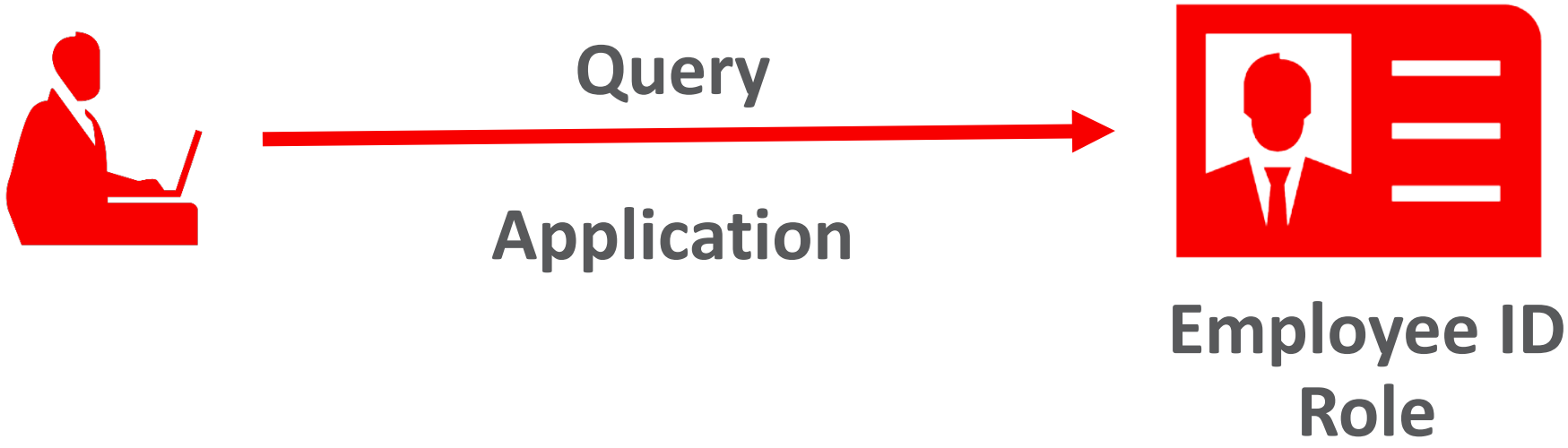
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Virtual Private Database

- VPD was one of the first database security innovations introduced nearly 20 years ago with Oracle 8i
- Also called Row Level Security (RLS) and Fine Grained Access Control (FGAC)

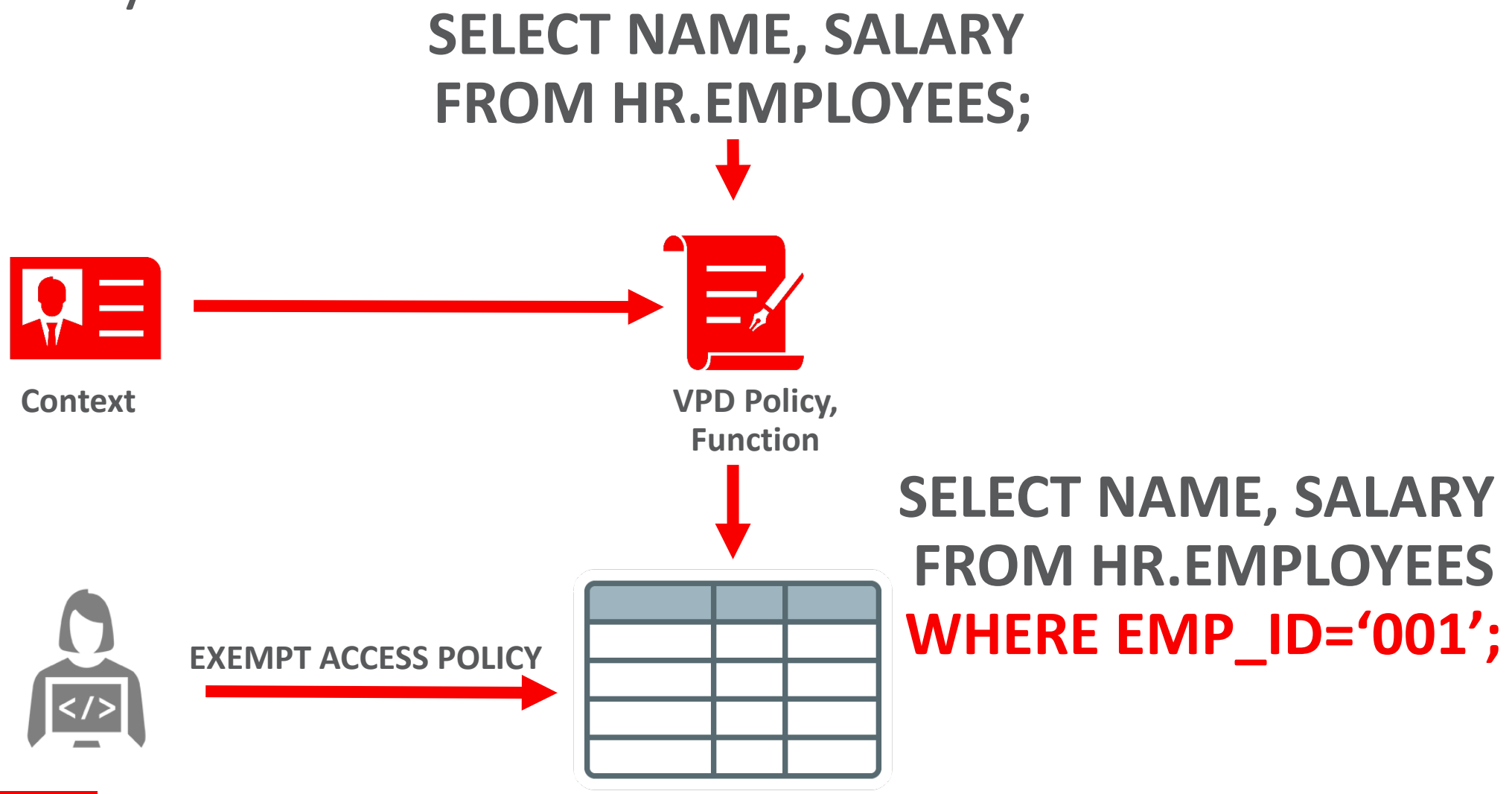
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Set User Context



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

VPD Policy



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

VPD Tips and Tricks

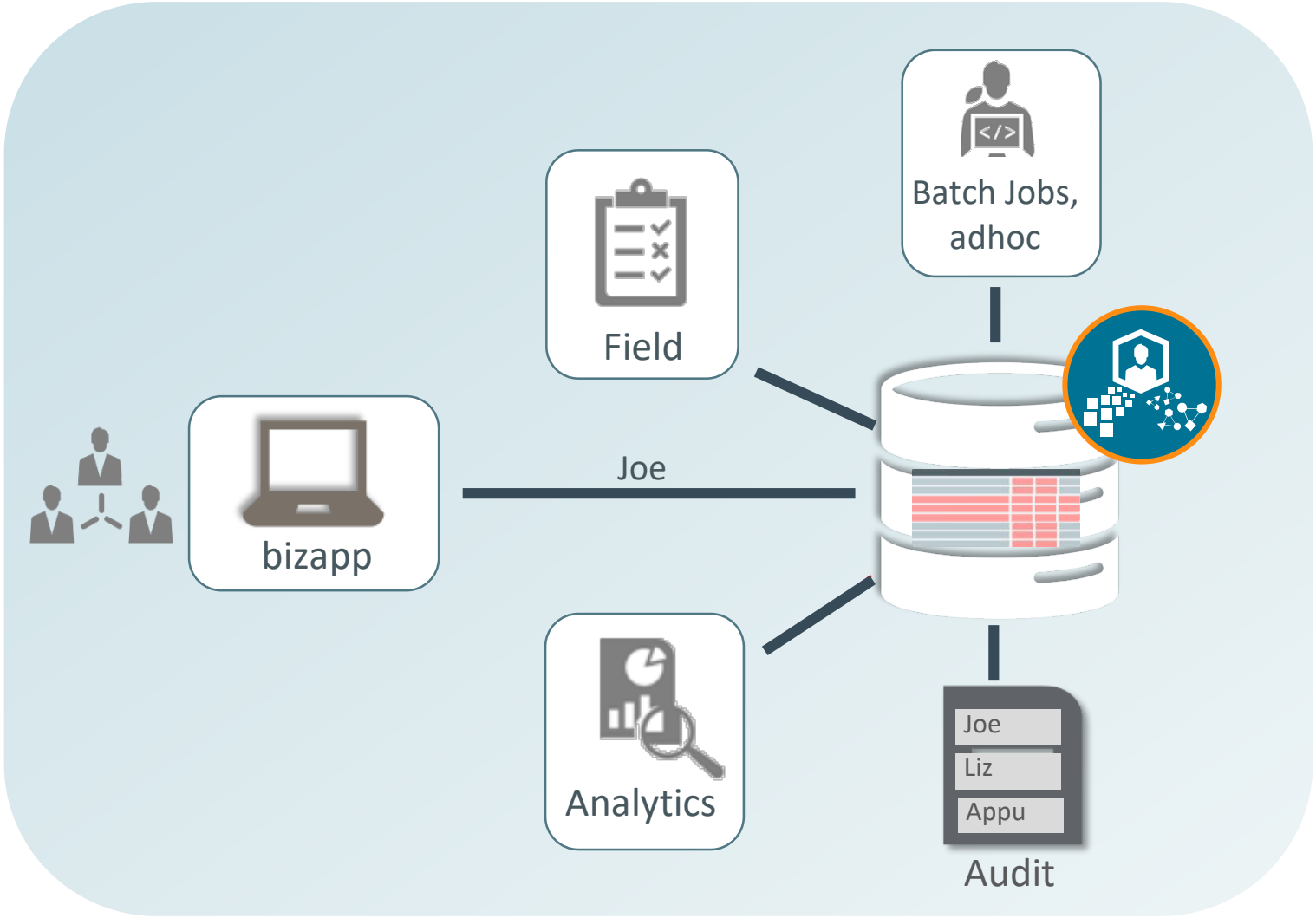
- Prevent SQL injection attacks from application layer
- Integrate with other DB security features
  - Redaction – redact column data
  - Label Security – protect column data
- Increased VPD complexity over time leads to maintainability concerns
- Use VPD to meet simple requirements

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Real Application Security (RAS)

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Oracle Real Application Security (RAS)

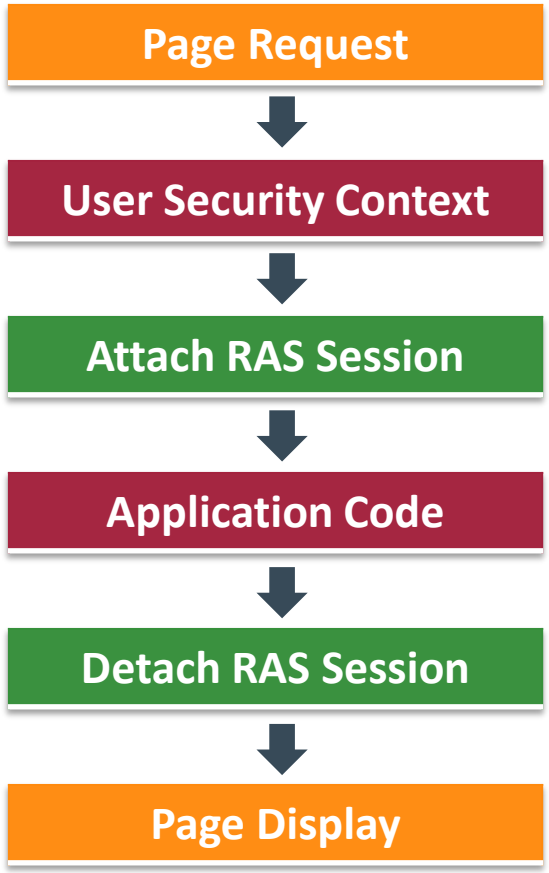


Highlights

- Application user session propagation to the database
- Data security based upon application users, role, privileges, and various relationships
- Centralized data access security controls
- Security enforced for all connections
- Audit of application user activity
- Simplified administration with declarative security

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

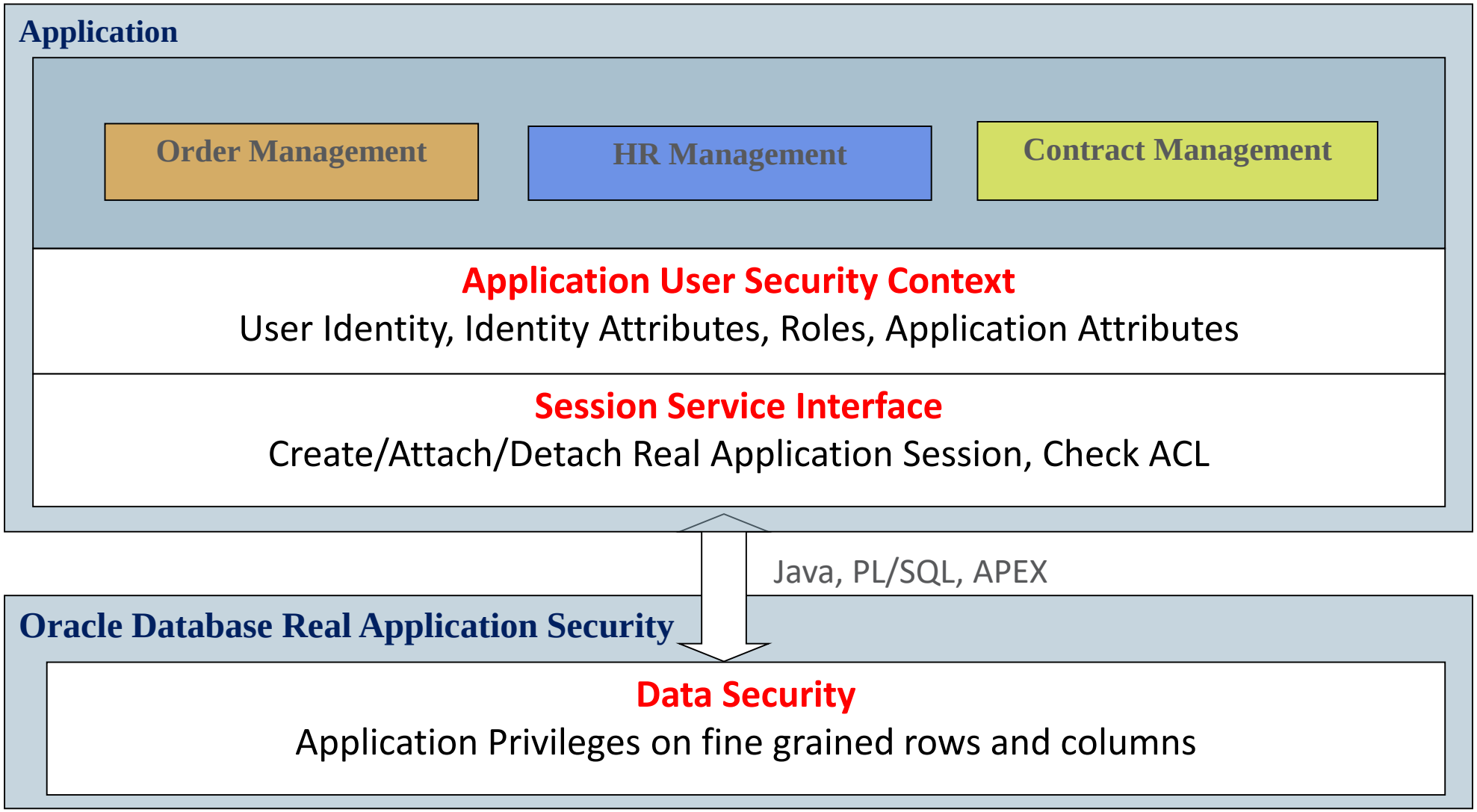
Application Framework Runtime Integration



- Application users authenticated in application layer
- RAS session contains application user, its roles, and session context
- Based on authenticated user's security context
- Application code executes within RAS session
- Attached and detached to a database session

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Oracle Real Application Security Services



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Oracle Real Application Security

Key Features Provided in the Database

- 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

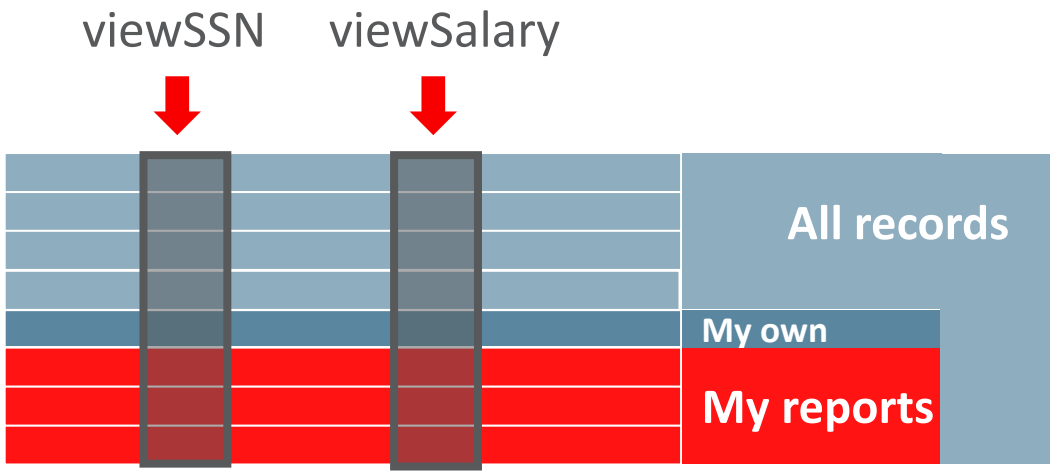
- Support fine-grained data access control on rows and columns
  - Based on user operation execution context
  - Enforce security close to data

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Real Application Security Concepts

Data Realms

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

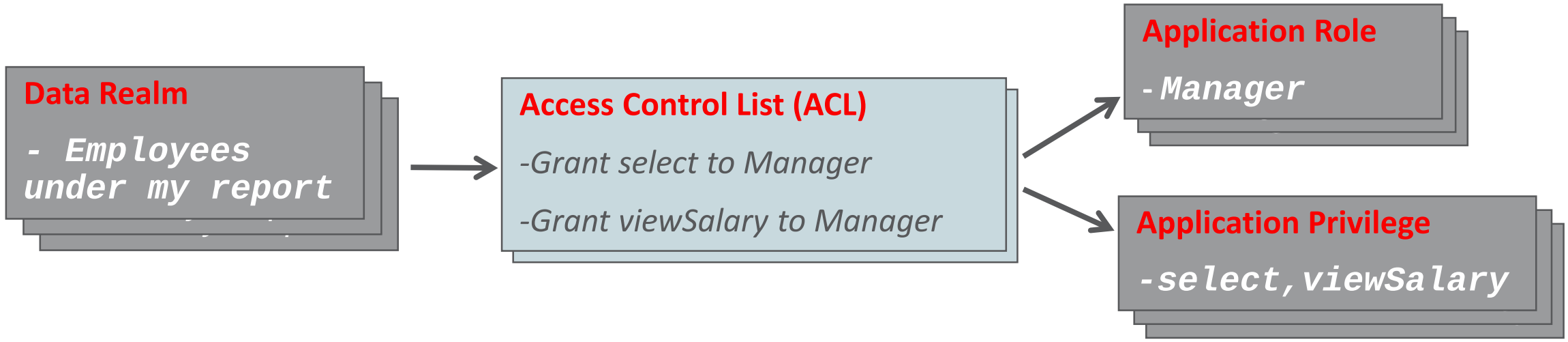


Employee table

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Real Application Security

Data Security Policy Components



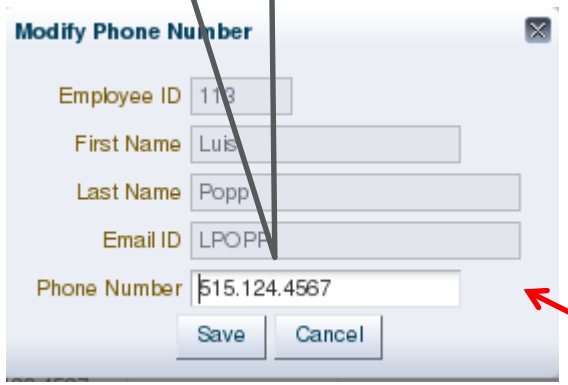
- Each Data Realm has an associated ACL with grants
- Data Security policy is a collection of Data Realms and ACLs

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

RAS HR Application

Luis Popp

Can update certain columns



http://local...empmgr.jspx | Employee Report

localhost:7001/hrdemo/faces/myempmgr.jspx

Most Visited | RAS-FMW Demo | RAS-APEX Demo | RASADM | APEX Admin | WLS Console

ORACLE HR Information *Secured by RAS* LPOPP Logout

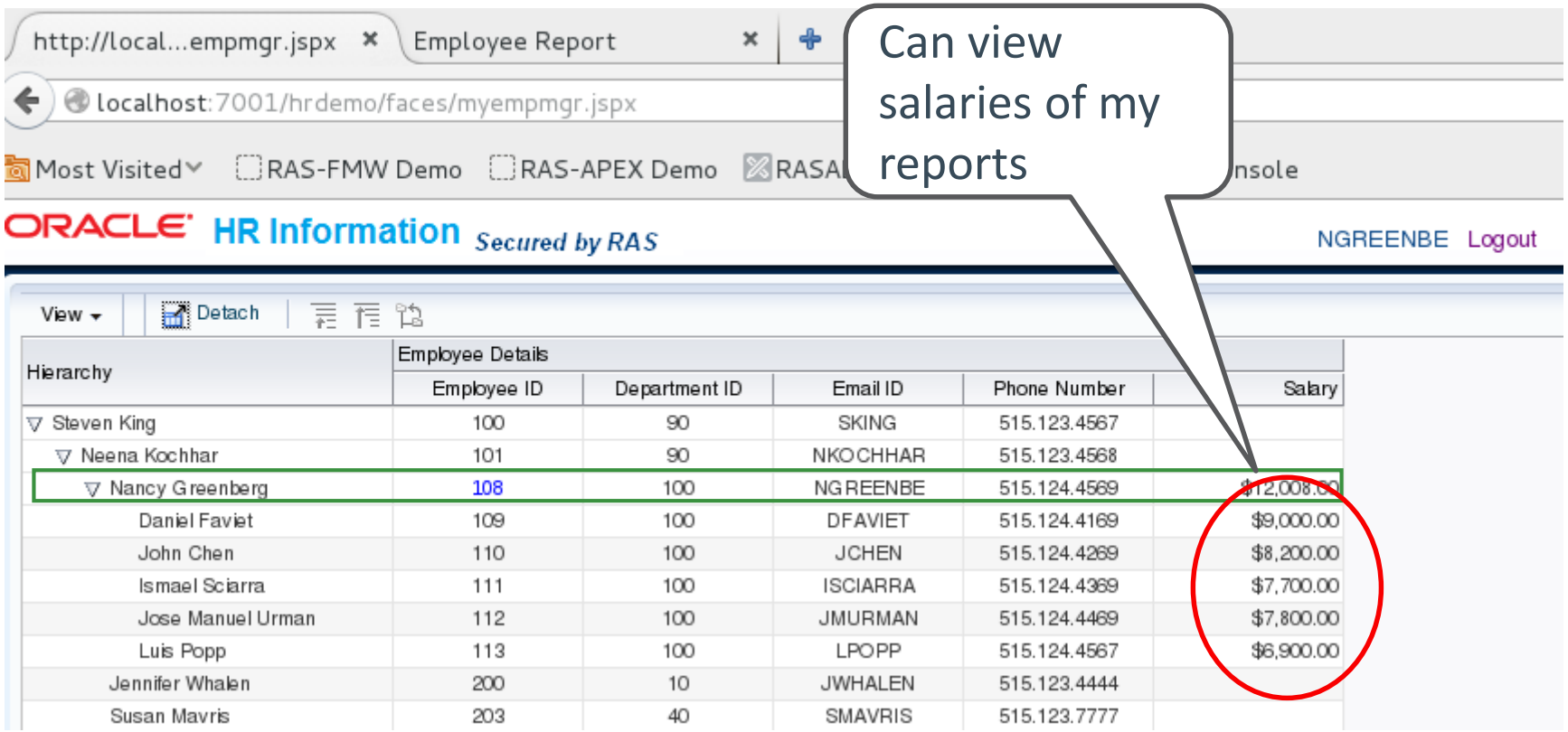
View | Detach

Hierarchy	Employee Details				
	Employee ID	Department ID	Email ID	Phone Number	Salary
Steven King	100	90	SKING	515.123.4567	
Neena Kochhar	101	90	NKOCHHAR	515.123.4568	
Nancy Greenberg	108	100	NGREENBE	515.124.4569	
Daniel Faviet	109	100	DFAVIET	515.124.4169	
John Chen	110	100	JCHEN	515.124.4269	
Ismael Sciarra	111	100	ISCIARRA	515.124.4369	
Jose Manuel Urman	112	100	JMURMAN	515.124.4469	
Luis Popp	113	100	LPOPP	515.124.4567	$6,900.00
Jennifer Whalen	200	10	JWHALEN	515.123.4444	
Susan Mavris	203	40	SMAVRIS	515.123.7777	
Hermann Baer	204	70	HBAER	515.123.8888	
Shelley Higgins	205	110	SHIGGINS	515.123.8080	
William Gietz	206	110	WGIETZ	515.123.8181	

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

RAS HR Application

Manager “Nancy”



Hierarchy	Employee Details				
	Employee ID	Department ID	Email ID	Phone Number	Salary
▽ Steven King	100	90	SKING	515.123.4567	
▽ Neena Kochhar	101	90	NKOCHHAR	515.123.4568	
▽ Nancy Greenberg	108	100	NGREENBE	515.124.4569	$12,008.00
Daniel Faviet	109	100	DFAVIET	515.124.4169	$9,000.00
John Chen	110	100	JCHEN	515.124.4269	$8,200.00
Ismael Sciarra	111	100	ISCIARRA	515.124.4369	$7,700.00
Jose Manuel Urman	112	100	JMURMAN	515.124.4469	$7,800.00
Luis Popp	113	100	LPOPP	515.124.4567	$6,900.00
Jennifer Whalen	200	10	JWHALEN	515.123.4444	
Susan Mavris	203	40	SMAVRIS	515.123.7777	

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

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
Sigal Tobias         STOBIAS                                    515.127.4564
```

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Enterprise Application Data Security Patterns and Features

- Session attribute based
- Master/Detail
- Parameterized Grant
- Conditionally related
- Exceptions
- Controlled Delegation
- Effective-date support
- Negative grants
- Code-based security
- Function Security
- Auditing

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

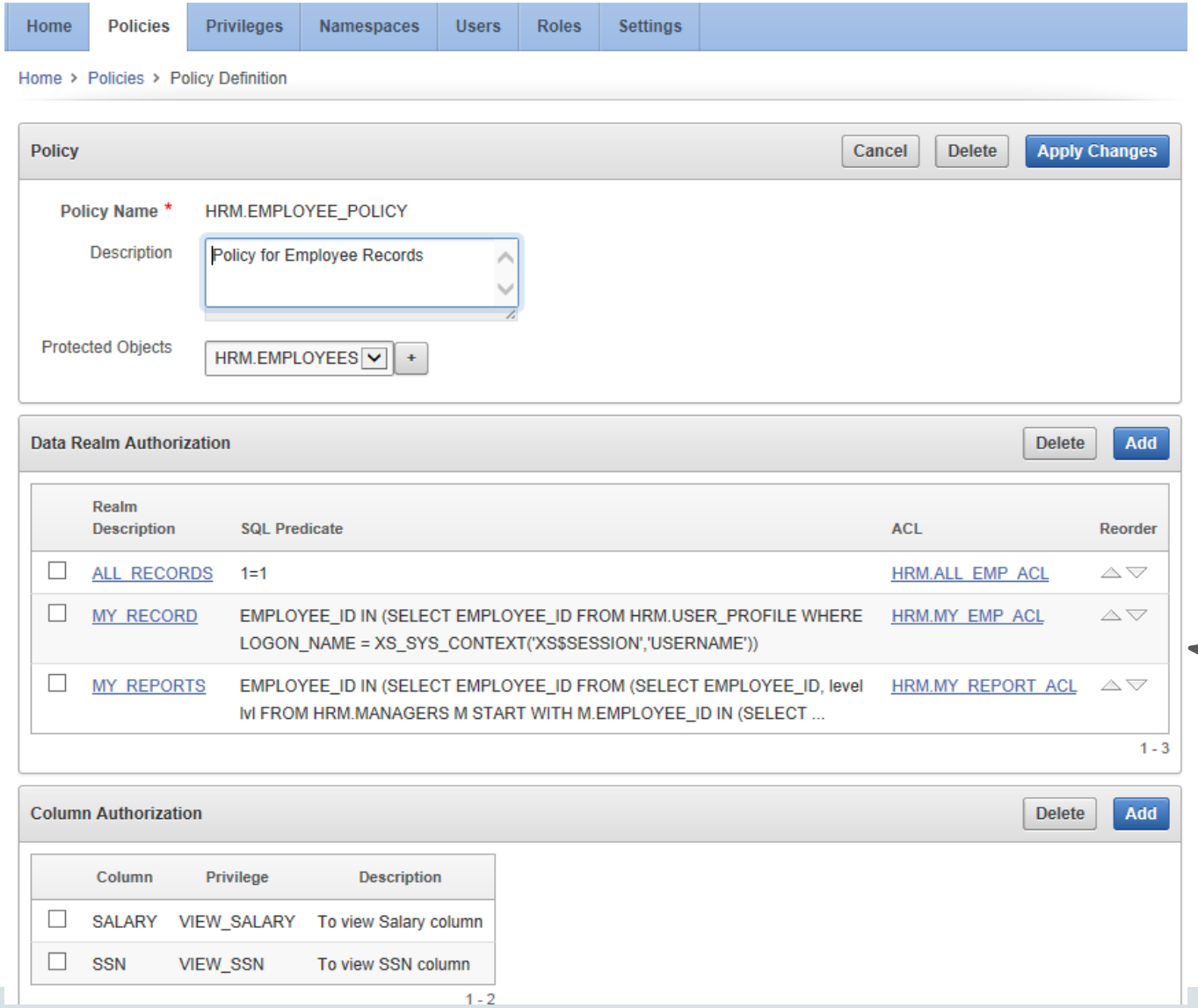
RAS Administration Tool

Data Security

Employees Table

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

Restricted Salary & SSN Columns



Privilege Grants

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Real Application Security

- Application and Database Development
- Best used with new Java or APEX application development
- Normally not practical with 3rd party applications due to required application changes
- Develop using API and GUI

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Oracle Label Security (OLS)

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

What is Oracle Label Security and what does it do?

- Oracle Label Security provides fine-grained access to individual table rows
- OLS shortly after VPD
- Embedded in DB starting with in 12c
  - `EXEC LBACSYS.OLS_ENFORCEMENT.ENABLE_OLS`
- SQL query transparent (e.g. same query returns 10 rows instead of all 1000 rows)
- Management via Oracle Enterprise Manager Cloud Control or APIs
- Integrated with Oracle Database Vault, Oracle Advanced Security Data Redaction, Real Application Security

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Components of Oracle Label Security

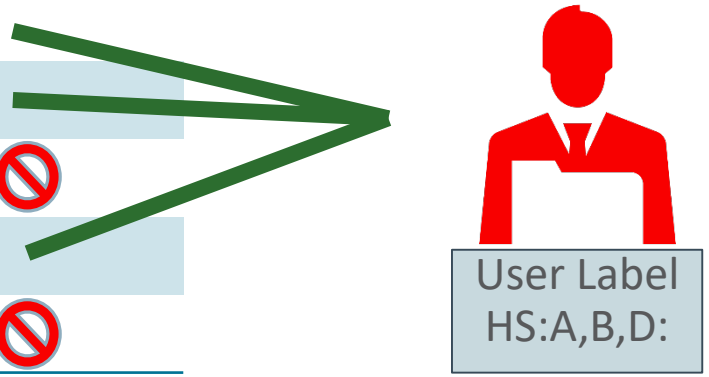
- Oracle Label Security has two high-level components
  - Labels
    - Consists of User and Data labels
    - Governs access to specific protected objects
  - Policies
    - Labels, rules, authorizations, and protected tables
- A database can have
  - One or *more* Policy
  - One or *more* Label

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Oracle Label Security Example

Project Data

Name	Budget	Status	Announce	Label
Drug A	$1.5M	Green	2/1/2019	HS:A:
Drug B	$4 M	Red	2/15/2019	HS:B:
Drug C	$.5 M	Red	4/1/2019	HS:C:
Drug D	$1.7 M	Yellow	11/1/2019	HS:D:
Drug E	$4 M	Yellow	8/1/2019	HS:E:



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

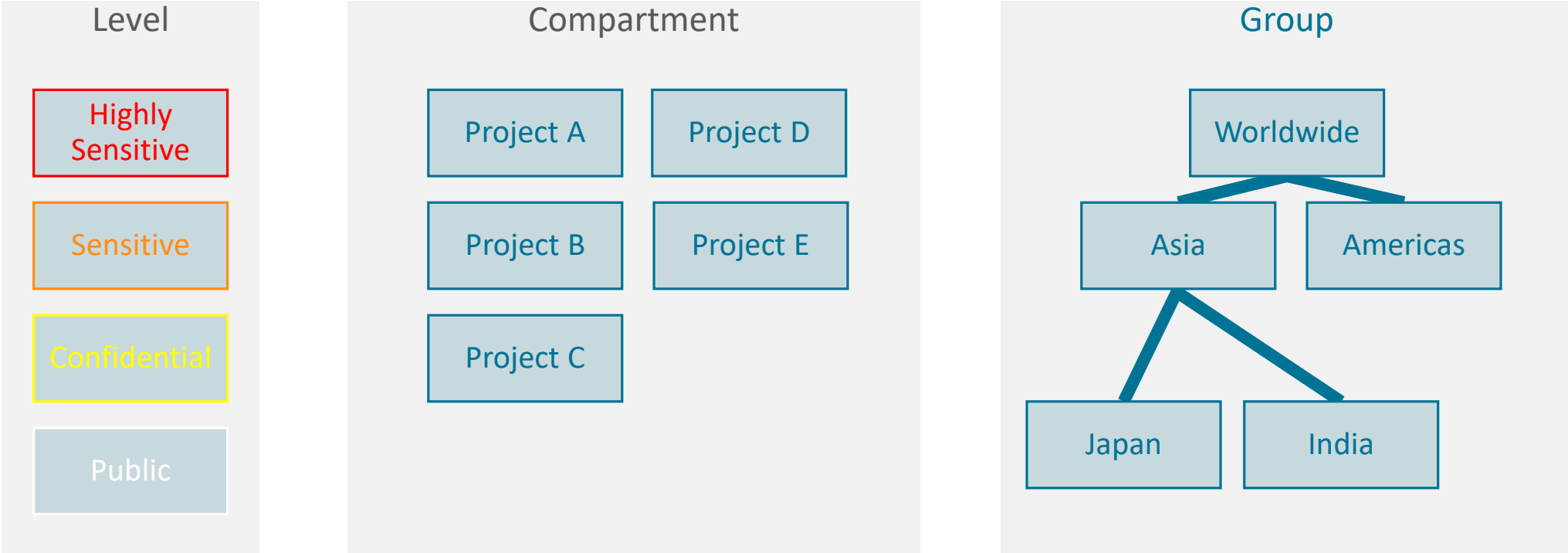
Oracle Label Security Example

Project Data				
Name	Budget	Status	Announce	Label
Drug A	$1.5M	Green	2/1/2019	HS:A:
Drug B	$4 M	Red	2/15/2019	HS:B:
Drug D	$1.7 M	Yellow	11/1/2019	HS:D:

OLS displays authorized data records only

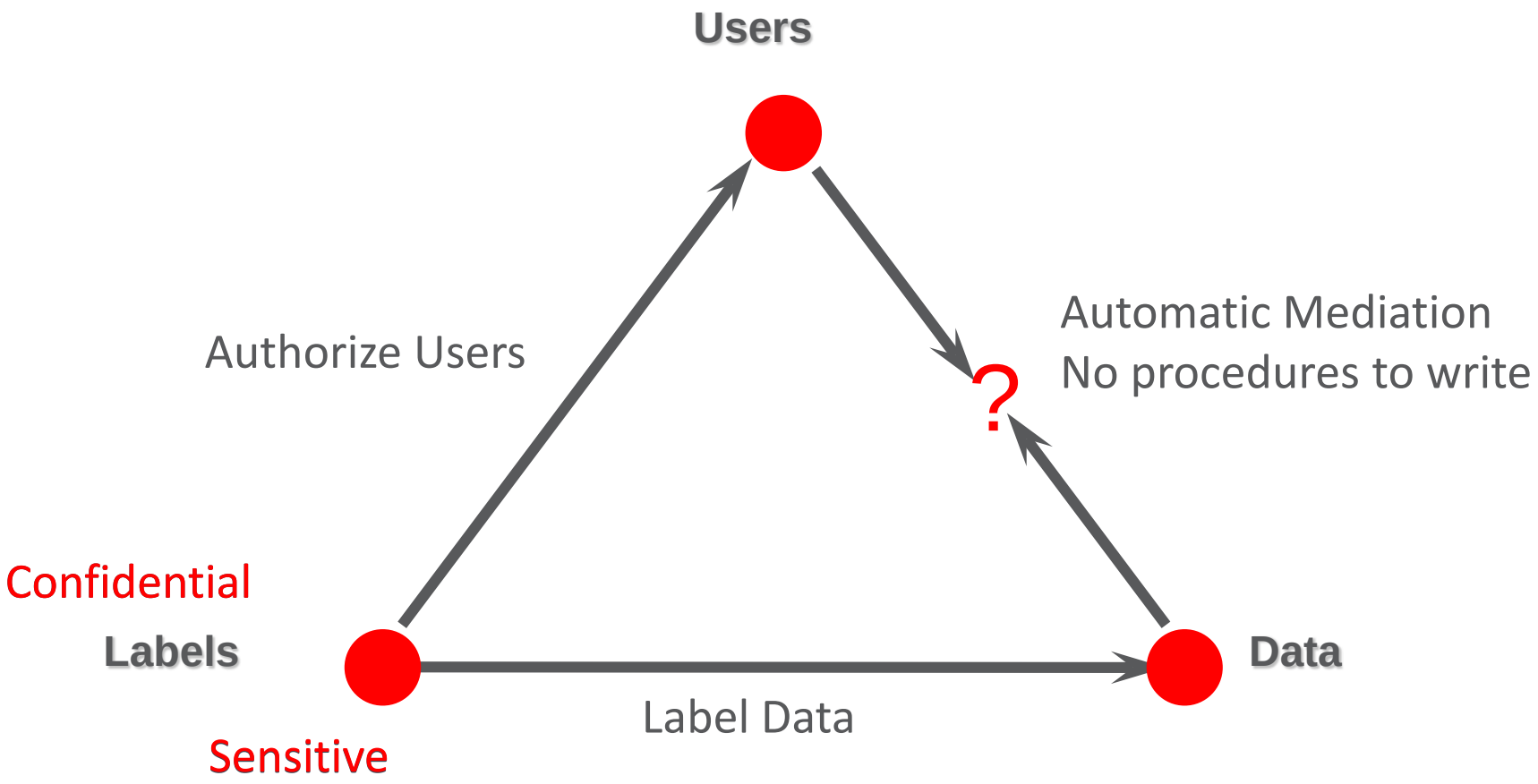
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Understanding a Label



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Controlling Access to Classified Data



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Use Case: GDPR and OLS

Opt-in consent	• Clear to user, no opt-out, use data only as agreed with user (owner)
Right to be forgotten	• Right to removal/erasure/corrected/to be forgotten—user can request this any time

- Labels to describe user data state
  - Marketable
  - Do Not Send
  - Request to Forget
  - Anonymized

- Marketing applications can only access rows labeled ‘Marketable’
- Anonymizer Procedure can only access rows marked ‘Request to Forget’
- Analysis tool can access all data except those that have been Requested to Forget but not yet anonymized

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle Public

Other OLS Use Cases

- Consolidating Retail Databases
- ISV Applications – Record Separated Customers
- Military/Intelligence

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Summary

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Technology Comparison

Technology	Features	When to use
VPD	• Programmatic	• Simple requirements • Data is part of record to filter
RAS	• Declarative • Application User, Roles, Privileges • Enterprise application features	• As part of new Java/APEX application development
OLS	• Declarative • Data and User Labels • Adjudication	• Application security model aligns with OLS • Sharing data across applications

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal

Q&A

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Safe Harbor Statement

The preceding 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 © 2018, Oracle and/or its affiliates. All rights reserved. |

Integrated Cloud

Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |


ORACLE®