IBM Software Group

IBM Optim Data Privacy and Guardium POT

Data Security and Compliance

An IBM Proof of Technology

Ken Lee

kklee@ca.ibm.com

Welcome to the Technical Exploration Center

- Introductions
- Access restrictions
- Restrooms
- Emergency Exits
- Smoking Policy
- Breakfast/Lunch/Snacks – location and times
- Special meal requirements?

Objectives

- To obtain a basic understanding of the regulatory issues surrounding managing data in corporate environments.
- Understanding the IBM® Optim™ Data Privacy and Guardium offerings and how they will help meet those regulatory issues.
- Understanding the IBM Optim Test Data Management offerings.
- IBM software solutions are reinforced with hands on labs to further demonstrate product capabilities.

Agenda

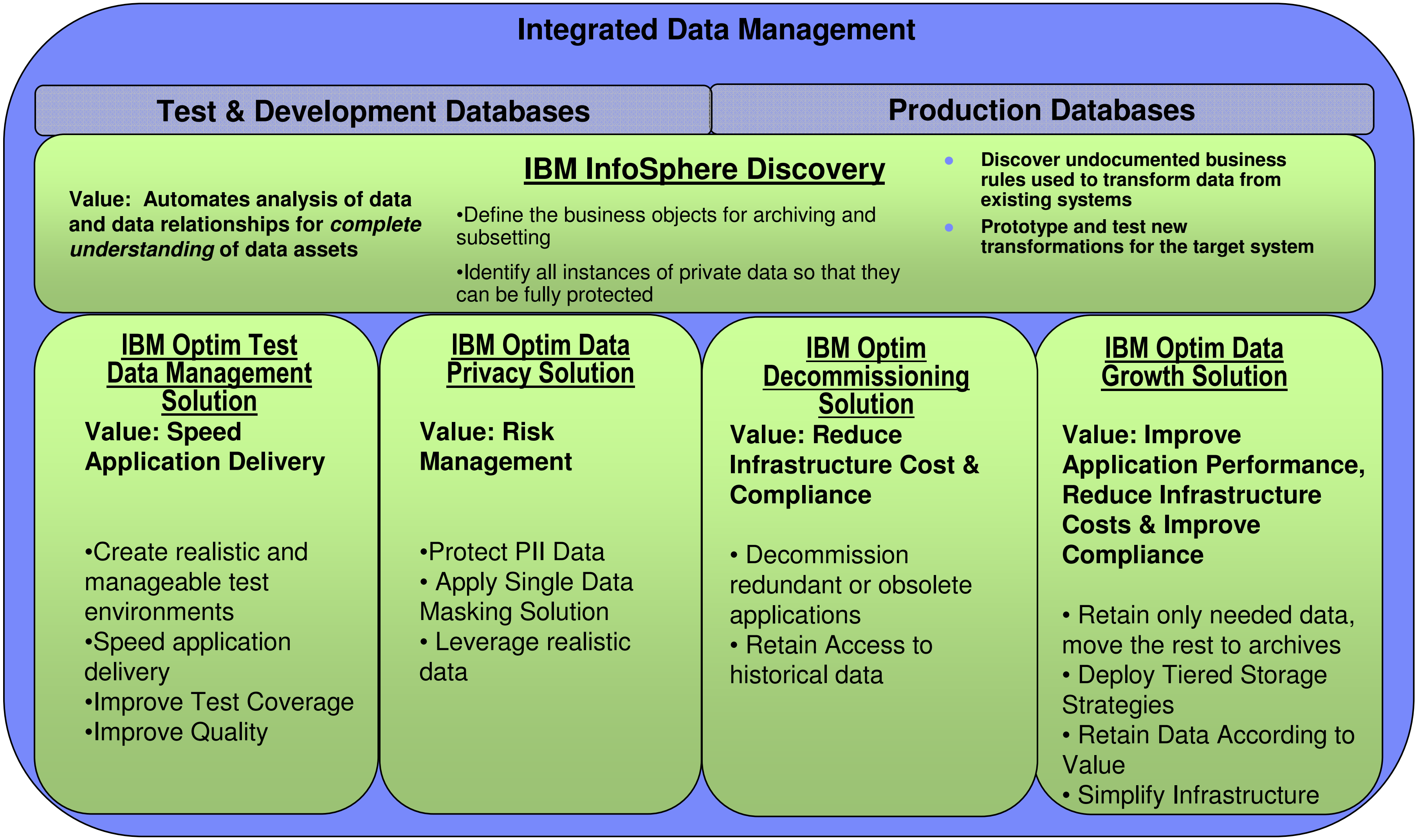
- MORNING
  - Introduction
  - IBM Optim Enterprise Data Management Overview
  - IBM Optim Test Data Management Overview
  - IBM Optim Data Privacy
  - Break
  - IBM Optim Test Data Management Lab
  - IBM Optim Data Privacy Lab
- LUNCH
- AFTERNOON
  - Guardium Overview
  - Break
  - Guardium Labs

IBM Software Group

IBM Optim High Level Overview

An IBM Proof of Technology

Optim is a Platform for Integrated Data Management



Integrated Data Management

Test & Development Databases

Production Databases

IBM InfoSphere Discovery

Value: Automates analysis of data and data relationships for *complete understanding* of data assets

- •Define the business objects for archiving and subsetting
- •Identify all instances of private data so that they can be fully protected

- **Discover undocumented business rules used to transform data from existing systems**
- **Prototype and test new transformations for the target system**

IBM Optim Test Data Management Solution

Value: Speed Application Delivery

- •Create realistic and manageable test environments
- •Speed application delivery
- •Improve Test Coverage
- •Improve Quality

IBM Optim Data Privacy Solution

Value: Risk Management

- •Protect PII Data
- • Apply Single Data Masking Solution
- • Leverage realistic data

IBM Optim Decommissioning Solution

Value: Reduce Infrastructure Cost & Compliance

- • Decommission redundant or obsolete applications
- • Retain Access to historical data

IBM Optim Data Growth Solution

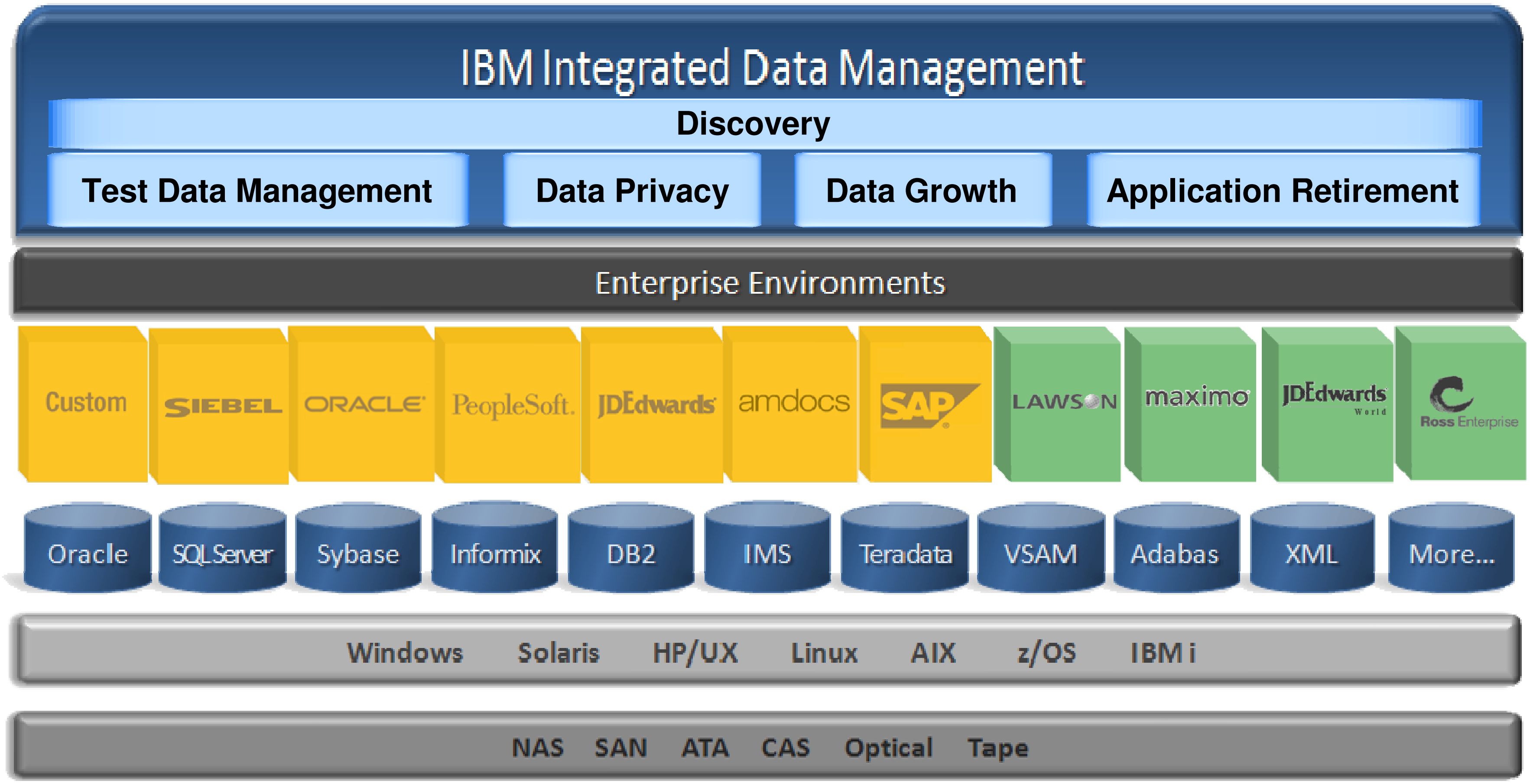
Value: Improve Application Performance, Reduce Infrastructure Costs & Improve Compliance

- • Retain only needed data, move the rest to archives
- • Deploy Tiered Storage Strategies
- • Retain Data According to Value
- • Simplify Infrastructure

Optim - Four Key Features

1. **Enterprise Architecture**
2. **Complete Business Object**
3. **Extract, Store, Restore & Dispose**
4. **Universal Access**

Enterprise Architecture



IBM Integrated Data Management

Discovery

Test Data Management | Data Privacy | Data Growth | Application Retirement

Enterprise Environments

Custom, SIEBEL, ORACLE, PeopleSoft, JDEdwards, amdocs, SAP, LAWSON, maximo, JDEdwards World, Ross Enterprise

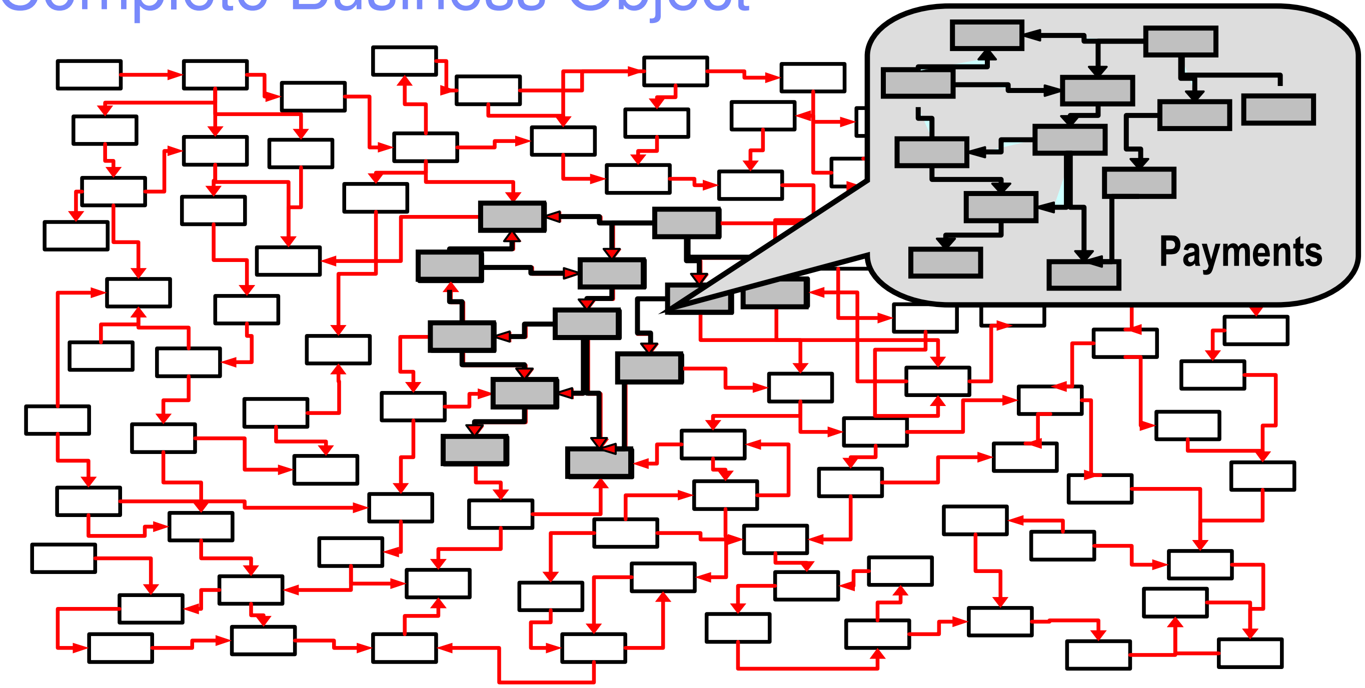
Oracle, SQLServer, Sybase, Informix, DB2, IMS, Teradata, VSAM, Adabas, XML, More…

Windows, Solaris, HP/UX, Linux, AIX, z/OS, IBM i

NAS, SAN, ATA, CAS, Optical, Tape

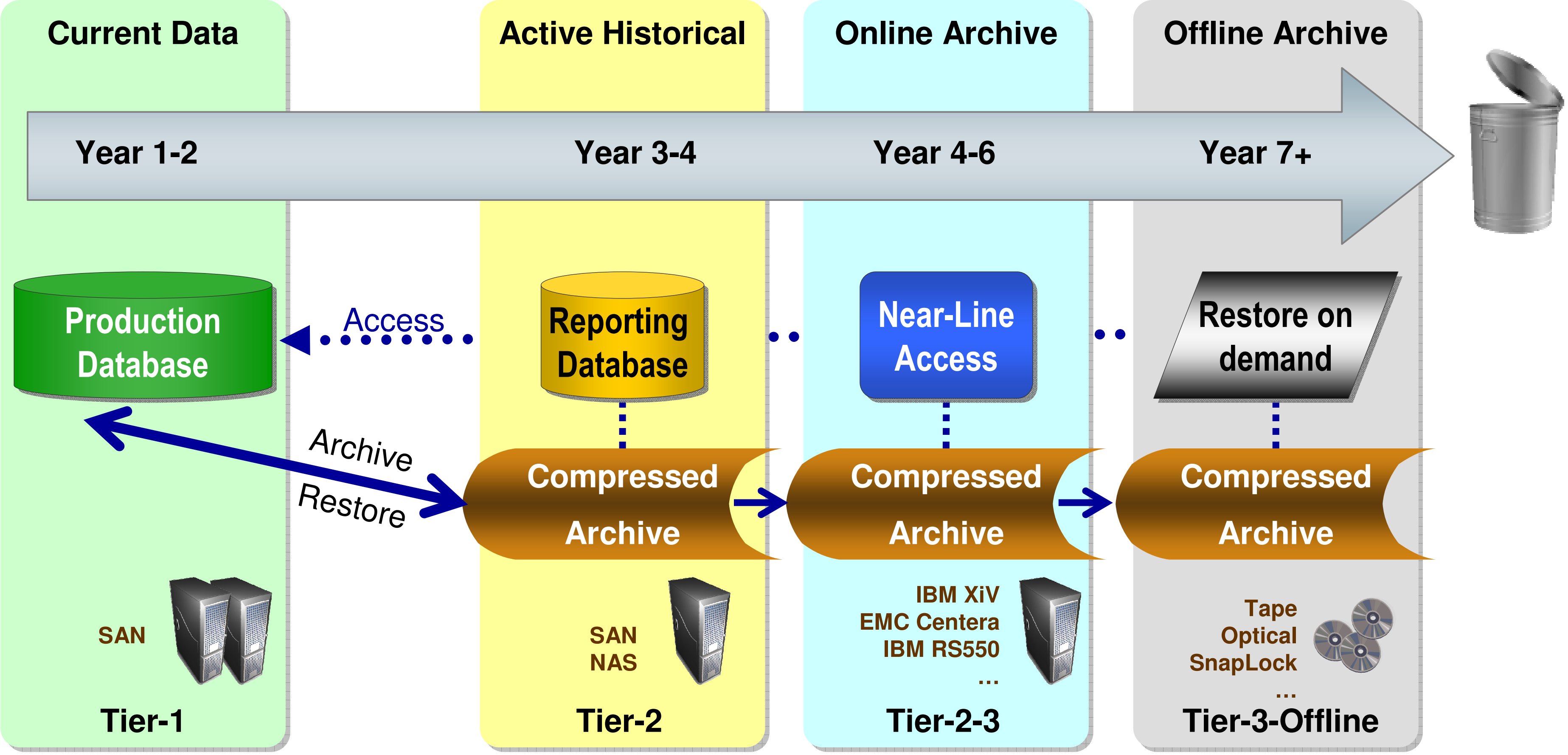
An <u>integrated</u>, <u>modular</u> environment to manage <u>enterprise application data</u> and optimize data-driven applications from requirements to retirement across <u>heterogeneous</u> environments.

Complete Business Object



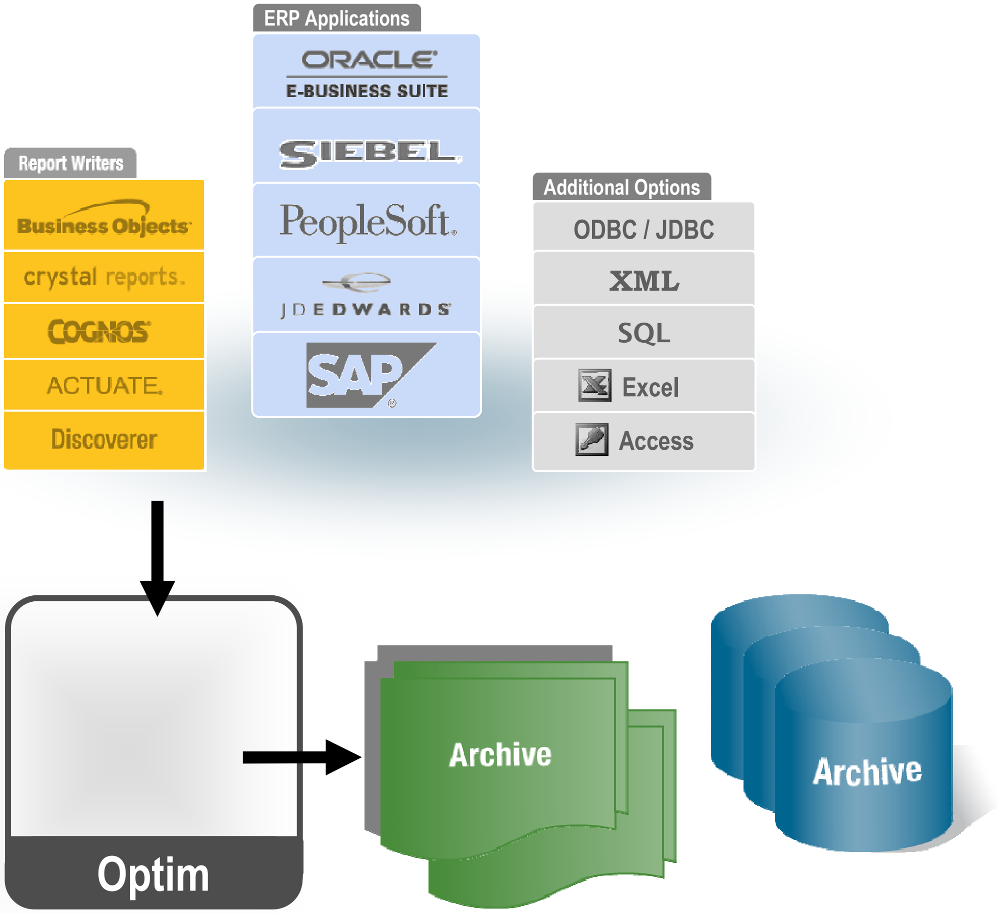
- Represents application data record – payment, invoice, customer
  - Referentially-intact subset of data across related tables and applications; includes metadata
- Provides “historical reference snapshot” of business activity
- Federated object support across enterprise data stores

Extract, Store & Manage Archived Data Across any Platform



Compression: 70%-95%

4 Universal Access



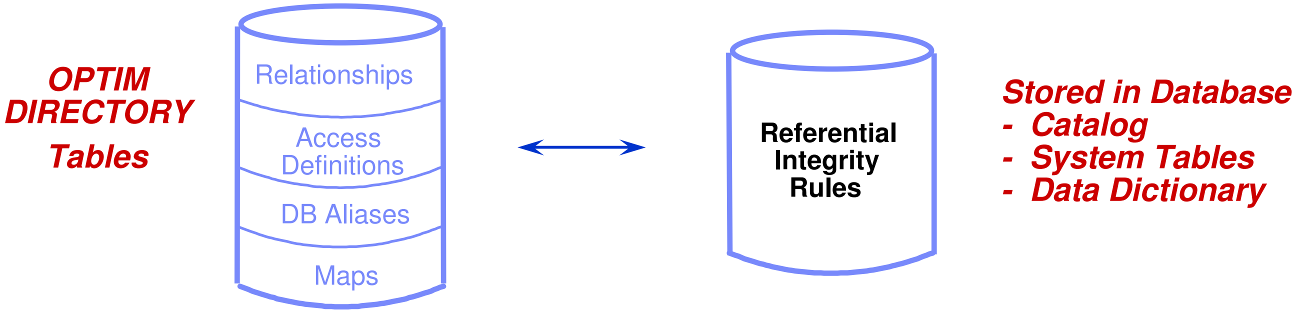
- Native application access
  - Familiar screens and processes
- Application independent access
  - Industry standard methods: SQL, ODBC/JDBC, XML
  - Portals
  - Report writers: Crystal Reports, Cognos, Business Objects, Discoverer, Actuate
  - Desktop formats: Excel, CSV, MS Access
  - Database formats

Access Any Record, Anytime, Anywhere!

Terminology

- **Optim Directory**
- **Database Aliases**
- **Relationships (Native, Imported and Extended)**
- **Access Definitions**
- **Table Maps**
- **Column Maps**
- **Move**
  - Extract
  - Insert/Load
- **Edit**
- **Compare**

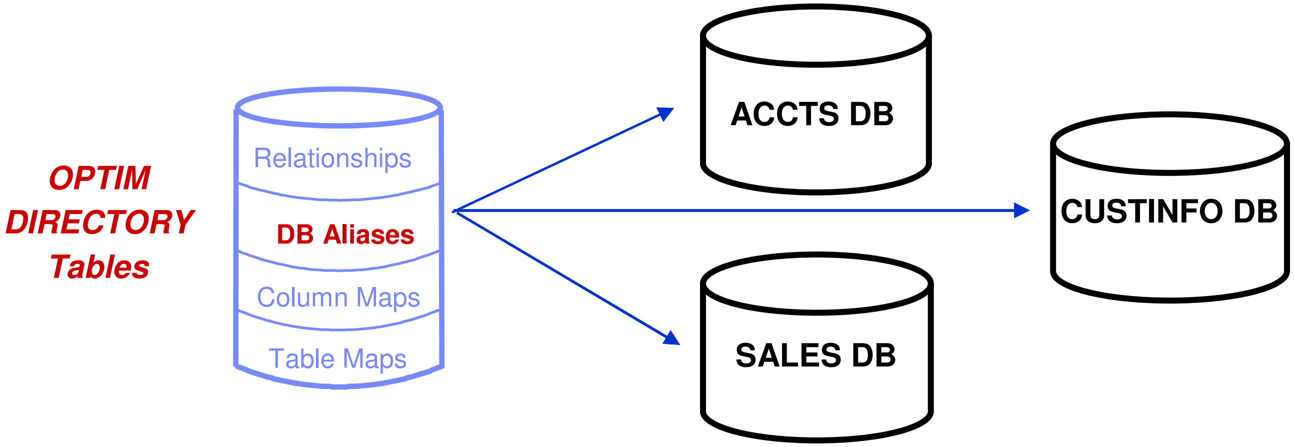
The OPTIM Directory



- Optim catalog
  - Supplements information stored in the database (DB)
  - Maintains product definitions and tracks processing
  - Stores database connection information (DB Aliases)
  - Stores user-defined relationships

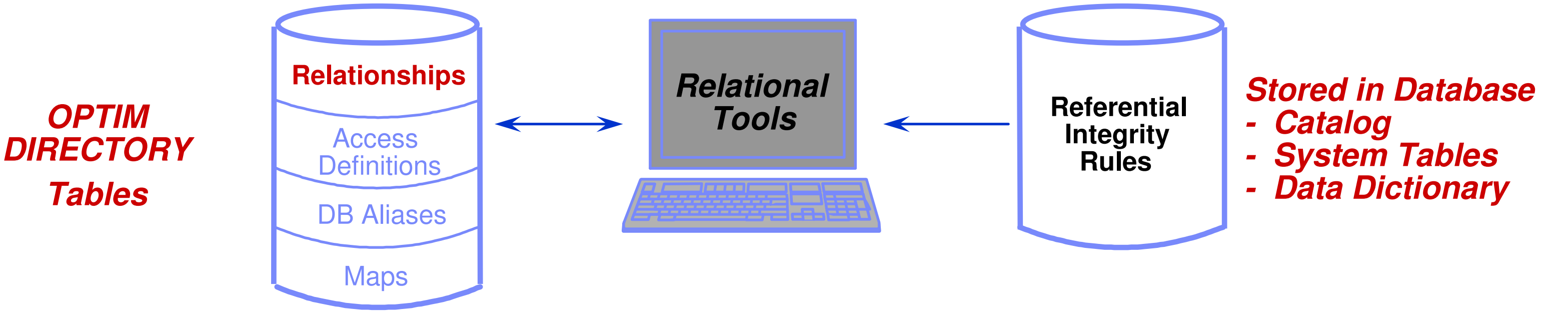
Database Alias

Establishing the Database Connection



- Optim view of a database connection
  - High-level qualifier for database object names
    - DBalias.creatorid.objectname
  - Enables cross-Database access
  - Saved in Optim Directory

Relationships



- **Automatically derived from database RI rules**
- **OR… defined within OPTIM**
- **OR… imported from DDL**

Shared by all OPTIM components

Extended Relationships

Sales Table

SALESMAN_ID Char (5)	MANAGER_ID Char (7)
(NC)003	NC00123
NW012	NW00564
SC005	SC00234
SE012	SE00582

District Table

DISTRICT_CD Char (2)	MANAGER_NO Char (5)
NC	00123
SC	00564
SE	00234
NW	00582

Example 1
Using Substr Function

Parent Table Sales

Substr(SALESMAN_ID,1,2)

Child Table ***District***

DISTRICT_CD

Example 2
Using Concat Function

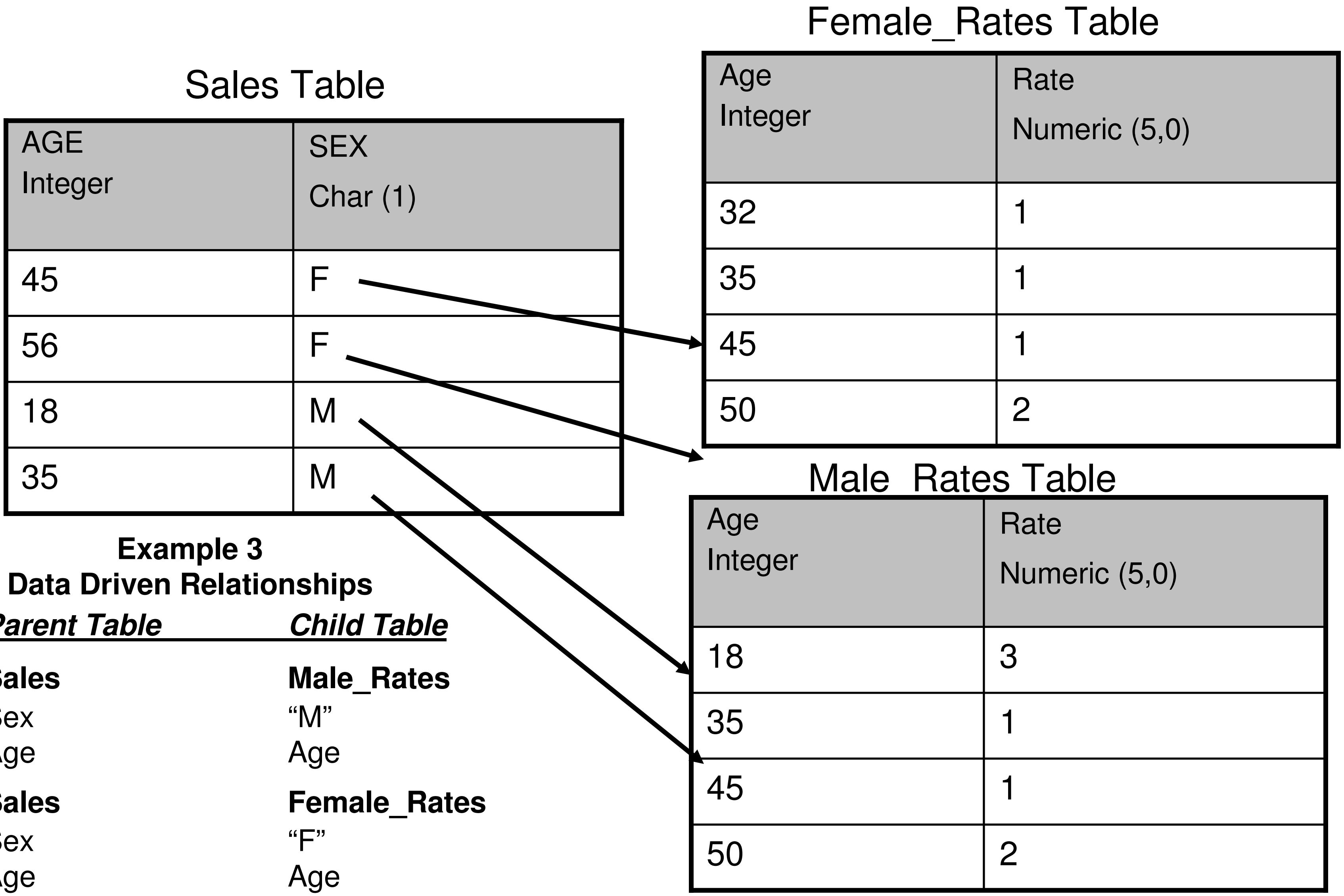
Parent Table **Sales**

MANAGER_ID

Child Table **District**

DISTRICT_CD || MANAGER_ID

Extended Relationships



Sales Table

AGE Integer	SEX Char (1)
45	F
56	F
18	M
35	M

Female_Rates Table

Age Integer	Rate Numeric (5,0)
32	1
35	1
45	1
50	2

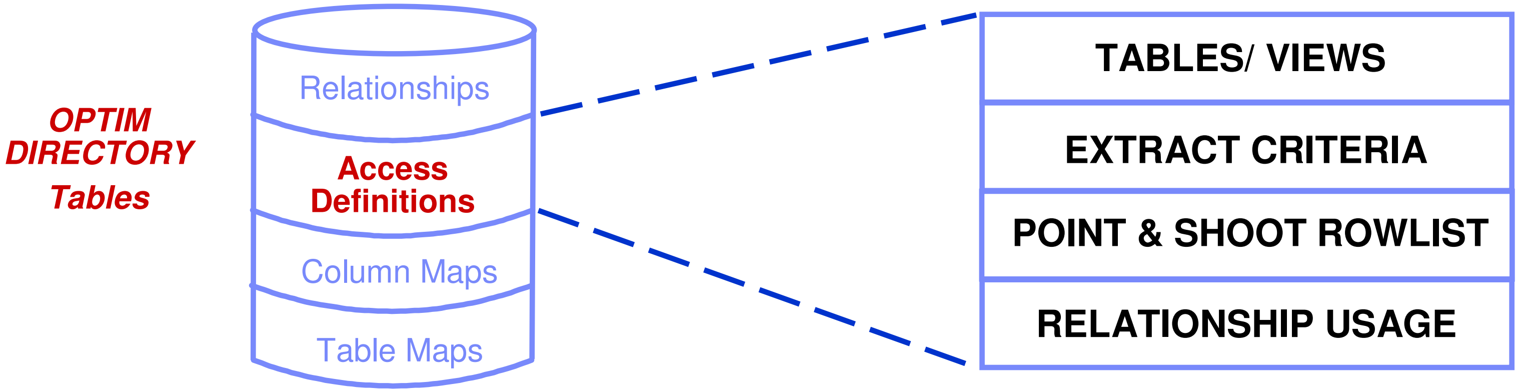
Male_Rates Table

Age Integer	Rate Numeric (5,0)
18	3
35	1
45	1
50	2

Example 3
Data Driven Relationships

Parent Table	***Child Table***
Sales	**Male_Rates**
Sex	“M”
Age	Age
Sales	**Female_Rates**
Sex	“F”
Age	Age

The Access Definition



OPTIM DIRECTORY Tables

Relationships

Access Definitions

Column Maps

Table Maps

TABLES/ VIEWS

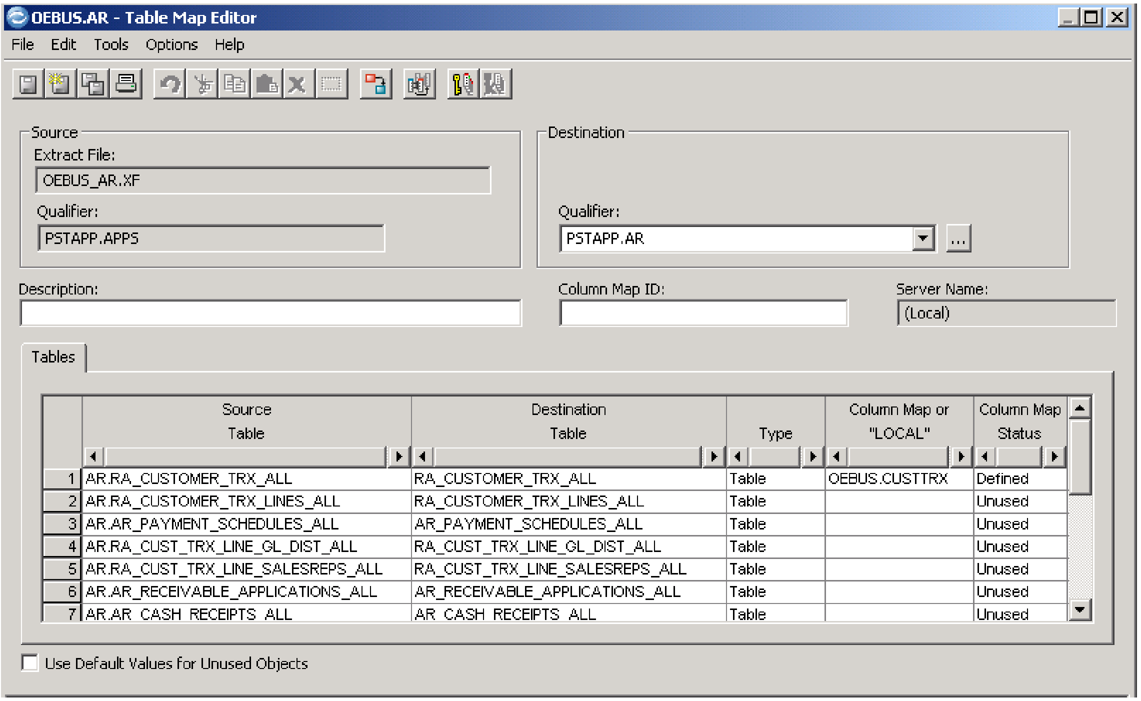
EXTRACT CRITERIA

POINT & SHOOT ROWLIST

RELATIONSHIP USAGE

- **Created dynamically during archive definition**
- **Use to re-create archive batch job when changes are needed**

Table Map



Source

Extract File: OEBUS_AR.XF

Qualifier: PSTAPP.APPS

Destination

Qualifier: PSTAPP.AR

Description:

Column Map ID:

Server Name: (Local)

Tables

	Source Table	Destination Table	Type	Column Map or "LOCAL"	Column Map Status
1	AR.RA_CUSTOMER_TRX_ALL	RA_CUSTOMER_TRX_ALL	Table	OEBUS.CUSTTRX	Defined
2	AR.RA_CUSTOMER_TRX_LINES_ALL	RA_CUSTOMER_TRX_LINES_ALL	Table		Unused
3	AR.AR_PAYMENT_SCHEDULES_ALL	AR_PAYMENT_SCHEDULES_ALL	Table		Unused
4	AR.RA_CUST_TRX_LINE_GL_DIST_ALL	RA_CUST_TRX_LINE_GL_DIST_ALL	Table		Unused
5	AR.RA_CUST_TRX_LINE_SALESREPS_ALL	RA_CUST_TRX_LINE_SALESREPS_ALL	Table		Unused
6	AR.AR_RECEIVABLE_APPLICATIONS_ALL	AR_RECEIVABLE_APPLICATIONS_ALL	Table		Unused
7	AR.AR_CASH_RECEIPTS_ALL	AR_CASH_RECEIPTS_ALL	Table		Unused

□ Use Default Values for Unused Objects

- **Map unlike table names, qualifiers**
- **Exclude individual tables from restore**
- **Can be saved in Optim Directory**

Column Map

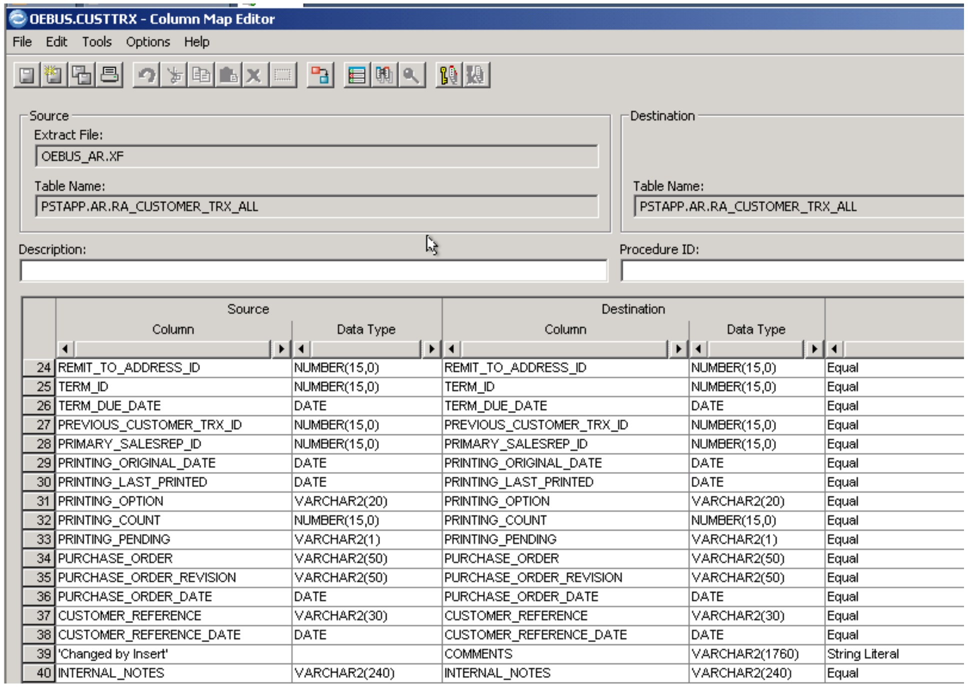
Literals

Special Registers

Expressions

Default Values

User exits



Source

Extract File: OEBUS_AR.XF

Table Name: PSTAPP.AR.RA_CUSTOMER_TRX_ALL

Destination

Table Name: PSTAPP.AR.RA_CUSTOMER_TRX_ALL

Description:

Procedure ID:

	Source		Destination		
	Column	Data Type	Column	Data Type	
24	REMIT_TO_ADDRESS_ID	NUMBER(15,0)	REMIT_TO_ADDRESS_ID	NUMBER(15,0)	Equal
25	TERM_ID	NUMBER(15,0)	TERM_ID	NUMBER(15,0)	Equal
26	TERM_DUE_DATE	DATE	TERM_DUE_DATE	DATE	Equal
27	PREVIOUS_CUSTOMER_TRX_ID	NUMBER(15,0)	PREVIOUS_CUSTOMER_TRX_ID	NUMBER(15,0)	Equal
28	PRIMARY_SALESREP_ID	NUMBER(15,0)	PRIMARY_SALESREP_ID	NUMBER(15,0)	Equal
29	PRINTING_ORIGINAL_DATE	DATE	PRINTING_ORIGINAL_DATE	DATE	Equal
30	PRINTING_LAST_PRINTED	DATE	PRINTING_LAST_PRINTED	DATE	Equal
31	PRINTING_OPTION	VARCHAR2(20)	PRINTING_OPTION	VARCHAR2(20)	Equal
32	PRINTING_COUNT	NUMBER(15,0)	PRINTING_COUNT	NUMBER(15,0)	Equal
33	PRINTING_PENDING	VARCHAR2(1)	PRINTING_PENDING	VARCHAR2(1)	Equal
34	PURCHASE_ORDER	VARCHAR2(50)	PURCHASE_ORDER	VARCHAR2(50)	Equal
35	PURCHASE_ORDER_REVISION	VARCHAR2(50)	PURCHASE_ORDER_REVISION	VARCHAR2(50)	Equal
36	PURCHASE_ORDER_DATE	DATE	PURCHASE_ORDER_DATE	DATE	Equal
37	CUSTOMER_REFERENCE	VARCHAR2(30)	CUSTOMER_REFERENCE	VARCHAR2(30)	Equal
38	CUSTOMER_REFERENCE_DATE	DATE	CUSTOMER_REFERENCE_DATE	DATE	Equal
39	'Changed by Insert'		COMMENTS	VARCHAR2(1760)	String Literal
40	INTERNAL_NOTES	VARCHAR2(240)	INTERNAL_NOTES	VARCHAR2(240)	Equal

- **Map unlike column names**
- **Datatype conversions**
- **Populate new destination columns**

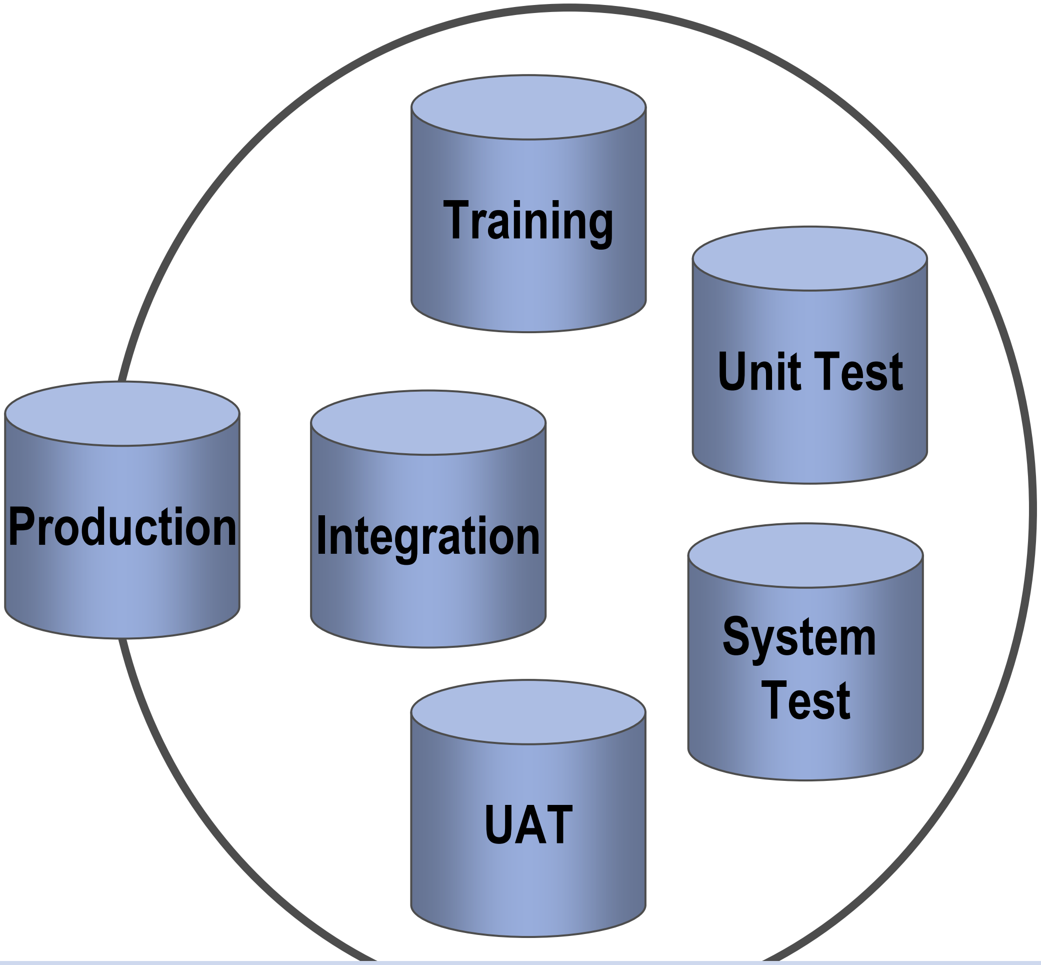
IBM Optim
Test Data Management

An IBM Proof of Technology

The Symptoms of Poor Testing Strategies

- Management notices that new application functionality is delayed three months
- The business is unable to compete for customers because their software lacks “state-of-the-art” functionality
- The CFO is complaining over how high the IT budget has become to fix application defects
- Developers are sitting around waiting for their copy of the database to work with

How Does Test Data Management Impact Cost?

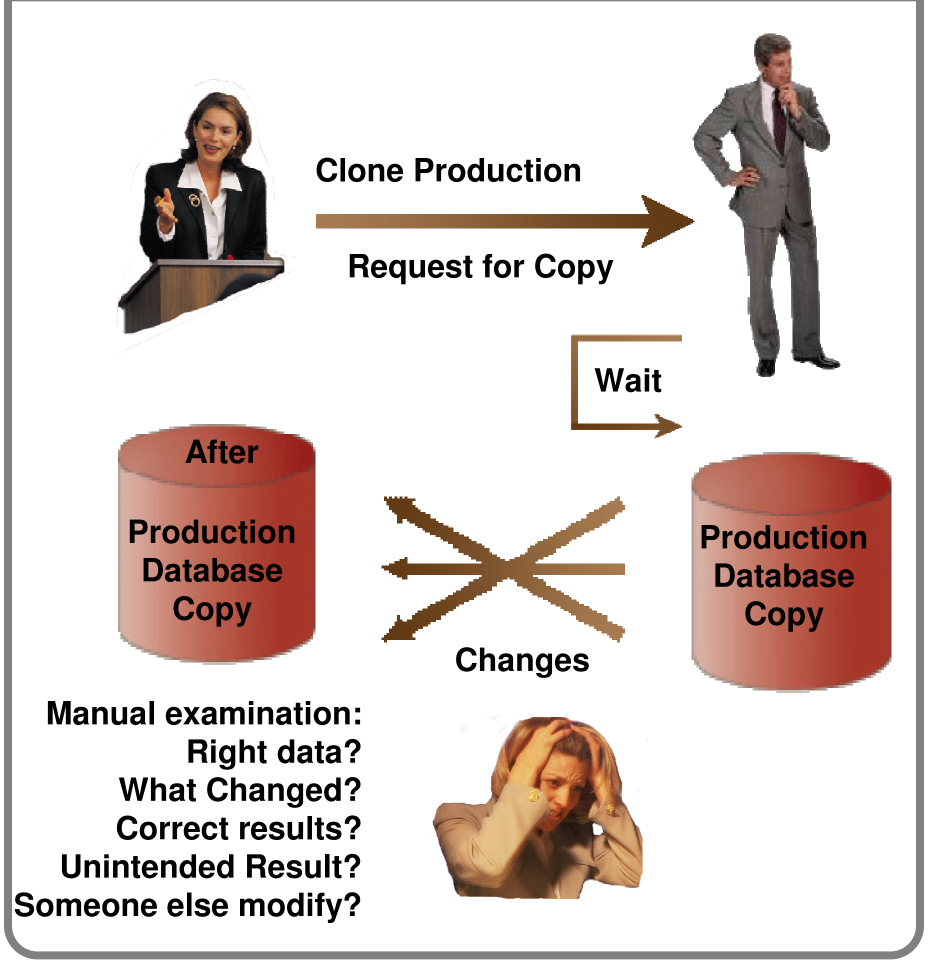


Production	500GB
Training	500GB
Unit Test	500GB
System Test	500GB
UAT	500GB
Integration	500GB
Total	3 TB

Creating right-sized targeted test environments saves storage costs & speeds testing

Some Current Practices

#1 - Clone Production



Clone Production

Request for Copy

Wait

After

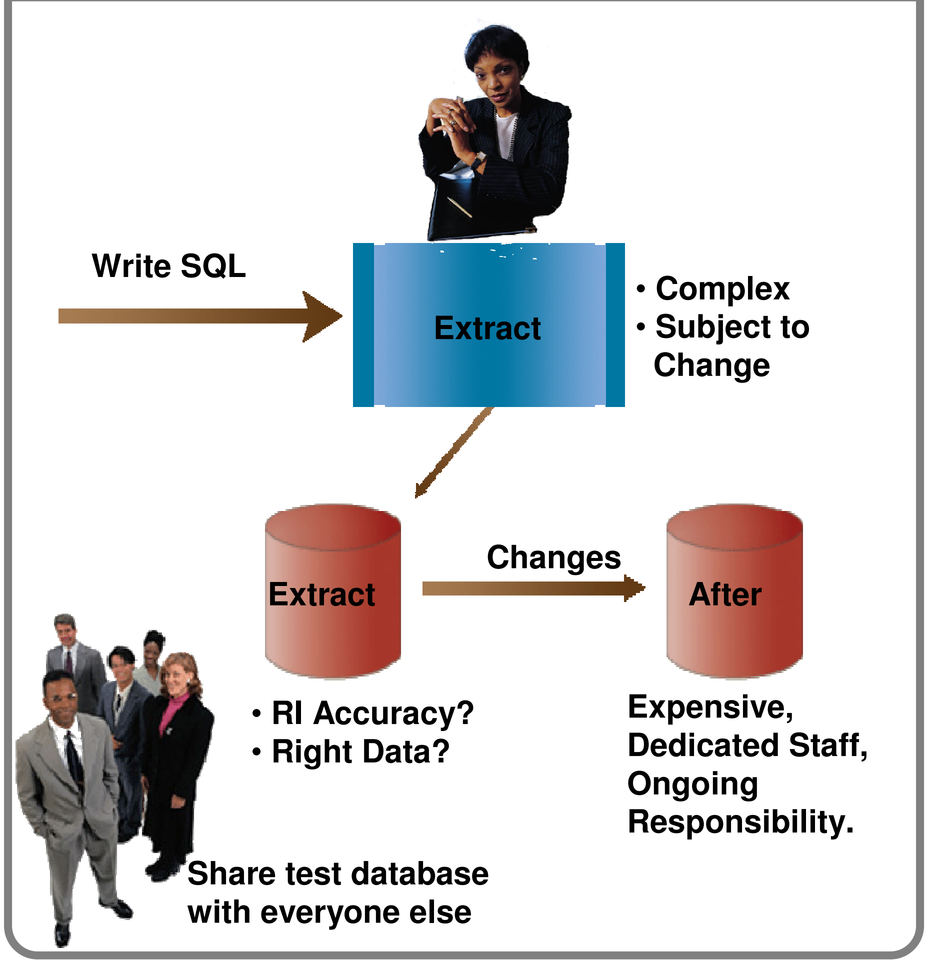
Production Database Copy

Changes

Production Database Copy

Manual examination:
Right data?
What Changed?
Correct results?
Unintended Result?
Someone else modify?

#2 – Write SQL



Write SQL

Extract

- Complex
- Subject to Change

Extract

Changes

After

- RI Accuracy?
- Right Data?

Expensive, Dedicated Staff, Ongoing Responsibility.

Share test database with everyone else

Test Data Management – Concepts

Test Data Management (TDM) refers to the need to manage data used in various pre- production environments and is a vital part of Application Quality & Delivery

Extract production data into referentially intact data subsets to be used to support application data in other environments

De-identify (mask) extracted production data to protect privacy

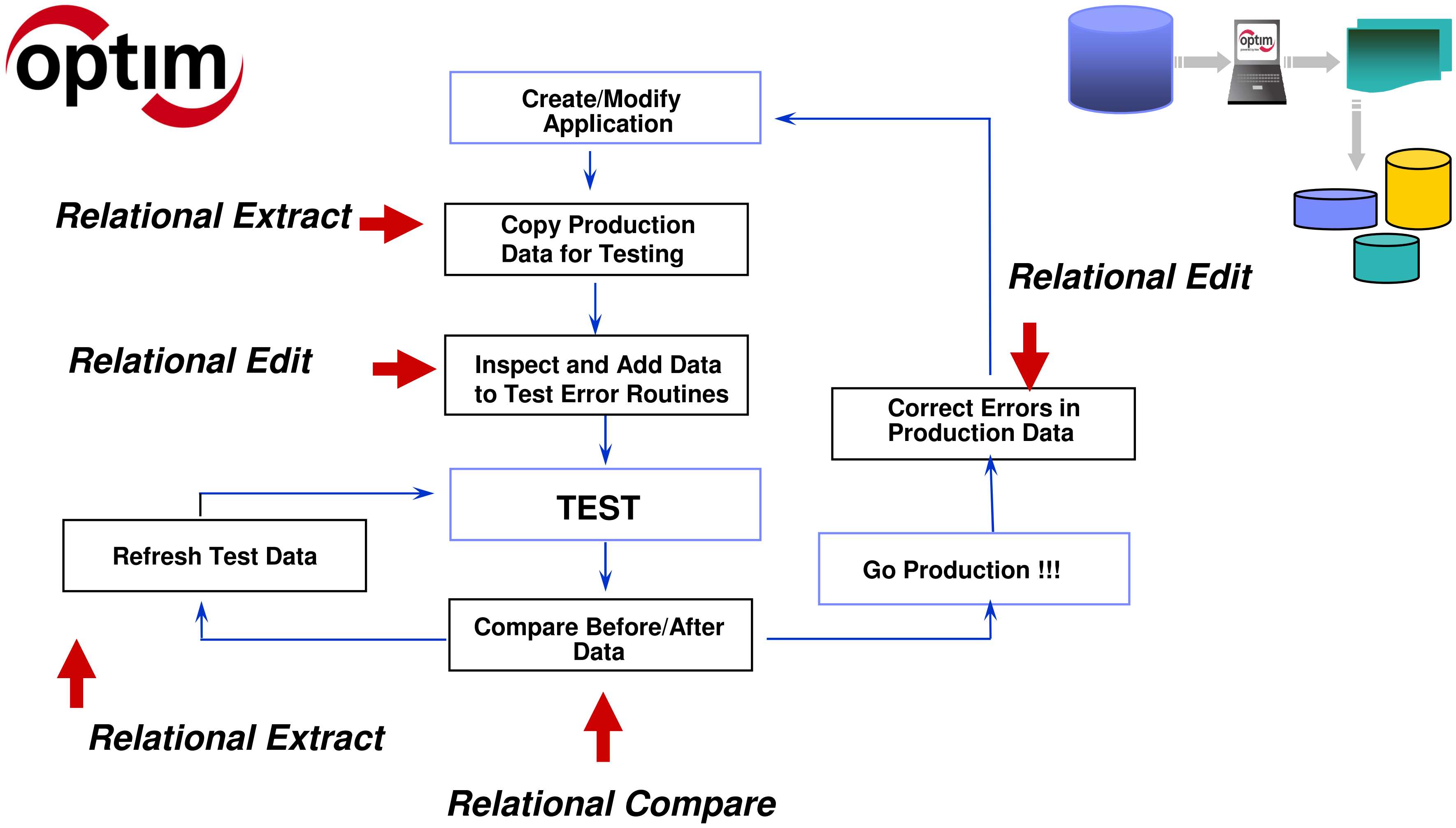
Compare “before” and “after” images of test data

Speed application quality and delivery

Key Requirements for a Test Data Management Solution

1. Subset capabilities to create realistic and manageable test databases
2. Easily refresh test environments
3. Edit data to create targeted test cases
4. Compare ‘before’ and ‘after’ images of the test data
5. De-identify (mask) data to protect privacy

Product Overview : Optim Test Data Management



optim

Create/Modify Application

Relational Extract

Copy Production Data for Testing

Relational Edit

Inspect and Add Data to Test Error Routines

TEST

Refresh Test Data

Compare Before/After Data

Relational Extract

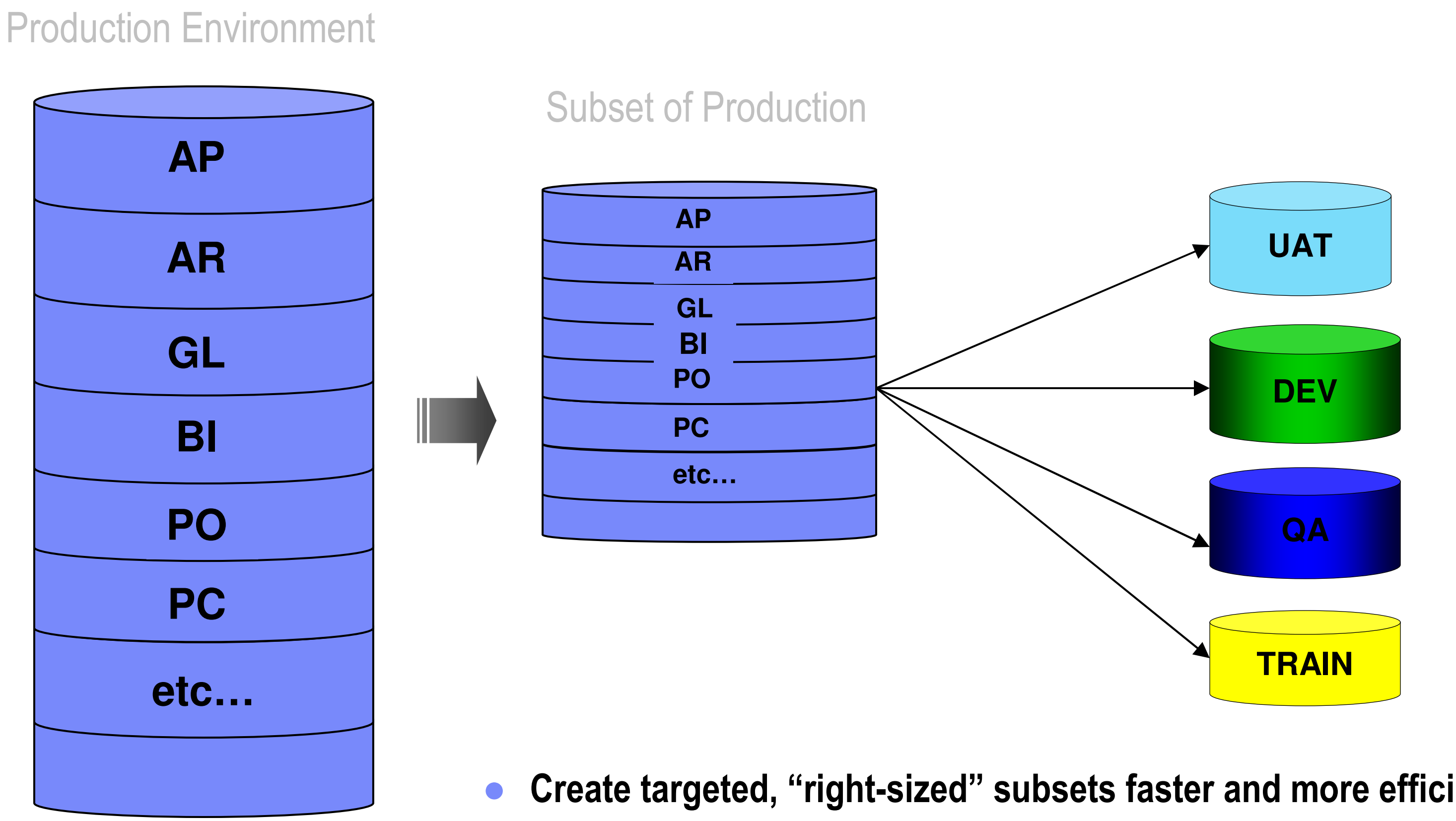
Relational Compare

Relational Edit

Correct Errors in Production Data

Go Production !!!

Optim Test Data Management using Optim Subsetting:



- Create targeted, “right-sized” subsets faster and more efficiently than cloning
- Compare to pinpoint and resolve application defects faster
- Improve development efficiencies

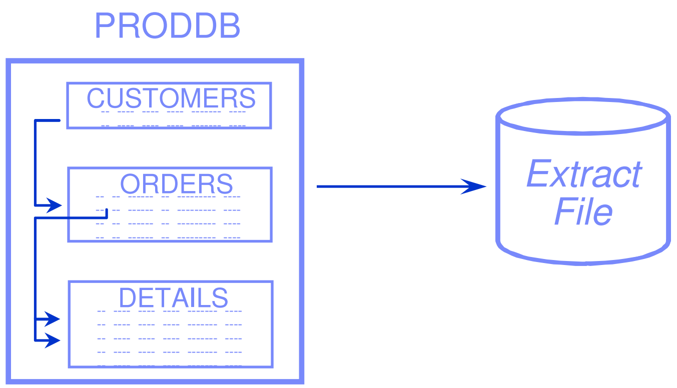
Defining the Extract…..

Tables

Views

Synonyms

Aliases



Required:

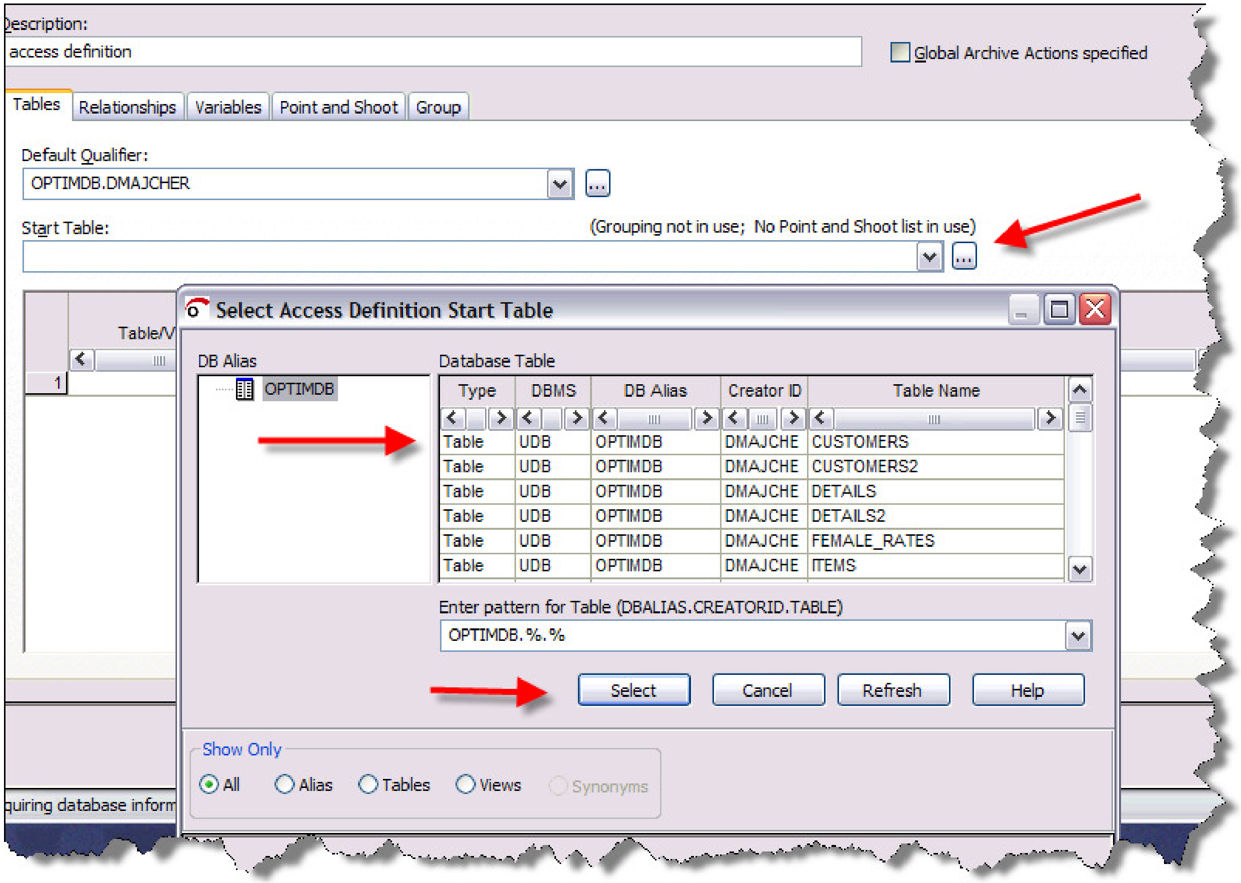
- **Start Table**
- **Set of Tables**

Optional:

- Selection Criteria
- Data Sampling
- Data Grouping
- Point and Shoot
- Relationship Usage

Extract Process

- Identify the Start Table
- Choose from a list or type in a known table name



Description:
access definition

□ Global Archive Actions specified

Default Qualifier: OPTIMDB.DMAJCHER

Start Table:

(Grouping not in use; No Point and Shoot list in use)

Select Access Definition Start Table

DB Alias: OPTIMDB

Database Table

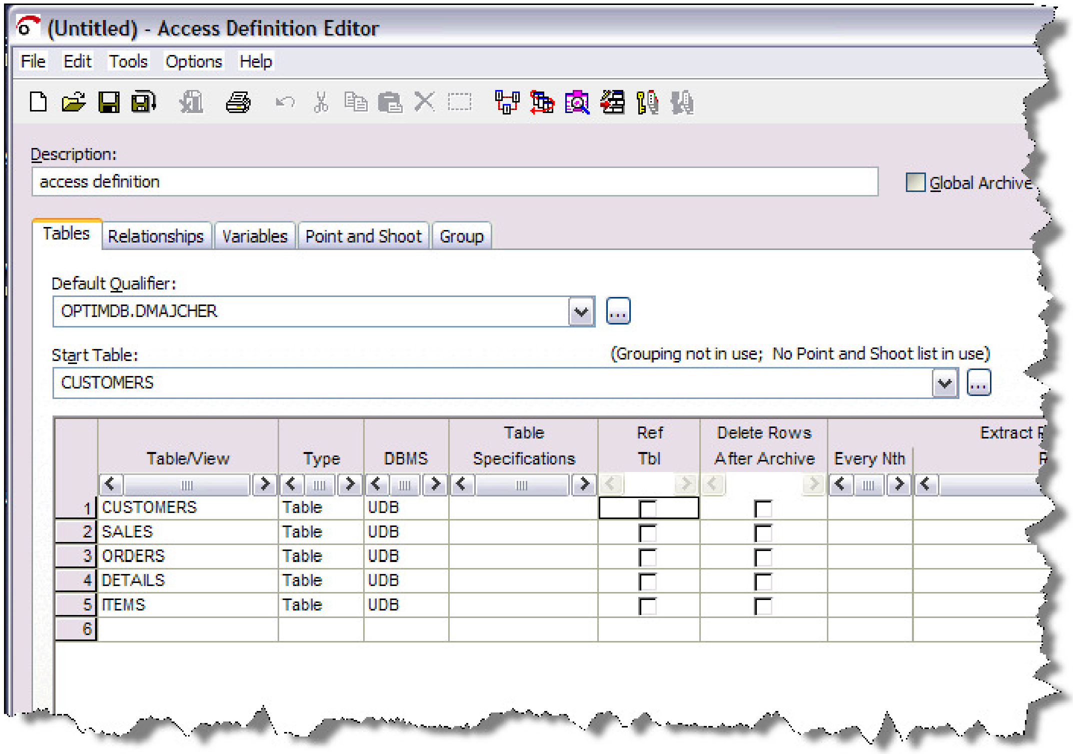
Type	DBMS	DB Alias	Creator ID	Table Name
Table	UDB	OPTIMDB	DMAJCHE	CUSTOMERS
Table	UDB	OPTIMDB	DMAJCHE	CUSTOMERS2
Table	UDB	OPTIMDB	DMAJCHE	DETAILS
Table	UDB	OPTIMDB	DMAJCHE	DETAILS2
Table	UDB	OPTIMDB	DMAJCHE	FEMALE_RATES
Table	UDB	OPTIMDB	DMAJCHE	ITEMS

Enter pattern for Table (DBALIAS.CREATORID.TABLE)
OPTIMDB.%.%

Show Only
● All ○ Alias ○ Tables ○ Views ○ Synonyms

Extract Process

Defining the Access Definition



(Untitled) - Access Definition Editor
File Edit Tools Options Help
Tables Relationships Variables Point and Shoot Group

Description: access definition

☐ Global Archive

Default Qualifier: OPTIMDB.DMAJCHER

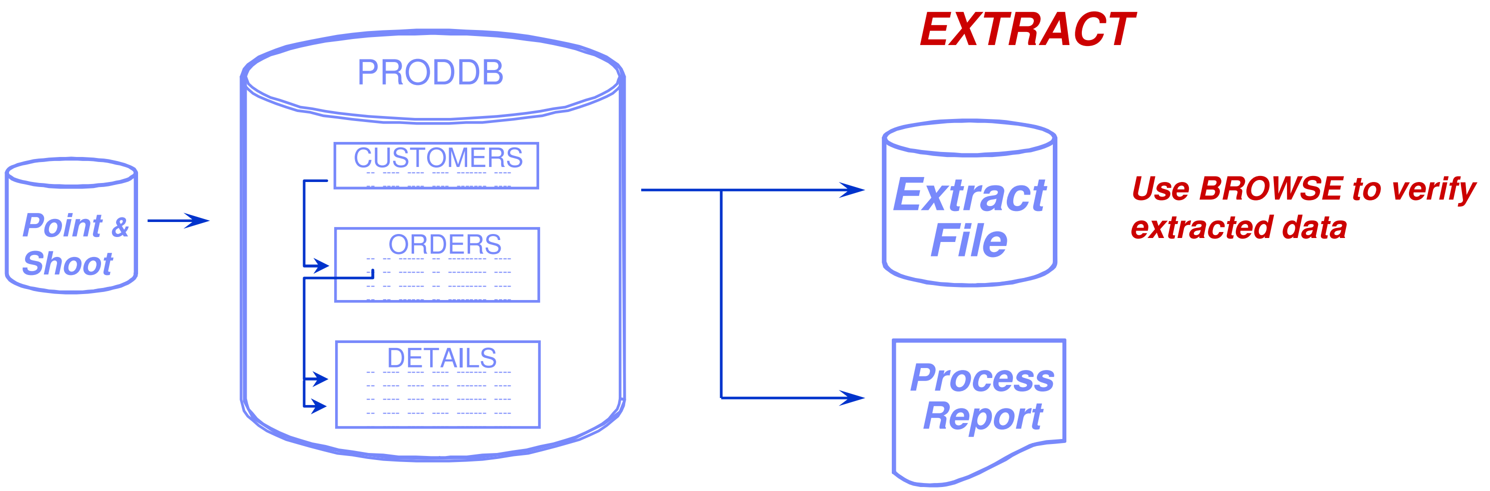
Start Table: CUSTOMERS

(Grouping not in use; No Point and Shoot list in use)

	Table/View	Type	DBMS	Table Specifications	Ref Tbl	Delete Rows After Archive	Every Nth	Extract R
1	CUSTOMERS	Table	UDB		☐	☐		
2	SALES	Table	UDB		☐	☐		
3	ORDERS	Table	UDB		☐	☐		
4	DETAILS	Table	UDB		☐	☐		
5	ITEMS	Table	UDB		☐	☐		
6								

- Include random selection factor, extract limits and selection criteria
- Use the RELATED functions to populate list with other tables

Extract Process



- Extract from source tables
  - using dynamic SQL
- Extract data and/or object definitions

Browse Extract file

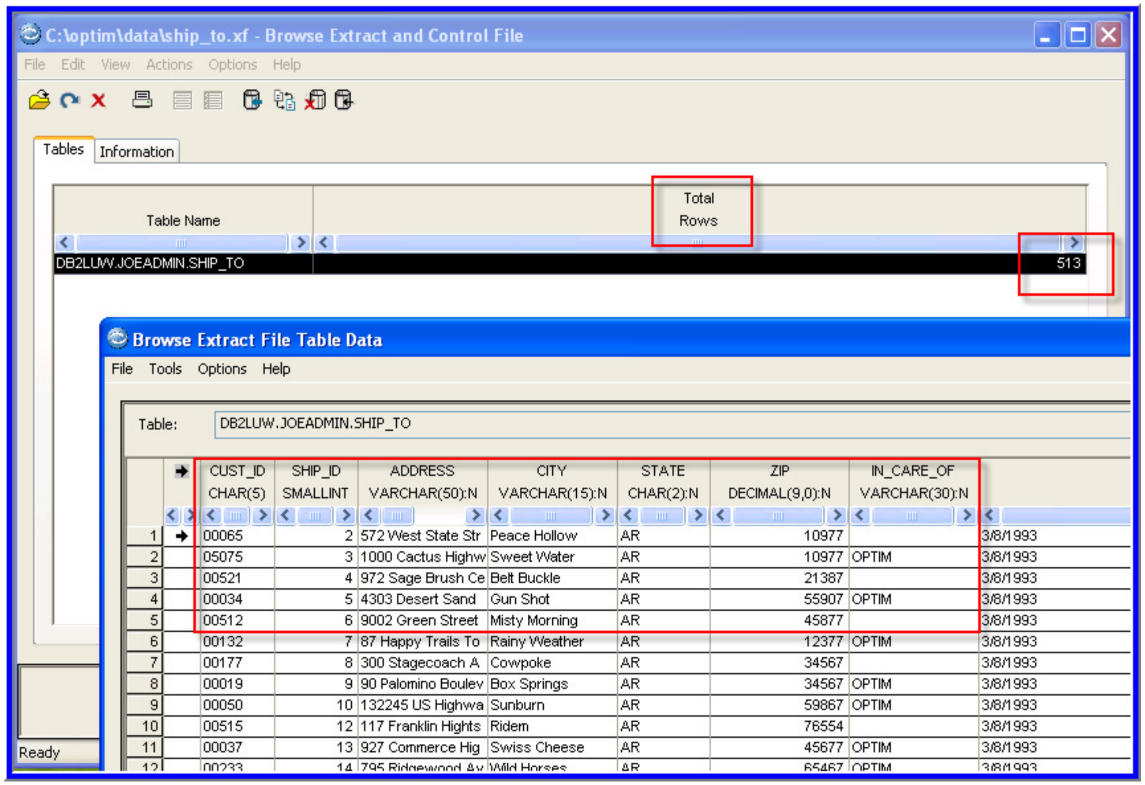

C:\optim\data\ship_to.xf - Browse Extract and Control File
File Edit View Actions Options Help
Tables
Information
Browse Extract File Table Data
File Tools Options Help
Ready

Table Name	Total Rows
DB2LUW.JOEADMIN.SHIP_TO	513

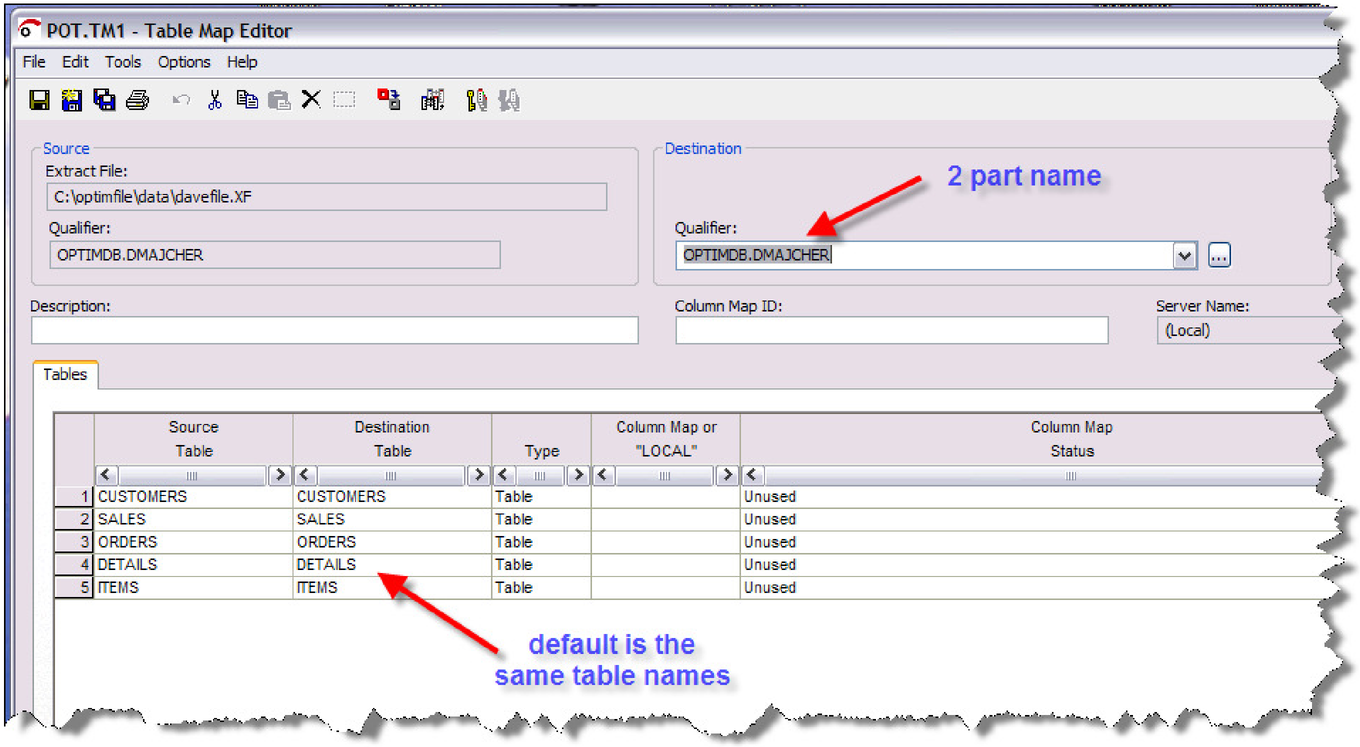
Table: DB2LUW.JOEADMIN.SHIP_TO

	CUST_ID CHAR(5)	SHIP_ID SMALLINT	ADDRESS VARCHAR(50):N	CITY VARCHAR(15):N	STATE CHAR(2):N	ZIP DECIMAL(9,0):N	IN_CARE_OF VARCHAR(30):N	
1	00065	2	572 West State Str	Peace Hollow	AR	10977		3/8/1993
2	05075	3	1000 Cactus Highw	Sweet Water	AR	10977	OPTIM	3/8/1993
3	00521	4	972 Sage Brush Ce	Belt Buckle	AR	21387		3/8/1993
4	00034	5	4303 Desert Sand	Gun Shot	AR	55907	OPTIM	3/8/1993
5	00512	6	9002 Green Street	Misty Morning	AR	45877		3/8/1993
6	00132	7	87 Happy Trails To	Rainy Weather	AR	12377	OPTIM	3/8/1993
7	00177	8	300 Stagecoach A	Cowpoke	AR	34567		3/8/1993
8	00019	9	90 Palomino Boulev	Box Springs	AR	34567	OPTIM	3/8/1993
9	00050	10	132245 US Highwa	Sunburn	AR	59867	OPTIM	3/8/1993
10	00515	12	117 Franklin Hights	Ridem	AR	76554		3/8/1993
11	00037	13	927 Commerce Hig	Swiss Cheese	AR	45677	OPTIM	3/8/1993
12	00233	14	795 Ridgewood Av	Wild Horses	AR	65467	OPTIM	3/8/1993

- Extract from source tables
  - using dynamic SQL
- Extract data and/or object definitions

Populate Destination Tables

- Table Map
  - Table names need not match
  - Change qualifier and/or table name
  - Can be saved in PST Directory



Source
Extract File: C:\optimfile\data\davefile.XF
Qualifier: OPTIMDB.DMAJCHER

Destination
Qualifier: OPTIMDB.DMAJCHER

Description:

Column Map ID:

Server Name: (Local)

	Source Table	Destination Table	Type	Column Map or "LOCAL"	Column Map Status
1	CUSTOMERS	CUSTOMERS	Table		Unused
2	SALES	SALES	Table		Unused
3	ORDERS	ORDERS	Table		Unused
4	DETAILS	DETAILS	Table		Unused
5	ITEMS	ITEMS	Table		Unused

2 part name

default is the same table names

Populate Destination Tables

- Column Map
  - Map unlike column names
  - Transform/mask sensitive data
  - Datatype conversions
  - Column-level date aging

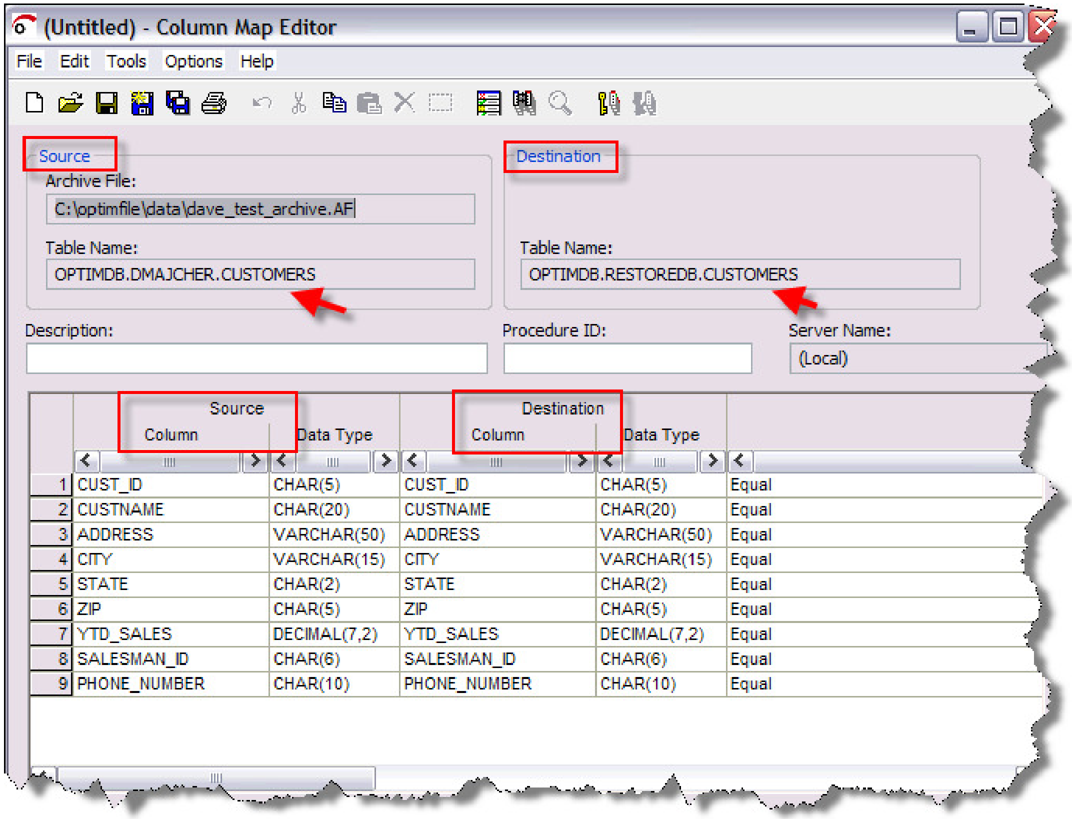
Literals

Special Registers

Expressions

Default Values

User exits



Source

Archive File: C:\optimfile\data\dave_test_archive.AF

Table Name: OPTIMDB.DMAJCHER.CUSTOMERS

Destination

Table Name: OPTIMDB.RESTOREDB.CUSTOMERS

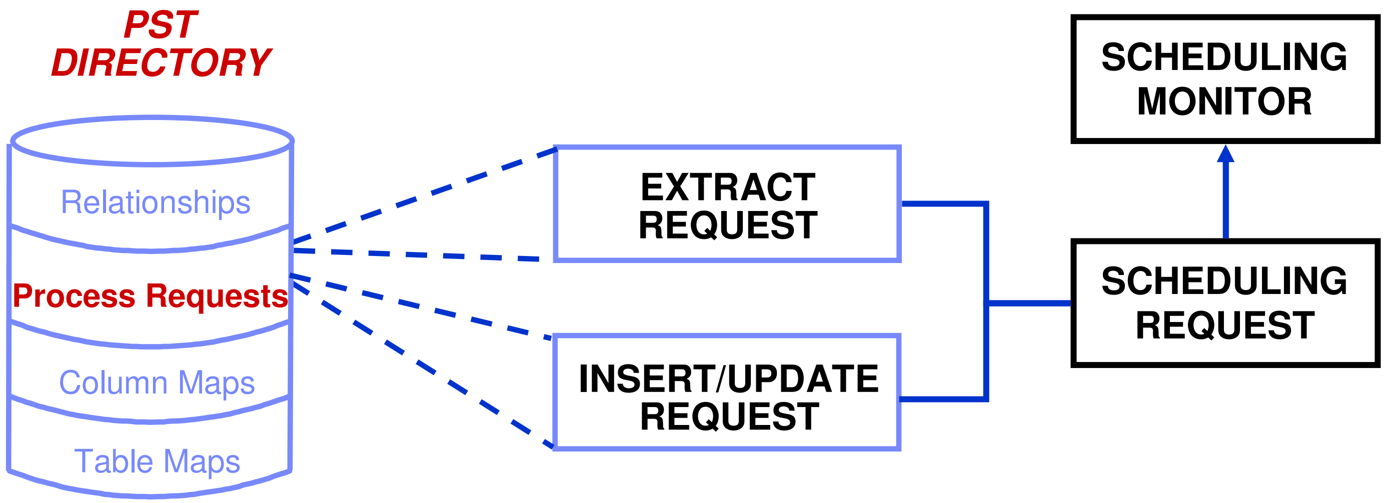
Description:

Procedure ID:

Server Name: (Local)

	Source		Destination		
	Column	Data Type	Column	Data Type	
1	CUST_ID	CHAR(5)	CUST_ID	CHAR(5)	Equal
2	CUSTNAME	CHAR(20)	CUSTNAME	CHAR(20)	Equal
3	ADDRESS	VARCHAR(50)	ADDRESS	VARCHAR(50)	Equal
4	CITY	VARCHAR(15)	CITY	VARCHAR(15)	Equal
5	STATE	CHAR(2)	STATE	CHAR(2)	Equal
6	ZIP	CHAR(5)	ZIP	CHAR(5)	Equal
7	YTD_SALES	DECIMAL(7,2)	YTD_SALES	DECIMAL(7,2)	Equal
8	SALESMAN_ID	CHAR(6)	SALESMAN_ID	CHAR(6)	Equal
9	PHONE_NUMBER	CHAR(10)	PHONE_NUMBER	CHAR(10)	Equal

Scheduling



- Package saved Process Requests for a complete job
- Schedule requests for automated operation
- Command line interface available

IBM Software Group

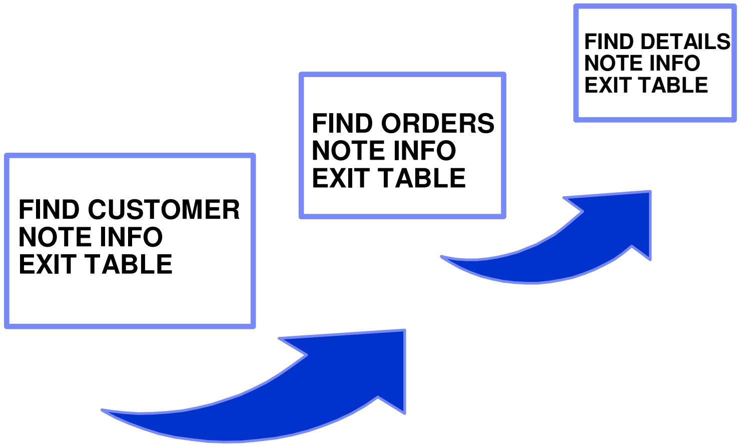
IBM Optim Editor

An IBM Proof of Technology

Traditional vs. Relational Tools

Single Table Editors

- One table/view at a time
- No edit of related data from multiple tables



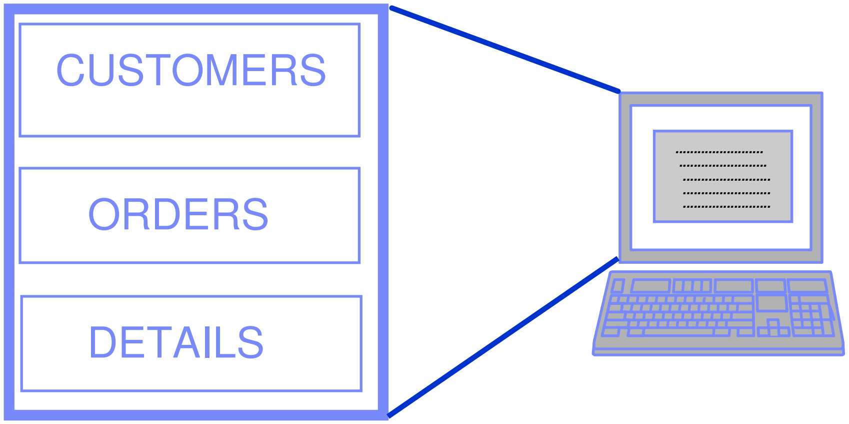
FIND CUSTOMER
NOTE INFO
EXIT TABLE

FIND ORDERS
NOTE INFO
EXIT TABLE

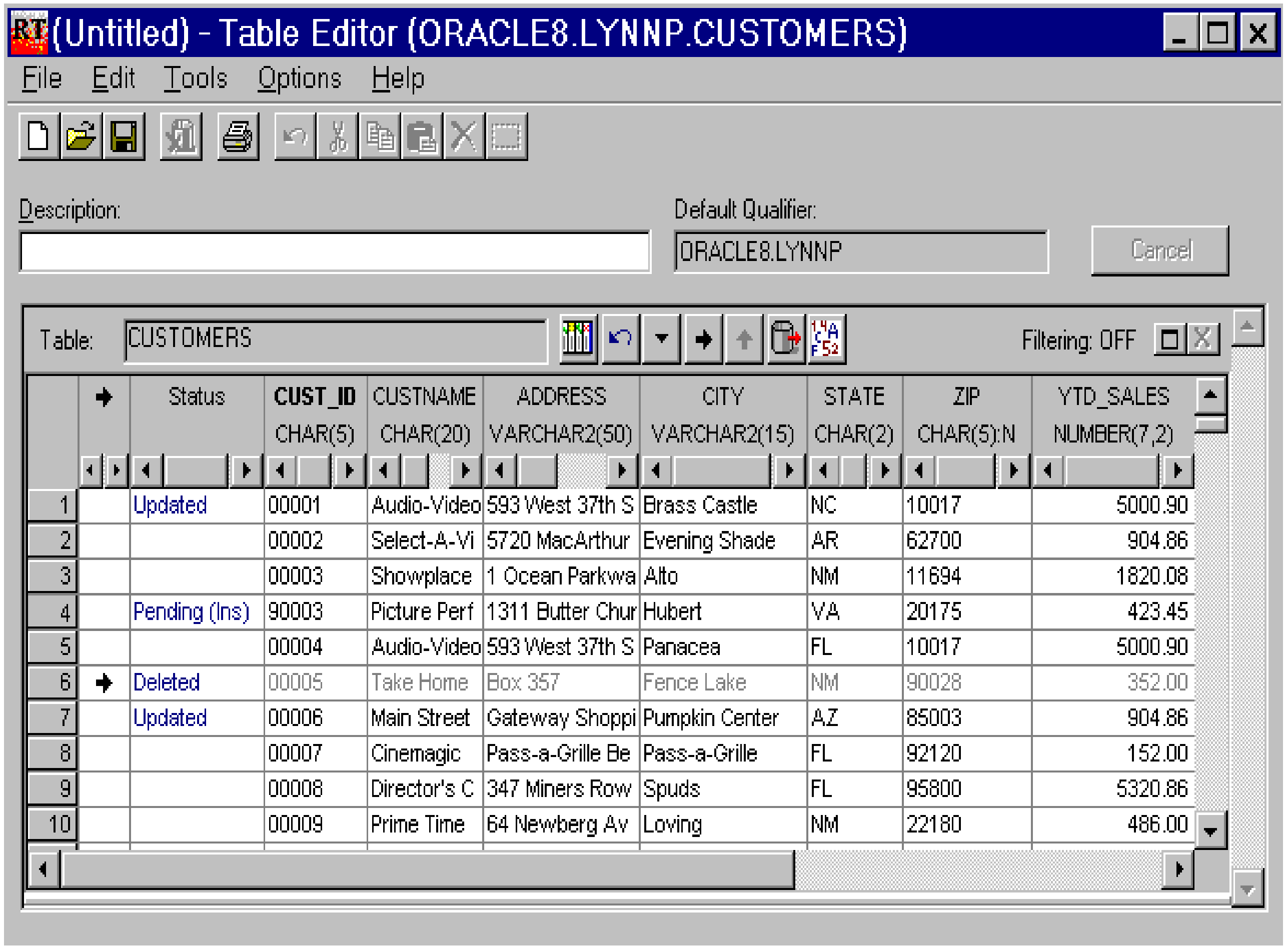
FIND DETAILS
NOTE INFO
EXIT TABLE

The Relational Editor

- ***Simultaneous* browse/edit of related data from multiple tables**



Editing Data



Description:

Default Qualifier: ORACLE8.LYNNP

Table: CUSTOMERS

Filtering: OFF

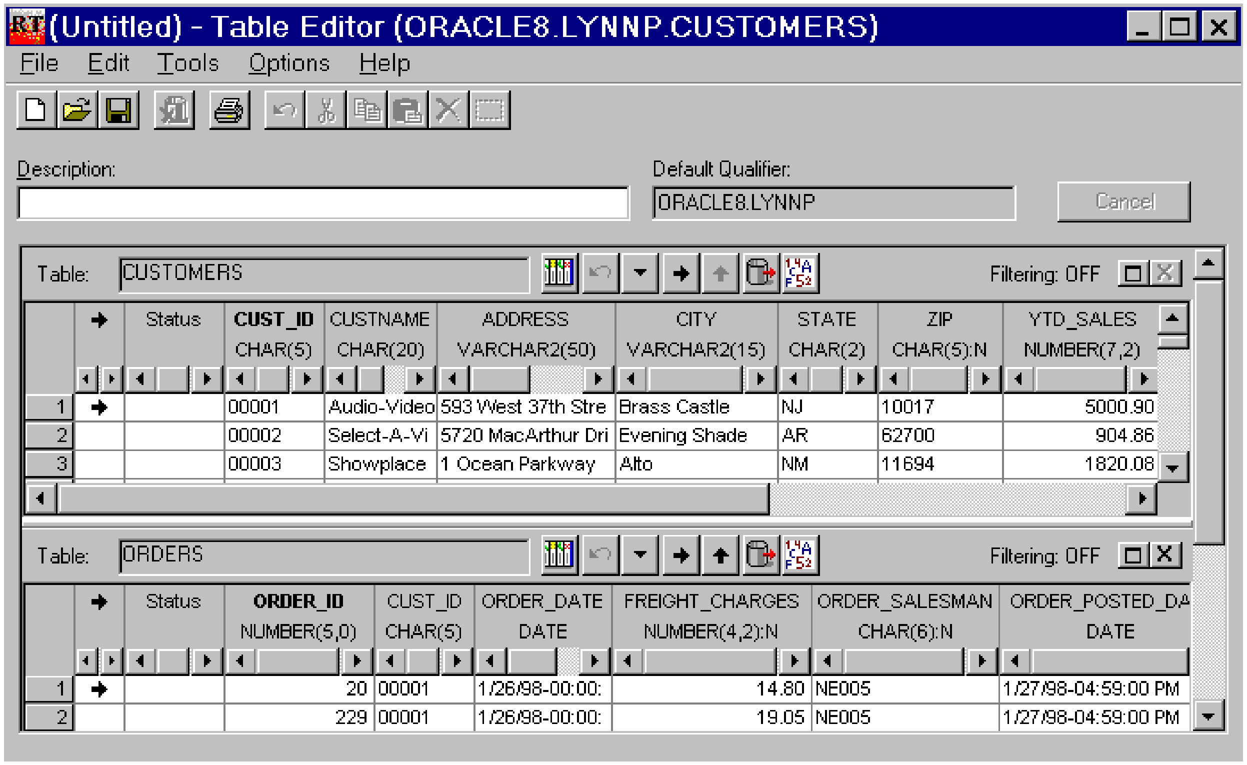
	➔	Status	CUST_ID CHAR(5)	CUSTNAME CHAR(20)	ADDRESS VARCHAR2(50)	CITY VARCHAR2(15)	STATE CHAR(2)	ZIP CHAR(5):N	YTD_SALES NUMBER(7,2)
1		Updated	00001	Audio-Video	593 West 37th S	Brass Castle	NC	10017	5000.90
2			00002	Select-A-Vi	5720 MacArthur	Evening Shade	AR	62700	904.86
3			00003	Showplace	1 Ocean Parkwa	Alto	NM	11694	1820.08
4		Pending (Ins)	90003	Picture Perf	1311 Butter Chur	Hubert	VA	20175	423.45
5			00004	Audio-Video	593 West 37th S	Panacea	FL	10017	5000.90
6	➔	Deleted	00005	Take Home	Box 357	Fence Lake	NM	90028	352.00
7		Updated	00006	Main Street	Gateway Shoppi	Pumpkin Center	AZ	85003	904.86
8			00007	Cinemagic	Pass-a-Grille Be	Pass-a-Grille	FL	92120	152.00
9			00008	Director's C	347 Miners Row	Spuds	FL	95800	5320.86
10			00009	Prime Time	64 Newberg Av	Loving	NM	22180	486.00

Edit data to:

- Insert Rows
- Delete Rows
- Update Rows

Relationally Joined Data

- Browse or edit related rows
- Scroll of higher-level table automatically synchronizes all lower-joined tables



Description:

Default Qualifier: ORACLE8.LYNNP

Table: CUSTOMERS Filtering: OFF

	→	Status	CUST_ID	CUSTNAME	ADDRESS	CITY	STATE	ZIP	YTD_SALES
			CHAR(5)	CHAR(20)	VARCHAR2(50)	VARCHAR2(15)	CHAR(2)	CHAR(5):N	NUMBER(7,2)
1	→		00001	Audio-Video	593 West 37th Stre	Brass Castle	NJ	10017	5000.90
2			00002	Select-A-Vi	5720 MacArthur Dri	Evening Shade	AR	62700	904.86
3			00003	Showplace	1 Ocean Parkway	Alto	NM	11694	1820.08

Table: ORDERS Filtering: OFF

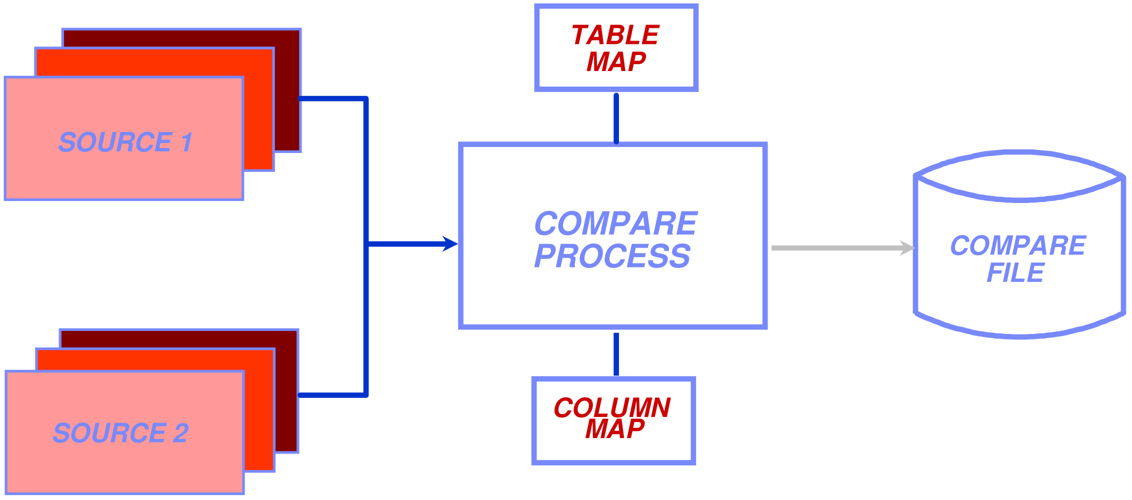
	→	Status	ORDER_ID	CUST_ID	ORDER_DATE	FREIGHT_CHARGES	ORDER_SALESMAN	ORDER_POSTED_DA
			NUMBER(5,0)	CHAR(5)	DATE	NUMBER(4,2):N	CHAR(6):N	DATE
1	→		20	00001	1/26/98-00:00:	14.80	NE005	1/27/98-04:59:00 PM
2			229	00001	1/26/98-00:00:	19.05	NE005	1/27/98-04:59:00 PM

IBM Software Group

IBM Optim Compare

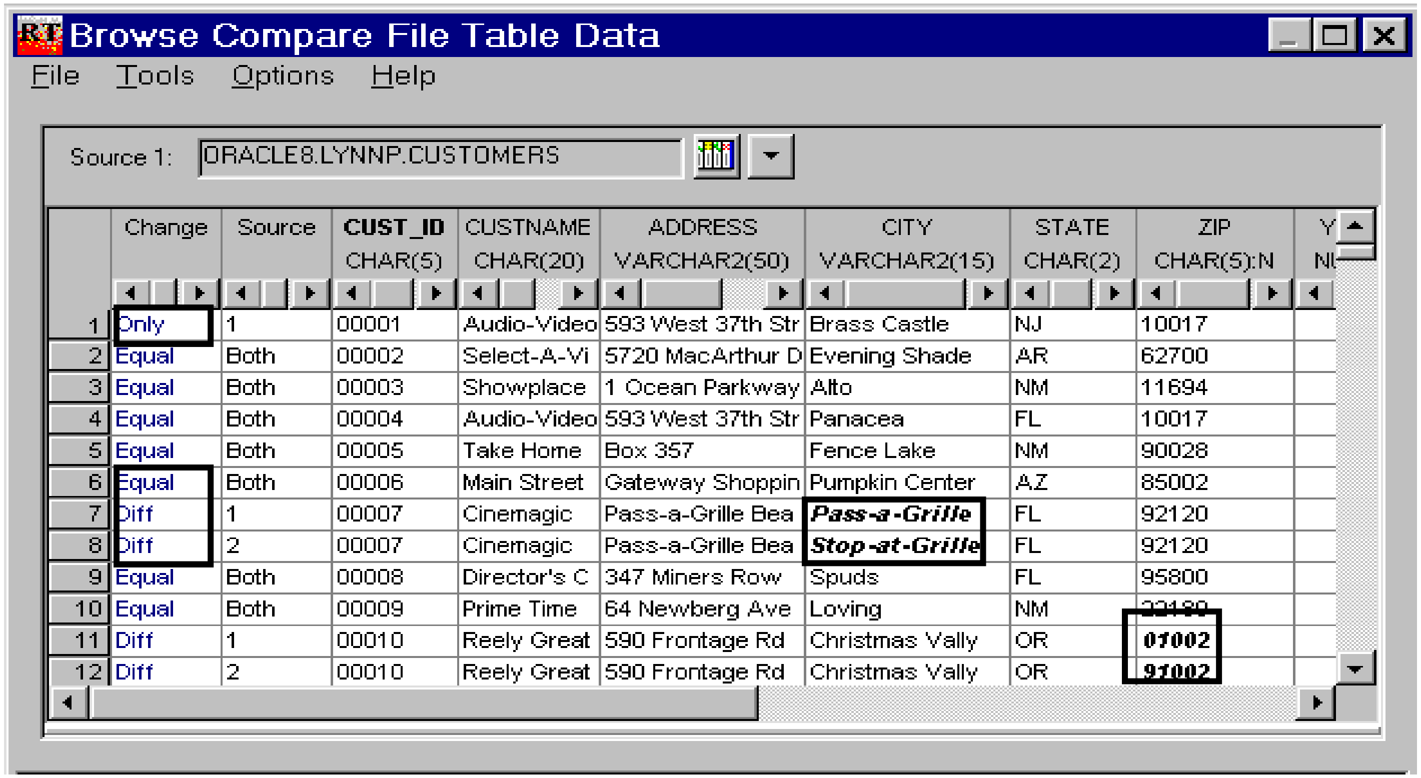
An IBM Proof of Technology

OPTIM Relational Compare Facility



- Single-table or multi-table compare
- Creates compare file of results
- Displays results on screen
- For application testing, QA, and to verify database contents
- Enhances productivity by finding unexpected changes in the data

Browsing the Compare File



Source 1: ORACLE8.LYNNP.CUSTOMERS

	Change	Source	CUST_ID CHAR(5)	CUSTNAME CHAR(20)	ADDRESS VARCHAR2(50)	CITY VARCHAR2(15)	STATE CHAR(2)	ZIP CHAR(5):N	Y NI
1	Only	1	00001	Audio-Video	593 West 37th Str	Brass Castle	NJ	10017	
2	Equal	Both	00002	Select-A-Vi	5720 MacArthur D	Evening Shade	AR	62700	
3	Equal	Both	00003	Showplace	1 Ocean Parkway	Alto	NM	11694	
4	Equal	Both	00004	Audio-Video	593 West 37th Str	Panacea	FL	10017	
5	Equal	Both	00005	Take Home	Box 357	Fence Lake	NM	90028	
6	Equal	Both	00006	Main Street	Gateway Shoppin	Pumpkin Center	AZ	85002	
7	Diff	1	00007	Cinemagic	Pass-a-Grille Bea	***Pass-a-Grille***	FL	92120	
8	Diff	2	00007	Cinemagic	Pass-a-Grille Bea	***Stop-at-Grille***	FL	92120	
9	Equal	Both	00008	Director's C	347 Miners Row	Spuds	FL	95800	
10	Equal	Both	00009	Prime Time	64 Newberg Ave	Loving	NM	22180	
11	Diff	1	00010	Reely Great	590 Frontage Rd	Christmas Vally	OR	**01002**	
12	Diff	2	00010	Reely Great	590 Frontage Rd	Christmas Vally	OR	**91002**	

- Change column identifies the type of change
- Source column identifies input source row
- Data differences are highlighted

IBM Optim Data Privacy

An IBM Proof of Technology

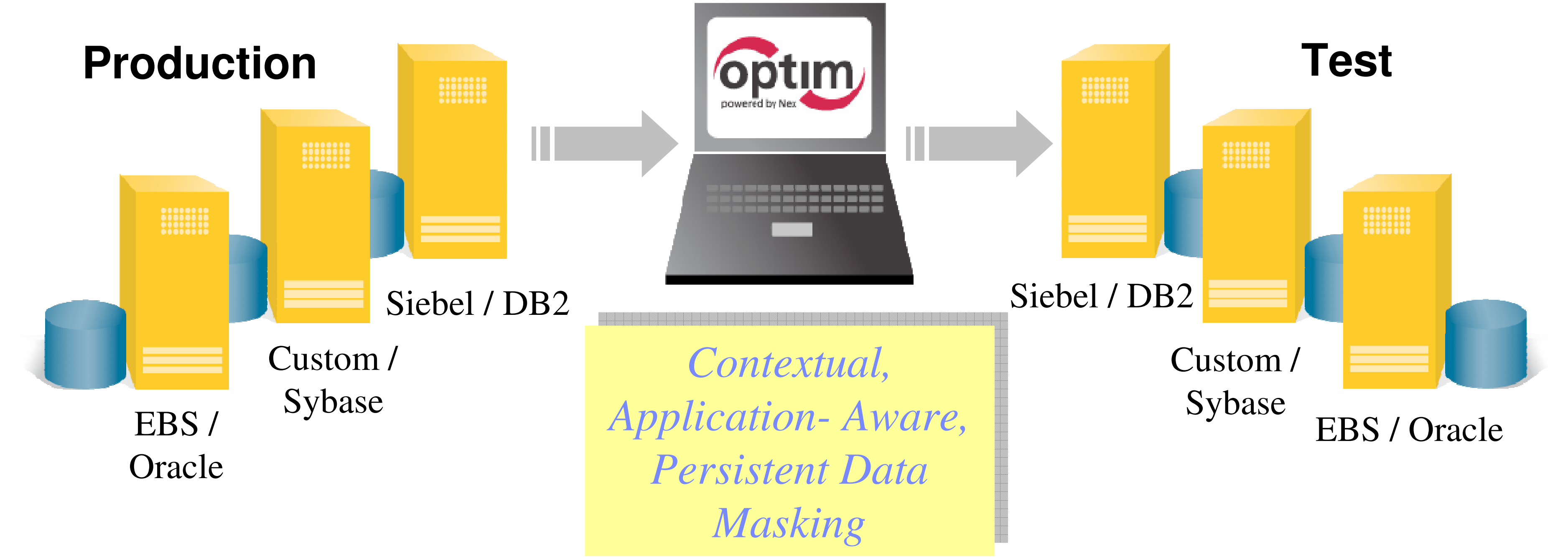
Challenges of Enterprise Data Privacy

- Multi-platforms
- Relational database applications in the enterprise
  - Complex data model
  - Multiple databases
  - Legacy data components
  - Interconnected applications
- Distributed work teams
  - Employees and contractors
  - Global 24 x 7 operations

How does Optim Protect Privacy?

- IBM Optim provides the fundamental components of test data management and enables organizations to ***de-identify, mask and transform*** sensitive data
- Companies can apply a range of transformation techniques to substitute customer data with ***contextually-accurate but fictionalized data*** to produce ***accurate test results***
- By masking personally-identifying information, Optim protects the ***privacy and security*** of confidential customer data, and ***supports compliance*** with local, state, national, international and industry-based privacy regulations

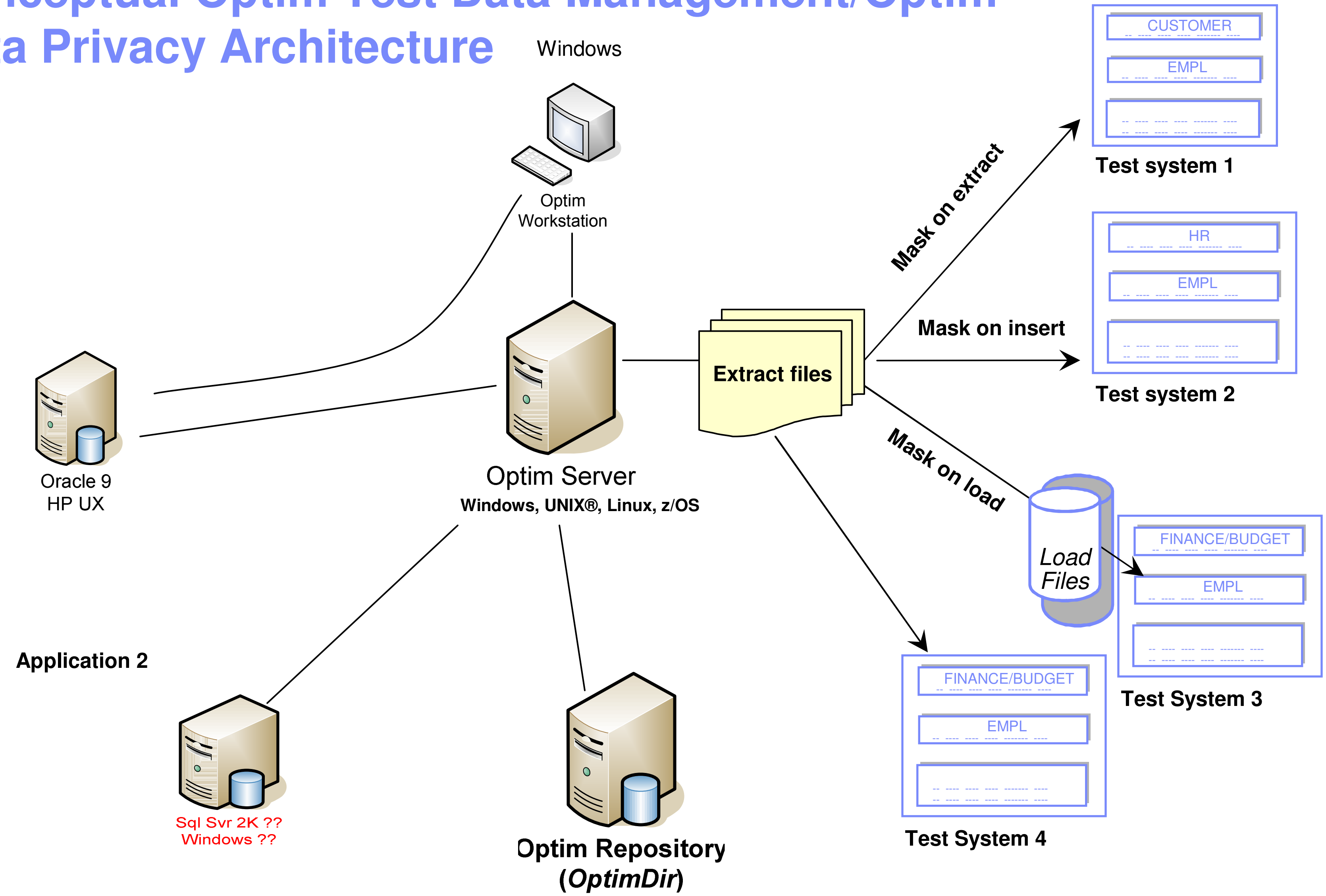
Optim Data Privacy Solution



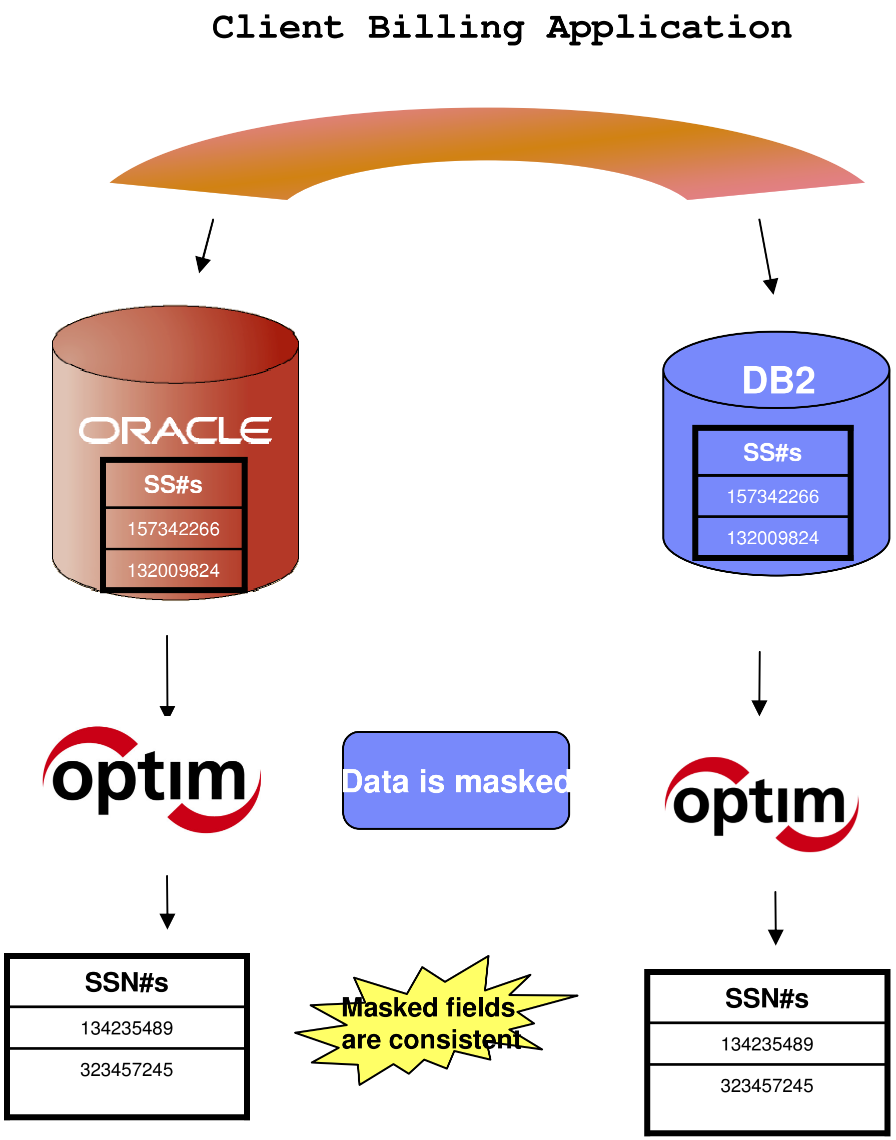
Contextual, Application- Aware, Persistent Data Masking

- Substitute confidential information with fictionalized data
- Deploy multiple masking algorithms
- Provide consistency across environments and iterations
- Enable off-shore testing
- Protect private data in non-production environments

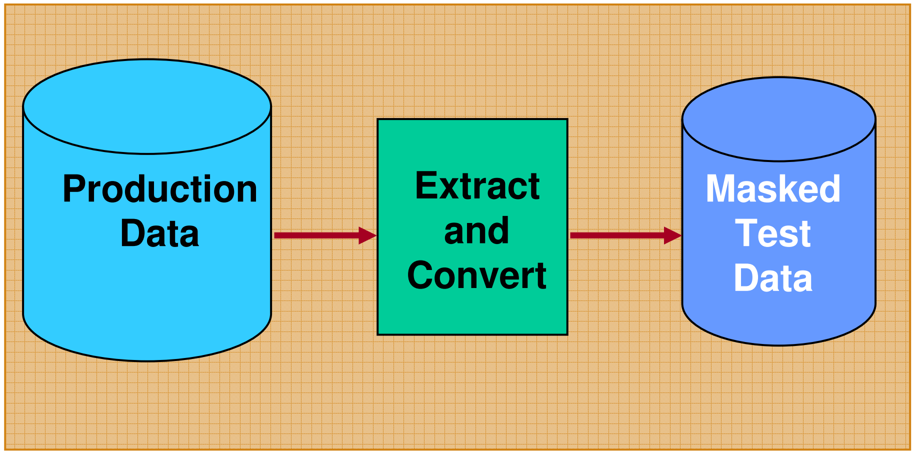
Conceptual Optim Test Data Management/Optim Data Privacy Architecture



Consistent Masking across the Enterprise



De-Identify test data



During Extract Process

Or

Standalone Convert Process

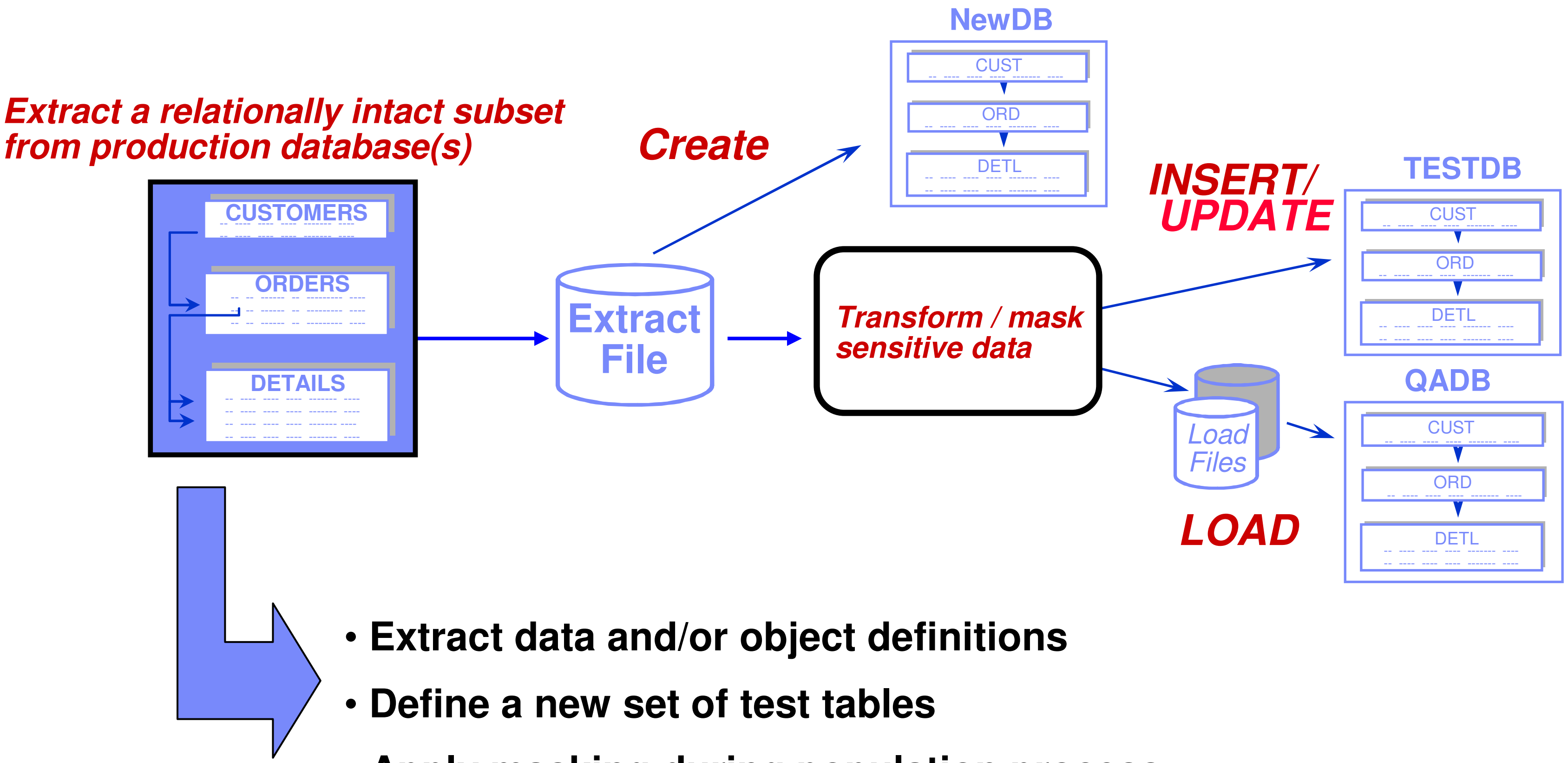
Or

During Insert/Load Process

Transform or Replace sensitive data using

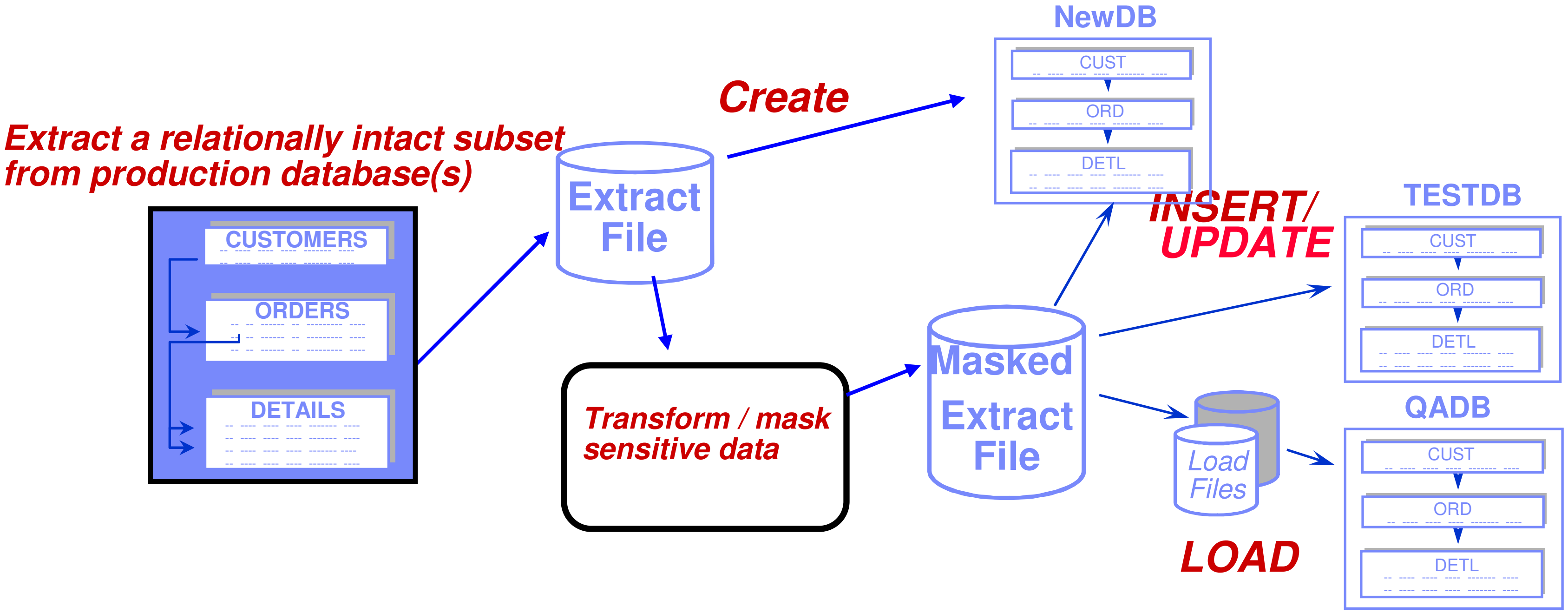
- Standard mapping rules: Literals, Special Registers, Expressions, Default Values, Look-up tables
- Complex mapping rules: User exits

Optim Data Privacy in Application Testing



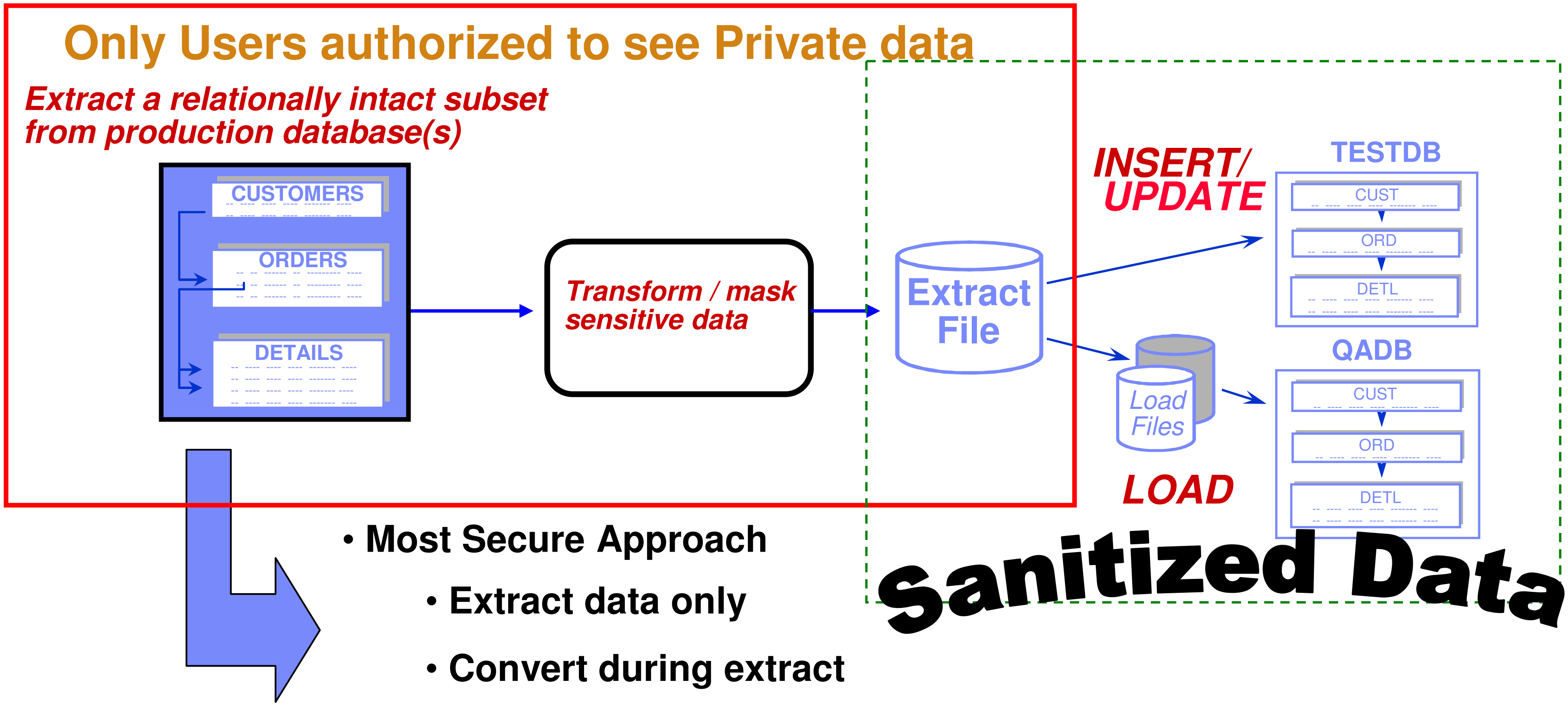
- Extract data and/or object definitions
- Define a new set of test tables
- Apply masking during population process
- Extract file may be reused but contains un-Masked data
- Good practice for testing masks

Optim Data Privacy in Application Testing



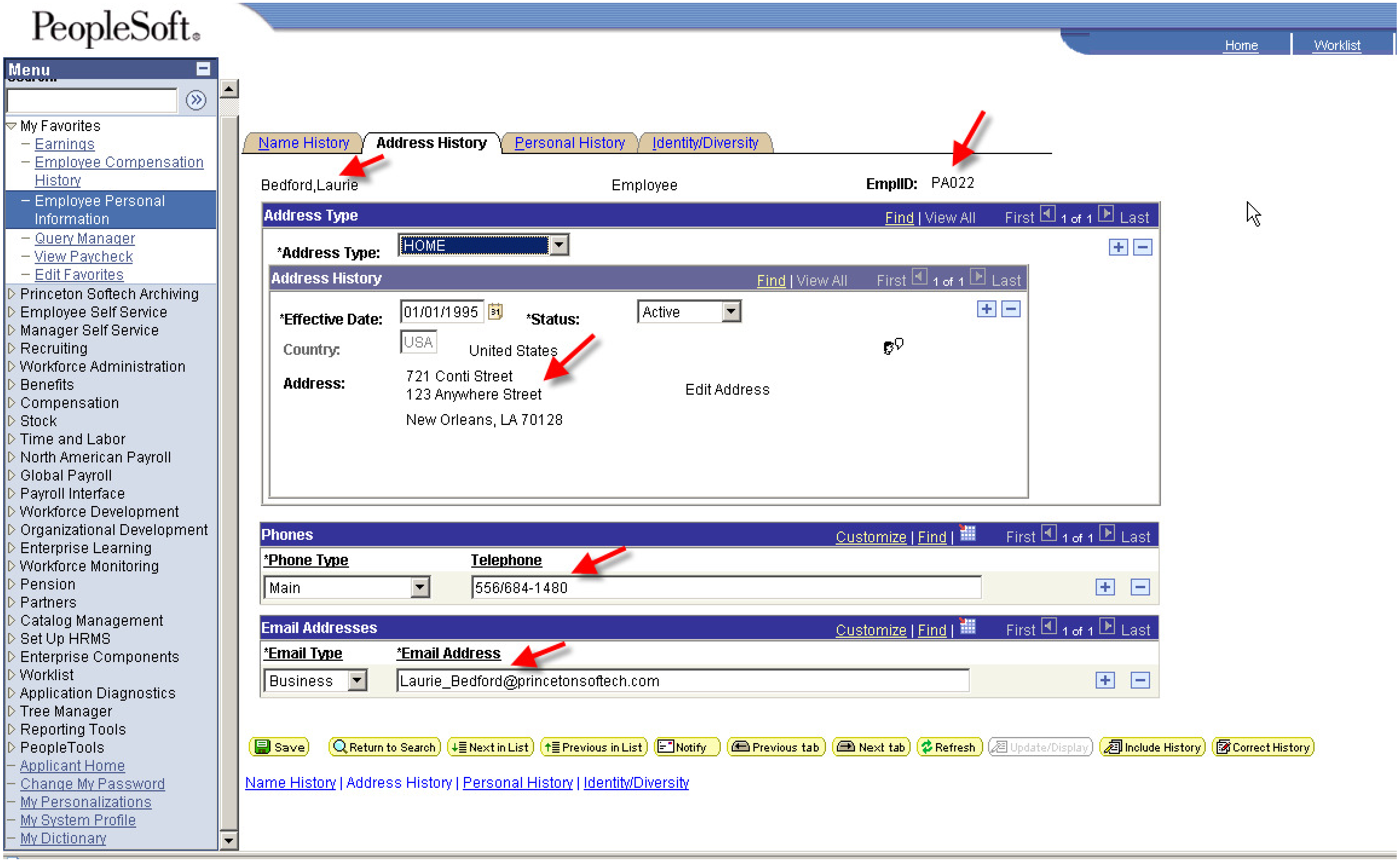
- Extract data and/or object definitions in pre-masked file
- Use pre-masked Extract file to create new set of tables
- Convert Pre-masked extract file data into second masked extract file
- Share masked extract file to be reused for population step
- Good practice for testing masks using COMPARE

Optim Data Privacy in Application Testing


Only Users authorized to see Private data
Extract a relationally intact subset from production database(s)
CUSTOMERS
ORDERS
DETAILS
Transform / mask sensitive data
Extract File
INSERT/ UPDATE
TESTDB
CUST
ORD
DETL
Load Files
LOAD
QADB
CUST
ORD
DETL
Sanitized Data

- Most Secure Approach
  - Extract data only
  - Convert during extract
- Extract file already contains masked data
  - Can be shared with testers to reuse

Before Data Masking



Bedford,Laurie Employee **EmplID:** PA022

Address Type

*Address Type: HOME

Address History

*Effective Date: 01/01/1995 *Status: Active

Country: USA United States

Address: 721 Conti Street
123 Anywhere Street
New Orleans, LA 70128

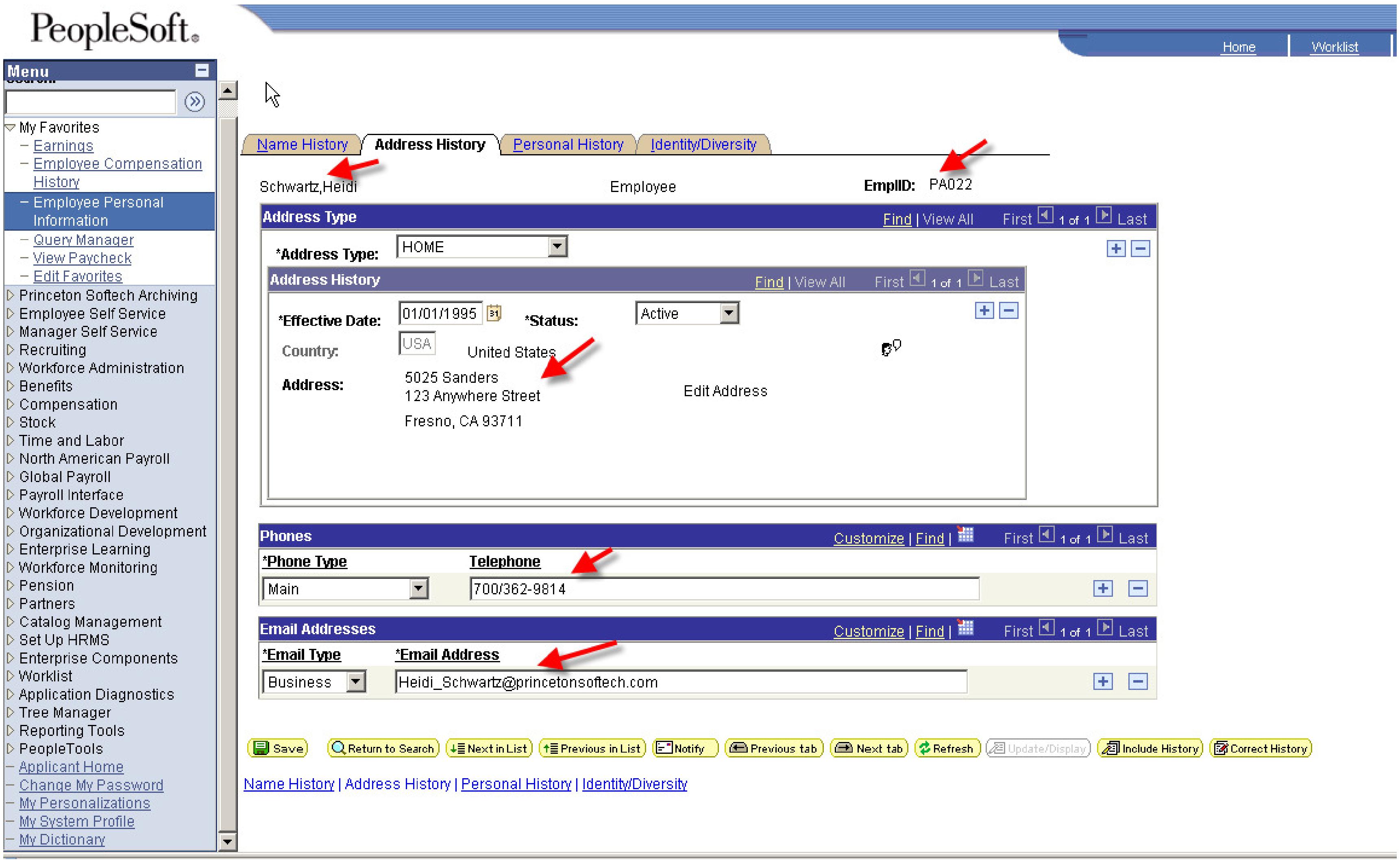
Phones

*Phone Type	Telephone
Main	556/684-1480

Email Addresses

*Email Type	*Email Address
Business	Laurie_Bedford@princetonsoftech.com

After Data Masking



Schwartz,Heidi Employee EmplID: PA022

Address Type

*Address Type: HOME

Address History

*Effective Date: 01/01/1995 *Status: Active

Country: USA United States

Address: 5025 Sanders
123 Anywhere Street
Fresno, CA 93711

Edit Address

Phones

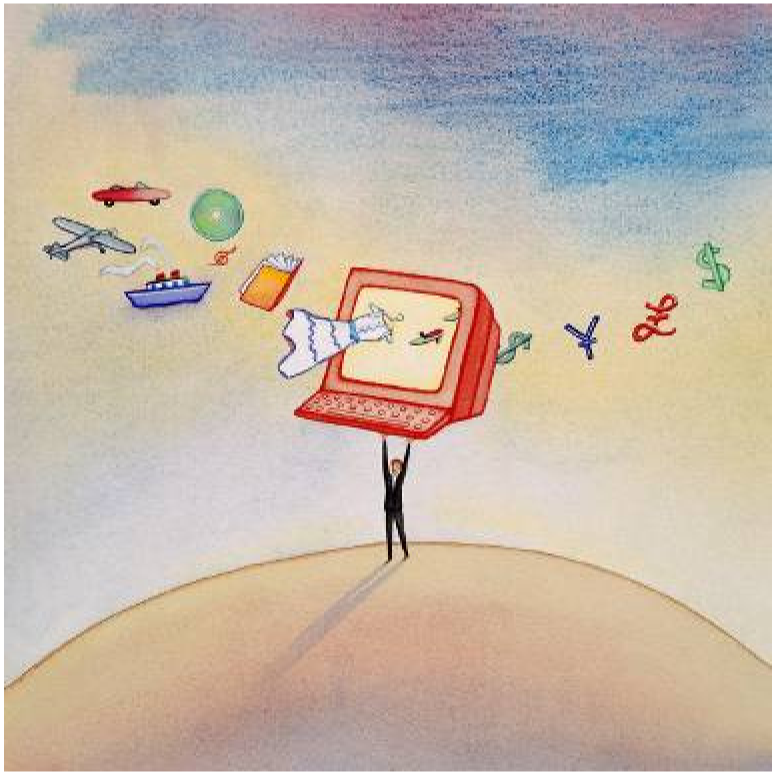
*Phone Type	Telephone
Main	700/362-9814

Email Addresses

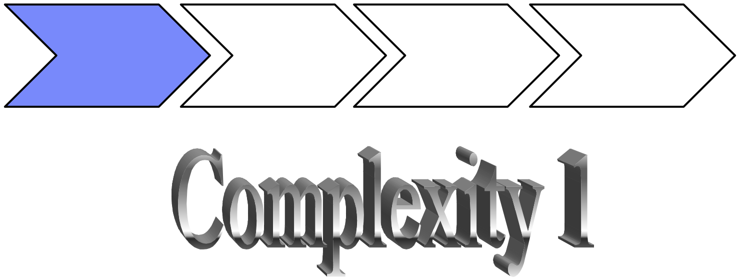
*Email Type	*Email Address
Business	Heidi_Schwartz@princetonsoftech.com

Transformation Techniques

- String literal values
- Character substrings
- Random or sequential numbers
- Arithmetic expressions
- Concatenated expressions
- Date aging
- Lookup values
- Intelligence



Example: Bank Account Numbers


Complexity 1

- First Financial Bank’s account numbers are formatted “123-4567” with the first three digits representing the type of account (checking, savings, or money market) and the last four digits representing the customer identification number
- To mask account numbers for testing, use the *actual first three digits*, plus a *sequential four-digit number*
- The result is a fictionalized account number with a valid format:
  - “001-9898” becomes “001-1000”
  - “001-4570” becomes “001-1001”

Example: Addresses

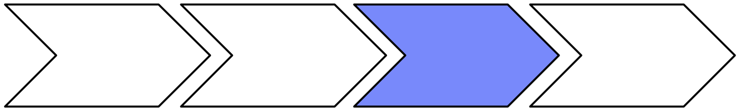
- Direct Response Marketing, Inc. is testing its order fulfillment system
- Fictionalize customer addresses to pull an entire address from the Customer Information table:

  "11110 Campus Drive Princeton, NJ 08541"

  becomes…

  "1223 E. 12th Street NY, NY 10079"

  ▸ **Optim ships with over 100,000 valid CASS addresses**



Complexity 2

Street Address/City/State/Zip Code Data Sets

Total Assets	Customers	Street	City	State	Zip Code
$534,674,233	54,999	12 Buttercup Ln	Cleveland	OH	44101
$8,777,733,811	105,333	6767 Rte 10 S	Princeton	NJ	08594

1) Client is a Bank who wishes to mask its assets by location

Address Lookup Table

2) Optim provides corresponding Street Address/City/State/Zip Codes for masking

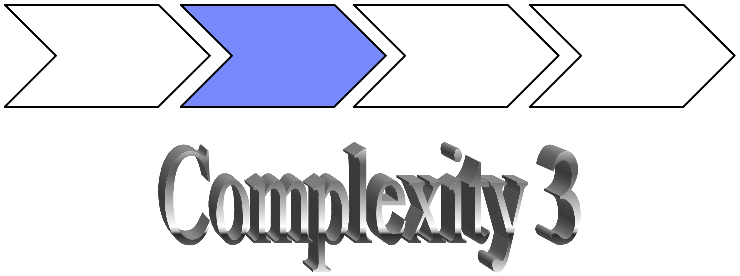
288 Helm St	Milwaukee	WI	53201
12 Roden Dr	Los Angeles	CA	90001
3526 Diamond Rd	Seattle	WA	98101
12 Street Road	Las Vegas	NV	89101
2 Applegarth Ln	Brunswick	ME	04011

3) Leverage Multiple Column Replacement. Entire address row can be masked with a valid Coding Accuracy Support System (CASS) address using enhanced random lookup function

New Table with Masked Data

Total Assets	Customers	Street	City	State	Zip Code
$534,674,233	54,999	**3526 Diamond Rd**	**Seattle**	**WA**	**98101**
$8,777,733,811	105,333	**21 Street Rd**	**Las Vegas**	**NV**	**89101**

Example: First and Last Name



- Direct Response Marketing, Inc. is testing its order fulfillment system
- Fictionalize customer names to pull first and last names randomly from the Customer Information table:
  - "Adam Adams" becomes "Ronald Smith"
  - "Anna Adams" becomes "Elena Wu"
  - **Optim ships with over 5,000 male/female names and over 80,000 last names**

First Names and Last Names Data Sets

Production Database

First Name	Last Name	GPA	High School	Advisor	State
Paul	Smith	3.2	Princeton	Johnson	NJ
Kate	Jones	2.7	Albany	Kline	NY

First Name Lookup Table
John
Bob
Danielle
Dave
Stacey

Last Name Lookup Table
Newton
Nelson
Kline
Howell
Reese

1) Client is a University who wishes to mask the first and last name fields in their admissions database

2) Optim now has a first name lookup table with over 5,000 male/female names and a last name lookup table with over 80,000 names

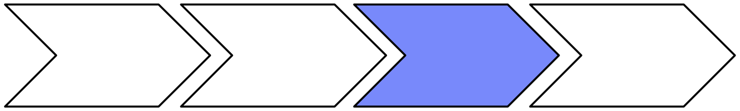
3) Use Lookup Tables to randomly replace table first and last names

Test Database

First Name	Last Name	GPA	High School	Advisor	State
Stacey	**Nelson**	3.2	Princeton	Johnson	NJ
Dave	**Reese**	2.7	Albany	Kline	NY

Example: Semantic Transformation

- Generating valid **social security** numbers (as defined by the US Social Security Administration)
- Generate valid **credit card** numbers (as defined by credit card issuers)
- Generate **desensitized e-mail** addresses
  - *Generate Email address based on format: name@domain*



Complexity 3

Social Security Numbers and Credit Cards

Production Database

F. Name	L. Name	Credit Card#	SSN#
John	Jones	5298774132478855	254-77-6644
Vanessa	Jones	4324115574123654	154-74-7788

Data before Masking

Test Database

Valid

Valid

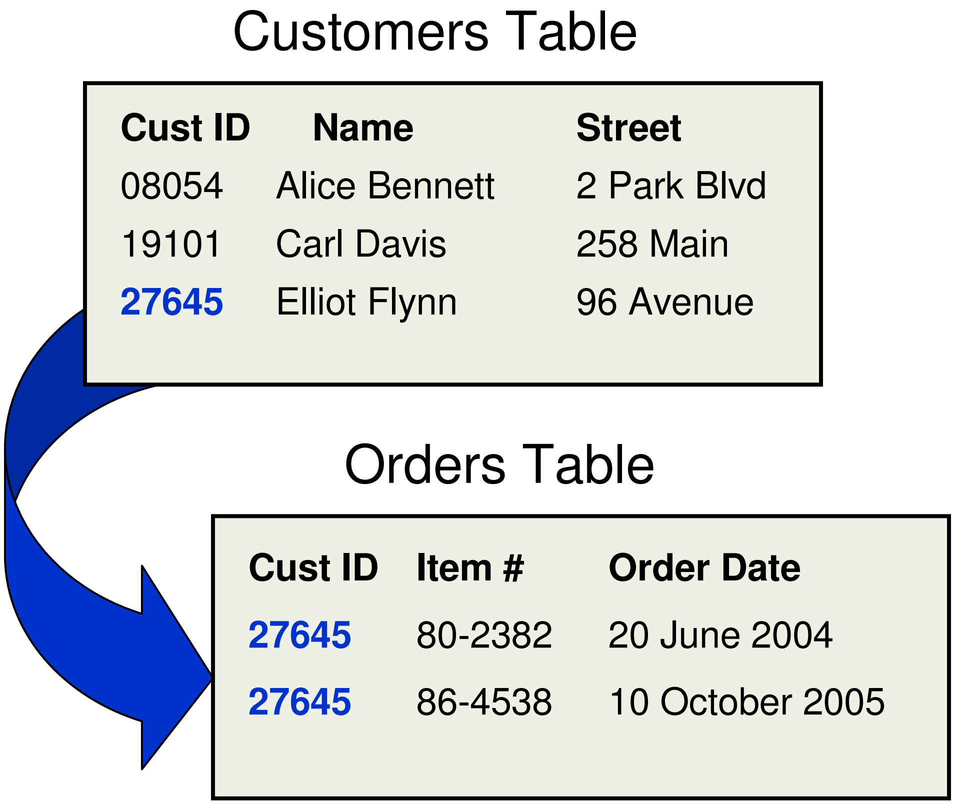
F. Name	L. Name	Credit Card#	SSN#
John	Jones	**5326458711224956**	**854-77-6644**
Vanessa	Jones	**4972584612457744**	**258-74-7788**

Data after Masking… Masked with Valid CC# and SS#

How are these numbers valid?

For Social Security Numbers	For Credit Card Numbers
A Social Security Number (SSN) consists of nine digits. The first three digits is called the "area number'. The central, two-digit field is called the "group Number". The final four-digit field is called the "serial Number". All numbers must fit the latest available criteria for each section.	Most credit card numbers are encoded with a "Check Digit". A check digit is a digit added to a number (either at the end or the beginning) that validates the authenticity of the number. A simple algorithm is applied to the other digits of the number which yields the check digit.

Propagating Masked Data



Customers Table

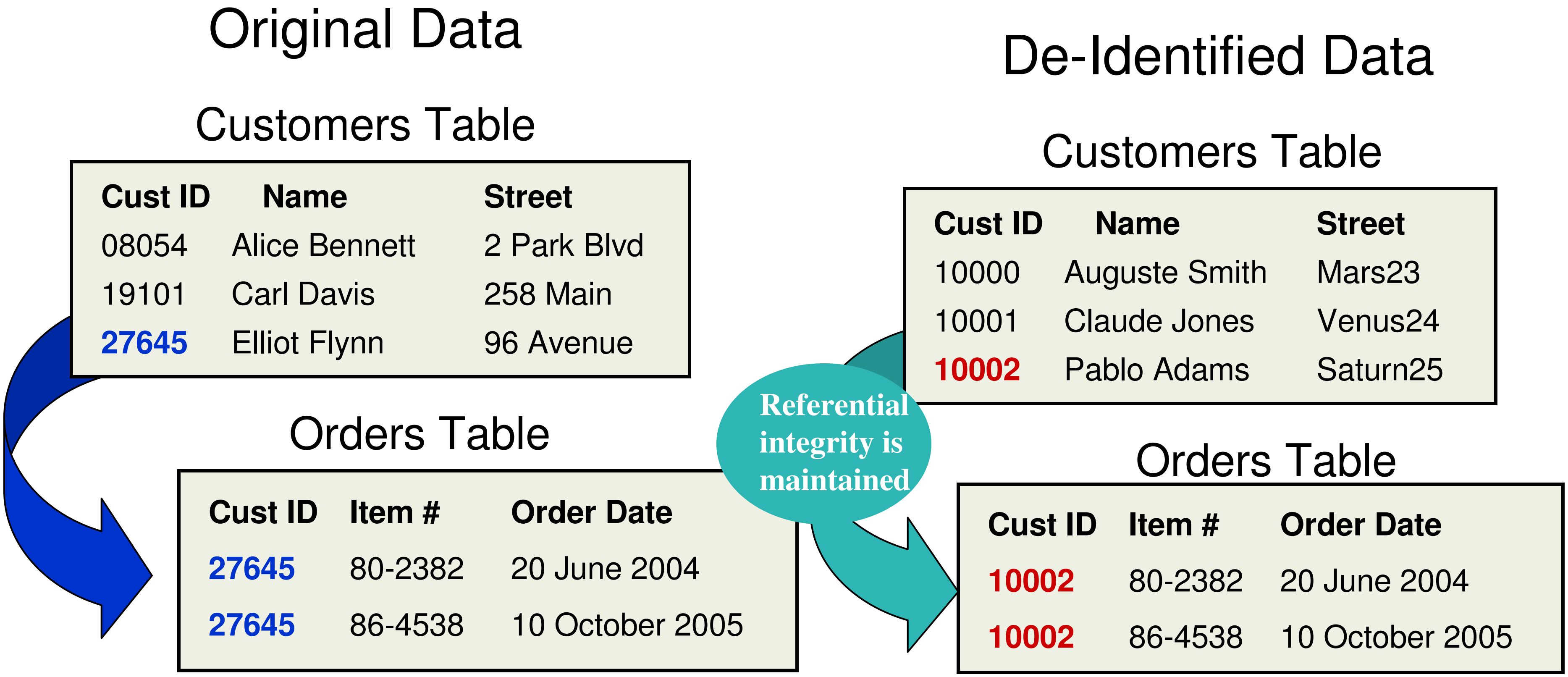
Cust ID	Name	Street
08054	Alice Bennett	2 Park Blvd
19101	Carl Davis	258 Main
27645	Elliot Flynn	96 Avenue

Orders Table

Cust ID	Item #	Order Date
27645	80-2382	20 June 2004
27645	86-4538	10 October 2005

- Key propagation
  - Propagate values in the primary key to all related tables
  - Necessary to maintain referential integrity

Masking with Key Propagation



Original Data

Customers Table

Cust ID	Name	Street
08054	Alice Bennett	2 Park Blvd
19101	Carl Davis	258 Main
27645	Elliot Flynn	96 Avenue

Orders Table

Cust ID	Item #	Order Date
27645	80-2382	20 June 2004
27645	86-4538	10 October 2005

Referential integrity is maintained

De-Identified Data

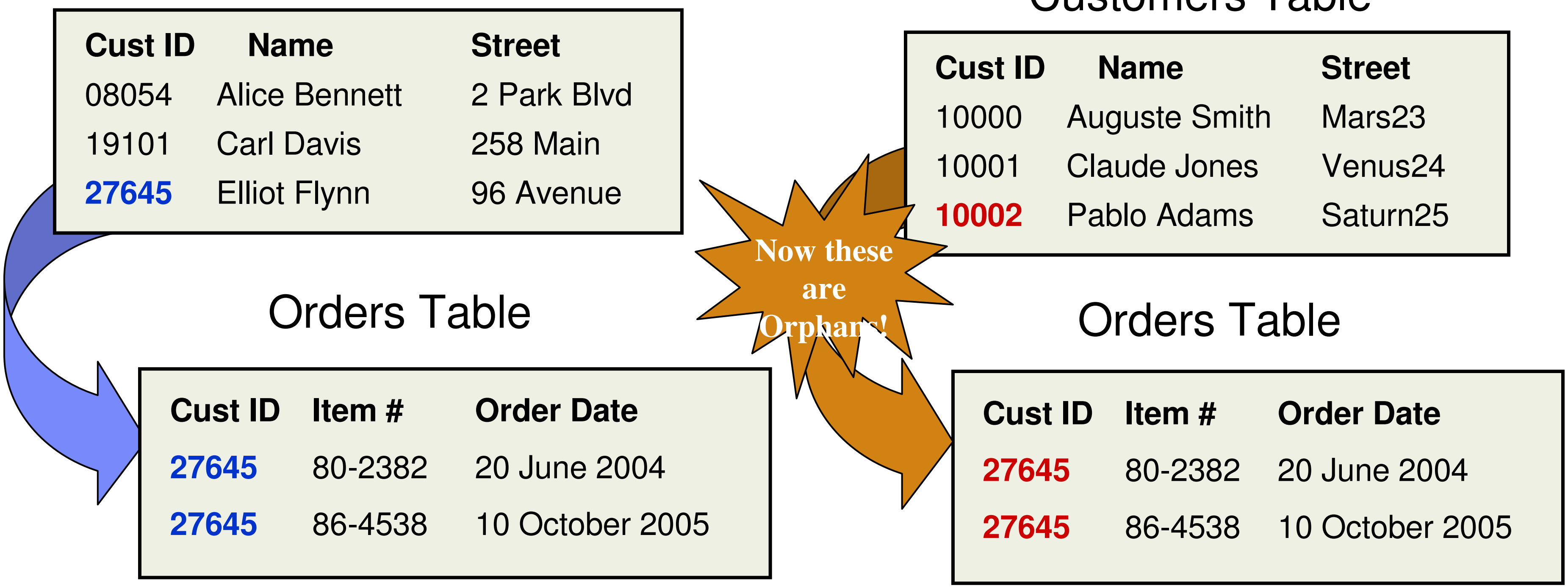
Customers Table

Cust ID	Name	Street
10000	Auguste Smith	Mars23
10001	Claude Jones	Venus24
10002	Pablo Adams	Saturn25

Orders Table

Cust ID	Item #	Order Date
10002	80-2382	20 June 2004
10002	86-4538	10 October 2005

Without Key Propagation…



Original Data

Customers Table

Cust ID	Name	Street
08054	Alice Bennett	2 Park Blvd
19101	Carl Davis	258 Main
27645	Elliot Flynn	96 Avenue

Orders Table

Cust ID	Item #	Order Date
27645	80-2382	20 June 2004
27645	86-4538	10 October 2005

Without Key Propagation

Customers Table

Cust ID	Name	Street
10000	Auguste Smith	Mars23
10001	Claude Jones	Venus24
10002	Pablo Adams	Saturn25

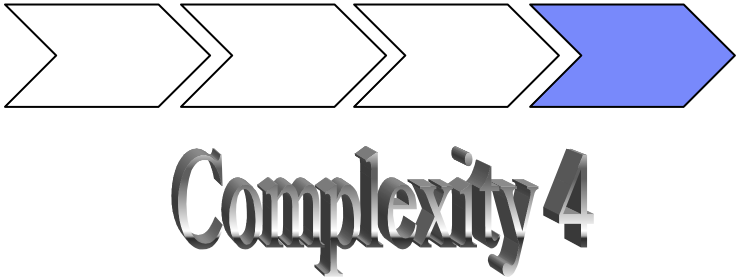
Orders Table

Cust ID	Item #	Order Date
27645	80-2382	20 June 2004
27645	86-4538	10 October 2005

Now these are Orphans!

Using Custom Masking Exits

- Apply complex **data transformation algorithms** and populate the resulting value to the destination column
- Selectively **include or exclude rows** and apply logic to the masking process
- Valuable where the desired transformation is beyond the scope of supplied Column Map functions
- Example: Generate a value for CUST_ID based on customer location, average account balance, and volume of transaction activity



Questions

Optim TDM and DP Labs

An IBM Proof of Technology

Introduction

IBM InfoSphere Guardium

Outline

- Business Drivers for Database Security
- Guardium Architecture
- Case Studies
- Summary

Key Business Drivers for Database Activity Monitoring (DAM)

Continuously Monitor All Access to Sensitive Data:

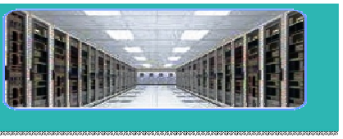
1. **Prevent data breaches**
   - Cybercriminals & rogue insiders
   - Protect customer data & corporate secrets (IP)

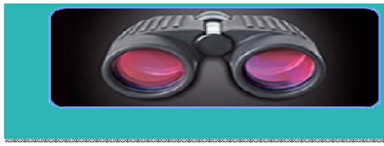
2. **Assure data governance**
   - Prevent unauthorized changes to sensitive data by privileged users

3. **Reduce audit costs**
   - Automated, continuous controls
   - Simplified processes

Top Data Protection Challenges

Where is my sensitive data - and who's accessing it (including privileged users)?





How can I enforce access control & change control policies for databases?

How do I check for vulnerabilities and lock-down database configurations?

How do I reduce costs by automating & centralizing compliance controls?

Addressing Key Stakeholders

SECURITY OPERATIONS

- ✓ Real-time policies
- ✓ Secure audit trail
- ✓ Data mining & forensics

COMPLIANCE AUDIT

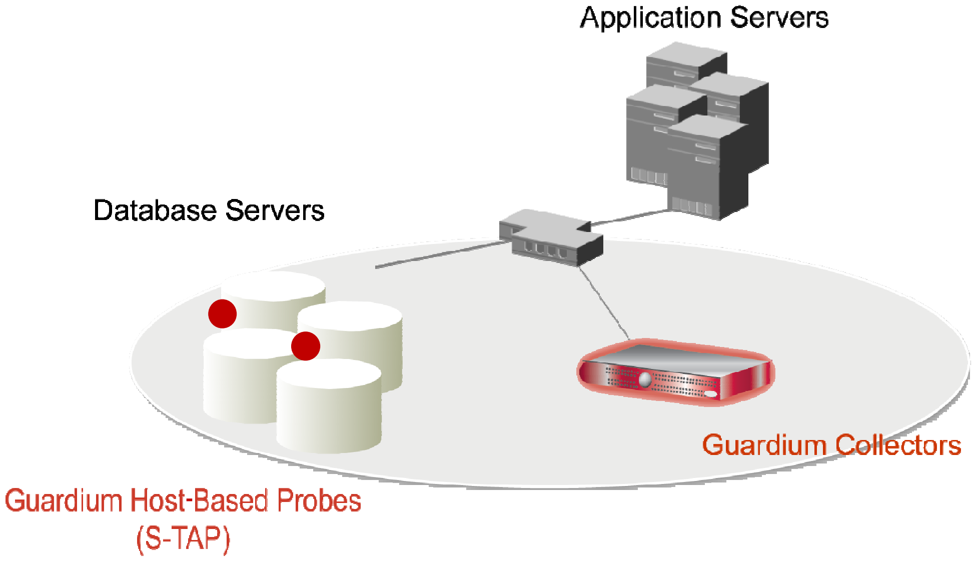
- ✓ Separation of duties
- ✓ Best practices reports
- ✓ Automated controls

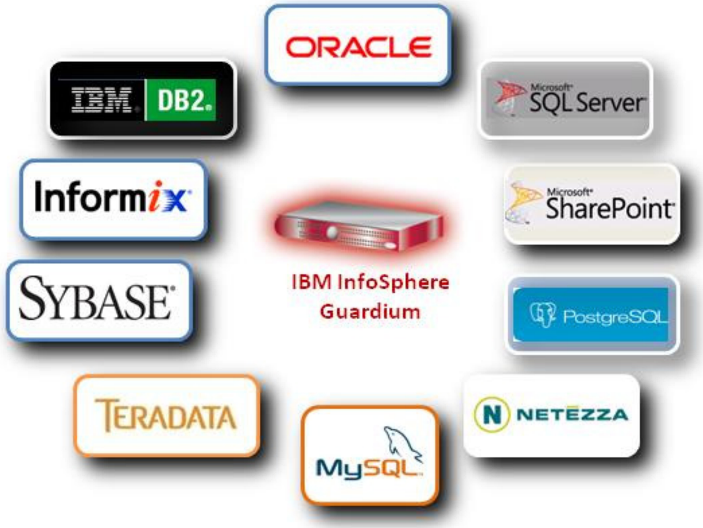
APPLICATION & DATABASE

- ✓ Minimal impact
- ✓ Change management
- ✓ Performance optimization

100% Visibility & Unified View

Non-Invasive, Real-Time Database Security & Monitoring

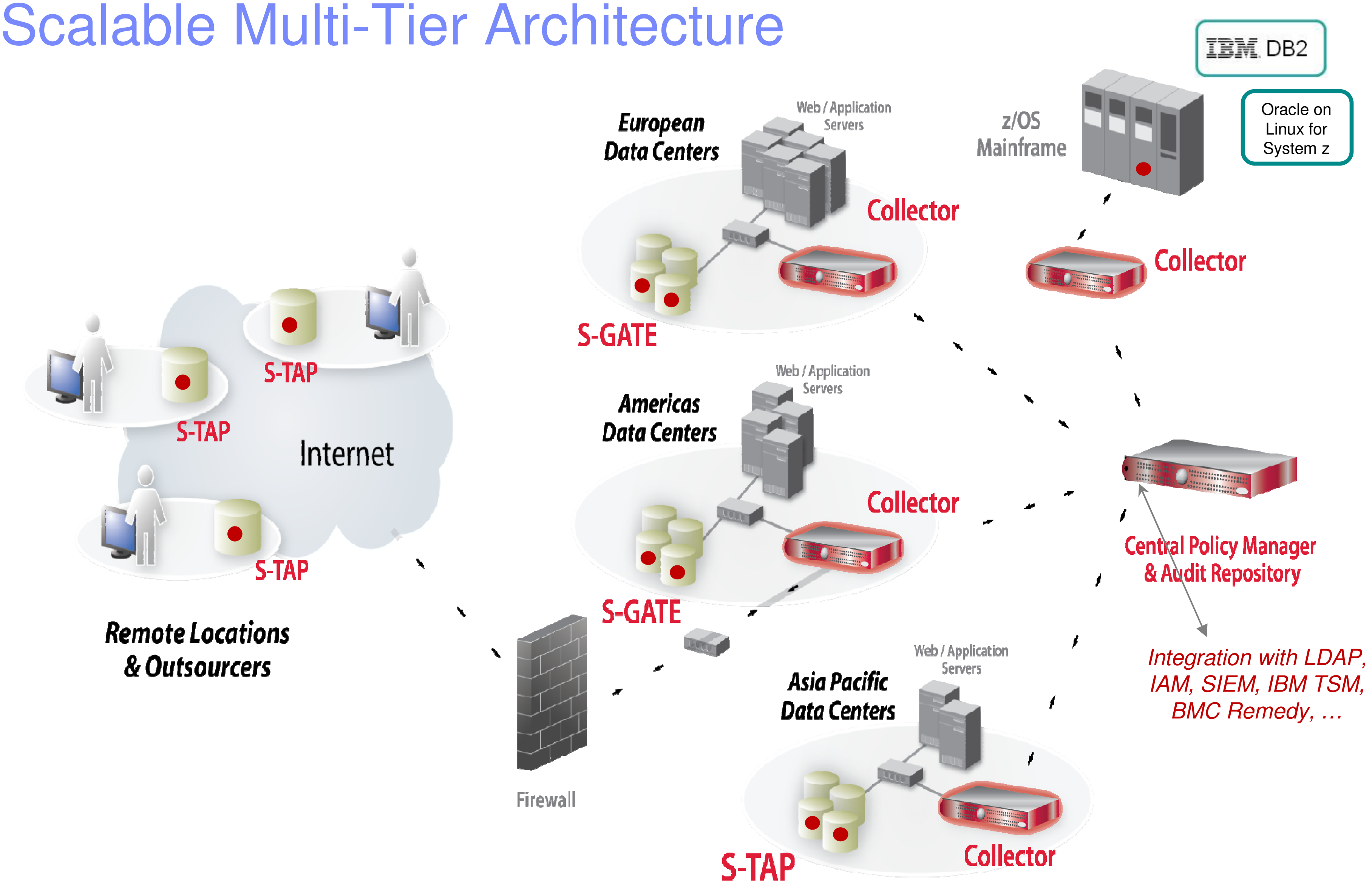




- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact
- No DBMS or application changes

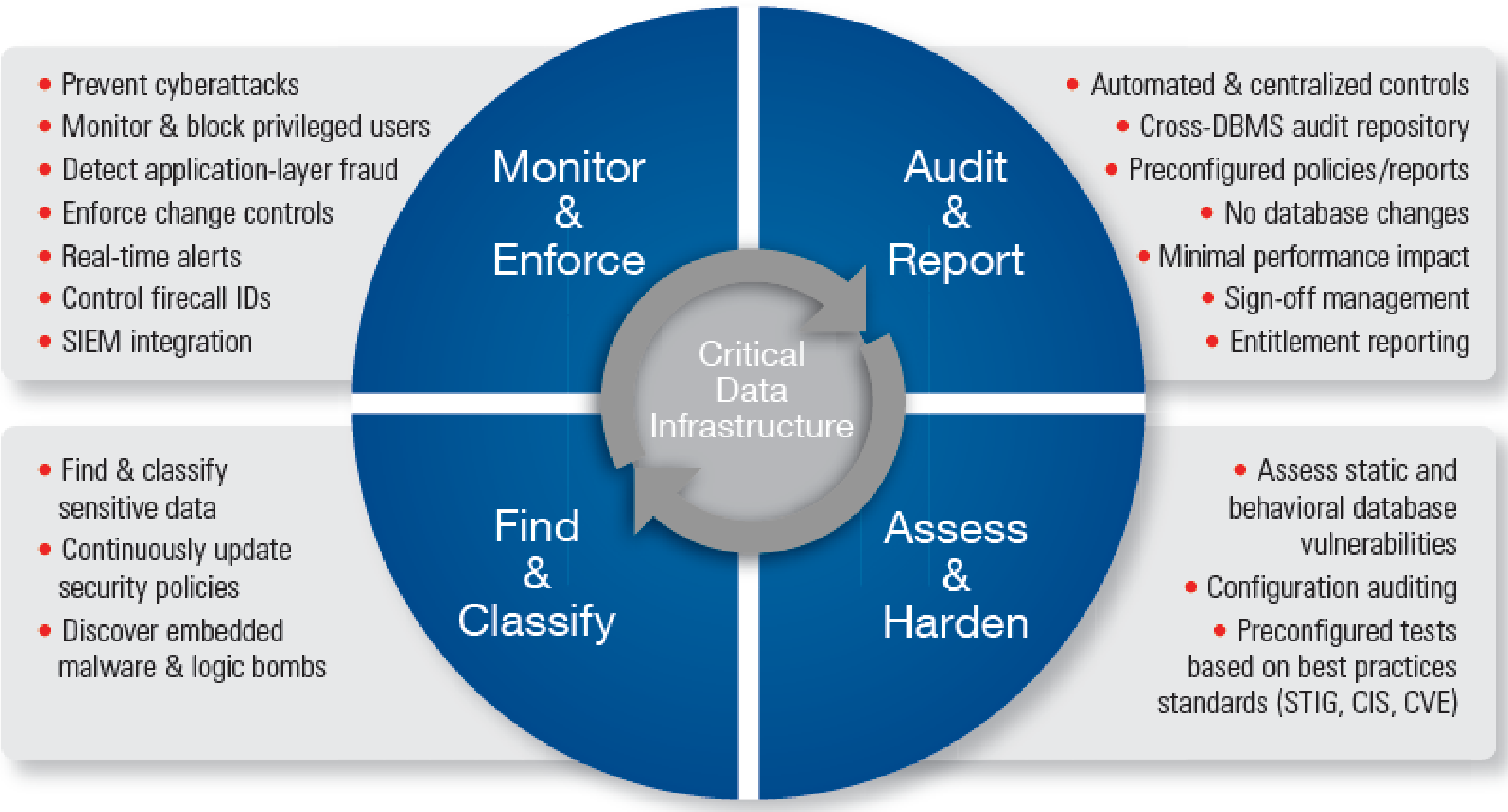
- Supports Separation of Duties
- Activity logs can’t be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

Scalable Multi-Tier Architecture


IBM DB2
Oracle on Linux for System z
European Data Centers
Web / Application Servers
z/OS Mainframe
Collector
Collector
S-GATE
S-TAP
S-TAP
Internet
S-TAP
Remote Locations & Outsourcers
Americas Data Centers
Web / Application Servers
Collector
S-GATE
Central Policy Manager & Audit Repository
Integration with LDAP, IAM, SIEM, IBM TSM, BMC Remedy, …
Firewall
Asia Pacific Data Centers
Web / Application Servers
S-TAP
Collector

Addressing the Full Lifecycle of Database Security

Real-time Database Security & Monitoring



Monitor & Enforce

- Prevent cyberattacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Control firecall IDs
- SIEM integration

Audit & Report

- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- No database changes
- Minimal performance impact
- Sign-off management
- Entitlement reporting

Find & Classify

- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

Assess & Harden

- Assess static and behavioral database vulnerabilities
- Configuration auditing
- Preconfigured tests based on best practices standards (STIG, CIS, CVE)

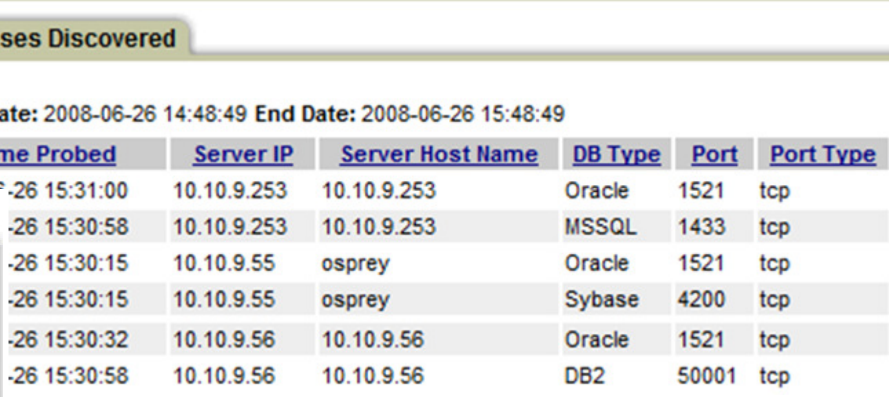
Critical Data Infrastructure

3 Step Method to Reduce Risk and Improve Operational Efficiencies

1. Discover
   - Discover databases on the network
   - Discover where sensitive data is located
2. Identify Risk
   - Perform an assessment to understand risk
   - Harden the database to eliminate unnecessary risk
3. Comply
   - Monitor database activity to verify security controls
   - Automate reporting for proper evidence in compliance process

1. Discover

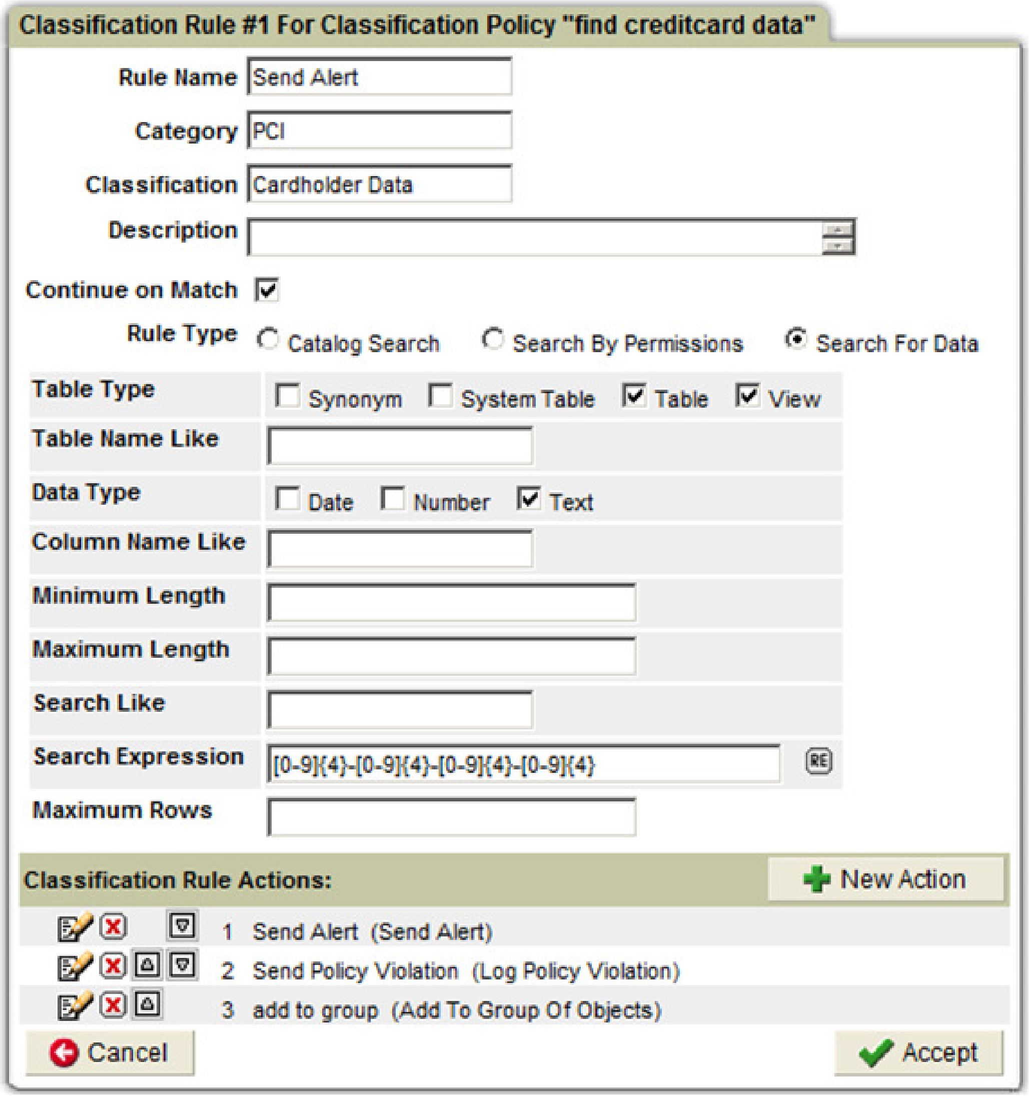
Find Cardholder Data



Databases Discovered

Start Date: 2008-06-26 14:48:49 **End Date:** 2008-06-26 15:48:49

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp
-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp
-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp
-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp
-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp
-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp



Classification Rule #1 For Classification Policy "find creditcard data"

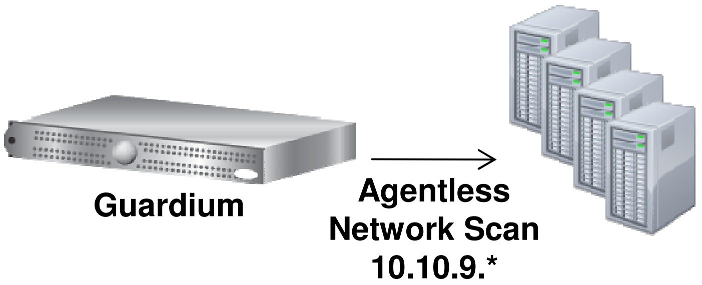
Rule Name	Send Alert
Category	PCI
Classification	Cardholder Data
Description	
Continue on Match	☑
Rule Type	○ Catalog Search ○ Search By Permissions ● Search For Data
Table Type	□ Synonym □ System Table ☑ Table ☑ View
Table Name Like	
Data Type	□ Date □ Number ☑ Text
Column Name Like	
Minimum Length	
Maximum Length	
Search Like	
Search Expression	[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}
Maximum Rows	

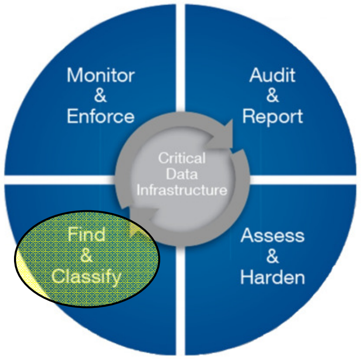
Classification Rule Actions:

1 Send Alert (Send Alert)

2 Send Policy Violation (Log Policy Violation)

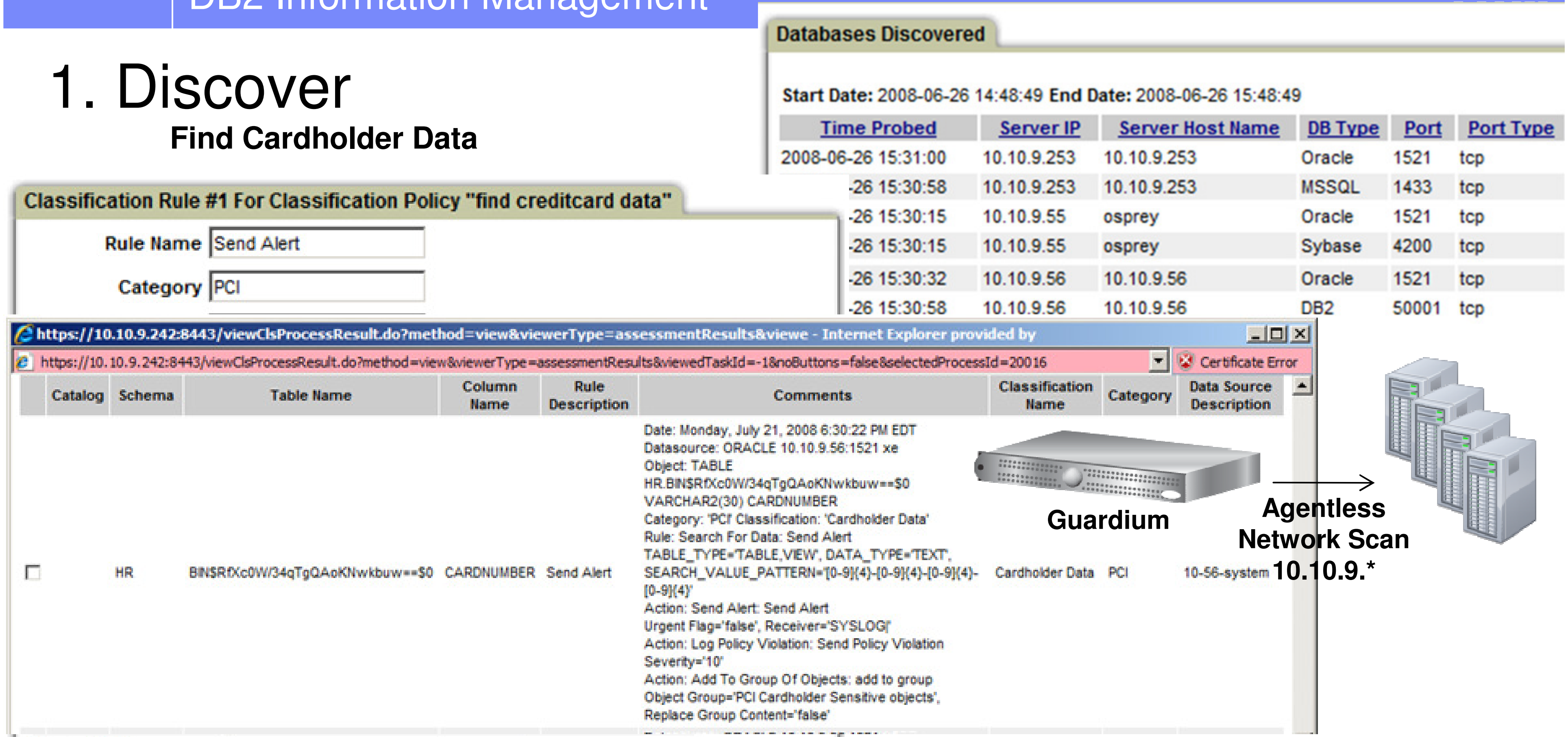
3 add to group (Add To Group Of Objects)





1. Discover

Find Cardholder Data



Databases Discovered

Start Date: 2008-06-26 14:48:49 **End Date:** 2008-06-26 15:48:49

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp
-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp
-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp
-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp
-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp
-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp

Classification Rule #1 For Classification Policy "find creditcard data"

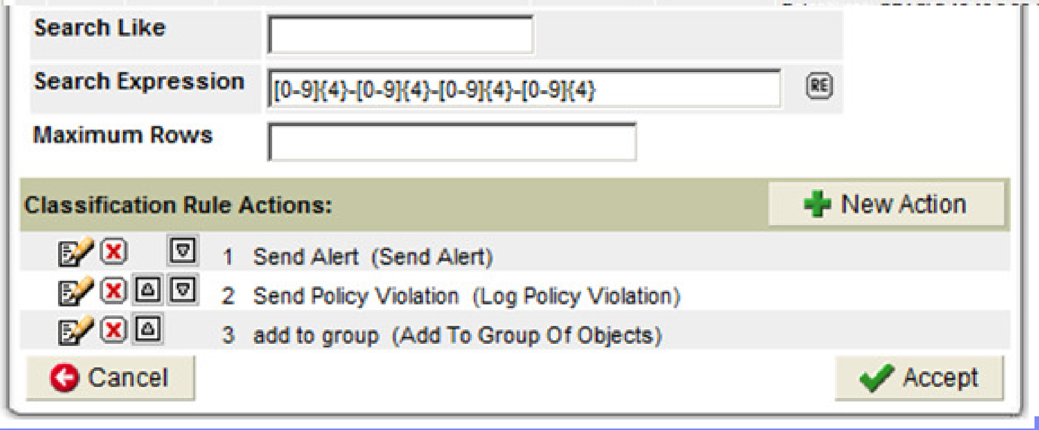
Rule Name	Send Alert
Category	PCI

https://10.10.9.242:8443/viewClsProcessResult.do?method=view&viewerType=assessmentResults&viewe - Internet Explorer provided by

https://10. 10.9.242:8443/viewClsProcessResult.do?method=view&viewerType=assessmentResults&viewedTaskId=-1&noButtons=false&selectedProcessId=20016

Certificate Error

	Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Data Source Description
☐		HR	BIN$RfXc0W/34qTgQAoKNwkbuw==$0	CARDNUMBER	Send Alert	Date: Monday, July 21, 2008 6:30:22 PM EDT Datasource: ORACLE 10.10.9.56:1521 xe Object: TABLE HR.BIN$RfXc0W/34qTgQAoKNwkbuw==$0 VARCHAR2(30) CARDNUMBER Category: 'PCI' Classification: 'Cardholder Data' Rule: Search For Data: Send Alert TABLE_TYPE='TABLE,VIEW', DATA_TYPE='TEXT', SEARCH_VALUE_PATTERN='[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}' Action: Send Alert: Send Alert Urgent Flag='false', Receiver='SYSLOG' Action: Log Policy Violation: Send Policy Violation Severity='10' Action: Add To Group Of Objects: add to group Object Group='PCI Cardholder Sensitive objects', Replace Group Content='false'	Cardholder Data	PCI	10-56-system



Search Like	
Search Expression	[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}
Maximum Rows	

Classification Rule Actions:

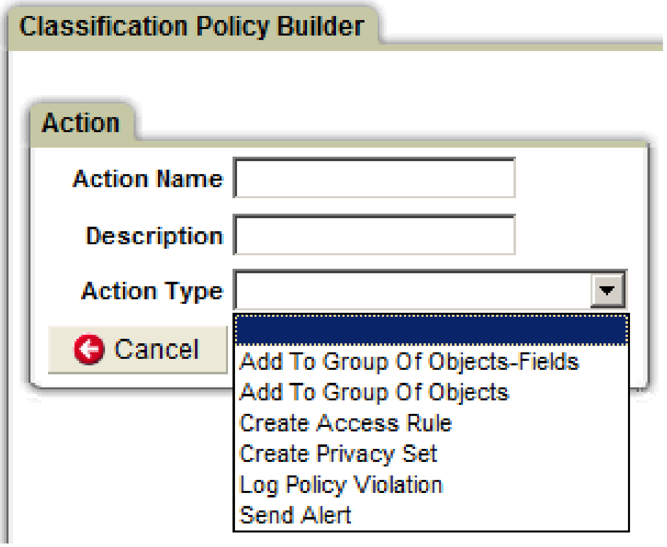
1 Send Alert (Send Alert)

2 Send Policy Violation (Log Policy Violation)

3 add to group (Add To Group Of Objects)

Monitor & Enforce
Audit & Report
Critical Data Infrastructure
Find & Classify
Assess & Harden

1. Discover



Classification Policy Builder

Action

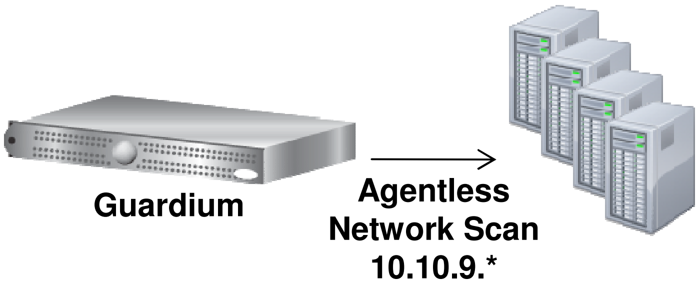
Action Name

Description

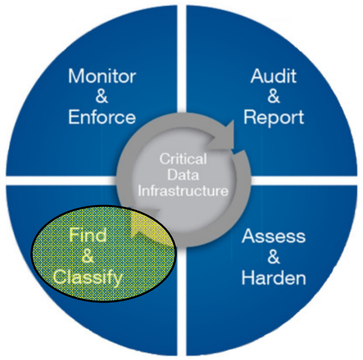
Action Type

Cancel

- Add To Group Of Objects-Fields
- Add To Group Of Objects
- Create Access Rule
- Create Privacy Set
- Log Policy Violation
- Send Alert

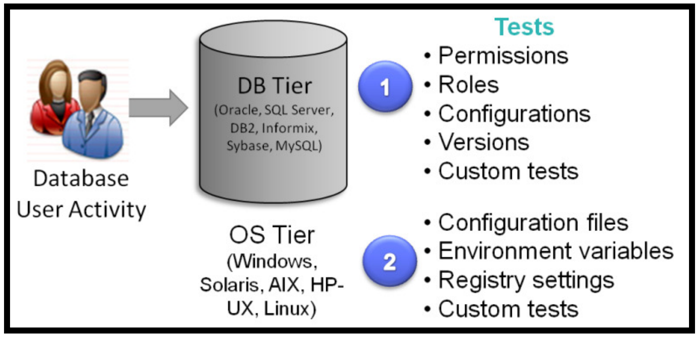


- Compliment Security Risk Management
  - Database discovery
  - Data discovery
  - Compliment other security devices and fill the database gap



2. Identify Risk

- Based on industry standards such as STIG and CIS benchmark tests.
- Complete coverage of the entire database environment.
  1. Observed Behavior
  2. Database
  3. Operating System



Database User Activity

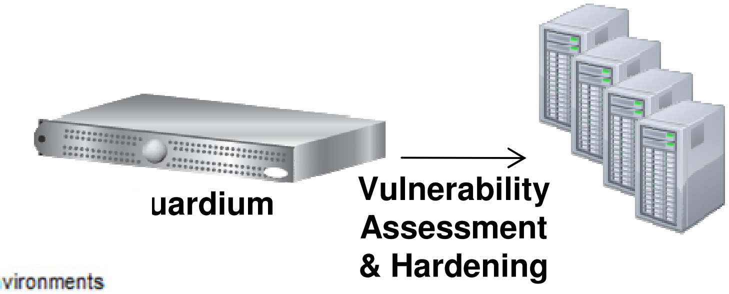
DB Tier
(Oracle, SQL Server, DB2, Informix, Sybase, MySQL)

OS Tier
(Windows, Solaris, AIX, HP-UX, Linux)

Tests

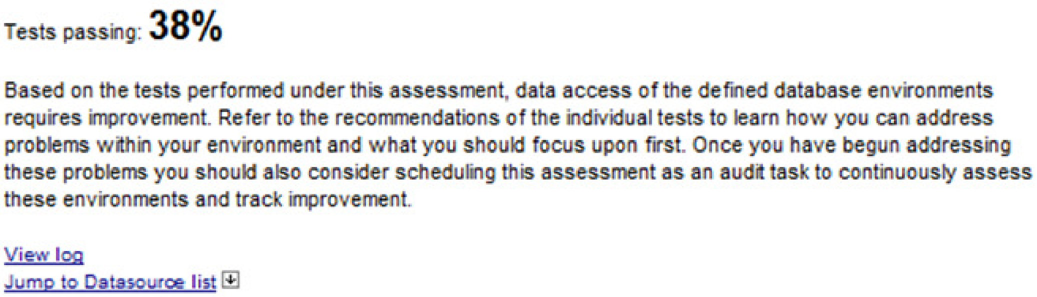
1
- Permissions
- Roles
- Configurations
- Versions
- Custom tests

2
- Configuration files
- Environment variables
- Registry settings
- Custom tests



uardium

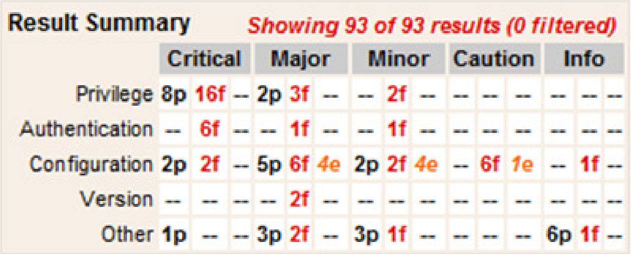
Vulnerability Assessment & Hardening



Tests passing: **38%**

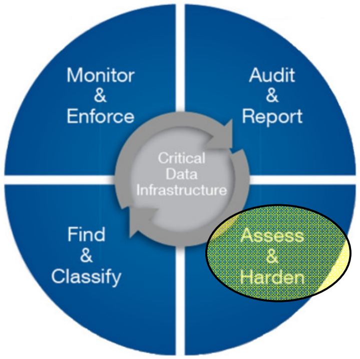
Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

View log
Jump to Datasource list

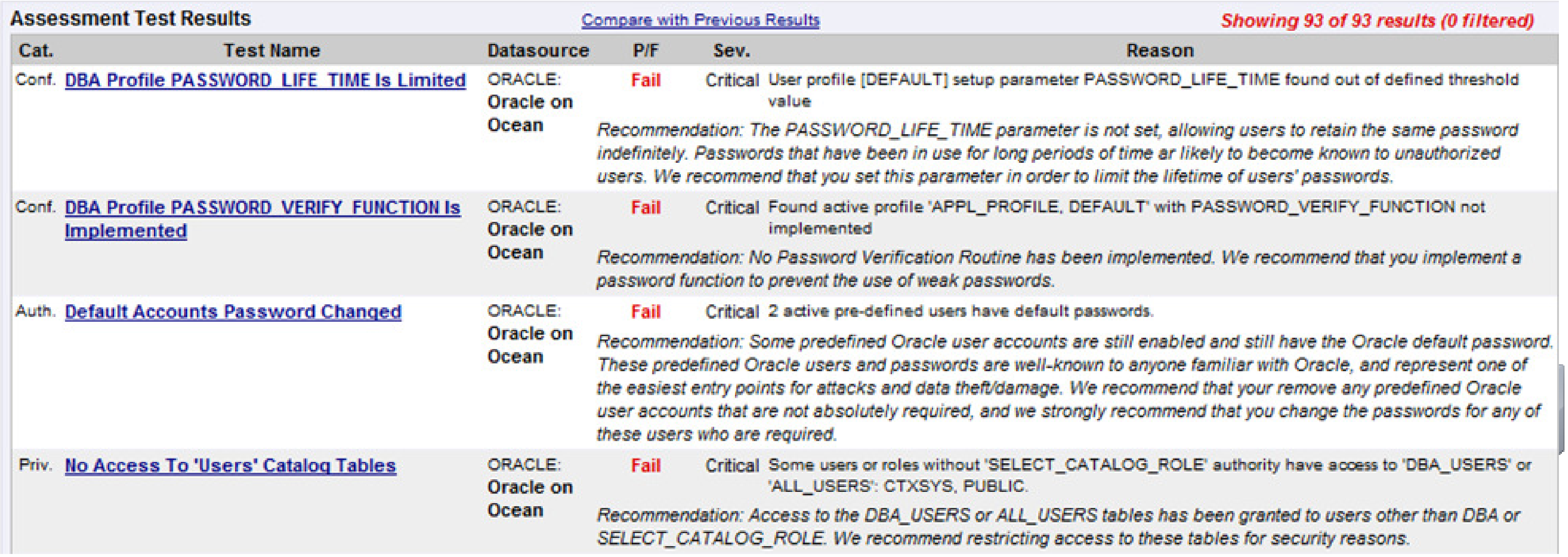


Result Summary *Showing 93 of 93 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	8p	16f	--	2p	3f	--	--	2f	--	--	--	--	--	--	--
Authentication	--	6f	--	--	1f	--	--	1f	--	--	--	--	--	--	--
Configuration	2p	2f	--	5p	6f	4e	2p	2f	4e	--	6f	1e	--	1f	--
Version	--	--	--	--	2f	--	--	--	--	--	--	--	--	--	--
Other	1p	--	--	3p	2f	--	3p	1f	--	--	--	--	6p	1f	--



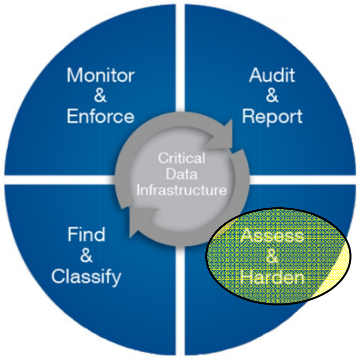
2. Identify Risk



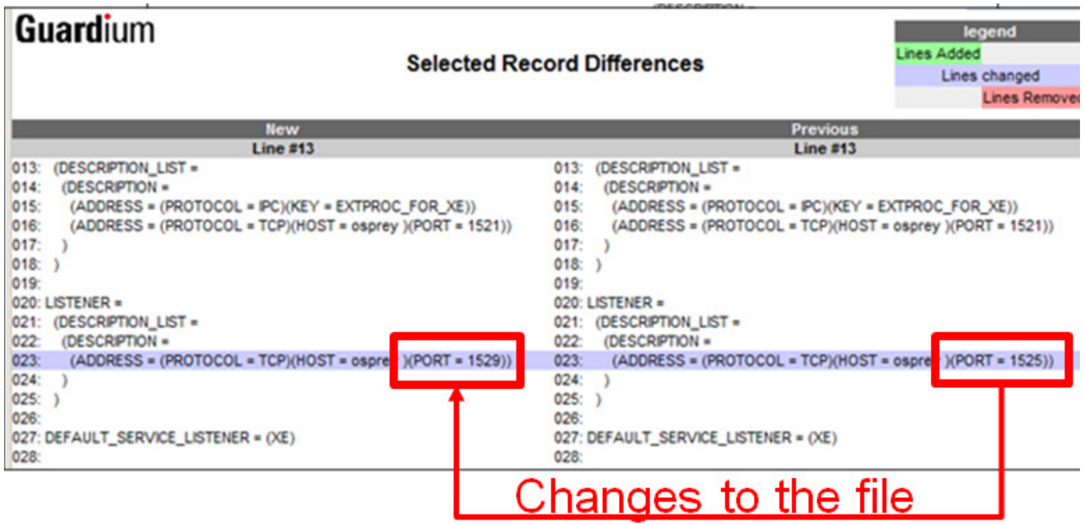
Assessment Test Results — Compare with Previous Results — *Showing 93 of 93 results (0 filtered)*

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Conf.	DBA Profile PASSWORD_LIFE_TIME Is Limited	ORACLE: Oracle on Ocean	Fail	Critical	User profile [DEFAULT] setup parameter PASSWORD_LIFE_TIME found out of defined threshold value *Recommendation: The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods of time ar likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords.*
Conf.	DBA Profile PASSWORD_VERIFY_FUNCTION Is Implemented	ORACLE: Oracle on Ocean	Fail	Critical	Found active profile 'APPL_PROFILE, DEFAULT' with PASSWORD_VERIFY_FUNCTION not implemented *Recommendation: No Password Verification Routine has been implemented. We recommend that you implement a password function to prevent the use of weak passwords.*
Auth.	Default Accounts Password Changed	ORACLE: Oracle on Ocean	Fail	Critical	2 active pre-defined users have default passwords. *Recommendation: Some predefined Oracle user accounts are still enabled and still have the Oracle default password. These predefined Oracle users and passwords are well-known to anyone familiar with Oracle, and represent one of the easiest entry points for attacks and data theft/damage. We recommend that your remove any predefined Oracle user accounts that are not absolutely required, and we strongly recommend that you change the passwords for any of these users who are required.*
Priv.	No Access To 'Users' Catalog Tables	ORACLE: Oracle on Ocean	Fail	Critical	Some users or roles without 'SELECT_CATALOG_ROLE' authority have access to 'DBA_USERS' or 'ALL_USERS': CTXSYS, PUBLIC. *Recommendation: Access to the DBA_USERS or ALL_USERS tables has been granted to users other than DBA or SELECT_CATALOG_ROLE. We recommend restricting access to these tables for security reasons.*

- Fill in the database assessment gap
  - Customize VA tests
  - Assessment review and remediation plan
    - Super users accessing sensitive data
    - Password Policy
    - Role and responsibility review
  - Change management process configuration management



2. Identify Risk



Guardium

Selected Record Differences

legend

- Lines Added
- Lines changed
- Lines Removed

New — **Line #13**

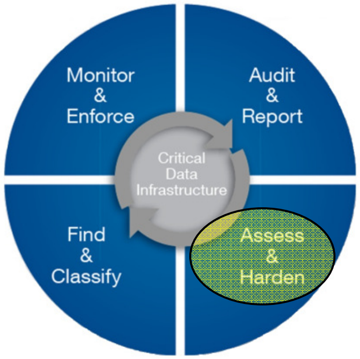
```
013:  (DESCRIPTION_LIST =
014:    (DESCRIPTION =
015:      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC_FOR_XE))
016:      (ADDRESS = (PROTOCOL = TCP)(HOST = osprey )(PORT = 1521))
017:    )
018:  )
019:
020: LISTENER =
021:  (DESCRIPTION_LIST =
022:    (DESCRIPTION =
023:      (ADDRESS = (PROTOCOL = TCP)(HOST = ospre )(PORT = 1529))
024:    )
025:  )
026:
027: DEFAULT_SERVICE_LISTENER = (XE)
028:
```

Previous — **Line #13**

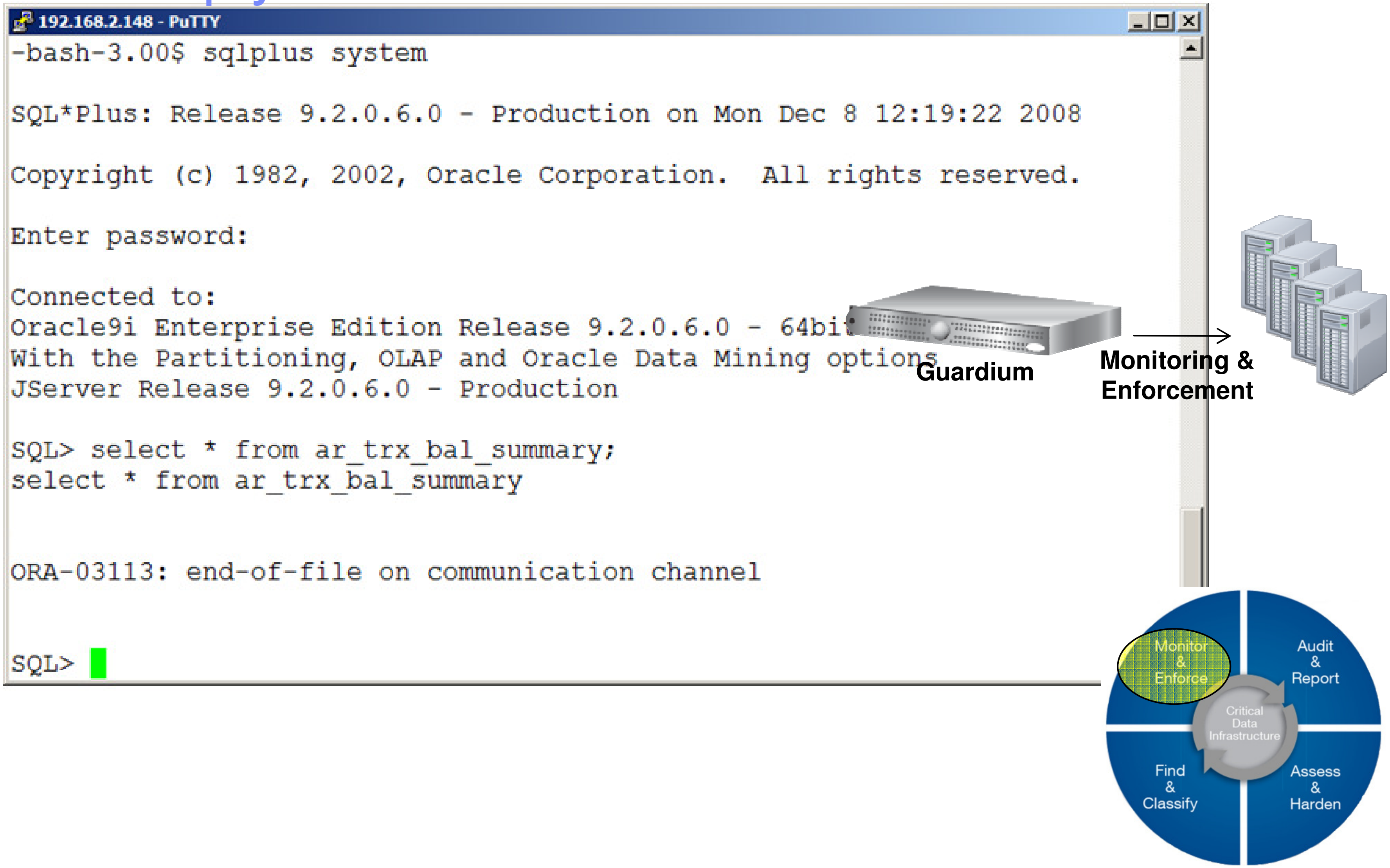
```
013:  (DESCRIPTION_LIST =
014:    (DESCRIPTION =
015:      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC_FOR_XE))
016:      (ADDRESS = (PROTOCOL = TCP)(HOST = osprey )(PORT = 1521))
017:    )
018:  )
019:
020: LISTENER =
021:  (DESCRIPTION_LIST =
022:    (DESCRIPTION =
023:      (ADDRESS = (PROTOCOL = TCP)(HOST = ospre )(PORT = 1525))
024:    )
025:  )
026:
027: DEFAULT_SERVICE_LISTENER = (XE)
028:
```

Changes to the file

- Fill in the database assessment gap
  - Customize VA tests
  - Assessment review and remediation plan
    - Super users accessing sensitive data
    - Password Policy
    - Role and responsibility review
  - Change management process configuration management

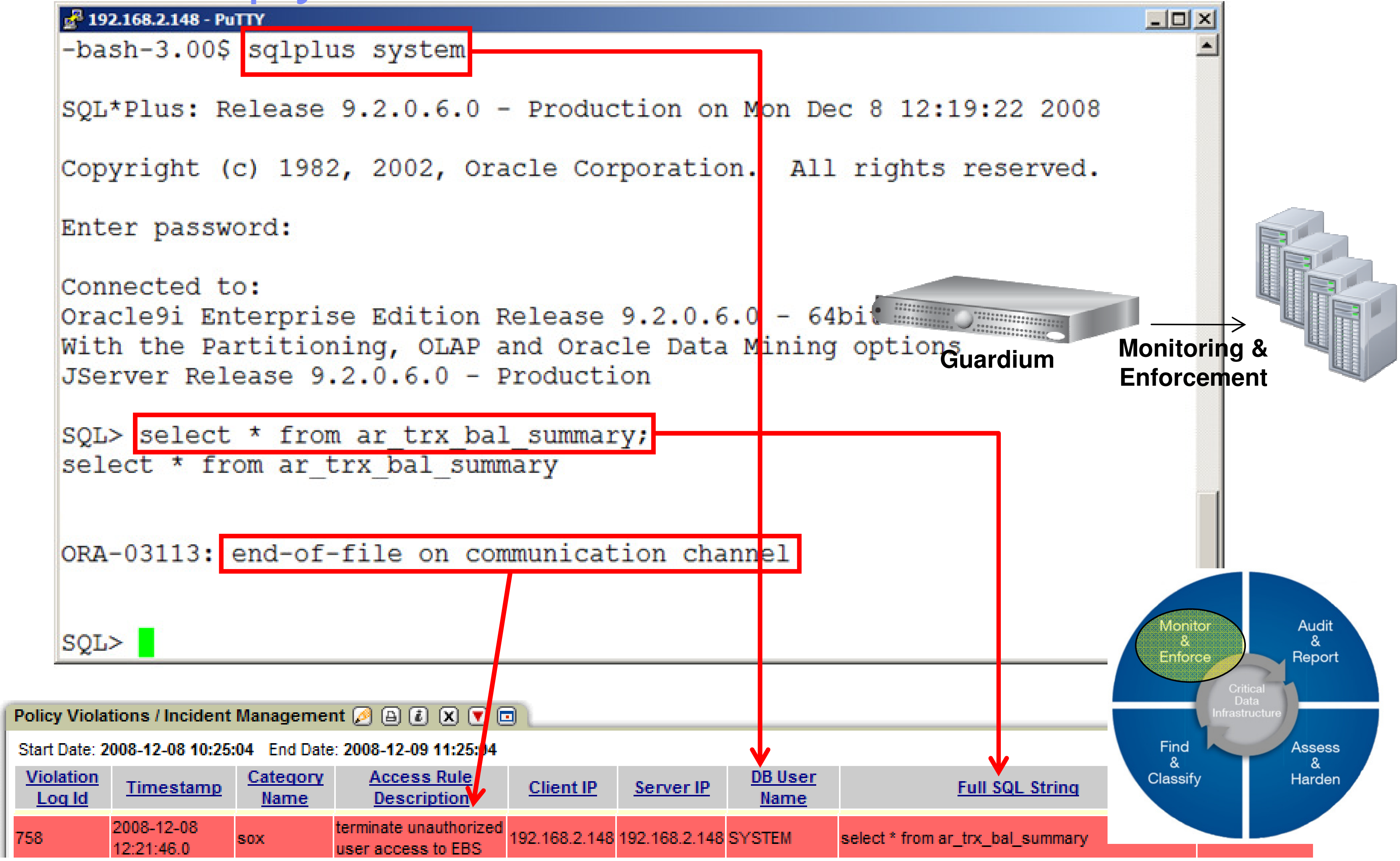


3. Comply



```
-bash-3.00$ sqlplus system

SQL*Plus: Release 9.2.0.6.0 - Production on Mon Dec 8 12:19:22 2008

Copyright (c) 1982, 2002, Oracle Corporation.  All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - 64bit
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production

SQL> select * from ar_trx_bal_summary;
select * from ar_trx_bal_summary


ORA-03113: end-of-file on communication channel


SQL> 
```

3. Comply



192.168.2.148 - PuTTY

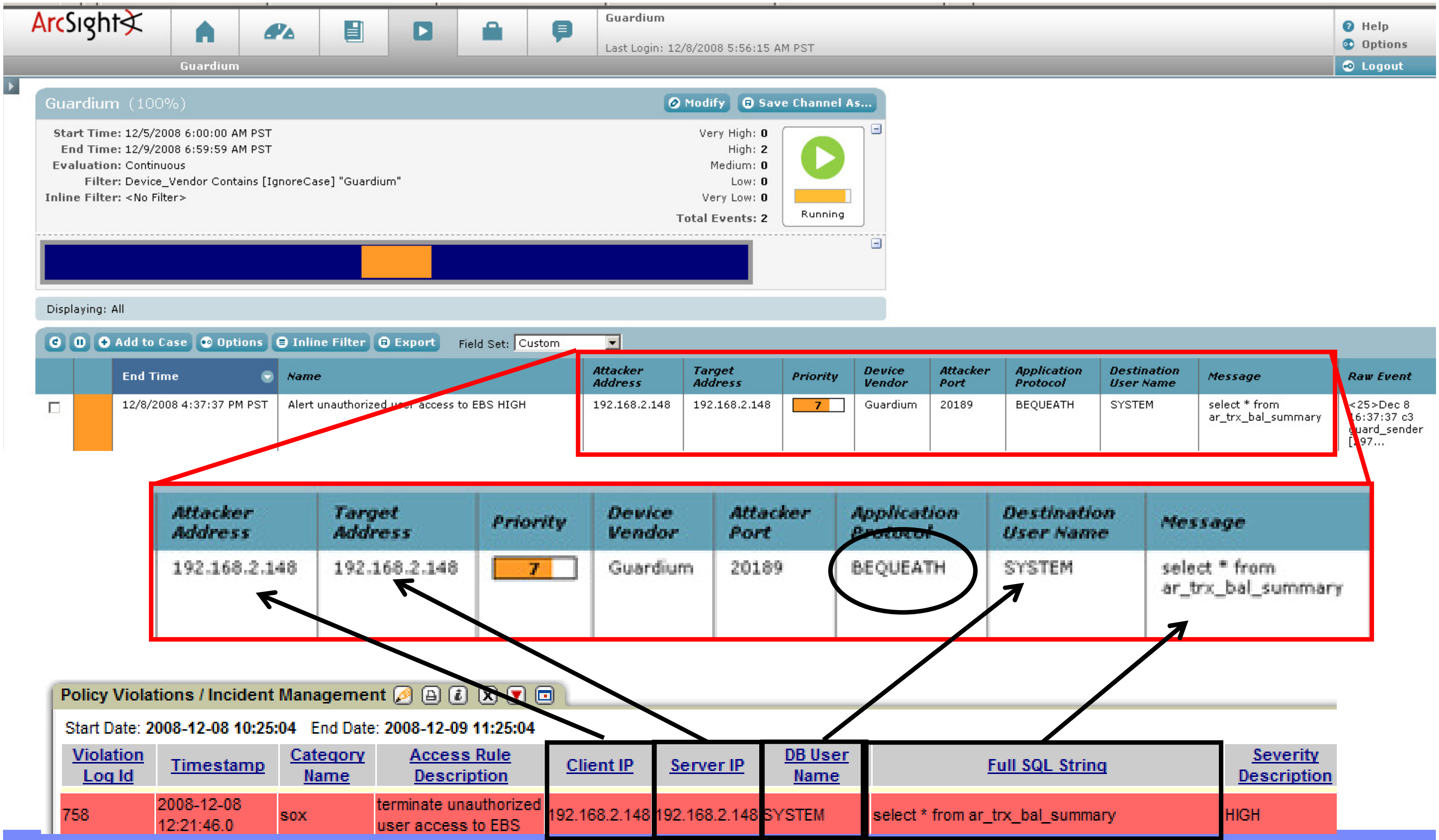
```
-bash-3.00$ sqlplus system

SQL*Plus: Release 9.2.0.6.0 - Production on Mon Dec 8 12:19:22 2008

Copyright (c) 1982, 2002, Oracle Corporation.  All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - 64bit
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production

SQL> select * from ar_trx_bal_summary;
select * from ar_trx_bal_summary


ORA-03113: end-of-file on communication channel


SQL>
```

Policy Violations / Incident Management

Start Date: 2008-12-08 10:25:04   End Date: 2008-12-09 11:25:04

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String
758	2008-12-08 12:21:46.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	SYSTEM	select * from ar_trx_bal_summary

Connection Terminated – Sent Event to SIEM



Guardium

Last Login: 12/8/2008 5:56:15 AM PST

Guardium (100%)

Start Time: 12/5/2008 6:00:00 AM PST
End Time: 12/9/2008 6:59:59 AM PST
Evaluation: Continuous
Filter: Device_Vendor Contains [IgnoreCase] "Guardium"
Inline Filter: <No Filter>

Very High:	**0**
High:	**2**
Medium:	**0**
Low:	**0**
Very Low:	**0**
Total Events:	**2**

Displaying: All

Field Set: Custom

End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Attacker Port	Application Protocol	Destination User Name	Message	Raw Event
12/8/2008 4:37:37 PM PST	Alert unauthorized user access to EBS HIGH	192.168.2.148	192.168.2.148	7	Guardium	20189	BEQUEATH	SYSTEM	select * from ar_trx_bal_summary	<25>Dec 8 16:37:37 c3 guard_sender [397...

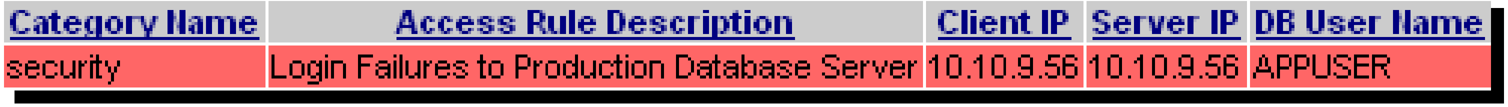
Attacker Address	Target Address	Priority	Device Vendor	Attacker Port	Application Protocol	Destination User Name	Message
192.168.2.148	192.168.2.148	7	Guardium	20189	BEQUEATH	SYSTEM	select * from ar_trx_bal_summary

Policy Violations / Incident Management

Start Date: **2008-12-08 10:25:04** End Date: **2008-12-09 11:25:04**

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
758	2008-12-08 12:21:46.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	SYSTEM	select * from ar_trx_bal_summary	HIGH

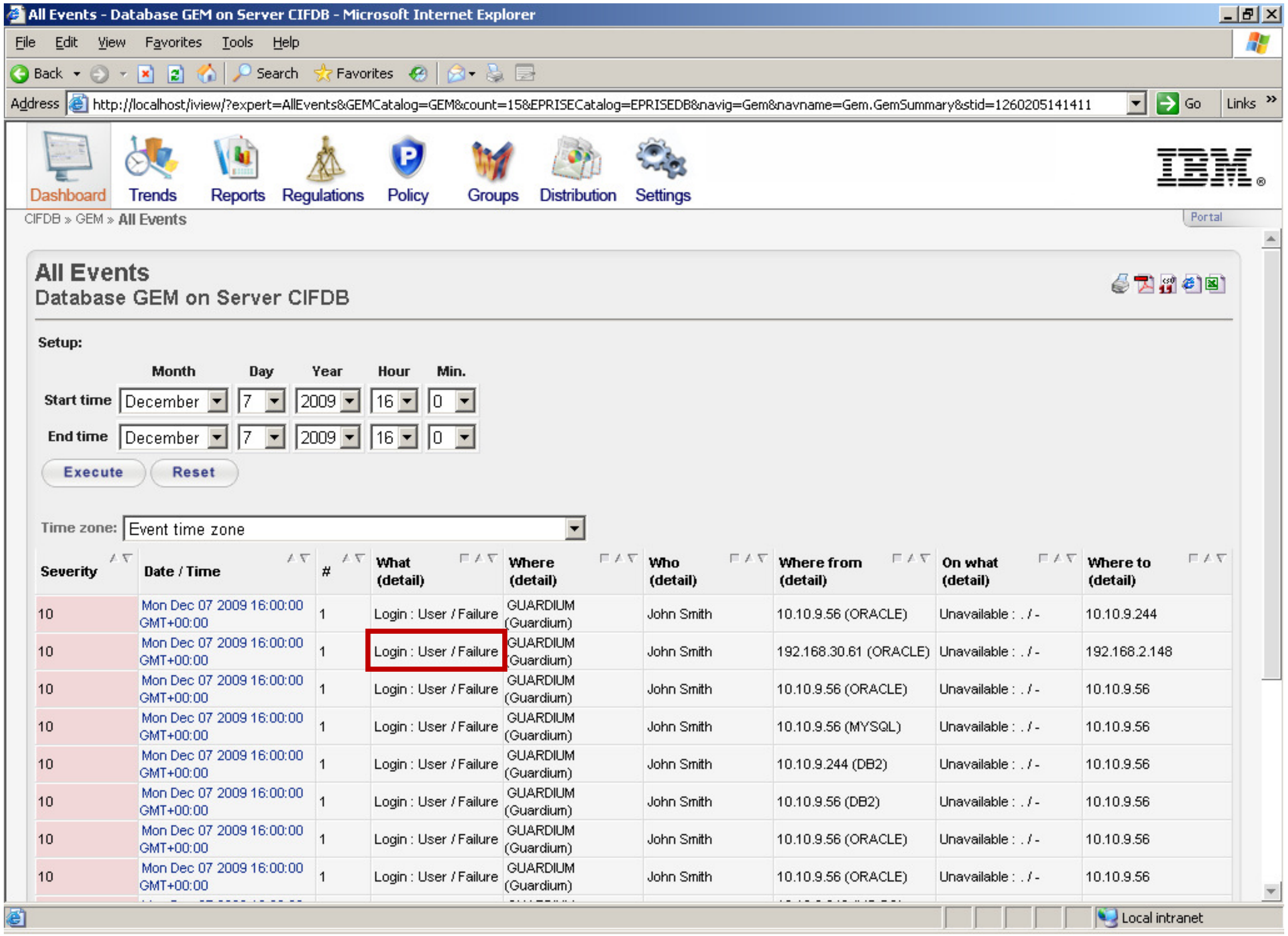
Integrating with IBM TSIEM



Category Name	Access Rule Description	Client IP	Server IP	DB User Name
security	Login Failures to Production Database Server	10.10.9.56	10.10.9.56	APPUSER

Policy violation in Guardium system

Events in IBM SIEM



All Events - Database GEM on Server CIFDB - Microsoft Internet Explorer

Address http://localhost/iview/?expert=AllEvents&GEMCatalog=GEM&count=15&EPRISECatalog=EPRISEDB&navig=Gem&navname=Gem.GemSummary&stid=1260205141411

CIFDB » GEM » All Events

All Events
Database GEM on Server CIFDB

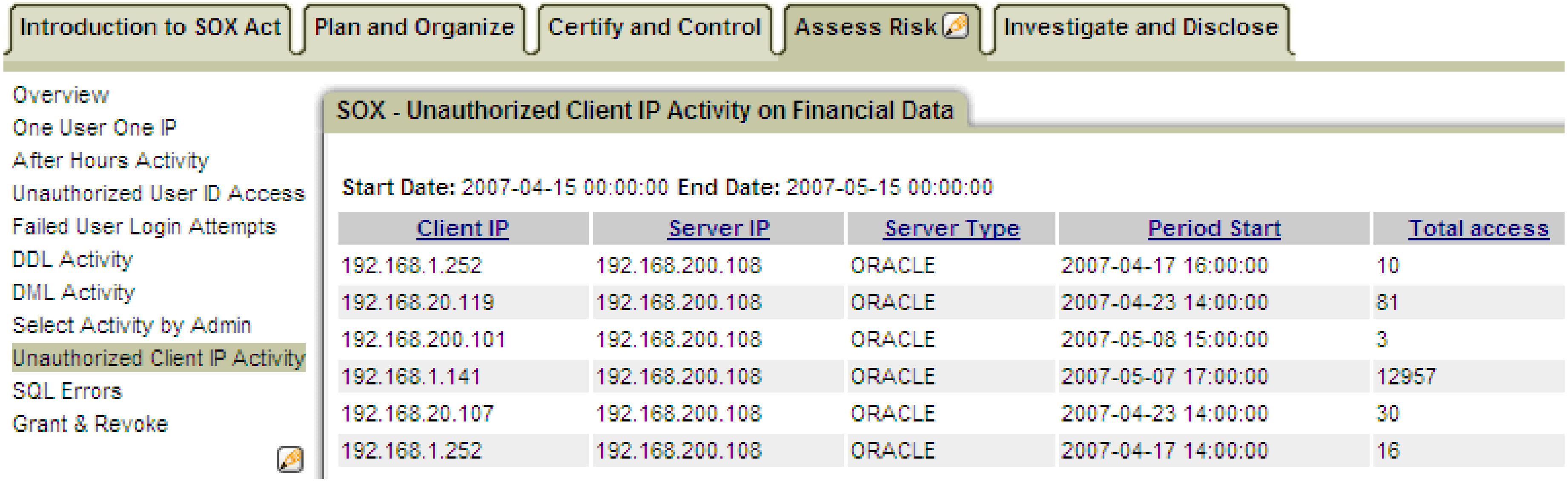
Setup:

	Month	Day	Year	Hour	Min.
Start time	December	7	2009	16	0
End time	December	7	2009	16	0

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : . / -	10.10.9.244
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	192.168.30.61 (ORACLE)	Unavailable : . / -	192.168.2.148
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (MYSQL)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.244 (DB2)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (DB2)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : . / -	10.10.9.56

3. Comply

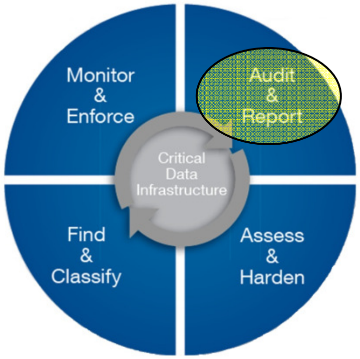


SOX - Unauthorized Client IP Activity on Financial Data

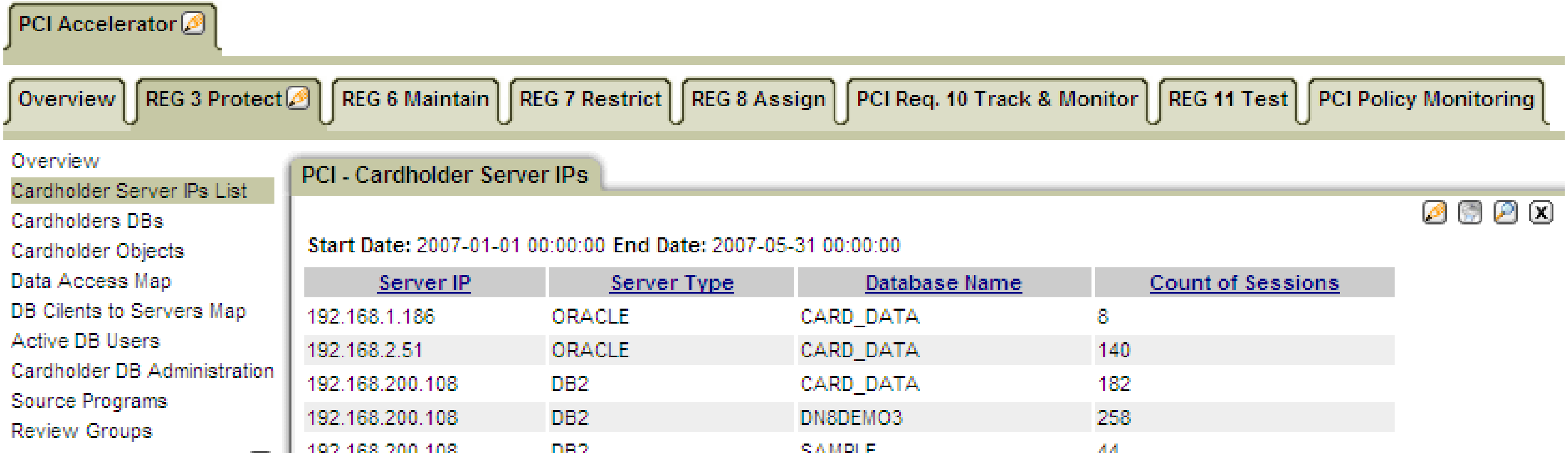
Start Date: 2007-04-15 00:00:00 **End Date:** 2007-05-15 00:00:00

Client IP	Server IP	Server Type	Period Start	Total access
192.168.1.252	192.168.200.108	ORACLE	2007-04-17 16:00:00	10
192.168.20.119	192.168.200.108	ORACLE	2007-04-23 14:00:00	81
192.168.200.101	192.168.200.108	ORACLE	2007-05-08 15:00:00	3
192.168.1.141	192.168.200.108	ORACLE	2007-05-07 17:00:00	12957
192.168.20.107	192.168.200.108	ORACLE	2007-04-23 14:00:00	30
192.168.1.252	192.168.200.108	ORACLE	2007-04-17 14:00:00	16

- PCI & SOX accelerators
  - Application monitoring (SAP, EBS, Cognos, Peoplesoft, etc)
  - Authorized application access only



3. Comply

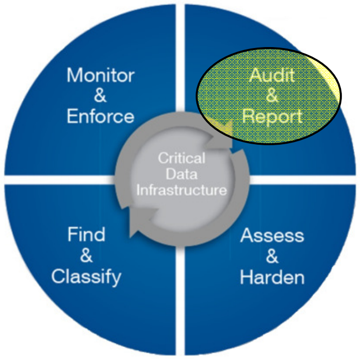


PCI - Cardholder Server IPs

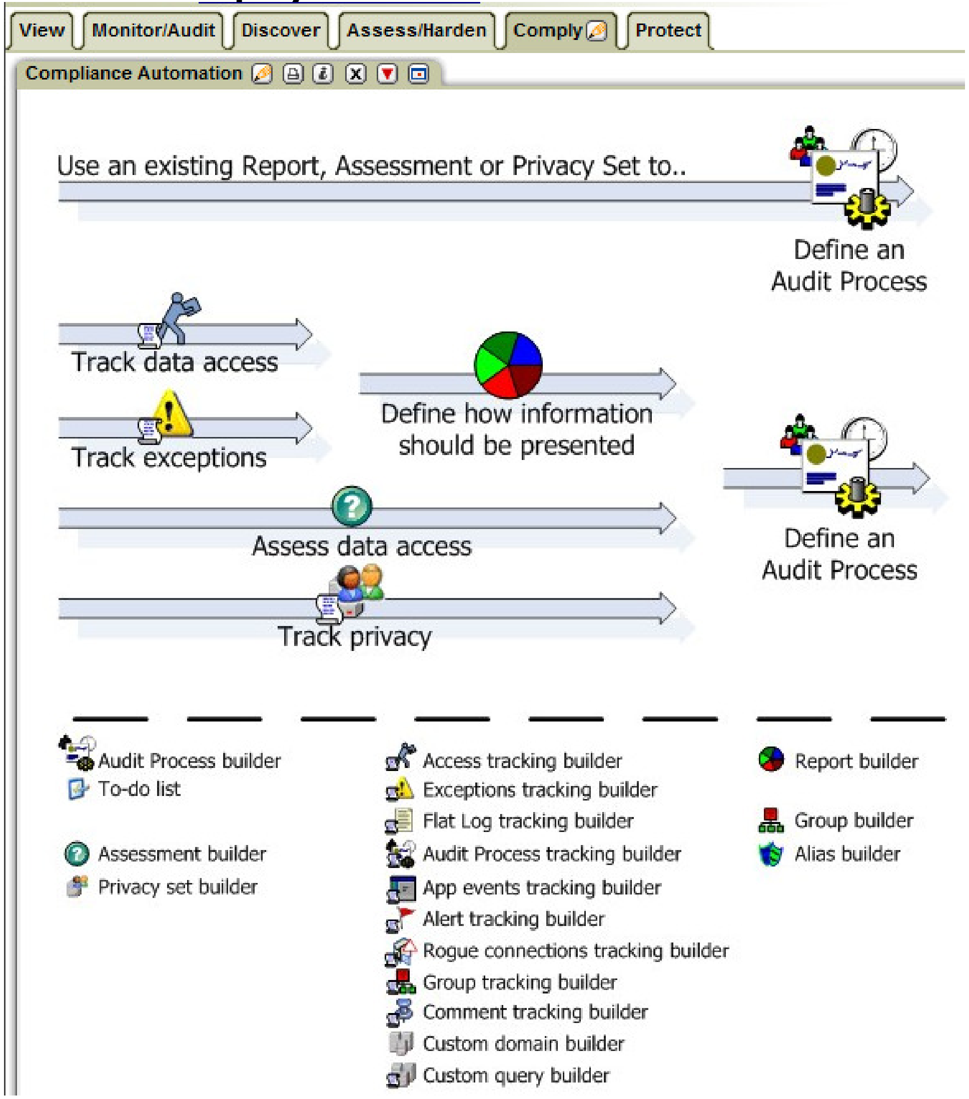
Start Date: 2007-01-01 00:00:00 **End Date:** 2007-05-31 00:00:00

Server IP	Server Type	Database Name	Count of Sessions
192.168.1.186	ORACLE	CARD_DATA	8
192.168.2.51	ORACLE	CARD_DATA	140
192.168.200.108	DB2	CARD_DATA	182
192.168.200.108	DB2	DN8DEMO3	258
192.168.200.108	DB2	SAMPLE	44

- PCI & SOX accelerators
  - Application monitoring (SAP, EBS, Cognos, Peoplesoft, etc)
  - Authorized application access only



3. Comply



Use an existing Report, Assessment or Privacy Set to..

Define an Audit Process

Track data access

Track exceptions

Define how information should be presented

Assess data access

Track privacy

Define an Audit Process

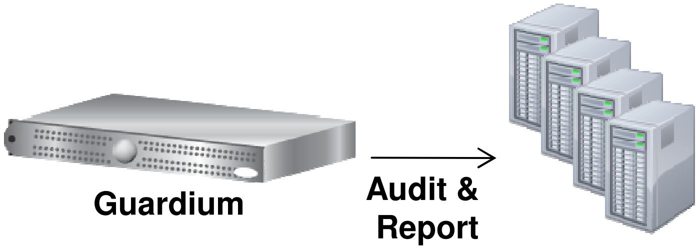
Audit Process builder
To-do list

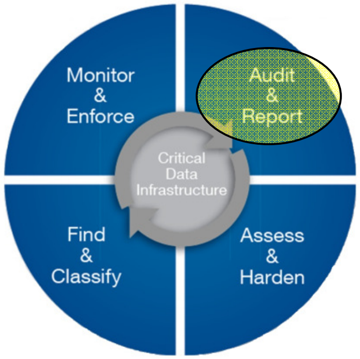
Assessment builder
Privacy set builder

Access tracking builder
Exceptions tracking builder
Flat Log tracking builder
Audit Process tracking builder
App events tracking builder
Alert tracking builder
Rogue connections tracking builder
Group tracking builder
Comment tracking builder
Custom domain builder
Custom query builder

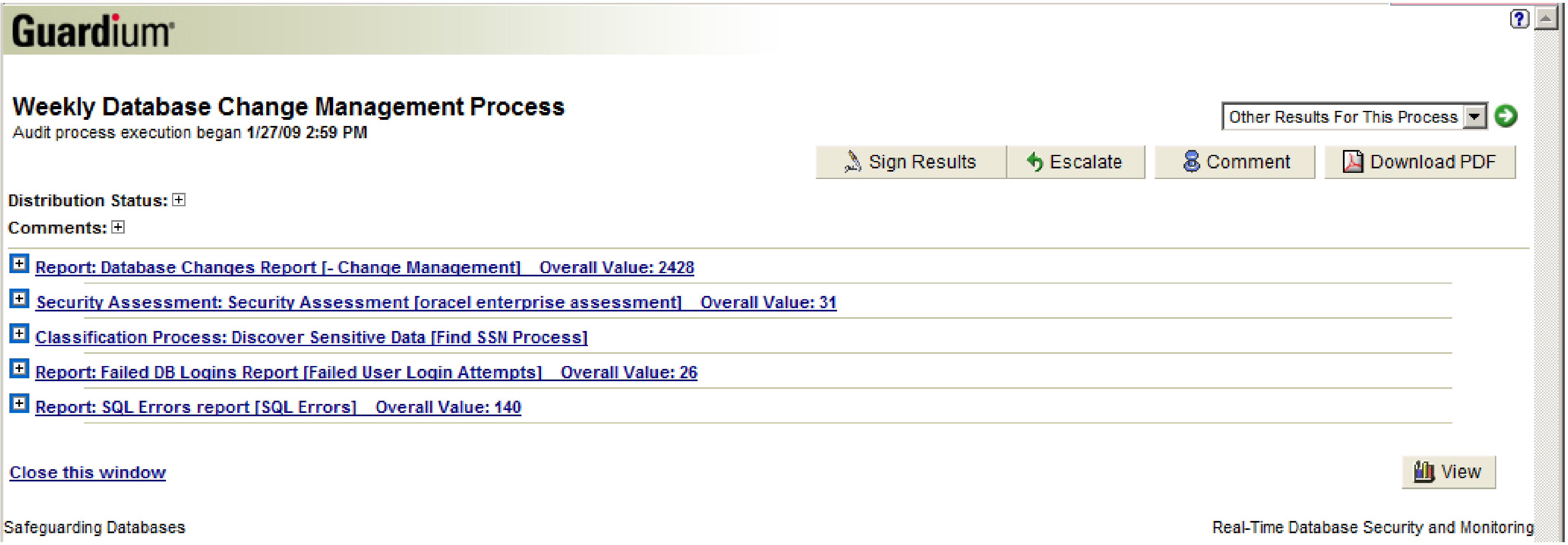
Report builder

Group builder
Alias builder





3. Comply



Guardium

Weekly Database Change Management Process

Audit process execution began 1/27/09 2:59 PM

Distribution Status: ⊞

Comments: ⊞

⊞ Report: Database Changes Report [- Change Management] Overall Value: 2428

⊞ Security Assessment: Security Assessment [oracel enterprise assessment] Overall Value: 31

⊞ Classification Process: Discover Sensitive Data [Find SSN Process]

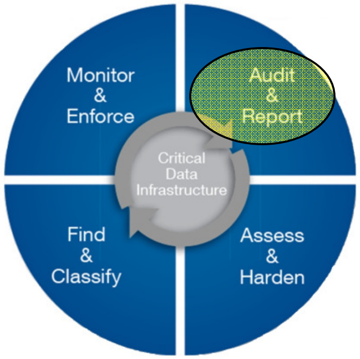
⊞ Report: Failed DB Logins Report [Failed User Login Attempts] Overall Value: 26

⊞ Report: SQL Errors report [SQL Errors] Overall Value: 140

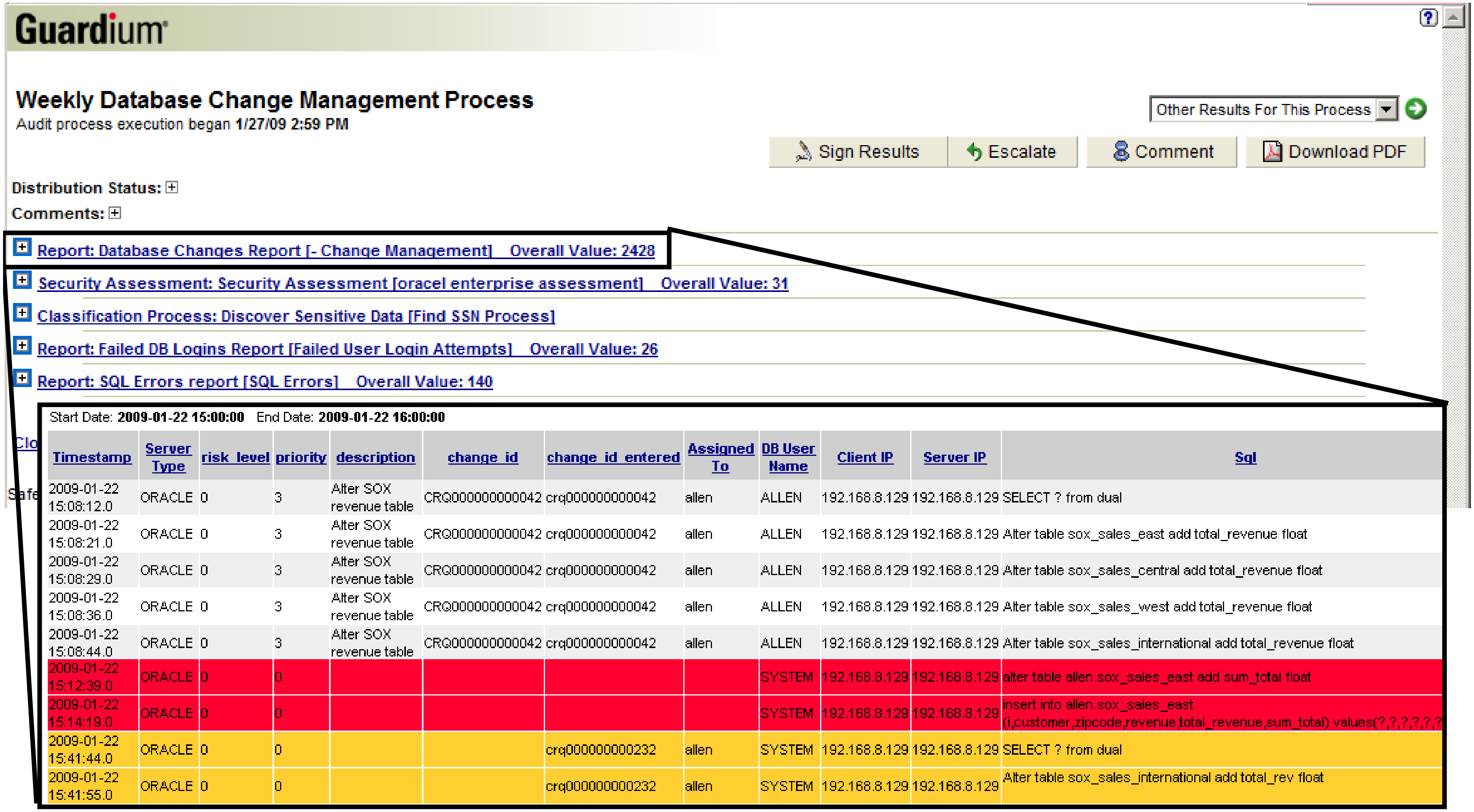
Close this window

Safeguarding Databases

Real-Time Database Security and Monitoring



3. Comply



Weekly Database Change Management Process

Audit process execution began 1/27/09 2:59 PM

Distribution Status: ⊞

Comments: ⊞

⊞ Report: Database Changes Report [- Change Management]   Overall Value: 2428

⊞ Security Assessment: Security Assessment [oracel enterprise assessment]   Overall Value: 31

⊞ Classification Process: Discover Sensitive Data [Find SSN Process]

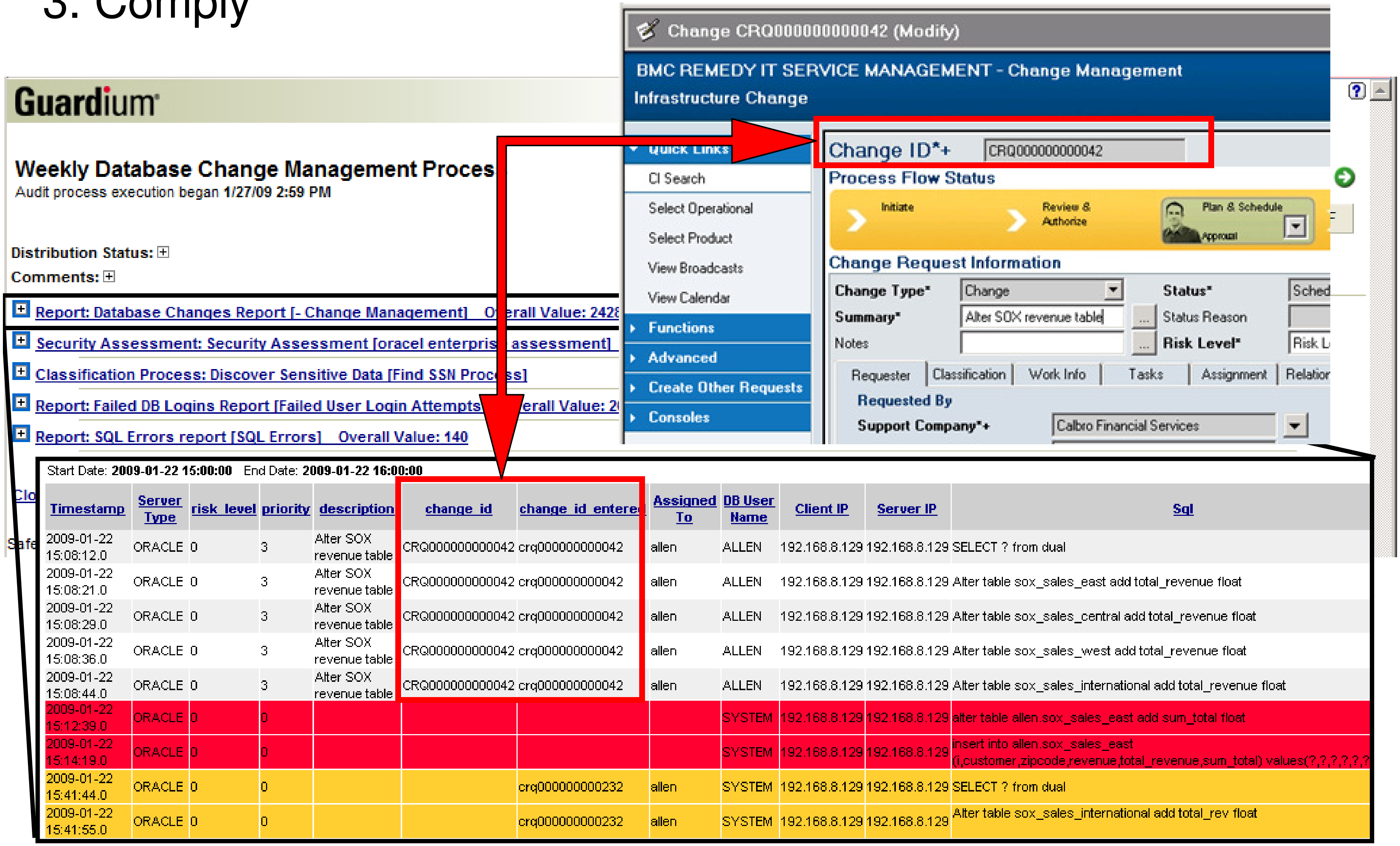
⊞ Report: Failed DB Logins Report [Failed User Login Attempts]   Overall Value: 26

⊞ Report: SQL Errors report [SQL Errors]   Overall Value: 140

Start Date: **2009-01-22 15:00:00**   End Date: **2009-01-22 16:00:00**

Timestamp	Server Type	risk_level	priority	description	change_id	change_id_entered	Assigned To	DB User Name	Client IP	Server IP	Sql
2009-01-22 15:08:12.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (i,customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?,?
2009-01-22 15:41:44.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:41:55.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float

3. Comply



Change CRQ000000000042 (Modify)

BMC REMEDY IT SERVICE MANAGEMENT - Change Management

Infrastructure Change

Change ID*+ CRQ000000000042

Process Flow Status

Change Request Information

Change Type* Change
Status* Sched
Summary* Alter SOX revenue table
Status Reason
Notes
Risk Level* Risk L

Requested By

Support Company*+ Calbro Financial Services

Guardium

Weekly Database Change Management Proces

Audit process execution began 1/27/09 2:59 PM

Distribution Status: ⊞

Comments: ⊞

⊞ Report: Database Changes Report [- Change Management]   Overall Value: 2428

⊞ Security Assessment: Security Assessment [oracel enterprise assessment]

⊞ Classification Process: Discover Sensitive Data [Find SSN Process]

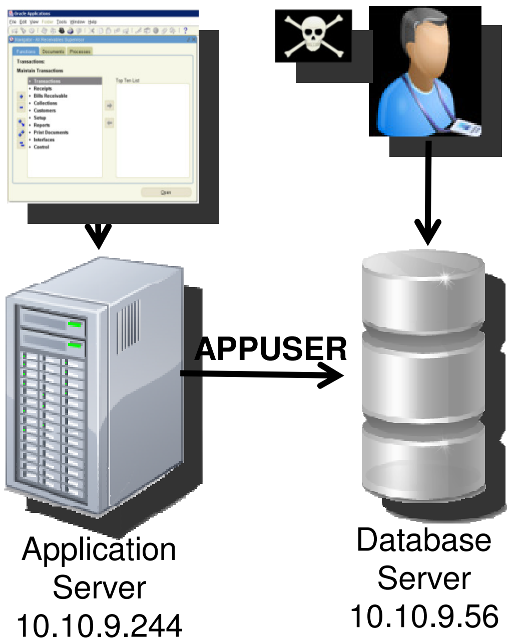
⊞ Report: Failed DB Logins Report [Failed User Login Attempts] Overall Value: 2

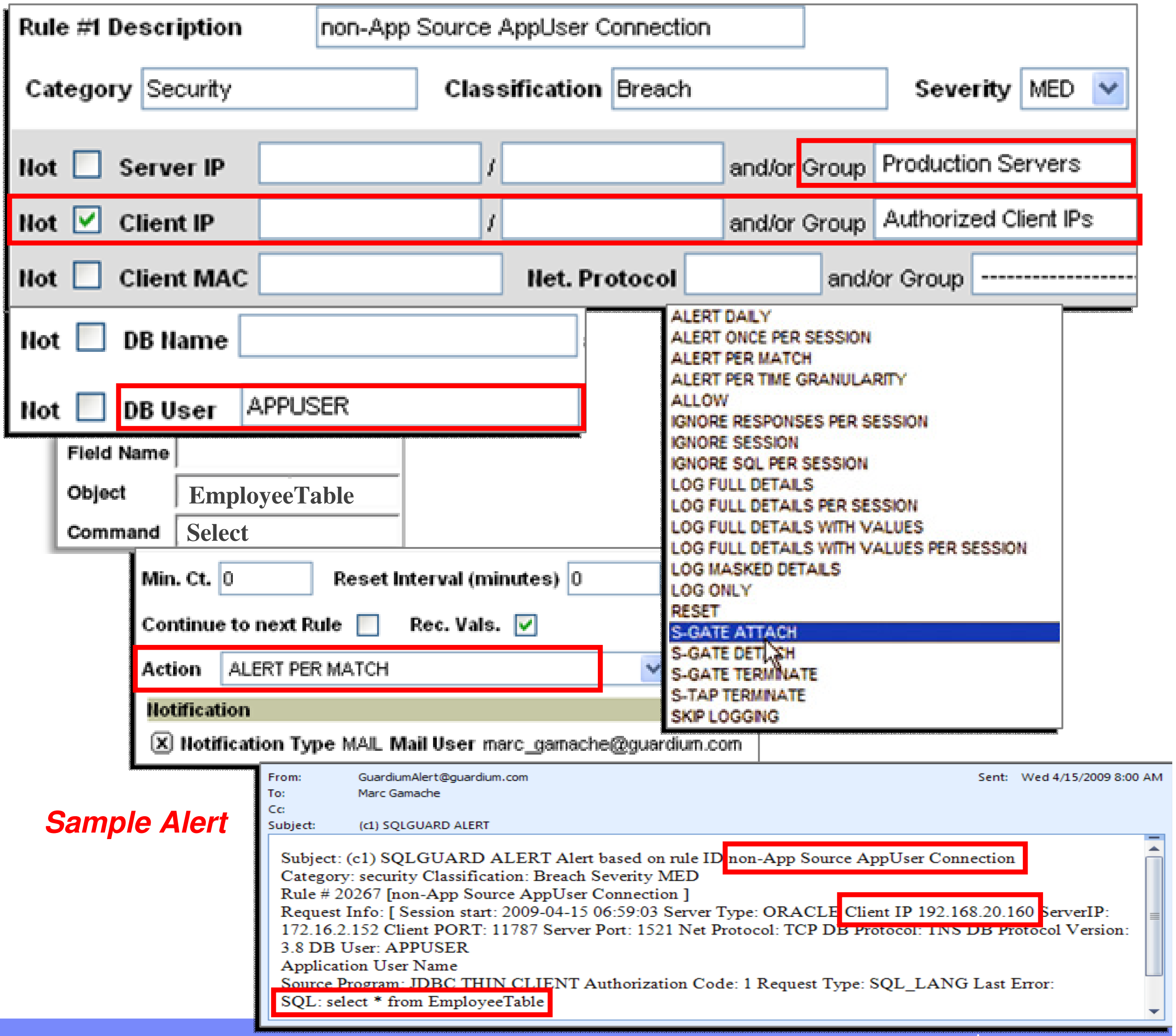
⊞ Report: SQL Errors report [SQL Errors]   Overall Value: 140

Start Date: **2009-01-22 15:00:00**   End Date: **2009-01-22 16:00:00**

Timestamp	Server Type	risk_level	priority	description	change_id	change_id_entered	Assigned To	DB User Name	Client IP	Server IP	Sql
2009-01-22 15:08:12.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (i,customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?,?
2009-01-22 15:41:44.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:41:55.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float

Granular Policies with Real-Time Alerts & Preventive Controls





Rule #1 Description: non-App Source AppUser Connection

Category: Security — Classification: Breach — Severity: MED

☐ Not Server IP: / — and/or Group: Production Servers

☑ Not Client IP: / — and/or Group: Authorized Client IPs

☐ Not Client MAC: — Net. Protocol: — and/or Group: ------------------

☐ Not DB Name:

☐ Not DB User: APPUSER

Field Name:

Object: EmployeeTable

Command: Select

Min. Ct. 0 — Reset Interval (minutes) 0

Continue to next Rule ☐ — Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

☒ Notification Type MAIL Mail User marc_gamache@guardium.com

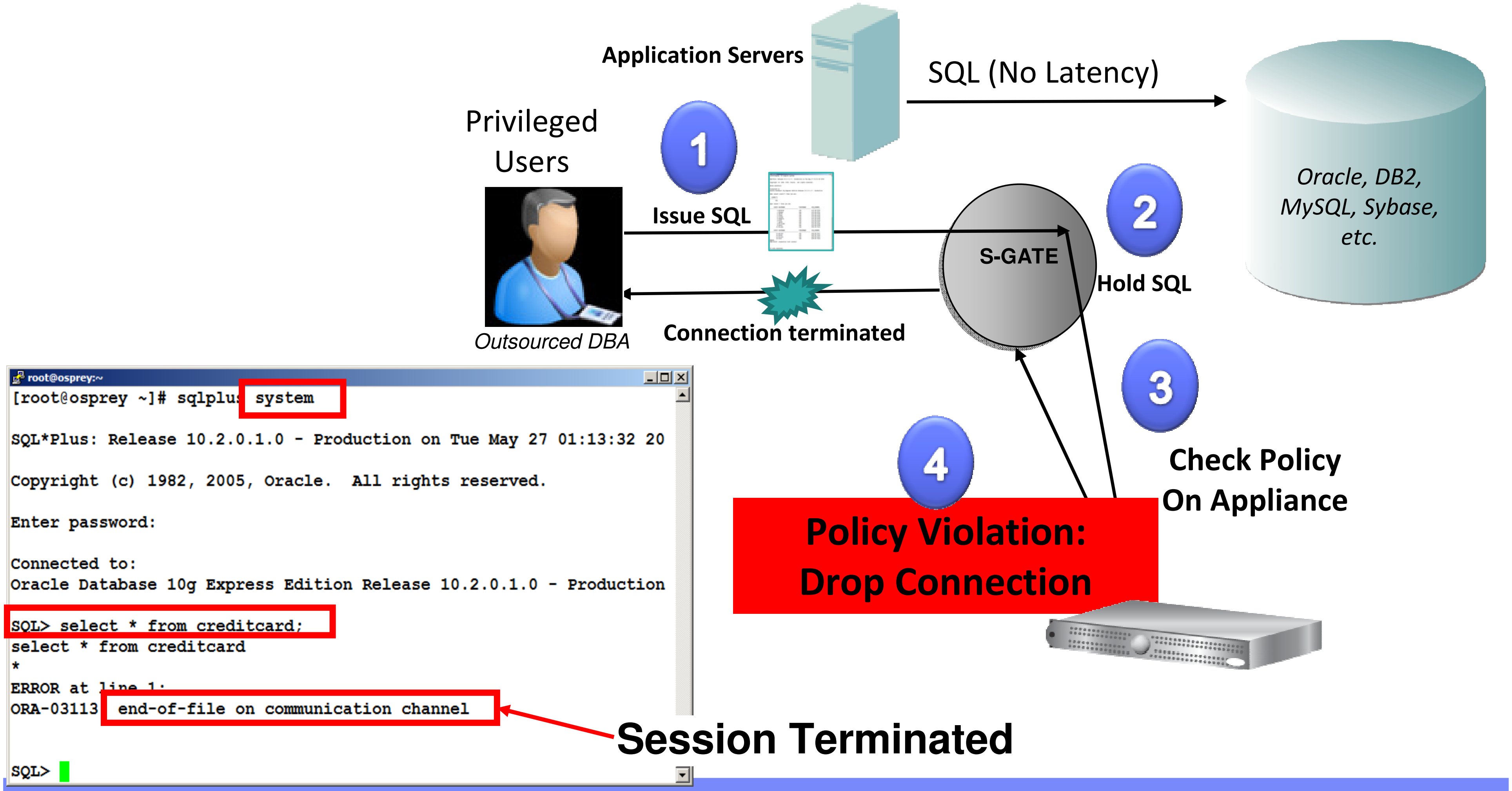
Sample Alert

From: GuardiumAlert@guardium.com — Sent: Wed 4/15/2009 8:00 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
Category: security Classification: Breach Severity MED
Rule # 20267 [non-App Source AppUser Connection]
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: TNS DB Protocol Version: 3.8 DB User: APPUSER
Application User Name
Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable

S-GATE: Blocking Access Without Inline Appliances

"DBMS software does not protect data from administrators, so DBAs today have the ability to view or steal confidential data stored in a database." Forrester, "Database Security: Market Overview," Feb. 2009



```
[root@osprey ~]# sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113 end-of-file on communication channel


SQL>
```

Chosen by Leading Organizations Worldwide

- 5 of the top 5 global banks
- 2 of the top 3 global retailers
- 3 of the top 5 global insurers
- 2 of the world’s favorite beverage brands
- The most recognized name in PCs
- 15 of the world’s leading telcos

- Top government agencies
- Top 3 auto maker
- #1 dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands

Financial Services Firm with 1M+ Sessions/Day

- **Who: Global NYSE-traded company with 75M customers**
- **Need: Enhance SOX compliance & data governance**
  - *Phase 1*: Monitor all privileged user activities, especially DB changes.
  - *Phase 2:* Focus on data privacy.
- **Environment: 4 data centers managed by IBM Global Services**
  - 122 database instances on 100+ servers
  - Oracle, IBM DB2, Sybase, SQL Server on AIX, HP-UX, Solaris, Windows
  - PeopleSoft plus 75 in-house applications
- **Alternatives considered: Native auditing**
  - Not practical because of performance overhead; DB servers at 99% capacity
- **Results: Now auditing 1M+ sessions per day (GRANTs, DDL, etc.)**
  - Caught DBAs accessing databases with Excel & shared credentials
  - Producing daily automated reports for SOX with sign-off by oversight teams
  - Automated change control reconciliation using ticket IDs
  - Passed 2 external audits

Major Retailer with PCI & SOX Controls

- **Who: National retailer with $50B+ in sales & 6,400 stores**
- **Need: Initially PCI, then extended to SOX, SAS70, data privacy**
- **Environment: 5 major data centers (via M&A)**
  - Oracle, SQL Server, DB2, UDB on AIX, Solaris, Windows
  - Dell, IBM midrange, Sun, IBM Z10 on RACF
  - PeopleSoft, SAP plus proprietary claims engines
- **Alternatives considered:**
  - Native auditing; DB encryption; DB appliance from major security vendor
- **Results:**
  - Implemented in ~ 4 weeks
  - PCI certified in stipulated time, saving millions in potential penalties
  - Requirement 3.4: Compensating control for DB encryption
  - Requirement 6: Maintain secure systems (enforce change controls)
  - Requirement 10: Track & monitor all access to cardholder data [automated]
  - Failed DB calls identified for performance optimization
  - Load distribution quantified between servers

Global Manufacturer with 239% ROI

- **Who: F500 consumer food manufacturer ($15B revenue)**
- **Need: Secure SAP & Siebel data**
  - Enforce change controls & implement consistent auditing
- **Environment:**
  - SAP, Siebel, Manugistics, IT2 + 21 other KFS
  - Oracle & IBM DB2 on AIX; SQL Server on Windows
- **Results: 239% ROI & 5.9 months payback, plus:**
  - Proactive security: Real-time alert when changes made to critical tables
  - Simplified compliance: Passed 4 audits (internal & external)
    - *"The ability to associate changes with a ticket number makes our job a lot easier. The other products didn't have that capability to automatically put in an associated ticket number with the activity that was going on within the database, which is something the auditors ask about."*

      Lead Security Analyst
  - Strategic focus on data security
    - *"There's a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers. We now have a clearer focus on security and compliance, promoted in large part by the presence and operation of the Guardium product."*

Forrester Consulting

Prepared for Guardium, Inc.
January 2008

The Total Economic Impact™ Of Guardium Database Monitoring, Security and Auditing

For A Global Consumer Products Company

Project Director: Jeffrey North, Principal Consultant

Commissioned Forrester Consulting Case Study

Major European Telco

- **Who: Global telco with 70M mobile customers; €30B revenue.**
- **Need: Ensure privacy of call records for compliance with data privac laws.**
  - Phase 1: Safeguard OSS systems
  - Phase 2: Safeguard BSS systems
- **Environment: 15 heterogeneous, geographically-distributed data centers**
  - Oracle, SQL Server, Informix, Sybase
  - HP-UX, HP Tru64, Solaris, Windows, UNIX
  - SAP, Remedy plus in-house applications (billing, Web portal, etc.)
- **Alternatives considered: Native auditing; Oracle Audit Vault.**
  - Not practical because of performance overhead; lack of granularity; non-support for older versions; need for multi-DBMS support.
- **Results:**
  - Deployed to 12 initial data centers in only 2 weeks!
  - Now auditing all traffic in high-traffic environment; centrally managed.
  - Passed several external audits
  - Future plans: Implement application user monitoring; 2-factor authentication; expand scope to other applications.

Washington DC Based Metro Authority

- **Who: The Metro operates the 2nd largest U.S. rail transit system and transports more than a third of the federal government to work**
- **Need: Metro needed to safeguard sensitive customer data and simplify compliance with PCI-DSS -- without impacting performance or changing database configurations**
  - Protecting customer data
  - Passing audits more quickly and easily
  - Monitoring for potential fraud in PeopleSoft system
  - Leveraging scalable architecture; automated oversight workflows (electronic sign-offs, escalations); library of best practices PCI policies and reports; application-layer monitoring
- **Environment:**
  - More than 9 million transactions per year (Level 1 merchant)
  - Complex, multi-tier heterogeneous environment
- **Alternatives considered: Native logging and auditing impractical**
- **Customer Impact: "Our customers trust us to transport them safely and safeguard their personal information."**
  - "We looked at native DBMS logging and auditing, but it's impractical because of its high overhead, especially when you're capturing every SELECT in a high-volume environment like ours. In addition, native auditing doesn't enforce separation of duties or prevent unauthorized access by privileged insiders."

Validated by Industry Experts

FORRESTER

"Dominance in this space"

#1 Scores for Current Offering, Architecture & Product Strategy

the 451 group

"Guardium is ahead of the pack and gaining speed."

SQL SERVER MAGAZINE

2007 Editor's Choice Award in "Auditing and Compliance"

ChannelWeb

"Most Powerful Compliance Regulations Tools ... Ever"

InformationWeek

"Top of DBEP Class"

"Practically every feature you'll need to lock down sensitive data."

INFORMATION SECURITY MAGAZINE

"Enterprise-class data security product that should be on every organization's radar."

SC MAGAZINE

"5-Star Ratings: Easy installation, sophisticated reporting, strong policy-based security."

RED HERRING WINNER 100 N. AMERICA

INFORMATION SECURITY Hotpick

Summary & Conclusions

- **Traditional log management, network scanners, SIEM & DLP insufficient to secure high-value databases**
  - No real-time monitoring at data level to detect unauthorized access
  - Inability to detect fraud at application layer
  - No knowledge about DBMS commands, vulnerabilities & structures
  - Native logging/auditing require database changes & impact performance
- **IBM InfoSphere Guardium is the most widely-deployed solution, with ongoing feedback from the most demanding data center environments worldwide**
  - Scalable enterprise architecture
  - Broad heterogeneous support
  - 100% visibility & granular control
  - Deep automation to reduce workload
  - Holistic approach

Questions

Guardium Labs

An IBM Proof of Technology

Thank
You