ORACLE

Oracle Key Vault
Data Subsetting and Masking

Paul White
Database Security Specialist

Safe Harbor Statement

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

ORACLE

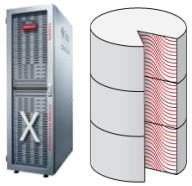
Database Security
Oracle Key Vault Overview

Oracle Database Security Solutions

Defense-in-Depth for Maximum Security

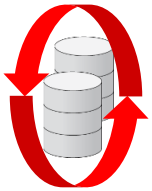
PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption & Redaction	Activity Monitoring	Privilege Analysis
Data Masking	Database Firewall	Sensitive Data Discovery
Privileged User Controls	Auditing and Reporting	Encryption Keys and Certificates

ORACLE



ORACLE

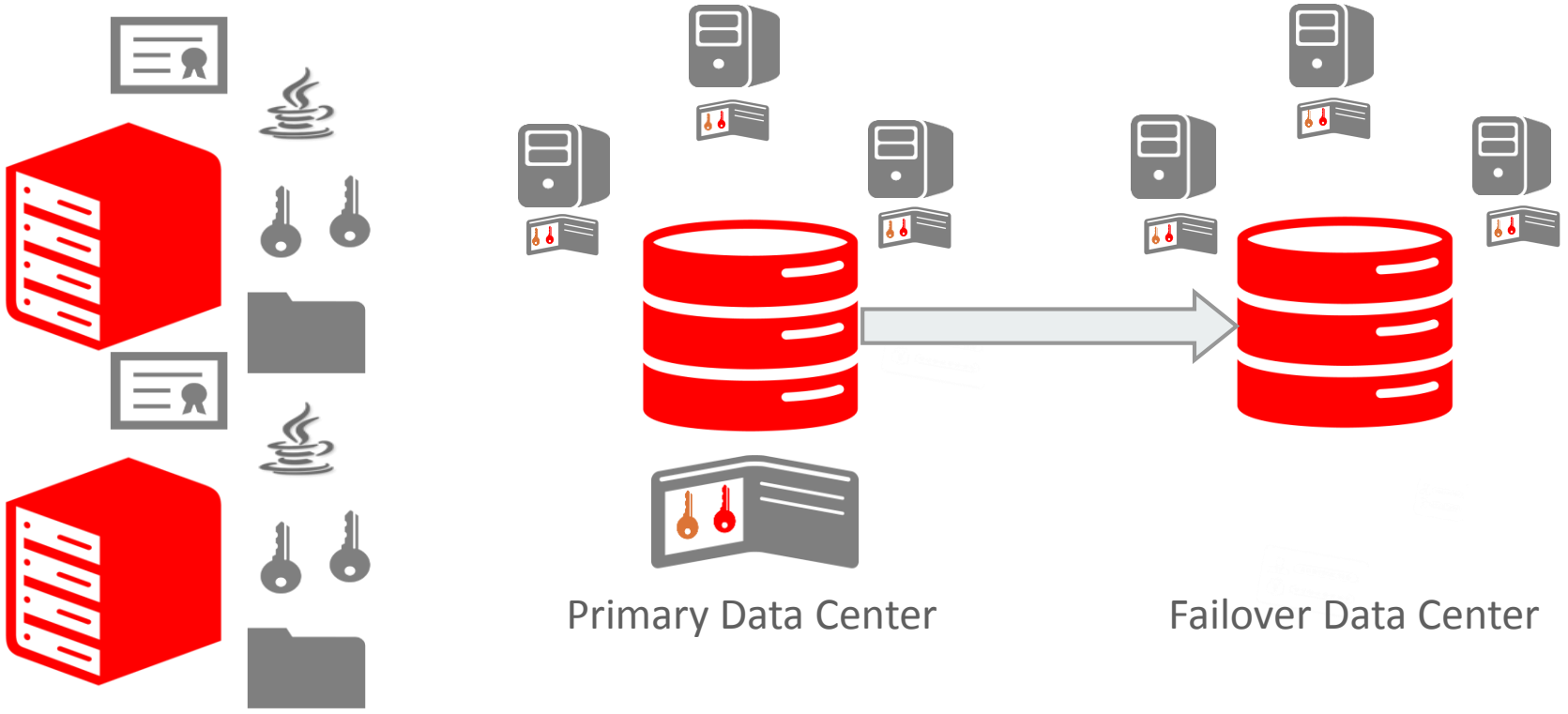
ORACLE



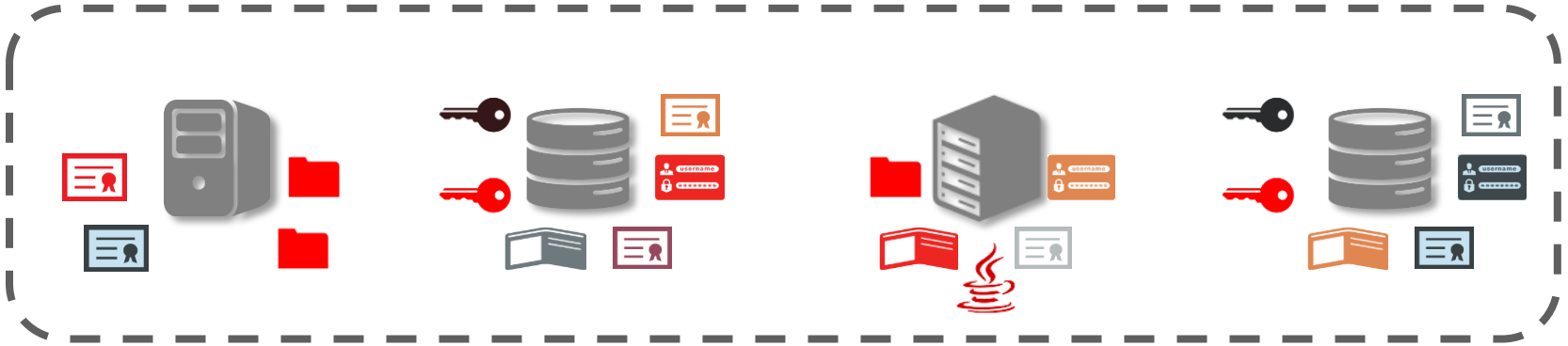
Managing Master Keys in Oracle Wallet

- ***CRITICAL***: Remember wallet password
- ***CRITICAL***: Do not delete wallet. Retain copy of password-based wallet even if using auto-login
- ***CRITICAL:*** Do not have multiple databases share same wallet
- Set strong wallet password using numbers, capitalization, length >= 12 characters…
- Rotate master encryption key and wallet password approximately every six months
- Backup wallet before and after each rotation operation
- Keep wallet backup separate from encrypted data backup
- Restrict wallet directory and file permissions
- Keep wallet read-only for daily use, set immutable bit where available
- For RAC, consider storing wallet in ACFS (DB 11gR2) or ASM (DB 12*c*R1)
- For DB 12*c*R1, separate duties using SYSKM

Management Challenges: Proliferation



The Challenges of Key Management



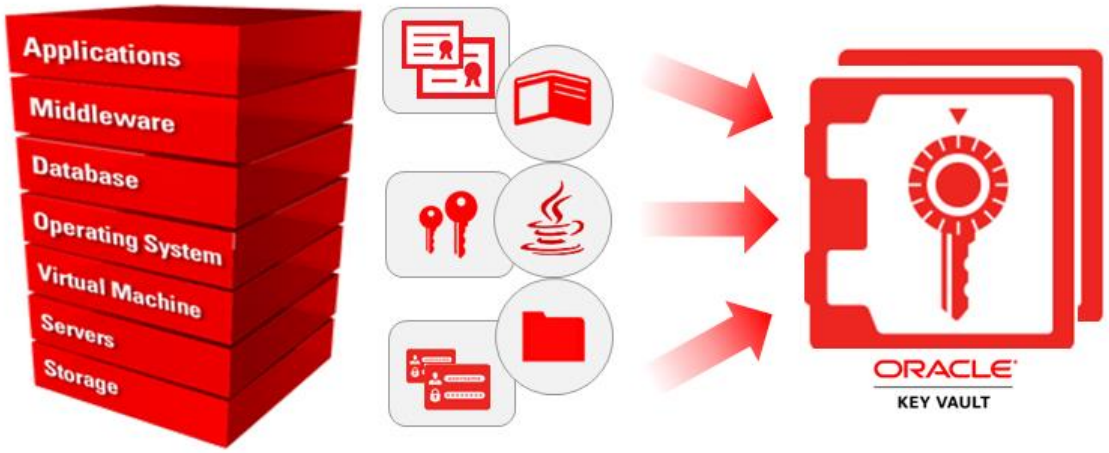
Management

- Proliferation of encryption wallets and keys
- Authorized sharing of keys
- Key availability, retention, and recovery
- Custody of keys and key storage files

Regulations

- Physical separation of keys from encrypted data
- Periodic key rotations
- Monitoring and auditing of keys
- Long-term retention of keys and encrypted data

Key Management with Oracle Key Vault

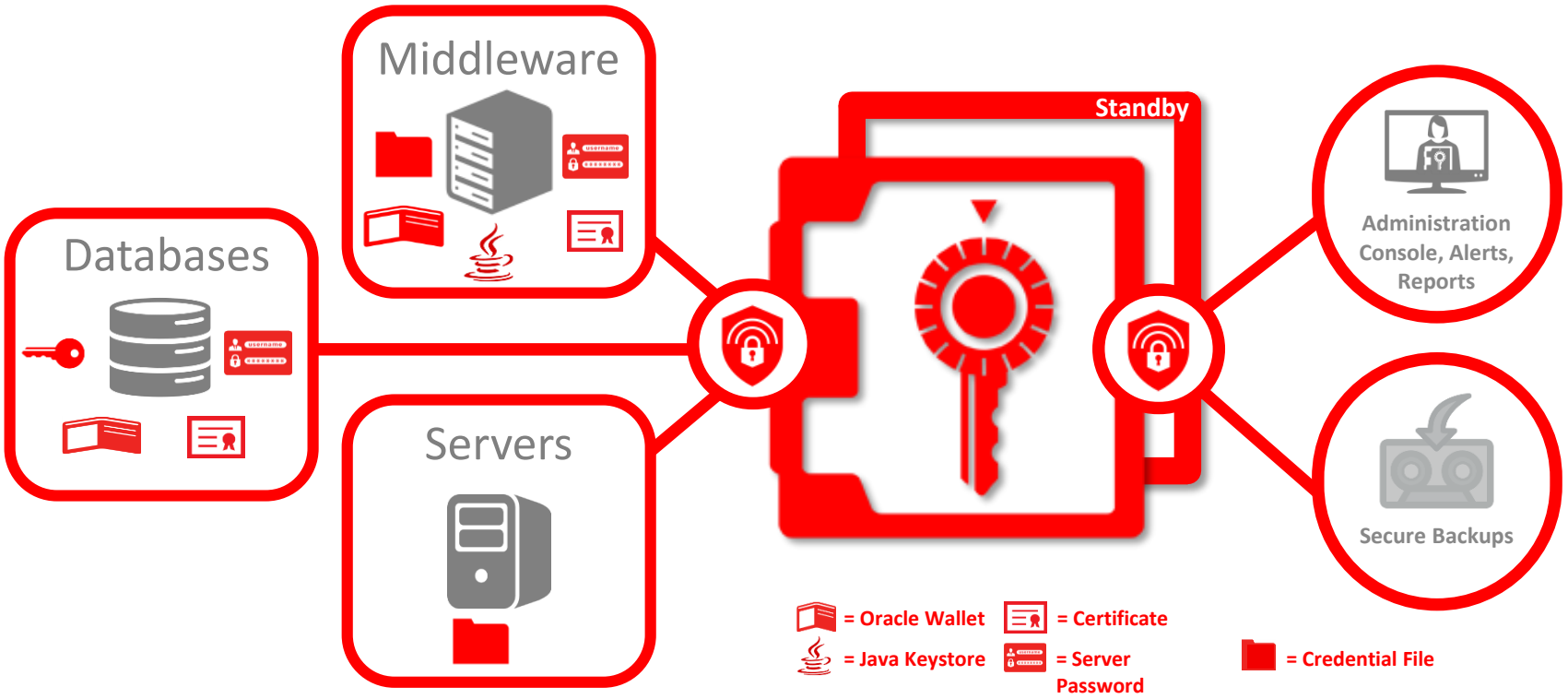


- Centrally manage and share keys, secrets, Oracle wallets, Java keystores, and more
- Optimized for Oracle stack (Database, Middleware, Systems) and Advanced Security TDE
- Robust, secure, and standards compliant (OASIS KMIP) key manager

Oracle Key Vault Software Appliance Platform

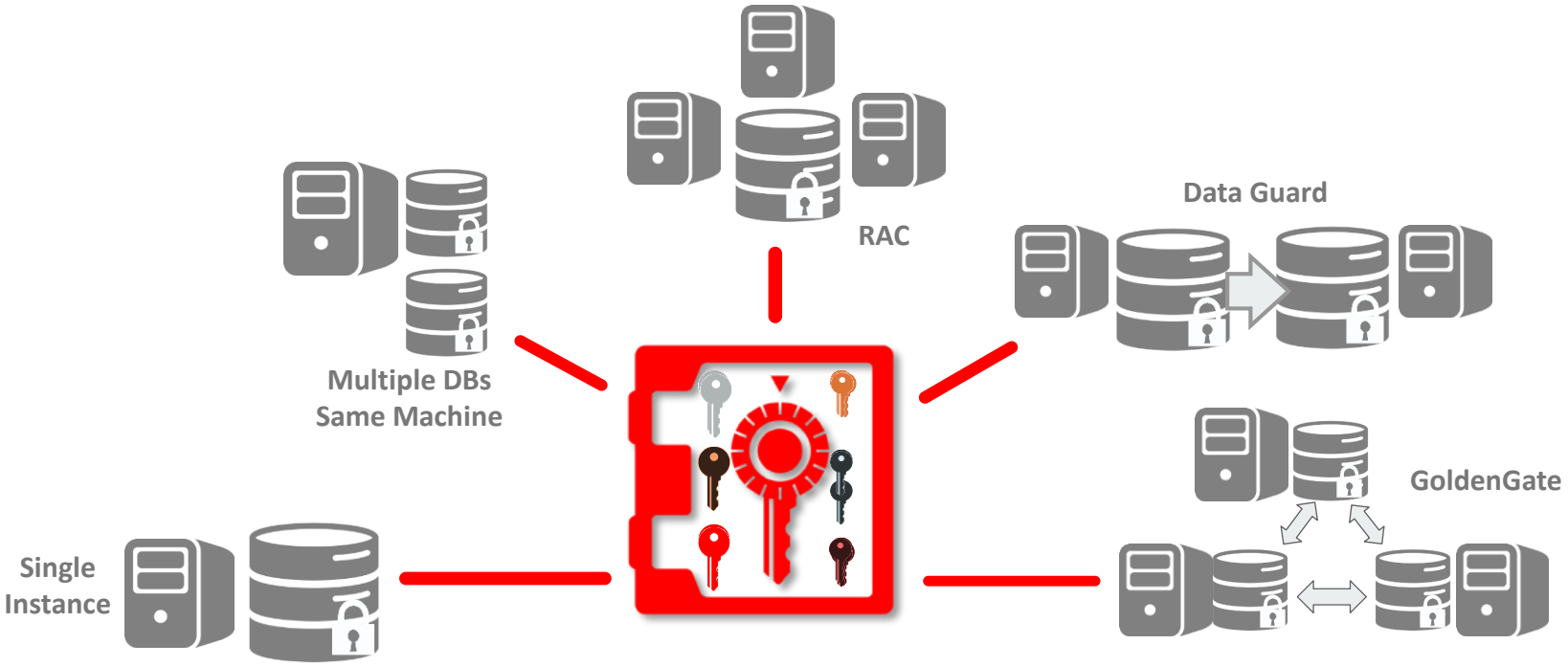
- Full-stack solution based on hardened configuration
  - Easy to install, configure, deploy, and patch
  - Open x86-64 hardware to choose from
- Includes Oracle Database security options
  - Transparent Data Encryption, Database Vault, Virtual Private Database
- Separation of duties for administrative users
- Full auditing and alerts
- Preconfigured reports

Oracle Key Vault High-Level Architecture

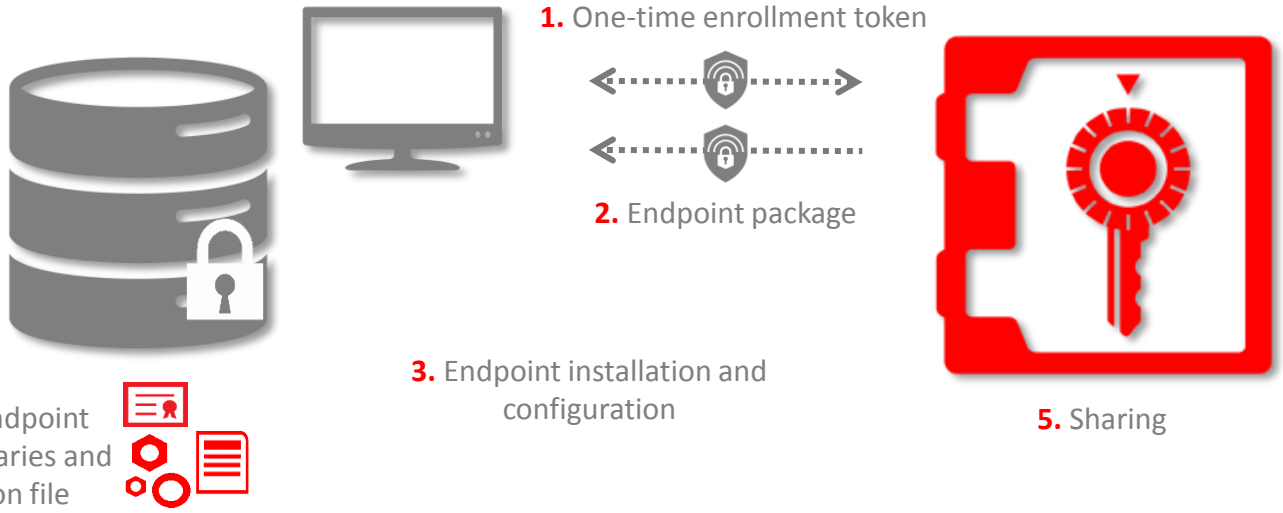


Oracle Advanced Security Transparent Data Encryption (TDE)

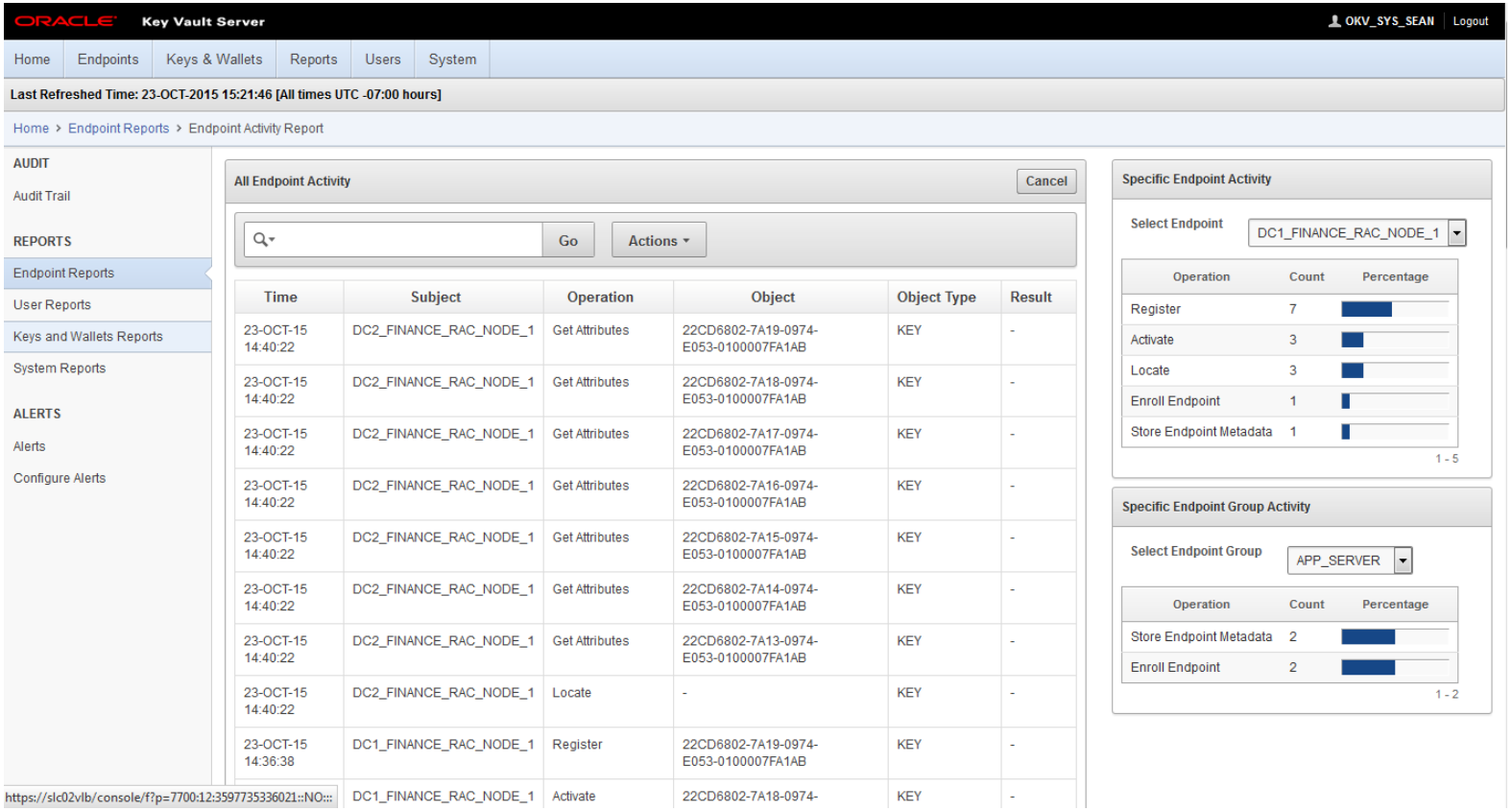
Online Master Key Scenarios



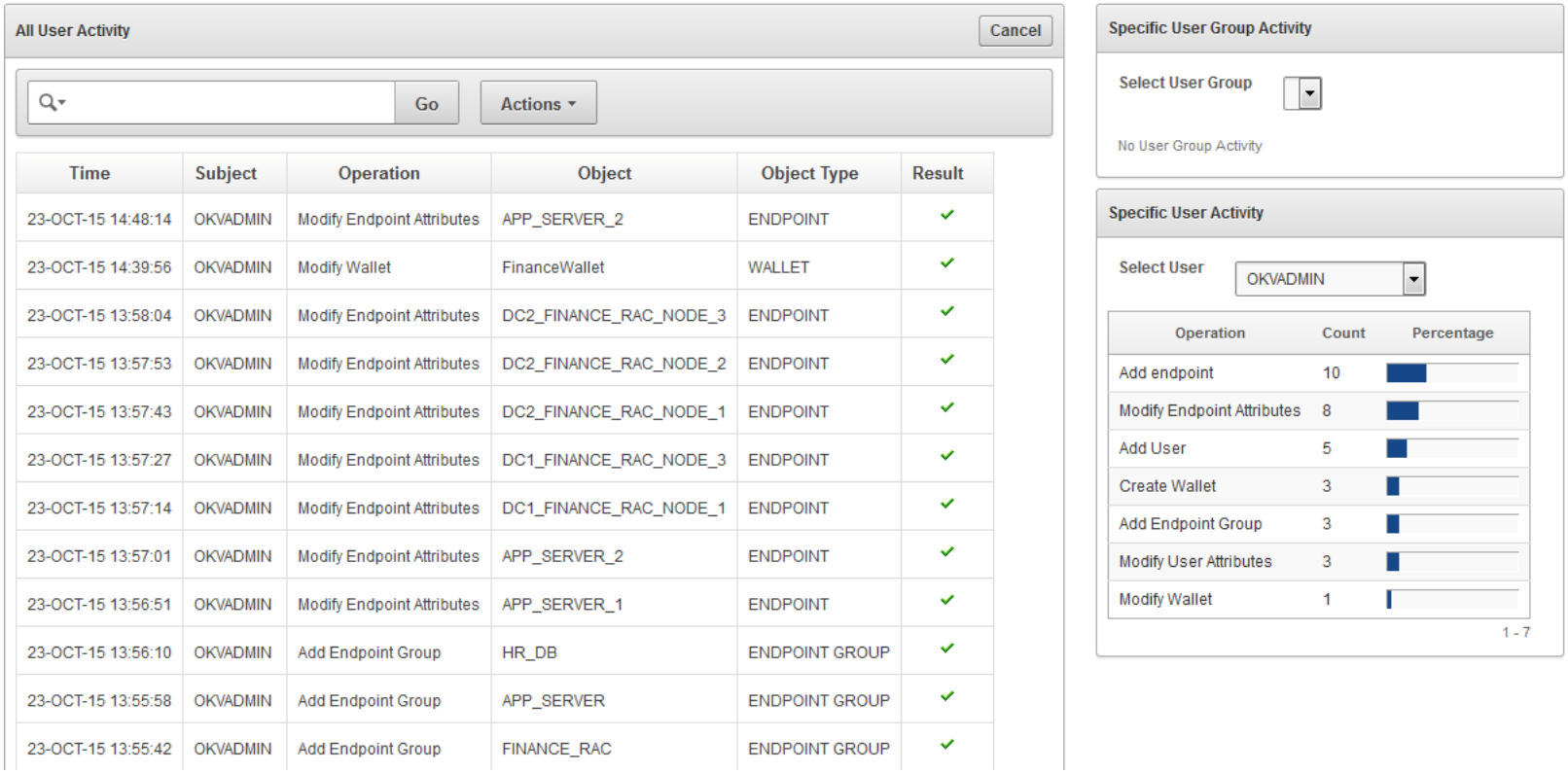
Provisioning Endpoints



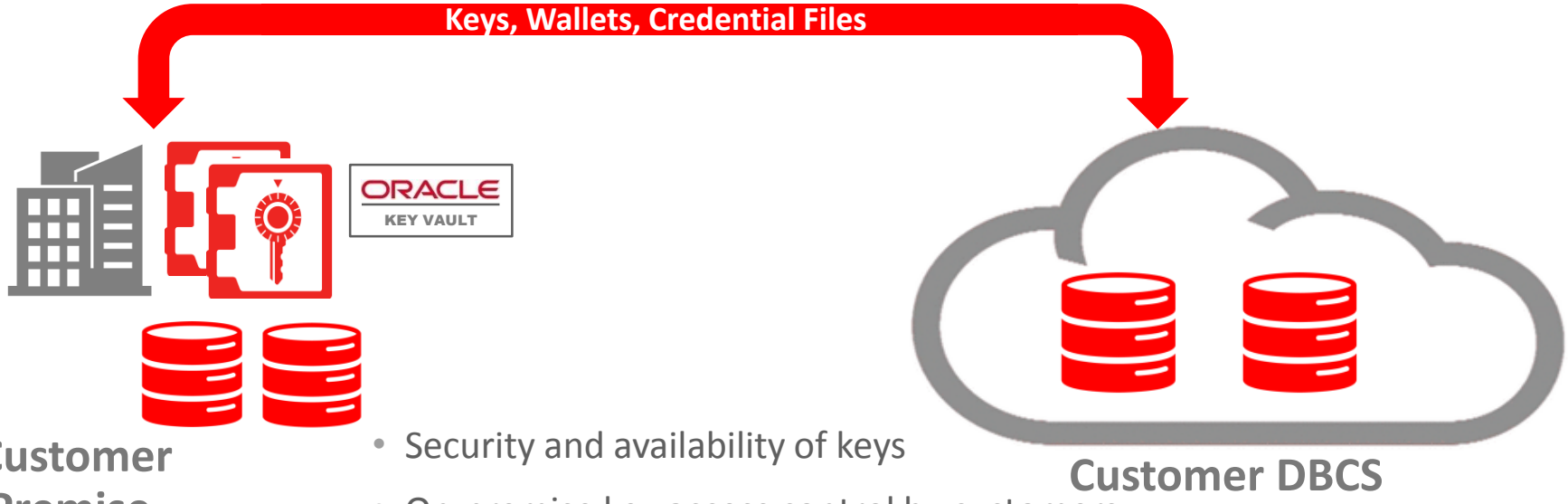
Management Reports – Endpoint Activity



User Activity



Control Keys with On-Prem Key Vault



- Security and availability of keys
- On-premise key access control by customers
- Isolation of keys per tenant
- Maintain control and visibility

ORACLE

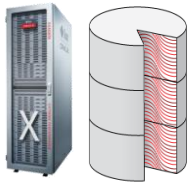
Database Security Data Subsetting and Masking Pack Technical Overview

ORACLE DATABASE SECURITY

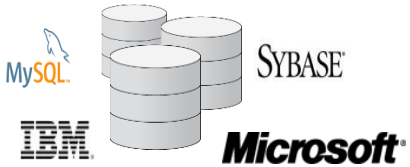
MAXIMUM SECURITY FOR CRITICAL DATA INFRASTRUCTURE

PREVENTION	DETECTION	ADMINISTRATION
Encryption & Redaction	Activity Monitoring	Privilege Analysis
Subsetting and Data Masking	Database Firewall	Sensitive Data Discovery
Privileged User Controls	Auditing and Reporting	Encryption Keys and Certificates

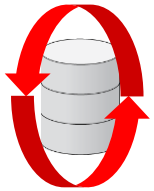
ORACLE



ORACLE



ORACLE



ORACLE

Need to Mask and Subset Data

Use Cases

Limit Sensitive Data Proliferation

- Test, Dev, QA, Training, Research, Outsourced, Cloud, and more

Compliance

- PCI-DSS, HIPAA, European Data Protection, Canada PIPEDA, and more

Save Storage Costs

- Non-Prod such as Test/Dev, Mega Data warehouses, and more

Share What is Necessary

- With Subscribers, auditors, courts, partners, testers, developers, and more

Right to be Forgotten/Erasure (New GDPR in Europe)

Challenges

How to Locate Sensitive Data?

- In the midst of numerous applications, databases, and environments

How to Accurately Protect Sensitive Data?

- Data has different shapes and forms: VISA, AMEX, Discoverer, Master, SSN, and more

Is the Protected Data Usable?

- To developers, testers, applications, and more

We Do Not Have Resources?

- To develop and maintain such solution in this ever-changing IT landscape

Will the Applications Continue to Work?

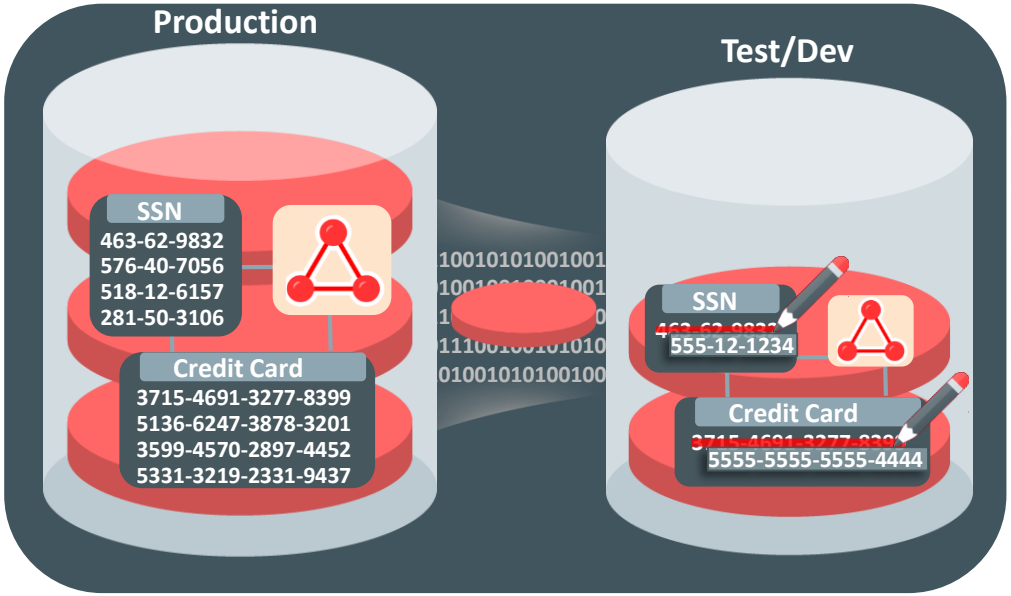
and More .....

PRELIMINARY DRAFT

Oracle Data Masking and Subsetting Pack

ORACLE ENTERPRISE MANAGER 12c

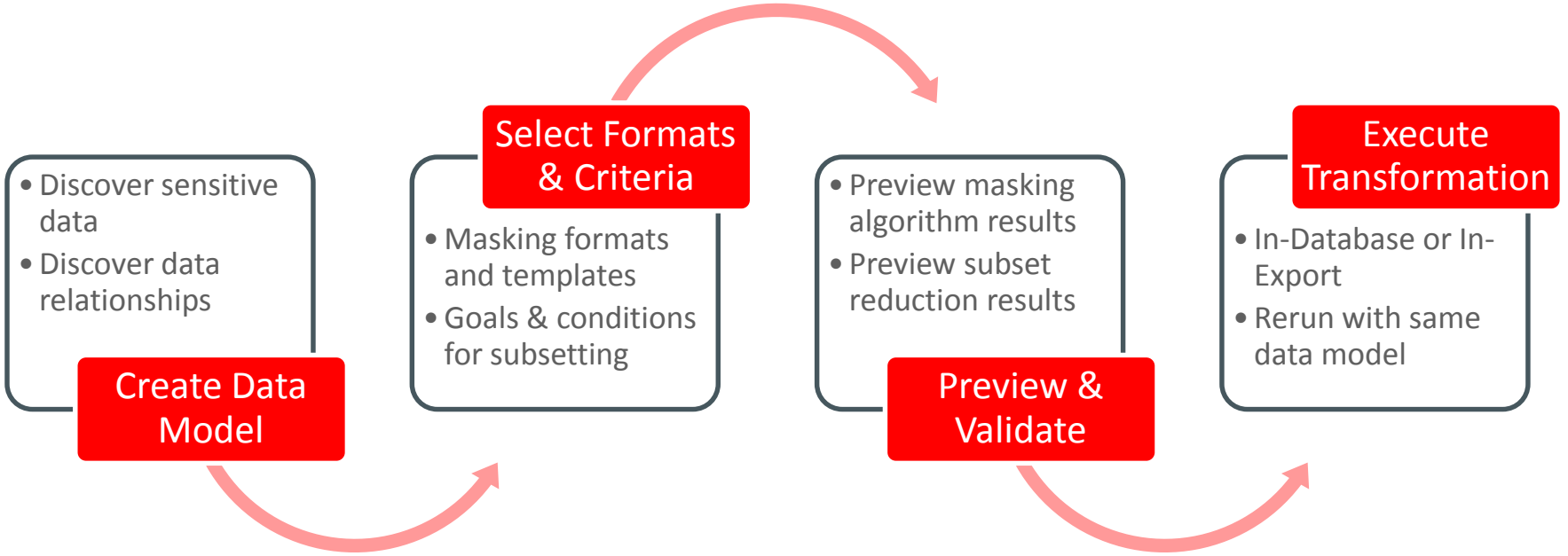
Reduces Risk in Sharing by Obfuscating or Removing Sensitive Data



- Discover Sensitive Data
- Modeling Application Data
- Mask Data using Format Library
- Subset Based on Goal/Condition
- Mask/Subset in Export or on Staging
- Mask in Workload Captures & Clones
- Pre-installed in Enterprise Manager

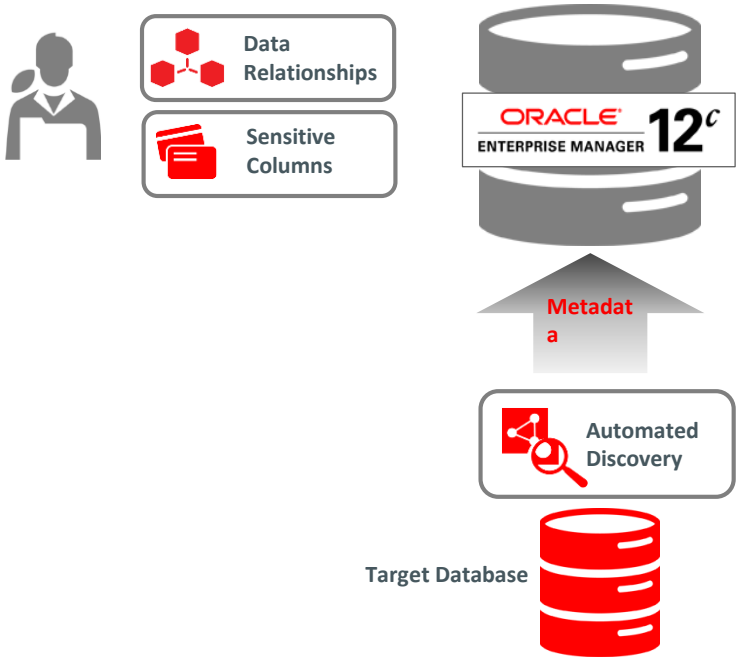
ORACLE

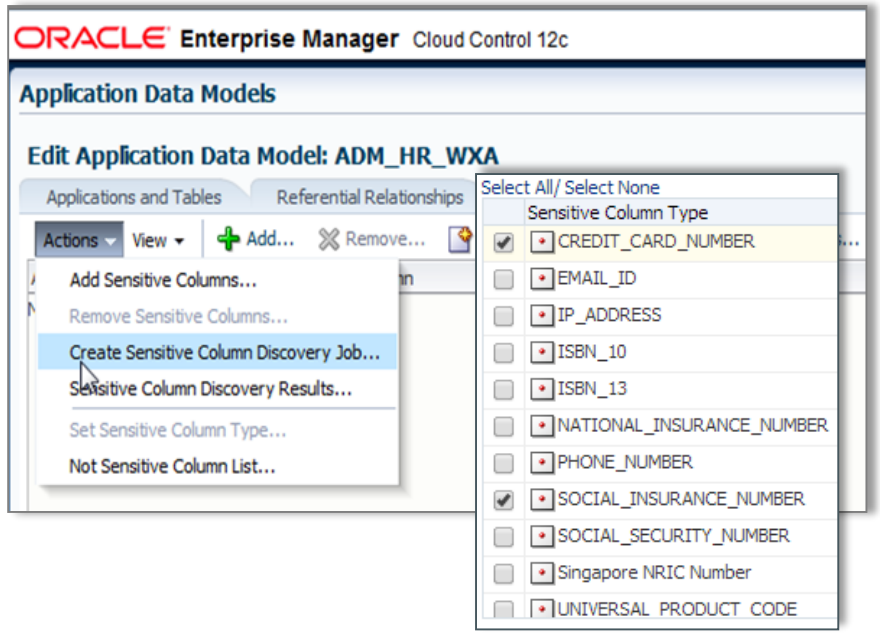
Data Masking and Subsetting Methodology



Application Data Modeling

Sensitive Data Discovery

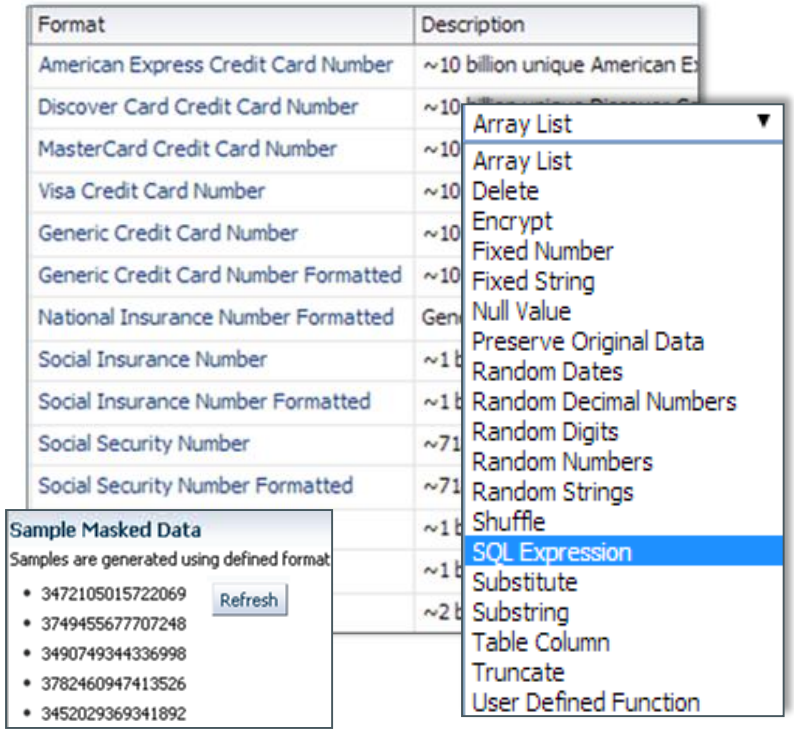




Extensive Masking Format Library

- Provides common masking formats
- Supports custom masking formats
  - Random numbers/strings/dates
  - Substitute
  - User defined PL/SQL function

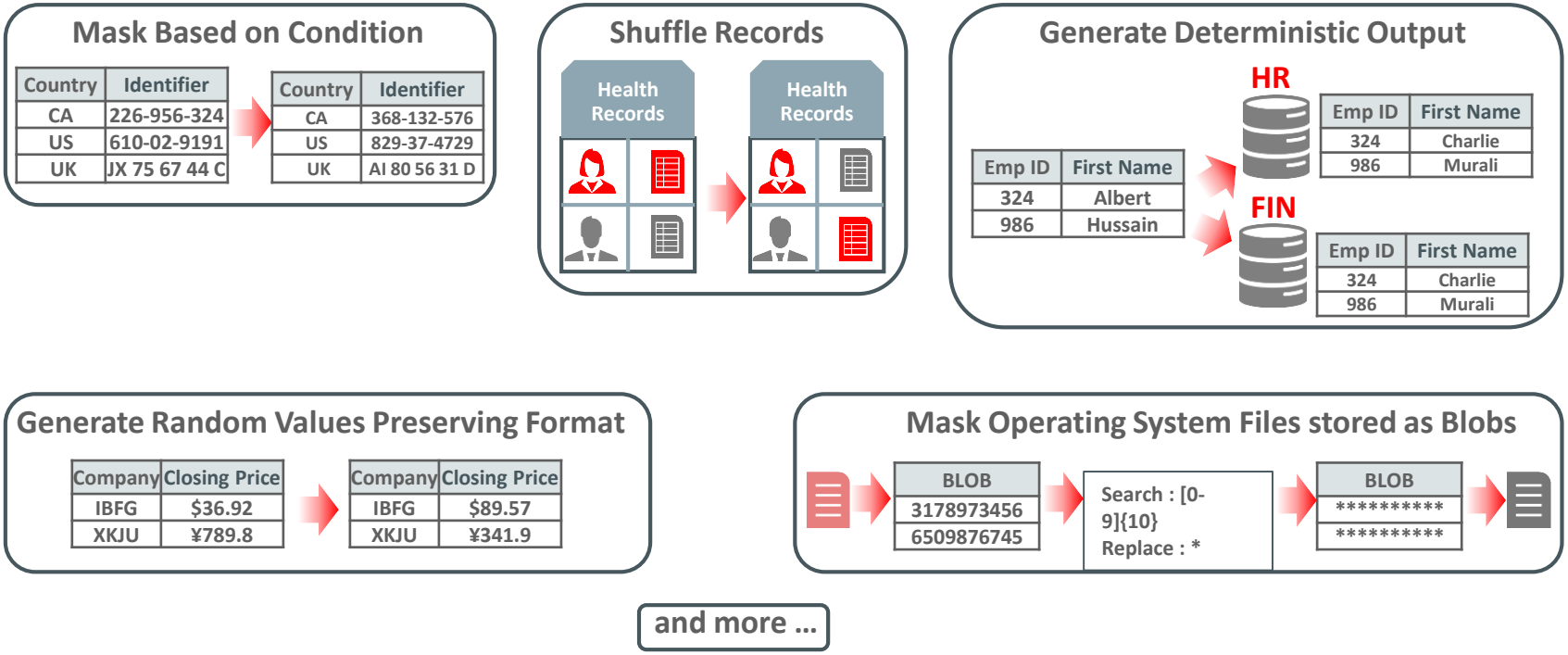
    … and more
- Generates sample masked values
- Templates for specific versions of E-Business Suite and Fusion Applications



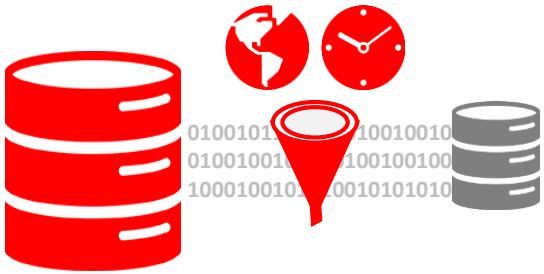
Comprehensive Masking Transformations

Conditional masking	Masks rows differently based on condition *E.g. Mask national identifiers based on country*
Consistent masking	Ensures the masked values is same across multiple databases *E.g. Mask employee identifiers consistently across schemas and databases*
Compound masking	Reduces masking time by grouping related columns *E.g. Mask related columns: address (street, state, country), or dates (birth , joining)*
Format preserving	Generates random values that maintain the original format *E.g. Mask passport numbers or tax identifiers while keeping the format*
Perturbation	Generates random values within a user defined range *E.g. Generate random dates within a specific range*
Shuffling	Shuffles the values within a column *E.g. Shuffle clinical data or PII between electronic health records*
Reversible masking	Encrypts and decrypts data based on a passphrase *E.g. Outsourced data processing team can unmask data*

Masking Examples

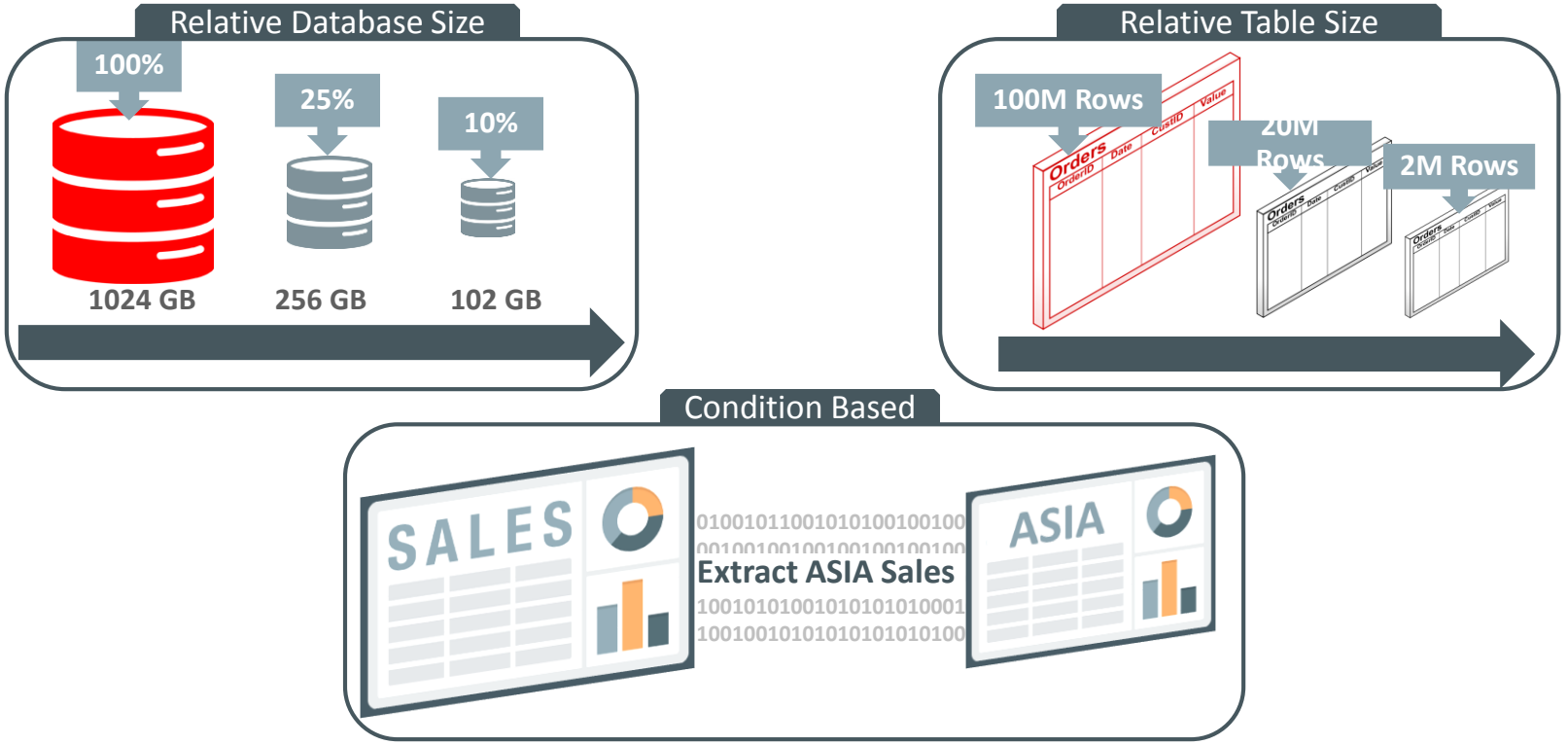


Data Subsetting Use Cases

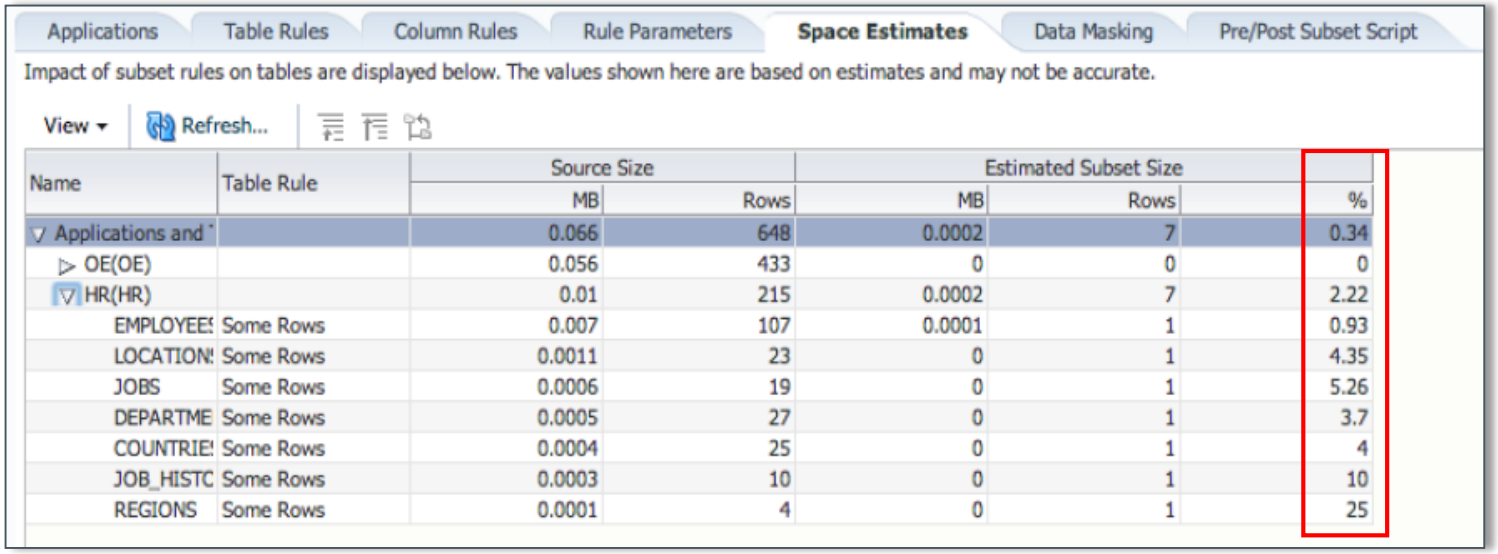


- Share relevant subset of data with internal and external teams
- Reduce storage cost for test/dev
- Extract subscriber data from SaaS
- Perform research and analysis on a subset of data
- Extract subset of data as part of e-discovery requests

Goal or Condition Based Subsetting



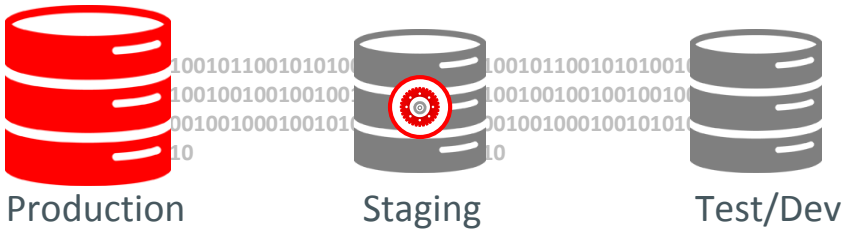
Preview and Validate Subset Results



Name	Table Rule	Source Size		Estimated Subset Size		
		MB	Rows	MB	Rows	%
▽ Applications and		0.066	648	0.0002	7	0.34
▷ OE(OE)		0.056	433	0	0	0
▽ HR(HR)		0.01	215	0.0002	7	2.22
EMPLOYEES	Some Rows	0.007	107	0.0001	1	0.93
LOCATIONS	Some Rows	0.0011	23	0	1	4.35
JOBS	Some Rows	0.0006	19	0	1	5.26
DEPARTME	Some Rows	0.0005	27	0	1	3.7
COUNTRIES	Some Rows	0.0004	25	0	1	4
JOB_HISTC	Some Rows	0.0003	10	0	1	10
REGIONS	Some Rows	0.0001	4	0	1	25

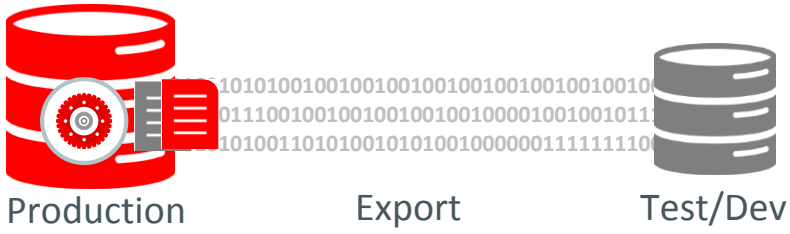
Deployment Options

In-Database



Minimal impact on the production environment

In-Export



Sensitive data remains within the production perimeter

Hardware and Software

ORACLE

Engineered to Work Together