



Oracle Security Solutions

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.



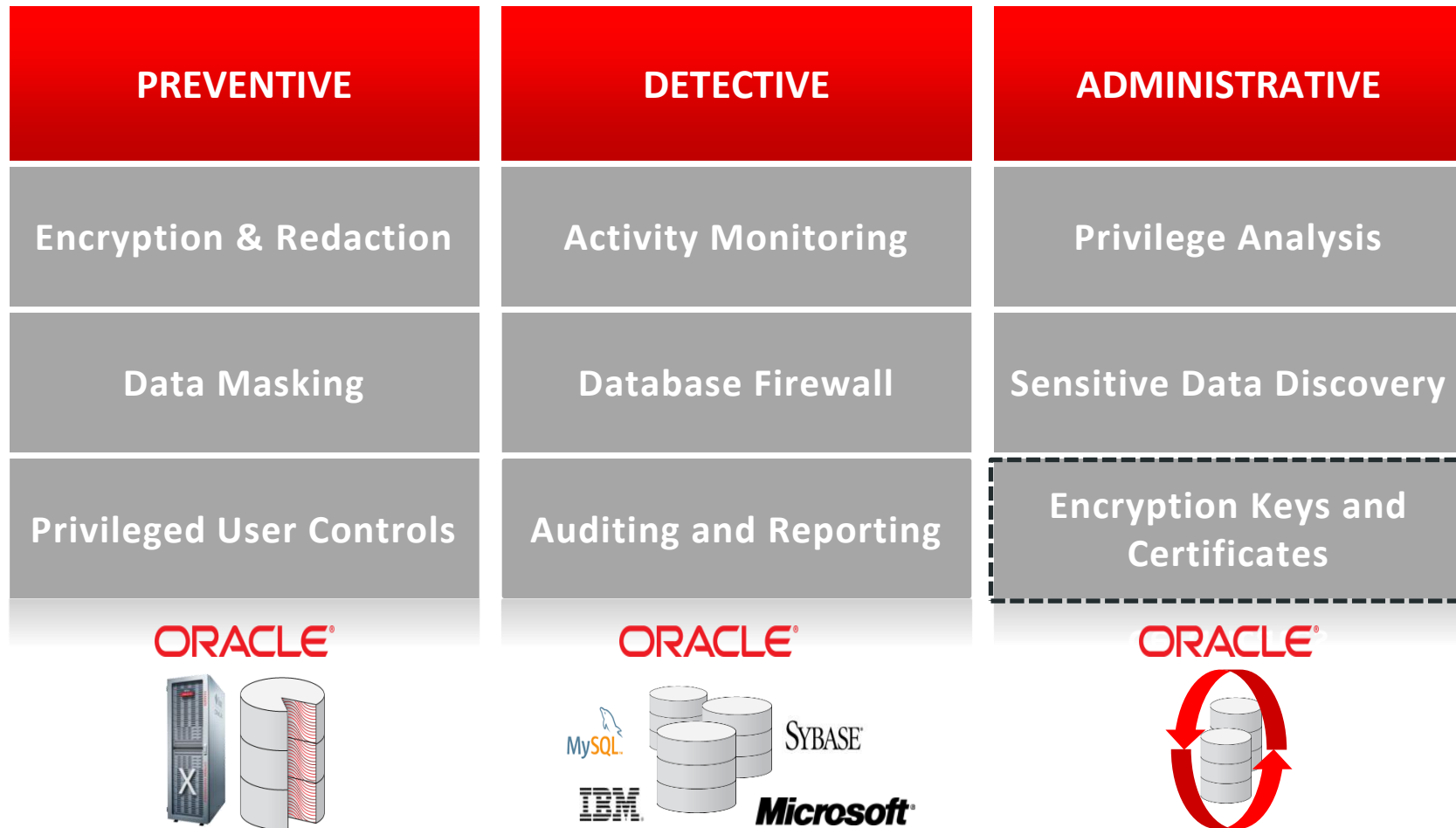
Database Security Oracle Key Vault Overview

Oracle Security Solutions



Oracle Database Security Solutions

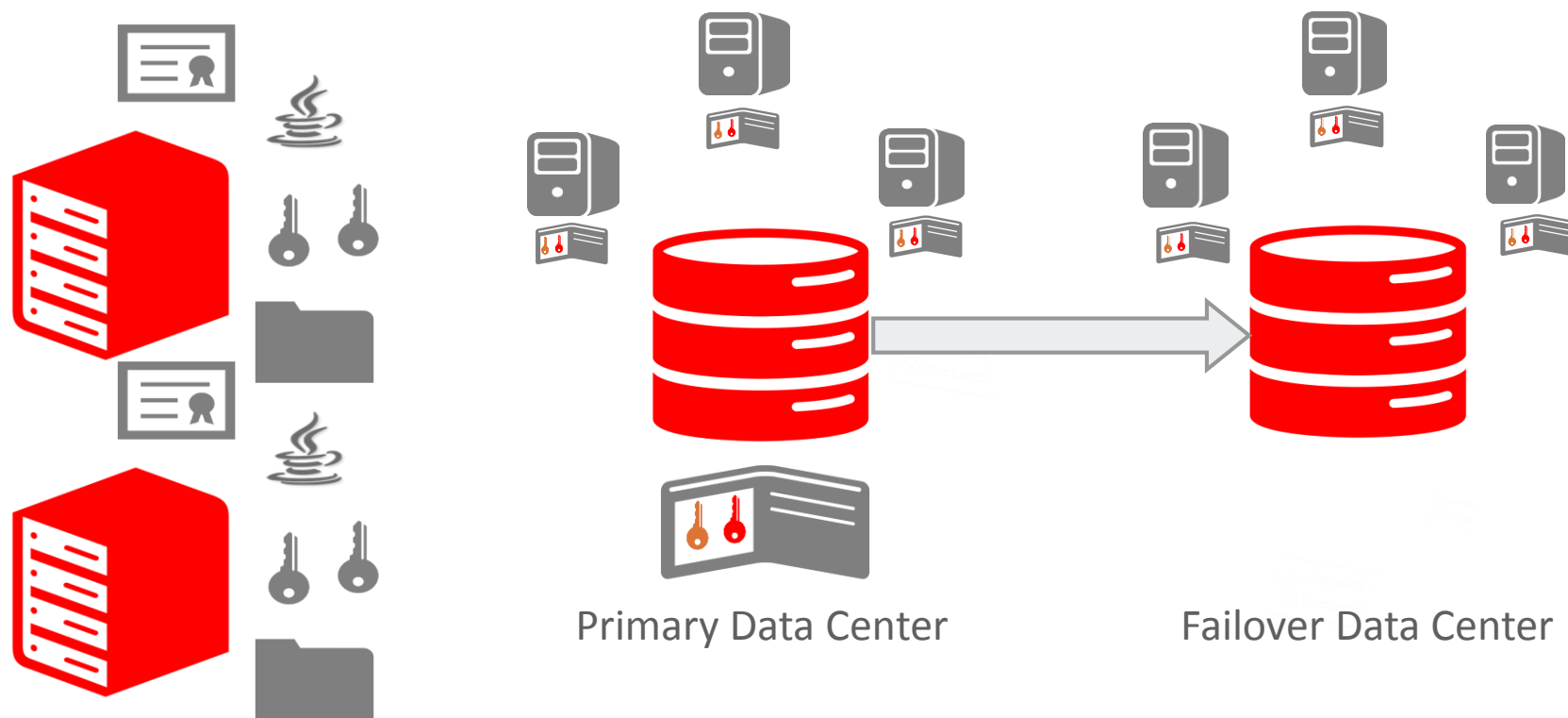
Defense-in-Depth for Maximum Security



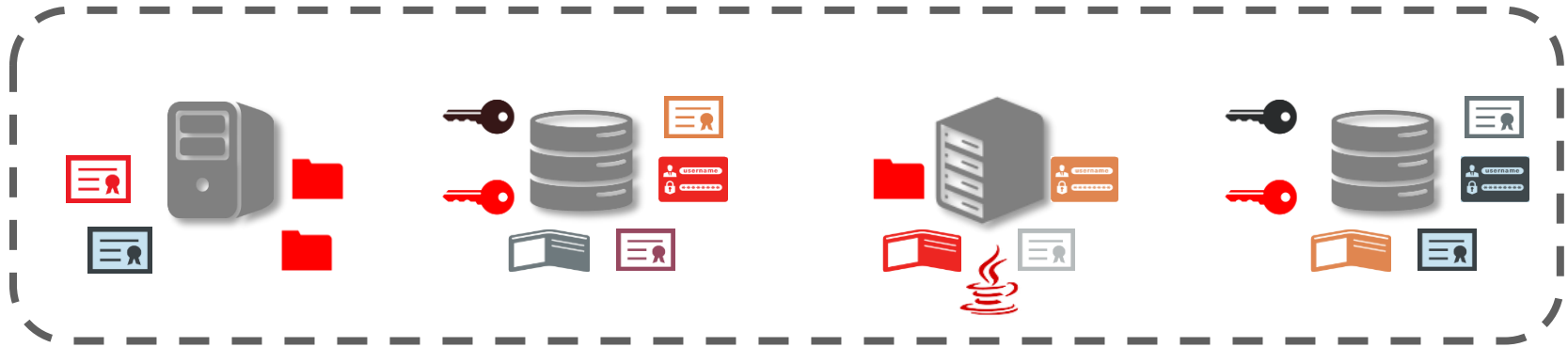
Managing Master Keys in Oracle Wallet

- **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 12cR1)
- For DB 12cR1, separate duties using SYSKM

Management Challenges: Proliferation



The Challenges of Key Management



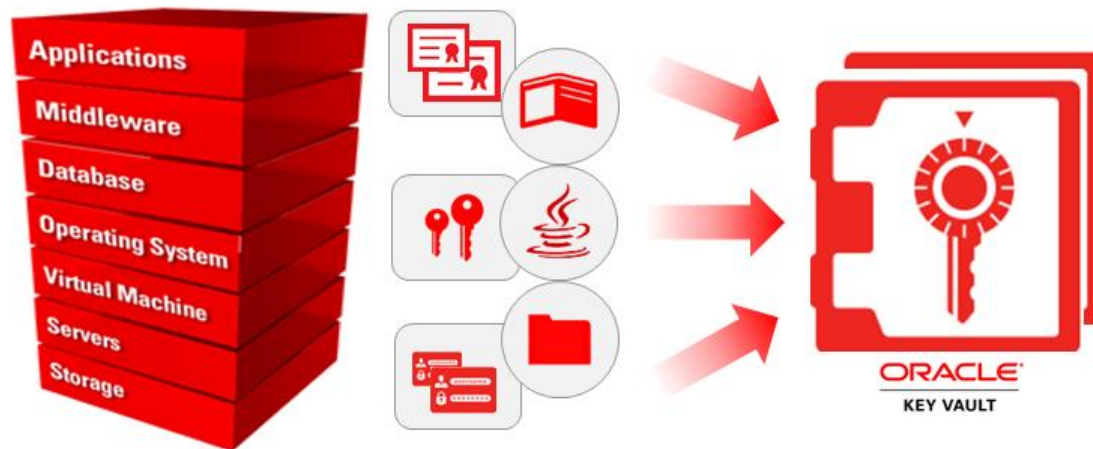
Management

- 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

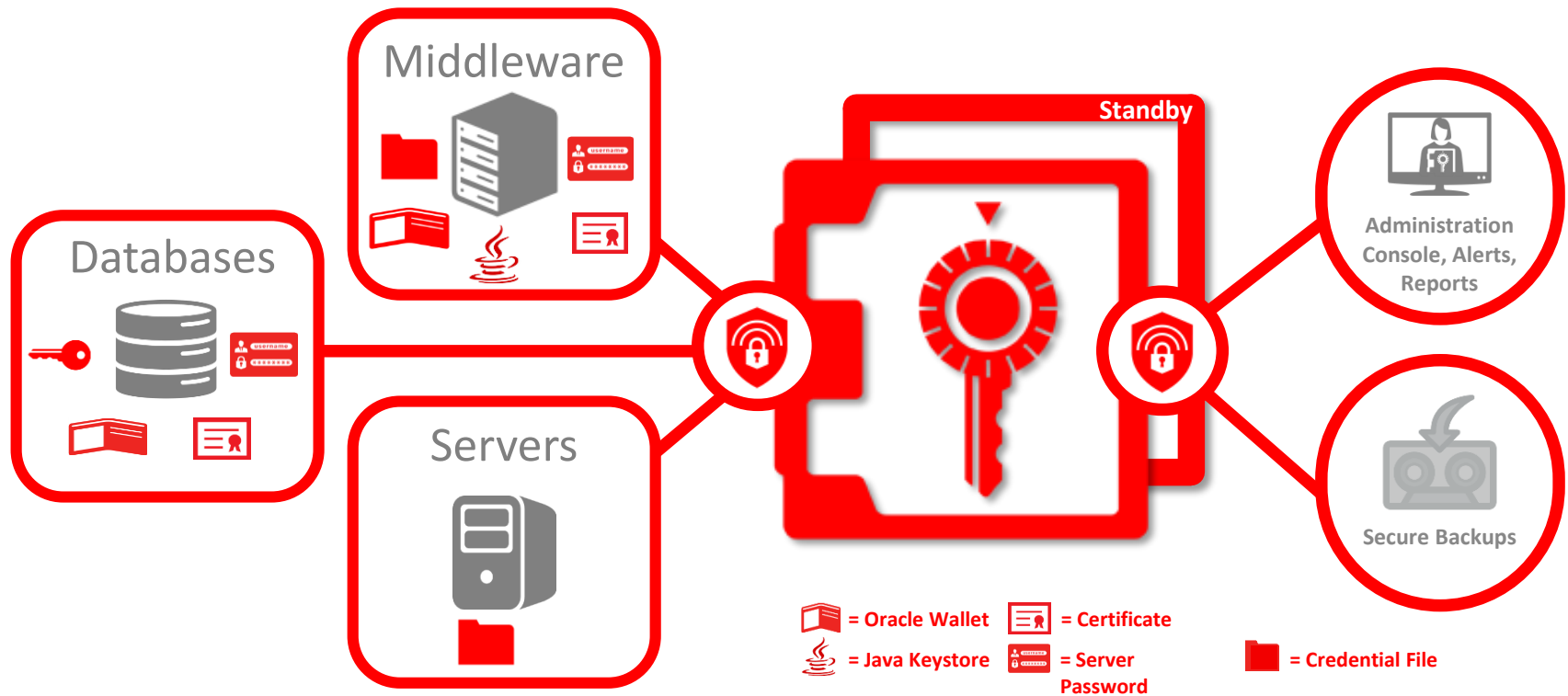


- Centrally manage and share keys, secrets, Oracle wallets, Java keystores, and more
- Optimized for Oracle stack (Database, Middleware, Systems) and Advanced Security TDE
- Robust, secure, and standards compliant (OASIS KMIP) key manager

Oracle Key Vault Software Appliance Platform

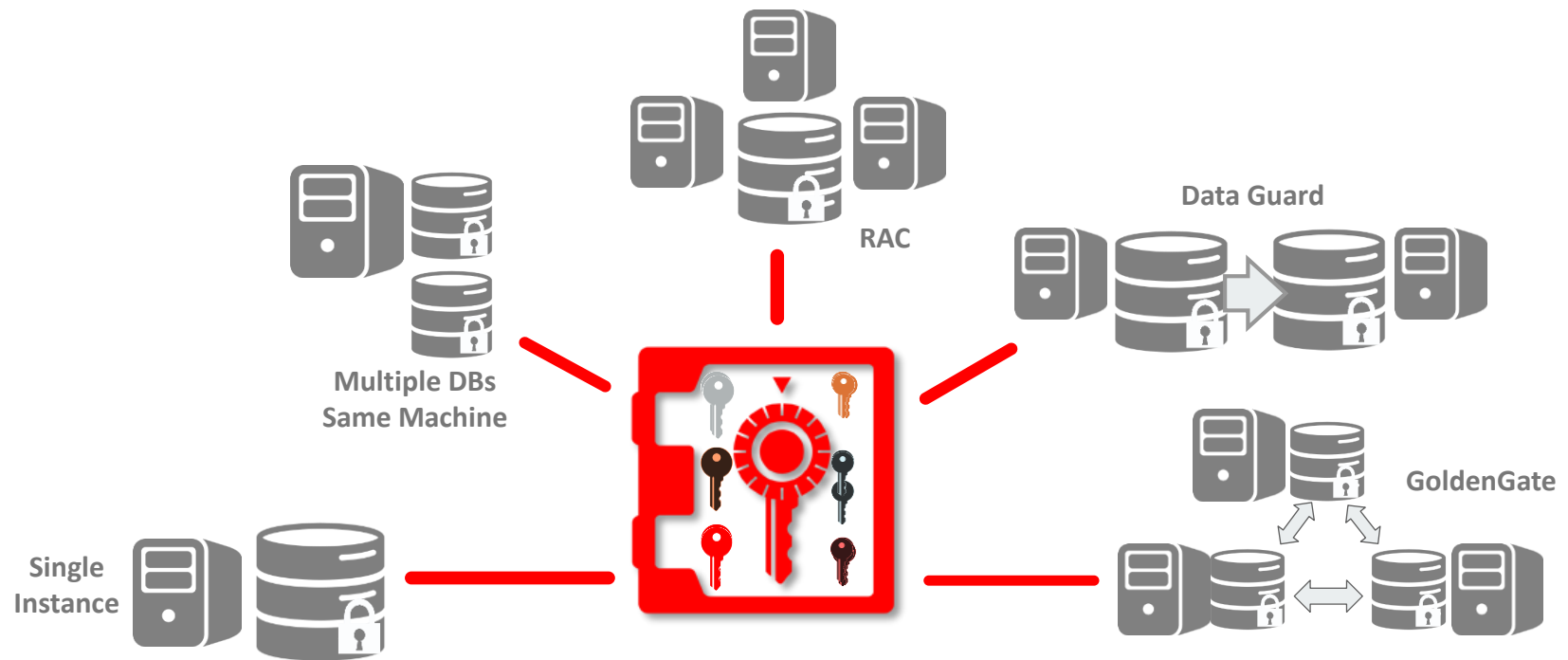
- Full-stack solution based on hardened configuration
 - Easy to install, configure, deploy, and patch
 - Open x86-64 hardware to choose from
- Includes Oracle Database security options
 - Transparent Data Encryption, Database Vault, Virtual Private Database
- Separation of duties for administrative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

Oracle Key Vault High-Level Architecture

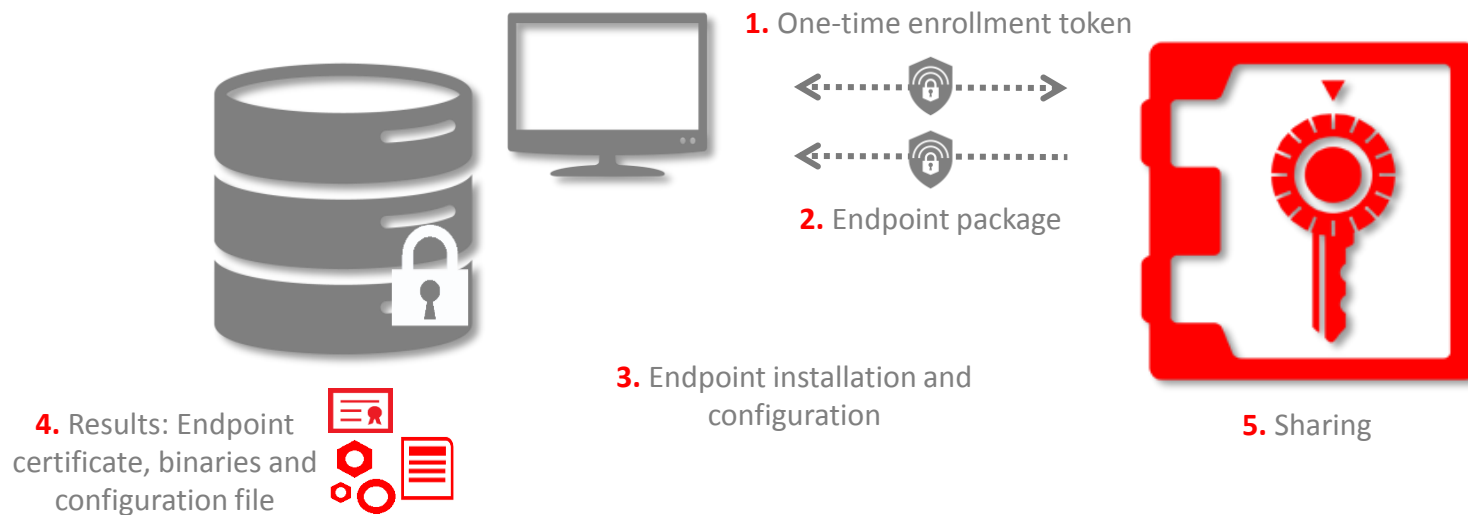


Oracle Advanced Security Transparent Data Encryption (TDE)

Online Master Key Scenarios



Provisioning Endpoints



Management Reports – Endpoint Activity

ORACLE Key Vault Server OKV_SYS_SEAN Logout

Home Endpoints Keys & Wallets Reports Users System

Last Refreshed Time: 23-OCT-2015 15:21:46 [All times UTC -07:00 hours]

Home > Endpoint Reports > Endpoint Activity Report

AUDIT
Audit Trail

REPORTS
Endpoint Reports
User Reports
Keys and Wallets Reports
System Reports

ALERTS
Alerts
Configure Alerts

All Endpoint Activity Cancel

Go Actions ▾

| Time | Subject | Operation | Object | Object Type | Result |
|---|------------------------|----------------|--------------------------------------|-------------|--------|
| 23-OCT-15 14:40:22 | DC2_FINANCE_RAC_NODE_1 | Get Attributes | 22CD6802-7A19-0974-E053-0100007FA1AB | KEY | - |
| 23-OCT-15 14:40:22 | DC2_FINANCE_RAC_NODE_1 | Get Attributes | 22CD6802-7A18-0974-E053-0100007FA1AB | KEY | - |
| 23-OCT-15 14:40:22 | DC2_FINANCE_RAC_NODE_1 | Get Attributes | 22CD6802-7A17-0974-E053-0100007FA1AB | KEY | - |
| 23-OCT-15 14:40:22 | DC2_FINANCE_RAC_NODE_1 | Get Attributes | 22CD6802-7A16-0974-E053-0100007FA1AB | KEY | - |
| 23-OCT-15 14:40:22 | DC2_FINANCE_RAC_NODE_1 | Get Attributes | 22CD6802-7A15-0974-E053-0100007FA1AB | KEY | - |
| 23-OCT-15 14:40:22 | DC2_FINANCE_RAC_NODE_1 | Get Attributes | 22CD6802-7A14-0974-E053-0100007FA1AB | KEY | - |
| 23-OCT-15 14:40:22 | DC2_FINANCE_RAC_NODE_1 | Get Attributes | 22CD6802-7A13-0974-E053-0100007FA1AB | KEY | - |
| 23-OCT-15 14:40:22 | DC2_FINANCE_RAC_NODE_1 | Locate | - | KEY | - |
| 23-OCT-15 14:36:38 | DC1_FINANCE_RAC_NODE_1 | Register | 22CD6802-7A19-0974-E053-0100007FA1AB | KEY | - |
| https://slc02vlb/console/f?p=7700:12:3597735336021::NO... | DC1_FINANCE_RAC_NODE_1 | Activate | 22CD6802-7A18-0974- | KEY | - |

Specific Endpoint Activity

Select Endpoint DC1_FINANCE_RAC_NODE_1 ▾

| Operation | Count | Percentage |
|-------------------------|-------|-------------|
| Register | 7 | <div></div> |
| Activate | 3 | <div></div> |
| Locate | 3 | <div></div> |
| Enroll Endpoint | 1 | <div></div> |
| Store Endpoint Metadata | 1 | <div></div> |

1 - 5

Specific Endpoint Group Activity

Select Endpoint Group APP_SERVER ▾

| Operation | Count | Percentage |
|-------------------------|-------|-------------|
| Store Endpoint Metadata | 2 | <div></div> |
| Enroll Endpoint | 2 | <div></div> |

1 - 2

User Activity

| All User Activity Cancel | | | | | |
|---|----------|----------------------------|------------------------|----------------|--------|
| <input type="text"/> Go Actions ▾ | | | | | |
| Time | Subject | Operation | Object | Object Type | Result |
| 23-OCT-15 14:48:14 | OKVADMIN | Modify Endpoint Attributes | APP_SERVER_2 | ENDPOINT | ✓ |
| 23-OCT-15 14:39:56 | OKVADMIN | Modify Wallet | FinanceWallet | WALLET | ✓ |
| 23-OCT-15 13:58:04 | OKVADMIN | Modify Endpoint Attributes | DC2_FINANCE_RAC_NODE_3 | ENDPOINT | ✓ |
| 23-OCT-15 13:57:53 | OKVADMIN | Modify Endpoint Attributes | DC2_FINANCE_RAC_NODE_2 | ENDPOINT | ✓ |
| 23-OCT-15 13:57:43 | OKVADMIN | Modify Endpoint Attributes | DC2_FINANCE_RAC_NODE_1 | ENDPOINT | ✓ |
| 23-OCT-15 13:57:27 | OKVADMIN | Modify Endpoint Attributes | DC1_FINANCE_RAC_NODE_3 | ENDPOINT | ✓ |
| 23-OCT-15 13:57:14 | OKVADMIN | Modify Endpoint Attributes | DC1_FINANCE_RAC_NODE_1 | ENDPOINT | ✓ |
| 23-OCT-15 13:57:01 | OKVADMIN | Modify Endpoint Attributes | APP_SERVER_2 | ENDPOINT | ✓ |
| 23-OCT-15 13:56:51 | OKVADMIN | Modify Endpoint Attributes | APP_SERVER_1 | ENDPOINT | ✓ |
| 23-OCT-15 13:56:10 | OKVADMIN | Add Endpoint Group | HR_DB | ENDPOINT GROUP | ✓ |
| 23-OCT-15 13:55:58 | OKVADMIN | Add Endpoint Group | APP_SERVER | ENDPOINT GROUP | ✓ |
| 23-OCT-15 13:55:42 | OKVADMIN | Add Endpoint Group | FINANCE_RAC | ENDPOINT GROUP | ✓ |

Specific User Group Activity

Select User Group

No User Group Activity

Specific User Activity

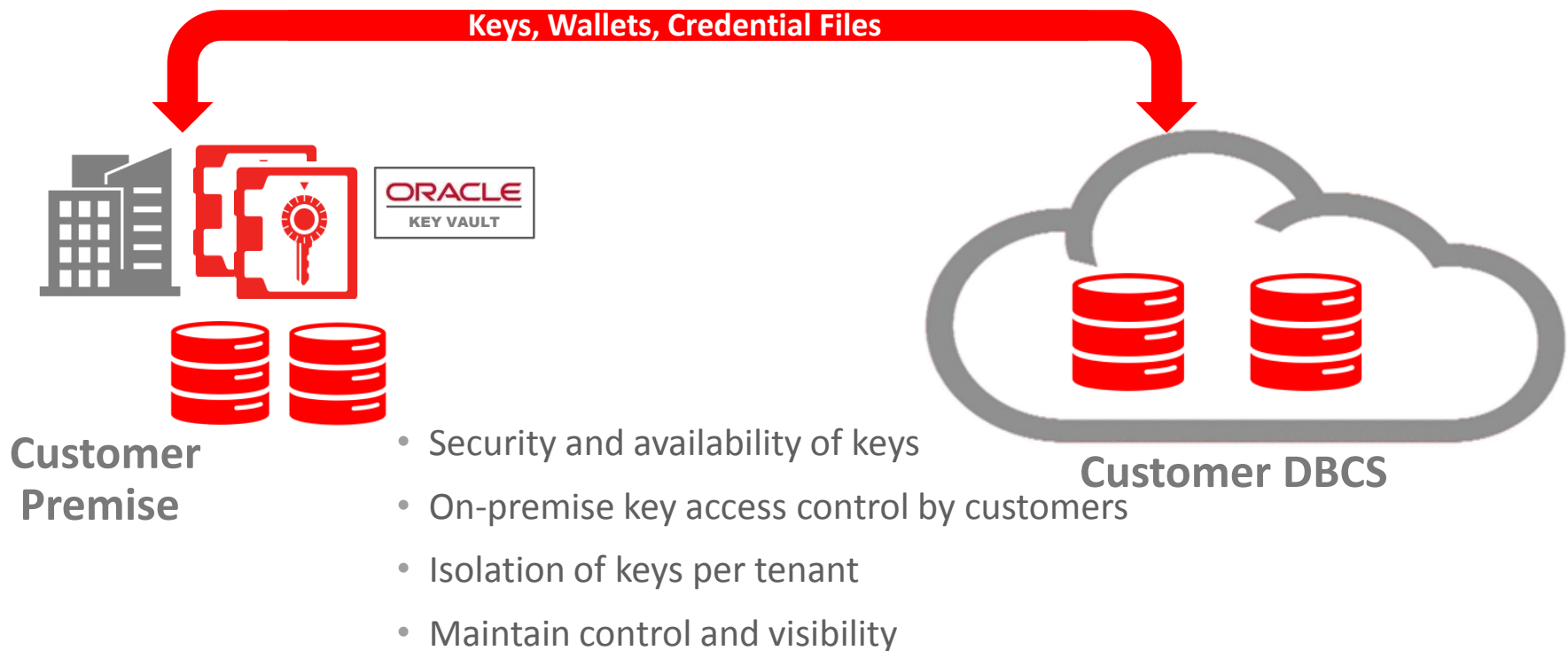
Select User

OKVADMIN

| Operation | Count | Percentage |
|----------------------------|-------|-------------|
| Add endpoint | 10 | <div></div> |
| Modify Endpoint Attributes | 8 | <div></div> |
| Add User | 5 | <div></div> |
| Create Wallet | 3 | <div></div> |
| Add Endpoint Group | 3 | <div></div> |
| Modify User Attributes | 3 | <div></div> |
| Modify Wallet | 1 | <div></div> |

1 - 7

Control Keys with On-Prem Key Vault





Database Security Data Subsetting and Masking Pack Technical Overview

Oracle Security Solutions

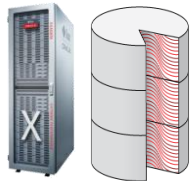


ORACLE DATABASE SECURITY

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®



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

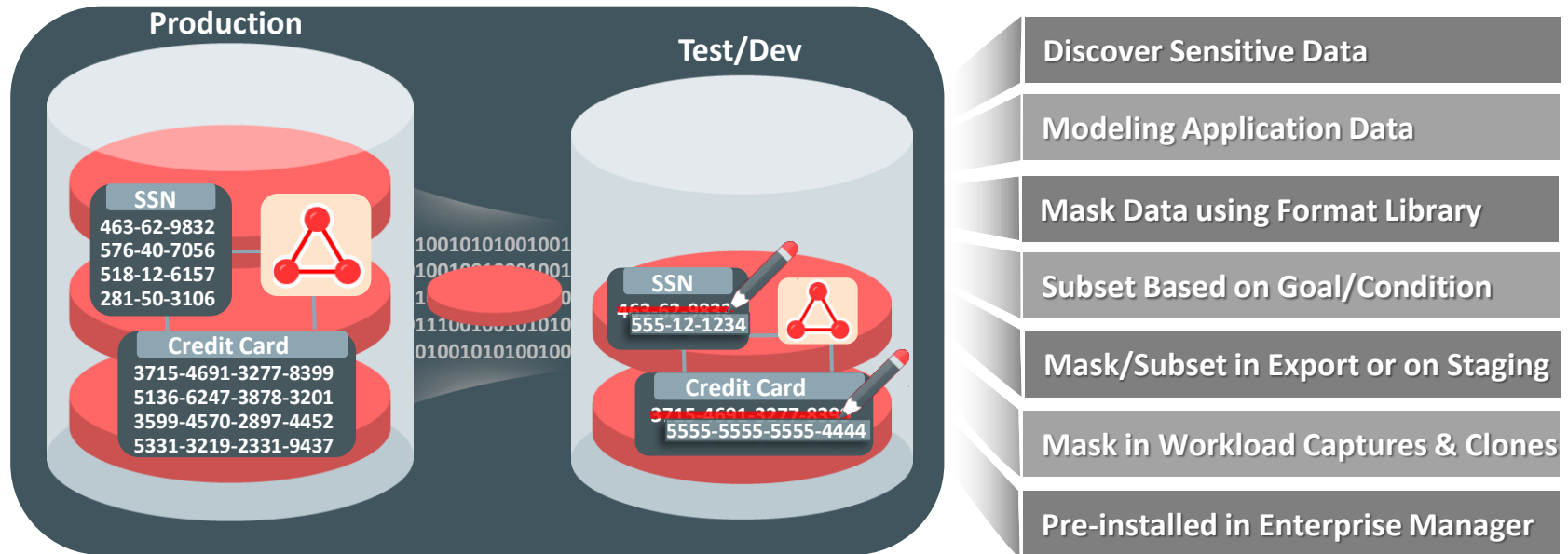
Will the Applications Continue to Work?

and More

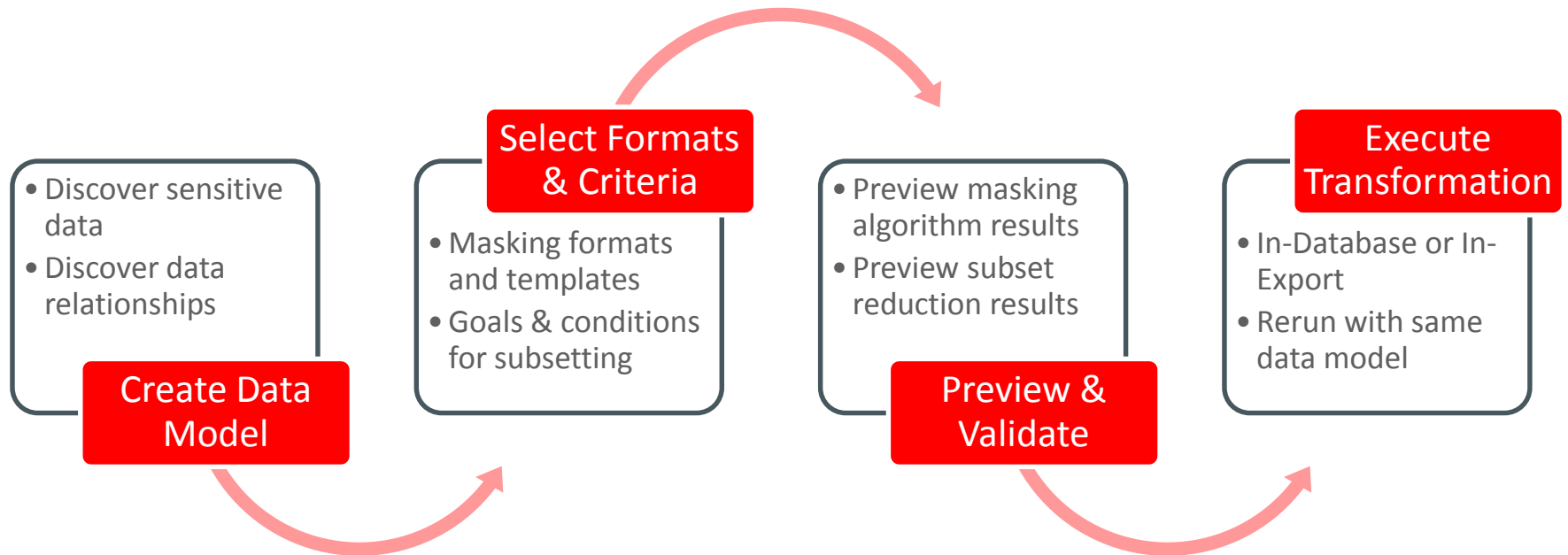
Oracle Data Masking and Subsetting Pack

ORACLE[®] 12^c
ENTERPRISE MANAGER

Reduces Risk in Sharing by Obfuscating or Removing Sensitive Data

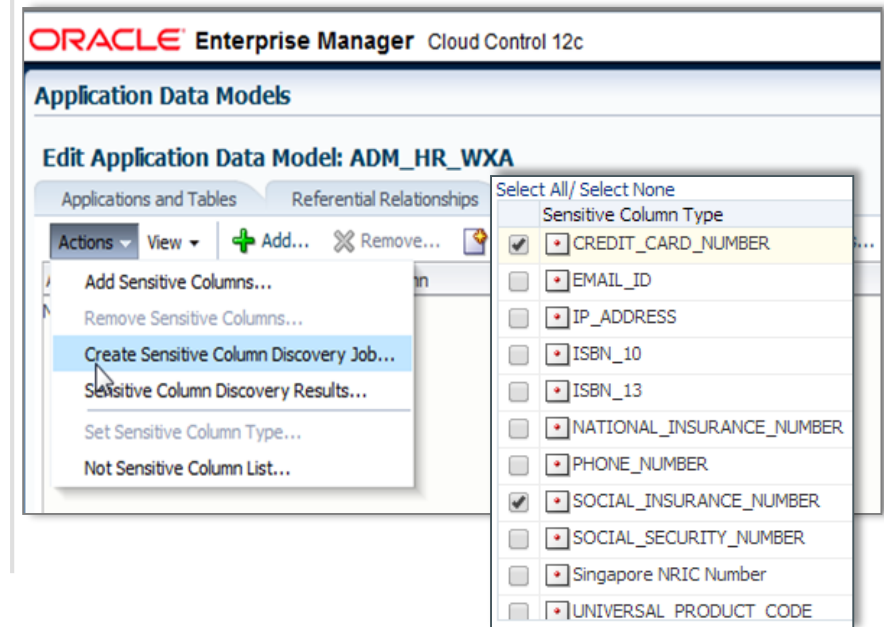
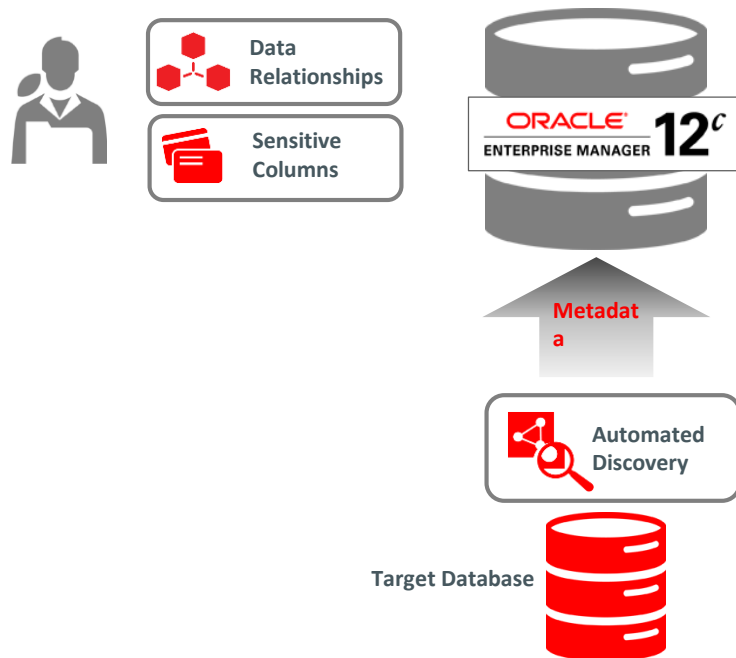


Data Masking and Subsetting Methodology



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

| Format | Description |
|--------------------------------------|--------------------------------|
| American Express Credit Card Number | ~10 billion unique American Ex |
| Discover Card Credit Card Number | ~10 billion unique Discover C |
| MasterCard Credit Card Number | ~10 billion unique MasterCard |
| Visa Credit Card Number | ~10 billion unique Visa |
| Generic Credit Card Number | ~10 billion unique |
| Generic Credit Card Number Formatted | ~10 billion unique |
| National Insurance Number Formatted | Gen |
| Social Insurance Number | ~1 b |
| Social Insurance Number Formatted | ~1 b |
| Social Security Number | ~71 |
| Social Security Number Formatted | ~71 |

Sample Masked Data
Samples are generated using defined format

- 3472105015722069
- 3749455677707248
- 3490749344336998
- 3782460947413526
- 3452029369341892

Refresh

Array List
▼

- Array List
- Delete
- Encrypt
- Fixed Number
- Fixed String
- Null Value
- Preserve Original Data
- Random Dates
- Random Decimal Numbers
- Random Digits
- Random Numbers
- Random Strings
- Shuffle
- SQL Expression**
- Substitute
- Substring
- Table Column
- Truncate
- User Defined Function

Comprehensive Masking Transformations

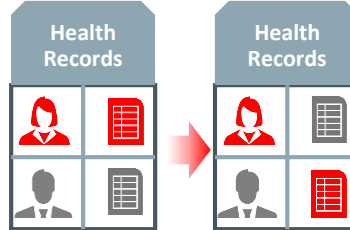
| | |
|----------------------------|--|
| Conditional masking | Masks rows differently based on condition <i>E.g. Mask national identifiers based on country</i> |
| Consistent masking | Ensures the masked values is same across multiple databases <i>E.g. Mask employee identifiers consistently across schemas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

Masking Examples

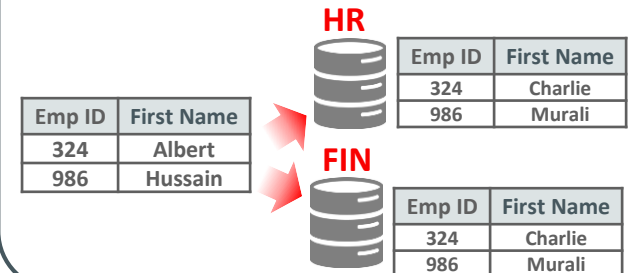
Mask Based on Condition

| Country | Identifier | Country | Identifier |
|---------|---------------|---------|---------------|
| CA | 226-956-324 | CA | 368-132-576 |
| US | 610-02-9191 | US | 829-37-4729 |
| UK | JX 75 67 44 C | UK | AI 80 56 31 D |

Shuffle Records



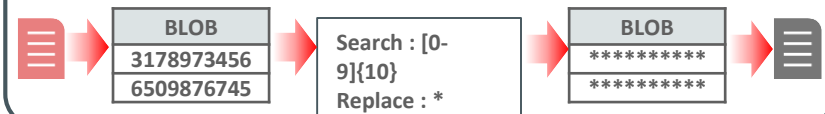
Generate Deterministic Output



Generate Random Values Preserving Format

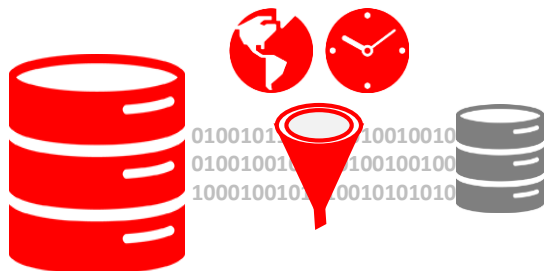
| Company | Closing Price | Company | Closing Price |
|---------|---------------|---------|---------------|
| IBFG | \$36.92 | IBFG | \$89.57 |
| XKJU | ¥789.8 | XKJU | ¥341.9 |

Mask Operating System Files stored as Blobs



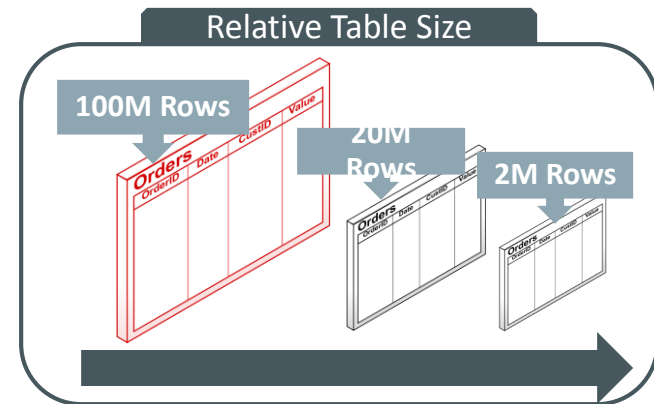
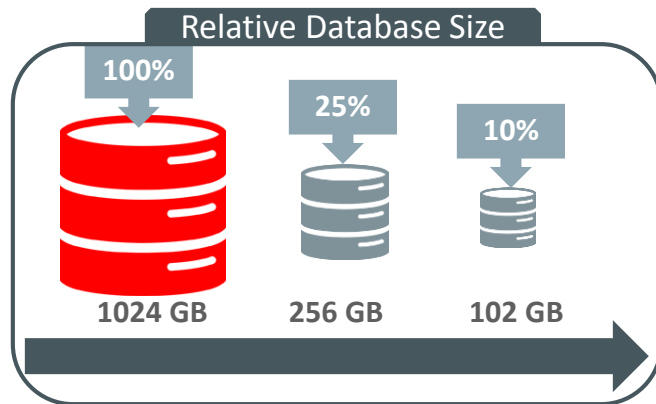
and more ...

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

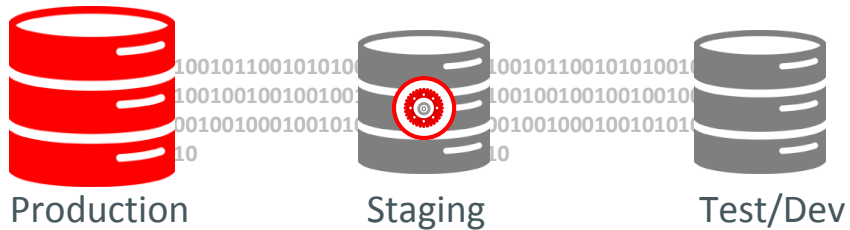


Preview and Validate Subset Results

| Applications Table Rules Column Rules Rule Parameters Space Estimates Data Masking Pre/Post Subset Script | | | | | | | |
|---|------------|-------------|------|-----------------------|------|------|--|
| Impact of subset rules on tables are displayed below. The values shown here are based on estimates and may not be accurate. | | | | | | | |
| View ▾ | | Refresh... | | | | | |
| 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 | |
| EMPLOYEE | Some Rows | 0.007 | 107 | 0.0001 | 1 | 0.93 | |
| LOCATION | 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 | |
| COUNTRIE | 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 | |

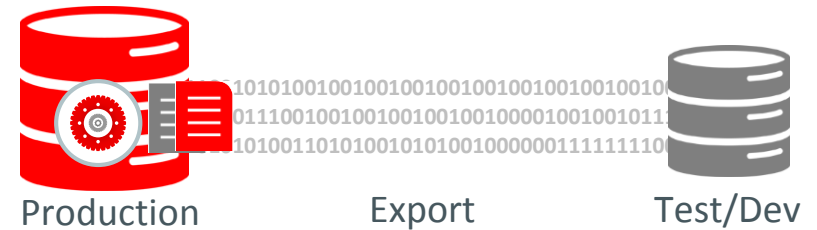
Deployment Options

In-Database



Minimal impact on the production environment

In-Export



Sensitive data remains within the production perimeter

Hardware and Software

The Oracle logo, consisting of the word "ORACLE" in white, uppercase, sans-serif font, centered within a solid red rectangular background.

ORACLE®

Engineered to Work Together