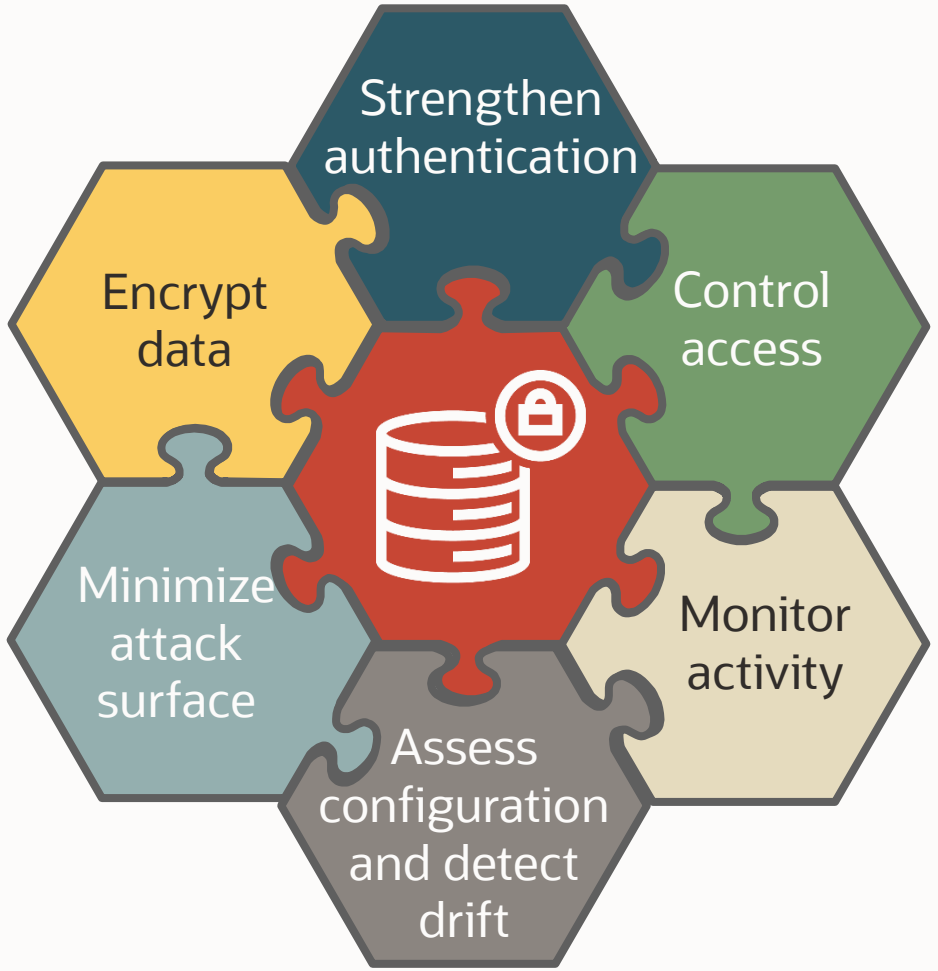
Security for Oracle Databases

On-Premises

Alexandre Fagundes
Cloud Architect, Oracle Corporation

Securing the Oracle Database

Securing the Oracle Database



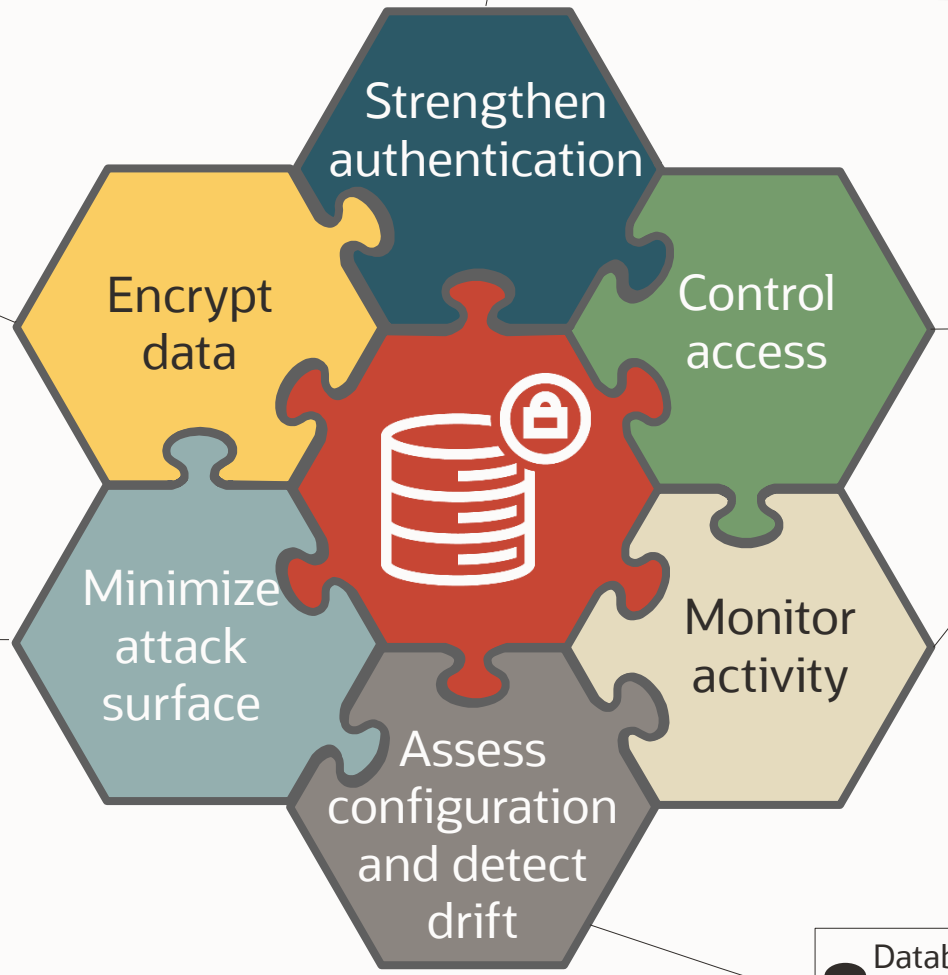
Getting down to details

- Database *Strong Authentication*
- Database *Centrally Managed Users*
- Database *IAM integration*
- Database *Password Profiles*

- Database *Roles and Privileges*
- Database *Centrally Managed Users*
- Database *Virtual Private Database*
- Database *Real Application Security*
- Database *Blockchain and immutable tables*
- Database Vault
- Label Security
- Advanced Security *Data Redaction*

- Advanced Security *Transparent Data Encryption*
- Key Vault

- Database *Native Network Encryption*
- Database *Transport Layer Security (TLS)*



- Data Safe *User Assessment*
- Database Security Assessment Tool
- Database *Privilege Analysis*

- Data Safe *Masking*
- Data Masking and Subsetting

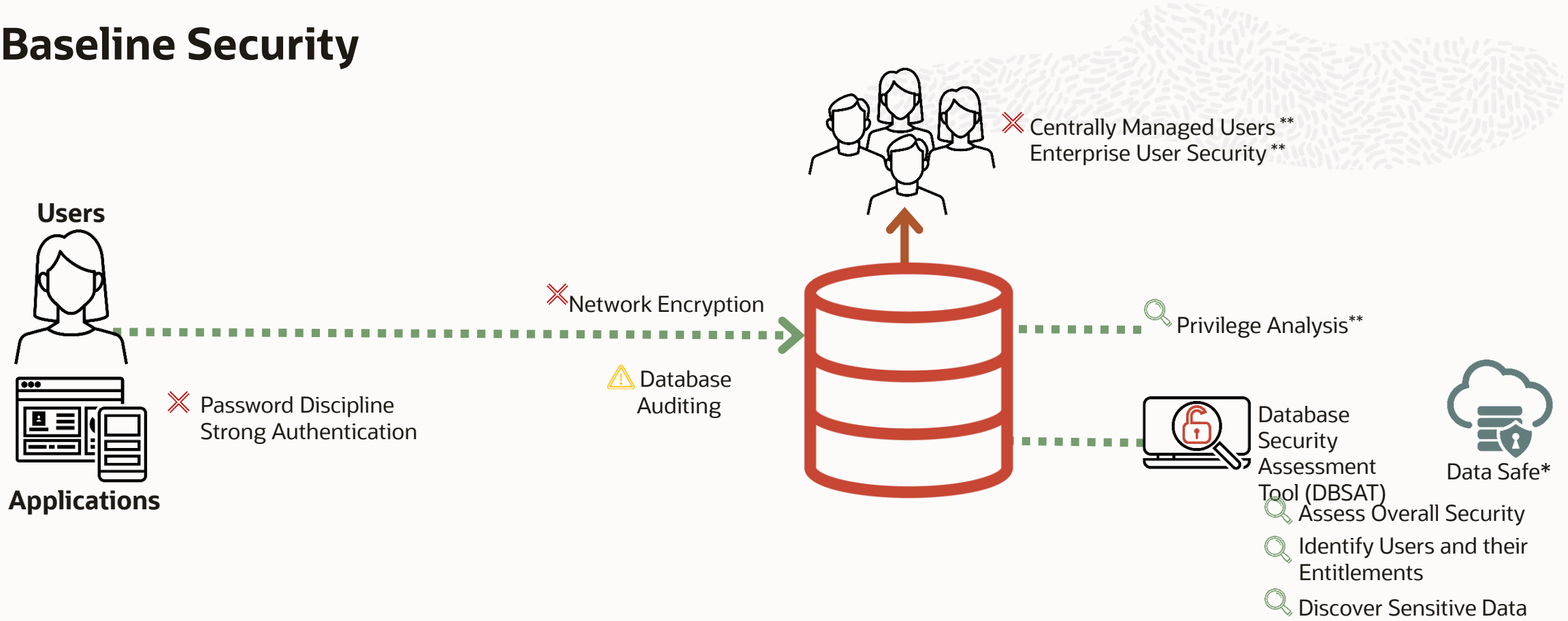
- Database *Unified Auditing*
- Audit Vault and Database Firewall
- Data Safe *Auditing*

- Database Security Assessment Tool
- Data Safe *Security Assessment*

Legend

- Feature
- Option
- Product
- Service

Baseline Security



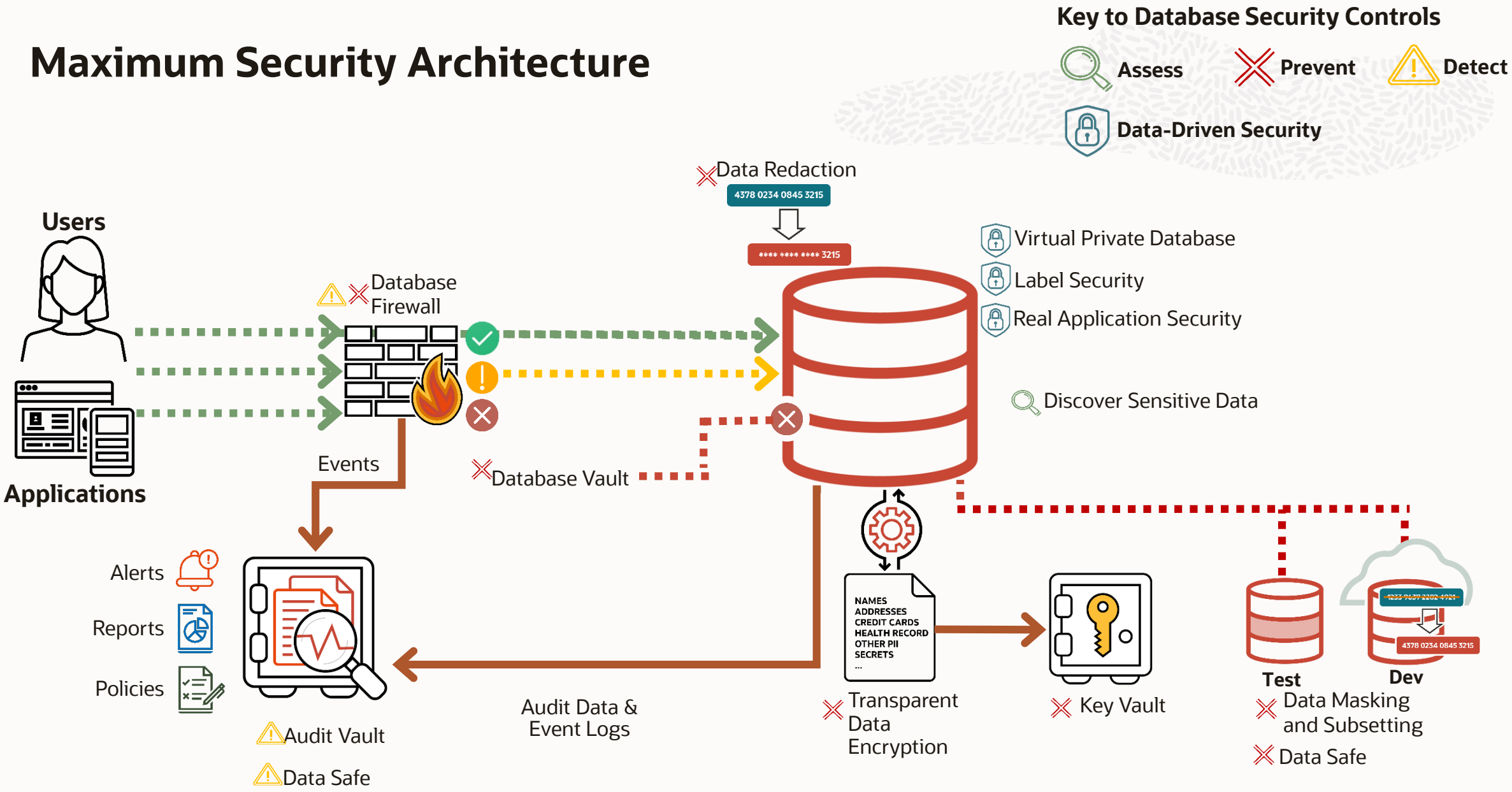
* Included with Database Cloud, additional cost on-premises

** Only available with Enterprise Edition

Key to Database Security Controls

Assess **Prevent** **Detect**

Maximum Security Architecture



How we look at Database Security

Assess

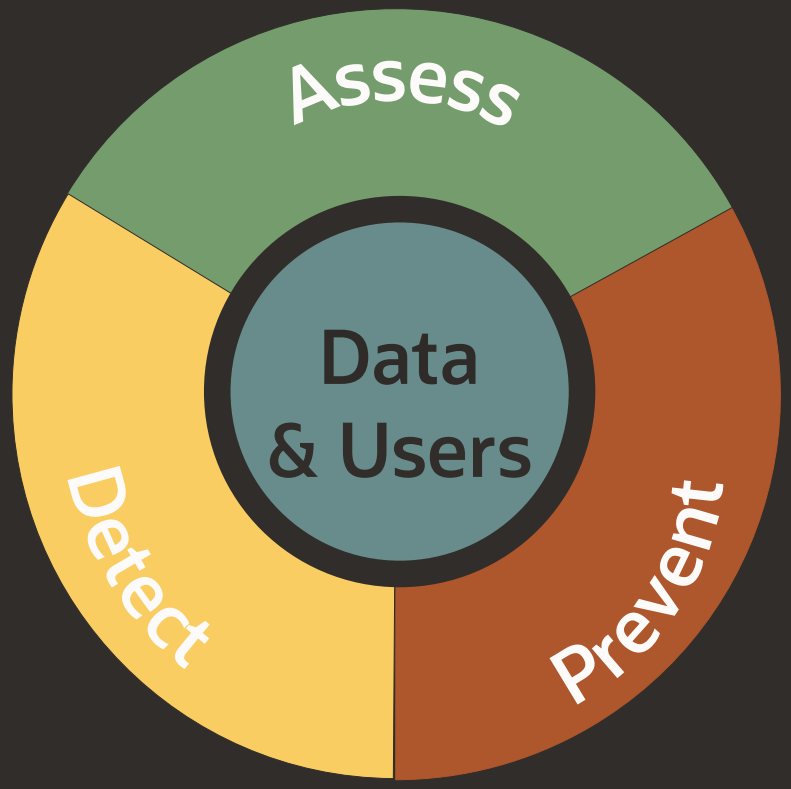
Assess the current state of security for the database

Detect

Detect attempts to access data, especially attempts that violate policy

Prevent

Prevent unauthorized or out-of-policy access to data



Data

Data stored in a database is your organization's most valuable asset, but also a source of significant risk.

Users

Users and applications connecting to your database are prime targets

Comprehensive security controls for Oracle Databases

Assess

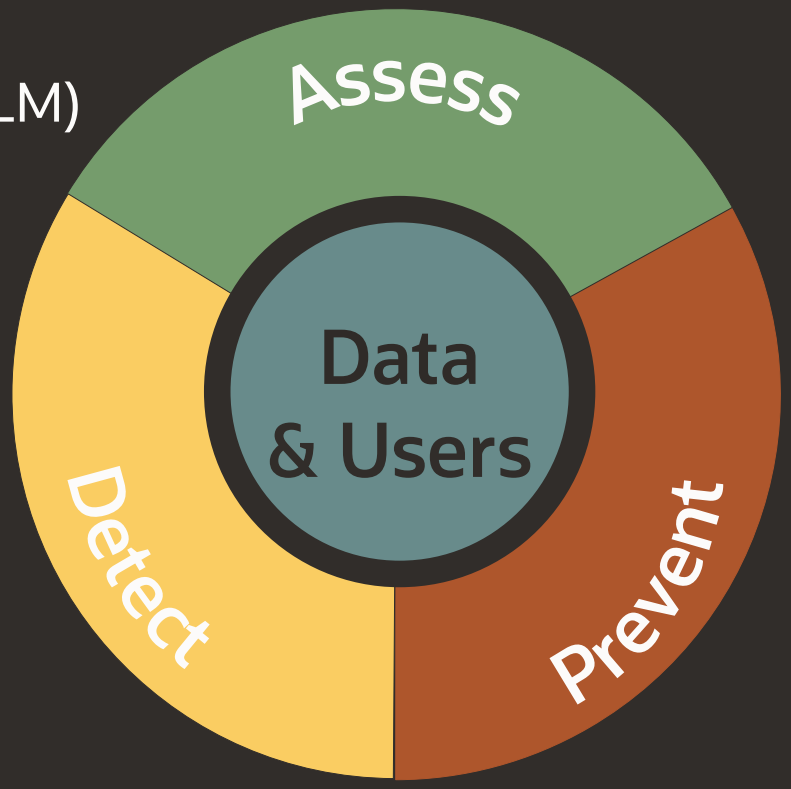
Config-Assessment(DBSAT, DBLM)
Data Discovery
Privilege Analysis*

Detect

Activity Auditing
Audit Vault
Database Firewall*

Prevent

Transparent Data Encryption & Key Vault
Data Masking, Data Redaction
Database Vault*



Data

Label Security
Virtual Private Database (VPD)
Real Application Security (RAS)*
DB Cryptographic Toolkit

Users

Password, PKI, Kerberos, Radius
Proxy Users, Password Profiles
Roles and Privileges
Oracle & Active Directory

* Unique to Oracle

Database Security Assessment Tool (DBSAT)

Assess

Let DBSAT help assess your security profile

Understand how (in)secure is your database

- Database securely configured
- Identify privileged users and risks you carry
- Discover your sensitive data for regulations

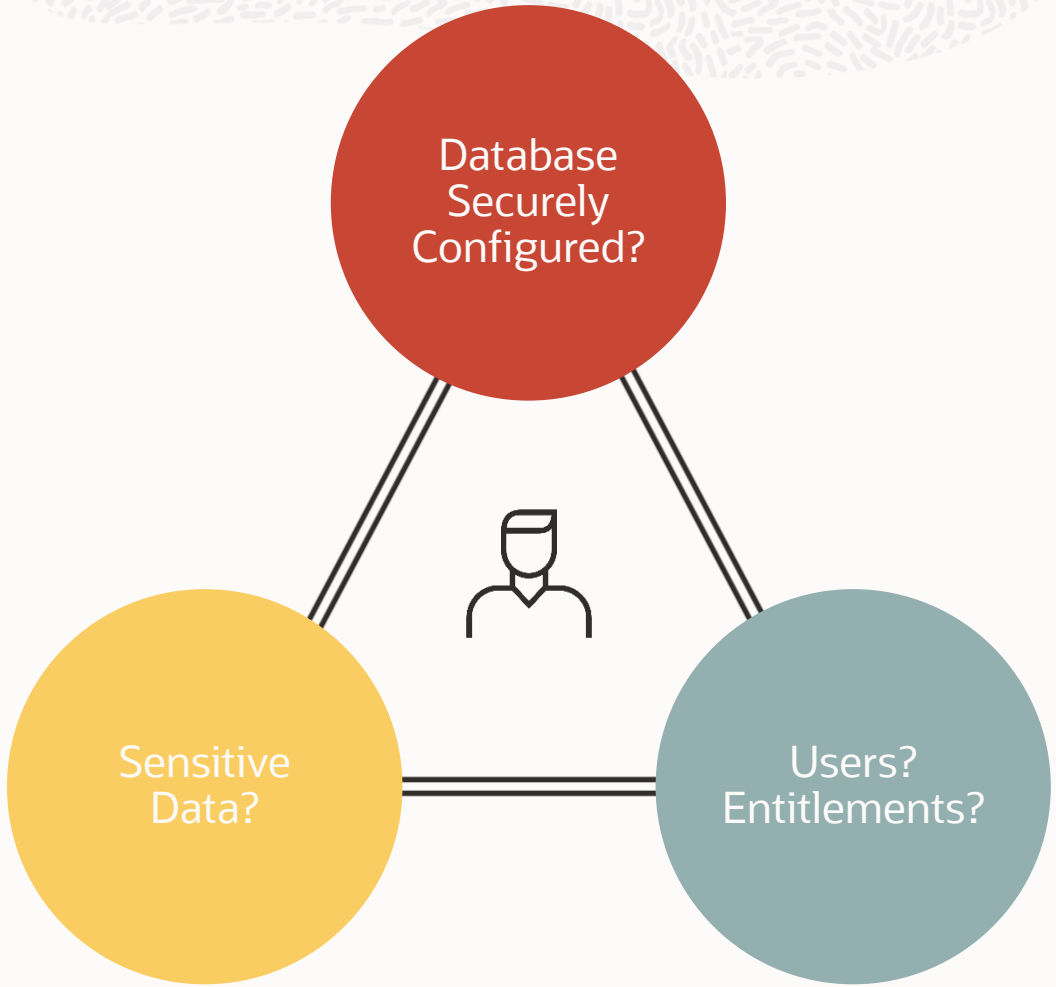
Actionable Reports

- Summary and detailed reports
- Prioritized recommendations
- CIS, STIG, GDPR findings

Analyze Oracle Database 11g and later

Stand-alone tool: Quick, Easy

FREE to current Oracle customers



Assess your database security before hackers come knocking

Assess Configuration

Patches

Data Encryption

Auditing policies

OS file permissions

Database configuration

Listener configuration

Fine-grained access control

Identify Risky Users

Database accounts

User privileges

User roles

Discover Sensitive Data

What type, where, and how much?

Sample pattern files for Greek, German, Dutch, French, Spanish, Italian, and Portuguese based data models as well.

Assessment Reports

Summary and detailed information

Prioritized, actionable and target specific recommendations

Mapping to EU GDPR, STIG and CIS Benchmark

Runs on 11g to 21c Oracle Databases

Sample Findings

INFO.PATCH CIS STIG

Status High Risk

Summary Latest comprehensive patch not found.

Details

```
Latest comprehensive patch: Jun 28 2018 (243 days ago)

SQL Patch History:
Action time: Mon Oct 15 2018 15:50:00
Action: APPLY
Version: 18.1.0.0.0
Description: OJVM RELEASE UPDATE: 18.3.0.0.180717 (27923415)

Action time: Mon Oct 15 2018 15:50:00
Action: APPLY
Version: 18.3.0.0.0
Description: Database Release Update : 18.3.0.0.180717 (28090523)
```

Remarks It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates, Patch Set Updates, and Bundle Patches on a regular quarterly schedule. These updates should be applied as soon as they are available.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.1
Oracle Database 12c STIG v1 r10: Rule SV-76029r2

USER.PASSWD CIS

Status Medium Risk

Summary Found 21 users not using password verification function.

Details

```
Profiles with password verification function:
    ORA_STIG_PROFILE(ORA12C_STIG_VERIFY_FUNCTION)
Profiles without password verification function: DEFAULT
Users without password verification function: ACME, ANONYMOUS, APEX_050100,
    APEX_LISTENER, APEX_PUBLIC_USER, APEX_REST_PUBLIC_USER, DBJSON, DBSAT,
    FLOWS_FILES, HR, HRREST, MYDBA, OBE, ORDS_PUBLIC_USER, PDBADMIN, SCOTT,
    SYS, SYSTEM, XDBEXT, XDBPM, XFILES
```

Remarks Password verification functions are used to ensure that user passwords meet minimum requirements for complexity, which may include factors such as length, use of numbers or punctuation characters, difference from previous passwords, etc. Oracle supplies several predefined functions, or a custom PL/SQL function can be used. Every user profile should include a password verification function.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 3.8

USER.DEFPWD CIS

Status High Risk

Summary Found 1 unlocked user account with default password.

Details

```
Users with default password: SCOTT
```

Remarks Default account passwords for predefined Oracle accounts are well known. Active accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2

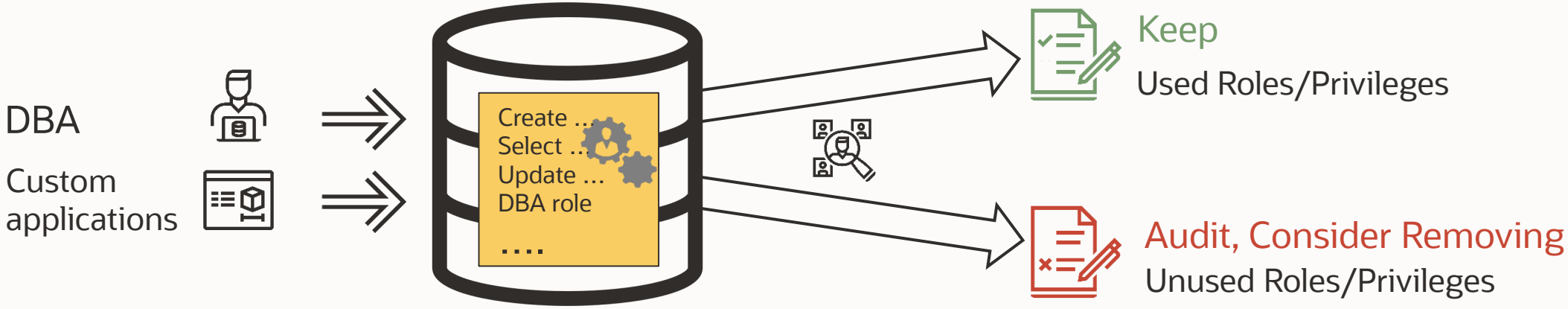
Sensitive Column Details

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type	Risk Level
FINACME	COMPANY_DATA	CITY	--	BIOGRAPHIC INFO - ADDRESS	CITY	High Risk
FINACME	COMPANY_DATA	STATE	--	BIOGRAPHIC INFO - ADDRESS	STATE	High Risk
FINACME	COMPANY_DATA	TAX_PAYER_ID	--	IDENTIFICATION INFO - PERSONAL IDS	TAX ID NUMBER (TIN)	High Risk
FINACME	COMPANY_DATA	ZIP	--	BIOGRAPHIC INFO - ADDRESS	POSTAL CODE	High Risk
HCM1	COUNTRIES	COUNTRY_NAME	--	BIOGRAPHIC INFO - ADDRESS	COUNTRY	High Risk

Privilege Analysis

Assess

Privilege Analysis



Track privilege/role usage by a database user for a period of time

Identify and consider removing unused privileges

Minimal performance impact – processing done during report generation

Moved to core database in November 2018. No dependency on Database Vault Licensing.

Unused Privileges Report

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

Used Privileges Report

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

Privilege Analysis Benefits

Work toward a least-privilege model

Reduce the impact of a compromised DBA account

Minimal performance impact during capture

Runs in individual CDBs or PDBs, not globally

Oracle Audit Vault and Database Firewall

Detect

Oracle Audit Vault and Database Firewall – Key differentiators

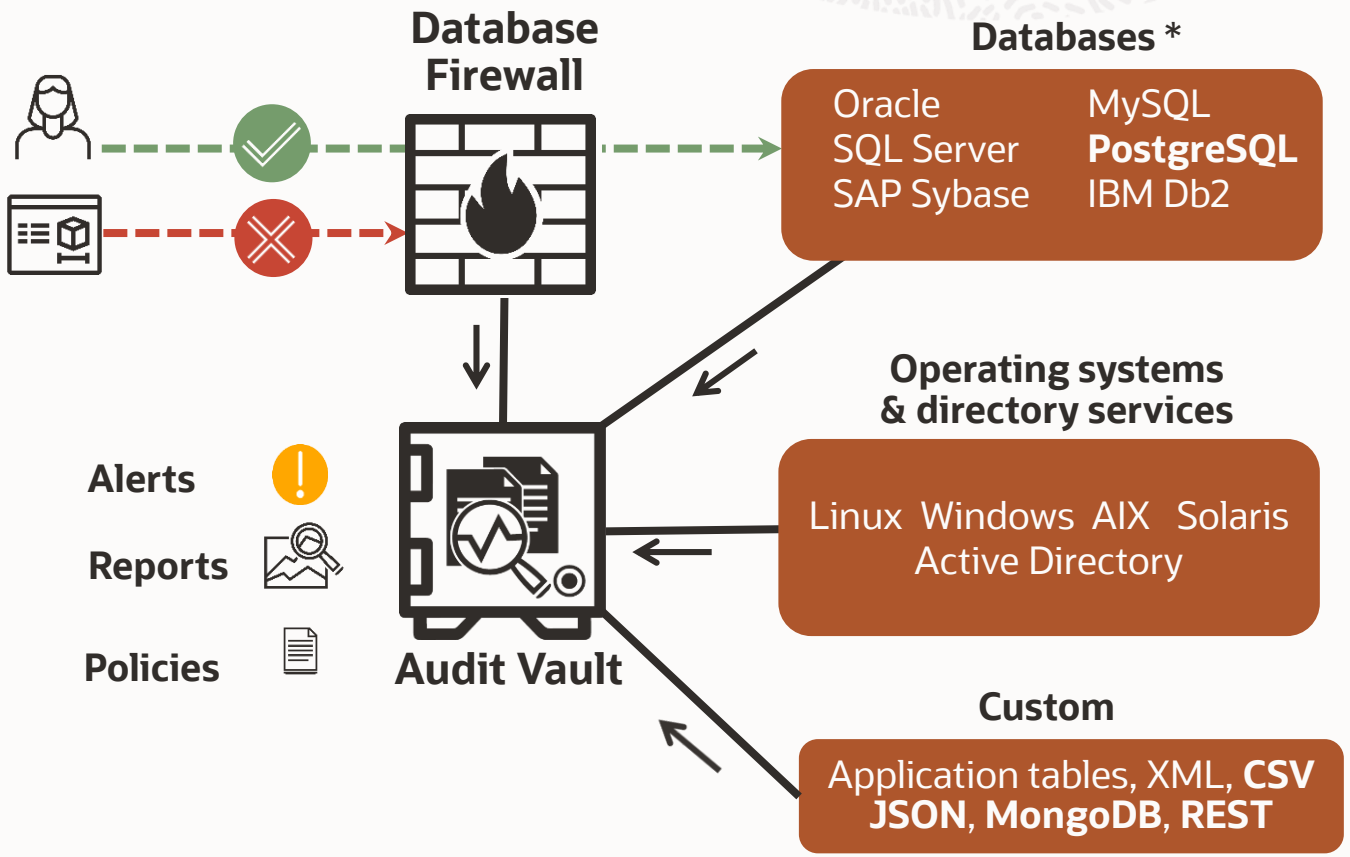
Monitoring network database activity AND collecting audit records

- Before/after values, entitlement changes , stored procedure changes
- SQL Injection detection and prevention based on SQL grammar analysis & clustering
- Enforce trusted path access for applications

Enterprise-level scale, security, automation, and extensibility

- An open schema for integration with third-party reporting tools
- Extensible with custom collector framework
- Supports on-premises & cloud databases
- Life-cycle support for audit data, archival

Address compliance requirements (LGPD, PCI, HIPAA, GDPR, CCPA, etc.)



* Audit log collection targets can be onprem or in the cloud

AVDF 20: What's new

Expanded audit collection

- Built-in support for PostgreSQL
- Extending custom collector support to include JSON, REST, MongoDB and CSV***
- Before/After values for Oracle databases
- Extending audit collection to Oracle Cloud autonomous databases – Dedicated***

Simplified database firewall

- Multi-stage firewall with simplified configuration
- Simpler policy creation using SQL cluster sets
- Session profile filtering in Database Object rule***
- NIC bonding for increased throughput
- Detect exfiltration attempts for SQL SELECT statements**

Modernized user interface

- Simplified navigation for common workflows
- Rich dashboards for auditors and admins
- Audit policy provisioning for Oracle with fine-grained enforcement for database users or roles***
- Unified console for audit and firewall management

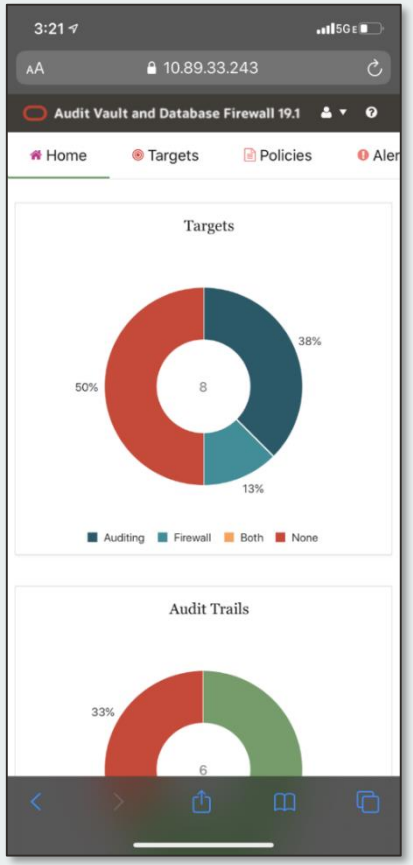
Improved enterprise support

- LDAP/Active Directory authentication
- Automated archiving of event data
- FIPS 140-2 compatibility***
- 2X audit collection rate capability***
- Multi-path Fiber Channel support for high availability
- Multiple IP addresses for agent in cluster setup**

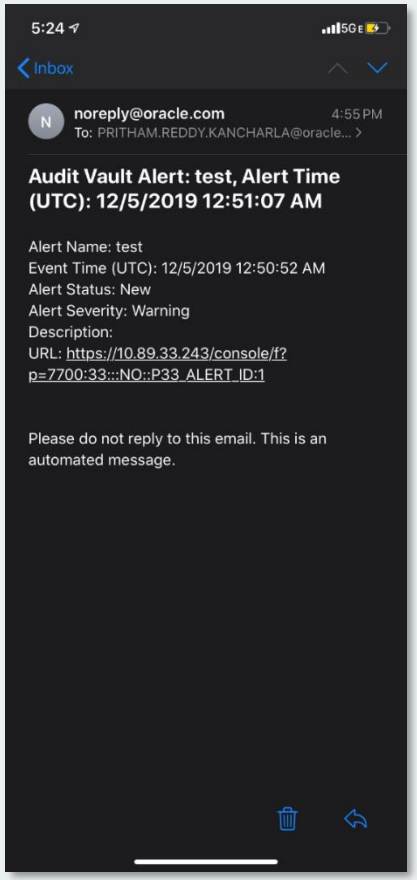
: Added in RU3 *: Added in RU4

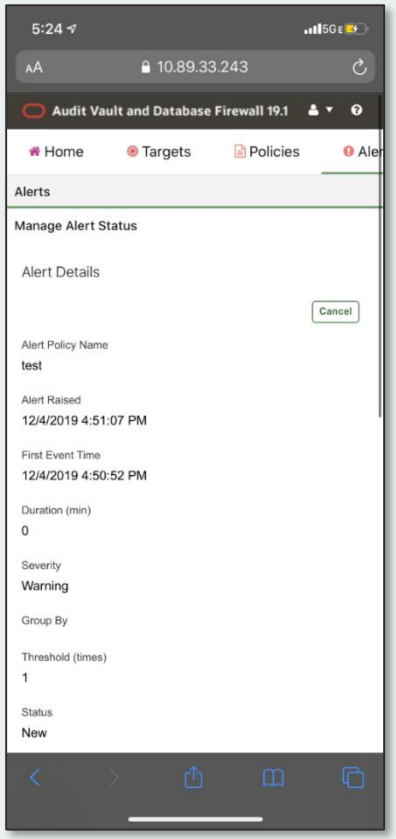
View AVDF 20 Reports and Alerts

Dashboard



Alerts





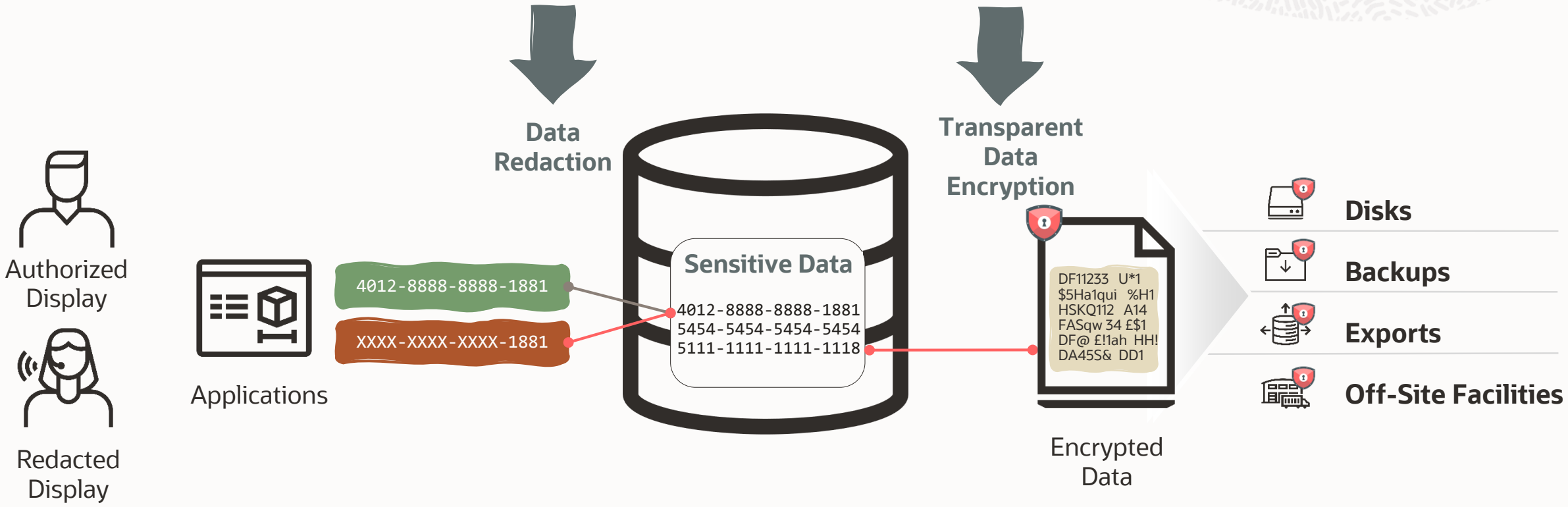
Oracle Audit Vault and Database Firewall Targets & Deployment Modes

- Supports both on premises and Cloud secured targets for audit log collection
- Can be deployed on-premises

Advanced Security

Prevent

Advanced Security Option



Transparent Data Encryption

Prevent

Why Encrypt Data?

Reduce risk of a data breach

- Data-at-rest, backups, exports are encrypted

Regulatory compliance

- Government regulation to protect personal data (GDPR, CCPA), patient data (HIPAA), credit card data (PCI-DSS), frequently require companies to encrypt

e.g. Under **GDPR**:

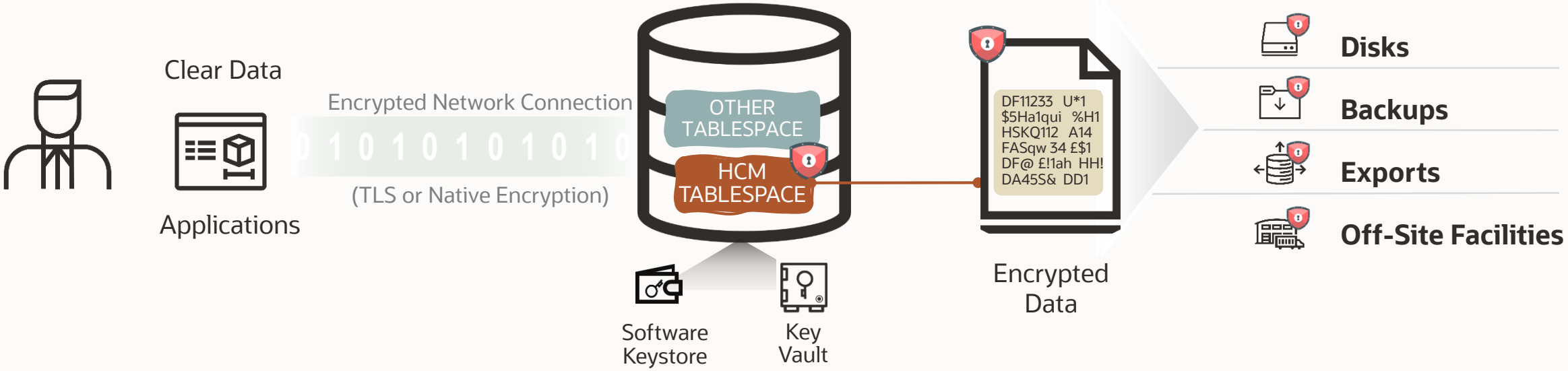
Article 34

Communication of a personal data breach to the data subject

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

Oracle Transparent Data Encryption (TDE)



Encrypts entire application tablespaces or an application column

Protects the database files on disk and in backups

No application changes required

Integrated with the Oracle technology stack

TDE Key Architecture

Two-tier encryption key

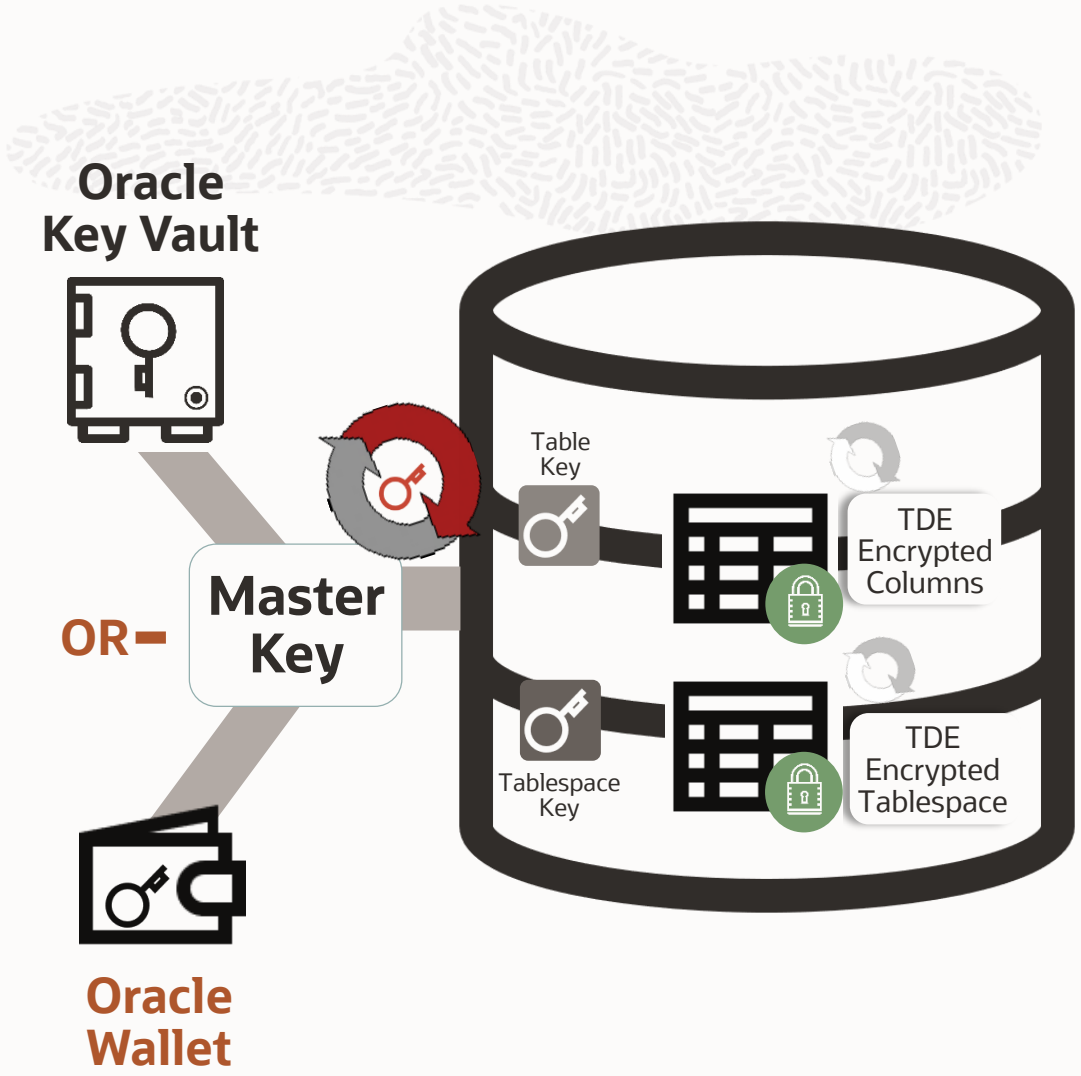
- Data Encryption Key (Table or Tablespace Key)
- Key Encrypting Key (Master Key)

Data encryption keys are created and managed by TDE automatically

The master encryption key encrypts the data encryption keys

The master key typically is stored outside of the database

- Wallet
- Key Management System (Key Vault)



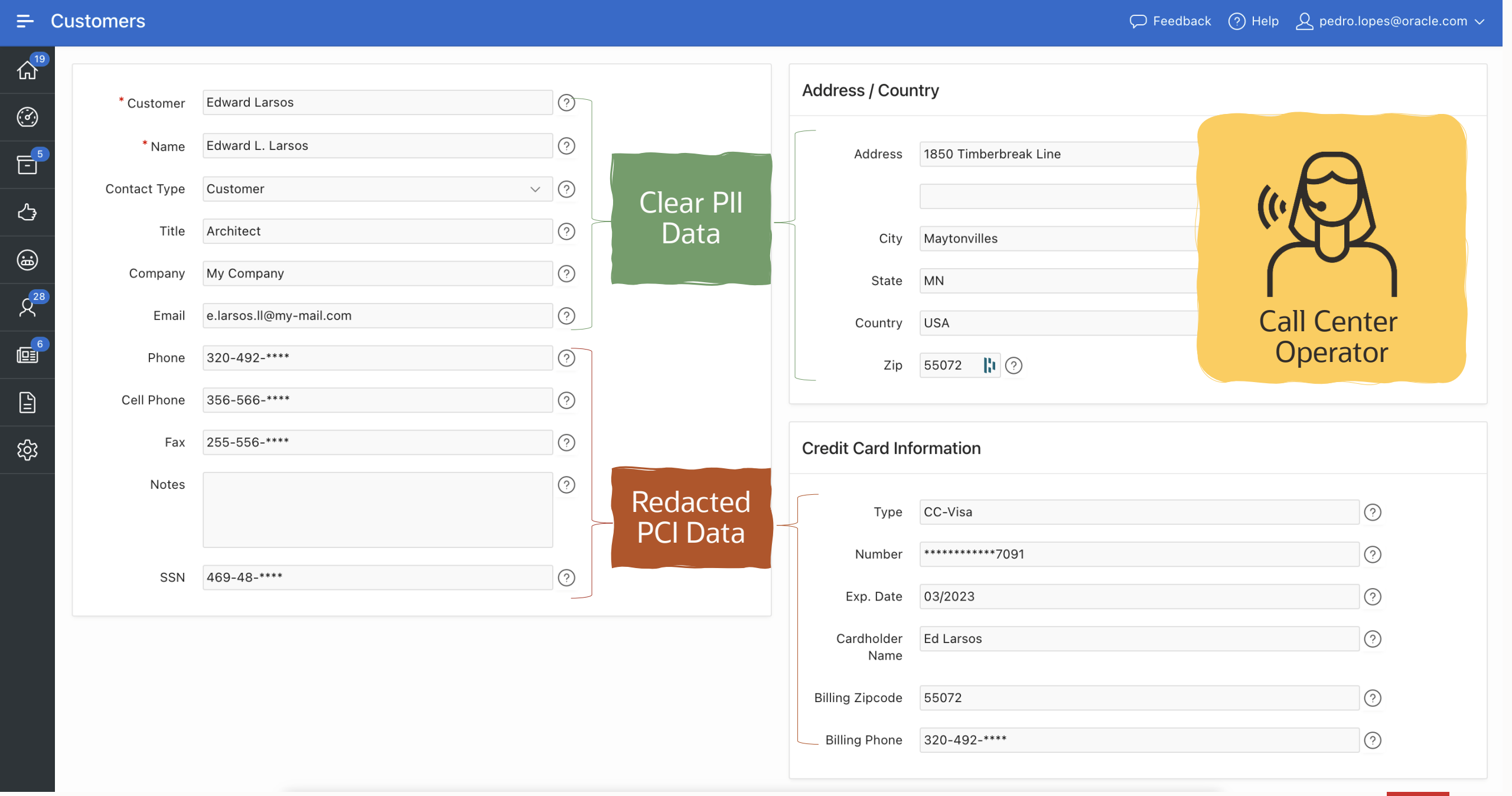
Data Redaction

Prevent

Data Redaction (Part of Advanced Security Option)

Oracle Data Redaction was introduced in **Oracle Database 12c** and back-ported to 11.2

- Dynamic masking of application data based upon username, IP, application context, and other session factors
- Library of redaction policies and point-and-click policy definition via EM

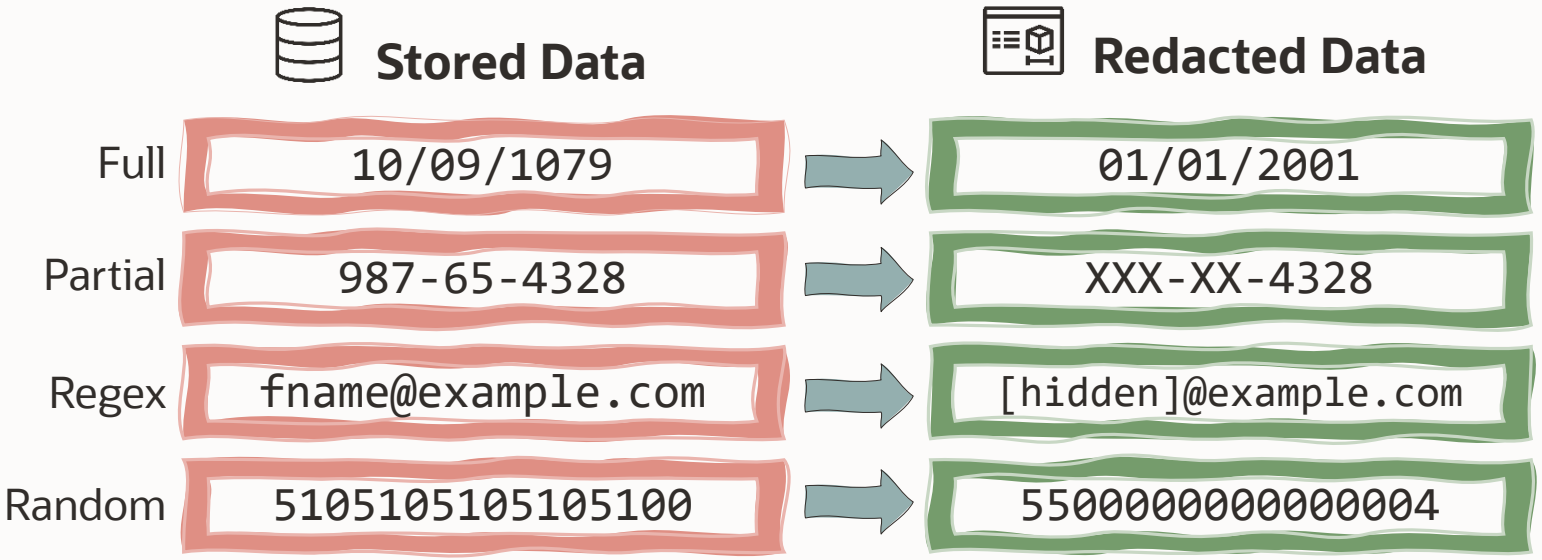


Data Redaction Target Use Cases

Usage Guidelines

Application screens with **read-only static pages** such as dashboard and reports. Good candidates include display-oriented screens, reports, and dashboards.	✓
Serve redacted data to APIs (GET)	✓
Application screens with **read-only static pages** such as dashboard and reports Using **GROUP BY** and **ORDER BY** operators	⚠
Application screens with **actives pages** such as forms which can post redacted data back to the database	✗
Privileged DB users (e.g. DBA) who can bypass applications and access redacted fields using **backend SQLs**	✗
Any DB user who can write **exhaustive and ad-hoc SQLs** to access redacted data . e.g. Multi-layered SQLs with several sub-queries; multiple joins using set operators such as UNION ALL; in-line views; and no-merge hint;	✗
As an alternative to VPD, OLS, Database Vault, and Data Masking(in test/dev)	✗

Supported Transformations



Data Masking and Subsetting

Prevent

Proliferation of sensitive data increases security risk

Your dilemma

To do, or not to do

Your wish

- Get actionable insights from your data to take smarter business decisions
- Use realistic data for development and analysis
- Quickly share data with developers, data scientists, and partners

The Solution?

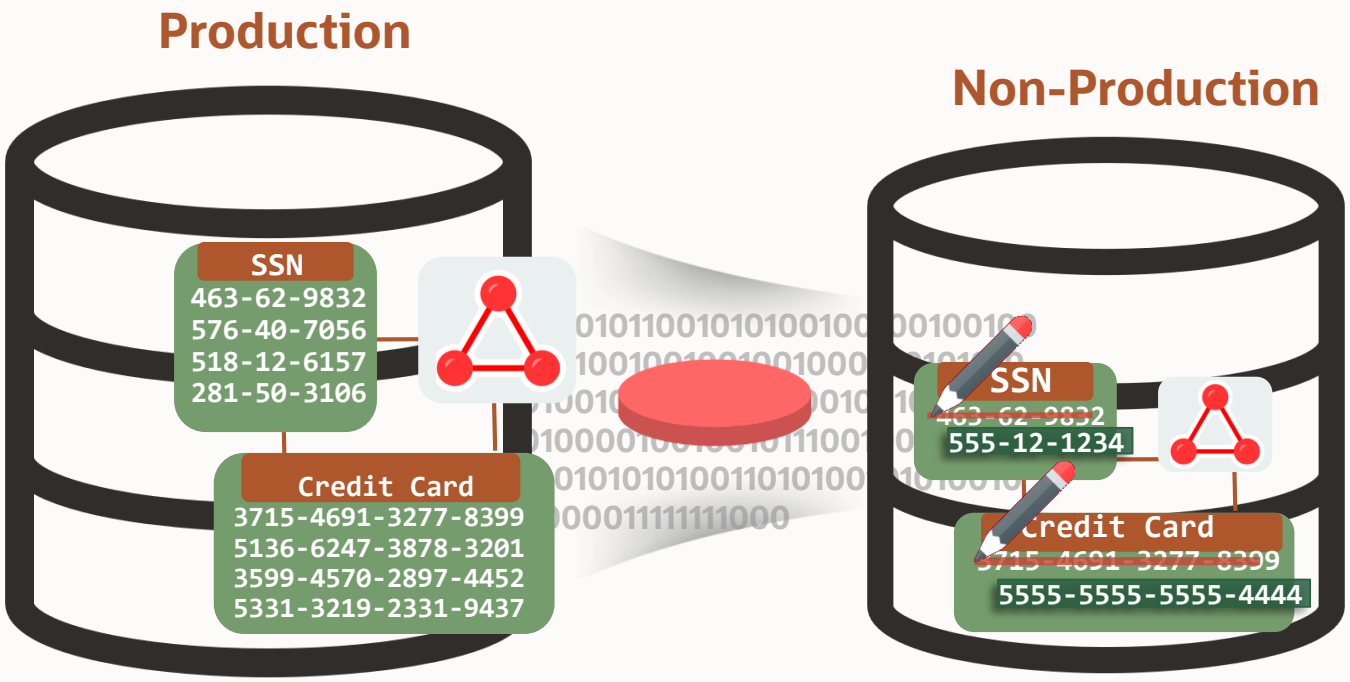
Your concern

- Avoid proliferation of sensitive data to non-production environments
- Comply with data privacy regulations such as GDPR
- Minimize time and storage costs

Oracle Data Masking and Subsetting

Minimize proliferation of sensitive data to non-production environment

ORACLE ENTERPRISE MANAGER 13c



- Sensitive Data Discovery
- Comprehensive Masking Options
- Goal/Condition Based Subsetting
- In-Database or In-Export Masking
- Support for Cloud and Non-Oracle DBs
- Workload Capture & Clone Masking
- Pre-installed in Enterprise Manager

Data Masking

Comprehensive and flexible masking formats

Common predefined masking formats

- Credit Card Number
- Social Security Number
- National Insurance Number

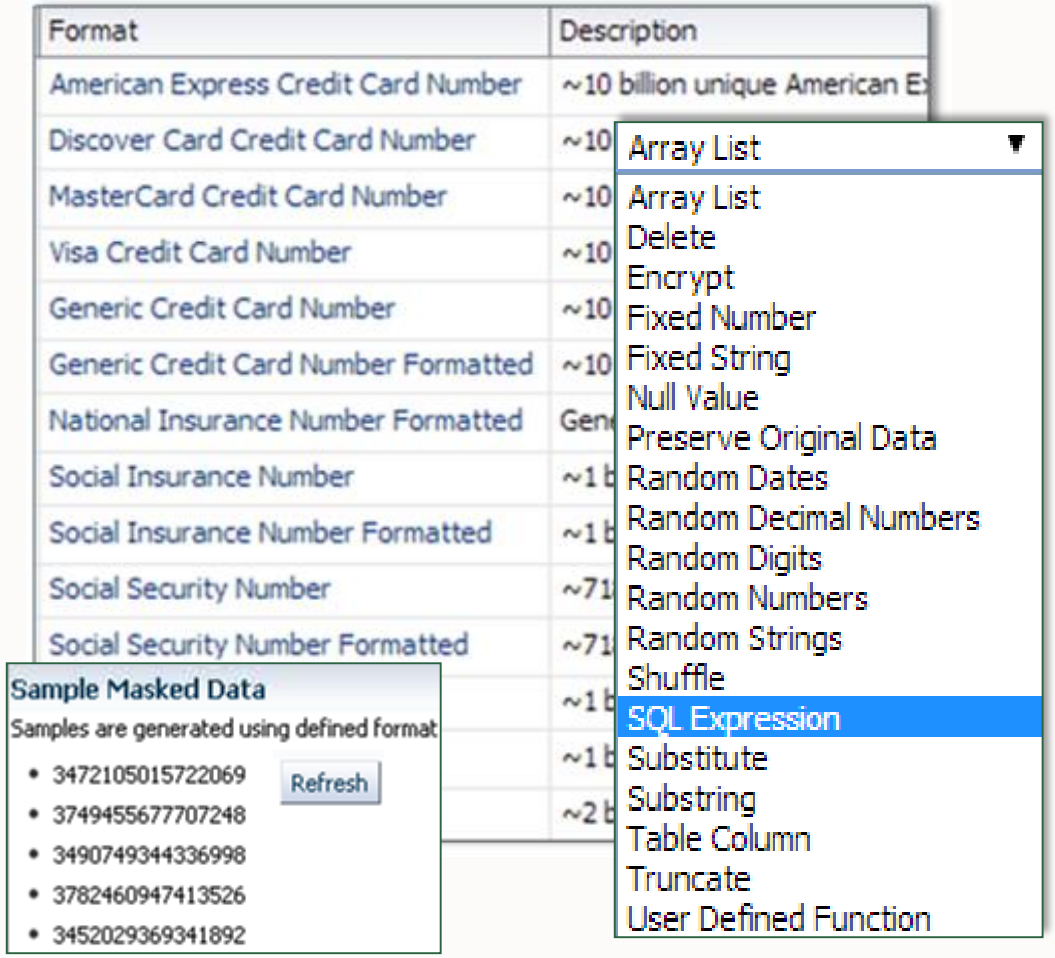
… and more

Flexibility to customize masking formats

- Fixed number / string
- Random numbers / strings / dates / list
- Substitute, Encrypt, Shuffle, Nullify
- User Defined PL/SQL Function

… and more

Sample masked values help preview and validate the masked data



Data Masking

Masking transformations to meet diverse business use cases

Conditional masking	Masks rows differently based on condition Example: Mask national identifiers based on country
Deterministic masking	Masks data to the same consistent values across multiple databases or masking jobs Example: Mask employee identifiers consistently across schemas and databases
Compound masking	Ensures masked values across related columns retain the same relationship Example: Mask address fields such as state, postal code, and country as a group
Format preserving	Masks data while preserving its format such as length and special characters Example: Mask tax identifiers while preserving spaces and hyphens
Reversible masking	Encrypts and decrypts data using cryptographic key Example: Unmask data after receiving the processed data from a partner
Shuffling	Shuffles the values within a column Example: Shuffle age of employees in a organization
Perturbation	Generates random values within a user-provided range Example: Generate random dates within a specified data range

Data Masking

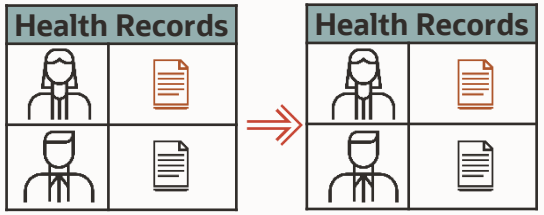
Examples

Mask based on conditions

Country	Identifier
CA	226-956-324
US	610-02-9191
UK	JX 75 67 44 C

Country	Identifier
CA	368-132-576
US	829-37-4729
UK	AI 80 56 31 D

Shuffle records



Generate deterministic output

Emp ID	First Name
324	Albert
986	Hussain

HR

Emp ID	First Name
324	Charlie
986	Murali

FIN

Emp ID	First Name
324	Charlie
986	Murali

Generate random values while preserving format

Name	License#
Richard	7ZPN788
Rishabh	DL 12TC 0204

Name	License#
Richard	5AMC942
Rishabh	KP 73GD 1948

Mask operating system files stored as LOBs

LOB
3178973456
6509876745

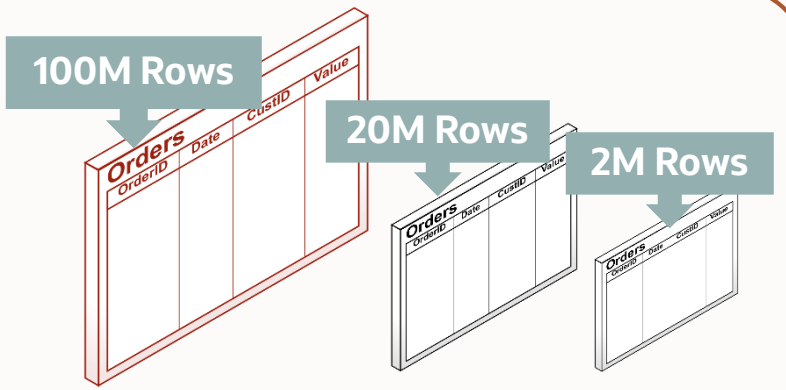
```
Search : [0-9]{10}
Replace : *
```

LOB
****
****

Data Subsetting

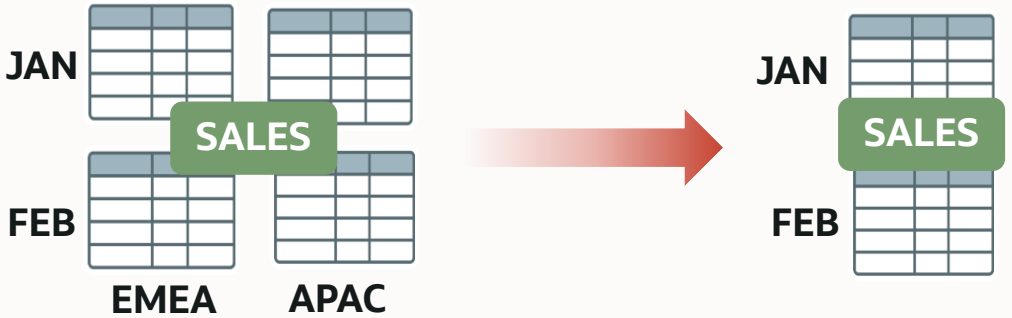
Goal or condition based subsetting

Relative Table Size



Condition Based

Table Partitions



Learn More

O.com: www.oracle.com/security/database-security/
OTN: www.oracle.com/database/technologies/security.html
Blog: http://blogs.oracle.com/cloudsecurity/db-sec

NEW: eBook 4th Edition: www.oracle.com/securingthedatabase

Oracle LiveLabs - Try it yourself:

- Database Security: https://bit.ly/golivelabsdbsec

Oracle LiveLabs

AskTOM Office Hours offers free, open Q&A sessions with Oracle Database PM/experts. We hold a LIVE session on the second Wednesday of each month, at 15:00 UTC

https://bit.ly/asktomdbsec

Ask Tom Database Security

ORACLE