ORACLE®

Welcome to

ITOUG

ITALIAN ORACLE USER GROUP

Soluzioni di sicurezza Oracle per la conformità al GDPR

Protezione del dato tramite Transparent Database Encryption

GDPR DATA PROTECTION 3 MONTHS until enforcement 25-May-2018

Natale Paonita
Oracle Principal Sales Consultant
Oracle Database Security

Febbraio, 2018

ORACLE

ITOUG ITALIAN ORACLE USER GROUP

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.

Agenda

- ➢ **Regolamento Europeo per la Protezione dei Dati Personali - GDPR**

- ➢ Oracle Database Maximum Security Architecture

- ➢ Oracle Advanced Security Option
  - TDE Nuove Funzionalità
  - TDE Impatti prestazionali
  - TDE Casi d’uso

Attori principali del GDPR

Attore	Descrizione
Interessato (Data Subject)	**persona fisica identificata o identificabile**. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Dato personale (Personal Data)	qualsiasi informazione riguardante l’Interessato, es.: **indirizzo, data nascita**, ecc..
Gestore Trattamento (Processor)	la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo **responsabile di qualsiasi operazione** o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come **la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione**.
Titolare del trattamento (Controller)	la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**
Autorità di controllo (Authority)	**autorità pubblica indipendente** istituita da uno Stato membro, agenzia di auditing
Destinatario (Recipient)	la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che **riceve comunicazione di dati personali, accede ai dati personali**

Principi Chiave di Sicurezza del GDPR

Obblighi del Titolare del Trattamento (controller) e del Gestore del Trattamento (processor)

VALUTARE	PREVENIRE	INVESTIGARE
Processi Organizzativi, Analisi di Rischi	Cifratura, Pseudonimizzazione, Anonimizzazione, Controlli di Accesso a Grana Fine, Controllo degli Accessi Privilegiati, Separazione delle Funzioni	Auditing, Monitoraggio delle Attività, Allertamento, Reporting

Oracle e il GDPR

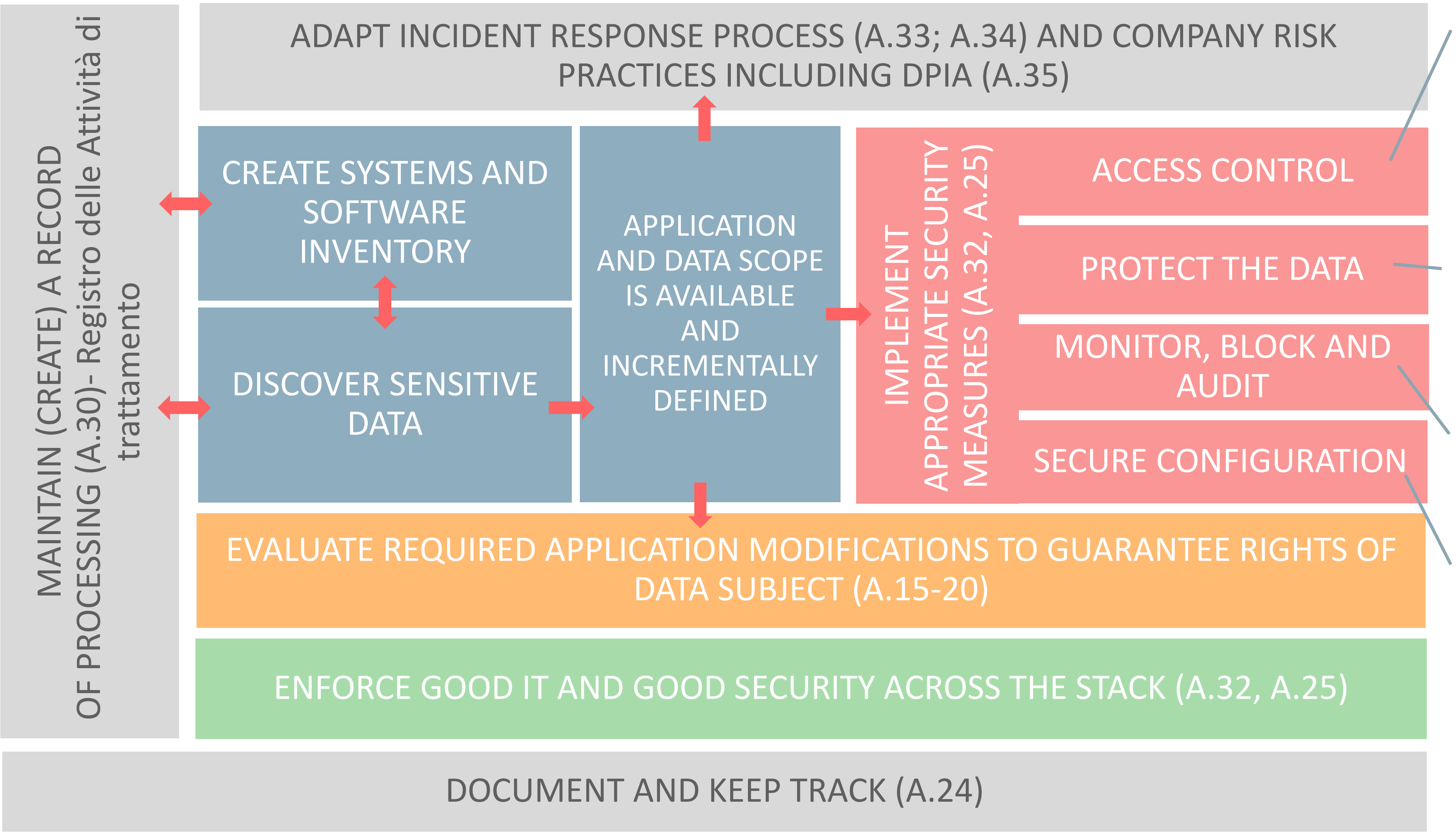
- Oracle è un “data controllers” nei confronti dei dati personali dei suoi dipendenti

- Oracle è un “processor” quando fornisce ai suoi clienti servizi cloud (ospitandone i dati personali)

- Oracle è un ” technology provider ” quando fornisce soluzioni (prodotti e servizi) per supportare i clienti in merito alla compliance alla normativa

ORACLE

Un percorso verso il GDPR – compiti e attività



MAINTAIN (CREATE) A RECORD OF PROCESSING (A.30)- Registro delle Attività di trattamento

ADAPT INCIDENT RESPONSE PROCESS (A.33; A.34) AND COMPANY RISK PRACTICES INCLUDING DPIA (A.35)

CREATE SYSTEMS AND SOFTWARE INVENTORY

DISCOVER SENSITIVE DATA

APPLICATION AND DATA SCOPE IS AVAILABLE AND INCREMENTALLY DEFINED

IMPLEMENT APPROPRIATE SECURITY MEASURES (A.32, A.25)

ACCESS CONTROL

PROTECT THE DATA

MONITOR, BLOCK AND AUDIT

SECURE CONFIGURATION

EVALUATE REQUIRED APPLICATION MODIFICATIONS TO GUARANTEE RIGHTS OF DATA SUBJECT (A.15-20)

ENFORCE GOOD IT AND GOOD SECURITY ACROSS THE STACK (A.32, A.25)

DOCUMENT AND KEEP TRACK (A.24)

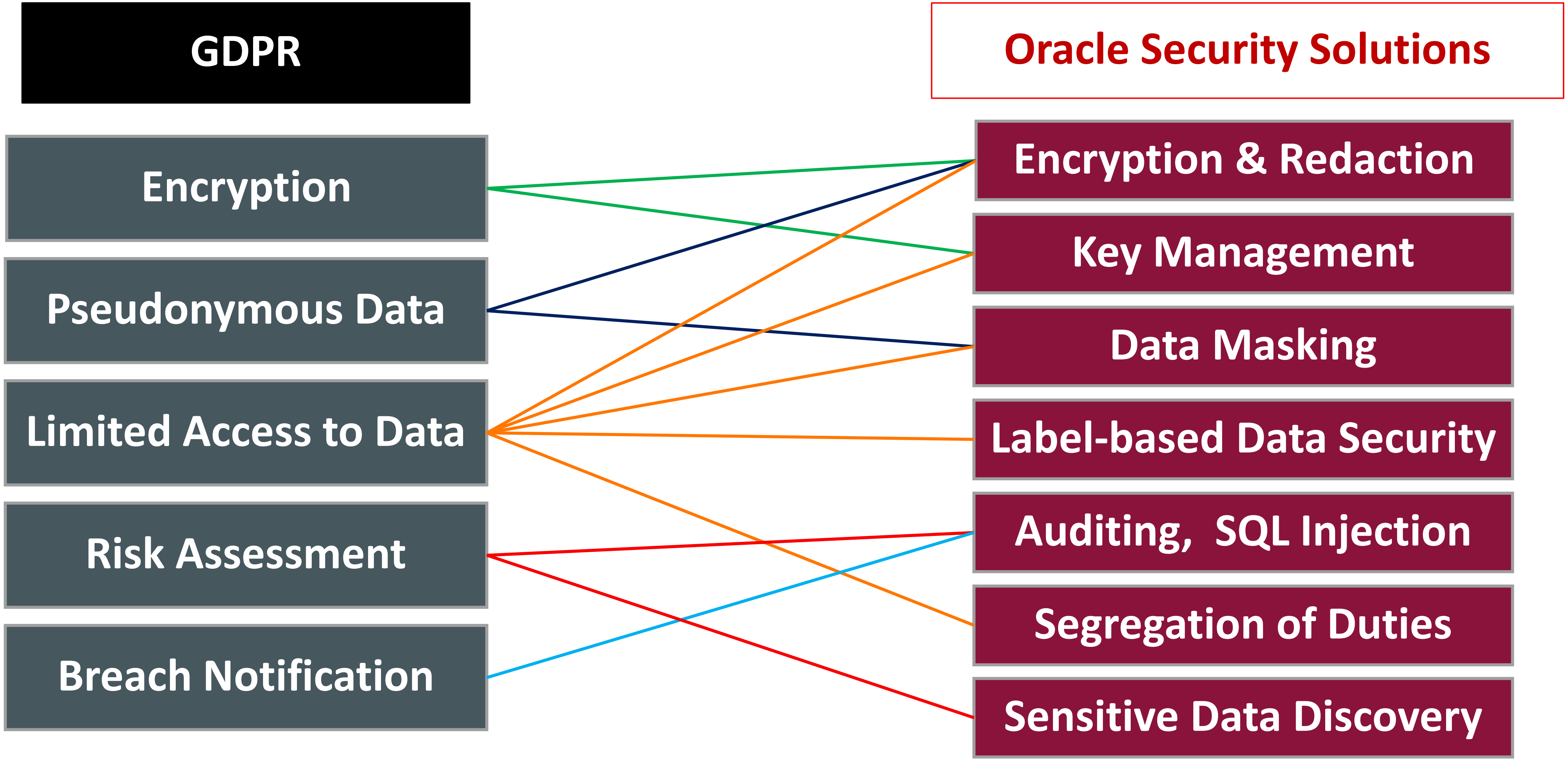
Modernize identity management to guarantee authentication and authorization both for business user and IT personnel

Protect the data wherever it is (encryption A.32) and avoid using real data where non necessary (A.5 and W.26)

Collect, secure and analyze audit logs and implement boundary defenses

Secure configurations, remediate vulnerabilities, and control production baselines

Soluzioni Oracle DB che assistono alla GDPR compliance



GDPR

Oracle Security Solutions

Encryption

Pseudonymous Data

Limited Access to Data

Risk Assessment

Breach Notification

Encryption & Redaction

Key Management

Data Masking

Label-based Data Security

Auditing, SQL Injection

Segregation of Duties

Sensitive Data Discovery

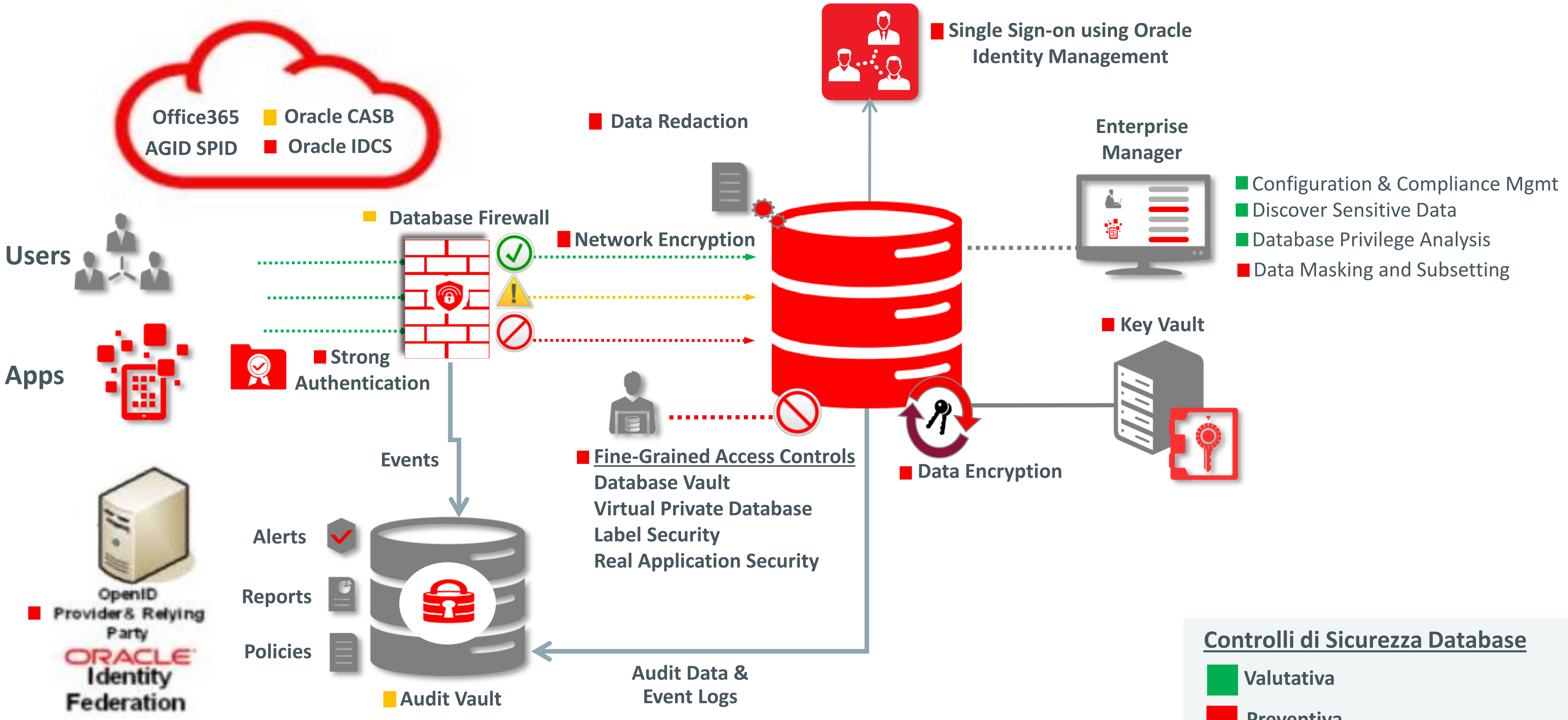
Agenda

- Regolamento Europeo per la Protezione dei Dati Personali – GDPR

- **Oracle Database Maximum Security Architecture**

- Oracle Advanced Security Option
  - TDE Nuove Funzionalità
  - TDE Impatti prestazionali
  - TDE Casi d’uso

Oracle Database Maximum Security Architecture



Office365 🟨 Oracle CASB

AGID SPID 🟥 Oracle IDCS

🟥 Single Sign-on using Oracle Identity Management

🟥 Data Redaction

Enterprise Manager

🟩 Configuration & Compliance Mgmt

🟩 Discover Sensitive Data

🟩 Database Privilege Analysis

🟥 Data Masking and Subsetting

Users

Apps

🟨 Database Firewall

🟥 Network Encryption

🟥 Strong Authentication

🟥 Key Vault

Events

🟥 Fine-Grained Access Controls
Database Vault
Virtual Private Database
Label Security
Real Application Security

🟥 Data Encryption

🟥 OpenID Provider & Relying Party
ORACLE Identity Federation

Alerts

Reports

Policies

🟨 Audit Vault

Audit Data & Event Logs

Controlli di Sicurezza Database

🟩 Valutativa

🟥 Preventiva

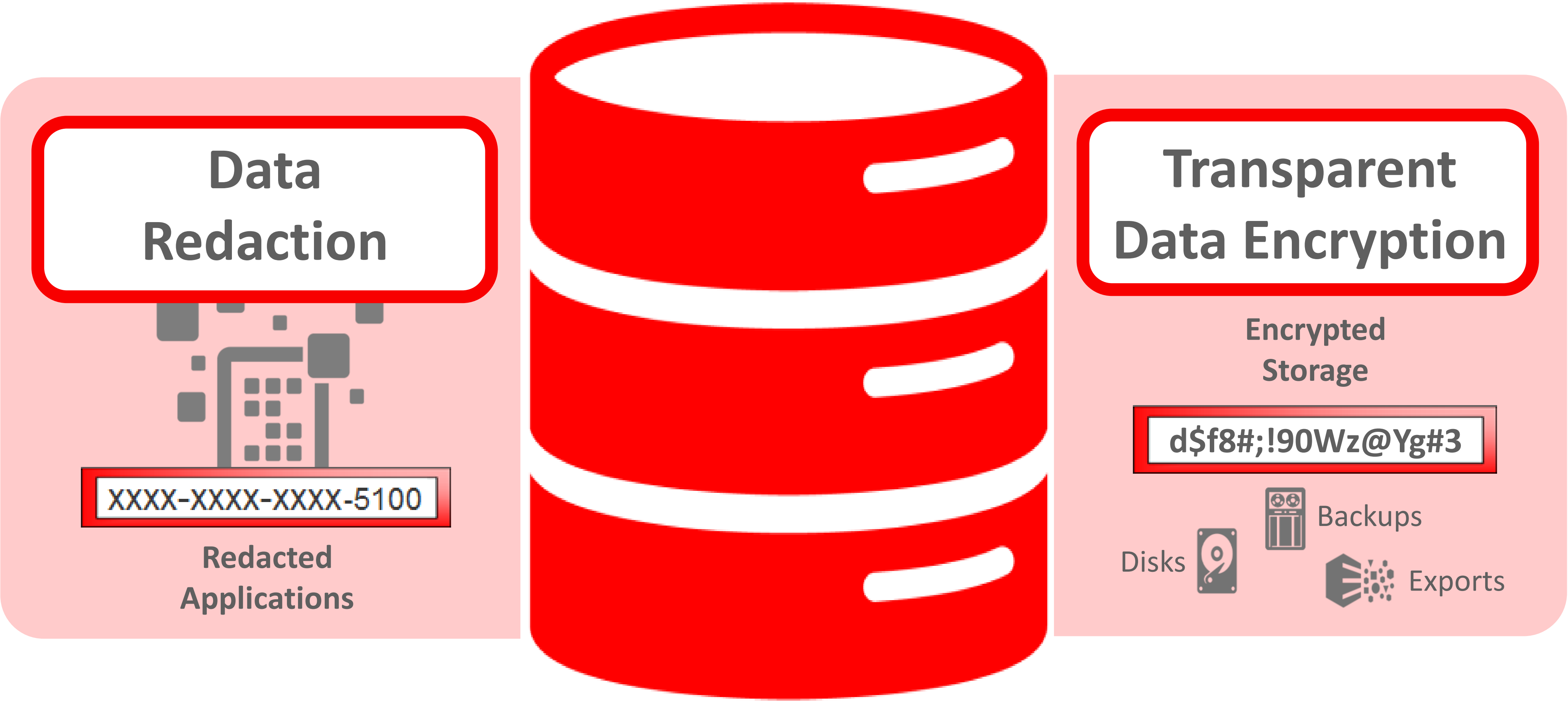
🟨 Investigativa

Agenda

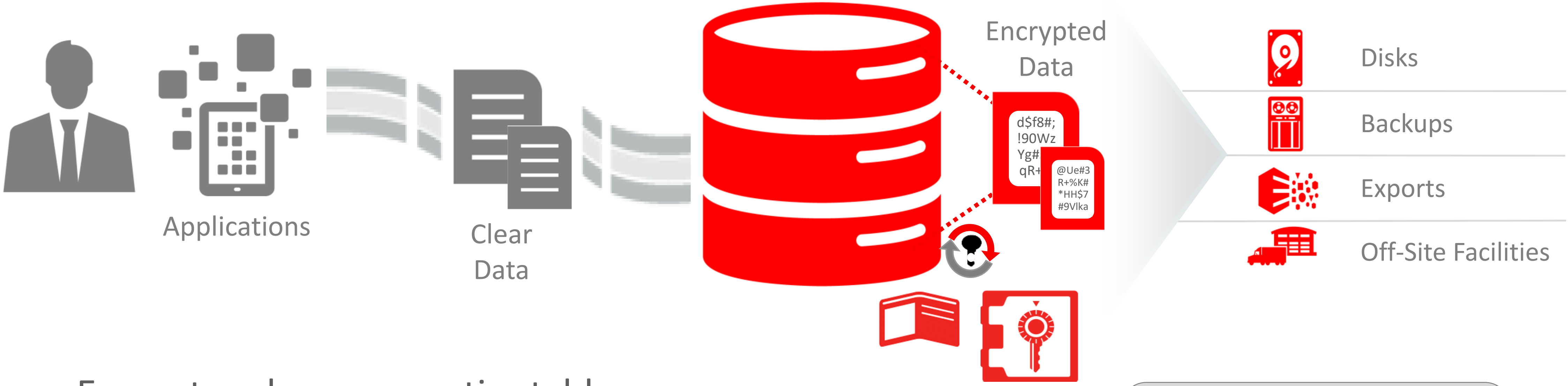
- General Data Protection Regulation
- Oracle Database Maximum Security Architecture
- **Oracle Advanced Security Option**
  - **TDE Nuove Funzionalità**
  - TDE Impatti prestazionali
  - TDE Casi d'uso

ORACLE

Oracle Advanced Security



Transparent Data Encryption is Foundation – Art.32 GDPR



- Encrypts columns or entire tablespaces
- Protects the database files on disk and on backups
- High-speed performance
- Integrated with Oracle DB technologies
- Transparent to applications, no changes required

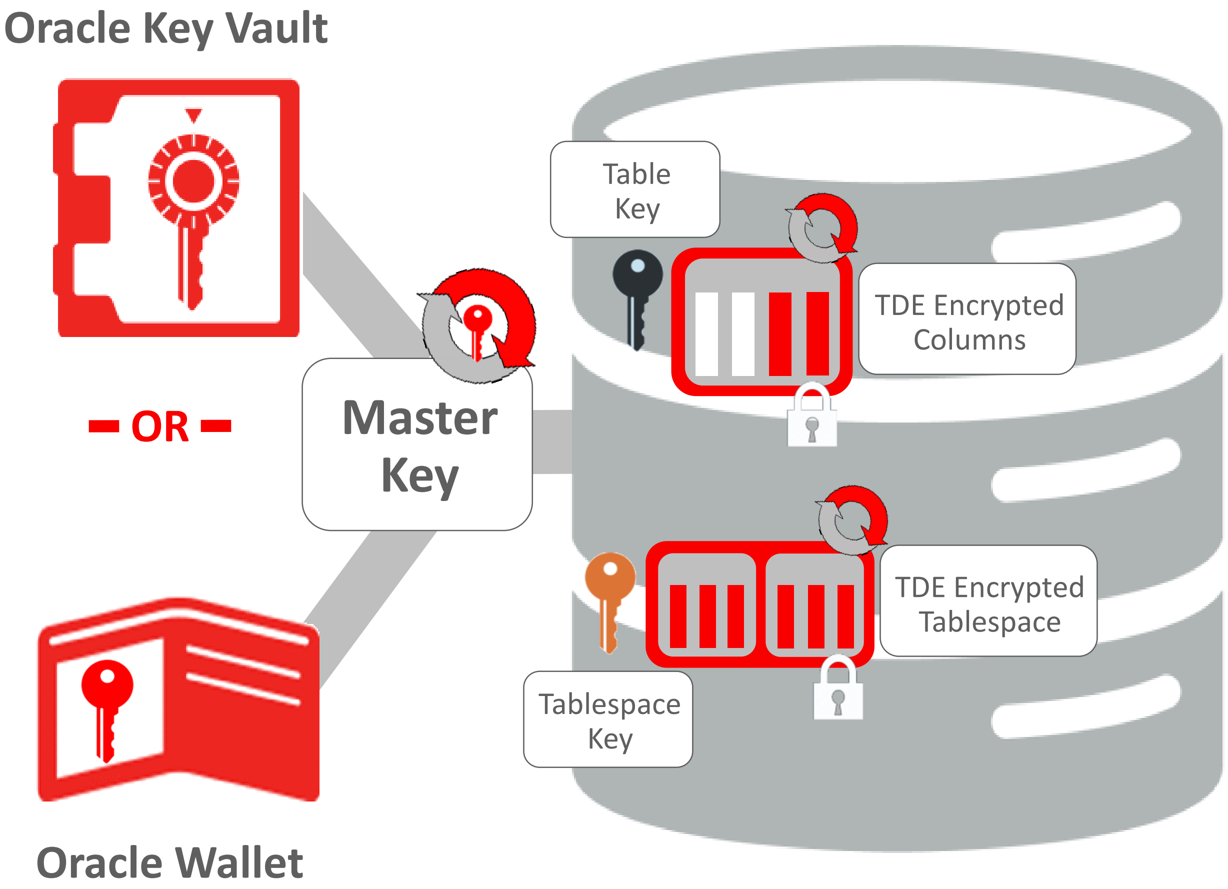
ORACLE JDEDWARDS SIEBEL SAP PeopleSoft ✓

TDE Integration with Oracle Database

Database Technologies	Example Points of Integration	TDE Support
High-Availability Clusters	Oracle Real Application Clusters (RAC), Data Guard, Active Data Guard	✓
Backup and Restore	Oracle Recovery Manager (RMAN), Oracle Secure Backup	✓
Export and Import	Oracle Data Pump Export and Import	✓
Database Replication	Oracle Golden Gate	✓
Pluggable Databases	Oracle Multitenant Option	✓
Engineered Systems	Oracle Exadata Smart Scans	✓
Storage Management	Oracle Automatic Storage Management (ASM)	✓
Data Compression	Oracle Standard, Advanced , and Hybrid Columnar Compression	✓

TDE Key Architecture

- Data encryption keys are created and managed by TDE automatically
- A master encryption key encrypts the data encryption keys
- The master key typically is stored in Oracle Wallet or Oracle Key Vault



TDE Algorithms and Key Lengths

Functionality	3DES168	AES128	AES192	AES256
Tablespace Encryption	✓	✓	✓	✓
Column Encryption	✓	✓	✓	✓
TDE Master Key				✓
Oracle Wallet (.p12)	✓			✓

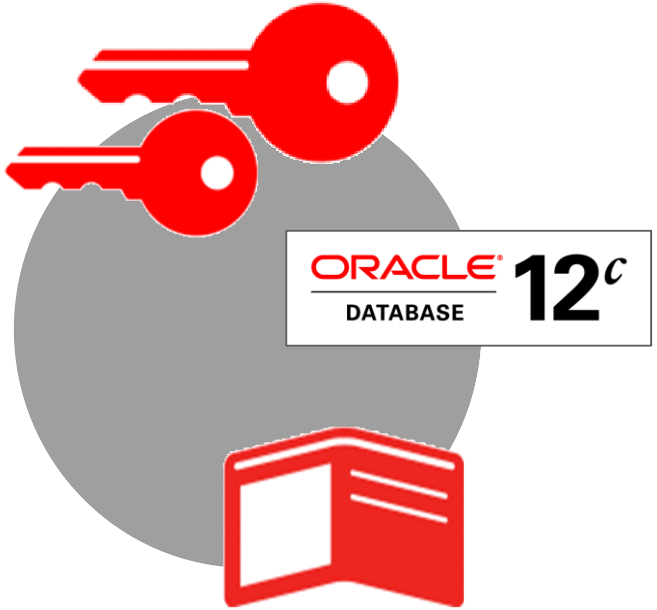
TDE Advancements in Oracle Database *12cR1, 12cR2*

12c release 1

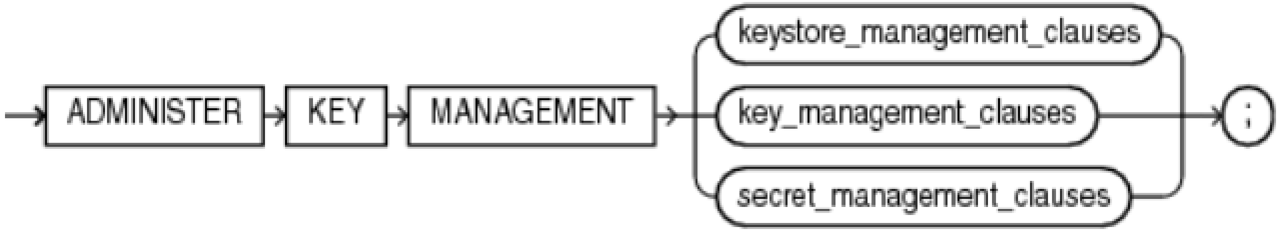
- Oracle Wallet
  - Storage in ASM, automatic backup
- TDE Master Key
  - New SQL commands for key management, alter system deprecated
  - Improved S.O.D. (SYSKM)

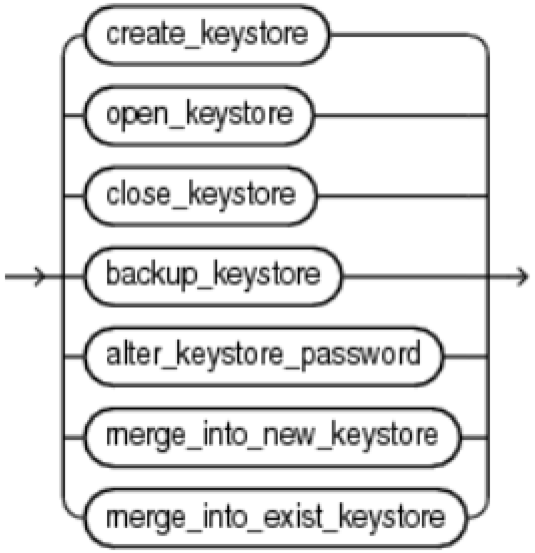
12c release 2

- Tablespace conversion from clear-text to encrypted
  - Online tablespace encryption in background with no downtime
  - Offline tablespace conversion with no storage overhead
- Encrypt full database
  - Oracle-supplied tablespaces SYSTEM, SYSAUX, TEMP, and UNDO



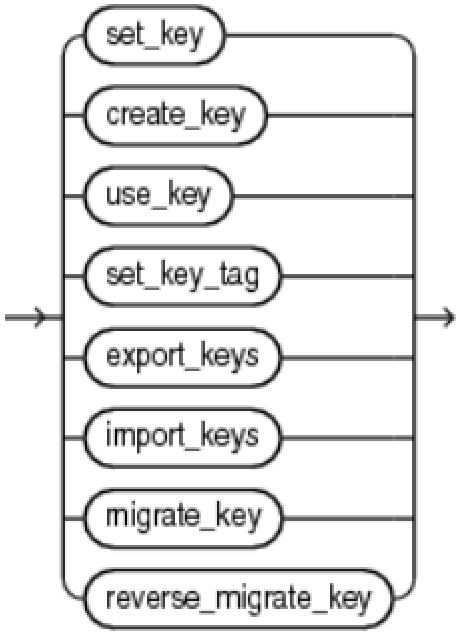
Wallet Keystore and Key management features





- Wallet keystore features: change pwd, backup, move to new location, migrate to HSM, merge into new keystore

View: *(G)V$ENCRYPTION_WALLET*



TDE Master key features: set (create and activate, rotate), create (not activate), activate, export, import, tagging with label

View: *V$ENCRYPTION_KEYS*

Online vs. Offline Tablespace Conversion

Functionality	Offline Encryption	Online Encryption
When can I run the conversion?	Offline tablespace OR Database in mount stage	Online tablespace AND Database is open in read write mode
Do I need to plan for downtime?	Requires temporarily taking the tablespace offline, unless using Data Guard	No, encrypts tablespace in background with no downtime
Do I need additional storage space?	No	Yes, storage overhead is only 2x the largest tablespace file
Can I run encryption operations in parallel?	Yes, enables simultaneous encryption of multiple data files across multiple cores	Yes, at the tablespace level with multiple sessions running
Can data encryption keys be rekeyed or rotated?	No	Yes, supports live re-encryption of tablespace data (a.k.a. data key rotation)
Backported to earlier release	Releases 12.1.0.2 and 11.2.0.4	No (only DB 12c Release 2)

Deploying TDE on Existing Data Now

- Offline migration during maintenance
  - Oracle DataPump Export / Import
  - Alter table move + alter index rebuild
  - Dbms_metadata.get_ddl + insert as select
  - Create table as select (CTAS)
- Online migration with near-zero downtime
  - Oracle Online Table Redefinition (DBMS_REDEFINITION)
  - Combine usage of Data Pump and Data Guard for Oracle Database [11*g*R2]() and [12*c*R1]()

White Papers Available on OTN

Oracle Maximum Availability Architecture

Converting to Transparent Data Encryption Using Data Guard Transient Logical Standby

Oracle Database 11g Release 2

ORACLE WHITE PAPER | MAY 2015

Oracle Maximum Availability Architecture

Converting to Transparent Data Encryption Using Active Data Guard (DBMS_ROLLING)

Oracle Database 12c

ORACLE WHITE PAPER | MAY 2015

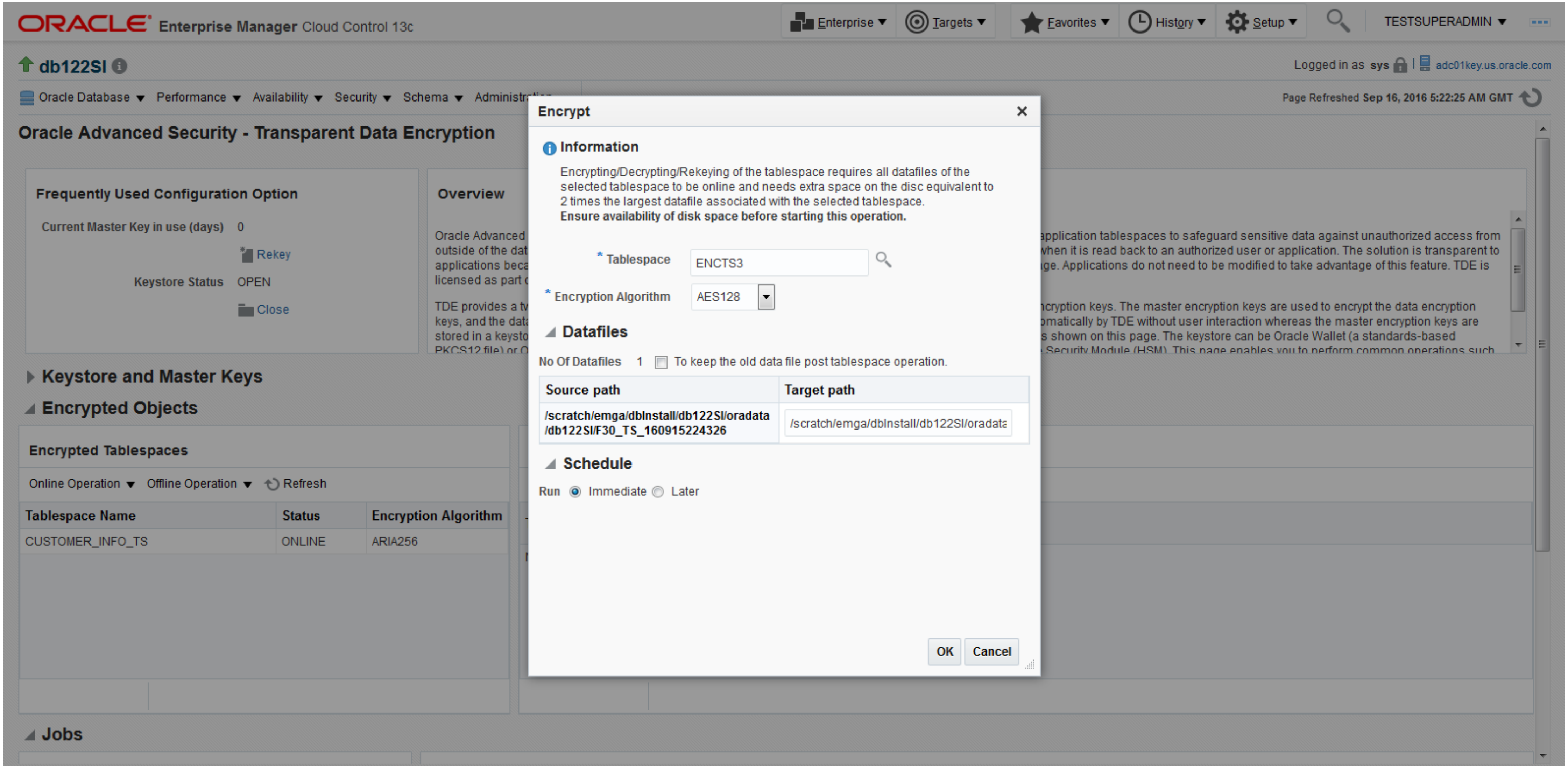
TDE ONLINE MIGRATION: DBMS_REDEFINITION

- The dbms_redefinition package allows you to copy a table (using CTAS), create a snapshot on the table, enqueue changes during the redefinition, and then re-synchronize the restructured table with the changes that have accumulated during reorganization.
- The following are the key basic steps:
- 1. Verify that the table is a candidate for online redefinition: dbms_redefinition.can_redef_table
- 2. Create an interim table into the encrypted tablespace
- 3. Enable parallel DML operations
- 4. Start the redefinition process : dbms_redefinition.start_redef_table (schema, table, int_table)
- 5. Copy dependent objects: dbms_redefinition.copy_table_dependents
- 6. Check for any errors: *select object_name, base_table_name, ddl_txt from DBA_REDEFINITION_ERRORS*;
- 7. Synchronize the interim table: dbms_redefinition.sync_interim_table
- 8. Complete the redefinition: dbms_redefinition.finish_redef_table
- 9. Drop the interim table

TDE ONLINE MIGRATION: DBMS_ROLLING

- 1. Presence of an Active Data Guard physical standby database with no archive log gaps.
- 2. Conversion of the physical standby to a logical standby using the DBMS_ROLLING PL/SQL package: DBMS_ROLLING.START_PLAN
- 3. Pausing the standby apply process.
- 4. Rebuilding tablespaces with TDE and setup of the TDE configuration at the logical standby.
- 5. Starting the logical apply process to resynchronize the standby (now encrypted) with the primary database.
- 6. Data Guard switchover, DBMS_ROLLING.SWITCHOVER. The estimated application downtime using best practices is less than 5 minutes.
- 7. Conversion of the old primary (momentarily a logical standby) to a new physical standby database, DBMS_ROLLING.FINISH_PLAN.
- 8. Starting the Active Data Guard physical apply process on the new standby database (the original primary).
- 9. Optionally – switching production back to the original primary. Estimated downtime using best practices is less than 5 minutes.

Integrated with Oracle Enterprise Manager 13c



Logged in as sys | adc01key.us.oracle.com

Page Refreshed Sep 16, 2016 5:22:25 AM GMT

Oracle Advanced Security - Transparent Data Encryption

Frequently Used Configuration Option

Current Master Key in use (days) 0

Keystore Status OPEN

Overview

Oracle Advanced … application tablespaces to safeguard sensitive data against unauthorized access from outside of the dat… when it is read back to an authorized user or application. The solution is transparent to applications beca… ge. Applications do not need to be modified to take advantage of this feature. TDE is licensed as part …

TDE provides a tw… cryption keys. The master encryption keys are used to encrypt the data encryption keys, and the dat… omatically by TDE without user interaction whereas the master encryption keys are stored in a keysto… s shown on this page. The keystore can be Oracle Wallet (a standards-based PKCS12 file) or O… Security Module (HSM). This page enables you to perform common operations such

Keystore and Master Keys

Encrypted Objects

Encrypted Tablespaces

Tablespace Name	Status	Encryption Algorithm
CUSTOMER_INFO_TS	ONLINE	ARIA256

Jobs

Encrypt

Information

Encrypting/Decrypting/Rekeying of the tablespace requires all datafiles of the selected tablespace to be online and needs extra space on the disc equivalent to 2 times the largest datafile associated with the selected tablespace. **Ensure availability of disk space before starting this operation.**

* Tablespace: ENCTS3

* Encryption Algorithm: AES128

Datafiles

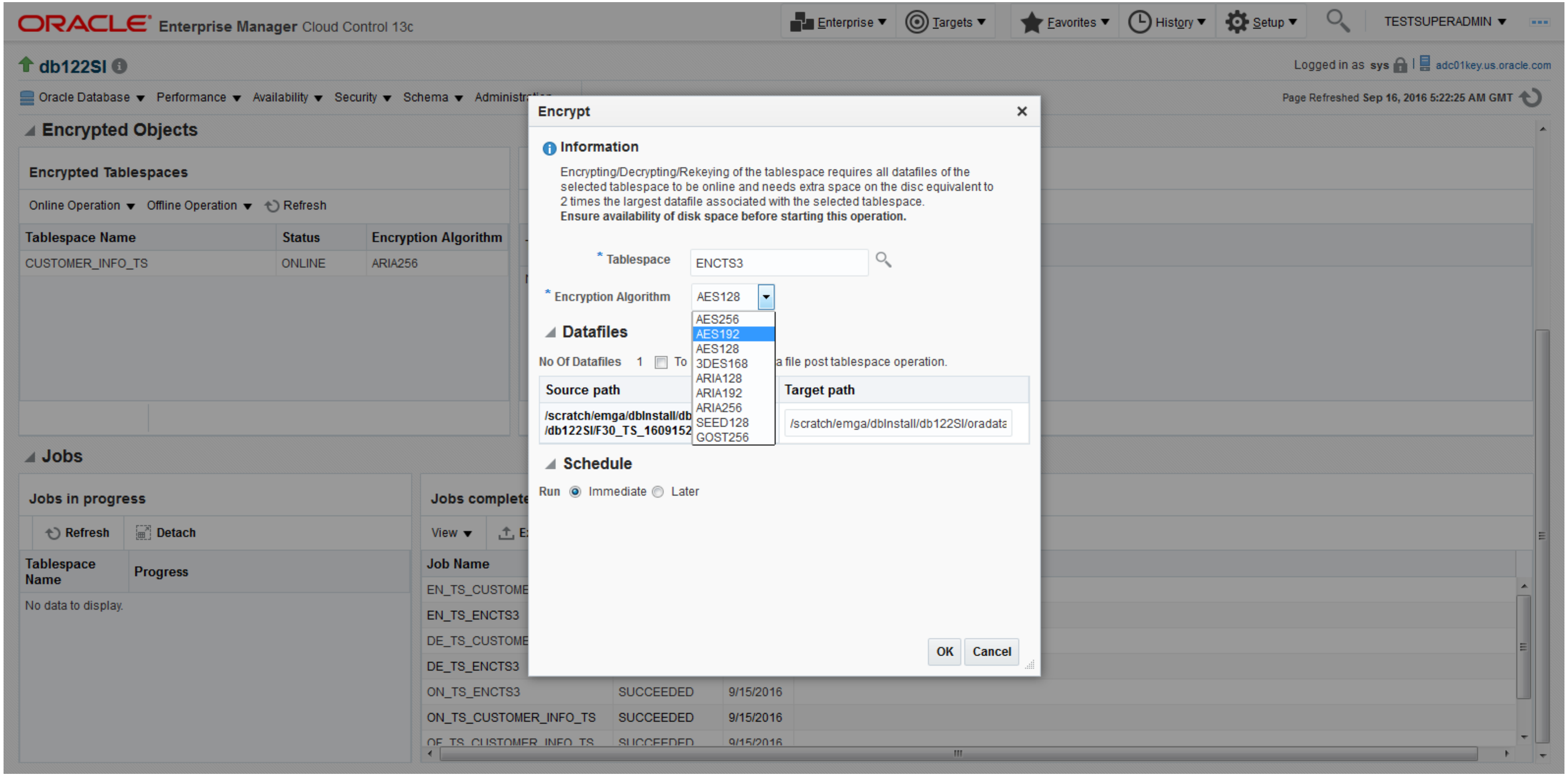
No Of Datafiles 1 ☐ To keep the old data file post tablespace operation.

Source path	Target path
/scratch/emga/dbInstall/db122SI/oradata/db122SI/F30_TS_160915224326	/scratch/emga/dbInstall/db122SI/oradata

Schedule

Run ● Immediate ○ Later

Integrated with Oracle Enterprise Manager 13c



Encrypted Objects

Encrypted Tablespaces

Tablespace Name	Status	Encryption Algorithm
CUSTOMER_INFO_TS	ONLINE	ARIA256

Jobs

Jobs in progress

Tablespace Name	Progress
No data to display.	

Jobs complete

Job Name		
EN_TS_CUSTOME		
EN_TS_ENCTS3		
DE_TS_CUSTOME		
DE_TS_ENCTS3		
ON_TS_ENCTS3	SUCCEEDED	9/15/2016
ON_TS_CUSTOMER_INFO_TS	SUCCEEDED	9/15/2016
OF_TS_CUSTOMER_INFO_TS	SUCCEEDED	9/15/2016

Encrypt

Information

Encrypting/Decrypting/Rekeying of the tablespace requires all datafiles of the selected tablespace to be online and needs extra space on the disc equivalent to 2 times the largest datafile associated with the selected tablespace.
Ensure availability of disk space before starting this operation.

* Tablespace: ENCTS3

* Encryption Algorithm: AES128

AES256
AES192
AES128
3DES168
ARIA128
ARIA192
ARIA256
SEED128
GOST256

Datafiles

No Of Datafiles 1 □ To a file post tablespace operation.

Source path	Target path
/scratch/emga/dbInstall/db… /db122SI/F30_TS_1609152…	/scratch/emga/dbInstall/db122SI/oradata

Schedule

Run ● Immediate ○ Later

Agenda

- ➢ Regolamento Europeo per la Protezione dei Dati Personali – GDPR

- ➢ Oracle Database Maximum Security Architecture

- ➢ **Oracle Advanced Security Option**
  - TDE Nuove Funzionalità
  - **TDE Impatti prestazionali**
  - TDE Casi d'uso

Typical Customer Experience with Performance

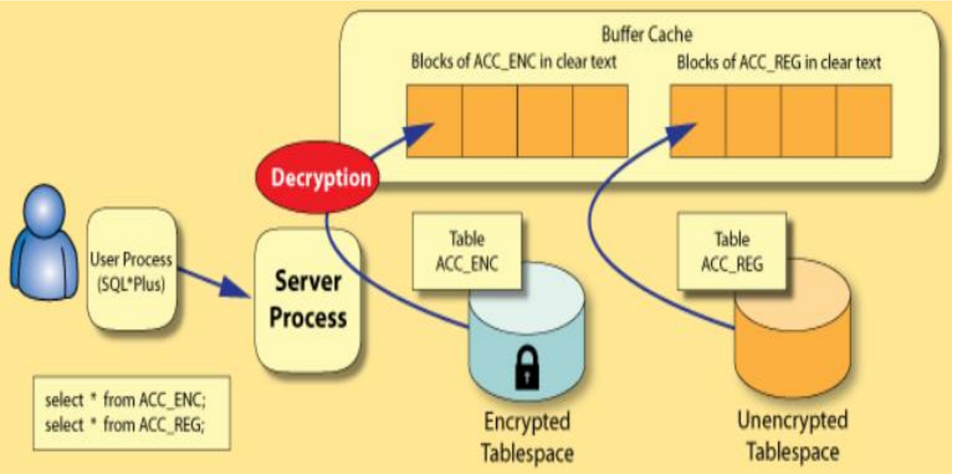
- The performance overhead typically is small on modern hardware
- Intel the instruction set has been expanded with AES-NI to include specific instructions that implement AES encryption rounds. Oracle supports these instructions as of RDBMS version 11.2.0.2 on Linux x86-64 for tablespace encryption (*Doc ID 1365021.1*)
  - Case Studies: ETS (1-2%), Columbia U (1-3%)
  - *alter system set "_use_platform_encryption_lib" = false scope=spfile;*
- Measured overhead for a given test may vary
- Following the tuning tips for TDE will help

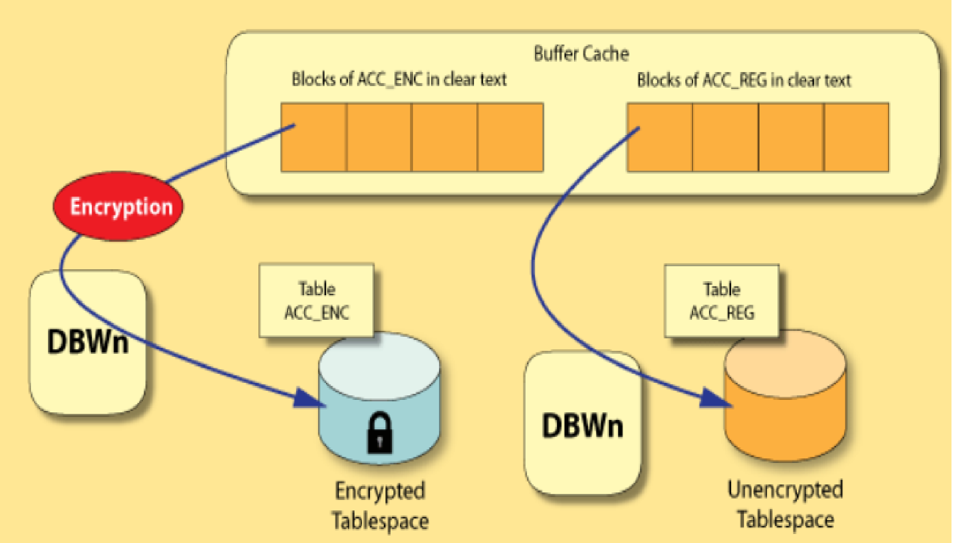
Managing Master Keys in Oracle Wallet

- ***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), See *Note: 567287.1 Managing TDE Wallets in a RAC Environment*
- For DB 12*c*R1, separate duties using SYSKM

ORACLE

TDE Tablespace encryption - Performance Impact





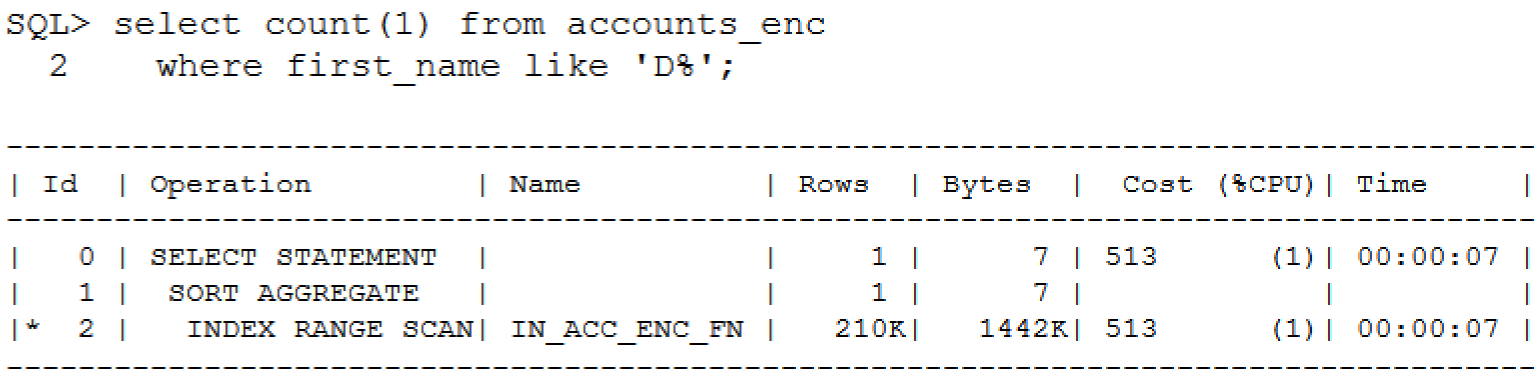
- The data is encrypted on disk and decrypted in the buffer cache and subsequently when processed in the PGA. The data is encrypted when written to disk by the DBWR
- Encryption and decryption are typically CPU intensive operations and would always require additional CPU resources
- Generally time needed to decrypt the data should not be compared to the time needed to execute a statement or read a block from disk
- Performing a **full table scan on a huge table can increase significantly the execution time**
- if a table is not very large, queried mostly with full table scan operations and must reside in an encrypted tablespace, consider the possibility of keeping it as much as possible in the buffer cache by enabling **the keep buffer pool** and setting the table to use it
- Consider increasing the **degree of parallelism** for huge tables

TDE Column Encryption – Performance Impact

- The data is encrypted on disk and in the buffer cache and decrypted in the session private memory (PGA).
- TDE doesn't support encrypting columns with foreign key constraints, individual tables have their own unique encryption key
- Encryption with SALT is therefore more secure. Encrypting with SALT (default) involves a random value being added to the value to be encrypted before encryption, 16 byte extra. Without SALT, the same plaintext also creates the same encrypted value with the same algorithm.
- The most common performance **problem is a change of execution plans**. Indexes on an encrypted column are built on the encrypted values, Index keys are not sorted in the same order as in the non-encrypted → **Index range scan becomes a full index scan**
- If a column to be encrypted is in an index, however, this column must be encrypted with the NO SALT option: **ORA-28338: can not encrypt indexed column(s) with salt**
- SELECT OWNER, TABLE_NAME, COLUMN_NAME, SALT, ENCRYPTION_ALG FROM DBA_ENCRYPTED_COLUMNS ORDER BY OWNER, TABLE_NAME, SALT;
- When encrypting a column with an existing index, it is recommended to first extract the index definition with dbms_metadata.get_ddl, then drop the index, encrypt the column with the 'no salt' option, and re-build the index.

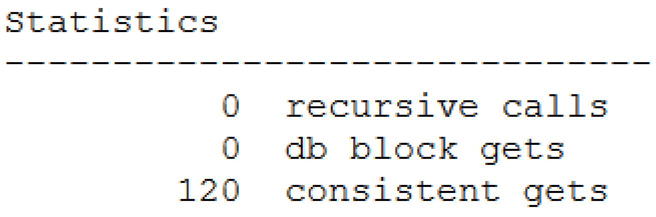
TDE Tablespace Encryption vs Column Encryption

Table in Tablespace Encryption



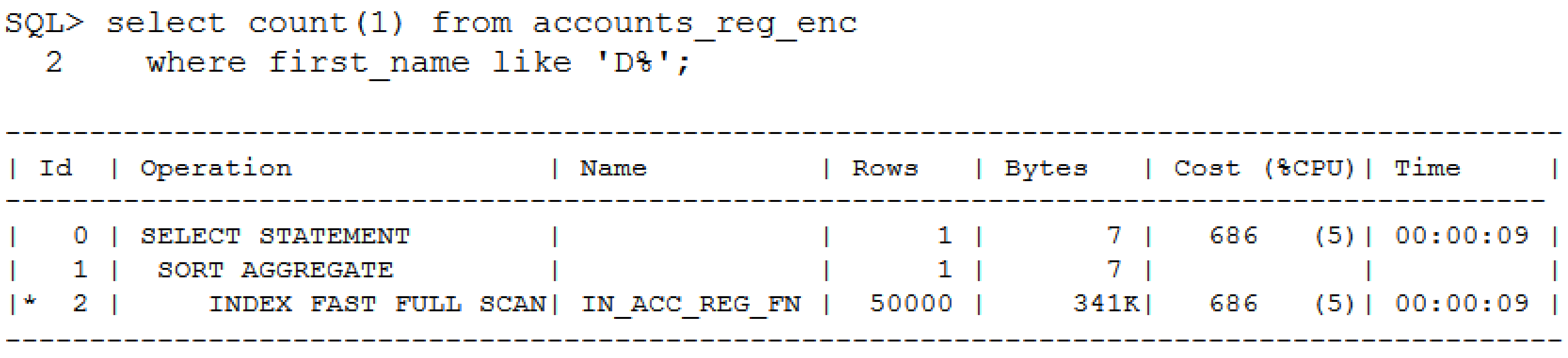
```
SQL> select count(1) from accounts_enc
  2    where first_name like 'D%';

----------------------------------------------------------------------------------
| Id  | Operation          | Name          | Rows  | Bytes  |  Cost  (%CPU)| Time     |
----------------------------------------------------------------------------------
|   0 | SELECT STATEMENT   |               |     1 |      7 | 513      (1)| 00:00:07 |
|   1 |  SORT AGGREGATE    |               |     1 |      7 |             |          |
|*  2 |   INDEX RANGE SCAN| IN_ACC_ENC_FN |  210K|  1442K| 513      (1)| 00:00:07 |
----------------------------------------------------------------------------------
```



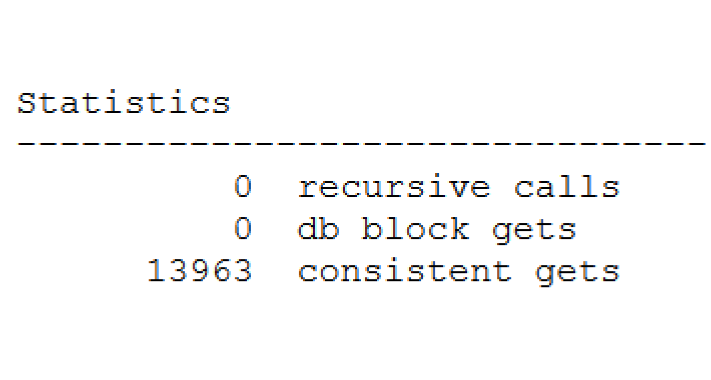
```
Statistics
------------------------------
          0  recursive calls
          0  db block gets
        120  consistent gets
```

Table with Column Encryption in not encrypted tablespace



```
SQL> select count(1) from accounts_reg_enc
  2    where first_name like 'D%';

---------------------------------------------------------------------------------------
| Id  | Operation                | Name          | Rows    | Bytes    | Cost  (%CPU)| Time     |
---------------------------------------------------------------------------------------
|   0 | SELECT STATEMENT         |               |       1 |        7 |   686    (5)| 00:00:09 |
|   1 |  SORT AGGREGATE          |               |       1 |        7 |             |          |
|*  2 |     INDEX FAST FULL SCAN| IN_ACC_REG_FN |  50000 |     341K|   686    (5)| 00:00:09 |
---------------------------------------------------------------------------------------
```



```
Statistics
--------------------------------
          0  recursive calls
          0  db block gets
      13963  consistent gets
```

Agenda

- ➢ Regolamento Europeo per la Protezione dei Dati Personali – GDPR
- ➢ Oracle Database Maximum Security Architecture
- ➢ **Oracle Advanced Security Option**
  - TDE Nuove Funzionalità
  - TDE Impatti prestazionali
  - **TDE Casi d’uso**

TDE and SAP NetWeaver: SAP Note 974876

- Oracle home shared between different database instances, sqlnet.ora:
  - ENCRYPTION_WALLET_LOCATION =(SOURCE =(METHOD = FILE)(METHOD_DATA =(DIRECTORY = $SAPDATA_HOME/orawallet)))
  - srvctl setenv database -d <DBNAME> -T "SAPDATA_HOME=/oracle/<DBNAME>"
  - DB in RAC: $SAPDATA_HOME/orawallet consigliata su ACFS, altrimenti link simbiloco
- Columns of tables of the SAP Basis application should not be encrypted if possible (autologin wallet)
- To verify the wallet path:
  - brspace -u <user>/<pwd> -f mdencr -a show
  - SELECT INST_ID, WRL_PARAMETER, STATUS FROM GV$ENCRYPTION_WALLET ORDER BY INST_ID;
- Use only BRSPACE (v 7.0 patch level 24) for wallet administration because backup copies of the wallet are then created automatically if the wallet is changed
- Create wallet, save and make a backup copy, rekey, set wallet password:
  - brspace -u <user>/<pwd> -f mdencr -a create
  - brspace -f mdencr -a save
  - brspace -f mdencr -a newkey
  - brspace -f mdencr -a chpass -password -newpass

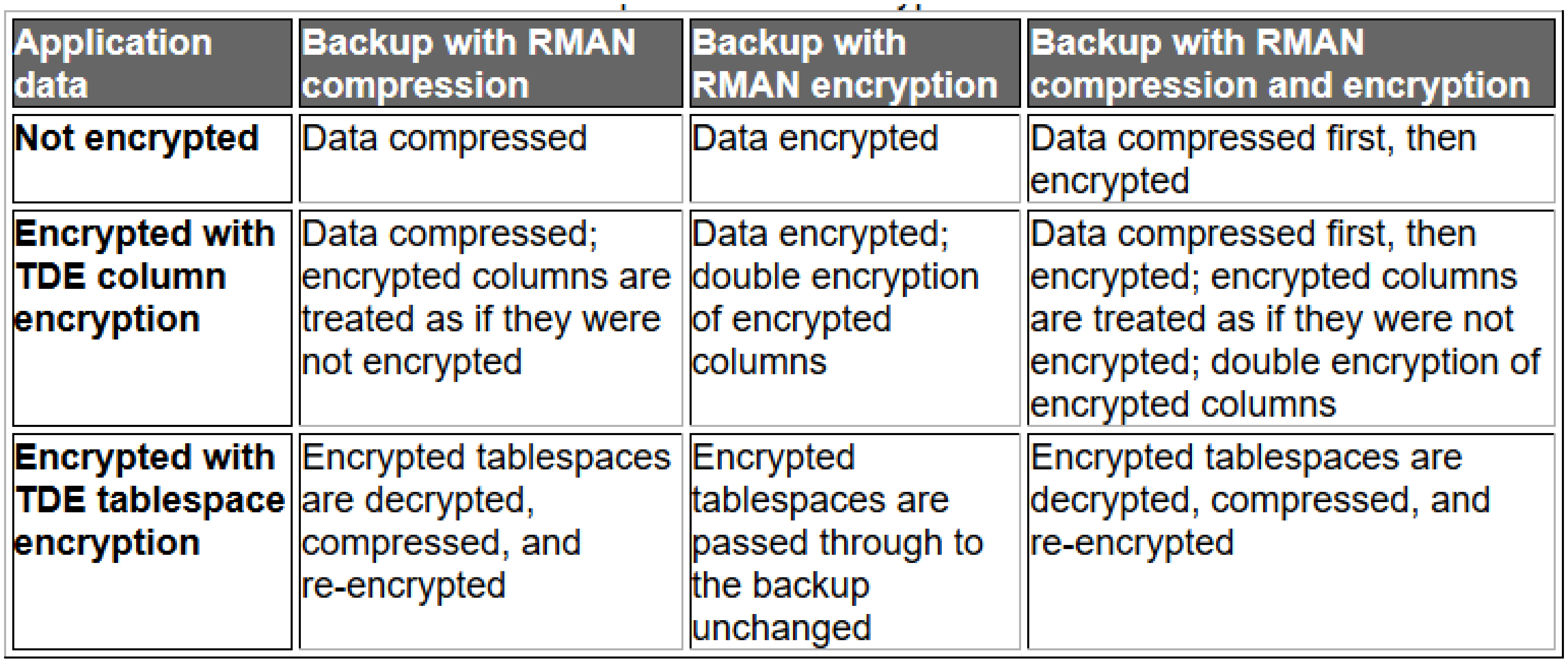
TDE in Multitenancy Environment

- **In a CDB database:** We have a single Keystore (Wallet) owned by the ROOT container (CDB$ROOT) and a separate Master Encryption Key for each of the associated pluggable databases as well as a Master encryption Key for the ROOT (CDB$ROOT) container.
- In CDB$ROOT with ASM (*Doc ID 2193264.1: How To Manage A TDE Wallet Created In ASM*):
  - ASMCMD> cd +DATA/PRODCDB
  - ASMCMD> mkdir WALLET
  - sys@PRODCDB> ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '+DATA/PRODCDB/WALLET' IDENTIFIED BY encWallet;
  - ASMCMD>ls -l +DATA/PRODCDB/WALLET

```
Type       Redund  Striped  Time            Sys  Name
KEY_STORE  MIRROR  COARSE   JAN 28 15:00:00  N    ewallet.p12 => +DATA/PRODCDB/KEY_STORE/ewallet.338.875546829
```

  - sys@PRODCDB> ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY encWallet [CONTAINER=ALL|CURRENT];
  - sys@PRODCDB> ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE FROM KEYSTORE '+DATA/PRODCDB/WALLET' IDENTIFIED BY encWallet;
- In CDB$ROOT or any PDBs:
  - Create master key for CDB$ROOT o for PDBs: ADMINISTER KEY MANAGEMENT SET KEY [USING TAG 'tag'] IDENTIFIED BY password [WITH BACKUP [USING 'backup_identifier']] [CONTAINER = ALL | CURRENT];
  - Query for encryption keys in CDB or PDBs: select CON_ID,KEY_ID,KEYSTORE_TYPE,CREATOR_DBNAME,CREATOR_PDBNAME from v$encryption_keys;

TDE and RMAN

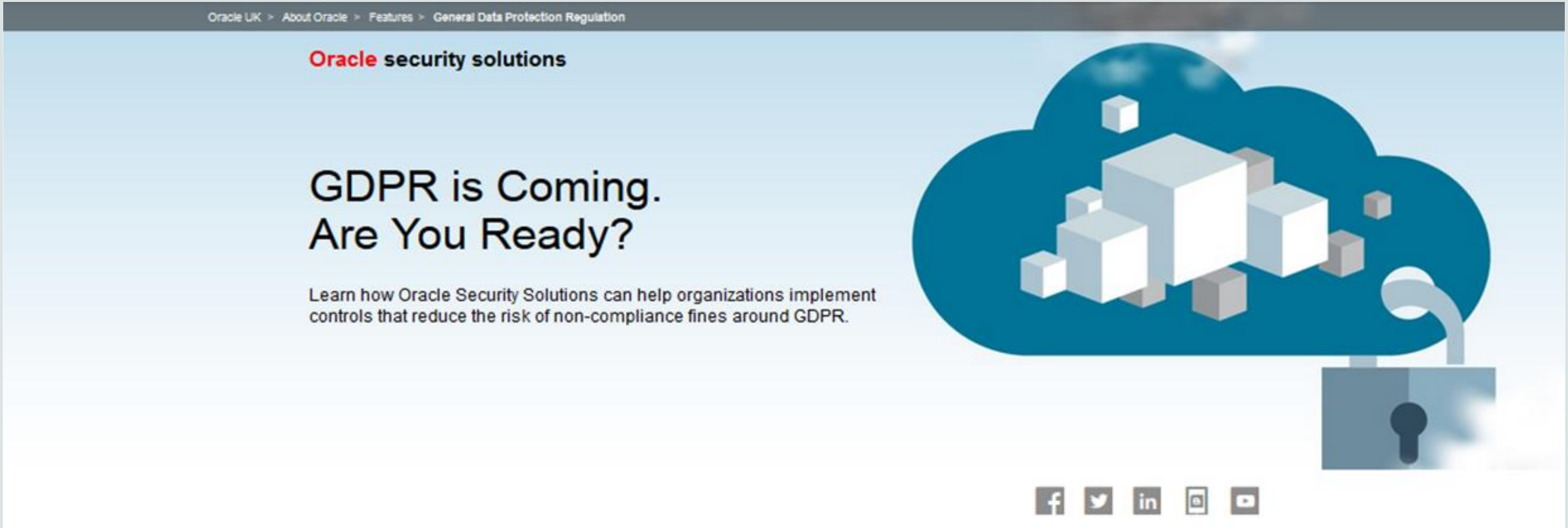


Application data	Backup with RMAN compression	Backup with RMAN encryption	Backup with RMAN compression and encryption
Not encrypted	Data compressed	Data encrypted	Data compressed first, then encrypted
Encrypted with TDE column encryption	Data compressed; encrypted columns are treated as if they were not encrypted	Data encrypted; double encryption of encrypted columns	Data compressed first, then encrypted; encrypted columns are treated as if they were not encrypted; double encryption of encrypted columns
Encrypted with TDE tablespace encryption	Encrypted tablespaces are decrypted, compressed, and re-encrypted	Encrypted tablespaces are passed through to the backup unchanged	Encrypted tablespaces are decrypted, compressed, and re-encrypted

```
RMAN> connect target <ORACLE_SID>/<SYS pwd>
RMAN> set encryption on;
RMAN> backup [as compressed backupset] database;
```

TDE and Database Filesystem DBFS

- SecureFiles Encryption introduces a new encryption facility for LOBs. The data is encrypted using Transparent Data Encryption (TDE), which allows the data to be stored securely, and still allows for random read and write access. It is not required to create the DBFS table in a TDE(Transparent Data Encryption) tablespace.
- Deduplication, Compression and Encryption can be setup independently or as a combination of one or more features. If all three features are turned on, Oracle will perform deduplication first and then compression followed by encryption
- SecureFiles supports the following encryption algorithms:
  - 3DES168:Triple Data Encryption Standard with a 168-bit key size
  - AES128:Advanced Encryption Standard with a 128 bit key size
  - AES192:Advanced Encryption Standard with a 192-bit key size (default)
  - AES256:Advanced Encryption Standard with a 256-bit key size
- To create DBFS with encryption: *sqlplus @dbfs_create_filesystem_advanced tablespace_name file_system-name [compress-high | compress-medium | compress-low | nocompress] [deduplicate | nodeduplicate] [**encrypt** | noencrypt] [partition | non-partition]*
- Secret key in TDE for DBConnectString in tnsnames entry with username/password:
  - mkstore -wrl wallet_location -createCredential db_connect_string username password
  - *$ORACLE_HOME/bin/dbfs_client -o wallet /@DBConnectString /mnt/dbfs*



Oracle UK > About Oracle > Features > General Data Protection Regulation

Oracle security solutions

GDPR is Coming.
Are You Ready?

Learn how Oracle Security Solutions can help organizations implement controls that reduce the risk of non-compliance fines around GDPR.

Visit us: oracle.com/goto/gdpr

Integrated Cloud

Applications & Platform Services