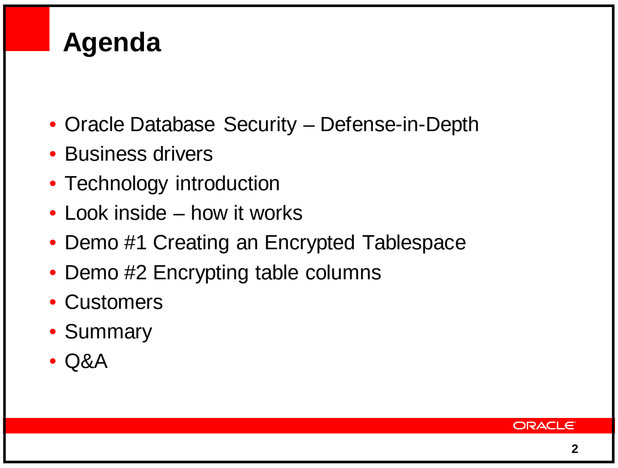
SECURITY INSIDE OUT

Complete Protection for Your Database, Middleware, and Applications

ORACLE

Oracle Advanced Security

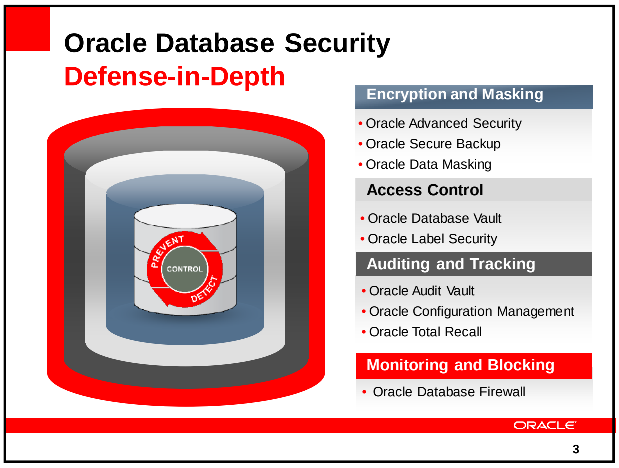
Technical Overview



Agenda

- Oracle Database Security – Defense-in-Depth
- Business drivers
- Technology introduction
- Look inside – how it works
- Demo #1 Creating an Encrypted Tablespace
- Demo #2 Encrypting table columns
- Customers
- Summary
- Q&A

ORACLE



Oracle Database Security

Defense-in-Depth

Encryption and Masking

- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

Access Control

- Oracle Database Vault
- Oracle Label Security

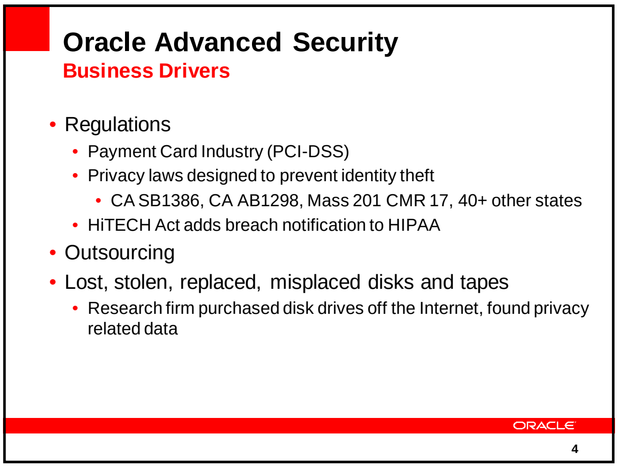
Auditing and Tracking

- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

Monitoring and Blocking

- Oracle Database Firewall

ORACLE

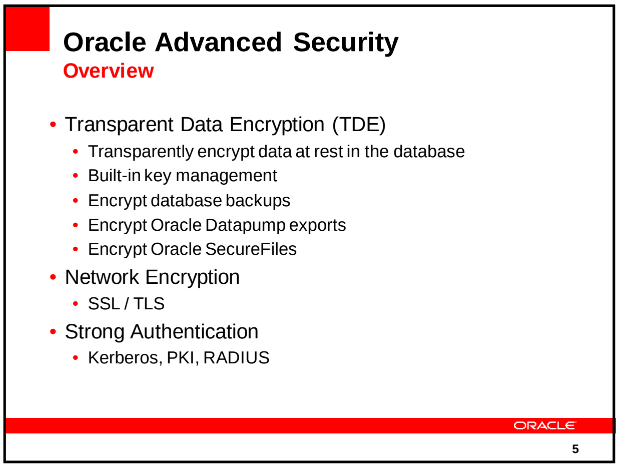


Oracle Advanced Security

Business Drivers

- Regulations
  - Payment Card Industry (PCI-DSS)
  - Privacy laws designed to prevent identity theft
    - CA SB1386, CA AB1298, Mass 201 CMR 17, 40+ other states
  - HiTECH Act adds breach notification to HIPAA
- Outsourcing
- Lost, stolen, replaced, misplaced disks and tapes
  - Research firm purchased disk drives off the Internet, found privacy related data

ORACLE

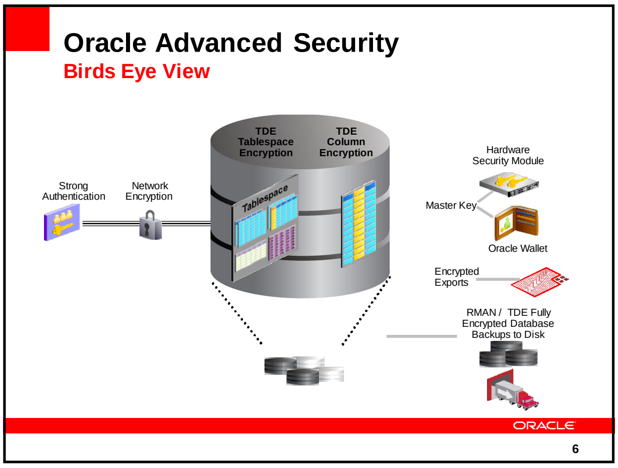


Oracle Advanced Security

Overview

- Transparent Data Encryption (TDE)
  - Transparently encrypt data at rest in the database
  - Built-in key management
  - Encrypt database backups
  - Encrypt Oracle Datapump exports
  - Encrypt Oracle SecureFiles
- Network Encryption
  - SSL / TLS
- Strong Authentication
  - Kerberos, PKI, RADIUS

ORACLE



Oracle Advanced Security

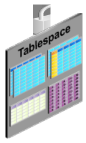
Birds Eye View

ORACLE

Oracle Advanced Security
Key Features By Release

	Oracle Database 9i Release 2	Oracle Database 10g Release 2	Oracle Database 11g Release 1	Oracle Database 11g Release 2
TDE with Exadata				✓
TDE tablespace encryption with HSM				✓
TDE tablespace encryption			✓	✓
TDE column encryption for SecureFiles			✓	✓
TDE column encryption with HSM			✓	✓
TDE column encryption		✓	✓	✓
Network encryption	✓	✓	✓	✓
Strong authentication	✓	✓	✓	✓

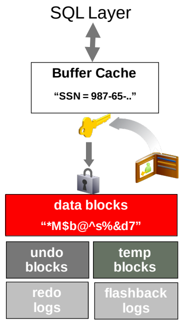
Oracle Advanced Security
TDE tablespace encryption



- Available since Oracle Database 11g Release 1
  - Recommended version 11.1.0.7 or later
- Encrypts entire application tablespaces
- Key management
  - One key for each encrypted tablespace
  - Tablespace key is encrypted using the TDE master encryption key – 2 tier key architecture

Oracle Advanced Security
TDE tablespace encryption

- Encrypt all application data
  - Encrypt entire tablespace
  - No need to identify specific columns
  - No limitations on data types, index searches or foreign key enforcement
- Highly efficient
  - No additional storage overhead
  - High performance (~ 5% average)
  - Certified with Oracle Advanced Compression - blocks are compressed before they are encrypted


SQL Layer

Buffer Cache

“SSN = 987-65-..”

data blocks

“*M$b@^s%&d7”

undo blocks

temp blocks

redo logs

flashback logs

Oracle Advanced Security
TDE Tablespace Encryption Application Certification

- Encrypt personally identifiable data
- Built-in key management
- Transparent to existing applications

Oracle E-Business Suite 11i / R12 ✓

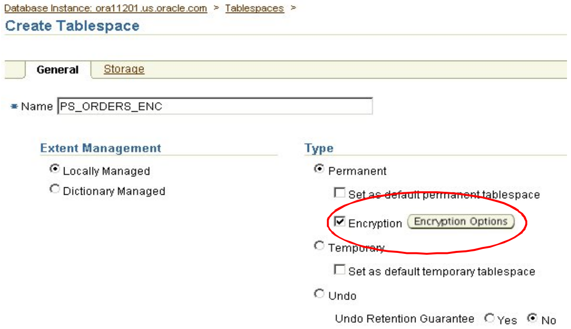
PeopleSoft Applications ✓

Siebel, i-Flex ✓

JD Edwards Enterprise One ✓

SAP ✓

Oracle Advanced Security
Creating an Encrypted Tablespace


Database Instance: ora11201.us.oracle.com > Tablespaces >

Create Tablespace

General | Storage

* Name PS_ORDERS_ENC

Extent Management

● Locally Managed

○ Dictionary Managed

Type

● Permanent

□ Set as default permanent tablespace

☑ Encryption

○ Temporary

□ Set as default temporary tablespace

○ Undo

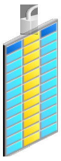
Undo Retention Guarantee ○ Yes ● No

Oracle Advanced Security
Creating an Encrypted Tablespace – Command Line

- Create new tablespace
  - `SQL> create tablespace SECURE datafile ‘/opt/enc_tbs.dbf’ size 100M encryption using ‘AES256’ default storage(encrypt);`
- Options
  - AES256, AES192, AES128 (default) and 3DES168

Oracle Advanced Security

TDE column encryption



- Available since Oracle Database 10g Release 2
  - Recommended version 10.2.0.4 or later
- Encrypts sensitive columns in application tables
  - Credit card numbers, SSN, driver license, …
- Key management
  - One key per table
  - Table keys are encrypted using the TDE master encryption key – 2 tier key architecture

Oracle Advanced Security

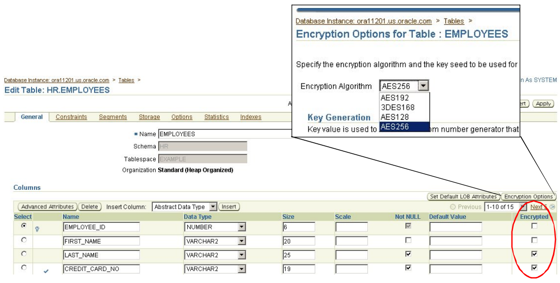
TDE Column Encryption Application Certification

- Encrypt personally identifiable data
- Built-in key management
- Transparent to existing applications

- Oracle E-Business Suite 11i / R12 ✓
- PeopleSoft Applications ✓
- Siebel, i-Flex ✓
- JD Edwards Enterprise One ✓
- SAP ✓
- Infosys Finacle ✓

Oracle Advanced Security

Integrated with Oracle Enterprise Manager



Database Instance: ora11201.us.oracle.com > Tables >

Edit Table: HR.EMPLOYEES

* Name EMPLOYEES
Schema HR
Tablespace EXAMPLE
Organization **Standard (Heap Organized)**

Columns

Insert Column: Abstract Data Type
1-10 of 15

Select		Name	Data Type	Size	Scale	Not NULL	Default Value	Encrypted
●		EMPLOYEE_ID	NUMBER	6		☑		☐
○		FIRST_NAME	VARCHAR2	20		☐		☐
○		LAST_NAME	VARCHAR2	25		☑		☑
○	✓	CREDIT_CARD_NO	VARCHAR2	19		☑		☑

Database Instance: ora11201.us.oracle.com > Tables >

Encryption Options for Table : EMPLOYEES

Specify the encryption algorithm and the key seed to be used for

Encryption Algorithm AES256

Key Generation

Key value is used to … m number generator that

Oracle Advanced Security

Encrypting Columns - Command Line Syntax

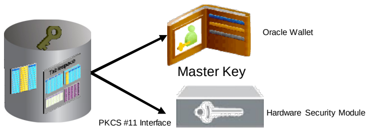
- Encrypt column in existing table
  - `SQL> alter table clients modify (cr_card_nbr encrypt)`
- Encrypt column in new table

  -
    ```
    SQL> create table customers(
        first_name    varchar2(64),
        last_name     varchar2(64) encrypt using 'AES256',
        cr_card_nbr   varchar2(32) encrypt no salt 'nomac');
    ```
- Storage Overhead
  - Approximately 48 bytes per row
  - New 'nomac' option (save 20 bytes per encrypted value), reducing storage to approximately 28 bytes per row

Oracle Advanced Security

TDE Key Management

- Generate, store, and rotate encryption keys
- Two tier key architecture
  - Master key protects table keys and tablespace keys
  - Master key is stored in External Security Module:
    - Oracle Wallet (PKCS #12 file)
    - Certified Hardware Security Modules: RSA, Safenet, Thales, Utimaco



Oracle Advanced Security

TDE for Unstructured Data

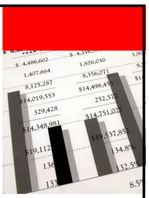
- Protection for unstructured data in the database
  - X-ray images (DICOM)
  - Scanned financial documents
- Encrypt using TDE **column** encryption
  - Oracle SecureFiles were introduced in Oracle Database 11g
- Encrypt using TDE **tablespace** encryption
  - Encrypt the entire tablespace containing data in Oracle SecureFile or traditional LOBs

Oracle Advanced Security
TDE for Data Pump and RMAN

- Oracle Data Pump
  - Bulk export/import to operating system flat files
- Oracle RMAN
  - Database backups and recovery
- Use local master encryption key or passphrase to encrypt export or backup file

Oracle Advanced Security
Network Encryption and Strong Authentication

- Encrypts SQL traffic to and from the database
  - AES (256, 192, 128 bit keys)
  - RSA RC4 (256, 128 bit keys)
  - 3DES (3 and 2 key)
  - Diffie-Hellman key exchange
- Data integrity with checksums
  - SHA-1
  - Automatically detects modifications, replays, missing packets
- Strong Authentication
  - Kerberos, PKI, and RADIUS



Oracle Advanced Security Customers

U.S. Retailer
Oracle Advanced Security Helps Comply with Massachusetts Law

Business Challenges	• Compliance with MA Law 201 CMR 17 requires encryption of data at rest and on the wire • Custom application cannot be modified
Solution	• Deployed Oracle Advanced Security TDE column encryption for custom application
Business Results	• Achieved compliance goal in one day; long before deadline • Efficient encryption of sensitive data with no application changes

U.S. Specialty Retailer
Oracle Advanced Security Helped with PCI Compliance

Business Challenges	• PCI compliance • Oracle E-Business Suite i-Expense and Oracle PeopleSoft Human Resource Applications • PeopleSoft's own PET tool insufficient, inflexible
Solution	• Oracle Advanced Security TDE column encryption • Maintain flexibility in terms of customization to PSFT application
Business Results	• Cost effective and transparent implementation of data encryption with no application changes • Protection of sensitive data at rest and on network • Built-in encryption key management

Customer Snapshots

Customer	Overview
Dress Barn	Encrypt credit card numbers as soon as they enter their tokenization server ***"Within a few hours we were up and running with no performance impact"***
Yuntaa (Belgium)	TDE column encryption in 11gR1 to encrypt 'SecureFile' columns, where their customer's personal data is stored ***"I wouldn't trust the encryption of our content to anything or anyone else"***
Daewoo Securities	TDE used to encrypt PII data in relation to financial transactions ***"We used Oracle's database security solutions to resolve internal security issues, a common challenge for financial institutions. … while Oracle Advanced Security has automated encryption functions that further protects sensitive information."***