ORACLE ADVANCED SECURITY

KEY FEATURES AND BENEFITS

- Transparently encrypt data without application changes
- Built-in key management
- Encrypt entire application tables or individual columns
- Encrypt database exports and RMAN backups
- Encrypt Oracle SQL*Net network traffic
- Fully interoperable with Oracle Advanced Compression technologies
- Fully Interoperable with Oracle GoldenGate 11.1.1.1
- Exadata X2 'Smart Scan' and EHCC support
- Cryptographic acceleration with AES-NI on Intel® XEON® 5600
- Industry standards – AES, 3DES, PKCS#11,PKCS#12, X.509v3

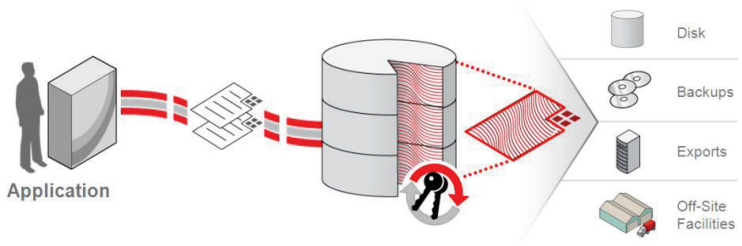
Oracle Advanced Security helps customers address regulatory compliance requirements by protecting sensitive data on the network, on storage media and within the database from unauthorized disclosure. Transparent Data Encryption, a major component of Oracle Advanced Security, provides the industry's most advanced database encryption solution for protecting sensitive information without requiring changes to applications.

Overview

Oracle Advanced Security is an option to the Oracle Database 11g Enterprise Edition that helps address privacy and regulatory requirements including the Payment Card Industry Data Security Standard (PCI), Health Insurance Portability and Accountability Act (HIPAA), and numerous breach notification laws. Oracle Advanced Security provides data encryption and strong authentication services to the Oracle database, safeguarding sensitive data against unauthorized access from the network and the operating system. It also protects against theft, loss, and improper decommissioning of storage media and database backups.

Transparent Data Encryption

Transparent data encryption (TDE) encrypts data before it is written to storage and automatically decrypts data when reading it from storage without any changes to existing applications – no triggers, views or other costly changes. Access controls that are enforced by the Oracle database, including object grants, roles, virtual private database and Oracle Database Vault, still remain in effect.



63

TDE supports two modes: tablespace encryption and column encryption. TDE *tablespace* encryption, introduced with Oracle Database 11g, provides an efficient solution for encrypting entire application tables. TDE tablespace encryption fully supports Exadata X2 including Smart Scan and Hybrid Columnar Compression (EHCC). Starting with Oracle Database 11.2.0.2, TDE tablespace encryption automatically utilizes the hardware acceleration of the Intel® Xeon® 5600 CPUs with AES-NI, enabling Oracle Database 11g to encrypt and decrypt data up to 10 times faster on Intel® platforms, including the Oracle Exadata Database Machine. TDE *column* encryption, introduced with Oracle Database 10g Release2, provides an efficient solution for encrypting individual data elements such as credit card and social security numbers. For TDE column and tablespace encryption, frequently

Oracle Advanced Security TDE supports these critical database operational activities and helps ensure that the data remains encrypted. Tablespace encryption integrates with Oracle Recovery Manager (backup and restore), Oracle Data Pump (data movement), Oracle Data Guard (redundancy and failover), and Oracle GoldenGate (replication). TDE also integrates with internal features of the database such as redo to prevent possible data leakage in logs. This fully integrated approach to database encryption makes the solution easy to deploy in complex real-world environments while protecting against bypass attacks that attempt to take advantage of gaps in operational processes.

63

Oracle Database 19c TDE provides two options for performing tablespace conversions from clear-text to encrypted tablespaces. For deployments which require conversion to be performed with no downtime, online tablespace encryption runs in the background to convert tablespaces from clear text to encrypted text while systems remain operational. TDE also offers an offline tablespace conversion mode which efficiently converts tablespaces with no storage overhead.

LIMITING SENSITIVE DATA EXPOSURE WITH DATA REDACTION

Privacy and compliance require a cost-effective approach to managing data exposure in applications. The embrace of smartphone and tablet devices make the issue of sensitive data exposure even more urgent as data access beyond the traditional office environment becomes commonplace. Even traditional applications require a more comprehensive solution for reducing exposure to sensitive data, for example, a call center application with a screen that exposes customer credit card information and personally identifiable information to call center operators. Exposing that information, even to valid application users, may violate privacy regulations and put the data at unnecessary risk.

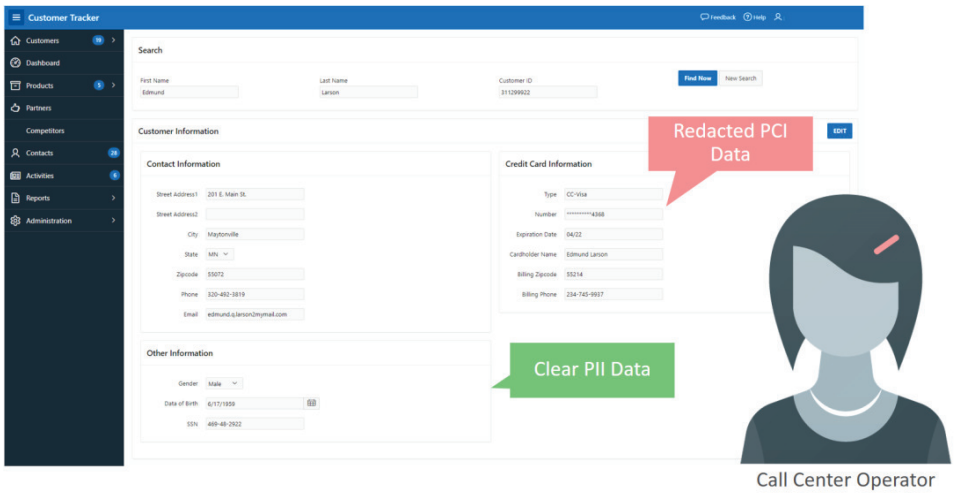


Figure 4. Clear and redacted information displayed in a call center application