



NoCOUG

Sprint Conference 2008

Date: Thursday, May 15, 2008

Time: 2:30 PM – 3:30 PM

Venue: Crowne Plaza, Columbus Room

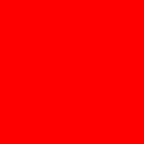
Foster City, CA

ORACLE®

Oracle Database Security in a Nutshell

Daniel T. Liu

Principal Solution Architect



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 remain at the sole discretion of Oracle.

Agenda

- 1. Introduction**
- 2. Security Requirements Overview**
- 3. Security Solutions Overview**
- 4. Oracle Database Security Features and Options**



Agenda

- 5. Auditing/Monitoring**
- 6. Authentication**
- 7. Authorization/Access Control**
- 8. Encryption**
- 9. Summary**





Introduction

1

Key Drivers for Data Security

Regulatory Compliance

- Sarbanes-Oxley (SOX), J-SOX, GLBA
- Payment Card Industry (PCI)
- HIPAA, EU Privacy Directives
- Breach Disclosure Laws
- COSO, COBIT frameworks
- Separation of duty, Proof of compliance, Risk Assessment and Monitoring



Insider / External Threats

- Large percentage of threats go undetected
- Outsourcing and off-shoring trend
- Customers want to monitor insider & DBA

Industry Security Standards

- **ISO 17799**
 - ISO-17799 is an international standard of security practices. It includes best practices, certification, and risk assessment.
 - <http://www.computersecuritynow.com/>
- **SANS Institute**
 - The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world.
 - <http://www.sans.org/index.php>
- **CERT/CC**
 - CERT/CC operated by Carnegie Mellon University for the Department of Defense
 - <http://www.cert.org/nav/index.html>



Security Requirements Overview

2

Define Organization Security Policy

- What is a Security Policy
- Developing your Security Policy
- Consider the following dimensions:
 - Physical
 - Personnel
 - Technical
 - Procedural
- Implementing Security Policy
- Easing Administration

Fundamental Data Security Requirements

- Confidentiality
- Integrity
- Availability
- Auditing

Components for Enforcing Security

- Authentication
- Authorization/Access Control
- Auditing
- Encryption

Principle of Least Privilege

- Install only the required software on the machine.
- Activate only the required services on the machine.
- Give operating system (OS) and database access to only those users who require access.
- Limit access to the root or administrator account.
- Limit access to SYSDBA and SYSOPER accounts.
- Limit users' access to only the database objects that are required to do their jobs.

Defense in Depth

- The concept of “defense in depth” is that no one failure jeopardizes the entire system. Detection and prevention measures are applied at every level.
 - Enforce security policies
 - Harden the operating system
 - Use firewalls
 - Use network security
 - Use database-security features
 - Train users



Security Solutions Overview

3

Oracle Database Security

Continuous Innovation



EM Data Masking

Oracle Database 11g

TDE Tablespace Encryption

Oracle Audit Vault

Oracle Database Vault

Secure Backup (Tape)

TDE Column Encryption

Oracle Database 10g

VPD Column Masking

VPD Column Relevant

EM Secure Config Scanning

Oracle Database 9i

Client Identity Propagation

Fine Grained Auditing

Oracle Label Security

Oracle8i

Proxy authentication

Enterprise User Security

Virtual Private Database (VPD)

Database Encryption API

Strong Authentication

Oracle7

Native Network Encryption

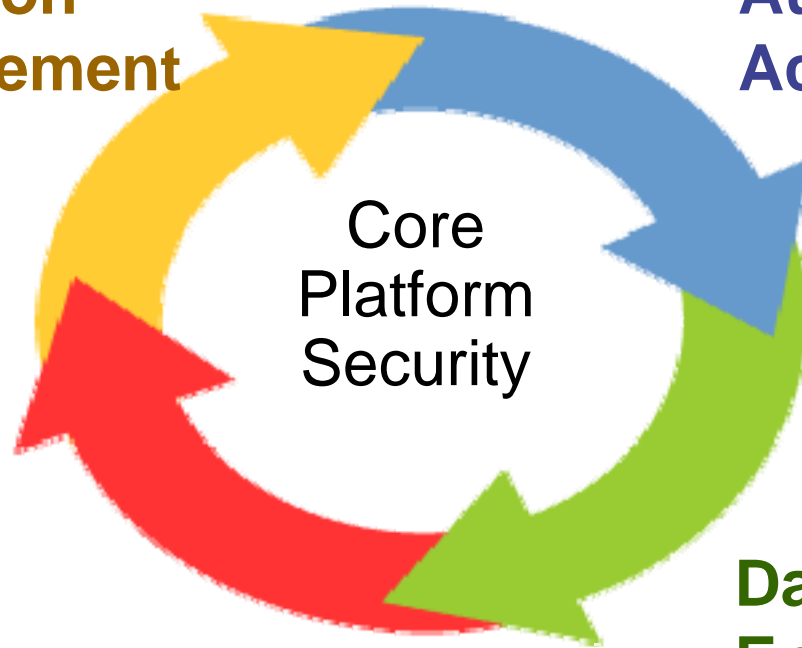
Database Auditing

Government customer

Data Security Components

Authentication
User Management

Authorization
Access Control



Auditing
Monitoring

Data Protection
Encryption

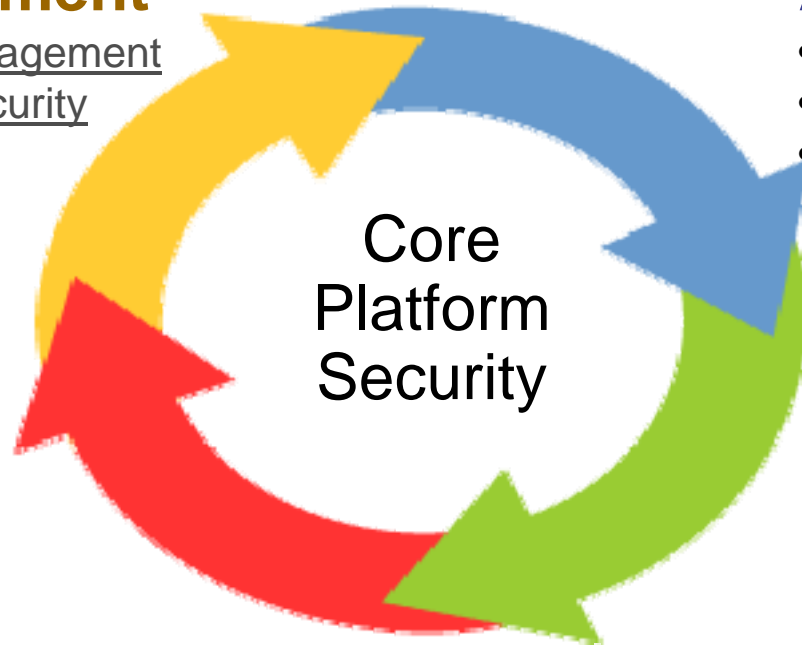
Data Security: Oracle Key Products

Authentication User Management

- Oracle Identity Management
- Enterprise User Security

Authorization Access Control

- Oracle Database Vault
- Virtual Private Database
- Oracle Label Security











































































Auditing Monitoring

- Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Data Protection Encryption

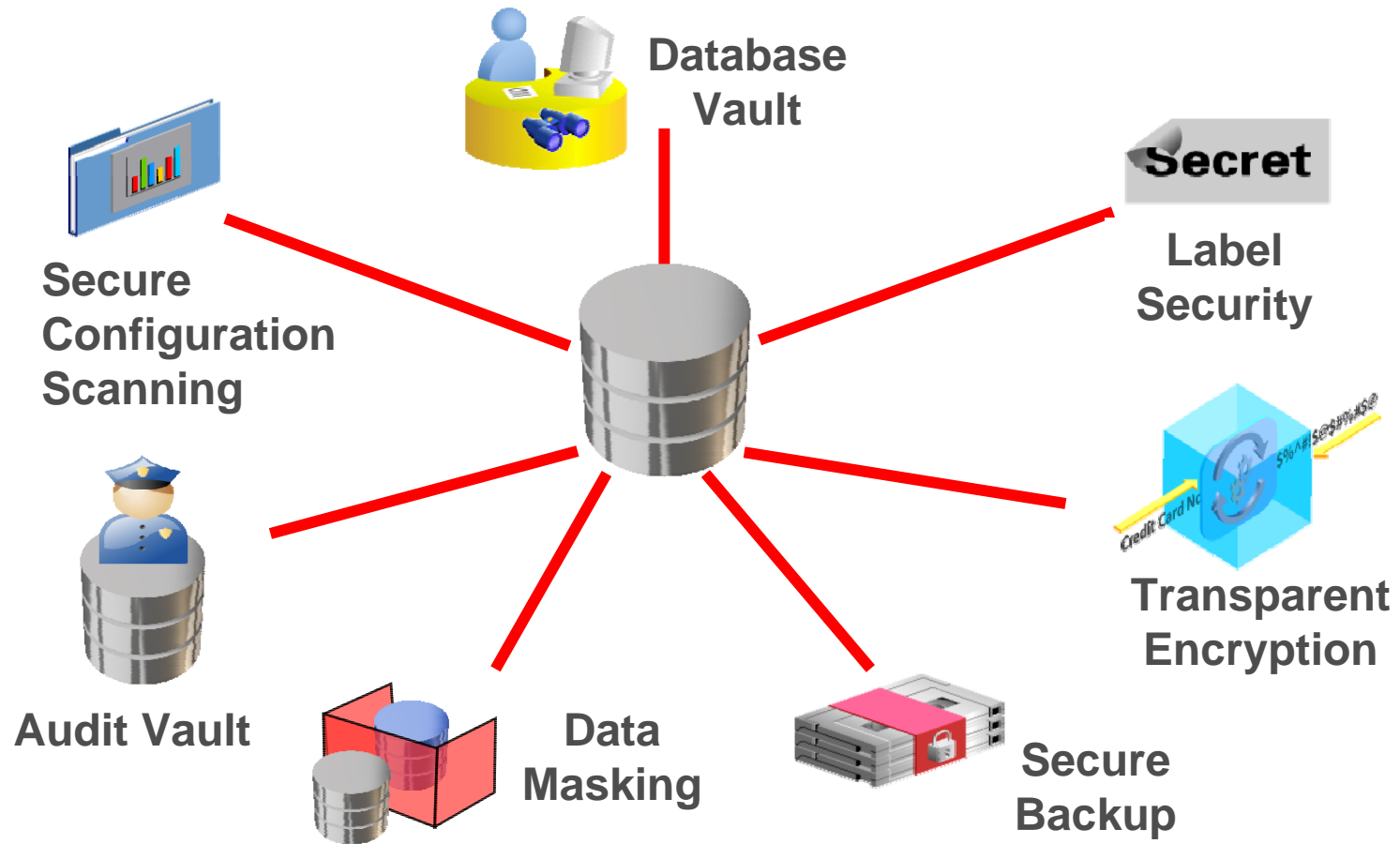
- Oracle Advanced Security
- Oracle Secure Backup
- EM Data Masking

Release Wide Map of Security Products

Solution	Oracle 8i	Oracle Database 9iR1	Oracle Database 9iR2	Oracle Database 10g R1	Oracle Database 10g R2	Oracle Database 11gR1
Database Auditing						
Network Encryption						
Virtual Private Database						
Label Security						
Privileged User Controls						
Enterprise User Security						
Fine Grained Auditing						
Client Identifier						
EM Configuration Scanning						
TDE Column Encryption						
TDE Tablespace Encryption						
EM Data Masking						

Oracle Database Security Products

Solution Summary for Security and Compliance





Oracle Database Security Features and Options

4

Oracle Database Security Features and Options

- Auditing
 - Auditing Database Users, Privileges, and Objects
 - Auditing DML Statements (FGA)
 - Audit Vault
- Authentication
 - Using Basic User Authentication
 - Using Strong Authentication
 - Using Enterprise User Security
 - Using Proxy Authentication

Oracle Database Security Features and Options

- Authorization and Access Control
 - Using Privileges and Roles
 - Implementing Database Vault
 - Implementing Fine-Grained Access Control (VPD)
 - Implementing Oracle Label Security

Oracle Database Security Features and Options

- Encryption
 - Concepts
 - Applying Column Encryption
 - Using Application-Based Encryption
 - Using Transparent Data Encryption (TDE)
 - Applying File Encryption
 - RMAN Encrypted Backups
 - Oracle Secure Backup



Auditing/Monitoring

5

Auditing/Monitoring

- Types of Databases Auditing
 - Basic Database Auditing
 - Value-based Auditing
 - Fine-grained Auditing (FGA)
- Oracle Audit Vault
- Oracle EM Configuration Pack

Data Security: Oracle Products

Authentication

User Management

- Oracle Identity Management
- Enterprise User Security

Authorization

Access Control

- Oracle Database Vault
- Virtual Private Database
- Oracle Label Security



Core
Platform
Security

Data Protection

Encryption

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

Auditing Monitoring

- **Oracle Database Auditing**
- Oracle Audit Vault
- EM Configuration Pack

Oracle Database Auditing

- Standard Database Auditing
 - Login events
 - Use of system and object privileges
 - Unsuccessful
- Value-based Auditing
 - Database Triggers
 - Capturing the actual values that were inserted, updated, or deleted
- Fine-grained auditing (FGA)
 - DBMS_FGA PL/SQL packages to created audit policy
 - SQL statements based on content

Standard Database Auditing

- Setup Auditing Destination

- Set the `AUDIT_TRAIL` parameter (static)
 - **NONE**: Disables collection of audit records (default)
 - **DB**: Enables auditing with records stored in the database
 - **DB,EXTENDED**: Populates `SQLBIND` and `SQLTEXT` columns
 - **XML**: Enables auditing with records stored in XML format OS files.
 - **XML,EXTENDED**: Includes `SQLBIND` and `SQLTEXT` columns
 - **OS**: Enables auditing with records stored in the OS audit trail
- Set the `AUDIT_FILE_DEST` parameter
- Set the `AUDIT_SYSLOG_LEVEL` parameter
- Set the `AUDIT_SYS_OPERATIONS` parameter for `SYSDBA` or `SYSOPER` actions

Standard Database Auditing

- Specifying Audit Options

- SQL statement auditing:

```
SQL> AUDIT table;
```

- System-privilege auditing (nonfocused and focused):

```
SQL> AUDIT select any table, create any trigger;
```

```
SQL> AUDIT select any table BY hr BY SESSION;
```

- Object-privilege auditing (nonfocused and focused):

```
SQL> AUDIT ALL on hr.employees;
```

```
SQL> AUDIT UPDATE,DELETE on hr.employees BY ACCESS;
```

Value-Based Auditing

- Database auditing records that inserts, updates, and deletes have occurred on audited objects, but does not capture the actual values that have been changed.
- Value-based auditing extends database auditing, capturing the actual values that have been changed.
- Value-based auditing leverages database triggers (event-driven PL/SQL constructs).
- Prior to Oracle Database 10g, value-based auditing was the only way to capture certain information. Transaction flashback can now be used to view the data as it was at a particular point-in-time.

Example 1

```
SQL> create table emp (name    varchar2(10),  
                        salary number(8,2));
```

Table created.

```
SQL> insert into emp  
      values ('DANIEL',2000);
```

1 row created.

```
SQL> commit;
```

Commit complete.

Example 1

```
SQL> update emp set salary = 3000  
      where name = 'DANIEL';
```

1 row updated.

```
SQL> commit;
```

Commit complete.

Example 1

```
SQL> select * from emp;
```

```
NAME                SALARY
```

```
-----
```

```
DANIEL                3000
```

```
SQL> select * from emp
```

```
versions between scn minvalue and maxvalue;
```

```
NAME                SALARY
```

```
-----
```

```
DANIEL                3000
```

```
DANIEL                2000
```

Example 2

```
SQL> select    versions_xid, name, salary
  2  from      emp
  3  versions between scn minvalue and maxvalue;
```

VERSIONS_XID	NAME	SALARY
0003000E00000FE2	DANIEL	3000
	DANIEL	2000

```
SQL> select *
  2  from flashback_transaction_query
  3  where  xid = '0003000E00000FE2';
```

Example 2

```
SQL> select xid, start_scn, start_timestamp,
 2         table_name, undo_sql
 3   from flashback_transaction_query
 4  where xid = '0009001F0000000B2';
```

XID	START_SCN	START_TIMESTAMP	TABLE_NAME
0009001F0000000B2	714980	Feb 21 2004 23:30:31	EMP

```
UNDO_SQL
-----
update "ORACLE"."EMP" set "SALARY" = `2000' where ROWID =
  'AAAMWJAAEAAAFsAAA';
```

Fine-Grained Auditing (FGA)

- Monitors data access based on content
- Audits `SELECT`, `INSERT`, `UPDATE`, or `DELETE`
- Can be linked to a table or view
- May fire a procedure
- Is administered with the `DBMS_FGA` package
- The FGA method was introduced in Oracle 9i database release. However this method provided support for only the 'SELECT' statements.
- With 10g database release, it becomes possible extend the FGA method to `UPDATE`, `INSERT`, and `DELETE` statements as well.

FGA on DML Example

BEGIN

```
dbms_fga.add_policy(  
    object_schema    => 'HR',  
    object_name      => 'EMPLOYEES',  
    policy_name      => 'EMP_AUDIT',  
    audit_condition  => 'SALARY > 1500',  
    audit_column     => 'COMMISSION_PCT',  
    handler_schema   => 'EMP_SCHEMA',  
    handler_module   => 'ALERT_HR',  
    enable           => TRUE,  
    statement_types  => 'SELECT,UPDATE,DELETE');
```

END

Data Security: Oracle Products

Authentication

User Management

- Oracle Identity Management
- Enterprise User Security

Authorization

Access Control

- Oracle Database Vault
- Virtual Private Database
- Oracle Label Security



Core
Platform
Security

Data Protection

Encryption

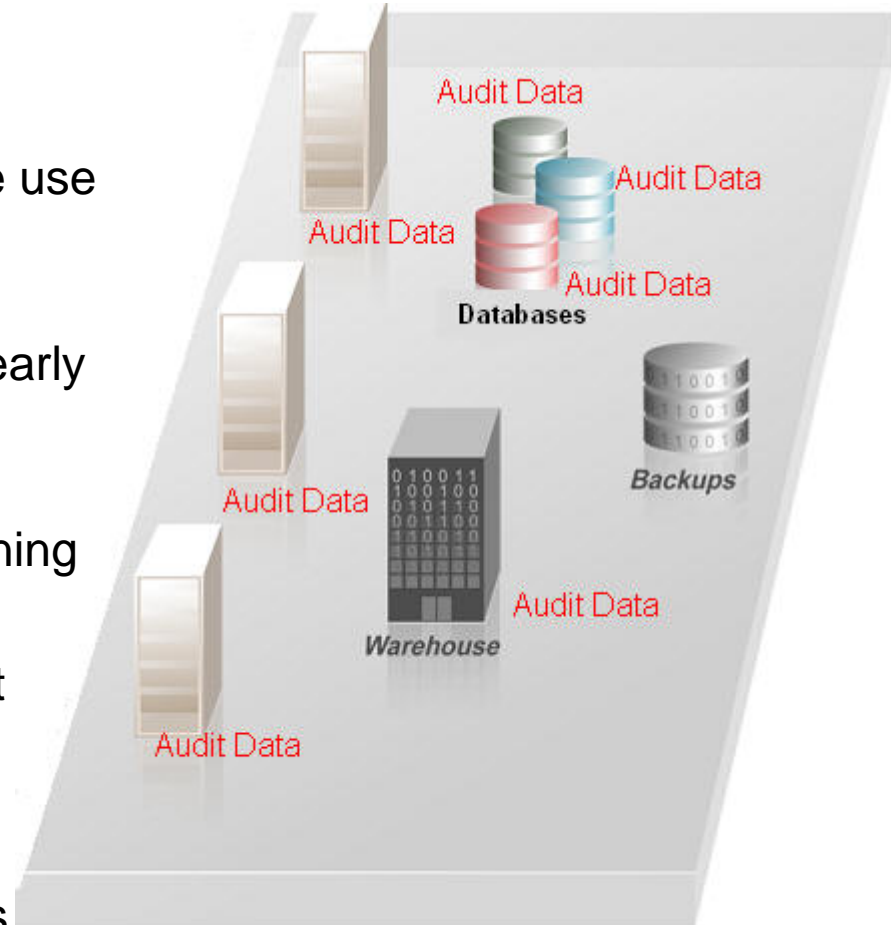
- Oracle Advanced Security
- Oracle Secure Backup
- EM Data Masking

Auditing Monitoring

- Oracle Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Need for Enterprise Auditing

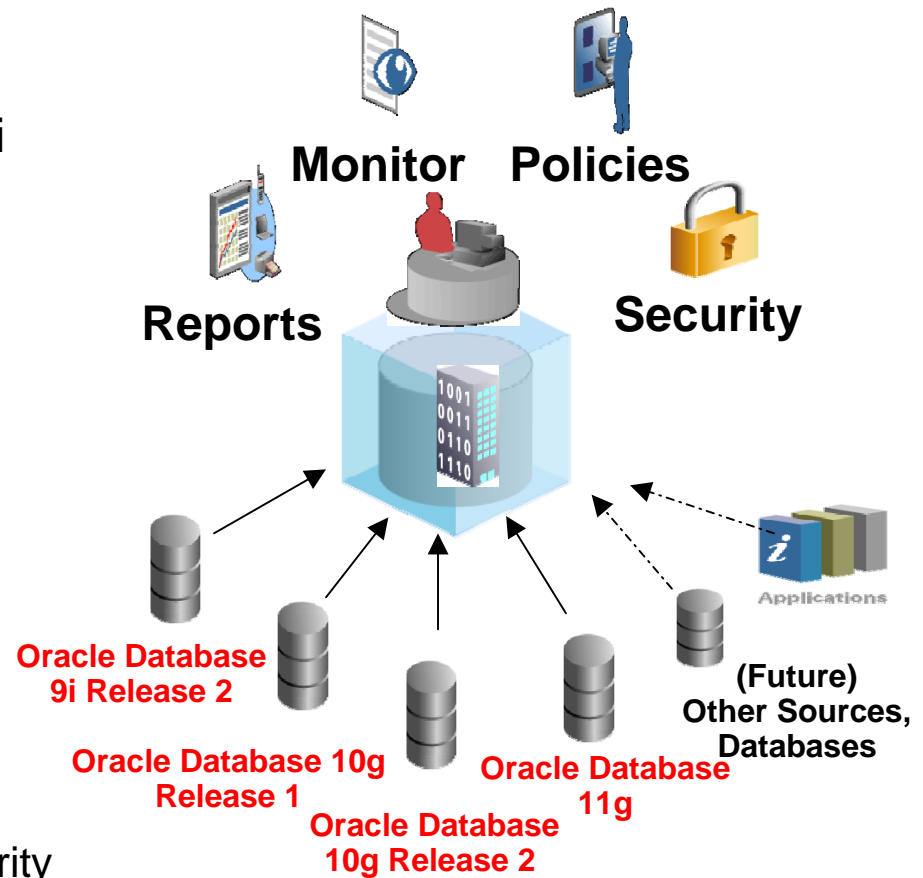
- Distributed audit data
 - Audit silos impact timely and effective use of audit data
- Reporting
 - Reporting on distributed audit data nearly impossible
- Monitoring and detection
 - Need efficiencies of centralized scanning
- Scalability and management
 - Need scale for large amounts of audit data
 - Need to secure audit data
 - Need ability to easily provision and monitor audit settings across systems



Oracle Audit Vault

Trust-but-Verify

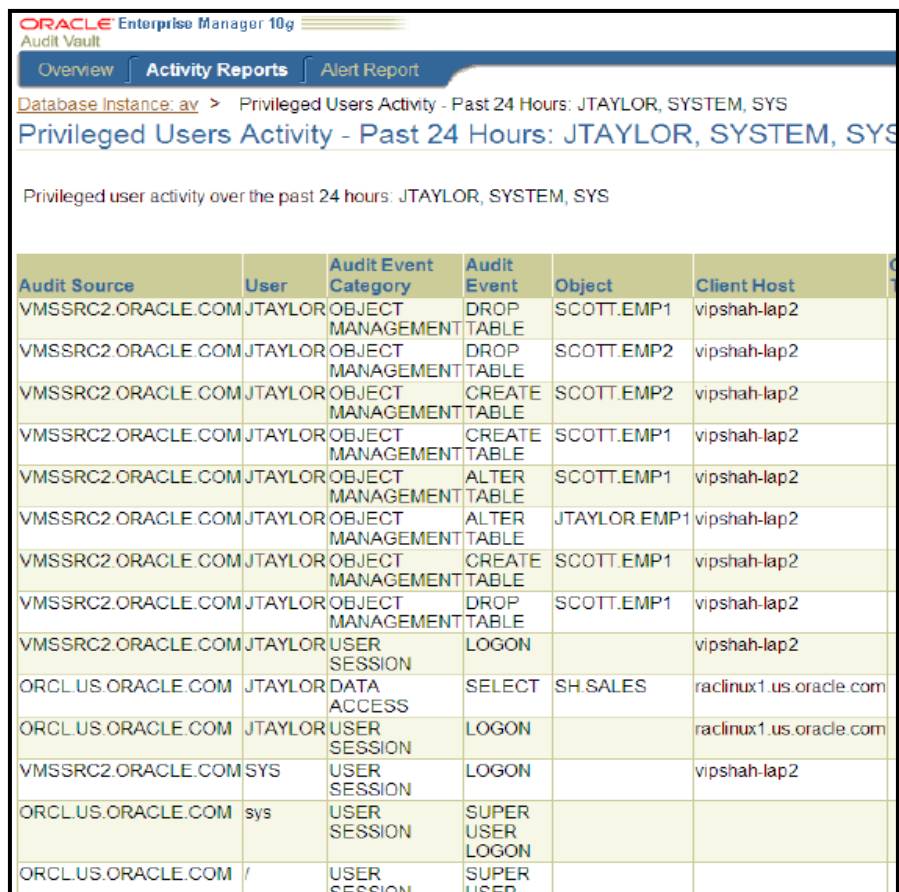
- Audit management
 - Consolidate audit data from Oracle 9i Release 2 and higher
 - Centrally manage / provision audit settings
- Compliance reporting
 - Built-in reports
 - Custom reports
- Detect and prevent
 - Insider Threats
 - Alert suspicious activity
- Security and scale
 - Embeds Database Vault, Advanced Security
 - Oracle Partitioning



Audit Vault Reports

Out-of-the-box Audit Assessments & Custom Reports

- Out-of-the-box reports
 - Privileged user activity
 - Access to sensitive data
 - Role grants, DDL activity
 - Login/logout
- User-defined reports
 - What privileged users did on the financial database?
 - What user 'A' did across multiple databases?
 - Who accessed sensitive data?
- Custom reports
 - Oracle BI Publisher, Application Express, or 3rd party tools



ORACLE Enterprise Manager 10g
Audit Vault

Overview Activity Reports Alert Report

Database Instance: av > Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

Privileged user activity over the past 24 hours: JTAYLOR, SYSTEM, SYS

Audit Source	User	Audit Event Category	Audit Event	Object	Client Host
VMSSRC2.Oracle.com	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.Oracle.com	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.Oracle.com	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.Oracle.com	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.Oracle.com	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.Oracle.com	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	JTAYLOR.EMP1	vipshah-lap2
VMSSRC2.Oracle.com	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.Oracle.com	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.Oracle.com	JTAYLOR	USER SESSION	LOGON		vipshah-lap2
ORCL.US.Oracle.com	JTAYLOR	DATA ACCESS	SELECT	SH.SALES	raclinux1.us.oracle.com
ORCL.US.Oracle.com	JTAYLOR	USER SESSION	LOGON		raclinux1.us.oracle.com
VMSSRC2.Oracle.com	SYS	USER SESSION	LOGON		vipshah-lap2
ORCL.US.Oracle.com	sys	USER SESSION	SUPER USER LOGON		
ORCL.US.Oracle.com	/	USER SESSION	SUPER USER		

Data Security: Oracle Products

Authentication

User Management

- Oracle Identity Management
- Enterprise User Security

Authorization

Access Control

- Oracle Database Vault
- Virtual Private Database
- Oracle Label Security



Core
Platform
Security

Data Protection

Encryption

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

Auditing Monitoring

- Oracle Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Configuration Pack

Oracle Enterprise Manager - Secure Config Scanning

ORACLE Enterprise Manager 10g
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports

Policy Groups Policies Security At a Glance

Evaluation Results: Secure Configuration for Oracle Database

View: All Results Filter By Target: All (Choose Target) (Clear) (Return)

Secure Configuration for Oracle Database

- Post Installation
- Oracle Directory and File Permissions
- Oracle Parameter Settings
- Database Password Profile Settings
 - Secure Failed Login Attempts Setting
 - Secure Password Life Time Setting
 - Secure Password Lock Time Setting
 - Secure Password Grace Time Setting
- Password Complexity Checking Enabled
- Database Access Settings

Policy Group: Secure Configuration for Oracle Database

Summary Trend Overview

Average Compliance Score (%) **87**

Summary For this policy group, 4 Database Instance targets were evaluated resulting in 59 violations. There were 28 rules violated.

Description Ensures adherence with best-practice security configuration settings that help protect against database-related threats and attacks, providing a more secure operating environment for the Oracle database.

Results

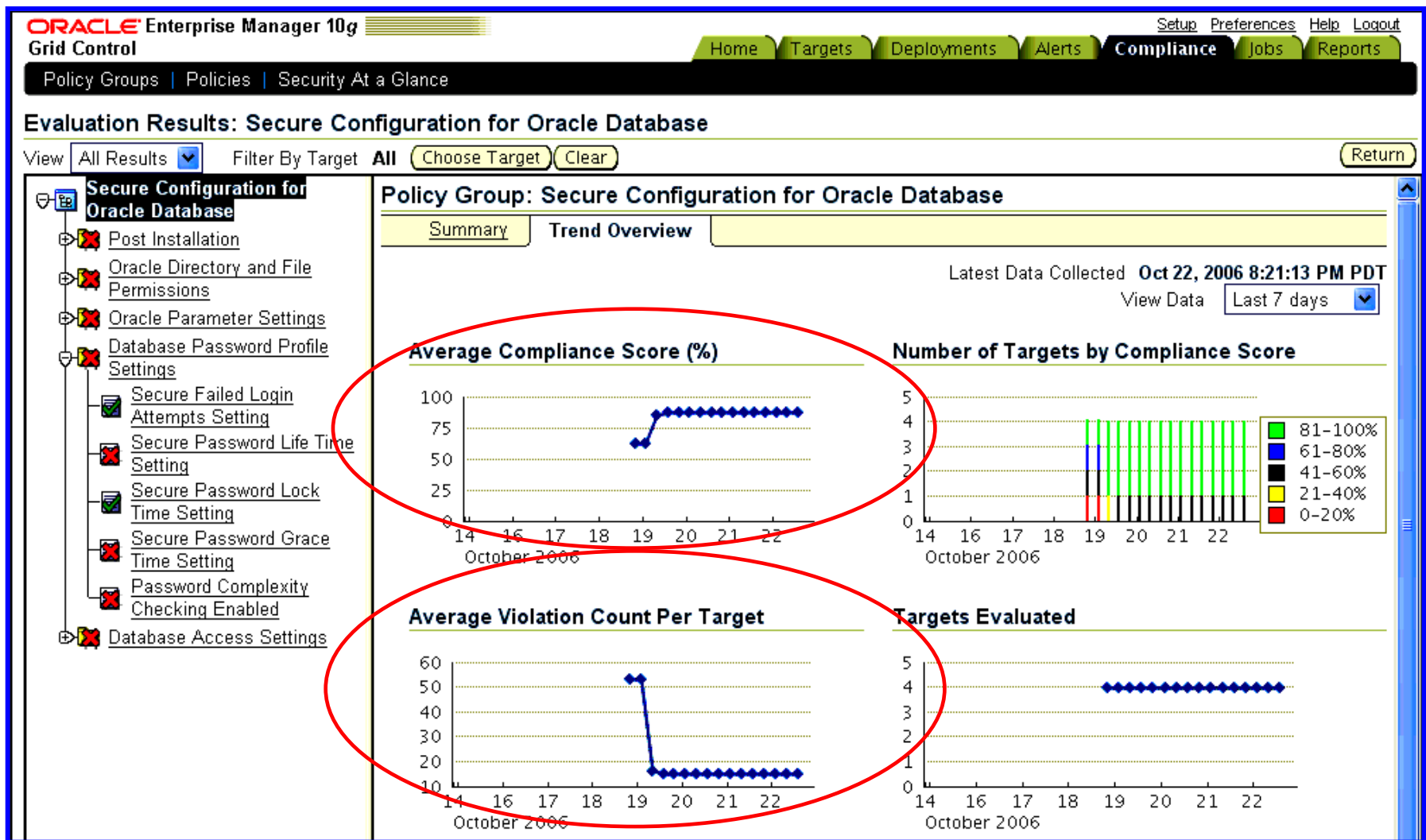
Target	Compliance Score (%)	Violations	Rules			Last Evaluation
			Violated	Compliant	Not Evaluated	
Oemrep Database	46	59	28	23	0 Oct 19, 2006 10:26:14 AM PDT	
Finance Prod	100	0	0	51	0 Oct 18, 2006 2:49:39 PM PDT	
Finance Dev	100	0	0	51	0 Oct 18, 2006 2:49:39 PM PDT	
ORCL_WORLD	100	0	0	51	0 Oct 18, 2006 2:49:39 PM PDT	

Map policies to best practices for continued compliance

"Implementation of EM security policies with round the clock monitoring and reporting helped demonstrate to our SoX auditors that Transcontinental were in control of their IT environment "
- Transcontinental

Tracking Compliance Over Time

Compliance Trend across IT infrastructure



Example of Security Policy Rules

Over 250 Built-in Policy Rules for Oracle9i and Higher

Database Services

- Enable listener logging
- Password-protect listeners
- Disallow default listener name
- Ensure listener log file is valid and owned by Oracle
- Ensure listener host name is specified with IP

Database File Permissions

- Init.ora should have restricted file permission
- Files in \$OH/bin should be owned by Oracle
- Data files should be owned by Oracle

Database Profile/Configuration

- Default Passwords
- Disallow access to objects by a fixed user link
- Disallow default tablespace set to SYSTEM
- Set password_grace_time
- Limit or deny access to DBMS_LOB
- Set password_reuse_max
- Avoid using utl_file_dir parameter

Host

- Detect open ports
- Detect insecure services
- Ensure NTFS file system type (Windows)

Application Server

- HTTPD has minimal privileges
- Use HTTP/S
- Apache logging should be on
- Demo applications disabled
- Disable default banner page
- Disable access to unused directories
- Disable directory indexing
- Forbid access to certain packages
- Disable packages not used by DAD owner
- Remove unused DAD configurations
- Password complexity enabled



Authentication

6

Authentication

- A basic security requirement is that you must know your users. Users can be authenticated in a different ways before they are allowed to create a database session.
 - Basic Authentication
 - Strong Authentication
 - Enterprise User Security
 - Proxy Authentication

Data Security: Oracle Products

Authentication User Management

- Basic Database Authentication
- Oracle Identity Management
- Enterprise User Security

Authorization Access Control

- Oracle Database Vault
- Virtual Private Database
- Oracle Label Security



Core
Platform
Security

Data Protection Encryption

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

Auditing Monitoring

- Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Basic Authentication

- User Identified by a Password
 - A database user:
 - Has a schema
 - Is easily audited
 - Is authenticated by a password in the database
 - `CREATE USER username IDENTIFIED BY password;`
 - `Sqlplus scott/tiger`

Basic Authentication

- User Identified Externally
 - A database user:
 - Has a schema
 - Is easily audited
 - Is authenticated by the operating system
 - `CREATE USER username IDENTIFIED EXTERNALLY;`
 - The parameter `OS_AUTHENT_PREFIX` (default to `OPS$`) determines the relationship between the OS account name and the database account name.
 - `CREATE USER OPS$MIKE IDENTIFIED EXTERNALLY;`
 - `su – mike`
 - `sqlplus /`
 - Set parameter `REMOTE_OS_AUTHENT = FALSE`

Strong Authentication

- Strong user authentication is a way of confirming the identity of the user with something other than a password.
- Smart cards, biometrics, certificates, and Kerberos tokens provide strong user authentication.
- Some of these methods are known as two-factor or multifactor authentication.
- Two-factor authentication requires something that the user knows plus something that the user has.

Strong Authentication

- Is stronger than password authentication
- Often includes single sign-on functionality
- Is supported by the following authentication technologies:
 - Certificates, public key infrastructure (PKI)
 - RADIUS, token, and smart cards
 - Kerberos
- Integrates with Oracle Net Services
- Requires Oracle Advanced Security
- `CREATE USER username IDENTIFIED GLOBALLY AS 'CN=architect, OU=it, O=oracle, C=US';`

External Secure Password Store

- Oracle Wallet

- The password store is an Oracle wallet created to provide a secure method of storing user login passwords.
- This is an auto login wallet by default so a password is not needed to open the wallet.
- The OS authenticates the user, and file system permissions control access to the wallet.
- The credentials to access the database are extracted from the wallet for the user.

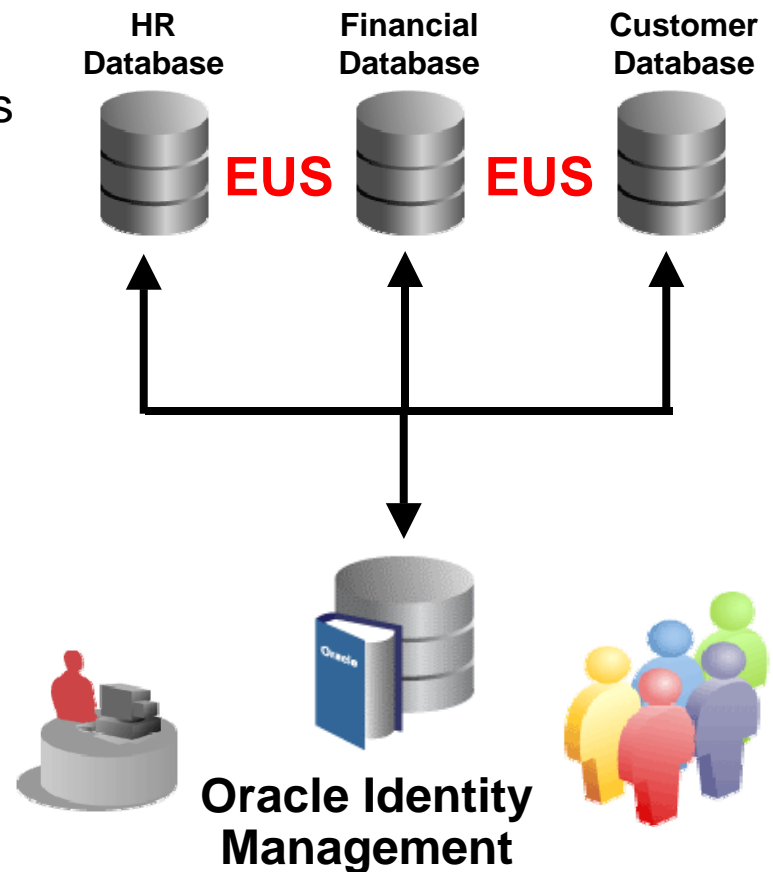
```
Mkstore -wrl <wallet_location> -create
```

```
Mkstore -wrl <wallet_location> -createCredential <db_connect_string>  
<username> <password>
```

Enterprise User Security

Database User Management

- User Management for Compliance
 - Centralized User Management
 - Map users to shared database schemas
 - Requires Oracle Directory Services
- Enterprise Roles
 - Centralized user role management
 - Centralized SYSDBA membership
- Authentication Methods
 - Password
 - Kerberos (Microsoft, MIT)
 - PKI (x.509v3)
- Heterogeneous Directory Support
 - Oracle Virtual Directory connectivity to Active Directory, Sun, Novell



Proxy Authentication

- Security challenges of Three-Tier computing
 - Who is the real user?
 - Can the user be re-authenticated to the database?
 - Does the middle tier have more privileges than required?
- Common Implementations of Authentication
 - Pass-through: The user is unknown to the application
 - One big-application user: The user is unknown to the database
 - Other methods
 - The user is re-authenticated to the database
 - The user is identified to the database
 - The user is proxied

Proxy Authentication

- Using Proxy Authentication for Database Users

- Authenticate the user without a database password:

```
ALTER USER john  
GRANT CONNECT  
THROUGH appuser;
```

- Authenticate the user with a database password:

```
ALTER USER john  
GRANT CONNECT  
THROUGH appuser  
AUTHENTICATED USING PASSWORD;
```




Authorization Access Control



Authorization

- Authorization is the process that determines the privileges that the user is allowed to exercise. In the Oracle database, authorization is determined by the grant of system and object privileges. A named set of grants is a role, and it may be granted as a unit.
 - Using Privileges and Roles
 - Using Application Contexts

Privileges

- There are two types of user privileges:
 - System privileges:
 - Enables users to perform particular actions in the database.
 - There are over 150 distinct system privileges.
 - Object privileges:
 - Enables users to access and manipulate a specific object, such as a table, view, sequence, procedure, function, or package.

Roles

- Roles are named groups of related privileges that are granted to users or to other roles. They are designed to ease the administration of privileges in the database and, therefore, improve security.
- Role Characteristics
 - Privileges are granted to and revoked from roles as if the role were a user.
 - Roles can be granted to and revoked from users or other roles as if they were system privileges.
 - A role can consist of both system and object privileges.
 - A role can be enabled or disabled for each user who is granted the role.
 - A role can require a password to be enabled.
 - Roles are not owned by anyone, and they are not in any schema.

Predefined Roles

CONNECT	CREATE SESSION
RESOURCE	CREATE TABLE, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, CREATE TYPE, CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR
SCHEDULER_ ADMIN	CREATE ANY JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER
DBA	Most system privileges, several other roles. Do not grant to Non-administrators.
SELECT_ CATALOG_ ROLE	No system privileges, but over 1600 object privileges on the data dictionary

CONNECT Role Change

- Prior to Oracle Database 10g Release 2, the CONNECT role had the following privileges:
 - ALTER SESSION, CREATE SESSION, CREATE CLUSTER, CREATE SYNONYM, CREATE DATABASE LINK, CREATE TABLE, CREATE SEQUENCE, and CREATE VIEW.
- Now, the CONNECT role has only the CREATE SESSION privilege
- The rstrconn.sql script located in the \$ORACLE_HOME/rdbms/admin directory is provided to restore the old privileges to the CONNECT role.
- After a database upgrade or new database creation, this script can be used to grant back the privileges removed from the CONNECT role.

Access Control

- Implementing Database Vault
- Implementing Fine-Gained Access Control (VPD)
- Implementing Oracle Label Security

Data Security: Oracle Products

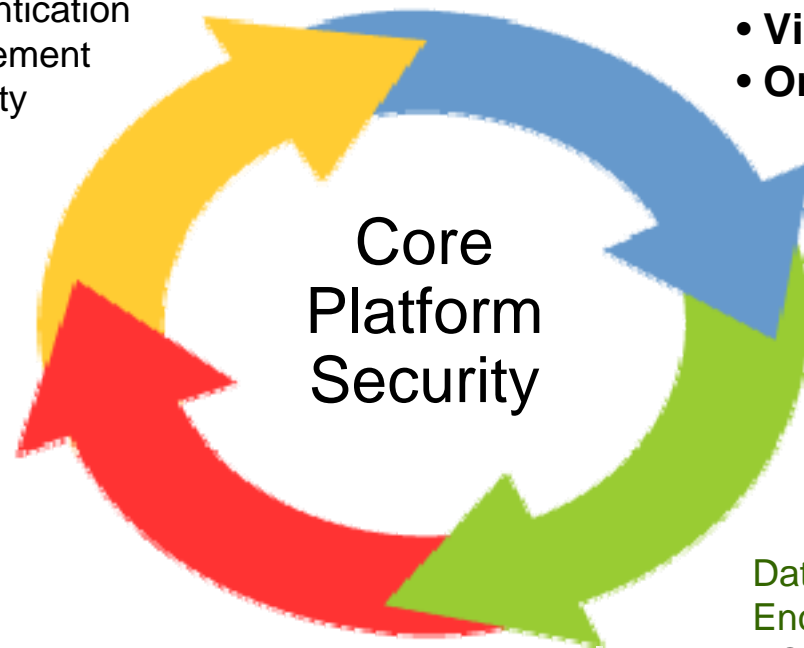
Authentication

User Management

- Basic Database Authentication
- Oracle Identity Management
- Enterprise User Security

Authorization Access Control

- **Oracle Database Vault**
- **Virtual Private Database**
- **Oracle Label Security**



Monitoring Auditing

- Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

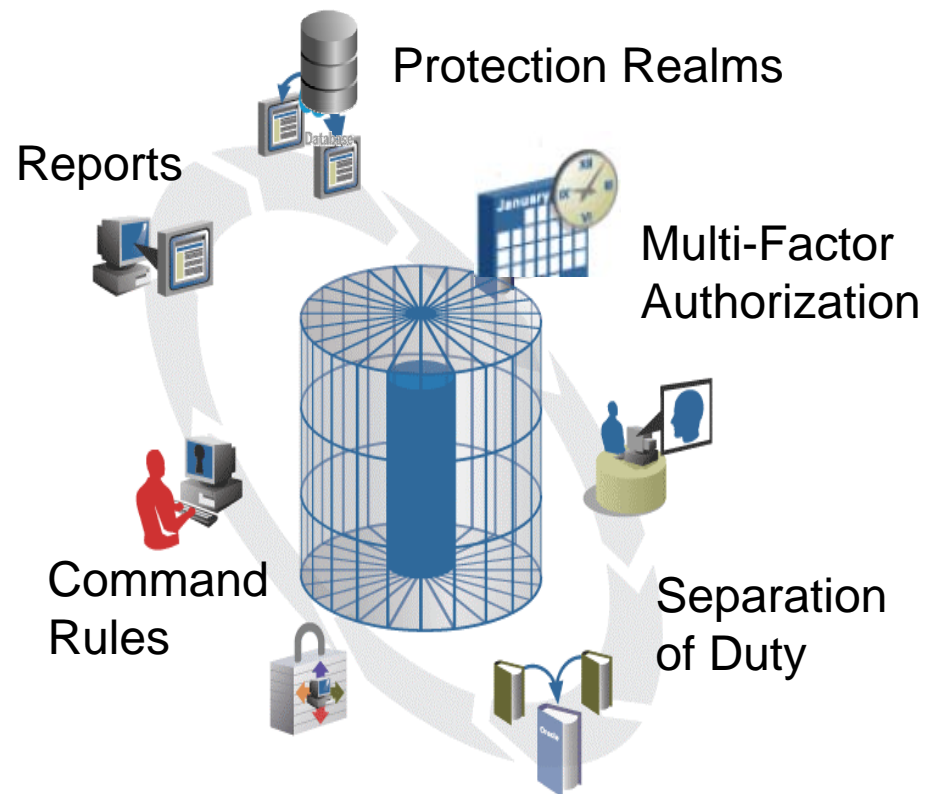
Data Protection Encryption

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

Oracle Database Vault

Compliance and Insider Threats

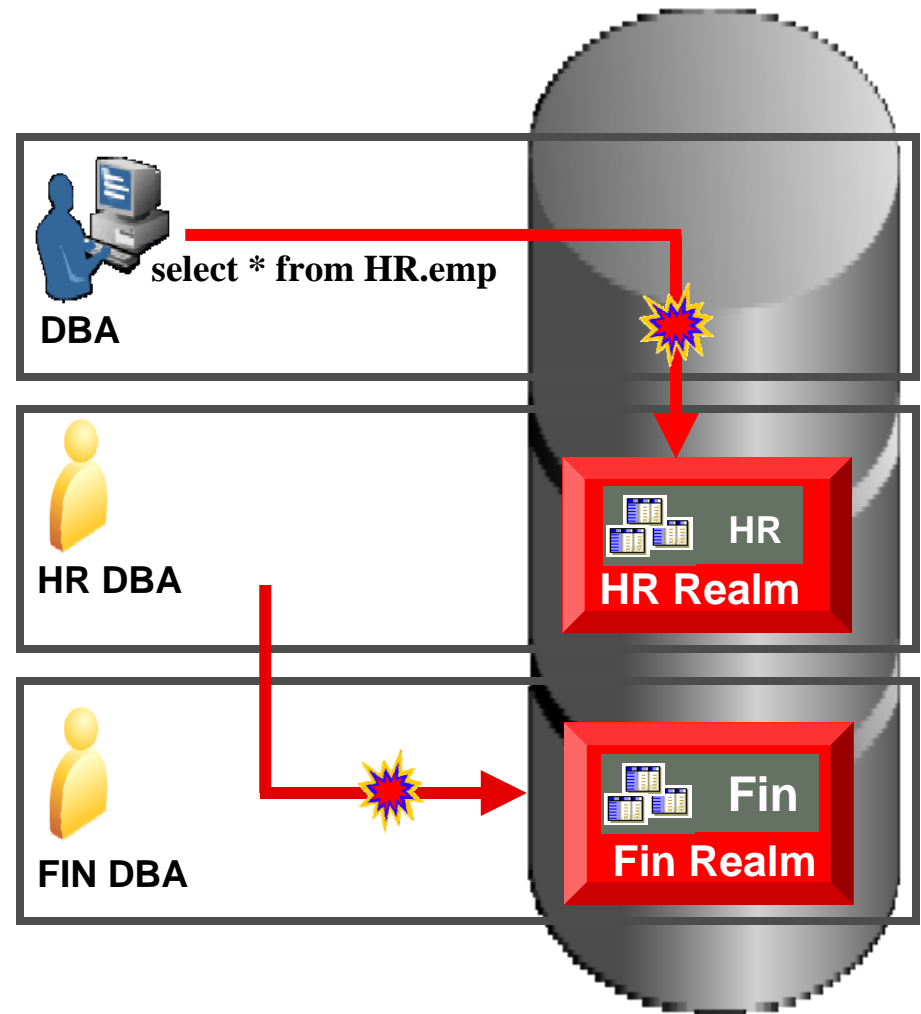
- Controls on privileged users
 - Restrict highly privileged users from application data
 - Provide Separation of Duty
 - Security for database and information consolidation
- Real time access controls
 - Control who, when, where and how data is accessed
 - Make decision based on IP address, time, auth...



Oracle Database Vault

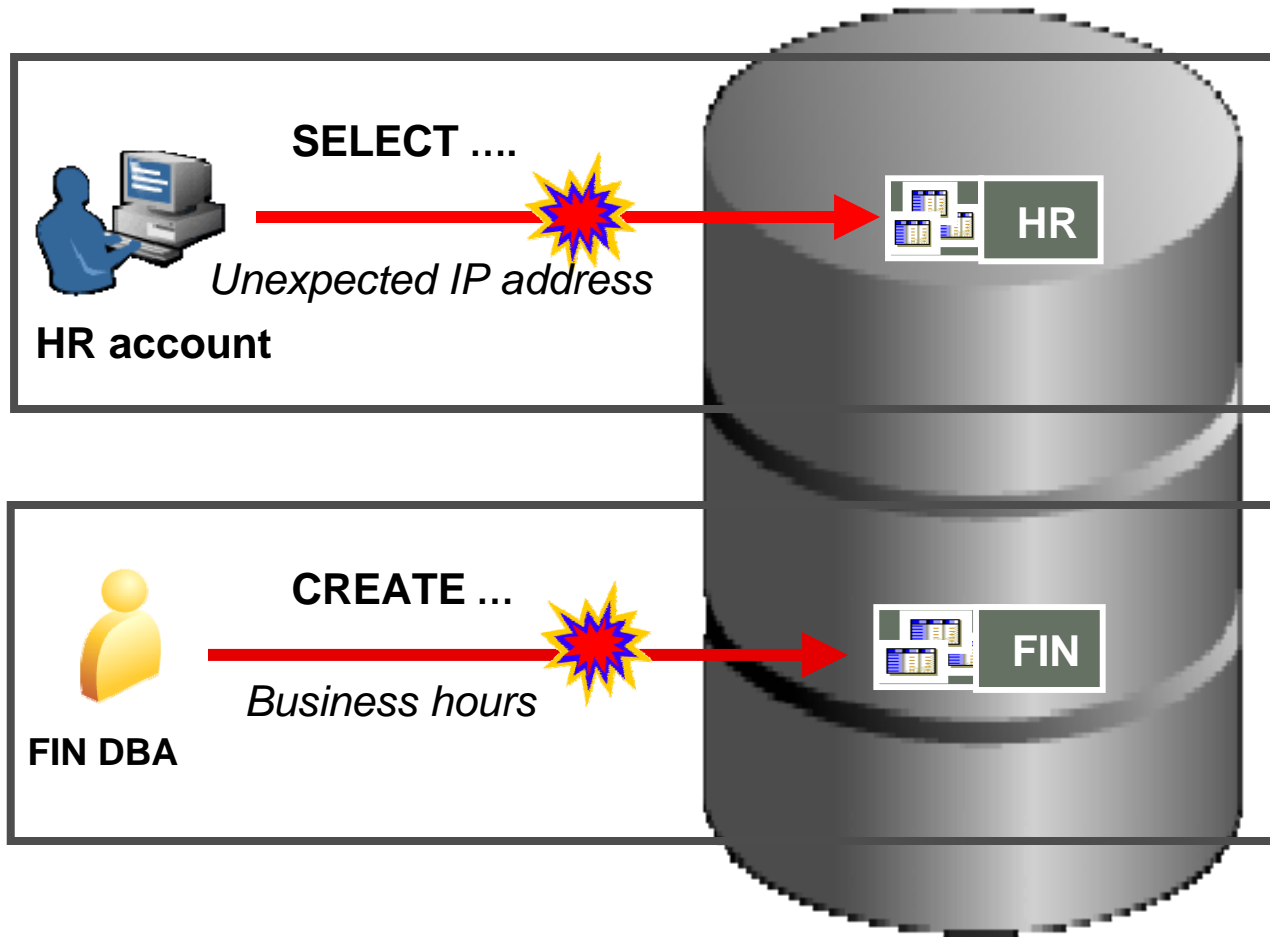
Protection Realms

- Database DBA views HR data
Compliance and protection from insiders
- HR DBA views Fin. data
Eliminates security risks from server consolidation



Oracle Database Vault

Transparent Multi-factor Authorization



Oracle Database Vault

Availability and Application Certification

- Availability
 - Oracle 9.2.0.8*
 - Oracle 10.2.0.3
 - Oracle Database 11g
- Application certification
 - PeopleSoft (Done)
 - E-Business Suite (Done)
 - Siebel (Near completion)
 - Other Partner applications (In process)

Data Security: Oracle Products

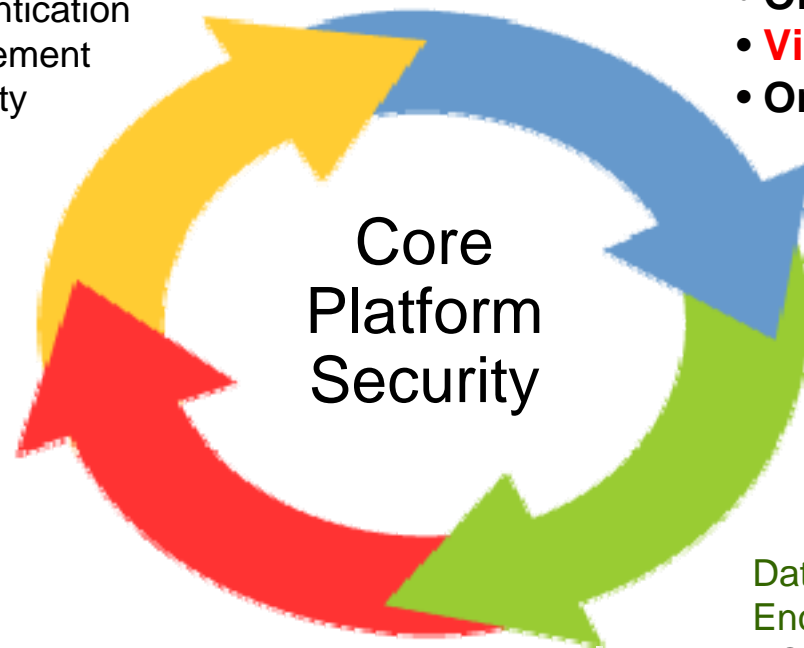
Authentication

User Management

- Basic Database Authentication
- Oracle Identity Management
- Enterprise User Security

Authorization Access Control

- Oracle Database Vault
- **Virtual Private Database**
- Oracle Label Security



Monitoring Auditing

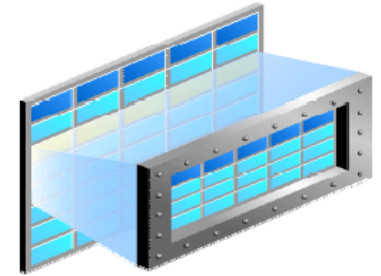
- Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Data Protection Encryption

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

Virtual Private Database (VPD)

Real Time Fine Grained Access Control



- Database enforced security
 - Attach to table, view (Oracle8i)
 - Attach to table column (Oracle Database 10g)
 - Optional column masking (Oracle Database 10g)
- Application context
 - Database protected security attributes
 - Defined and initialized by application
 - Reference using sys_context
- DBMS_RLS package
 - VPD API

Virtual Private Database

Real Time Fine Grained Access Control



```
Select * from  
customers;
```

```
VPD  where account_mgr_id =  
sys_context('APP', 'CURRENT_MGR');
```

CUST_LAST_NAME	SSN	CREDIT_LIMIT	ACCOUNT_MGR_ID
Edwards	701-495-2123	25000	145
Mahoney	121-791-4212	15000	145
Warden	181-095-1232	10000	147
Landis	581-295-7603	12000	147
Dvrrie	431-395-9332	17000	148
Belushi	381-395-9223	15000	148
Seignier	483-562-0912	1200	149
Powell	461-978-8212	1200	149



SYS_CONTEXT can be initialized via database login trigger or application login module

Virtual Private Database

Column Relevant Fine Grained Access Control

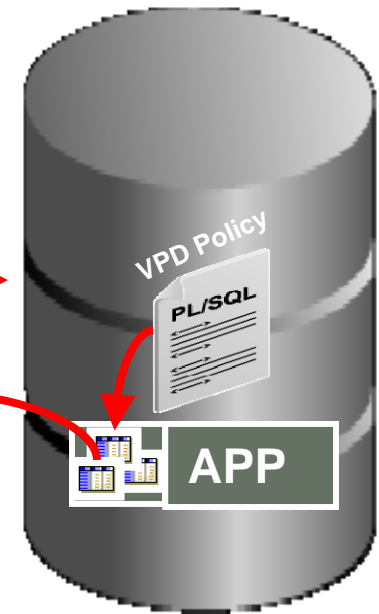
- Introduced in Oracle Database 10g
- Filter rows if specific column is referenced
- Optionally return all rows but mask column



```
Select * from  
customers;
```

```
VPD  where account_mgr_id =  
sys_context('APP', 'CURRENT_MGR');
```

CUST_LAST_NAME	SSN	CREDIT_LIMIT	ACCOUNT_MGR_ID
Edwards	701-495-2123	25000	145
Mahoney	121-791-4212	15000	145
Warden	181-095-1232	10000	147
Landis	581-295-7603	12000	147
Dvrrie	431-395-9332	17000	148
Belushi	381-395-9223	15000	148
Seignier	483-562-0912	1200	149
Powell	461-978-8212	1200	149



Data Security: Oracle Products

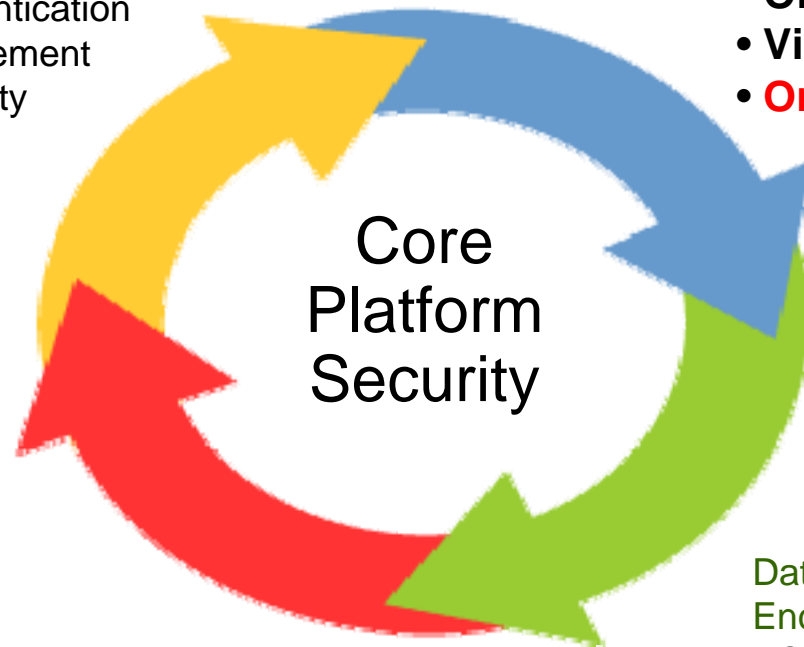
Authentication

User Management

- Basic Database Authentication
- Oracle Identity Management
- Enterprise User Security

Authorization Access Control

- Oracle Database Vault
- Virtual Private Database
- **Oracle Label Security**



Monitoring Auditing

- Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Data Protection Encryption

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

Need for Label Based Access Control

- Key Drivers
 - Multi-Level Security (MLS)
 - Government & defense
 - Data classification
 - Security and compliance
- Key Requirements
 - Transparent
 - Performant
 - Highly flexible
 - Evaluated*

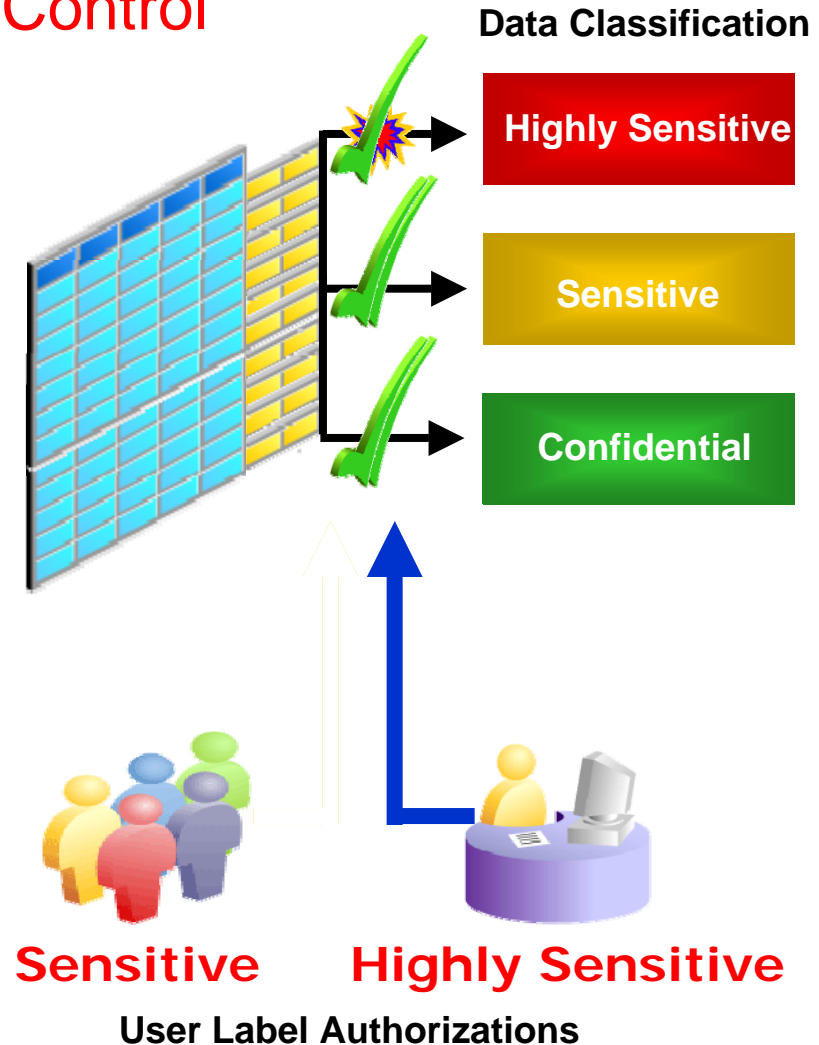


* Note - US NTISSP #11 requires all systems used in National Security systems to be evaluated

Oracle Label Security

Real Time Label Based Access Control

- Data Classification
 - Assign data classification to rows
 - Transparent, hidden column
 - Low storage overhead
- Enforce need-to-know
 - Assign label authorizations to database and application users
 - Transparent enforcement
 - Built-in proxy capability for application user models



Oracle Label Security 10.2.0.3 has a Common Criteria (CC) EAL4+ evaluation

Encryption



Encryption

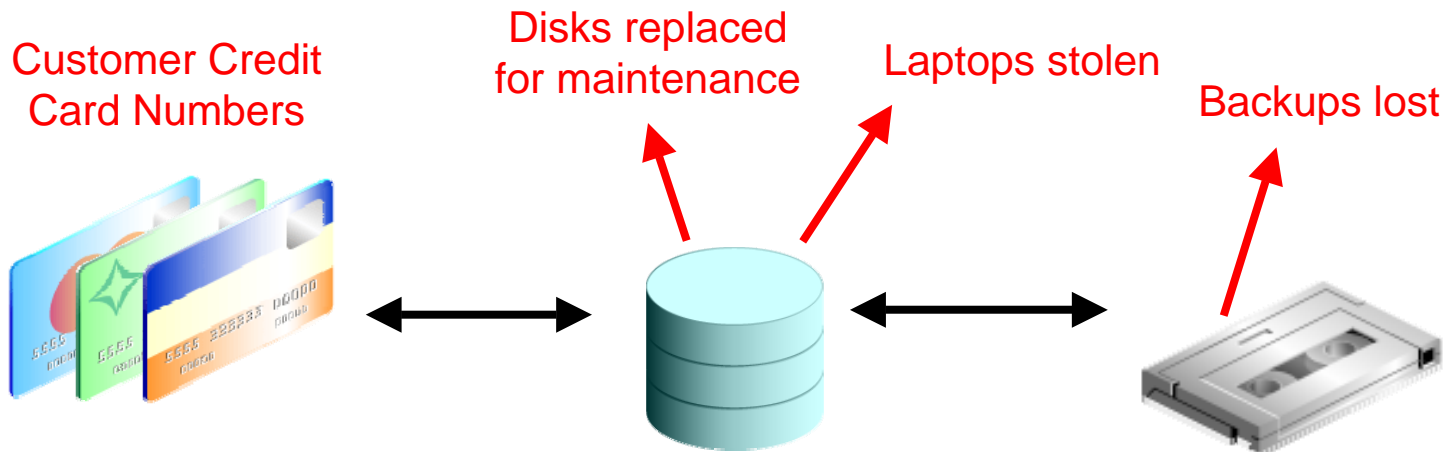
- Concepts
- Applying Column Encryption
 - Application-Based Encryption
 - Transparent Data Encryption (TDE)
- File Encryption
 - RMAN Encrypted Backups
 - Secure Backup
- EM Data Masking

Encryption Concept

- In cryptology, **encryption** is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is **encrypted** information (in cryptography, referred to as ciphertext). In many contexts, the word **encryption** also implicitly refers to the reverse process, **decryption** (e.g. “software for encryption” can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

The Need for Encryption

- Key Drivers
 - Millions of records lost and many more vulnerable
 - Worldwide privacy, security and compliance regulations
 - Personal privacy data: Credit Cards, Social ID, ...
 - PCI, breach notification laws, Country-specific laws
- Key Requirements
 - Encrypting data in existing applications with minimal perf impact
 - Automated Key Management



Encryption Issues

- Cost of Encryption
 - Performance related to encryption and decryption of data
 - Management of encryption keys
- Access Control
 - Encrypting stored data must not interfere with access control
- Access by Privileged Users
 - DBAs can access all data
 - System Administrator has access to all data files
 - Backup Media may be compromised
- What to Encrypt
 - Whole database, tables, columns

Key Management

- Key Generation
 - DBMS_CRYPTO.RANDOMBYTES is based on RSA x9.31 PRNG
 - DBMS_OBFUSCATION_TOOLKIT.GETKEY is still available
 - DBMS_RANDOM is not approved
- Key Modification
 - Modify periodically
 - Re-encrypt the data while data is not being accessed
- Key Transmission
 - Electronic transmission
 - Physical transmission
- Key Storage
 - Store in Database
 - Store in Operating system file
 - Letting the user manage the key

Data Security: Oracle Products

Authentication

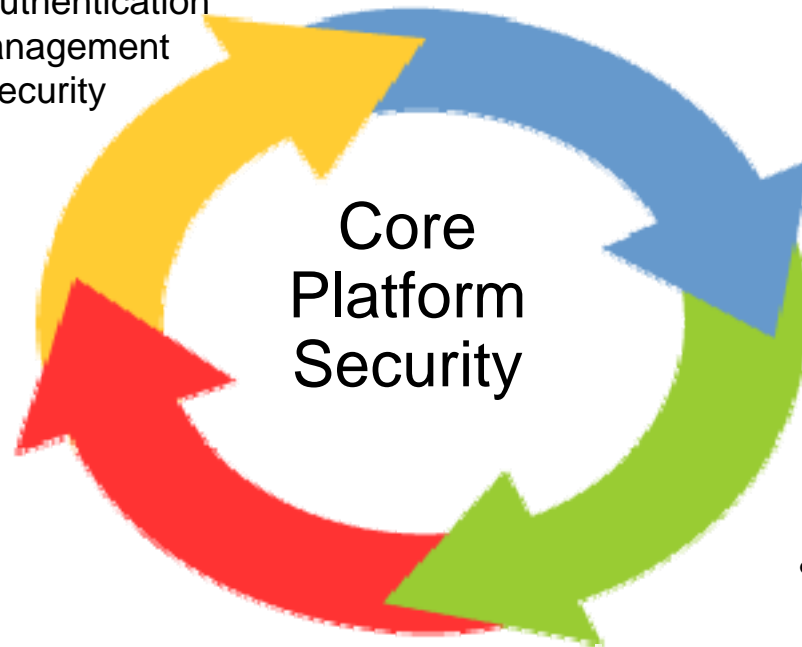
User Management

- Basic Database Authentication
- Oracle Identity Management
- Enterprise User Security

Authorization

Access Control

- Oracle Database Vault
- Virtual Private Database
- Oracle Label Security



Data Protection Encryption

- **Oracle Advanced Security**
 - DBMS_CRYPTO
 - TDE
 - RMAN Encrypted Backups
- **Oracle Secure Backup**
- **EM Data Masking**

Monitoring

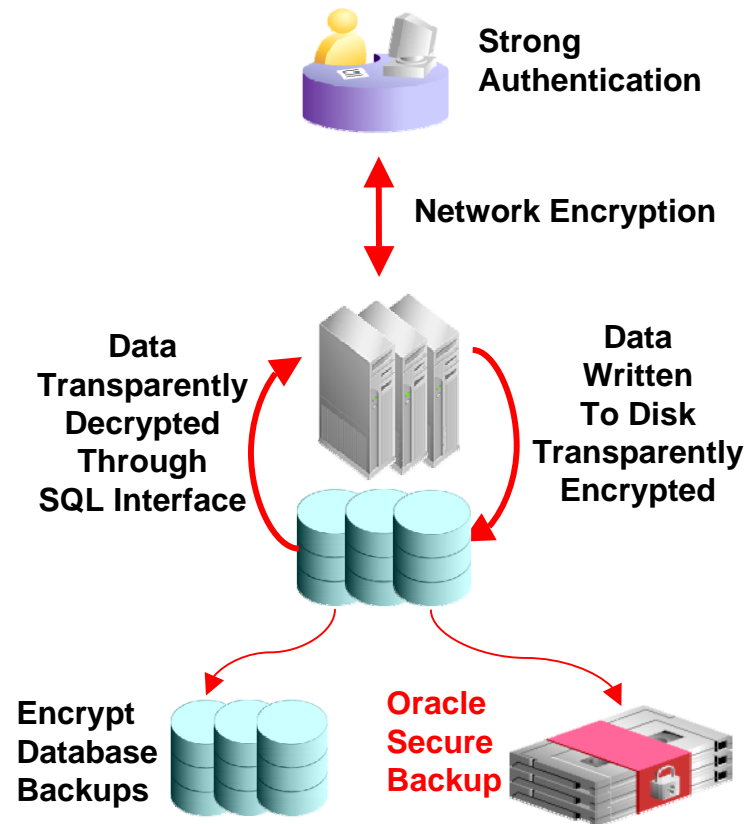
Auditing

- Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Oracle Advanced Security

Transparent Data Encryption at Rest and in Transit

- Network Encryption
 - Native encryption for fast easy setup
 - Secure Sockets Layer (SSL)
- Data at Rest Encryption
 - Column (10gR2)
 - RMAN backup (10gR2)
 - Tablespace (11g)
 - Data Pump export files (11g)
- Key Management
 - Built-in two tier architecture
 - Oracle Wallet (PKCS #12)



Application-Based Encryption

- Encryption of data stored in the database
- DBMS_CTYPTO package :
 - Encrypts column data
 - Decrypts column data
 - Supersedes DBMS_OBFUSCATION_TOOLKIT (9i and earlier), provides enhanced procedures and functions for encryption, decryption, hash functions, and key generation
 - Random number generator for generating secure encryption keys
 - Including RAW and large objects (LOBs)

Application-Based Encryption

- **ENCRYPT:**

```
encrypted_raw := dbms_crypto.Encrypt (  
    src => raw_input,  
    typ => dbms_crypto.DES3_CBC_PKCS5,  
    key => raw_key);
```

- **DECRYPT:**

```
decrypted_raw := dbms_crypto.Decrypt (  
    encrypted_raw,  
    dbms_crypto.DES3_CBC_PKCS5,  
    raw_key);
```

Transparent Data Encryption

- Encryption of data stored in the database
- Encryption of column data
- Encrypts data:
 - In the data files
 - In redo log and archive log files
 - In memory
 - In file backups
- Manages keys automatically
- Allows data access only when authorized by the database mechanisms

Transparent Data Encryption

Manageability

ORACLE Enterprise Manager 11g Database Control

Database Instance: orcl.us.oracle.com > Tables > Logged in As SYSTEM

Encryption Options for Table : CUSTOMERS

Specify the encryption algorithm and the key seed to be used for all encrypted columns in this table. The SALT option for a column encryption can be configured on Advanced Attribute page.

Encryption Algorithm: AES192

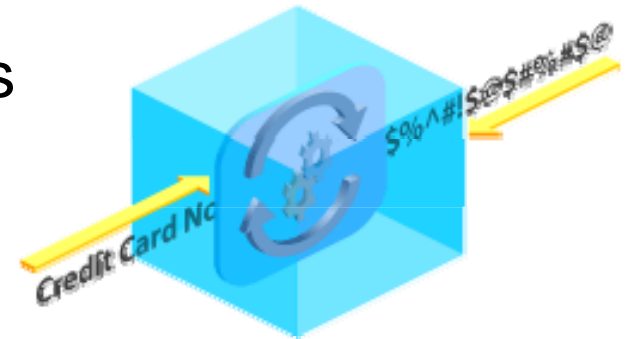
Key Generation: Key value is used to seed the random number generator that generates

Select	Name	Data Type	Size	Scale	Not NULL	Default Value	Encrypted
<input type="checkbox"/>	CUSTOMER_ID	NUMBER	6		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	CUST_FIRST_NAME	VARCHAR2	20		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	CUST_LAST_NAME	VARCHAR2	20		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	CREDIT_CARD_NUMBER	VARCHAR2	16		<input type="checkbox"/>		<input checked="" type="checkbox"/>

Transparent Data Encryption

Easy Uptake

- No changes to existing applications
 - No triggers, no views
 - Minimal performance impact
 - Built-in key management
- No crash-course needed in encryption or key management; just focus on business logic
- Simple `Alter Table` statement for TDE column
- Simple addition to `Create Tablespace` syntax



See E-business Suite Metalink note on TDE

SAP has support notes on using TDE

Transparent Data Encryption

- TDE Encrypt/Decrypt data via an External Security Module (ESM)
- The default ESM is the Oracle Wallet (holds the Master Key)
- Oracle Database 11g support storing the TDE master encryption key externally on a hardware security module (HSM) device
- TDE creates a key for each table that uses encrypted columns. The table key is stored in the data dictionary.
- There is one master key for the database.

Transparent Data Encryption

- The master key is required to access any encrypted data.
- Regenerating the master key does not cause the column data to be re-encrypted.

```
SQL> ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "walled  
password"
```

- TDE is supported only with Data Pump export and import
- SYS schema objects cannot be encrypted

File Encryption

- RMAN Encrypted Backups
- Oracle Secure Backup Encryption

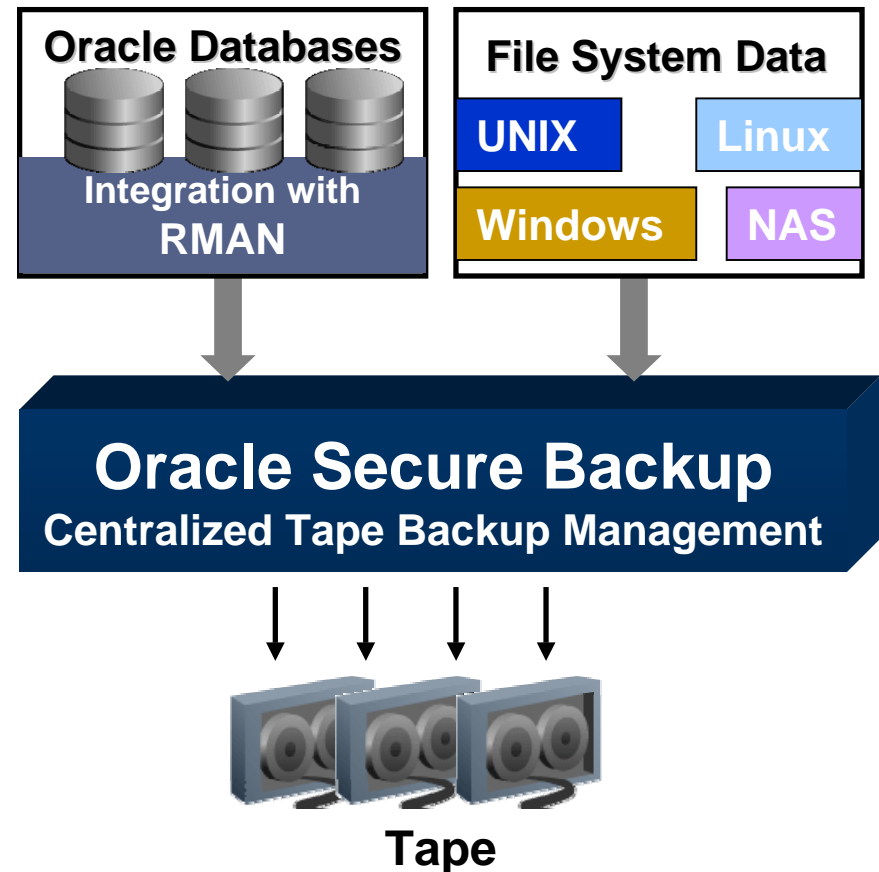
RMAN Encrypted Backups

- Recovery manager (RMAN) can create encrypted backup to either tape or disk as long as the required Oracle key management infrastructure is available.
- RMAN encryption can use either a password-based key or a generated key held in the Oracle wallet.
- RMAN backup encryption is only available in Enterprise Edition, and the COMPATIBLE parameter must set to 10.2.0 or higher.
- Encrypt backup to disk required Advance Security Option (ASO) to provide the key infrastructure.

Oracle Secure Backup

Integrated Tape Backup Management

- Protects entire environment
 - Oracle Database 11g, Oracle Database 10g, Oracle9i
 - Application files (OSB 10.2)
- Built-in Oracle advantage
 - Single-vendor advantage
- Fastest backup for Oracle
 - 25-40% faster than competition
- Express version
 - OSB express protects one server to one attached tape drive
 - No encryption
 - Bundled with Oracle Database



Data Security: Oracle Products

Authentication

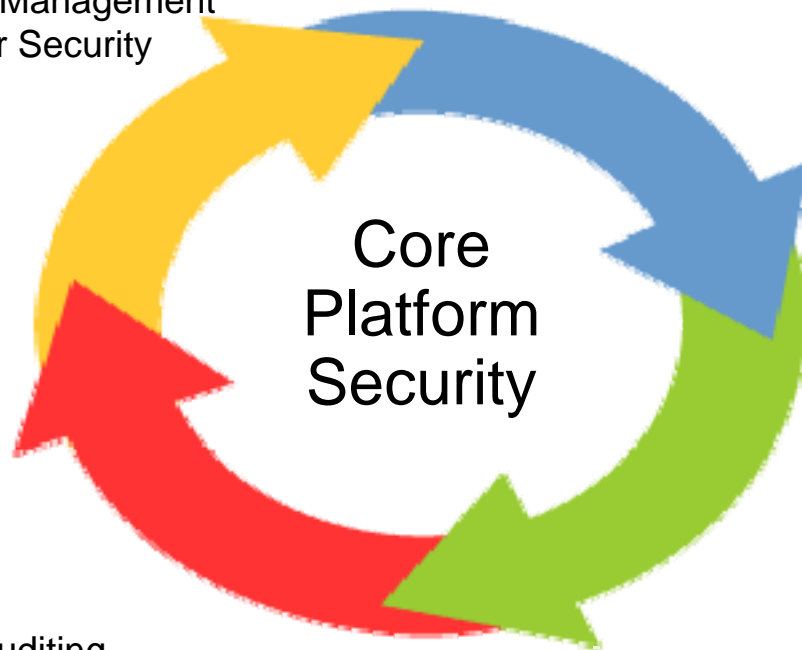
User Management

- Basic Database Authentication
- Oracle Identity Management
- Enterprise User Security

Authorization

Access Control

- Oracle Database Vault
- Virtual Private Database
- Oracle Label Security



Core
Platform
Security

Data Protection Encryption

- Oracle Advanced Security
 - DBMS_CRYPTO
 - TDE
 - RMAN Encrypted Backups
- Oracle Secure Backup
- **EM Data Masking**

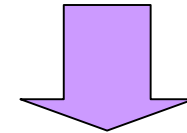
Monitoring Auditing

- Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Need for Data Masking

- Key Drivers
 - Privacy and compliance
 - HIPAA, Breach Notification Laws
 - EU Data Privacy Directive
 - Application testing
 - Offshore application development
 - Offshore / In-house software QA
- Key Requirements
 - Support database and application referential integrity
 - Minimal performance impact
 - Protect against reverse transformation

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000
D'SOUZA	989-22-2403	80,000
FIORANO	093-44-3823	45,000

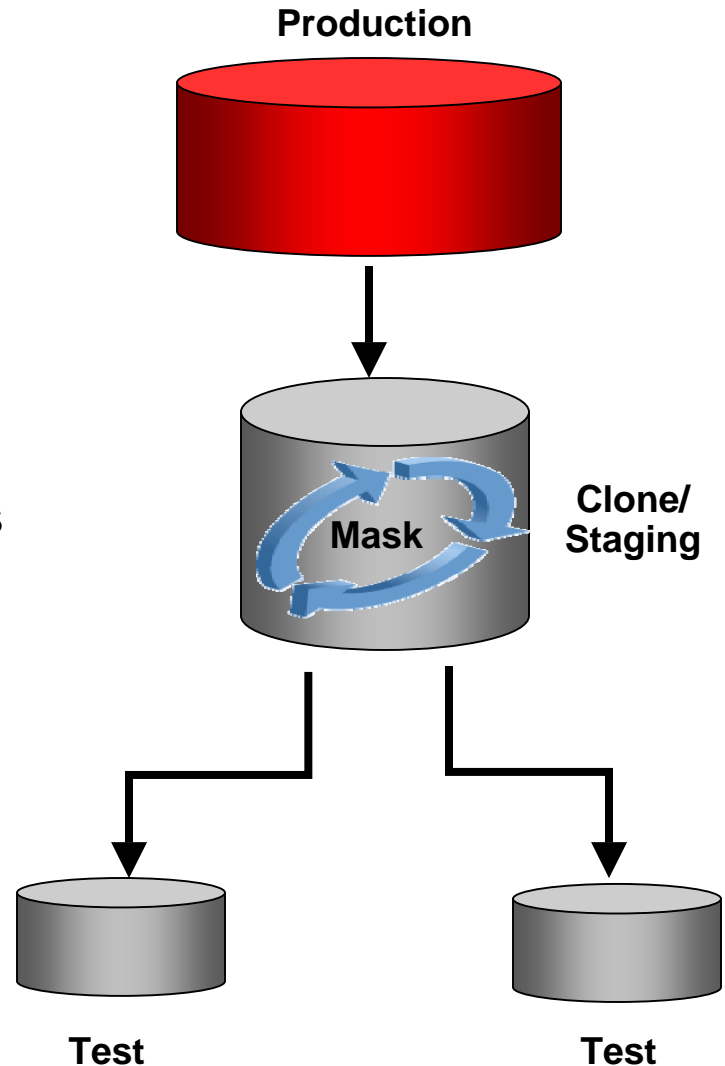


LAST_NAME	SSN	SALARY
ANSKEKSL	111-23-1111	40,000
BKJHHEIEDK	111-34-1345	60,000
KDDEHLHESA	111-97-2749	80,000
FPENZXIEK	111-49-3849	45,000

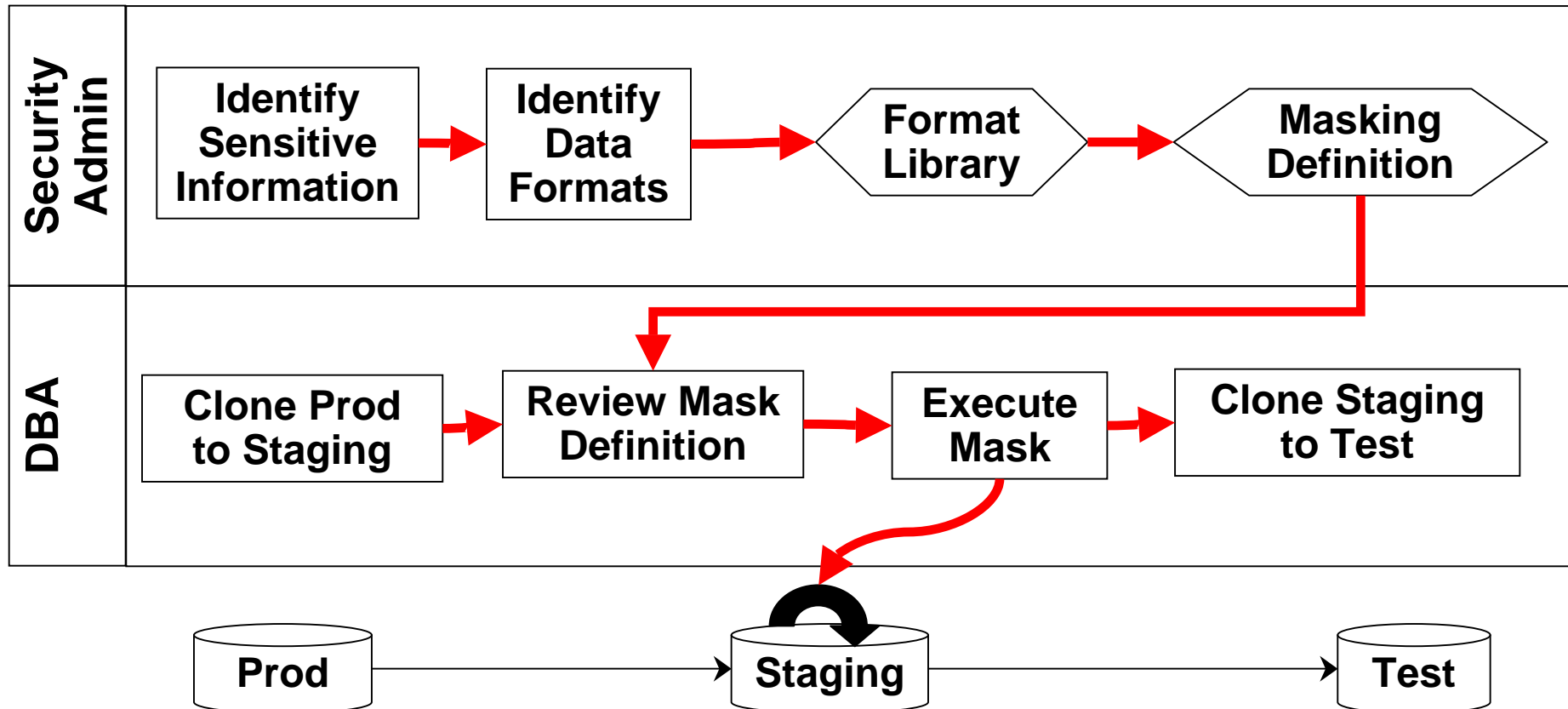
Data Masking Pack

Oracle Enterprise Manager

- Automates production data masking
 - Mask data from a production database
 - Define rules once
- Data relationship discovery
 - Automates data relationship enforcement using existing foreign keys
 - Enter custom data relationships known to the application
- Rules repository
 - Format library, masking definitions
- Testing
 - View sample data before masking



Masking Workflow





Summary

9

Oracle Database Security

Continuous Innovation



Oracle Database 11g

EM Data Masking

TDE Tablespace Encryption

Oracle Audit Vault

Oracle Database Vault

Secure Backup (Tape)

TDE Column Encryption

Oracle Database 10g

VPD Column Masking

VPD Column Relevant

EM Secure Config Scanning

Client Identity Propagation

Oracle Database 9i

Fine Grained Auditing

Oracle Label Security

Oracle8i

Proxy authentication

Enterprise User Security

Virtual Private Database (VPD)

Database Encryption API

Strong Authentication

Oracle7

Native Network Encryption

Database Auditing

Government customer

Data Security: Oracle Products

Authentication

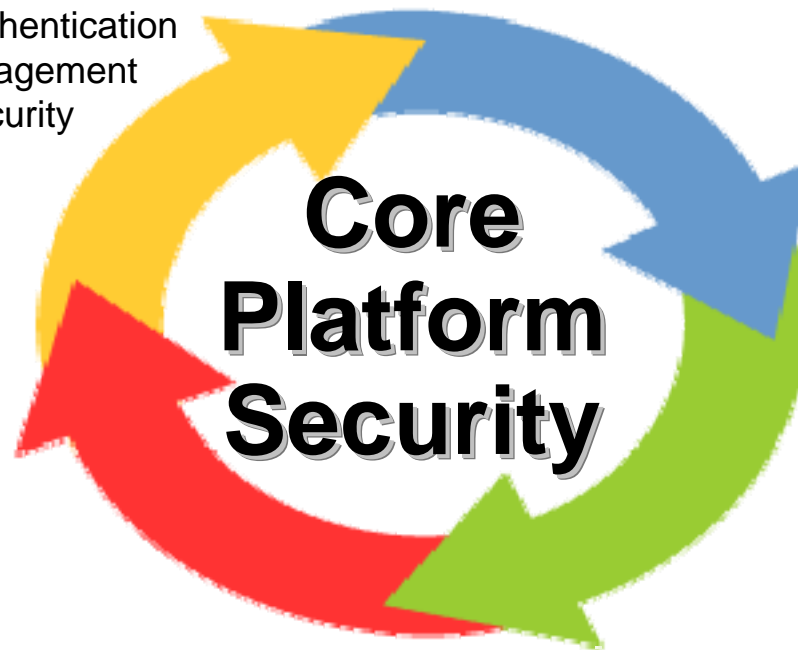
User Management

- Basic Database Authentication
- Oracle Identity Management
- Enterprise User Security

Authorization

Access Control

- Oracle Database Vault
- Virtual Private Database
- Oracle Label Security



Data Protection

Encryption

- Oracle Advanced Security
 - DBMS_CRYPT
 - TDE
 - RMAN Encrypted Backups
- Oracle Secure Backup
- EM Data Masking

Monitoring

Auditing

- Database Auditing
- Oracle Audit Vault
- EM Configuration Pack

Oracle Database Security in a Nutshell

- Auditing
 - Auditing Database Users, Privileges, and Objects
 - Auditing DML Statements (FGA)
 - Audit Vault
- Authentication
 - Using Basic User Authentication
 - Using Strong Authentication
 - Using Enterprise User Security
 - Using Proxy Authentication

Oracle Database Security in a Nutshell

- Authorization and Access Control
 - Using Privileges and Roles
 - Implementing Database Vault
 - Implementing Fine-Grained Access Control (VPD)
 - Implementing Oracle Label Security

Oracle Database Security in a Nutshell

- Encryption
 - Concepts
 - Applying Column Encryption
 - Using Application-Based Encryption
 - Using Transparent Data Encryption (TDE)
 - Applying File Encryption
 - RMAN Encrypted Backups
 - Oracle Secure Backup

Learn More



Technology Overview

- Visit: oracle.com/database/security
 - View Whitepapers and webinars



Technical Information, Demos, Software

- Visit OTN: otn.oracle.com -> products -> database -> security and compliance
 - PCI matrix, Maximum Security Architecture
 - Step by step examples for Database Vault, Transparent Data Encryption and more

ORACLE®



Thanks For Coming !!

Daniel Liu Contact Information

Phone: (714) 376-8416

Email: daniel.liu@oracle.com

Email: daniel_t_liu@yahoo.com

Company Web Site:

<http://www.oracle.com>