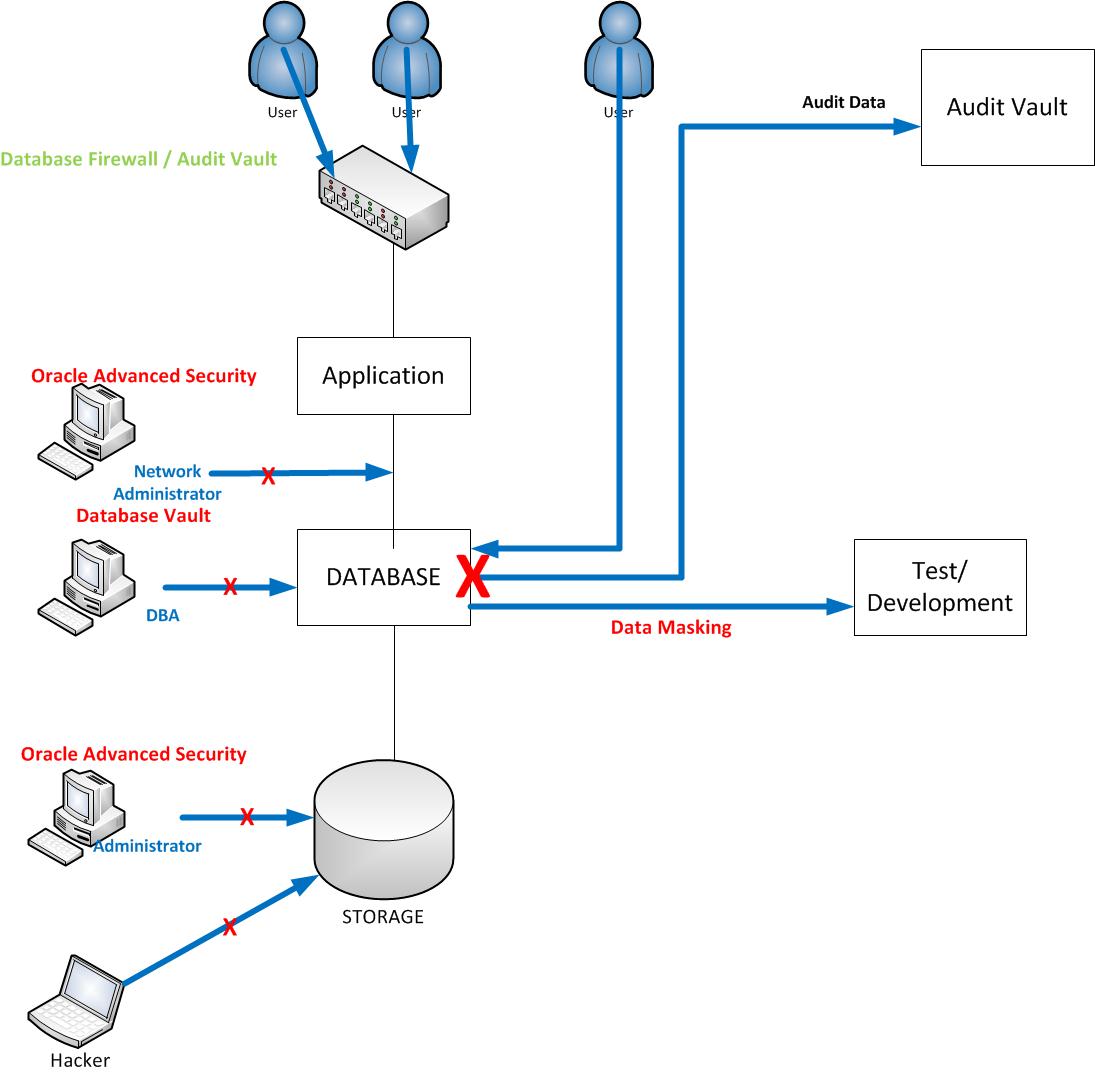
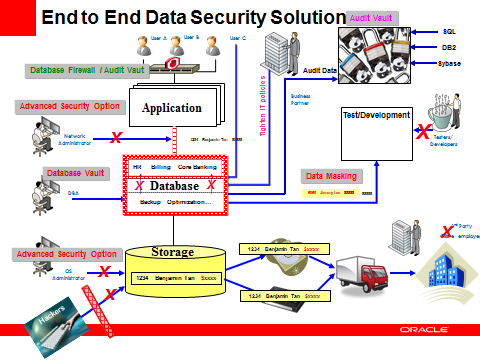
**Oracle Security Outline**

Mô hình về Oracle Security





1. Phương hướng nghiên cứu chung:

* Các yêu cầu liên quan: hệ thống, phần mềm, các bản vá,…
* Thông tin về license cho software or tool.
* Công dụng của software or tool.
* Cách thức cài đặt, cấu hình.
* Cách thức quản trị.
* Demo nếu có.

1. Các phần nghiên cứu
2. Database

* Các tính năng sẵn có sau khi cài đặt DB:

+ user accounts

+ authentication methods

+ privileges and roles

+ application security

+ user session information using application context

+ database access on the row and colum level using Virtual Private DB

+ encryption

+ auditing database activities.

Trong các phần này nói về công dụng của từng tính năng ở mức cơ bản, đi sâu nói về một số tính năng như: user accounts, authentication methods, privileges and roles, auditing database activities.

* Các tính năng cần phải cài đặt thêm và liên quan đến license: database vault
* Tool liên quan: data masking, audit vault ( có thể sẽ có demo )

1. Storage

* Tìm hiểu về Oracle Advanced Security theo phương hướng chung.

1. Netwrok

* Tìm hiểu về Database firewall theo phương hướng chung.

1. Tool quản lý chung:

* Oracle audit vault
* Oracle Enterprise Manager

1. Công việc phải làm
2. Database

* Nói qua về license khi cài đặt Oracle Database ( RDBMS).

Khái niệm về security, khung tổng thể, ứng dụng.

1. DB ( 12c)

+ quản lý người dùng (User )

default (predefined) user accounts

Basic DB security

Basic User Authentication

Strong Authentication

Proxy Authentication

Privileges and Roles

+ quản lý truy cập dữ liệu ( access control)

App context

Virtual Private DB

Manually Encrytion data

+ kết nối dữ liệu qua network

Oracle Net Services

Securing the Listener

+ aduit

Auditing DB users, privileges, objects

Auditing DML statements

1. Software security and solution

2.1. Oracle Secure Backup

2.2. Oracle Advanced Security

2.3. Oracle DB vault

2.4. Oracle Label Security

2.5. Oracle Data Masking

2.6. Oracle Audit Vault and DB Firewall

1. Tool quản lý chung:
   1. Oracle EM
2. **Introduction to Database Security**
   1. Fundamental Data Security Requirements
   2. Data Security Concerns
   3. Compliance Mandates
   4. Security Risks
   5. Developing Your Security Policy
   6. Defining a Security Policy
   7. Implementing a Security Policy
   8. Techniques to Enforce Security
3. **Choosing Security Solutions**
   1. Maintaining Data Integrity
   2. Protecting Data
   3. Controlling Data Access
   4. Oracle Database Vault Overview
   5. Oracle Audit Vault Overview
   6. Combining Optional Security Features
   7. Compliance Scanner
   8. Enterprise Manager Database Control: Policy Trend
4. **Basic Database Security**
   1. Database Security Checklist
   2. Applying Security Patches
   3. Default Security Settings
   4. Secure Password Support
   5. Enforcing Password Management
   6. Protecting the Data Dictionary
   7. System and Object Privileges
5. **Auditing Database Users, Privileges, and Objects**
   1. Monitoring for Suspicious Activity
   2. Standard Database Auditing
   3. Setting the AUDIT\_TRAIL
   4. Specifying Audit Options
   5. Viewing Auditing Options
   6. Auditing the SYSDBA Users
   7. Audit to XML Files
   8. Value-Based Auditing
6. **Auditing DML Statements**
   1. Fine-Grained Auditing (FGA)
   2. Using the DBMS\_FGA Package
   3. FGA Policy
   4. Triggering Audit Events
   5. Data Dictionary Views
   6. DBA\_FGA\_AUDIT\_TRAIL
   7. Enabling and Disabling an FGA Policy
   8. Maintaining the Audit Trail
7. **Using Basic User Authentication**
   1. User Authentication
   2. Protecting Passwords
   3. Creating Fixed Database Links
   4. Encrypting Database Link Passwords
   5. Using Database Links without Credentials
   6. Using Database Links and Changing Passwords
   7. Auditing with Database Links
   8. Restricting a Database Link with Views
8. **Using Strong Authentication**
   1. Strong Authentication
   2. Single Sign-On
   3. Public Key Infrastructure (PKI) Tools
   4. Configuring SSL on the Server
   5. Certificates
   6. Using the orapki Utility
   7. Using Kerberos for Authentication
   8. Configuring the Wallet
9. **Using Enterprise User Security**
   1. Enterprise User Security
   2. Oracle Identity Management Infrastructure: Default Deployment
   3. Oracle Database: Enterprise User security Architecture
   4. Installing Oracle Application Server Infrastructure
   5. Managing Enterprise User Security
   6. Creating a Schema Mapping Object in the Directory
   7. Creating a Schema Mapping Object in the Directory
10. **Using Proxy Authentication**
    1. Security Challenges of Three-Tier Computing
    2. Common Implementations of Authentication
    3. Restricting the Privileges of the Middle Tier
    4. Authenticating Database and Enterprise Users
    5. Using Proxy authentication for Database Users
    6. Proxy Access Through SQL\*Plus
    7. Revoking Proxy Authentication
    8. Data Dictionary Views for Proxy Authentication
11. **Using Privileges and Roles** 
    1. Authorization
    2. Privileges
    3. Benefits of Roles
    4. CONNECT Role Privileges
    5. Using Proxy Authentication with Roles
    6. Creating an Enterprise Role
    7. Securing Objects with Procedures
    8. Securing the Application Roles
12. **Access Control**
    1. Description of Application Context
    2. Using the Application Context
    3. Setting the Application Context
    4. Application Context Data Sources
    5. Using the SYS\_CONTEXT PL/SQL Function
    6. PL/SQL Packages and Procedures
    7. Implementing the Application Context Accessed Globally
    8. Data Dictionary Views
13. **Implementing Virtual Private Database** 
    1. Understanding Fine-Grained Access Control
    2. Virtual Private Database (VPD)
    3. How Fine-Grained Access Control Works
    4. Using DBMS\_RLS
    5. Exceptions to Fine-Grained Access Control Policies
    6. Implementing a VPD Policy
    7. Implementing Policy Groups
    8. VPD Best Practices
14. **Oracle Label Security Concepts** 
    1. Access Control: Overview
    2. Discretionary Access Control
    3. Oracle Label Security
    4. How Sensitivity Labels are Used
    5. Installing Oracle Label Security
    6. Comparing Oracle Label Security and VPD
    7. Analyzing Application Needs
15. **Implementing Oracle Label Security** 
    1. Implementing the Oracle Label Security Policy
    2. Creating Policies
    3. Defining Labels Overview
    4. Defining Compartments
    5. Identifying Data Labels
    6. Access Mediation
    7. Adding Labels to Data
    8. Assigning User Authorization Labels
16. **Using the Data Masking Pack** 
    1. Understanding Data Masking
    2. Data Masking Pack Features
    3. Identifying Sensitive Data for Masking
    4. Types of Built-in Masking Primitives and Routines
    5. Data Masking of the EMPLOYEES Table
    6. Implementing a Post-Processing Function
    7. Viewing the Data Masking Impact Report
    8. Creating an Application Masking Template by Exporting Data Masking Definitions
17. **Encryption Concepts** 
    1. Understanding Encryption
    2. Problems that Encryption Solves
    3. Encryption is not Access Control
    4. What to Encrypt
    5. Data Encryption Challenges
    6. Storing the Key in the Database
    7. Letting the User Manage the Key
    8. Storing the Key in the Operating System
18. **Using Application-Based Encryption** 
    1. DBMS\_CRYPTO Package Overview
    2. Using the DBMS\_CRYPTO Package
    3. Generating Keys Using RANDOMBYTES
    4. Using ENCRYPT and DECRYPT
    5. Enhanced Security Using the Cipher Block Modes
    6. Hash and Message Authentication Code
19. **Applying Transparent Data Encryption** 
    1. Transparent Data Encryption (TDE)
    2. Creating the Master Key
    3. Opening the Wallet
    4. Using Auto Login Wallet
    5. Resetting (Rekeying) the Unified Master Encryption Key \*\* 11.2 \*\*
    6. Using Hardware Security Modules
    7. TDE Column Encryption Support
    8. Creating an Encrypted Tablespace
20. **RMAN Encrypted Backups**
    1. Oracle Secure Backup Encryption
    2. Creating RMAN Encrypted Backups
    3. Using Password Mode Encryption
    4. Restoring Encrypted Backups
    5. Data Pump Encryption
    6. Using Dual Mode Encryption
    7. Encrypting Dump Files
21. **Oracle Net Services: Security Checklists** 
    1. Overview of Security Checklists
    2. Securing the Client Computer
    3. Configuring the Browser
    4. Network Security Checklist
    5. Using a Firewall to Restrict Network Access
    6. Restricting Network IP Addresses: Guidelines
    7. Configuring IP Restrictions with Oracle Net Manager
    8. Configuring Network Encryption
22. **Securing the Listener**
    1. Listener Security Checklist
    2. Restricting the Privileges of the Listener
    3. Moving the Listener to a Nondefault Port
    4. Preventing Online Administration of the Listener
    5. Using the INBOUND\_CONNECT\_TIMEOUT Parameter
    6. Analyzing Listener Log Files
    7. Administering the Listener Using TCP/IP with SSL
    8. Setting Listener Logging Parameters