



ORACLE®

End to End Security – White board

Niel Pandya

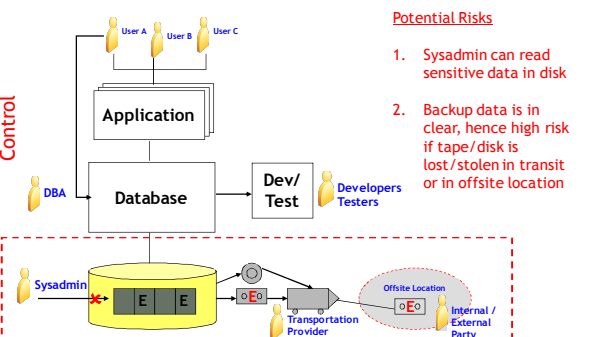
Agenda

- Oracle Database Security Options Mappings
- Oracle Identity Management (IdM/OIM)

ORACLE

2

Oracle Database Security Vulnerabilities



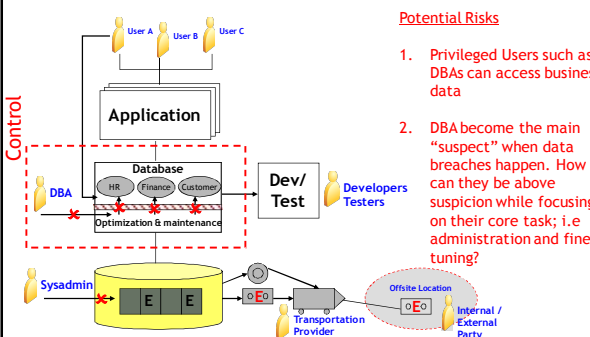
Potential Risks

1. Sysadmin can read sensitive data in disk
2. Backup data is in clear, hence high risk if tape/disk is lost/stolen in transit or in offsite location

ORACLE

3

Oracle Database Security Vulnerabilities



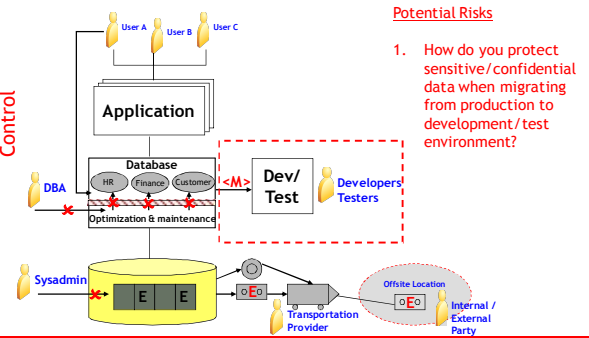
Potential Risks

1. Privileged Users such as DBAs can access business data
2. DBA become the main "suspect" when data breaches happen. How can they be above suspicion while focusing on their core task; i.e administration and fine-tuning?

ORACLE

4

Oracle Database Security Vulnerabilities



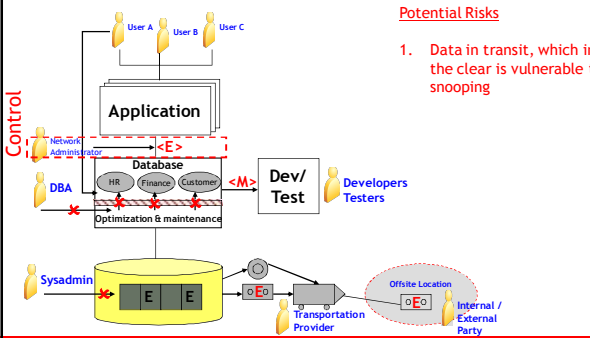
Potential Risks

1. How do you protect sensitive/confidential data when migrating from production to development/test environment?

ORACLE

5

Oracle Database Security Vulnerabilities

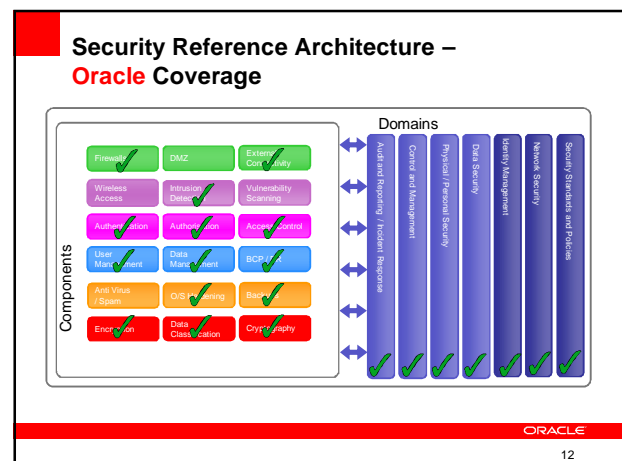
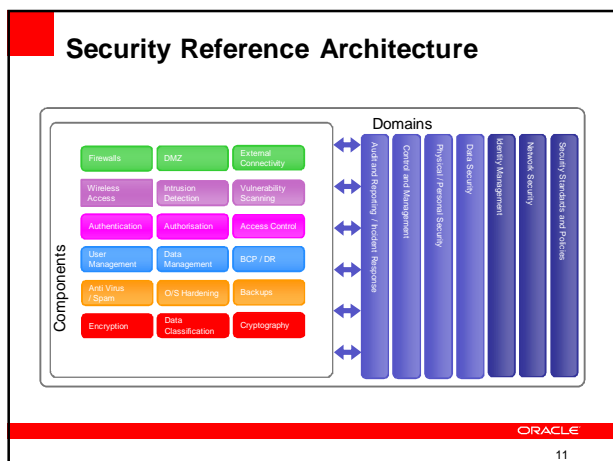
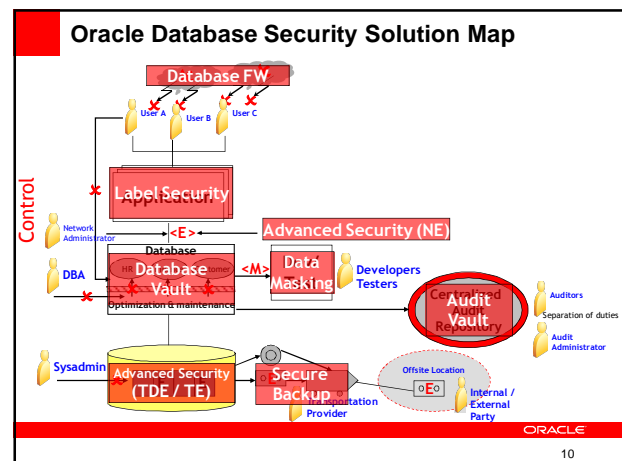
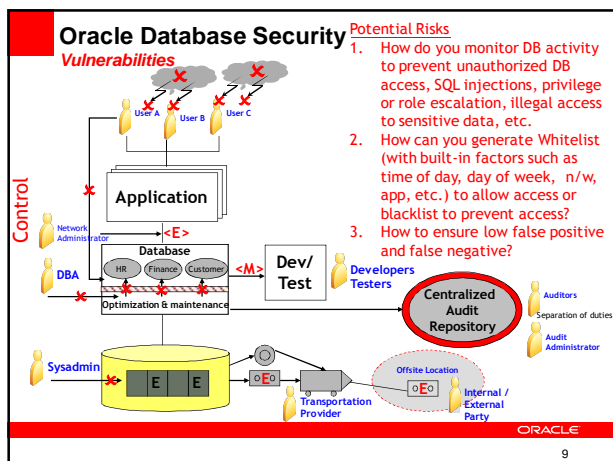
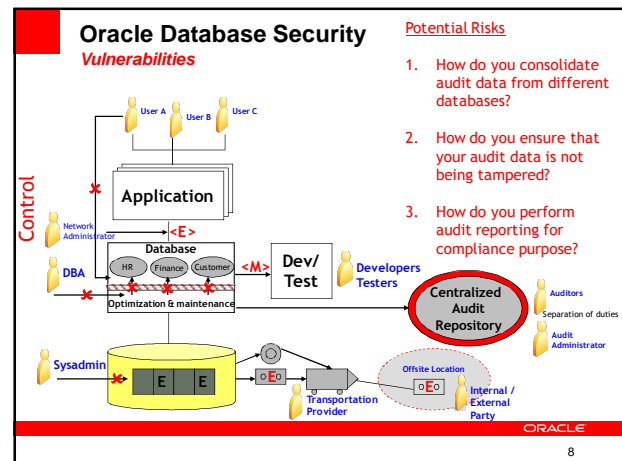
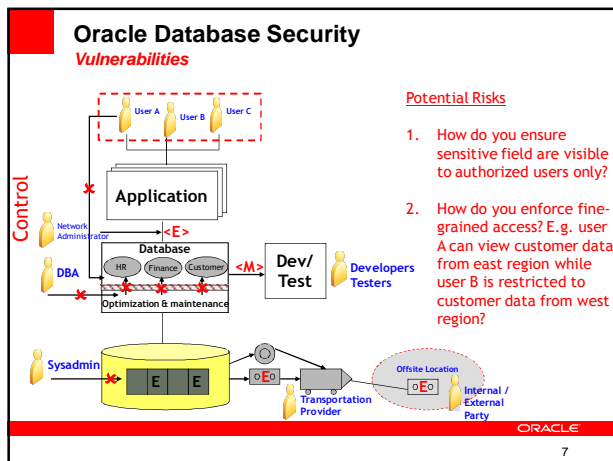


Potential Risks

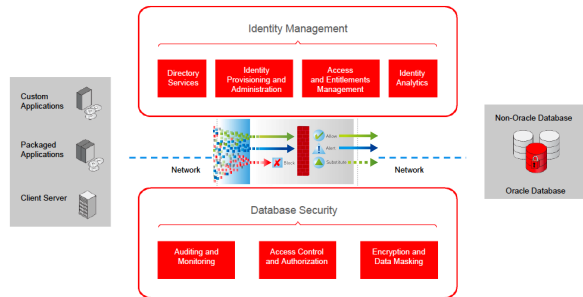
1. Data in transit, which is in the clear is vulnerable to snooping

ORACLE

6



Oracle Security Strategy

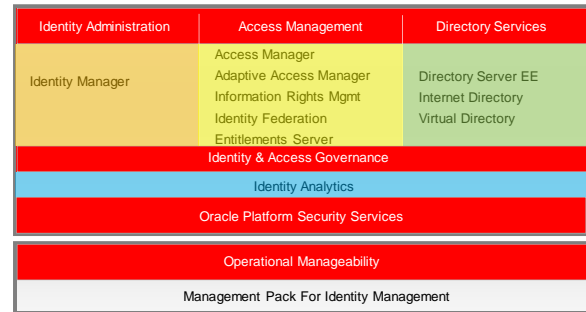


ORACLE

13

13

Oracle Identity Management



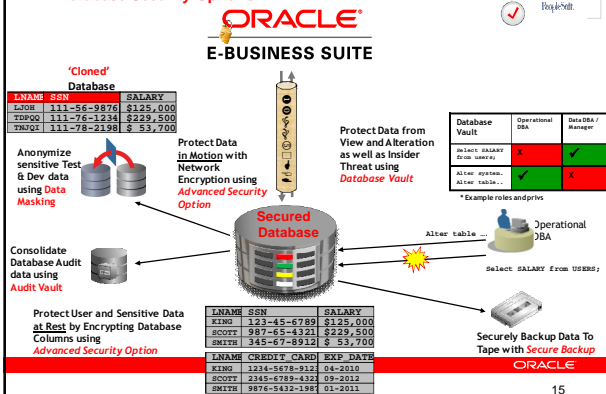
ORACLE

Oracle Confidential – For Internal Use Only

14

Example: Secured Database Access

Database Security Options



15

Question & Answer



ORACLE

16

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.