



ORACLE®

**SECURITY**  
**INSID=OUT**

Complete Protection for Your Database,  
Middleware, and Applications

ORACLE®

**Hardening your Database to protect your Data**

Luc Wijns  
Antonio Mata Gomez



ORACLE

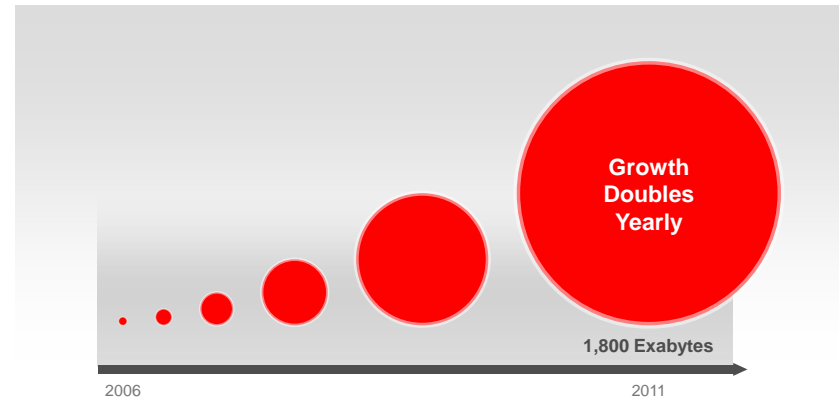


The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

ORACLE



## More data than ever...

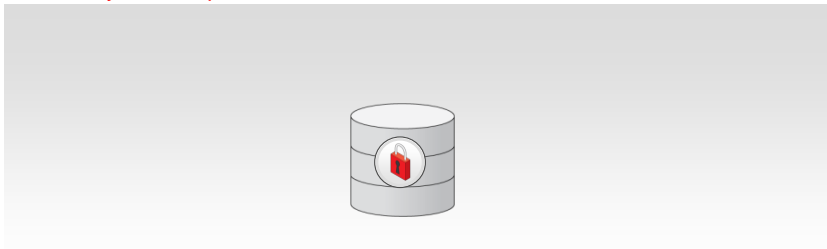


Source: IDC, 2008

ORACLE

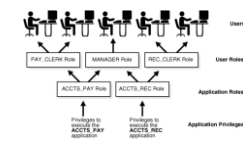
# Is your Data @ Risk ?

Layers of Exposures



# Oracle DB Security Model

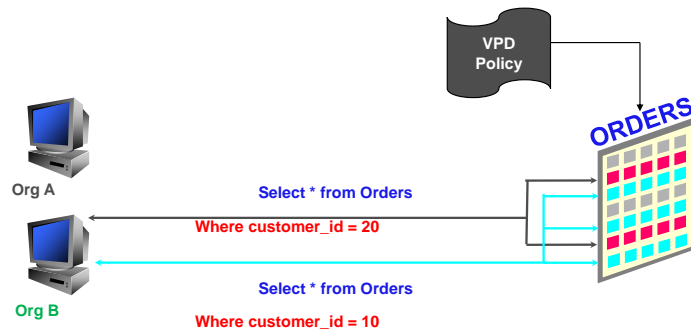
- Privileges
- Roles
  - Contextual/Application Roles
- Password Policies
- Strong Authentication
- Profiles
- LDAP enabled
- Multi Tenancy ?
  - Virtual Private Database
  - Label Security



## Virtual Private Database

Fine Grained Access Control

- Database enforced
- Programmable Row Level Security



ORACLE

## Oracle Label Security

Data Classification for Fine Grained Access Control



- Classify users and data based on business drivers
- Database enforced row level access control
- Users classification through Oracle Identity Management Suite
- Classification labels can be factors in other policies

ORACLE

## Oracle Label Security



Sensitive : ACME

Application Table

Store ID	Revenue	Department	Sensitivity Label	
AX703	10200.34	Finance	Sensitive : ACME	OK
B789C	18020.34	Engineering	Sensitive : WIDGET	X
JFS845	15045.23	Legal	Highly Sensitive: ACME	X
SF78SD	21004.45	HR	Unclassified: ACME	OK

ORACLE

## Is your Data @ Risk ?

Layers of Exposures



ORACLE

## Managing Power Users

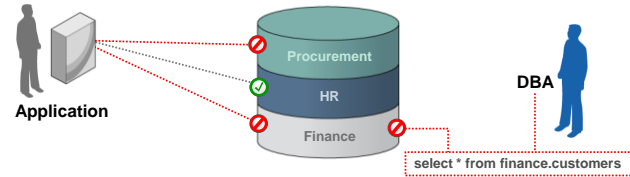
How to scale ?



- Database Power Users
  - Sys
  - System
  - Sysdba
- OS Power Users
  - Root
  - Administrator
  - Oracle binaries owner

## Oracle Database Vault

Separation of Duties & Privileged User Controls

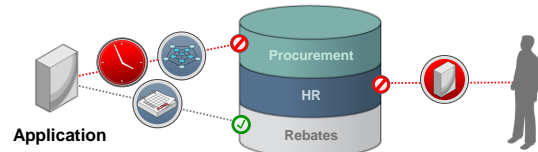


- DBA separation of duties
- Limit powers of privileged users
- Securely consolidate application data
- No application changes required



## Oracle Database Vault

### Realms



- Protect application data and prevent application by-pass
- Enforce who, where, when, and how using rules and factors
- Out-of-the box policies for Oracle applications, customizable

ORACLE

14

## Oracle Database Vault

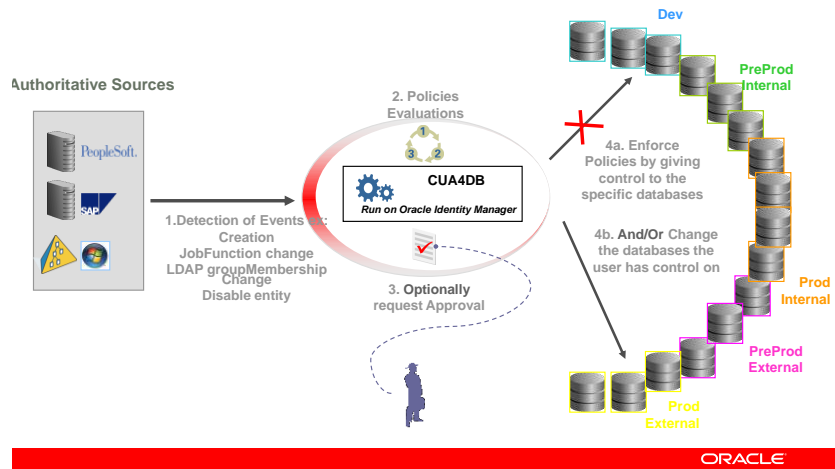
### Command Rules

- Alter table
- Alter trigger
- Alter package
- Alter tablespace
- Connect / login
- Create table
- Create index
- Create view
- **Drop table**
- **Drop user**
- **Drop index**
- **Truncate table**
- ....
- ....
- ....

ORACLE

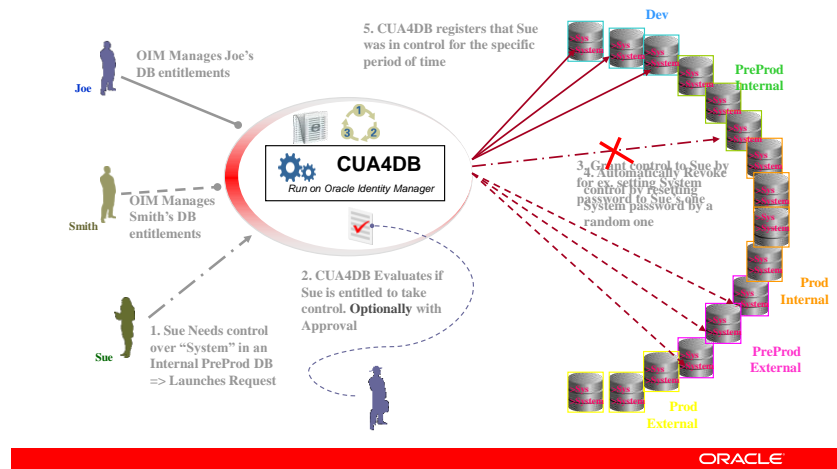
## Managing Database Accounts

Staying in control ...



## Managing Database Accounts

About Accountability ...



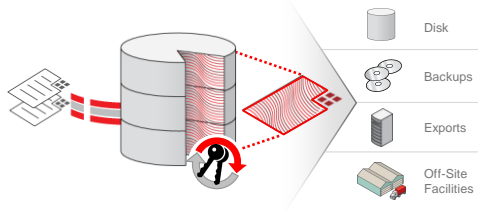
# Is your Data @ Risk ?

Layers of Exposures



# Oracle Advanced Security

Transparent Data Encryption



- Complete encryption for data at rest
- No application changes required
- Efficient encryption of all application data
- Built-in key lifecycle management



## Oracle Advanced Security

### TDE column encryption



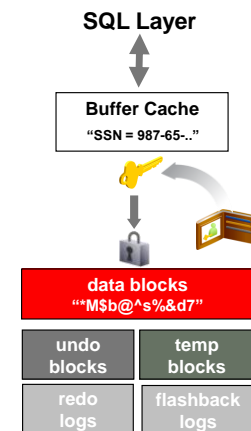
- Key management
  - One key per table
  - Table keys are encrypted using the TDE master encryption key – 2 tier key architecture
- Encrypt column in existing table
  - `SQL> alter table clients modify (cr_card_nbr encrypt)`
- Encrypt column in new table
  - `SQL> create table customers(
 first_name 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
  - 'nomac' option (save 20 bytes per encrypted value)
    - reducing storage to approximately 28 bytes per row

ORACLE

## 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

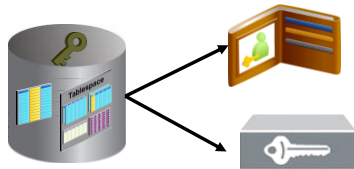


ORACLE

## Oracle Advanced Security

### TDE Key Management

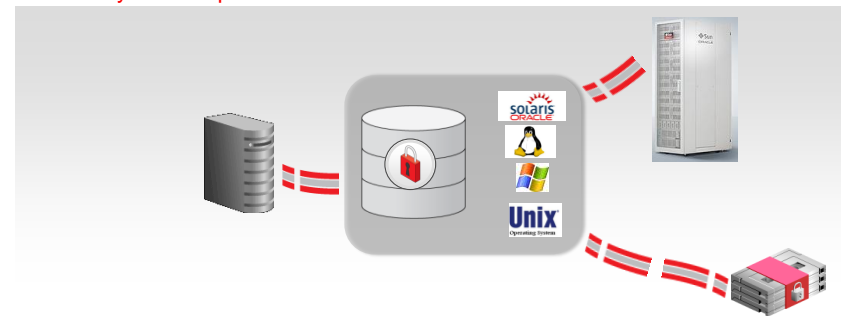
- Generate, store, and rotate encryption keys
- Two tier key architecture
  - Master key protects table keys and tablespace keys
  - Master key is stored in External Security Module:
    - Oracle Wallet (PKCS #12 file)
    - Certified Hardware Security Modules: RSA, Safenet, Thales, Utimaco



ORACLE

## Is your Data @ Risk ?

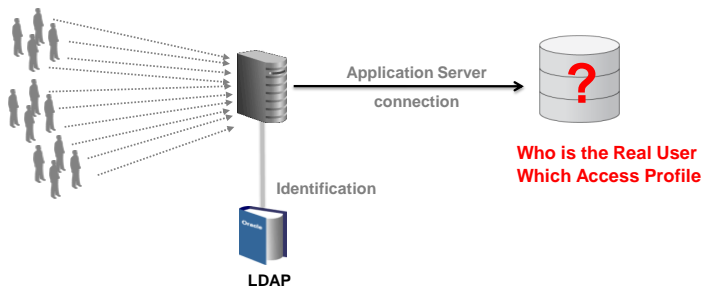
### Layers of Exposures



ORACLE

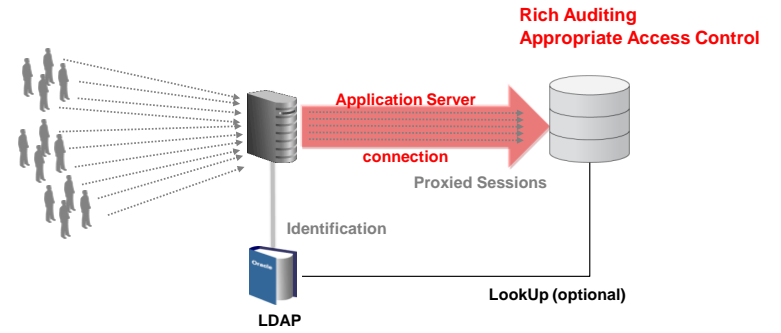
# End to End Security

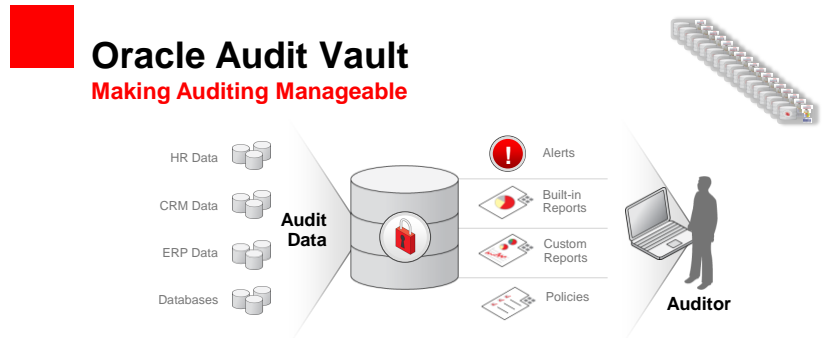
## Proxy Authentication



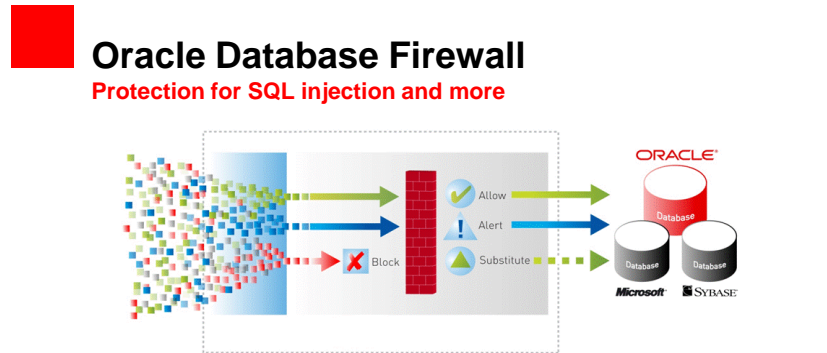
# End to End Security

## Proxy Authentication





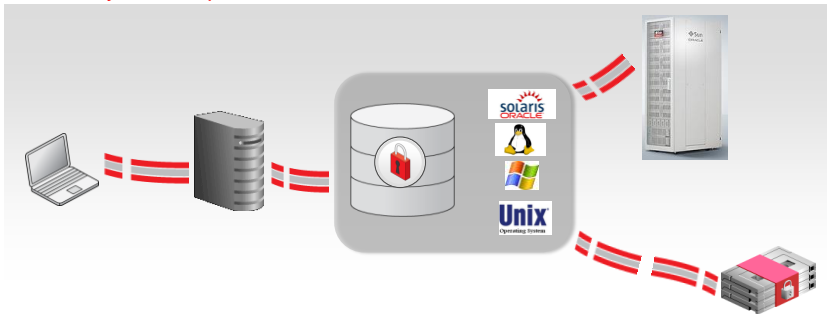
- Consolidate audit data into secure repository
  - Detect and alert on suspicious activities
  - Out-of-the box compliance reporting
  - Centralized audit policy management
- 



- Monitor database activity and block unauthorized database access
- Highly accurate SQL grammar based analysis to enforce normal activity
- Built-in and custom compliance reports for SOX, PCI, and other regulations

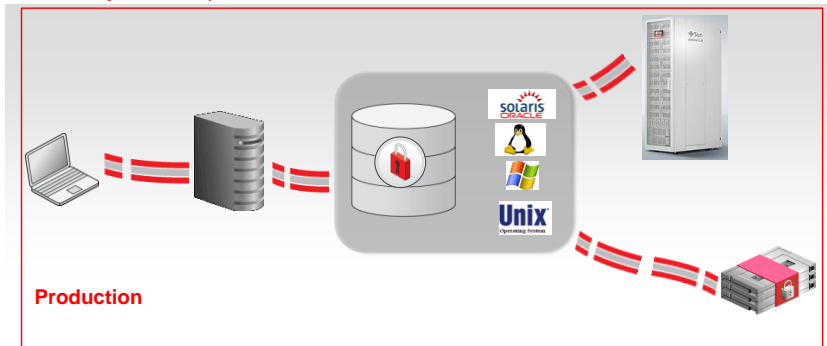
# Is your Data @ Risk ?

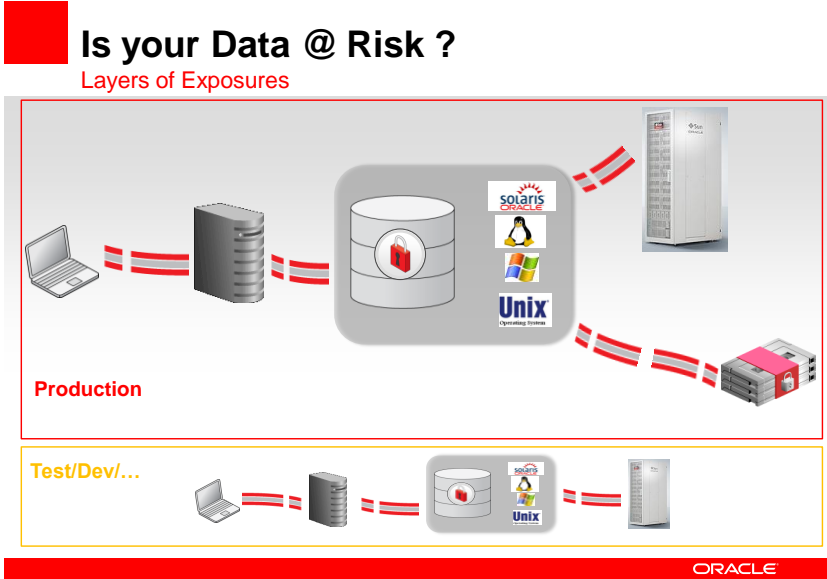
Layers of Exposures



# Is your Data @ Risk ?

Layers of Exposures





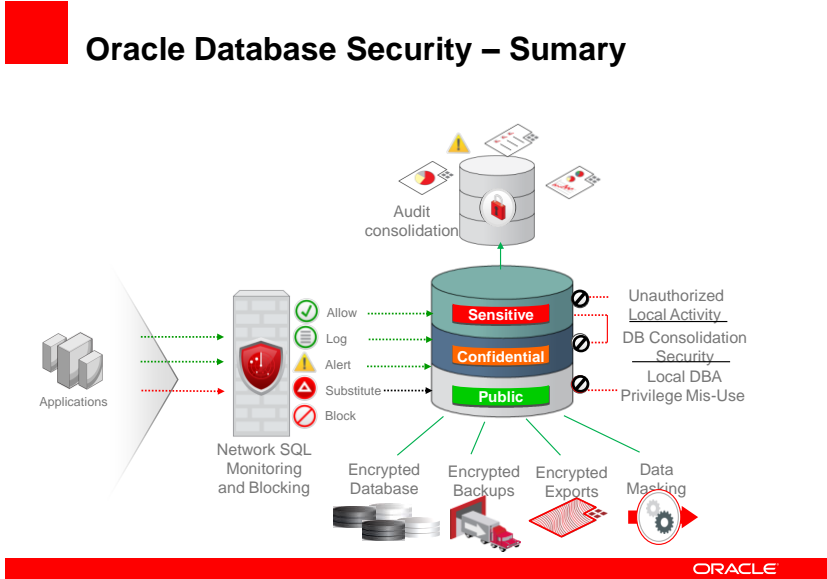
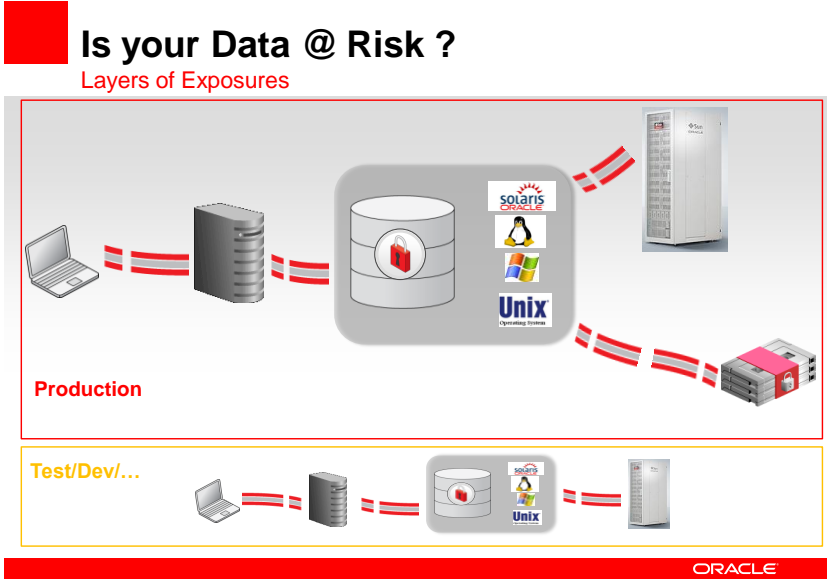
## Oracle Data Masking

Irreversible De-Identification

Production			Non-Production			
LAST_NAME	SSN	SALARY		LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000	→	ANSKERSL	111-23-1111	60,000
BENSON	323-22-2943	60,000	→	BKJHHEIEDK	222-34-1345	40,000

- Remove sensitive data from non-production databases
- Referential integrity preserved so applications continue to work
- Sensitive data never leaves the database
- Extensible template library and policies for automation

ORACLE



 For More Information

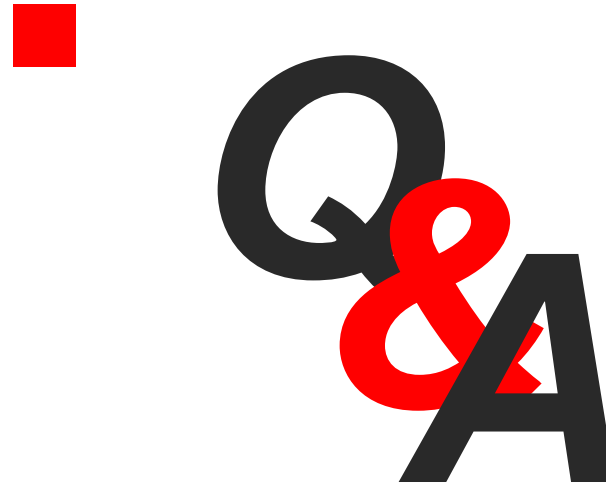


search.oracle.com

Search for:  In the section: All  [Refine Search](#)

or

[oracle.com/database/security](http://oracle.com/database/security)





ORACLE IS THE **INFORMATION** COMPANY