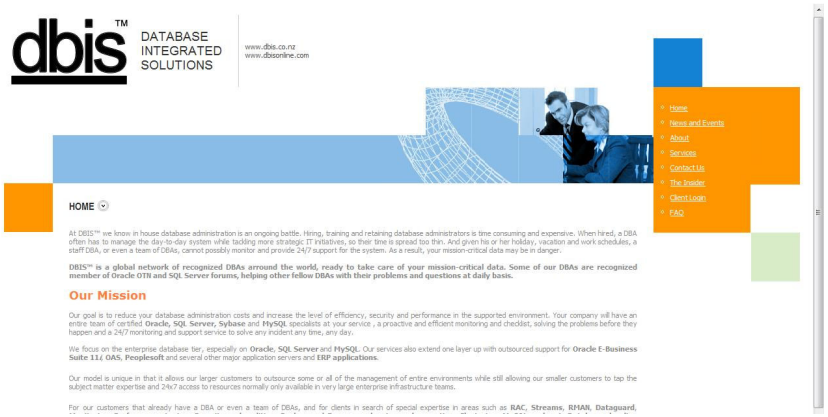
ORACLE SECURITY OPTIONS

PEOUG' 2009

2009 Lima, Peru



By:

Francisco Munoz Alvarez

dbis™ DATABASE INTEGRATED SOLUTIONS

ORACLE SECURITY OPTIONS

(Based on Oracle EMEA Security Workshop)

Francisco Munoz Alvarez

Oracle ACE Director
President CLOUG, LAOUC & NZOUG
8/9/10g/11g OCP, RAC OCE, AS OCA, E-Business OCP, SQL/PLSQL OCA, Oracle 7 OCM
Oracle 7 & 11GR2 Beta Tester
ITIL Certified

Blog: www.oraclenz.com - Email: franciscoa@dbisonline.com – Twitter : fcomunoz
Blog: www.oracleenespanol.com - Comunidad Oracle: www.oraclemania.ning.com

CEO at DBIS ™
Database Integrated Solutions
www.dbisonline.com
www.dbis.co.nz

dbis™ DATABASE INTEGRATED SOLUTIONS

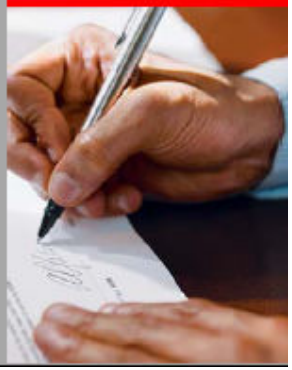
Information Security Has Changed

1996

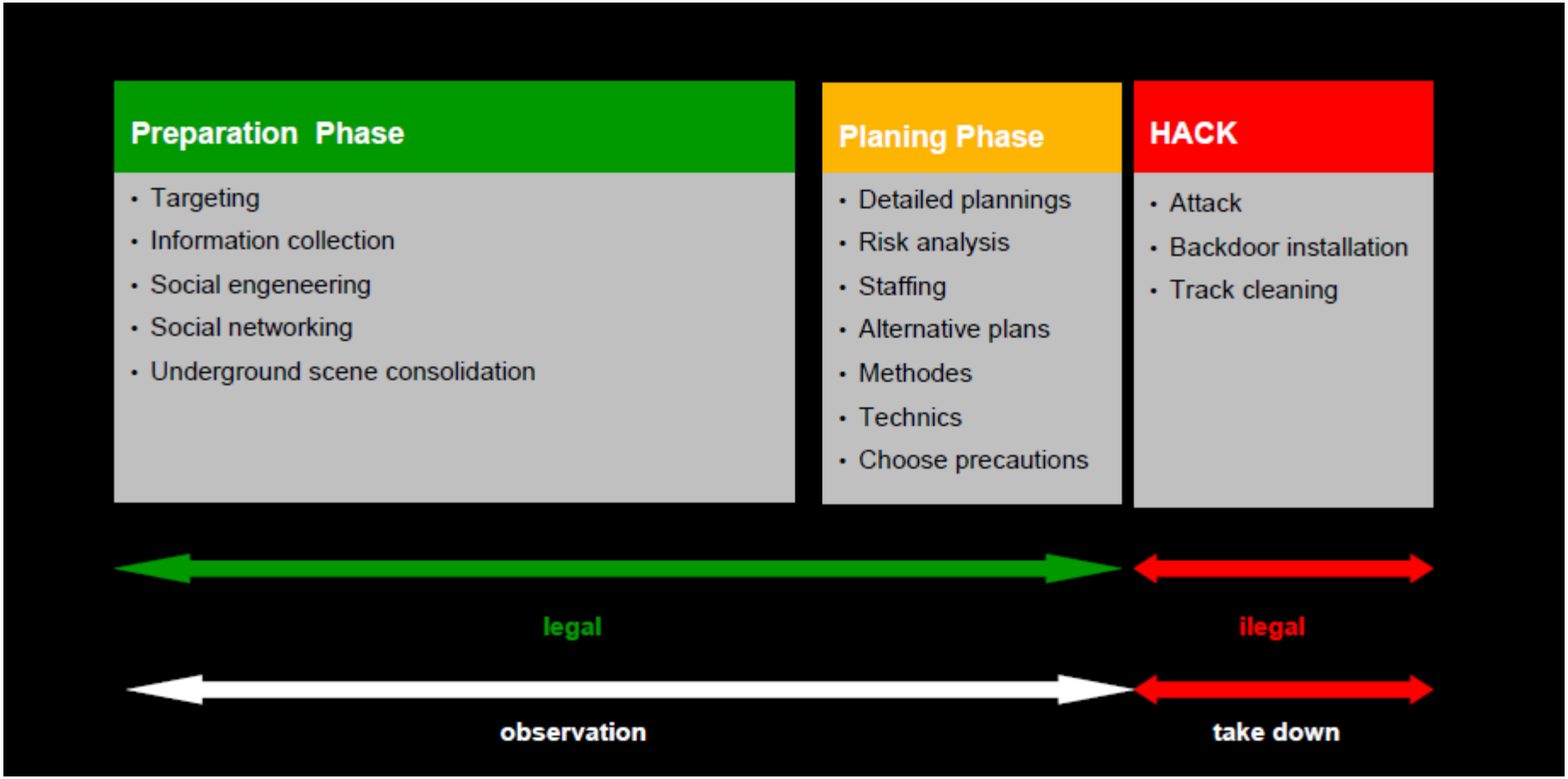
- Hobby Hackers
- Web Site Defacement
- Viruses
- Infrequent Attacks

2009

- **Rentable professional Hackers**
- Criminals
- Denial of Service
- Identity Theft
- Constant Threat

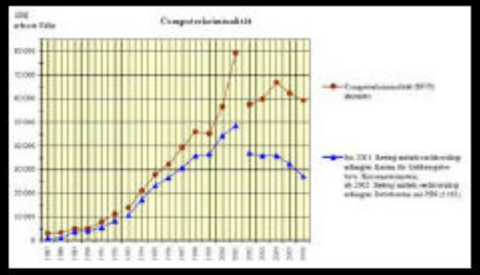


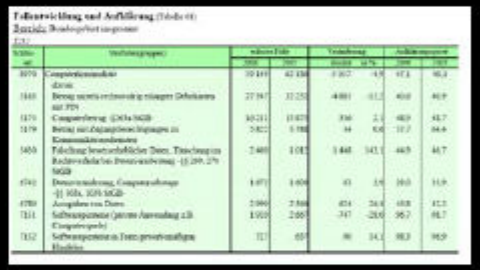
Hacking Steps



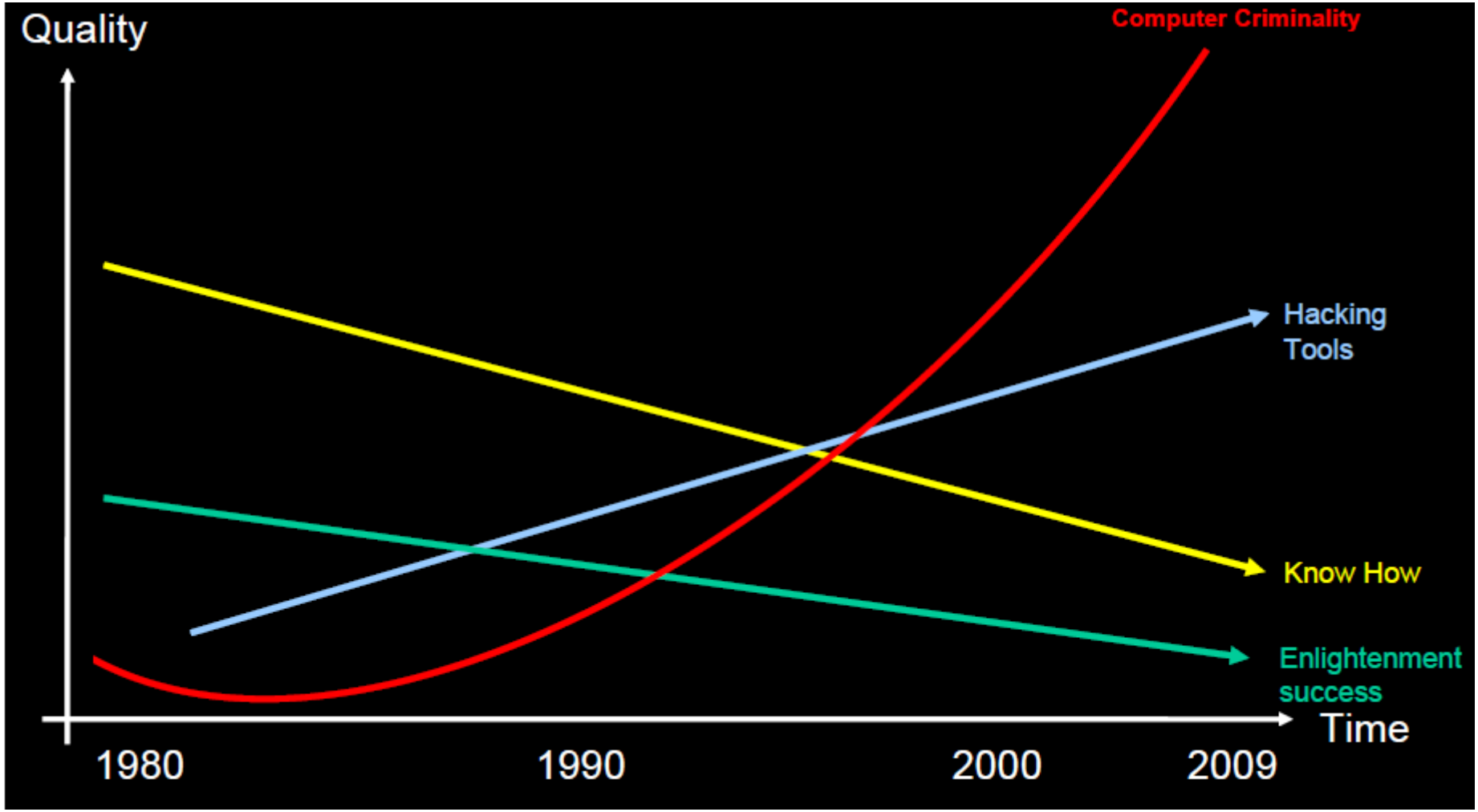
OFFICIAL STATISTICS
from Secret Service Germany

- Dramatical increas of the computer crime since the last 12 years (professionalism)
- Bigest damage by insiders (sabotage, spying, Information selling)
- Typical Hacker is male and over 21; BUT starts with 14 !!!





COMPUTER CRIME DEVELOPMENT



SOME SHORT FACTS

87 % of all Databases are compromised over the operating system

80 % of the damage is caused by insiders

1 % of all professional hacks are only recognized

10 % of all “standard hacks” are made public

HIGH SCORE LIST

Source: Black Hat Convention 2008

40sec Windows XP SP2

55sec Windows Vista

63sec Windows NT4.0 WKST, SP4

70sec Windows 2003 Server

140sec Linux Kernel 2.6.

190sec Sun Solaris 5.9 with rootkit

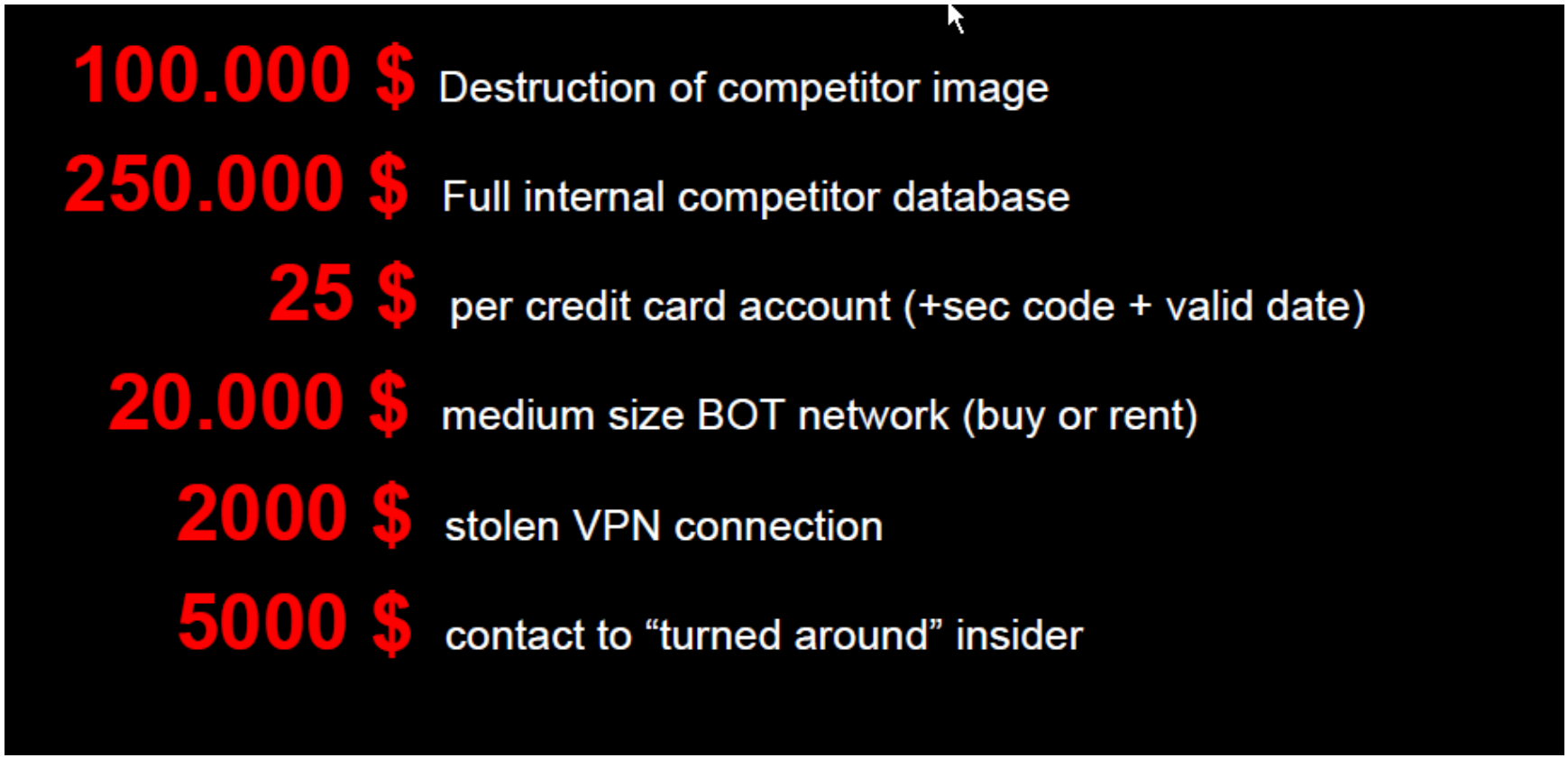
...

List includes also AIX, HPUX, OS2, OSX, IRIX, ...

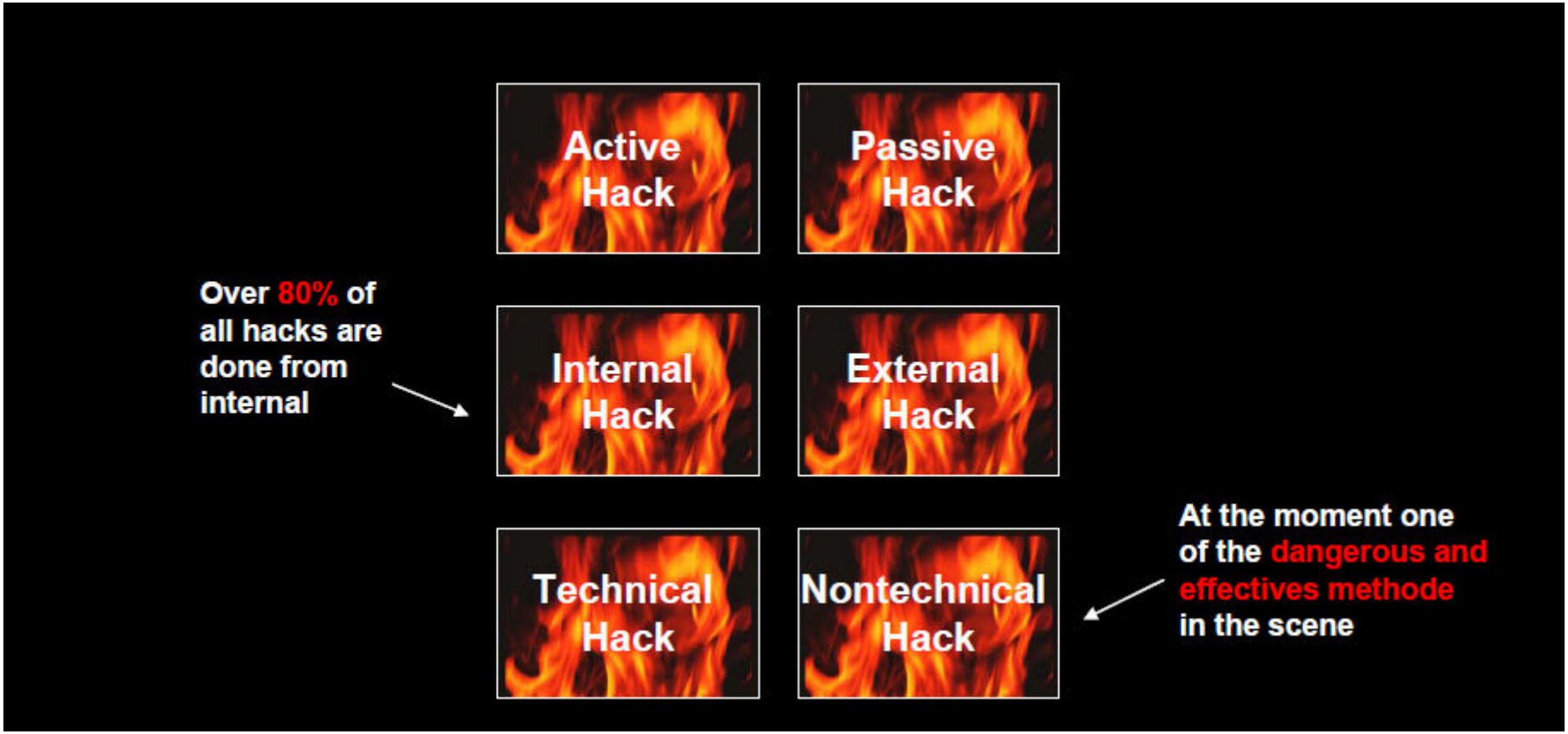
2007/2008 SHOPPING LIST

50.000 $	Windows Vista Exploit (4000$ for WMF Exploit in Dec2005)
7 $	per ebay-Account
20.000 $	medium size BOT network
30.000 $	unknown security holes in well known applications
25-60 $	per 1000 BOT clients / week

CRISIS SHOPPING LIST 2009



HACKING METHODS AND TECHNIQUES



INSIDER ATTACKS EXAMPLES
European Headlines 2008

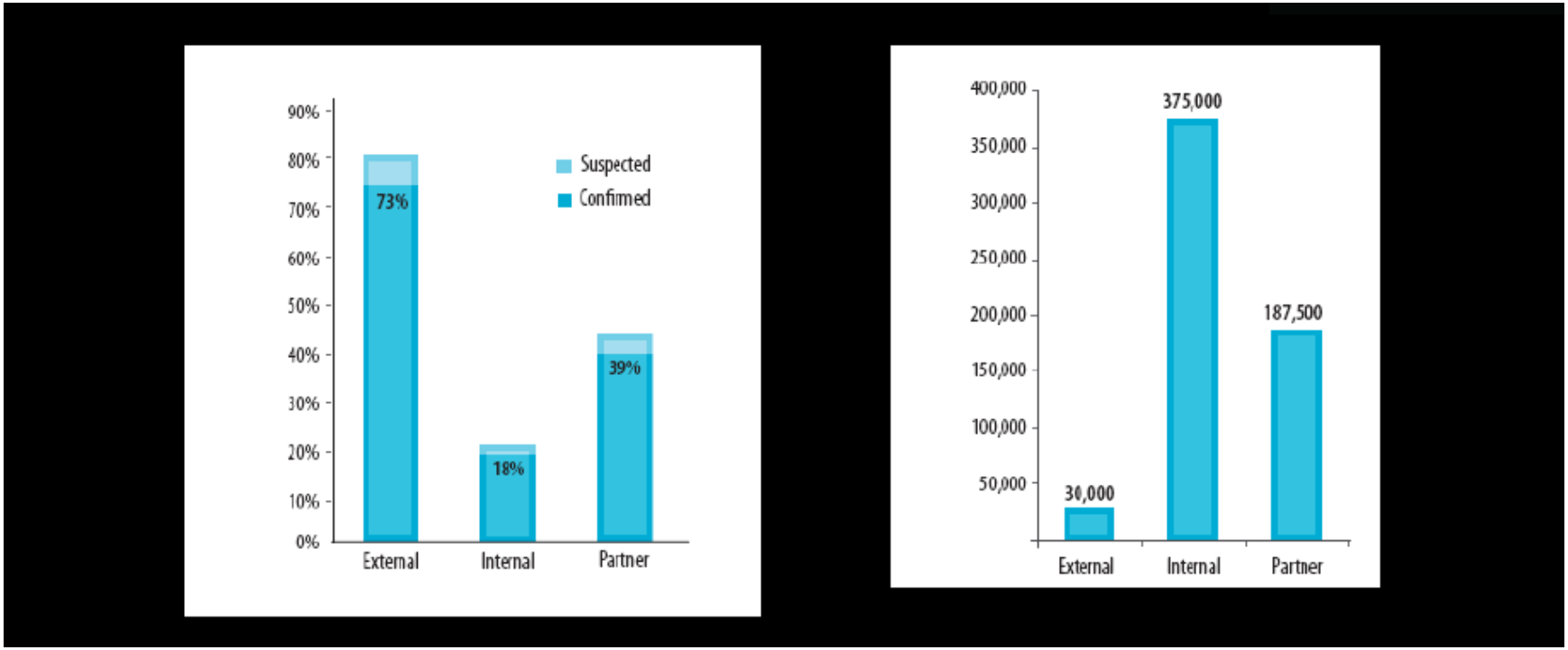
- lost top secret document about Al Quaida (public train)
- stolen data of thousand prisoners and prison guards
- personal information of 70Mio people unencrypted on DVD‘s lost
- bank employee gambled with 5.4Bio US$
- 88% of admins would steal sensitive corporate informations
- Industry espionage by insiders increased dramatically
- biggest criminal network (RBN) still operating
- Tousends of stolen hardware equipement @ US Army
- US Army lost 50.000 personal data of former soliers
- Chinas „Red Dragon“ organization cracked german gov network
- Lichtenstein Affaire – Insider vs. Secret Service

THE INSIDER THREAT

- Outsourcing and off-shoring trend becomes now a governmental problem (judgement decission)
- Large percentage of threats go undetected
  - huge internal know how
  - powerful privileges
  - track cleaning
  - „clearance“ problem
  - foreign contact persons / turnovers
- Easier exchange of sensitive data

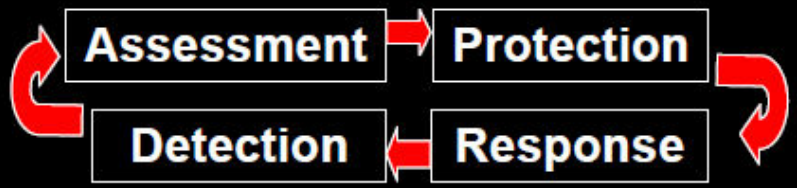
  (hacker‘s ebay, RBN, paralell internet, dead postboxes...)

OFFICIAL STATISTICS
EXTERNAL/INTERNAL THREAT



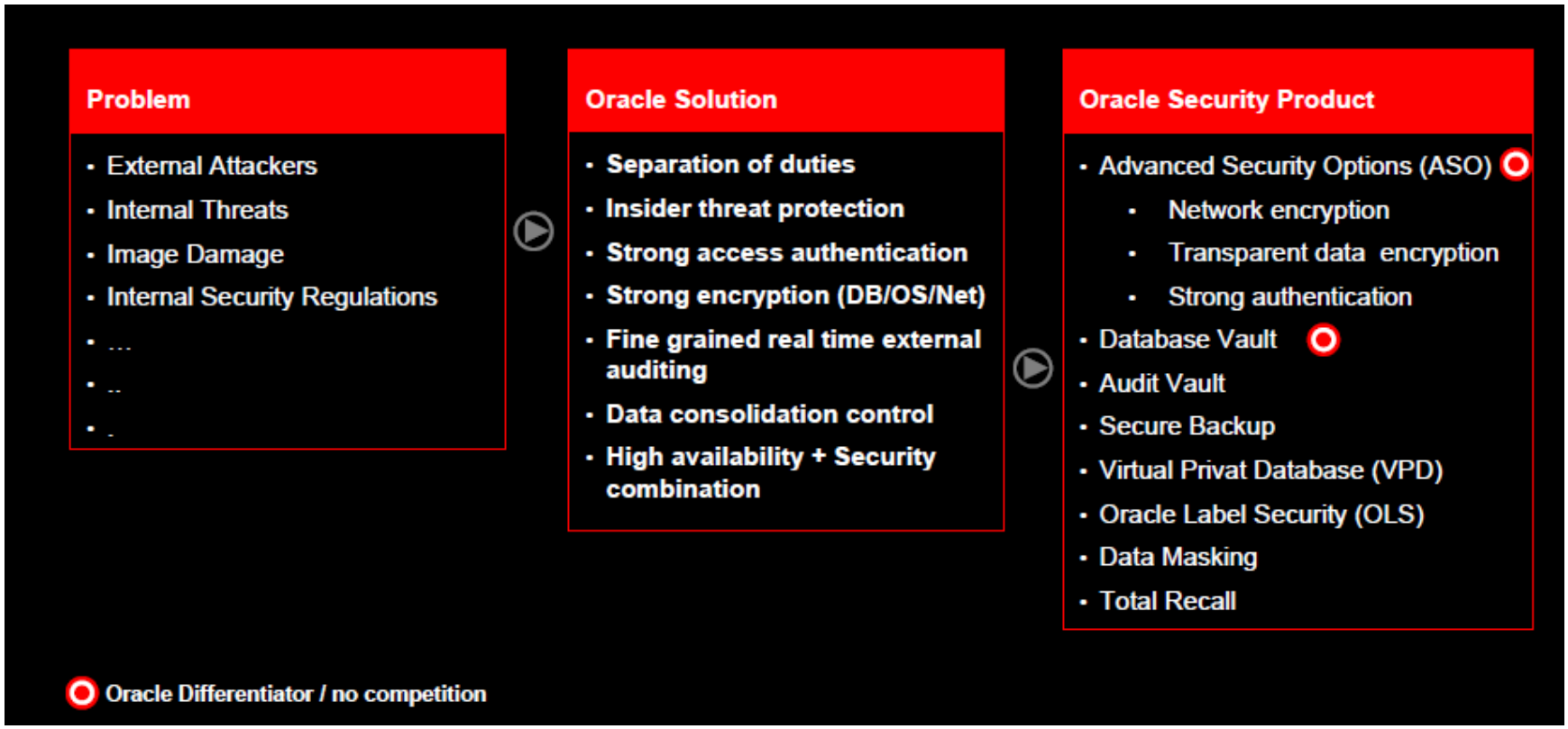
CONCLUSION

- Security is a „race“, if you stop running you‘ll lose
- Security IS NOT a product; it‘s an ongoing living process



- Security IS an intelligent combination of more areas -> „Big picture“
- Focus on your data, not only on the technic

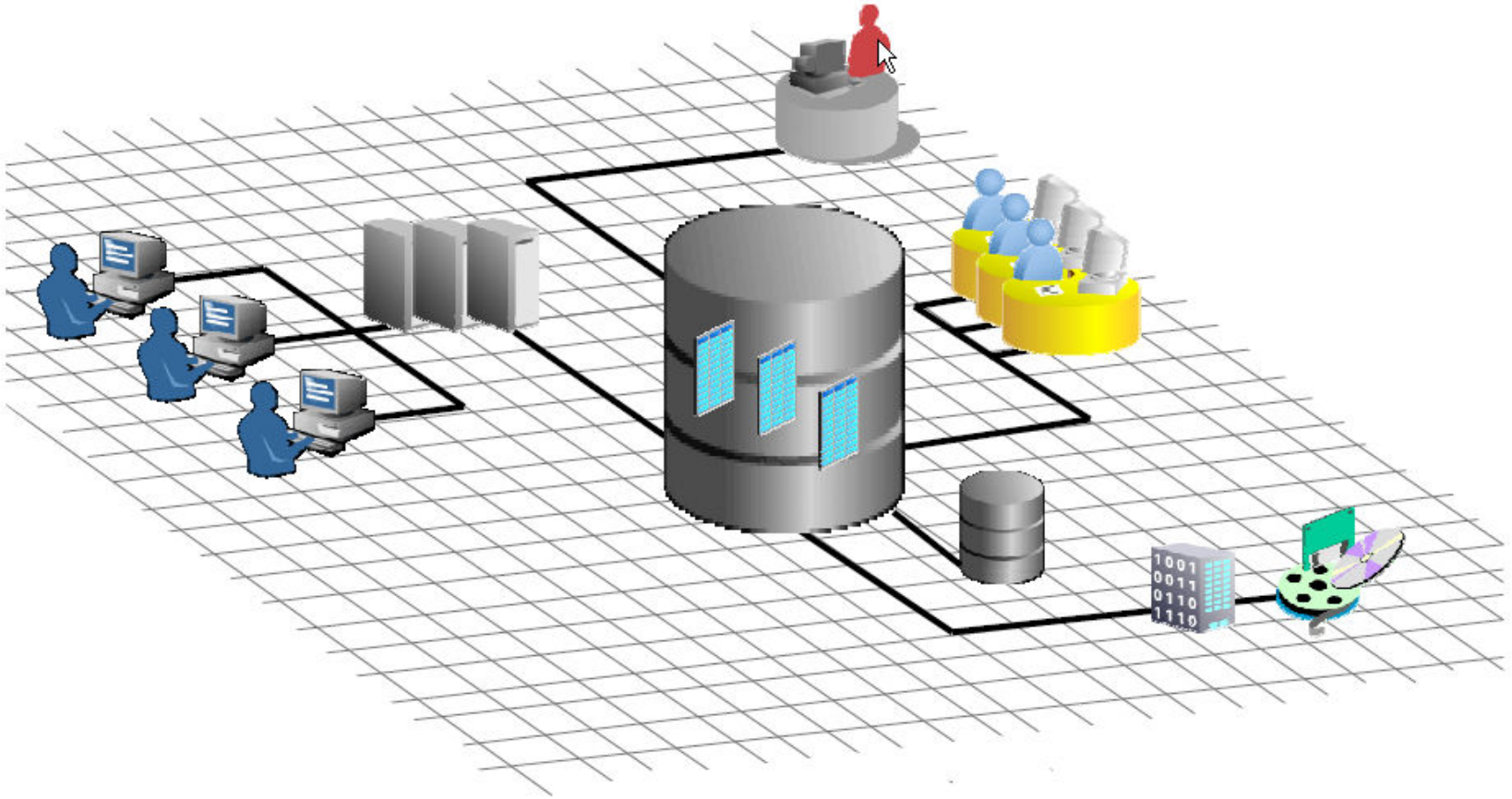
Oracle Security Solutions



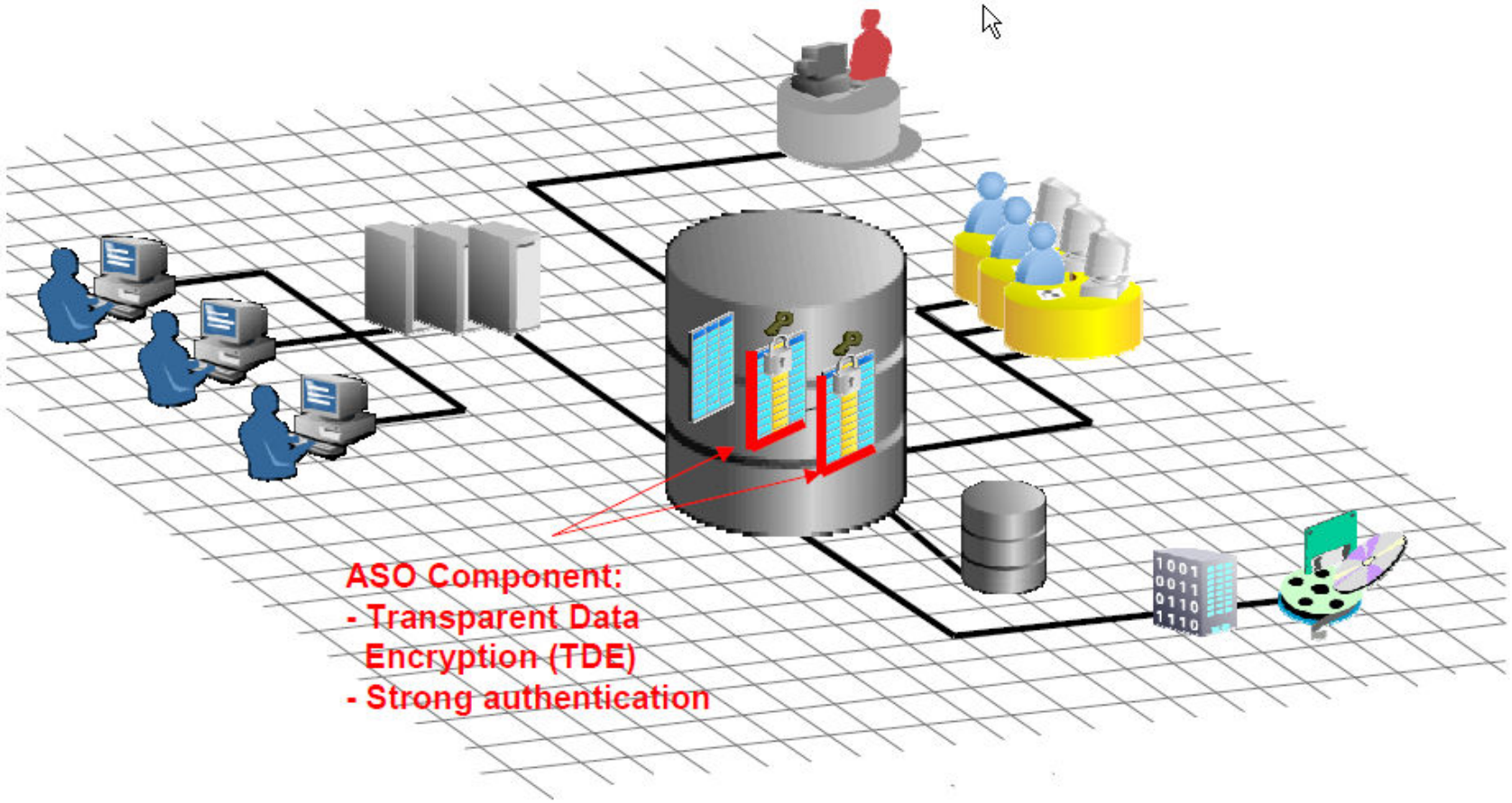
Oracle Security Components

Shortcut	Name	Description	Insider	Compl
OLS	Oracle Label Security	Row level security		o
VPD	Virtual Private Database	Row level security		o
ASO	Advanced Security Options	Security package includes:	o	o
TDE	Transparent Data Encryption	Column encryption (DB & OS)	o	o
NE	Network Encryption	Network traffic encryption	o	o
SA	Strong Authentication	Strong (Two factor) authentication	o	o
DBV	Database Vault	Separation of duties / Data privacy	o	o
AV	Audit Vault	Logging / Monitoring / Reporting	o	o
OSB	Oracle Secure Backup	Backup encryption	o	o
CPU	Critical Patch Update	Necessary security patches		o
DM	Data Masking	„Scrambling“ of production data	o	o

DB ENVIRONMENT



Security Data in Rest/Access Control



WHAT IS ASO?

- ASO = Advanced Security Option
- an Oracle Database option
- a package of 3 security features:
  - TDE (Transparent Data Encryption)
  - Network Encryption
  - Strong Authentication against DB
- available for all 10g / 11g databases

What Security Problems does ASO solve?

- Insider Threats

  - Strong encryption (network/DB/file level)
  - Strong authentication

- Regulatory compliances (external / internal)

- Separation of duty

ASO BENEFITS

- Easy installation (database component)
- Easy to use
- NO NEED TO CHANGE THE DB STRUCTURE OR APPLICATION
- Bundel of important security components

TDE – Transparent Data Encryption

ID	AMEX Nr.	Expenses
01	83929843700	50.320
02	54220494833	29.872
03	00428274712	33.432

Name	Job	ID	Salary
King	CEO	01	850.000
Blake	CFO	02	700.000
Custodes	CSO	03	550.000
McLord	CIO	04	570.000
Smith	DBA	05	50.000

FY	Q1	Q2	Q3	Q4
04	1.3M	1.8M	4.9M	10.1M
05	2.2M	3.5M	6.5M	14.4M
06	3.0M	3.9M	6.7M	16.5M
07	3.8M	5.5M	12.2M	20.4M

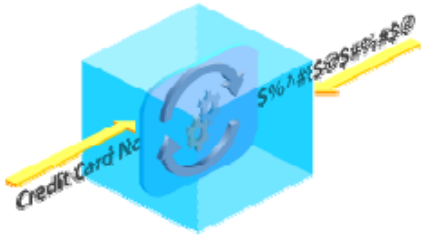
TDE – Transparent Data Encryption

ID	AMEX Nr.	Expenses
01	♦♐✋☠☝♓◆&♦●	50.320
02	♦♏♋□♦●●♦📱🖱♦	29.872
03	♠&♦●♓👍♐✋☠☝	33.432

Name	Job	ID	Salary
King	CEO	01	♦♋♎♐♂
Blake	CFO	02	♦♋●♦□□
Custodes	CSO	03	●&♦♍♍
McLord	CIO	04	☒♍♍■❖
Smith	DBA	05	●♑♒♑

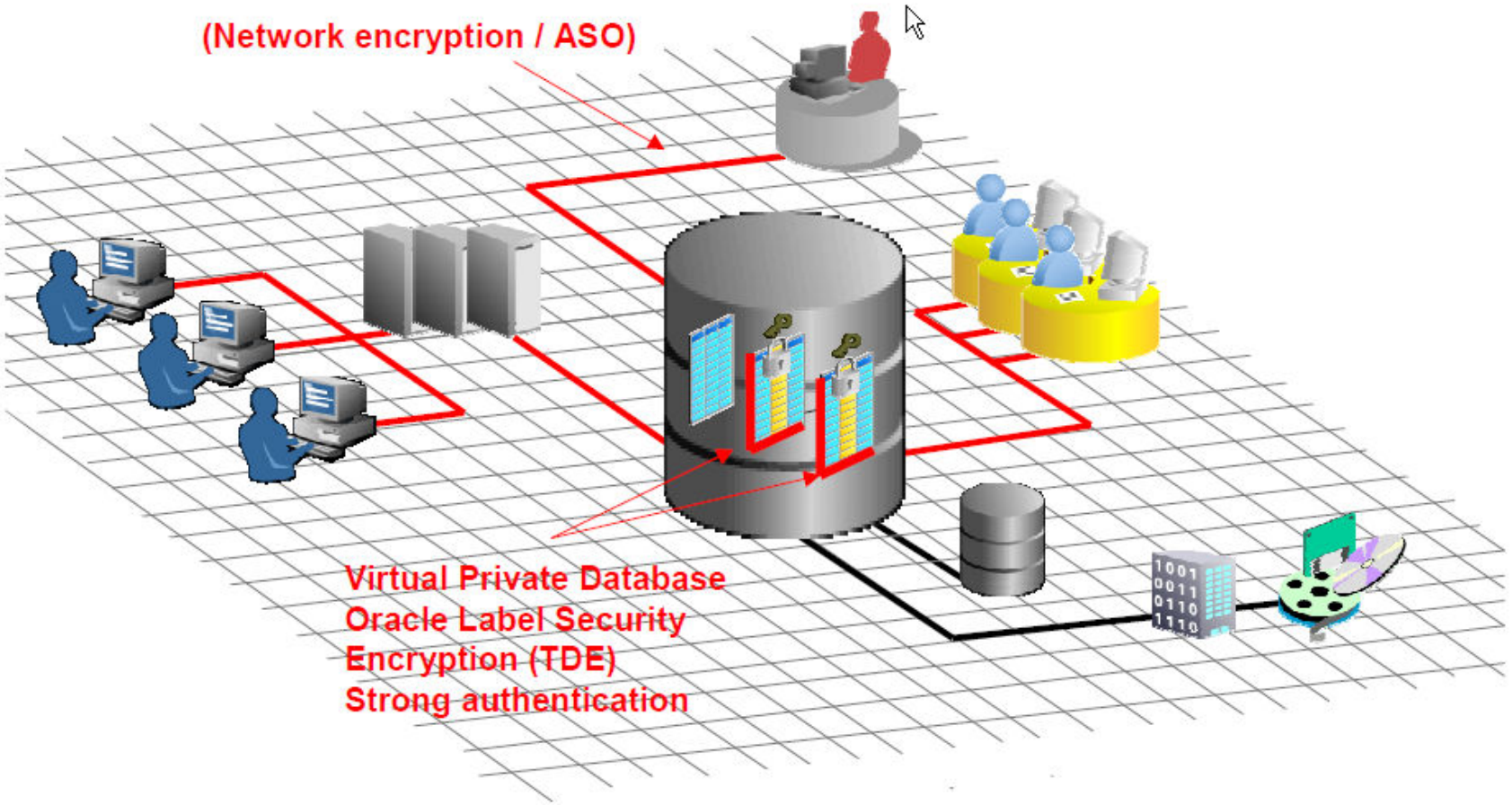
FY	Q1	Q2	Q3	Q4
04	1.3M	1.8M	4.9M	□♦♓♏◆
05	2.2M	3.5M	6.5M	●♦&♎♠
06	3.0M	3.9M	6.7M	♍♍■☒♦
07	3.8M	5.5M	12.2M	♌⌘♒◆♦

TDE – Transparent Data Encryption

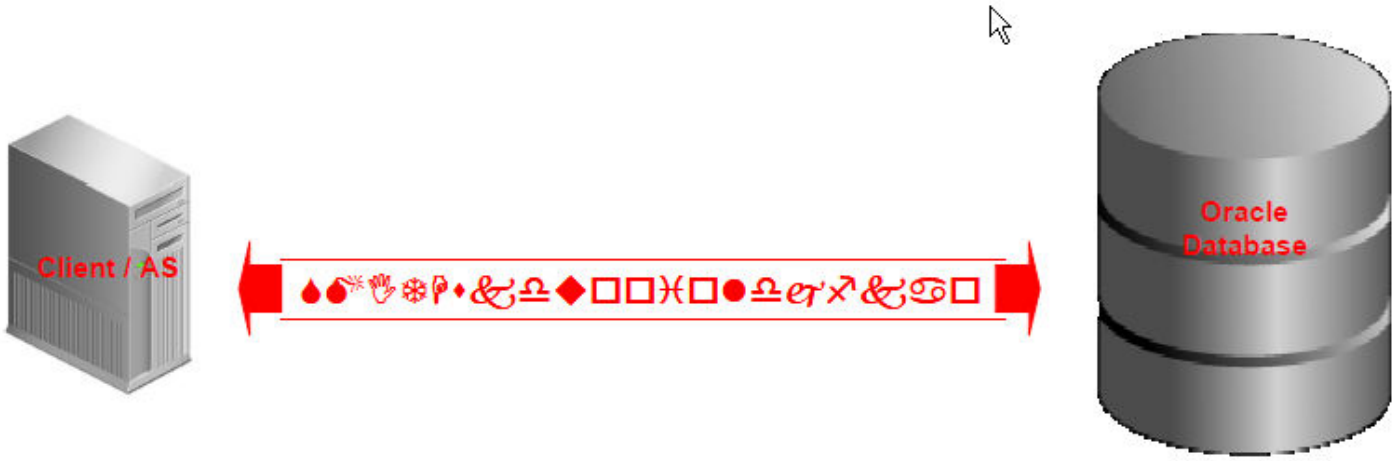


- Integrated into DB-Kernel
  - Alter table encrypt column …
- Transparent for all applications
  - No need for database triggers or views
- Performance
  - Works with existing index
- Data are also encrypted on file level (OS)
  - 3DES, AES (128, 192, and 256 bit)
- Uses Oracle wallet technology

SECURING DATA IN MOTION



NETWORK ENCRYPTION



sqlnet.ora (Client)

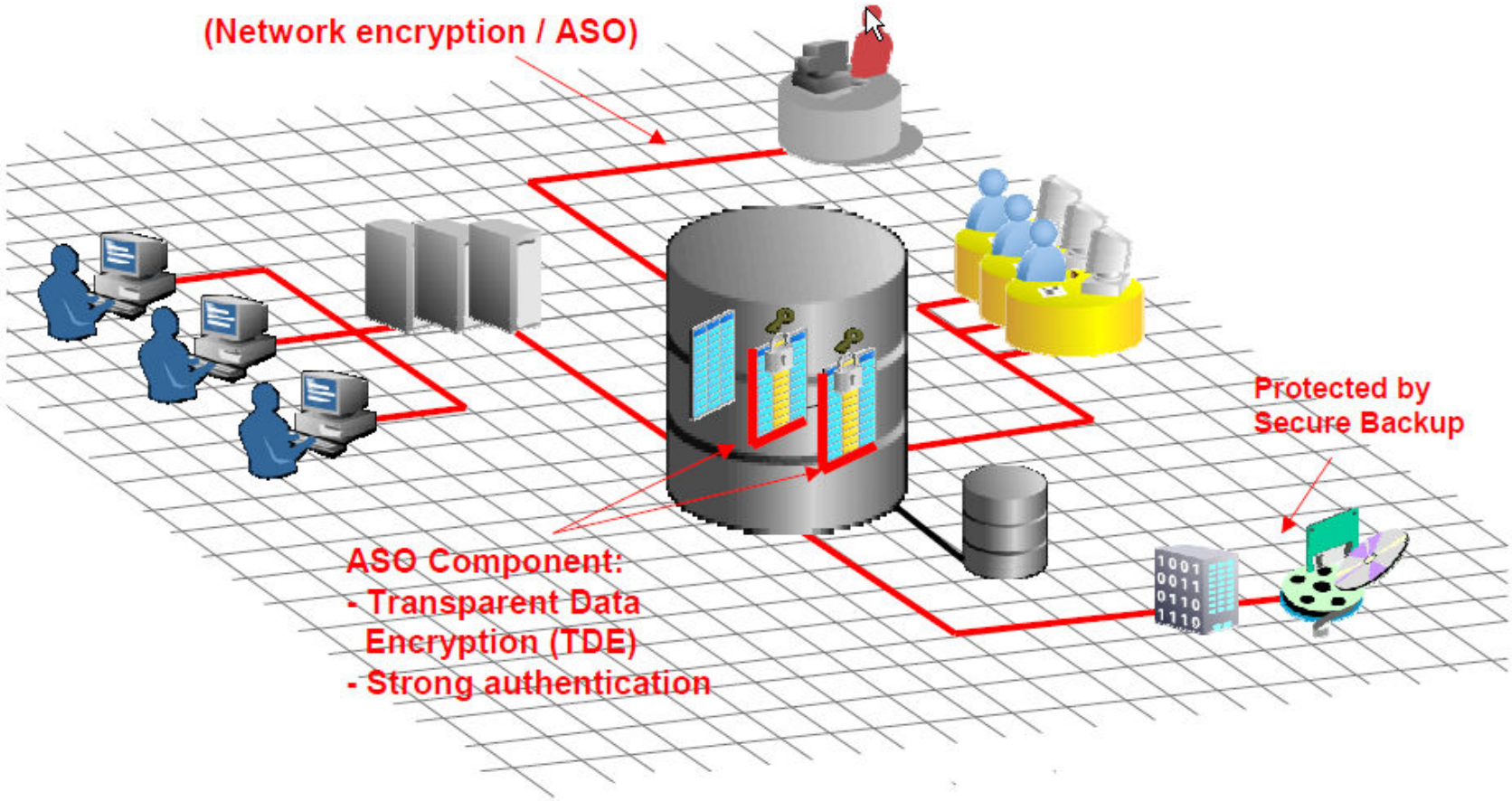
1. sqlnet.crypto_seed=„salkdjfaoiwjoiejlksjflksajuoiwjlks“
2. sqlnet.encryption_client = required
3. sqlnet.encryption_types_client = (RC4_40)
4. sqlnet.crypto_checksum_client = requested
5. sqlnet.crypto_checksum_types_client = (MD5)

sqlnet.ora (Server)

1. sqlnet.crypto_seed=„salkdjfaoiwjoiejlksjflksajuoiwjlks“
2. sqlnet.encryption_server = required
3. sqlnet.encryption_types_server = (RC4_40)
4. sqlnet.crypto_checksum_servert = requested
5. sqlnet.crypto_checksum_types_client = (MD5)

Note: RC4_40, RC4_56, RC4_128, DES, DES_40, Accepted, Rejected, Requested, Required

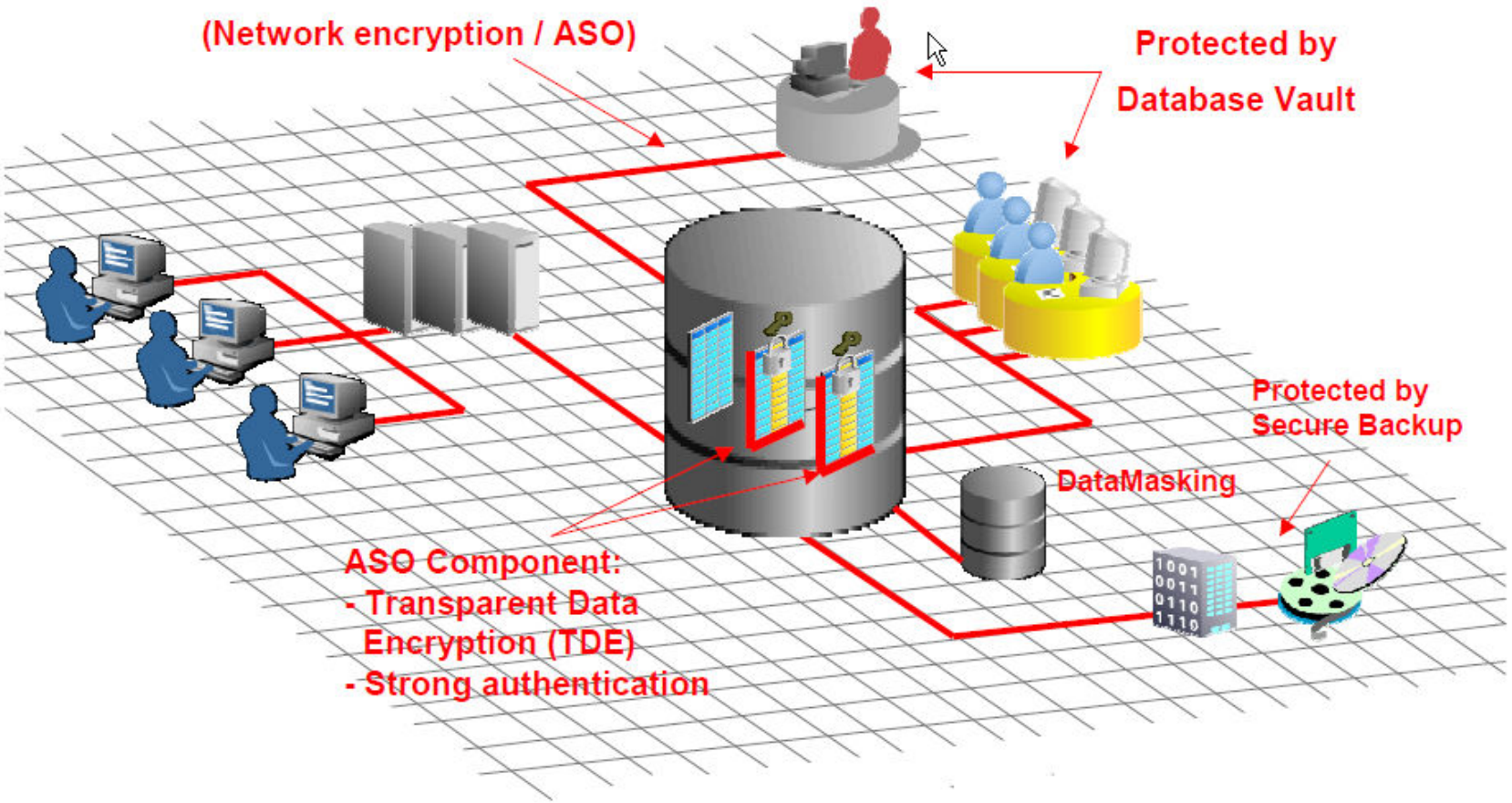
SECURING BACKUP



SECURING BACKUP
Examples

- Works with RMAN
- Encrypts data before it leaves the database
- Encrypts data on backup media
- Fastest Oracle Database backups to tape
- Singel point of control with Oracle Enterprise Manager

DATAMASKING

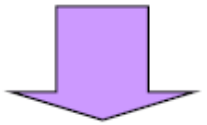


WHAT IS DATAMASKING?

Key Drivers

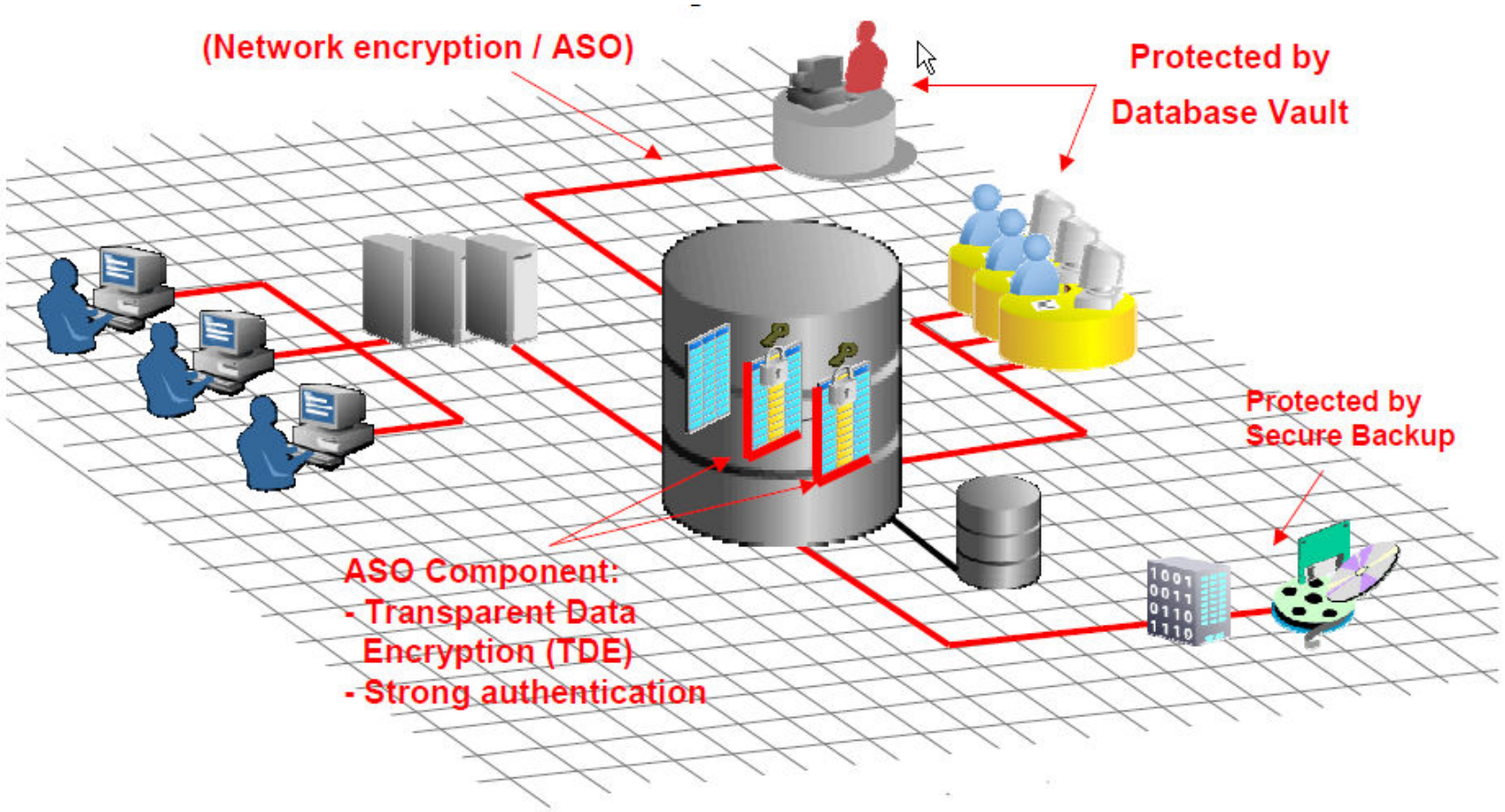
- Application Development & QA
  - Offshore / in-house
- Data Sharing
  - Claims processing
  - Marketing analysis of customer data
- Regulations
  - PCI
  - Sarbanes-Oxley
  - HIPAA
  - Graham-Leach-Bliley
  - EU Data Protection Directive

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

PREVENT MODIFICATIONS BY UNAUTHORIZED USERS



WHAT IS DATA VAULT?

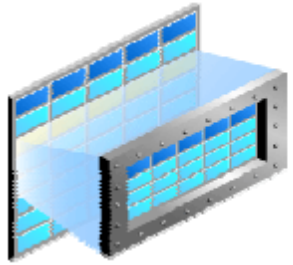
- Database component (installable within 20min)
- One of our „strongest security weapon“ (no competition)
- An easy configureable (GUI/sqlplus) „tool box“
  - to reach a high level of security
  - fulfill internal / external compliances
  - implemented auditing/reporting function
- available for all 9i /10g /11g databases

DATA VAULT HELP TO SOLVE:

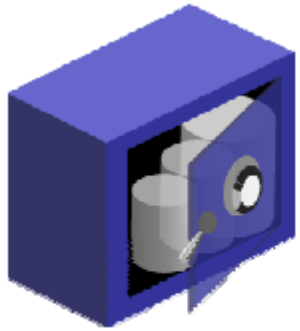
- **Internal threats** require enforcement of operational security policies - who, what, when and where can data be accessed?
- Database consolidation can result in **Multiple All Powerful (DBA)** users in the database
- Regulations **Strong Internal Controls** and **Separation of Duty** (such as Sarbanes-Oxley and Basel II etc)

DATA VAULT Vs VPD and OLS

- Virtual Private Database (VPD):
  - Restricts access to certain rows for user by modifying the `WHERE` clause
- Oracle Label Security (OLS):
  - Mediates access to a given row, based on the label on the row and the security level of the user

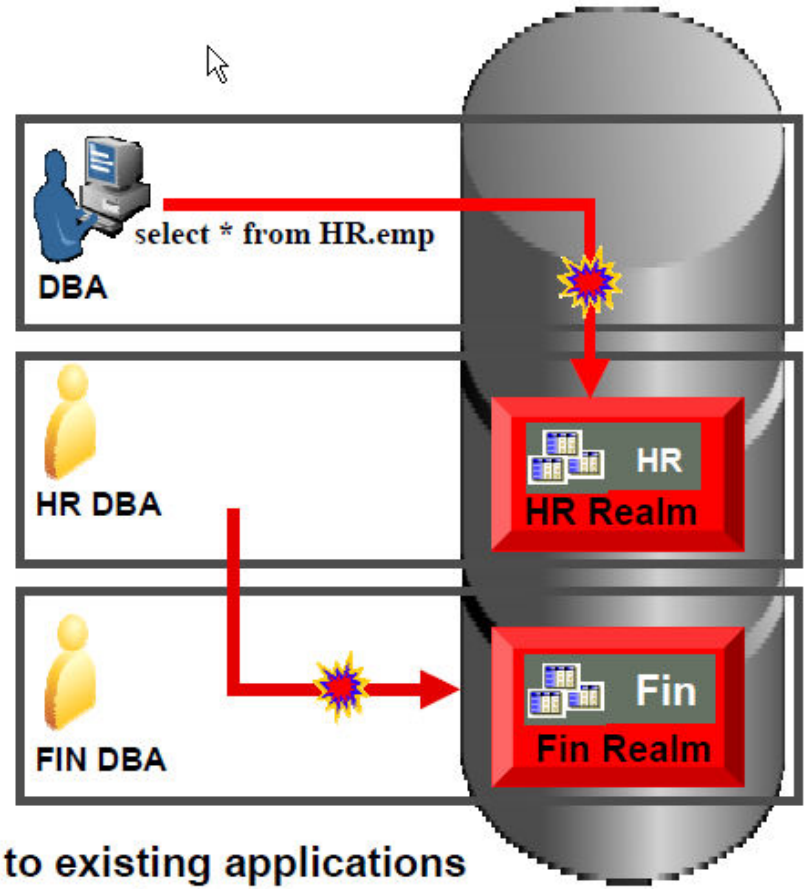


VPD and OLS restrict access at the row level, while Database Vault restricts access at the object and command levels.



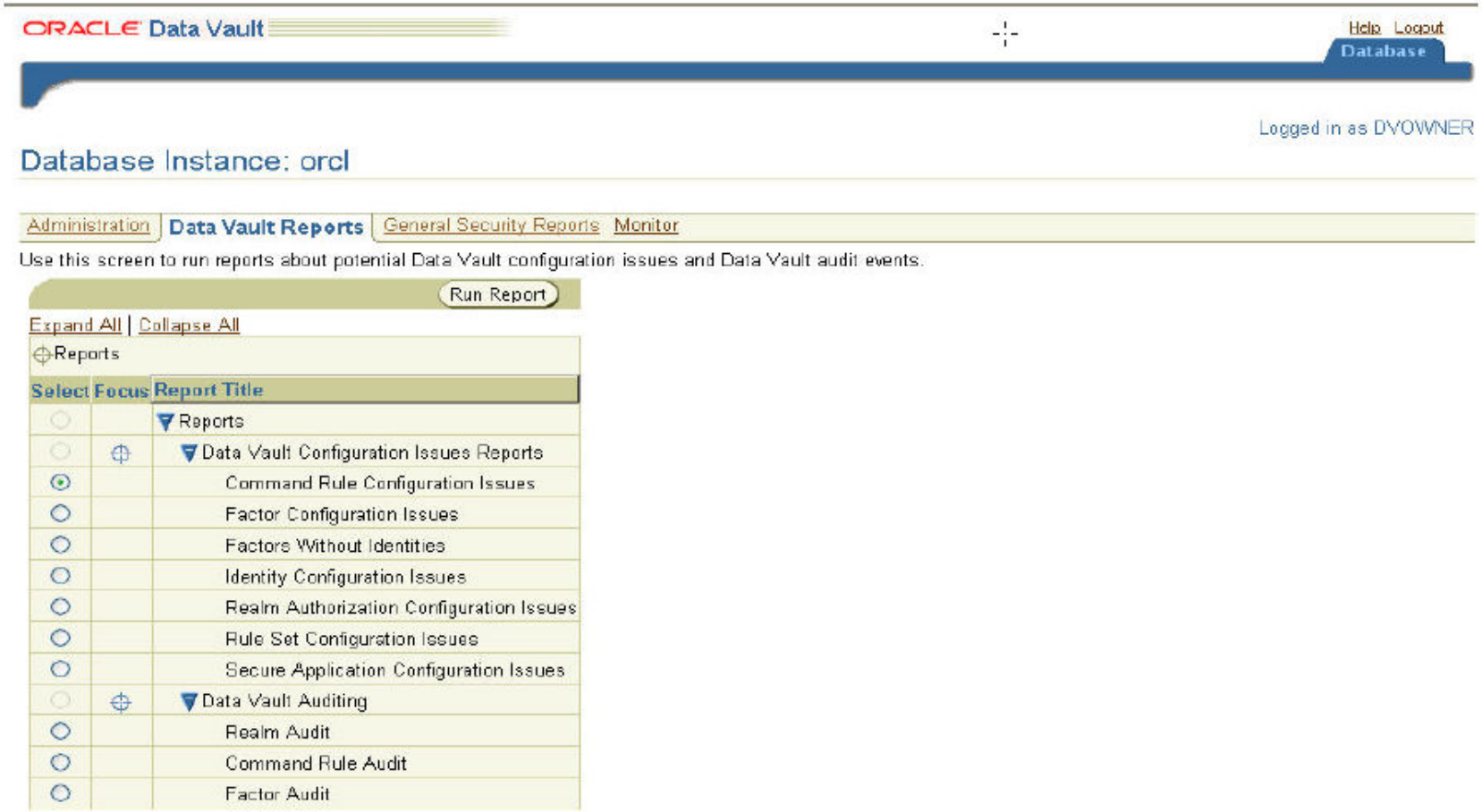
DATABASE VAULT Realms and Rule

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

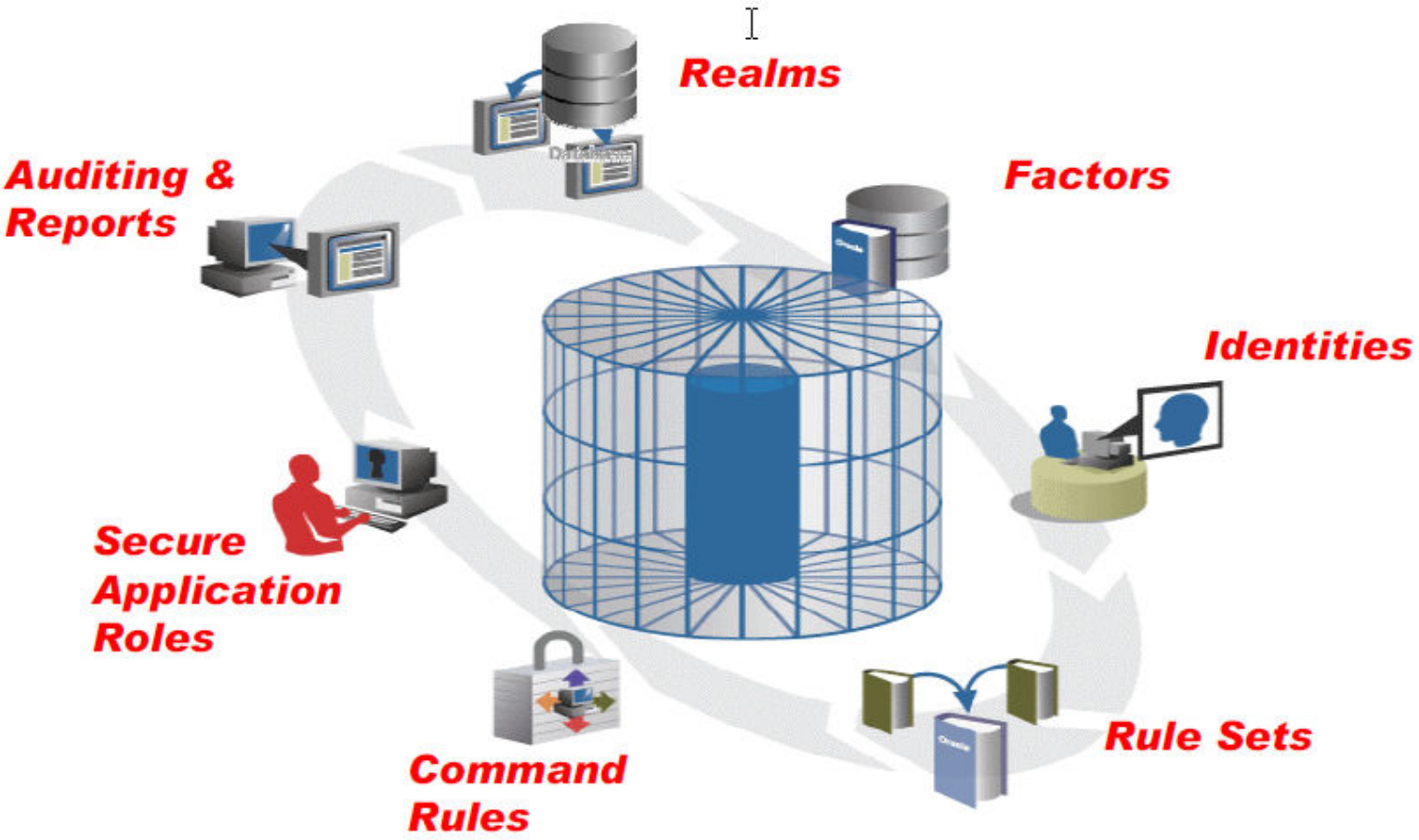


Realms can be easily applied to existing applications with minimal performance impact

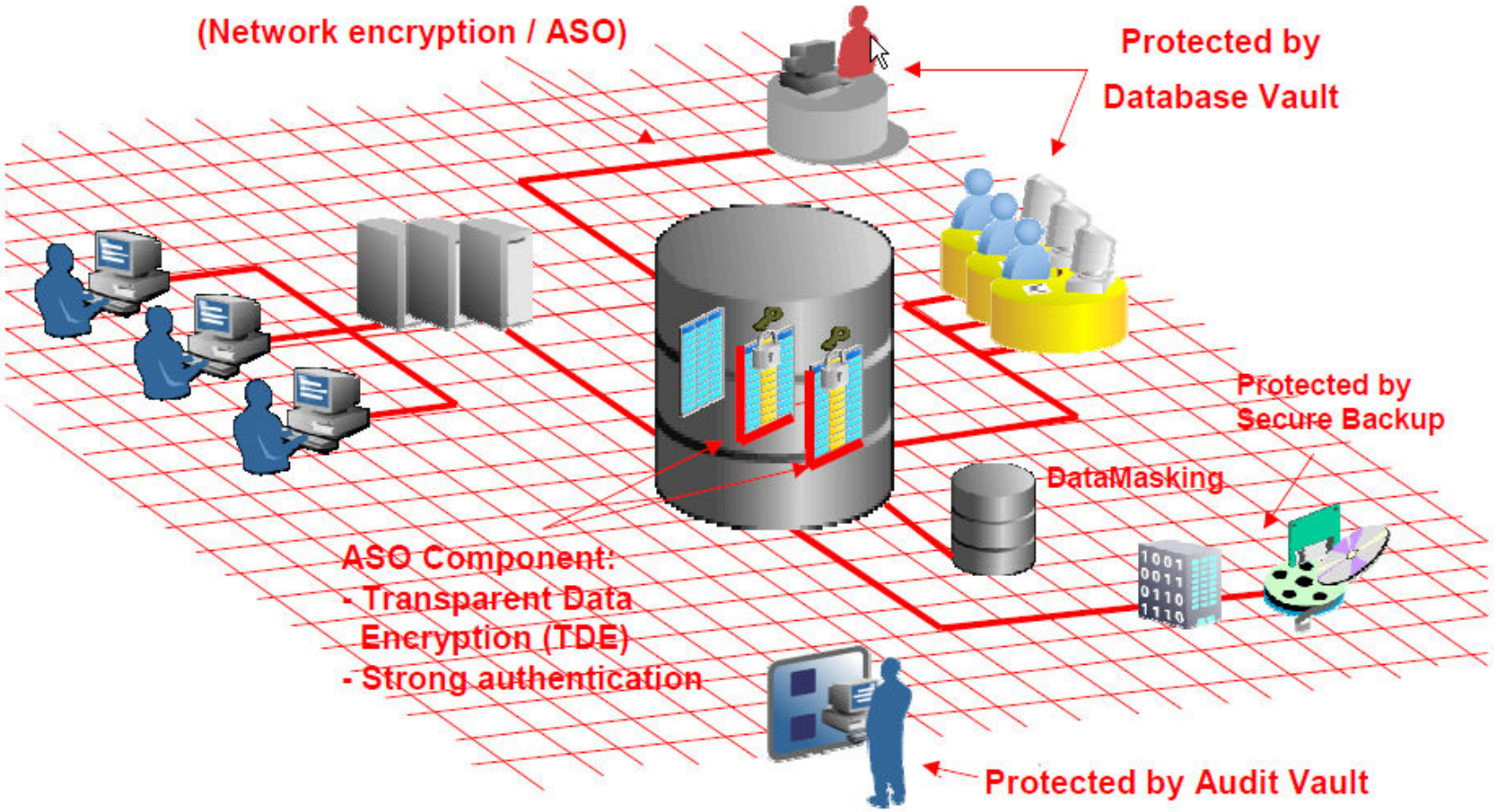
DATA VAULT REPORTS



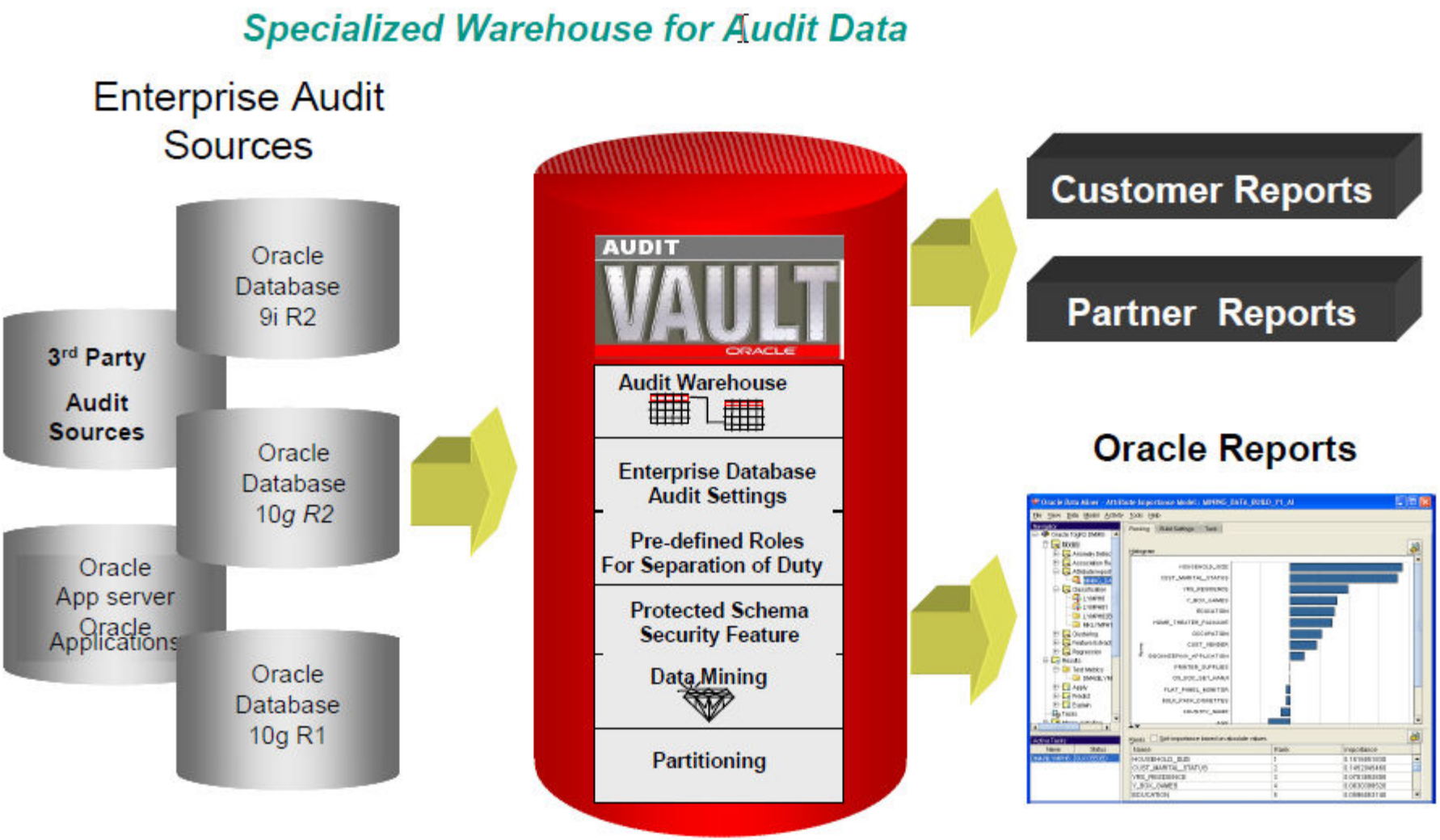
DATA VAULT EXAMPLES



HIGHLY SECURED ENVIROMENTS
AUDIT VALT



AUDIT VAULT EXAMPLES



AUDIT VAULT REPORTS
Who, What, When, Where

User	VSHAH	
OS User	oracle	
End User		
Terminal		ORCLDB
Host	oel4upd4.oracle.vm	HR ORACLE VM
Host		
Subr		
Dom		

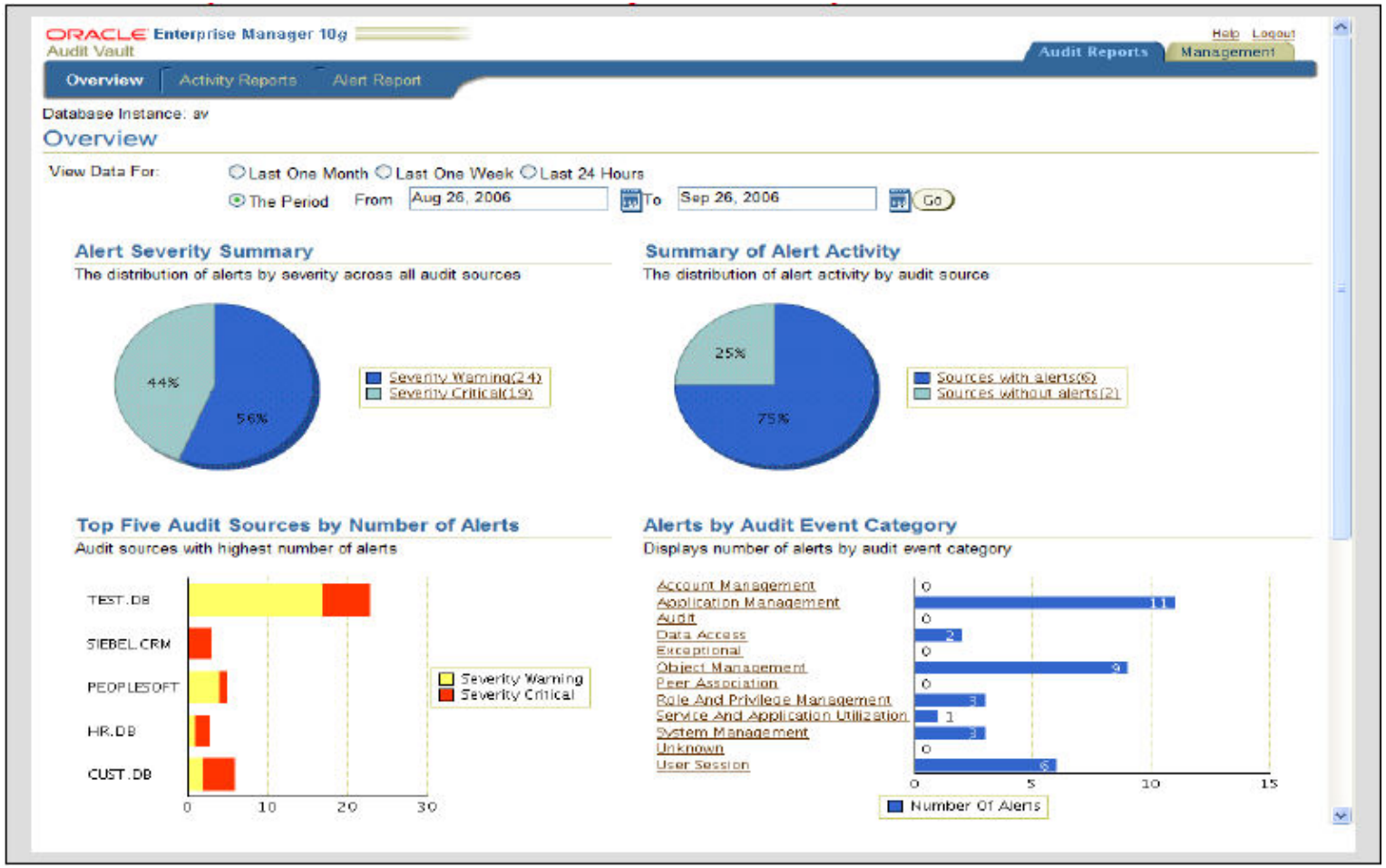
SQL Bind	
SQL Text	update oe.orders set order_total=order_total*1.5 where order_id=2458
Undo SQL text	

SCN 668999

Column	Old Value	New value
ORDER_TOTAL	264193.65	396290.48

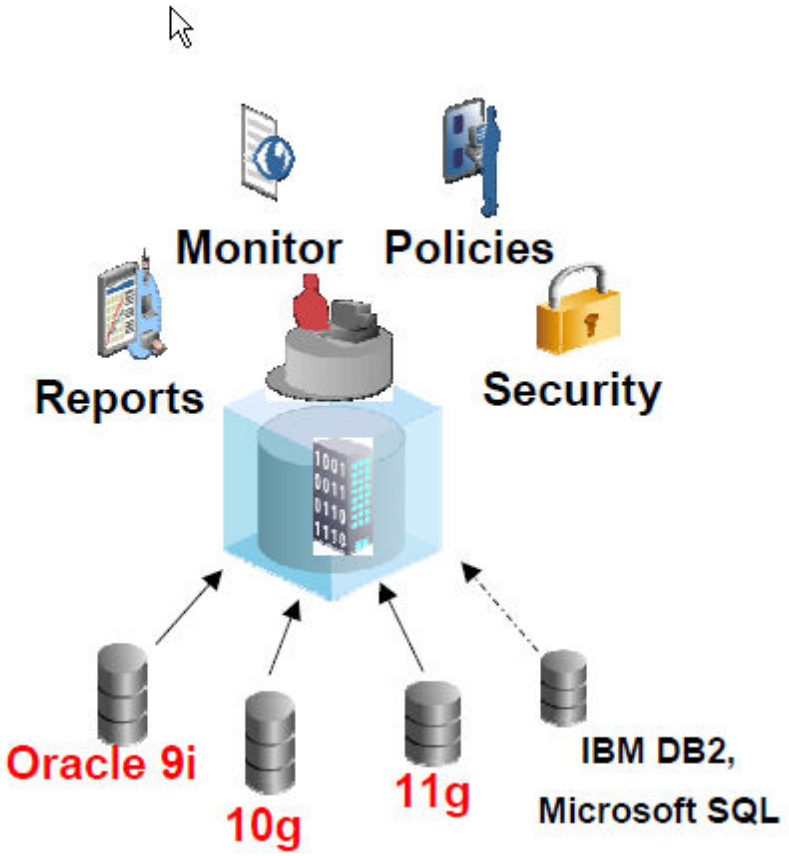
Collection Time	2007-09-12 10:34:51
Object	OE.ORDERS
Owner	OE

AUDIT VAULT DASHBOARD



AUDIT VAULT SUMMARY

- Collect and Consolidate Audit Data
- Simplify Compliance Reporting
- Detect and Prevent Insider Threats
- Lower IT Costs With Audit Policies
- Scale and Security



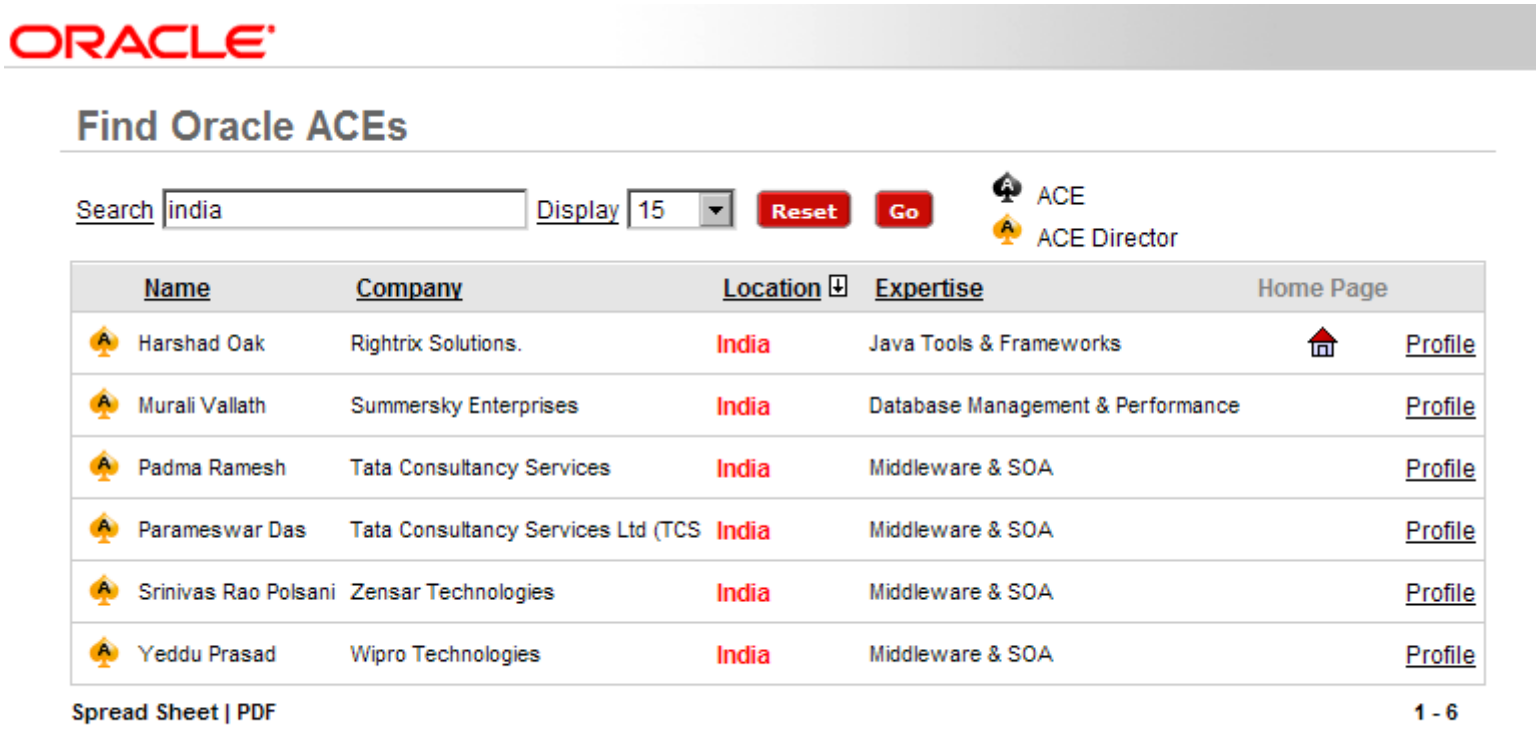
Oracle ACE PROGRAM

The Oracle ACE Program is designed to recognize and reward members of the Oracle Technology and Applications communities for their contributions to those communities. These individuals are technically proficient (when applicable) and willingly share their knowledge and experiences.

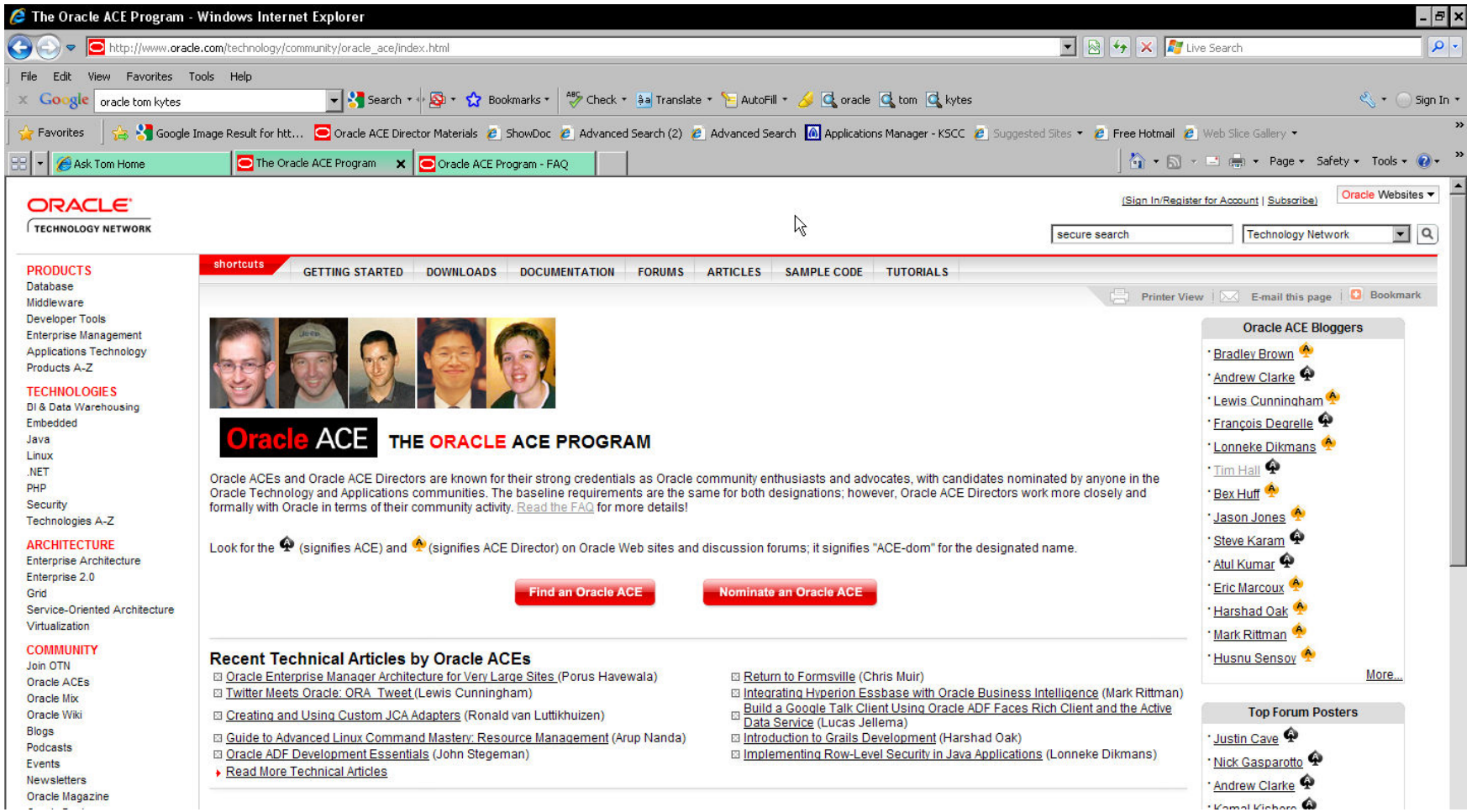
The program comprises two levels**: Oracle ACE and Oracle ACE Director.**

The former designation is Oracle's way of saying "thank you" to community contributors for their efforts; we (and the community) appreciate their enthusiasm. The latter designation is for community enthusiasts who not only share their knowledge (usually in extraordinary ways), but also want to increase their community advocacy and work more proactively with Oracle to find opportunities for the same. In this sense, Oracle ACE is "backward looking" and Oracle ACE Director is "forward looking."

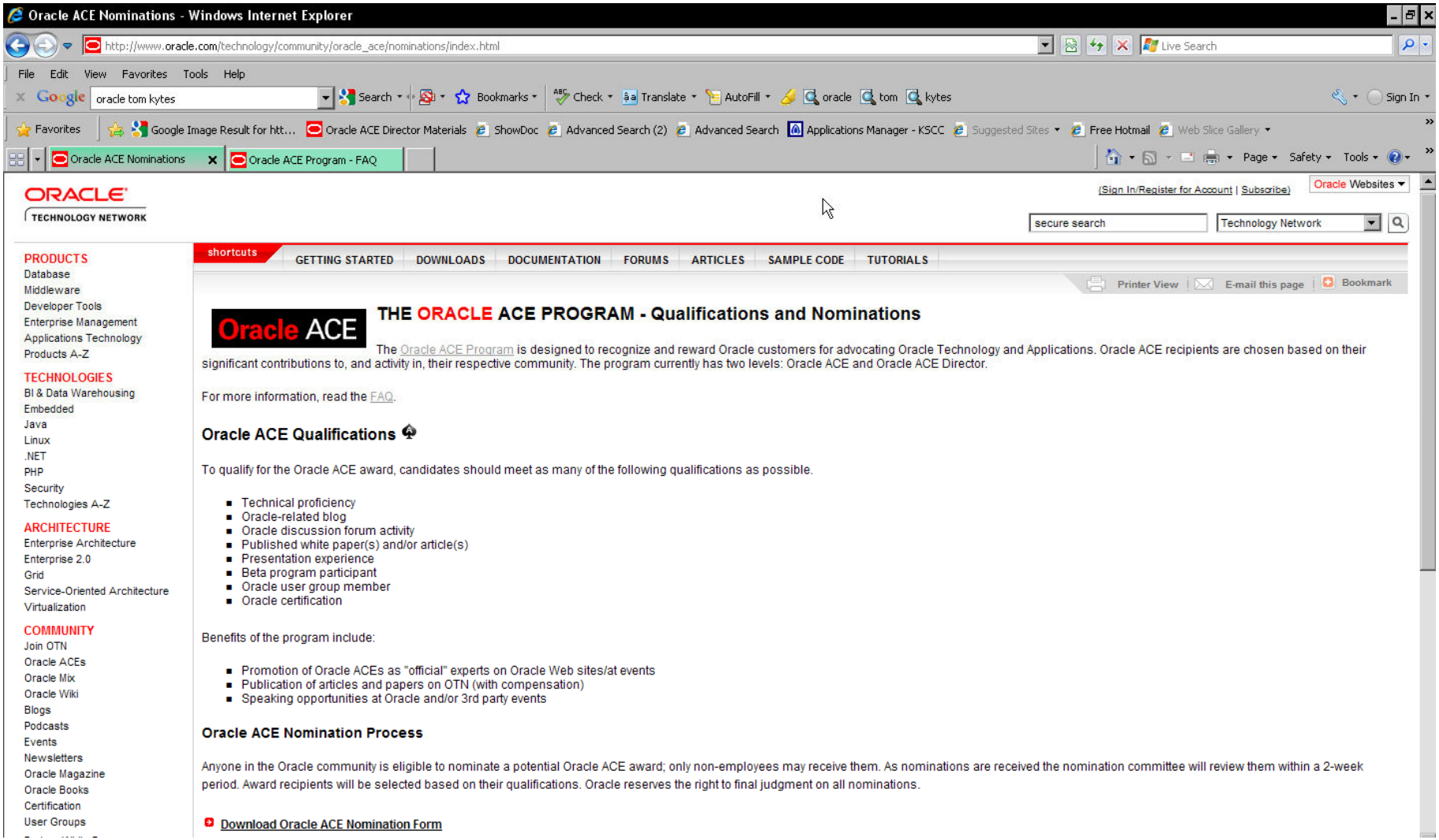
Oracle ACE PROGRAM



Oracle ACE PROGRAM



Oracle ACE PROGRAM



Questions?

dbis™ DATABASE INTEGRATED SOLUTIONS

Thank you !

dbis™ DATABASE INTEGRATED SOLUTIONS