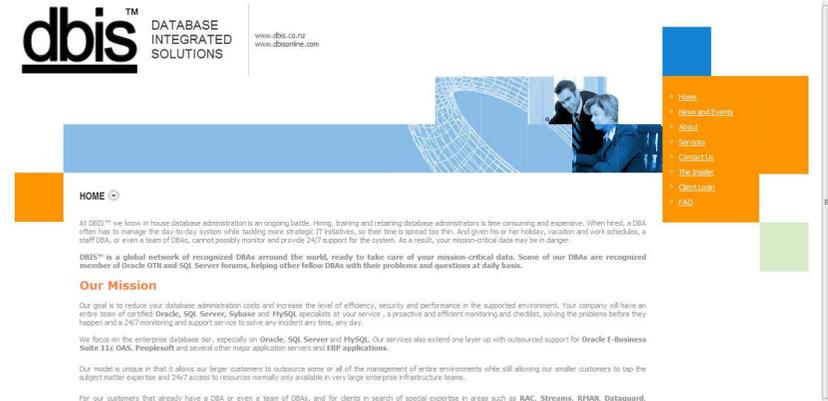


ORACLE SECURITY OPTIONS

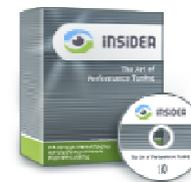
PEOUG' 2009

2009 Lima, Peru



The screenshot shows the dbis website homepage. At the top left is the logo 'dbis™ DATABASE INTEGRATED SOLUTIONS' with the website addresses 'www.dbis.co.pe' and 'www.dbisonline.com'. A navigation menu on the right includes links for Home, Issues and Events, About, Services, Contact Us, The Insider, Client Login, and FAQ. The main content area features a 'HOME' link with a dropdown arrow, followed by a paragraph about database administration challenges, a section titled 'Our Mission' with a sub-header, and several short paragraphs describing their services and expertise.

By:
Francisco Munoz Alvarez 🇵🇪



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](https://twitter.com/fcomunoz)

Blog: www.oracleenespanol.com - Comunidad Oracle: www.oraclemania.ning.com

CEO at DBIS™

Database Integrated Solutions

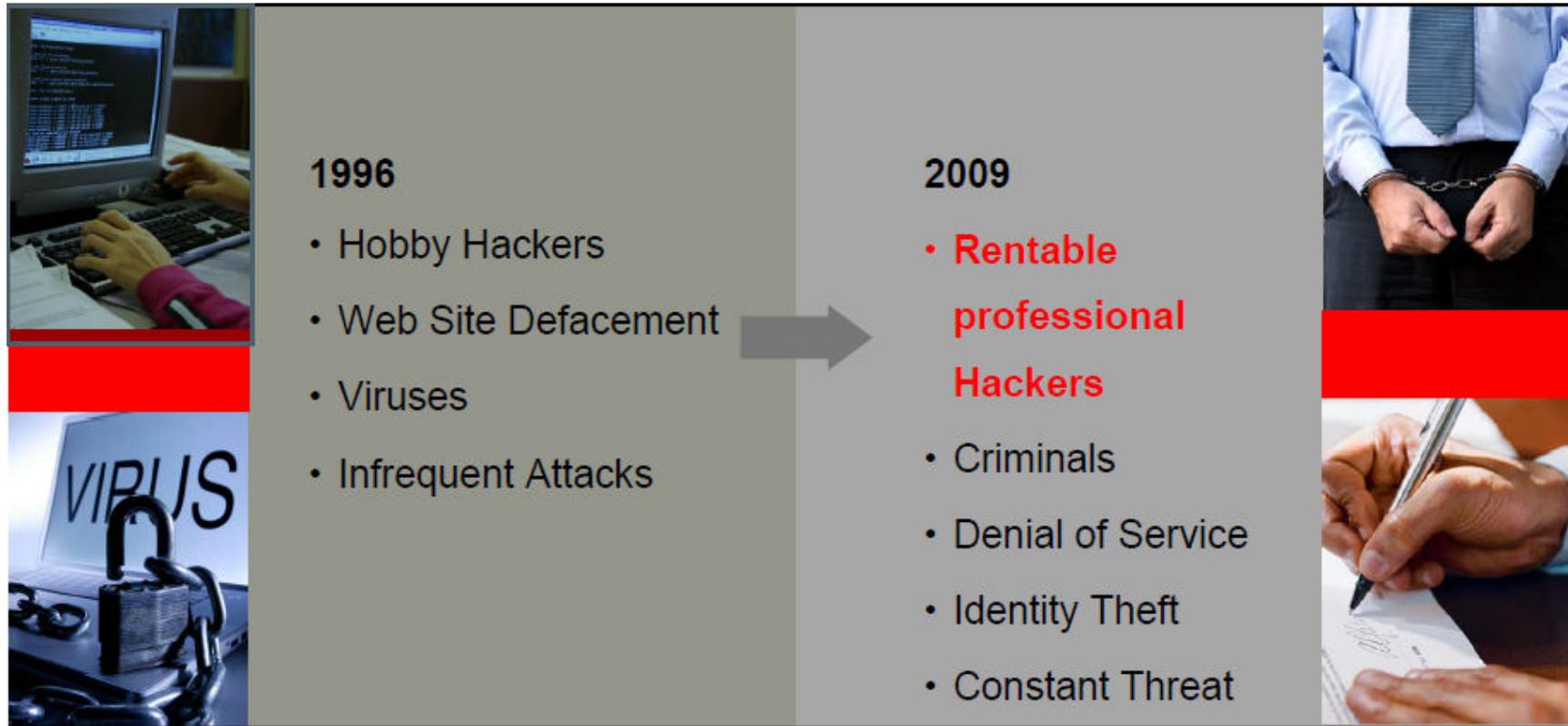
www.dbisonline.com

www.dbis.co.nz



dbis™
DATABASE
INTEGRATED
SOLUTIONS

Information Security Has Changed



1996

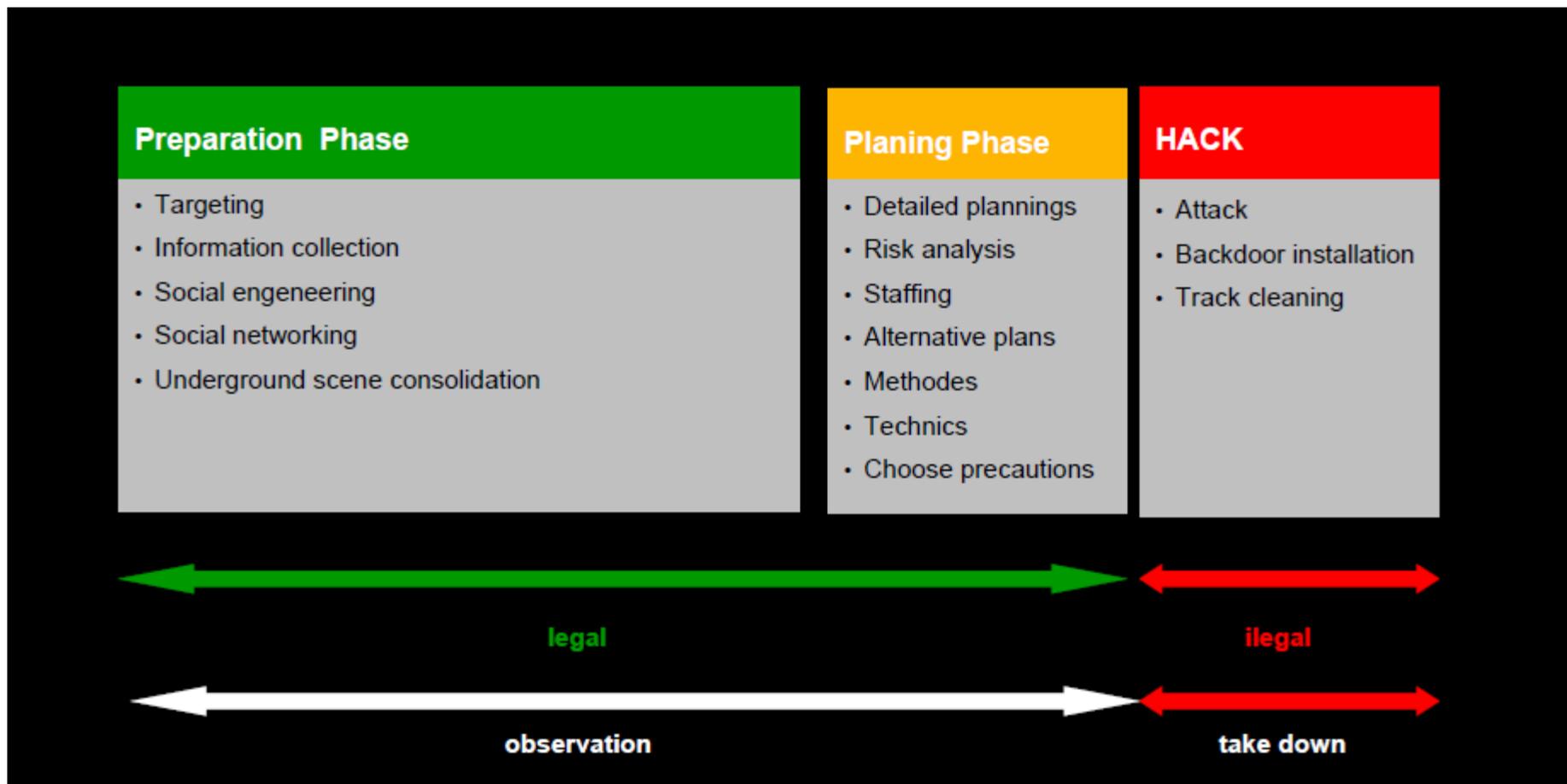
- Hobby Hackers
- Web Site Defacement
- Viruses
- Infrequent Attacks

→

2009

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

Hacking Steps



OFFICIAL STATISTICS from Secret Service Germany



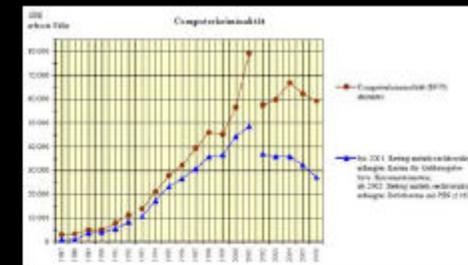
Dramatical increas of the computer crime since the last 12 years (professionalism)



Bigest damage by insiders (sabotage, spying, Information selling)



**Typical Hacker is male and over 21;
BUT starts with 14 !!!**



Tätigkeits- und Aufklärung (Tabelle 1)
Bereich: Wirtschaftswachstum

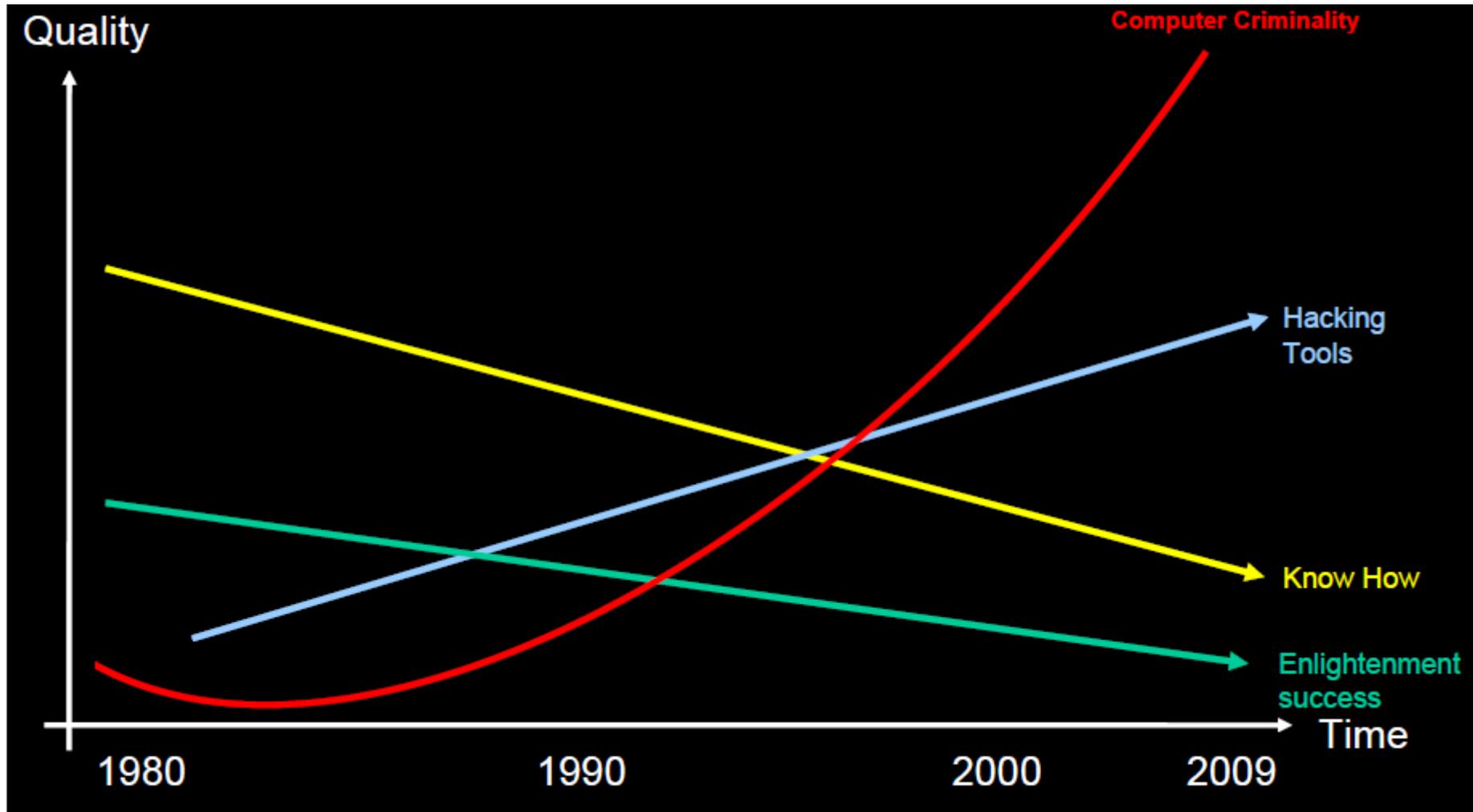
Statistik-Nr.	Tätigkeitsgruppe	Fallzahl		Veränderung		Aufklärungsrate	
		2011	2012	2012/2011	2012	2011	2012
8770	Computerkriminalität alle	32.141	42.134	+12,7	9,5	12,1	10,1
1843	Diebstahl von Daten mit Hilfe von IT-Systemen	27.141	31.232	+14,9	11,1	10,9	10,9
1870	Computerkriminalität (DfK) SGB	30.211	37.873	+12,6	11,1	10,9	10,7
1879	Diebstahl von Daten mit Hilfe von IT-Systemen in Unternehmen	2.922	5.198	+76,3	8,0	11,7	10,6
5405	Fälschung von elektronischen Daten, Täuschung von Behörden bei Datenverarbeitung (S. 209, 270 SGB)	2.440	1.012	-58,5	14,1	10,9	10,7
4743	Diebstahl von Daten mit Hilfe von IT-Systemen	1.477	1.404	-5,0	10,0	10,0	11,9
4780	Angelegenheiten von Daten	2.944	2.844	-3,4	10,0	10,0	11,1
7111	Schwarzmarkt für Datenverarbeitung (S. 209, 270 SGB)	1.920	2.067	+7,6	10,0	10,0	10,7
7112	Schwarzmarkt für Datenverarbeitung (S. 209, 270 SGB)	11	67	+509,1	14,1	10,0	10,0

Geschlecht- und Altersverteilung (Tabelle 2)
Bereich: Wirtschaftswachstum

Statistik-Nr.	Tätigkeitsgruppe	Geschlecht		Alter			
		weiblich	männlich	14-17	18-20	21-29	30-39
8770	Computerkriminalität alle	18.019	24.115	1,3	3,5	11,1	84,1
1843	Diebstahl von Daten mit Hilfe von IT-Systemen	7.811	29.421	2,8	11,8	14,9	80,5
1870	Computerkriminalität (DfK) SGB	4.944	25.929	1,2	4,3	11,6	82,9
1879	Diebstahl von Daten mit Hilfe von IT-Systemen in Unternehmen	2.922	2.276	8,8	6,5	11,1	81,1
5405	Fälschung von elektronischen Daten, Täuschung von Behörden bei Datenverarbeitung (S. 209, 270 SGB)	660	3.552	8,8	9,5	10,7	71,0
4743	Diebstahl von Daten mit Hilfe von IT-Systemen	144	1.330	1,1	6,2	7,1	85,6
4780	Angelegenheiten von Daten	1.477	1.367	8,4	1,8	8,7	81,1
7111	Schwarzmarkt für Datenverarbeitung (S. 209, 270 SGB)	1.175	892	8,8	8,9	7,1	83,2
7112	Schwarzmarkt für Datenverarbeitung (S. 209, 270 SGB)	11	56	8,8	1,4	7,6	82,2

Bei der Computerkriminalität im Vergleich zu anderen Verbrechen ist 21 Jahre.

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

100.000 \$ Destruction of competitor image

250.000 \$ Full internal competitor database

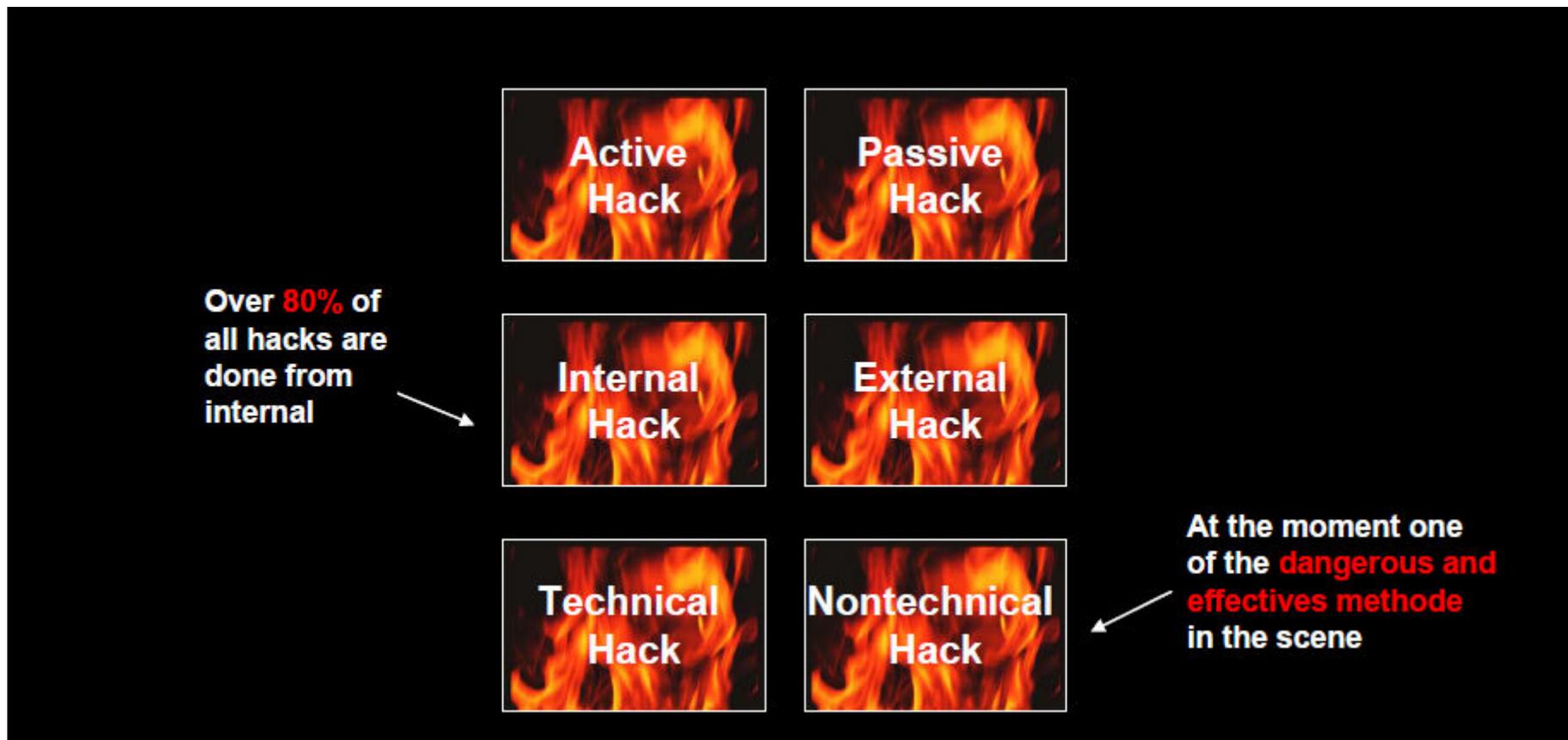
25 \$ per credit card account (+sec code + valid date)

20.000 \$ medium size BOT network (buy or rent)

2000 \$ stolen VPN connection

5000 \$ contact to “turned around” insider

HACKING METHODS AND TECHNIQUES



INSIDER ATTACKS EXAMPLES

European Headlines 2008

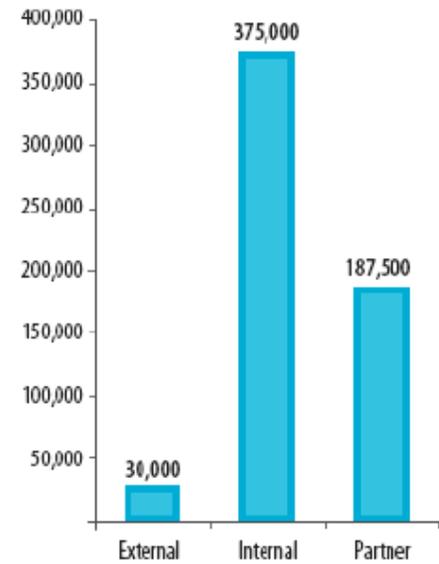
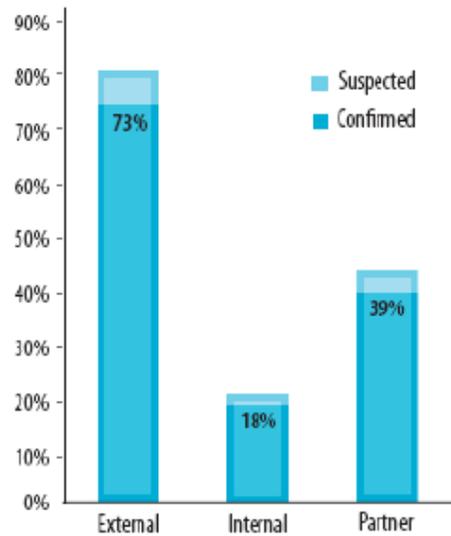
- **lost top secret document about Al Quaida (public train)**
- **stolen data of thousand prisoners and prison guards**
- **personal information of 70Mio people unencrypted on DVD's lost**
- **bank employee gambled with 5.4Bio US\$**
- **88% of admins would steal sensitive corporate informations**
- **Industry espionage by insiders increased dramatically**
- **biggest criminal network (RBN) still operating**
- **Tousands 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 decision)
- 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...)

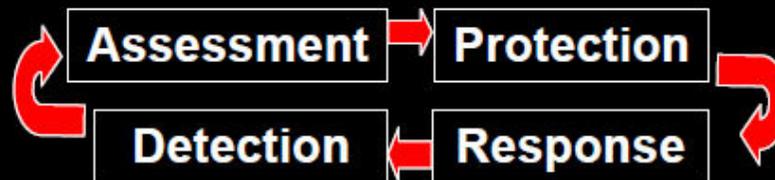
OFFICIAL STATISTICS

EXTERNAL/INTERNAL THREAT



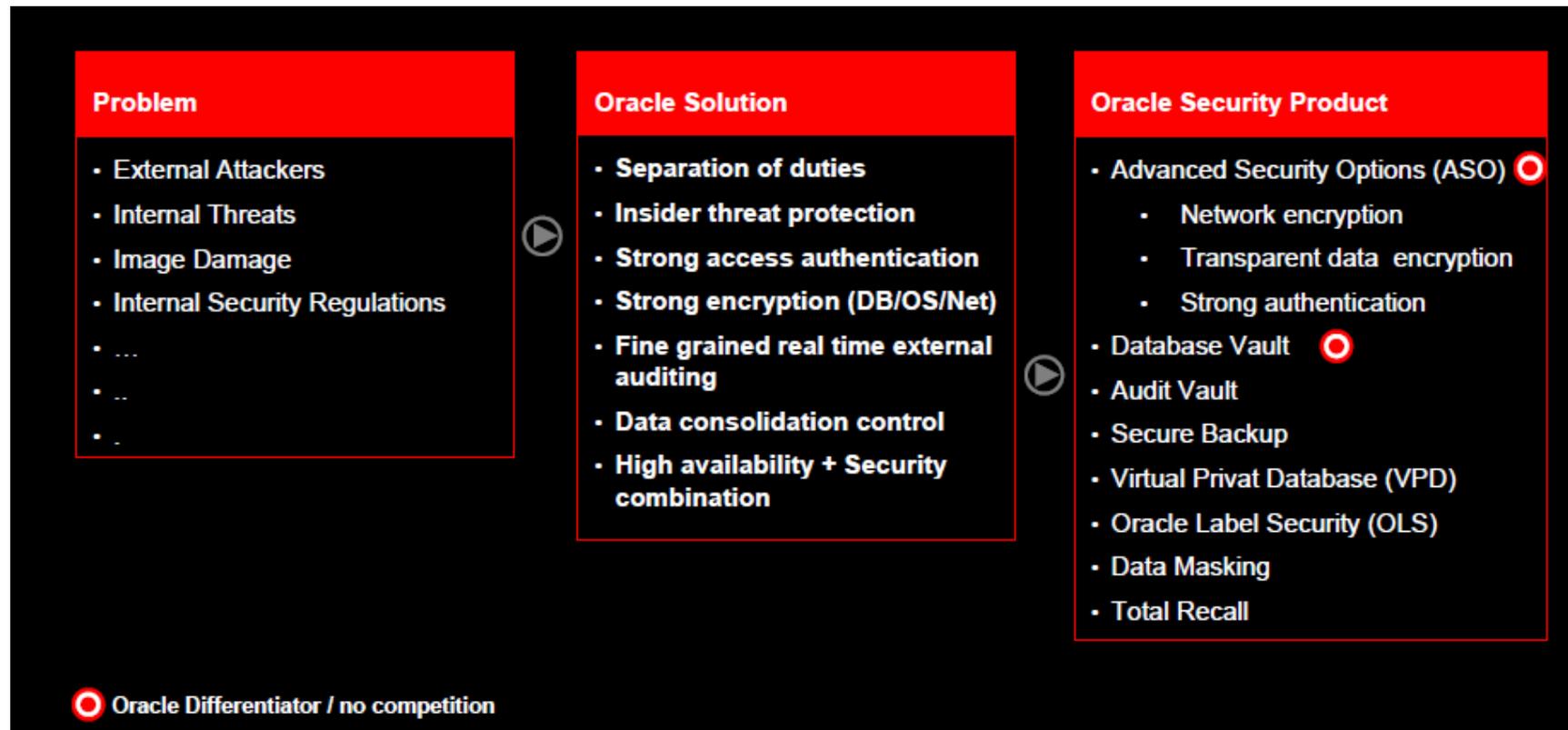
CONCLUSION

- 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

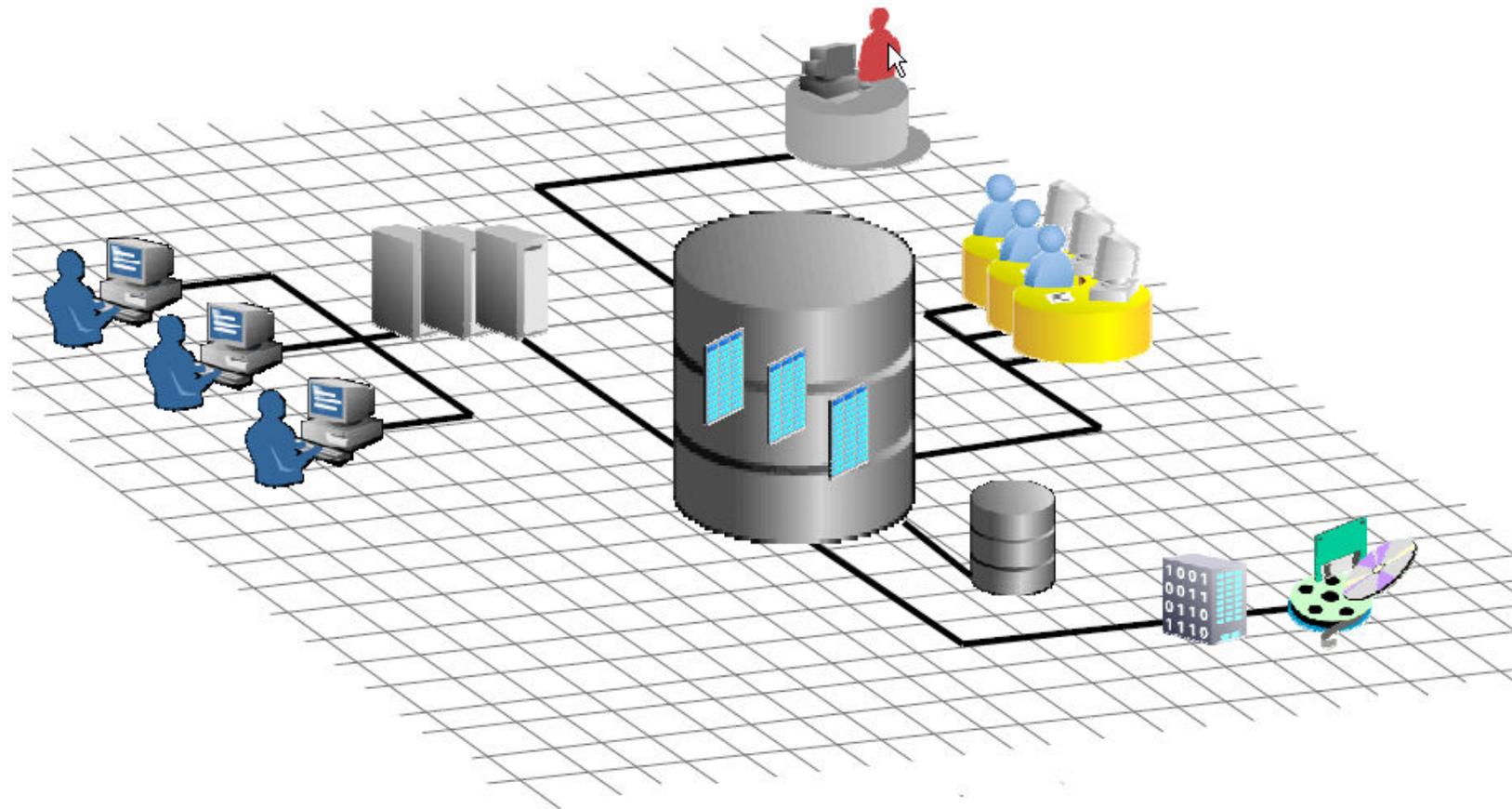
Oracle Security Solutions



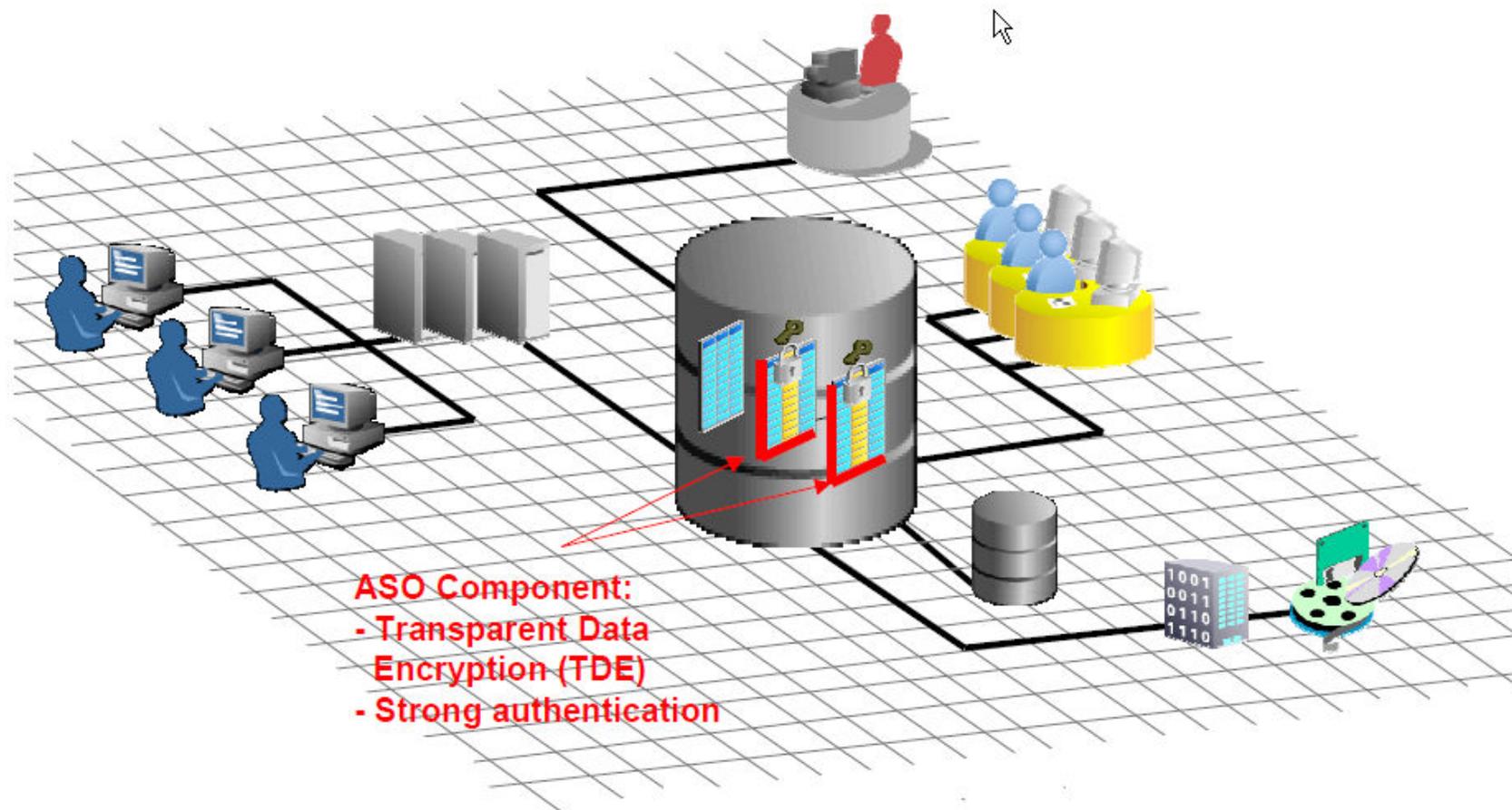
Oracle Security Components

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

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

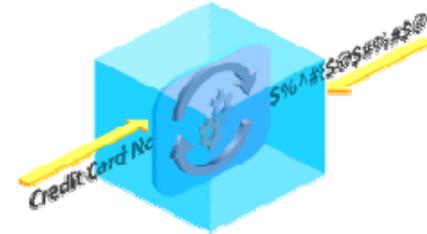
ID	AMEX Nr.	Expenses
01	83929843700	50.320
02	54220494833	29.872
03	00428274712	33.432

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

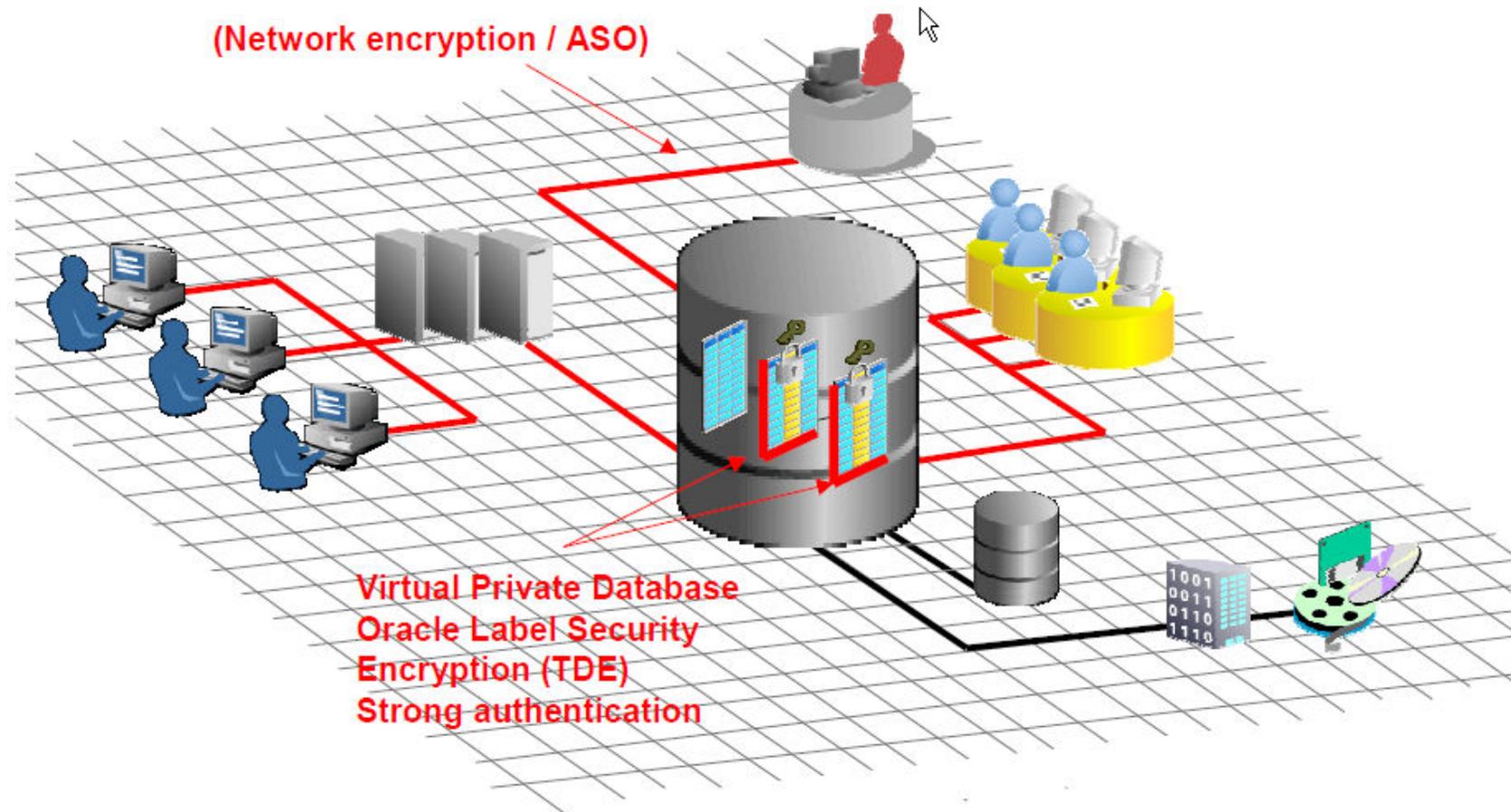
FY	Q1	Q2	Q3	Q4
04	1.3M	1.8M	4.9M	10.1M
05	2.2M	3.5M	6.5M	14.4M
06	3.0M	3.9M	6.7M	16.5M
07	3.8M	5.5M	12.2M	20.4M

TDE – Transparent Data Encryption

- 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)

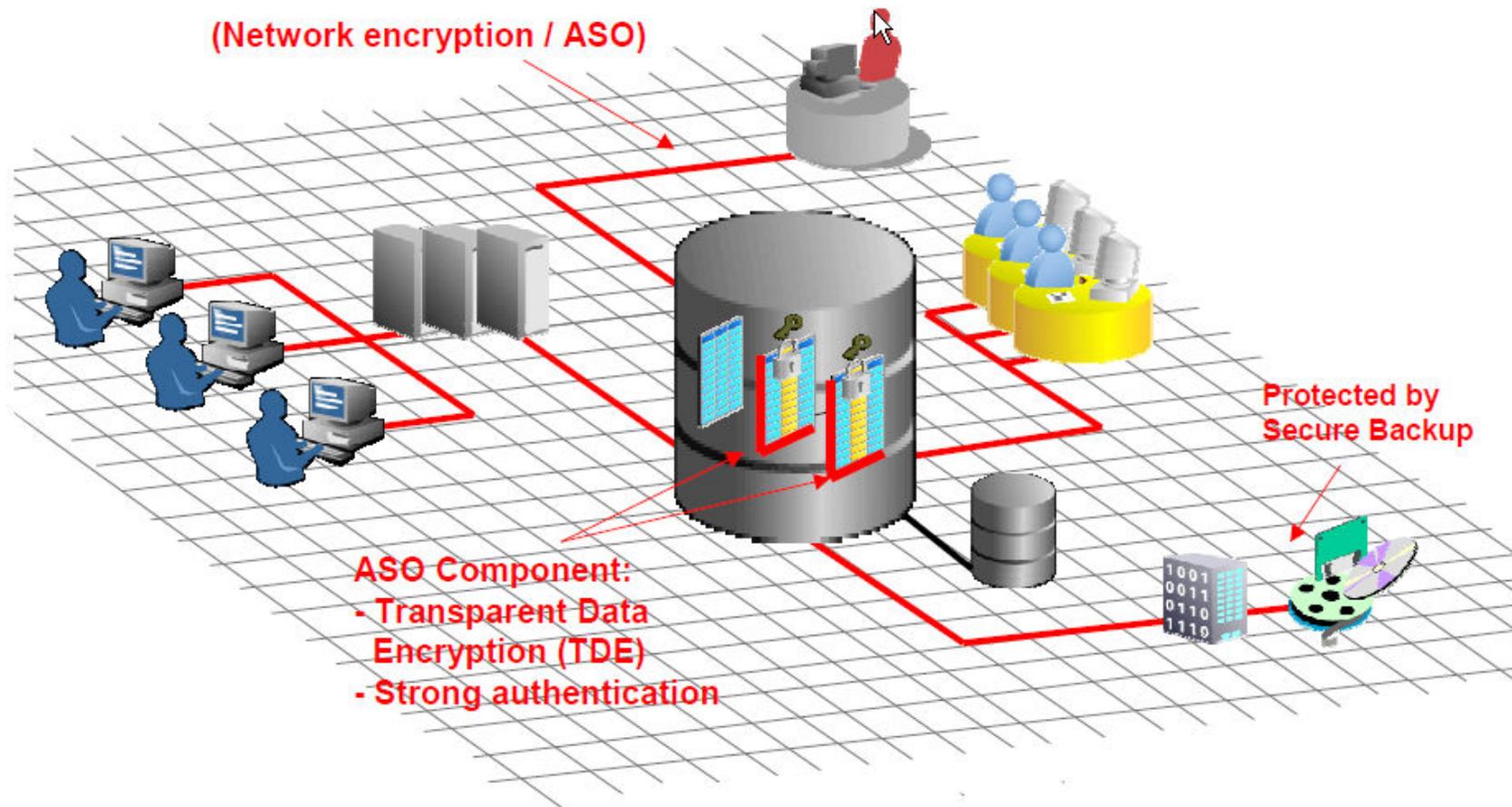
1. sqlnet.crypto_seed=„salkdjfaoiwjoiejlkjsjflksajuoiwjls“
2. sqlnet.encryption_client = required
3. sqlnet.encryption_types_client = (RC4_40)
4. sqlnet.crypto_checksum_client = requested
5. sqlnet.crypto_checksum_types_client = (MD5)

sqlnet.ora (Server)

1. sqlnet.crypto_seed=„salkdjfaoiwjoiejlkjsjflksajuoiwjls“
2. sqlnet.encryption_server = required
3. sqlnet.encryption_types_server = (RC4_40)
4. sqlnet.crypto_checksum_server = requested
5. sqlnet.crypto_checksum_types_server = (MD5)

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

SECURING BACKUP

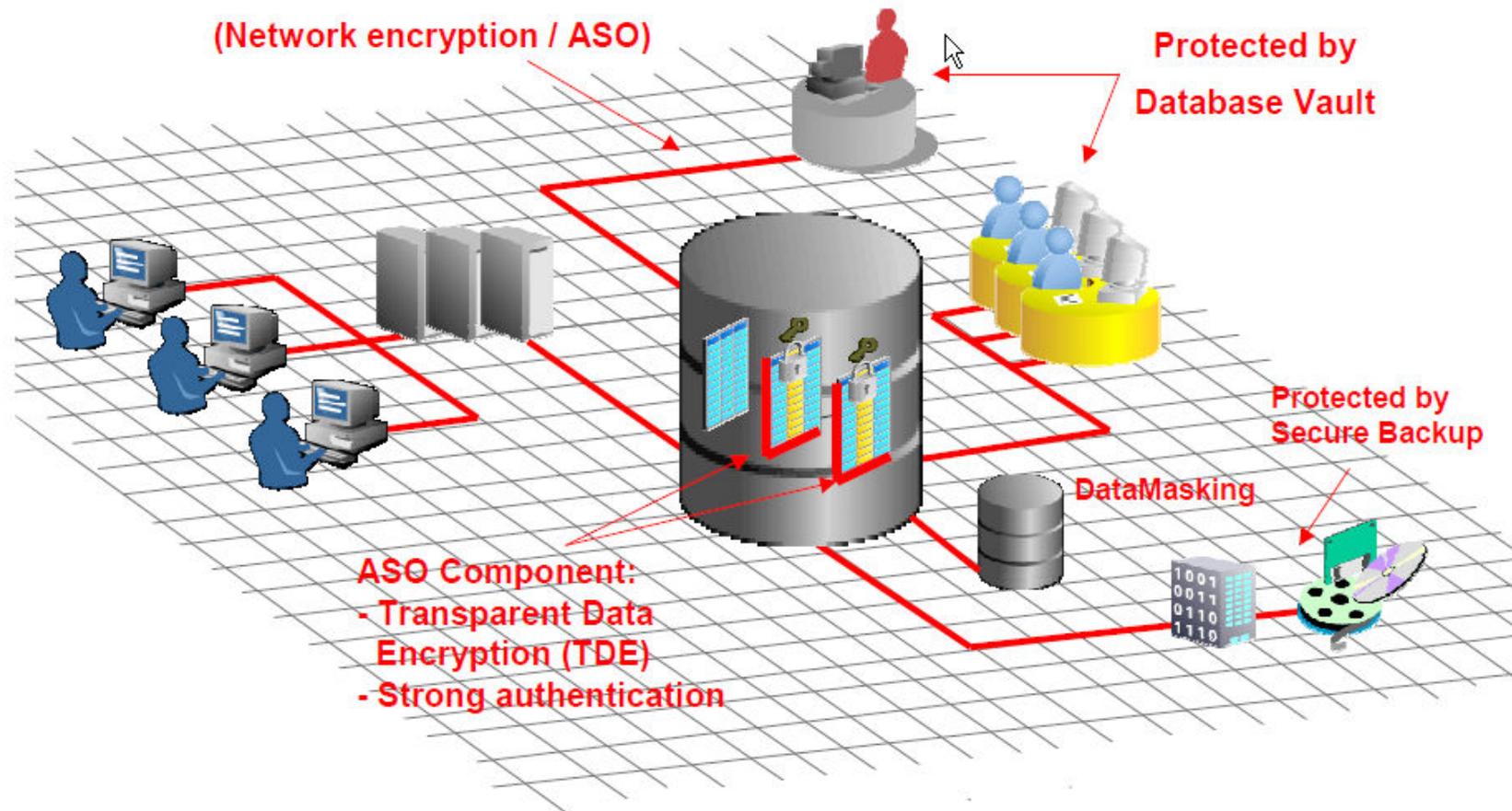


SECURING BACKUP

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



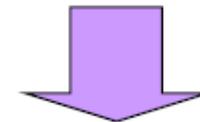
WHAT IS DATAMASKING?

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

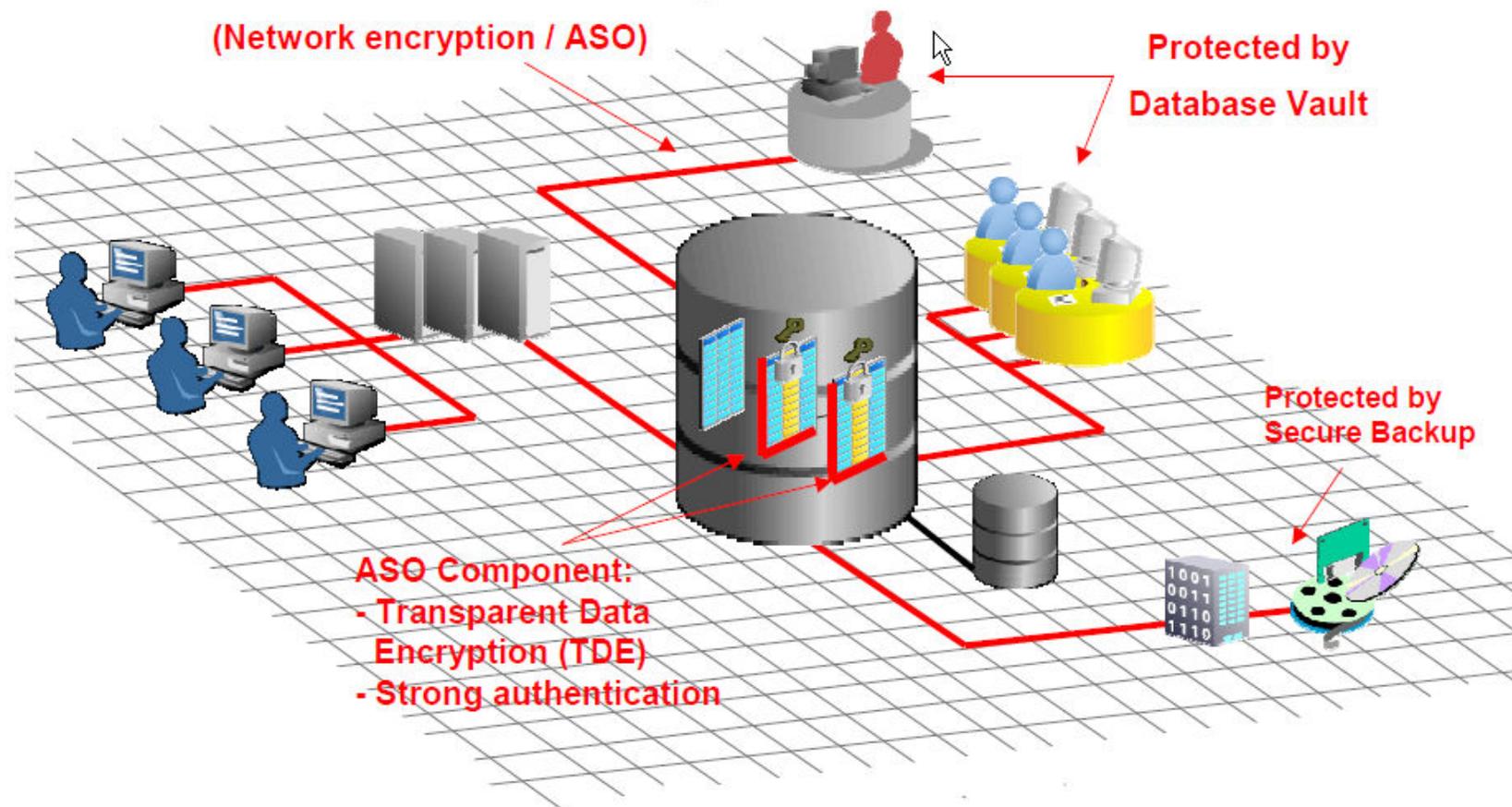


LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000
D'SOUZA	989-22-2403	80,000
FIORANO	093-44-3823	45,000



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

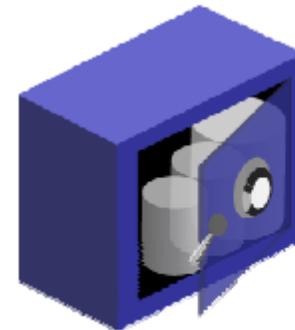
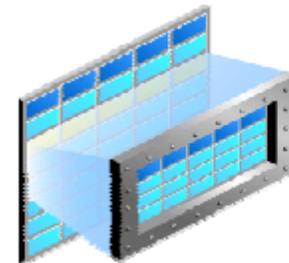
DATA VAULT HELP TO SOLVE:

- **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

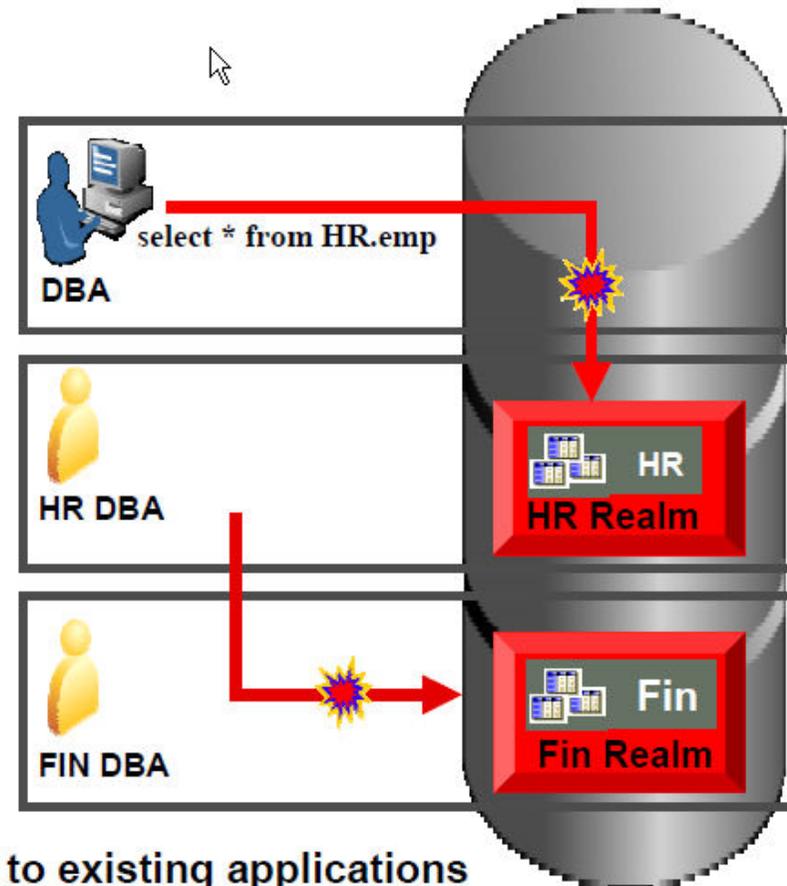
VPD and OLS restrict access at the row level, while Database Vault restricts access at the **object and **command** levels.**



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

Database Instance: orcl

[Administration](#) [Data Vault Reports](#) [General Security Reports](#) [Monitor](#)

Use this screen to run reports about potential Data Vault configuration issues and Data Vault audit events.

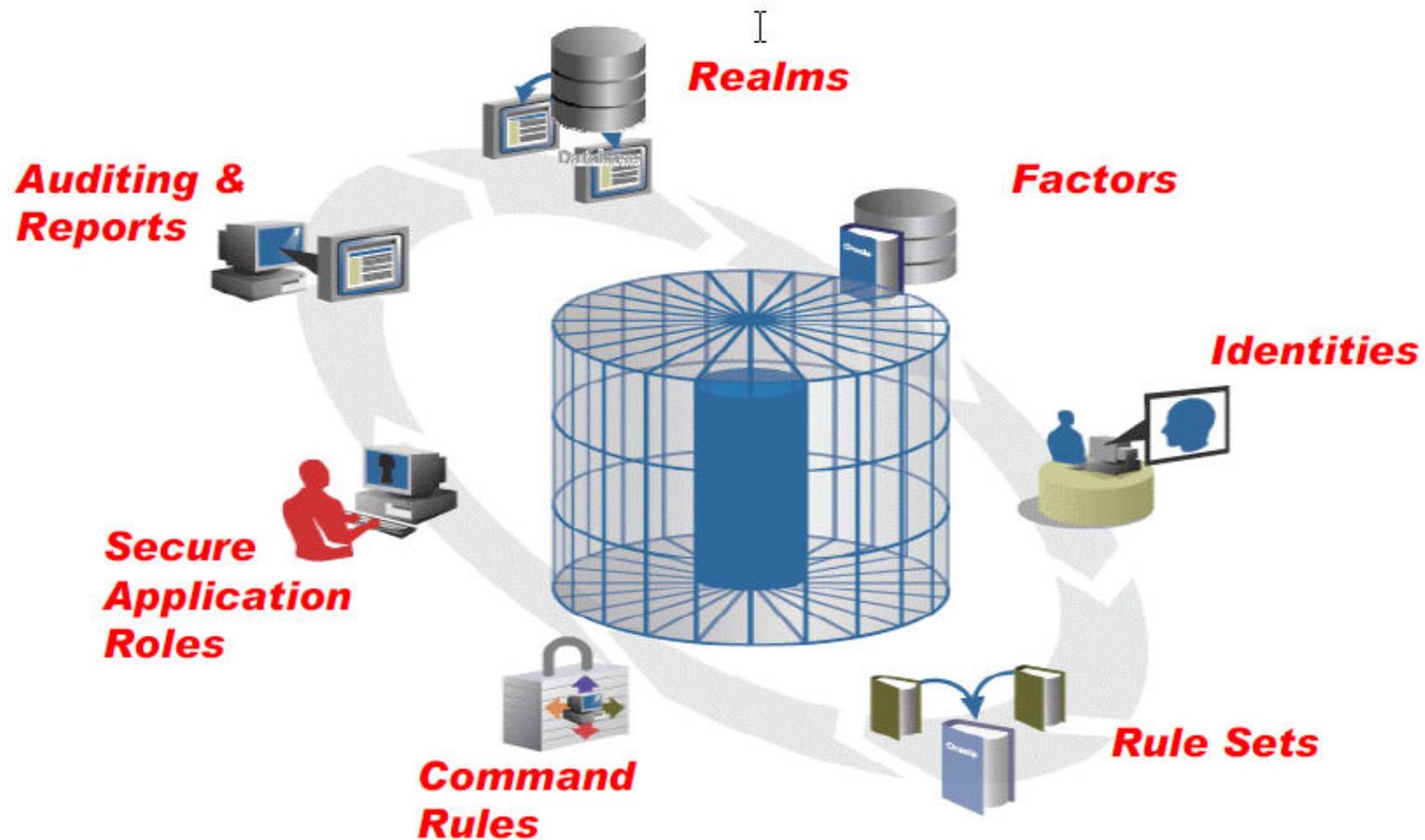
Run Report

[Expand All](#) | [Collapse All](#)

⊕ Reports

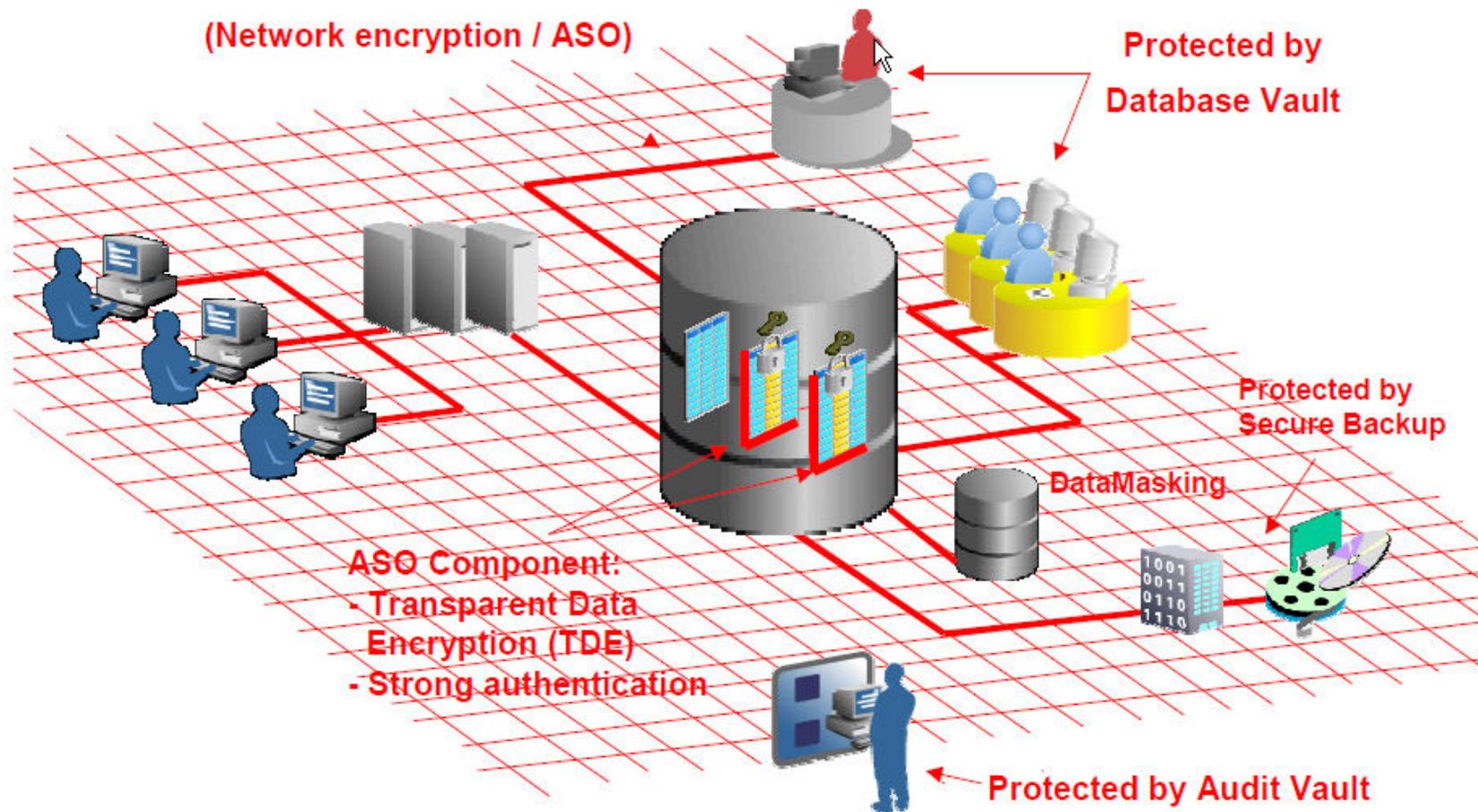
Select	Focus	Report Title
<input type="radio"/>		▼ Reports
<input type="radio"/>	⊕	▼ Data Vault Configuration Issues Reports
<input checked="" type="radio"/>		Command Rule Configuration Issues
<input type="radio"/>		Factor Configuration Issues
<input type="radio"/>		Factors Without Identities
<input type="radio"/>		Identity Configuration Issues
<input type="radio"/>		Realm Authorization Configuration Issues
<input type="radio"/>		Rule Set Configuration Issues
<input type="radio"/>		Secure Application Configuration Issues
<input type="radio"/>	⊕	▼ Data Vault Auditing
<input type="radio"/>		Realm Audit
<input type="radio"/>		Command Rule Audit
<input type="radio"/>		Factor Audit

DATA VAULT EXAMPLES



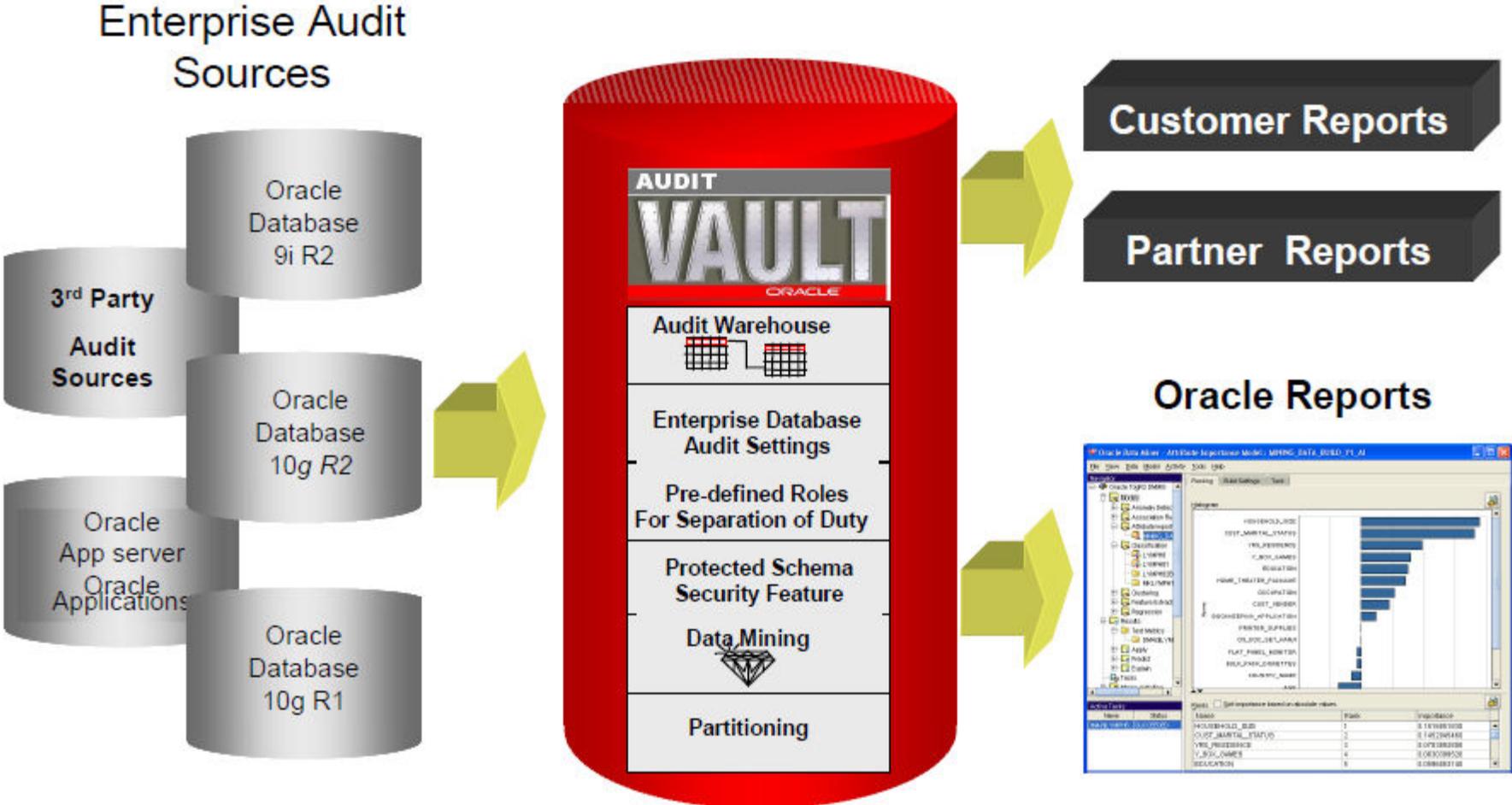
HIGHLY SECURED ENVIROMENTS

AUDIT VAULT



AUDIT VAULT EXAMPLES

Specialized Warehouse for Audit Data



AUDIT VAULT REPORTS

Who, What, When, Where

User	VSHAH	
OS User	oracle	
End User		
Terminal		ORCLDB
Host	oel4upd4.oracle.vm	HR ORACI F VM
Host	transaction	
Subr	SQL Bind	
Dom	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

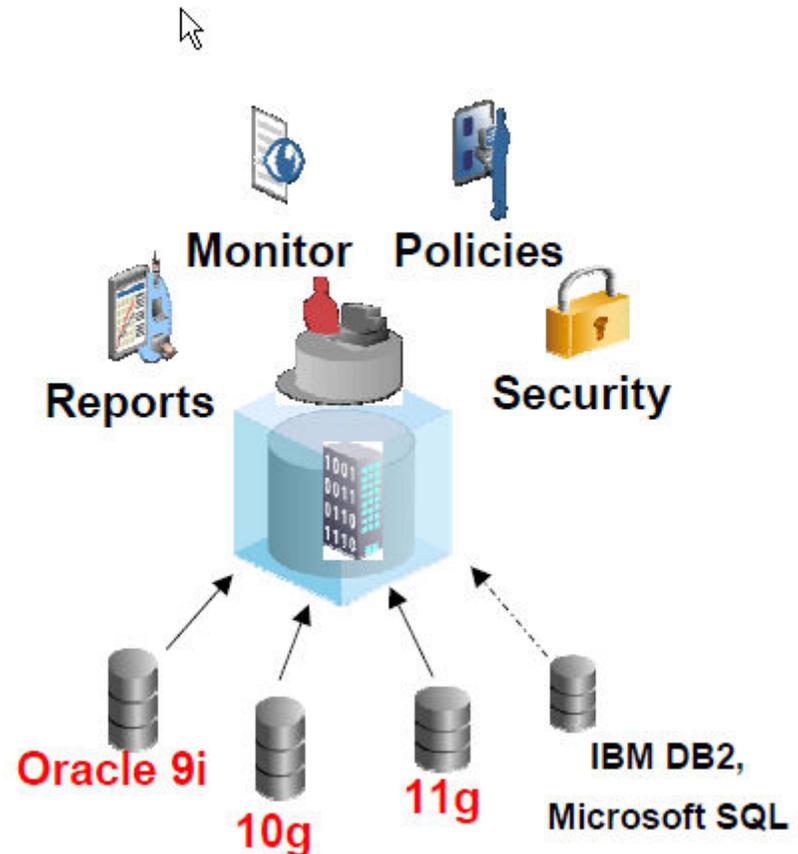
**Collect and Consolidate
Audit Data**

**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

Find Oracle ACEs

Search Display  ACE
 ACE Director

Name	Company	Location 	Expertise	Home Page
 Harshad Oak	Rightrix Solutions.	India	Java Tools & Frameworks	 Profile
 Murali Vallath	Summersky Enterprises	India	Database Management & Performance	Profile
 Padma Ramesh	Tata Consultancy Services	India	Middleware & SOA	Profile
 Parameswar Das	Tata Consultancy Services Ltd (TCS)	India	Middleware & SOA	Profile
 Srinivas Rao Polsani	Zensar Technologies	India	Middleware & SOA	Profile
 Yeddu Prasad	Wipro Technologies	India	Middleware & SOA	Profile

Oracle ACE PROGRAM

The Oracle ACE Program - Windows Internet Explorer

http://www.oracle.com/technology/community/oracle_ace/index.html

File Edit View Favorites Tools Help

Google oracle tom kytes Search Bookmarks Check Translate AutoFill oracle tom kytes Sign In

Ask Tom Home The Oracle ACE Program Oracle ACE Program - FAQ

ORACLE TECHNOLOGY NETWORK

(Sign In/Register for Account | Subscribe) Oracle Websites

secure search Technology Network

shortcuts GETTING STARTED DOWNLOADS DOCUMENTATION FORUMS ARTICLES SAMPLE CODE TUTORIALS

Printer View E-mail this page Bookmark



Oracle ACE THE ORACLE ACE PROGRAM

Oracle ACEs and Oracle ACE Directors are known for their strong credentials as Oracle community enthusiasts and advocates, with candidates nominated by anyone in the Oracle Technology and Applications communities. The baseline requirements are the same for both designations; however, Oracle ACE Directors work more closely and formally with Oracle in terms of their community activity. [Read the FAQ](#) for more details!

Look for the  (signifies ACE) and  (signifies ACE Director) on Oracle Web sites and discussion forums; it signifies "ACE-dom" for the designated name.

[Find an Oracle ACE](#) [Nominate an Oracle ACE](#)

Recent Technical Articles by Oracle ACEs

<ul style="list-style-type: none">Oracle Enterprise Manager Architecture for Very Large Sites (Porus Havewala)Twitter Meets Oracle: ORA_Tweet (Lewis Cunningham)Creating and Using Custom JCA Adapters (Ronald van Luttikhuisen)Guide to Advanced Linux Command Mastery: Resource Management (Arup Nanda)Oracle ADF Development Essentials (John Stegeman)Read More Technical Articles	<ul style="list-style-type: none">Return to Formsville (Chris Muir)Integrating Hyperion Essbase with Oracle Business Intelligence (Mark Rittman)Build a Google Talk Client Using Oracle ADF Faces Rich Client and the Active Data Service (Lucas Jellema)Introduction to Grails Development (Harshad Oak)Implementing Row-Level Security in Java Applications (Lonneke Dikmans)
---	---

Oracle ACE Bloggers

- [Bradley Brown](#) 
- [Andrew Clarke](#) 
- [Lewis Cunningham](#) 
- [François Degrelle](#) 
- [Lonneke Dikmans](#) 
- [Tim Hall](#) 
- [Bex Huff](#) 
- [Jason Jones](#) 
- [Steve Karam](#) 
- [Atul Kumar](#) 
- [Eric Marcoux](#) 
- [Harshad Oak](#) 
- [Mark Rittman](#) 
- [Husnu Sensor](#) 

[More...](#)

Top Forum Posters

- [Justin Cave](#) 
- [Nick Gasparotto](#) 
- [Andrew Clarke](#) 
- [Kamal Kishore](#) 

Oracle ACE PROGRAM 🎖️ 🏆

Oracle ACE Nominations - Windows Internet Explorer

http://www.oracle.com/technology/community/oracle_ace/nominations/index.html

File Edit View Favorites Tools Help

Google oracle tom kytes Search Bookmarks Check Translate AutoFill oracle tom kytes Sign In

Oracle ACE Nominations Oracle ACE Program - FAQ

ORACLE TECHNOLOGY NETWORK

(Sign In/Register for Account | Subscribe) Oracle Websites

secure search Technology Network

shortcuts GETTING STARTED DOWNLOADS DOCUMENTATION FORUMS ARTICLES SAMPLE CODE TUTORIALS

Printer View E-mail this page Bookmark

Oracle ACE THE ORACLE ACE PROGRAM - Qualifications and Nominations

The [Oracle ACE Program](#) is designed to recognize and reward Oracle customers for advocating Oracle Technology and Applications. Oracle ACE recipients are chosen based on their significant contributions to, and activity in, their respective community. The program currently has two levels: Oracle ACE and Oracle ACE Director.

For more information, read the [FAQ](#).

Oracle ACE Qualifications 🎖️

To qualify for the Oracle ACE award, candidates should meet as many of the following qualifications as possible.

- Technical proficiency
- Oracle-related blog
- Oracle discussion forum activity
- Published white paper(s) and/or article(s)
- Presentation experience
- Beta program participant
- Oracle user group member
- Oracle certification

Benefits of the program include:

- Promotion of Oracle ACEs as "official" experts on Oracle Web sites/at events
- Publication of articles and papers on OTN (with compensation)
- Speaking opportunities at Oracle and/or 3rd party events

Oracle ACE Nomination Process

Anyone in the Oracle community is eligible to nominate a potential Oracle ACE award; only non-employees may receive them. As nominations are received the nomination committee will review them within a 2-week period. Award recipients will be selected based on their qualifications. Oracle reserves the right to final judgment on all nominations.

📄 [Download Oracle ACE Nomination Form](#)

PRODUCTS
Database
Middleware
Developer Tools
Enterprise Management
Applications Technology
Products A-Z

TECHNOLOGIES
BI & Data Warehousing
Embedded
Java
Linux
.NET
PHP
Security
Technologies A-Z

ARCHITECTURE
Enterprise Architecture
Enterprise 2.0
Grid
Service-Oriented Architecture
Virtualization

COMMUNITY
Join OTN
Oracle ACEs
Oracle Mix
Oracle Wiki
Blogs
Podcasts
Events
Newsletters
Oracle Magazine
Oracle Books
Certification
User Groups

Questions?



dbisTM DATABASE
INTEGRATED
SOLUTIONS

Thank you !



dbisTM DATABASE
INTEGRATED
SOLUTIONS