NSS Enriching Knowledge for Information and Communication Technology Curriculum Series - (2) ICT Development and Applications in Hong Kong: Database Security & ICT Trend

10 Jan 2008

Oracle Security Briefing

Hong Kong

Jan 10, 2008

ORACLE

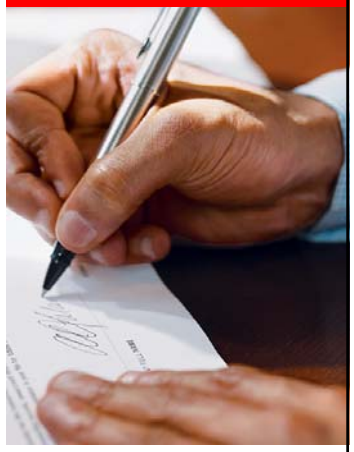
Unlock Potential, Lock Out Risk: Securing Businesses for Today and Tomorrow

Paul Lee
Senior Director, Database Sales Consulting
Oracle Greater China

Security Inside Out

1996 to 2007: Threats Intensify; Band-Aid Solutions

1996	2007
• Amateur hackers	• Organized crime
• Web site defacement	• IP theft
• Viruses	• Identity theft
• Infrequent attacks	• Constant threat



SMEs are as vulnerable as large enterprises.

Did you know …

“By 2007, 40% of new enterprise security spending will be directed toward data security issues, not perimeter security”
—Gartner, August 2005, Organizations Must Employ Effective Data Security Strategies

“The most prevalent attack style, responsible for 39% of data thefts, was authorized users exploiting their privileges.”
—Forrester, April 2006, Aligning Data Protection Priorities With Risks

SECURITY

Some Recent Security Breaches in the News …

The New York Times

Data Breach at [redacted]

By THE ASSOCIATED PRESS
Published: March 24, 2006

BOSTON, March 23 (AP) — A laptop computer belonging to [redacted] and containing sensitive data on about 196,000 retirement-account customers was stolen last week, the company said.

The company, t
Thursday that th
[redacted] pensi
offering them fre

AHN All Headline News

Content Services | Client Login

TOP STORIES | BUSINESS | ENTERTAINMENT | HEALTH | OFFBEAT | POLITICS

Social Security Numbers For 13,000 Employees Stolen

June 19, 2006 12:30 p.m. EST

Richard Rittierodt - All Headline News Staff Writer

Washington DC
the social secur
and retirees last

WSJ.com THE WALL STREET JOURNAL. ONLINE

July 7, 2006 1:40 p.m. EDT

[redacted] Discloses Data Breach

By JAIME LEVY PESSIN
July 7, 2006 1:40 p.m.

NEW YORK -- An i
Inc. affected approxi
person familiar with th

[redacted] wouldn't confirm
November 2005 and
of public companies"
companies.

WSJ.com THE WALL STREET JOURNAL. ONLINE

June 6, 2006

Stolen Laptop Puts [redacted] com Users' Personal Data at Risk

REUTERS NEWS SERVICE
June 6, 2006

NEW YORK --
information expo
of [redacted]

FOX NEWS .com

E-MAIL STORY | PRINTER FRIENDLY | FOXFAN CENTRAL

FOXNEWS.COM HOME > TECHNOLOGY

File Server With 970,000 Names Stolen From Insurance Giant

Thursday, June 22, 2006
By Matt Hines

eWEEK.COM

Insurance provider [redacted] has confirmed the theft of a file server and other hardware that held the personal information of approximately 970,000 potential customers.

CNNMoney.com

GET QUOTES | SYMBOL LOOK-UP | SEARCH | Entire Site

HOME | NEWS | MARKETS | TECHNOLOGY | JOBS & ECONOMY | PERSONAL FINANCE | LIFESTYLE | REAL ESTATE

NEWS > Fortune 500

SAVE | EMAIL | PRINT | RSS

Bank security breach may be biggest yet

Account info at [redacted] sold by employees; more arrests expected, N.J. police say.

Some Recent Security Breaches in the News …

贵州省惟一全国地方重点新闻网站 金黔在线 贵州日报报业集团主办

首 页 | 新 闻 | 旅 游 | 美 食 | 健 康 | 伊 人 | 娱 乐 | 汽 车 | 黔 景 | 食 府 | 科 技 | 社 区 | 闪 讯 | 彩 信 | 股 市 | 游 戏 | 贵州日报 | 贵州都市报 | 贵州商报 | 西部开发报 | 经济信息时报 | 天下文摘 | 六盘水日报 | 中国贵州 | 贵州民族报 | 新报 | 新闻

金黔科技 | 综合新闻 | 品科论技 | 贵州信息化 | 游戏动态 | 游戏评测 | 游戏杂谈 | COSPLAY | 最新软件 | 最新游戏

专业、准确、及时报道贵州科

首页>>金黔科技>>品科论技>>本页

黑客偷袭网银账户

http://www.gog.com.cn 2006年08月30日 11时56分13秒 金黔在线 『字号：大 中 小』

专家提醒：要提防登陆虚假银行，尽量使用银行提供的安全措施

日前，市区的陈小姐不小心登陆了不法分子伪造的虚假银行网址，损失了一笔数目

子站：首页 | 资讯中心 | 通信产业 • 手机 | 技术应用 | 商业采购 | 中国信息化 | 人物报道 | ezIT |

服务：情报中心 | 赛迪网校 | 报价中心 | 嘉宾聊天 | 直播 | 专题 | 短信 | 电子杂志 | 调查 | IT博客 | 社区 | 技

赛迪网资讯中心 CCID news.ccidnet.com 首页 | 互联网 | 通信 | 业界 | 财经 | 人物 | 数码手机 | 软件 | 硬件 | 请输入关键字搜索 本站 百度 Google • 平板电视

当前页面位置：首页 >>资讯中心>>即时新闻>>文章

对抗内部网络威胁

作者:陈思 2005年10月18日 16:35 来源:赛迪网-中国计算机报

[发表评论] [字体：大 中 小] [打印] [短信快递] [进入博客] [进入论坛] [推荐给朋友]

【赛迪网讯】网络环境的复杂性、多变性，以及信息系统的脆弱性，决定了网络安全威胁的客观存在。据IDC报告，70%的安全损失是由企业内部原因造成的，也就是说企业中不当的资源利用及员工上网行为往往是“罪魁”，间谍软件、恶意程序、计算机病毒、端对端文档分享等不当的上网行为，导致了企业机密资料被窃，网络资源的浪

HC360慧聪网 企业管理

首页 | 产经 | 交易市场 | 搜索 | 专题 | 人才 | 论坛 | 商务 | 管理

战略 | 运作 | 营销 | 人力 | 领导力 | 财务 | 信息化 | 工具箱

铃声下载 ♪希望 ♪猪之歌 ♪丁香花 ♪快乐崇拜 ♪两只蝴蝶 ♪不得不爱 ♪美丽的神话 ♪你到底爱谁 ♪童话 ♪啥啊啊 ♪欧若拉 ♪六月的雨 ♪想唱就唱 ♪不想长大 ♪一万个理由 ♪寂寞沙洲冷 ♪红颜 ♪逍遥呗 ♪上海滩 ♪爱海滔滔 ♪爸爸妈妈 ♪光辉岁月 ♪老鼠爱大米 ♪再见北极雪

我要找 输入关键字 行业资讯 搜索 寻址 如何找

• 平价眼镜, 赚钱风暴 • 开纳米服装店赚大钱 • 万元开店 低价风暴 • 特色餐饮赚大钱
• 巧克力浓情馆火爆招商 • 十年练摊掘回了第一桶金 • 开家庆典产品出租店 • 2000元投资月赚20万

您目前的位置： 慧聪网首页 > 企业管理 > 财务管理

CFO担忧 信息失窃威胁日渐显现

http://www.hc360.com 2005年9月19日8时25分 慧聪网

如今令人担忧的是个人信息失窃和资料外泄，遗憾的是，一份最新的CFO IT调查结果显示，CFO们也许并未充分关注这一日渐显现的威胁。窃取个人信息被称为美国目前增长最快的白领犯罪，它不仅是消费者和金融机构面临的一个问题，而且对任何使用电脑和互联网的企业都构成了实实在在的威胁。

Chinabyte首页 | 新闻 | 评论 | 通信 | 互联网 | 专栏 | CB博客 | 信息化 | 企业软件 | 解决方案 | 商用系统

天极 ChinaByte.com

DELL 网上订购价 ¥6,999 免费4重升级 采用英特尔®迅驰™双核移动计算技术 14.1"宽屏 800-858-0410 intel Centrino Duo 双核无限可能

北京 上海 重庆 成都 Yesky.com

您现在的位置： 天极ChinaByte> 企业软件 ¥4999获双内核奔腾®D处理器、19英

客户信息频频丢失 信息化呼唤安全

作者：张杰 出处：中国计算机用户 [2005-06-23 11:23]

摘要：客户是企业生存之本，是一句响亮的口号。如果客户信息频频丢失，企业就失去了立身之本。今天，信息就是资产的观念需要不断强化

DELL Dimension™5150 800-858-0410 网上订购价 ¥4,999 免费升级至19"液晶显示器

客户是企业生存之本，是一句响亮的口号。如果客户信息频频丢失，企业就失去了立身之本。今天，信息就是资产的观念需要不断强化。

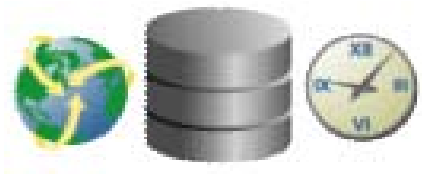
HongKong Security Landscape

- Exponential Needs
  - Risks with fast-growing online transactions (telco, banking, online gaming, etc)
  - Geographically diverse operations need more security
- Conflicting Priorities
  - Security concerns mostly on external IT threats
  - Internal security treated as an after-thought

Major Security Considerations

- Insider Threat – Intellectual Property Theft
- Adopting Information Security Best Practices
- Securing Consolidated Infrastructures

“Insider Threat” : Solution



Control Access to Data

Limitation of Privileges

Adopt Security Best Practices

Separation of Duties

Realms of Responsibility

Regular Auditing & Reporting

Pre-defined Reports

IT Consolidation and Security

- Infrastructure consolidation keeps costs down by
  - Keeping pace with your growth
  - Reducing complexity
  - Increasing business agility
- But creates security concerns, due to
  - Common database
  - Information access

Addressing Security Challenges of Consolidated IT Infrastructure

Separation of duties

Protection of sensitive data

Key Drivers for Data Security

Regulatory Compliance

- Sarbanes-Oxley (SOX), Payment Card Industry (PCI), HIPAA, GLBA, …
- Privacy Directives: EU, CA SB 1386….
- Adequate IT controls: COSO/COBIT
  - Separation of duty, Proof of compliance, Risk Assessment and Monitoring

Insider Threats

- Large percentage of threats go undetected
- Outsourcing and off-shoring trend
- Customers want to monitor insider/DBA

Top 5 Enterprise Security Technologies Sought

RSA Security Conference San Francisco, California USA - Feb 2007

- ✓ Controlling Privileged Users
- ✓ Data Encryption
- ✓ Monitoring Database Activity
- ✓ Configuration Scanning / Vulnerability Assessment
- ✓ Data Masking

Oracle's Answers to Security Challenges

Challenges	Solutions	Oracle's Answers
Insider Threat	Control Access to Data Limitation of Privileges	**Oracle Database Vault/ Transparent Data Encryption ***
Adopt Security Best Practices	Realms of responsibility Pre-defined reports	**Oracle Database Vault**
Infrastructure Consolidation	Separation of duties Protection of Sensitive Data	**Oracle Database Vault/ Transparent Data Encryption ***

More …

ORACLE DATABASE 10g

ORACLE DATABASE 11g

* Either or both products can be used depending on business need

Oracle's Security DNA

- From the start, built with security in mind
- Non-stop security firsts
  - First Trusted Database – 1990
  - First Network Encryption – 1995
  - First Biometric Authentication – 1996
  - First Data at Rest Encryption – 1998
  - First Super User Access Restrictions – 2006
- Independent security evaluations – 21. No one has more!
- Always a generation ahead in security

Oracle Database Security

30 years of Innovation

Oracle Audit Vault (Beta)

Oracle Database Vault

DB Security Evaluation #19

Transparent Data Encryption

EM Configuration Scanning

Fine Grained Auditing (9i)

Secure application roles

Client Identifier / Identity propagation

Oracle Label Security (2000)

Proxy authentication

Enterprise User Security

Global roles

Virtual Private Database (8i)

Database Encryption API

Strong authentication (PKI, Kerberos, RADIUS)

Native Network Encryption (Oracle7)

Database Auditing

1977 Government customer

2007

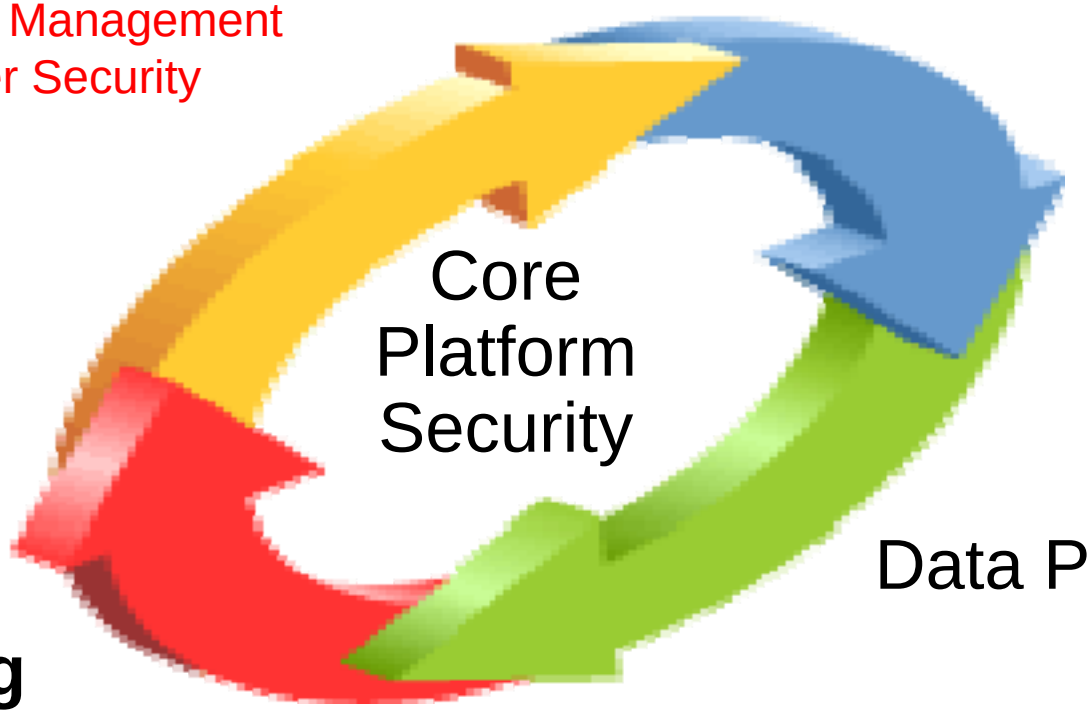
ORACLE DATABASE 11g

Data Security: Oracle Products

Access Control

User Management

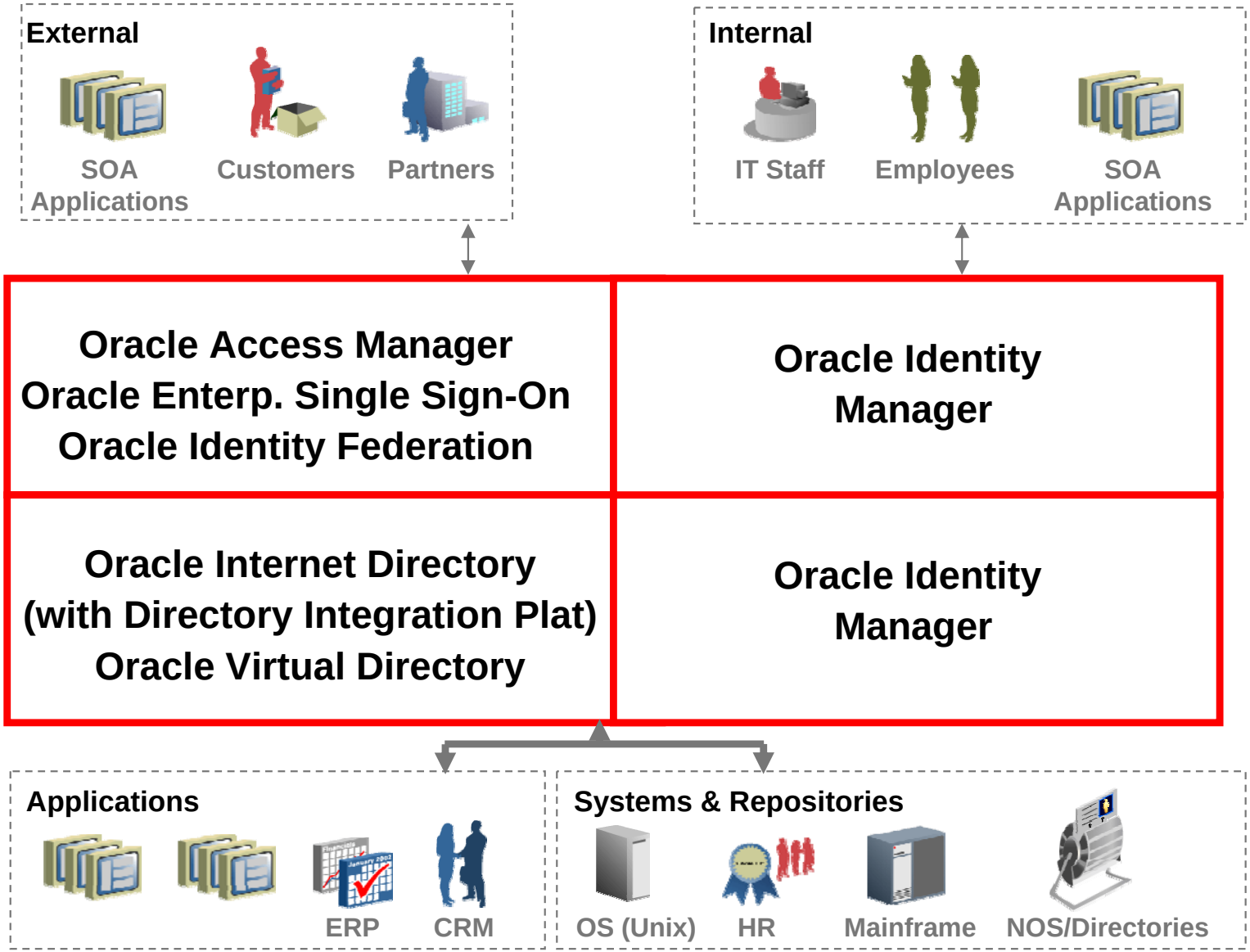
- Oracle Identity Management
- Enterprise User Security



Data Protection

Monitoring

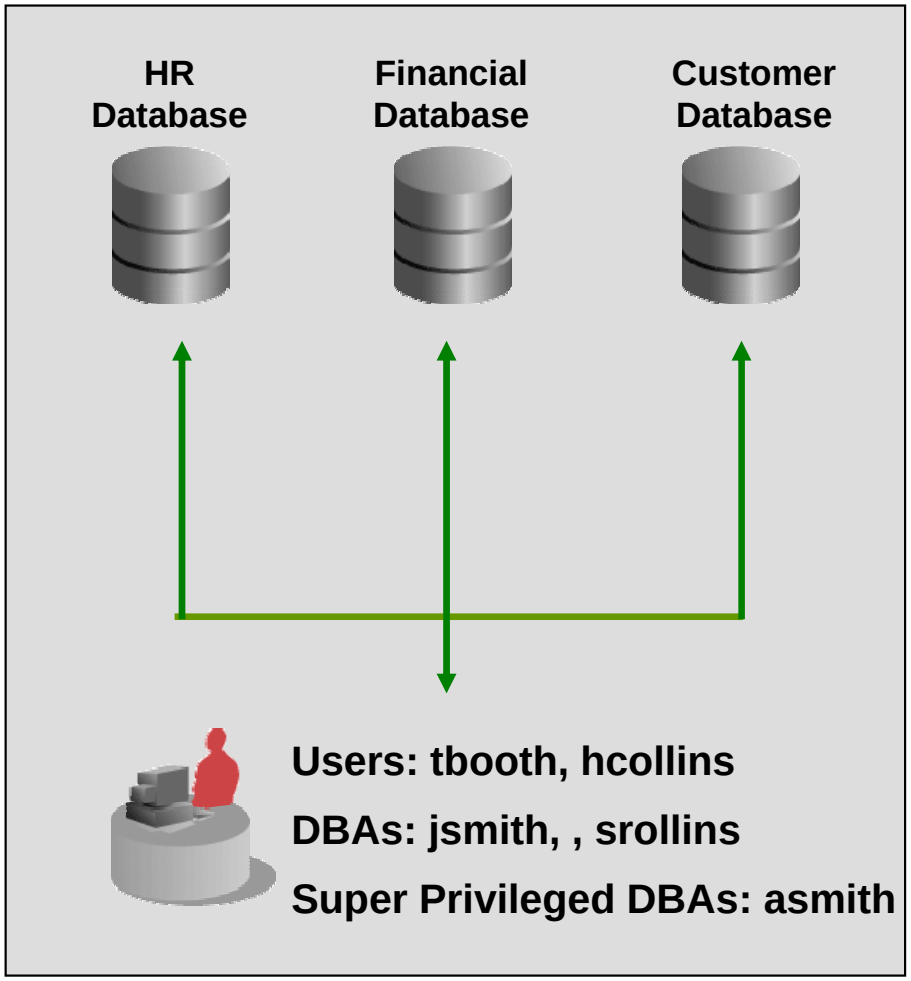
Oracle Identity Management



Enterprise User Security

Centralized Database Account Management

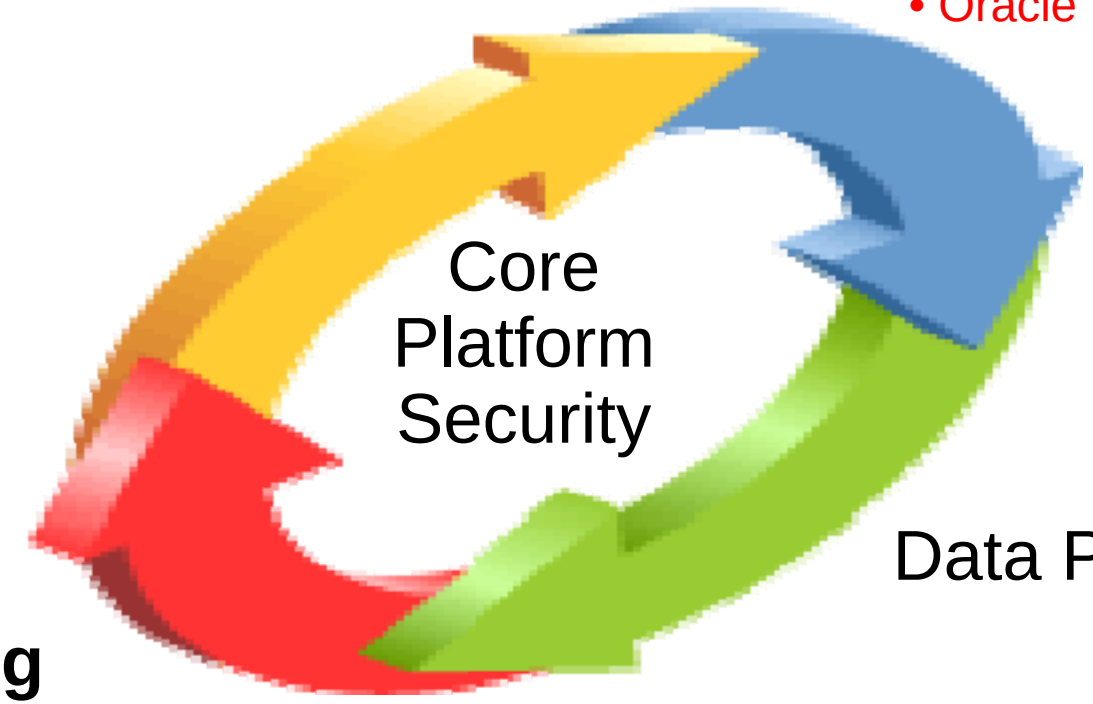
- Centralized User Management
  - Accounts and roles managed in Identity Management (8i)
  - Manage super-privileged DBAs across databases ORACLE DATABASE 11g
- SYSDBA Strong Authentication
  - PKI, Kerberos ORACLE DATABASE 11g
- Enterprise Manager
  - Enterprise Manager integration replaces Enterprise Security Manager ORACLE DATABASE 11g



Data Security: Oracle Products

User Management

Access Control
- Oracle Database Vault
- Oracle Label Security



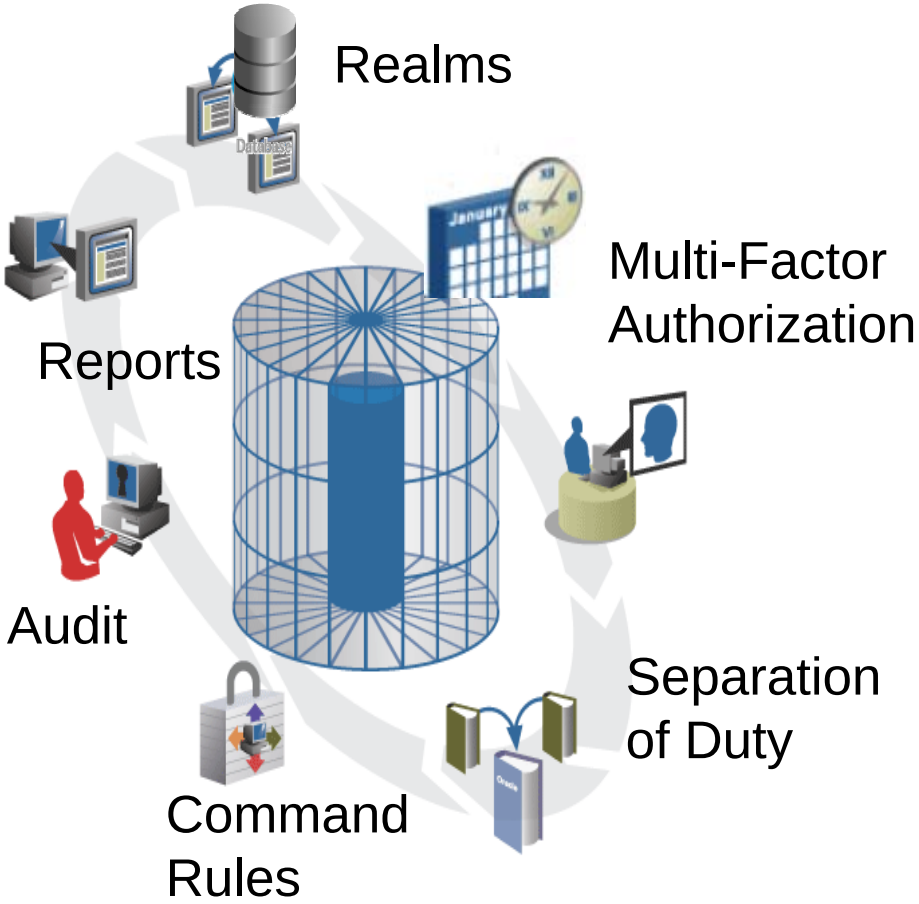
Data Protection

Monitoring

Oracle Database Vault

Mitigate Internal Threat and Enforce Compliance

- Controls on privileged users
  - Restrict DBA access to application data
  - Provide Separation of Duty
  - Security for database and information consolidation
- Enforce data access security policies
  - Control who, when, where and how is data accessed
  - Make decision based on IP address, time, auth…
- Enterprise Edition Security Option
- Supports Oracle9iR2+



Oracle Database Vault

Control Access To Data, Enforce Separation of Privileges, Automate Reports On Data Access

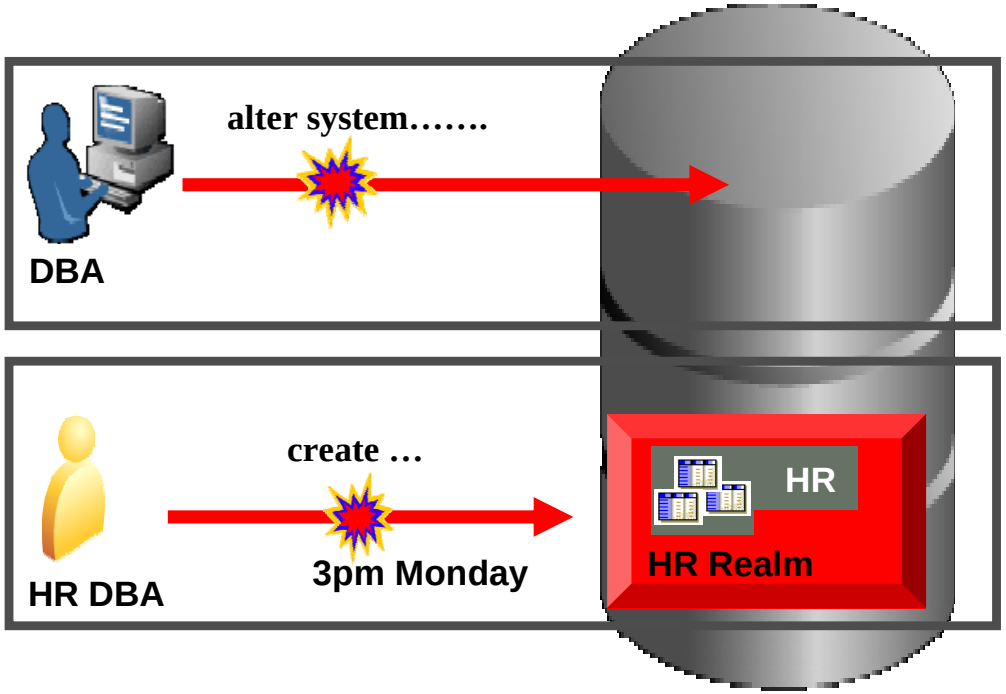
- Prevents the DBA from getting at Application Data
- Addresses key concerns for “insider threat” and separation of duty - automating compliance controls

- **Database DBA attempts remote “*alter system*”**

  Rule based on IP Address blocks action

- **HR DBA performs unauthorized actions during production**

  Rule based on Date and Time blocks action



Oracle Database Vault

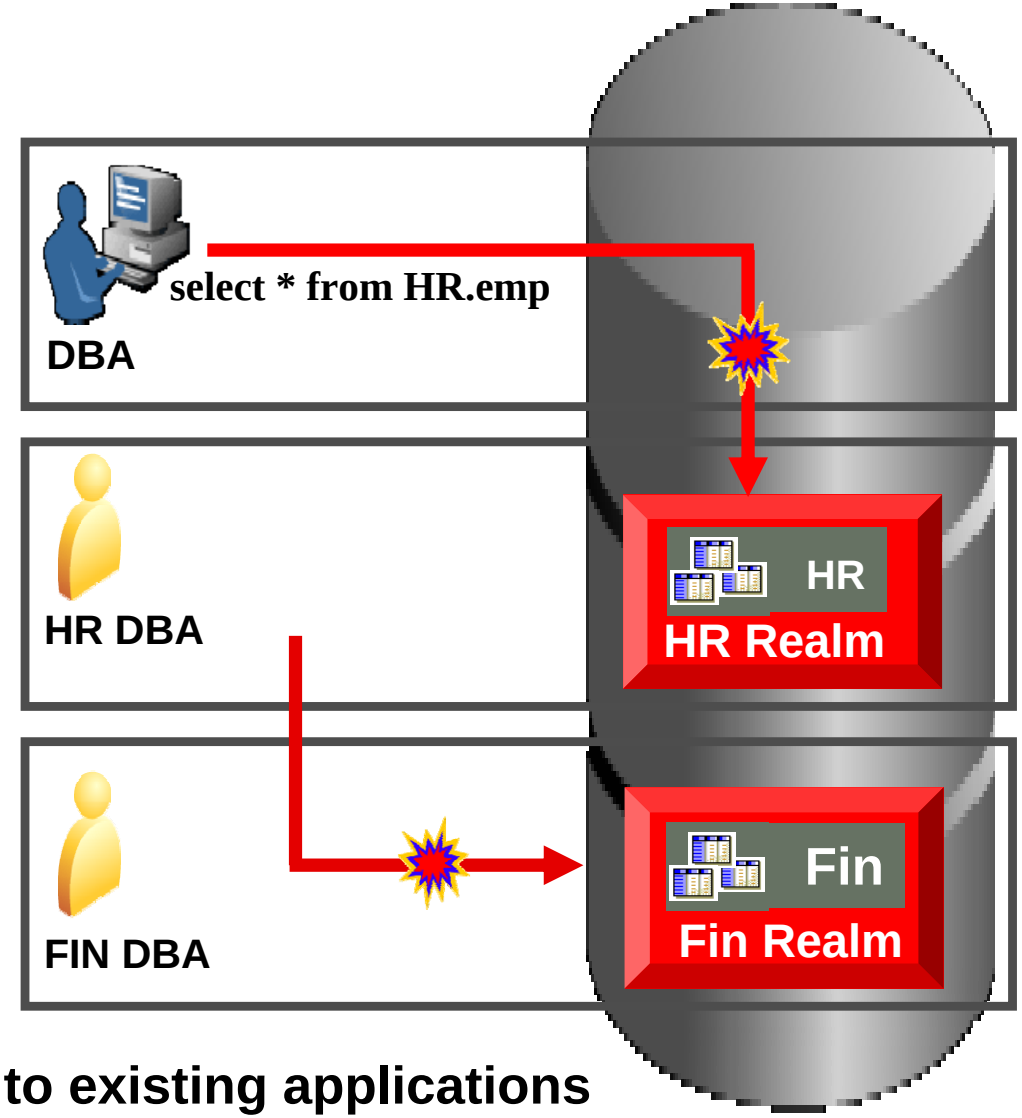
Realms

- **Database DBA views HR data**

  Compliance and protection from insiders

- **HR DBA views Fin. data**

  Eliminates security risks from server consolidation

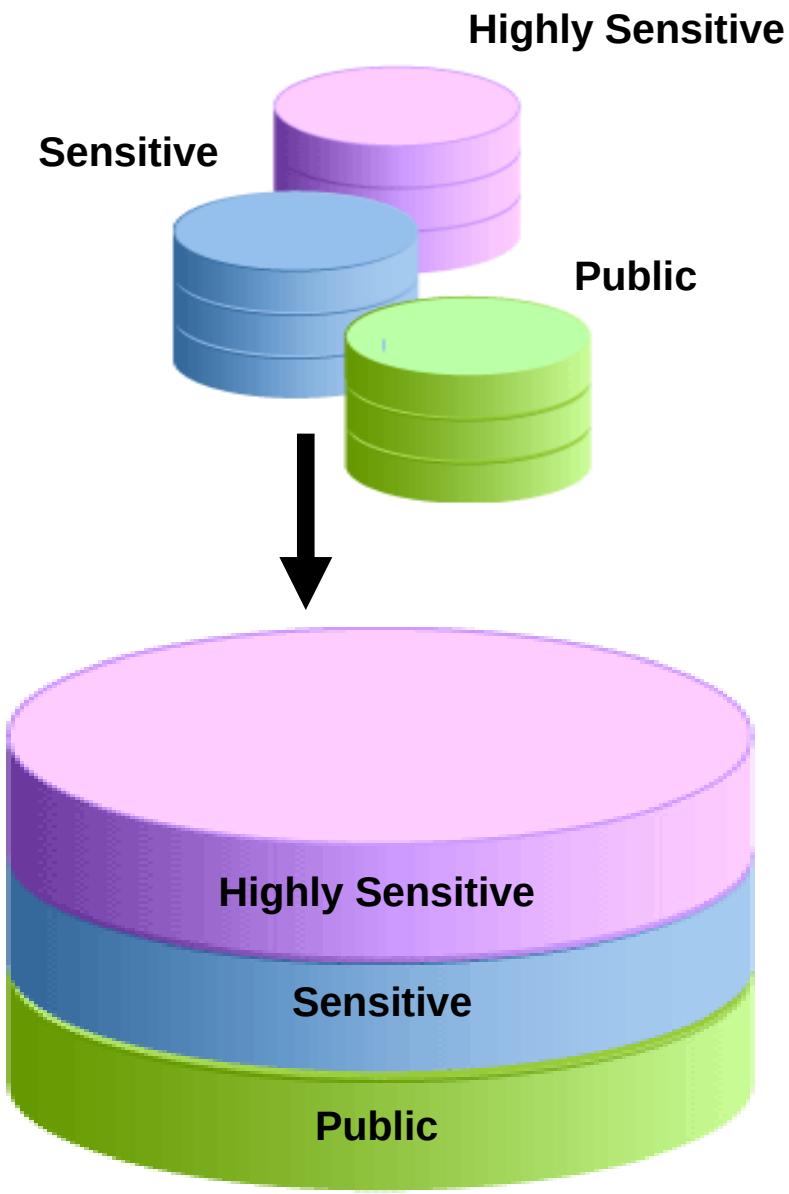


Realms can be easily applied to existing applications with minimal performance impact

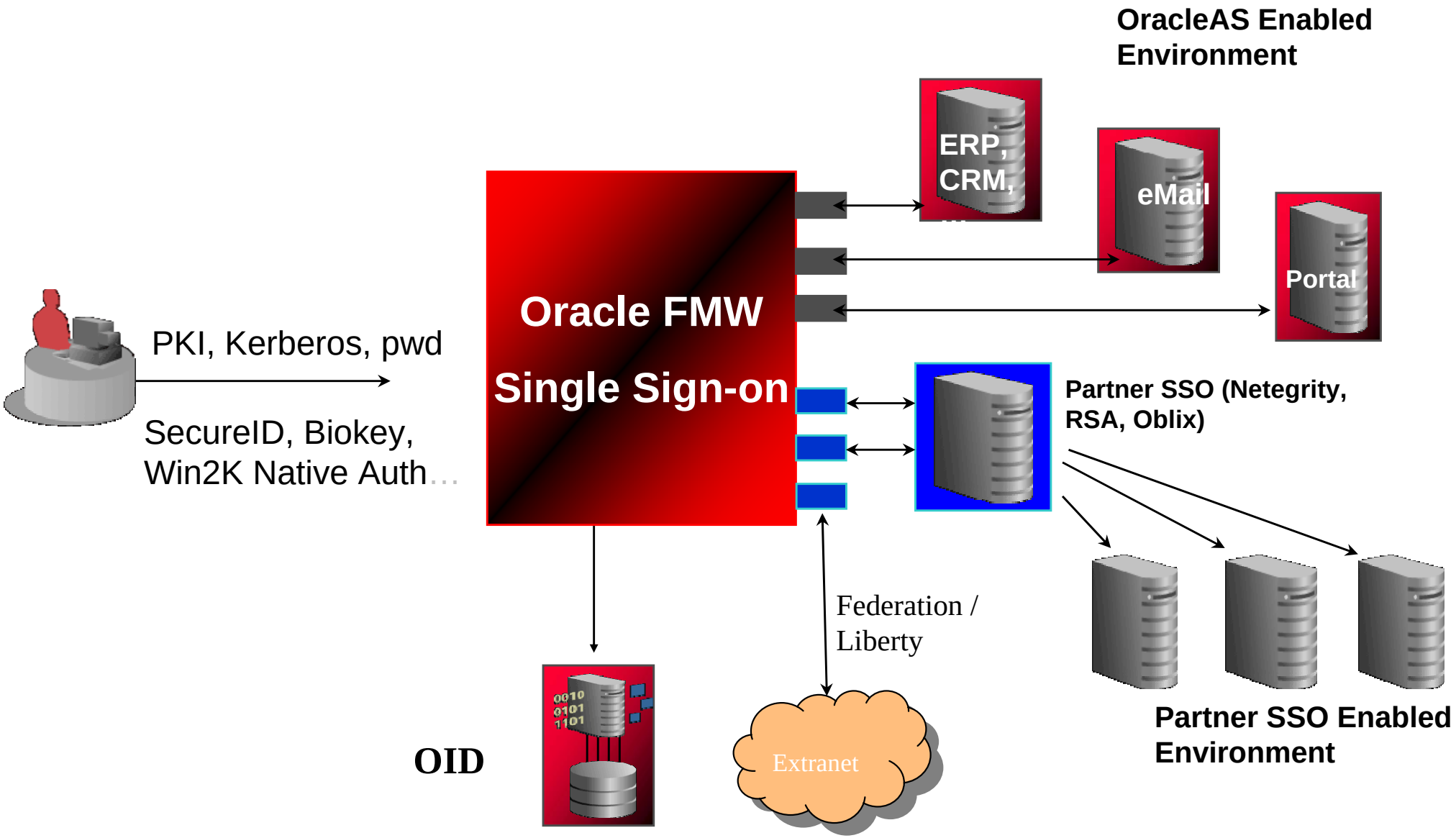
Oracle Label Security

Label Based Access Control

- Data Classification
  - Row level labeling
  - Automated Access Mediation
  - Multi-level Security (MLS)
- Highly Flexible and Adaptable
  - Multiple enforcement options
  - Special privileges
  - Trusted Stored Programs
  - Extensible
- Centralized Administration
  - Integrated with Identity Management
  - Complete API

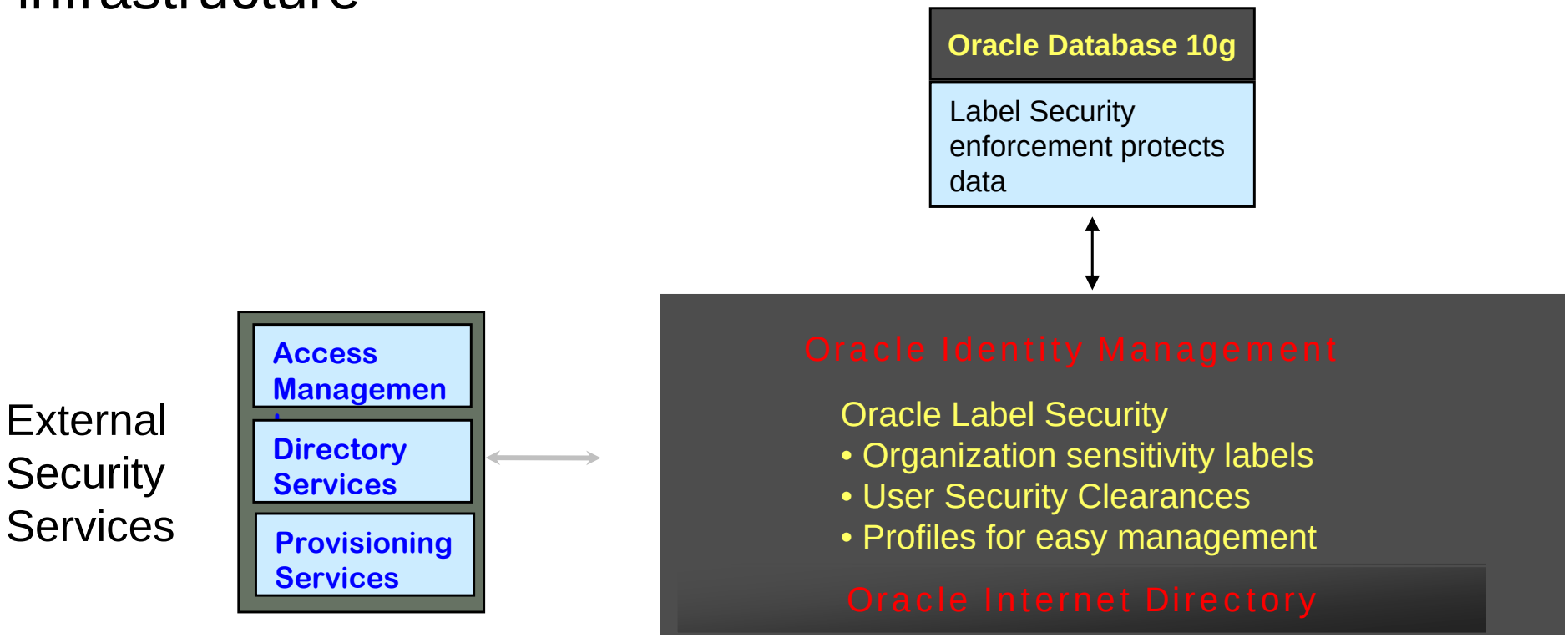


Single Sign-on & Identity Propagation



Oracle Database 10g
Label Security Integration with Identity Management

- Manage sensitivity labels, user security clearances in Oracle Application Server 10g Identity Management infrastructure



Oracle Label Security Identity Management Integration

- Centrally administer
  - Oracle Label Security policies
  - sensitivity labels
  - user label authorizations
- Benefit
  - Label authorizations enforced for directory users
  - Enforce uniform policies centrally
    - Aids GRID computing - security clearance for the GRID
  - Eases administration

Oracle Label Security (OLS)

Sensitive : ACME

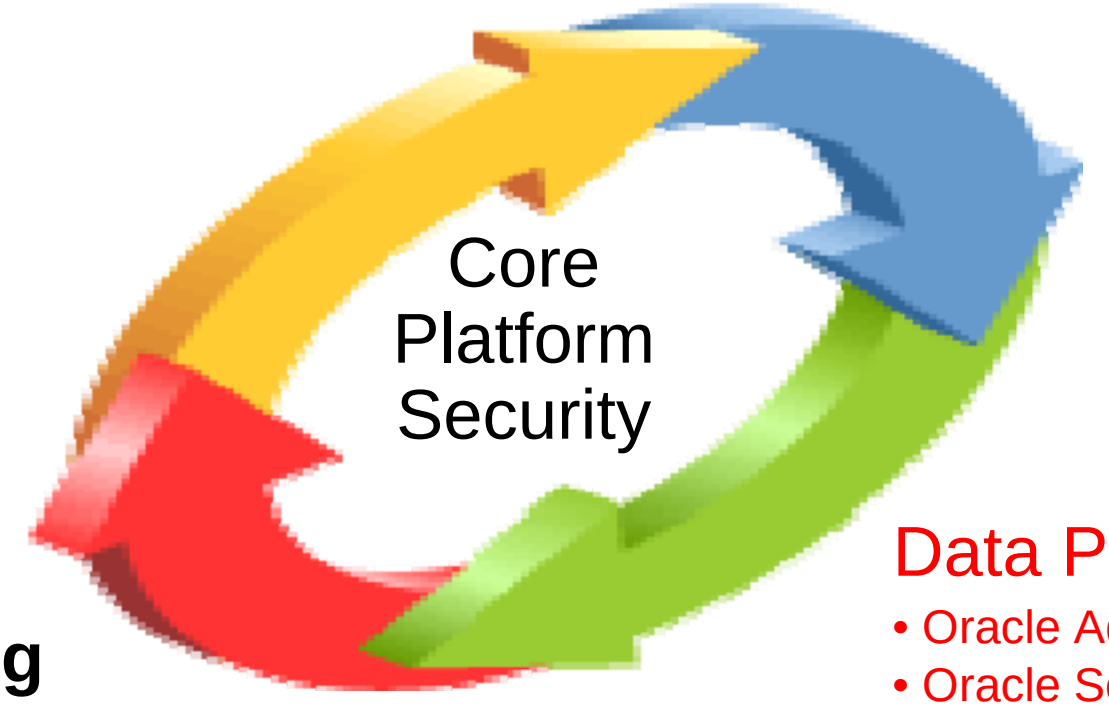
Application Table

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

Data Security: Oracle Products

Access Control

User Management



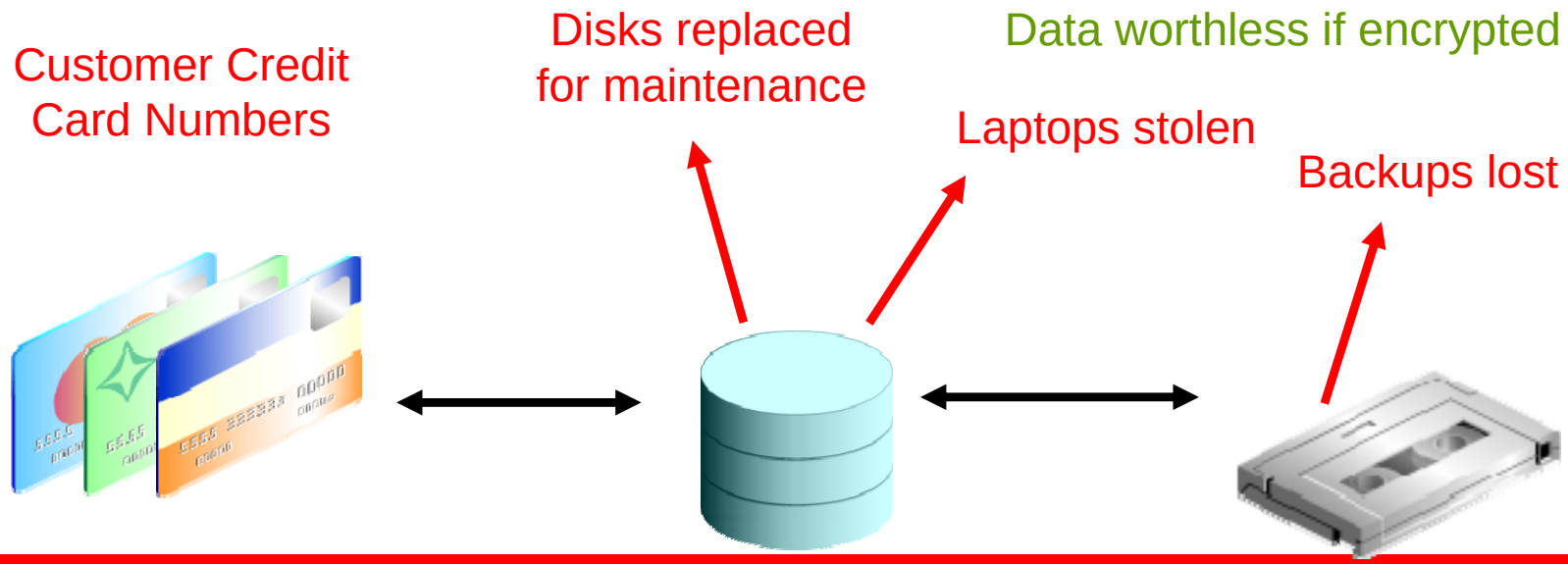
Data Protection

- Oracle Advanced Security
- Oracle Secure Backup

Monitoring

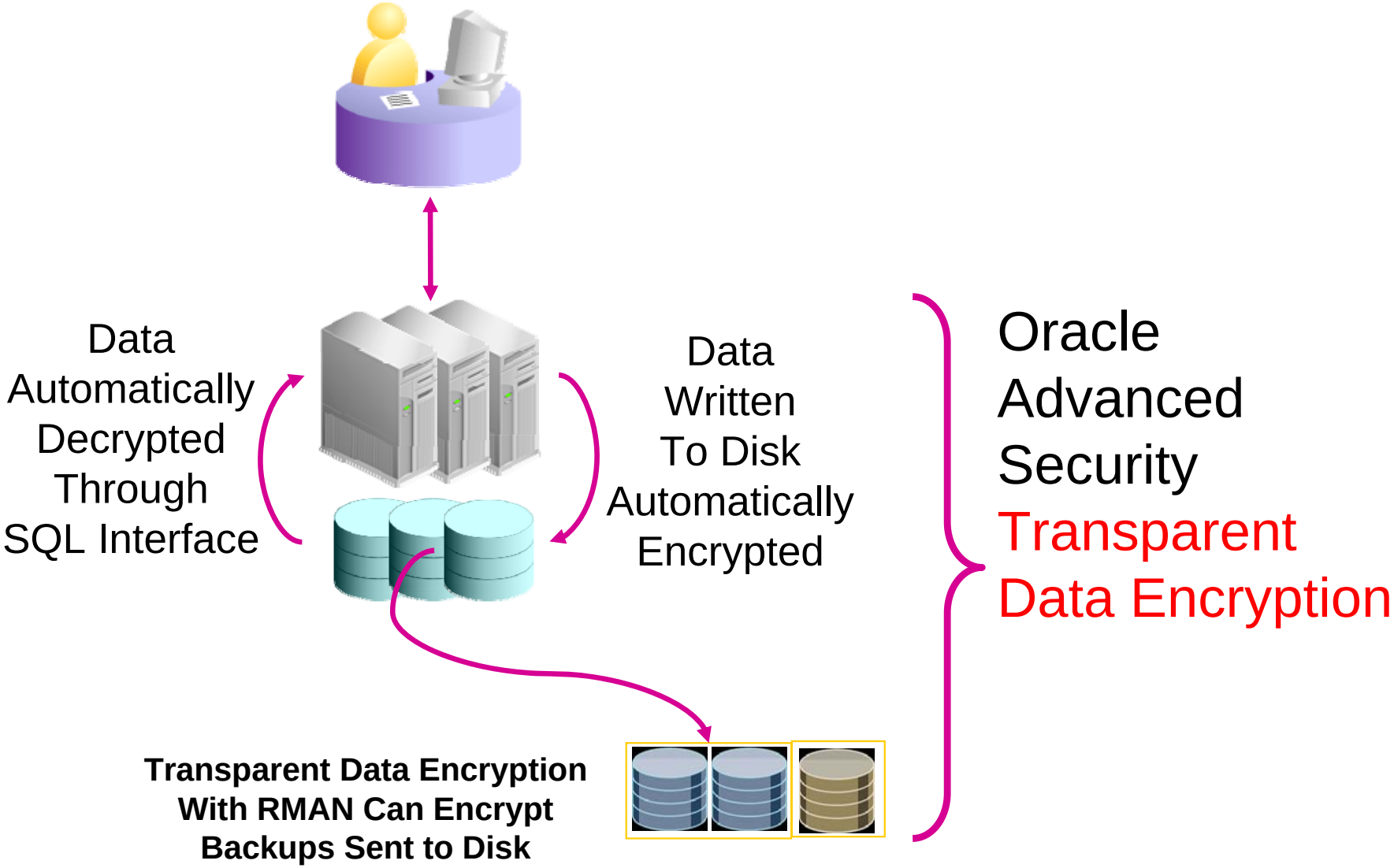
Need for Encryption

- Millions of records lost and many more vulnerable
  - Data theft and privacy
- Worldwide privacy, security and compliance regulations
  - PCI
  - Country-specific laws



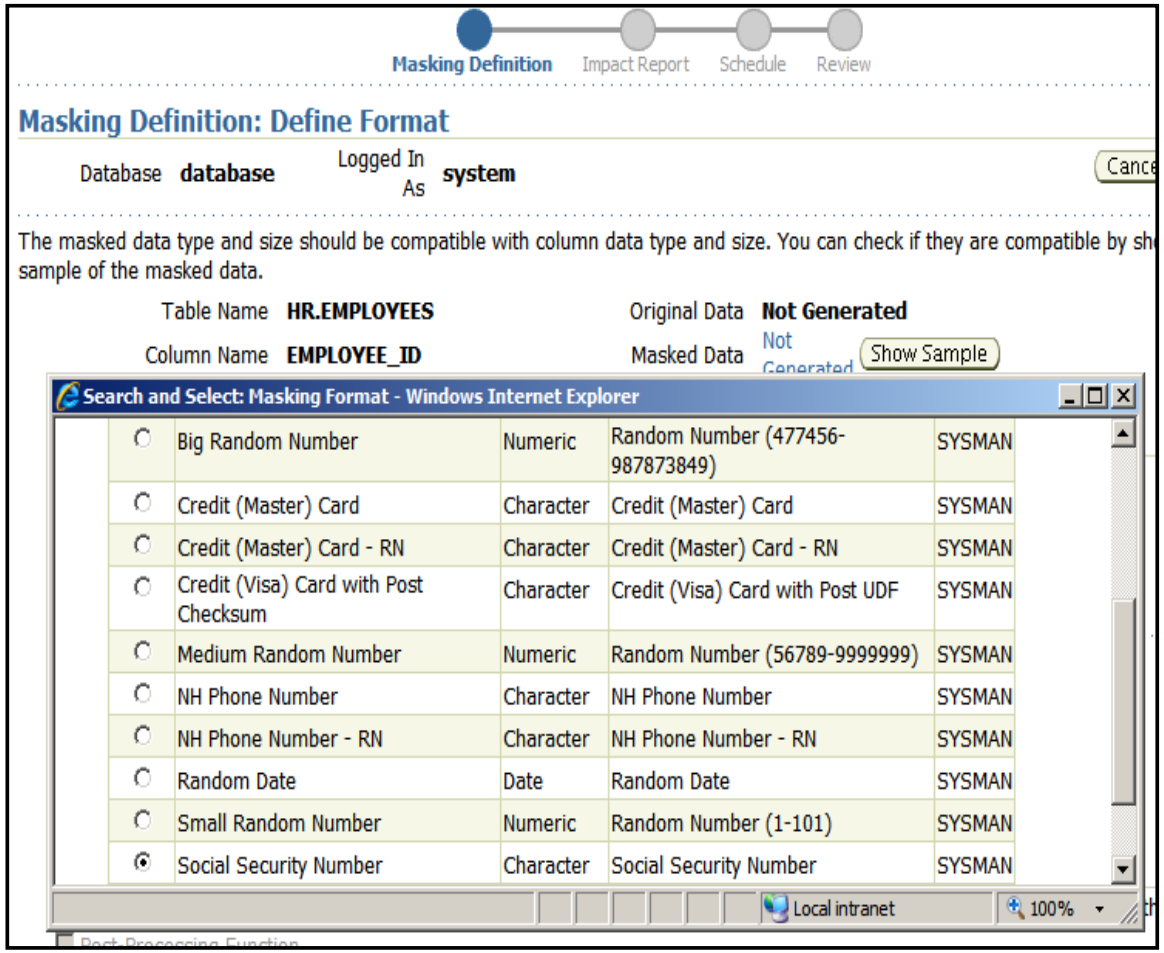
Oracle Advanced Security

Transparent Data Encryption



Data Masking (Beta)

- Protect PII and sensitive data during test, support, and analysis
  - Credit Card, Taxpayer IDs
  - Business sensitive data
  - In-house or off-shore
- Masking process
  - Identify data to mask
  - Define format mask or choose from library
  - Schedule masking job
- Customized masking rules

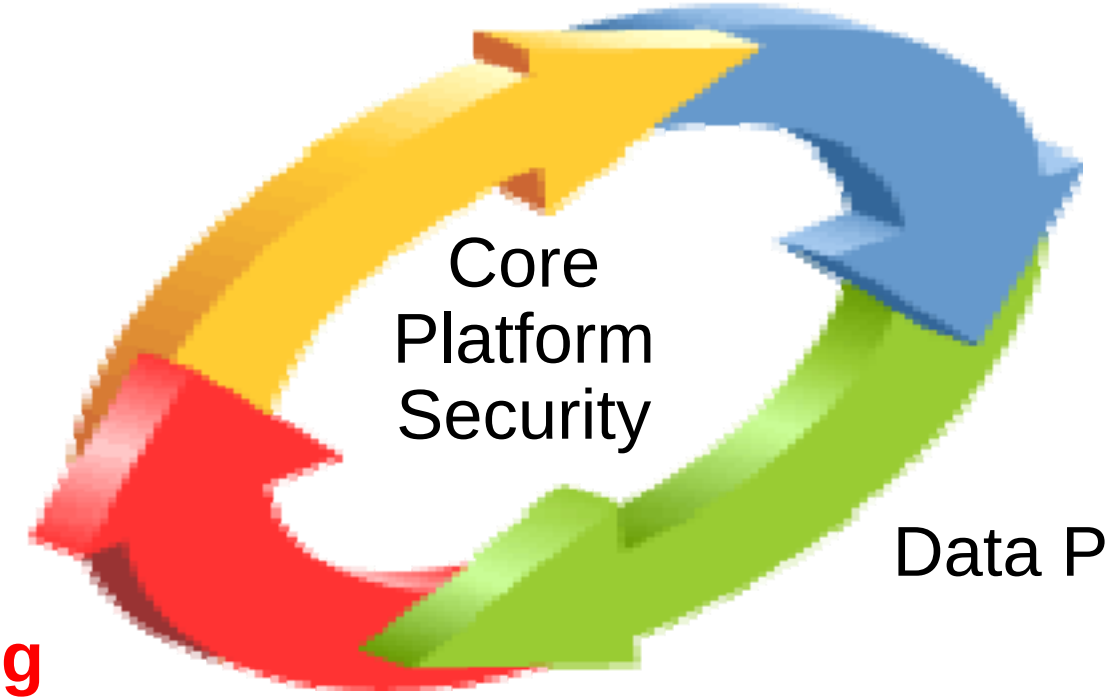


ORACLE
申骨文

Data Security: Oracle Products

Access Control

User Management



Data Protection

Monitoring

- Oracle Audit Vault
- EM Configuration Pack

Enterprise Mgr: Configuration Mgmt Pack

Compliance-driven Secure Configuration Policies

- Automate Database Security Assessment
  - Database Parameters
  - Database Profile
  - Database Access
  - Database File Permissions
  - Post-installation Checks
- Track Configuration Drift across all monitored databases
- Supports 8i and higher database release

Compliance Score Trends

ORACLE Enterprise Manager 10g
Grid Control

Setup | Preferences | Help | Logout

Home | Targets | Deployments | Alerts | Compliance | Jobs | Reports

Policy Groups | Policies | Security At a Glance

Evaluation Results: Secure Configuration for Oracle Database

View: All Results | Filter By Target: All | Choose Target | Clear | Return

- Secure Configuration for Oracle Database
  - Post Installation
  - Oracle Directory and File Permissions
  - Oracle Parameter Settings
  - Database Password Profile Settings
    - Secure Failed Login Attempts Setting
    - Secure Password Life Time Setting
    - Secure Password Lock Time Setting
    - Secure Password Grace Time Setting
    - Password Complexity Checking Enabled
  - Database Access Settings

Policy Group: Secure Configuration for Oracle Database

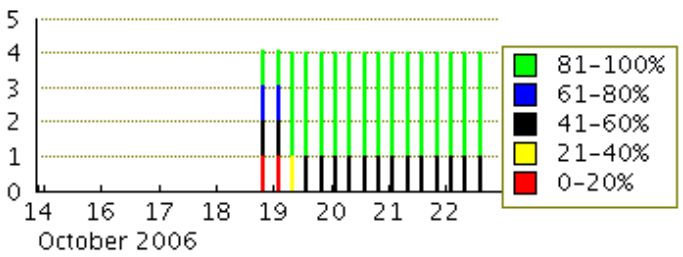
Summary | Trend Overview

Latest Data Collected **Oct 22, 2006 8:21:13 PM PDT**

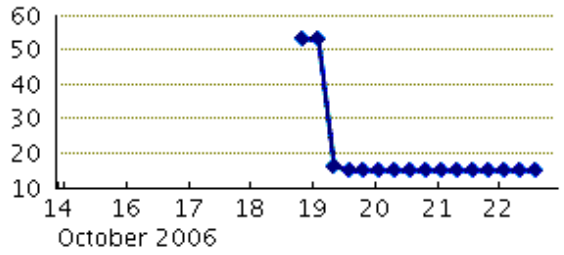
View Data: Last 7 days

Average Compliance Score (%)

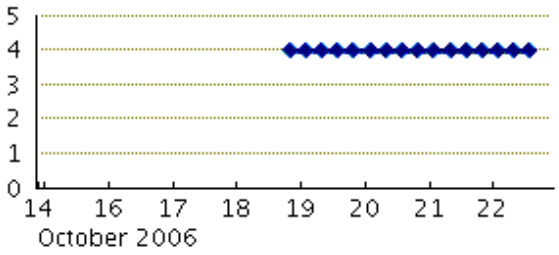
Number of Targets by Compliance Score



Average Violation Count Per Target



Targets Evaluated



Database Auditing

Who did What, When, Where, and How

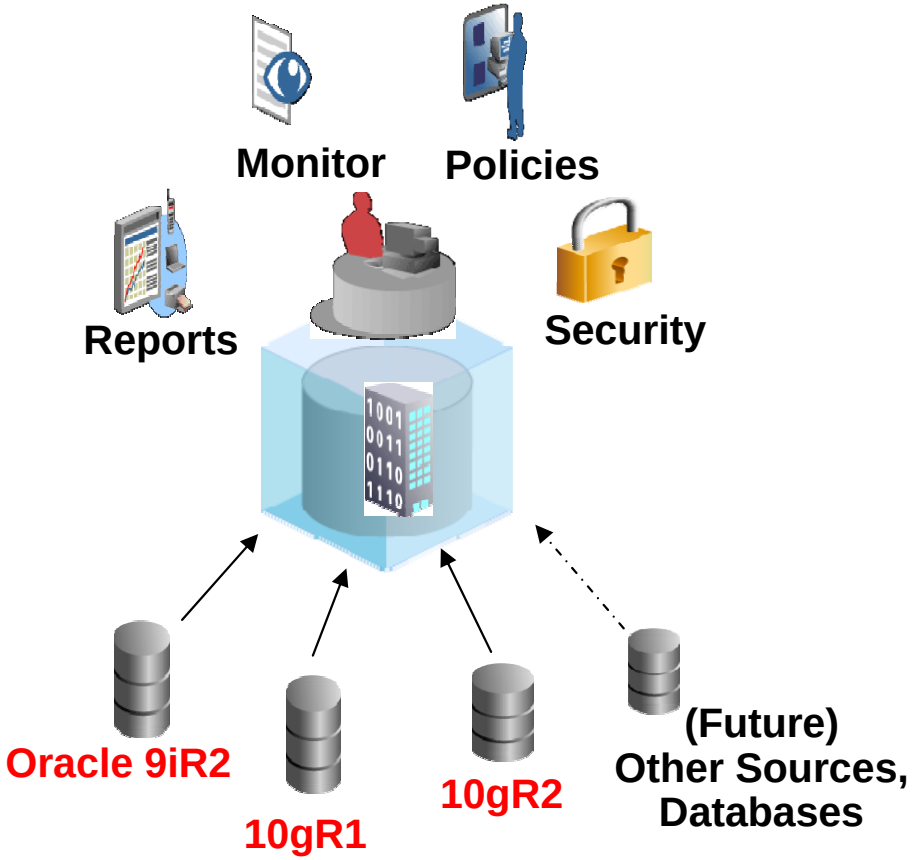
- Provide assurance that data is used as intended
  - Document and record user activity
  - Deter users from inappropriate actions
- Detect anomalies and intrusions
  - Detect suspicious activities early
- Facilitate regulatory compliance reporting
  - Demonstrate adequate IT controls
- Audit key events
  - Access and changes to sensitive data
  - Changes to database structure
  - Privileged user activities
  - Account/Role management

Oracle Audit Vault Overview

Trust-but-Verify

ANNOUNCED IN MAY 2007

- Collect and Consolidate Audit Data
  - Oracle 9i Release 2 and higher
- Simplify Compliance Reporting
  - Built-in reports
  - Custom reports
- Detect and Prevent Insider Threats
  - Alert suspicious activity
- Scale and Security
  - Robust Oracle Database technology
  - Database Vault, Advanced Security
  - Partitioning
- Lower IT Costs with Audit Policies
  - Centrally manage/provision audit settings



Oracle Audit Vault Reports

Out-of-the-box Audit Assessments & Custom Reports

- Out-of-the-box reports
  - Privileged user activity
  - Access to sensitive data
  - Role grants
  - DDL activity
  - Login/logout
- User-defined reports
  - What privileged users did on the financial database?
  - What user 'A' did across multiple databases?
  - Who accessed sensitive data?
- Custom reports
  - Oracle BI Publisher, Application Express, or 3rd party tools

ORACLE Enterprise Manager 10g
Audit Vault

Overview | Activity Reports | Alert Report

Database Instance: av > Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

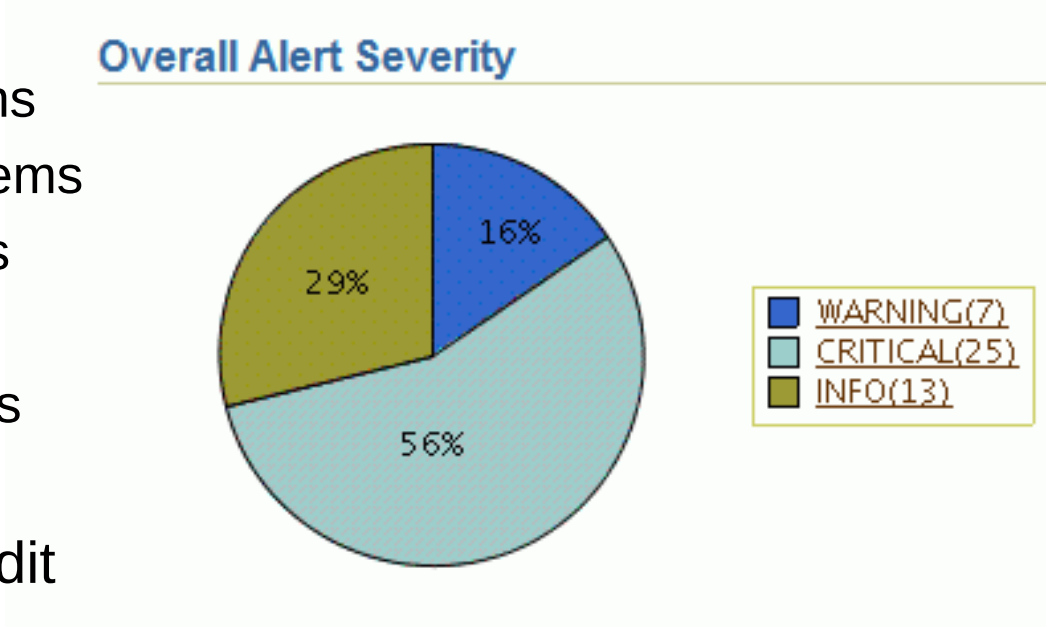
Privileged user activity over the past 24 hours: JTAYLOR, SYSTEM, SYS

Audit Source	User	Audit Event Category	Audit Event	Object	Client Host
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	JTAYLOR.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	JTAYLOR	DATA ACCESS	SELECT	SH.SALES	raclinux1.us.oracle.com
ORCL.US.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		raclinux1.us.oracle.com
VMSSRC2.ORACLE.COM	SYS	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	sys	USER SESSION	SUPER USER LOGON		
ORCL.US.ORACLE.COM	/	USER SESSION	SUPER USER		

Oracle Audit Vault Alerts

Early Detection With Alerting

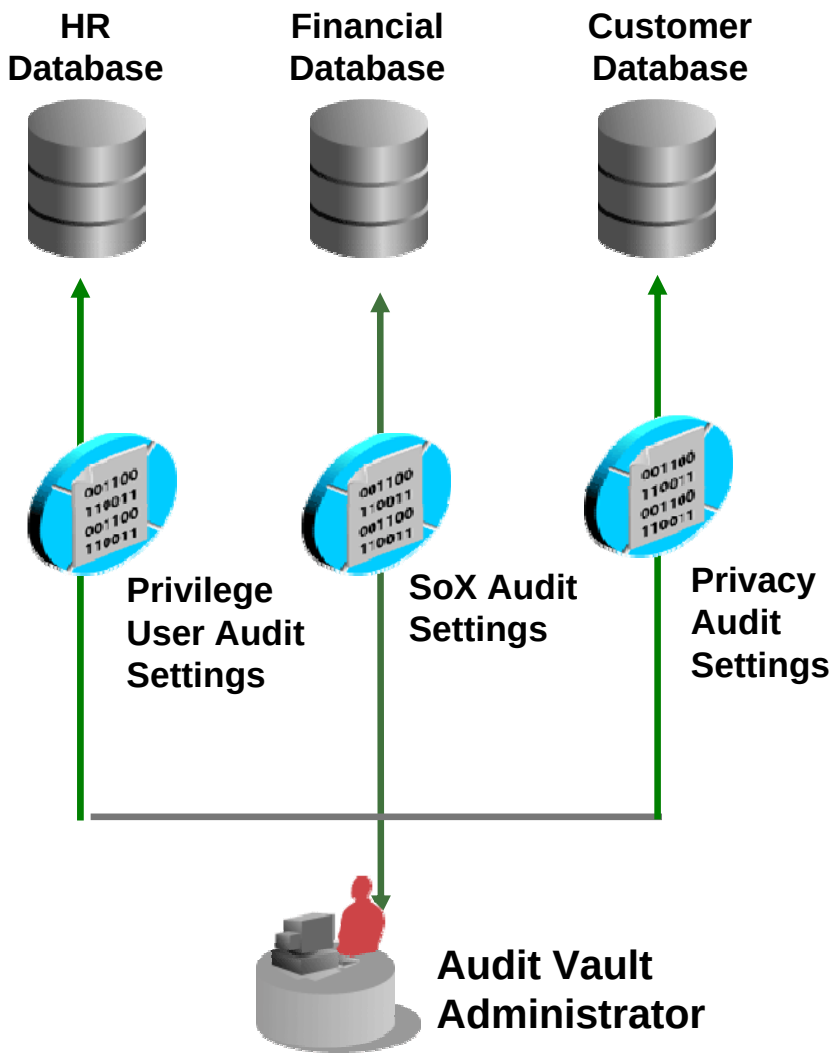
- Alerts can be defined for
  - Directly viewing sensitive columns
  - Creating users on sensitive systems
  - Role grants on sensitive systems
  - “DBA” grants on all systems
  - Failed logins for application users
  - …
- Alerts evaluated on incoming audit data
- Generate alert reports on suspicious activity



Oracle Audit Vault Policies

Centralized Management of Audit Policies

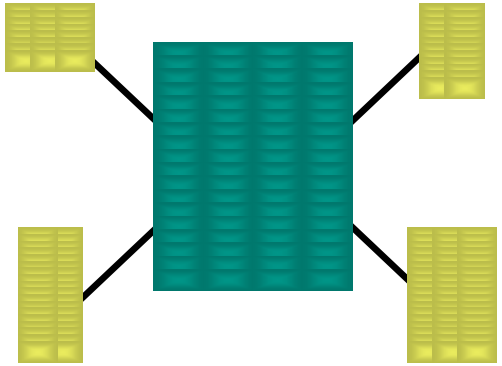
- Audit Policies - collection of audit settings on the databases
- Compare against existing audit settings on source
- Provision audit settings centrally
- Demonstrate compliance



Oracle Audit Vault Data Warehouse

Scalable & Flexible Warehouse

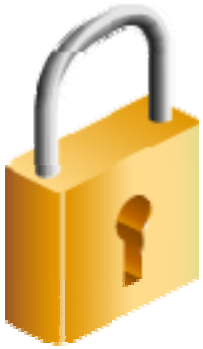
- Audit Warehouse
  - Enable business intelligence and analysis
  - Enable reporting
- Audit Vault Warehouse Dimensions
  - Time, Host, Source, User, Event, …
  - Schema documented and published
  - Allows third party reporting tools
- Performance and Scalability
  - Built-in partitioning
  - Scales to Terabytes
- Oracle RAC certified



Oracle Audit Vault Security

Audit Data is as sensitive as actual data

- Protected with Built-in Security
  - Encrypted audit data transmission
  - Separation of Duty
    - Audit Vault Administrator
    - Audit Vault Auditor
- Protected using
  - Oracle Database Vault
  - Oracle Advanced Security



Oracle Audit Vault Dashboard

Enterprise-wide Security & Compliance view

ORACLE Enterprise Manager 10g
Audit Vault

Help Logout

Audit Reports | Management

Overview | Activity Reports | Alert Report

Database Instance: av

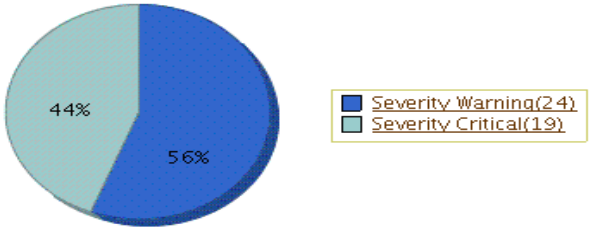
Overview

View Data For: ○ Last One Month ○ Last One Week ○ Last 24 Hours

◉ The Period From Aug 26, 2006 To Sep 26, 2006 Go

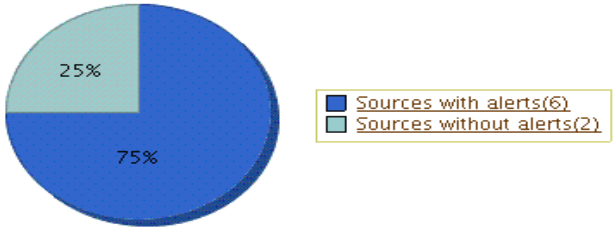
Alert Severity Summary

The distribution of alerts by severity across all audit sources



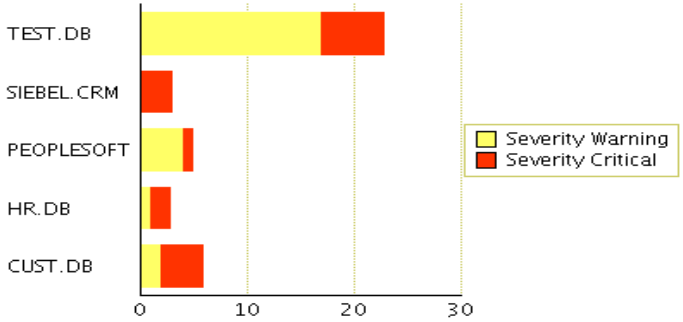
Summary of Alert Activity

The distribution of alert activity by audit source



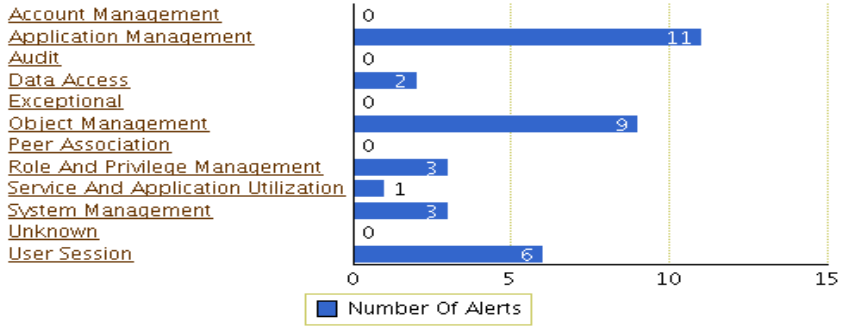
Top Five Audit Sources by Number of Alerts

Audit sources with highest number of alerts



Alerts by Audit Event Category

Displays number of alerts by audit event category

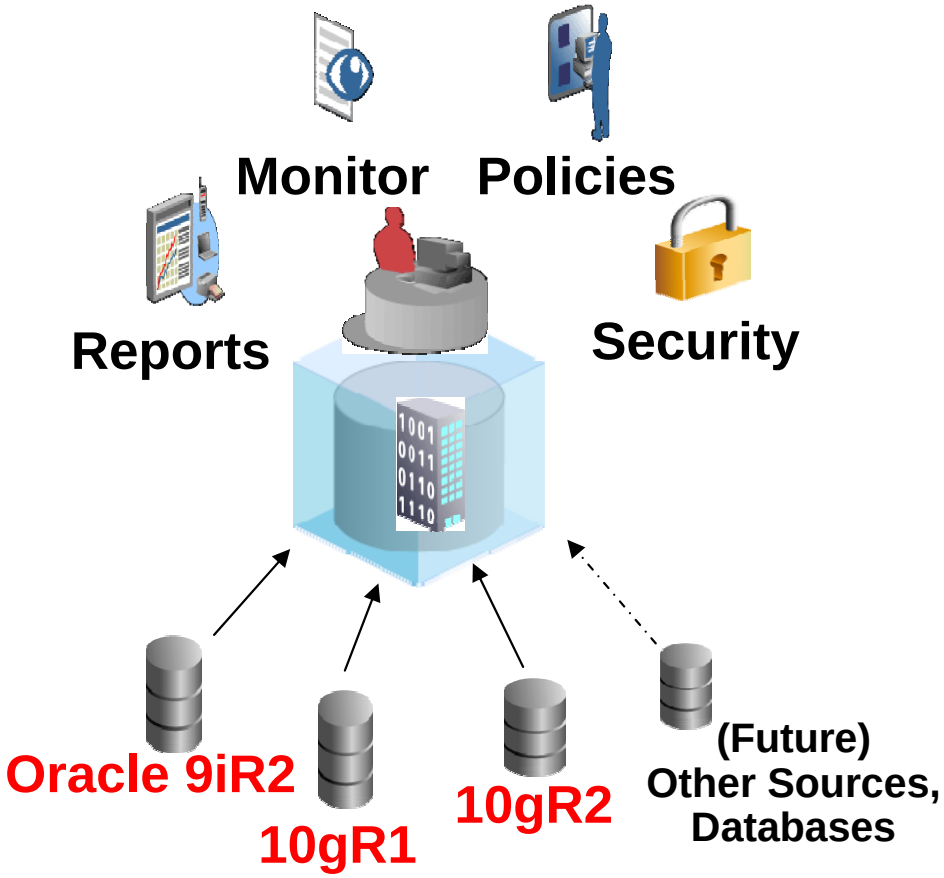


ORACLE
申骨文

Summary

Oracle Audit Vault

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



Summary

- Database security should protect against both external and internal threats
- Database security should provide separation of duty
- Database security should verify the integrity of your data