SECURITY INSIDE OUT

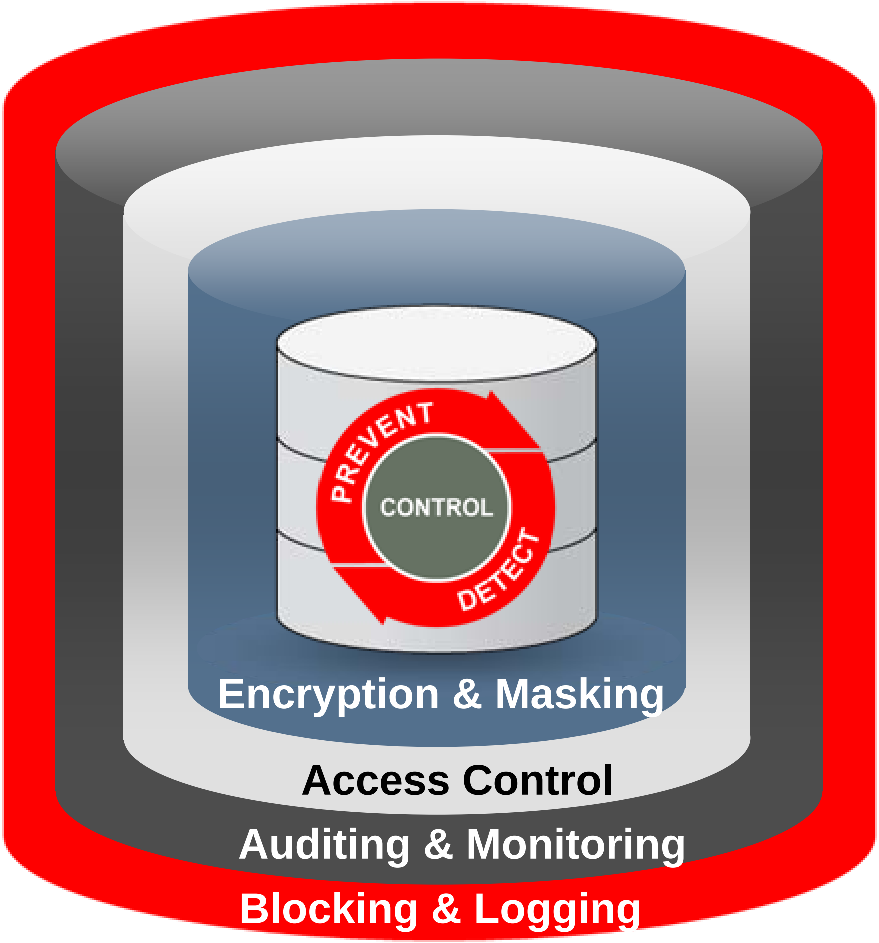
Complete Protection for Your Database, Middleware, and Applications

ORACLE®

Database Security
Audit Vault & Database Firewall

Morana Kobal Butković
Senior Sales Consultant

Database Defense-in-Depth



Encryption and Masking

- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

Access Control

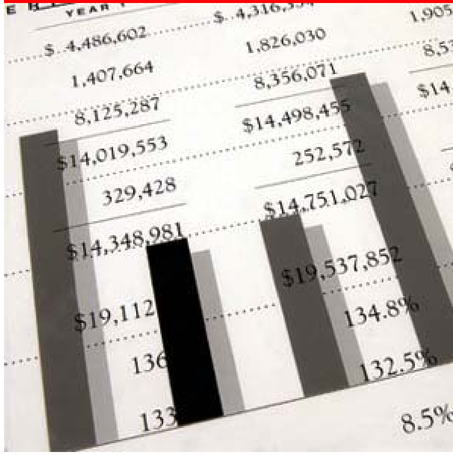
- Oracle Database Vault
- Oracle Label Security

Auditing and Monitoring

- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

Blocking and Logging

- Oracle Database Firewall



Oracle Audit Vault

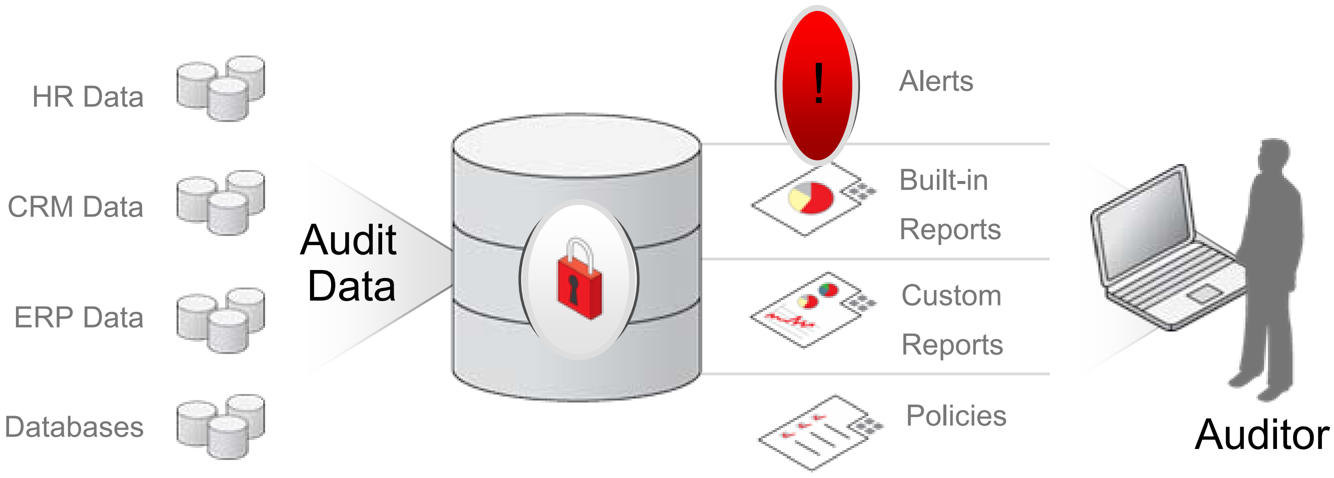
Oracle Audit Vault

Business Drivers

- Detective controls
  - Monitor privileged application user accounts for non-compliant activity – trust but verify
  - Audit non-application access to sensitive data (credit card, financial data, personal identifiable information, etc)
  - Verify that no one is trying to bypass the application security controls
  - PO line items are changed so it does not require more approvals
- Cost of compliance
  - Eliminate costly and complex scripts for reporting
  - Reduce reporting costs for specific compliance audits
  - SOX, PCI, HIPAA, SAS 70, STIG

Oracle Audit Vault

Automated Activity Monitoring & Audit Reporting

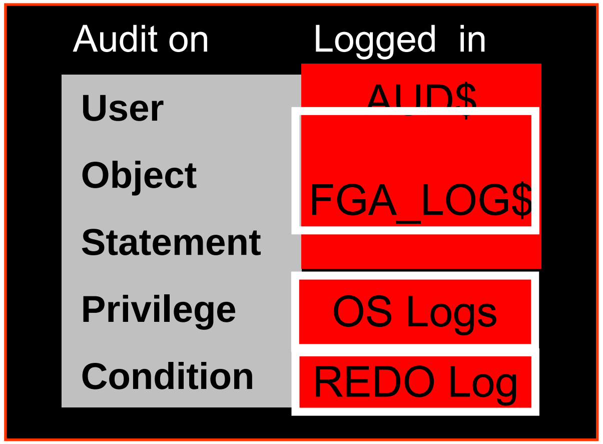


- Consolidate audit data into secure repository
- Detect and alert on suspicious activities
- Out-of-the box compliance reporting
- Centralized audit policy management

Oracle Audit Vault

Oracle Database Audit Support

- Database Audit Tables
  - Collect audit data for standard and fine-grained auditing
- Oracle audit trail from OS files
  - Collect audit records written in XML or standard text file
- Operating system SYSLOG
  - Collect Oracle database audit records from SYSLOG
- Redo log
  - Extract before/after values and DDL changes to table
- Database Vault specific audit records



Audit on

Logged in

User

Object

Statement

Privilege

Condition

AUD$

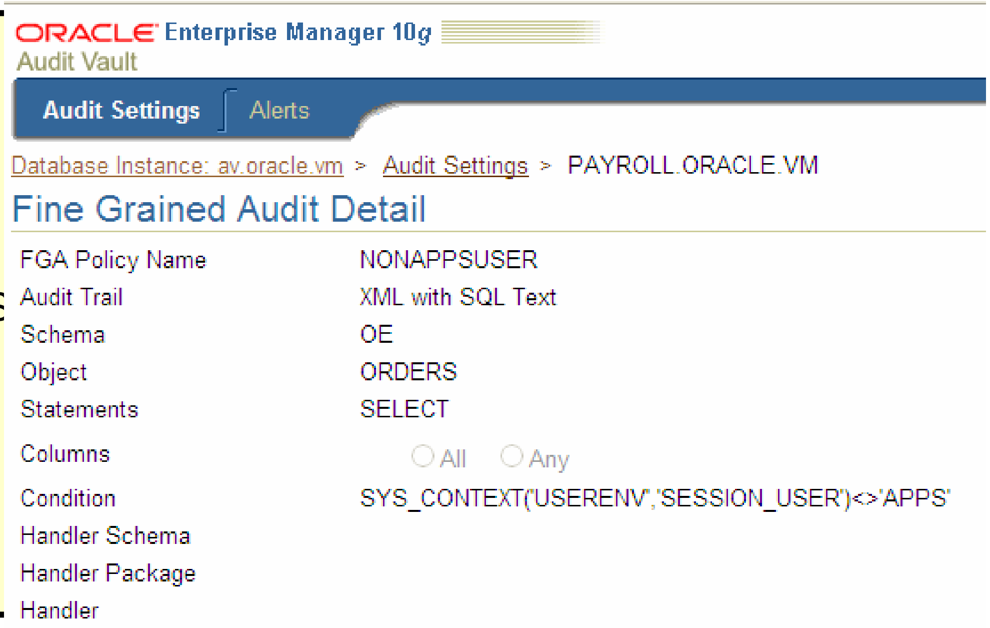
FGA_LOG$

OS Logs

REDO Log

Applying Fine-Grained Auditing

```
DBMS_FGA.ADD_POLICY (
 object_schema   =>  ‘OE',
 object_name     =>  ‘ORDERS',
 policy_name     =>  ‘NONAPPSUSER,
 audit_condition =>
SYS_CONTEXT('USERENV','SESSION_US
'APPS' ,
 enable          =>  TRUE,
 statement_types =>  'SELECT' );
```



ORACLE Enterprise Manager 10g
Audit Vault

Database Instance: av.oracle.vm > Audit Settings > PAYROLL.ORACLE.VM

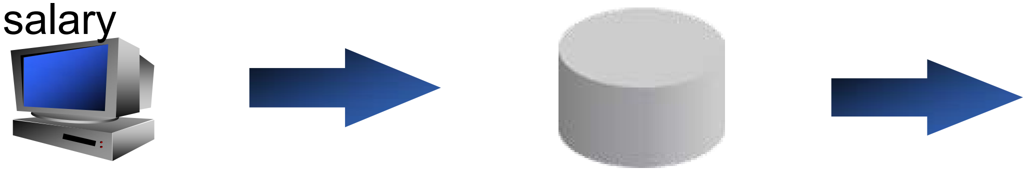
Fine Grained Audit Detail

FGA Policy Name	NONAPPSUSER
Audit Trail	XML with SQL Text
Schema	OE
Object	ORDERS
Statements	SELECT
Columns	○ All ○ Any
Condition	SYS_CONTEXT('USERENV','SESSION_USER')<>'APPS'
Handler Schema	
Handler Package	
Handler	

Enforce Audit Policy in Database

... SYS_CONTEXT('USERENV','SESSION_USER')<>'APPS'

Select names, salary
from ORDERS
where...



Generate Audit Record

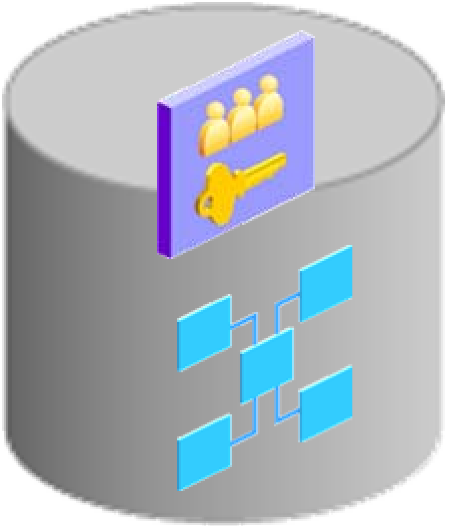
Oracle Audit Vault

Heterogeneous Database Support

- Microsoft SQL server versions 2000, 2005, & 2008
  - Server side trace – set specific audit event
  - Windows event audit – specific audit events that are viewed by the windows event viewer
  - C2 - automatically sets all auditable events and collects them in the audit log
  - Support for 2008 audit facility targeted for CY2010
- IBM DB2 8.2 - 9.5 on Linux, Unix, Windows
  - Extract binary audit files into a trace file
- Sybase ASE 12.5.4 - 15.0.x
  - Utilize the native audit tables

Secure & Scalable Audit Warehouse

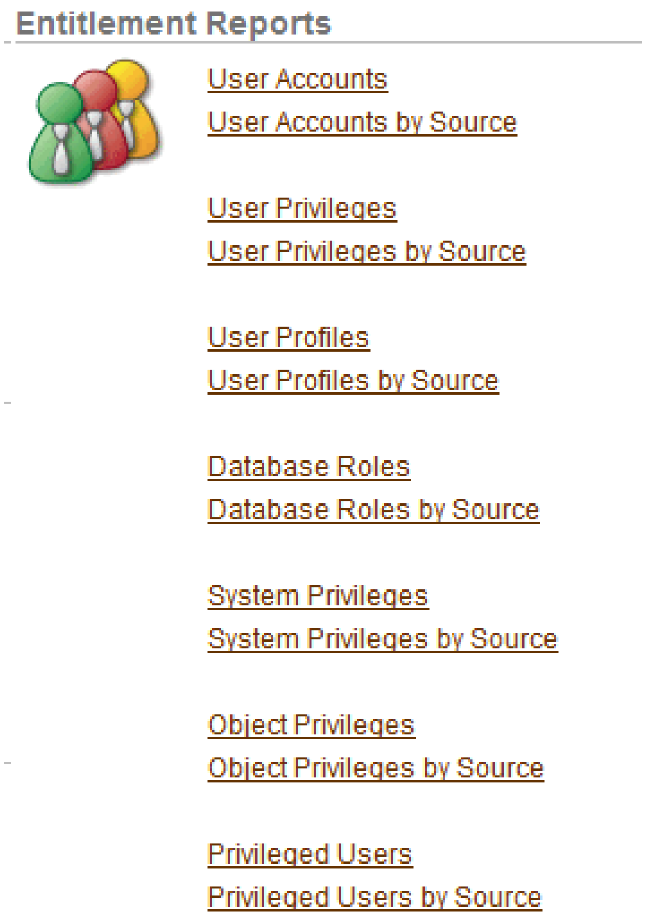
- Audit Warehouse
  - Document Schema
  - Enable BI and analysis
- Performance and Scalability
  - Built-in partitioning
  - Database compression
  - Scales to Terabytes
  - Certified with Oracle RAC
- Protected with Built-in Security
  - Encrypted audit data transmission
  - Separation of Duty provided by Database Vault
    - Audit Vault Administrator
    - Audit Vault Auditor



Audit Vault

User Entitlements

NEW!



Entitlement Reports

User Accounts
User Accounts by Source

User Privileges
User Privileges by Source

User Profiles
User Profiles by Source

Database Roles
Database Roles by Source

System Privileges
System Privileges by Source

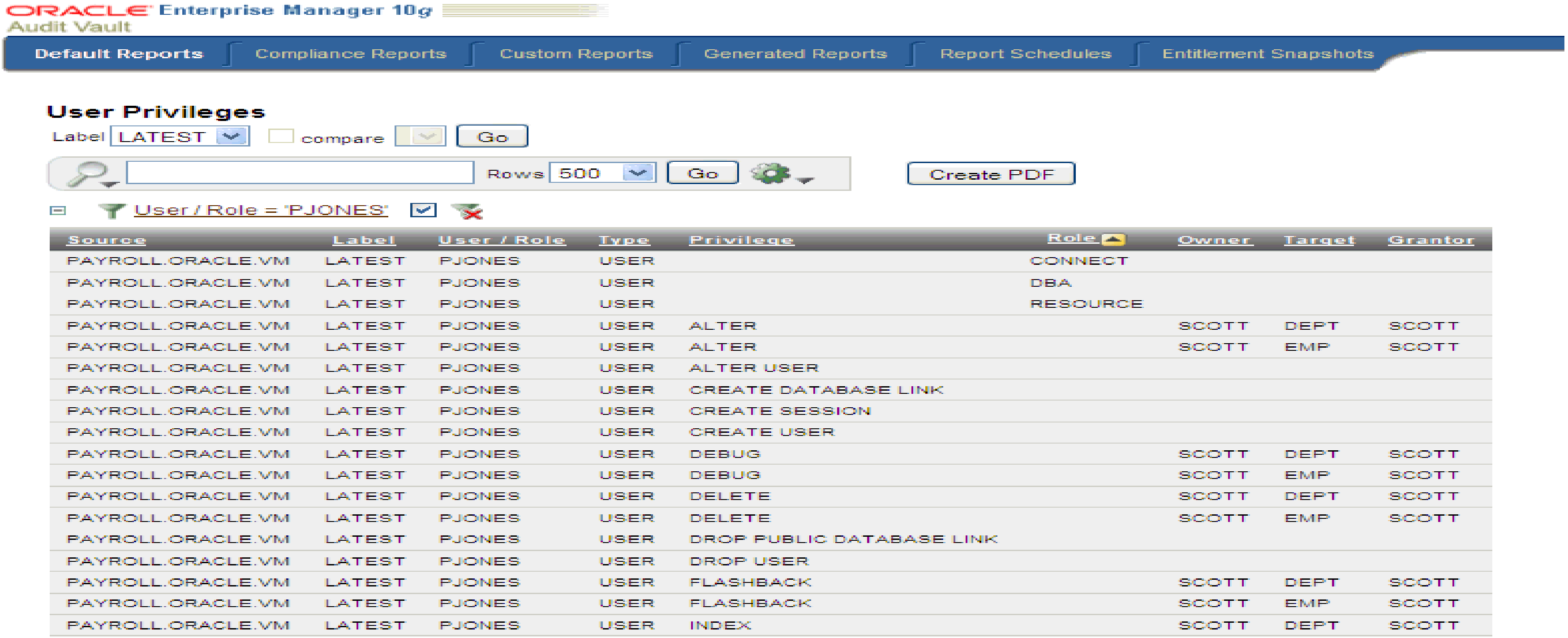
Object Privileges
Object Privileges by Source

Privileged Users
Privileged Users by Source

- View all user accounts in the Oracle database
- Retrieve a snapshot of user entitlement data
- Filter data based on users or privileges
- View or print report in PDF format
- Compare changes in user accounts and privileges
- View SYSDBA/SYSOPER privileges

Database User Privileges Report

- Display all Oracle database users, privileges, and roles
- Reports accounts and their level of access
- Regulations: SOX, PCI, HIPAA, SAS 70, STIG



User Privileges

Label LATEST

Rows 500

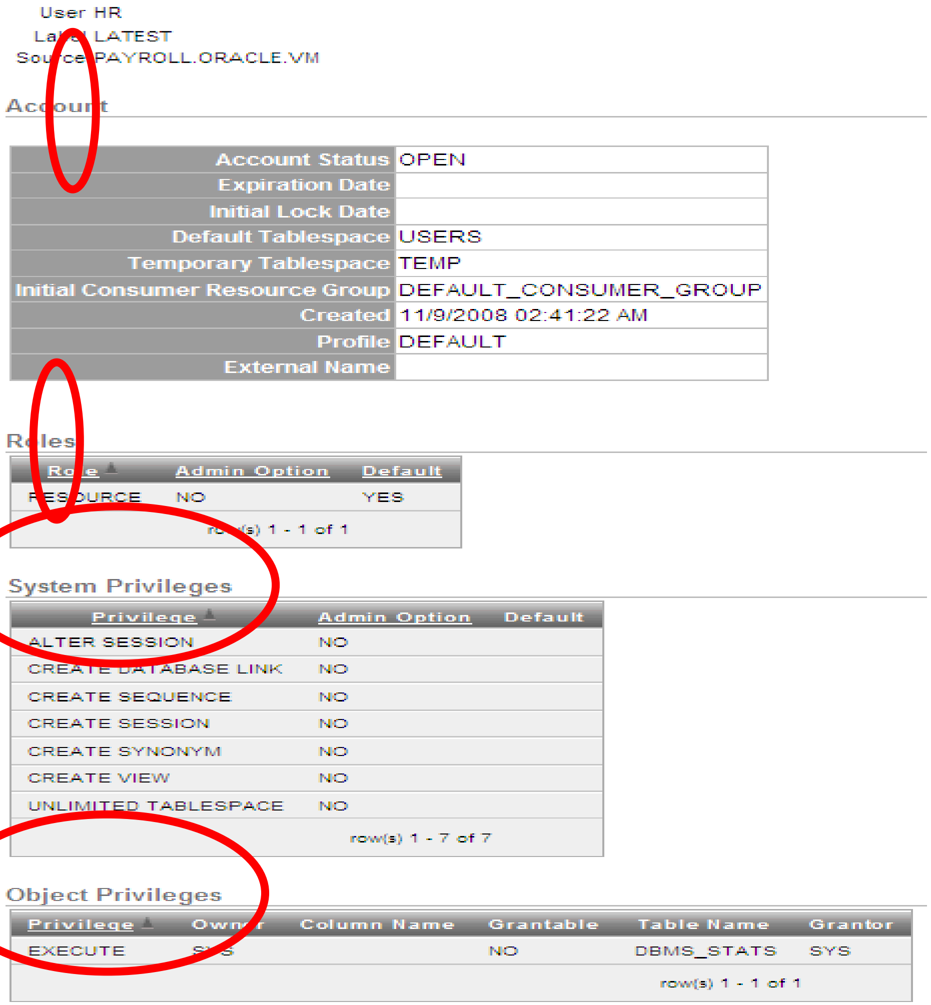
User / Role = 'PJONES' ☑

Source	Label	User / Role	Type	Privilege	Role	Owner	Target	Grantor
PAYROLL.ORACLE.VM	LATEST	PJONES	USER		CONNECT			
PAYROLL.ORACLE.VM	LATEST	PJONES	USER		DBA			
PAYROLL.ORACLE.VM	LATEST	PJONES	USER		RESOURCE			
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	ALTER		SCOTT	DEPT	SCOTT
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	ALTER		SCOTT	EMP	SCOTT
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	ALTER USER				
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	CREATE DATABASE LINK				
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	CREATE SESSION				
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	CREATE USER				
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	DEBUG		SCOTT	DEPT	SCOTT
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	DEBUG		SCOTT	EMP	SCOTT
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	DELETE		SCOTT	DEPT	SCOTT
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	DELETE		SCOTT	EMP	SCOTT
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	DROP PUBLIC DATABASE LINK				
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	DROP USER				
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	FLASHBACK		SCOTT	DEPT	SCOTT
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	FLASHBACK		SCOTT	EMP	SCOTT
PAYROLL.ORACLE.VM	LATEST	PJONES	USER	INDEX		SCOTT	DEPT	SCOTT

User Account Details

Account, Roles, System/Object Privileges

NEW!



User HR
Label LATEST
Source PAYROLL.ORACLE.VM

Account

Account Status	OPEN
Expiration Date	
Initial Lock Date	
Default Tablespace	USERS
Temporary Tablespace	TEMP
Initial Consumer Resource Group	DEFAULT_CONSUMER_GROUP
Created	11/9/2008 02:41:22 AM
Profile	DEFAULT
External Name	

Roles

Role	Admin Option	Default
RESOURCE	NO	YES

row(s) 1 - 1 of 1

System Privileges

Privilege	Admin Option	Default
ALTER SESSION	NO	
CREATE DATABASE LINK	NO	
CREATE SEQUENCE	NO	
CREATE SESSION	NO	
CREATE SYNONYM	NO	
CREATE VIEW	NO	
UNLIMITED TABLESPACE	NO	

row(s) 1 - 7 of 7

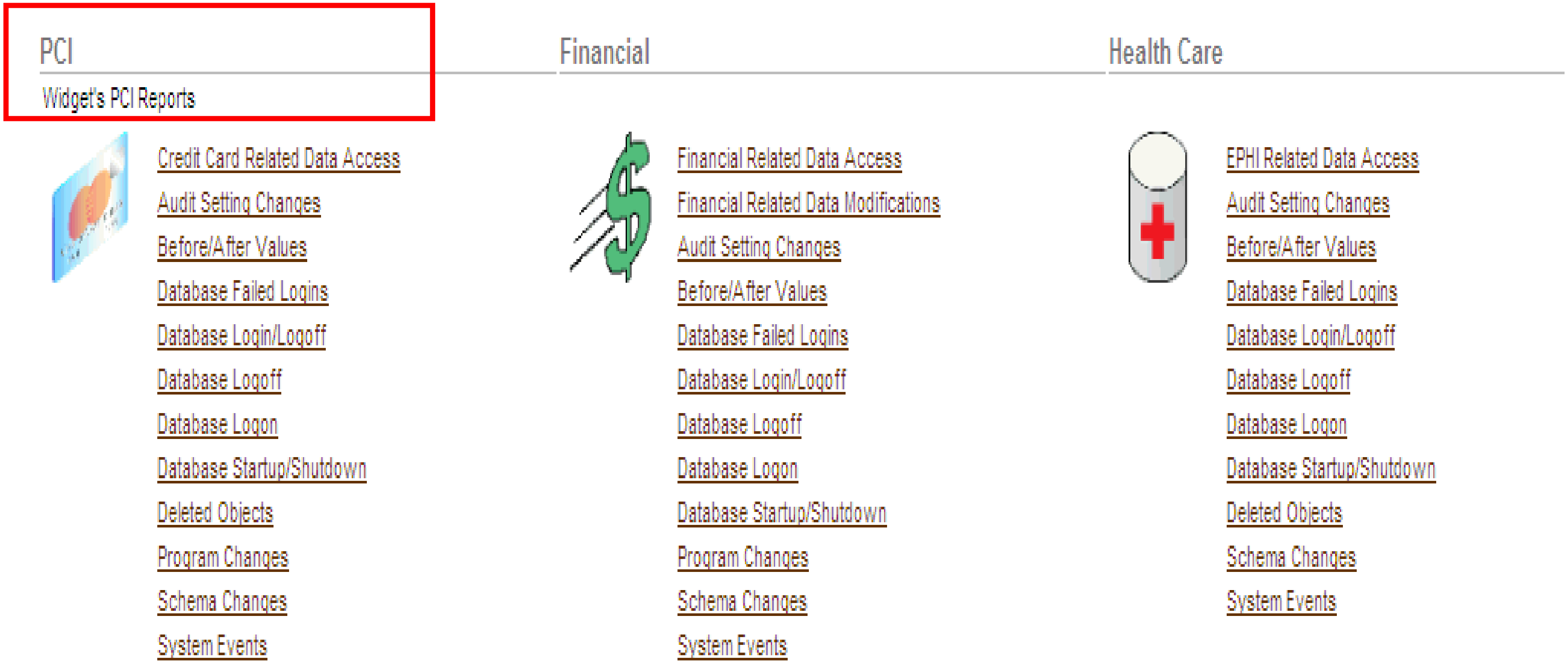
Object Privileges

Privilege	Owner	Column Name	Grantable	Table Name	Grantor
EXECUTE	SYS		NO	DBMS_STATS	SYS

row(s) 1 - 1 of 1

Out-of-the-box Compliance Reports

NEW!



PCI

Widget's PCI Reports

- Credit Card Related Data Access
- Audit Setting Changes
- Before/After Values
- Database Failed Logins
- Database Login/Logoff
- Database Logoff
- Database Logon
- Database Startup/Shutdown
- Deleted Objects
- Program Changes
- Schema Changes
- System Events

Financial

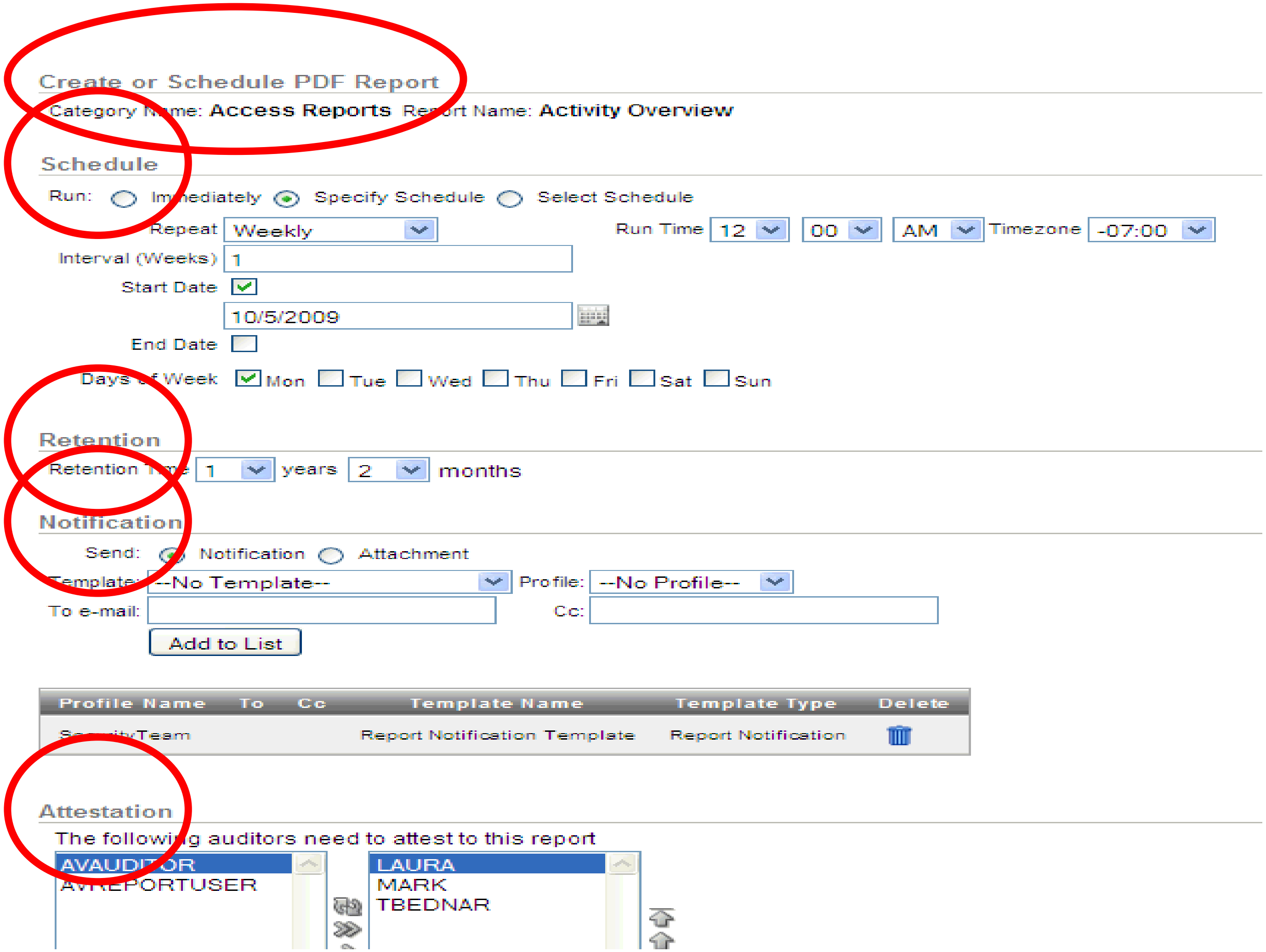
- Financial Related Data Access
- Financial Related Data Modifications
- Audit Setting Changes
- Before/After Values
- Database Failed Logins
- Database Login/Logoff
- Database Logoff
- Database Logon
- Database Startup/Shutdown
- Program Changes
- Schema Changes
- System Events

Health Care

- EPHI Related Data Access
- Audit Setting Changes
- Before/After Values
- Database Failed Logins
- Database Login/Logoff
- Database Logoff
- Database Logon
- Database Startup/Shutdown
- Deleted Objects
- Schema Changes
- System Events

Reports Management

Schedule, Retention, Notification, Attestation



Create or Schedule PDF Report

Category Name: Access Reports Report Name: Activity Overview

Schedule

Run: ○ Immediately ● Specify Schedule ○ Select Schedule

Repeat: Weekly

Run Time: 12 : 00 AM

Timezone: -07:00

Interval (Weeks): 1

Start Date: ☑ 10/5/2009

End Date: □

Days of Week: ☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Retention

Retention Time: 1 years 2 months

Notification

Send: ● Notification ○ Attachment

Template: --No Template--

Profile: --No Profile--

To e-mail:

Cc:

Add to List

Profile Name	To	Cc	Template Name	Template Type	Delete
SecurityTeam			Report Notification Template	Report Notification	🗑

Attestation

The following auditors need to attest to this report

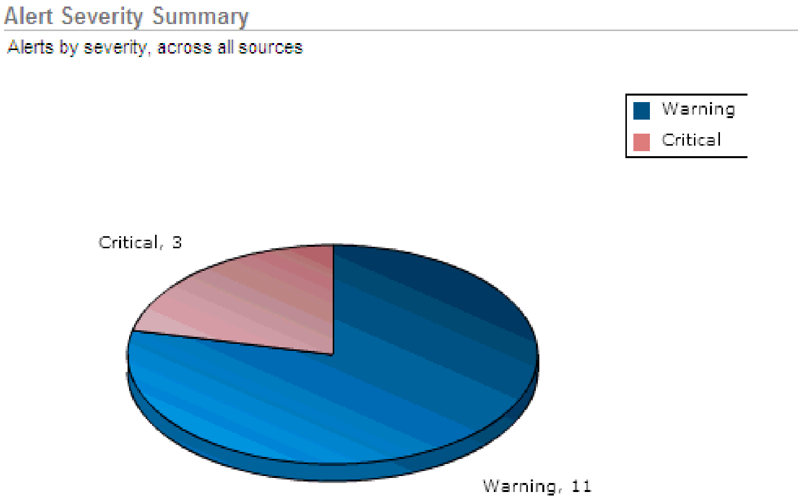
AVAUDITOR
AVREPORTUSER

LAURA
MARK
TBEDNAR

Oracle Audit Vault Alerts

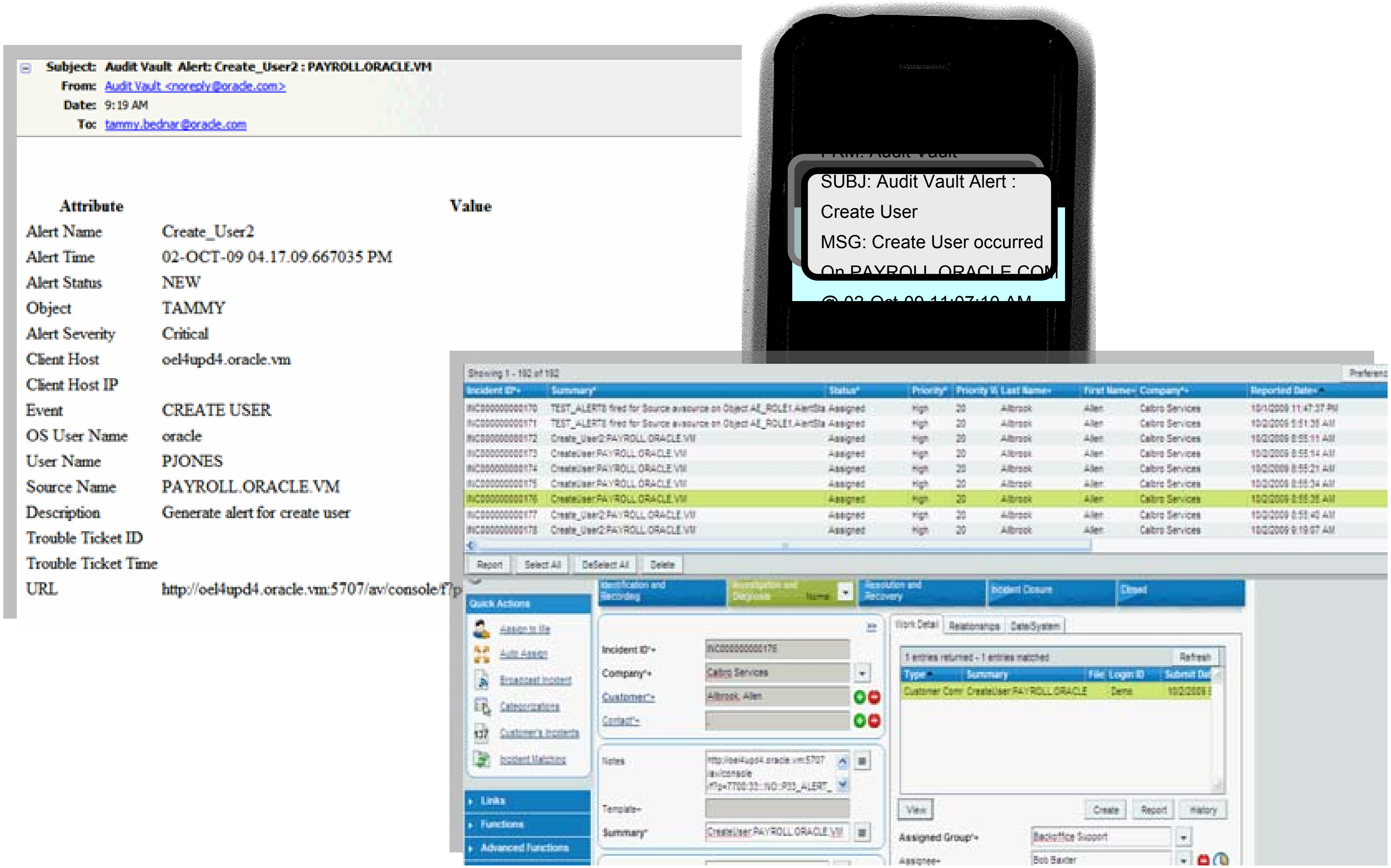
Threat Detection with Custom Alerts

- Alerts can be defined for
  - Creating users on sensitive systems
  - Role grants on sensitive systems
  - “DBA” grants on all systems
  - Failed logins for application users
  - Directly viewing sensitive columns
  - ….
- Add workflow for alerts
- Track alerts
- Drill down from the dashboard
- Send alerts to distribution lists



Integration with Email / SMS / Remedy

NEW!



Subject: Audit Vault Alert: Create_User2 : PAYROLL.ORACLE.VM
From: Audit Vault <noreply@oracle.com>
Date: 9:19 AM
To: tammy.bednar@oracle.com

Attribute	Value
Alert Name	Create_User2
Alert Time	02-OCT-09 04.17.09.667035 PM
Alert Status	NEW
Object	TAMMY
Alert Severity	Critical
Client Host	oel4upd4.oracle.vm
Client Host IP	
Event	CREATE USER
OS User Name	oracle
User Name	PJONES
Source Name	PAYROLL.ORACLE.VM
Description	Generate alert for create user
Trouble Ticket ID	
Trouble Ticket Time	
URL	http://oel4upd4.oracle.vm:5707/av/console/f?p

FRM: Audit Vault
SUBJ: Audit Vault Alert :
Create User
MSG: Create User occurred
On PAYROLL.ORACLE.COM
@ 02-Oct-09 11:07:10 AM

Showing 1 - 192 of 192

Incident ID*	Summary*	Status*	Priority*	Priority W	Last Name*	First Name*	Company*	Reported Date*
INC000000000170	TEST_ALERTS fired for Source avsource on Object AE_ROLE1 AlertSta	Assigned	High	20	Allbrook	Allen	Calbro Services	10/1/2009 11:47:37 PM
INC000000000171	TEST_ALERTS fired for Source avsource on Object AE_ROLE1 AlertSta	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:51:35 AM
INC000000000172	Create_User2:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:11 AM
INC000000000173	CreateUser:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:14 AM
INC000000000174	CreateUser:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:21 AM
INC000000000175	CreateUser:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:34 AM
INC000000000176	CreateUser:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:35 AM
INC000000000177	Create_User2:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:40 AM
INC000000000178	Create_User2:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 9:19:07 AM

Incident ID*: INC000000000176
Company*: Calbro Services
Customer*: Allbrook, Allen
Contact*:
Notes: http://oel4upd4.oracle.vm:5707/av/console/f?p=7700:33::NO::P33_ALERT_
Template:
Summary*: CreateUser:PAYROLL.ORACLE.VM

1 entries returned - 1 entries matched

Type	Summary	File	Login ID	Submit Da
Customer Com	CreateUser:PAYROLL.ORACLE		Demo	10/2/2009

Assigned Group*: Backoffice Support
Assignee*: Bob Baxter

Oracle Recommended Audit Settings

- Auditing should be selective and effective – target privileges users, selective tables, and secure configurations
- **Oracle Database 11g provides default audit policy configuration**

ALTER ANY PROCEDURE	CREATE ANY JOB	DROP ANY TABLE	ALTER ANY TABLE
CREATE ANY LIBRARY	DROP PROFILE	ALTER DATABASE	CREATE ANY PROCEDURE
DROP USER	ALTER PROFILE	CREATE ANY TABLE	EXEMPT ACCESS POLICY
AUDIT ROLE BY ACCESS	CREATE EXTERNAL JOB	GRANT ANY OBJECT PRIVILEGE	ALTER SYSTEM
CREATE PUBLIC DATABASE LINK	GRANT ANY PRIVILEGE	ALTER USER	CREATE SESSION
GRANT ANY ROLE	AUDIT SYSTEM	CREATE USER	AUDIT SYSTEM BY ACCESS
DROP ANY PROCEDURE			

Included in the demo directory of the Audit Vault Server:
$ORACLE_HOME/demo/secconf.sql

Auditing Resources

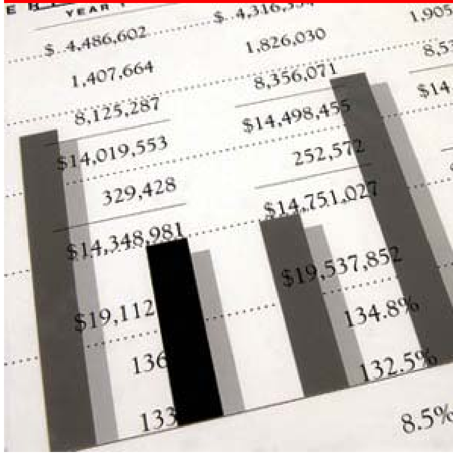
Impact on CPU performance

- Original workload CPU 1.08% for 10 audit/sec case
- Original workload CPU 1.56% for 100 audit/sec case

Audit Source	**Database auditing / No Audit Vault**	**Audit Vault collection turned on**	**Database auditing / No Audit Vault**	**Audit Vault collection turned on**
Audit Load	10 records / second	10 records / second	100 records / second	100 records / second
OS Log	0.08%	0.7%	0.15%	2.7%
DB Audit	0.13%	0.5%	1.6%	3.4%
Redo	0%	3.7%	0%	8.2%

*Internal testing: Source: 4x32GB 3GHz Intel Xeons RHEL3.0, running 2 Oracle Database 10.2.0.3.0

AV Server: 2x6GB 3GHz Intel Xeons RHEL3.0, AV Server 10.2.2.0.0

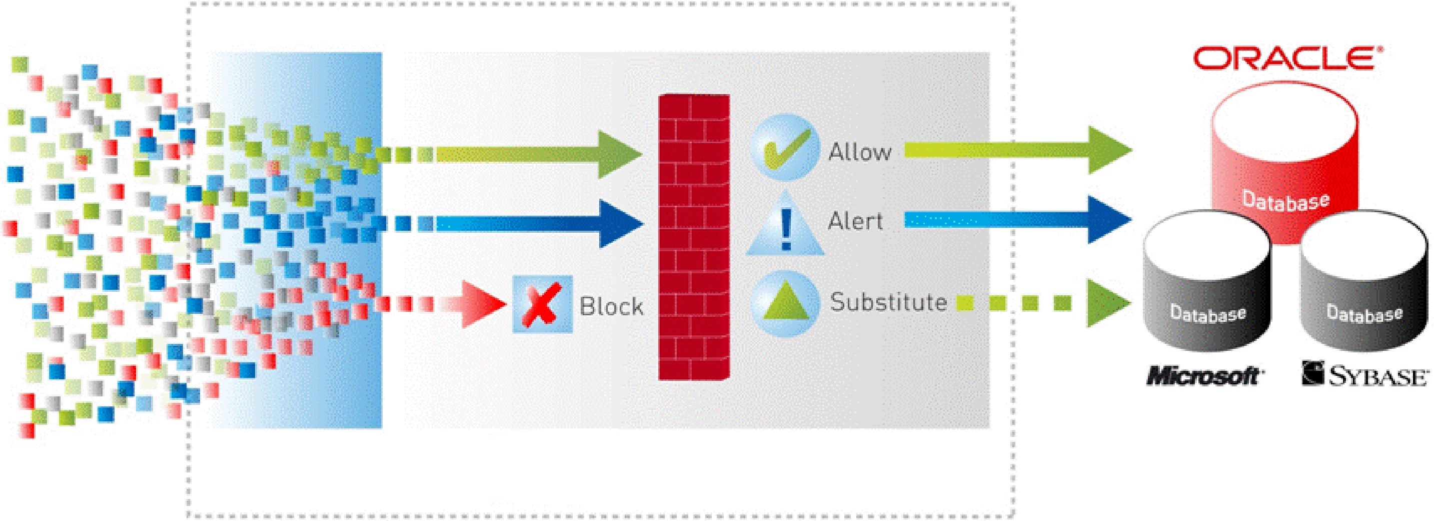


New Product:

Oracle Database Firewall

Oracle Database Firewall

First Line of Defense

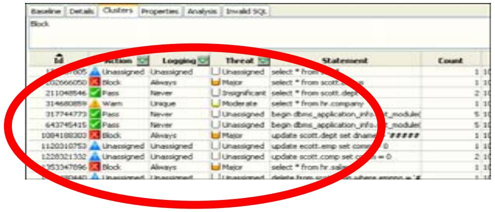


- Monitor database activity on network and log/block unauthorized database access
- Highly accurate SQL grammar based analysis to enforce normal activity
- Built-in and custom compliance reports for SOX, PCI, and other regulations

Challenges of a Database Firewall

- Building accurate policy profiles of good application behavior with changes over time
- Performance to your application as the number of transactions increase over the network
- Needing to throw more hardware on the network to handle my workload for scalability

Security Model and Policy Enforcement



Baseline | Details | Clusters | Properties | Analysis | Invalid SQL

Block

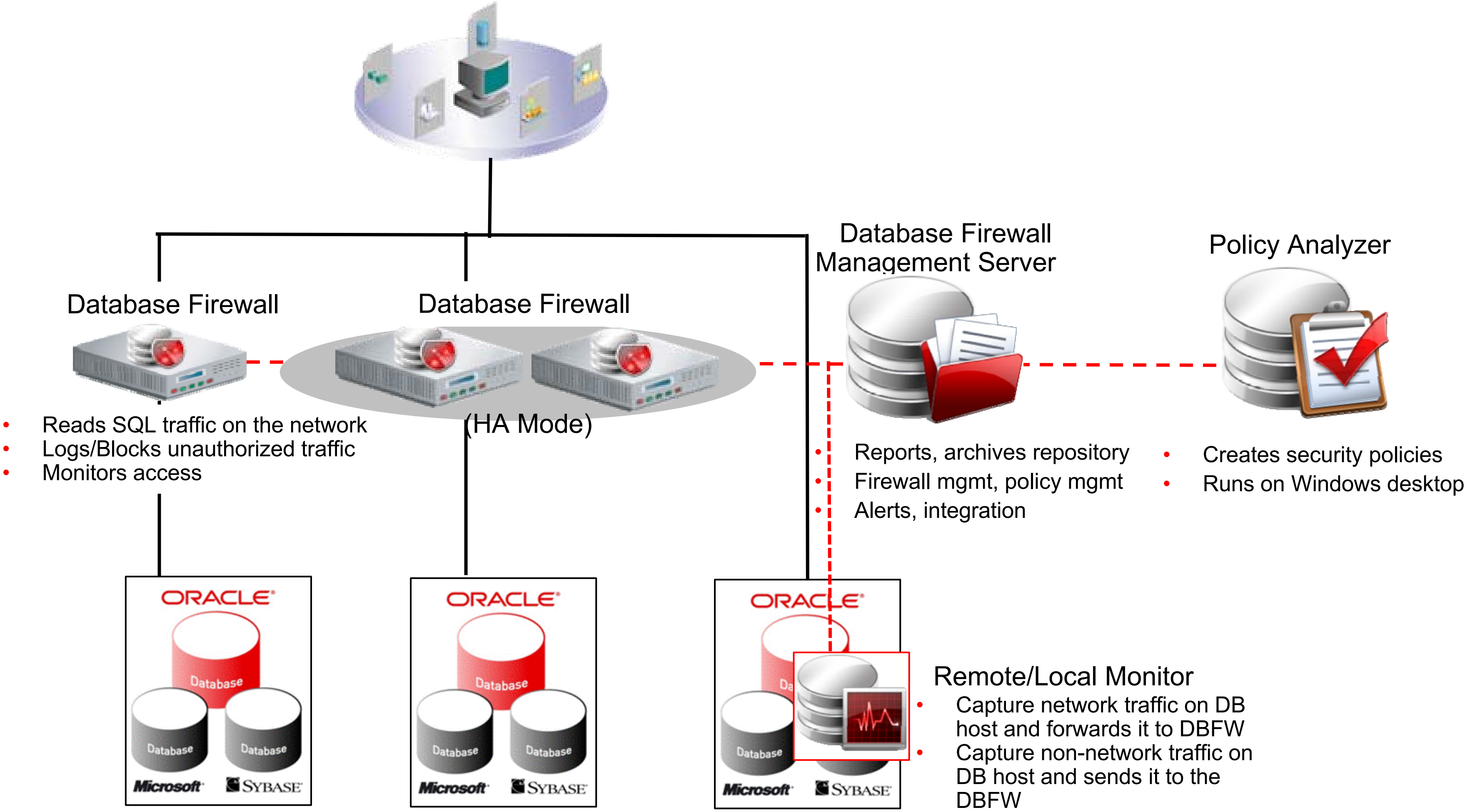
Id	Action	Logging	Threat	Statement	Count	
[illegible]605	▲ Unassigned	Unassigned	Unassigned	select * from [illegible]	1	[illegible]
1026666050	☒ Block	Always	Major	select * from scott.[illegible]	1	[illegible]
211048546	✓ Pass	Never	Insignificant	select * from scott.dept	2	[illegible]
314680859	⚠ Warn	Unique	Moderate	select * from hr.company	1	[illegible]
317744773	✓ Pass	Never	Unassigned	begin dbms_application_info.[illegible]t_module(	5	[illegible]
643745415	✓ Pass	Never	Unassigned	begin dbms_application_info.[illegible]t_module(	5	[illegible]
1084188303	☒ Block	Always	Major	update scott.dept set dname[illegible] '#####	1	[illegible]
1120310753	▲ Unassigned	Unassigned	Unassigned	update ecott.emp set comm[illegible] 0	1	[illegible]
1228321332	▲ Unassigned	Unassigned	Unassigned	update scott.comp set co[illegible] = 0	2	[illegible]
1353347896	☒ Block	Always	Major	select * from hr.sala[illegible]	1	[illegible]
[illegible]80440	▲ Unassigned	Unassigned	Unassigned	delete from [illegible] where empno = '#	1	[illegible]

- Policy Enforcement
  - Performance and scalability since millions of statements can be simplified into a small number of SQL characteristics or “clusters”
  - High level of accuracy
  - Flexible enforcement: block, substitute, alert and pass, log only
- Policies are easily configured using:
  - White List
    - Can be automatically generated for any application
    - “Allowed” behavior can be defined for any user or application
    - Transactions found not to match the policy instantly rejected
  - Black List
    - Stop unwanted transactions, users or schema access
    - Prevent privilege or role escalation and illegal access to sensitive data by using factors
    - Selectively block any part of transaction in context to your business and security goals

Heterogeneous Database Support

- Oracle 8i, 9i, 10g, 11g
- MS-SQL 2000, 2005, 2008
- Sybase 12.5.3 to 15
- SQL Anywhere v10

The Basic Components



Database Firewall

- Reads SQL traffic on the network
- Logs/Blocks unauthorized traffic
- Monitors access

Database Firewall

(HA Mode)

Database Firewall Management Server

- Reports, archives repository
- Firewall mgmt, policy mgmt
- Alerts, integration

Policy Analyzer

- Creates security policies
- Runs on Windows desktop

Remote/Local Monitor

- Capture network traffic on DB host and forwards it to DBFW
- Capture non-network traffic on DB host and sends it to the DBFW

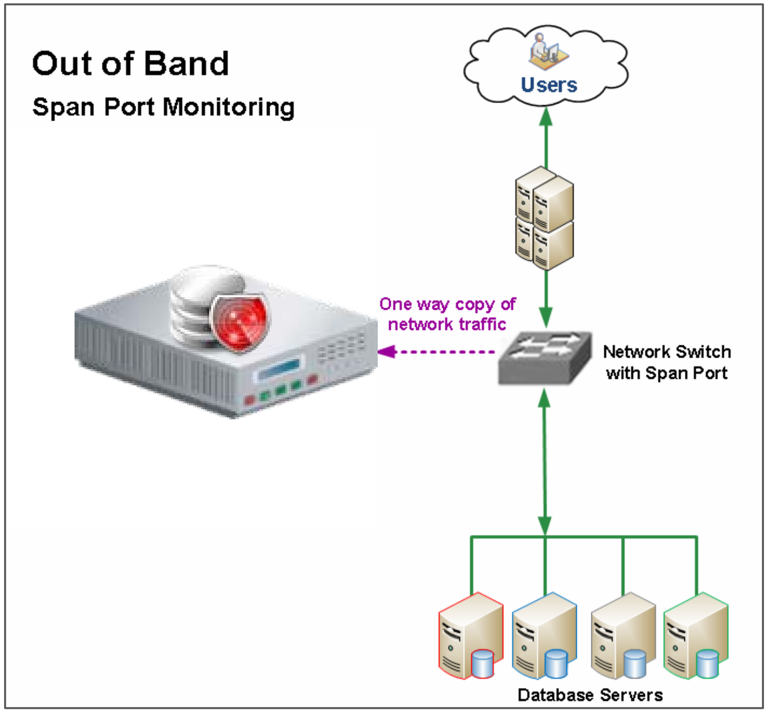
Oracle Database Firewall
Flexible Deployment Model

- Deploy on customer’s existing or new hardware:
  - Runs Oracle Enterprise Linux base operating system
  - Firewall blocking mode requires certified NIC card
- Scales vertically
  - Add CPU, disk, and memory to the servers versus adding more and more appliances
- Database Firewall and Database Firewall Management Server can co-reside

Oracle Database Firewall

Out of Band Deployment Mode

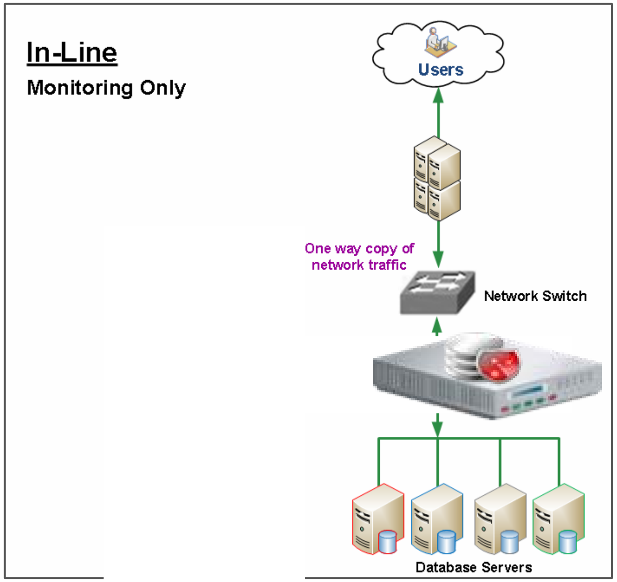
- **Monitor Only Mode – No Blocking**
- Also known as “SPAN” or “Span port” or “Mirrored” or “Tap”
- SQL logging and reporting only
- Easy for demo / POC or lab test
- Easy to deploy, no risk of impacting databases or applications

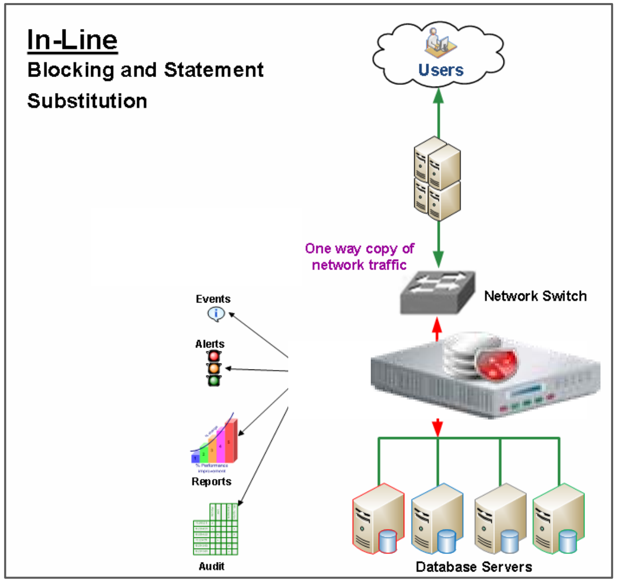

Out of Band
Span Port Monitoring
Users
One way copy of network traffic
Network Switch with Span Port
Database Servers

Oracle Database Firewall

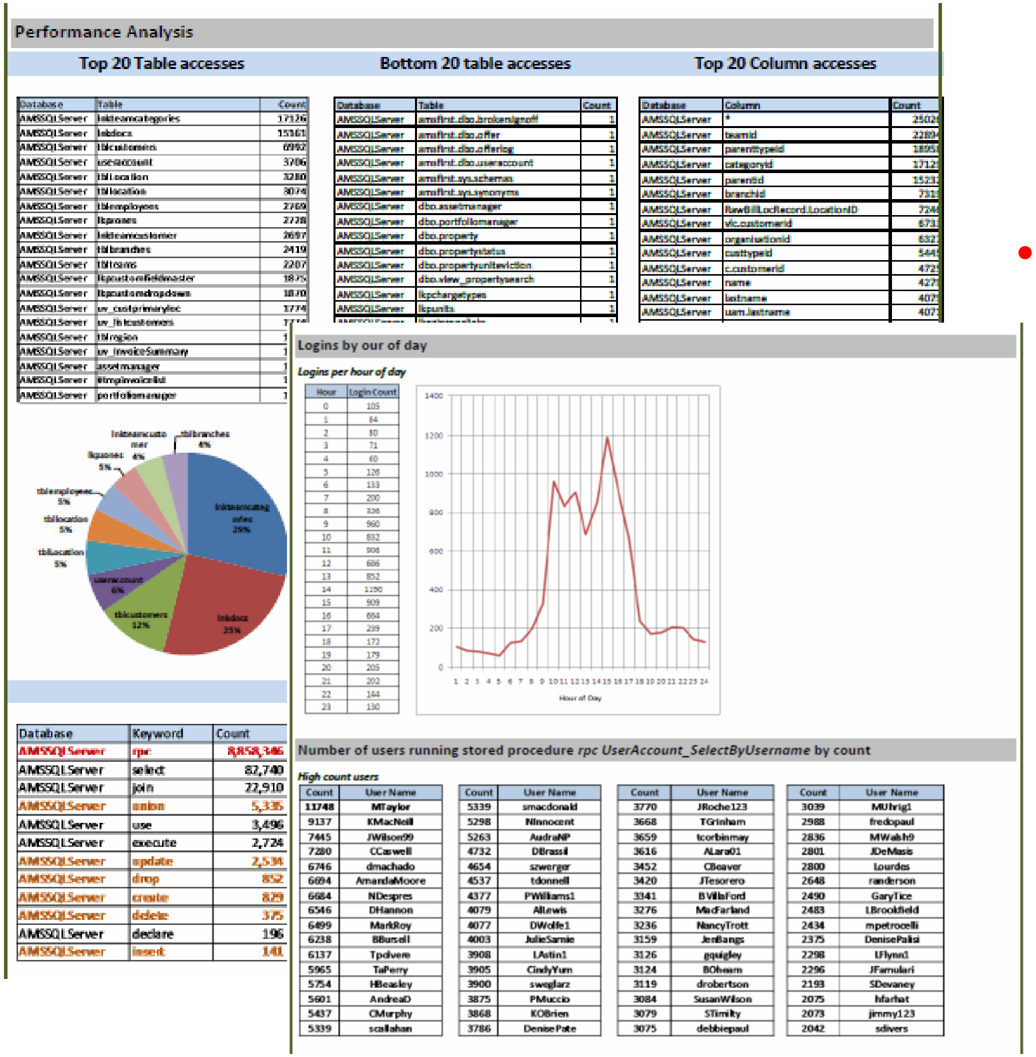
In-Line Deployment Modes

- **Blocking and Monitoring**
  - SQL traffic is inspected and verified against policy
  - Also known as a “Bridge” or “transparent bridge”
  - Sometimes only option if out-of-band ports are not available




In-Line
Blocking and Statement Substitution
Users
One way copy of network traffic
Network Switch
Events
Alerts
Reports
Audit
Database Servers

Reporting



Performance Analysis

Top 20 Table accesses

Database	Table	Count
AMSSQLServer	inkteamcategories	17126
AMSSQLServer	inkdocs	15161
AMSSQLServer	tblcustomers	6992
AMSSQLServer	useraccount	3706
AMSSQLServer	tblLocation	3280
AMSSQLServer	tbllocation	3074
AMSSQLServer	tblemployees	2769
AMSSQLServer	lkpzones	2728
AMSSQLServer	inkteamcustomer	2697
AMSSQLServer	tblbranches	2419
AMSSQLServer	tblteams	2207
AMSSQLServer	lkpcustomfieldmaster	1875
AMSSQLServer	lkpcustomdropdown	1870
AMSSQLServer	uv_custprimaryloc	1774
AMSSQLServer	uv_lnkcustomers	[illegible]
AMSSQLServer	tblregion	1
AMSSQLServer	uv_InvoiceSummary	1
AMSSQLServer	assetmanager	1
AMSSQLServer	#tmpinvoicelist	1
AMSSQLServer	portfoliomanager	1

Bottom 20 table accesses

Database	Table	Count
AMSSQLServer	amsfirst.dbo.brokersignoff	1
AMSSQLServer	amsfirst.dbo.offer	1
AMSSQLServer	amsfirst.dbo.offerlog	1
AMSSQLServer	amsfirst.dbo.useraccount	1
AMSSQLServer	amsfirst.sys.schemas	1
AMSSQLServer	amsfirst.sys.synonyms	1
AMSSQLServer	dbo.assetmanager	1
AMSSQLServer	dbo.portfoliomanager	1
AMSSQLServer	dbo.property	1
AMSSQLServer	dbo.propertystatus	1
AMSSQLServer	dbo.propertyuniteviction	1
AMSSQLServer	dbo.view_propertysearch	1
AMSSQLServer	lkpchargetypes	1
AMSSQLServer	lkpunits	1

Top 20 Column accesses

Database	Column	Count
AMSSQLServer	*	25028
AMSSQLServer	teamid	22894
AMSSQLServer	parenttypeid	18958
AMSSQLServer	categoryid	17129
AMSSQLServer	parentid	15232
AMSSQLServer	branchid	7319
AMSSQLServer	RawBillLocRecord.LocationID	7246
AMSSQLServer	vlc.customerid	6731
AMSSQLServer	organisationid	6321
AMSSQLServer	custtypeid	5445
AMSSQLServer	c.customerid	4725
AMSSQLServer	name	4275
AMSSQLServer	lastname	4075
AMSSQLServer	uam.lastname	4073

Database	Keyword	Count
AMSSQLServer	rpc	8,858,346
AMSSQLServer	select	82,740
AMSSQLServer	join	72,910
AMSSQLServer	union	5,335
AMSSQLServer	use	3,496
AMSSQLServer	execute	2,724
AMSSQLServer	update	2,534
AMSSQLServer	drop	852
AMSSQLServer	create	829
AMSSQLServer	delete	375
AMSSQLServer	declare	196
AMSSQLServer	insert	141

Logins by our of day

Logins per hour of day

Hour	Login Count
0	105
1	84
2	80
3	71
4	60
5	126
6	133
7	200
8	326
9	960
10	832
11	906
12	686
13	852
14	1190
15	909
16	664
17	239
18	172
19	179
20	205
21	202
22	144
23	130

Number of users running stored procedure *rpc UserAccount_SelectByUsername* by count

High count users

Count	User Name	Count	User Name	Count	User Name	Count	User Name
11748	MTaylor	5339	smacdonald	3770	JRoche123	3039	MUhrig1
9137	KMacNeill	5298	NInnocent	3668	TGrinham	2988	fredopaul
7445	JWilson99	5263	AudraNP	3659	tcorbinmay	2836	MWalsh9
7280	CCaswell	4732	DBrassil	3616	ALara01	2801	JDeMasis
6746	dmachado	4654	szwerger	3452	CBeaver	2800	lourdes
6694	AmandaMoore	4537	tdonnell	3420	JTesorero	2648	randerson
6684	NDespres	4377	PWilliams1	3341	BVillaFord	2490	GaryTice
6546	DHannon	4079	AlLewis	3276	MacFarland	2483	LBrookfield
6499	MarkRoy	4077	DWolfe1	3236	NancyTrott	2434	mpetrocelli
6238	BBursell	4003	JulieSarnie	3159	JenBangs	2375	DenisePalisi
6137	Tpdivere	3908	LAstin1	3126	gquigley	2298	LFlynn1
5965	TaPerry	3905	CindyYum	3124	BOhearn	2296	JFamulari
5754	HBeasley	3900	sweglarz	3119	drobertson	2193	SDevaney
5601	AndreaD	3875	PMuccio	3084	SusanWilson	2075	hfarhat
5437	CMurphy	3868	KOBrien	3079	STimilty	2073	jimmy123
5339	scallahan	3786	DenisePate	3075	debbiepaul	2042	sdivers

- Database Firewall log data consolidated into reporting database
- Over 130 built in reports that can be modified/customized
  - Entitlement report for database attestation
  - Activity and privileged user reports
  - Supports demonstrating PCI, SOX, HIPAA, etc.

Accurate, Scalable, Flexible

- **Most accurate**

  Zero false positives and the competition can never get the policy created

- **Most scalable**

  Scales easily by adding more CPU’s, more disk, more memory to accommodate growth.

- **Most flexible**

  Software and can be deployed onto any server that supports OEL. These platforms can be servers, blades or virtual platforms.

Fast, Transparent, Open

- **Fastest**
  You get more transactions through put per second that an equivalent competitive solution

- **Easiest to deploy**
  Ability to understand the SQL language and categorize 10’s of thousands of transactions, results in simple policy configuration

- **Open Reporting**
  Documented database tables enables customers to use virtually any reporting tool to extract forensic or summary data.

Q&A

ORACLE IS THE INFORMATION COMPANY