

SECURE DATA AT THE SOURCE  
SAVE TIME AND MONEY



Security Inside Out

Oracle Database Security

**ORACLE<sup>®</sup>**

## **Oracle Database Security**

**Paul Needham, Senior Director, Product Management, Database Security**



# Target of Data Breaches

2010 Data Breach  
Investigations Report

Type	Category	% Breaches	% Records
Database Server	Servers & Applications	25%	92%
Desktop Computer	End-User Devices	21%	1%

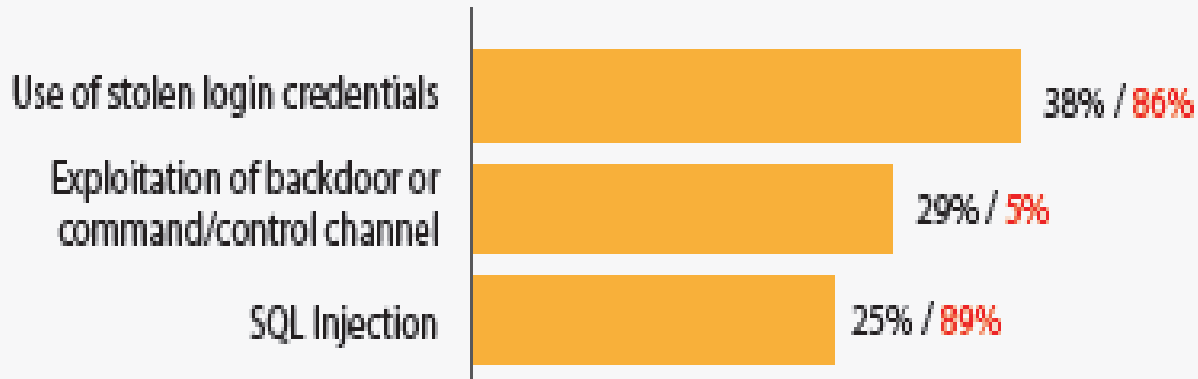
Web app/server	Servers & Applications	19%	13%
Payment card	Offline Data	18%	<1%
POS server (store controller)	Servers & Applications	11%	<1%
Laptop computer	End-User Devices	7%	<1%
Documents	Offline Data	7%	<1%
POS terminal	End-User Devices	6%	<1%
File server	Servers & Applications	4%	81%
Automated Teller Machine (ATM)	End-User Devices	4%	<1%
FTP server	Servers & Applications	2%	3%
Mail server	Servers & Applications	2%	4%

# How do Database Breaches Occur?

2010 Data Breach  
Investigations Report

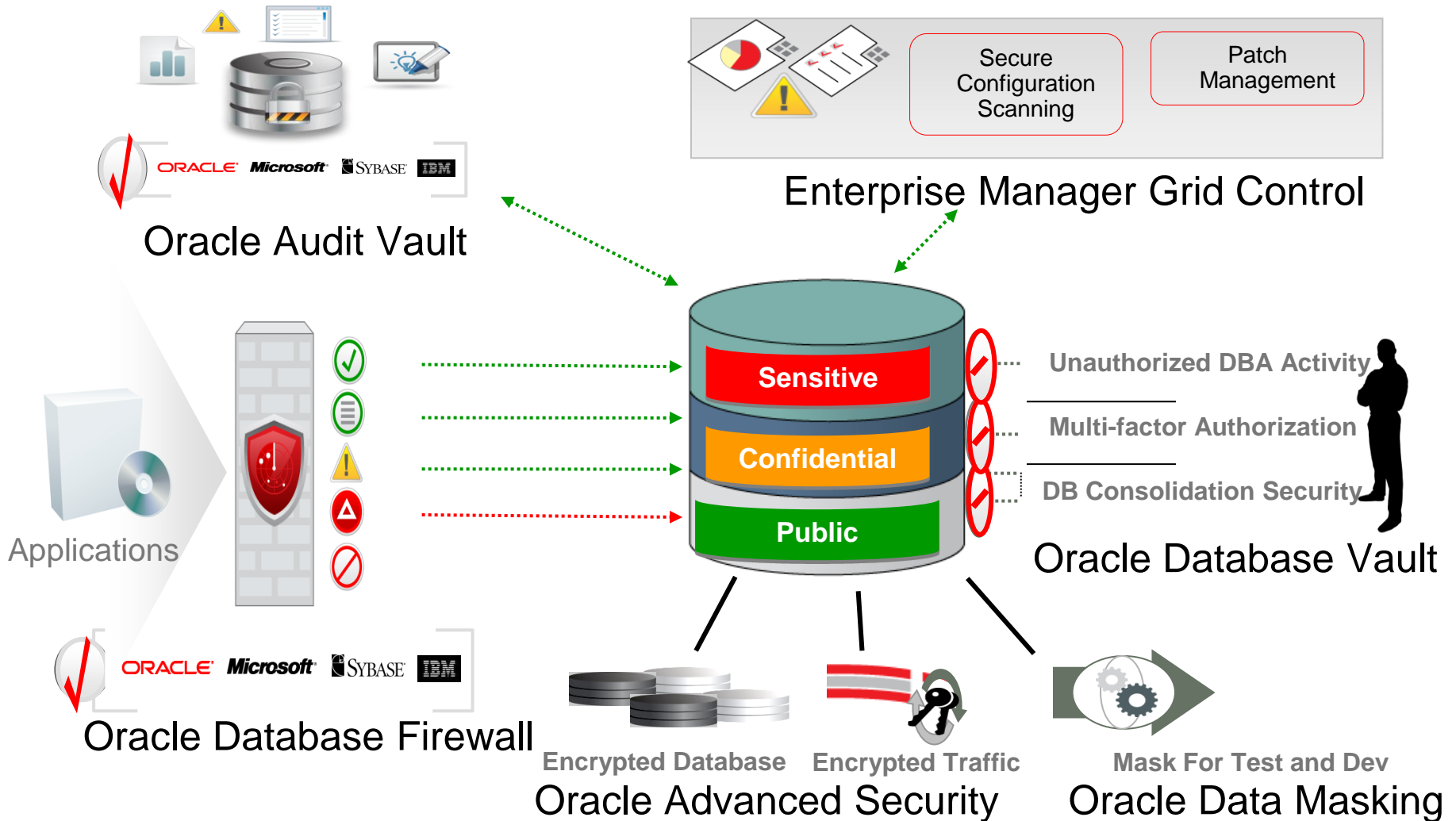
48% involved privilege misuse  
40% resulted from hacking

Figure 21. Types of hacking by percent of breaches within Hacking and percent of records



38% utilized malware  
28% employed social tactics  
15% comprised physical attacks

# Oracle Maximum Security Architecture



# Database Defense-in-Depth



## Monitoring and Blocking

- Oracle Database Firewall

## Auditing and Tracking

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

## Access Control

- Oracle Database Vault
- Oracle Label Security

## Encryption and Masking

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

# Database Defense-in-Depth

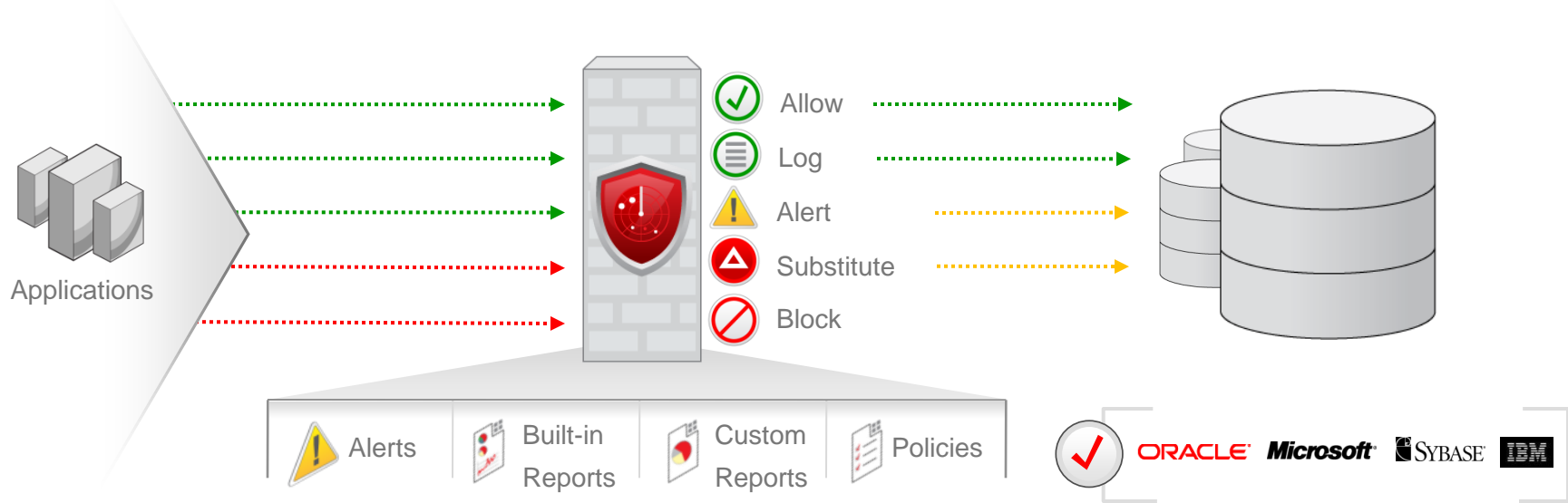


## Blocking and Monitoring

- Oracle Database Firewall

# Oracle Database Firewall

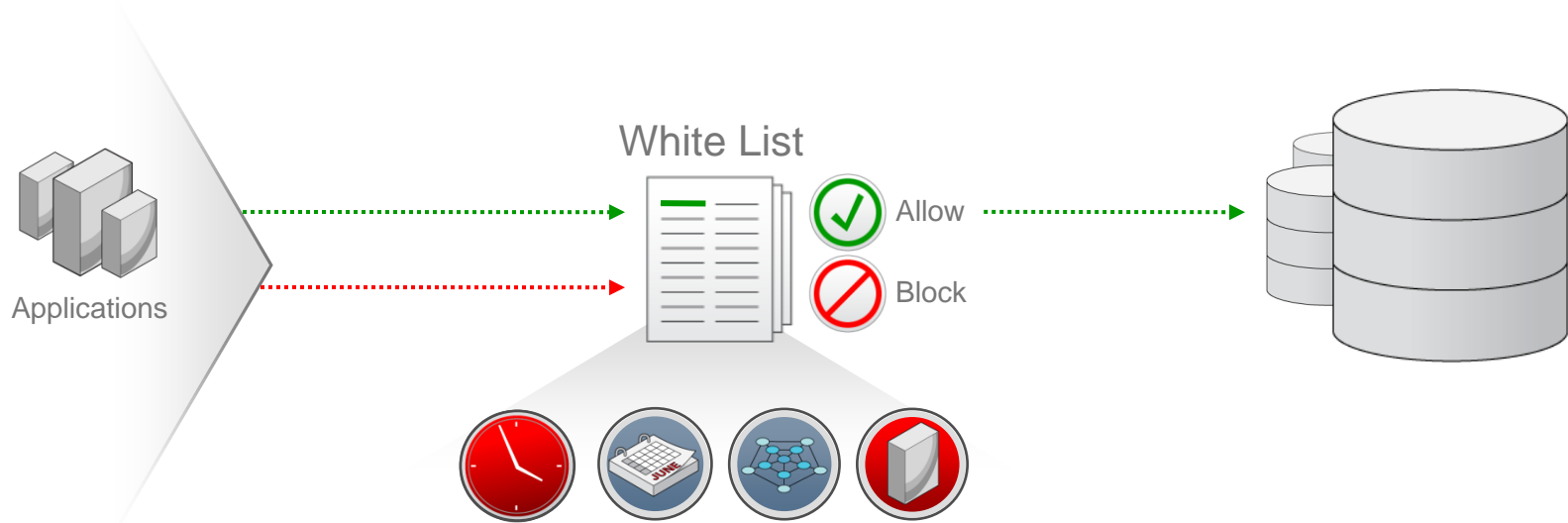
## First Line of Defense



- Monitor database activity to help prevent unauthorized activity, application bypass and SQL injections
- Highly accurate SQL grammar based analysis
- White-list, black-list, and exception-list based security policies
- Built-in and custom compliance reports for regulations

# Oracle Database Firewall

## Positive Security Model Based Enforcement

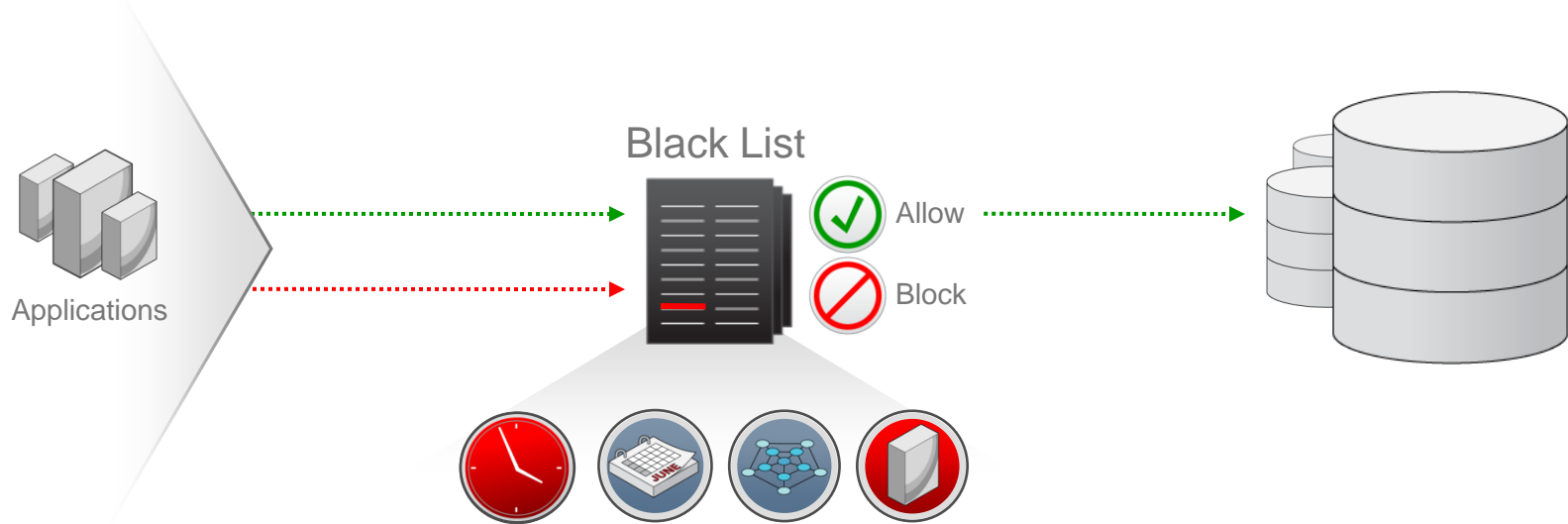


- White-list based policies enforce normal or expected behavior
- Policies evaluate factors such as time, day, network, and application
- Easily generate white-lists for any application
- Out of policy SQL statements can be logged, alerted, blocked or substituted with a harmless SQL statement
- SQL substitution foils attackers without disrupting applications



# Oracle Database Firewall

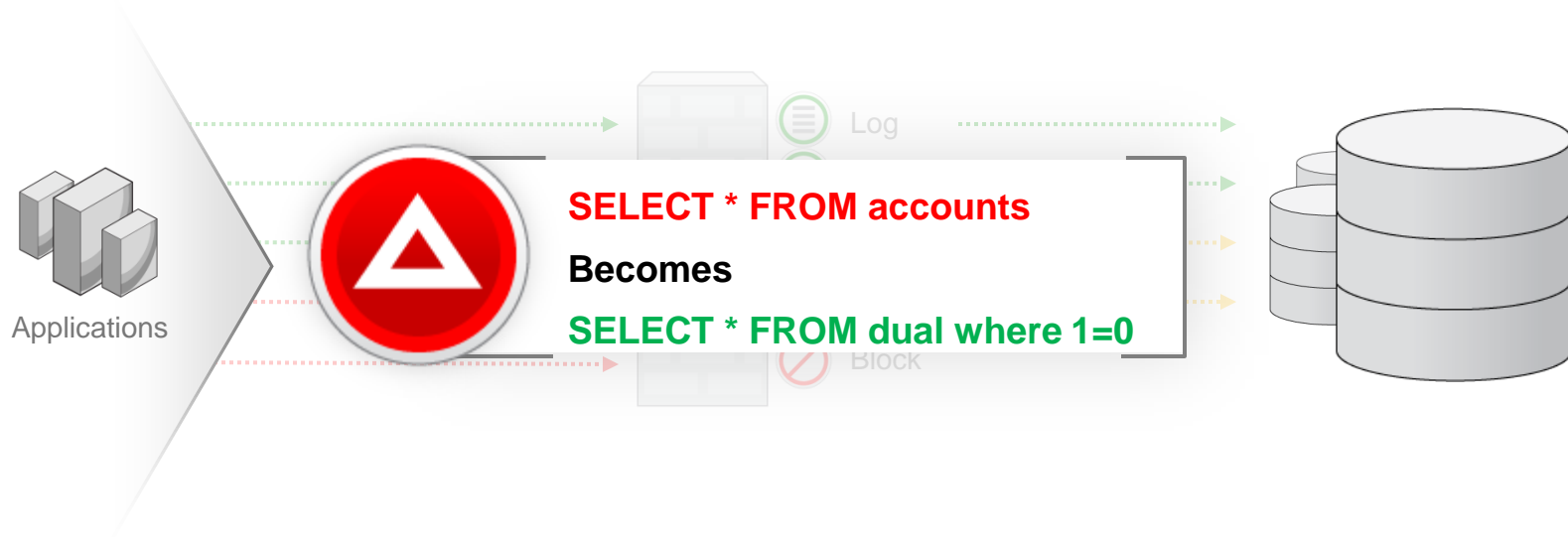
## Negative Security Model Based Enforcement



- Stop specific unwanted SQL commands, user, or schema access
- Prevent privilege or role escalation and unauthorized access to sensitive data
- Black list policies can evaluate factors such as day, time, network, and application

# Oracle Database Firewall

## Scalable and Safe Policy Enforcement



- Innovative SQL grammar technology reduces millions of SQL statements into a small number of SQL characteristics or “clusters”
- Flexible enforcement at SQL level: block, substitute, alert and pass, log only
  - SQL substitution foils attackers without disrupting applications
- Centralized policy management and reporting
- Superior performance and policy scalability

## Online Orders

Logout | Welcome JTAYLOR

[Home](#)
[My Orders](#)
[New Orders](#)
[Shipping](#)
[Reports](#)
[Help](#)

**Search Orders**

Order Number	Customer Name	Order Amount	Region
753031	Albany Motors	2,500	AMERICAS
351134	Atlantic Boat Repair	10,000	AMERICAS
652178	Bethesda Flowers	12,000	AMERICAS
256124	Connecticut Composites	8,500	AMERICAS
652177	Lexington Exports	3,600	AMERICAS
626847	NYC Taxi Co	10,000	AMERICAS

1 - 6

## Online Orders

Logout | Welcome JTAYLOR

Home **My Orders** New Orders Shipping Reports Help

UNION SELECT ORDER\_NUMBER, CUSTOMER\_NAME

Search Orders

Order Number	Customer Name	Order Amount	Region
181467	Acme Glass	8,800	4074 0049 0000 8125
753031	Albany Motors	2,500	3715 0990 5550 7814
351245	Asymmetrical Antibiotics Inc	22,000	6011 0880 0000 8285
351134	Atlantic Boat Repair	10,000	6793 0000 2342 7692
652178	Bethesda Flowers	12,000	4926 0050 0000 2188
529152	Brookhaven Landscaping	5,000	4264 0000 0000 7084
302599	Central NJ Cable	7,200	4018 0065 0087 1416
185847	Colorado Clinicians	4,600	3715 0930 0000 4558
256124	Connecticut Composites	8,500	4264 0660 0000 4175
214115	Department of Elegant Programming	1,250	4264 0000 0000 9129
461536	Healthy Foods	9,800	3715 0330 1430 2205
.....	.. . . .	.....	.....



### Oracle Database Firewall Administration Console

Threat Status: Warning

Throughput Status: OK

Traffic Snapshot at 2010-09-21 15:01

	Known Blocked:	0
	Unseen Blocked:	1
	Known Warned:	0
	Unseen Warned:	12

	Statement Rate:	0
	Total Statements:	476
	(In Last Hour)	

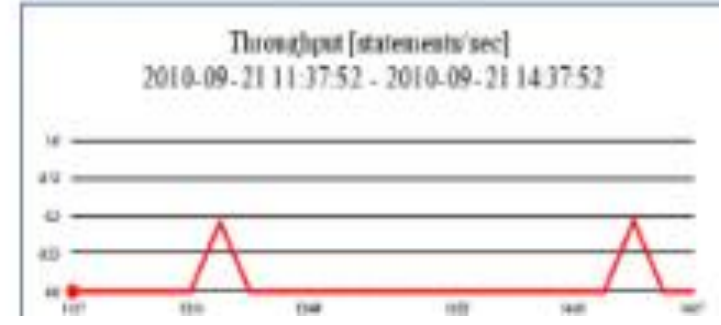
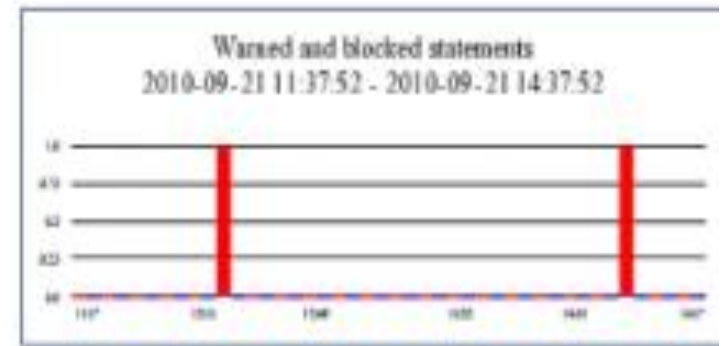
Filter (no filter active)

#### Quick Start

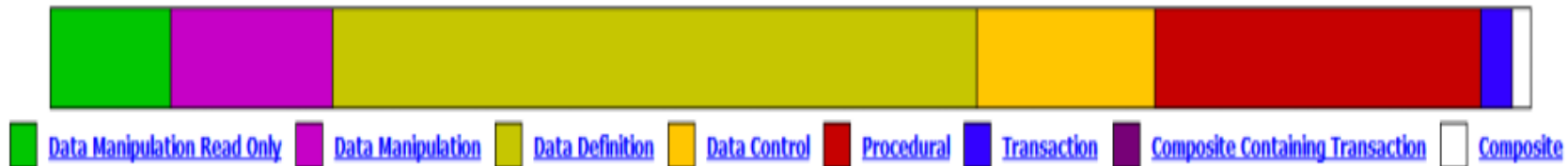
- Monitor databases
- System settings

#### Top Ten Threats (Last Week)

Count	Status	Statement	Seen	Log Level	Source	Destination
2		select order_numbe...	no	always	192.168.56.10	192.168.56.41
1		select order_numbe...	no	always	192.168.56.10	192.168.56.41



Statement Class Distribution



Data manipulation (read only):	15
Data manipulation:	20
Data definition:	79
Data control:	22
Procedural:	40
Transaction:	0
Composite Containing Transaction:	0
Composite:	0

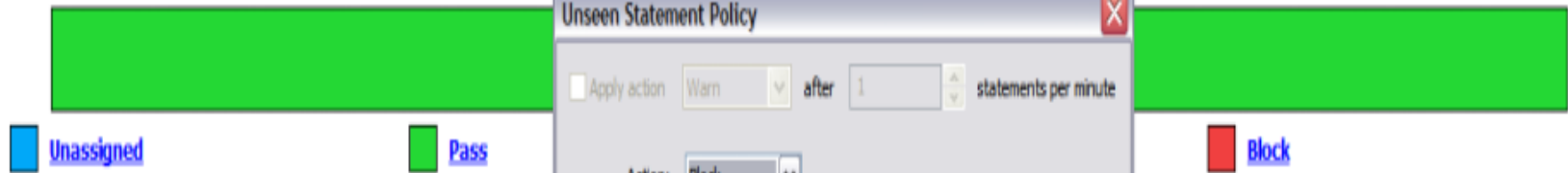
Threat Severity Distribution



Assign Threat Severities

Unassigned:	0
Insignificant:	181
Minor:	0
Moderate:	0
Major:	0
Catastrophic:	0

Action Distribution



Assign Policies

Unassigned:	0
Passed:	181
Warned:	0
Blocked:	0

Baseline Rules

Novelty statement policies

Baseline Defaults

**Unseen Statement Policy** [Close]

Apply action Warn after 1 statements per minute

Action: Block

Logging Level: Always

Threat Severity: Major

Substitute Statement: `select 100 from dual where 1=2`

Notes:

New Novelty Policy...

Action:	Block
Threat:	Major

# Online Orders

Logout | Welcome JTAYLOR

Home | **My Orders** | New Orders | Shipping | Reports | Help

UNION SELECT ORDER\_NUMBER, CUSTOMER\_NAME

Search Orders

no data found

Built using Oracle Application Express



# Database Defense-in-Depth



## Monitoring and Blocking

- Oracle Database Firewall

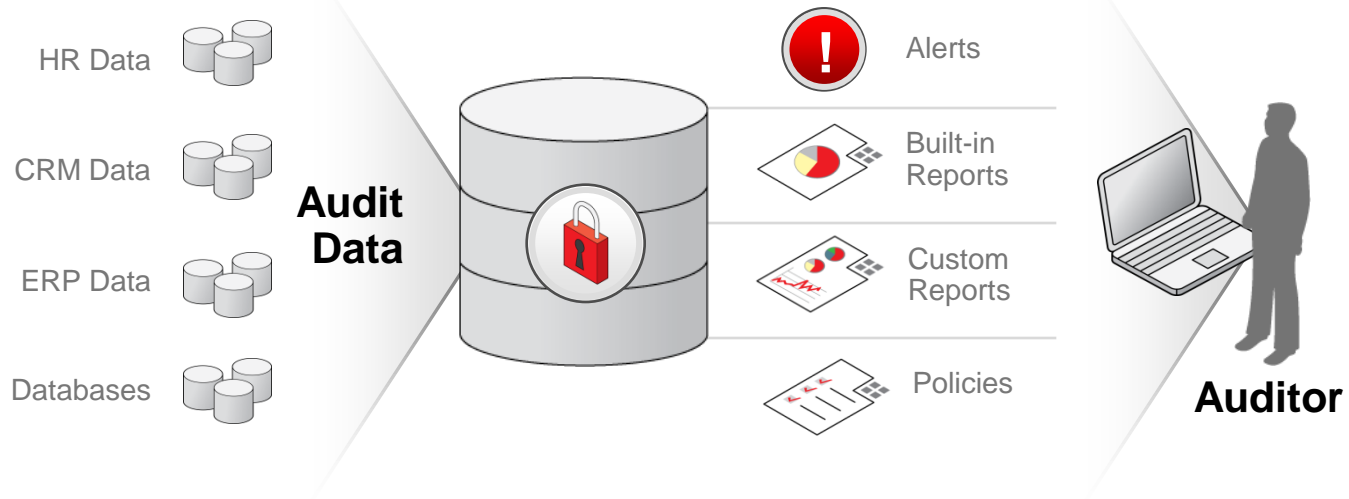
## Auditing and Tracking

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



# 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



Access Reports



- [Activity Overview](#)
- [Data Access](#)
- [Database Vault](#)
- [Distributed Database](#)
- [Procedure Executions](#)
- [User Sessions](#)

Management Activity Reports



- [Account Management](#)
- [Audit Commands](#)
- [Object Management](#)
- [Procedure Management](#)
- [Role and Privilege Management](#)
- [System Management](#)

System Exception Reports



- [Exception Activity](#)
- [Invalid Audit Record Activity](#)
- [Uncategorized Activity](#)

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](#)

Alert Reports



- [All Alerts](#)
- [Critical Alerts](#)
- [Warning Alerts](#)

All times are UTC-08:00

Credit Card



- [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](#)
- [User Privilege Change Activity](#)

SOX

Widget's SOX Reports



- [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](#)
- [User Privilege Change Activity](#)

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](#)
- [User Privilege Change Activity](#)

Tasks

- Customize Categories

All times are UTC-08:00



Data Access

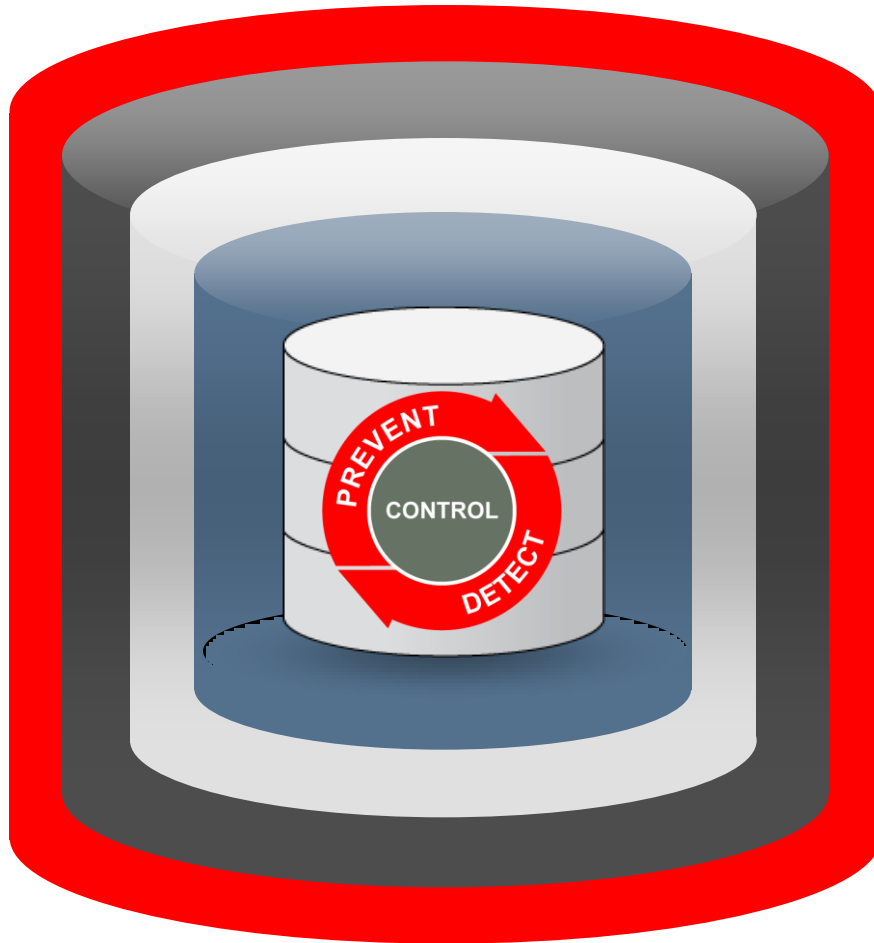
Rows

Event Time is in the last 24 hours

Source	Target	Event	Event Status	User	Host	Event Time
PAYROLL.ORACLE.VM	INVENTORIES	SELECT	SUCCESS	APPS	oel4upd4.oracle.vm	3/11/2010 02:14:17 PM
PAYROLL.ORACLE.VM	INVENTORIES	SELECT	SUCCESS	APPS	oel4upd4.oracle.vm	3/11/2010 02:14:17 PM
PAYROLL.ORACLE.VM	CUSTOMERS	DELETE	UNKNOWN:FGA	OE	oel4upd4.oracle.vm	3/11/2010 02:14:16 PM
PAYROLL.ORACLE.VM	CUSTOMERS	INSERT	UNKNOWN:FGA	OE	oel4upd4.oracle.vm	3/11/2010 02:14:15 PM
PAYROLL.ORACLE.VM	CUSTOMERS	UPDATE	UNKNOWN:FGA	OE	oel4upd4.oracle.vm	3/11/2010 02:14:15 PM
PAYROLL.ORACLE.VM	ORDERS	UPDATE	UNKNOWN:FGA	OE	oel4upd4.oracle.vm	3/11/2010 02:14:15 PM
PAYROLL.ORACLE.VM	SALES	SELECT	UNKNOWN:FGA	PJONES	oel4upd4.oracle.vm	3/11/2010 02:14:1 PM
PAYROLL.ORACLE.VM	ORDERS	SELECT	UNKNOWN:FGA	PJONES	oel4upd4.oracle.vm	3/11/2010 02:14:0 PM
PAYROLL.ORACLE.VM	ORDERS	SELECT	UNKNOWN:FGA	PJONES	oel4upd4.oracle.vm	3/11/2010 02:14:0 PM
PAYROLL.ORACLE.VM	RDF_RULEBASES	SELECT	942	JSMITH	oel4upd4.oracle.vm	3/11/2010 02:13:53 PM
PAYROLL.ORACLE.VM	EMP2	TRUNCATE TABLE	SUCCESS	JTAYLOR	oel4upd4.oracle.vm	3/11/2010 02:13:47 PM
PAYROLL.ORACLE.VM	RDF_RULEBASES	SELECT	942	PJONES	oel4upd4.oracle.vm	3/11/2010 02:13:43 PM
PAYROLL.ORACLE.VM	RDF_RULEBASES	SELECT	942	PJONES	oel4upd4.oracle.vm	3/11/2010 02:13:22 PM
PAYROLL.ORACLE.VM	SRC_TAB1	DELETE	UNKNOWN:FGA	JSCHAFFER	oel4upd4.oracle.vm	3/11/2010 02:13:2 PM
PAYROLL.ORACLE.VM	SRC_TAB1	DELETE	UNKNOWN:FGA	JSCHAFFER	oel4upd4.oracle.vm	3/11/2010 02:13:2 PM

1 - 15

# Database Defense-in-Depth



## Monitoring and Blocking

- Oracle Database Firewall

## Auditing and Tracking

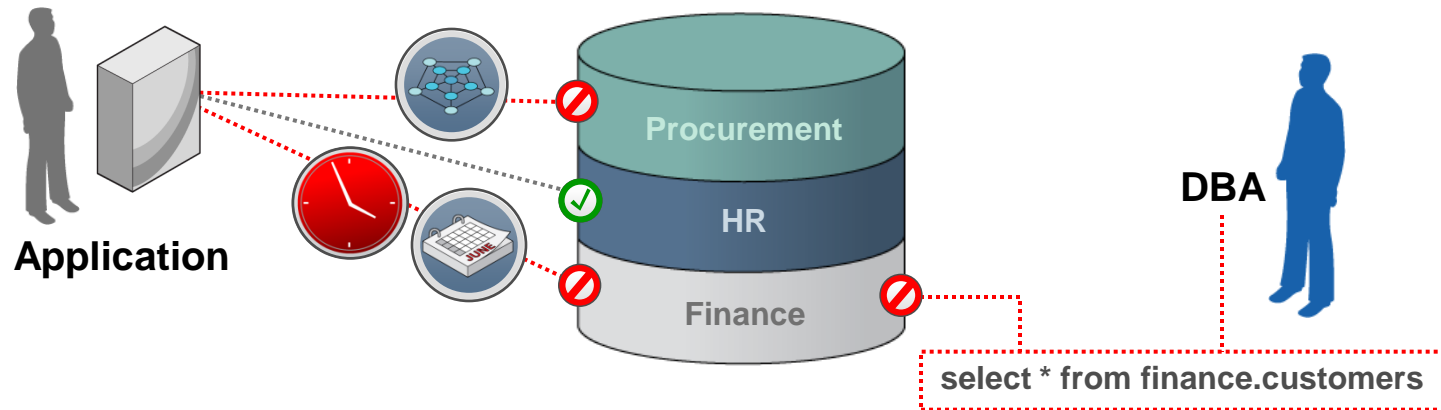
- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

## Access Control

- Oracle Database Vault
- Oracle Label Security

# Oracle Database Vault

## Privileged Account Controls



- Limit access of privileged accounts
- No application changes required
- Works with Oracle Exadata Database Machine
- Protect application data and prevent application by-pass





Connections Reports



Connections

- DBA - JSMITH
  - Tables
  - Views
  - Indexes
  - Packages
  - Procedures
  - Functions
  - Triggers
  - Types
  - Sequences
  - Materialized Views
  - Materialized View Logs
  - Synonyms
  - Public Synonyms
  - Database Links
  - Directories
  - Recycle Bin
  - Other Users
  - Financials - DBA

DBA - JSMITH



0.065 seconds

DBA - JSMITH

Enter SQL Statement:

```
select * from sysadm.t_ps_acct_1n;
```

Results Script Output Explain DBMS Output OWA Output

Results:

	PURCHASE_PRICE	BUSINESS_UNIT	FISCAL_YEAR	PRODUCT	TRANSACTION_ID
1	13354.00	AJ123	2006	C22	T9837JR867
2	786221.00	FJ33	2006	S22	T991856123
3	81954.00	LX82	2006	Z83	T97856842
4	98174.00	LX82	2006	Z83	T918356834
5	76985.00	LX82	2006	Z83	T98568234
6	87675.00	AJ123	2006	C22	T978892384
7	27579.00	FJ33	2006	S22	T995928345
8	38692.00	ST385	2006	L11	T97384956
9	78963.00	ST385	2006	L11	T903984856
10	19877.00	ST385	2006	L11	T97728356
11	76785.00	FJ33	2006	S22	T938682934
12	45636.00	LX82	2006	Z83	T998868283
13	17733.00	AK123	2006	C22	T988612571

# Step 2. Adding Protected Schema

The screenshot shows the Oracle Database Vault interface. At the top left is the Oracle logo and 'Database Vault'. At the top right are 'Help' and 'Logout' links, and a 'Database' tab. Below the header is a breadcrumb trail: 'Database Instance: un102232 > Realms > Edit Realm: PeopleSoft Realm > Create Realm Secured Object logged in as DBV\_OWNER'. The main title is 'Create Realm Secured Object'. There are 'Cancel' and 'OK' buttons at the top right. The instruction reads: 'Define a database schema or database role that is protected by the realm.' There are three input fields: 'Object Owner' with a dropdown menu showing 'SYSADM', 'Object Type' with a dropdown menu showing '%', and 'Object Name' with a text box containing '%'. At the bottom right, there are 'Cancel' and 'OK' buttons.

ORACLE Database Vault Help Logout

**Database**

Database Instance: un102232 > Realms > Edit Realm: PeopleSoft Realm > Create Realm Secured Object logged in as DBV\_OWNER

## Create Realm Secured Object

Cancel OK

Define a database schema or database role that is protected by the realm.

**Object Owner**

SYSADM

**Object Type**

%

**Object Name**

%

Cancel OK





Connections Reports



Connections

DBA - JSMITH

- Tables
- Views
- Indexes
- Packages
- Procedures
- Functions
- Triggers
- Types
- Sequences
- Materialized Views
- Materialized View Logs
- Synonyms
- Public Synonyms
- Database Links
- Directories
- Recycle Bin
- Other Users
- Financials - DBA



DBA - JSMITH



0.026 seconds

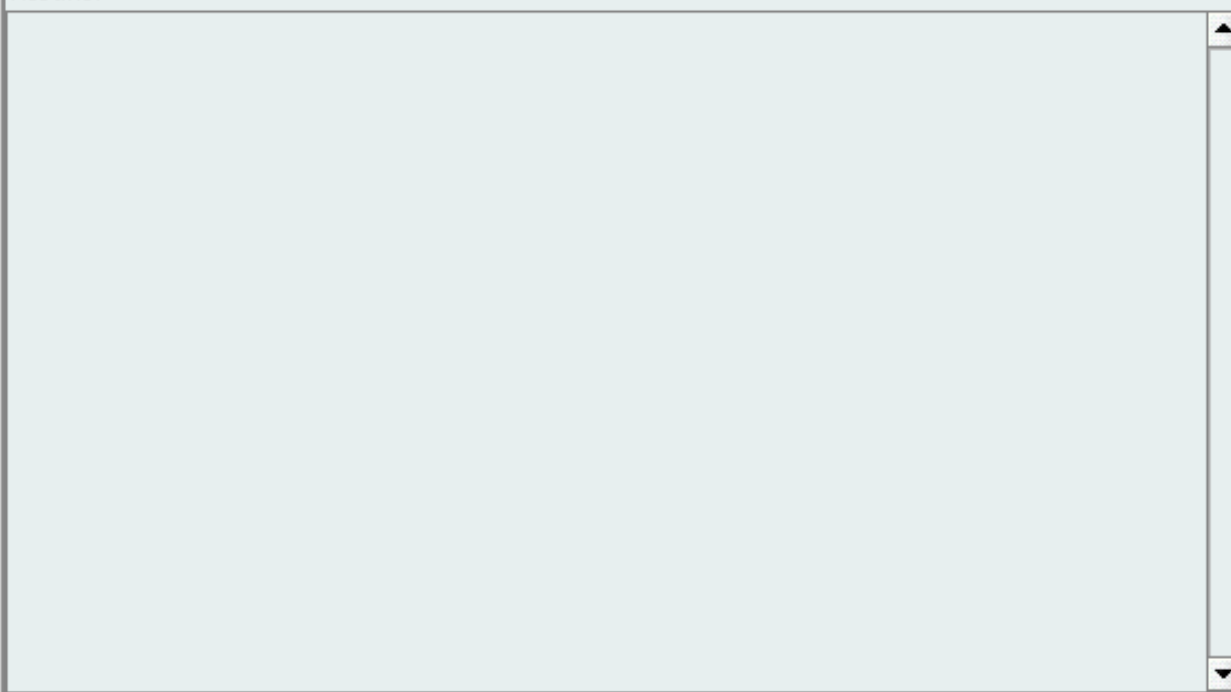
DBA - JSMITH

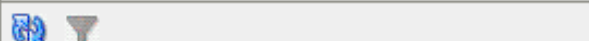
Enter SQL Statement:

```
select * from sysadm.t_ps_acct_1n;
```

Results Script Output Explain DBMS Output OWA Output

Results:





```
select * from sysadm.t_ps_acct_1n;
```

## ORA-01031: insufficient privileges



An error was encountered performing the requested operation:

ORA-01031: insufficient privileges

Error at line:1 Column:21

OK

- Tables
- Views
- Indexes
- Packages
- Procedures
- Functions
- Triggers
- Types
- Sequences
- Materialized Views
- Materialized View Logs
- Synonyms
- Public Synonyms
- Database Links
- Directories
- Recycle Bin
- Other Users
- Financials - DBA

# Database Defense-in-Depth



## Monitoring and Blocking

- Oracle Database Firewall

## Auditing and Tracking

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

## Access Control

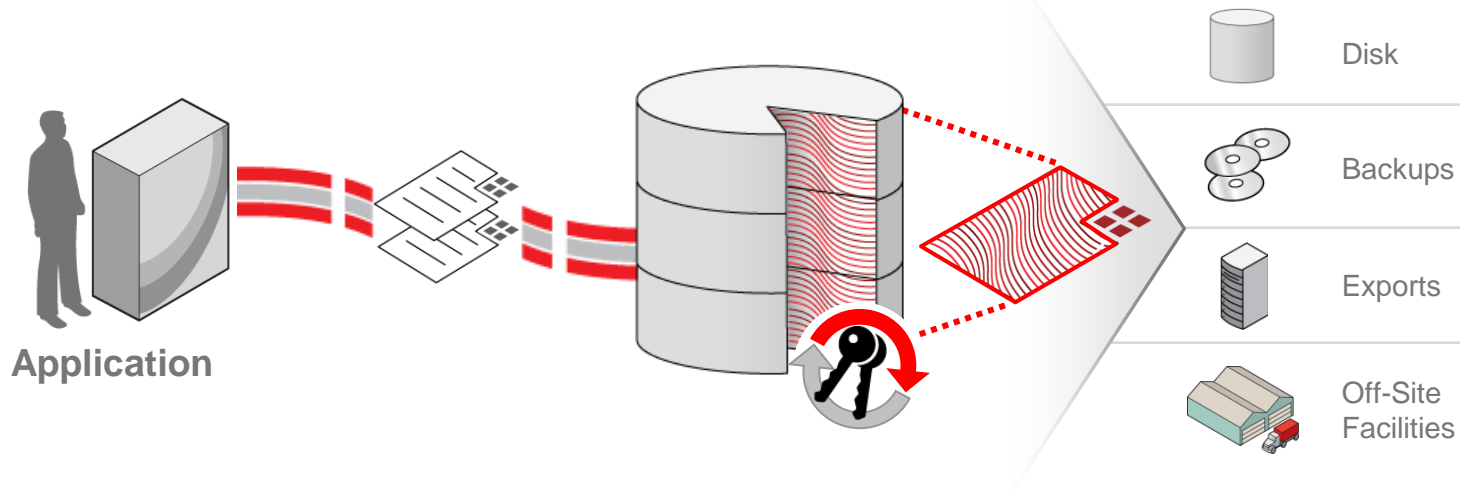
- Oracle Database Vault
- Oracle Label Security

## Encryption and Masking

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

# Oracle Advanced Security

## Transparent Data Encryption



- No application changes required
- Efficient encryption of all application data
- Built-in key lifecycle management
- Works with Exadata V2 Smart Scans
- Works with Oracle Advanced Compression



ORACLE

JDE EDWARDS

SIEBEL

SAP

PeopleSoft

ORACLE



## Create Tablespace

[Show SQL](#) [Cancel](#) [OK](#)

## Information

Modification to the datafile will not take effect until you click "OK" button.

## General

## Storage

\* Name 

## Extent Management

- Locally Managed  
 Dictionary Managed

## Type

- Permanent  
 Set as default permanent tablespace  
 Encryption [Encryption Options](#)  
 Temporary  
 Set as default temporary tablespace  
 Undo  
Undo Retention Guarantee  Yes  No

## Status

- Read Write  
 Read Only  
 Offline

## Datafiles

- Use bigfile tablespace

Tablespace can have only one datafile with no practical size limit.

[Edit](#) [Remove](#)[Add](#)

Edit Table: SCOTT.EMP

Actions Create Like Go Show SQL Schedule Job Revert Apply

General Constraints Segments Storage Options Statistics Indexes

\* Name EMP

Schema SCOTT

Tablespace USERS

Organization Standard (Heap Organized)

Columns

Set Default LOB Attributes Encryption Options

Advanced Attributes Delete Insert Column: Abstract Data Type Insert

Previous 1-10 of 12 Next 2

Select	Name	Data Type	Size	Scale	Not NULL	Default Value	Encrypted
<input type="radio"/>	EMPNO	NUMBER	4		<input checked="" type="checkbox"/>		<input type="checkbox"/>
<input type="radio"/>	ENAME	VARCHAR2	10		<input type="checkbox"/>		<input type="checkbox"/>
<input type="radio"/>	JOB	VARCHAR2	9		<input type="checkbox"/>		<input type="checkbox"/>
<input type="radio"/>	MGR	NUMBER	4		<input type="checkbox"/>		<input type="checkbox"/>
<input type="radio"/>	HIREDATE	DATE			<input type="checkbox"/>		<input type="checkbox"/>
<input checked="" type="radio"/>	SAL	NUMBER	7	2	<input type="checkbox"/>		<input checked="" type="checkbox"/>
<input type="radio"/>	COMM	NUMBER	7	2	<input type="checkbox"/>		<input type="checkbox"/>
<input type="radio"/>	DEPTNO	NUMBER	2		<input type="checkbox"/>		<input type="checkbox"/>

# Oracle Data Masking

## Irreversible De-Identification



- Remove sensitive data from non-production databases
- Referential integrity preserved so applications continue to work
- Extensible template library and policies for automation

# Oracle Database Security Products

Heterogeneous	Oracle Databases
Oracle Database Firewall	Oracle Advanced Security
Oracle Audit Vault	Oracle Database Vault
Oracle Data Masking	Oracle Label Security
	Oracle Configuration Management



# Oracle Database Security Solutions

## Inside. Outside. Complete.

- Preventive and detective controls within the Oracle database
- Database Firewall to prevent threats from reaching databases
- Transparent – no changes to existing applications
- Complete integrated solutions for lower TCO



### Encryption & Masking

- Advanced Security
- Secure Backup
- Data Masking



### Access Control

- Database Vault
- Label Security
- Identity Management



### Auditing & Tracking

- Audit Vault
- Total Recall
- Configuration Management

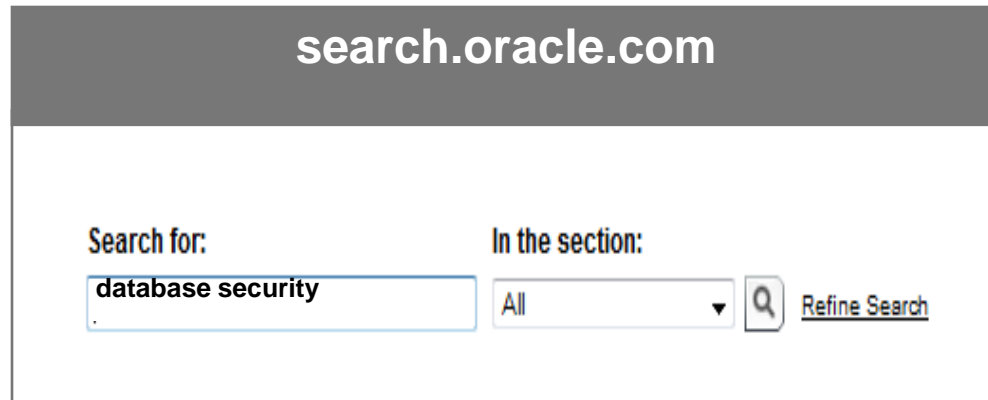


### Monitoring & Blocking

- Database Firewall



# For More Information



search.oracle.com

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

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



Q&A

# **Hardware and Software Engineered to Work Together**