



Oracle Database Security

Paul Needham
Senior Director, Product Management
Database Security

Oracle Security Solutions



Safe Harbor Statement

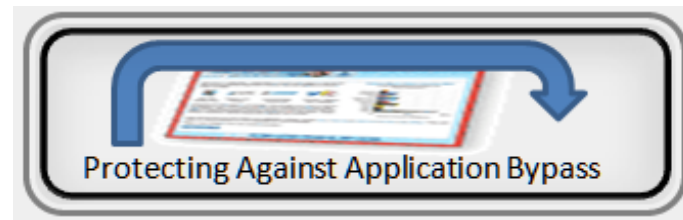
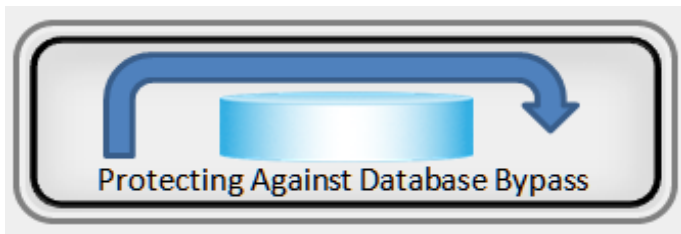
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

MEGA BREACHES ON THE RISE



Considerations for Maximum Security

Preventive and Detective Controls



ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



ORACLE®

Oracle Database Security Innovations

Privilege Analysis

Data Redaction

Real Application Security

Conditional and Unified Auditing

SQL Grammar based Database Firewall

Privileged User Controls

SQL Command Controls

At-source Data Masking

Sensitive Data Discovery

Transparent Data Encryption

Label-based Access Control

Virtual Private Database

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



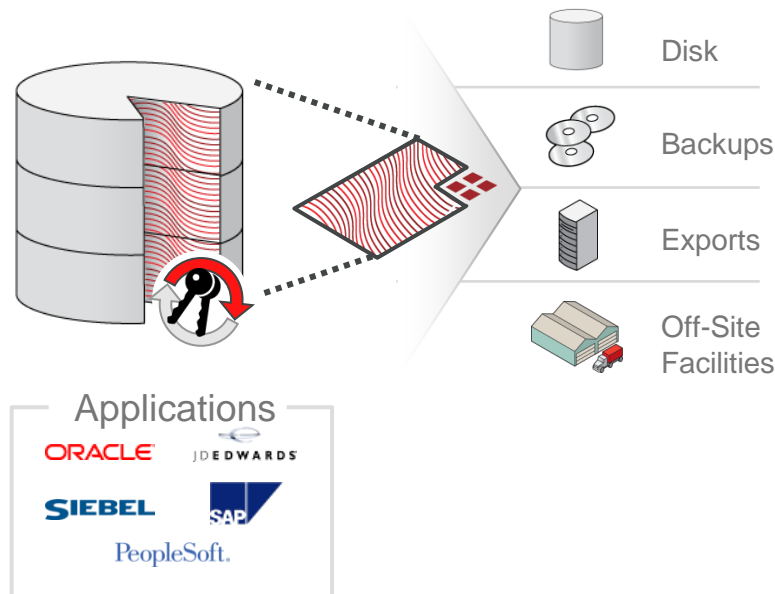
ORACLE®

Encryption is the Foundation

Preventive Control for Oracle Databases

Advanced Security

- Transparent data encryption
- Prevents access to data at rest
- Requires no application changes
- Built-in two-tier key management
- “Near Zero” overhead with hardware
- Integrations with Oracle technologies
 - e.g. Exadata, Advanced Compression, ASM, GoldenGate, DataPump, etc.

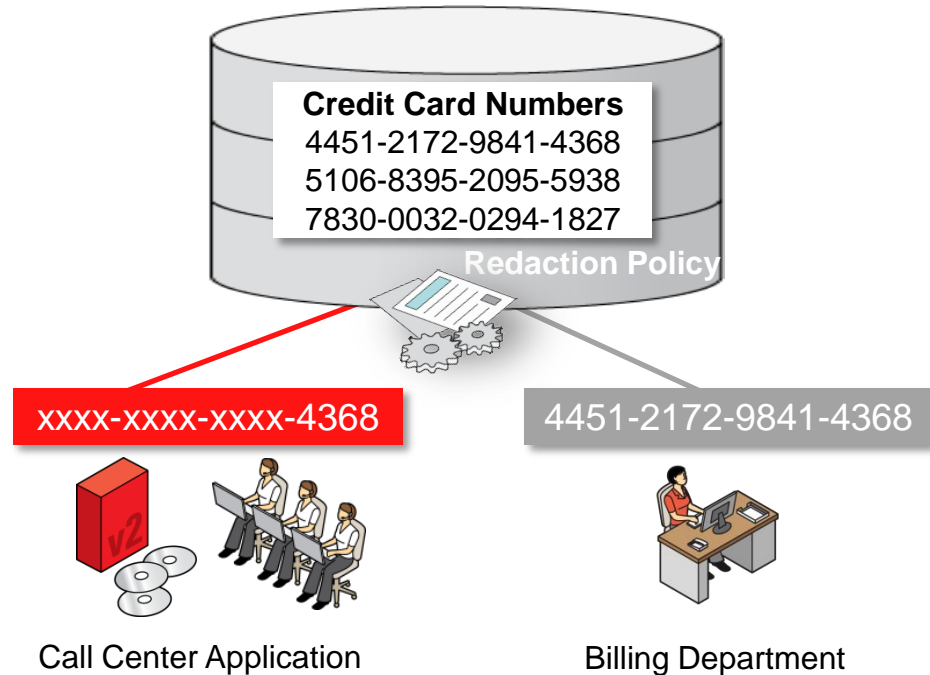


Redaction of Sensitive Data Displayed

Preventive Control for Oracle Database 12c and 11g (11.2.0.4)

Advanced Security

- Real-time redaction based upon user, IP, app context, session factors, ...
- Applies to columns on tables/views
- Full/partial, random/fixed redaction
- Transparent to typical applications
- No impact on operational activities



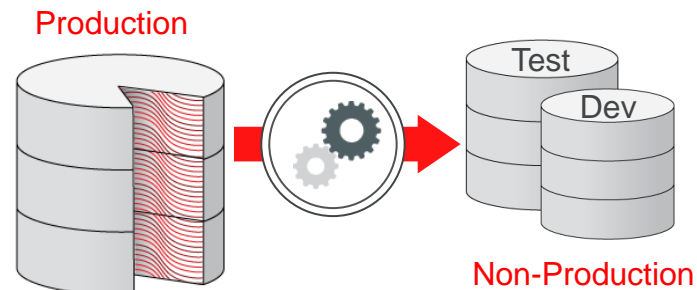
Masking Data for Non-Production Use

Preventive Control for Oracle Databases

Data Masking

- Replace sensitive application data
- Referential integrity detected/preserved
- Extensible template library and formats
- Application templates available
- Support for masking data in non-Oracle databases

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000



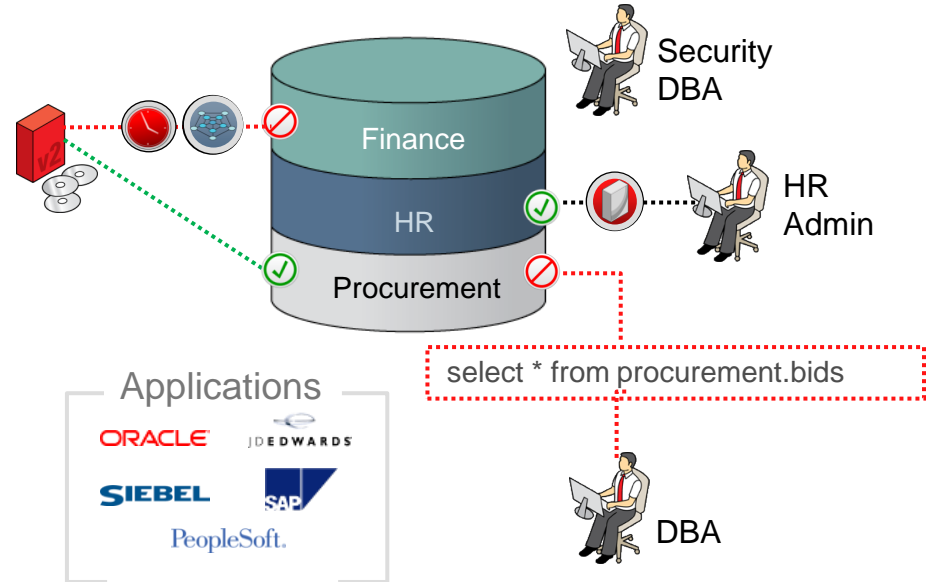
LAST_NAME	SSN	SALARY
ANSKEKSL	323—23-1111	60,000
BKJHHEIEDK	252-34-1345	40,000

Preventive Controls Inside the Oracle Database

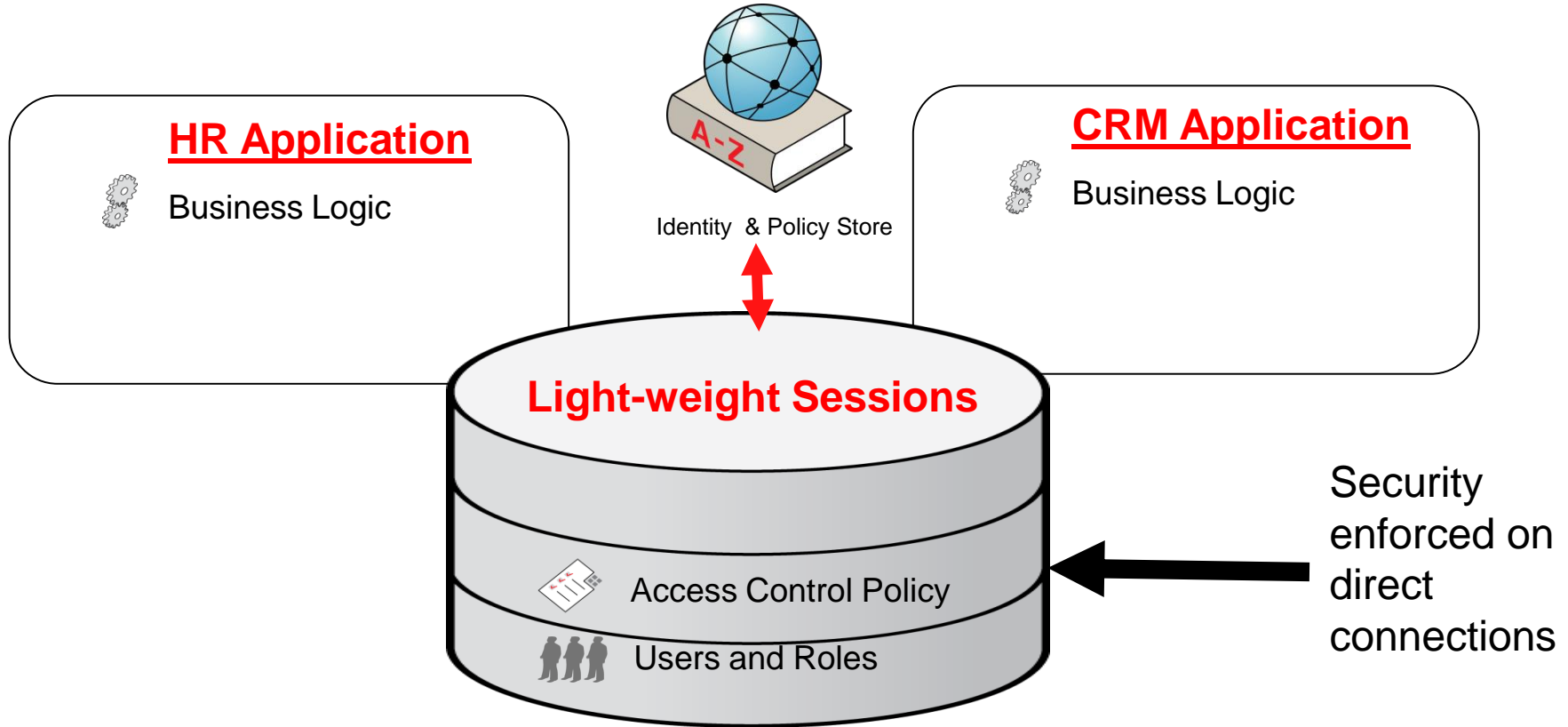
Preventive Control for Oracle Databases

Database Vault

- Realms around sensitive schemas or objects
- Restrict DBA access to realm data
- Support multi-factor SQL command rules
- Enforce separation of duties
- Block threats targeting privileged DB accounts
- Restrict all access unless explicitly authorized with Mandatory Realms (New)



Oracle Real Application Security



ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



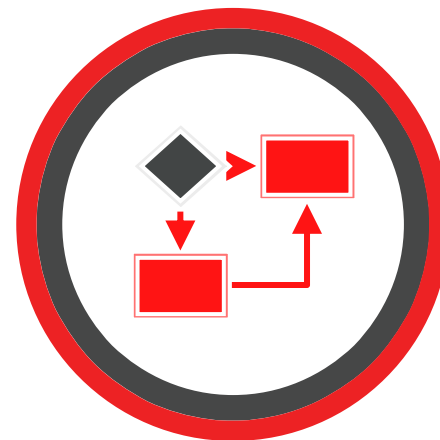
ORACLE®

New Conditional Auditing Framework

Detective Control for Oracle Database 12c

Database Auditing

- New policy and condition-based syntax
 - What: CREATE, ALTER, ALL, ...
 - Where: Set of Privileges, Roles, objects
 - When: IP_ADDRESS != "10.288.241.88"
 - Exceptions: Except HR
- Group audit settings for manageability
- New roles: Audit Viewer and Audit Admin
- Out-of-box audit policies
- Single unified database audit trail



Create Audit Policy : Privileges and Roles

* Name SENSITIVE OPERATIONS

Comments Audit sensitive operations in the database.

Privileges AVAILABLE

ADMINISTER ANY SQL TUNING SET
ADMINISTER DATABASE TRIGGER
ADMINISTER RESOURCE MANAGER
ADMINISTER SQL MANAGEMENT OBJECT
ADMINISTER SQL TUNING SET
ADVISOR
ALTER ANY ASSEMBLY
ALTER ANY CLUSTER
ALTER ANY CUBE
ALTER ANY CUBE BUILD PROC
ALTER ANY CUBE DIMENSION

SELECTED

ADMINISTER KEY MANAGEMENT
ALTER ANY PROCEDURE
ALTER ANY SQL TRANSLATION PROFILE
ALTER ANY TABLE
ALTER DATABASE
ALTER SYSTEM
AUDIT SYSTEM
CREATE ANY JOB

Roles AVAILABLE

ADM_PARALLEL_EXECUTE_TAS
APEX_ADMINISTRATOR_ROLE
APEX_GRANTS_FOR_NEW_USE
AQ_ADMINISTRATOR_ROLE

Policy Expression Builder

Oracle Database Environment

☒ Policy is in effect when session user is not APPS AND Add

Policy Expression

SYS_CONTEXT("USERENV", "SESSION_USER") != "APPS"

☐ Edit

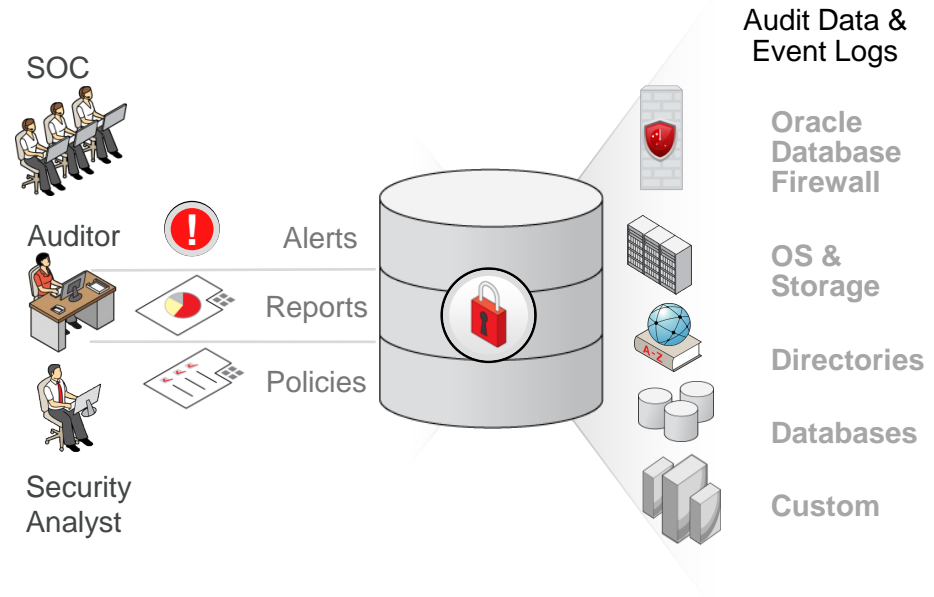
OK Cancel

Audit, Report, and Alert in Real-Time

Detective Control for Oracle and non-Oracle Databases

Audit Vault and Database Firewall

- Collect and Analyze audit/event data
- Centralized secure audit repository
- Consolidated multi-source reporting
- Out-of-the box and custom reports
- Conditional real-time alerts
- Fine-grain separation of duties
- Secure, scalable software appliance

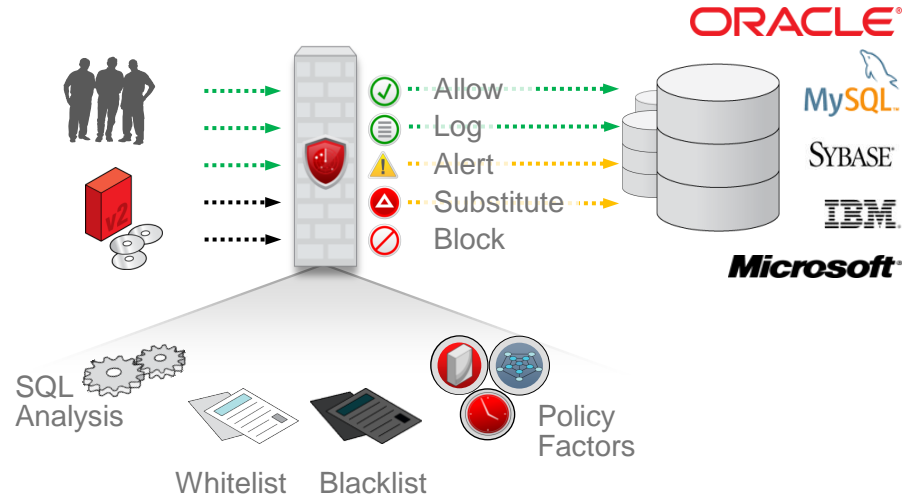


Database Activity Monitoring and Firewall

Detective Control for Oracle and non-Oracle Databases

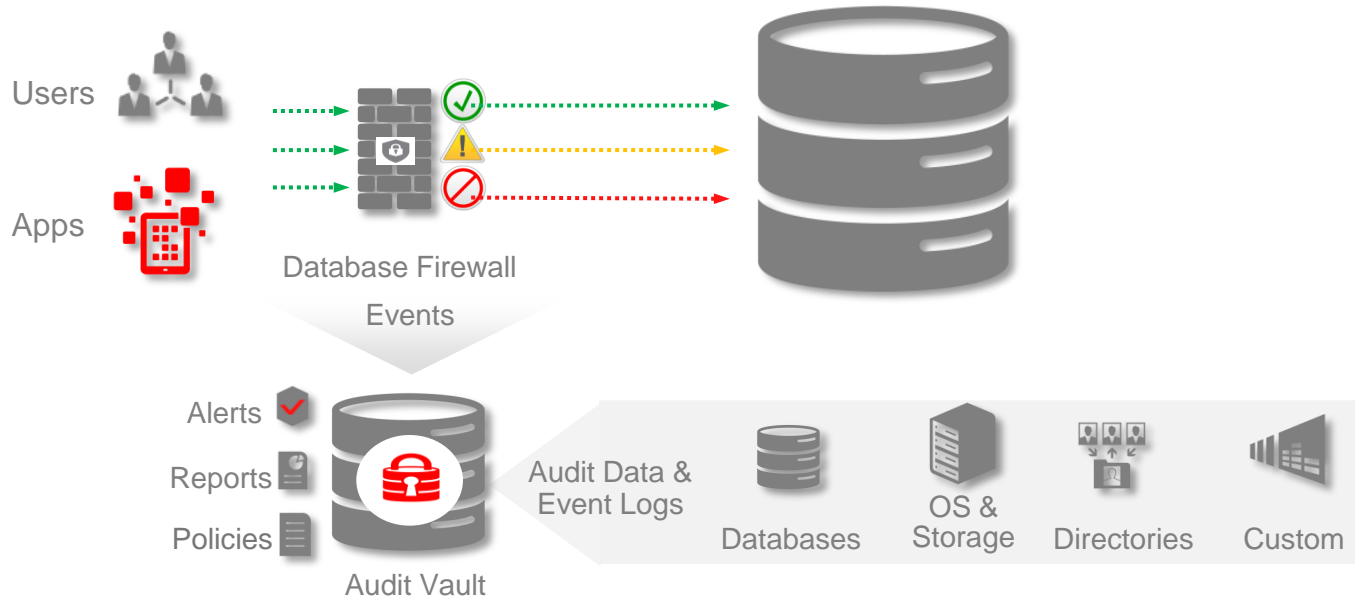
Audit Vault and Database Firewall

- Monitor network traffic, detect and block unauthorized database activity
- Detect/stop SQL injection attacks
- Highly accurate SQL grammar analysis
- Whitelist approach to enforce activity
- Blacklists for managing high risk activity
- Scalable secure software appliance



Oracle Audit Vault and Database Firewall

Detective Controls



ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

Configuration Management

ORACLE®



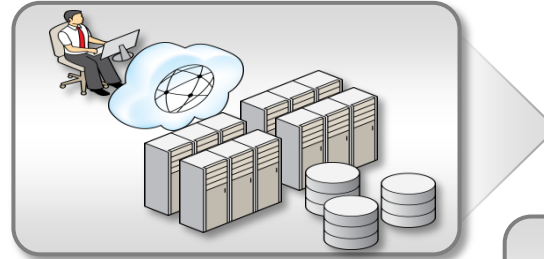
ORACLE®

Configuration Management

Administrative Control for Oracle Databases

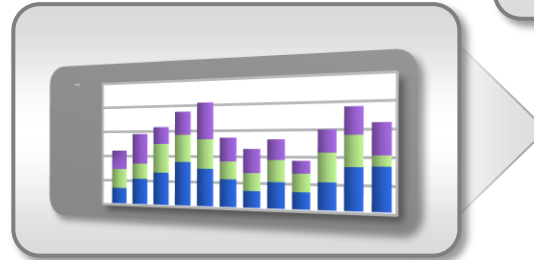
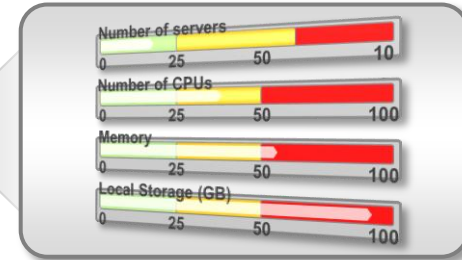
Database Lifecycle Management

- Discover and classify databases
- Scan for best practices, standards
- Detect unauthorized changes
- Patching and provisioning



Discover

Scan & Monitor



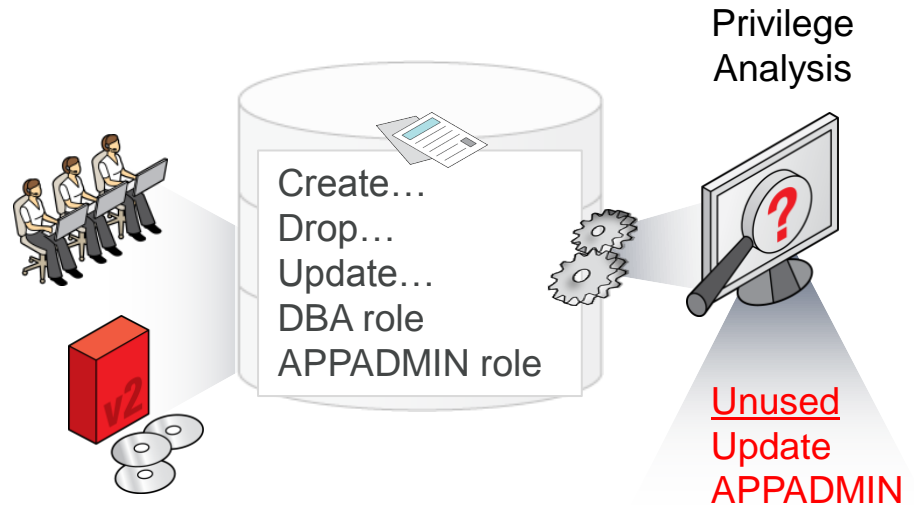
Patch

Discover Use of Privileges and Roles

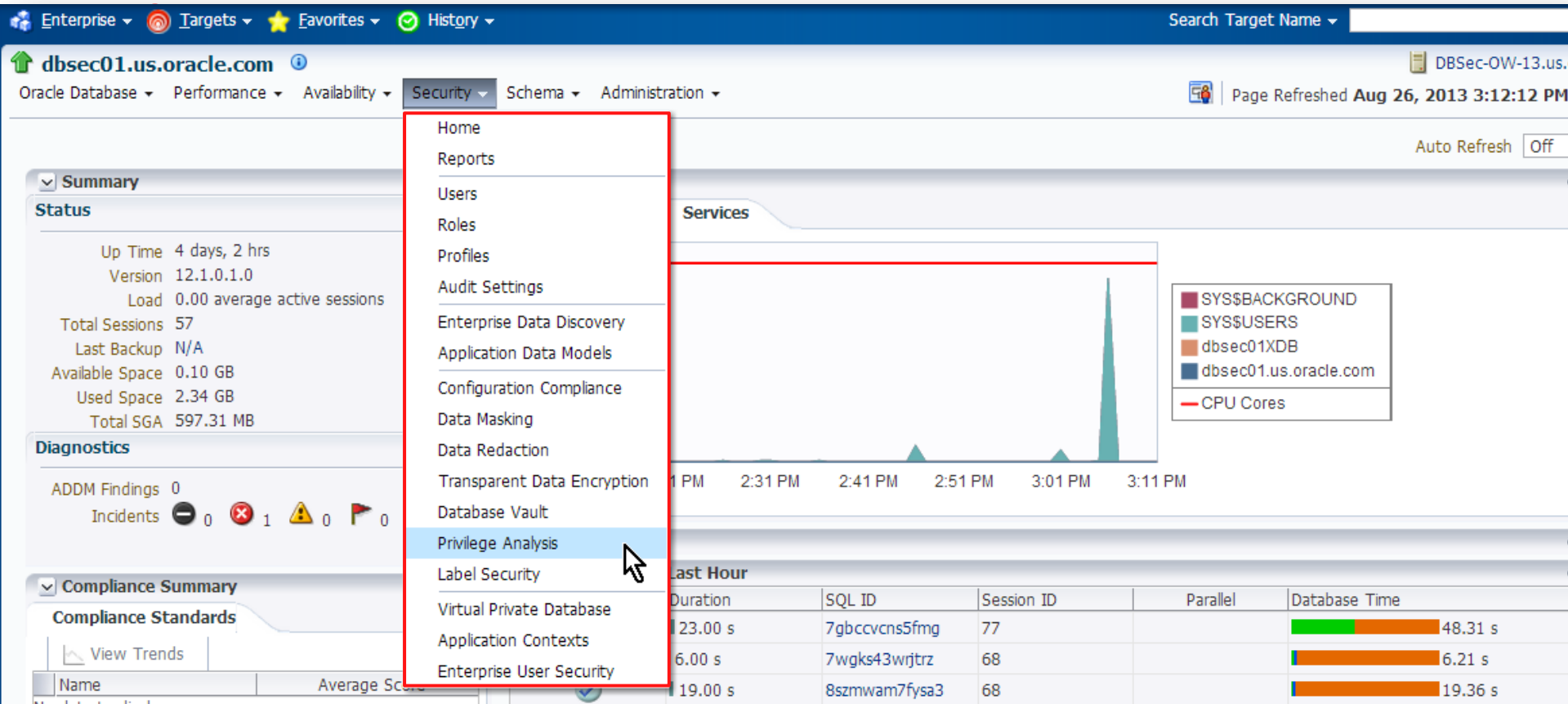
Administrative Control for Oracle Database 12c

Database Vault

- Capture privileges used per session, across sessions, per specific context, or full database
- Report on privileges/roles used/unused
- Help revoke unnecessary privileges
- Enforce least privilege and reduce risks
- Increase security without disruption



New Oracle Enterprise Manager Security Menu



The screenshot shows the Oracle Enterprise Manager interface. The top navigation bar includes links for Enterprise, Targets, Favorites, and History. The main header displays the target name 'dbsec01.us.oracle.com' and the database type 'Oracle Database'. The 'Security' menu is open, showing a list of options: Home, Reports, Users, Roles, Profiles, Audit Settings, Enterprise Data Discovery, Application Data Models, Configuration Compliance, Data Masking, Data Redaction, Transparent Data Encryption, Database Vault, Privilege Analysis (highlighted with a mouse cursor), Label Security, Virtual Private Database, Application Contexts, and Enterprise User Security. The background shows a 'Summary' section with database status (Up Time: 4 days, 2 hrs; Version: 12.1.0.1.0; Load: 0.00 average active sessions; Total Sessions: 57; Last Backup: N/A; Available Space: 0.10 GB; Used Space: 2.34 GB; Total SGA: 597.31 MB) and a 'Diagnostics' section with ADDM Findings (0) and Incidents (0). A 'Services' graph shows CPU usage for SYS\$BACKGROUND, SYS\$USERS, dbsec01XDB, and dbsec01.us.oracle.com. A 'Last Hour' table lists sessions with their duration, SQL ID, session ID, parallelism, and database time.

Enterprise ▾ Targets ▾ Favorites ▾ History ▾ Search Target Name ▾

dbsec01.us.oracle.com ⓘ

Oracle Database ▾ Performance ▾ Availability ▾ Security ▾ Schema ▾ Administration ▾

Page Refreshed Aug 26, 2013 3:12:12 PM

Auto Refresh Off

Summary

Status

Up Time 4 days, 2 hrs
Version 12.1.0.1.0
Load 0.00 average active sessions
Total Sessions 57
Last Backup N/A
Available Space 0.10 GB
Used Space 2.34 GB
Total SGA 597.31 MB

Diagnostics

ADDM Findings 0
Incidents 0 1 0 0

Compliance Summary

Compliance Standards

View Trends

Services

Legend: SYS\$BACKGROUND, SYS\$USERS, dbsec01XDB, dbsec01.us.oracle.com, CPU Cores

Last Hour

Duration	SQL ID	Session ID	Parallel	Database Time
123.00 s	7gbccvcns5fmg	77		48.31 s
6.00 s	7wgks43wrjtrz	68		6.21 s
19.00 s	8szmwam7fysa3	68		19.36 s

ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

PREVENTIVE

Encryption & Redaction

Masking & Subsetting

Privileged User Controls

ORACLE®



DETECTIVE

Activity Monitoring

Database Firewall

Auditing & Reporting

ORACLE®



ADMINISTRATIVE

Key Management

Privilege & Data Discovery

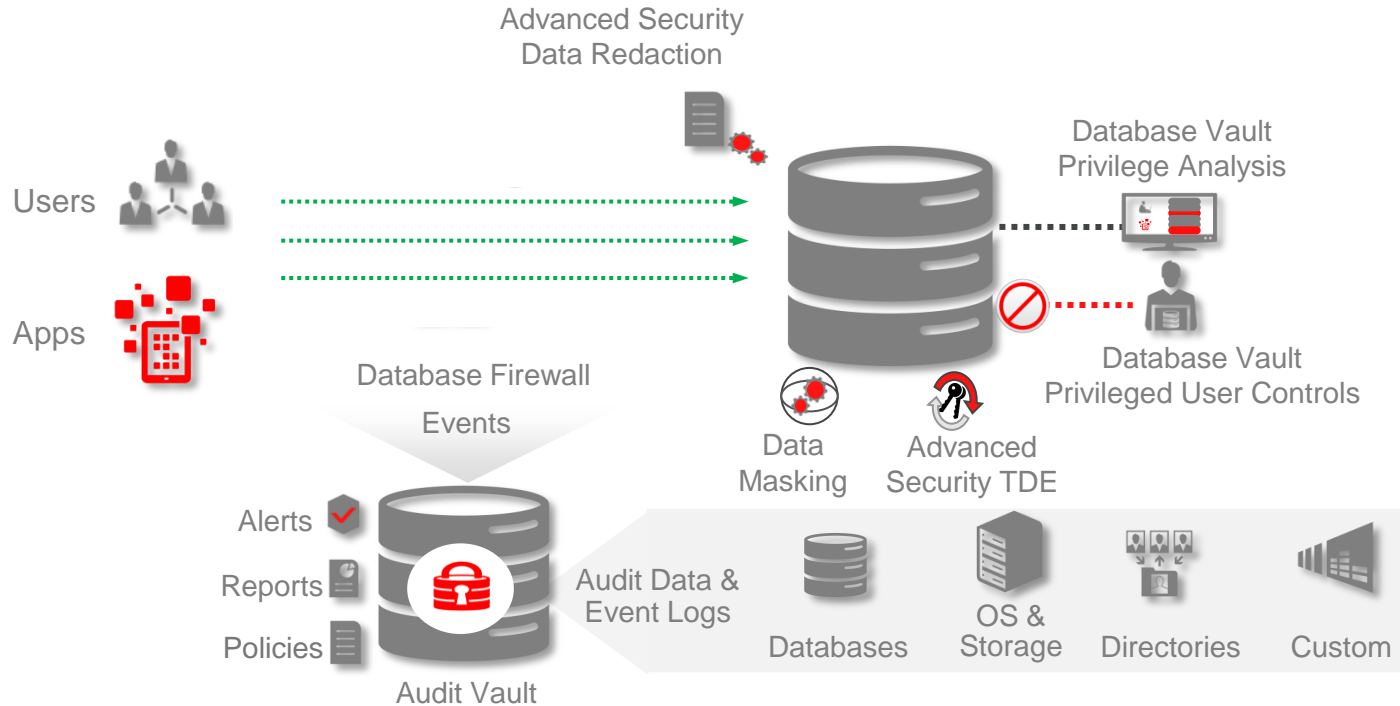
Configuration Management

ORACLE®



ORACLE®

Oracle Database Maximum Security Architecture



ORACLE®