Oracle Database Security

Paul Needham
Senior Director, Product Management
Database Security
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

- MAR '14
- DEC '13
- OCT '13
- SEP '13
- JAN '14
- FEB '14
Considerations for Maximum Security

Preventive and Detective Controls
# ORACLE DATABASE SECURITY

Maximum Security for Critical Infrastructure

<table>
<thead>
<tr>
<th>PREVENTIVE</th>
<th>DETECTIVE</th>
<th>ADMINISTRATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption &amp; Redaction</td>
<td>Activity Monitoring</td>
<td>Key Management</td>
</tr>
<tr>
<td>Masking &amp; Subsetting</td>
<td>Database Firewall</td>
<td>Privilege &amp; Data Discovery</td>
</tr>
<tr>
<td>Privileged User Controls</td>
<td>Auditing &amp; Reporting</td>
<td>Configuration Management</td>
</tr>
</tbody>
</table>
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

DETECTIVE
- Activity Monitoring
- Database Firewall
- Auditing & Reporting

ADMINISTRATIVE
- Key Management
- Privilege & Data Discovery
- Configuration Management
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

Credit Card Numbers
4451-2172-9841-4368
5106-8395-2095-5938
7830-0032-0294-1827

Redaction Policy

Billing Department
Call Center Application
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

<table>
<thead>
<tr>
<th>LAST_NAME</th>
<th>SSN</th>
<th>SALARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGUILAR</td>
<td>203-33-3234</td>
<td>40,000</td>
</tr>
<tr>
<td>BENSON</td>
<td>323-22-2943</td>
<td>60,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LAST_NAME</th>
<th>SSN</th>
<th>SALARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSKEKSL</td>
<td>323—23—1111</td>
<td>60,000</td>
</tr>
<tr>
<td>BKJHHEIEDK</td>
<td>252—34—1345</td>
<td>40,000</td>
</tr>
</tbody>
</table>
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

**HR Application**
- Business Logic

**CRM Application**
- Business Logic

**Light-weight Sessions**
- Access Control Policy
- Users and Roles

Security enforced on direct connections
ORACLE DATABASE SECURITY
Maximum Security for Critical Infrastructure

**PREVENTIVE**
- Encryption & Redaction
- Masking & Subsetting
- Privileged User Controls

**DETECTIVE**
- Activity Monitoring
- Database Firewall
- Auditing & Reporting

**ADMINISTRATIVE**
- Key Management
- Privilege & Data Discovery
- Configuration Management
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 PROCEDURE
- 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

Policy Expression Builder

Oracle Database Environment

- Policy is in effect when: session user is not APPS

Policy Expression:

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

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

<table>
<thead>
<tr>
<th>PREVENTIVE</th>
<th>DETECTIVE</th>
<th>ADMINISTRATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption &amp; Redaction</td>
<td>Activity Monitoring</td>
<td>Key Management</td>
</tr>
<tr>
<td>Masking &amp; Subsetting</td>
<td>Database Firewall</td>
<td>Privilege &amp; Data Discovery</td>
</tr>
<tr>
<td>Privileged User Controls</td>
<td>Auditing &amp; Reporting</td>
<td>Configuration Management</td>
</tr>
</tbody>
</table>

**ORACLE**

---

19 | Copyright © 2014, Oracle and/or its affiliates. All rights reserved.
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
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

- Create Privilege Analysis policy and enable it

Oracle Database Vault
## ORACLE DATABASE SECURITY
Maximum Security for Critical Infrastructure

<table>
<thead>
<tr>
<th>PREVENTIVE</th>
<th>DETECTIVE</th>
<th>ADMINISTRATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption &amp; Redaction</td>
<td>Activity Monitoring</td>
<td>Key Management</td>
</tr>
<tr>
<td>Masking &amp; Subsetting</td>
<td>Database Firewall</td>
<td>Privilege &amp; Data Discovery</td>
</tr>
<tr>
<td>Privileged User Controls</td>
<td>Auditing &amp; Reporting</td>
<td>Configuration Management</td>
</tr>
</tbody>
</table>

*Images and logos of various database systems are also shown.*
Oracle Database Maximum Security Architecture

Advanced Security Data Redaction

Database Vault Privilege Analysis

Database Vault Privileged User Controls

Data Masking Advanced Security TDE

Audit Data & Event Logs

Audit Vault

Reports Policies

OS & Storage Directories Custom

Databases

Alerts

Database Firewall Events

Users

Apps

Oracle Database Maximum Security Architecture