Oracle Database Security Assessment Tool (DBSAT)

Overview

Pedro Lopes
Product Manager
Oracle Database Security

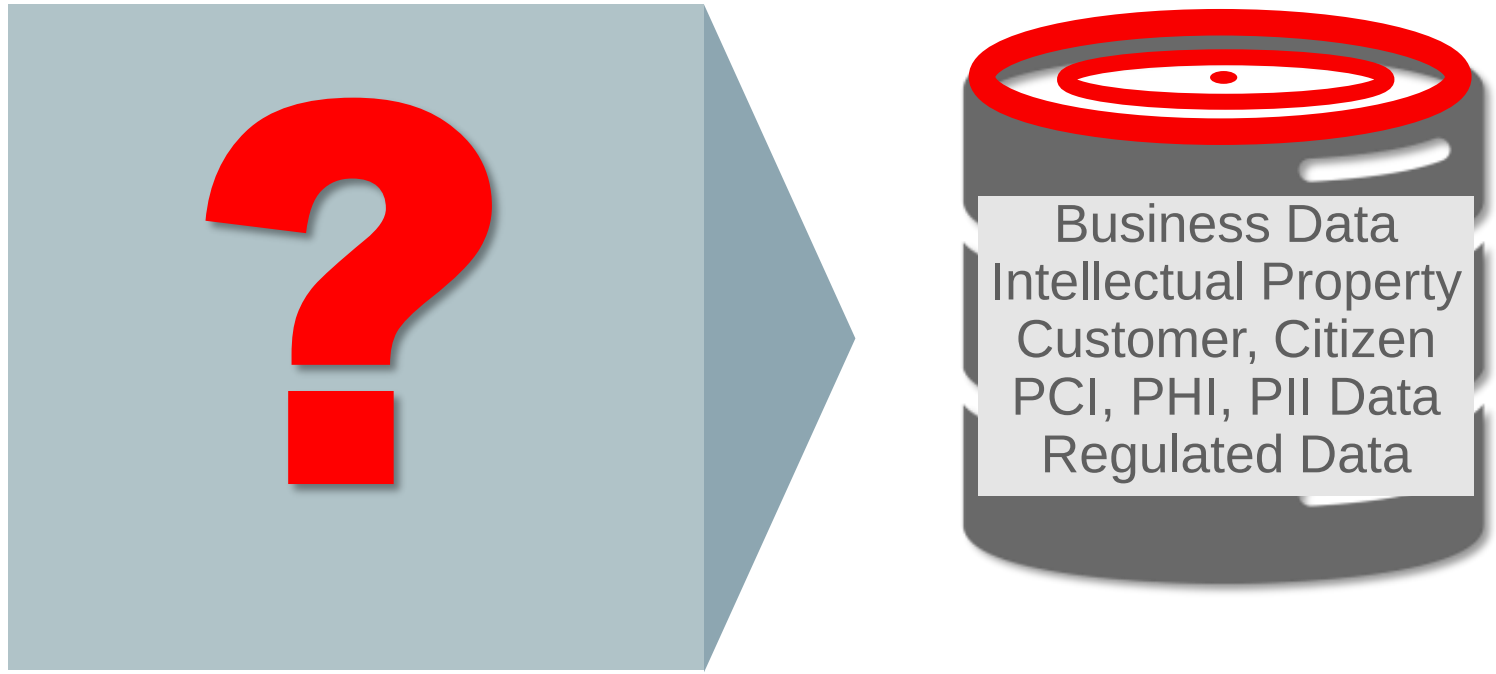
High-level Trends in Security

- Data breaches becoming bigger and bolder
  - New targets: Data aggregators, financial accounting firms, breach investigators, security companies, governments, ...
  - New target types: devices, cloud, …
- Data breaches becoming very costly
  - $80 billion spent every year on IT security but actual breach cost exceeds a trillion dollars
  - Average cost of a data breach is $7.35 million, $225 per stolen record
  - Litigation expenses account for almost 65% of breach expenses
  - Irreversible damage to victims, brand, and business
- Challenges
  - Severe shortage of security skills, no match to hacker expertise and automation
  - Many organizations don’t know how vulnerable they are

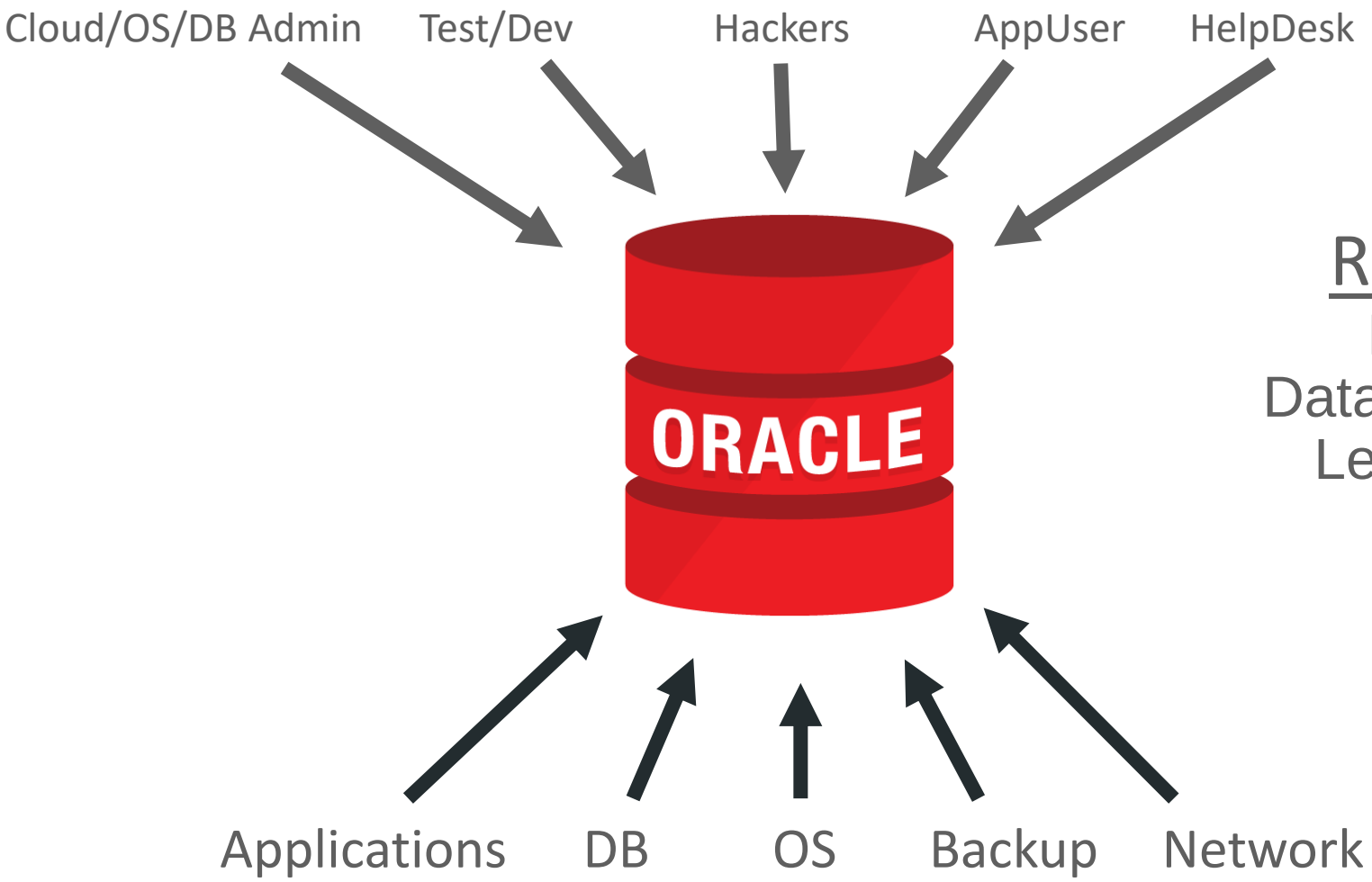
Are Your Laptops Secure?

Anti-virus
Desktop-firewall
Anti-malware
Biometric reader
Spam / email filtering
Patch management
Data encryption
Strong password policies

…and Your Databases?



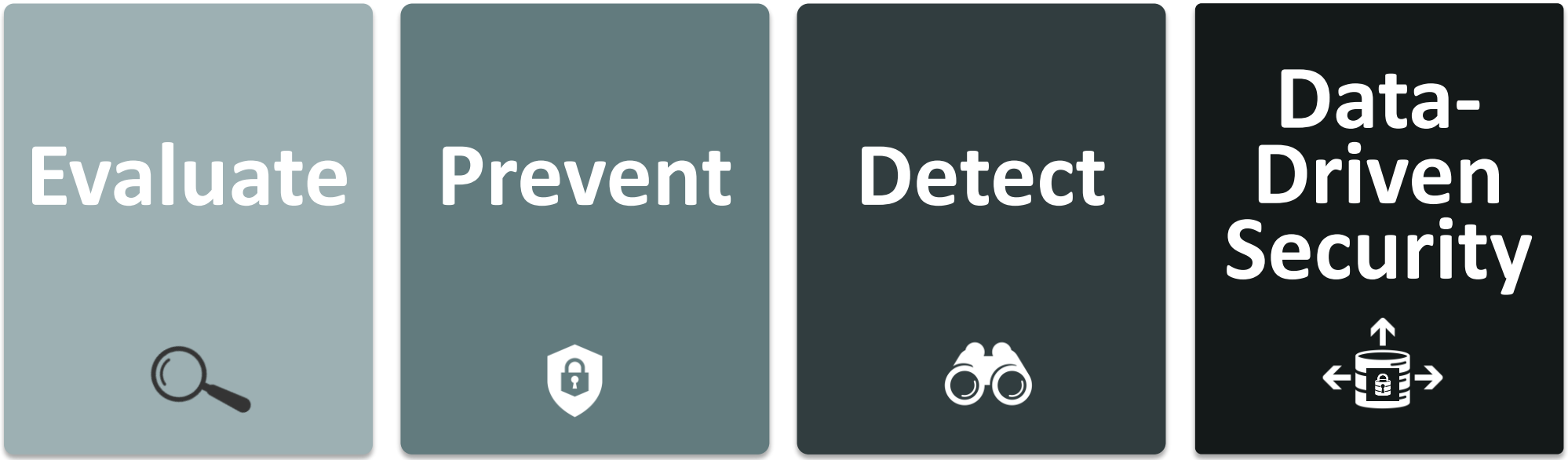
Common Threat Actors, Vectors, and Targets



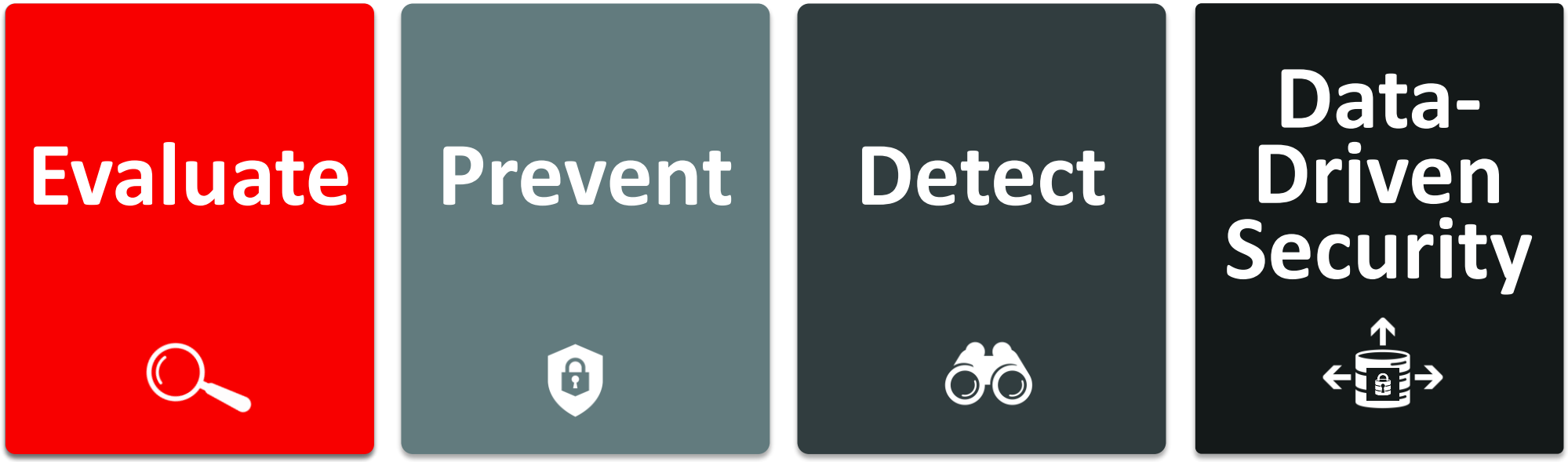
Risk Multipliers

High Availability
Database Consolidation
Legacy Applications
Outsourcing
Cloud

Comprehensive Database Security Controls



Comprehensive Database Security Controls



Evaluate database security posture before you secure the databases

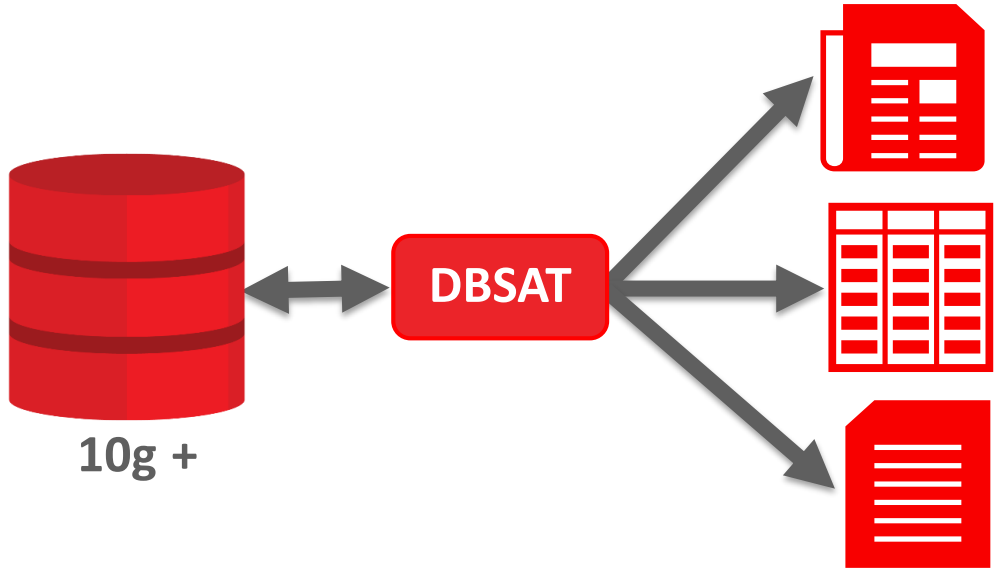
Where To Start & What to look for

Who are the users and their entitlements?
What controls do I have in place?
Is my Database securely configured?

Do we have a Database Security Team? Knowledge?
Analysis time?

Database Security Assessment Tool (DBSAT)

- Understand how (in)secure is your database
  - Database securely configured?
  - Identify privileged users and risks?
- Actionable Reports
  - Summary and detailed reports
  - Prioritized recommendations
- Analyze Oracle Database 10g and later
- Stand-alone command-line tool: Quick, Easy
- FREE to current Oracle customers

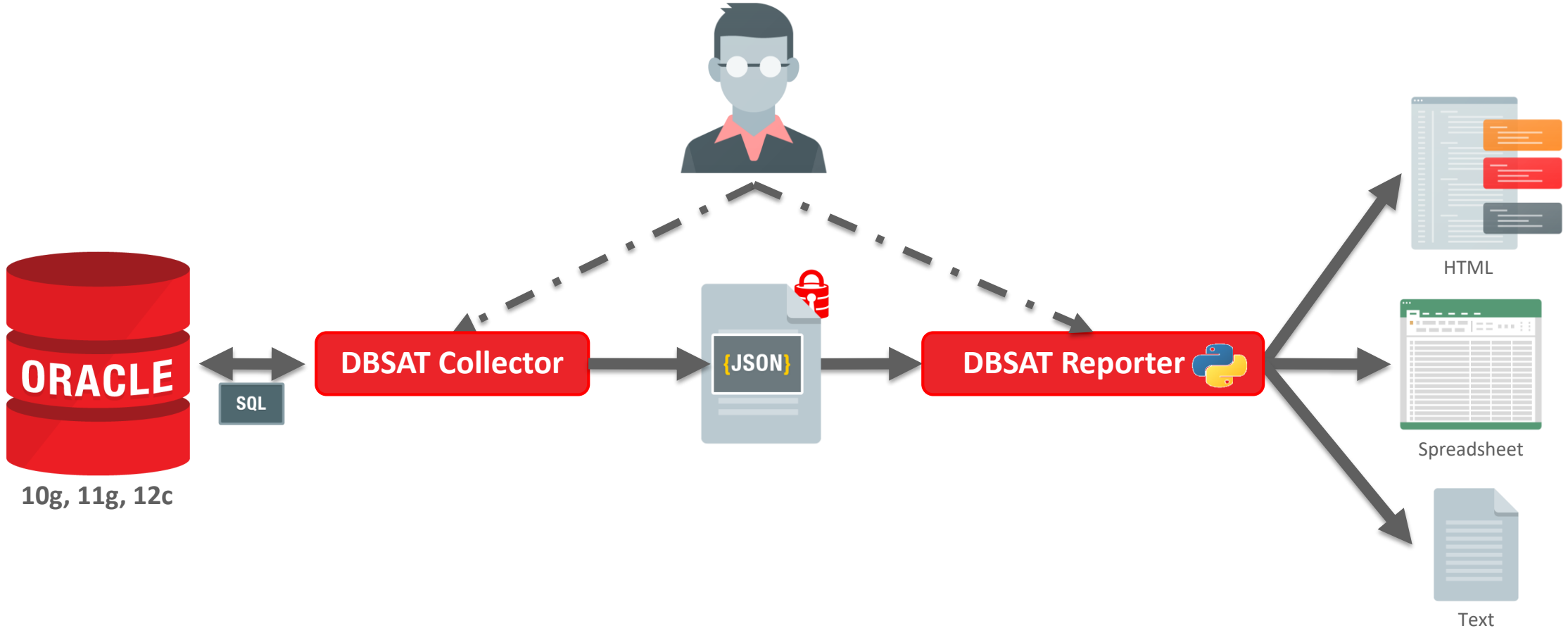


What does DBSAT Check?

- User Accounts, Privileges and Roles
- Authorization Control
- Data Encryption
- Fine-grained Access Control
- Auditing Policies
- Database Configuration
- Listener Configuration
- OS File permissions*

** except Windows*

Security Assessment Flow



Summary Output (HTML Report)

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Wed May 18 2016 16:20:00	Fri May 20 2016 10:43:21	1.0 (May 2016) - 1c0a

Database Identity

Name	Platform	Database Role	Log Mode	Created
DB	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Feb 03 2016 09:40:00

Summary

Section	Pass	Evaluate	Opportunity	Some Risk	Significant Risk	Severe Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	4	0	0	3	3	1	11
Privileges and Roles	5	11	0	1	0	0	17
Authorization Control	0	0	2	0	0	0	2
Data Encryption	0	1	1	0	0	0	2
Fine-Grained Access Control	0	0	5	0	0	0	5
Auditing	2	4	2	0	3	0	11
Database Configuration	5	4	0	3	0	0	12
Network Configuration	1	0	0	1	3	0	5
Operating System	3	1	0	0	1	0	5
Total	**20**	**21**	**10**	**8**	**10**	**2**	**71**

Security Features in Use – Quick Insight

Feature	Currently Used
AUTHORIZATION CONTROL	
Database Vault	Yes
Privilege Analysis	No
DATA ENCRYPTION	
Column Encryption	No
Tablespace Encryption	No
Network Encryption	No
ACCESS CONTROL	
Data Redaction	No
Virtual Private Database	No
Real Application Security	No
Label Security	Yes
Transparent Sensitive Data Protection	No
AUDITING	
Traditional Audit	Yes
Fine Grained Audit	No
Unified Audit	Yes
USER AUTHENTICATION	
External Authentication	No
Global Authentication	No

Privileged User Controls in place?
Data Encrypted?
Fine-Grained Access Control Policies?
Auditing?
User Authentication?

Sample Security Findings

Audit Records

AUDIT.RECORDS

Status Pass

Summary Examined 3 audit trails. Found records in 1 audit trail. No errors found in audit initialization parameters.

Details

```
Audit trails with records: Unified Audit Trail
Audit trails with no records: Traditional Audit Trail, FGA Audit Trail

AUDIT_FILE_DEST=/scratch/kaizhuan/app/kaizhuan/admin/orcl12202/adump
AUDIT_TRAIL=DB
```

Remarks Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users. For any attack that exploits gaps in other security policies, auditing cannot prevent the attack but it forms the critical last line of defense by detecting the malicious activity.

Sample Security Findings

Transparent Data Encryption

CRYPT.TDE

Status	Opportunity
Summary	No encrypted tablespaces found. No encrypted columns found. Examined 1 initialization parameter.
Details	`ENCRYPT_NEW_TABLESPACES=CLOUD_ONLY. Recommended value is ALWAYS.`
Remarks	Transparent Data Encryption automatically encrypts data as it is stored and decrypts it upon retrieval. This protects sensitive data from attacks that bypass the database to read data files directly. Encryption keys may be stored in wallets on the database server itself, or stored remotely in Oracle Key Vault for improved security. The ENCRYPT_NEW_TABLESPACES parameter ensures that TDE tablespace encryption is applied to all newly created tablespaces. Setting this parameter to ALWAYS is recommended in order to protect all data regardless of the options specified when the tablespace is created.

Sample Security Findings

Data Access Privileges

PRIV.DATA

Status Evaluate

Summary 46 grants of data access privileges

Details

```
Grants of ALTER ANY PROCEDURE, ALTER ANY TRIGGER, CREATE ANY PROCEDURE,
    CREATE ANY TRIGGER, DELETE ANY TABLE, INSERT ANY TABLE, READ ANY TABLE,
    SELECT ANY DICTIONARY, SELECT ANY TABLE, UPDATE ANY TABLE:

MACSYS <- DV_OWNER: ALTER ANY TRIGGER

SYSTEM: SELECT ANY TABLE
SYSTEM <- DBA: ALTER ANY PROCEDURE, ALTER ANY TRIGGER, CREATE ANY
    PROCEDURE, CREATE ANY TRIGGER, DELETE ANY TABLE, INSERT ANY TABLE, READ
    ANY TABLE, SELECT ANY DICTIONARY, SELECT ANY TABLE, UPDATE ANY TABLE
SYSTEM <- DBA <- DATAPUMP_EXP_FULL_DATABASE <- EXP_FULL_DATABASE:
    SELECT ANY TABLE
SYSTEM <- DBA <- DATAPUMP_IMP_FULL_DATABASE: DELETE ANY TABLE, SELECT
    ANY TABLE

                                ...

(no users) <- OEM_MONITOR: SELECT ANY DICTIONARY
```

Remarks Users with data access privileges (ALTER ANY PROCEDURE, ALTER ANY TRIGGER, CREATE ANY PROCEDURE, CREATE ANY TRIGGER, DELETE ANY TABLE, INSERT ANY TABLE, READ ANY TABLE, SELECT ANY DICTIONARY, SELECT ANY TABLE, UPDATE ANY TABLE) can override various access controls on data. Most administrative tasks do not require access to the data itself, so these privileges should be granted rarely even to administrators. In addition to minimizing grants of these privileges, consider the use of Database Vault realms to limit the use of these privileges to access sensitive data.

DBA Role

PRIV.DBA

Status Evaluate

Summary 3 grants of DBA role

Details

```
Grants of DBA role:

DBAUSER: DBA

TESTDBAUSER: DBA

(no users) <- TESTDBAROLE: DBA
```

Remarks The DBA role is very powerful and can be used to bypass many security protections. It should be granted to only a small number of trusted administrators. Furthermore, each trusted user should have an individual account for accountability reasons. As with any powerful role, avoid granting the DBA role with admin option unless absolutely necessary.

Sample Security Findings

Users with Default Passwords

USER.DEFPWD

Status	Severe Risk
Summary	Found 13 unlocked user accounts with default password.
Details	`Users with default password: ADAMS, BLAKE, CLARK, CTXSYS, HR, IX, JONES, OE, PM, SCOTT, SH, SYSTEM, XDB`
Remarks	Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.

Sample Rules

Rule	Summary
USER.EXPIRED	Users that did not change password for the last 30 days. Ghost accounts?
PRIV.DATA	Users that can access create/update/insert/delete data in all user schemas.
PRIV.DBA	Who has the DBA role?
AUTH.DV	Controls in place against insider threats, stolen credentials, and human error
CRYPT.TDE	Is sensitive/regulated data being encrypted?
ACCESS.REDACT	Data Redaction policies detail
AUDIT.UNIFIED	Audit policies detail
CONF.FILESYS	Which database server OS directories are accessible via PL/SQL?
NET.CRYPT	Are we encrypting network traffic?
OS.AGENT	How many agents are running on the database server?

Spreadsheet Format - Tracking & Prioritizing

Database Security Risk Assessment - Highly Confidential

Assessment Date & Time	Date of Data Collection Date of Report Reporter Version Wed Mar 30 2016 13:55:00 Thu Apr 7 2016 12:00:06 0.9 (Apr 2016) - ca6b
Database Identity	Name Platform Database Role Log Mode Created RDBMS2 Linux x86 64-bit PRIMARY NOARCHIVELOG Wed Mar 30 2016 13:44:00

Basic Information

Item	ID	Status	Result	Remarks
Database Version	Oracle Database 12c Enterprise Edition Release 12.2.0.0.3 - 64bit Production Security options used: Advanced Security, Database Vault, Label Security			
Security Features	Feature Currently Used AUTHORIZATION CONTROL Database Vault Yes Privilege Analysis Yes DATA ENCRYPTION Column Encryption Yes Tablespace Encryption Yes Network Encryption No ACCESS CONTROL Data Redaction Yes Virtual Private Database Yes Real Application Security Yes Label Security Yes Transparent Sensitive Data Protection Yes AUDITING Traditional Audit Yes Fine Grained Audit Yes Unified Audit Yes			

Users with Expired Passwords	USER.EXPIRED	Some Risk	Found 1 unlocked user(s) with password expired for more than 30 days.	Password expiration is used to ensure that users change their passwords on a regular basis. If a user's password has been expired for more than 30 days, it indicates that the user has not logged in for at least that long. Accounts that have been unused for an extended period of time should be investigated to determine whether they should remain active.
User Accounts in SYSTEM or SYSAUX Tablespace	USER.TBLSPACE	Significant Risk	40 user(s) use SYSTEM or SYSAUX tablespace.	The SYSTEM and SYSAUX tablespaces are reserved for Oracle-supplied user accounts. To avoid a possible denial of service caused by exhausting these resources, regular user accounts should not use these tablespaces. Prior to Oracle Database 12.2, the SYSTEM tablespace cannot be encrypted, and this is another reason to avoid user schemas in this
Sample Schemas	USER.SAMPLE	Significant Risk	Found 9 sample schema(s).	Sample schemas are well-known accounts provided by Oracle to serve as simple examples for developers. They generally serve no purpose in a production database and should be removed because they unnecessarily increase the attack surface of the
Users with Default Passwords	USER.DEFPWD	Severe Risk	12 unlocked user account(s) are using default password	Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.
Password Verifier Version	USER.VERIFIER	Pass	All user accounts have updated password verifiers.	Over time, Oracle releases have added support for increasingly secure algorithms for generating password verifiers for user accounts. In order to remain compatible with older client software, the database continues to generate password verifiers using the previous algorithms as well. Each user account should include a verifier for latest version supported by the database so that the user can be authenticated using the latest algorithm supported by the client. When all clients have been updated, the security of user accounts can be improved by removing the obsolete verifiers.

Text Format - For Inclusion in Other Reports

```
### Database Security Risk Assessment - Highly Confidential ###

* Assessment Date & Time *
Date of Data Collection  Date of Report          Reporter Version
------------------------ ------------------------ --------------------
Wed Mar 30 2016 13:55:00 Thu Apr 7 2016 12:00:06 0.9 (Apr 2016) - ca6b

* Database Identity *
Name   Platform         Database Role Log Mode     Created
------ ---------------- ------------- ------------ ------------------------
RDBMS2 Linux x86 64-bit PRIMARY       NOARCHIVELOG Wed Mar 30 2016 13:44:00

### Summary ###

Section                Pass Evaluate Opportunity Some Risk Significant Risk Severe Risk Total Findings
---------------------- ---- -------- ----------- --------- ---------------- ----------- --------------
Basic Information         0        0           0         0                0           1              1
User Accounts             3        0           0         3                4           1             11
Privileges and Roles      2       12           0         1                2           0             17
Authorization Control     0        2           0         0                0           0              2
Data Encryption           1        0           1         0                0           0              2
Access Control            0        5           0         0                0           0              5
Auditing                  5        5           0         0                1           0             11
Database Configuration    5        3           0         2                0           1             11
Network Configuration     1        0           0         1                3           0              5
Operating System          2        1           0         1                1           0              5
Total                    19       28           1         8               11           3             70

### Basic Information ###

* Database Version *
Oracle Database 12c Enterprise Edition Release 12.2.0.0.3 - 64bit Production
Security options used: Advanced Security, Database Vault, Label Security vmpsu.sql

* Security Features *
Feature                                  Currently Used
---------------------------------------- --------------
AUTHORIZATION CONTROL
Database Vault                                      Yes
Privilege Analysis                                  Yes

DATA ENCRYPTION
Column Encryption                                   Yes
Tablespace Encryption                               Yes
Network Encryption                                   No

ACCESS CONTROL
Data Redaction                                      Yes
Real Application Security                           Yes
Label Security                                      Yes
Transparent Sensitive Data Protection               Yes

AUDITING
Traditional Audit                                   Yes
Fine Grained Audit                                  Yes
Unified Audit                                       Yes

USER AUTHENTICATION
External Authentication                             Yes
Global Authentication                               Yes

•Patch Check *
Status: Severe Risk
Summary:
    Latest Oracle Database PSU not found.
Details:
    No patches have been applied.

•Remarks:
   It is vital to keep the database software up-to-date with security
   fixes as they are released. Oracle issues Patch Set Updates (PSU) and
   Critical Patch Updates (CPU) on a regular quarterly schedule. These
   updates should be applied as soon as they are available.

### User Accounts ###
    Note: Predefined Oracle accounts which are locked are not included in
    this report. To include all user accounts, run the report with the -a
    option.

* User Accounts *

User Name          Status           Profile    Default Tablespace Predefined
------------------ ---------------- ---------- ------------------ ----------
ABHIK              OPEN             DEFAULT    SYSTEM                     No
ADAMS              OPEN             DEFAULT    SYSTEM                    Yes
ANITA              OPEN             DEFAULT    SYSTEM                     No
ANTHONY            OPEN             DEFAULT    SYSTEM                     No
APP1_DATA          OPEN             DEFAULT    SYSAUX                     No
BIZAPP             OPEN             DEFAULT    SYSTEM                     No
BIZAPP_PROXY       OPEN             DEFAULT    SYSTEM                     No
BLAKE              OPEN             DEFAULT    SYSTEM                    Yes
CLARK              OPEN             DEFAULT    SYSTEM                    Yes
CTXSYS             OPEN             DEFAULT    SYSTEM                    Yes
```

DBSAT Requirements

- **Database: Run with DBA role or the following privileges/roles**
  - CREATE SESSION
  - SELECT on SYS.REGISTRY$HISTORY
  - SELECT on AUDSYS.AUD$UNIFIED (12c only)
  - SELECT on SYS.DBA_USERS_WITH_DEFPWD (11g and 12c)
  - Role SELECT_CATALOG_ROLE
  - Role DV_SECANALYST (if Database Vault is enabled)
  - Roles AUDIT_VIEWER (12c only) and CAPTURE_ADMIN (12c only)
- **OS**
  - DBSAT Collector: run with OS user who can read the ORACLE_HOME directory and files
  - DBSAT Reporter: Python 2.6 or later (can run on other machines also)

Easy to Install and Run

1. Download DBSAT from http://www.oracle.com/technetwork/database/security/dbsat.html
   - Available to all Oracle database customers with active support contract
   - Always check for the latest version
2. Collect security config data by executing ‘dbsat collect’ on the target
   - Needs read only privileges
   - Platform independent
   - Output file is by default compressed and password protected
3. Execute ‘dbsat report’ on the target or elsewhere
4. Restrict access to the generated reports as they have sensitive data

Where To Start & What to look for

Who are the users and their entitlements?
What controls do I have in place?
Is my Database securely configured?

Do we have a Database Security Team? Knowledge?
Analysis time?

DBSAT Summary

- Quickly evaluate risks to your Oracle databases
- Promptly identify security misconfigurations
- Identify users and their entitlements
- Reduce the attack surface and exposure to risk
- Safeguard your sensitive data by following recommendations
- Raise security posture for your Oracle Databases

Connect With Us

/OracleDatabase
#DBSAT

/OracleSecurity

blogs.oracle.com/
SecurityInsideOut

Oracle Database Insider

/Oracle/database

/OracleLearning

oracle.com/database/security

oracle.com/technetwork/database/security

pedro.lopes@oracle.com