

Oracle Database Security 23c New Features

Focusing on Major Security
Enhancements

November 2023

Stefan Oehrli

Stefan Oehrli – Data Platforms

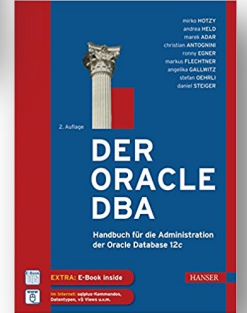


stefan.oehrli@accenture.com



Tech Architecture Manager

- Since 1997 active in various IT areas
- More than 25 years of experience in Oracle databases
- Focus: Protecting data and operating databases securely
 - Security assessments and reviews
 - Database security concepts and their implementation
 - Oracle Backup & Recovery concepts and troubleshooting
 - Oracle Enterprise User and Advanced Security, DB Vault, ...
 - Oracle Directory Services
- Co-author of the book The Oracle DBA (Hanser, 2016/07)



DATA PLATFORMS

WHY? We are the game changer for our client's data platform projects

HOW? Maximum automation, maximum efficiency, maximum quality!

WHAT? We build innovative data platforms based on our blueprints, assets and tools.



3 key benefits

- 1 Architecture expertise from hands-on projects
- 2 Delivery of tailor-made data platforms
- 3 Integrated Teams - Like a Rowing team, perfect alignment and interaction.



Tools and Blueprints

Key enabler for the implementation of modern data platforms at a high speed and quality.

Continuous Optimization

Tools and Blueprints are continuously optimized to the customer and project's needs.

Expertise

Expert group for modern data platforms from technical implementation to project management and organization



Oracle CMU

What needs to be considered besides the configuration of Oracle CMU?

- 1 Introduction
- 2 SQL Firewall
- 3 Authentication
- 4 Authorization
- 5 Auditing
- 6 Encryption
- 7 Further Innovations
- 8 Conclusion

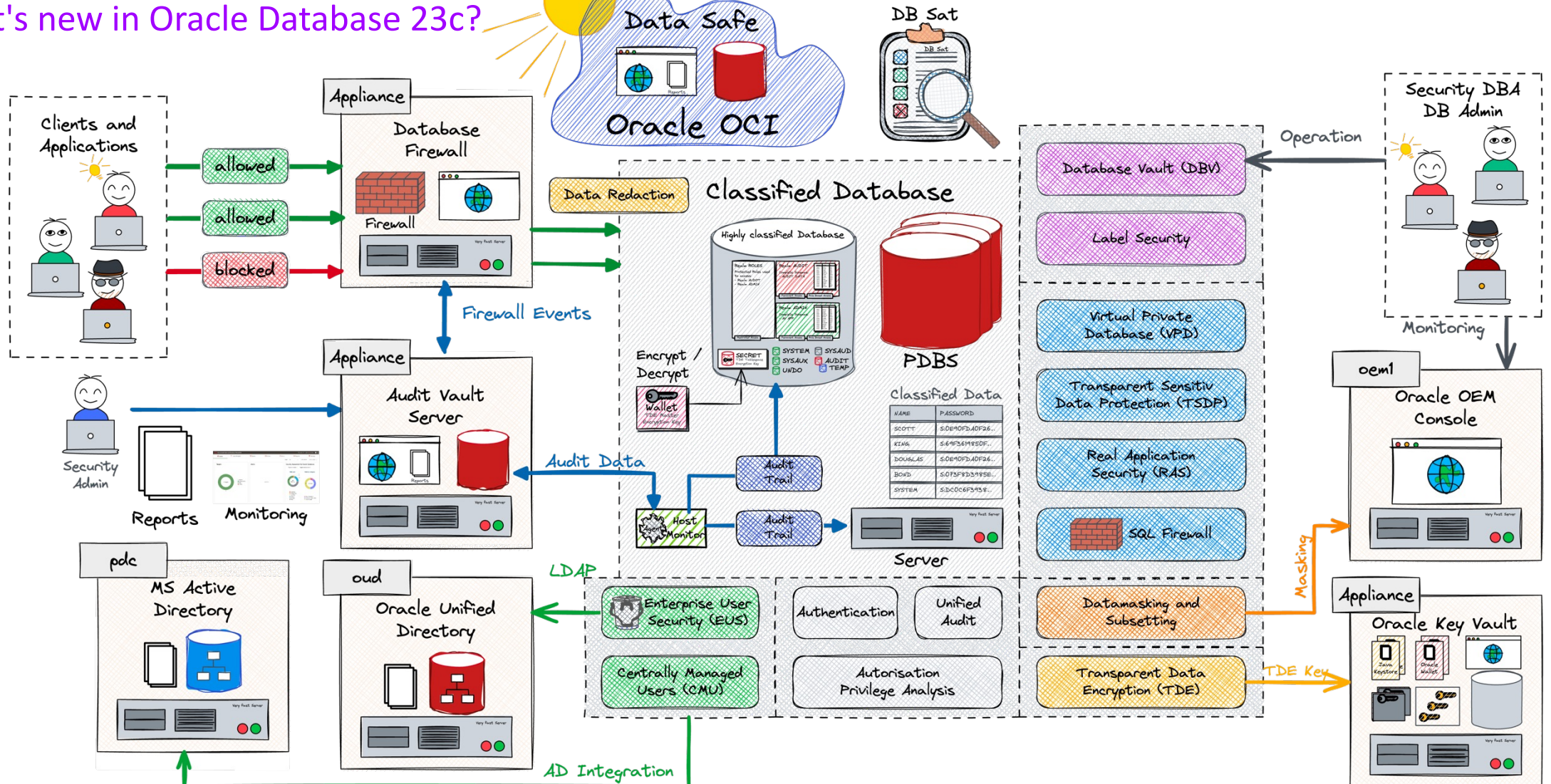
1

Introduction

What about the
Security Features in
23c?

Maximal Database Security Architecture

What's new in Oracle Database 23c?



In a Nutshell

New Security Features in Oracle Database 23c on the Horizon

Exploring New Frontiers

- SQL Firewall: A Major Leap in Database Security

Doing the Housework

- Adapting to new standards for enhanced security
- Incremental upgrades in auth, audit, and encryption

Saying Farewell to Familiar Features

- Deprecation of Enterprise User Security (EUS)
- Desupport of Traditional Auditing
- Desupport of Case Insensitive Passwords

Areas of Continued Development

- Oracle DB Nest?



2

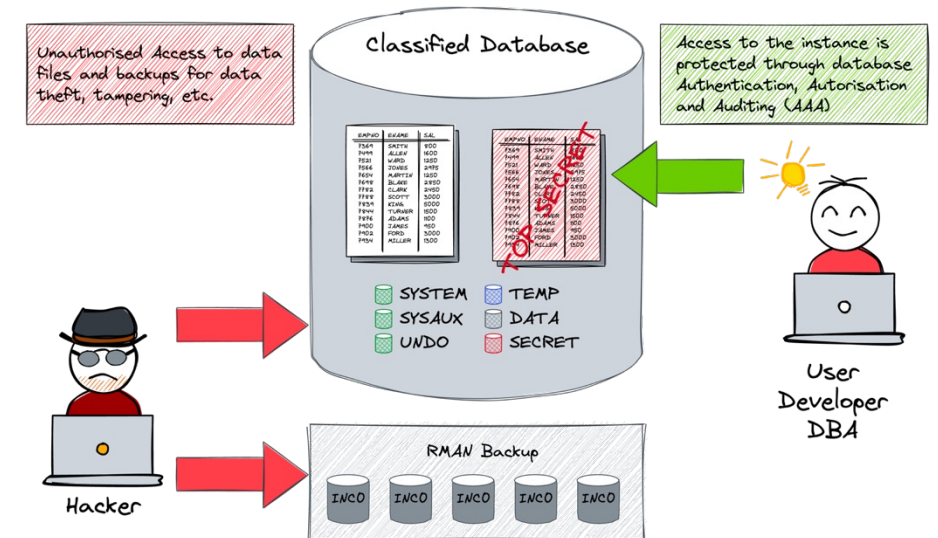
SQL Firewall

The latest Security
Achievement

The Security Challenges of a Database

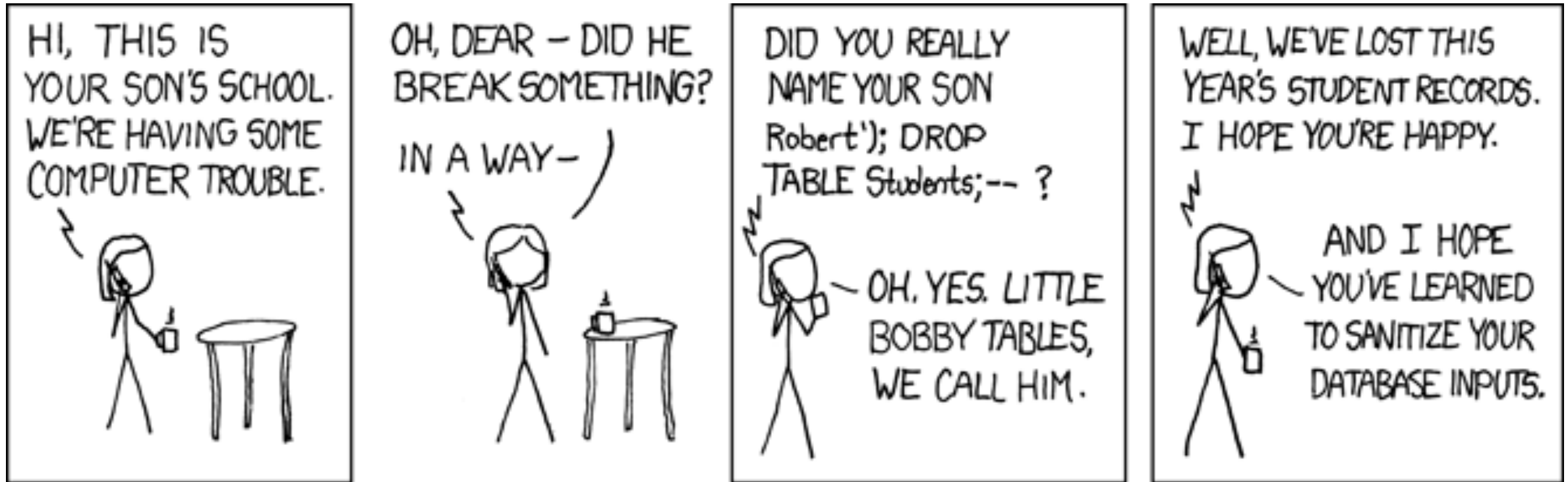
The dirty dozen...

- **Access Bypass:** Unpatched or misconfigured database vulnerabilities.
- **Privilege Abuse:** Exploiting application vulnerabilities for higher access.
- **Sensitive Data Search:** In unprotected systems and databases.
- **Credential Theft:** Via phishing, social engineering, or malware.
- **System Bridging:** Using less secure systems to target secure ones.
- **Password Exploitation:** Guessing or poor management.
- **SQL Injection:** Manipulating user input to exploit applications.
- **Rogue Accounts:** For reconnaissance and access escalation.
- **Non-Production Data Risks:** Targeting less secure dev/test environments.
- **Unencrypted Data Exposure:** Accessing or stealing files from disk or backups.



SQL Injection

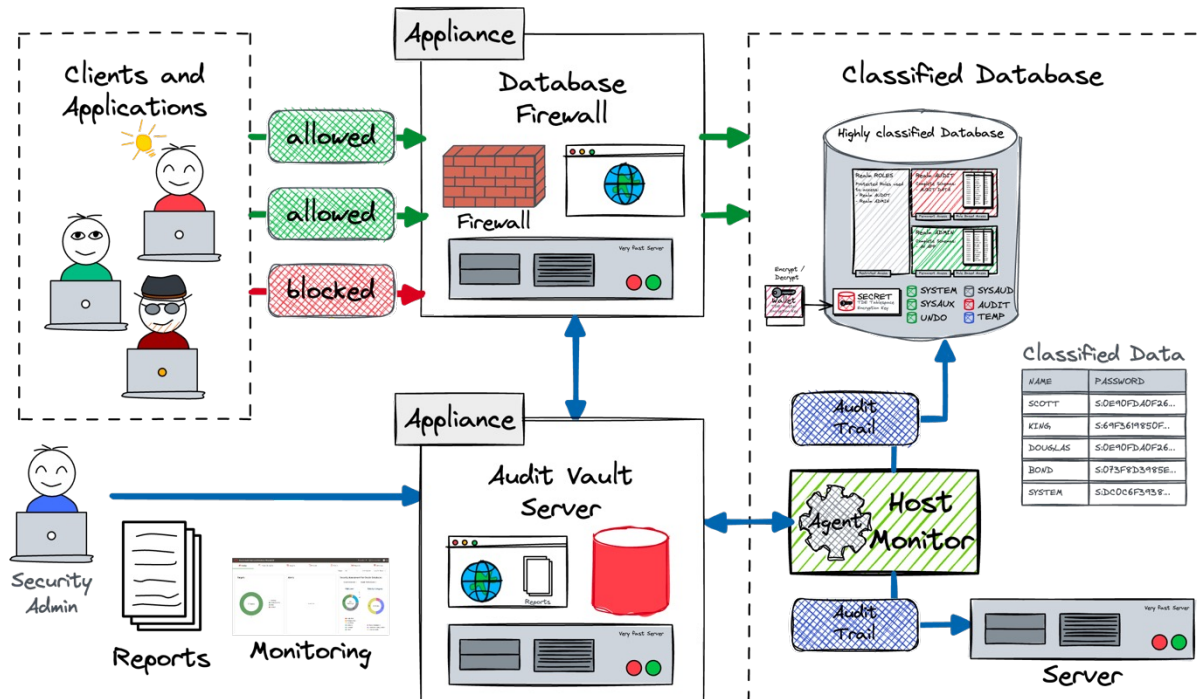
Exploits of a Mom



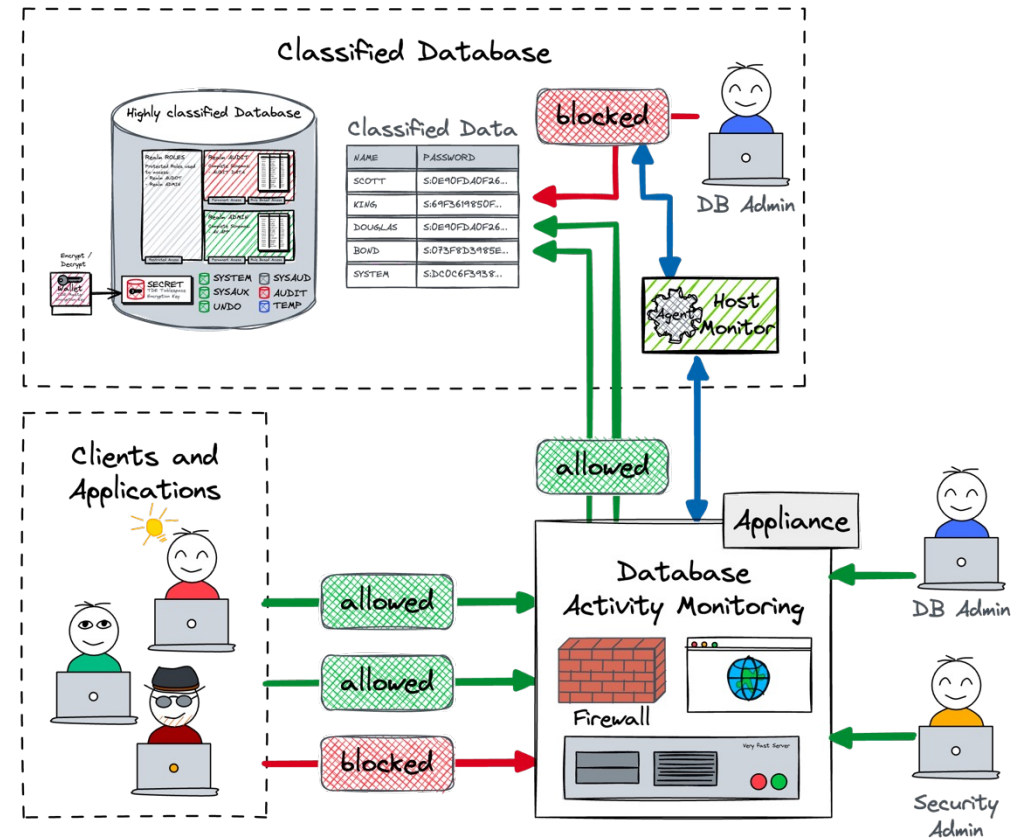
xkcd: <https://xkcd.com/327>

But we already have it, don't we?

Oracle Audit Vault and Database Firewall



Database Activity Monitoring



SQL Firewall Overview

What exactly is it about?

Real-Time Protection

- Blocks unauthorized SQL and preventing SQL injection and access anomalies

Customizable Allow-Lists

- Create specific SQL permissions for each user, with logging of unusual activities

Connection and Statement Control

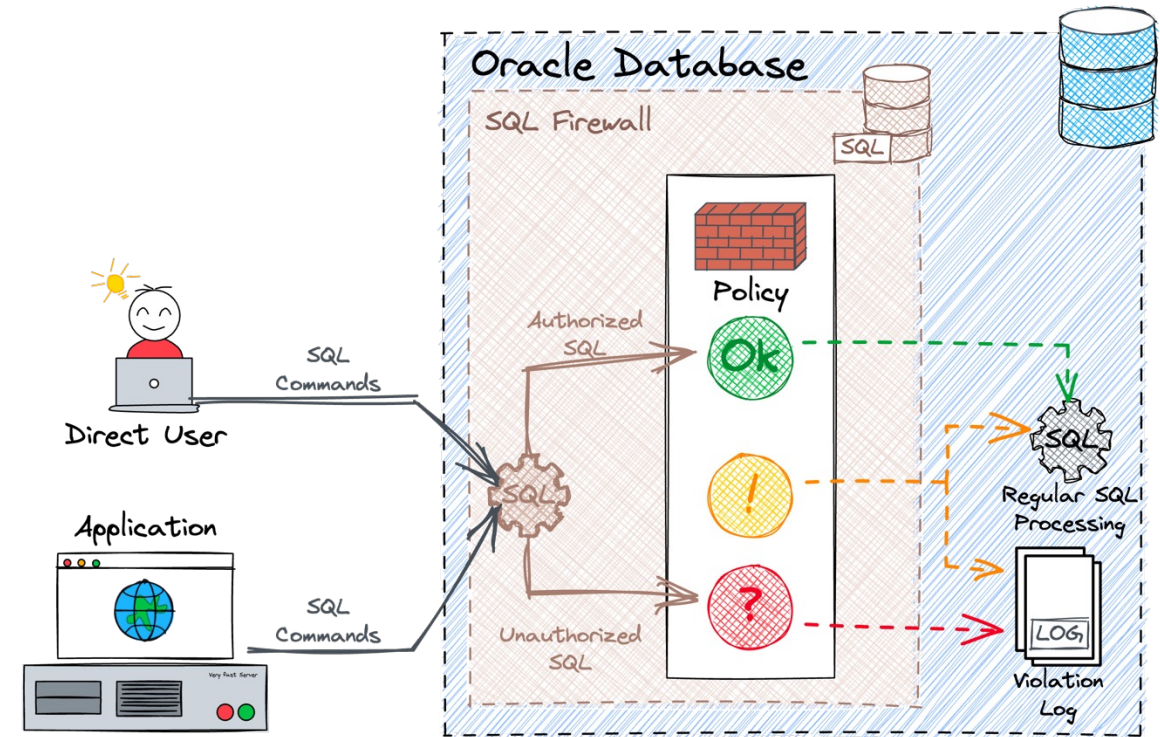
- Manages **allowed** SQL **statements** and **connection** paths, e.g. IP addresses, context etc.

Integrated into Oracle Database

- Ensures inspection of all SQL activities, including encrypted and network SQL

Flexible Policy Application

- Tailored policies for different database accounts, enhancing gradual security improvement



Navigating SQL Firewall - Processes

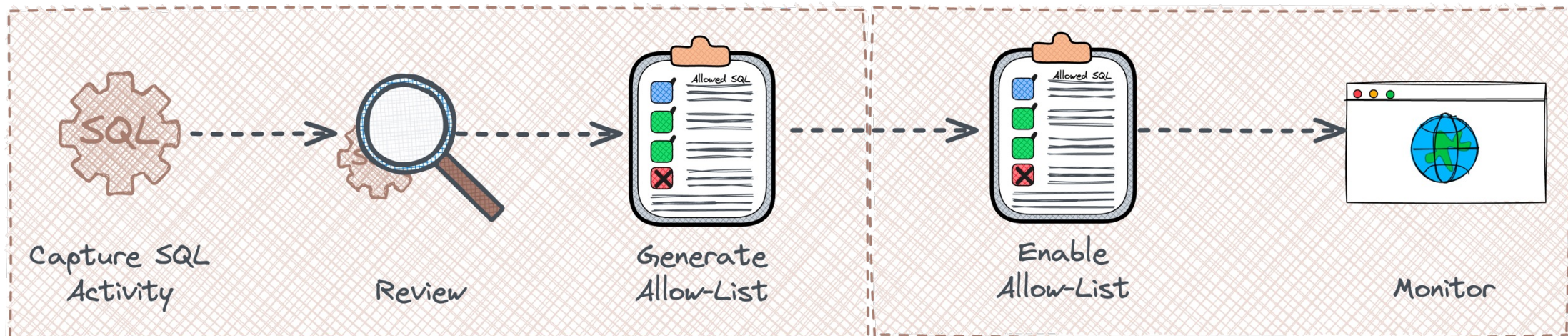
Understanding the Mechanics and Strategies for Optimal Deployment

Learning Stage

- **Capture** the user's SQL activities
- **Review** the capture
- **Generate** an allow-list

Protecting Stage

- **Enable** the allow-list
- **Monitor violations** SQL Firewall raises violation for any unexpected access patterns.



Navigating SQL Firewall - Usage

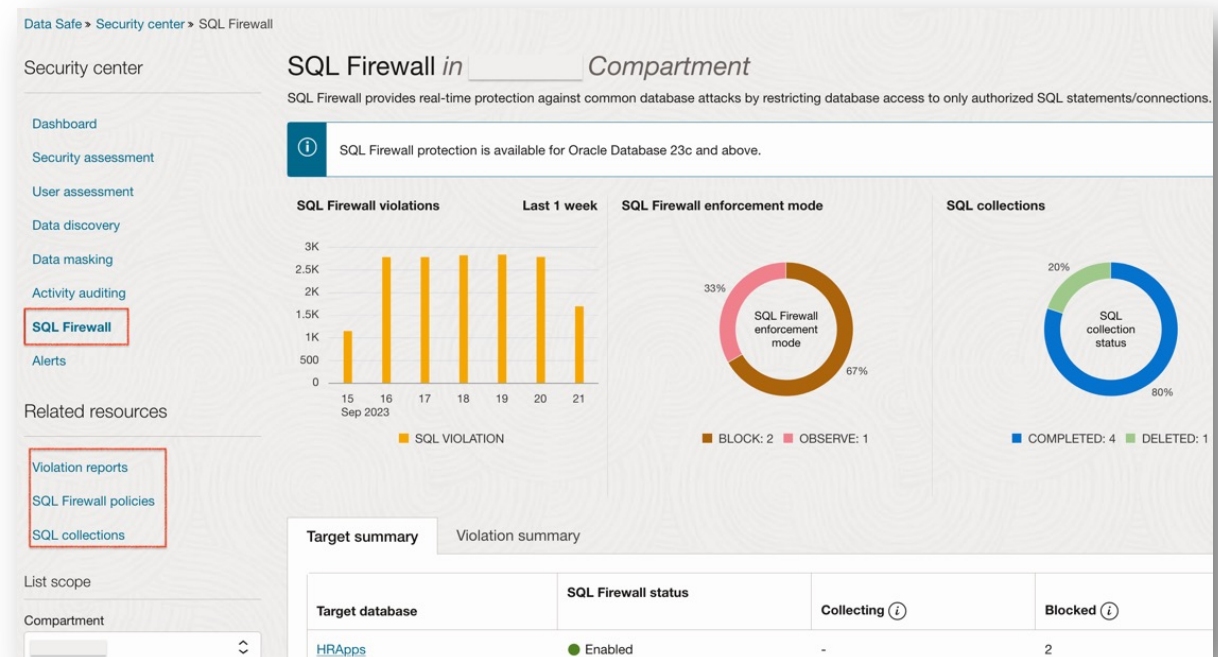
CLI or GUI you choose...

SQL Interface for the brave DBA

- System Privilege `ADMINISTER SQL FIREWALL`
- Predefined Roles
 - `SQL_FIREWALL_ADMIN`
 - `SQL_FIREWALL_VIEWER`
- Data Dictionary Views
- Violation Log `DBA_SQL_FIREWALL_VIOLATIONS`
- Capture Log `DBA_SQL_FIREWALL_CAPTURE_LOGS`
- A couple more `DBA_SQL_FIREWALL_`%
- Several base table in `SYSAUX` i.e.
`FW_CAPTURE$`, `FW_ALLOW_LIST$`,
`VIOLATION_LOG$`, ...

Oracle Data Safe on Oracle Cloud

- Manage multiple SQL Firewalls centrally
- Comprehensive view of SQL Firewall violations



SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Connect as user with `SQL_FIREWALL_ADMIN` role
- Enable SQL Firewall

```
EXEC DBMS_SQL_FIREWALL.ENABLE;
```

- Check the status of the SQL Firewall

```
SELECT * FROM dba_sql_firewall_status;
```

STATUS	STATUS_UPDATED_ON	EXCLUDE_JOBS
-----	-----	-----
ENABLED	21.11.23 06:30:01.430118000 +01:00	Y

SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Enable a capture for the user SCOTT

```
BEGIN
  DBMS_SQL_FIREWALL.CREATE_CAPTURE (
    username          => 'SCOTT',
    top_level_only    => TRUE,
    start_capture     => TRUE
  );
END;
/
```

- Verify what SCOTT is doing

```
SELECT sql_text FROM dba_sql_firewall_capture_logs
WHERE username = 'SCOTT';
```


SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Disable capture for user SCOTT

```
EXEC DBMS_SQL_FIREWALL.STOP_CAPTURE ('SCOTT');
```

- Generate an allow-list for user SCOTT

```
EXEC DBMS_SQL_FIREWALL.GENERATE_ALLOW_LIST ('SCOTT');
```

- Query the allowed activity for user SCOTT
 - DBA_SQL_FIREWALL_ALLOWED_IP_ADDR
 - DBA_SQL_FIREWALL_ALLOWED_OS_PROG
 - DBA_SQL_FIREWALL_ALLOWED_OS_USER
 - DBA_SQL_FIREWALL_ALLOWED_SQL



SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Customize the allow-list e.g. `DBMS_SQL_FIREWALL.ADD_ALLOWED_CONTEXT` and `DBMS_SQL_FIREWALL.DELETE_ALLOWED_CONTEXT`
- Enable the allow-list using `DBMS_SQL_FIREWALL.ENABLE_ALLOW_LIST`

```
BEGIN
  DBMS_SQL_FIREWALL.ENABLE_ALLOW_LIST (
    username      => 'SCOTT',
    enforce       => DBMS_SQL_FIREWALL.ENFORCE_SQL,
    block         => TRUE
  );
END;
/
```

- Start having fun with the protected Database...



SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Limited availability of SCOTT

```
SQL> SELECT ename,sal FROM scott.emp WHERE ename='SCOTT';  
SELECT ename,sal FROM scott.emp WHERE ename='SCOTT'  
                                     *  
  
ERROR at line 1:  
ORA-47605: SQL Firewall violation
```

- Chooses wisely what and when to capture application activity

Beyond the Basics - SQL Firewall Insights

Key Considerations and Advanced Knowledge

Smooth integration with other Oracle products

- **Multitenant Environment** both the CDB root and the individual PDB levels are affected
- **Oracle Centrally Managed Users** capture global user's activities is supported
- **Oracle Scheduler** jobs are excluded by default
- **Oracle Database Vault** tbd / not verified
- **Oracle Data Pump** Export and Import supports different use cases
 - Export and import SQL Firewall captures and allow-lists metadata e.g. `INCLUDE=SQL_FIREWALL`
 - Consider Procedures `DBMS_SQL_FIREWALL.EXPORT_ALLOW_LIST` or `DBMS_SQL_FIREWALL.IMPORT_ALLOW_LIST` to transfer allow-list

3

Authentication

The "*Who's Who*" in the database

Authentication

No breaking news, just continuous improvement

- Increased **Maximum** Password Length
 - Passwords now can have up to 1024 bytes used to be 30 bytes
- Desupport of Case Insensitive Passwords i.e. legacy 10g Password hash
 - Problem when a user only has a 10g password hash

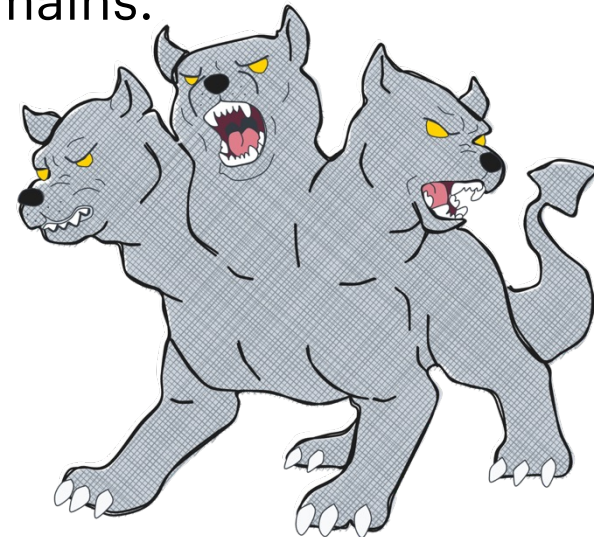
```
SELECT
    username
FROM
    dba_users
WHERE
    ( password_versions = '10G '
      OR password_versions = '10G HTTP ' )
AND username <> 'ANONYMOUS';
```



Authentication

No breaking news, just continuous improvement

- Clean up and adjust **Password Policies** i.e.g scripts `utlpwdmg.sql` and `catpvf.sql`
 - The Profile `ora_stig_profile` has now a password life time of 35days
 - Old verify function have been removed e.g. `verify_function_11G` and `verify_function`
- Updated **Kerberos Library** and **Improvements**
 - KERBEROS5_CC_NAME supports multiple principals and stores in encrypted format
 - It provides cross-domain support for accessing resources in other domains.
 - It supports Windows Credential Guard
 - Kerberos on Database can search for the KERBEROS5_CC_PRINCIPAL
 - The `okinit`, `oklist`, and `okdstry` utilities work with encrypted cache
- **RADIUS** Configuration Enhancement
 - Supports for Requests for Comments (RFC) 6613 and 6614 guidelines



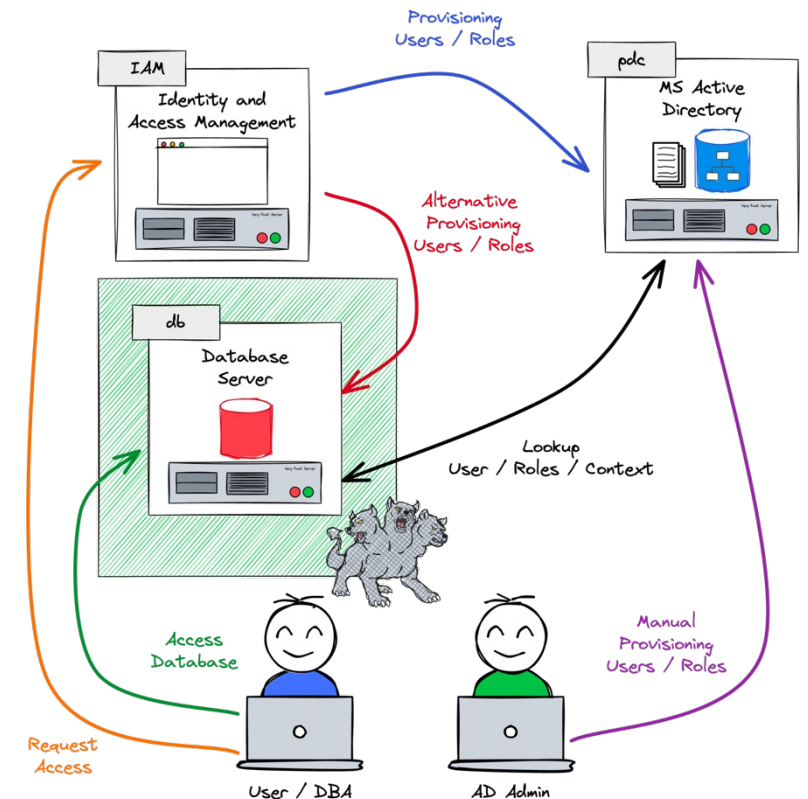
Deprecation Enterprise User Security (EUS)

It is time to say goodbye...

- Enterprise User Security (EUS) has been deprecated
 - No hurry, it will not be removed immediately
 - Consider next upgrade wisely
 - Along this mkstore is deprecated as well

Alternatives?

- Oracle **Centrally Managed Users** (CMU)
 - ... does not require an additional Oracle directory
 - ... enables the administration of users directly in MS AD
 - ... does not require an additional license but
 - ... Supported only by Oracle Enterprise or Free Edition



4

Authorization

Who can do what in the Database...

Authorization - Privileges

Simplified Operation and increased Security

Have you ever seen a database with **SELECT ANY** privileges?

- I.e. because someone needs access to the application schema
- Or tons of GRANT SELECT ON...

Oracle Database now does support schema privileges

- Grant access to a whole schema rather to individual objects

```
GRANT READ ANY TABLE ON SCHEMA SCOTT TO oehrli;
```

Introduction of new Views as part of this new privilege?

- DBA_SCHEMA_PRIVS, ROLE_SCHEMA_PRIVS, USER_SCHEMA_PRIVS, SESSION_SCHEMA_PRIVS, V\$ENABLEDSCHMAPRIVS

Authorization – READ Only

Allow restricted access to data

- Configure a user as **read only** user
 - override the privileges and roles that **have been** granted
 - allows SELECT operations but not CREATE, INSERT, UPDATE, or DELETE
- Create a read only user or alter

```
CREATE USER oehrli READ ONLY;
```

- Finding Information about read only user in ...
 - ...DBA_USERS

```
SELECT USERNAME, READ_ONLY from DBA_USERS  
WHERE USERNAME = 'OEHRLI';
```

- Granting **read only** access for maintenance or investigative reasons
- read-only access to parts of an application



Other Stuff

What else has been improved?

New database role for developers `DB_DEVELOPER_ROLE`

- **least-privilege** principles for application developer DBA role is not required
- **provides most of** the system and object privileges as well predefined roles, PL/SQL package privileges required for application development

Oracle Data **Dictionary Protection**

- Extended to **Non-SYS** Oracle schemas with separation of duties protection
- Other users cannot use system privileges e.g. ANY privileges) on the schema
- Can be enabled/disabled if required

```
SELECT username, dictionary_protected FROM dba_users  
WHERE dictionary_protected='YES';
```



5

Auditing

The DB is whatching
you...

Desupport of Traditional Auditing

Long announced and now finally implemented...

- Traditional Auditing not available any more
- Auditing as to be defined using audit policies
- Oracle Support Note [2909718.1](#) *Traditional to Unified Audit Syntax Converter - Generate Unified Audit Policies from Current Traditional Audit Configuration*
- Be carefull when upgrading Databases
 - Review your audit setting and concept

```
SQL> AUDIT CREATE TABLE;
```

```
AUDIT CREATE TABLE
```

```
*
```

```
ERROR at line 1:
```

```
ORA-46401: No new traditional AUDIT configuration is allowed. Traditional auditing is  
desupported, and you should use unified auditing in its place.
```


Audit Use Cases

It is time to define / implement a decent audit concept



Other Audit Enhancements

Small but helpful improvements...

- Column Level Audit for Tables and Views
 - Allow to specify a column for action UPDATE
 - Create more granular and focused audit policies
 - Does not make audit concept easier ☺

```
CREATE AUDIT POLICY scott_sal ACTIONS UPDATE(sal) ON scott.emp;
```

- Behaviour change for AUDIT POLICY statement
 - Changes made to the audit policy become effective **immediately...**
 - ...in the current session
 - ...in all active sessions without re-login
 - Audit deployment is therefore **much** easier => no downtime



Just one more thing...

It seems that there are new functions in the queue.

- New hidden parameter related to audit

```
SQL> @hip prote%audit
```

Parameter	Session Instance	S	I	D	Description
-----	-----	---	---	---	-----
_enable_protected_audit_policy	FALSE				Allow Protected Unified Audit Policy Enforcement

- Along with a new undocumented column in AUDIT_UNIFIED_POLICIES

```
SQL> desc AUDIT_UNIFIED_POLICIES
```

Name	Null?	Type
-----	-----	-----
POLICY_NAME		VARCHAR2(128)
...		
ORACLE_SUPPLIED		VARCHAR2(3)
PROTECTED		VARCHAR2(3)
COLUMN_NAME		VARCHAR2(128)

- Possibility to enforce audit policies in PDBs



6

Encryption

At REST and in transition

Encryption at REST

Changes around Transparent Data Encryption (TDE)

Encryption **Algorithm** changes

- The default encryption algorithm for TDE Column and Tablespace is now **AES256**
- Decryption libraries for the GOST and SEED are desupported

Changed Encryption **Modes**

- **TDE Column** Galois/Counter mode (GCM) instead of Cipher Block Chaining (CBC),
- **TDE Tablespace** Tweakable Block Ciphertext Stealing (XTS) operating mode or cipher feedback (CFB) (Default)

```
CREATE TABLESPACE users_enc DATAFILE  
'/u02/oradata/CDB23A/users_enc01CDB23A.dbf' SIZE 100M  
ENCRYPTION USING AES256 MODE 'XTS' ENCRYPT;
```

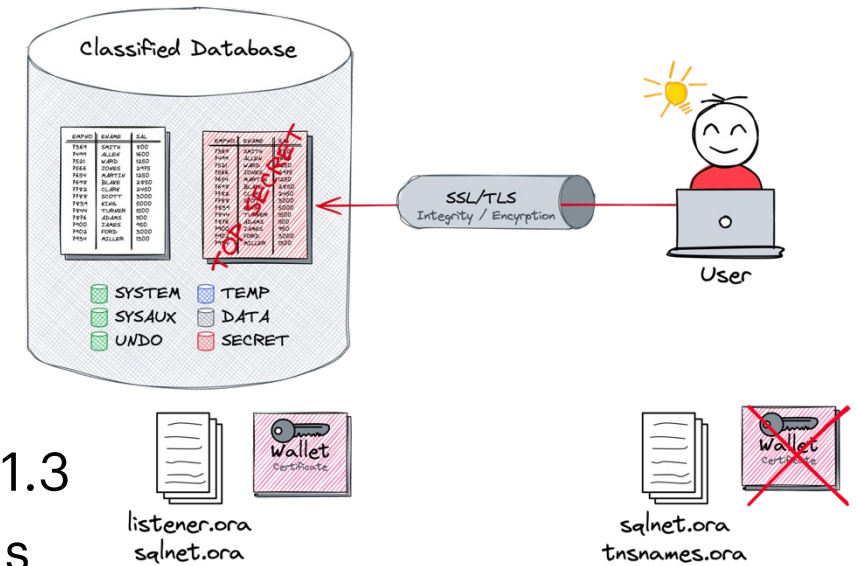


Encryption in Transition

Changes related to Network Encryption, Certificates, TLS

TLS 1.3 finally arrived in Oracle Database

- Oracle Database 23c Transport Layer Security (TLS) version 1.3
- Initial session setup more efficiently than earlier TLS versions
- Configure in *sqlnet.ora* using `SSL_VERSION` and `SSL_CIPHER_SUITES`



Simplified Transport Layer Security Configuration

- Ability to Configure Transport Layer Security Connections **without Client Wallets**
- `SSL_VERSION` parameter does accept a comma-separated list e.g. TLSv1.3, TLSv1.2
- Introduction of the `ALLOWED_WEAK_CERT_ALGORITHMS` parameter
- Modifications to how wallets are loaded
 - **Server-side wallets** `WALLET_LOCATION` deprecated use `WALLET_ROOT` from *init.ora*
 - **Client-side wallets** Still use `WALLET_LOCATION` parameter, now defaults to `TNS_ADMIN`

7

Further Innovations

What else?

Further Innovations

What else...

A bunch of new SQLNet Parameter to control **weak, deprecated** ciphers

- e.g. SSL_ALLOW_WEAK_DN_MATCH

Azure Active Directory Integration

- Autonomous Database now can accept Azure AD **OAuth2** tokens to access the database

Authenticating and Authorizing IAM Users for Autonomous Database on dedicated Exadata

- **Enhanced Connection** Options:
 - Applications connect using end-user, instance, and resource principals.
- **Proxy Capabilities** for IAM Users:
 - IAM users can proxy via database user schema.
- **Database Link** Support:
 - IAM connections now support database links.



Database Security Assessment Tool (DBSat)

Latest Release Ready for Oracle 23c

STIG V2R8 compliance

- includes 30 new STIG findings and revised STIG group IDs

Enhanced Auditing and Security

- New auditing results, overall, up to 120 Security checks
- Support for Oracle Database 23c SQL Firewall

Sensitive Data Discovery

- Indian PAN and Aadhaar numbers

Improved Clarity and Quality

- one-line summary outline
- Compliance labels

Operational Enhancements

- New parameter
- Linux 64-bit ARM Support

The screenshot displays a 'Patch Check' finding. Annotations include:

- Rule ID:** Points to the 'INFO.PATCH' header.
- Brief description of recommended Action:** Points to the title 'The Oracle Database should be patched'.
- Comprehensive breakdown of the finding:** Points to the 'Details' section.
- Rationale and Recommendations:** Points to the 'Remarks' section.
- Mapping to Regulations:** Points to the 'References' section.
- Label Indicating Relevance to Regulations:** Points to the 'CIS', 'OBP', and 'STIG' tabs.
- Possible Risk Levels:** Points to the 'High Risk' status label.

Patch Check	
INFO.PATCH	
The Oracle Database should be patched	
Status	High Risk
Summary	Oracle Database version is supported but latest patch is missing. Latest comprehensive patch has not been applied.
Details	Latest patch not applied for a supported database version.
Remarks	Unsupported commercial and database systems should not be used because fixes to newly identified bugs will not be implemented by the vendor. The lack of support can result in potential vulnerabilities. Systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities, which leaves them subject to exploitation. When maintenance updates and patches are no longer available, the database software is no longer considered supported and should be upgraded or decommissioned.
It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates on a regular quarterly schedule. These updates should be applied as soon as they are available.	
References	Oracle Best Practice CIS Benchmark: Recommendation 1.1 DISA STIG: V-237697, V-237748, V-251802

Conclusion

Database Security with Oracle 23c: Not Just a Simple Maintenance Update

SQL Firewall: A Major Milestone

- The SQL Firewall stands out as a pivotal feature in Oracle 23c

Continuous Enhancement, Not Just Maintenance

- Impactful improvements beyond routine updates
- Enhancements integral to ongoing security evolution

Assessing with the Latest Tools

- Utilize latest DB Sat for 23c security assessment
- Advanced tool alignment with Oracle 23c capabilities

Personal Favorite Immediate Audit Policy Implementation

- Simplifies and enhances audit processes

Security checklist

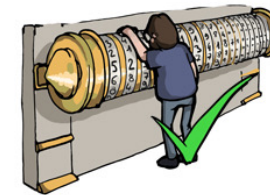
Anti-SQL-injection protection



SSL and OpenSSL up to date



Passwords hashed with salt



Multi-factor authentication on the back-office



AES encryption on sensitive data



Preventing the PM from sending the whole unencrypted database by email



**Oracle 23c's new security
features demand a
strategic approach to
unlock their full potential**

Thank You

