



Oracle Database 23ai New Security Features

What's new

Francisco Munoz Alvarez

Distinguished Product Manager

Competitive Intelligence - Mission Critical Database Product Management - Oracle Database High Availability (HA), Scalability, and Maximum Availability Architecture (MAA) Team



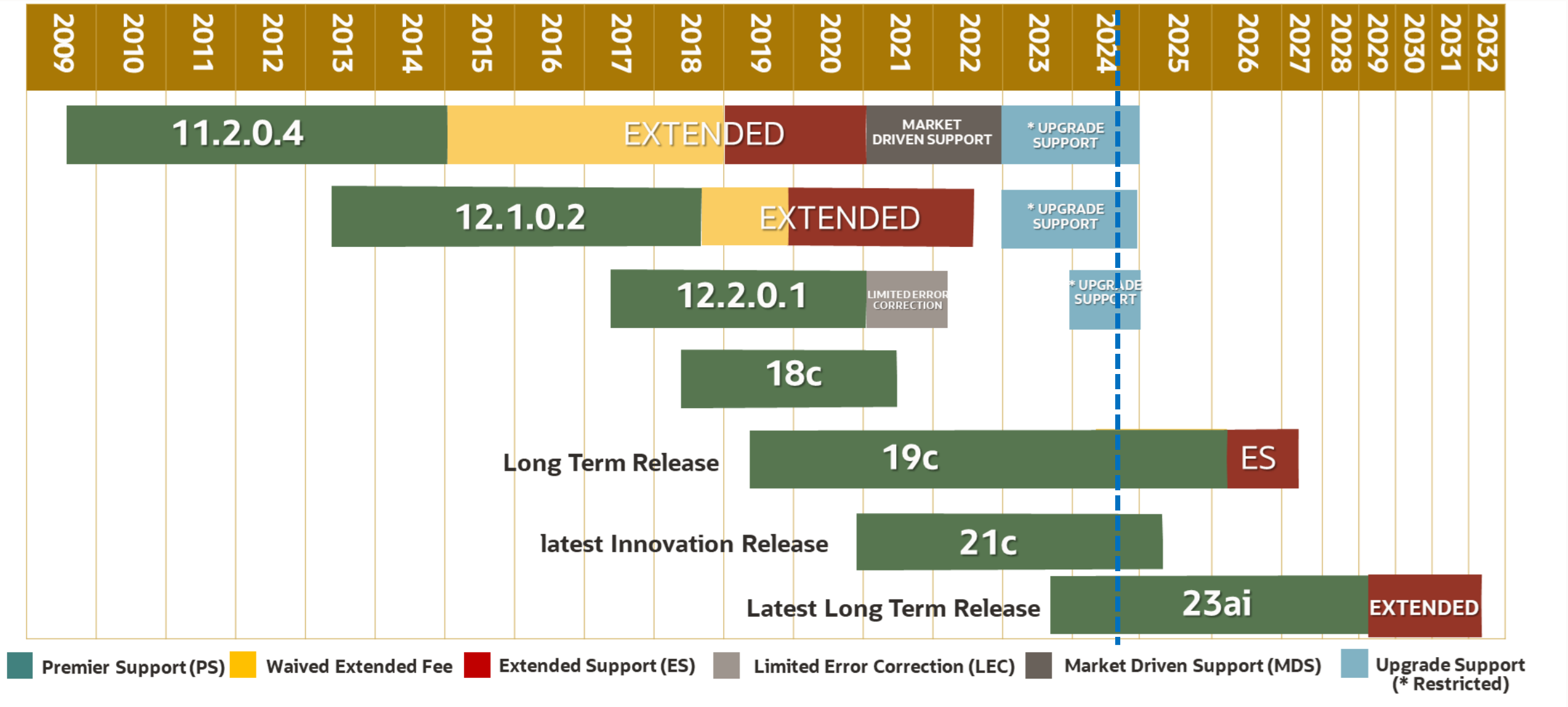
Oracle Database : 47 Years of Innovation

- World's most popular database
- Scales from a single CPU to thousands of CPUs
- Manages both OLTP and Data Warehousing workloads
- The most secure and highly available database for the enterprise

ORACLE®
Database



Database Releases and Support Timelines – September 2024



Always check MOS Note 742060.1 for the latest schedule
MOS note 161818.1 has details on support status.

* For more info on Upgrade Support, see:
• MOS note **2870402.1 (12.1)**
• **MOS note 2728619.1 (11.20)**



Oracle Database Security

A history of continuous innovation



Maximum Security Architecture (MSA)

A set of best practices for the integrated use of Oracle's database security technologies that minimizes security risks and assists with regulatory compliance requirements

Baseline security



Baseline security



Assess overall security

Baseline security



**Database Security
Assessment Tool
(DBSAT)**



Assess overall security

New in DBSAT 3.1 (April 2024)



Updated for Oracle Database 19c CIS Benchmark v1.2

- Added 10 CIS findings
- All CIS related findings updated to reflect changes in numbering scheme

Improved findings

- **USER.NOEXPIRE**
Improved logic and summary
- **USER.APPOWNER**
Optimizations to improve performance and reduce the level of detail
- **ENCRYPT.TDE**
Updated remarks to clarify the usage of the `TABLESPACE_ENCRYPTION` parameter and recommendations when upgrading to Oracle Database 23ai and you are using a de-supported algorithm

Added findings

- `USER.DEFAULTPROFILE`
- `PRIV.NETPACKAGEPUBLIC`
- `PRIV.FILESYSTEMPACKAGEPUBLIC`
- `PRIV.ENCRYPTPACKAGEPUBLIC`
- `PRIV.JAVAPACKAGEPUBLIC`
- `PRIV.JOBSCHPACKAGEPUBLIC`
- `PRIV.QUERYPACKAGEPUBLIC`
- `PRIV.CREDPACKAGEPUBLIC`
- `AUDIT.SYNONYMS`
- `CONF.DEFAULTPDBOSUSER`
- **CONF.PREAUTHTHREQUESTURL**
On ADBs, checks for pre-authenticated URLs

DBSAT 3.1.0.0.2 (July 2024) – Minor release



Improvements

- **AUDIT.CONNECTIONS**
User logon audit policies are now better identified in cloud databases
- **NET.ENCRYPTION**
improved network encryption query to properly handle Oracle Database 11g
- **Mentions to privileges and role grants to PUBLIC**
Improved “Summary” to clarify that once a role or privilege is granted to PUBLIC, all users will have that grant.
- **Updated “Remarks” to mention Oracle Database 23ai**
Replaced references to 23c
- **Removed STIG ID mapping**
STIG ID V-237748 mapping was removed as it is not part of STIG V2R8 for the Oracle Database
- **Fixed “logging not defined” error**
Logging exception is now correctly handled
- **Addressed JSON path escape sequence errors in Windows platforms**

New checks

■ DBSAT 3.0 (38)
■ DBSAT 3.1 (10)

Total findings: 132

USER.DEFAULTPROFILE
PRIV.NETPACKAGEPUBLIC
PRIV.FILESYSTEMPACKAGEPUBLIC
PRIV.ENCRYPTPACKAGEPUBLIC
PRIV.JAVAPACKAGEPUBLIC
PRIV.JOBSCHPACKAGEPUBLIC
PRIV.QUERYPACKAGEPUBLIC
PRIV.CREDPACKAGEPUBLIC
AUDIT.SYNONYMS
CONF.DEFAULTPDBOSUSER
CONF.PREAUTHREQUESTURL
USER.APPOWNER
USER.SHARED
USER.OBJOWNER
USER.OBJAUTHZ
USER.SECURITYOBS

USER.GRANTOPTION
USER.SENSITIVEDATA
USER.IDLETIME
USER.TEMP
USER.DEV
USER.REPCAT
PRIV.OBJPUBLIC
AUTHZ.PASSWORDSCRIPTS
AUTHZ.DATAMASKING
AUTHZ.PKI
ACCESS.TSDP
AUDIT.CONDITION
AUDIT.SHAREDPROXY
AUDIT.TABLESPACE
AUDIT.CLEANUPJOBS
AUDIT.DATAPUMP

AUDIT.STIGPOLICY
AUDIT.DATABASEVAULT
AUDIT.LABELSECURITY
ENCRYPT.TLSFIPS
CONF.CONTROLFILES
CONF.REDOLOGS
CONF.ARCHIVELOG
CONF.SQLFIREWALL
CONF.READONLYHOME
CONF.DBCOMPONENTS
CONF.JOB
CONF.SOURCEANALYSIS
NET.CONNECTIONLIMITS
OS.INSTALLATIONUSER
OS.MULTIDB
OS.CMANLOCAL
OS.DIAGNOSTICDEST



Baseline security



Database Security
Assessment Tool
(DBSAT)



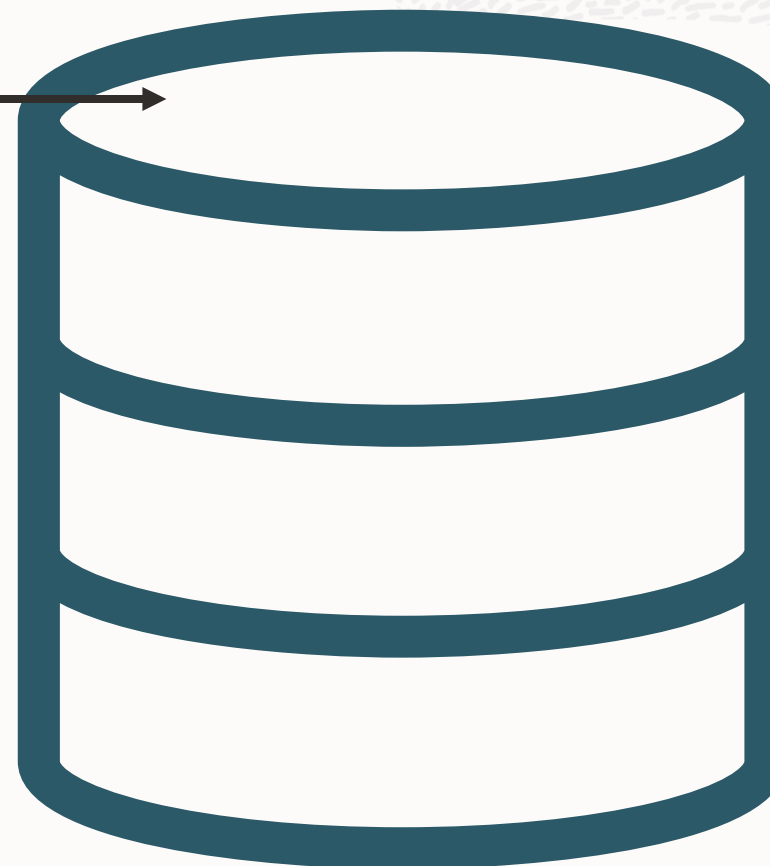
Assess overall security



* Included with Database Cloud, additional cost on-premises



Baseline security



Database Security
Assessment Tool
(DBSAT)



Assess overall security

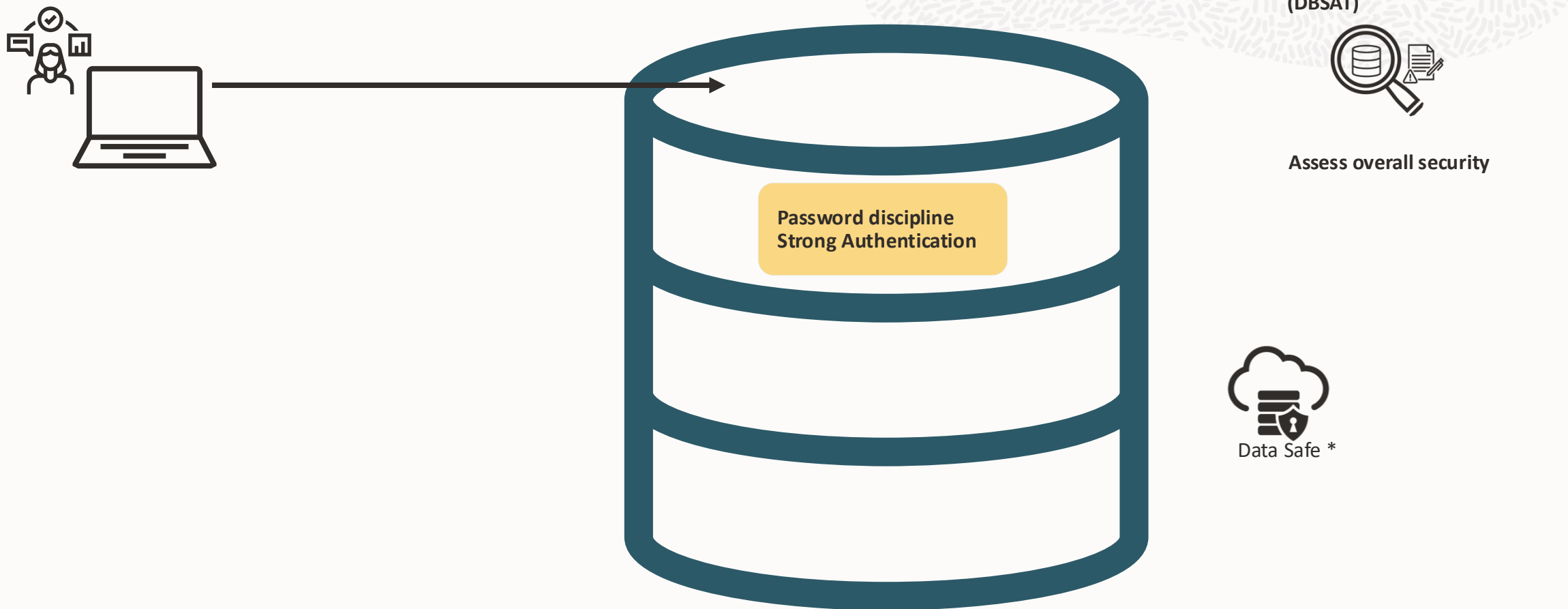


Data Safe *

* Included with Database Cloud, additional cost on-premises



Baseline security

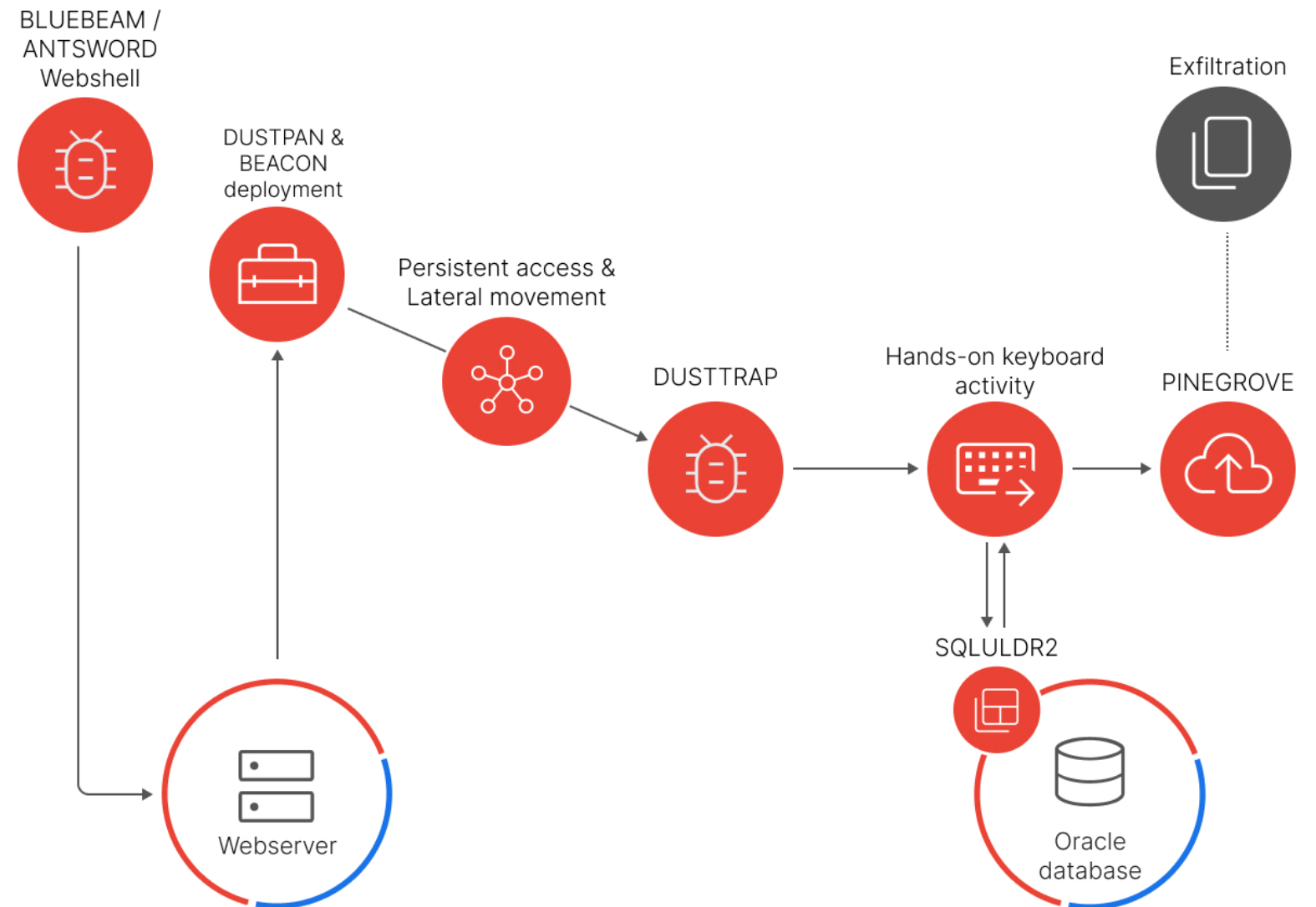


* Included with Database Cloud, additional cost on-premises

APT-41

From initial penetration to data exfiltration

Attack path diagram



<https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust>

SQLULDR2 – Stealing data from an Oracle Database

SQLULDR2 is a command-line utility written in C/C++ that can be used to export the contents of a remote Oracle database to a local text-based file. There are multiple command-line parameters available to specify the details of the data export including but not limited to: query, user, rows, and text.

APT41 exported data from Oracle Databases to CSV formats with the following command:

```
C:\ProgramData\luldr\luldr\sqluldr.exe user=<USER>@<SYSTEM>  
charset=utf8 safe=yes head=yes text=csv rows=50000000  
batch=yes query=<SQL QUERY> file=<OUTPUT>.csv
```

<https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust>



Longer passwords

Oracle Database 23ai expands the maximum length of a database password from 30 bytes to 1024 bytes

Benefits: Stronger password and passphrase support, especially for databases using multi-byte character sets

```
SQL> password
```

```
Changing password for TESTUSER
```

```
Old password: *****
```

```
New password:
```

Kerberos

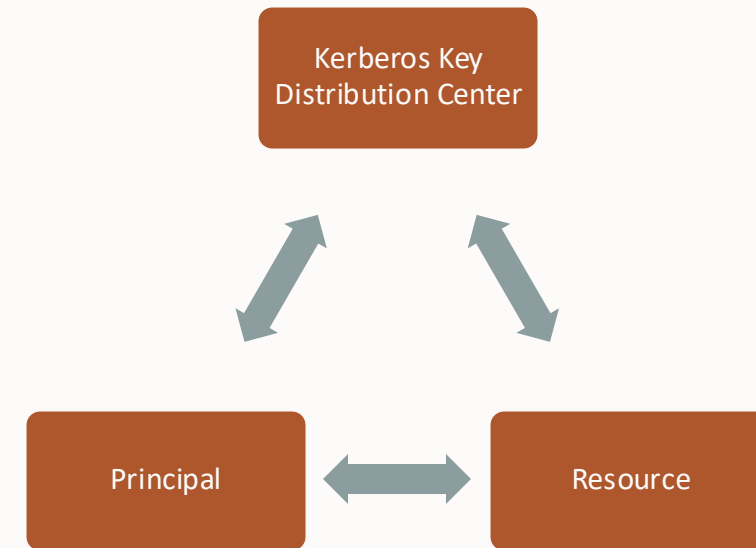
Kerberos is used for end-user authentication to the Oracle Database. 23ai adds:

Cross-domain support (client and server can be in separate domains – as long as a trust relationship exists between the domains!)

The MIT Kerberos library used by the Oracle Database and clients has been updated to version 1.21.2 (latest as of April 2024)

`sqlnet.ora` `KERBEROS5_CC_NAME` supports multiple principals

Clients can now specify the Kerberos principle and credential cache file as part of the connect string (`tnsnames.ora` or `ezconnect`)



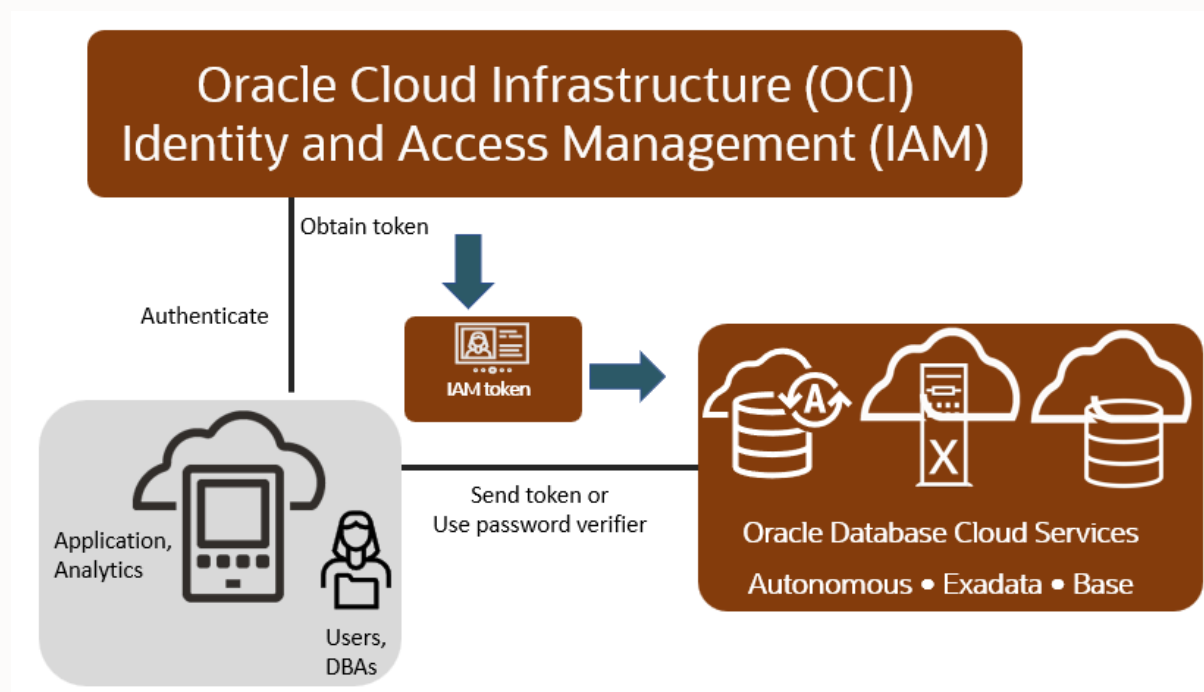
```

DATABASE_TNS_ALIAS=
(DESCRIPTION=
  (ADDRESS=(PROTOCOL=tcp)(HOST=sales-svr)(PORT=1521))
  (CONNECT_DATA=(SERVICE_NAME=sales.example.com))
  (SECURITY=
    (KERBEROS5_CC_NAME=/tmp/krbuser1/krb.cc)
    (KERBEROS5_PRINCIPAL=krbprinc1@example.com)))
  
```

OCI IAM integration

Use OCI IAM SSO tokens or IAM DB passwords

Backported to 19c OCI DBaaS databases



Microsoft Entra OAuth2 Integration

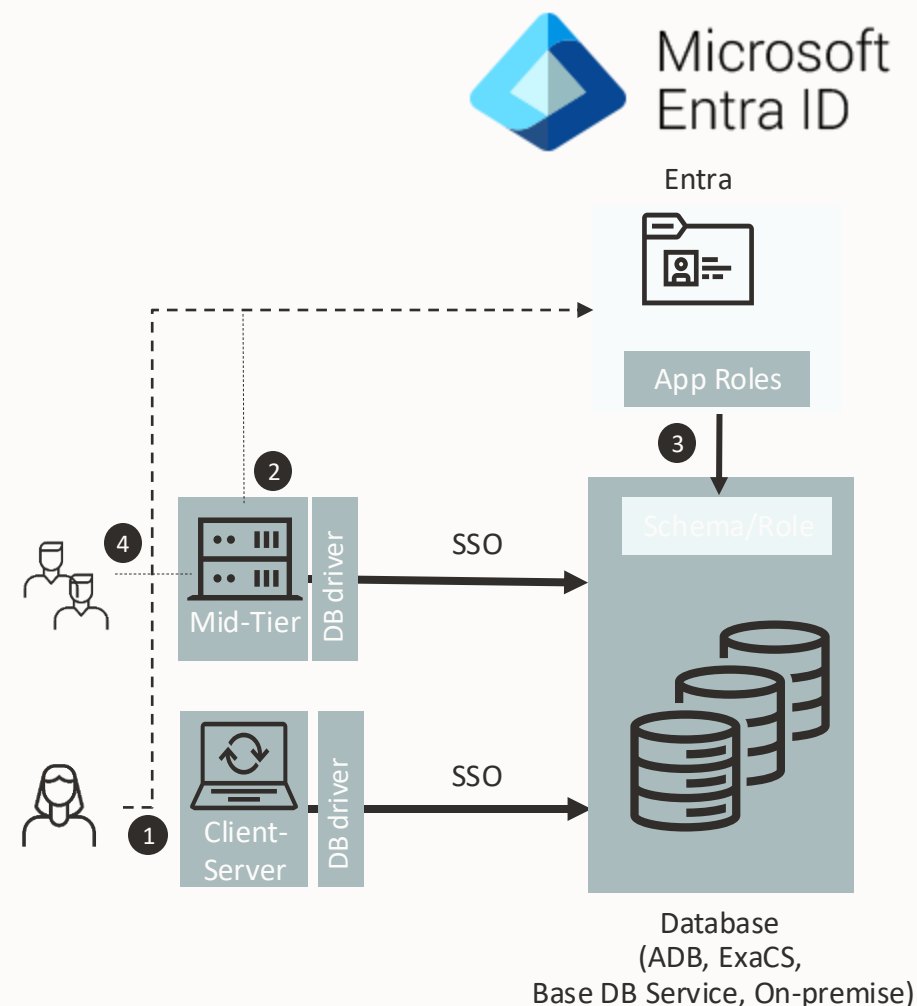
Formerly Azure AD – docs still say Azure AD

Entra users using client-server tools (e.g., SQL*Plus, SQL Dev) authenticate to databases using single-sign-on (SSO) OAuth2 tokens

Mid-tier/service accounts connect to databases using SSO tokens

Database maps the authenticated Entra user's app roles to local schema and roles for authorization

Applications can securely propagate end-user SSO token to the database



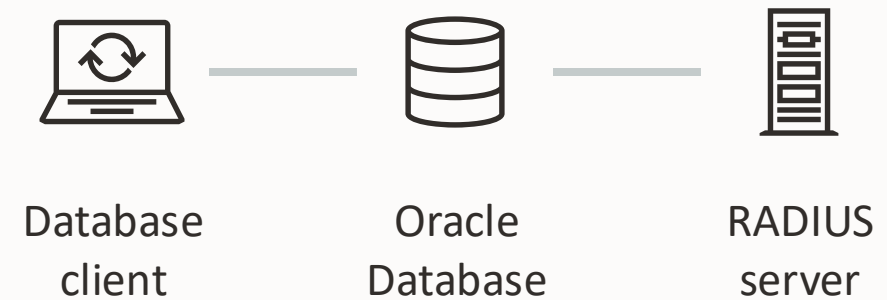
Backported to 19c OCI DBaaS databases

RADIUS API

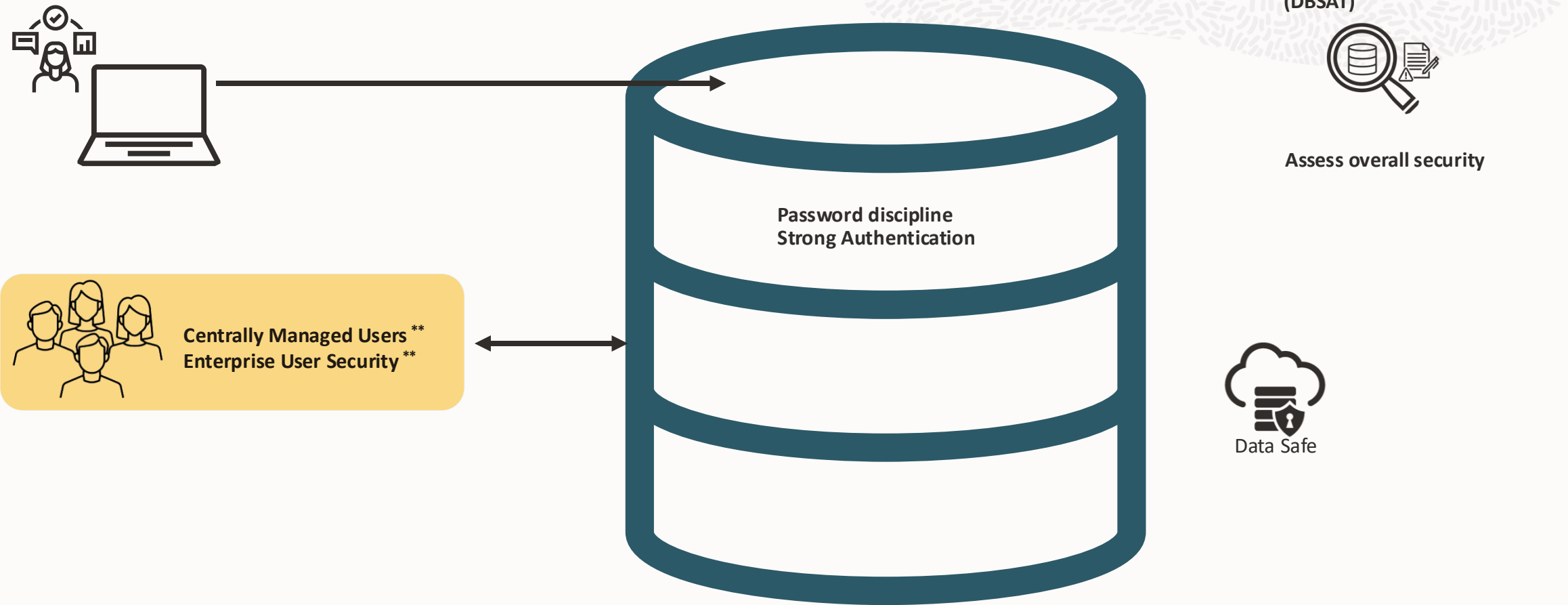
RADIUS API is used for multi-factor authentication for database administrators

New RADIUS API supports the latest standards

- RFC 6613, RFC 6614 for TLS.
- Legacy RADIUS API is deprecated but still available and can be used by setting a system parameter



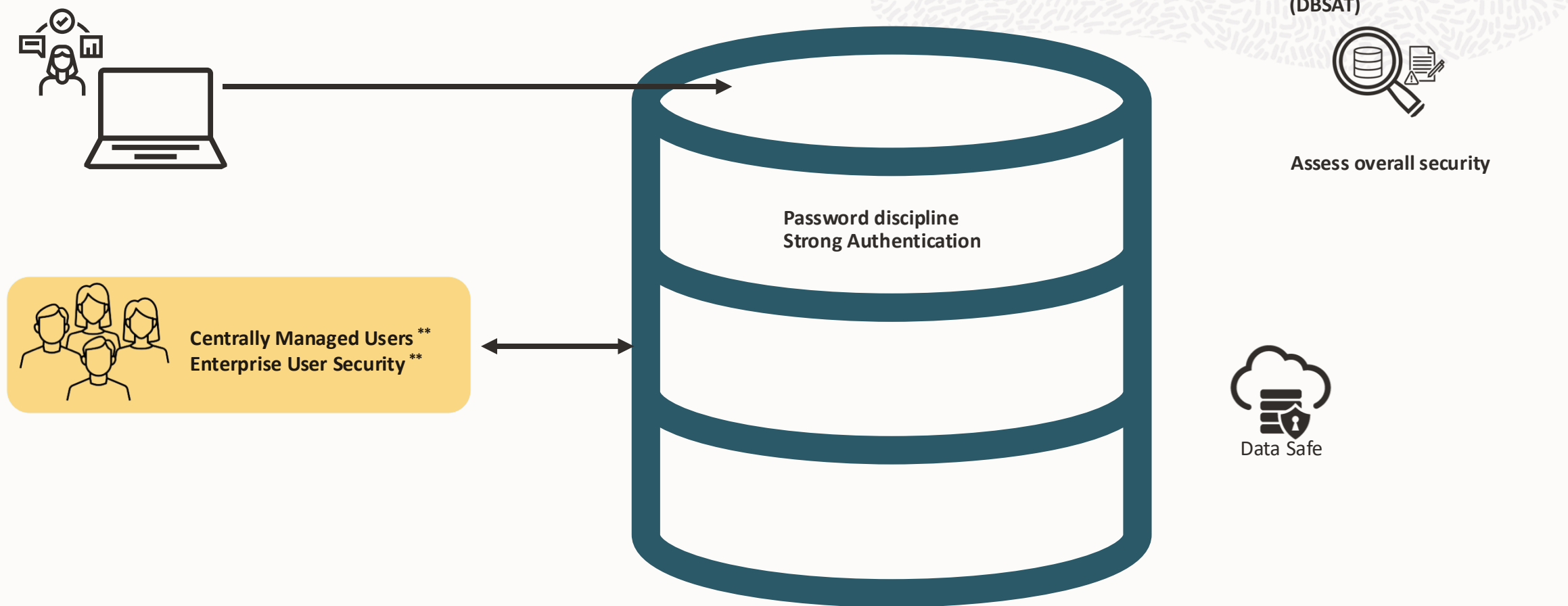
Baseline security



* Included with Database Cloud, additional cost on-premises
** Only available with Enterprise Edition



Baseline security

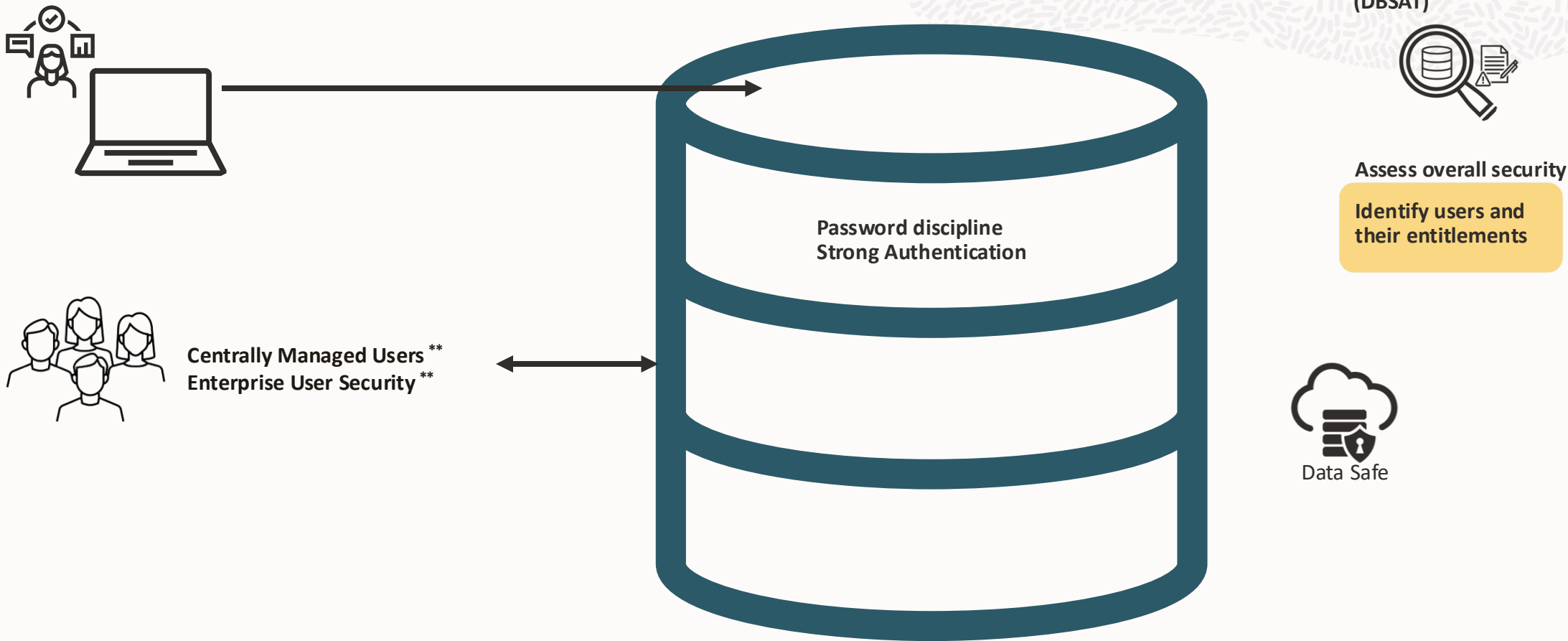


- * Included with Database Cloud, additional cost on-premises
- ** Only available with Enterprise Edition

Note: EUS is deprecated in 23ai



Baseline security



* Included with Database Cloud, additional cost on-premises
** Only available with Enterprise Edition



Schema privileges

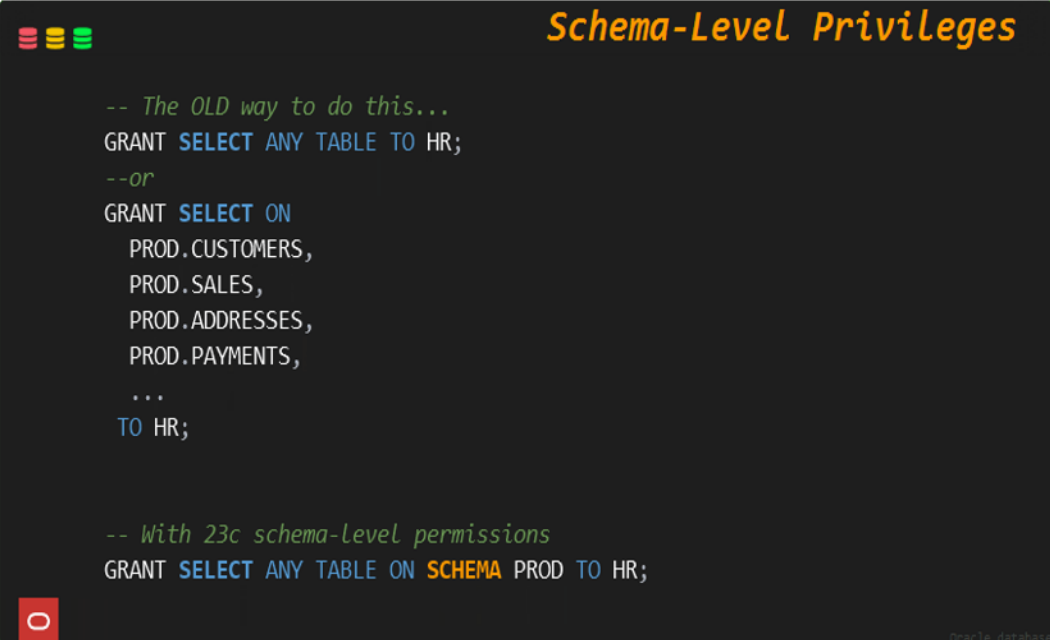
In many cases, a database account should have access to ALL objects in a schema, but schema objects change

- New tables or views added during upgrades or patching,
- Data analysis summaries and aggregation tables
- Ongoing development efforts

Schema-level privileges cover ALL the objects in a schema with a single grant request

More secure than granting * ANY privileges

Less maintenance intensive than individual object grants

A terminal window with a dark background and orange title bar. The title bar contains three colored squares (red, yellow, green) on the left and the text "Schema-Level Privileges" in orange on the right. The terminal shows two SQL grant statements. The first is commented as "-- The OLD way to do this..." and the second as "-- With 23c schema-level permissions". The first statement uses "GRANT SELECT ANY TABLE TO HR;" and the second uses "GRANT SELECT ANY TABLE ON SCHEMA PROD TO HR;". The word "SCHEMA" is highlighted in orange in the second statement. A small red square with a white 'O' logo is in the bottom left corner of the terminal window.

```
Schema-Level Privileges

-- The OLD way to do this...
GRANT SELECT ANY TABLE TO HR;

--or
GRANT SELECT ON
  PROD.CUSTOMERS,
  PROD.SALES,
  PROD.ADDRESSES,
  PROD.PAYMENTS,
  ...
TO HR;

-- With 23c schema-level permissions
GRANT SELECT ANY TABLE ON SCHEMA PROD TO HR;
```

Read-only users

Database users may be created as, or altered to READ ONLY status (default is READ WRITE)

Read-only users can not insert or update data, nor can they create database objects

Read-only account restrictions override privilege grants, including system or schema grants

```
ALTER USER joe READ ONLY;
```

```
SQL> INSERT INTO app_schema.data1  
VALUES ('MARY');
```

```
ERROR at line 1:  
ORA-28194: Can perform read  
operations only
```

```
SELECT username, read_only FROM  
dba_users WHERE username='JOE';
```

USERNAME	READ_ONLY
JOE	YES

Developer role

New out-of-the-box role for developers

DBA role used previously – with many more privileges than needed for development

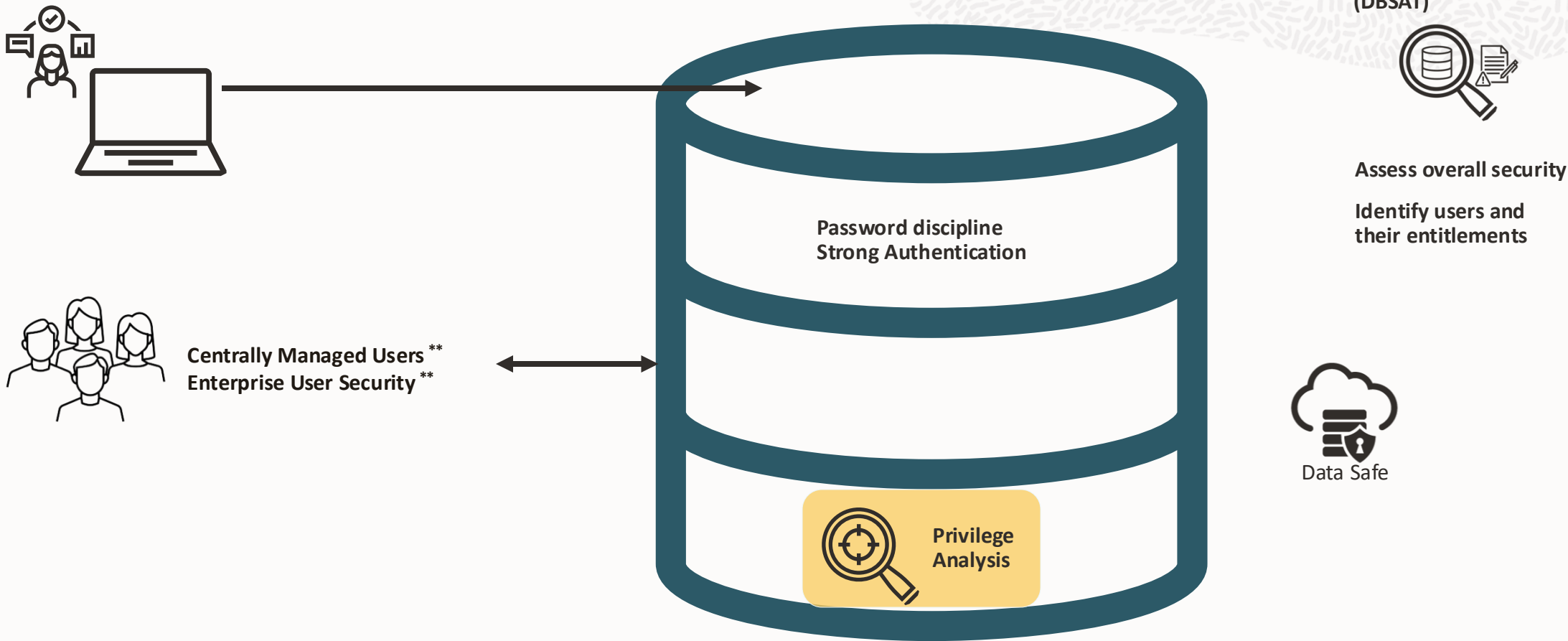
Oracle will update the privileges in the role

As with any out-of-the-box role, we recommend using it as a template instead of using it out of the box and following least privilege model

Use privilege analysis to dynamically identify used and unused privileges and roles



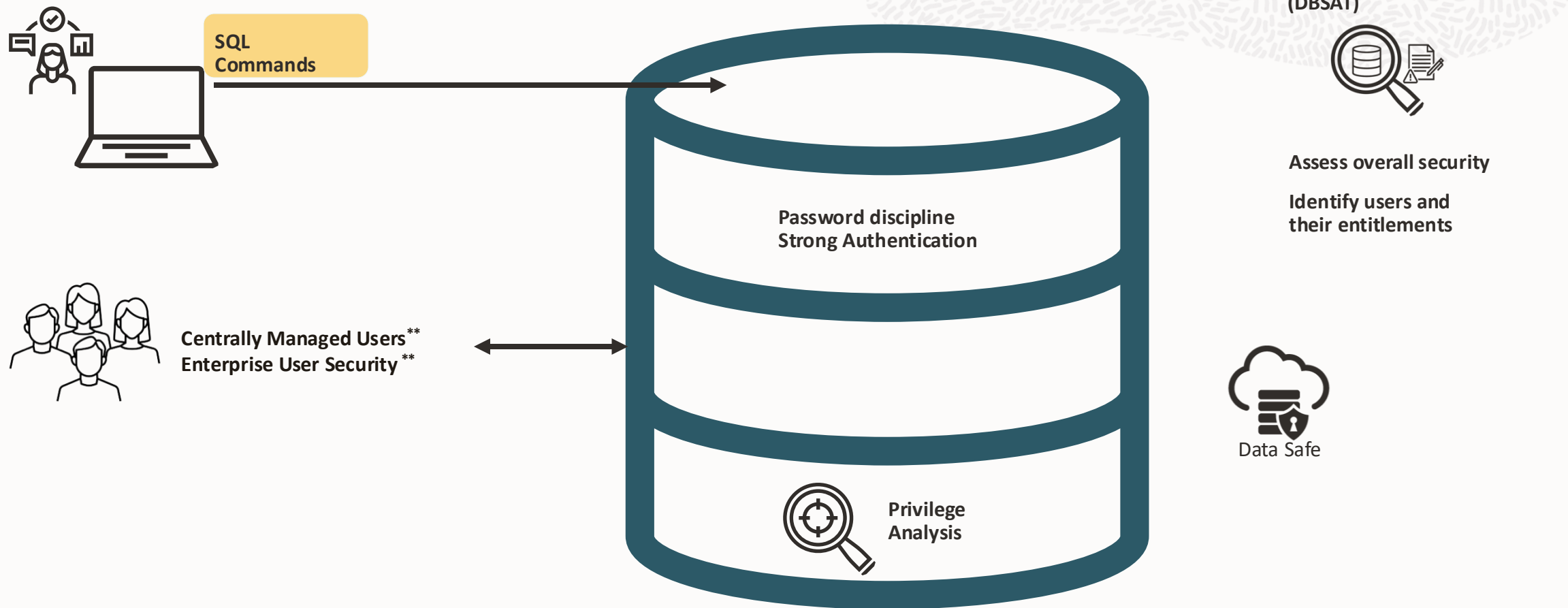
Baseline security



* Included with Database Cloud, additional cost on-premises
** Only available with Enterprise Edition



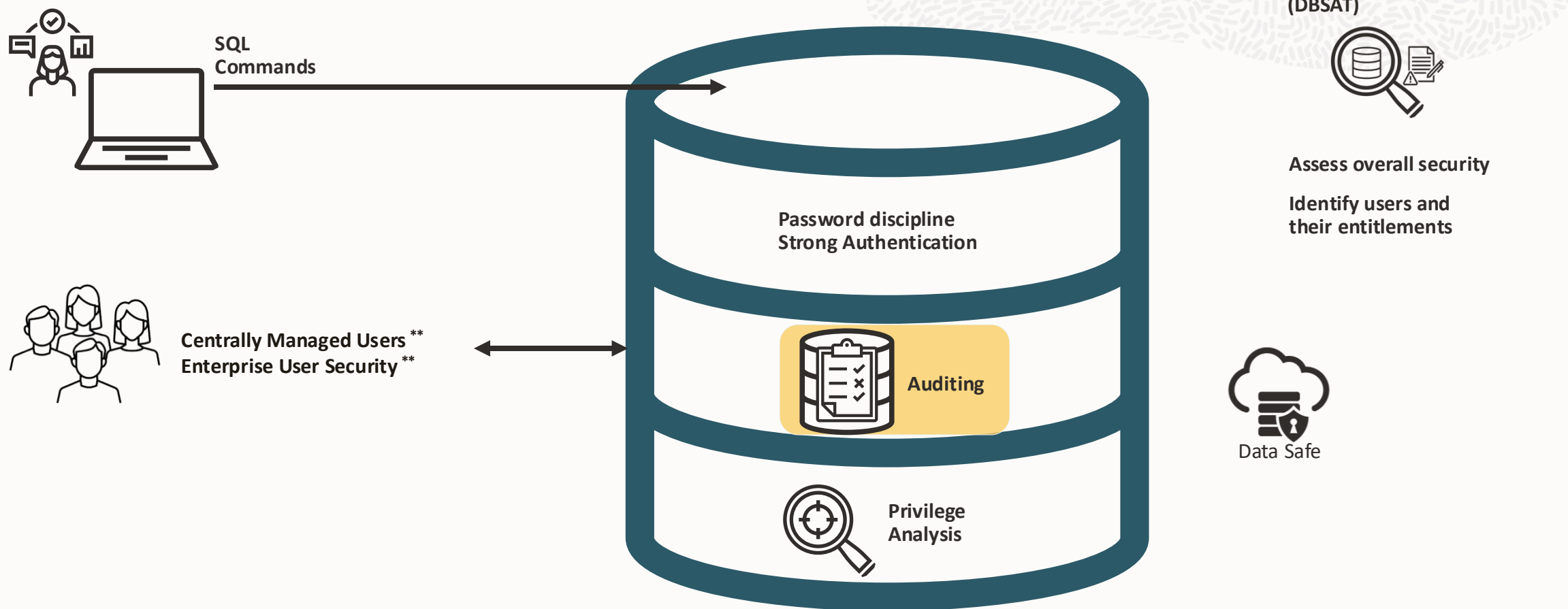
Baseline security



* Included with Database Cloud, additional cost on-premises
** Only available with Enterprise Edition



Baseline security



* Included with Database Cloud, additional cost on-premises

** Only available with Enterprise Edition

Changes to database audit

- Unified audit is the default auditing mechanism
 - All changes and new audit policies must use unified audit
- Traditional audit is desupported, but will continue to work in the new database
 - Deprecated with 19c
 - No changes can be made to existing policies
 - No new audit policies can be created

Best practices for unified
audit

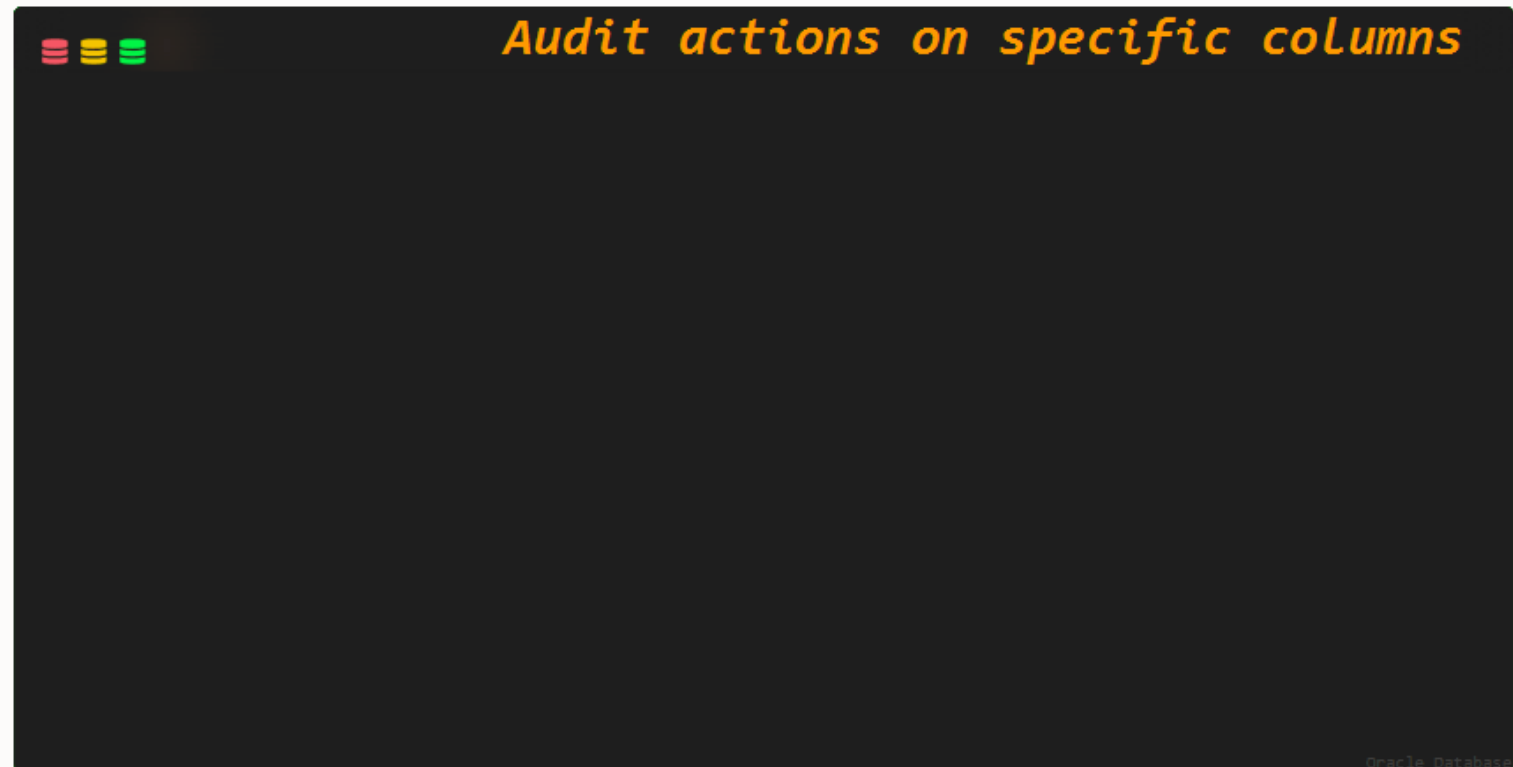


Column-specific audit policies

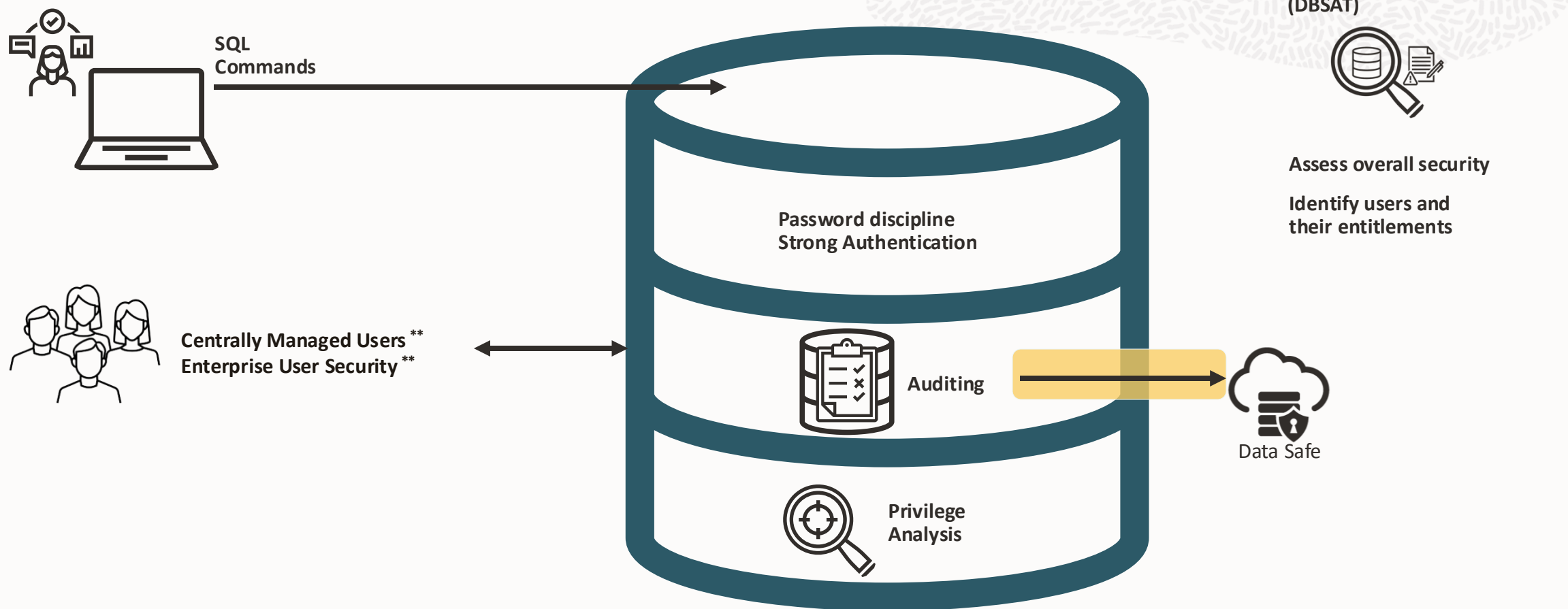
Both CREATE and ALTER AUDIT POLICY statements now let you specify a column

Examples:

- ```
CREATE AUDIT POLICY
employee_pii_access ACTIONS
SELECT(sal, ename) ON
scott.emp;
```
- ```
ALTER AUDIT POLICY  
employee_pii_access ADD  
ACTIONS UPDATE(sal) ON  
scott.emp;
```
- ```
CREATE AUDIT POLICY
employee_pii_access1 ACTIONS
INDEX(empid) on scott.emp;
```

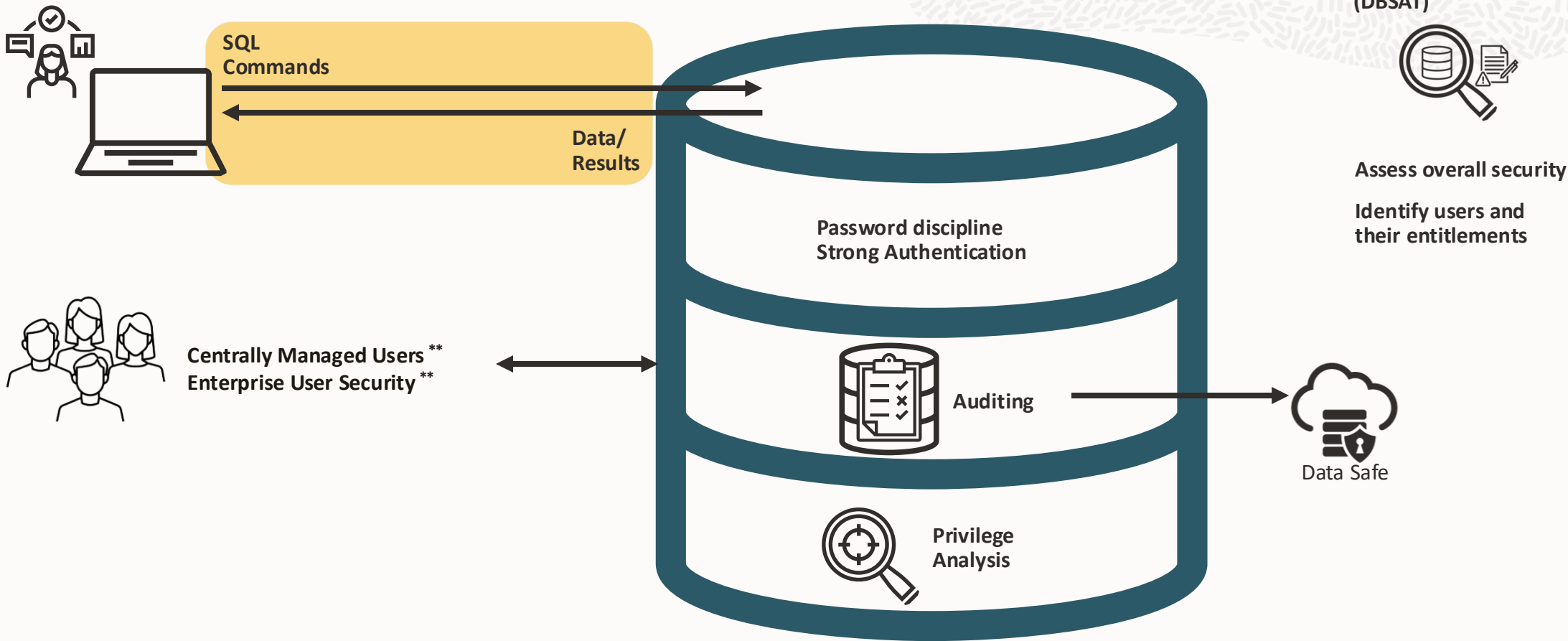


## Baseline security



- \* Included with Database Cloud, additional cost on-premises
- \*\* Only available with Enterprise Edition

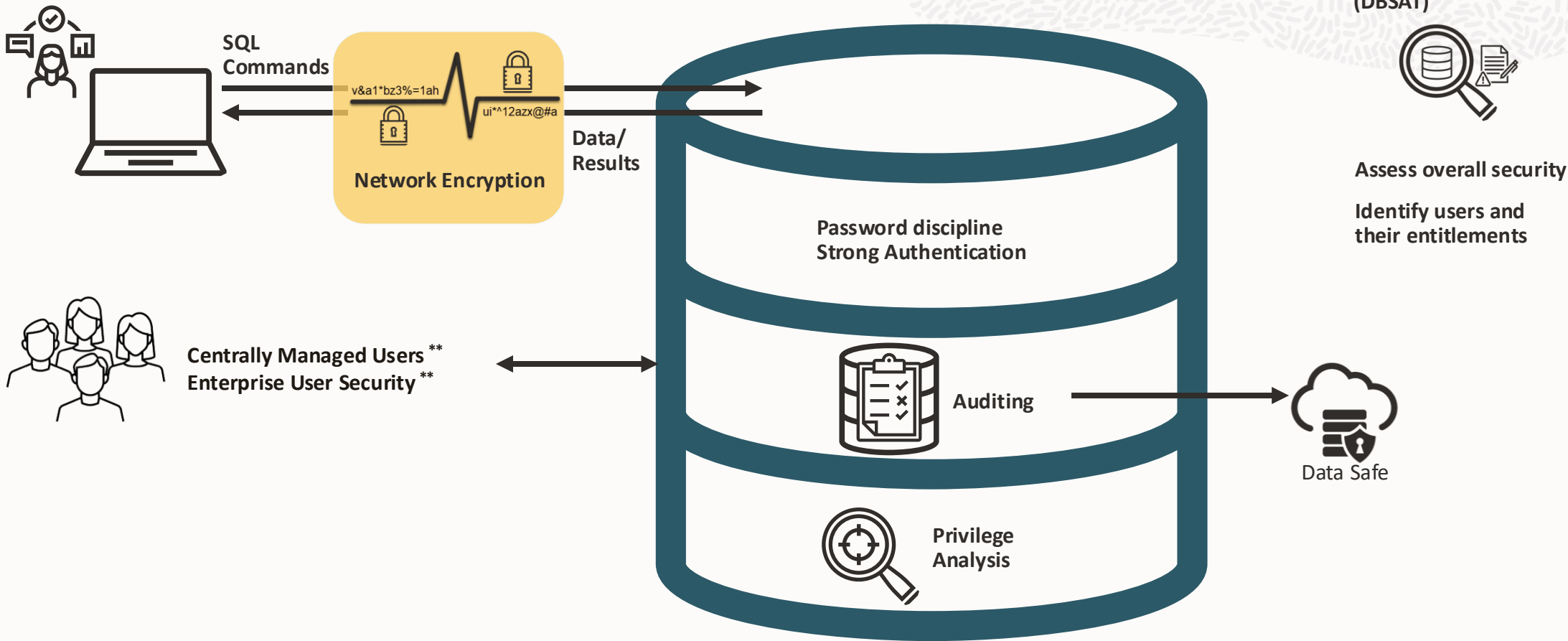
# Baseline security



\* Included with Database Cloud, additional cost on-premises  
\*\* Only available with Enterprise Edition



# Baseline security



\* Included with Database Cloud, additional cost on-premises  
\*\* Only available with Enterprise Edition



# Transport Layer Security (TLS) 1.3

Transport Layer Security (TLS) secures data in transit between the database server and clients or other services

- Inbound to the database from clients
- Outbound from the database to services (AD, OID, OCI IAM, Azure AD...)

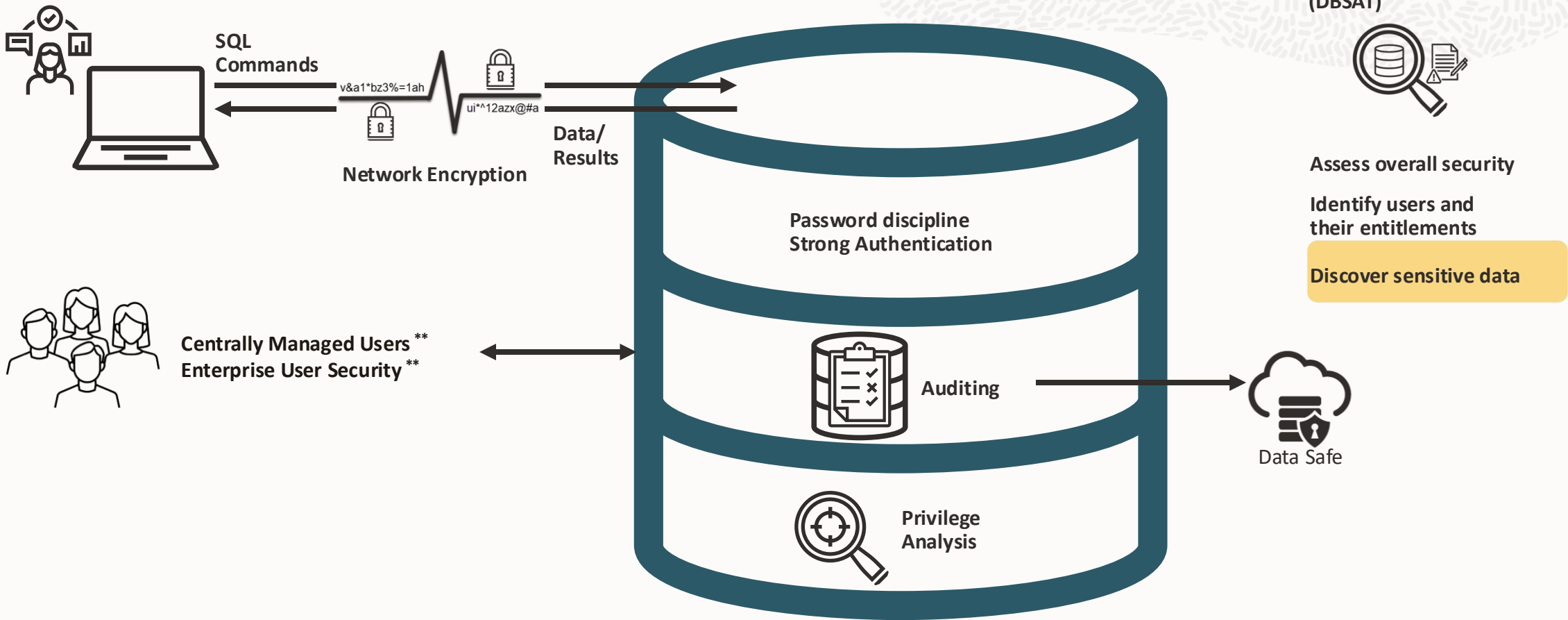
TLS 1.3 improves performance over TLS 1.2 for new connections

- 22% faster for initial connection
- 3% higher throughput

TLS 1.1, 1.0 support has been removed



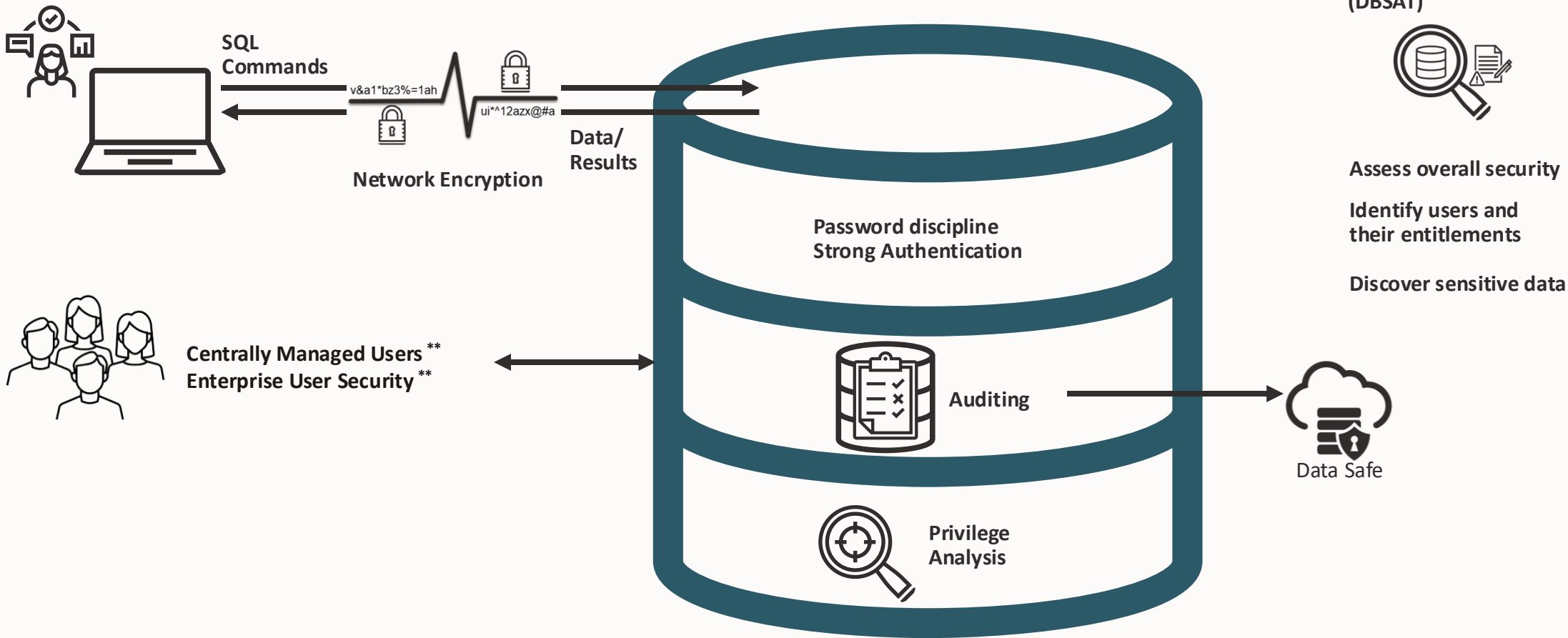
# Baseline security



\* Included with Database Cloud, additional cost on-premises  
\*\* Only available with Enterprise Edition



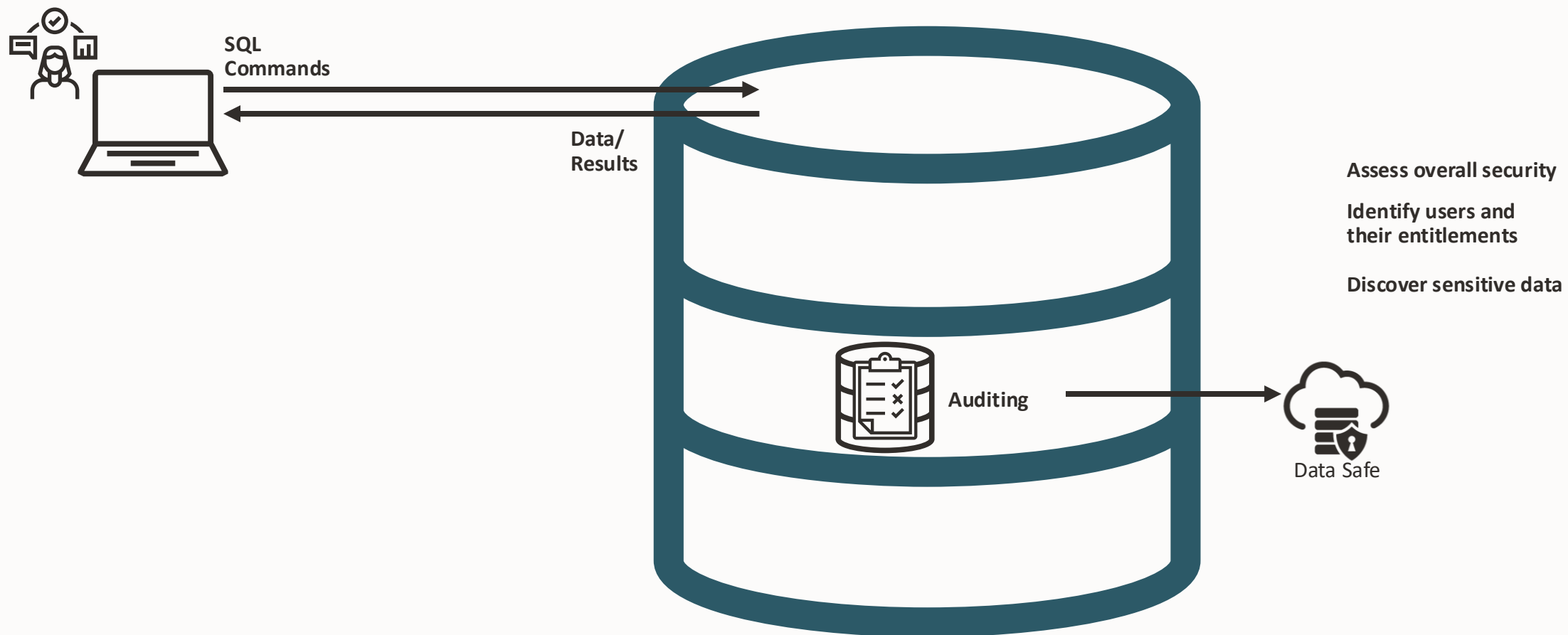
# Baseline security



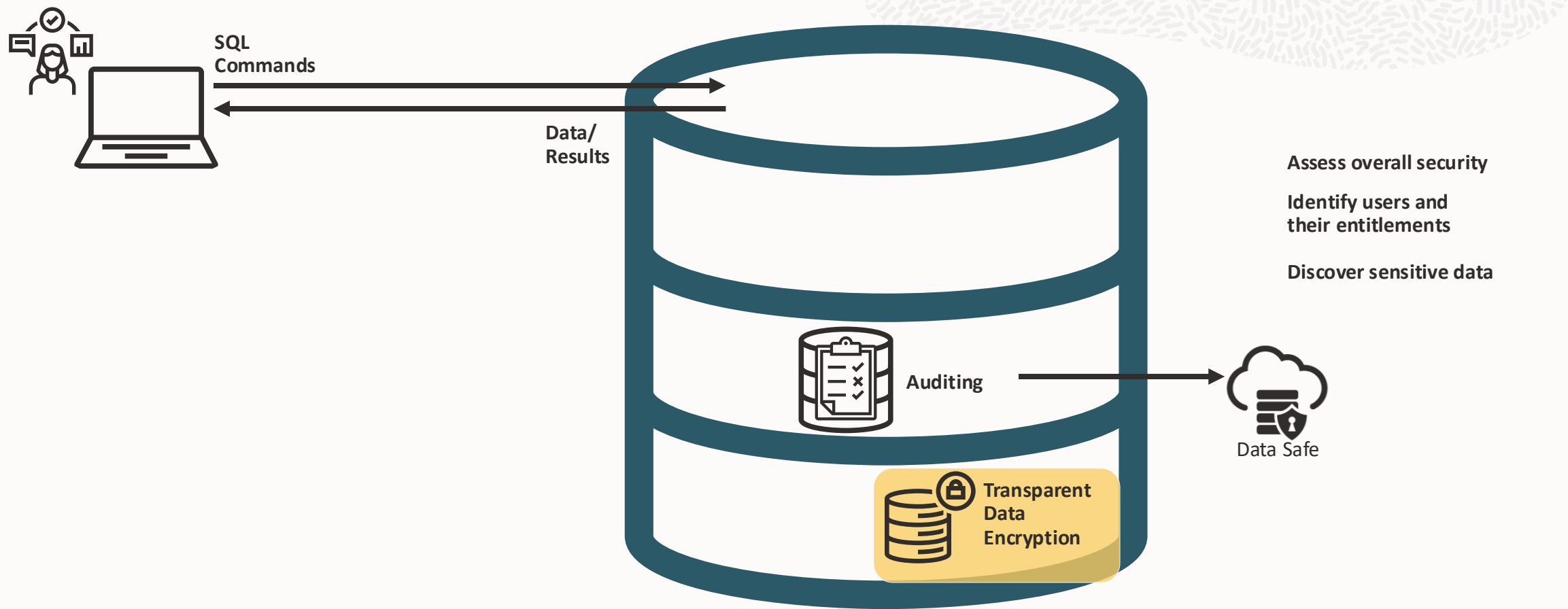
\* Included with Database Cloud, additional cost on-premises  
\*\* Only available with Enterprise Edition



## Beyond the baseline



## Beyond the baseline



# Encrypting data at rest

## Transparent Data Encryption

- New default for tablespace encryption is AES256
- Tablespace encryption now defaults to XEX-based mode with ciphertext stealing (XTS)
- Column encryption (seldom the right choice) now defaults to Galois/Counter mode (GCM)
- GOST and SEED algorithms are desupported



## Recovery Manager (RMAN)

- Integrity checks are now SHA512 (instead of SHA256)

## Wallets

- Improved local auto-login wallets now more tightly bound to the host

# Simpler FIPS configuration

Federal Information Processing Standard (FIPS) 140 sets a standard for cryptography for US government

New `FIPS_140` parameter enforces the use of FIPS 140 standard cryptography in:

- Transparent Data Encryption (TDE)
- DBMS\_CRYPTO PL/SQL package
- Transport Layer Security (TLS)
- Network native encryption (NNE)

Legacy configuration parameters will continue to work



# On-demand encryption using DBMS\_CRYPTO

Adds support for:

- SM2 sign and verify algorithm
- SM3 hashing algorithm
- SM4 cryptographic algorithm

Other new signature and verification algorithms:

- SIGN\_SHA224\_ECDSA
- SIGN\_SHA256\_ECDSA
- SIGN\_SHA384\_ECDSA
- SIGN\_SHA512\_ECDSA
- SIGN\_ECDSA

New chain modes GCM, CCM, and XTS

Say good by to...

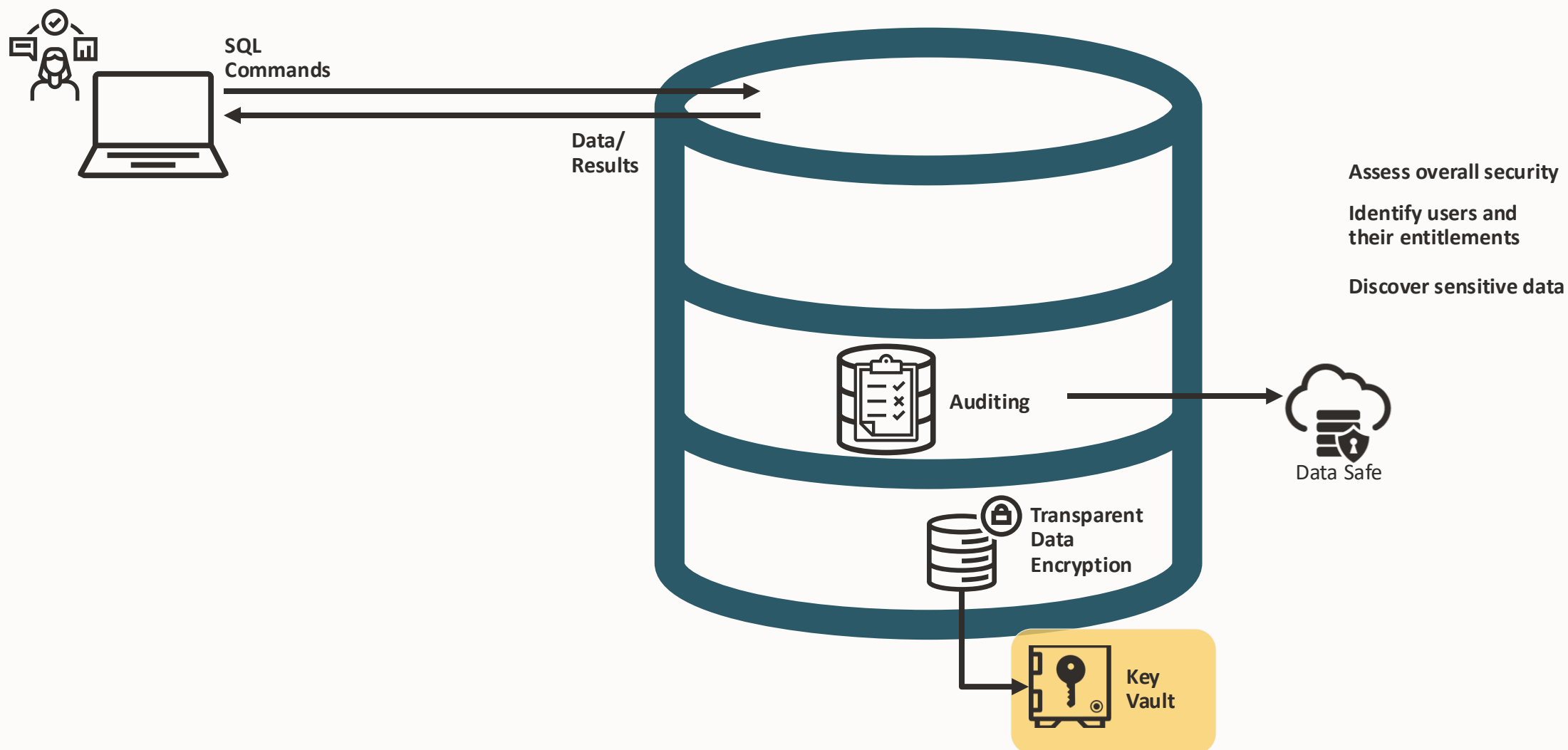
MD4 hashing algorithm is desupported

MD5 hashing algorithm is deprecated

SHA-1 hashing algorithm is deprecated



## Beyond the baseline



# Key Vault 21.9

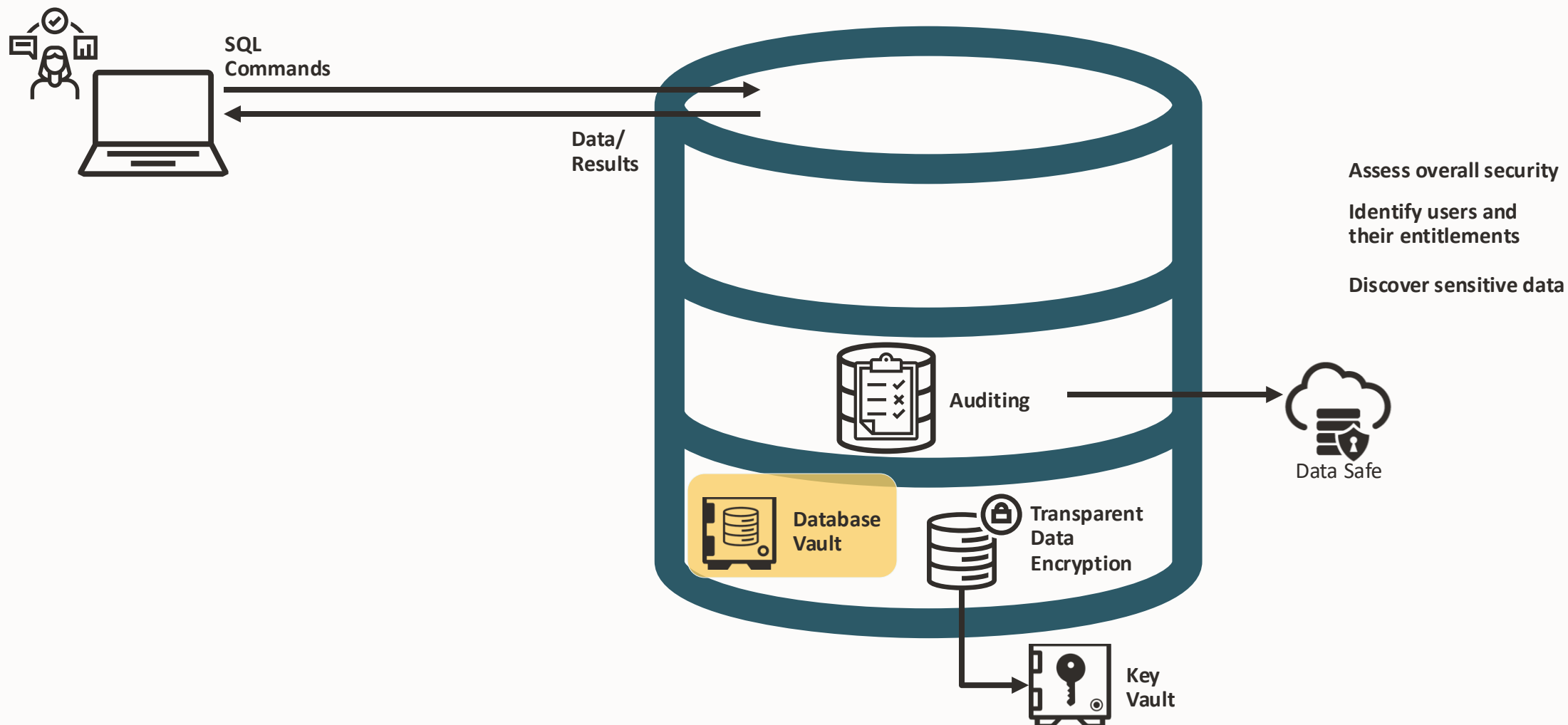
Added support for MongoDB, MySQL, Oracle Database ExaCC, ExaCS, Autonomous C@C, DB@Azure

Secrets Management

SSH Key governance/management



## Beyond the baseline



# Database Vault

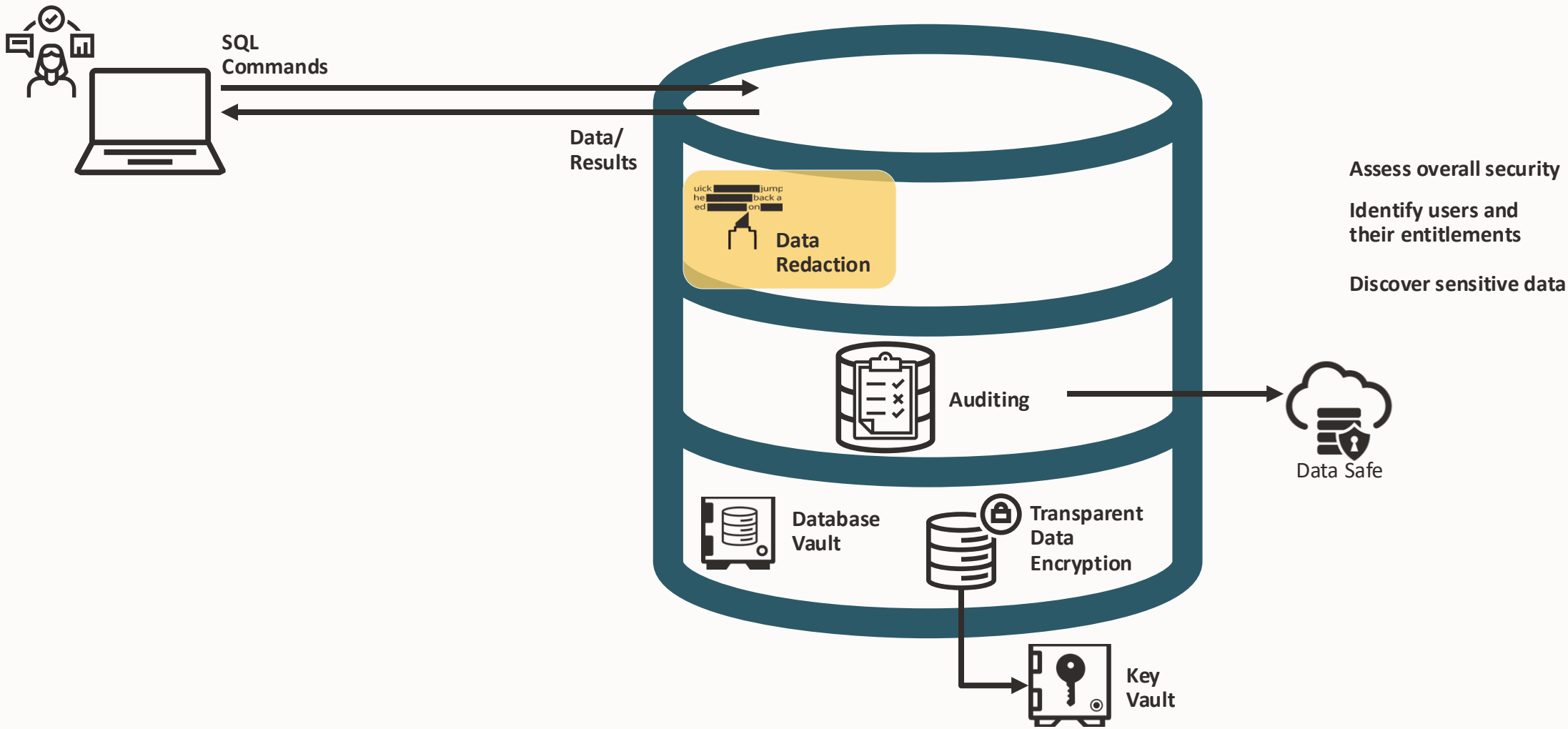
Protect audit roles using Database Vault authorizations

- `DVSYS.DBMS_MACADM.authorize_audit_admin`
- `DVSYS.DBMS_MACADM.authorize_audit_viewer`

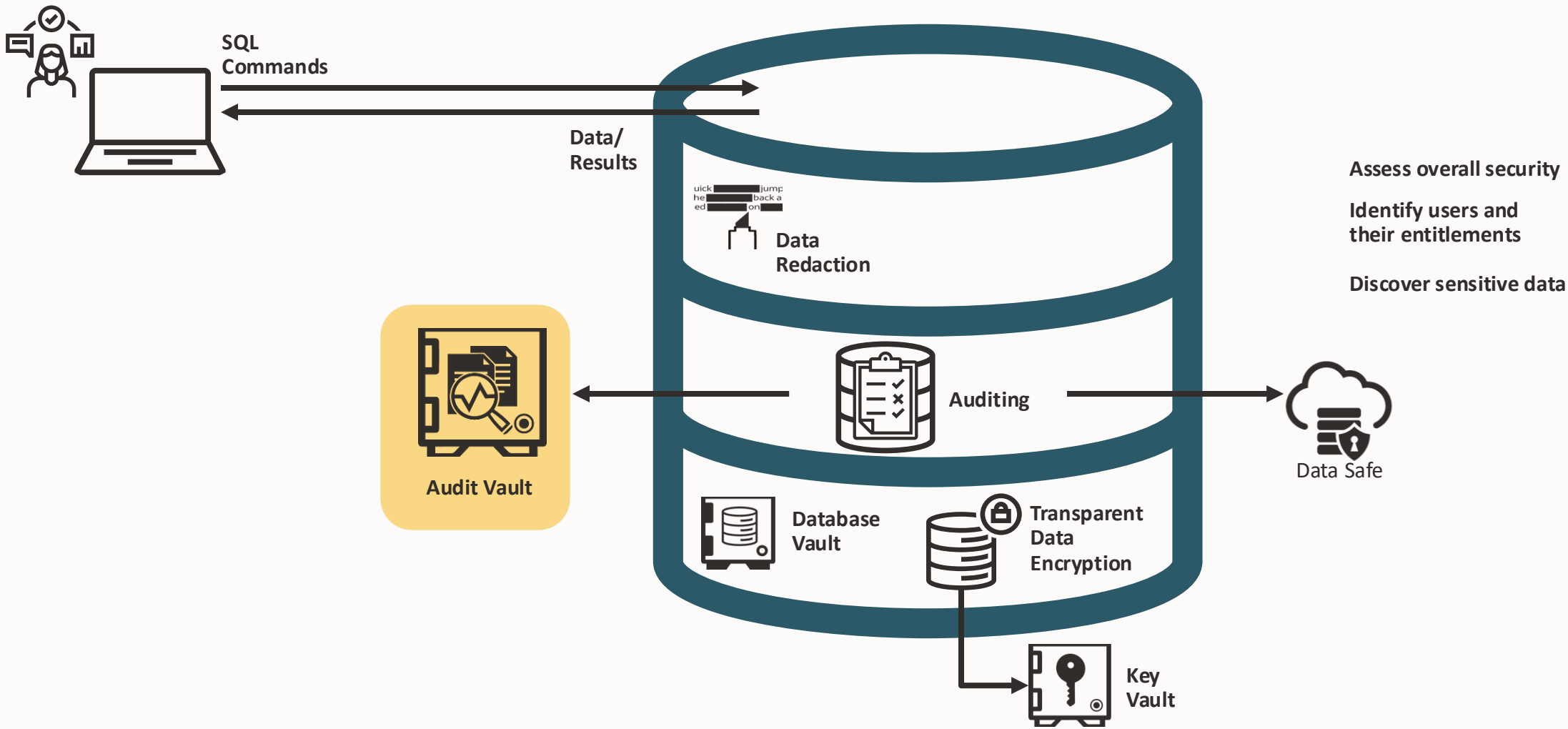
Plus, one other BIG new feature (wait for it)



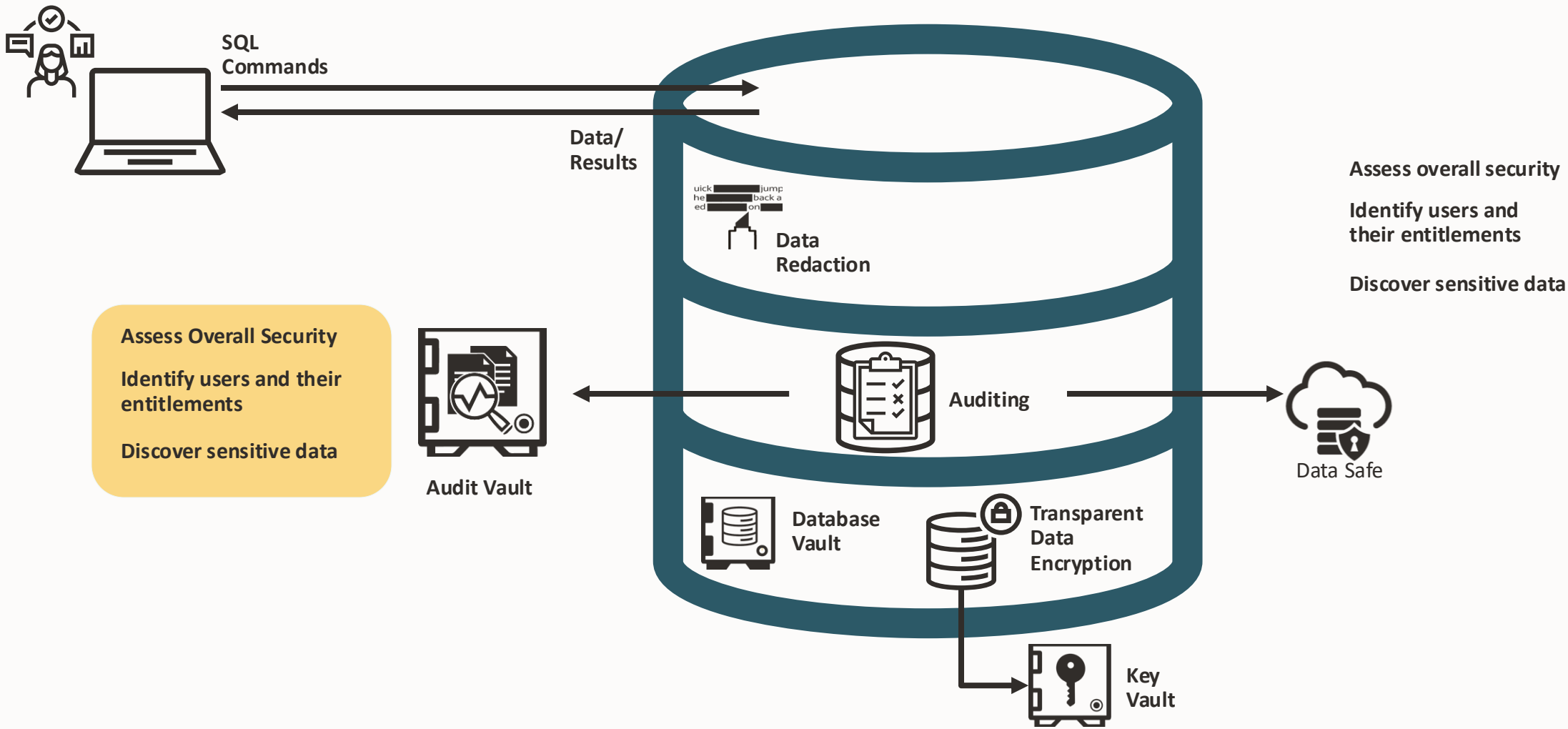
# Beyond the baseline



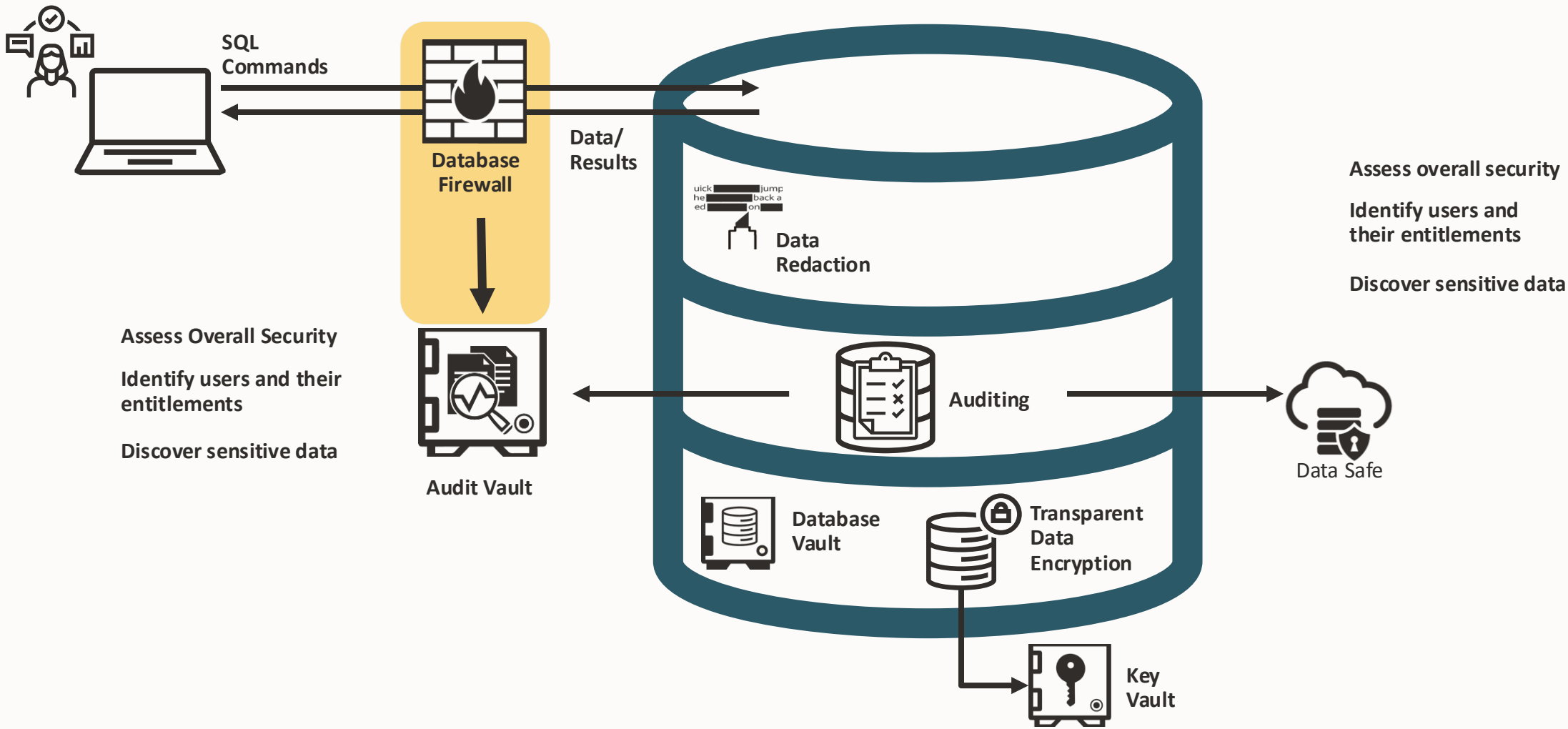
# Beyond the baseline



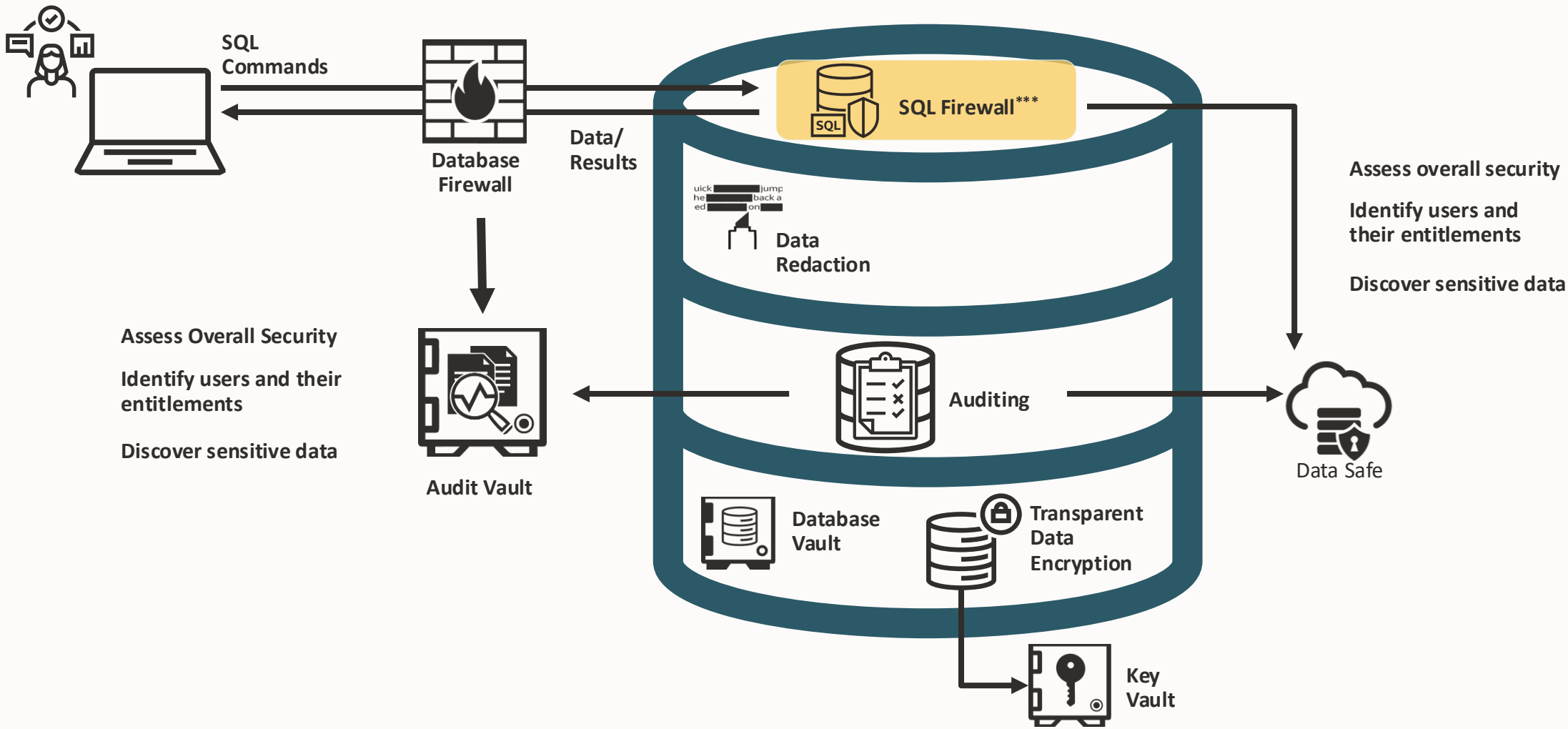
# Beyond the baseline



# Beyond the baseline



# Beyond the baseline



\*\*\* Only available in Oracle Database 23ai

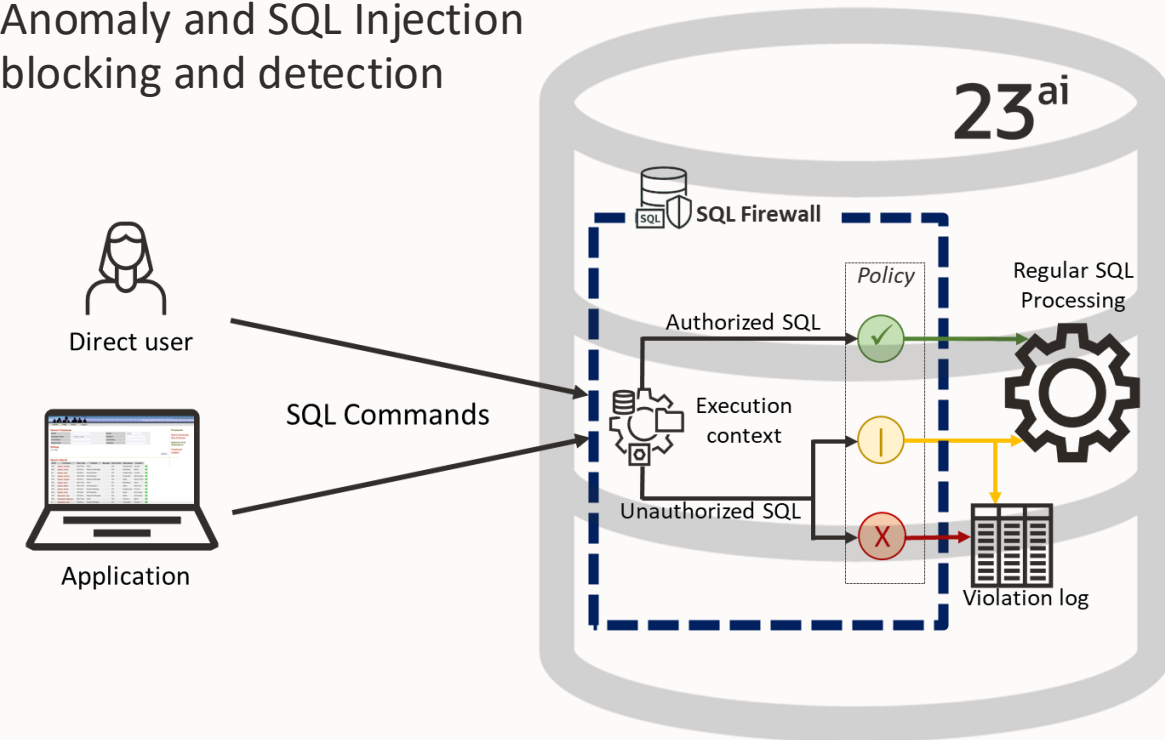


# Oracle SQL Firewall

- “Learns” how clients and applications work with the database
- Supports both permissive (logging only) and enforcing (logging and blocking) modes.
- Anomalies or SQL Injection attempts are handled before any other action is taken
- SQL Firewall is embedded in the database and can not be bypassed
- It has near-zero performance overhead with full visibility into the top-level SQL, stored procedures, and related database objects
- Management options
  - Data Safe (GUI, RESTful APIs)
  - PL/SQL `dbms_sql_firewall`



## Anomaly and SQL Injection blocking and detection



# Oracle Data Safe

Included with all database cloud services, including cloud@customer, DB@Azure

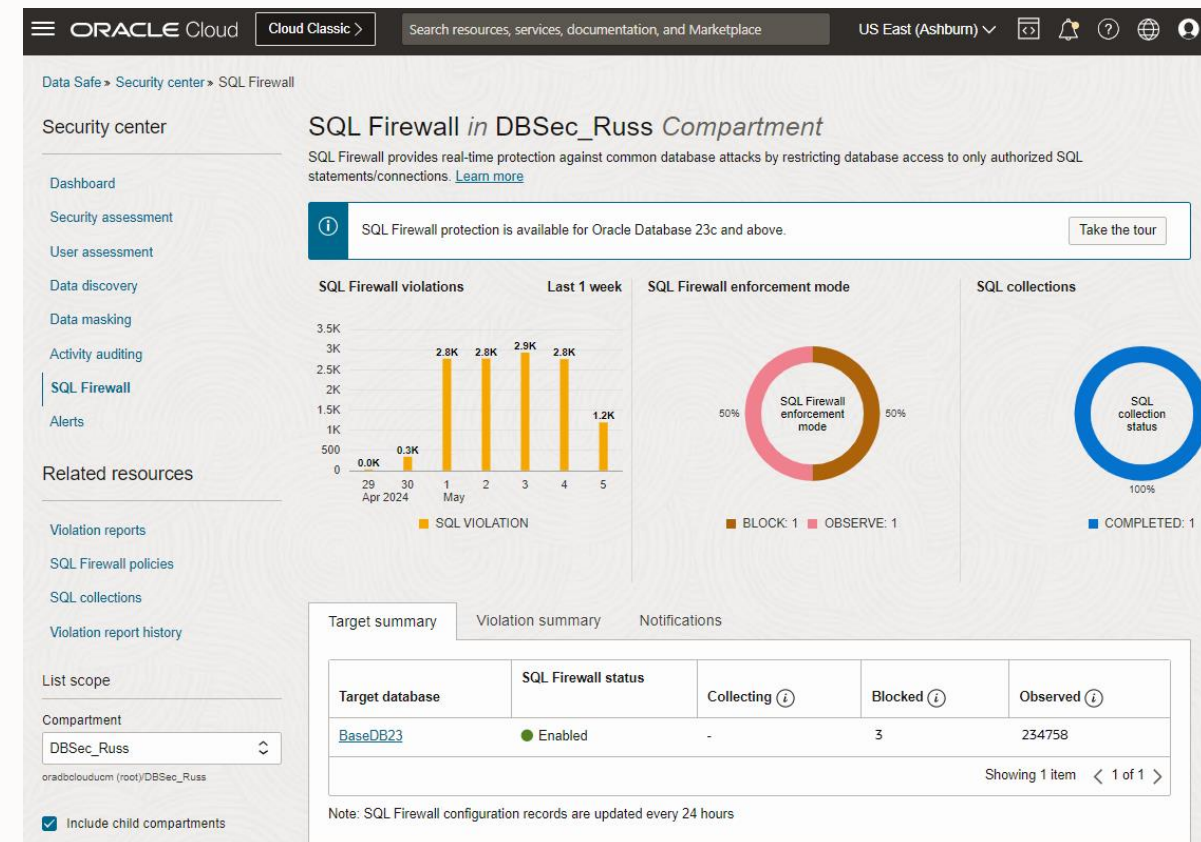
Data Safe offers:

- Complete management of SQL Firewall
- Violation log collection
- Violation analysis and reporting

Additional features

- Security assessment and drift detection
- User and profile assessment and drift detection
- Audit data collection for analysis, alerting, and reporting
- Sensitive data discover and masking

Available for on-premises



## But wait...

Didn't we already HAVE a firewall that protected against SQL Injection

### Audit Vault and Database Firewall

Heterogeneous – works with Oracle, MySQL, Microsoft SQL Server, IBM Db2, Sybase

Outside of the database, on a different server.  
Requires network changes to prevent firewall bypass

Makes decisions based only on the SQL, no visibility into database objects

Supports before/after value collection

Supports returned row count

### SQL Firewall

Oracle Database 23ai and above only

Built into the database, can not be bypassed. No network changes necessary

Full visibility into database objects, can not be fooled by dynamic SQL, encoded SQL, synonyms, etc.



## What about licensing?

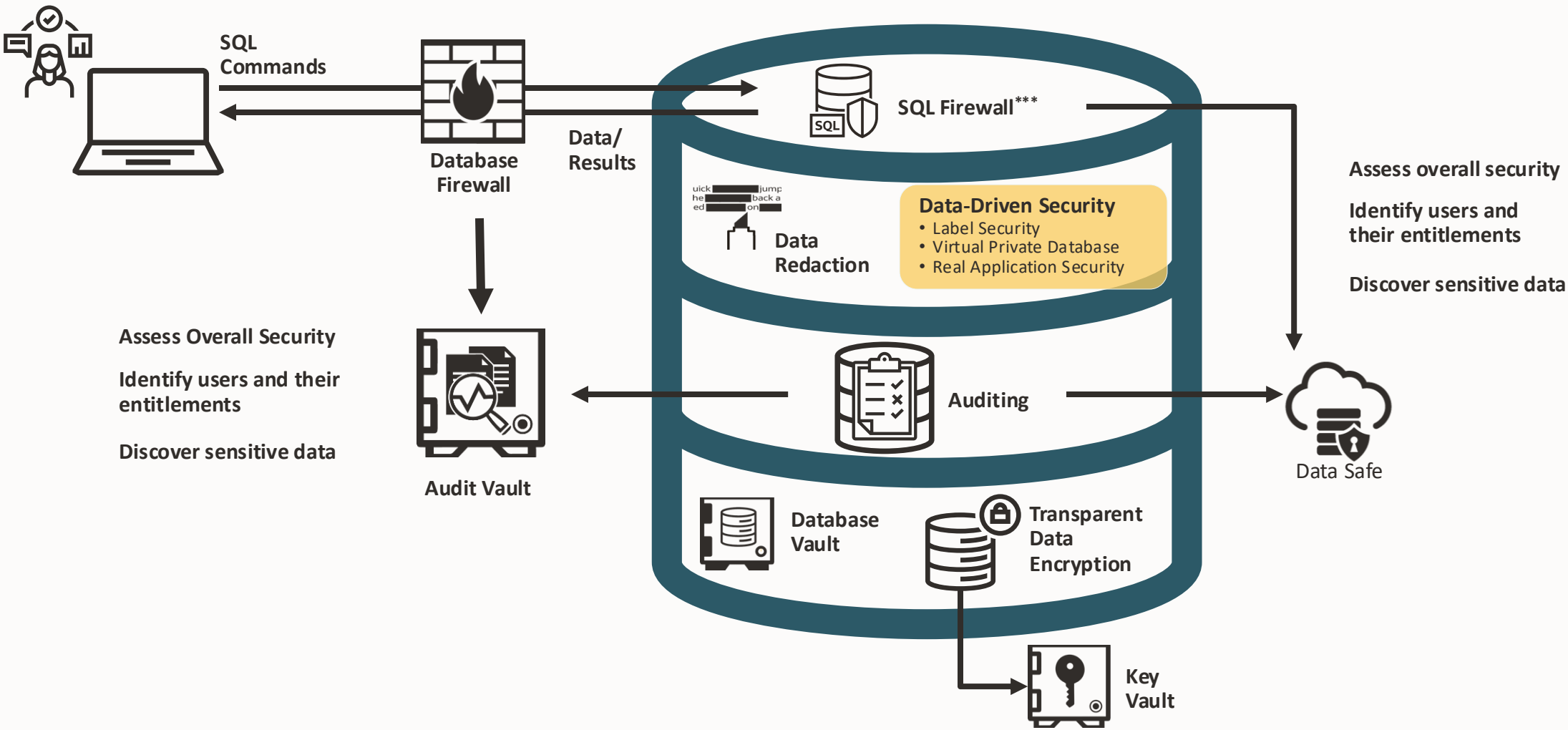
SQL Firewall is included as part of Oracle Database Vault



SQL Firewall is included as part of Oracle Audit Vault and Database Firewall



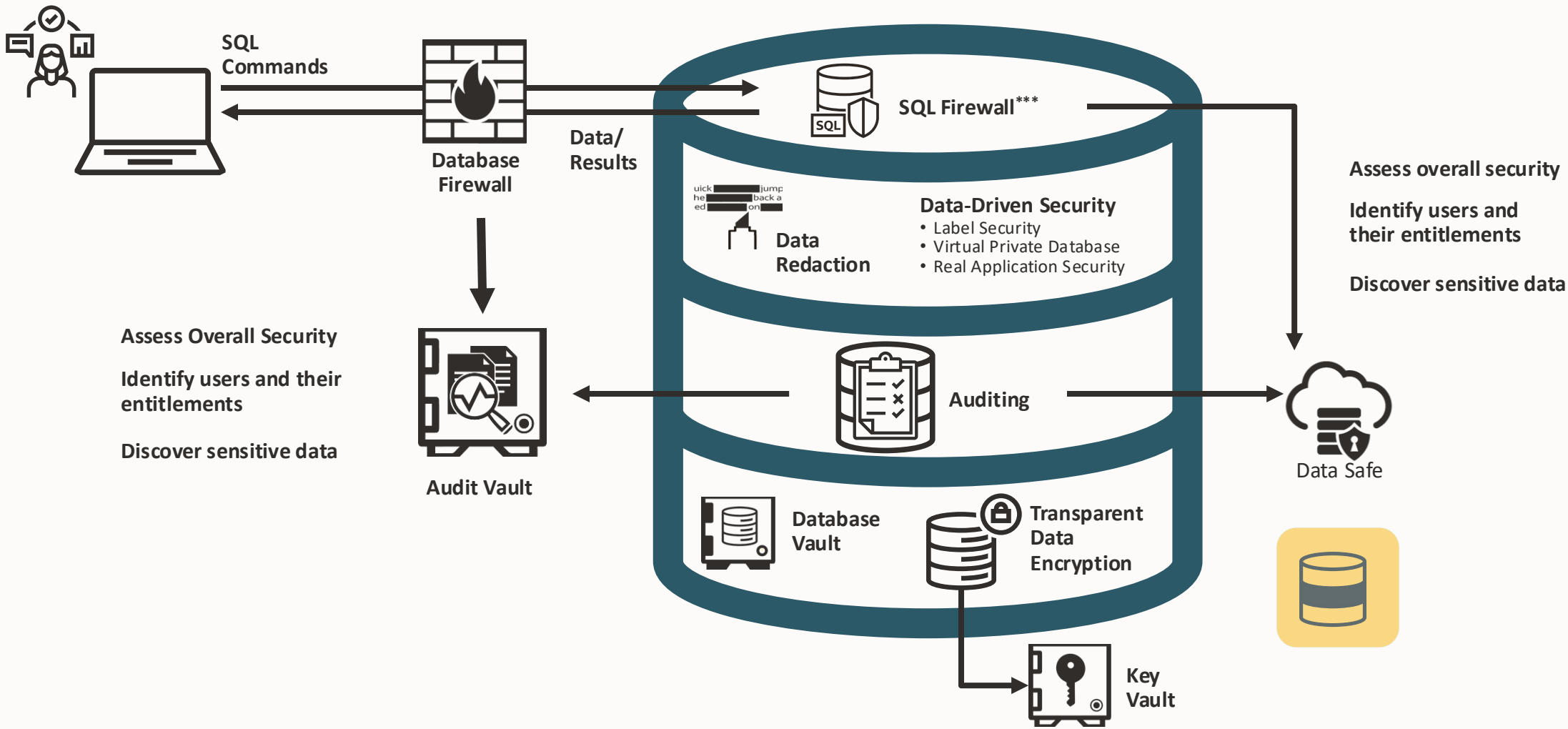
# Beyond the baseline



\*\*\* Only available in Oracle Database 23ai



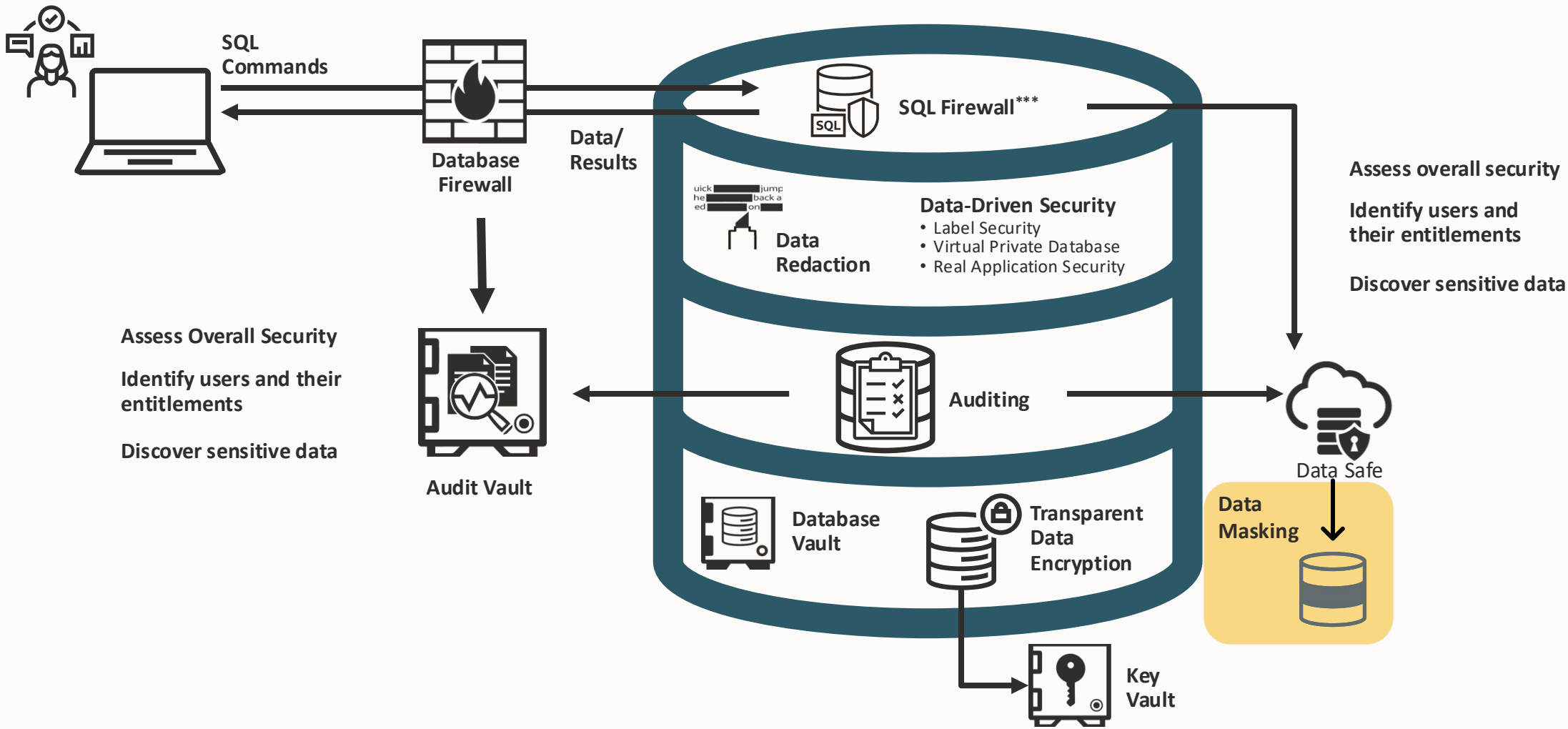
# Beyond the baseline



\*\*\* Only available in Oracle Database 23ai



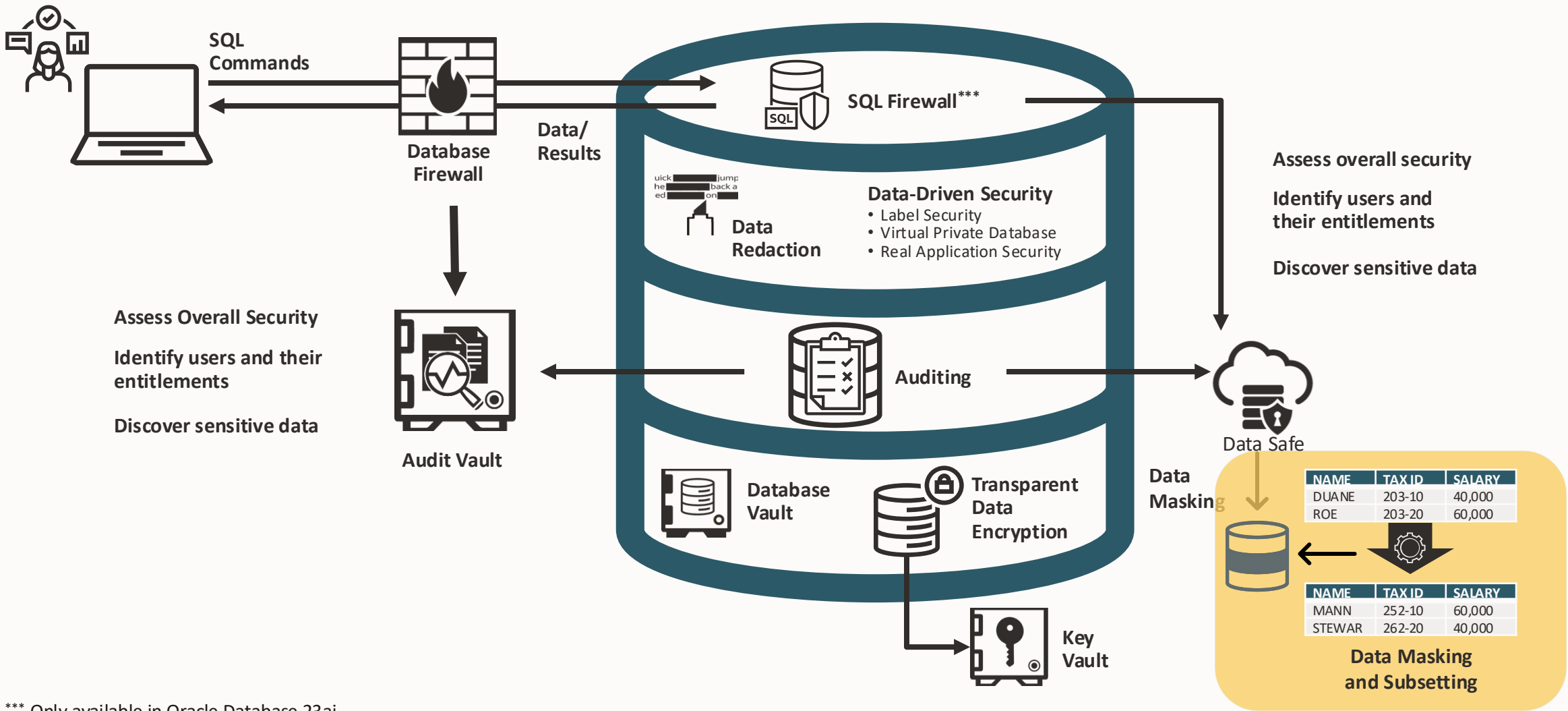
# Beyond the baseline



\*\*\* Only available in Oracle Database 23ai



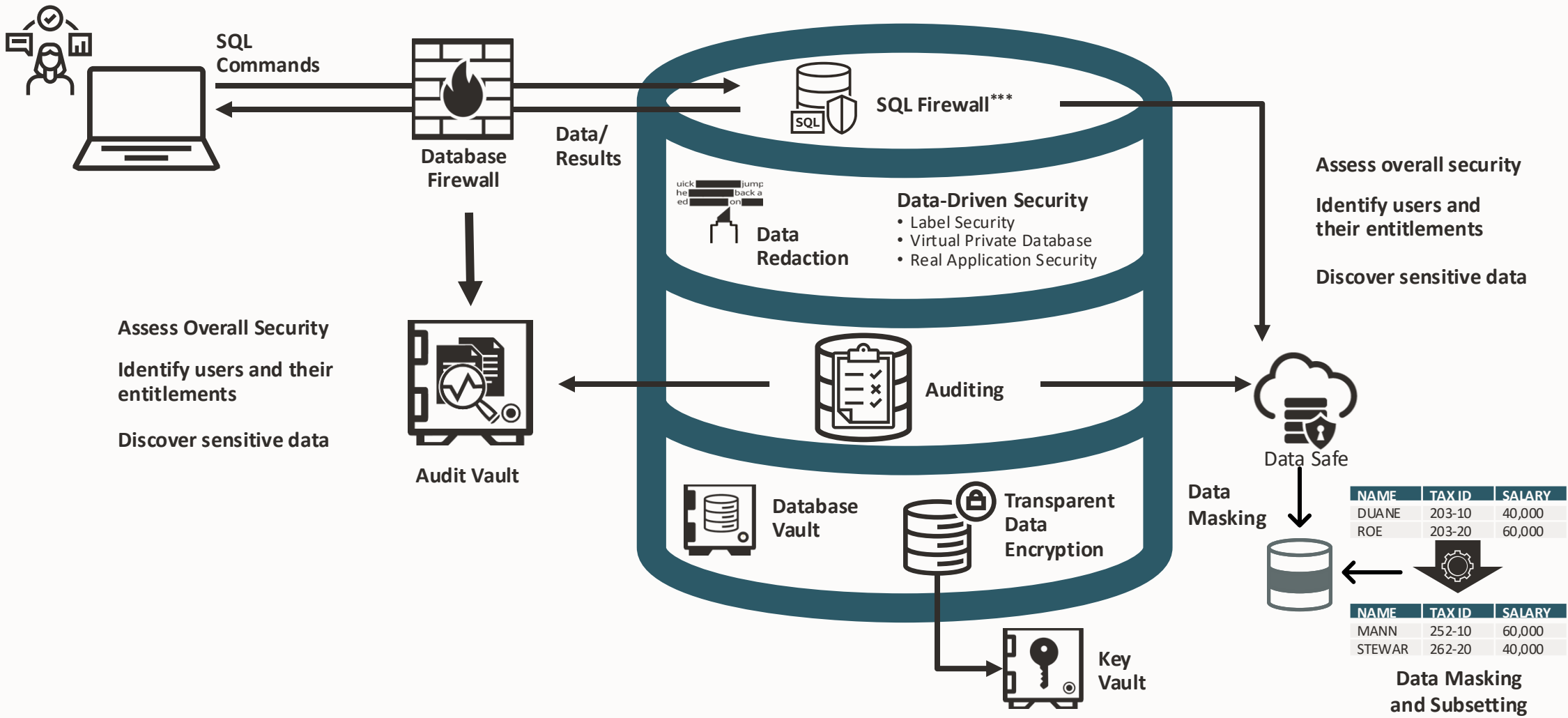
# Beyond the baseline



\*\*\* Only available in Oracle Database 23ai



# Maximum Security Architecture



\*\*\* Only available in Oracle Database 23ai



# How can I learn more?

## Want to learn more?

Free hands-on labs that help you learn how to use the different security features and options



[bit.ly/golivelabsdbsec](https://bit.ly/golivelabsdbsec)

## Database Security office hours – second Wednesday of each month



[bit.ly/asktomdbsec](http://bit.ly/asktomdbsec)

# Securing the Oracle Database – a technical primer (fifth edition)



[oracle.com/securingthedatabase](https://oracle.com/securingthedatabase)



# Questions?



# Thank you!

---

**Russ Lowenthal**

[russ.lowenthal@oracle.com](mailto:russ.lowenthal@oracle.com)

[@RussLowenthal](#)



# ORACLE