ORACLE

# Oracle Autonomous Database Security Features

March 2020

**Sinan Petrus Toma**

Passionate about Database
& Cloud Technologies

database-heartbeat.com
Linkedin
Twitter @SinanPetrus

# 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, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

# Agenda

- Encryption (Data, Backup, Connections)
- Network Access Control
- System & Data Protection
- Sensitive Data Discovery & Masking
- Auditing

# Data | Your Most Valuable Asset

# Examples of where data was not very well protected

Mar 2020: Unsecured Database Exposed 8 Million UK Shoppers Records

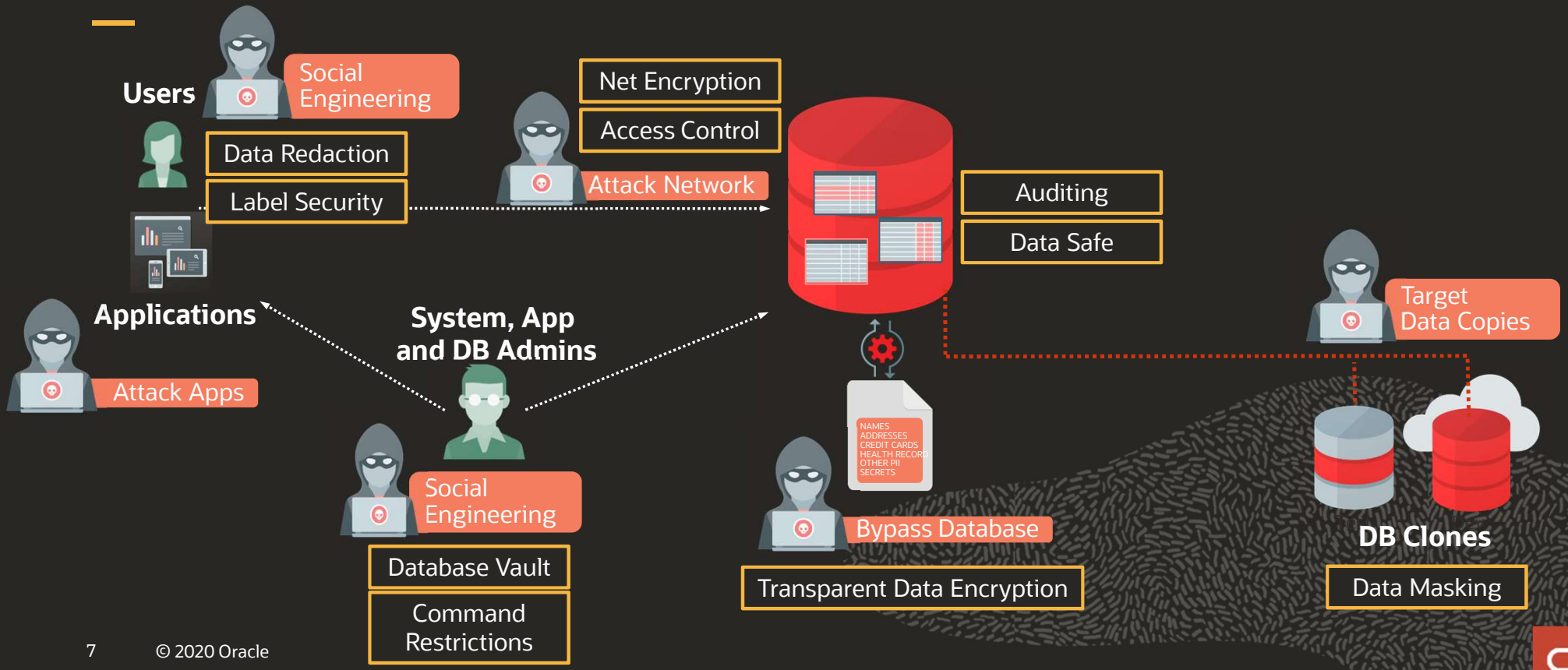
Jul 2019: records of more than 5 million Bulgarians got stolen by hackers from the country's tax revenue office

Jul 2019: hacker gained access to 100 million Capital One credit card applications and accounts

Nov 2018: Marriott said the Starwood guest reservation database was breached, potentially exposing information on about 500 million guests

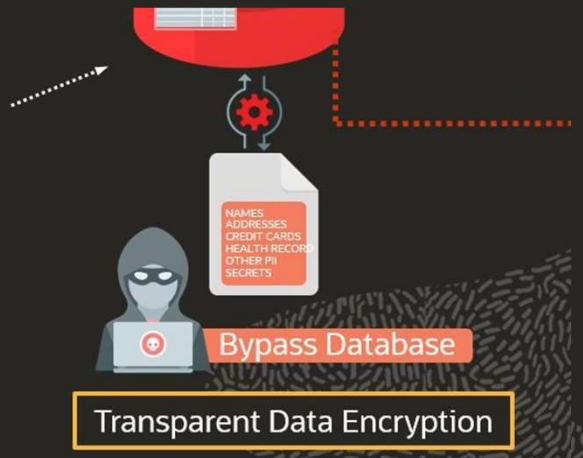
https://latesthackingnews.com/2020/03/16/unsecured-database-exposed-8-million-uk-shoppers-records/
https://edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/index.html
https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html
https://www.cnbc.com/2018/11/30/marriott-says-its-starwood-database-was-breached-onapproximately-500-million-guests-.html

# Database in focus



# Agenda

- Encryption (Data, Backup, Connections)
- Network Access Control
- System & Data Protection
- Sensitive Data Discovery & Masking
- Auditing



# Encryption | Transparent Data Encryption (TDE)

- Encryption of Application Data on media
- Enabled by default
- Encryption keys are managed automatically

```
SELECT * FROM v$encrypted_tablespaces;
```

| | TS# | ENCRYPTIONALG | ENCRYPTEDTS | ENCRYPTEDKEY | MASTERKEYID | BLOCKS_ENCRYPTED | BLOCKS_DECRYPTED | KEY_VERSION | STATUS | CON_ID |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 4 | AES128 | YES | B00E5C527150F... | 774C2999B80... | 1551 | 1460 | 0 | NORMAL | 96 |
| 2 | 5 | AES128 | YES | B17AC4144AC66... | 774C2999B80... | 458 | 441 | 0 | NORMAL | 96 |

# Encryption | Transparent Data Encryption (TDE)

```
[oracle@hostfraee datafile]$ strings o1_mf_system_h6doz8nv_.dbf | grep -i Firstname
getFirstNamespaceNode
m_firstName
getFirstName
%Firstname5 Lastname5 Account 87654321
%Firstname4 Lastname4 Account 87654321
%Firstname3 Lastname3 Account 87654321
%Firstname2 Lastname2 Account 87654321
%Firstname1 Lastname1 Account 87654321
```

Without TDE

```
[oracle@hostfraee datafile]$ strings o1_mf_users_h6dp31c7_.dbf | grep -i Firstname
[oracle@hostfraee datafile]$ strings o1_mf_users_h6dp31c7_.dbf | more
8iJk#0
6K":
u*C=
i6bY
_[sr
Fc}j
gl||
a:9;
E2xS
```

With TDE

In the event that the storage media or data file is stolen, it is not possible to read the data

# Encryption | Backups

All Backups are encrypted

```
SQL> SELECT count(*) FROM v$backup_set_details WHERE encrypted = 'YES';

  COUNT(*)
----------
      1985

SQL> SELECT count(*) FROM v$backup_set_details WHERE encrypted = 'NO';

  COUNT(*)
----------
         0
```

# Encryption | SQL*Net Connections

All connections **MUST** use TCP/IP + SSL (TCPS)

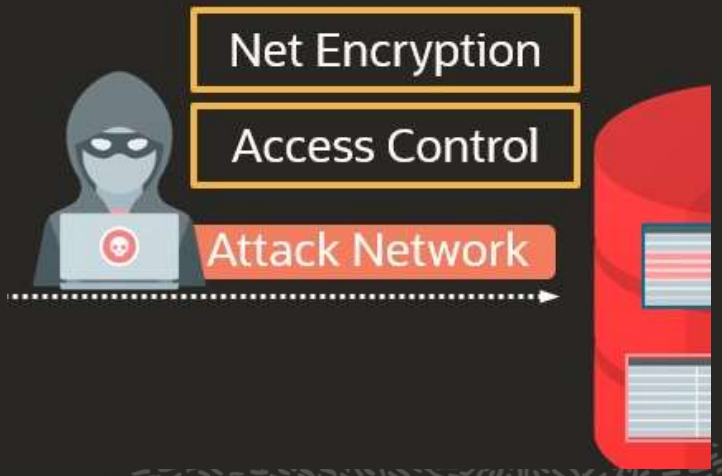
Customer's responsibility
- Store wallet files in a secure location
- Share wallet files only with authorized users

```
WALLET_LOCATION = (SOURCE = (METHOD = file)
SSL_SERVER_DN_MATCH=ON
SSL_CLIENT_AUTHENTICATION=FALSE
```

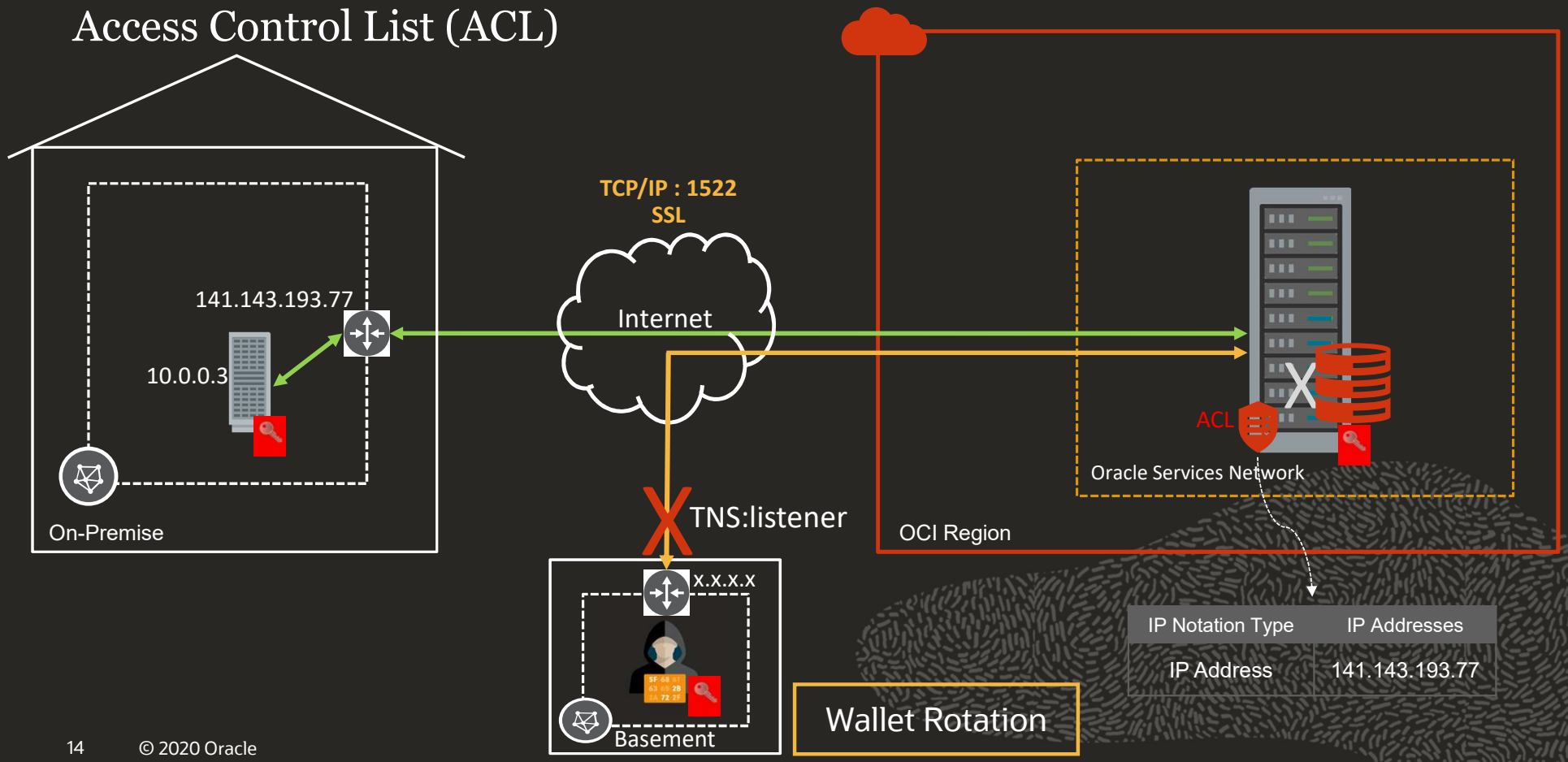
```
SQL*Plus: Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All ric

ERROR:
ORA-28860: Fatal SSL error
```

# Agenda

- Encryption (Data, Backup, Connections)
- Network Access Control
- System & Data Protection
- Sensitive Data Discovery & Masking
- Auditing



# Access Control List (ACL)



# Access Control List (ACL)

```
[opc@admin-interactivetech ~]$ ./connATPshared.sh

SQL*Plus: Release 18.0.0.0.0 - Production on Tue Mar 10 01:52:37 2020
Version 18.5.0.0.0

Copyright (c) 1982, 2018, Oracle.  All rights reserved.

Last Successful login time: Tue Mar 10 2020 01:34:37 +00:00

Connected to:
Oracle Database 18c Enterprise Edition Release 18.0.0.0.0 - Production
Version 18.4.0.0.0

SQL>
```

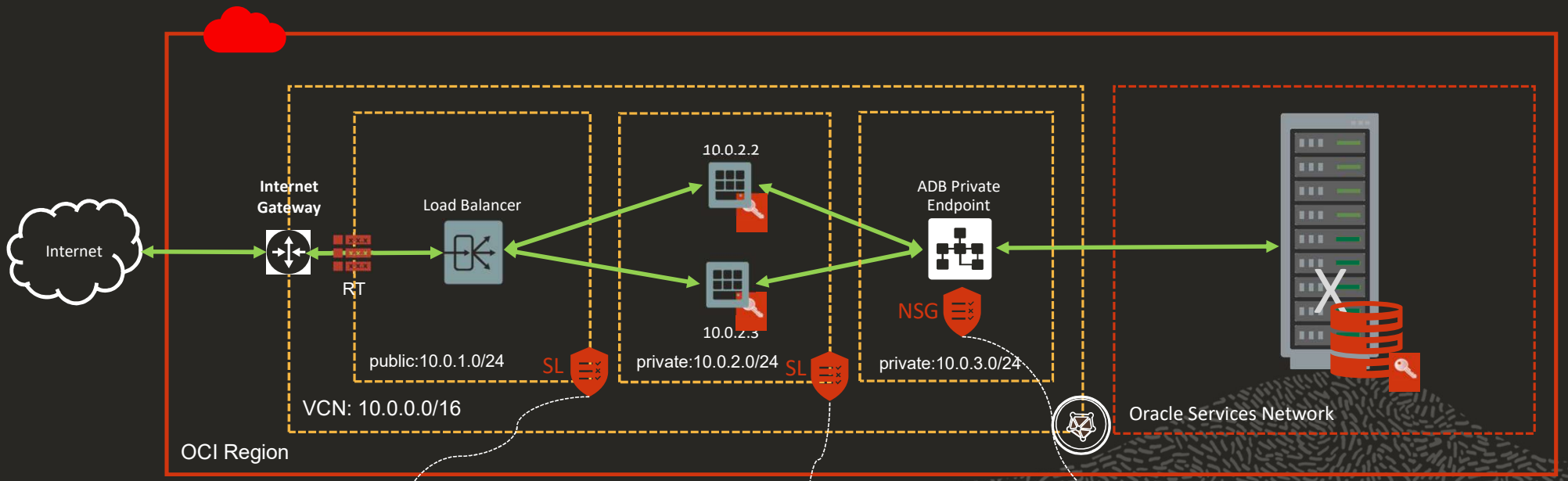
Without ACL

```
[opc@admin-interactivetech ~]$ ./connATPshared.sh

SQL*Plus: Release 18.0.0.0.0 - Production on Tue Mar 10 01:57:29 2020
Version 18.5.0.0.0

Copyright (c) 1982, 2018, Oracle.  All rights reserved.

ERROR:
ORA-12506: TNS:listener rejected connection based on service ACL filtering
```

With ACL

# Private Endpoints & Network Security Groups

https://www.linkedin.com/pulse/implement-private-endpoint-your-autonomous-database-sinan-petrus-toma/



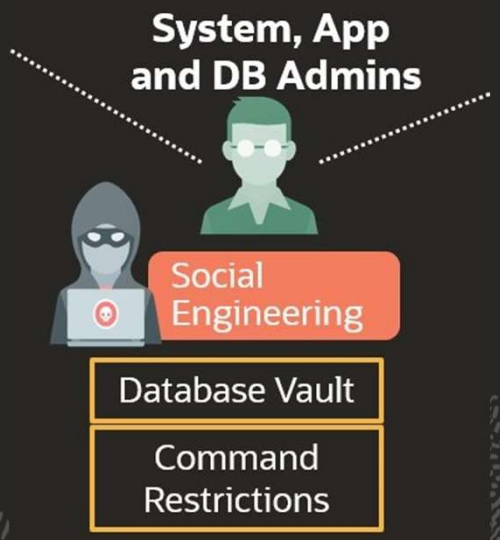

| Rule | Stateless | Source |
|---|---|---|
| Ingress | No | 0.0.0.0/0 |
| Egress | No | 10.0.2.0/24 |

| Rule | Stateless | Source |
|---|---|---|
| Ingress | No | 10.0.1.0/24 |
| Egress | No | 10.0.3.0/24 |

| Rule | Stateless | Source |
|---|---|---|
| Ingress | No | 10.0.2.0/24 |

# Agenda

- Encryption (Data, Backup, Connections)
- Network Access Control
- System & Data Protection
- Sensitive Data Discovery & Masking
- Auditing



# Database Vault

- Stolen privileged user credentials are one of the most common attack vectors used by hackers
- Database Vault restricts access to application data by privileged users
  - Prevent malicious or accidental changes that disrupt operations by privileged users
  - Reduce the risk of insider and outside threats
  - Address compliance with data privacy laws and standards such as the EU General Data Protection Regulation (GDPR)

```
SQL> SELECT * FROM DBA_DV_STATUS;

NAME                 STATUS
-------------------- ------------
DV_CONFIGURE_STATUS  TRUE
DV_ENABLE_STATUS     TRUE
```

# Database Vault

```
SELECT firstname, lastname, email, position, location FROM hr_data.demo_hr_employees;
```

| FIRSTNAME | LASTNAME | EMAIL | POSITION | LOCATION |
|---|---|---|---|---|
| jeroen | krabe | jeroen.krabe@mycompany.com | DBA | New York |
| Frank | Stok | Frank.Stok@mycompany.com | Project Director | Santa Clara |
| Martijn | Krabe | Martijn.Krabe@mycompany.com | DBA | Santa Clara |
| John | Forde | John.Forde@mycompany.com | DBA | New York |
| joop | kaptijn | joop.kaptijn@mycompany.com | DBA | New York |

Without DB Vault

```
SELECT firstname, lastname, email, position, location FROM hr_data.demo_hr_employees;
```

```
ORA-01031: insufficient privileges
01031. 00000 - "insufficient privileges"
*Cause:    An attempt was made to perform a database operation without
           the necessary privileges.
*Action:   Ask your database administrator or designated security
           administrator to grant you the necessary privileges
```

With DB Vault

# High Privileges Restrictions

No OS/root logon or SYSDBA privileges

Prevent installing or modifying any software on the system

```
SQL> GRANT sysdba TO admin;
GRANT sysdba TO admin
*
ERROR at line 1:
ORA-01031: insufficient privileges
```

# SQL Command Restrictions

```
SQL> ADMINISTER KEY MANAGEMENT SET KEYSTORE close;
ADMINISTER KEY MANAGEMENT SET KEYSTORE close
*
ERROR at line 1:
ORA-01031: insufficient privileges
```

Disable Encryption

```
SQL> ALTER PROFILE default LIMIT failed_login_attempts UNLIMITED;
ALTER PROFILE default LIMIT failed_login_attempts UNLIMITED
*
ERROR at line 1:
ORA-01031: insufficient privileges
```

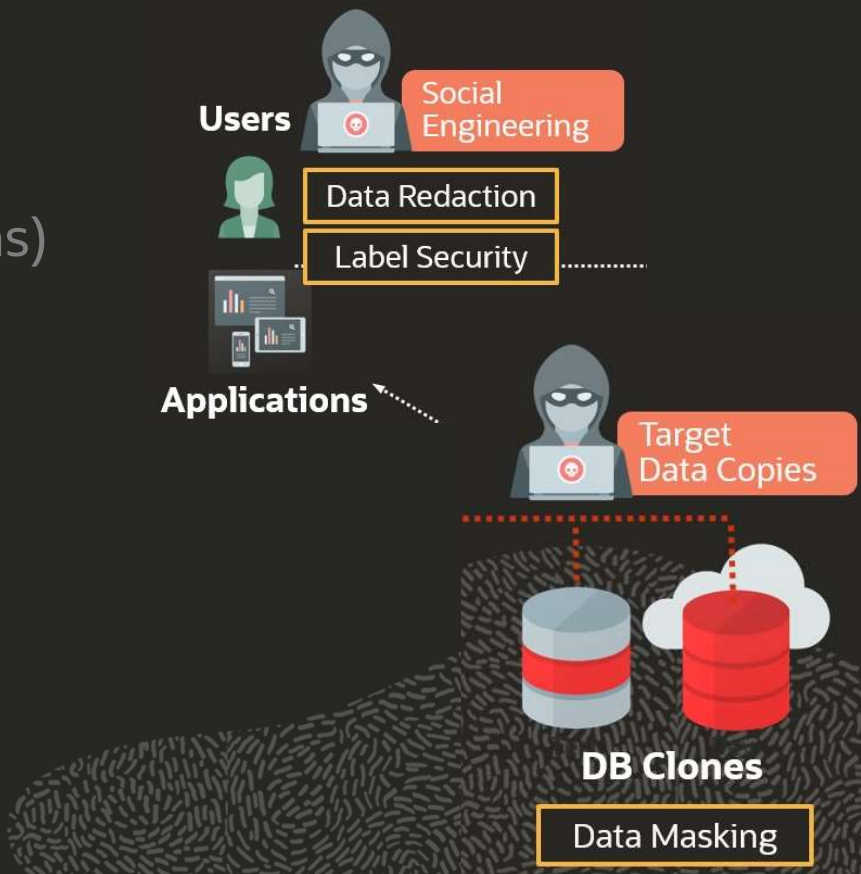
Unlimited Failed Logins

```
SQL> DROP TABLESPACE data INCLUDING CONTENTS;
DROP TABLESPACE data INCLUDING CONTENTS
*
ERROR at line 1:
ORA-01031: insufficient privileges
```

Drop Tablespace

# Agenda

- Encryption (Data, Backup, Connections)
- Network Access Control
- System & Data Protection
- Sensitive Data Discovery & Masking
- Auditing



# Data Redaction

- Mask (redact) data that is returned from queries issued by applications
- Redaction at runtime! Data itself is not changed!
- Redaction of Credit card, personal IDs, birth dates
- comply with industry regulations such as Payment Card Industry Data Security Standard (PCI DSS) and the Sarbanes-Oxley Act.
- Policies can be implemented by the customer

# Data Redaction

```
SQL> SELECT * FROM admin.payment_details ORDER BY id;

CUSTOMER_ID CARD_STRING         EXPIRY_DA   SEC_CODE
----------- ------------------- --------- ----------
       4000 1234-1234-1234-1234 10-MAR-21         123
       4001 2345-2345-2345-2345 10-MAR-21         234
       4002 3456-3456-3456-3456 10-MAR-21         345
       4003 4567-4567-4567-4567 10-MAR-21         456
       4004 5678-5678-5678-5678 10-MAR-21         567
```

Without Data Redaction

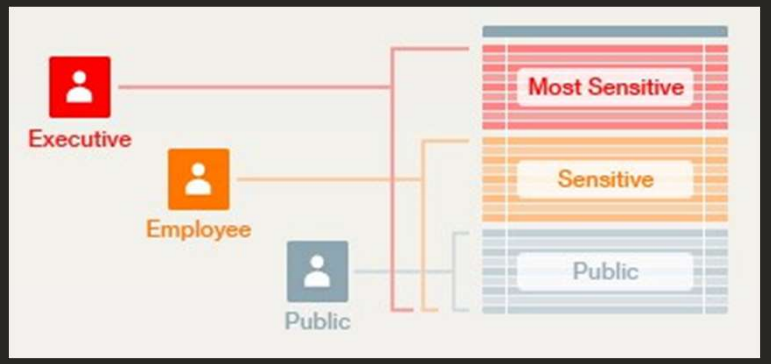
```
SQL> SELECT * FROM admin.payment_details ORDER BY id;

CUSTOMER_ID CARD_STRING         EXPIRY_DA   SEC_CODE
----------- ------------------- --------- ----------
       4000 ####-####-####-1234 10-MAR-21         123
       4001 ####-####-####-2345 10-MAR-21         234
       4002 ####-####-####-3456 10-MAR-21         345
       4003 ####-####-####-4567 10-MAR-21         456
       4004 ####-####-####-5678 10-MAR-21         567
```

With Data Redaction

# Oracle Label Security (OLS)

Label their data using different sensitivity levels

Users are allowed to access only those data records with the correspondent sensitivity level




```
SQL> SELECT STATUS FROM DBA_OLS_STATUS WHERE NAME = 'OLS_CONFIGURE_STATUS';

STATU
-----
TRUE
```

# Oracle Label Security (OLS)

Without OLS – All Users

```
SQL> select first_name, last_name, region
from customers;  2

FIRST_NAME LAST_NAME  REGION
---------- ---------- ----------
Harry      Hill       NORTH
Vic        Reeves     NORTH
Bob        Mortimer   WEST
Paul       Whitehouse SOUTH
Harry      Enfield    EAST
Jenifer    Lopez      WEST
```

```
SQL> select first_name, last_name, region
from customers;  2

FIRST_NAME LAST_NAME  REGION
---------- ---------- ----------
Harry      Hill       NORTH
Vic        Reeves     NORTH
Kylie      Minogue    NORTH
Thom       Yorke      NORTH
```

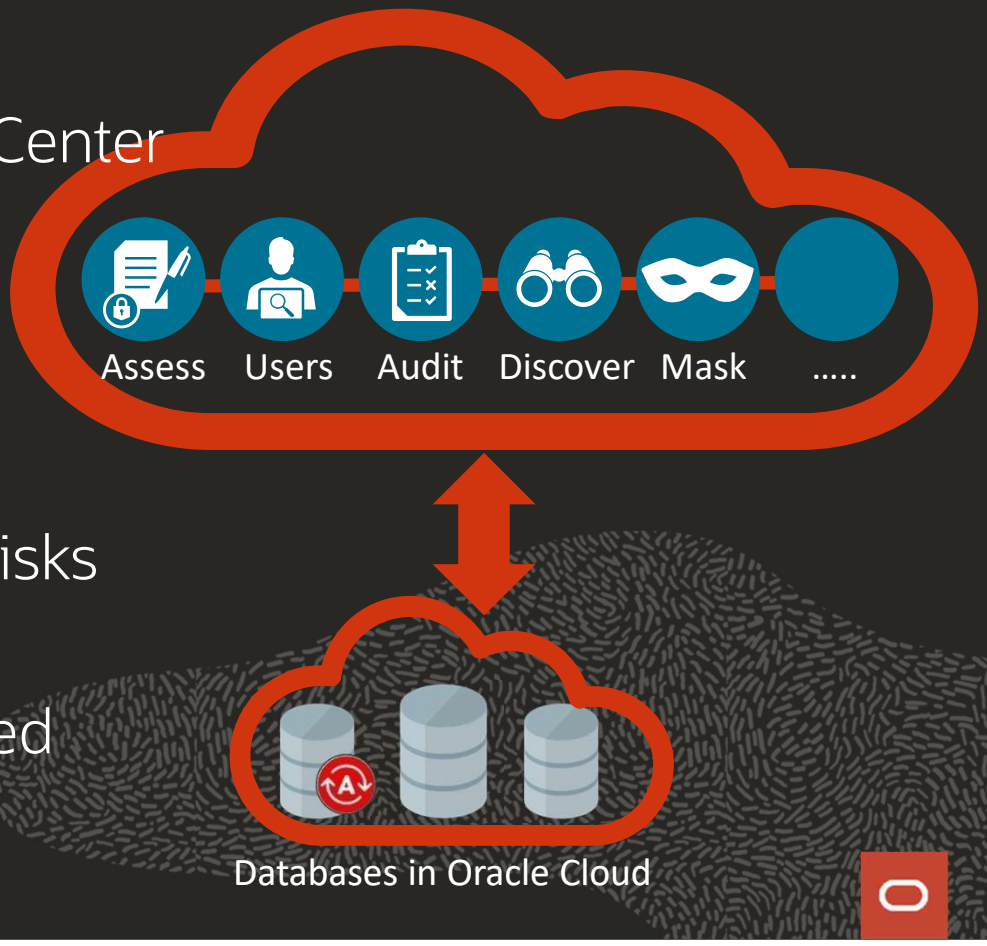
With OLS – User 1

```
SQL> select first_name, last_name, region
from customers;  2

FIRST_NAME LAST_NAME  REGION
---------- ---------- ----------
Bob        Mortimer   WEST
Jenifer    Lopez      WEST
Maria      Carey      WEST
Gareth     Gates      WEST
```

With OLS – User 2

# Data Safe

- Unified Database Security Control Center
  - Security Assessment
  - User Assessment
  - User Activity Auditing
  - Sensitive Data Discovery
  - Sensitive Data Masking
- Saves time and mitigates security risks
- Defense in Depth for all customers
- No special security expertise needed



# Data Masking

# Agenda

- Encryption (Data, Backup, Connections)
- Network Access Control
- System & Data Protection
- Sensitive Data Discovery & Masking
- Auditing

# Database Auditing

- Selective and effective auditing inside the Database using policies and conditions
- Predefined policies to monitor any abnormal activity
- Additional audit policies can be configured to audit based on specific IP addresses, programs, time periods, or connection types
- Enabled by default
- Can NOT be disabled!

# Database Auditing

```
SQL> SELECT value
FROM v$option
WHERE parameter = 'Unified Auditing';
  2    3
VALUE
----------------------------------------
TRUE
```

```
SELECT * FROM audit_unified_policies ORDER BY policy_name, audit_option;
```

t Output x | Query Result x

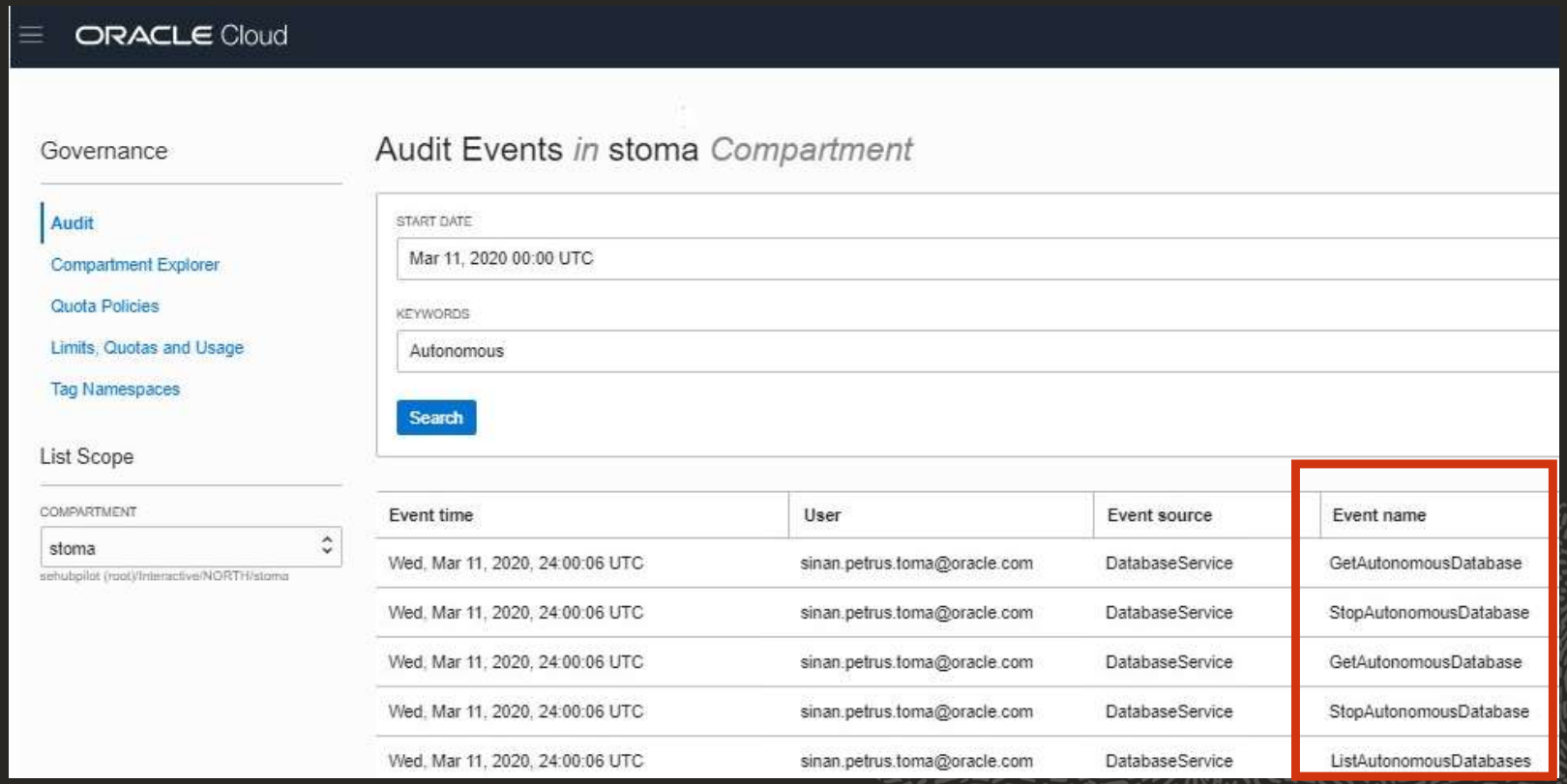
SQL | Fetched 50 rows in 2.221 seconds

| POLICY_NAME | AUDIT_CO... | CONDITIO... | AUDIT_OPTION | AUDIT_OPTION_TYPE |
|---|---|---|---|---|
| ADB_ADMIN_AUDIT | NONE | NONE | ALTER USER | STANDARD ACTION |
| ADB_ADMIN_AUDIT | NONE | NONE | CHANGE PASSWORD | STANDARD ACTION |
| ADB_MANDATORY_AUDIT | NONE | NONE | EXECUTE | OBJECT ACTION |
| ADB_MANDATORY_AUDIT | NONE | NONE | EXECUTE | OBJECT ACTION |
| COMMON_USER | NONE | NONE | ALL | STANDARD ACTION |
| ORA_ACCOUNT_MGMT | NONE | NONE | ALTER ROLE | STANDARD ACTION |
| ORA_ACCOUNT_MGMT | NONE | NONE | ALTER USER | STANDARD ACTION |

```
SELECT event_timestamp, dbusername, os_username, userhost, client_program_name, action_name, sql_text
FROM unified_audit_trail
ORDER BY event_timestamp desc;
```

| NT_TIMESTAMP | DBUSERNAME | OS_USERNAME | USERHOST | CLIENT_PROGRAM_NAME | ACTION_NAME | SQL_TEXT |
|---|---|---|---|---|---|---|
| AR-20 11.27.14.162204000 AM | C##CLOUD$SERVICE | oracle | wls-1.subapp0.v... | JDBC Thin Client | ALTER USER | ALTER USER OML$PROXY IDENTIFIED BY * |
| AR-20 11.23.06.589680000 AM | C##CLOUD$SERVICE | oracle | wls-3.subapp2.v... | JDBC Thin Client | ALTER USER | ALTER USER CVA_OML GRANT CONNECT THROUGH OML$PROXY |
| AR-20 04.06.16.232866000 AM | ADMIN | opc | admin-interacti... | sqlplus@admin-inter... | EXECUTE | begin DBMS_CLOUD.PUT_OBJECT('OBJ_STORE_CRED','https://swiftobjectstor.. |
| AR-20 04.06.15.809551000 AM | ADMIN | oracle | el0pod-8tlgg7.s... | oracle@el0pod-8tlgg... | DELETE | DELETE FROM LBACSYS.OLS$POLT WHERE TBL_NAME = :B2 AND OWNER = :B1 |
| AR-20 03.30.12.536690000 PM | CHRISTELLE | cvaltanc | CVALTANC-ES | SQL Developer | LOGON | (null) |

# API Audit Logs



# API Audit Logs

- Audit provides records of API operations performed against supported services
- Audit logs are maintained for 90 days
- Can be configured for up to 365 days

# VCN Flow Logs

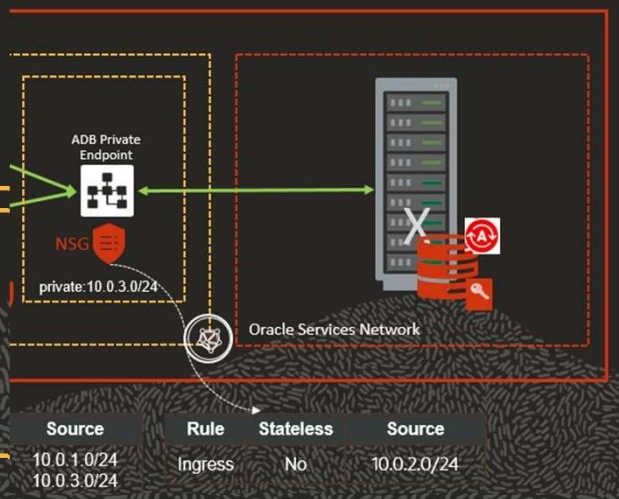
View connection information for traffic within your VCN

Keeps detailed records of every flow that passes through your VCN and presents this data for analysis

- Source and destination of the traffic
- Quantity of traffic
- Permit or Deny action taken

Information can be used for:

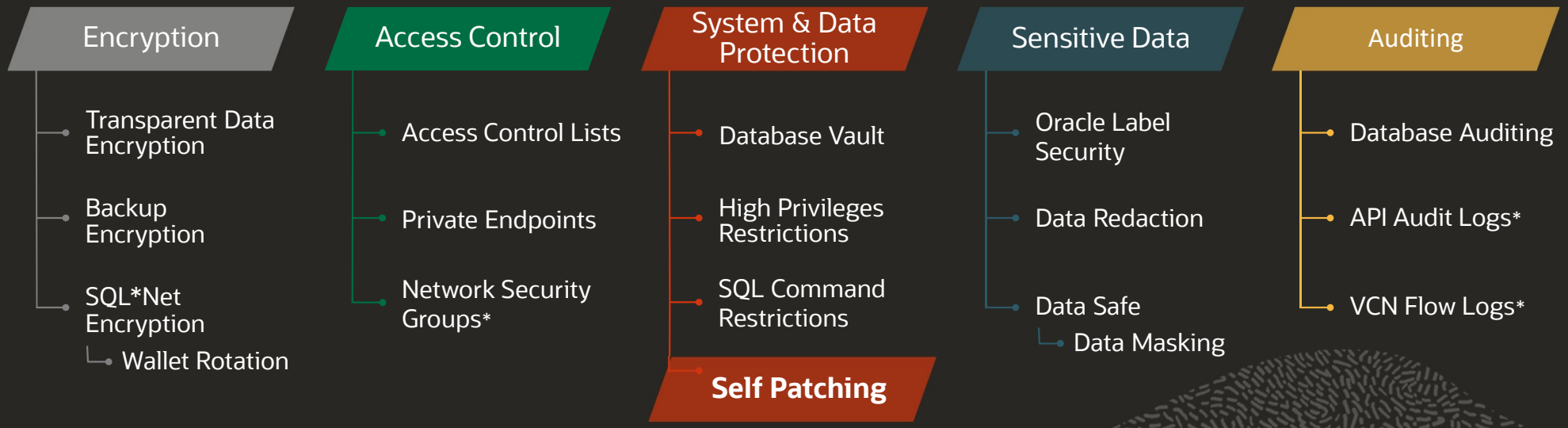
- Network monitoring
- Troubleshooting
- Compliance



# OCI Compliance: Current Audit Programs

| | | | | | | |
|---|---|---|---|---|---|---|
| Global | SOC 1 : SOC 2 : SOC 3 | 27001 : 27017 : 27018 | Self-Assessment | US Privacy Shield | | |
| Government | DoD DISA SRG IL2 | Moderate – Agency ATO | VPAT – Section 508 | G-Cloud 11 - UK | Model Clauses - EU | |
| Industry | HIPAA | PCI DSS Level 1 | FISC - Japan | IG Toolkit - UK | | |
| Regional | GDPR - EU | BSI C5 - Germany | TISAX - Germany | PIPEDA - Canada | Cyber Essentials Plus - UK | My Number - Japan | Cloud Security Principles - UK |

# Autonomous Database | Security Features




* OCI Security Features

# 85%

of security breaches occurred
after the CVE was published*


**Autonomous**

- No Downtime
- Applied Immediately
- No Customer Interaction

**On-Premise**

- Downtime Restrictions
- Takes Long Time
- Human Resources

* Verizon - 2018 Data Breach Investigation Report

# Security is Shared Responsibility

- Network security and monitoring
- OS and platform security
- Database patches and upgrades
- Data encryption by default
- Adminstrative separation of duties

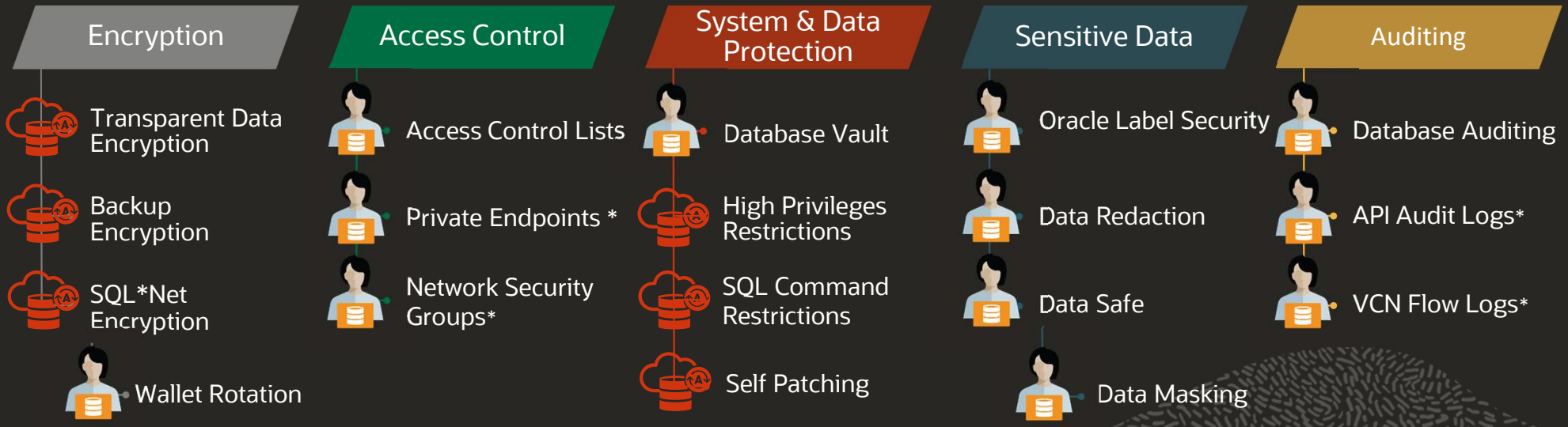
Oracle Responsibility

- Ongoing security assessments
- Users and privileges
- Sensitive data discovery
- Data protection
- Activity auditing

Customer Responsibility

Tools provided by Oracle

# Autonomous Database | Security Features




* OCI Security Features

# Further Reads

https://blogs.oracle.com/cloud-infrastructure/getting-up-to-speed-on-using-private-endpoints-for-autonomous-database-with-shared-exadata-infrastructure

https://blogs.oracle.com/oraclemagazine/getting-started-with-autonomous-database-security

https://blogs.oracle.com/oraclemagazine/autonomous-and-secure

https://www.oracle.com/a/ocom/docs/database/oracle-autonomous-database-strategy-wp.pdf

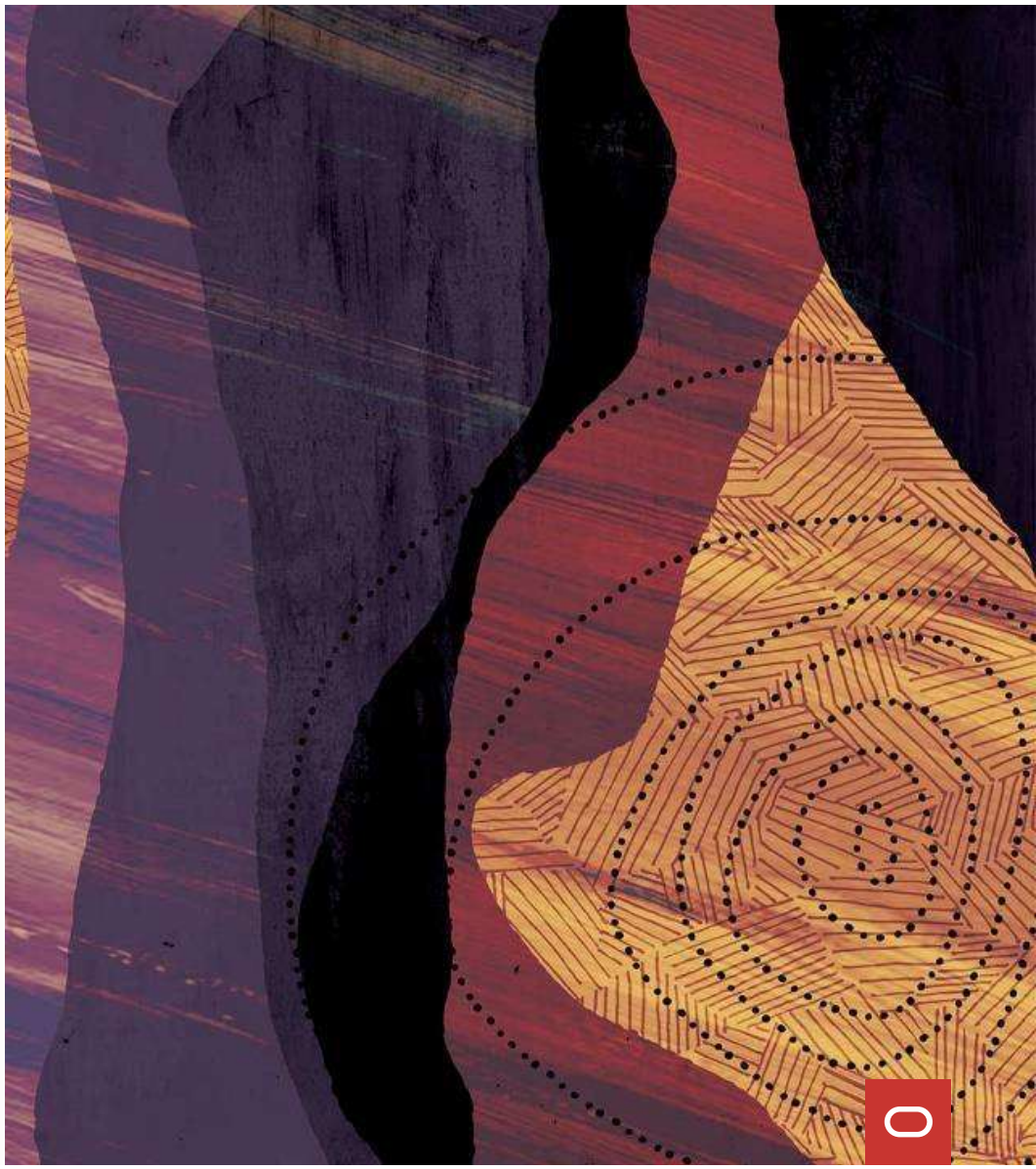
https://www.oracle.com/a/ocom/docs/dc/us44350118.pdf

# Q & A

sinan.petrus.toma@oracle.com

# Thank you

**Sinan Petrus Toma**




ORACLE