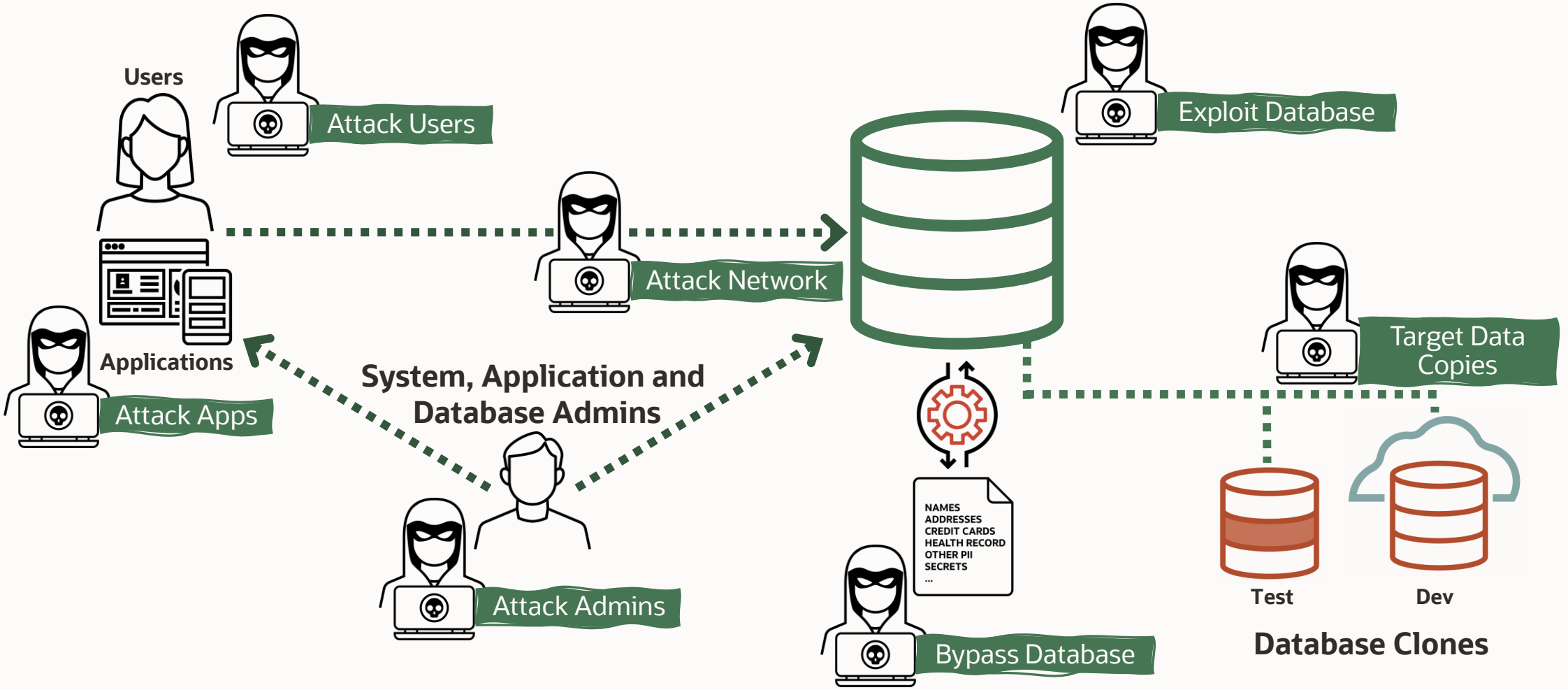
ORACLE

Oracle Database Authentication

Inge Os
Cloud Security Advisor
inge.os@oracle.com

How Do Hackers Attack the Database?



How we look at Database Security

Assess

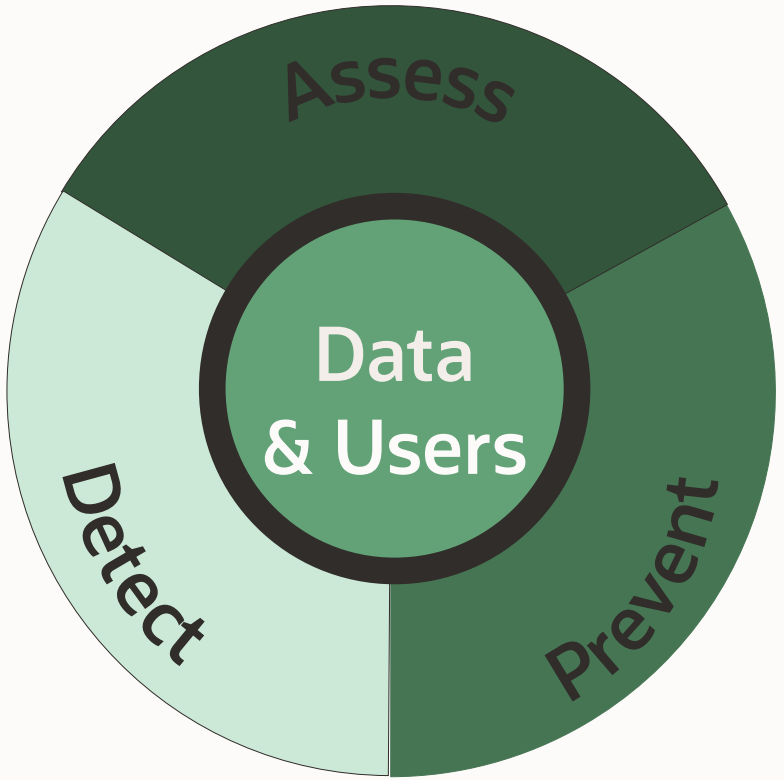
Assess the current state of security for the database

Detect

Detect attempts to access data, especially attempts that violate policy

Prevent

Prevent unauthorized or out-of-policy access to data



Data

Data stored in a database is your organization's most valuable asset, but also a source of significant risk.

Users

Users and applications connecting to your database are prime targets

Comprehensive security controls for Oracle Databases

Assess

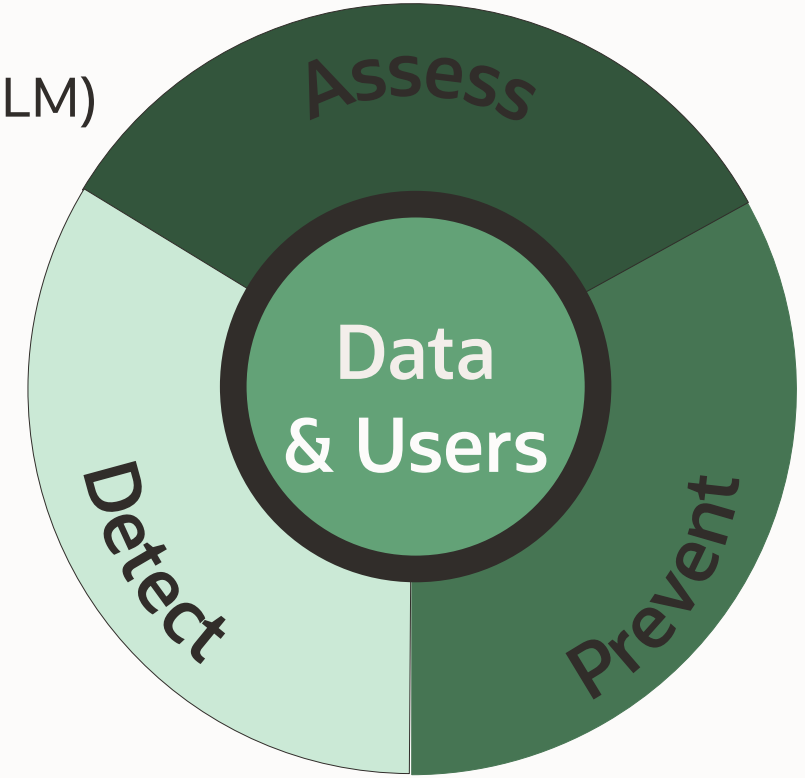
Config-Assessment(DBSAT, DBLM)
Data Discovery
Privilege Analysis*

Detect

Activity Auditing
Audit Vault
Database Firewall*

Prevent

Transparent Data Encryption & Key Vault
Data Masking, Data Redaction
Database Vault*



Data

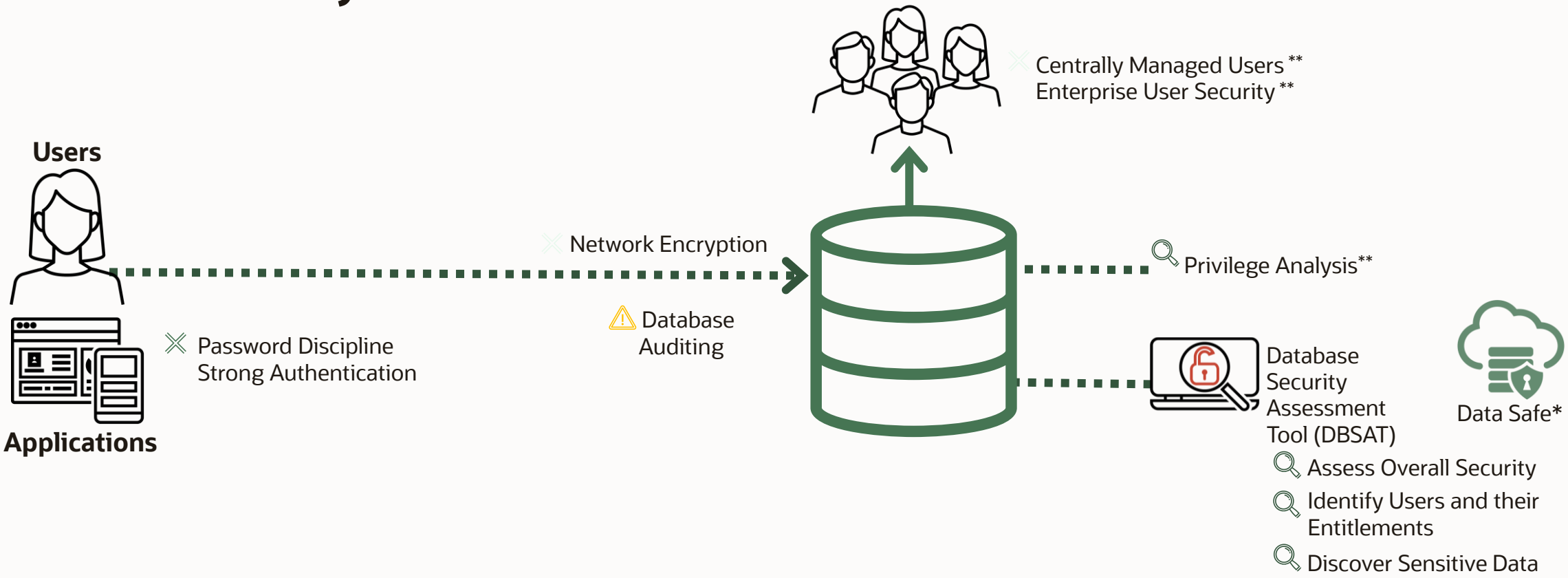
Label Security
Virtual Private Database (VPD)
Real Application Security (RAS)*
DB Cryptographic Toolkit

Users

Password, PKI, Kerberos, Radius
Proxy Users, Password Profiles
Roles and Privileges
Oracle & Active Directory

* Unique to Oracle

Baseline Security

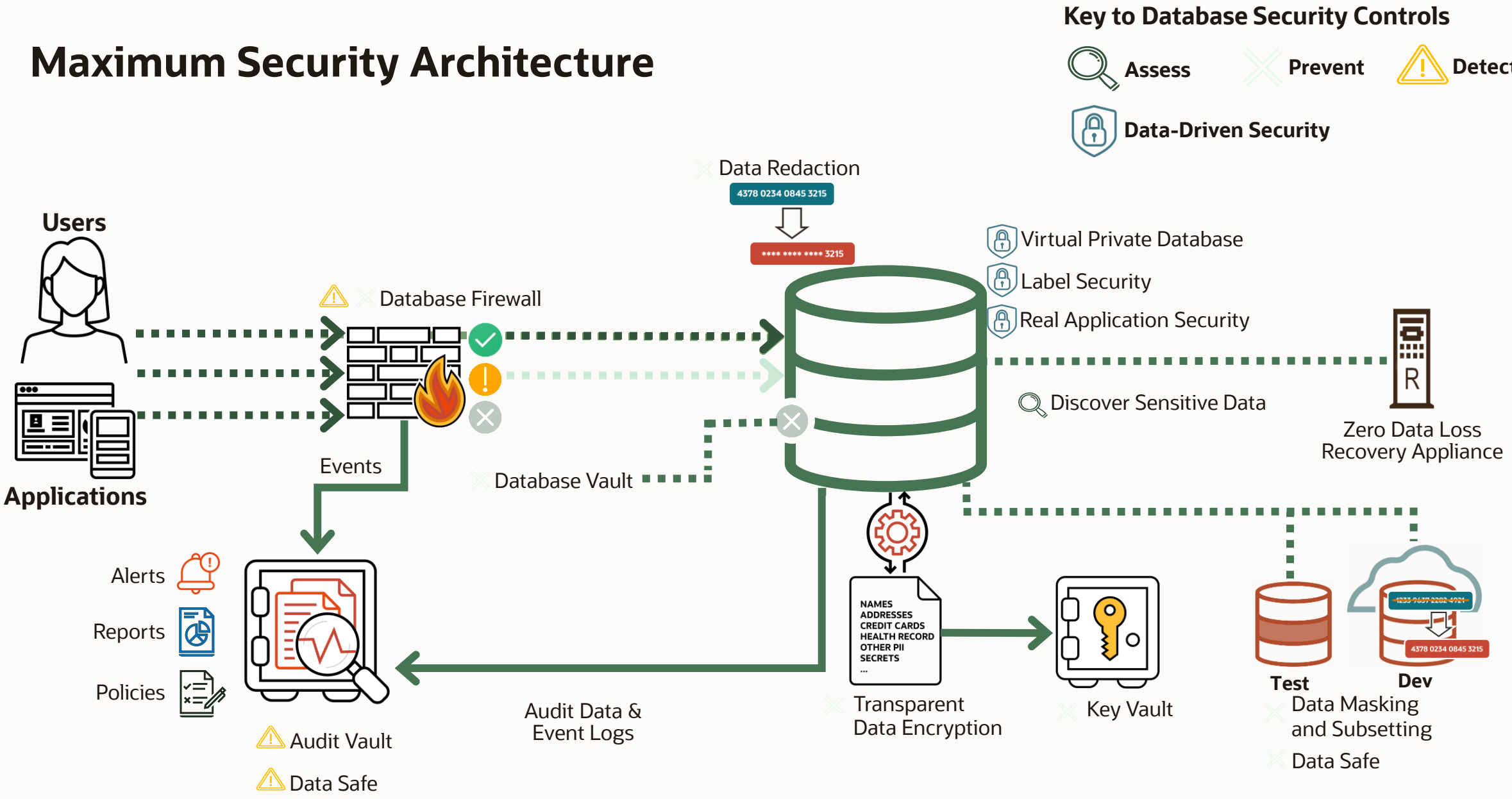


* Included with Database Cloud, additional cost on-premises
** Only available with Enterprise Edition

Key to Database Security Controls

Assess **Prevent** **Detect**

Maximum Security Architecture



User Management Through Authentication and Authorization

1. Authentication
2. User confirms their identity (username) with credentials (passwords, tickets, tokens, credentials…)

1. Authorization
2. What the user is allowed to access and execute AND what they are not allowed to do

Oracle Database Authentication and Authorization

Local Authentication and Authorization

- Password
- Operating System

Database accounts and DBA accounts sprawl.
Non personal privileged account.
No central enforcement and no central reporting

Centralized Authentication & Authorization

- EUS
- CMU
- AzureAD
- OCI Token

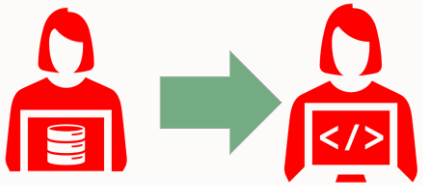
Centralized Authentication and Local Authorization

- Kerberos
- Certificate
- Radius

Need For Centralized Authentication and Authorization

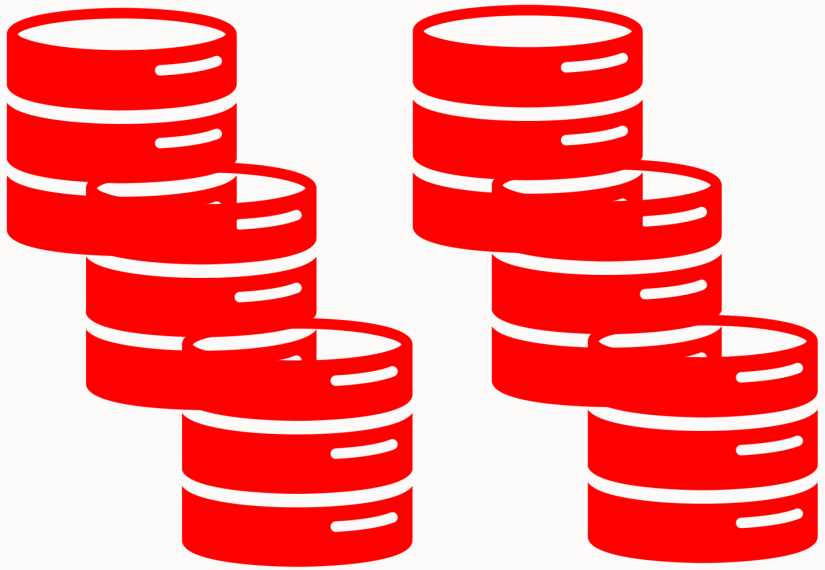
Joiners
Add new user
Grant roles/privileges

Mover
Change roles/privileges



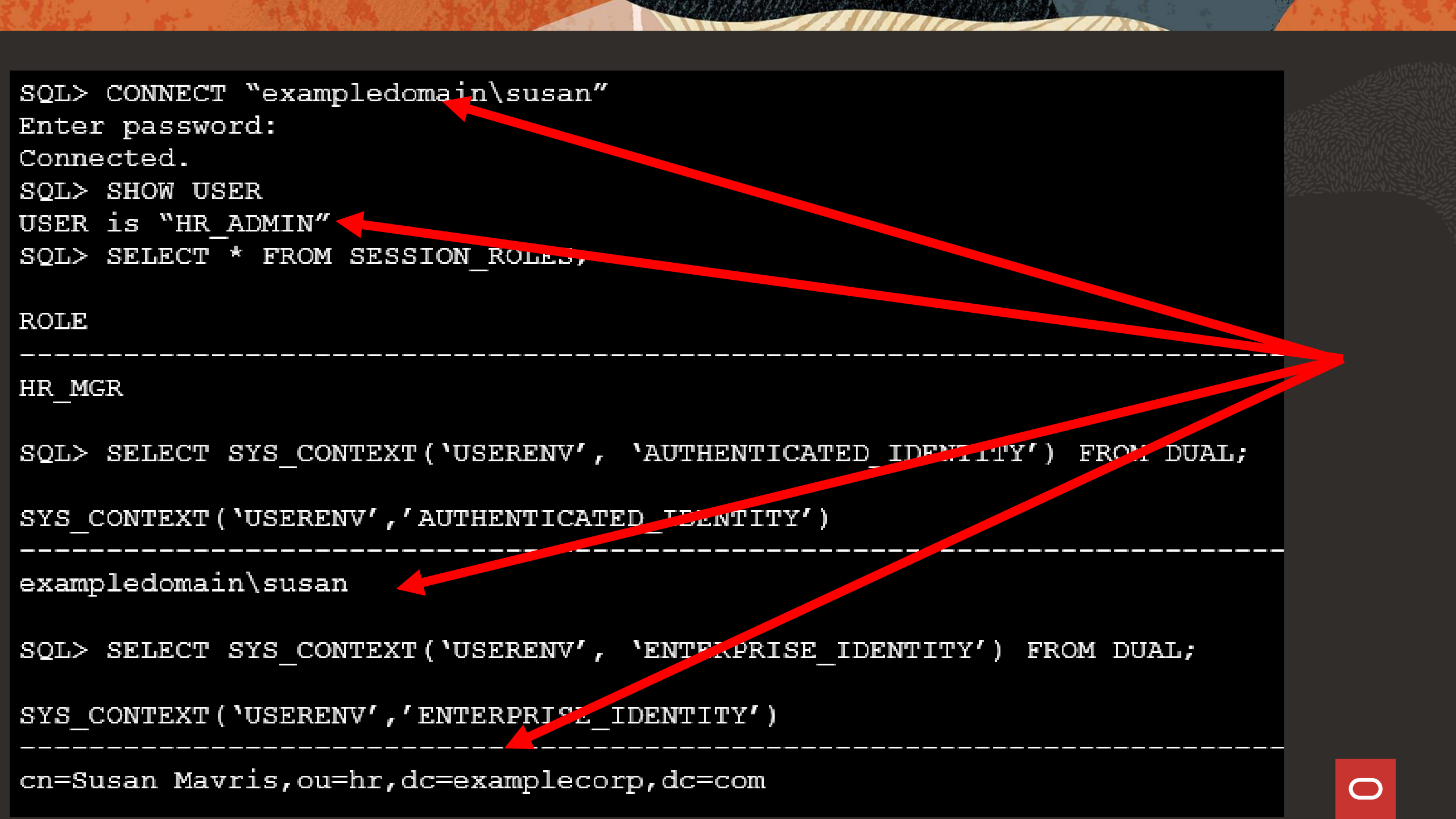
Leavers
Drop user

Repeat for each database

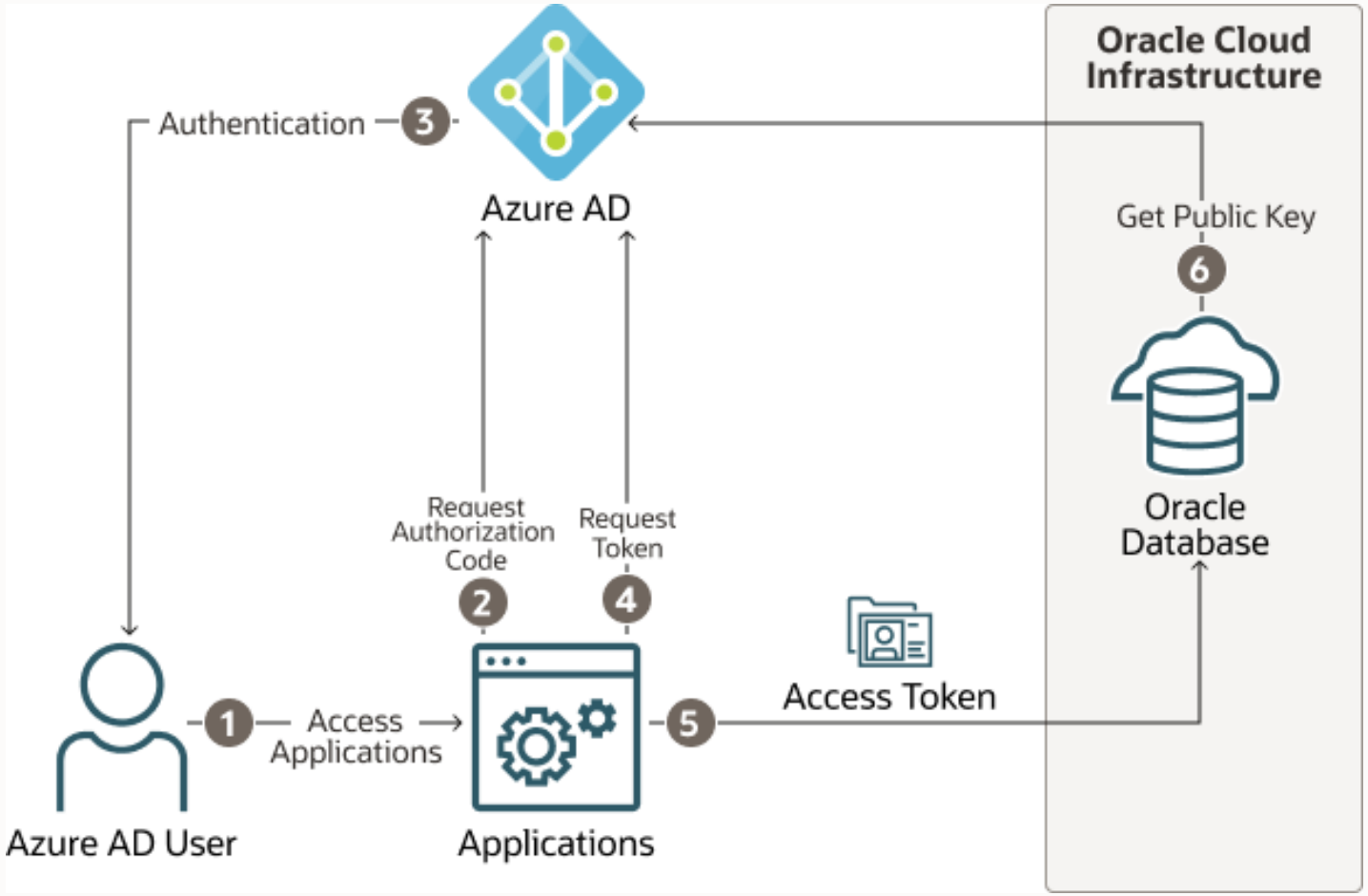


Centrally managed Users with AD

Azure AD token Authentication


SQL> CONNECT "exampledomain\susan"
Enter password:
Connected.
SQL> SHOW USER
USER is "HR_ADMIN"
SQL> SELECT * FROM SESSION_ROLES;
ROLE
HR_MGR
SQL> SELECT SYS_CONTEXT('USERENV', 'AUTHENTICATED_IDENTITY') FROM DUAL;
SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY')
exampledomain\susan
SQL> SELECT SYS_CONTEXT('USERENV', 'ENTERPRISE_IDENTITY') FROM DUAL;
SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY')
cn=Susan Mavris,ou=hr,dc=examplecorp,dc=com

OCI IAM Domain token Authentication



ios3db19c - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_IAM/ManagedAppMenuBlade/~/Users/objectId/0adad631-1725-407f-9972-ce1ecb59fe42/appId/98652ad5-06a6-49...

Oracle favorites folder | Oracle Applications | Cloud Sign In | Home | Oracle Clou...

Microsoft Azure | Search resources, services, and docs (G+/) | @oracle.com DEFAULT DIRECTORY

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > ios3db19c

ios3db19c | Users and groups

Enterprise Application

Application assignment succeeded
1 user & 0 groups have been assigned access

Add user/group | Edit assignment | Remove | Update credentials | Columns | Got feedback?

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
IO Inge Os	User	dba_role
IO Inge Os	User	dbusers

Create global user and global role

```
create user AZADUSER identified globally as 'AZURE_ROLE=dbusers';
create role azuread_dba identified globally as 'AZURE_ROLE=dba_role';
grant create session to AZADUSER;
grant pdb_dba to azuread_dba;
```

Enable azureAD as identity provider

```
ALTER SYSTEM SET IDENTITY_PROVIDER_TYPE=AZURE_AD SCOPE=BOTH;
ALTER SYSTEM SET IDENTITY_PROVIDER_CONFIG =
'{
   "application_id_uri" :"https://demooracle.onmicrosoft.com/1111122222-
2222-5703-8b12-3a029130b25c"  ,
   "tenant_id" : "8ce0a0e-1111-2222-8888-abababcdcdcd",
}' SCOPE=BOTH;
```


Token generation sample app based on msal Python SDK

https://msal-python.readthedocs.io/en/latest/

```
# pip install msal
# Python 3.x
#
#  (c) Inge Os, Oracle Norway 3/2-2023
#
from msal import PublicClientApplication
import sys
import os
import json
import platform

# Default values
client_id = None
tenant_id = None
scopes = None

#
# Retrieve CMD line arguments
#
if platform.system().lower() == 'linux':
    configFile="/home/oracle/azuread-demo/config.json"
else:
    configFile="azadconfig.json«
# Load configuration
#
with open(args.configfile) as f:
    configText = f.read()
try:
    cfg=json.loads(configText)
except (Exception, ValueError) as ex:
    print('invalid configuration in configfile: ' + str(ex))
    exit(1)
```

```
app = PublicClientApplication(
    client_id = client_id,
    authority = "https://login.microsoftonline.com/" +tenant_id
)

acquire_tokens_result = app.acquire_token_interactive(
    scopes = scopes
)

if 'error' in acquire_tokens_result:
    print("Error: " + acquire_tokens_result['error'])
    print("Description: " +
acquire_tokens_result['error_description'])
else:
    print("Access token:\n")
    print(acquire_tokens_result['access_token'])
    with open(args.tokenfile+'.jwt', 'w') as f:
        f.write(acquire_tokens_result['access_token'])
    print("\nRefresh token:\n")
    print(acquire_tokens_result['refresh_token'])
    with open(args.tokenfile+'.rjwt', 'w') as f:
        f.write(acquire_tokens_result['refresh_token'])
```

Token generation

```
(base) G:\demo_projects\cloud_labs\azuread_19c>python getazadtokenV3.py
Access token:

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lW
…
-o807nJEWtNEkIwPXTSdmy4lSv_cg_18DQZQZ6Grys0AsdG2xX9lFPNnjA

Refresh token:

0.AXMADvCtm5q4CkmXG73faHz-uRP1eOZHzJtEnqXdpUp-kSpzADk.AgABAAEAAAD—
…
pslJGWiV1nibOSc5EFTaqMDYoZHEpWqFbZMz8eCk_94K3lwL8kXGDylqrQofxJDxfDCGKkFx-B8a1YOBfrA
```

Upload the generated token to the tokenfile pointed at in the tnsnames.ora file

Run of test script

```
SQL> connect /@mydb
Connected.
logged on user

AZADUSER

sys_context('userenv','CURRENT_USER')
press any key


AZADUSER

sys_context('userenv','AUTHENTICATED_IDENTITY')
press any key


live.com#somebody@oracle.com

sys_context('userenv','ENTERPRISE_IDENTITY')
press any key



e678f513-cc47-449b-9ea5-dda54a7e912a
```


References

https://blogs.oracle.com/cloudsecurity/post/azure-active-directory-can-authenticate-database-users
https://www.youtube.com/watch?v=GkrulRzlNYI

https://msal-python.readthedocs.io/en/latest/