



Oracle Data Safe

Security for Cloud Databases

NoCOUG Fall Conference, Oakland

Bettina Schäumer

Senior Principal Product Manager
Oracle Database Security

November 21, 2019

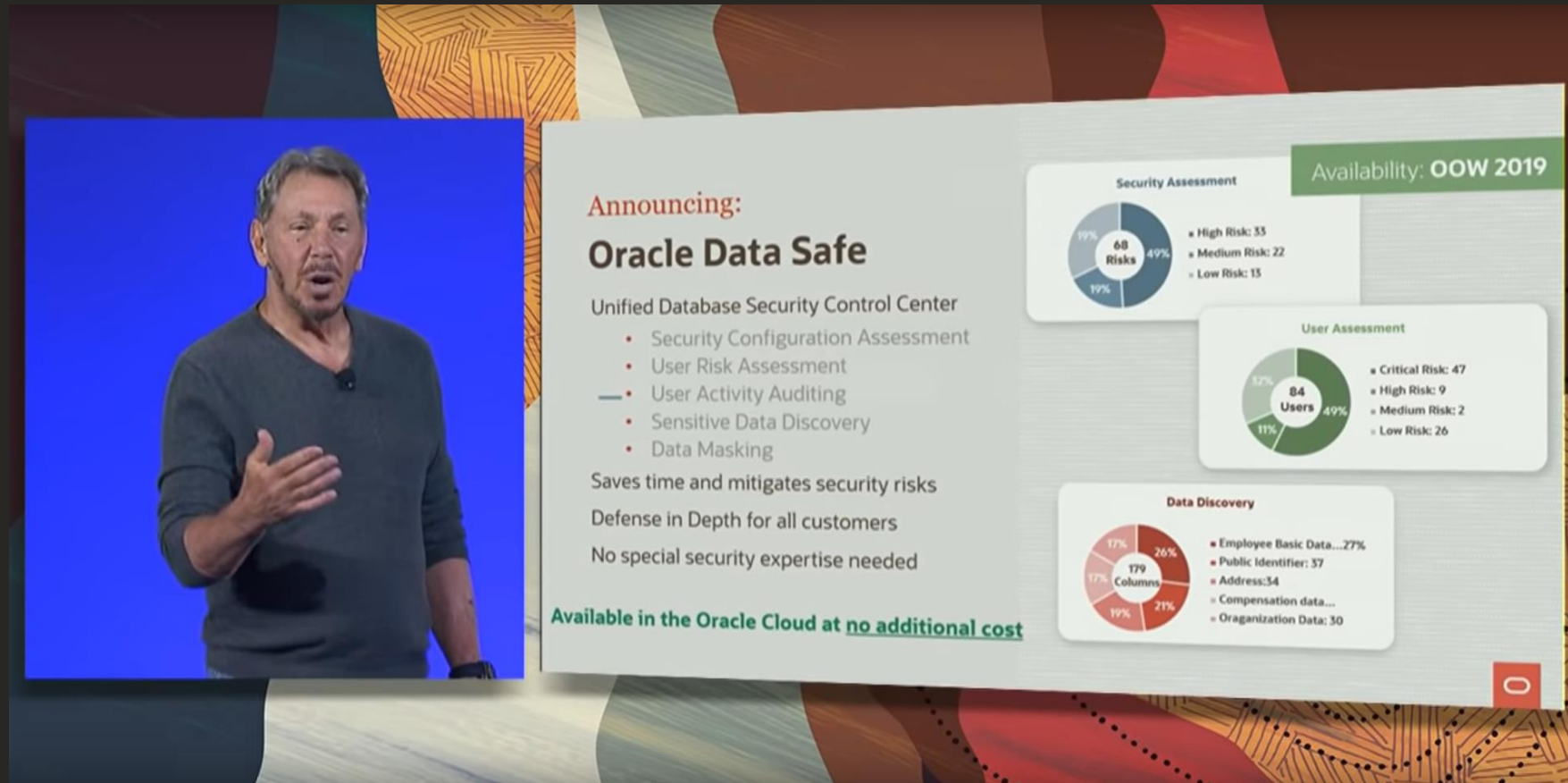
Safe Harbor

The preceding 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.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at <http://www.oracle.com/investor>. All information in this presentation is current as of September 2019 and Oracle undertakes no duty to update any statement in light of new information or future events.

Oracle Data Safe

Announced at Oracle Open World 2019



Announcing:
Oracle Data Safe

Unified Database Security Control Center

- Security Configuration Assessment
- User Risk Assessment
- User Activity Auditing
- Sensitive Data Discovery
- Data Masking

Saves time and mitigates security risks
Defense in Depth for all customers
No special security expertise needed

Available in the Oracle Cloud at no additional cost

Availability: OOW 2019

Security Assessment

68 Risks

- High Risk: 33
- Medium Risk: 22
- Low Risk: 13

User Assessment

84 Users

- Critical Risk: 47
- High Risk: 9
- Medium Risk: 2
- Low Risk: 26

Data Discovery

179 Columns

- Employee Basic Data...: 27%
- Public Identifier: 37
- Address: 34
- Compensation data...
- Organization Data: 30

2019 Headlines

- Data Breaches up 54% in 2019

More than 20 reported breaches per day on average¹

- Data Privacy Regulations Continue to Proliferate

58% of countries now have Data Privacy legislation²

- GDPR Fines Top € 359,205,300.00 (\$397M USD)

“the fines are no longer just about security breaches, but failures of transparency and failures to follow procedures.” – Karl Foster, Legal Director, Blake Morgan

¹Source: Risk Based Security- 2019 MidYear Data Breach QuickView Report

²Source: UN Conference on Trade and Development

Why Focus on Databases?

Most business data is in databases

- Manage large amounts of data
- Easy to retrieve, search and analyze
- High performance

Verizon Breach Report 2018

- Top asset breached: database (20%)
- Internal actors involved: 28% (up 12%)
- 57% of internal attacks on databases



**Databases may
be your most
valuable
information asset**

**Databases may
be one of your
greatest
liabilities**



Common Reasons for Database Breaches

- Unencrypted data
 - Security patches not applied
 - Administrator Snooping
 - Malware / Viruses
 - Poor Network Isolation
- Security configuration drift
 - Unmanaged privileged users
 - Unaudited users
 - Untracked sensitive data
 - Sensitive data in open

Addressed by
Autonomous Database

Currently
Customer Responsibility

Security Zones of Control

*now offered in Oracle Data Safe

Assess

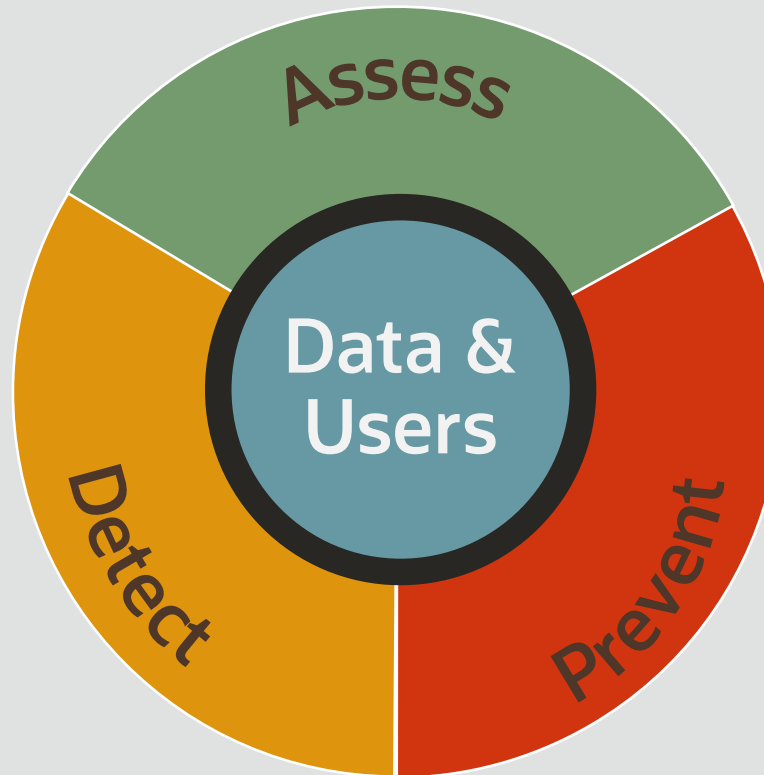
Data Discovery*
Security Assessment*
User Assessment*
Privilege Analysis**

Detect

Activity Auditing*
Reporting/Alerting*
Audit Vault
Database Firewall**

Prevent

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



Data

Crypto Toolkit
Virtual Private Database
Label Security
Real Application Security**

Users

PKI, Kerberos
Radius (pluggable)
Proxy Users
Oracle & Active Directory



New - Oracle Data Safe

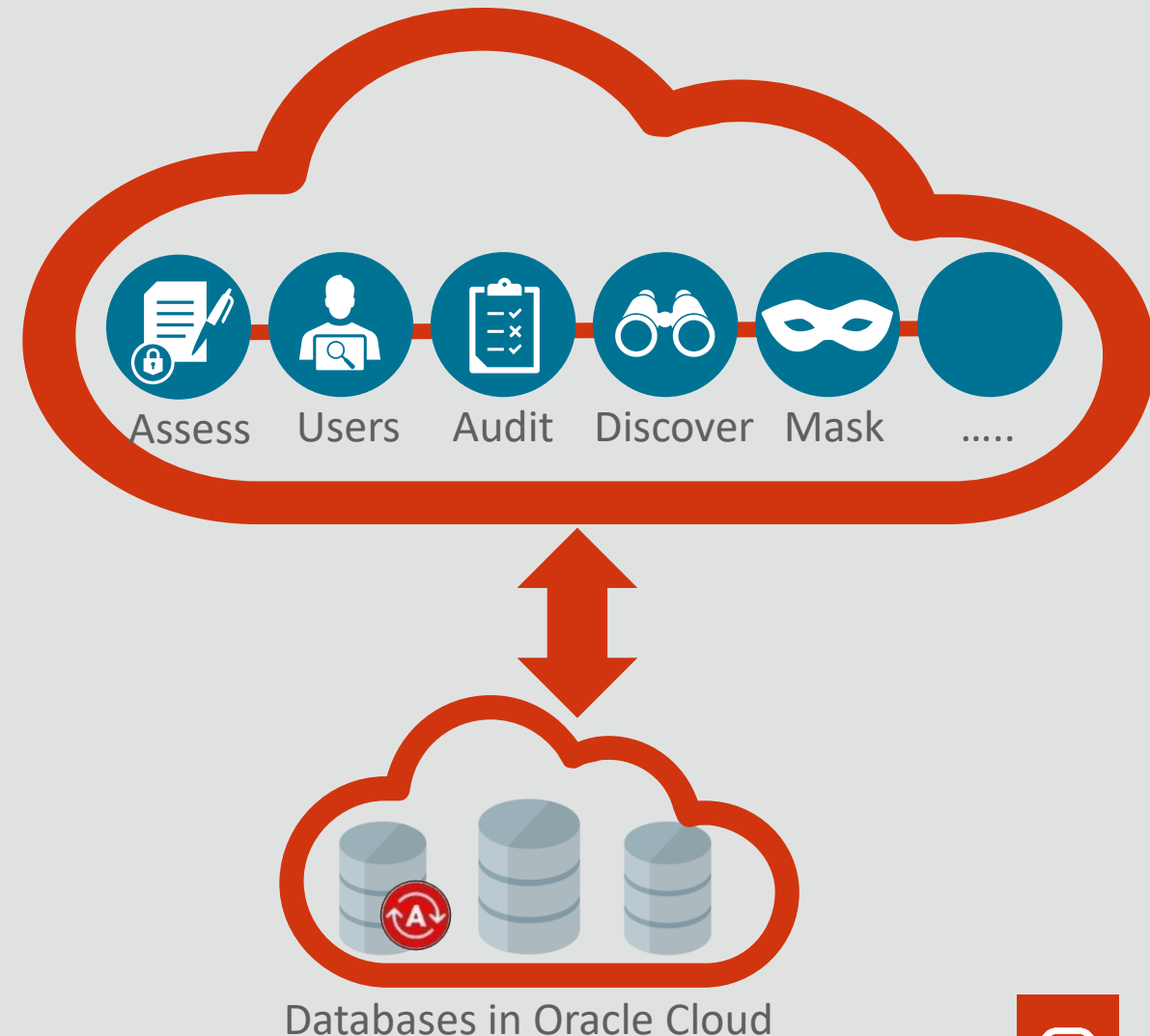
Security for Cloud Databases

- Delivers unified set of essential security services on the cloud
- Mitigates user, data, configuration risk
- Unified database security dashboard
- Addresses customer responsibilities
- Requires no special security expertise

Available with Oracle Cloud Database
Subscription at **No Additional Cost***

* includes 1M audit/records per month; Data retention up to 12 months

Copyright © 2019 Oracle and/or its affiliates.

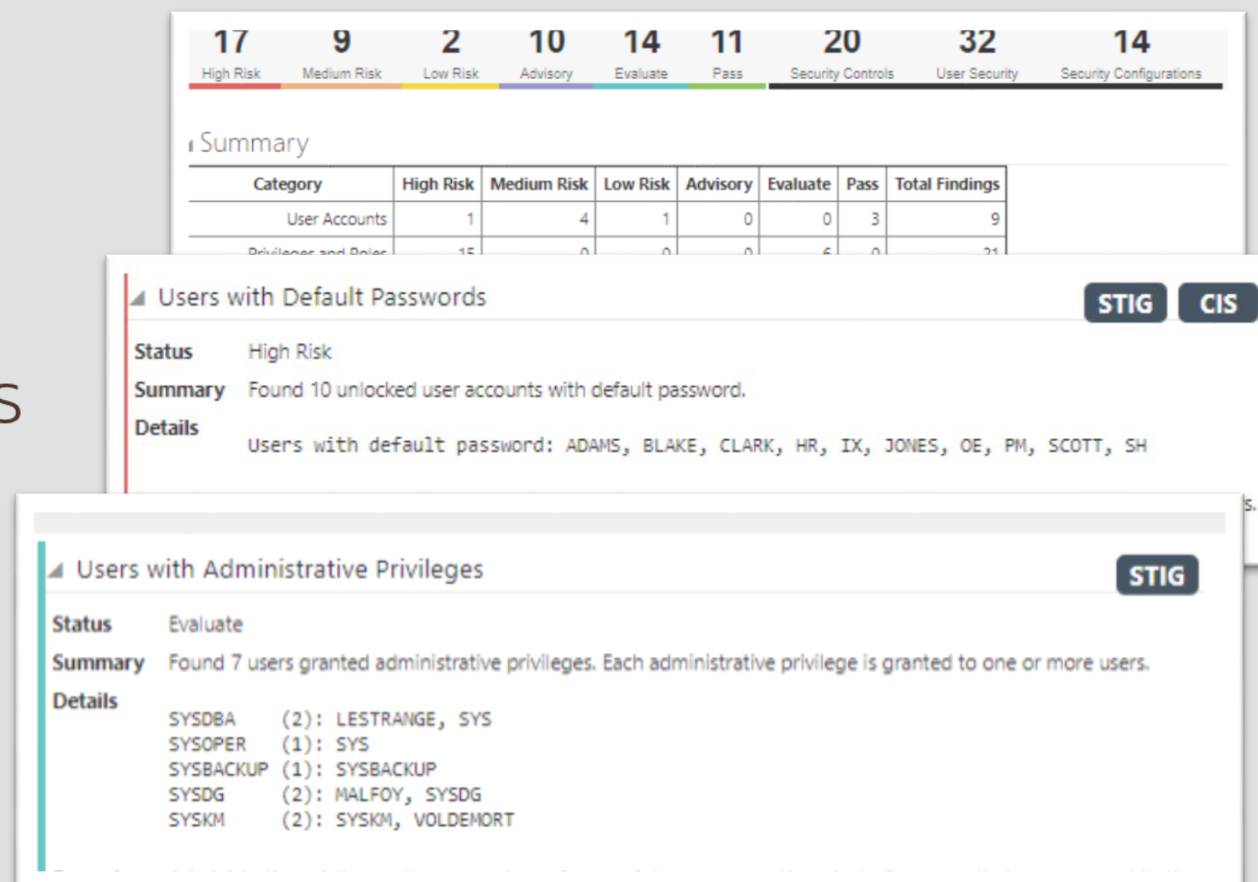


Database Security Assessment



Instant feedback on configurations that may introduce unnecessary risk

- Comprehensive assessment
 - Security parameters
 - Security controls in use
 - User Roles and Privileges
- Identify drift from best practices
- Actionable reports
 - Prioritized recommendations
 - Compliance mappings (GDPR, STIG, CIS)

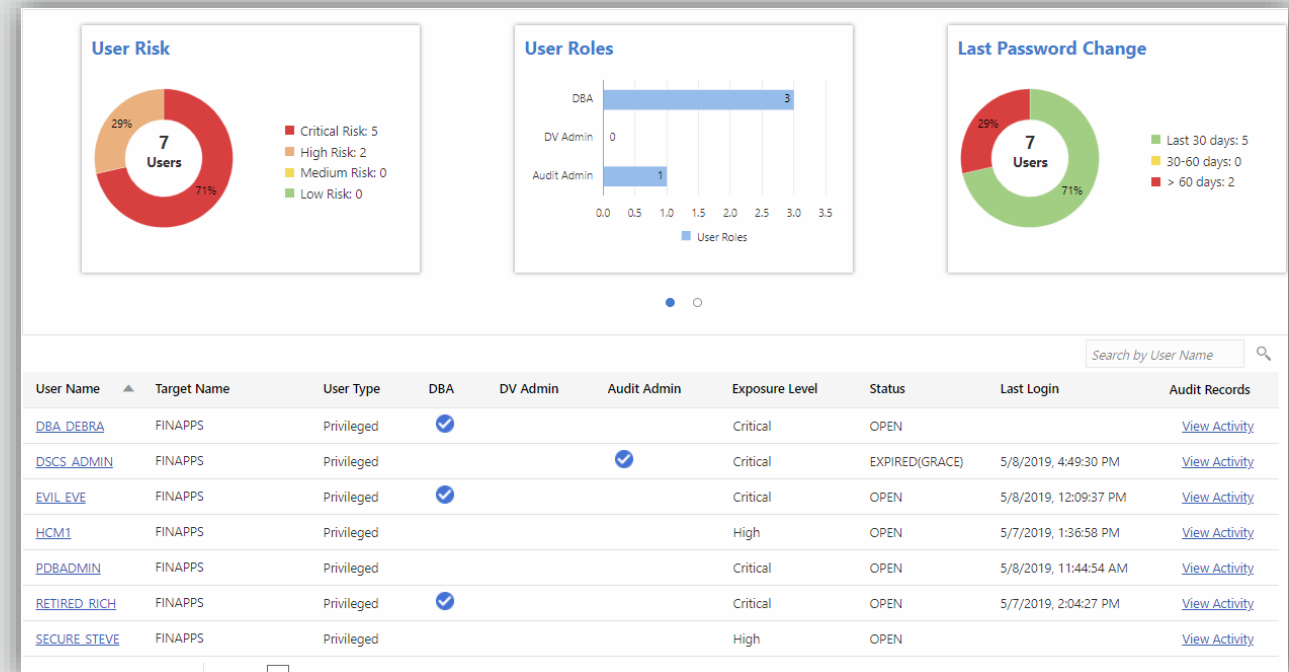


User Risk Assessment



Reduce user risk by managing roles/privileges and policies

- Identify over-privileged risky users
- Evaluate static profile: type of user, password policies, ...
- Evaluate dynamic profile: last login / IP / password change, audit data, ...



User Activity Auditing



Track user actions and streamline auditing with robust reporting

- Provision audit, compliance, and alert policies
- Collect audit data from databases, and track sensitive operations
- Audit Reports
 - Interactive reports for forensics
 - Summary and detailed reports
 - PDF reports for compliance

Edit Policies

Target Name : Call_Center_Prod

Audit Policies | Alert Policies

Basic Auditing ?

- ☒ Critical Database Activity
- ☒ Login Events
- Exclude Users:
- ☐ Database Schema Changes (DDL)

Admin Activity Auditing ?

- ☒ All Admin Activity

User Activity Auditing ?

- ☐ All User Activity
- List of Users *

Audit Compliance Standards ?

- ☐ Center for Internet Security (CIS) Configuration

Additional Audit Policies ?

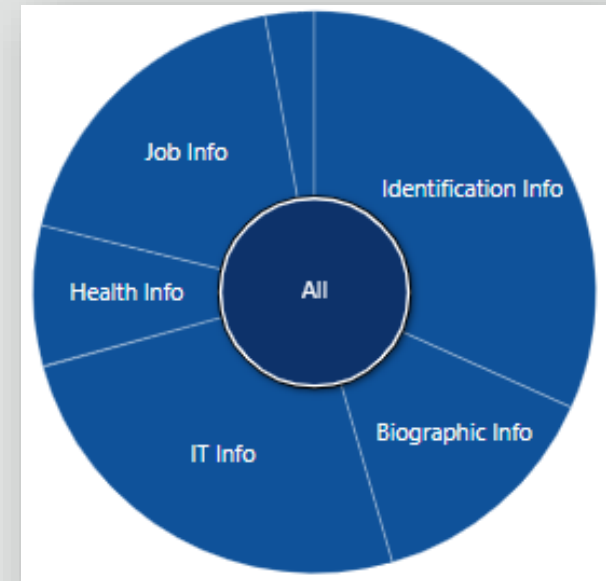
- ▶ Custom Policies
- ▶ Oracle Pre-seeded Policies

Sensitive Data Discovery

Prioritize security efforts by finding the location, type and amount of sensitive data



- Discovers/classifies 125+ sensitive types
- User-defined sensitive types
- Incremental discovery
- Validated Fusion SaaS & EBS templates
- Reports amount / type of sensitive data



3.6M Sensitive Values	30 Sensitive Types
18 Sensitive Tables	57 Sensitive Columns

Sensitive Data Discovery

125+ Pre-defined Sensitive Types



Identification

SSN
Name
Email
Phone
Passport
DL
Tax ID
...



Biographic

Age
Gender
Race
Citizenship
Address
Family Data
Date of Birth
Place of Birth
...



IT

IP Address
User ID
Password
Hostname
GPS location
...



Financial

Credit Card
CC Security PIN
Bank Name
Bank Account
IBAN
Swift Code
...



Healthcare

Provider
Insurance
Height
Blood Type
Disability
Pregnancy
Test Results
ICD Code
...



Employment

Employee ID
Job Title
Department
Hire Date
Salary
Stock
...



Academic

College Name
Grade
Student ID
Financial Aid
Admission Date
Graduation Date
Attendance
...

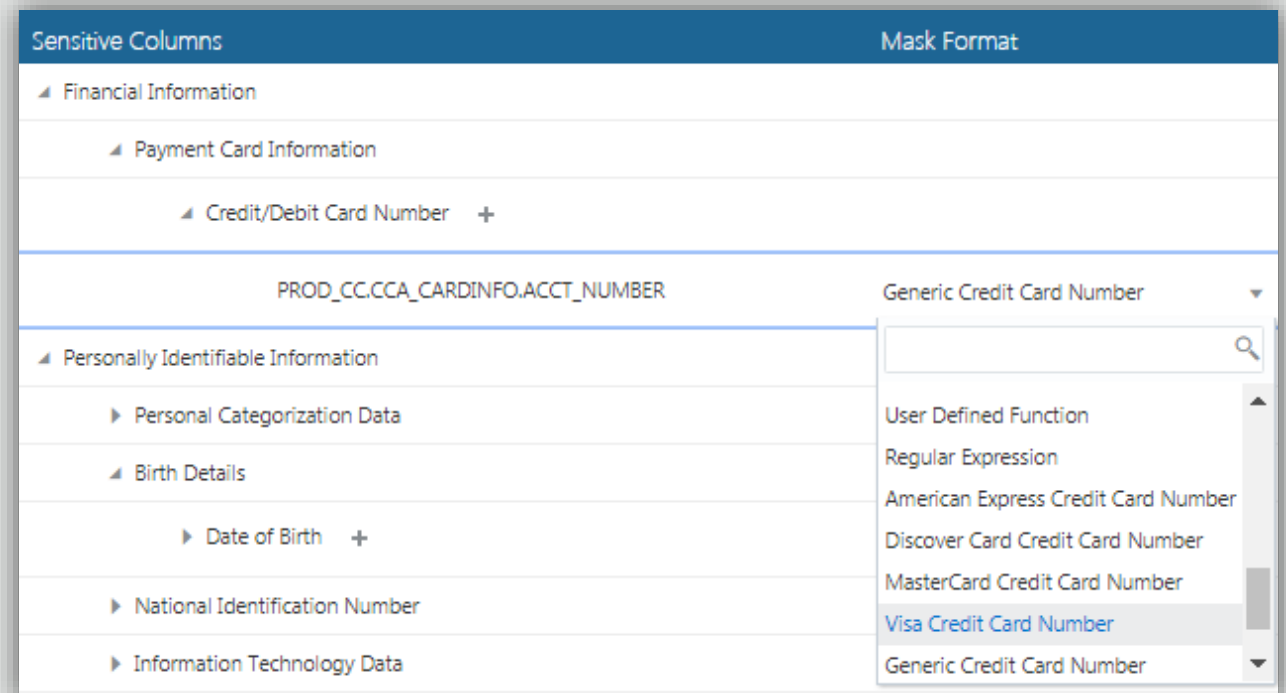


Sensitive Data Masking

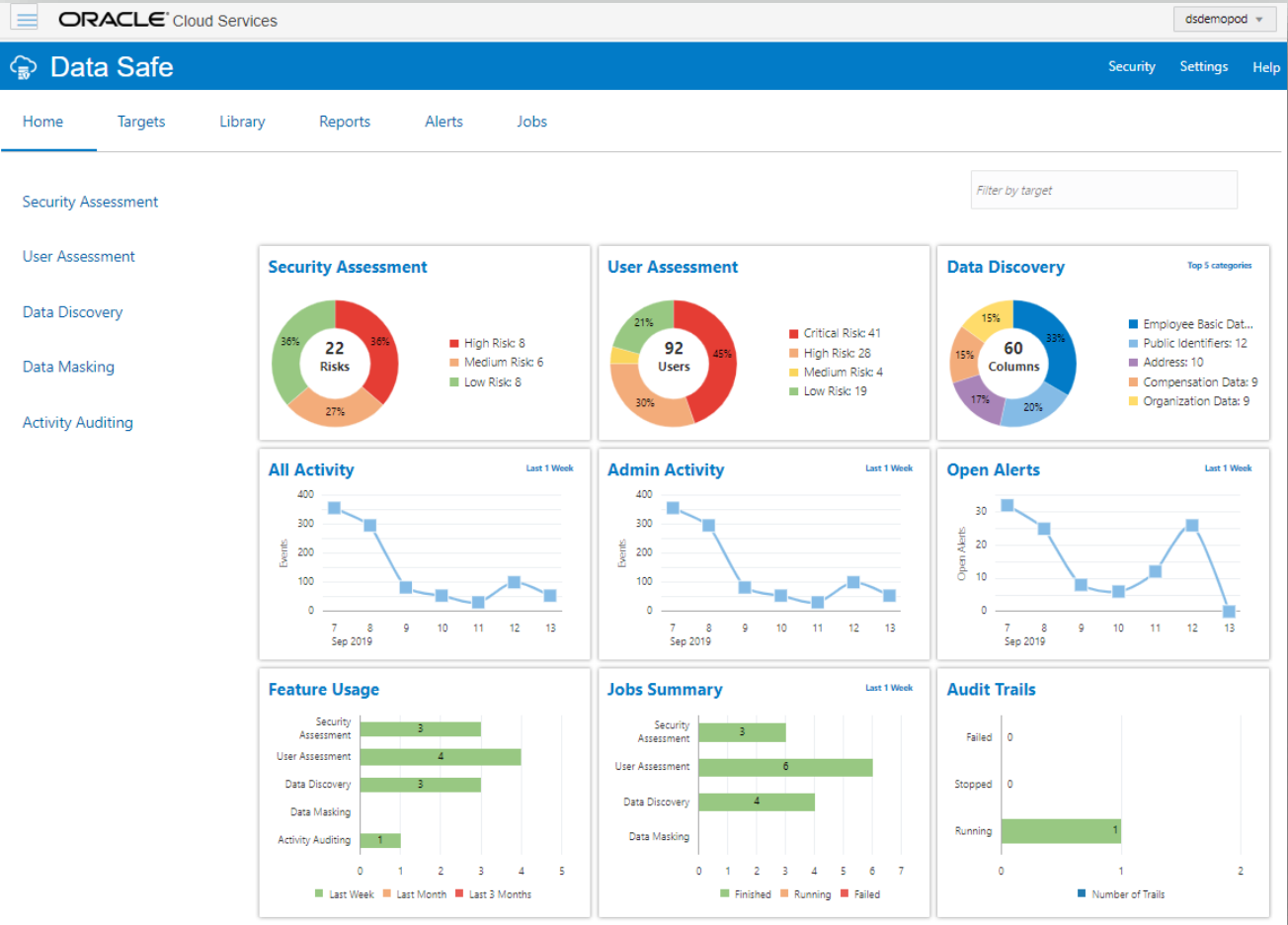


Minimize sensitive data exposure for dev & test, partners, analytics databases

- Mask data identified as sensitive
 - 50+ predefined masking formats
 - Automated format selection based upon sensitive type
 - Optional user-defined masking formats
- Rich masking transformations for complex cases
- Masking report



Demo



Getting Started with Data Safe in 15 Minutes

Enable Data Safe

Enable Data Safe for your region through the OCI console



Register a database

Register a database instance through the Autonomous Database Information page



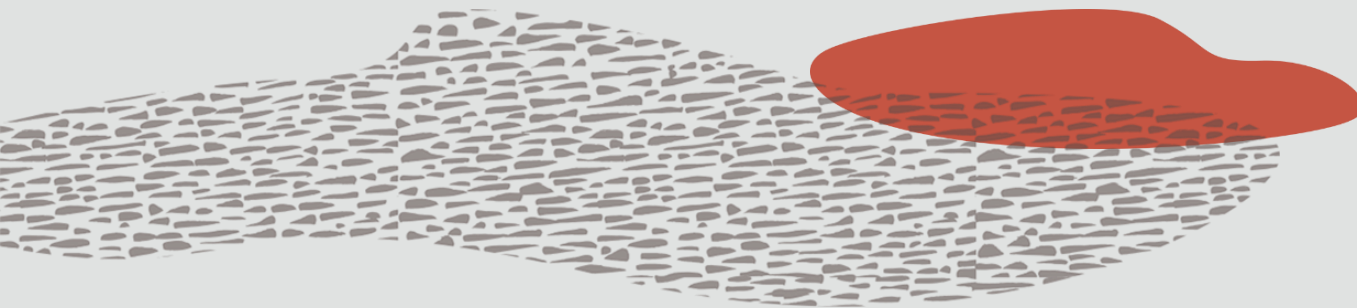
Access the console

Add role memberships and log on to the Data Safe console



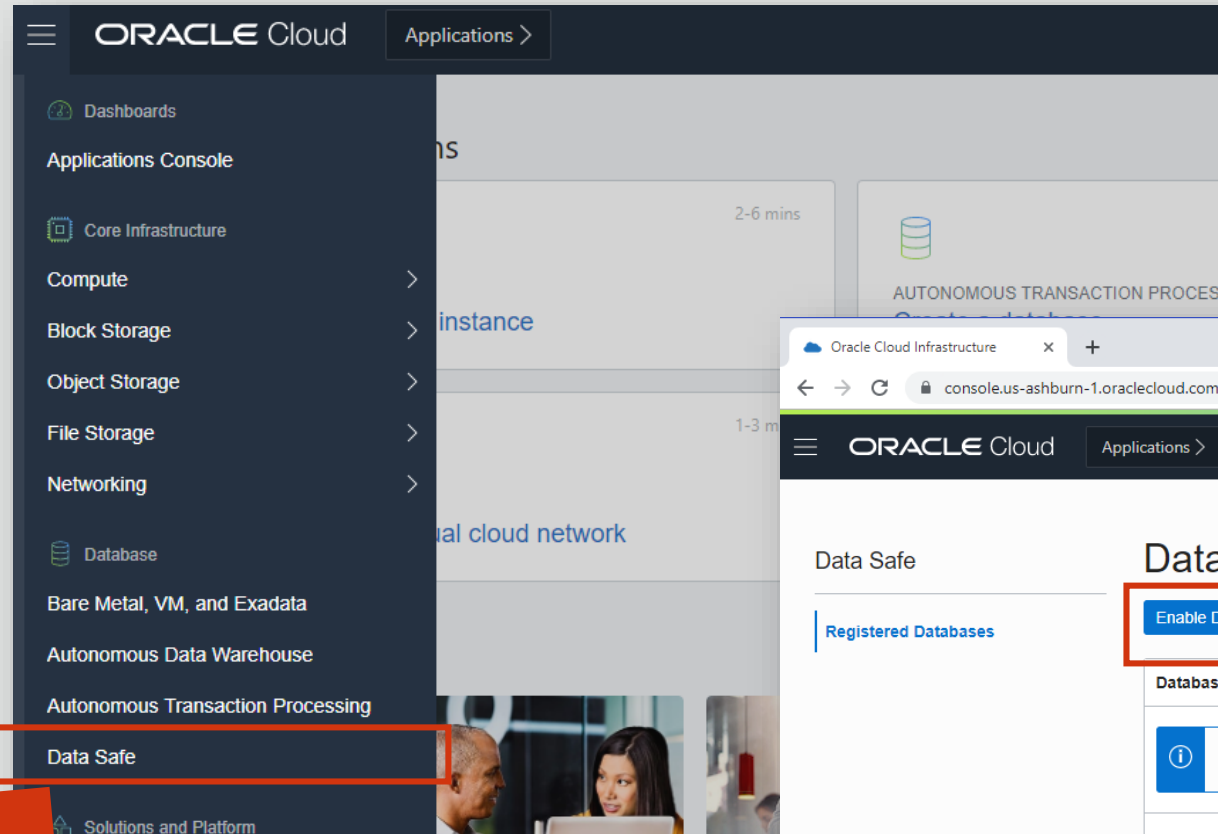
Run an assessment

Run your first assessment against a registered target database and view the results

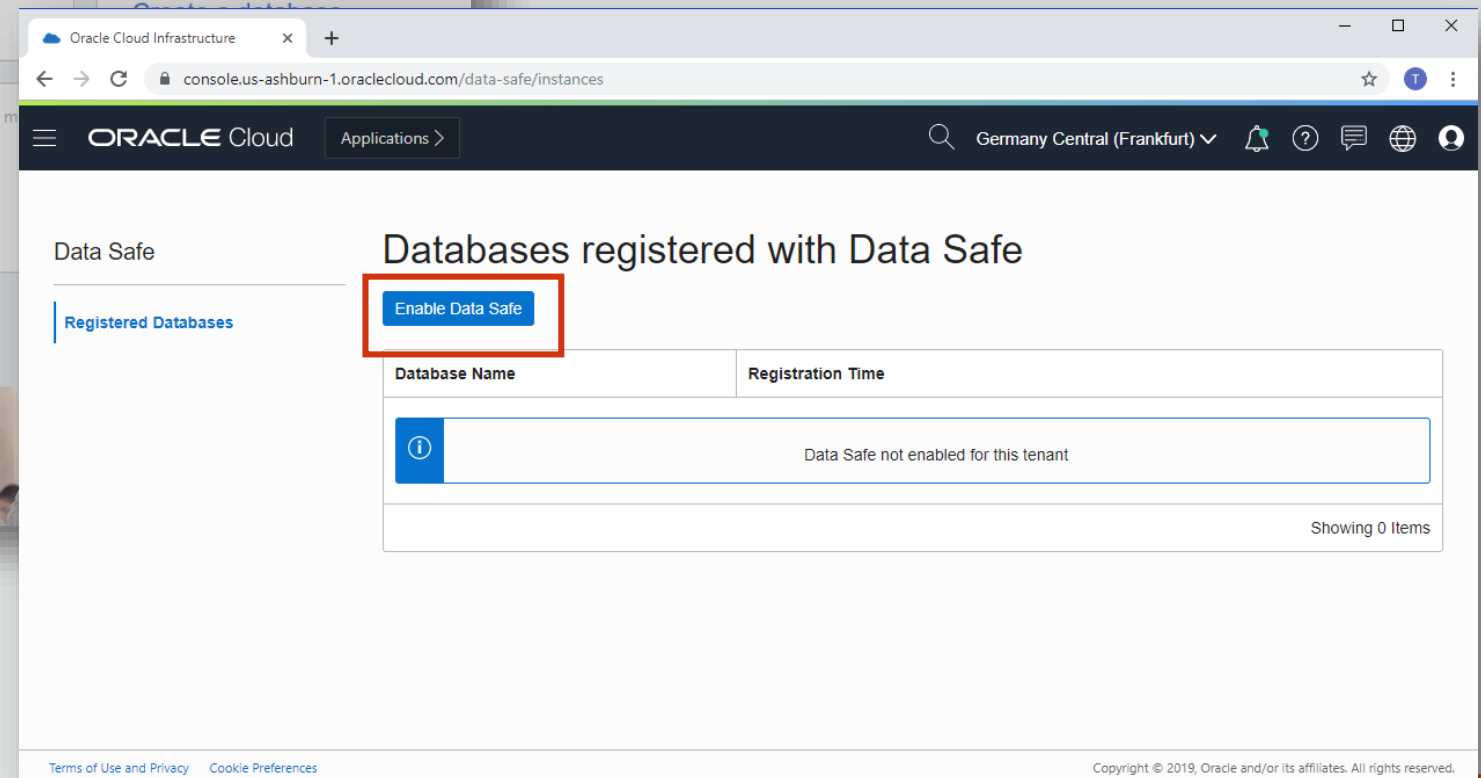


Enable Data Safe > Register a database > Access the Data Safe Console > Run an assessment

2 Press the Enable Data Safe button



1 Select Data Safe in the OCI menu under Database → Data Safe



Enable Data Safe



Register a database

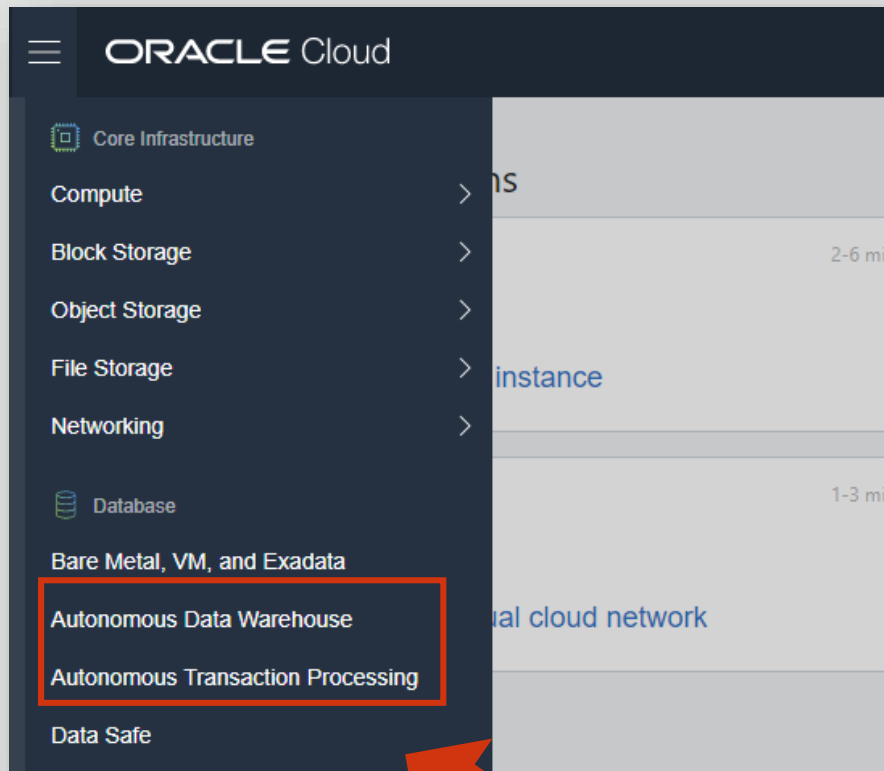


Access the Data Safe Console

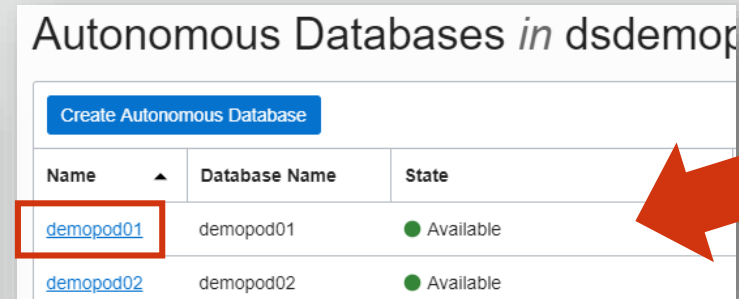


Run an assessment

ATP/ADW

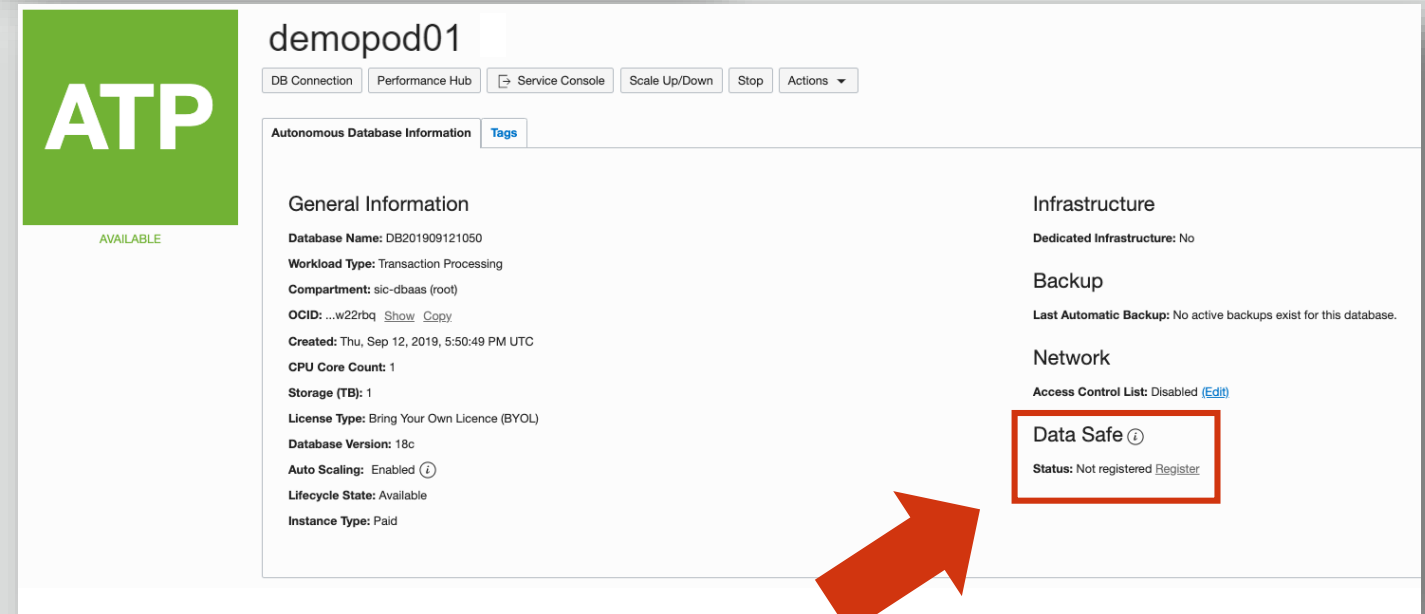


1 In the OCI menu select
Database → Autonomous Transaction Processing /
Autonomous Data Warehouse



2

Select your database



3

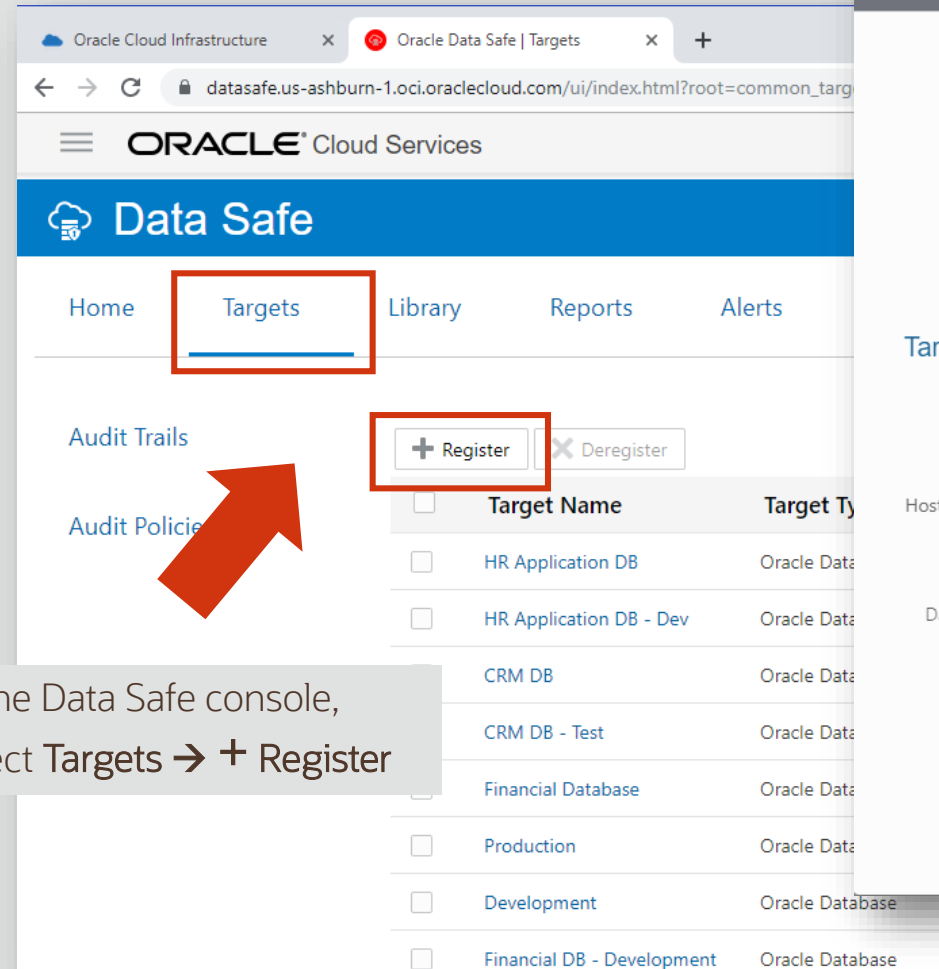
Press the register button under
Data Safe → Register*

Enable Data Safe > Register a database > Access the Data Safe Console > Run an assessment

Other Cloud DBs

1

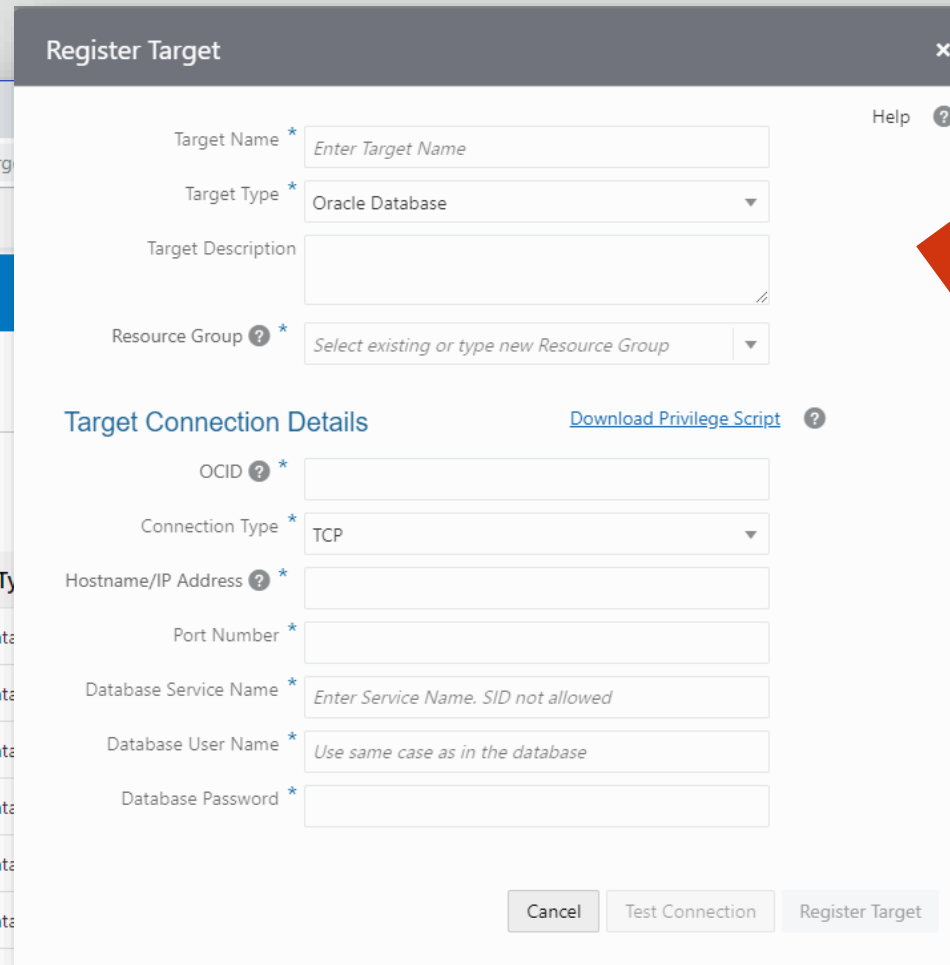
In the Data Safe console, select Targets → + Register



The screenshot shows the Oracle Data Safe console interface. The 'Targets' tab is selected and highlighted with a red box. Below the navigation bar, the '+ Register' button is also highlighted with a red box. A red arrow points from the text 'select Targets → + Register' to the '+ Register' button. The background shows a list of existing targets, including 'HR Application DB', 'HR Application DB - Dev', 'CRM DB', 'CRM DB - Test', 'Financial Database', 'Production', 'Development', and 'Financial DB - Development'.

2

Fill out the connection details



The screenshot shows the 'Register Target' dialog box. The 'Target Name' field is set to 'Enter Target Name'. The 'Target Type' dropdown is set to 'Oracle Database'. The 'Target Description' field is empty. The 'Resource Group' dropdown is set to 'Select existing or type new Resource Group'. The 'Target Connection Details' section includes fields for 'OCID', 'Connection Type' (set to 'TCP'), 'Hostname/IP Address', 'Port Number', 'Database Service Name' (set to 'Enter Service Name. SID not allowed'), 'Database User Name' (set to 'Use same case as in the database'), and 'Database Password'. The 'Download Privilege Script' link is visible. At the bottom, there are 'Cancel', 'Test Connection', and 'Register Target' buttons. A red arrow points from the text 'Fill out the connection details' to the 'Target Connection Details' section.

Enable Data Safe



Register a database

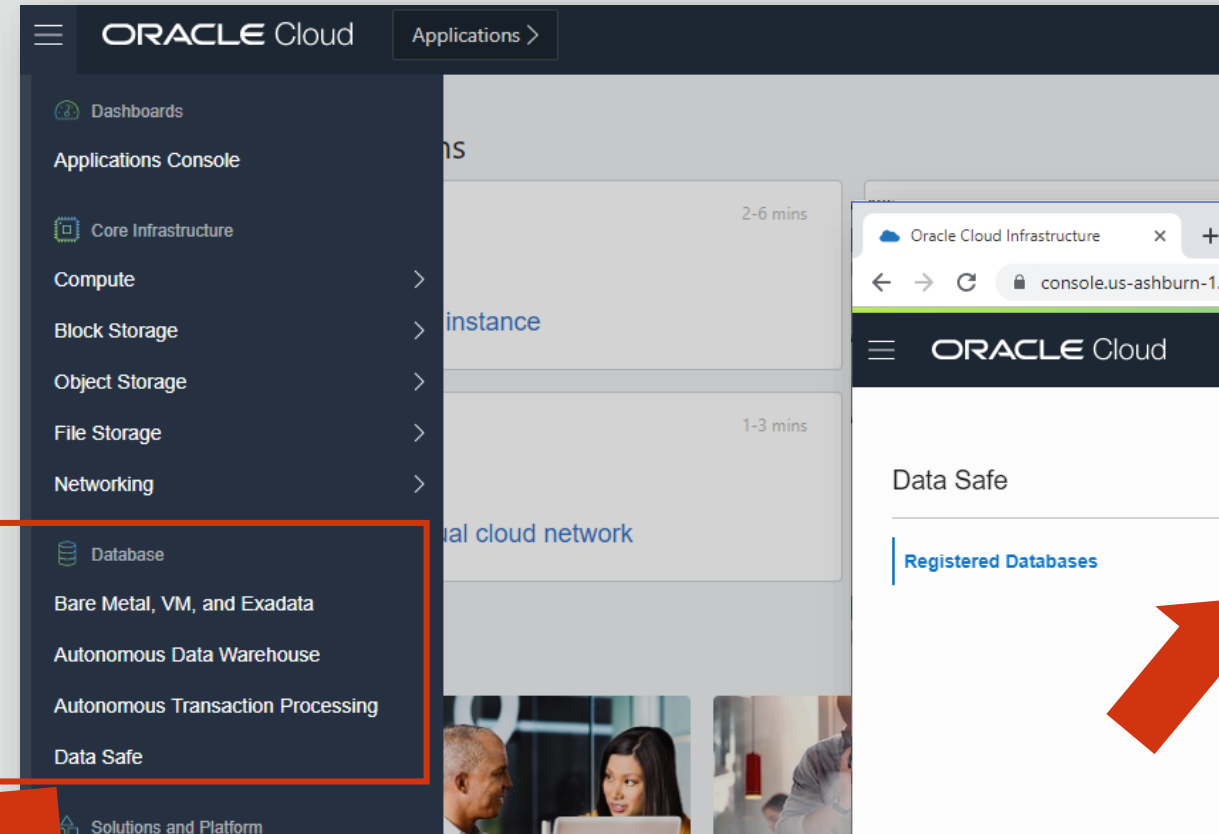


Access the Data Safe Console

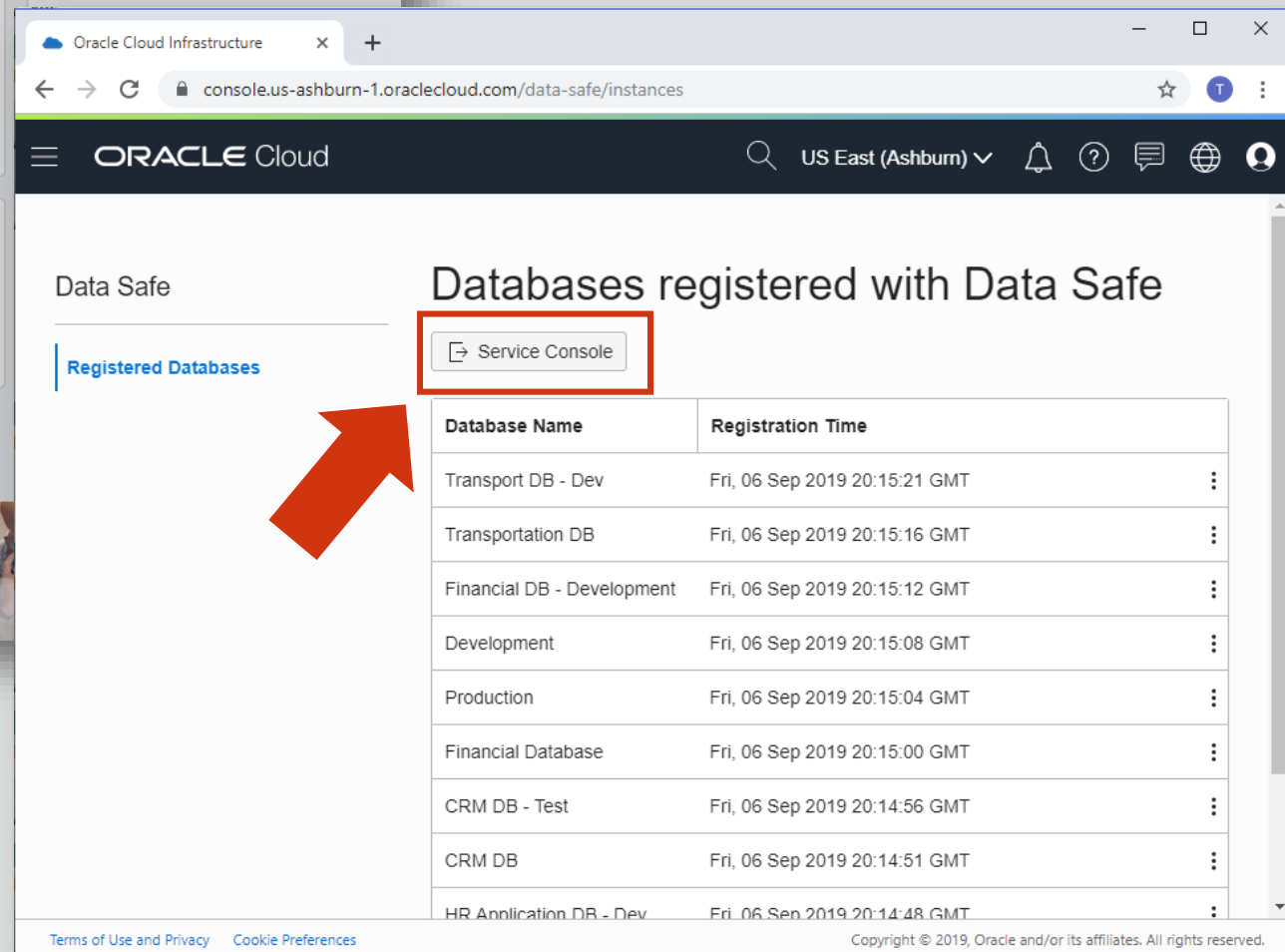


Run an assessment

2 Press the Service Console button



1 Select Data Safe in the OCI menu under Database → Data Safe



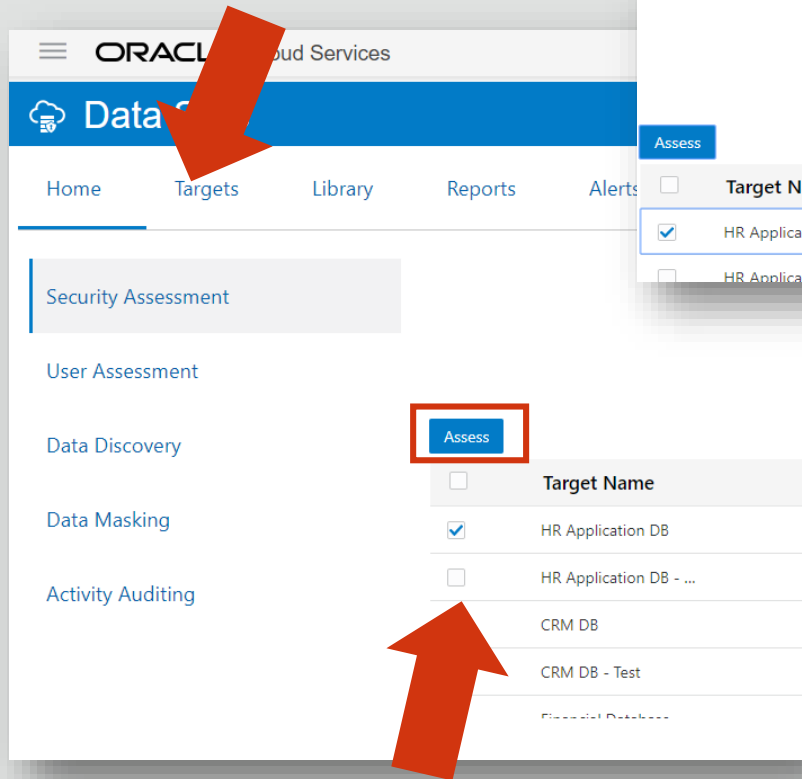
Enable Data Safe

Register a database

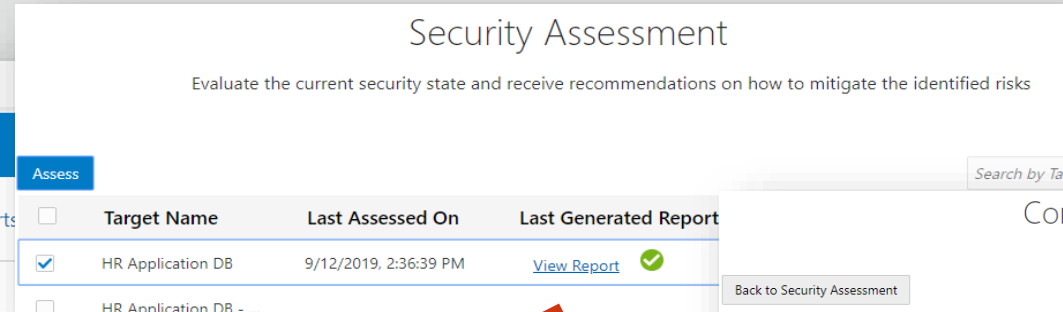
Access the Data Safe Console

Run an assessment

1 Select Security Assessment in the Data Safe Console

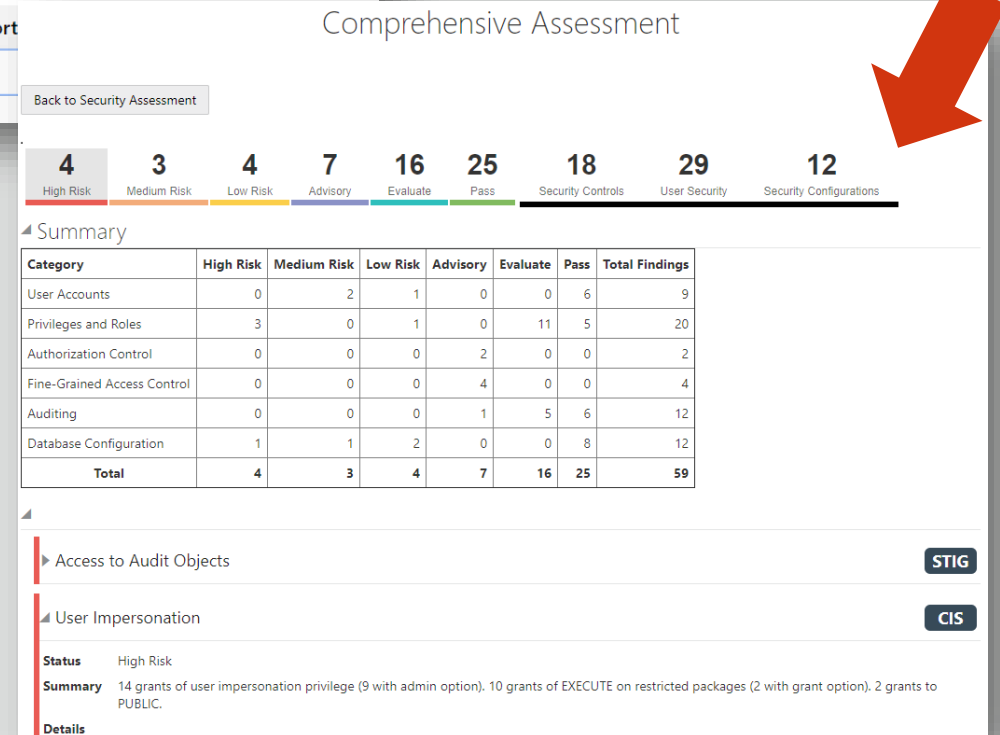


2 Select the target database and press the Assess button



3 Select View Report

4 Analyze the Report and remediate the risks



Summary: Oracle Data Safe

Simplified security management for cloud customers

Immediate visibility into risks with data, users, and configuration

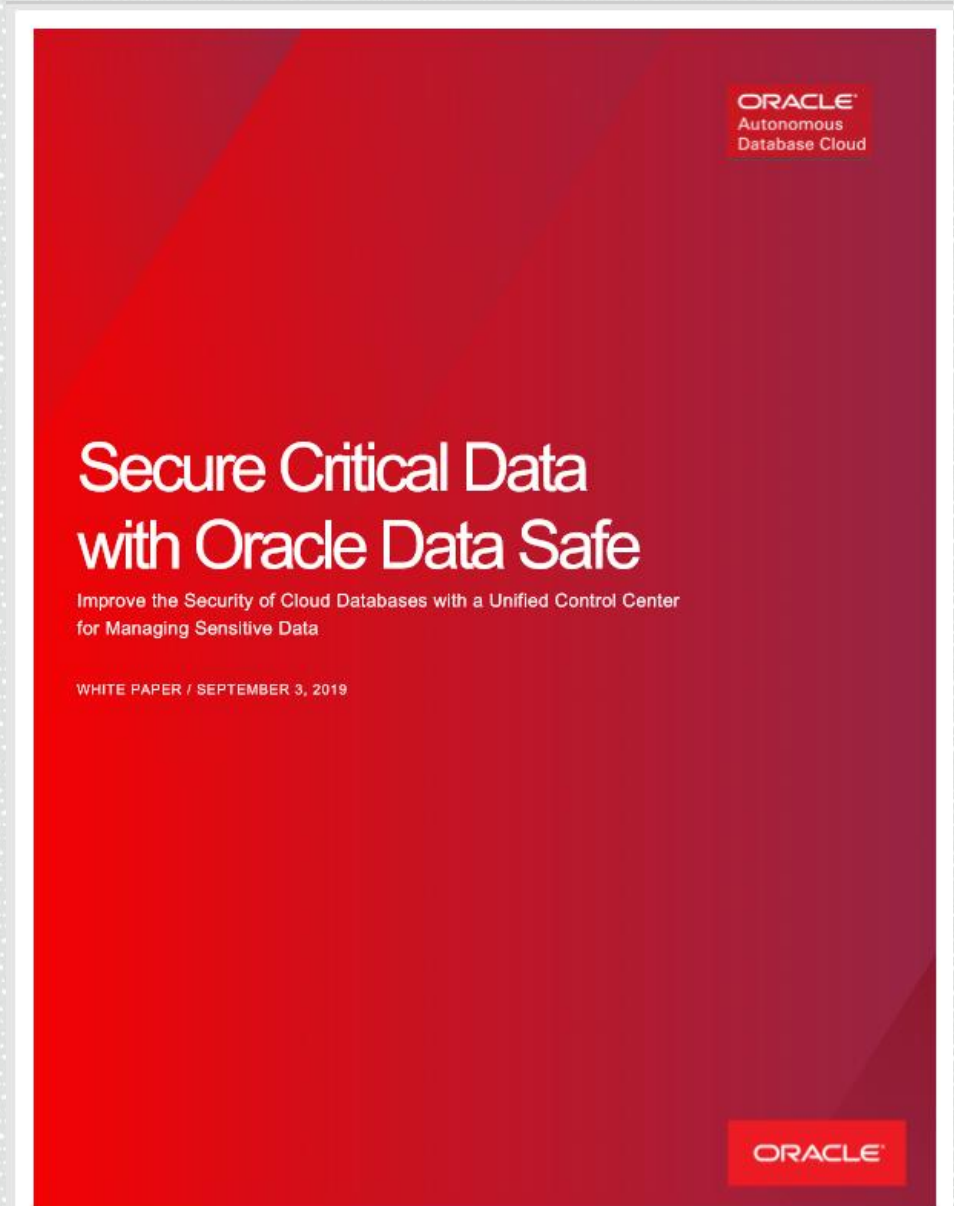
Easy-to-use single security control center - no special expertise needed

Leverage the most complete set of proven database security capabilities

More Information



- Check out the Oracle Data Safe White Paper:
<https://www.oracle.com/database/technologies/security.html>



Thank You

Bettina Schäumer

Senior Principal Product Manager
Oracle Database Security

Bettina.Schaeumer@oracle.com

Securing the Oracle Database

Third Edition

Oracle Database Security Team

URL: <https://oracle.com/securingthedatabase>



Database Security Office Hours

Direct line into Database Security PM

Second Thursday of every month, 09:00 and 20:00 UTC (identical sessions)

URL: <http://bit.ly/asktomdbsec>

*Or, just search
AskTom Database Security Office Hours*



Safe Harbor

The preceding 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.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at <http://www.oracle.com/investor>. All information in this presentation is current as of September 2019 and Oracle undertakes no duty to update any statement in light of new information or future events.