



ORACLE



Data Safe

L100

Sanjay Narvekar
Oracle Cloud Infrastructure
October 2019

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.

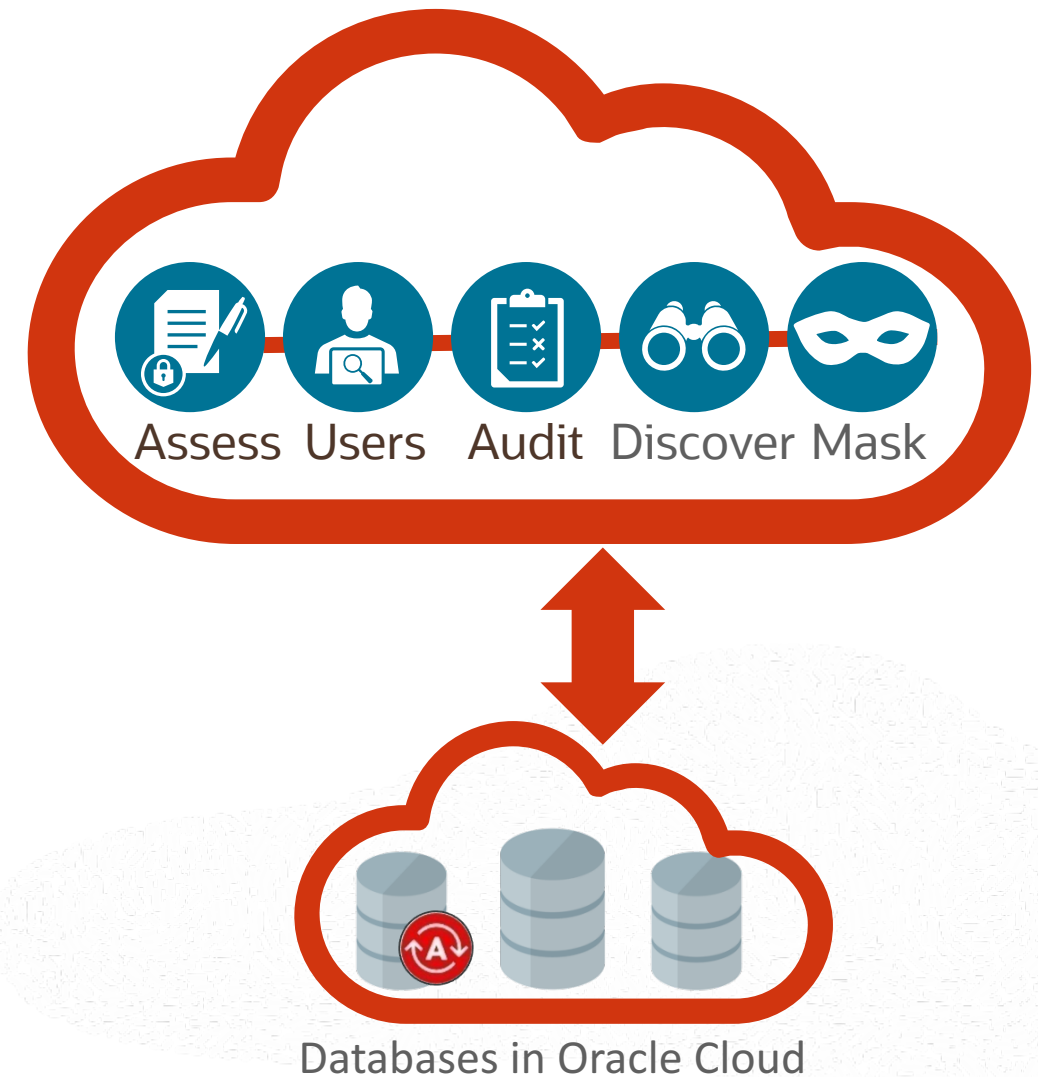
The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Objectives

- 1 Introduction to Data Safe
- 2 Security Assessment
- 3 User Assessment
- 4 Data Discovery
- 5 Data Masking
- 6 Activity Auditing

Introduction to 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



Security Assessment

Instant feedback on configurations that may introduce unnecessary risk

Security Assessment helps you to assess the security of your Oracle database configurations.

In Oracle Data Safe, Security Assessment analyzes your database configurations, user accounts, and security controls, and then reports findings with recommendations for remediation activities that follow best practices to reduce or mitigate risk.

Security Assessment generates four reports.

Report Name	Description
Comprehensive Assessments	Includes all findings for user accounts, privileges and roles, authorization control, data encryption, fine-grained access control, auditing, and database configuration
Security Controls	Filters findings based on various security controls
User Security	Filters findings based on users, privileges, and roles in the database
Security Configurations	Filters findings based on security-related configuration details

Security Assessment

The workflow for assessing your database security with Security Assessment is as follows:

1. If the target database that you want to assess is not yet registered in Oracle Data Safe, register it on the Targets tab.
2. Create a Security Assessment job against your target database by using Security Assessment wizard. You can assess multiple target databases at the same time.
3. Analyze the results in the following Security Assessment reports:
 - Comprehensive Assessments
 - Security Controls
 - User Security
 - Security Configurations

Security Assessment Demo

User Assessment

Reduce user risk by managing roles/privileges and policies

Over-privileged users are frequently targeted by cyber attackers to leverage their extensive set of privileges to mount data attacks.

User Assessment helps you assess the security of your database users and identify high risk users. This allows administrators apply appropriate security controls.

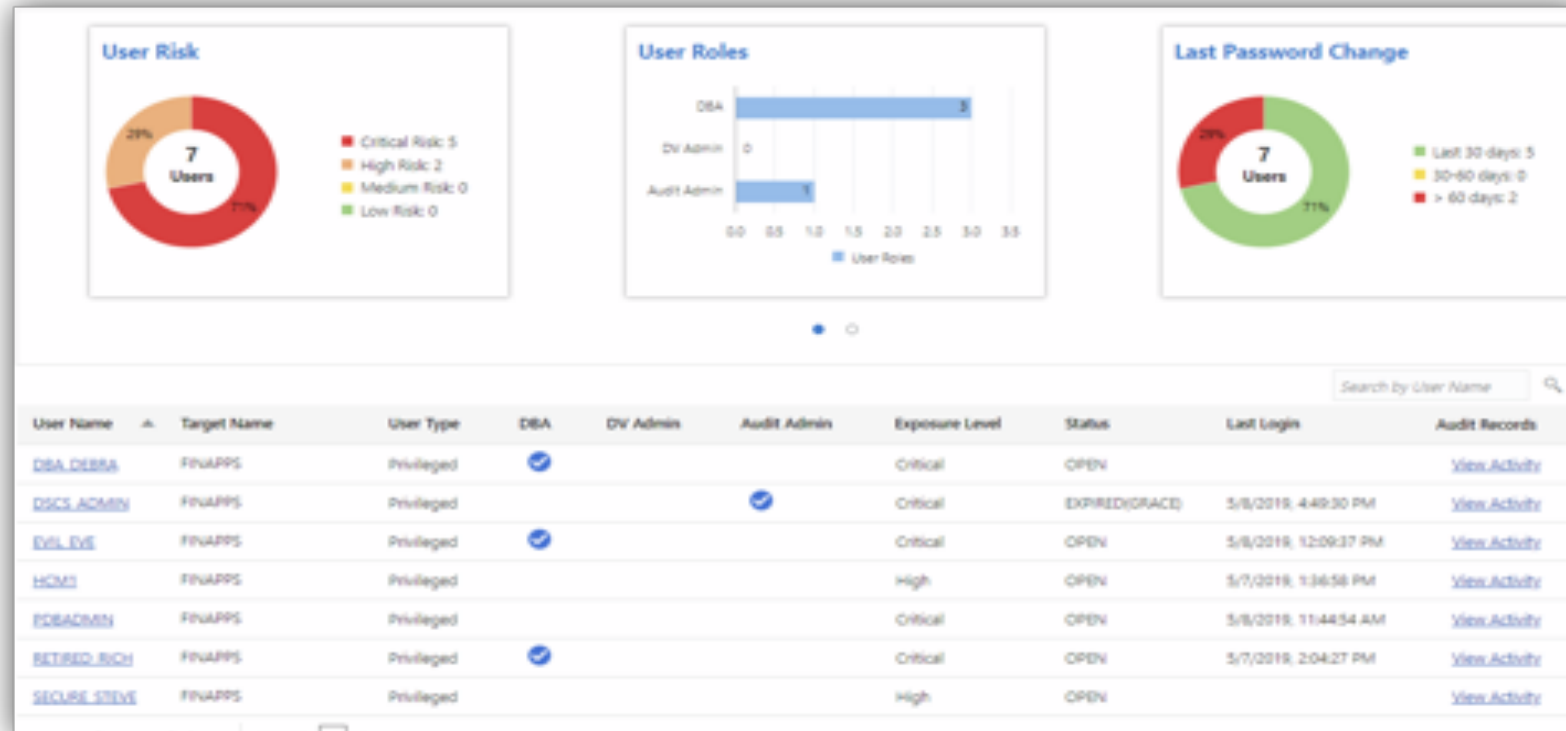
User Assessment reviews information about your users in the data dictionaries on your target databases, and then calculates a risk score for each user.

For example, it evaluates the user types, how users are authenticated, the password policies assigned to each user, and how long it has been since each user has changed their password.

With this information, you can decide whether to implement more restrictive password policies, use Oracle Database Vault, or do something to further limit user access, if needed.

User Assessment

Reduce user risk by managing roles/privileges and policies



User Assessment

The workflow for assessing your database security with User Assessment is as follows:

1. If the target database that you want to assess is not yet registered in Oracle Data Safe, register it on the Targets tab.
2. Create a User Assessment job against your target databases by using the User Assessment wizard.
3. Analyze the results in the User Assessment report. In the report, you can choose to view the audit records for individual user accounts.

User Assessment Demo

Activity Auditing

Track user actions and streamline auditing with robust reporting

The Activity Auditing feature lets you audit user activity on your Oracle Cloud databases so that you can monitor database usage and be alerted of unusual database activities.

- 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

Activity Auditing

The general workflow for setting up Activity Auditing involves these main steps:

1. Select the targets you want to audit.
2. Provision audit policies specifying what audit information will be collected
3. Create audit trails that tell Data Safe from where to collect audit information.

Once this is done, Data Safe automatically retrieves audit data and stores it in the secure Data Safe repository (separate from the database being monitored so it can't be deleted or altered).

You can setup alerts on key events based on the predefined set of alerts available in Data Safe Activity Auditing.

Interactive reports allow you to look at audit data, filter it as needed, and create scheduled reports to meet your security and compliance needs.

Activity Auditing Demo

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

Data Discovery

125+ Pre-defined Sensitive Types



Identification

Biographic

IT

Financial

Healthcare

Employment

Academic

SSN	Age	IP Address	Credit Card	Provider	Employee ID	College Name
Name	Gender	User ID	CC Security	Insurance	Job Title	Grade
Email	Race	Password	PIN	Height	Department	Student ID
Phone	Citizenship	Hostname	Bank Name	Blood Type	Hire Date	Financial Aid
Passport	Address	GPS location	Bank Account	Disability	Income	Admission
DL	Family Data	...	IBAN	Pregnancy	Stock	Date
Tax ID	Date of Birth		Swift Code	Test Results	...	Graduation
...	Place of Birth		...	ICD Code		Date
		Attendance
						...

Data Discovery

The general workflow for Data Discovery involves these main steps:

1. Register the target database in which you want to discover sensitive data.
2. Create a data discovery job using the Data Discovery wizard to discover the sensitive data on the target database and generate a sensitive data model (SDM)
3. Analyze your sensitive data in the target database by viewing the Data Discovery report.
4. Manage the SDM

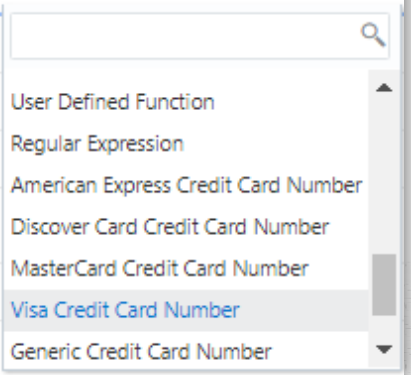
Data Discovery Demo

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

Sensitive Columns	Mask Format
Financial Information	
Payment Card Information	
Credit/Debit Card Number +	
PROD_CC.CCA_CARDINFO.ACCT_NUMBER	Generic Credit Card Number
Personally Identifiable Information	
Personal Categorization Data	
Birth Details	
Date of Birth +	
National Identification Number	
Information Technology Data	



Data Masking

The general workflow for Data Masking involves these main steps:

1. Create a backup of your production database. **This step is very important.**
2. Clone the backup of your production database to create a stage database. Do not expose the stage database to users. Create the stage database on the Oracle Cloud with supported services.
3. Register your stage database with Oracle Data Safe. Be sure to run the SQL privileges script on your stage database beforehand.
4. Use the Data Discovery wizard to discover sensitive data on the stage database and generate a sensitive data model (SDM).
5. Create new masking formats in the Library if you require masking formats other than the predefined ones.
6. Use the Data Masking wizard to create a masking policy and submit a data masking job.
7. Verify the masked data by reviewing the Data Masking report and validating data in the masked columns.
8. Clone the stage database to create a test database.
9. Grant your test and developer users access to your test database.

Data Masking Demo

Summary

- Simplified security management for cloud customers
- Complements existing infrastructure security with a single security control center for cloud databases
 - Easy-to-use service: click-and-secure
 - Immediate visibility into risks with data, users, and configuration
 - Leverage the most complete set of proven database security capabilities

Oracle Cloud always free tier:

[oracle.com/cloud/free/](https://www.oracle.com/cloud/free/)

OCI training and certification:

<https://www.oracle.com/cloud/iaas/training/>

<https://www.oracle.com/cloud/iaas/training/certification.html>

OCI hands-on labs:

ocitraining.qcloudable.com/provider/oracle

Oracle learning library videos on YouTube:

youtube.com/user/OracleLearning

