

ORACLE



Oracle Database Security

Be the CXM – Get Started Data Safe

Marcel Lamarca

Exadata Cloud Specialist

Oracle, Alliances and Channels LAD

April, 2024



SQL> select * from person where name = 'Marcel Lamarca'




MARCEL LAMARCA

Exadata Cloud Specialist

Upgrade, Utilities, Patching, Performance & Migrations

 [marcel-lamarca](#)

 marcel.lamarca@oracle.com

About My Career

- 22 Years dedicated to study and support Oracle Databases.
- 12 Years working with Exadata (On-prem, C@C and Cloud Services) .
- 5 Year working for Oracle do Brasil
- 2 Year on Alliances LAD knowledge Team

Certifications

Oracle Cloud Specialist (OCS)

- Exadata Database Machine X9M Certified Specialist
- OCI Foundation 2020 / 2023
- Oracle Autonomous Database Administrator Professional 2019 / 2023
- Oracle Cloud Database Migration and Integration 2021
- OCI Cloud Certified Architect Associate 2022
- OCI Cloud Certified Architect Professional 2022
- OCI Multi-Cloud Architect Professional 2023
- Oracle Database Services Certified Professional 2023

Oracle Certified Professional (OCP)

- Oracle Database certified professional 10g, 11g, 12c and 19c.
- Mysql 8.0 Database Administrator Certified Professional

Oracle Certified Specialist (OCE)

- Grid/RAC Database Administrator 11g
- Oracle Golden Gate 12c Certified Implementation Specialist



Agenda

- 1 Why Oracle Data Safe ?
- 2 Data Safe components
- 3 Data Safe database deploy options
- 4 Data safe demo
- 5 Resources

People are after your data !

Insiders

Nation States

Former Employees

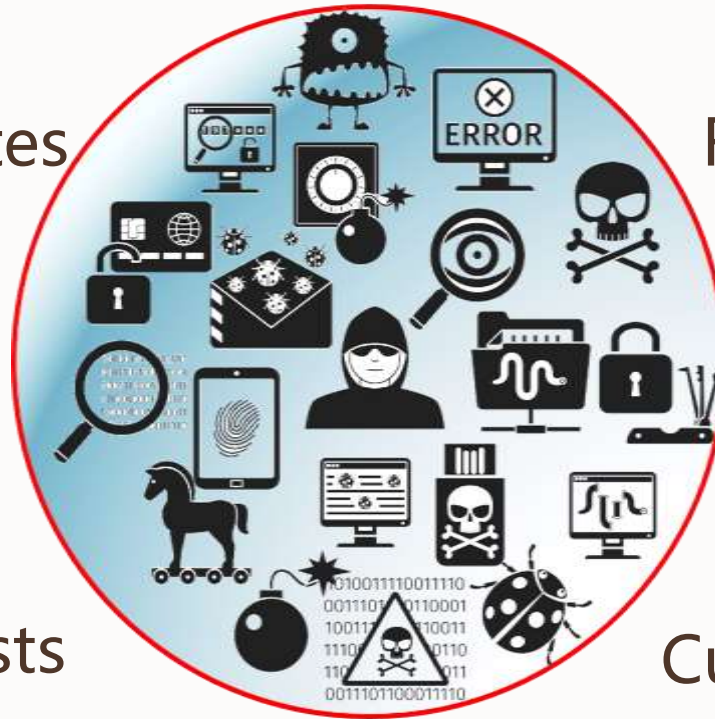
Criminals

Curiosity Seekers

Hacktivism

Customers

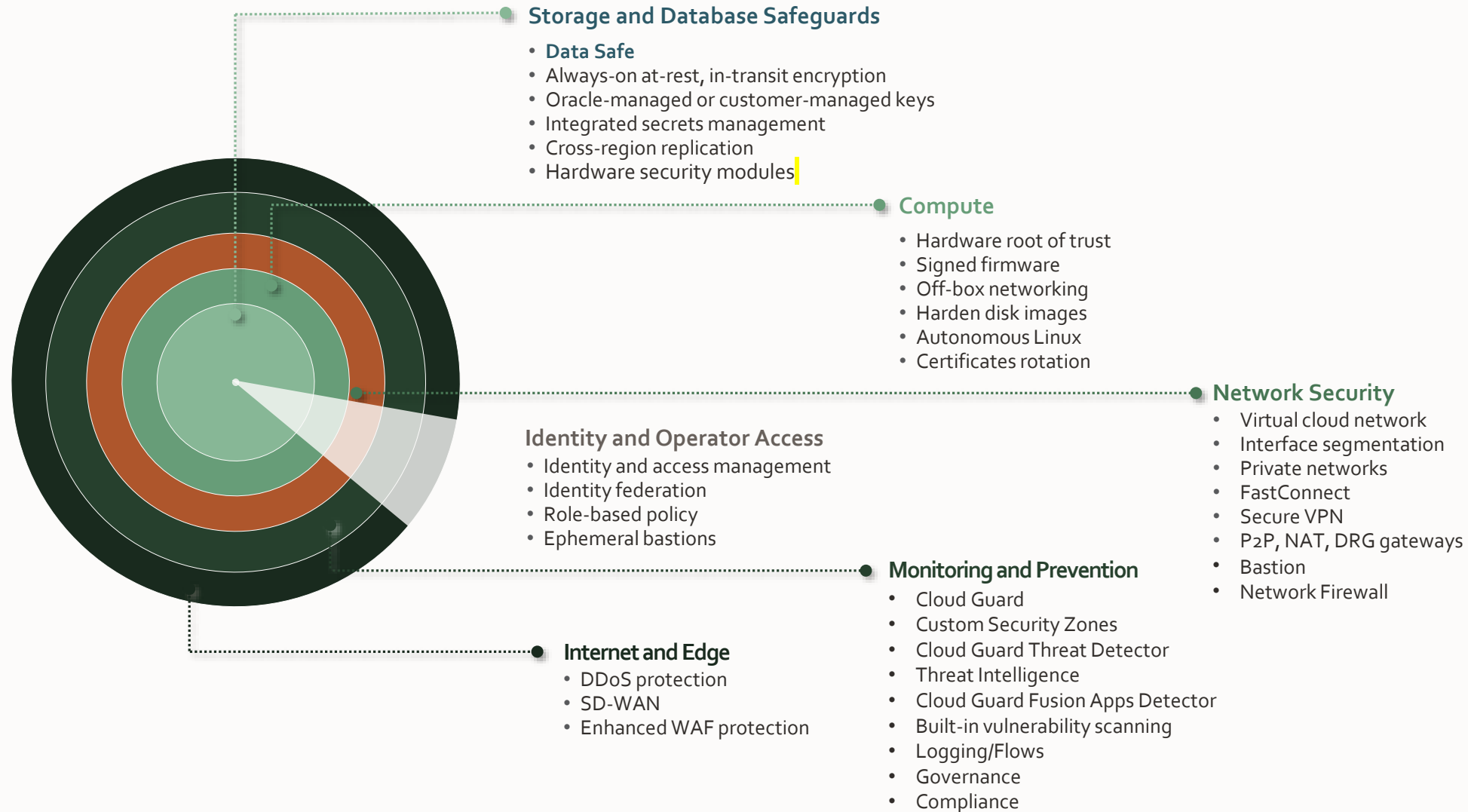
Competitors



Cyber attacks have been a reality for a long time!



Defense-in-depth, from data to the edge



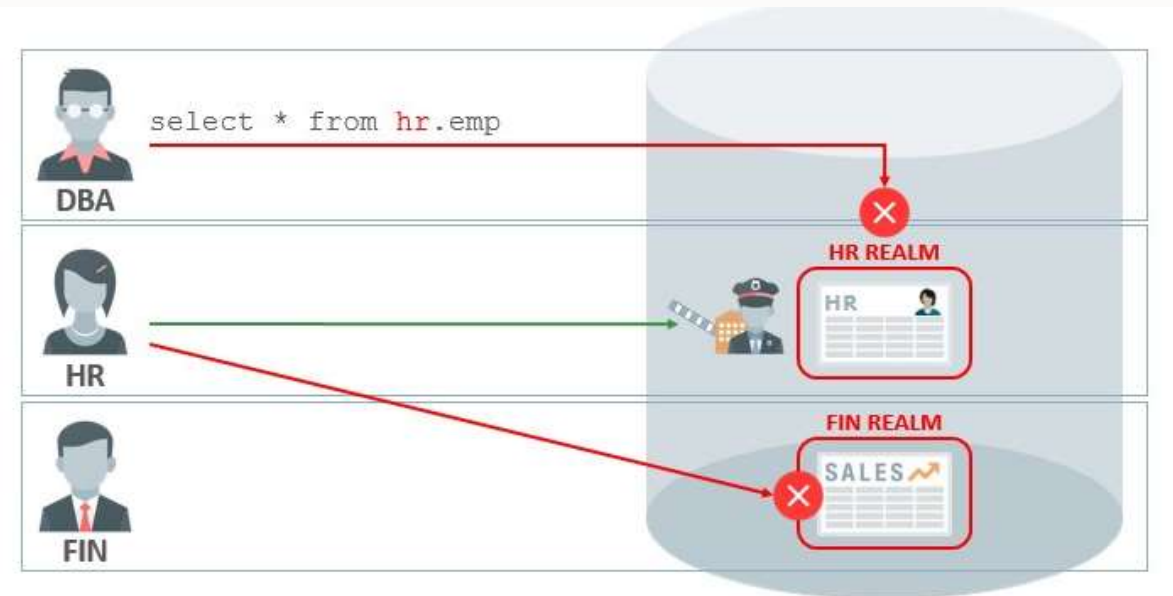


Database Audit Vault

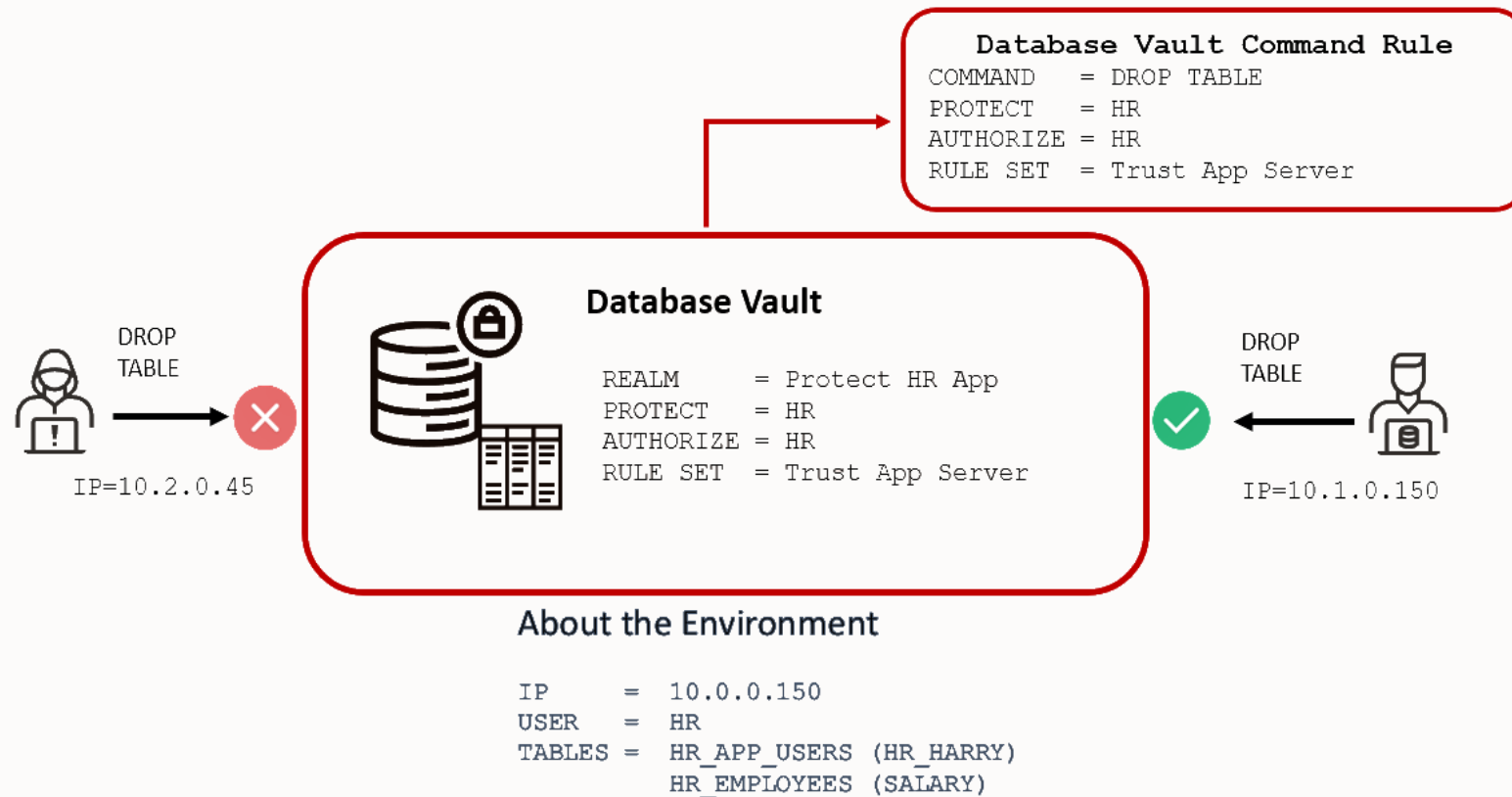


Oracle database Vault

- **Separation of duties**
 - Allow only security roles to manage users, profiles, and security controls while limiting admins to managing only the database.
- **Realms**
 - Block unauthorized access to sensitive data by creating restricted application environments within Oracle Database.
- **Command rules**
 - Block accidental or malicious changes to production databases attempted outside specific maintenance windows.
- **Trusted paths**
 - Use factors like client IP address, program, user name, and time of day to control access to data and data operations.

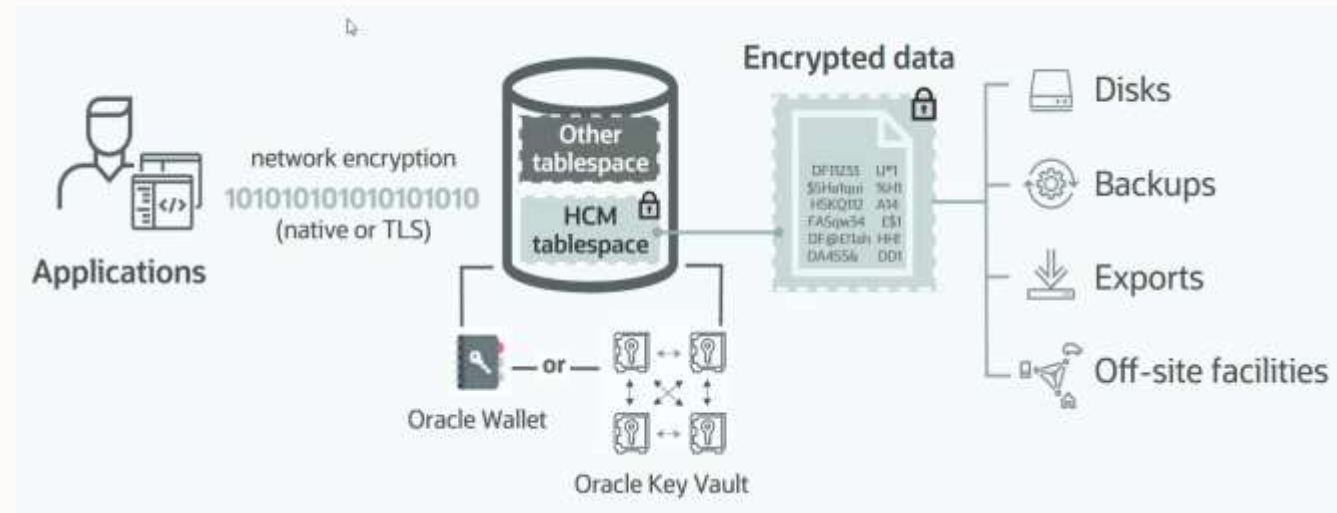


Control SQL commands with Oracle Database Vault

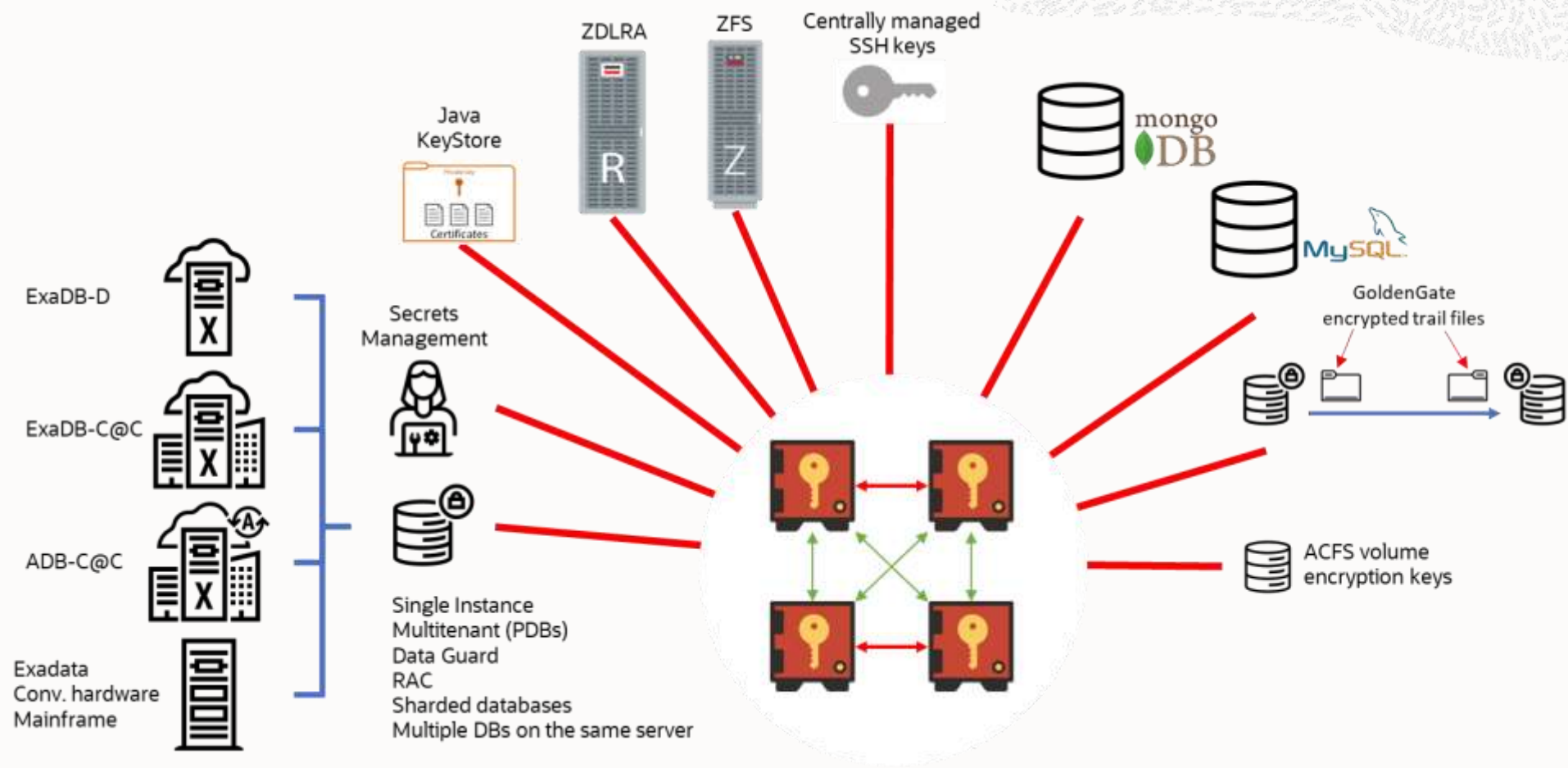


Oracle Advanced Security

- **Transparent Data Encryption**
 - Stop would-be attackers from bypassing the database and reading sensitive information directly from storage by enforcing data-at-rest encryption in the database layer.
- **Data redaction**
 - Reduce the risk of unauthorized data exposure in applications by redacting sensitive data before it leaves the database. Partial or full redaction prevents large-scale extraction of sensitive data
- **Transparent to applications**
 - Encryption is implemented at the database kernel level, eliminating the need for any changes to applications.



Centralized key management with Oracle Key Vault





Oracle Data Safe



Oracle Data Safe



Available for 23c databases only

Oracle Data Safe on OCI menu

The screenshot displays the Oracle Cloud console interface. At the top, the Oracle Cloud logo is on the left, followed by a 'Cloud Classic' button and a search bar. Below the logo is a search input field. On the left sidebar, a vertical menu lists various services: Home, Compute, Storage, Networking, **Oracle Database** (highlighted with a red dashed border), Databases, Analytics & AI, Developer Services, Identity & Security, and Observability & Management. The main content area is titled 'Oracle Database' and contains several sections: Overview, Autonomous Database (with sub-items: Autonomous Data Warehouse, Autonomous JSON Database, Autonomous Transaction Processing), Globally Distributed Autonomous Database, Autonomous Dedicated Infrastructure, Oracle Base Database Service, Oracle Exadata Database Service on Dedicated Infrastructure, Oracle Exadata Database Service on Cloud@Customer, Exadata Fleet Update, and External Database. On the right side, a red solid border highlights the 'Data Safe - Database Security' section, which includes sub-items: Overview, Security Assessment, User Assessment, Data Discovery, Data Masking, Activity Auditing, SQL Firewall, Database Backups, GoldenGate, and Operator Access Control.

Oracle Cloud Cloud Classic > Search resources, services, documentation, and Marketplace

Search

Home
Compute
Storage
Networking
Oracle Database
Databases
Analytics & AI
Developer Services
Identity & Security
Observability & Management

Oracle Database

Overview

Autonomous Database
Autonomous Data Warehouse
Autonomous JSON Database
Autonomous Transaction Processing

Globally Distributed Autonomous Database

Autonomous Dedicated Infrastructure

Oracle Base Database Service

Oracle Exadata Database Service on Dedicated Infrastructure

Oracle Exadata Database Service on Cloud@Customer

Exadata Fleet Update

External Database

Data Safe - Database Security
Overview
Security Assessment
User Assessment
Data Discovery
Data Masking
Activity Auditing
SQL Firewall

Database Backups

GoldenGate

Operator Access Control

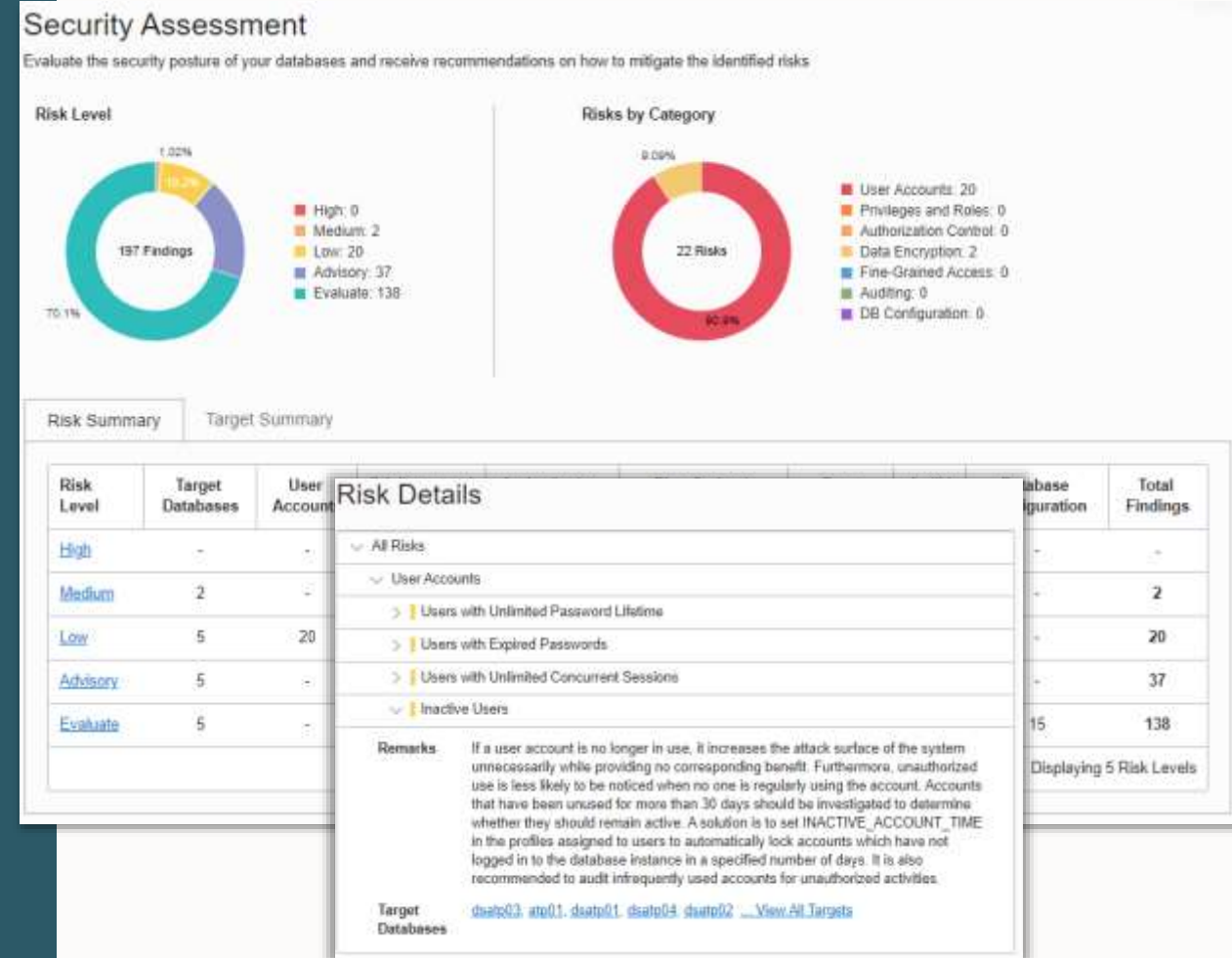
Database Security Assessment





Database Security Assessment

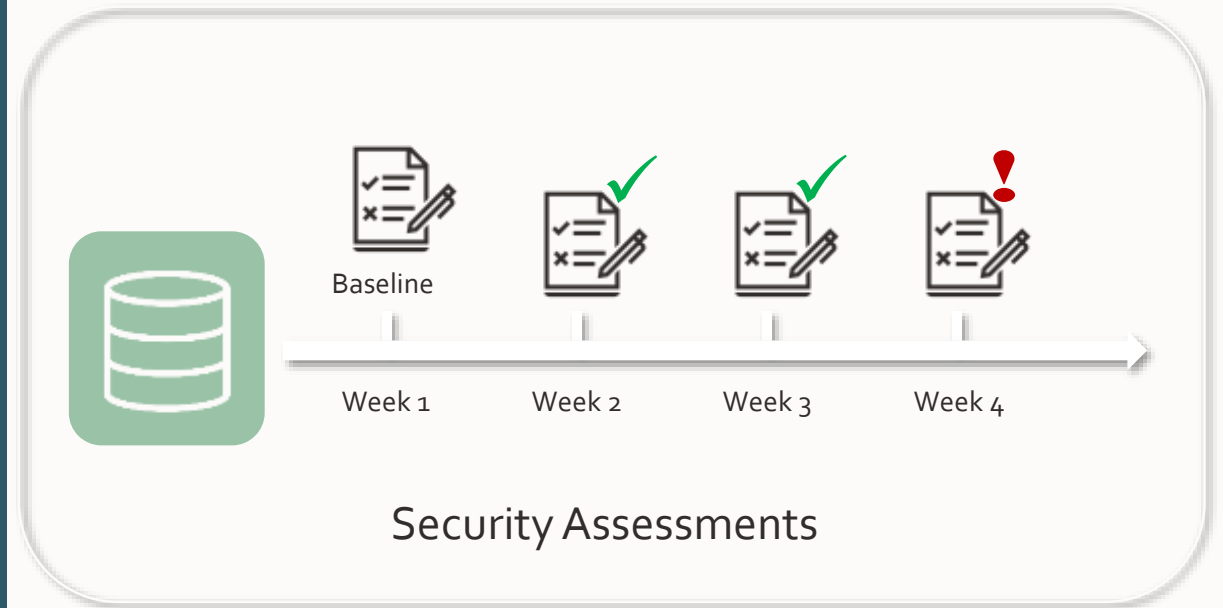
- Comprehensive assessment :
 - Security parameters
 - Security controls in use
 - User Roles and Privileges
- Landscape-wide view on identified risks and recommendations
- Compliance mappings (GDPR, STIG, CIS)





Database Security Assessment

- Establish a security baseline
- New assessments are automatically compared against the baseline
- Get notified and review any drift from your security baseline



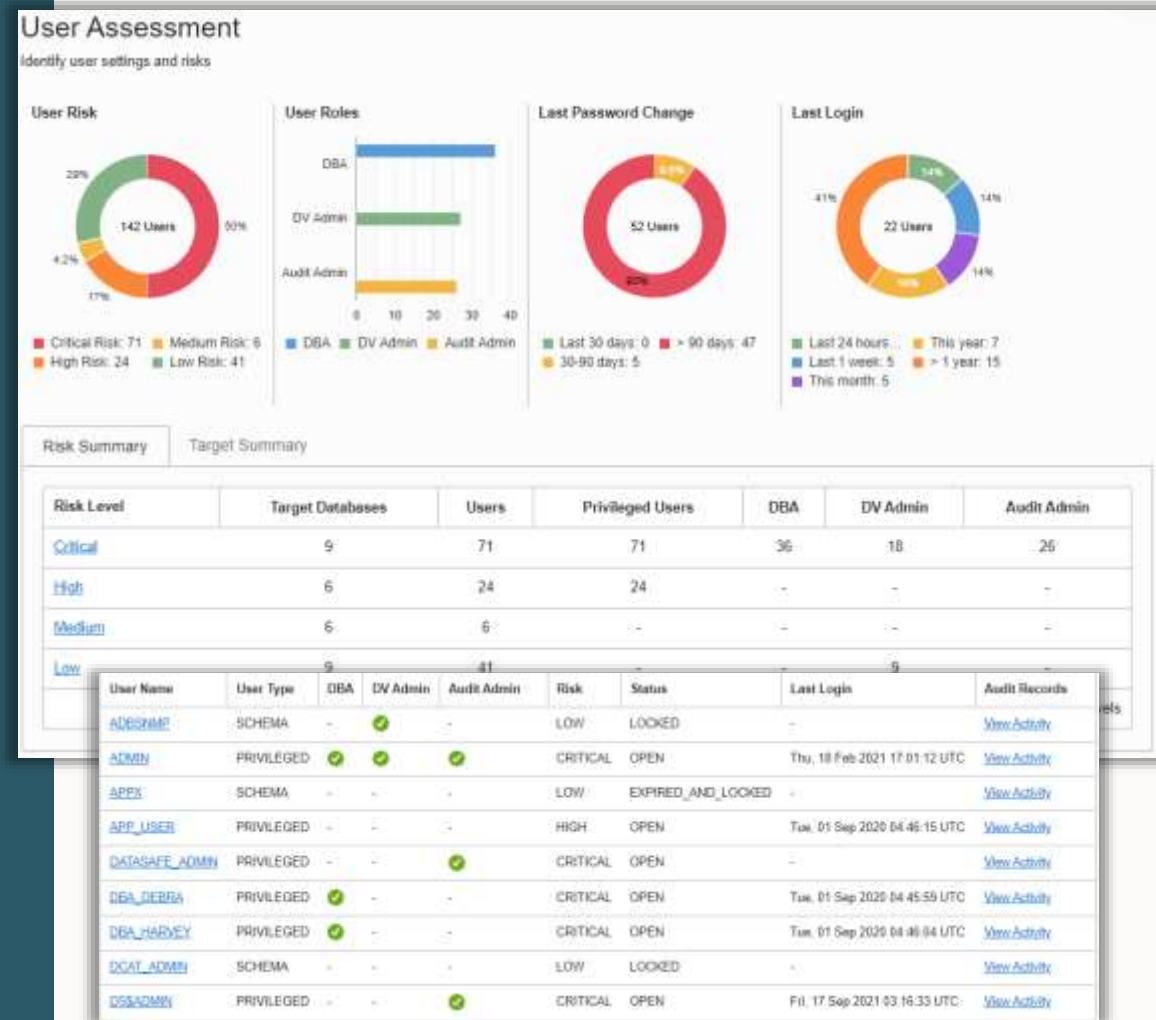
User Risk Assessment





User Risk Assessment

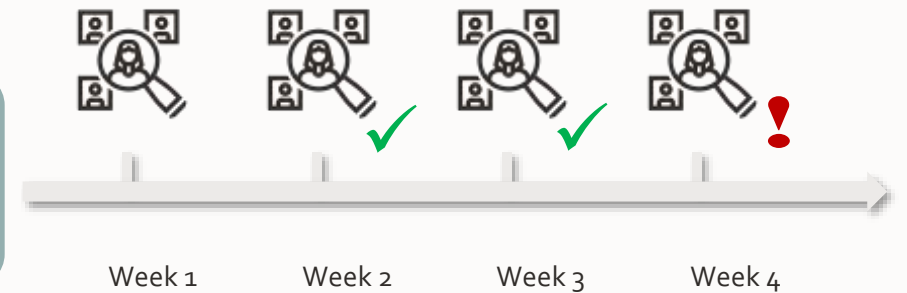
- Identify highly privileged users
- Review their roles and system privileges
- Evaluate user details like last login, password change, database activity
- Reduce risk from users by managing roles/privileges and policies





User Risk Assessment

- Run periodic user assessments
- Compare new assessments against previous assessments
- Get notified and identify newly added users or changed entitlements

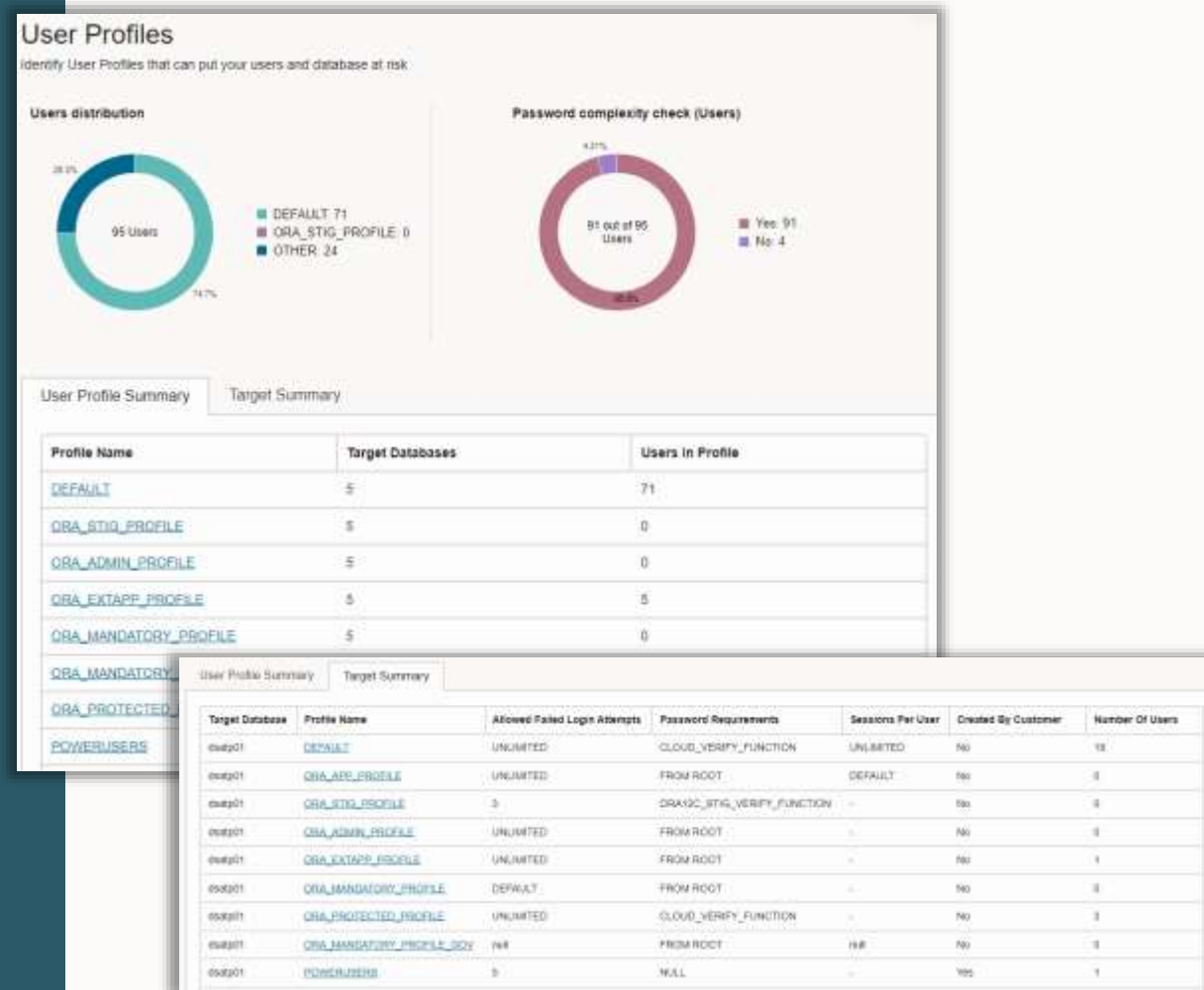


User Assessments



User Profile Insight

- Review existing user profiles and their parameters
- Identify which profiles are assigned to which users
- Easily identify users and profiles without a password complexity function
- Evaluate password-related attributes associated with user profiles



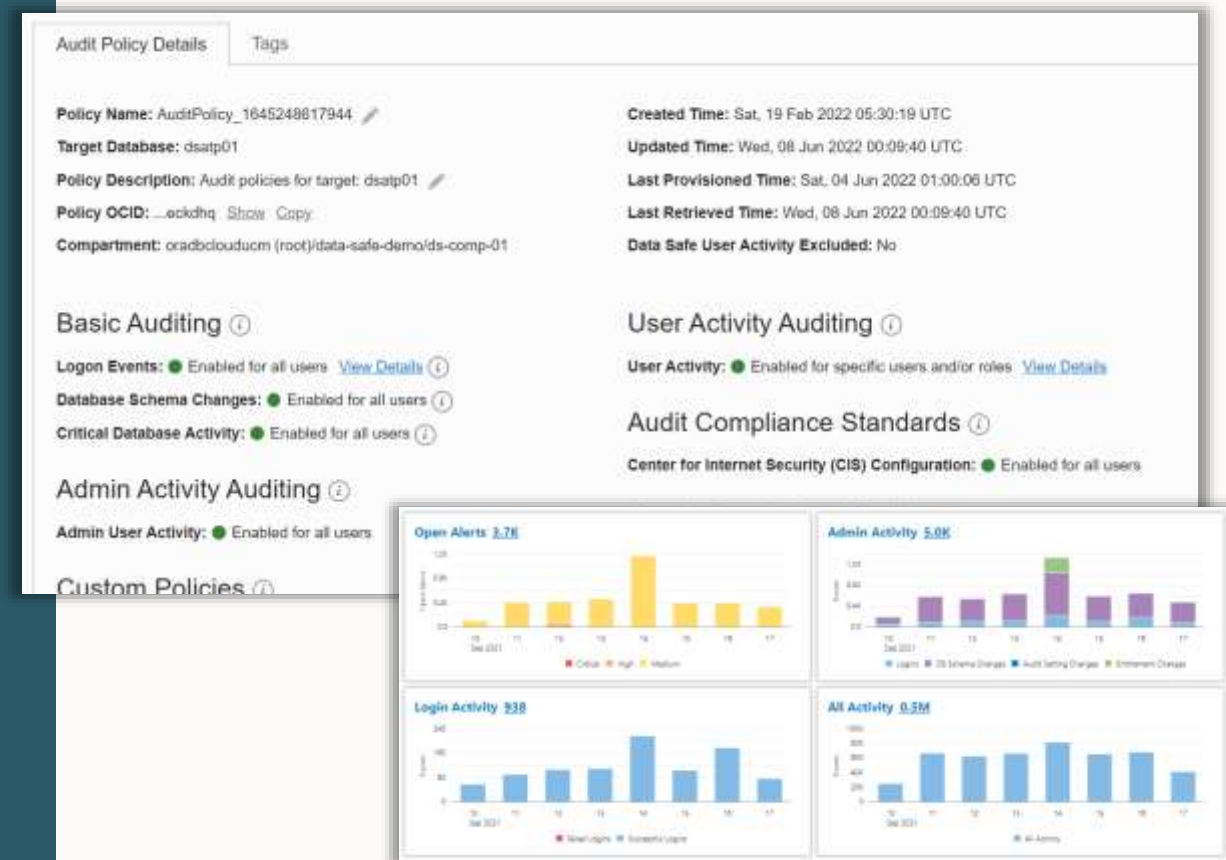
User Active Audit





User Active Auditing

- 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





Active Auditing Dashboard

- Get more insight into your audit data
 - Which audit policy is generating the most records ?
 - Which target is generating the highest volume ?
 - Which objects or schemas are accessed the most ?
- etc.





Audit Data Retention Management

- Keep your Audit Data for up to 7 years
 - Online retention period up to 1 year
 - Archive retention period up to 6 additional years ^{new}
- Configure retention periods globally and/or per target
- Easily retrieve audit records from the archive
- Fully managed by Data Safe



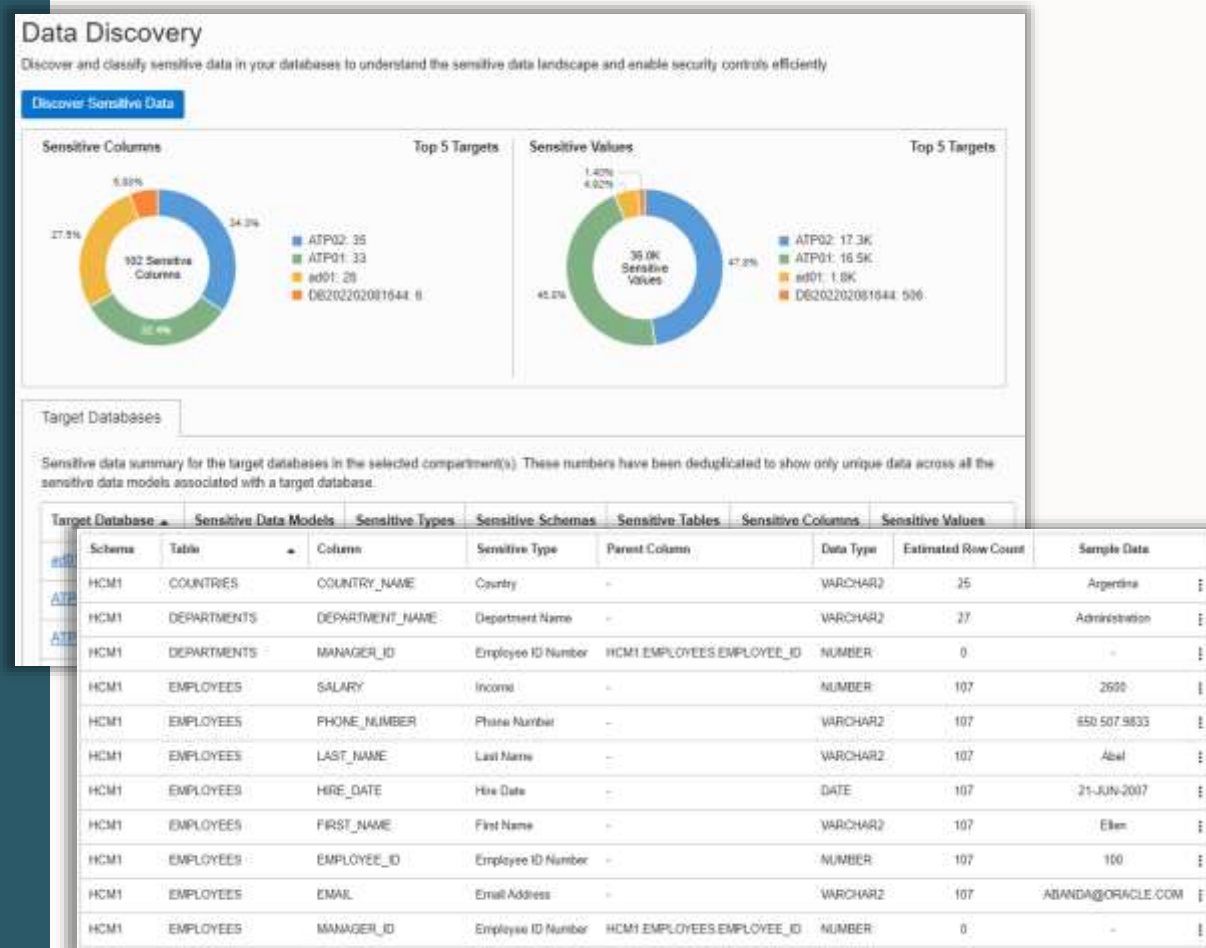
Sensitive Data Discover





Sensitive Data Discovery

- Prioritize security efforts by identifying the location, type and amount of sensitive data
- Discovers/classifies 150+ sensitive types
- User-defined sensitive types
- Incremental discovery
- Reports amount / type of sensitive data



Sensitive Data Discovery

150+ Pre-Defined Sensitive Data 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
...



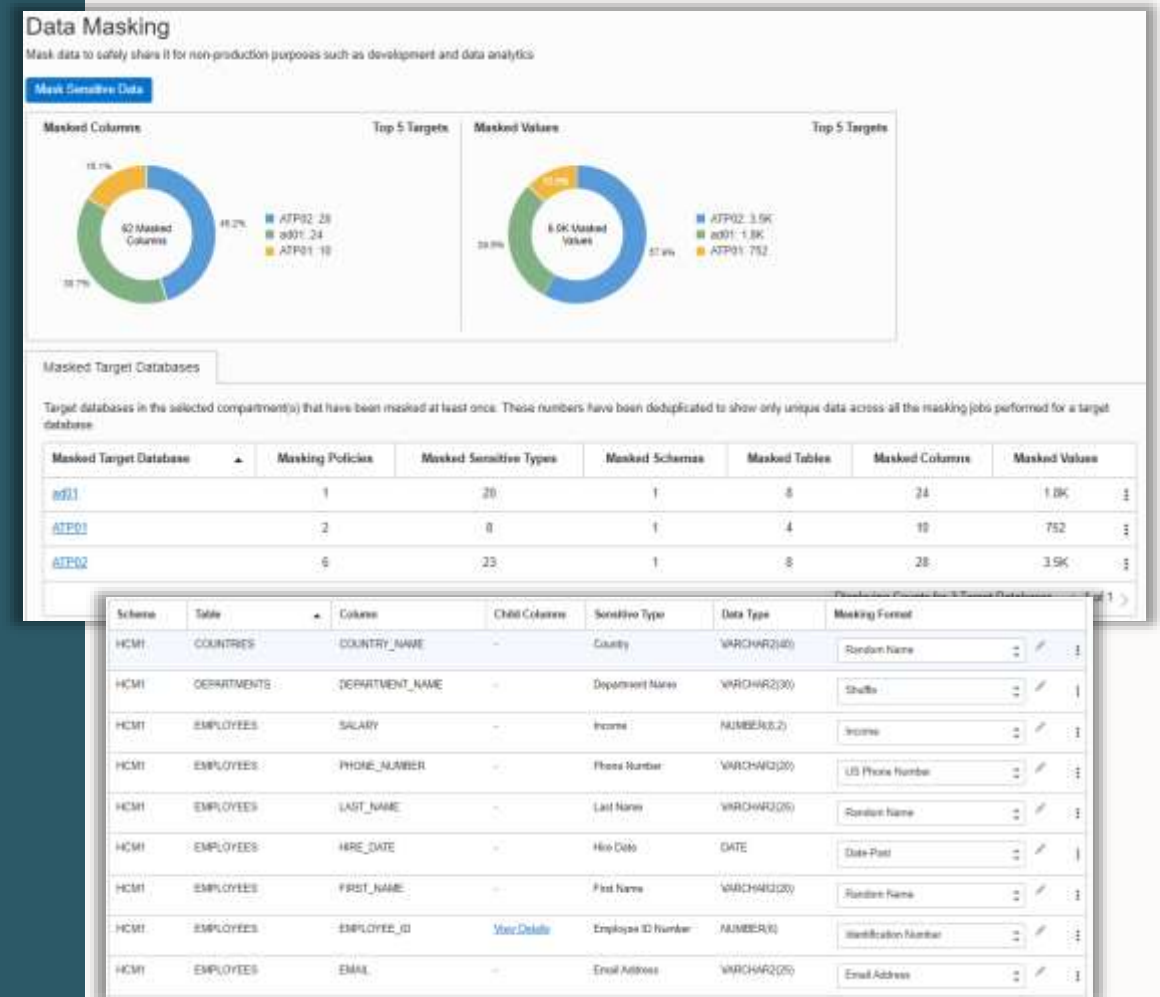
Sensitive Data Mask





Sensitive Data Mask

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





Sensitive Data Mask

- Pre-defined masking formats
- Specific masking formats like
 - social security number
 - credit card number
 - email address
 - etc.
- As well as generic masking formats
 - random date, number, name, ...
 - fixed number, fixed string
 - format preserving randomization
 - regular expression
 - truncate data
 - group masking
 - etc.

Masking Formats

Masking formats define the logic for masking data. This page lists the user-defined masking formats in the selected compartment, along with all the predefined masking formats. [Learn More](#)

Create Masking Format		
Name	Description	Oracle Predefined
Age	Replaces values with random numbers between 0 and 110	Yes
Bank Account Number	Replaces values with random 9 to 16 digit numbers	Yes
Bank Routing Number	Replaces values with random 9-digit numbers	Yes
Birthdate	-	No
Blood Type	Replaces with values picked randomly from a list. Possible values are A+, A-, B+, B-, AB+, AB-, O+, and O-	Yes
Canada Postal Code (Space-Separated)	Replaces values with random Canada postal codes. Postal codes are in A9A9A9 format, where A signifies a letter and 9 a digit	Yes
Canada Social Insurance Number	Replaces values with random Canada Social Insurance Numbers	Yes
Canada Social Insurance Number (Hyphenated)	Replaces values with random Canada Social Insurance Numbers. Social Insurance Numbers are in 999-999-999 format, where 9 signifies a digit	Yes
Credit Card Number	Replaces values with random credit card numbers. Card types covered are American Express, Diners Club, Discover, enRoute, JCB, Mastercard, and Visa	Yes
Credit Card Number (Hyphenated)	Replaces values with random hyphenated credit card numbers. Card types covered are American Express, Diners Club, Discover, enRoute, JCB, Mastercard, and Visa	Yes
Credit Card Number (Type and Format Preserving)	Replaces values with random credit card numbers while preserving their type and format. Card types covered are American Express, Diners Club, Discover, enRoute, JCB, Mastercard, and Visa. For other card types, preserves the number of digits and Luhn's check but may not preserve the card type	Yes
Credit Card Number American Express	Replaces values with random 15-digit American Express credit card numbers	Yes



Sensitive Data Discover Dashboard

ORACLE Cloud

Cloud Classic >

Search resources, services, documentation, and Marketplace

US East (Ashburn) v

Data Safe > Data masking > VE61VXRD74RV1G4H > MaskingPolicy_LL_202306141613 > Masking report details

MR

ACTIVE

Generate report

Download report

Download masking logs

Masking report information

Target database: VE61VXRD74RV1G4H

Masking policy: [MaskingPolicy_LL_202306141613](#)

Masking report OCID: ...ab7gqq [Show](#) [Copy](#)

Masking started: Wed, 14 Jun 2023 23:21:15 UTC

Masking finished: Wed, 14 Jun 2023 23:22:36 UTC

Masked sensitive types: 19

Masked schemas: 1

Masked tables: 8

Masked columns: 27

Masked values: 1.9K

Masking options: [View details](#)

Masked values summary chart

The masked value percentages/distribution shown in the graph for each of the sensitive types is with respect to its parent sensitive category.

Resources

Masked columns

Masking logs

Masked columns

+ Add filter

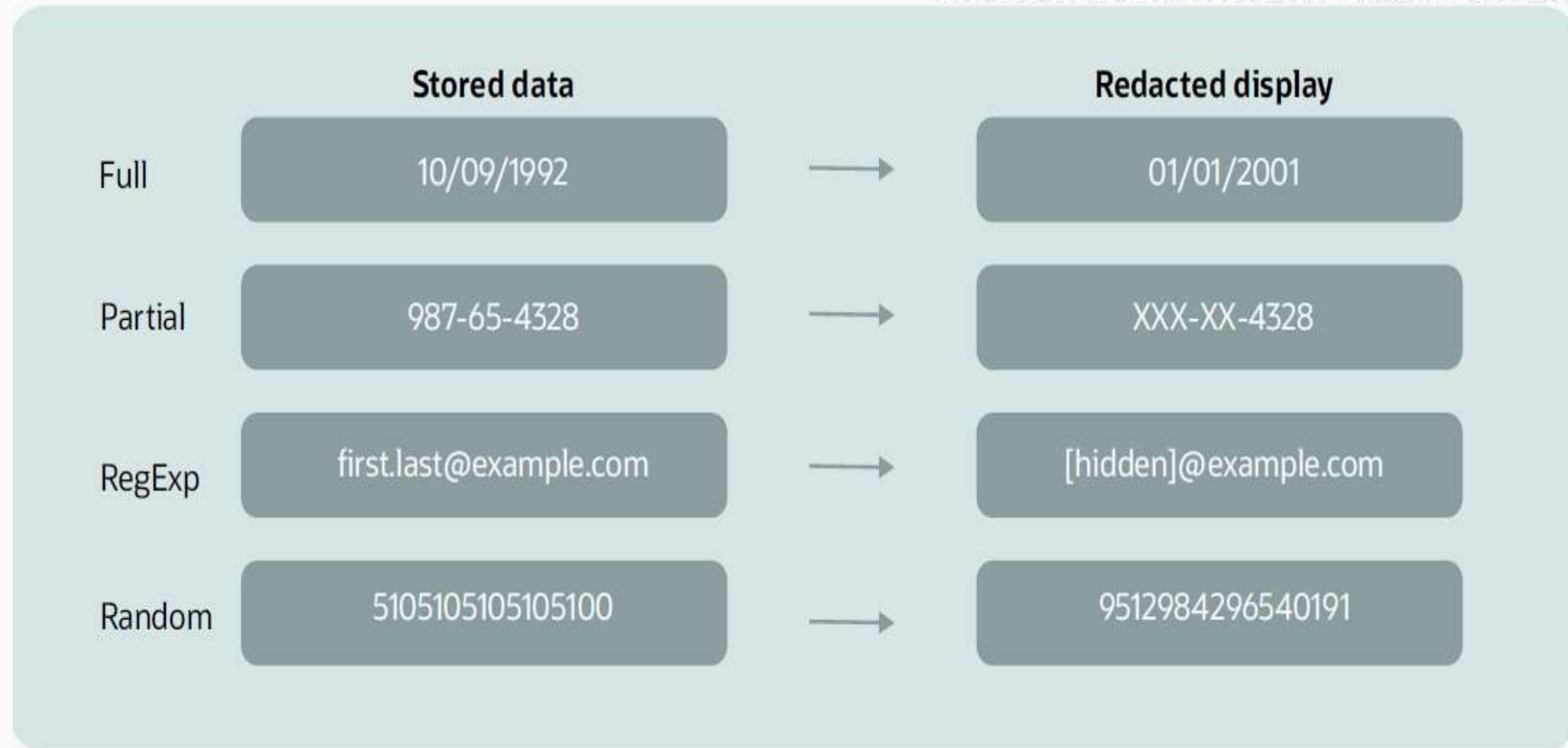
Apply

Schema	Table	Column	Masking format	Sensitive type	Parent column	Total masked values
HCM1	EMP_EXTENDED	PAYMENTACCOUNTNO	Credit Card Number	Card Number	-	107
HCM1	EMP_EXTENDED	TAXPAYERID	US Social Security Number	Tax ID Number (TIN)	-	107
HCM1	LOCATIONS	STATE_PROVINCE	Random Name	Province	-	17

32

Copyright © 2024, Oracle and/or its affiliates.

Data Redaction format sample



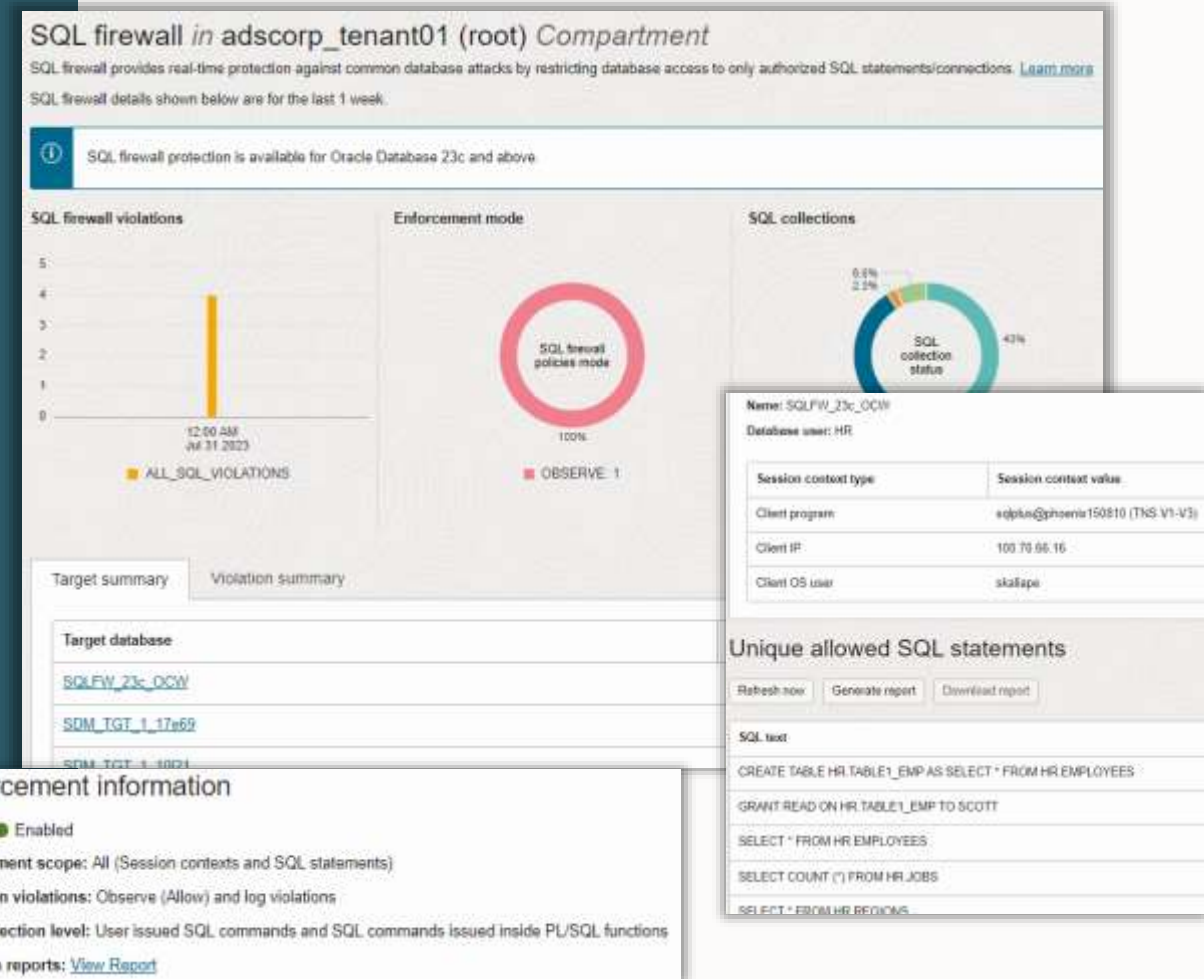
SQL Firewall



SQL Firewall

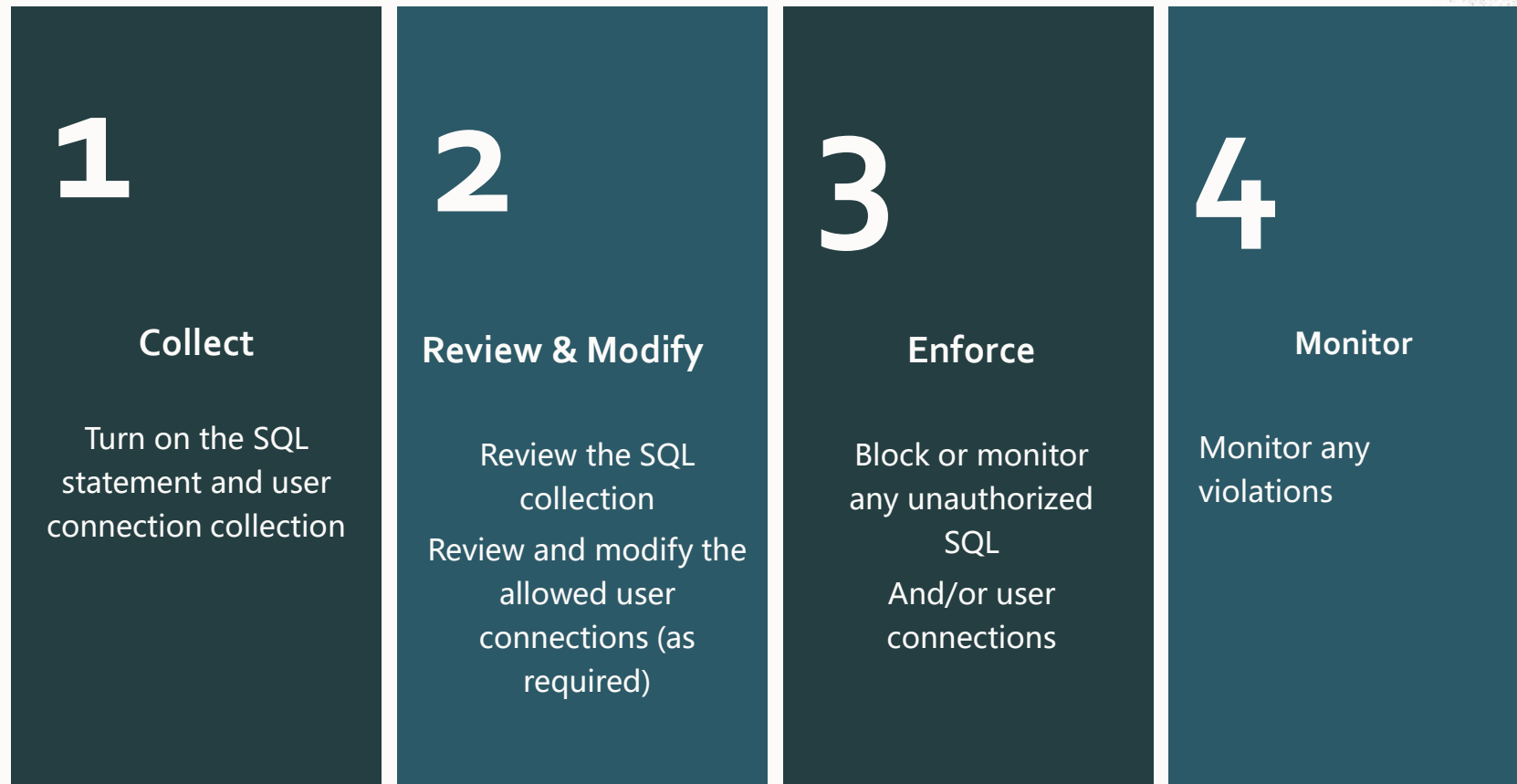


- Provides real-time protection against common database attacks by restricting database access to
 - Authorized connections
 - Authorized SQL statements
- Block or monitor any violations
- Mitigates risks from SQL injection attacks, anomalous access, and credential theft/abuse

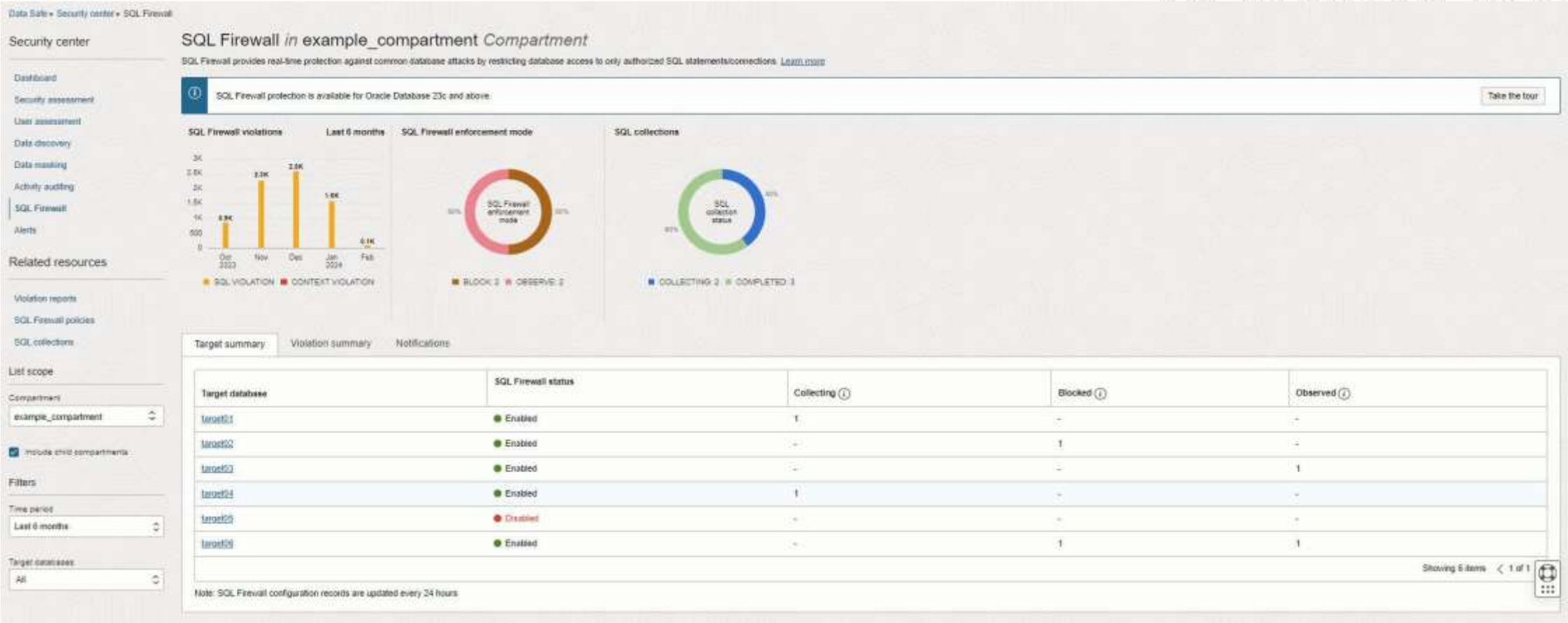


SQL Firewall

Easy configuration, management, and monitoring in Data Safe



SQL Firewall Dashboard in Data Safe





Data Safe register options

Three options to register databases with Data Safe

in the DB console
(Autonomous only)

Target registration wizards/
manually in Data Safe

via REST APIs / other interfaces

ATP
AVAILABLE

HR-Development

DB Connection Performance Hub Service Console Scale Up/Down More Actions

Autonomous Database Information Tools Tags

General Information

Database Name: dsatp03
Workload Type: Transaction Processing
Compartment: oradbclouducm (root)/data-safe-demo/ds-comp-02
OCID: ...ax665q [Show](#) [Copy](#)
Created: Fri, May 22, 2020, 21:42:16 UTC
OCPU Count: 1
Auto Scaling: Enabled ⓘ
Storage: 1 TB
License Type: Bring Your Own License (BYOL)
Database Version: 19c
Lifecycle State: Available
Instance Type: Paid
Mode: Read/Write [Edit](#)

Infrastructure

Dedicated Infrastructure: No

Autonomous Data Guard ⓘ

Status: Disabled [Enable](#)

Backup

Last Automatic Backup: No active backups exist for this database.
Manual Backup Store: Not Configured

Network

Access Type: Allow secure access from everywhere
Access Control List: Disabled [Edit](#)

Maintenance ⓘ

Next Maintenance: Sun, Aug 1, 2021, 12:00:00 UTC - 14:00:00 UTC [View History](#)
Customer Contacts: None ⓘ [Manage](#)

Operations Insights ⓘ

Status: Not Enabled [Enable](#)

APEX Instance

Instance Name: [HR-Development](#)

Data Safe ⓘ

Status: Registered [View](#) [Deregister](#)

Three options to register databases with Data Safe

in the DB console
(Autonomous only)

Target registration wizards/
manually in Data Safe

via REST APIs / other interfaces

Register Databases with Data Safe



Autonomous Databases

[Learn more](#)

- Autonomous Data Warehouse, Autonomous Transaction Processing and JSON databases

Start Wizard



Oracle Cloud Databases

[Learn more](#)

- Bare Metal, VM and Exadata databases

Start Wizard



Oracle On-Premises Databases

[Learn more](#)

- Installed database running on-premises



Oracle Databases on Compute

[Learn more](#)

- Databases in the Oracle Cloud Infrastructure

Register Autonomous Databases

- 1 Select Database
- 2 Connectivity Option
- 3 Add Security Rule
- 4 Review and Submit
- 5 Registration Progress

Data Safe Target Information

SELECT DATABASE IN DATA-SAFE-DEMO (CHANGE COMPARTMENT)

dsatp05

DATA SAFE TARGET DISPLAY NAME

dsatp05

COMPARTMENT

data-safe-demo

oracle/autonomous (1100)/data-safe-demo

DESCRIPTION (OPTIONAL)

Three options to register databases with Data Safe

in the DB console
(Autonomous only)

Target registration wizards/
manually in Data Safe

via REST APIs / other interfaces

CreateTargetDatabase DATASAFE

POST /20181201/targetDatabases

Registers the specified database with Data Safe and creates a Data Safe target database in the Data Safe Console.

Request

CreateTargetDatabase

Parameters

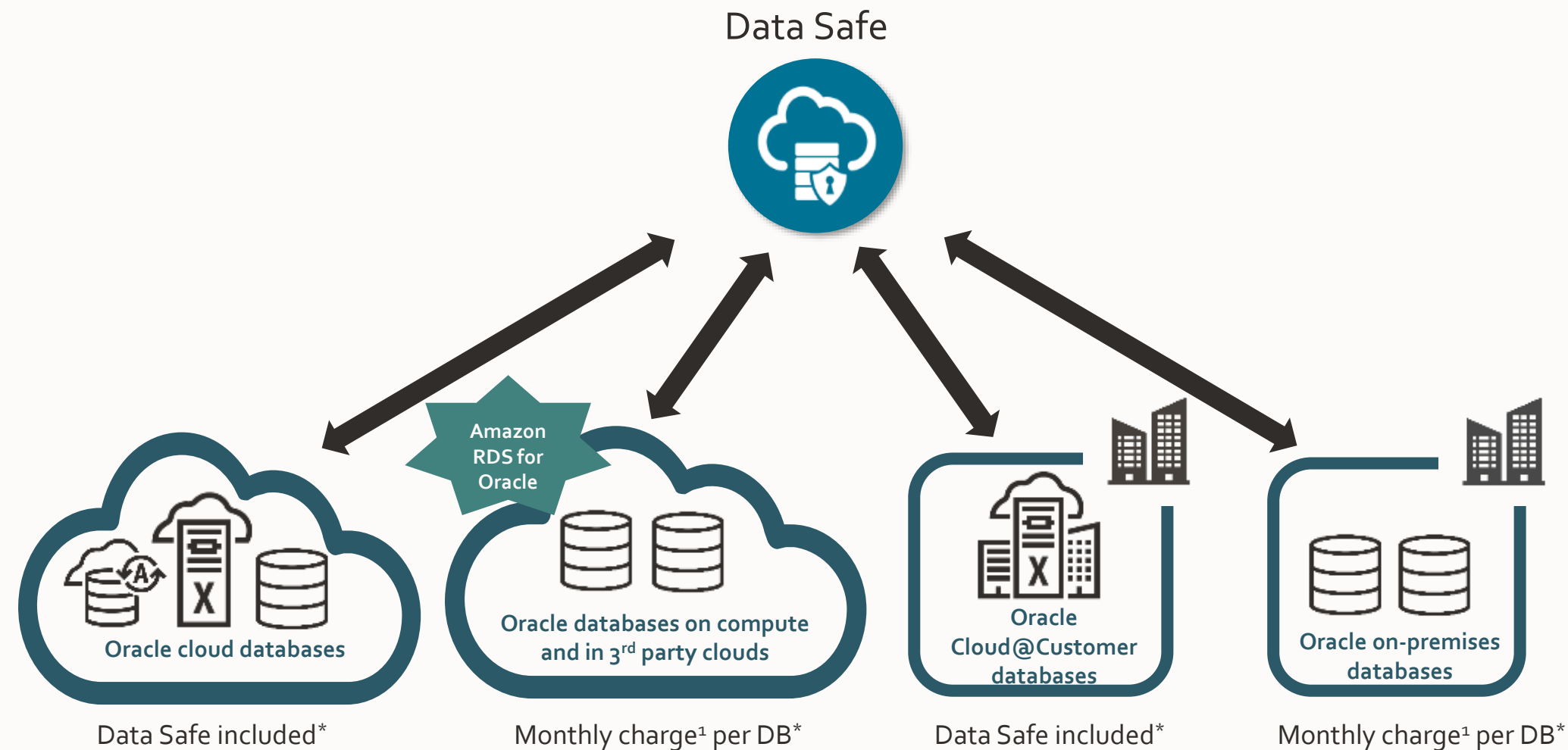
Name	Where	Description
opc-retry-token	header	<ul style="list-style-type: none">Required: noType: stringMin Length: 1Max Length: 64 <p>A token that uniquely identifies a request so it can be retried in case of a timeout or server error without risk of executing that same action again. Retry tokens expire after 24 hours, but can be invalidated before then due to conflicting operations. For</p>

Data Safe API

Version 20181201

Search...

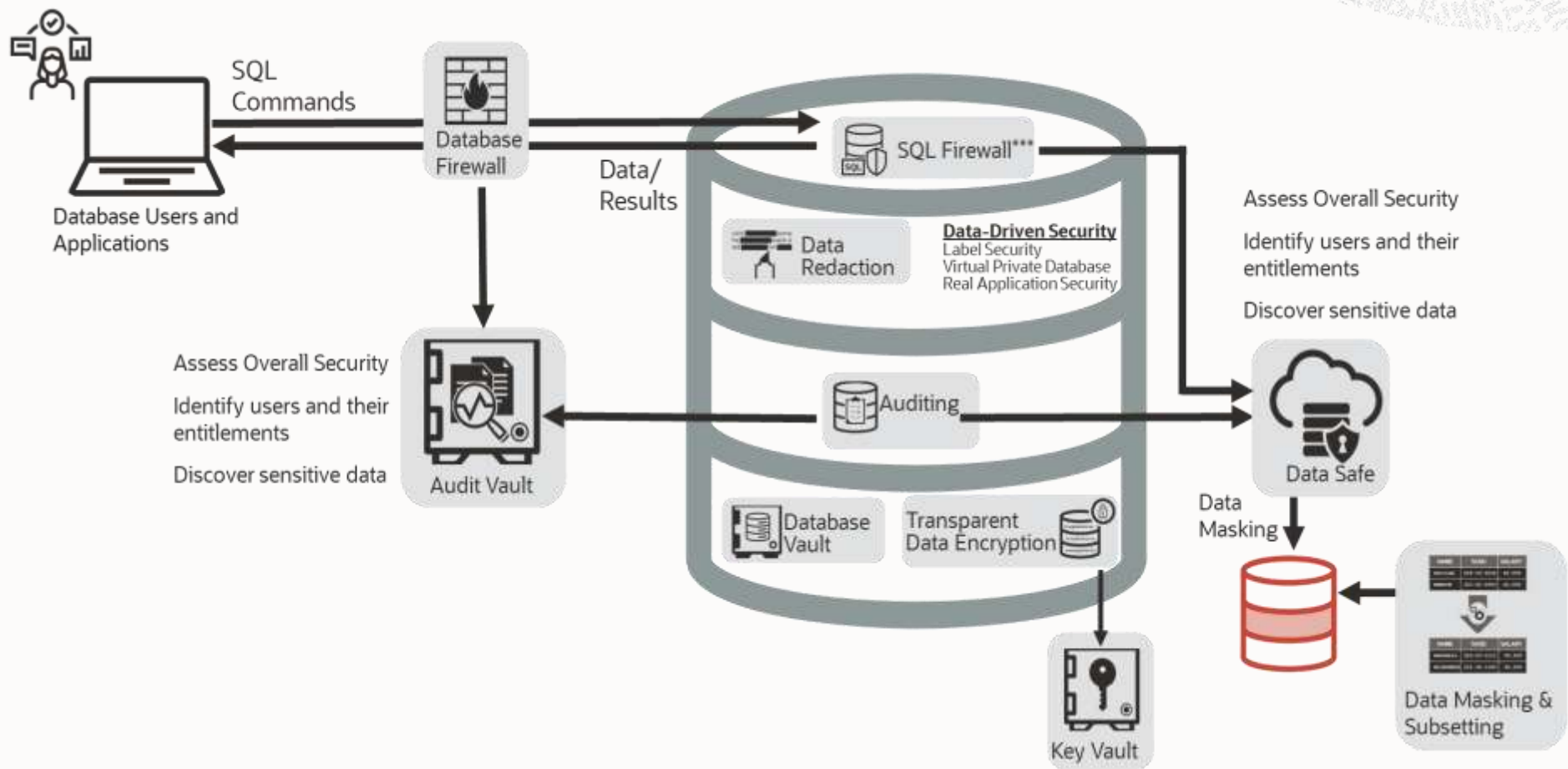
Data Safe is available for all your Oracle Databases



**Includes 1M audit records per database per month; \$0.10 per 10K records over the limit*
¹ tiered pricing applies ([price list](#))



Maximum security architecture





Resources



- **Oracle Data Safe product page**
<https://www.oracle.com/security/database-security/data-safe/>
- **Oracle Data Safe documentation**
<https://docs.oracle.com/en/cloud/paas/data-safe/>
- **Oracle Database Security a Technical Primer**
<https://download.oracle.com/database/oracle-database-security-primer.pdf>
- **OCI Data Safe price list**
<https://apexapps.oracle.com/pls/apex/r/dbpm/livelabs/view-workshop?wid=598>
- **Oracle Data Safe main document content**
<https://docs.oracle.com/en/cloud/paas/data-safe/udscs/using-oracle-data-safe.pdf>
- **DB Security - Database Security Assessment Tool BSAT (Live Labs)**
<https://apexapps.oracle.com/pls/apex/r/dbpm/livelabs/view-workshop?wid=699>
- **DB Security - Audit Vault and DB Firewall - Workshop (Live Labs)**
<https://apexapps.oracle.com/pls/apex/r/dbpm/livelabs/view-workshop?wid=711>

- **Oracle Database Audit Vault and Database Firewall product page**
<https://www.oracle.com/br/security/database-security/audit-vault-database-firewall/>
- **DB Security Basics (Live Labs)**
<https://apexapps.oracle.com/pls/apex/r/dbpm/livelabs/view-workshop?wid=698>
- **Get Started with Oracle Data Safe Fundamentals (Live Labs)**
<https://www.oracle.com/cloud/price-list/#data-safe>

Thank you

Marcel Lamarca

marcel.lamarca@oracle.com



ORACLE