



Adatvédelem, adatbázis

Kihívások, megfelelés cloud és on premise

Fekete Zoltán

Principal Solution Engineer

2020. június 24.

Safe harbor slide

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.

Data can be a liability

The scary side of data economy

- **Data breaches** are exploding world wide
 - Database is the most common asset involved in breaches
- Data losses can be **catastrophic for businesses** impacting
 - Finances due to compensations, penalties, legal, PR, recovery cost
 - Brand reputation, customer trust, intellectual property, competitiveness
 - Overall business and revenue
- Fast evolving, stringent **regulatory landscape**
 - Across industries and regions
 - Laws that aim to protect data and citizen privacy

Evolving **Attack Tools** and Techniques

Stolen Credentials

Phishing

SQL Injection

Buffer Overflow

Privilege Escalation

App Exploits

XSS Attacks

Unpatched Systems



Think **Like a Hacker**



Insider / Outsider

Known Users
Common Passwords
Privileged Users
Open Ports
Database
Encrypted Data
Auditing On
Database Version
Known Vulnerabilities
Known Packaged Apps



Data Owner

Biztonsági zónák: több megközelítés együtt működik!

Felmérés, értékelés

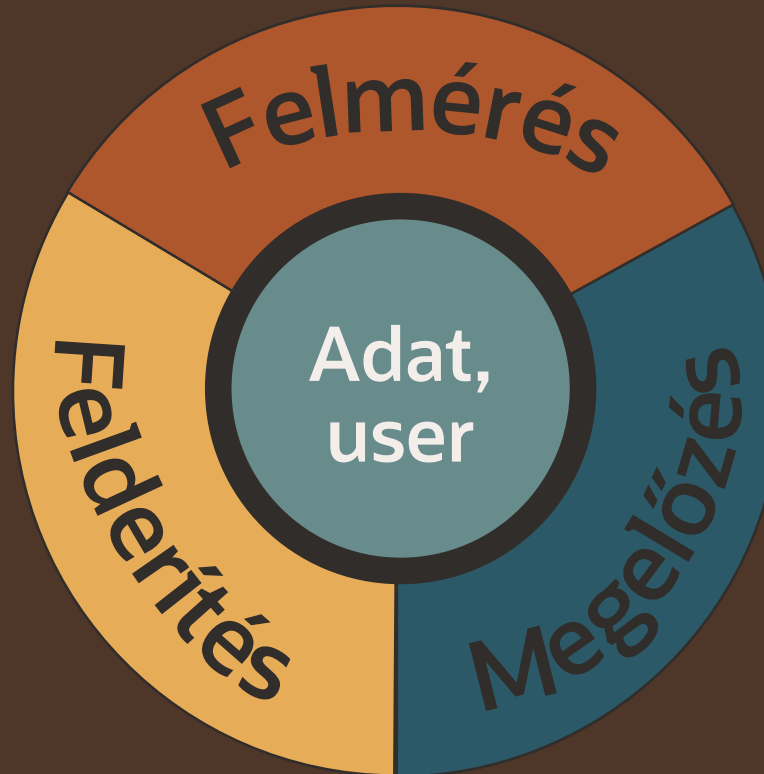
Az adatbázis aktuális állapotának felmérése.

Felderítés

Az adatelérési próbálkozások felderítése, különösen a szabályoknak nem megfelelők esetében.

Megelőzés

A nem megfelelő és szabályellenes adatelérés megelőzése.



Adatok

Az adatbázisok adatai értékesek: adatvagyon, ami komoly kockázatokkal járhat..

Felhasználók

Az adatbázisokhoz felhasználók és alkalmazások kapcsolódnak, üzleti feladatok elvégzéséhez.

USA, National Security Agency: Cybersecurity Information Mitigating Cloud Vulnerabilities

https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF



National Security Agency Cybersecurity Information

Mitigating Cloud Vulnerabilities

While careful cloud adoption can enhance an organization's security posture, cloud services can introduce risks that organizations should understand and address both during the procurement process and while operating in the cloud. Fully evaluating security implications when shifting resources to the cloud will help ensure continued resource availability and reduce risk of sensitive information exposures. To implement effective mitigations, organizations should consider cyber risks to cloud resources, just as they would in an on-premises environment.

This document divides cloud vulnerabilities into four classes (misconfiguration, poor access control, shared tenancy vulnerabilities, and supply chain vulnerabilities) that encompass the vast majority of known vulnerabilities. Cloud customers have a critical role in mitigating misconfiguration and poor access control, but can also take actions to protect cloud resources from the exploitation of shared tenancy and supply chain vulnerabilities. Descriptions of each vulnerability class along with the most effective mitigations are provided to help organizations lock down their cloud resources. By taking a risk-based approach to cloud adoption, organizations can securely benefit from the cloud's extensive capabilities.

This guidance is intended for use by both organizational leadership and technical staff. Organizational leadership can refer to the **Cloud Components** section, **Cloud Threat Actors** section, and the **Cloud Vulnerabilities and Mitigations** overview to gain perspective on cloud security principles. Technical and security professionals should find the document helpful for addressing cloud security considerations during and after cloud service procurement.

Cloud Components

Cloud architectures are not standardized and each Cloud Service Provider (CSP) implements foundational cloud services differently. Understanding a CSP's cloud implementation should be part of a customer's risk decision during cloud service procurement. Four cloud architectural services are common to most clouds:

- **Identity and Access Management (IdAM):** IdAM refers to controls in place for customers to protect access to their resources as well as controls that the CSP uses to protect access to back-end cloud resources. Secure customer and cloud back-end IdAM, both enforcement and auditing, is critical to protecting cloud customer resources.
- **Compute:** Clouds generally rely on virtualization and containerization to manage and isolate customer computation workloads. Serverless computing, the dynamic allocation of cloud compute resources to run customer code, is built upon either virtualization or containerization, depending on the cloud service.
 - **Virtualization** is a cloud backbone technology, not only for customer workloads, but also for the cloud architecture itself. Virtualization is an enabling technology that provides isolation in the cloud for both storage and networking. Virtualization typically implements and secures internal cloud nodes.
 - **Containerization** is a more lightweight technology that is commonly used in clouds to manage and isolate customer workloads. Containerization is less secure of an isolation technology than virtualization because of its shared kernel characteristics, but CSPs offer technologies that help address containerization security drawbacks.
- **Networking:** Isolation of customer networks is a critical security function of the cloud. In addition, cloud networking must implement controls throughout the cloud architecture to protect customer cloud resources from insider threat. Software Defined Networking is commonly used in the cloud to both logically separate customer networks and implement backbone networking for the cloud.
- **Storage (Objects, Blocks, and Database Records):** Customer data is logically separated from other customer data on cloud nodes. Security mechanisms must exist to ensure that customer data is not leaked to other customers and that customer data is protected from insider threat.

Cloud Encryption and Key Management

While not a base component of cloud architectures, encryption and key management (KM) form a critical aspect of protecting information in the cloud. While the CSP uses encryption (among other controls) to protect some aspects of customer data from other customers and CSP employees, cloud customers should understand the options that they have for further protecting their data. Understanding data sensitivity requirements is crucial for building a cloud encryption and key management strategy.

UDD/106445-20

PP-20-0025

22 JANUARY 2020

4 Top Cloud Vulnerabilities and Mitigations

- Key Recommendations:
 - Mitigating cloud vulnerabilities is a shared responsibility
 - Orgs need dedicated resources commensurate with the size of the org, to ensure adequate protection
 - CSP: Understanding the available vendors-specific countermeasures?



Figure 2: Cloud Vulnerabilities – Prevalence versus Sophistication of Exploitation

Oracle Active Defense



Architected-in full-stack protection

- Secure isolation in OCI
- Least privilege design for OCI
- OCI Hardware root of trust
- Exadata configurations and isolation policies



Automated actions and threat response

- Automatically identify and remediate user and event anomalies
- Self-Patching Autonomous Database and Autonomous Linux
- Automatic config for strong security posture for cloud infrastructure and database



Always-on for seamless protection

- Default-enabled encryption and TDE encryption
- Activity auditing and monitoring
- Adaptive authentication
- Defense in depth for full stack protection



NOS Minimizes Risk and Enhances Security

<https://www.oracle.com/customers/nos-1-database.html>

Scale

Security solutions for a growing IT environment

Compliance

Simplification of GDPR compliance

Time to Value

Tight deadline for implementation was met

CUSTOMER PERSPECTIVE



On our path towards EU GDPR compliance, we chose Oracle Database Security solutions including Oracle Advanced Security, Oracle Key Vault, Oracle Database Vault, Oracle Audit Vault and Oracle Database Firewall to streamline and simplify our Oracle deployment. With Oracle, we minimize risk and further enhance our overall security.

Henrique Zacarias, CIO from NOS



Ministerio de Justicia de España Encrypts and Locks Down Access to Citizen Data



<https://www.oracle.com/emea/customers/ministerio-de-justicia-1-adv-sec.html>

Industry-specific Privacy Laws

Responsible for handling the data of juvenile offenders, domestic violence victims and other special cases

Privileged Access

Granular access controls required to stratify privileges and enforce separation of duties

The Solution

Oracle Advanced Security for encryption of sensitive data and Oracle Data Masking and Subsetting Pack for test/dev purposes

CUSTOMER PERSPECTIVE



Oracle Advanced Security, Oracle Data Masking and Subsetting Pack, and Oracle Active Data Guard enable us to go beyond what is required by privacy laws, ensuring access to citizens' personal data is secure and trackable. Oracle's solutions are a proven investment in peace of mind and security.

Jose Luis Fernández Carrión, Assistant Manager, New Technologies, Ministerio de Justicia de España.



Pragmatyxs Secures Customer Data and Reaches Innovation Goals



<https://video.oracle.com/detail/video/5742688470001>

Trust

Customers increasingly demand that their data be protected

Hybrid

Requirement to provide solutions that extend on premises capabilities

Compliance

Customer organizations represented various industry verticals, with different regulatory requirements

CUSTOMER PERSPECTIVE



One of the key benefits of moving to the **Oracle Database Cloud Service** was transparent data encryption – we could ensure our customers that, right out of the gate, their data was secure, and the risk of compromise was minimum.

Paul Vanhout, CEO and Founder, Pragmatyxs



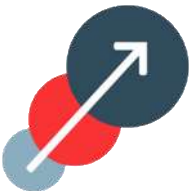
Oracle Converged Database Delivers Union of Best Capabilities

Oracle has invested billions of dollars over decades to make Oracle Database **best-in-class in every class**

Platforms



Scalability



Availability



Security



Management



Distributed

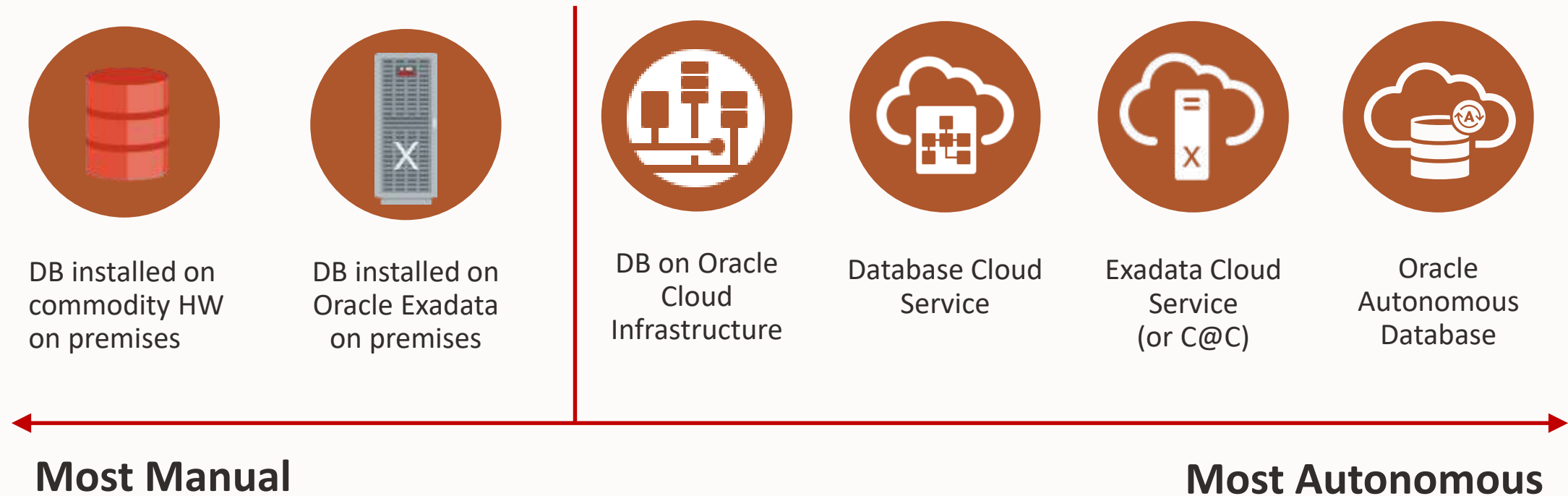


Development











No Risk or Compromise

Oracle Database – Choice of Deployment



Same database, same skills

Oracle Cloud Infrastructure: Complete services

Governance IAM, Tagging, Cost Analysis		Security IAM, Audit, KMS, CASB		Management Monitoring, Notifications, Alarms		Automation Resource Manager, Ansible	
Analytics / Integration / SOA Suite / Identity / Management / Content / API Platform / Developer / Visual Builder / Digital Assistant/ DataFlow / Data Science / Data Safe							
Containers Containers and Kubernetes		Data Movement Storage appliance, Data Transfer		Autonomous Database Transactions, Data Warehouse		Cloud Native Events, Streaming, Functions	
 Fully managed, certified Kubernetes service with Docker containers		 Software NAS gateway, data ingest service with full chain of custody (HDD or appliance)		 Fast provisioning. Automatic tuning, patching, securing. 99.995% availability.		 Fully-managed FaaS, event-triggered functions, high-volume data ingest, notifications	
Compute Bare metal/VM, CPUs/GPUs		Storage NVMe, Block, File, Object, Archive		Database Bare metal, VMs, Exadata		Networking VCN, LBaaS, FastConnect, VPN	
 Up to 64 CPU cores, 8 GPUs, 768 GB RAM, 51 TB local NVMe SSD, 5M IOPS, AMD and Intel processors		 Predictable IOPS Block Storage for up to 98% less, storage for whole lifecycle		 Millions of TPS; Full RAC and Active Data Guard support		 Isolated networks with reserved IPs, security lists, firewalls, lowest cost private connectivity	

Public regions

Government regions

Mission Critical Security

Full Architecture to Achieve Data Security – **Maximum Security Architecture**

Data Encryption

Prevent Admin Data Access

Key Management

Centralized Auditing

Testing Security

Centralized Security

→ **Advanced Security**

→ **Database Vault**

→ **Key Vault**

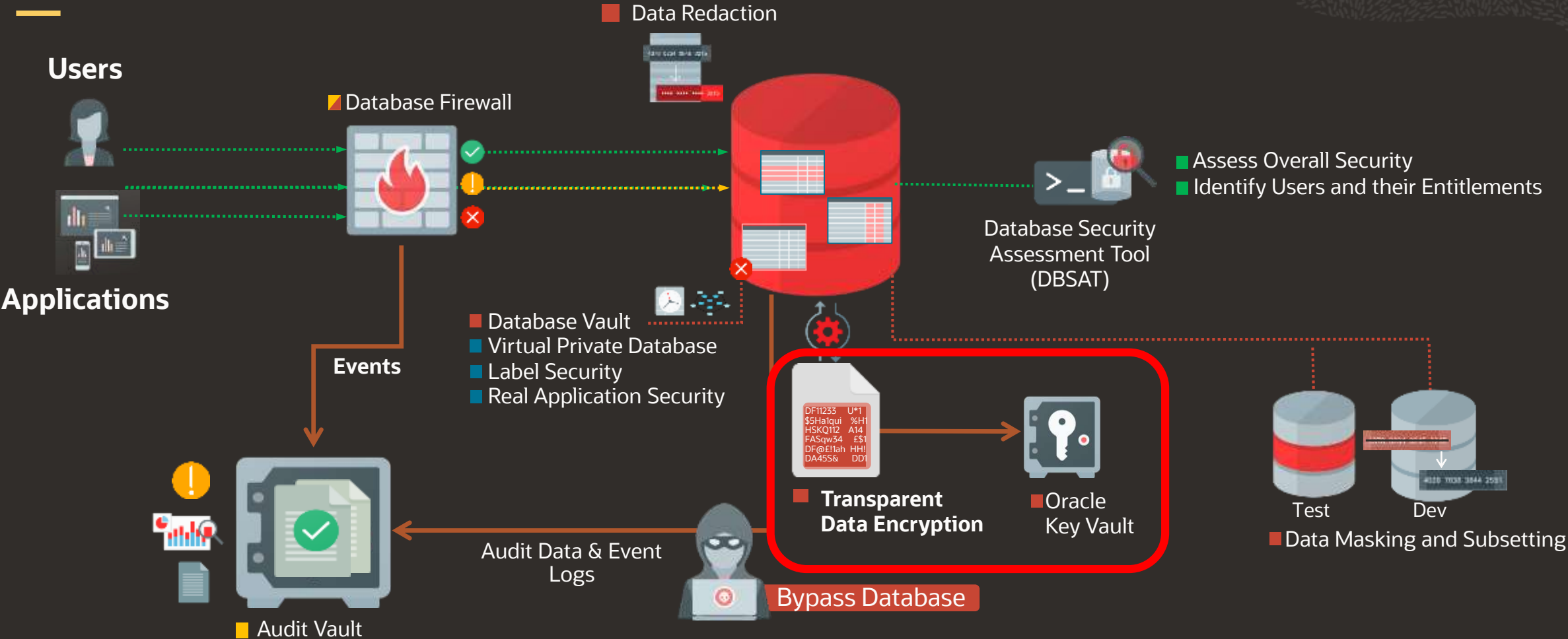
→ **Audit Vault**

→ **Data Masking and Subsetting**

→ **Data Safe**



Maximum Security Architecture



Database Security Controls

■ Assess ■ Prevent ■ Detect ■ Data Driven Security



Advanced Security Transparent Data Encryption

TDE Key Architecture

- Data encryption keys are created and managed by TDE automatically
- Tables and Tablespace Keys are the data encryption keys
- A master encryption key encrypts the data encryption keys
- The master key is stored in a Keystore such as Oracle Key Vault or Oracle Wallet

Oracle Key Vault



—OR—



Oracle Wallet

Master Key

Table Key

TDE Encrypted Columns

Tablespace Key

TDE Encrypted Tablespace

Oracle Database Cloud Migration Solutions

ZDM



MV2ADB

MAA



SQL Developer



Data Pump



RMAN



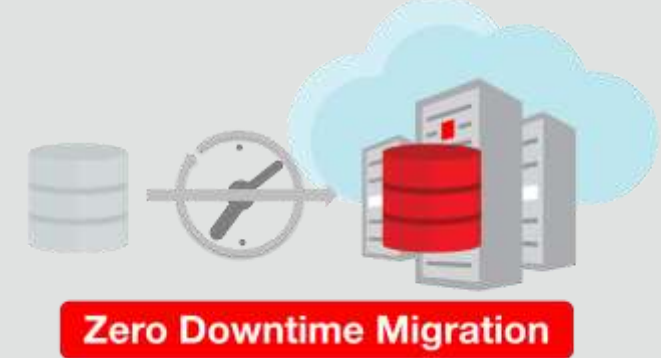
Plug / Unplug



Remote Cloning



TDE and Migrating to the Oracle Cloud



Oracle **Zero Downtime Migration** is the preferred method

To migrate large numbers of Linux-based databases to the Oracle Cloud

Move on-premises databases and Oracle Cloud Infrastructure Classic instances to:

- Oracle Cloud Infrastructure
- Exadata Cloud at Customer
- Exadata Cloud Service

Enables and allows fallback capability after database migration is complete

Database using TDE on-premises will continue to use TDE in the cloud standby

Databases not using TDE on-premises will use TDE for the initial configuration in the cloud standby

However, new tablespaces, redo generation, and archived redo logs will not use TDE encryption

Tips for ZDM

For 12c Release 2 and newer, TDE Wallet on source DB must be configured when using Oracle ZDM

Pause before switching to Cloud DB to verify you are 100% ready to go!

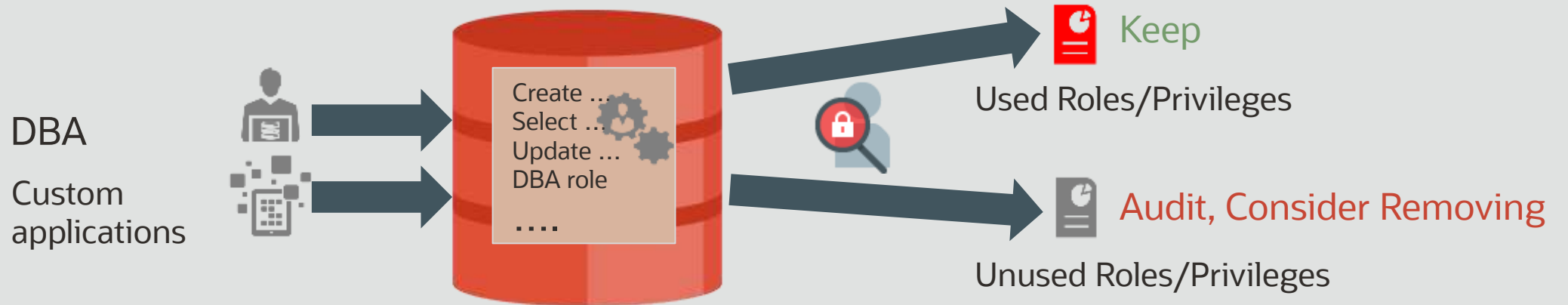
The Top Ten Takeaways: TDE

1. Encrypt data at rest (Transparent Data Encryption) and in motion (Native Network Encryption) as your **secure-by-default** baseline
2. Use Tablespace Encryption 99.99% of the time
3. New project should start with TDE tablespace encryption rather than retrofit it later
4. Use Encryption with Oracle Data Pump Exports
5. Protect your TDE wallet (ewallet.p12) as if your job depends on it - because it does!
6. Don't delete the wallet, read Peter Wahl's LinkedIn post from May 2020 explaining why
7. Use the new initialization parameters to make your life easier
8. Never backup the wallet and data (RMAN/exports) in the same location
9. Backup the wallet to a secure location on a regular basis
10. Upgrade your database to Oracle 19c
11. Oracle Key Vault Online Master Key can remove the TDE wallet from the OS and simplify your RMAN duplicates and RMAN backup and recovery operations

Privilege Analysis

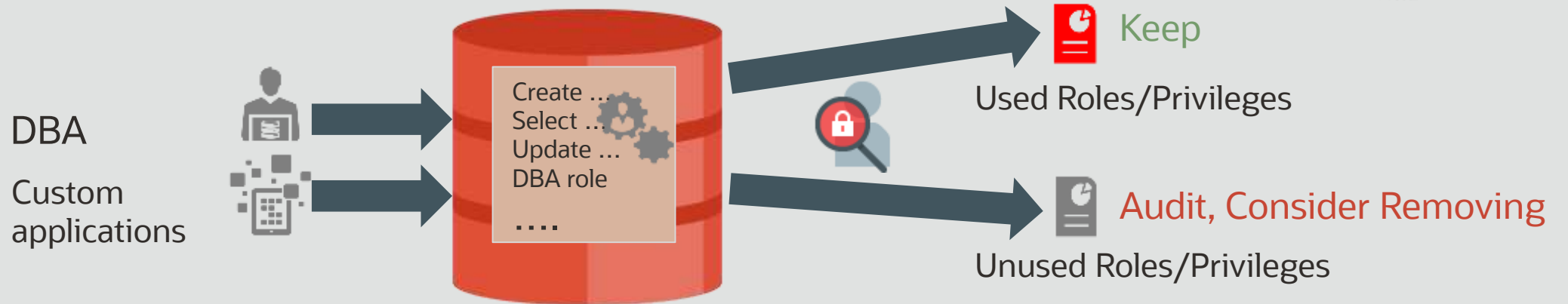
Privilege Analysis

Introduced in Oracle 12c Release 1, originally part of Database Vault
Moved to core database November 2018



Track privilege/role usage by a database user for a period of time
Identify and consider removing unused privileges

Privilege Analysis





- Built-in utility that captures privileges and roles used in the database
- Minimal performance impact – processing done during report generation
- No dependency on Database Vault Licensing

Unused Privileges Report

S/N	Policy	Grantee	Grantee Type	System Privileges	Grant Path
1	HR Analysis Policy	APPS	USER	DROP ANY TABLE	APPS
2	HR Analysis Policy	APPS	USER	ALTER ANY TABLE	APPS
3	HR Analysis Policy	APPS	USER	CREATE TABLE	APPS
4	HR Analysis Policy	APPS	USER	UNLIMITED TABLESPACE	APPS
5	HR Analysis Policy	APPS	USER	DROP ANY PROCEDURE	APPS,APPS_PATCHING
6	HR Analysis Policy	APPS	USER	CREATE PROCEDURE	APPS,APPS_PATCHING

Used Privileges Report

S/N	Policy	User Name	Used Role	System Privileges 	Object			Grant Path
					Owner 	Name	Type	
1	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	DEPARTMENTS	TABLE	APPS
2	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	JOB_HISTORY	TABLE	APPS
3	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	COUNTRIES	TABLE	APPS
4	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	EMPLOYEES	TABLE	APPS
5	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	LOCATIONS	TABLE	APPS
6	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	REGIONS	TABLE	APPS
7	HR Analysis Policy	APPS	APPS	SELECT ANY TABLE	HR	JOBS	TABLE	APPS
8	HR Analysis Policy	APPS	APPS	CREATE SESSION			(null)	APPS
9	HR Analysis Policy	APPS	PUBLIC	(null)	SYS	DBMS_APPLICATI...	PACKAGE	PUBLIC
10	HR Analysis Policy	APPS	PUBLIC	(null)	SYSTEM	PRODUCT_PRIVS	VIEW	PUBLIC
11	HR Analysis Policy	APPS	PUBLIC	(null)	SYS	DUAL	TABLE	PUBLIC

Database Security Assessment

Assess Your Database Security Before Hackers Come Knocking

Assess Configuration

- Patches
- Data Encryption
- Auditing policies
- OS file perm.
- Database config
- Listener config
- Fine-grained access control

Identify Risky Users

- Database accounts
- User privileges
- User roles

Discover Sensitive Data

What type, where, and how much?

Assessment Reports

- Summary and detailed info.
- Prioritized & actionable recomms
- Mapping to EU GDPR, STIG and CIS Benchmark.
- Runs on 10g to 19c Oracle DBs.

DBSAT 3-Step Flow

- 1 Run
./dbsat collect
- 2 Run
./dbsat report
- 3 Run
./dbsat discover

Easy to Install and Run

Download DBSAT 2.2 today from
<http://www.oracle.com/technetwork/database/security/dbsat.html>

Collect security config data by running 'dbsat collect' on the target

Run 'dbsat report' to generate security assessment report

Run 'dbsat discover' to generate sensitive data report

Available to all Oracle database customers with active support contract

Top 10 Findings From Database Security Assessments

- No Database Security policies/strategy in place
- No patching/patch management policy in place
- No personalized accounts; No separation of duties; Over-privileged accounts
- No encryption of sensitive/regulated data
- No monitoring/auditing in place
- No password policies; Weak password management
- Non-Production (DEV/TEST/TRAINING) systems w prod data
- No cleanup of test/sample accounts
- No anonymization of data sent to third parties
- No OS hardening

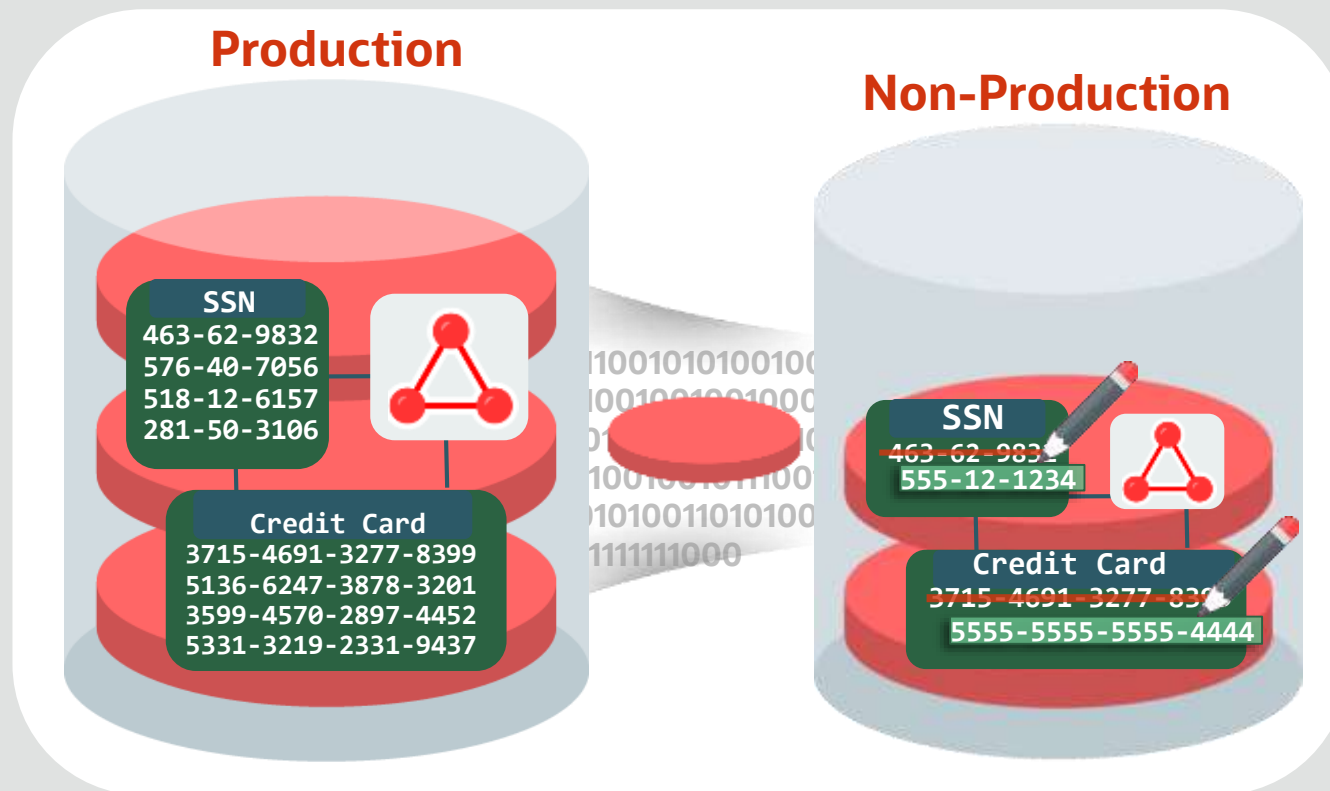


Data Masking and Subsetting

Oracle Data Masking and Subsetting

Minimize proliferation of sensitive data to non-production environment

ORACLE[®] 13^c
ENTERPRISE MANAGER



Sensitive Data Discovery

Comprehensive Masking Options

Goal/Condition Based Subsetting

In-Database or In-Export Masking

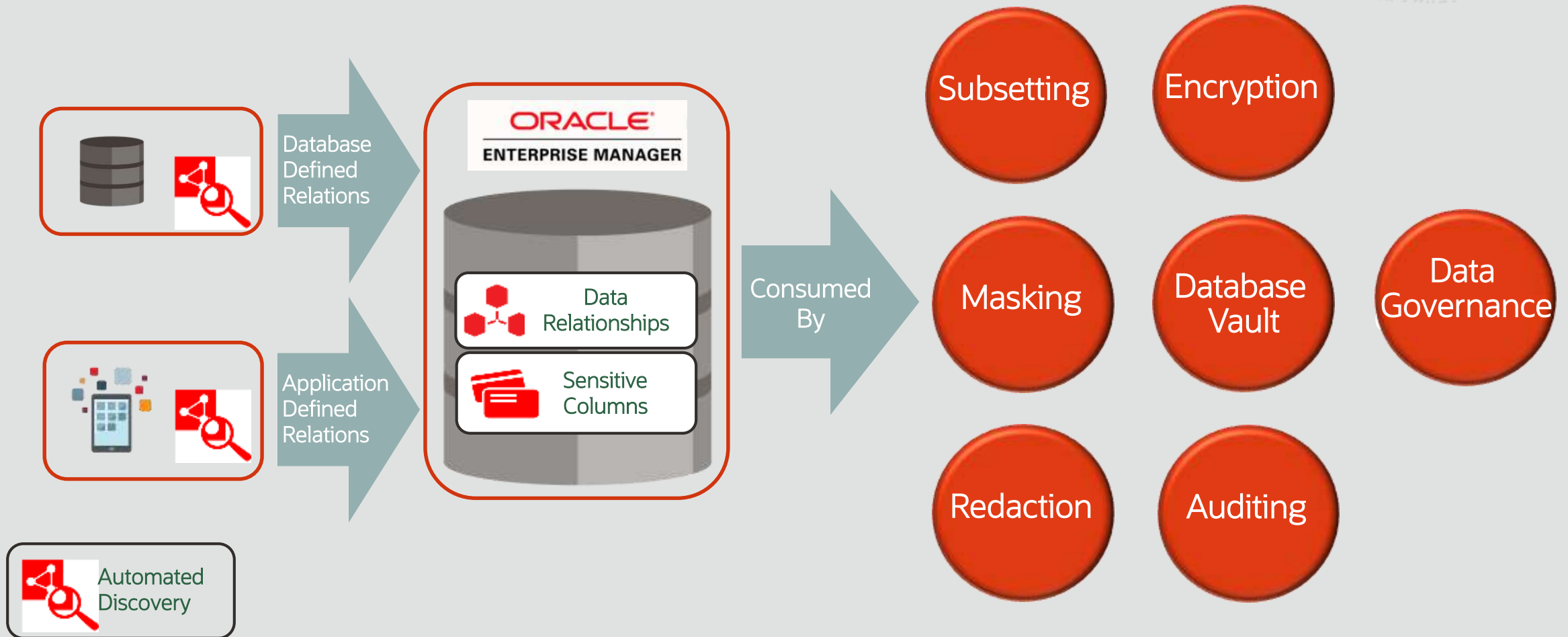
Support for Cloud and Non-Oracle DBs

Workload Capture & Clone Masking

Pre-installed in Enterprise Manager

Application Data Modeling

Sensitive Data Discovery



Data Masking

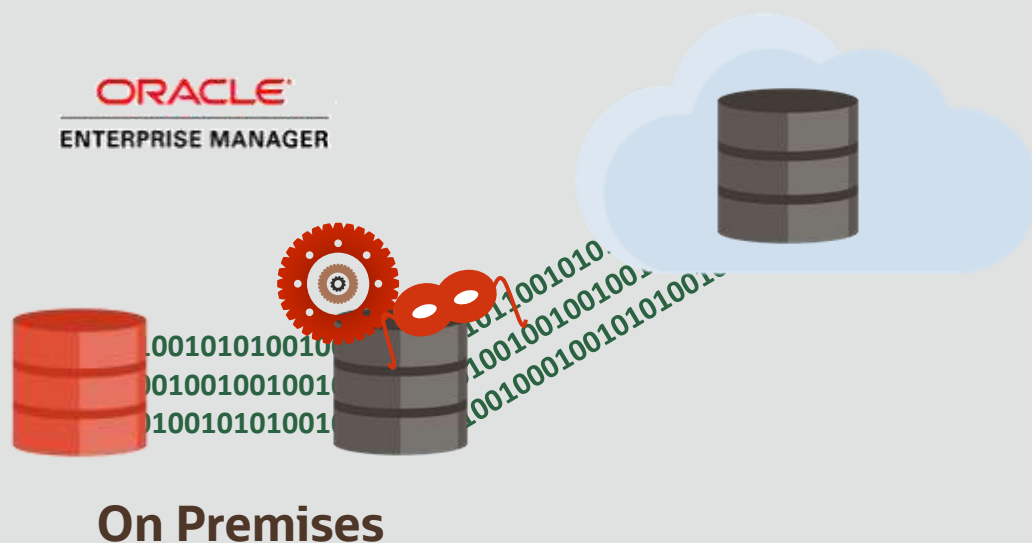
Masking transformations to meet diverse business use cases

Conditional masking	Masks rows differently based on condition Example: Mask national identifiers based on country
Deterministic masking	Masks data to the same consistent values across multiple databases or masking jobs Example: Mask employee identifiers consistently across schemas and databases
Compound masking	Ensures masked values across related columns retain the same relationship Example: Mask address fields such as state, postal code, and country as a group
Format preserving	Masks data while preserving its format such as length and special characters Example: Mask tax identifiers while preserving spaces and hyphens
Reversible masking	Encrypts and decrypts data using cryptographic key Example: Unmask data after receiving the processed data from a partner
Shuffling	Shuffles the values within a column Example: Shuffle age of employees in a organization
Perturbation	Generates random values within a user-provided range Example: Generate random dates within a specified data range

Mask on Premises and Upload to the Cloud

Oracle Database Cloud Service (PaaS)

Clone ➡ Mask/Subset ➡ Upload



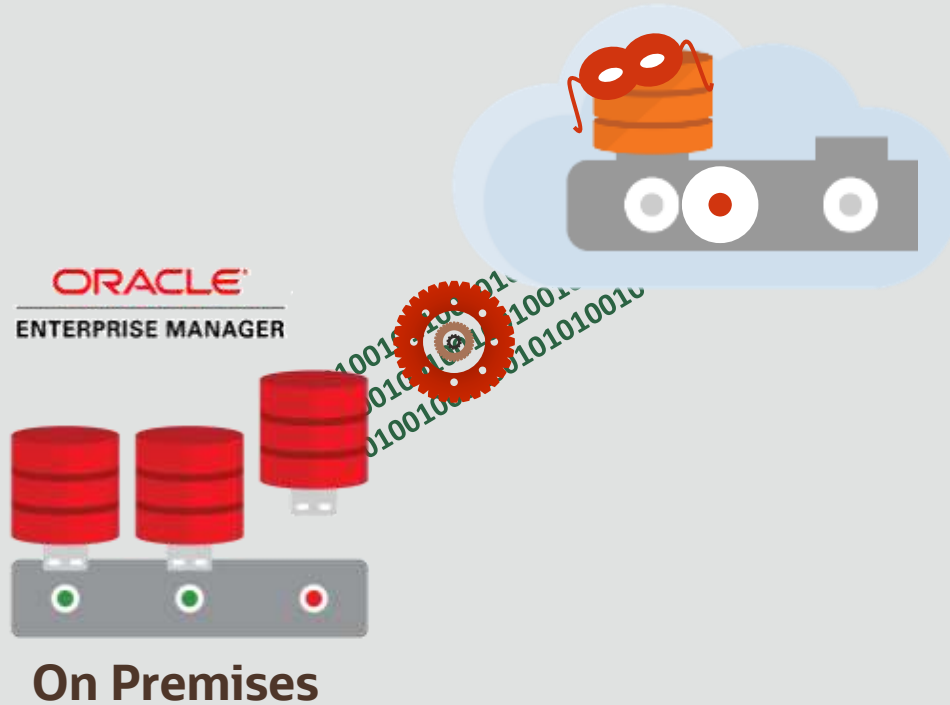
Extract ➡ Mask/Subset ➡ Upload



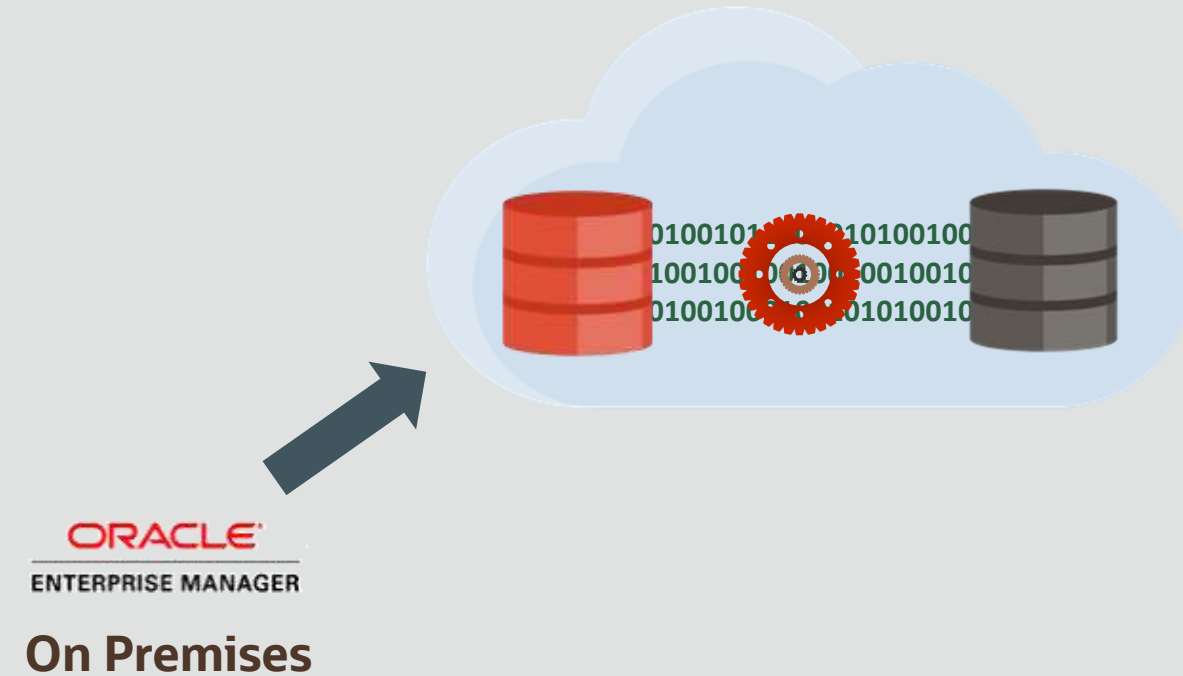
Mask on the Wire or in the Cloud

Oracle Database Cloud Service (PaaS)

Clone & Mask PDB to Cloud



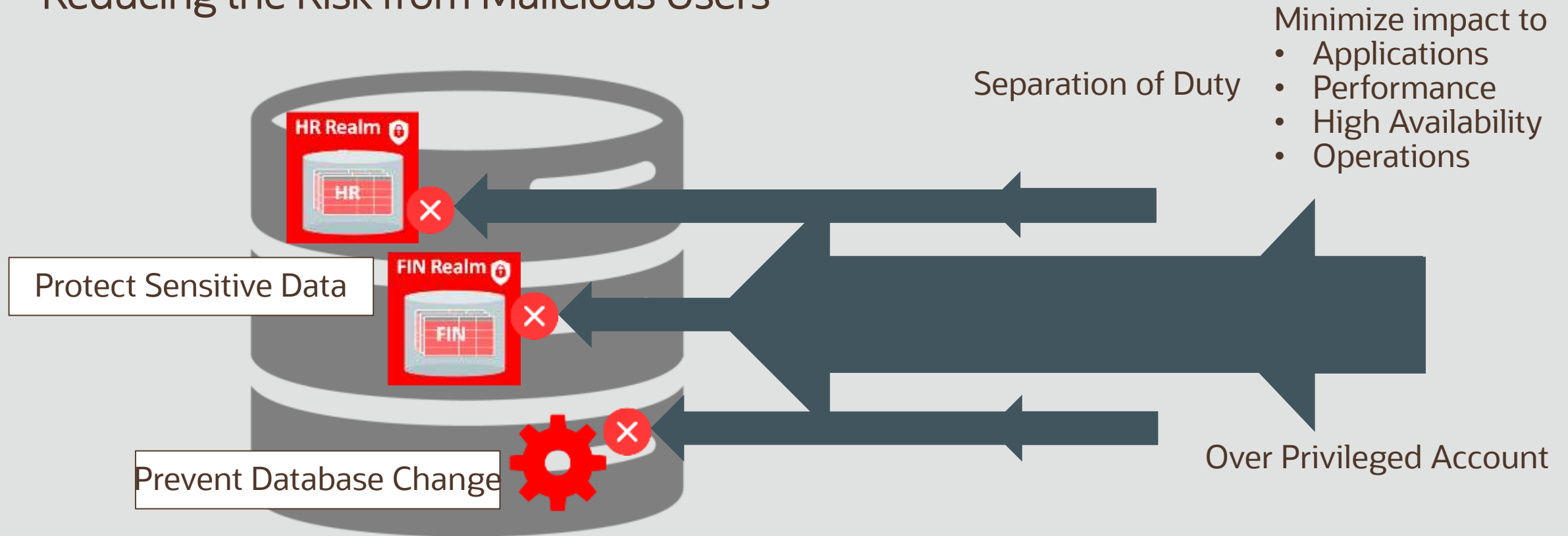
Mask/Subset in the Cloud



Database Vault

Oracle Database Vault

Reducing the Risk from Malicious Users



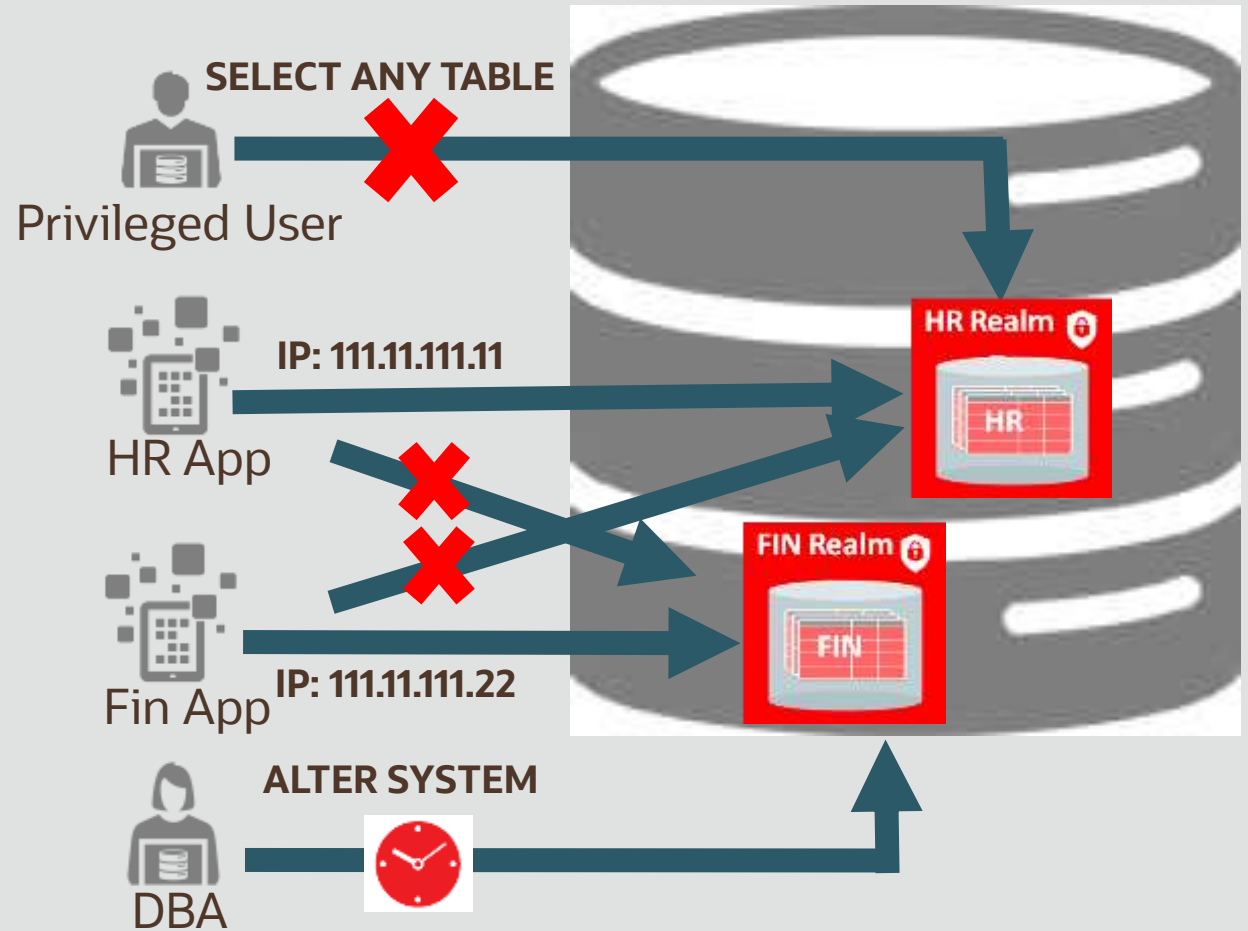
Oracle Database Vault

Realms and Command Rules Protect Sensitive Schemas and Objects

Protect sensitive data from privileged accounts

Enforce a trusted path to prevent application by-pass

Control database changes for security and compliance



Oracle Database Vault

Manageability

Starting with 12c, installed with Oracle Database Enterprise Edition

Configure, enable using two PL/SQL calls

Manage with Oracle Enterprise Manager or API

Protection travels with PDB unplug and backups

Integrated with Oracle High Availability options (Data Guard, RAC...)

Less than 2% performance overhead with Oracle application testing

Oracle Database Vault

Management: Reporting Attempted Violations

Database Vault Configuration Issues

Database Vault Enforcement Audit Reports

- Realm Audit Report**
- Command Rule Audit Report
- Factor Audit Report
- Label Security Integration Audit
- Core Database Vault Audit Trail
- Secure Application Role Audit

Realm Audit Report OK

The Realm Audit Report shows audit records generated by the realm protection and realm authorization operations. You can use this information to investigate attempts to break security.

Search

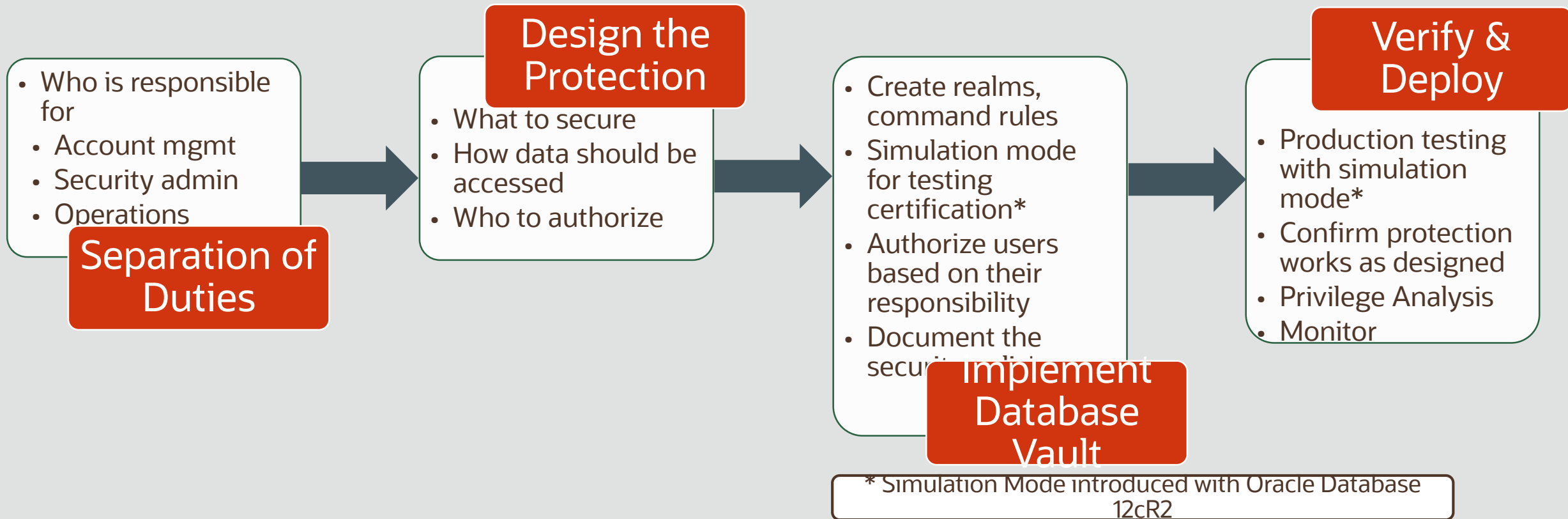
View

Timestamp	Violation	Account	Command	Realm Name
2013-08-06 10:15:05.0 PST...	Realm Violation Audit	OE	SELECT * FROM HR.EMPLOYEES	HR Application Protection
2013-08-06 10:13:59.0 PST...	Realm Violation Audit	OE	SELECT * FROM HR.EMPLOYEES	HR Application Protection
2013-08-06 10:13:38.0 PST...	Realm Violation Audit	OE	SELECT * FROM HR.EMPLOYEES	HR Application Protection
2013-08-06 10:05:07.0 PST...	Realm Violation Audit	OE	SELECT * FROM HR.EMPLOYEES	HR Application Protection
2013-08-06 10:02:22.0 PST...	Realm Violation Audit	OE	SELECT * FROM HR.EMPLOYEES	HR Application Protection

Attempted violations

- Audit on Failure, Success, both or none
- Collected by Database Vault reports, Unified Audit and Oracle Audit Vault and Database Firewall

Deployment Guidelines for Oracle Database Vault



What is an Oracle Autonomous Database?

Oracle Autonomous Database

Family of Cloud Services Introduced in 2018



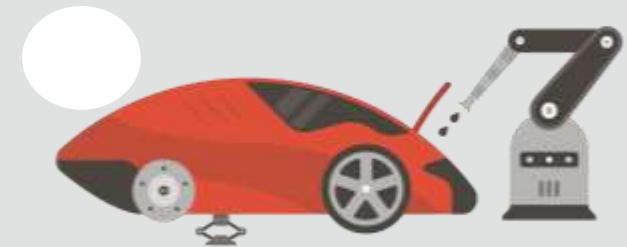
Self-Driving

Automates all database and infrastructure management, monitoring, tuning



Self-Securing

Protects from both external attacks and malicious internal users



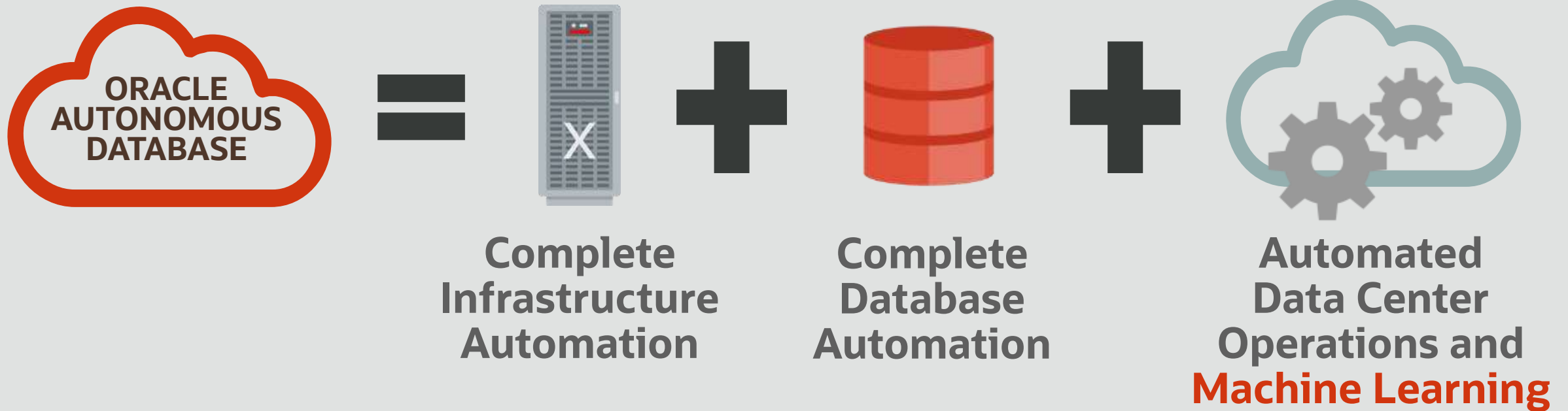
Self-Repairing

Protects from all downtime including planned maintenance

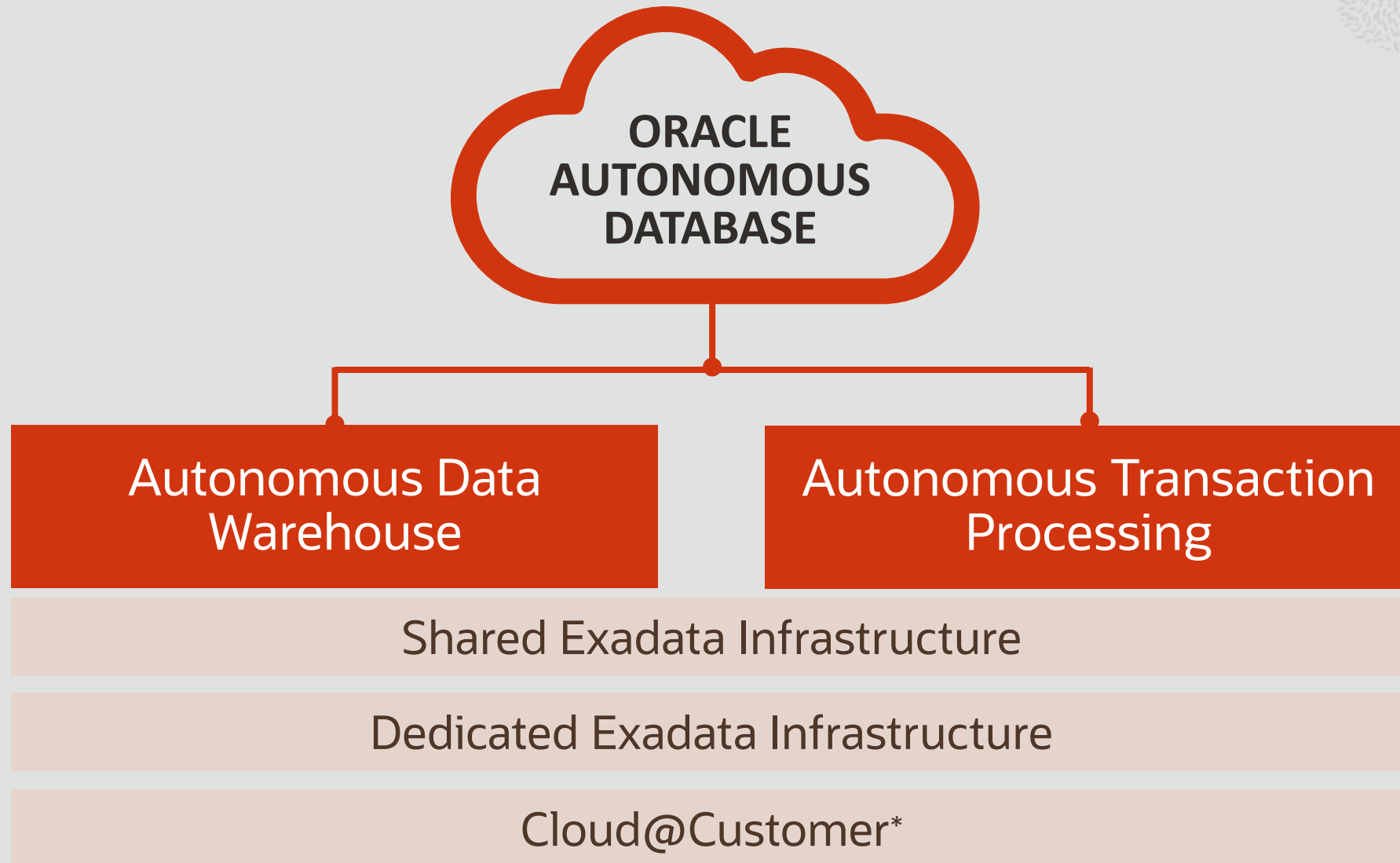
Spend Less, Reduce Risk, Innovate More

Oracle Autonomous Database | What's Inside?

Eliminates All the Complexity of Mission Critical Databases



Oracle Autonomous Database | Deployments



Top 10 Capabilities of Autonomous Database Technology

- 1 Auto-Provisioning**
Automatically deploys mission-critical databases (RAC on Exadata infrastructure) which are fault-tolerant and highly available. Enables seamless scale-out, protection in case of a server failure and allows updates to be applied in a rolling fashion, while apps continue to run.
- 2 Auto-Configuration**
Automatically configures the database to optimize for specific workloads. Everything from the memory configuration, data formats, and access structures are optimized to improve performance. Customers can simply load data and go.
- 3 Auto-Scaling**
Automatically scales compute resources when needed by workload. All scaling occurs online, while the application continuously runs. Enables true pay per use.
- 4 Auto-Indexing**
Automatically monitors workload and detects missing indexes that could accelerate applications. It validates each index to ensure its benefit, before implementing it and uses machine learning to learn from its own mistakes.
- 5 Automated Security**
Automatic encryption for the entire database, backups and all network connections. No access to OS or admin privileges prevents phishing attacks. Protects the system from both cloud operations and any malicious internal users.
- 6 Automated Data Protection**
Automatically protect sensitive and regulated data in the database, all via a unified management console. Assess the security of your configuration, users, sensitive data, and unusual database activities.
- 7 Auto-Patching**
Automatically patch or upgrade with zero downtime. Applications continue to run as patching occurs in a round-robin fashion across RAC nodes or servers.
- 8 Auto-Backups**
Automatic daily backup of database or on-demand. Restore or recover a database to any point-in-time you specify in the last 60 days.
- 9 Automated Detection and Resolution**
Using pattern recognition, hardware failures are automatically predicted without long timeouts. IOs are immediately redirected around unhealthy devices to avoid database hangs. Continuous monitoring for each database automatically generates service requests for any deviation.
- 10 Automatic Failover (Coming Soon)**
Automatic failover with zero-data loss to standby. It's completely transparent to end-user applications. Provides 99.995% SLA.

Self-Securing | Encryption by Default

Secure by default

Encryption for Data at Rest



- Automatically configured
- All application data is encrypted within the database at the tablespace level
- Database Backups are also encrypted

Encryption for Data in Motion



- Automatically configured
- All network access is encrypted to and from the database
- Choice of two methods
 - Oracle Native Network Encryption
 - Transport Layer Security (TLS) v1.2 (default)
- Oracle client credentials can be downloaded via encrypted wallet files

Self-Securing | Auditing

Users are unable to disable security configurations

- Autonomous Database leverages Oracle Unified Audit to capture security-relevant activity

Login failures

Changes to users, including creation of new accounts,
grants of privileges or roles

Changes to database structures, including tables, procedures,
and synonyms



- Customers have access to all audit data via the `UNIFIED_AUDIT_TRAIL` view
- The `DBMS_FGA` package can be used to add more policies

Self-Securing | Auto Patching

Automatic patching without downtime



Automatic Patching of all components (on-demand for critical security issue)

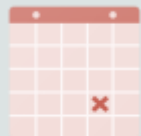
Firmware, OS, Hypervisor, Clusterware, Database



Patches applied in a rolling fashion across RAC nodes and Exadata storage servers

Database is continuously available to application

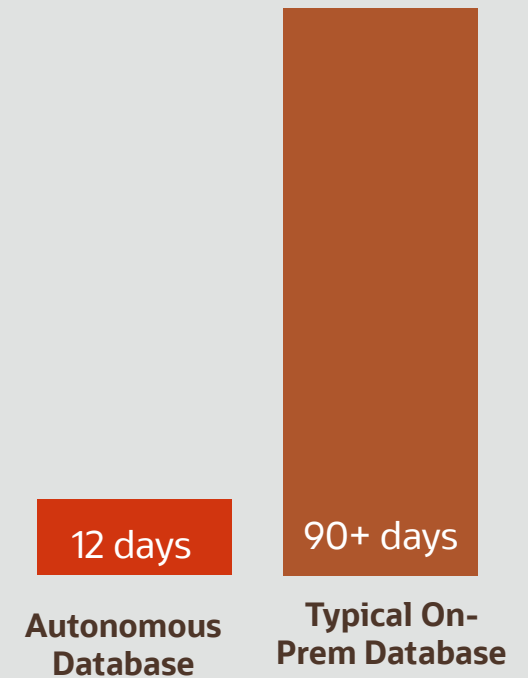
Applications using Application Continuity best practices, run without interruption



Patching is automatically scheduled

Customer can adjust patching window within a time range on Dedicated deployments

Average number of days between database patches



Self-Securing | Separation of Duty

*Security Is a **Shared** Responsibility*

Security Managed by Oracle

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



Security Managed by the Customer

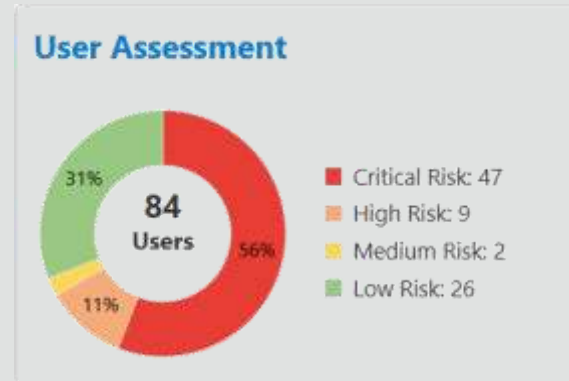
- Ongoing security assessments
- Users & Privileges
- Sensitive data discovery
- Data protection
- Activity auditing



Self-Securing | Oracle Data Safe

Automated Data Protection

- Unified database security control center
 - Security configuration assessment
 - User risk assessment
 - User activity auditing
 - Sensitive data discovery
 - Data masking
- Defense in depth for all customers
 - Saves time and mitigates security risks
 - No special security expertise needed
- Free with all Oracle Cloud Databases





Data Safe

egységes felület

automatizált adatbiztonság

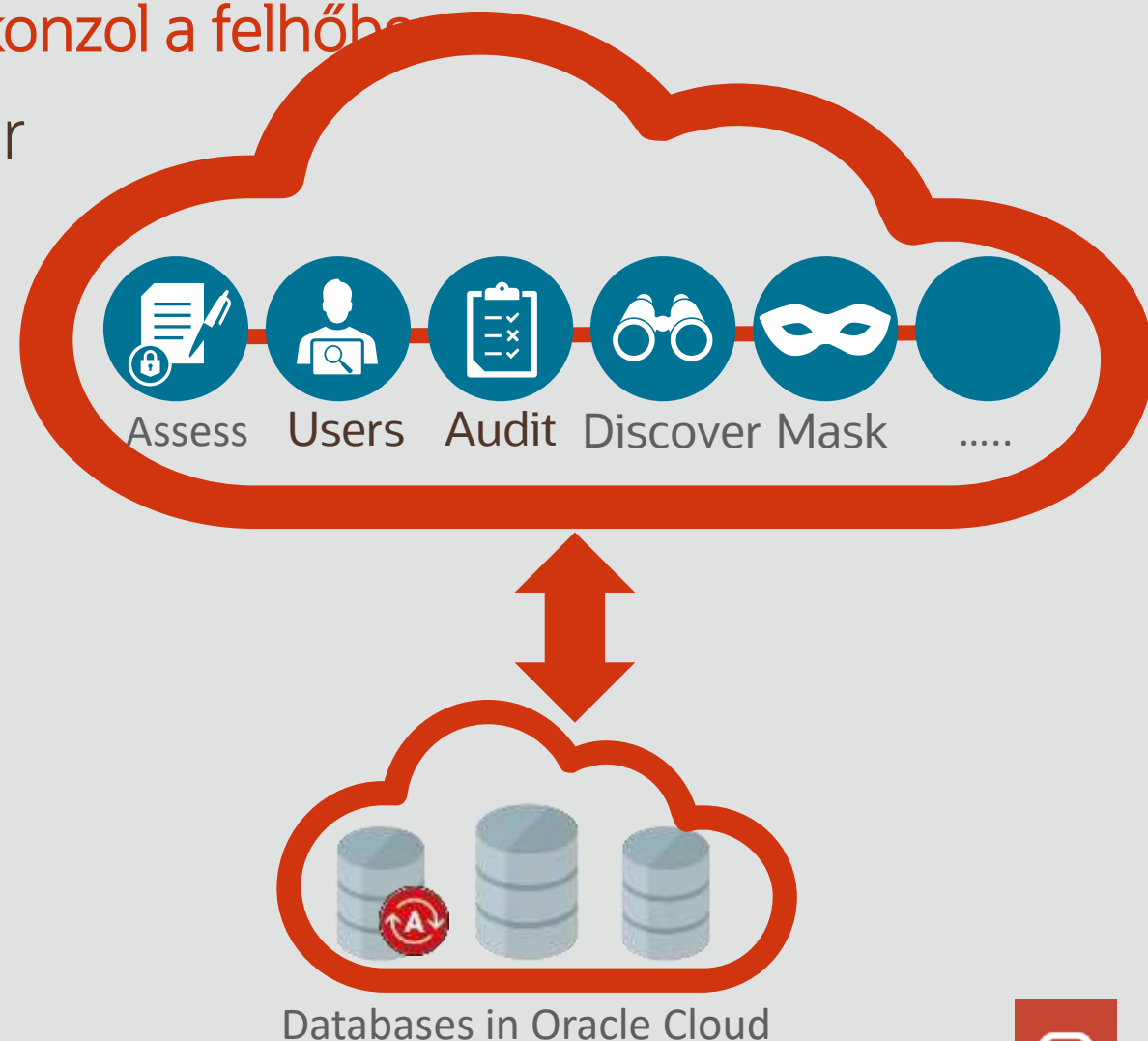
Oracle Data Safe

Egységes, ingyenes* adatbázis-biztonsági konzol a felhőben

- Egységes DB Security Control Center
 - Security Assessment
 - User Assessment
 - User Activity Auditing
 - Sensitive Data Discovery
 - Sensitive Data Masking
- Kezeli a DB-biztonsági kockázatokat
- Időt takarít meg
- Mélységi védelem
- Nincs szükség szakértői tudásra

* A legtöbb funkció ingyenes

Copyright © 2020 Oracle and/or its affiliates.



Security Assessment

User Assessment

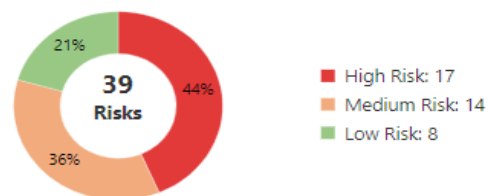
Data Discovery

Data Masking

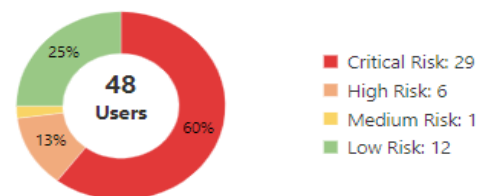
Activity Auditing

Filter by target

Security Assessment

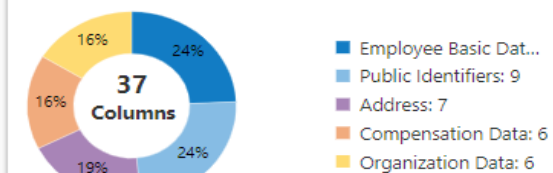


User Assessment



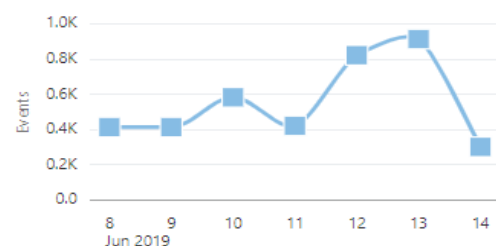
Data Discovery

Top 5 categories



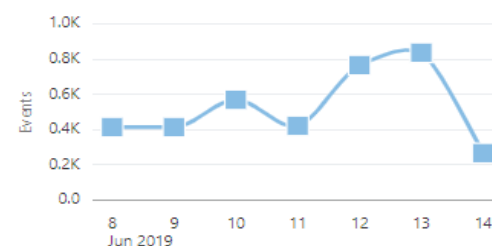
All Activity

Last 1 Week



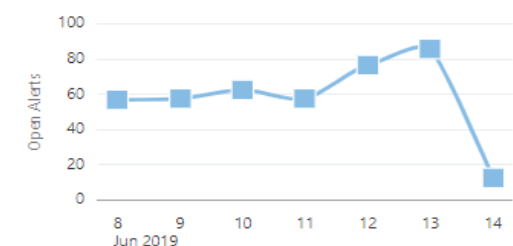
Admin Activity

Last 1 Week

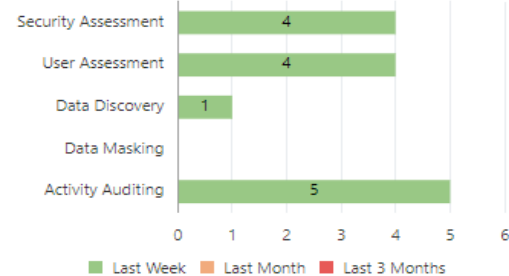


Open Alerts

Last 1 Week

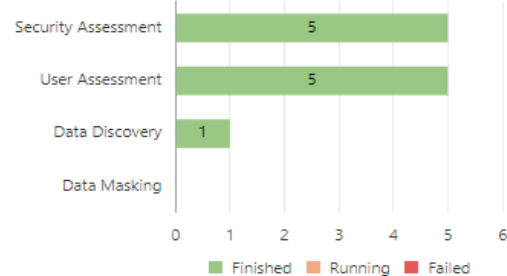


Feature Usage

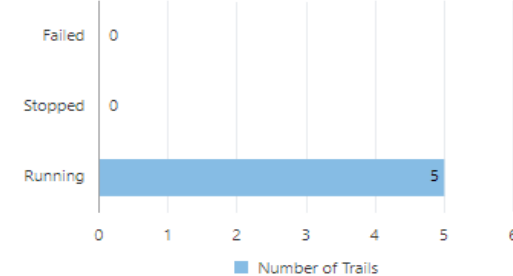


Jobs Summary

Last 1 Week



Audit Trails

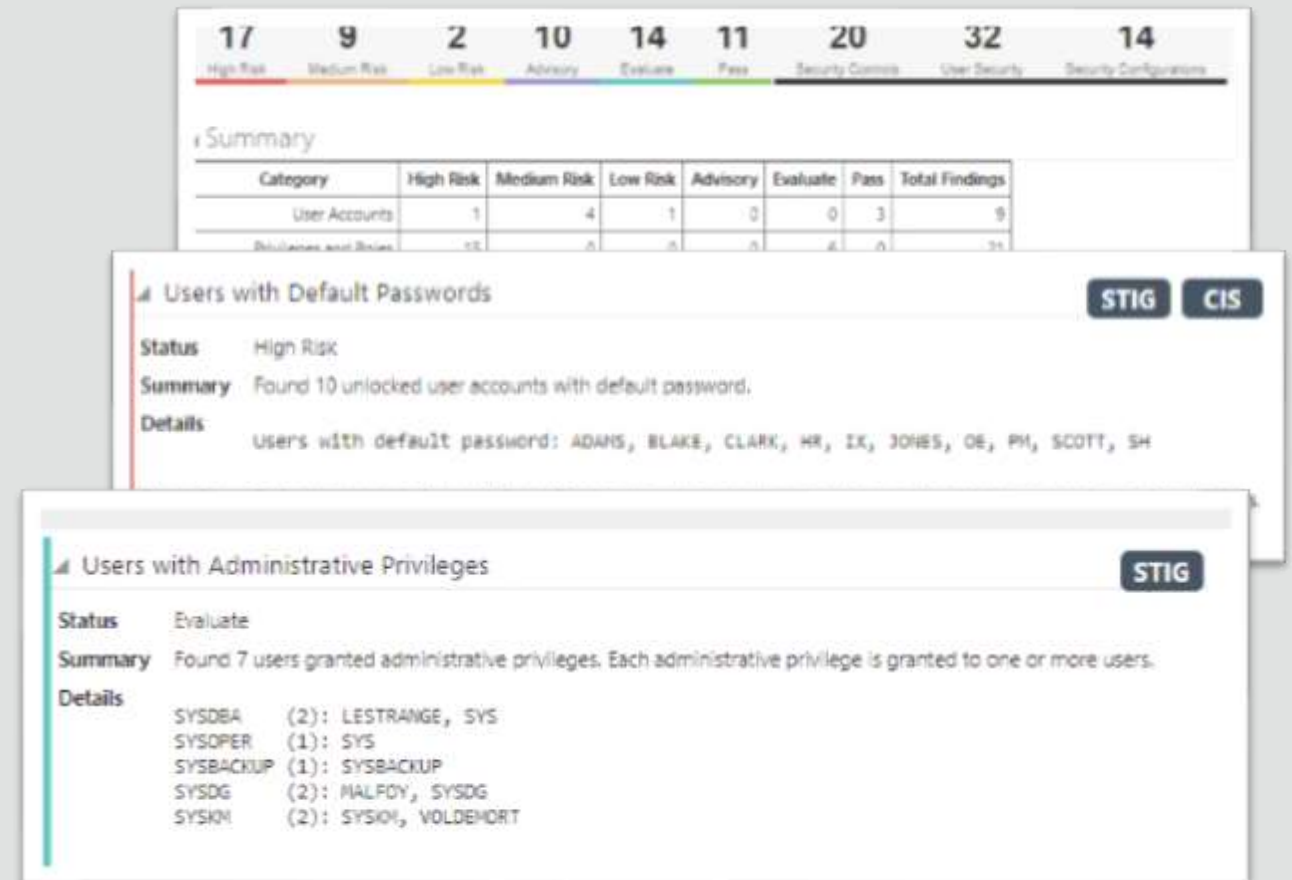


Database Security Assessment



Azonnali visszajelzés a konfiguráció kockázatairól

- Átfogó felmérés
 - Biztonsági beállítások
 - Biztonsági eszközök
 - Szerepkörök és privilégiumok
- Eltérés a legjobb gyakorlattól
- Riportok
 - Javaslatok fontossági sorrendben
 - Megfelelőségi leképezések (GDPR, STIG, CIS)

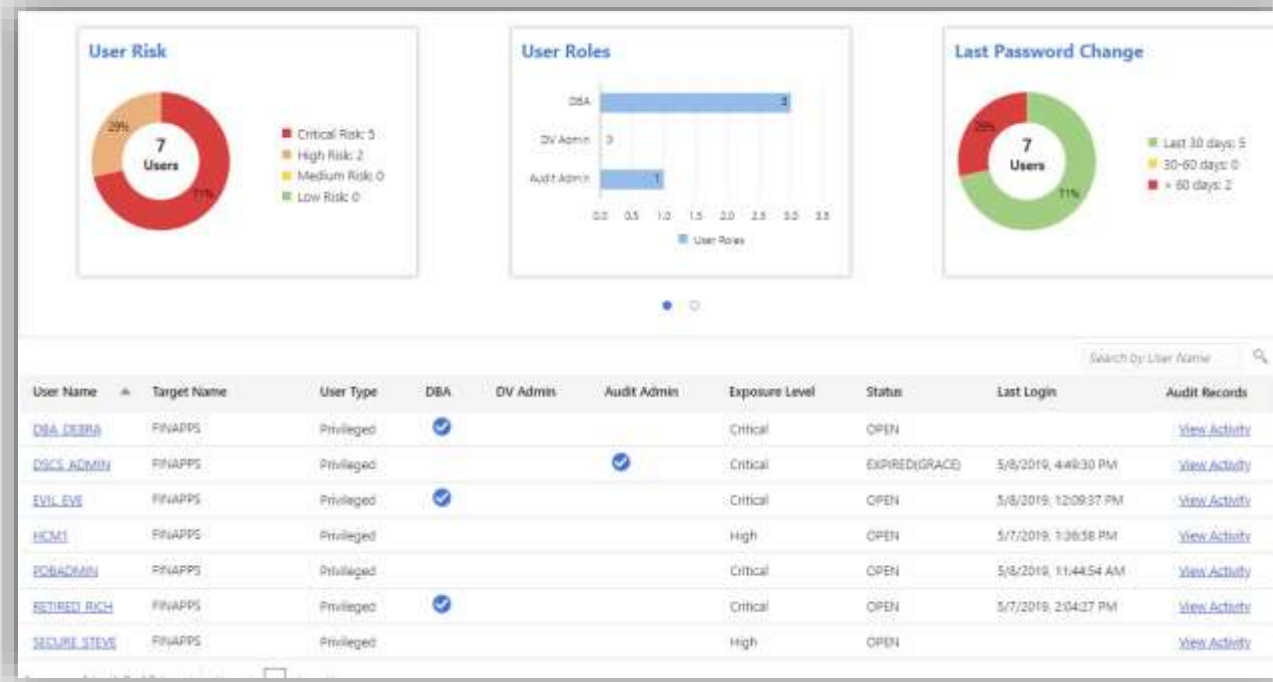


User Assessment



Felhasználói kockázatok csökkentése: roles/privileges/policies

- A túl sok jogosultsággal rendelkező felhasználók felderítése
- Statikus profilok kiértékelése: típus, jelszóbeállítások,...
- Dinamikus profilok kiértékelése: utolsó belépés / IP / jelszó változás, audit adatok, ...



Adatbázisok auditálása



Felhasználói tevékenységek auditálása, egyszerű riportálás

- Policy-k létrehozása: audit, megfelelőségi és riasztási
- Audit DB adatok összegyűjtése, érzékeny műveletek követése
- Audit riportok
 - Interaktív, nyomozáshoz
 - Összegző és részletes
 - PDF és xls exportálás: megfelelőség

Edit Policies [X]

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

Érzékeny adatok felderítése

Fontossági sorrendben segítség: hely, típus, mennyiség



- Felderít/besorol 125+ érzékeny adattípusokat
- Felhasználói érzékeny típusok
- Inkrementális felderítés
- Validált Fusion SaaS & EBS template-ek
- Csoportosítva riportál:
érzékeny adatok típusa, helye és mennyisége



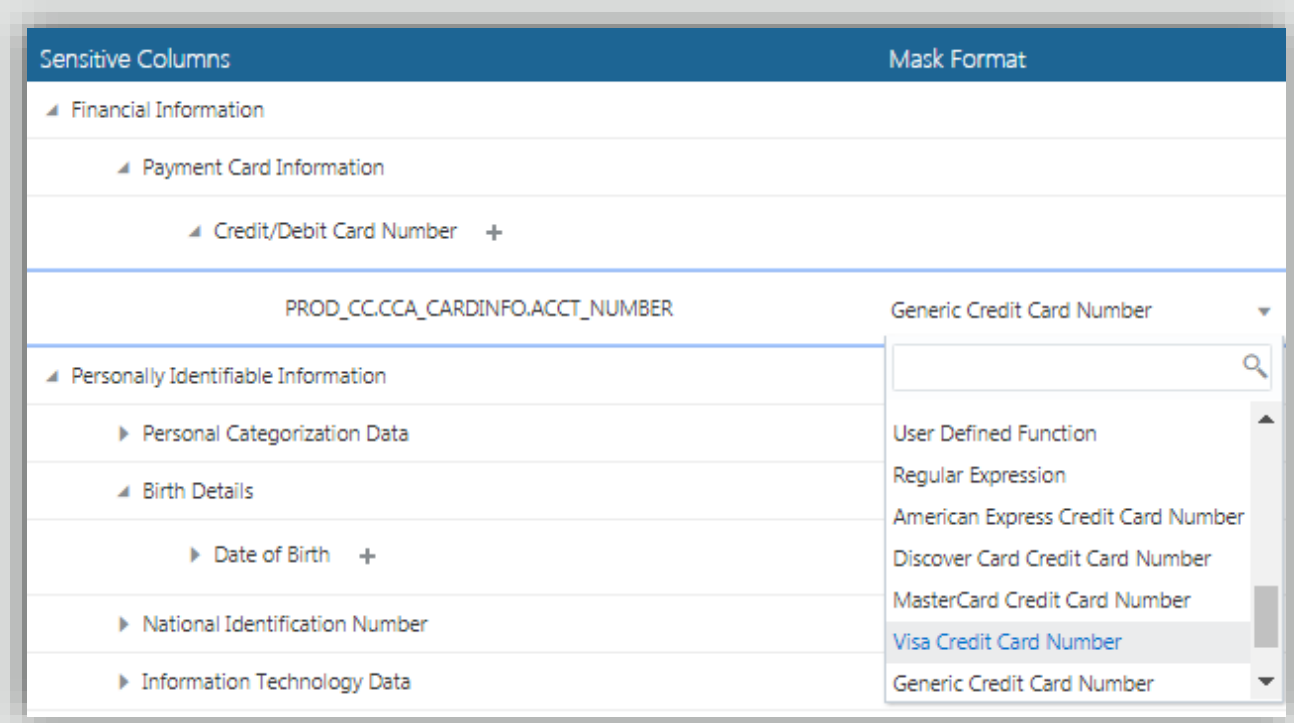
3.6M Sensitive Values	30 Sensitive Types
18 Sensitive Tables	57 Sensitive Columns

Adatmaszkolás érzékeny adatokra



Minimalizálja az érzékeny adatok kitettségét: teszt és fejlesztői környezetekben partnerek, elemzési adatbázisok

- Érzékenynek talált és megadott adatokra
 - 50+ predef. maszkolási formátum
 - Formátumok automatizált kiválasztása érzékeny adattípus alapján
 - Felhasználó által definiált maszkolási formátumok
- Gazdag transzformációs készlet, komplex esetekre is
- Maszkolási riport



Összefoglalás: Data Safe

Adatbázis-biztonsági szolgáltatás emelt szinten

- Egyszerűsített felület: célok: Database EE a felhőben
- Kiterjeszti a meglévő biztonsági infrastruktúrát egységes konzollal
 - Egyszerűen használható: néhány kattintás
 - Azonnal látható kockázatok: adatok, felhasználók, konfiguráció
 - Az iparág legteljesebb, gyakorlatban működő DB sec. megoldását használja
- „Demokrácia”: kis és nagy felhasználóknak is
- **Ingyenes** a felhő DB EE-k esetén
 - csak az audit rekordokra: 1 millió aud.rek. fölött /cél DB/hónap minimális díj

Data Safe Labs - https://is.gd/learn_datasafe <https://docs.oracle.com/en/cloud/paas/data-safe/learn.html>

Get Started

[Learn Oracle Data Safe](#)

Common Tasks

Architecture Overview

Books

Videos

Oracle Data Safe

Welcome to Oracle Data Safe! We're glad you're here. Oracle Data Safe is Oracle's platform for securing data in databases. As a native Oracle Cloud Infrastructure service, Oracle Data Safe lets you assess the security of your database configurations, find your sensitive data, mask that data in non-production environments, discover the risks associated with database users, and monitor database activity. The goal of the Hands On Labs is to teach you how to use each of the five main features of Data Safe. The labs are intended to be straight-forward and easy so no previous experience or expertise is needed!

Before starting, either you or your tenancy administrator needs to set up a target database in the Oracle Cloud. The labs refer to an Autonomous Transaction Processing (ATP) database. Please refer to the [Setup Guide](#).

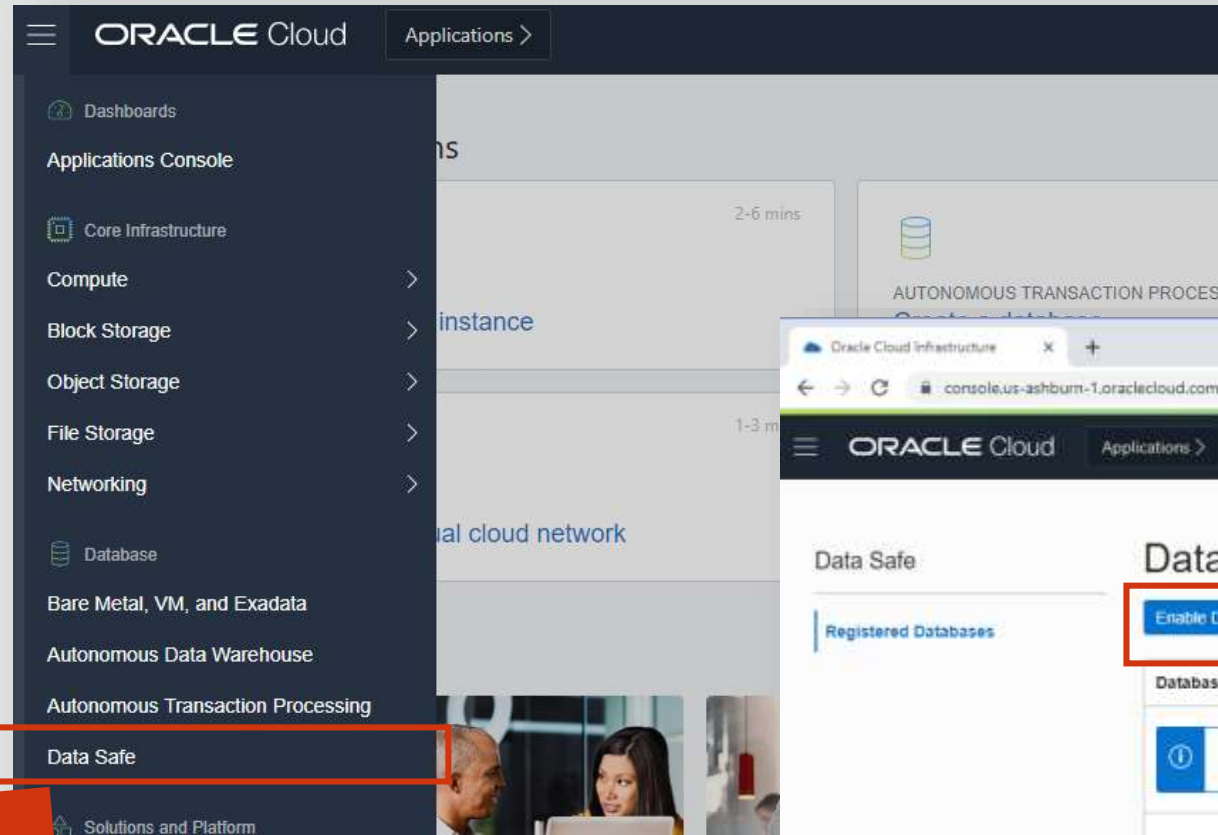
Hands on Labs - "The Fundamentals"

1. **View a registered target database:** We introduce you to the Oracle Data Safe Console and show you where your target database is listed.
2. **Provision audit and alert policies:** Start with the Activity Auditing feature and learn how to provision audit and alert policies on your target database.
3. **Analyze alerts and audit reports:** Continue with Activity Auditing to explore and analyze alerts as well as create a report.
4. **Assess database configurations and users:** Run User Assessment and Security Assessment jobs against your target database and then analyze the results.
5. **Discover and mask sensitive data:** Use the Data Discovery and Data Masking features to find sensitive data on your target database and then mask it.

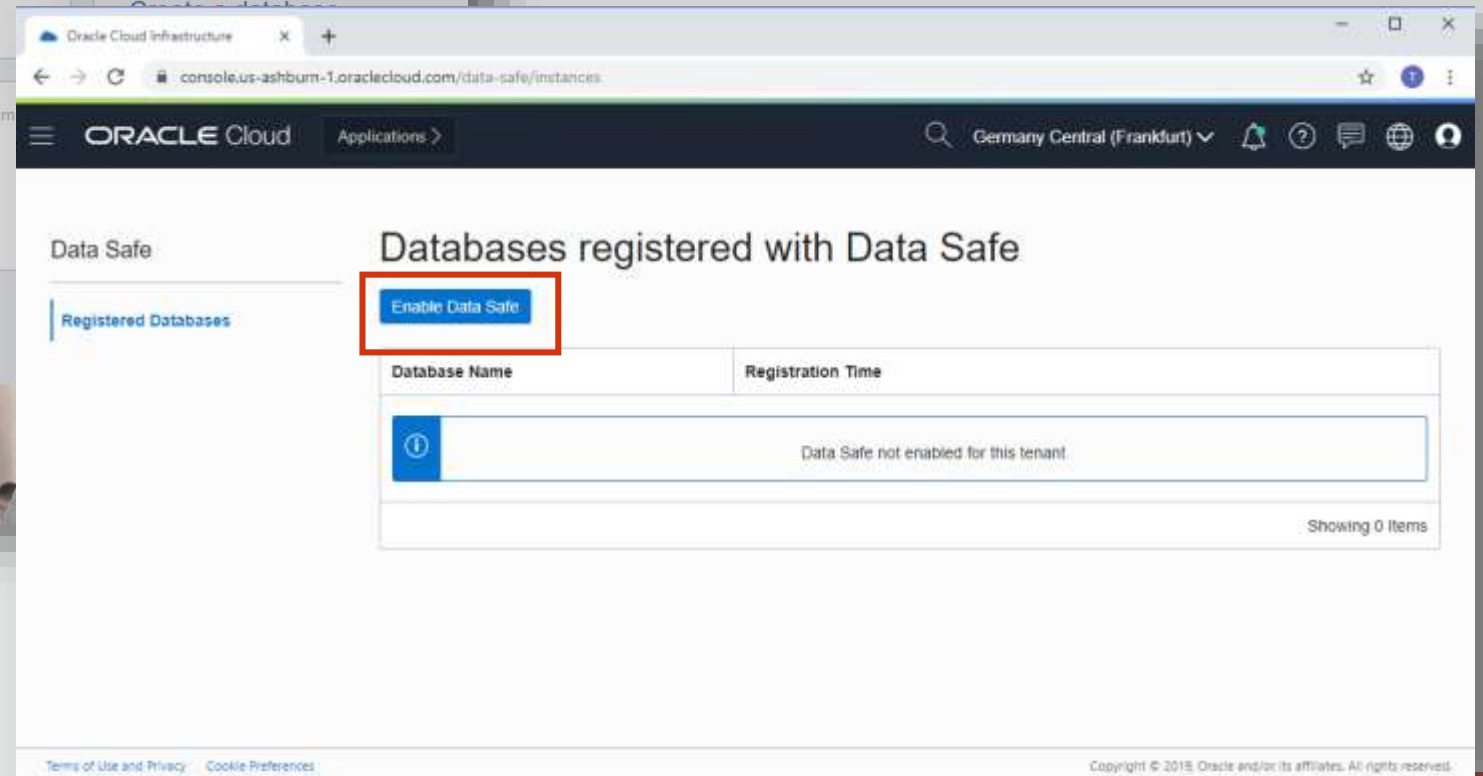
Click [here](#) to get started.

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

2 Press the Enable Data Safe button

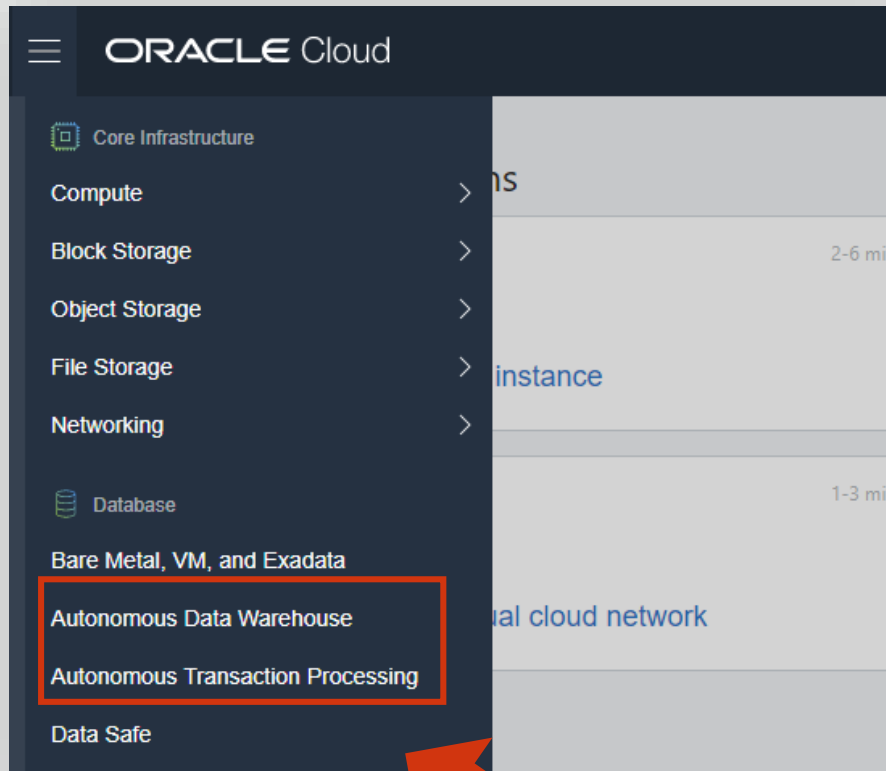


1 Select Data Safe in the OCI menu under Database → Data Safe

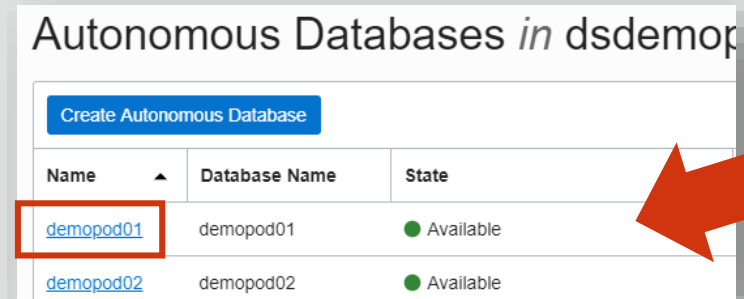


Enable Data Safe > Register a database > Access the Data Safe Console > Run an assessment

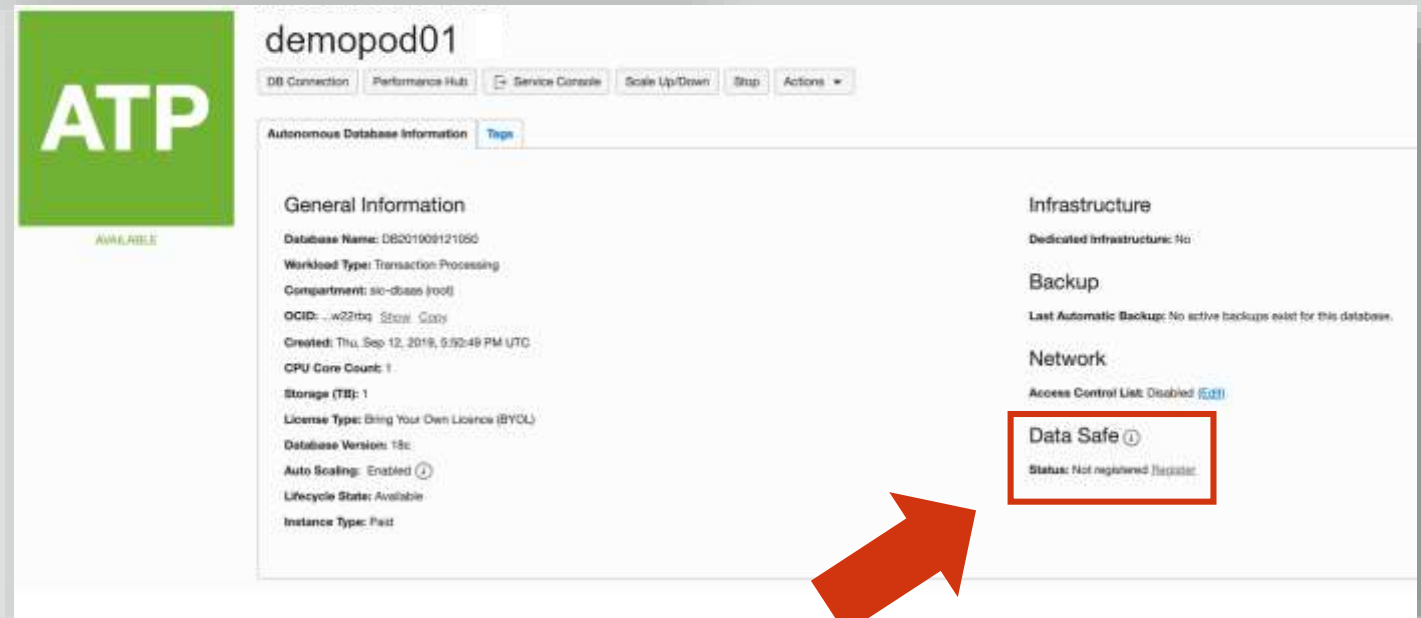
Autonomous Database: ATP/ADW, ami forradalmian alkalmazkodó



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



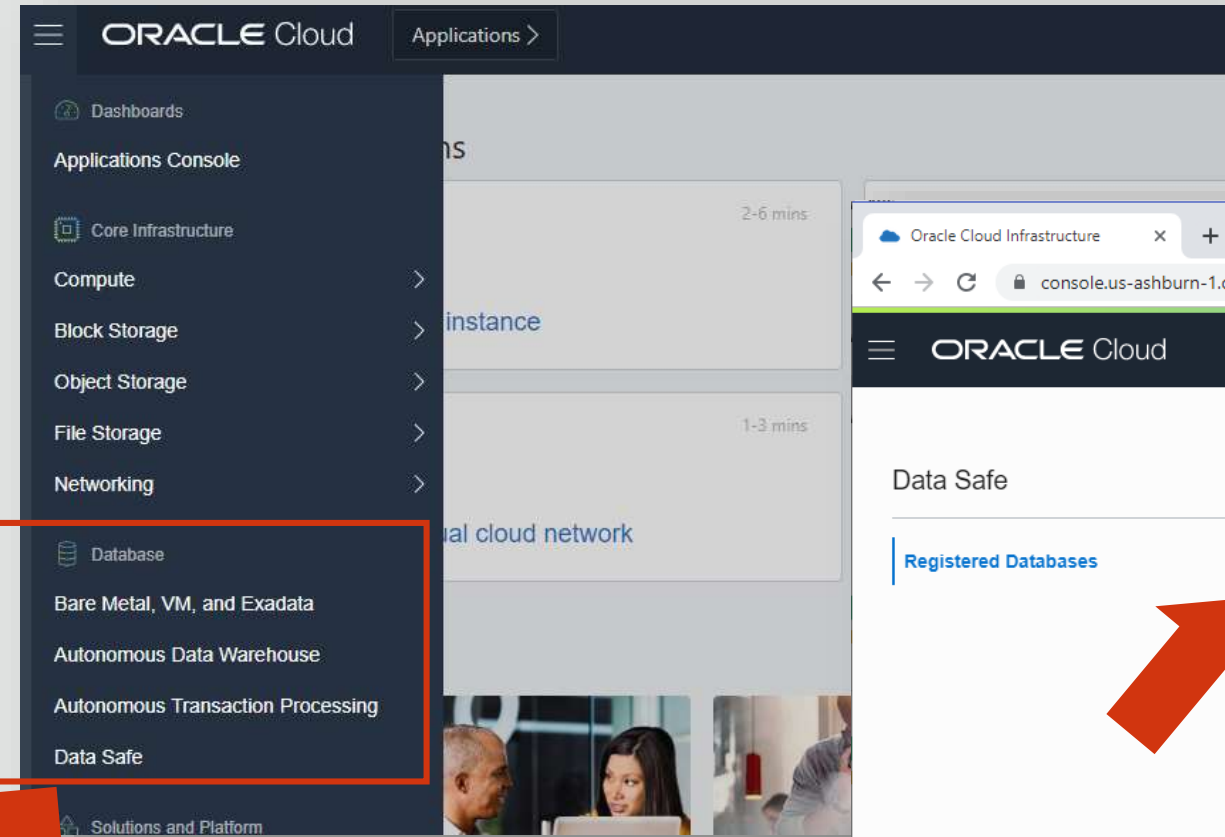
2 Select your database



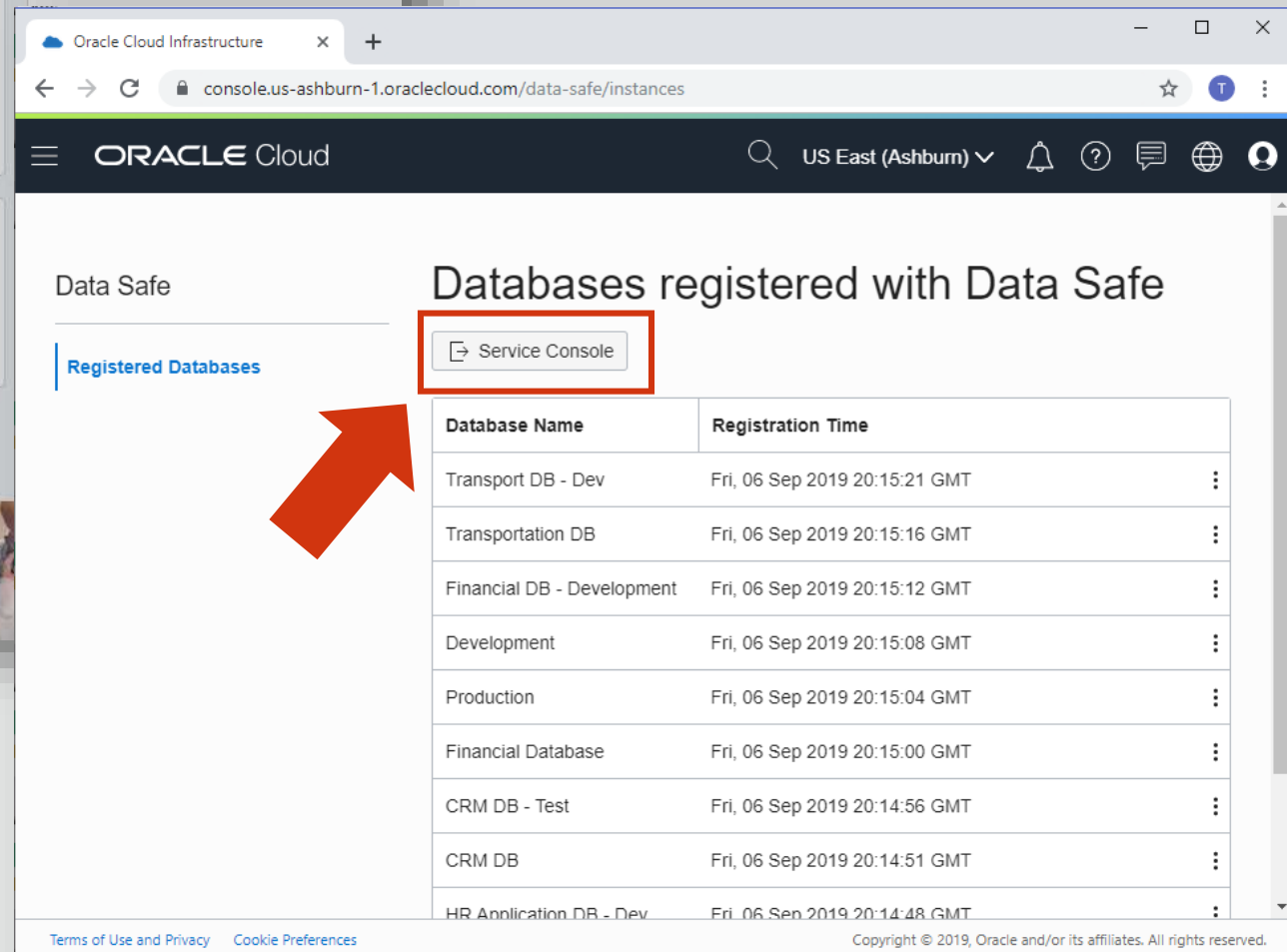
3 Press the register button under Data Safe → Register

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

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

Other Cloud DBs

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 '1 In the Data Safe console, 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'.

1

In the Data Safe console,
select Targets → + Register

The 'Register Target' dialog box is shown, with fields for 'Target Name', 'Target Type' (set to 'Oracle Database'), 'Target Description', and 'Resource Group'. Below these is the 'Target Connection Details' section, which includes fields for 'OCID', 'Connection Type' (set to 'TCP'), 'Hostname/IP Address', 'Port Number', 'Database Service Name', 'Database User Name', and 'Database Password'. A red arrow points from the text '2 Fill out the connection details' to the 'Target Connection Details' section. At the bottom of the dialog are buttons for 'Cancel', 'Test Connection', and 'Register Target'.

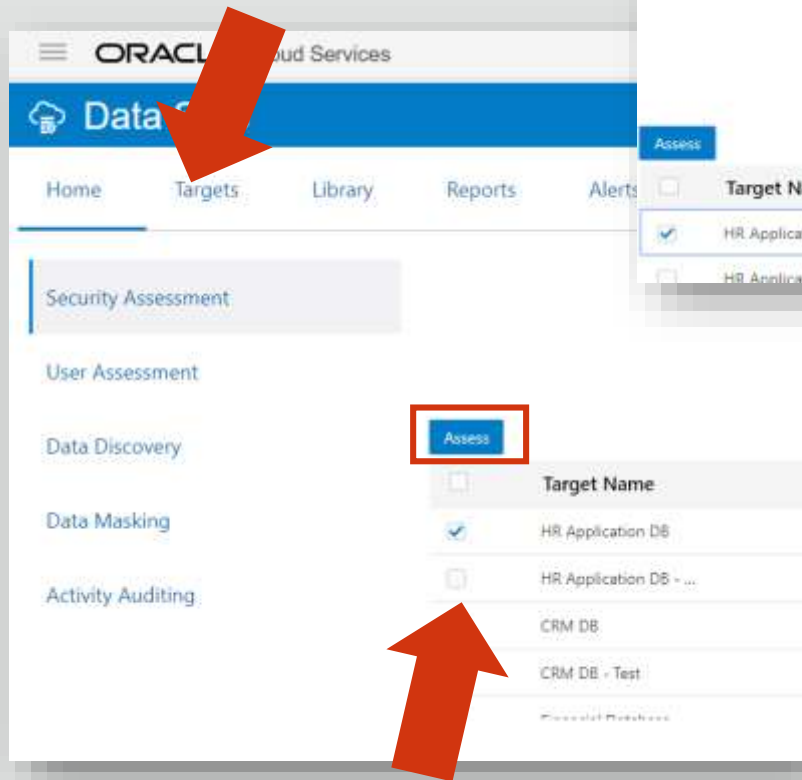
2

Fill out the connection details

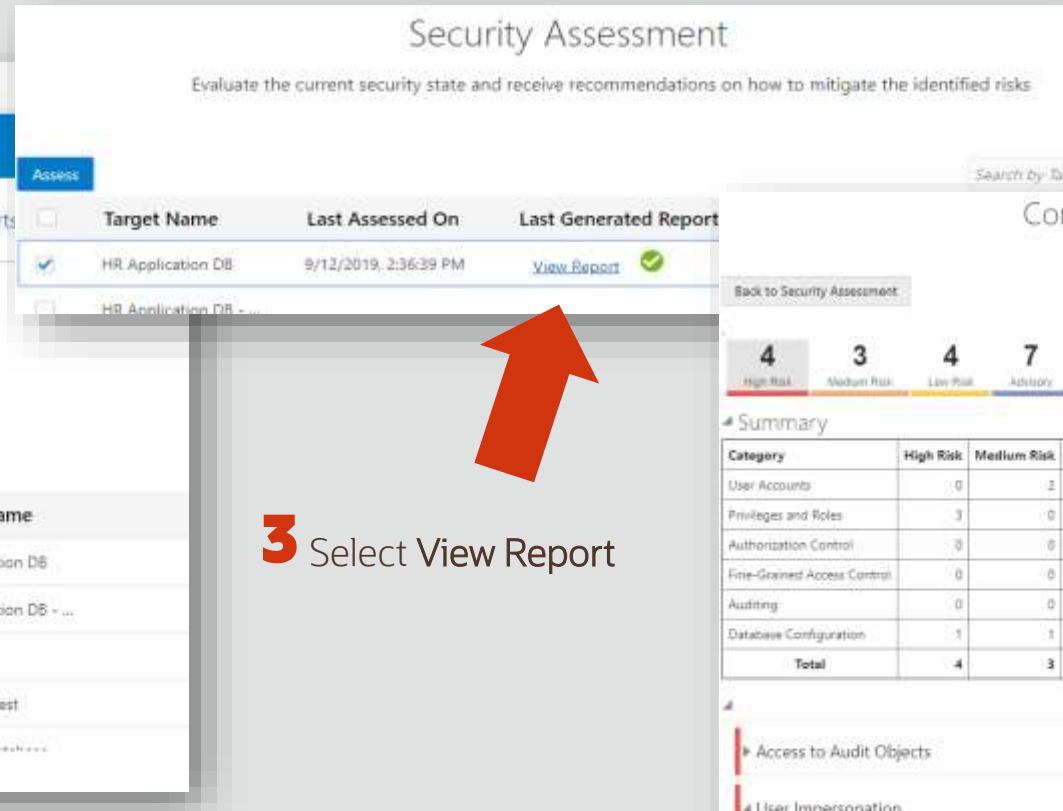


Enable Data Safe > Register a database > Access the Data Safe Console > Run an assessment

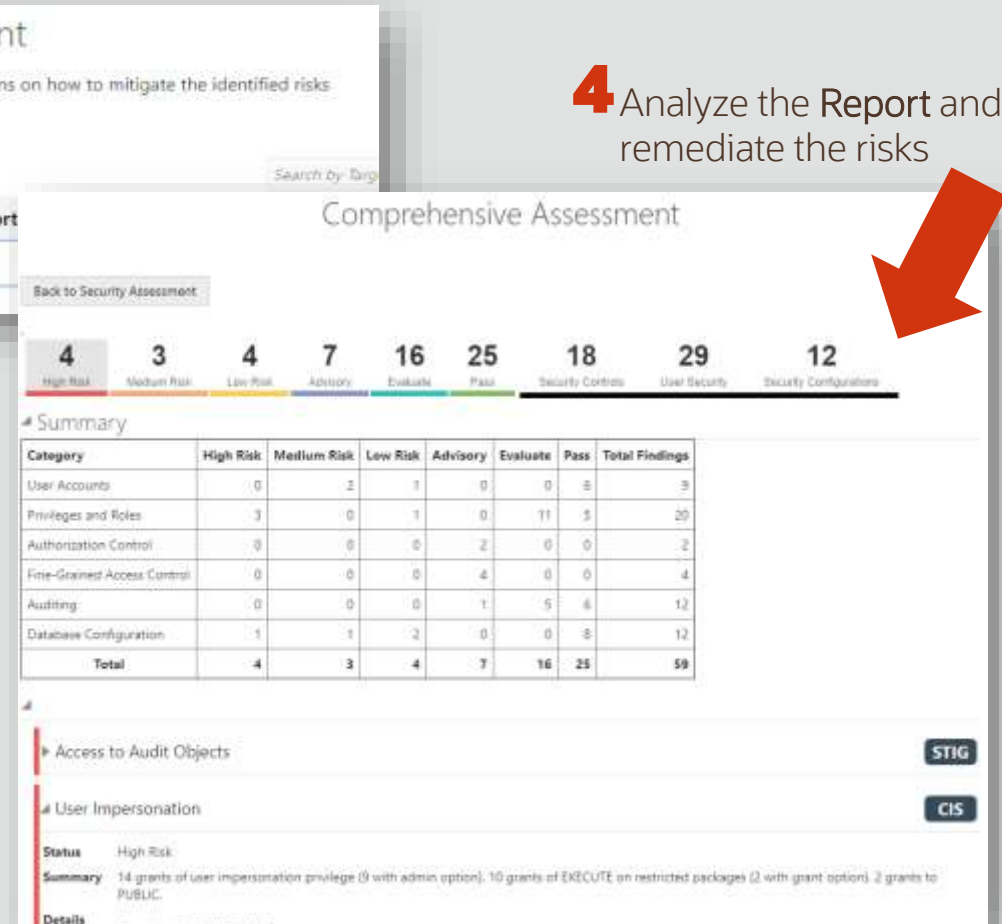
1 Select Security Assessment in the Data Safe Console



2 Select the target database and press the Assess button



3 Select View Report



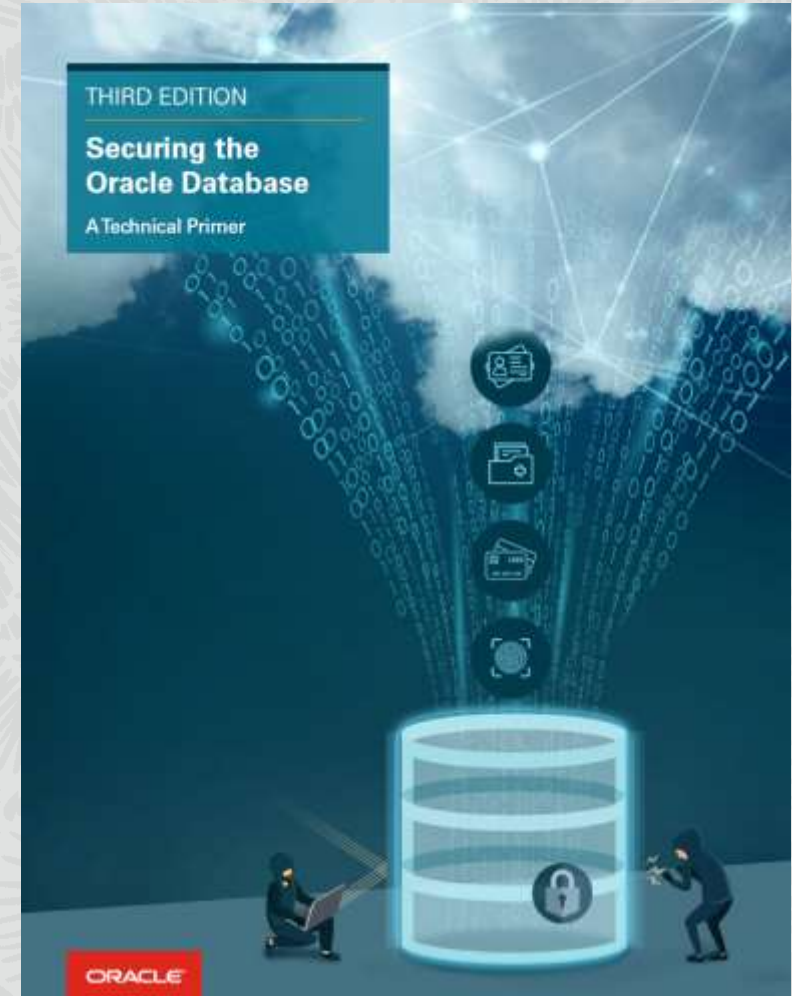
4 Analyze the Report and remediate the risks

Securing the Oracle Database

– A Technical Primer

Chapters

- Protecting Data
- Authentication and Authorization
- Enforcing Separation of Duty
- Data Encryption and Key Management
- Masking Sensitive Data
- Auditing Database Activity
- Activity Monitoring with Database Firewall
- Data-Driven Application Authorization
- Evaluating Security Posture
- EU GDPR and Database Security
- Securing Databases in the Cloud



oracle.com/securingthedatabase

Learn more about Database Security



AskTOM Database Security Office Hours

Direct line into Database Security Product Development

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

<http://bit.ly/asktomdbsec>

or Search “AskTom Database Security Office Hours”

köv. 2020. július 9. 11:00

Know more about Database Security:

<http://oracle.com/database/security>

Database Security Blog: <http://blogs.oracle.com/cloudsecurity/db-sec>

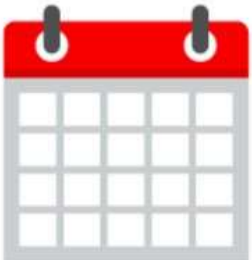
2020. június 30.
19h

Webcast

Discover Oracle's Machine Learning Platform

<https://go.oracle.com/LP=93669>

Oracle's Data-Science Apps Don't Require End User Data Science Skills



June 30, 2020
10 am PT/1 pm ET

[Click here if you are not zoltan.fekete@oracle.com](#) →

Business Email:

☐ Yes, send me emails on Oracle Products, Services, and E

[Register Now](#) →

Biztonságos mentés és helyreállítás Oracle adatbázis-környezetben

<https://go.oracle.com/LP=94307?elqCampaignId=233599>

Webinárium:

Biztonságos mentés és helyreállítás Oracle adatbázis környezetben



2020. július 1.
szerda
14:00 - 15:30

A mai vállalati informatika egyik legnagyobb kihívása az adatok védelme és mind a tervezett, mind a nem tervezett leállások minimalizálása. Ez

Kattintson ide, ha Ön nem „” zoltan.fekete@oracle.com

Üzleti e-mail cím:

zoltan.fekete@oracle.com

☐ Igen, küldjenek marketingcélú tájékoztatókat az Oracle te és eseményeiről.

Azonnali regisztráció →



Fekete Zoltán