ORACLE

AUTONOMOUS DATABASE LEARNING LOUNGE

Autonomous Database: SQL Firewall, because hackers deserve 404s

Autonomous Database Learning Lounge

Hosted by Marcos Arancibia

Autonomous Database Product Management

Agenda

Michelle Malcher

Topics

- Autonomous Database provides a high level of security for data including encryption, access control, auditing and compliance.
- Security patches are automatically applied reducing the risk of vulnerabilities.
- We will talk about this security framework in Autonomous Database and the new features that come with Oracle Database 23ai for privileges and in-database SQL Firewall.

Q&A

- Product Managers will answer any questions

Before we begin…

This session is for you !!!

Ask your questions using **Q&A**

Q&A

Product Managers are monitoring your questions

We will share links in **Chat**

Chat

The recording will be made available in a few days at
oracle.com/goto/adb-learning-lounge

Important links to bookmark

Links to get you started and to keep up to date with Autonomous Database

GET STARTED

1 New Get Started page:
oracle.com/autonomous-database/get-started/

2 Join us:

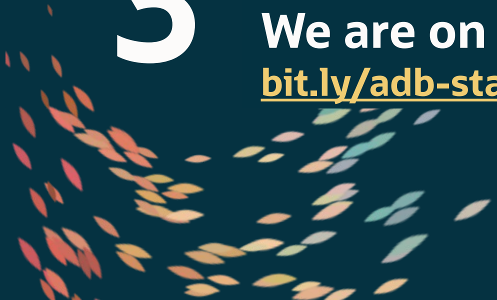
LinkedIn
bit.ly/adb-linkedin-grp

X
@AutonomousDW

Bluesky
autonomousdb.bsky.social

3 Got a question?
We are on stackoverflow
bit.ly/adb-stackoverflow

Join us on Developers Slack
(search #oracle-autonomous-database)
(odevrel_slack)

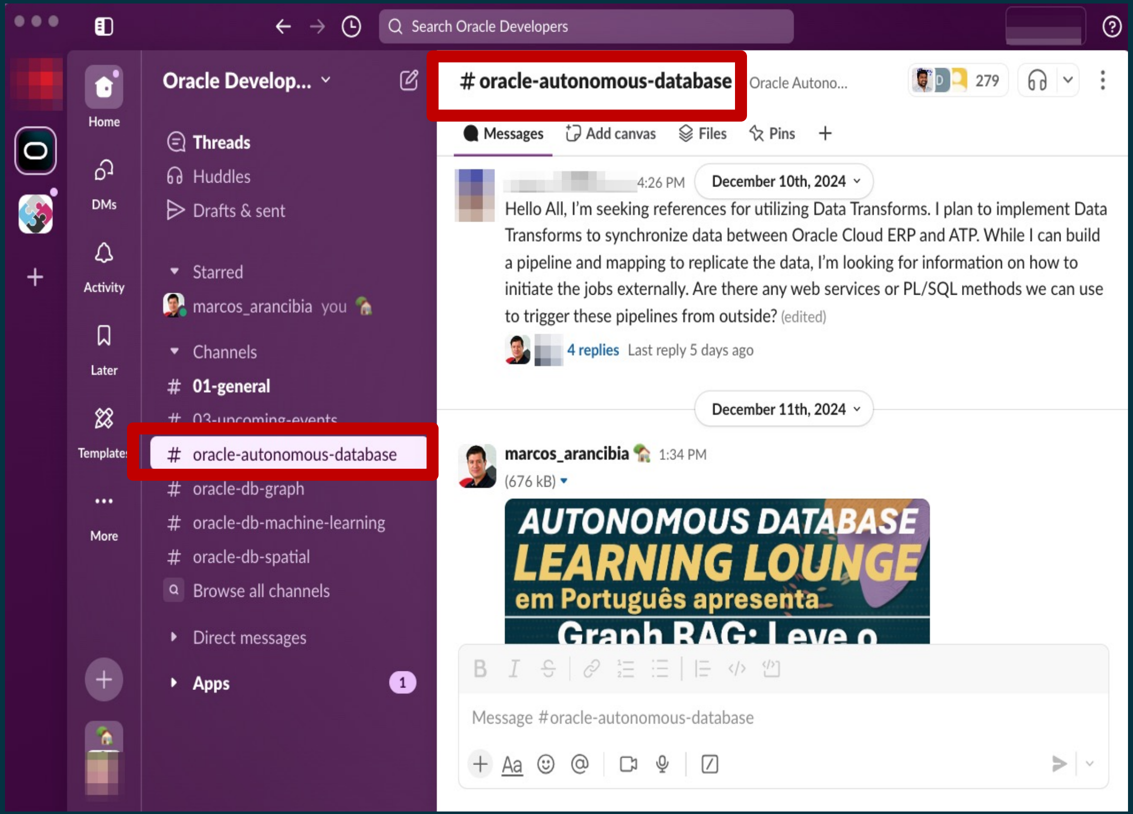


Join our External Slack

STEP 1: Join our Slack workspace at:

https://join.slack.com/t/oracledevs/shared_invite/zt-327lxqzeo-7cfyrWzWAY7curI7MCVF1w

STEP 2: search for #oracle-autonomous-database at the top and click on the Channel



December 10th, 2024

[redacted] 4:26 PM

Hello All, I'm seeking references for utilizing Data Transforms. I plan to implement Data Transforms to synchronize data between Oracle Cloud ERP and ATP. While I can build a pipeline and mapping to replicate the data, I'm looking for information on how to initiate the jobs externally. Are there any web services or PL/SQL methods we can use to trigger these pipelines from outside? (edited)

4 replies Last reply 5 days ago

December 11th, 2024

marcos_arancibia 1:34 PM

(676 kB)

Message #oracle-autonomous-database

Speaker

Michelle Malcher

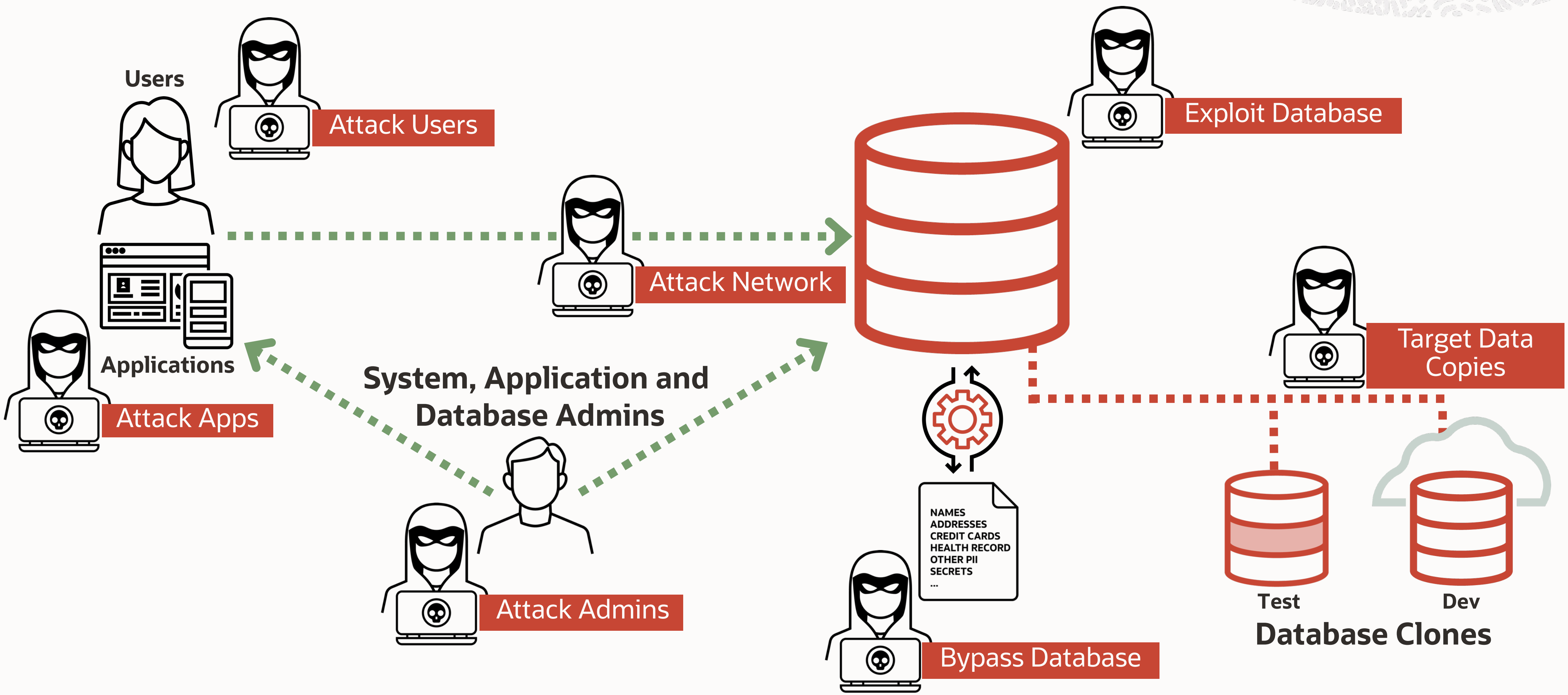
ORACLE

Autonomous Database
SQL Firewall, because hackers deserve 404s

Michelle Malcher

Director, Autonomous Database Product Management

How Do Hackers Attack the Database?



Common Reasons for Database Breaches

- Unencrypted data
- Security patches not applied
- Administrator Snooping
- Malware / Viruses
- Poor Network Isolation

Addressed by Autonomous Database

- Security configuration drift
- Unmanaged privileged users
- Unaudited users
- Untracked sensitive data
- Exposed sensitive data

Customer Responsibility

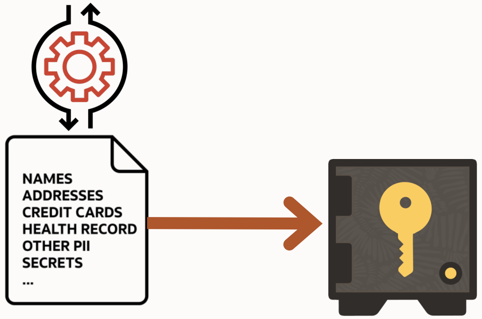
Autonomous Database Built-in Security and Tools

How do you protect the database?

Implement a secure configuration and monitor for configuration drift

- Check configuration against standards/best practices
- Verify that authentication is as strong as practical
- Review user privileges

Encrypt the data and protect the encryption keys



- Encrypt data in motion and at rest
- DO NOT rely on storage level encryption
- Securely manage encryption keys

Control access to the data

- Use database roles and privilege grants
- Control privileged user access
- Enforce separation of duties
- Establish and enforce a trusted path to data

Monitor access to the data

- Use native auditing capabilities to capture high-value activity
- Use network-based monitoring to examine ALL activity

Reduce risks with always-on security

Start with strong perimeter controls

Secure by default

- Customers are unable to disable security configurations
- No access to O/S, only access to database

Always up-to-date security patches

- Eliminates the largest security risk in current customer-managed systems

End-to-end encryption

- Full encryption for entire database, backups and all network connections

Infrastructure-level network isolation

- Customer Controlled CIDR
- Private or Public Subnet
- Security Lists and Gateways
- Network Security Groups, fully-managed firewalls

Cloud compartment/IAM controls

- LOB separation of duties
- Granular access controls to all ADB resource types

Customer configurable Access Control Lists

- ADB level isolation
- custom IP Address lists
- CIDR ranges

Database auditing always on

- Login failures and modifications to user accounts or database structures recorded
- No highly privileged access (system/sysdba/sysoper)

Reduce risk with clear separation of duties

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 customer

- Ongoing security assessments
- User roles & privileges
- Sensitive data discovery
- Data protection
- Activity auditing

cognizant

*The company's security is tighter than ever with OCI networking security, including **OCI Logging**, **Virtual Private Vault**, **Oracle Data Safe**, and Autonomous Data Warehouse security.*

*Cognizant has control over the **encryption keys** for data in the Autonomous Data Warehouse, while the IT team has ready access to **database audit data** and **centralized event logging** with OCI.*

The IT team also uses OCI Identity and Access Management to govern access management and update permissions in line with the hundreds of role changes that happen across Cognizant each week.

*This gives the company tight control over **who has access to sensitive financial data, down to the row level**.*

Security Zones of Control

Assess

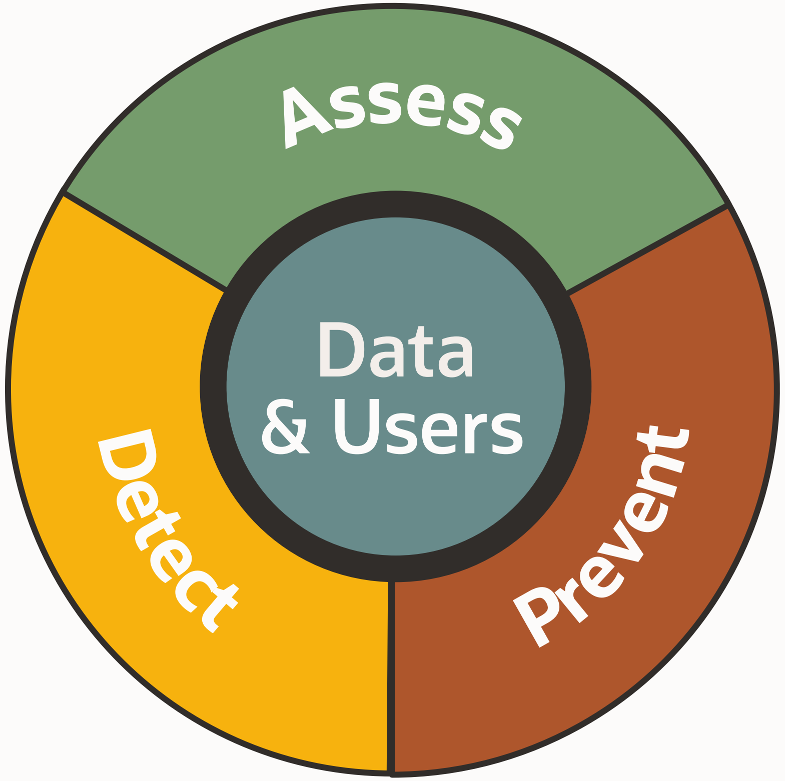
Assess the current state of the database

Detect

Detect attempts to access data, especially attempts that violate policy

Prevent

Prevent inappropriate or out of policy access to data



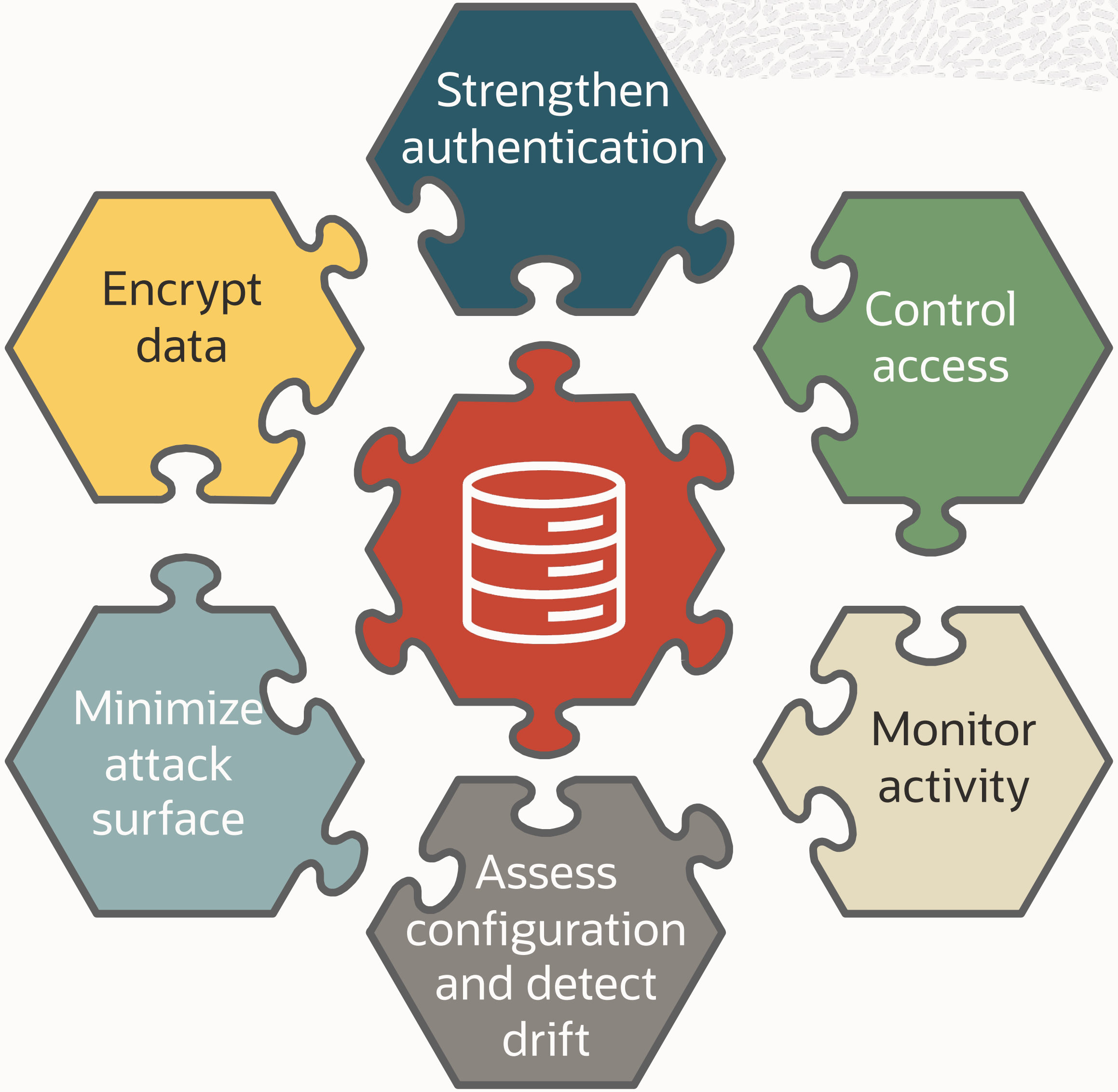
Data

In this case, data is stored in a database. Your organizations most valuable asset, but also a source of significant risk.

Users

Users and applications connect to your database to perform authorized business functions

Securing the Oracle Database



Strengthen authentication

Control access

Monitor activity

Assess configuration and detect drift

Minimize attack surface

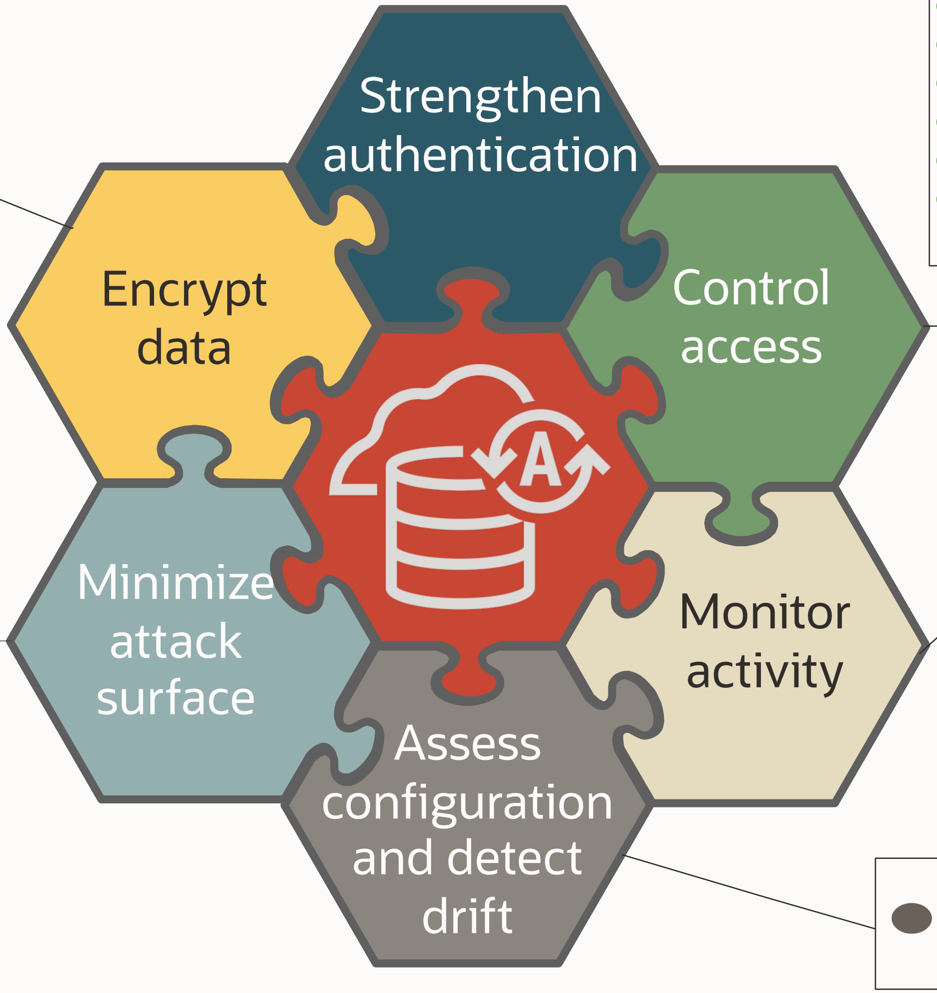
Encrypt data

Getting down to details

- Database *Strong Authentication*
- Database *Centrally Managed Users*
- Database *IAM integration*
- Database *Password Profiles*

- Database *Roles and Privileges*
- Database *Centrally Managed Users*
- Database *Virtual Private Database*
- Database *Real Application Security*
- Database *Blockchain and immutable tables*
- Database Vault
- SQL Firewall 23ai

- *Transparent Data Encryption*
- Key Vault
- Database *Transport Layer Security (TLS)*



- Database *Unified Auditing*
- Data Safe *Auditing*

- Data Safe *User Assessment*
- Database *Privilege Analysis*
- Data Safe *Masking*

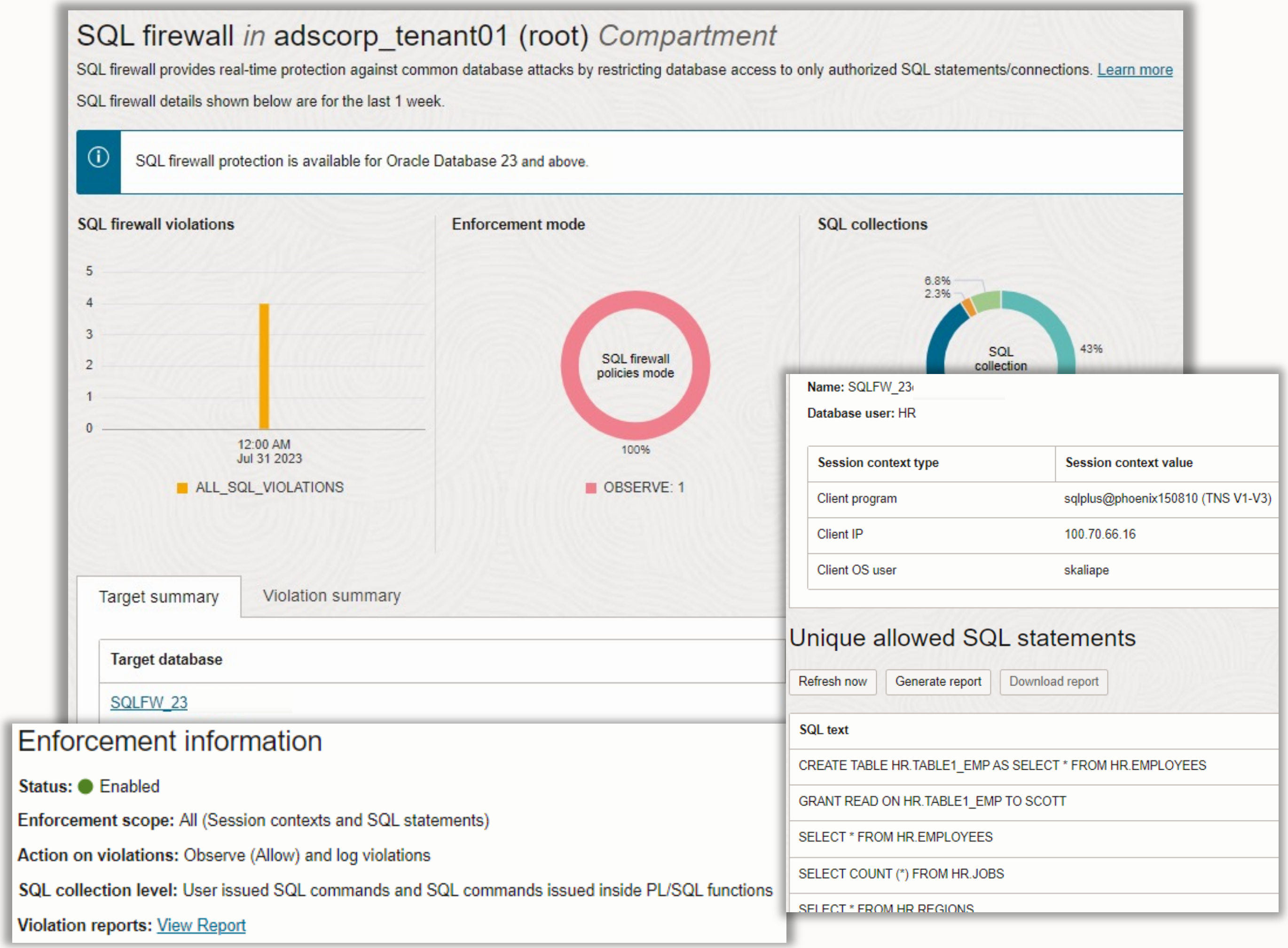
- Data Safe *Security Assessment*

New In 23ai

SQL Firewall management in Oracle Data Safe

Prevent SQL injection and access from unauthorized access points

- 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 *in* adscorp_tenant01 (root) *Compartment*

SQL firewall provides real-time protection against common database attacks by restricting database access to only authorized SQL statements/connections. Learn more

SQL firewall details shown below are for the last 1 week.

SQL firewall protection is available for Oracle Database 23 and above.

Target database
SQLFW_23

Name: SQLFW_23

Database user: HR

Session context type	Session context value
Client program	sqlplus@phoenix150810 (TNS V1-V3)
Client IP	100.70.66.16
Client OS user	skaliape

Unique allowed SQL statements

SQL text
CREATE TABLE HR.TABLE1_EMP AS SELECT * FROM HR.EMPLOYEES
GRANT READ ON HR.TABLE1_EMP TO SCOTT
SELECT * FROM HR.EMPLOYEES
SELECT COUNT (*) FROM HR.JOBS
SELECT * FROM HR.REGIONS

Enforcement information

Status: ● Enabled

Enforcement scope: All (Session contexts and SQL statements)

Action on violations: Observe (Allow) and log violations

SQL collection level: User issued SQL commands and SQL commands issued inside PL/SQL functions

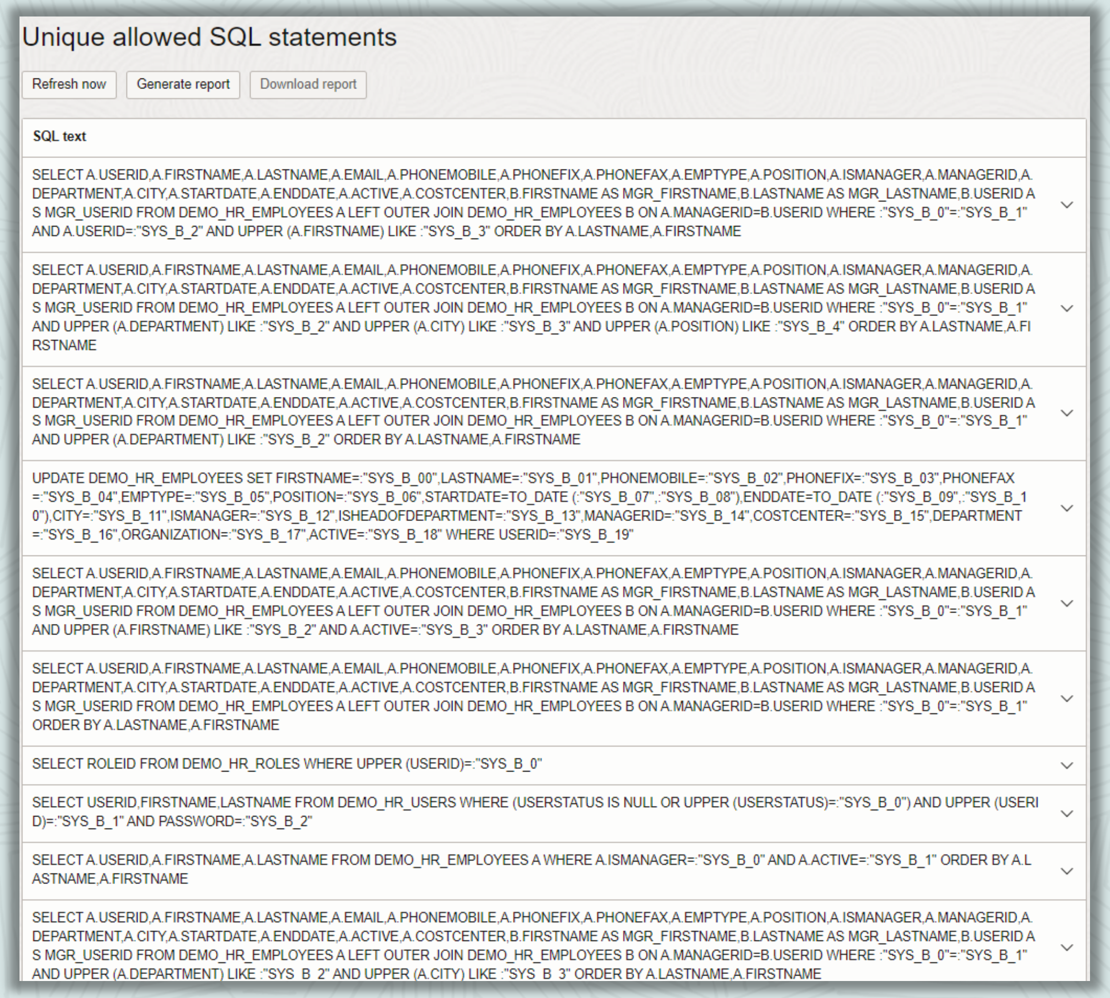
Violation reports: View Report

Use Case – Allow approved SQL statements only

Restrict database access to only authorized SQL statements

Benefit:

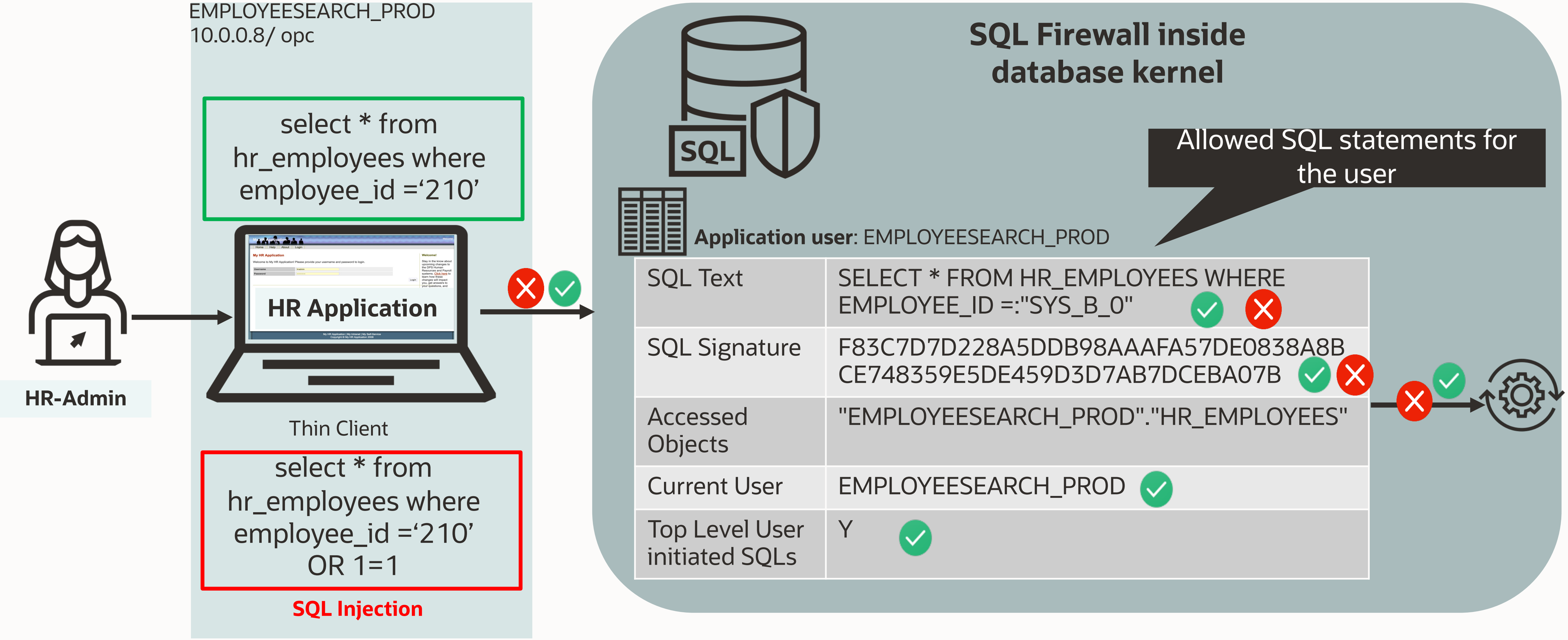
Mitigate risks of SQL Injection attacks



Unique allowed SQL statements

SQL text
SELECT A.USERID,A.FIRSTNAME,A.LASTNAME,A.EMAIL,A.PHONEMOBILE,A.PHONEFIX,A.PHONEFAX,A.EMPTYPE,A.POSITION,A.ISMANAGER,A.MANAGERID,A.DEPARTMENT,A.CITY,A.STARTDATE,A.ENDDATE,A.ACTIVE,A.COSTCENTER,B.FIRSTNAME AS MGR_FIRSTNAME,B.LASTNAME AS MGR_LASTNAME,B.USERID AS MGR_USERID FROM DEMO_HR_EMPLOYEES A LEFT OUTER JOIN DEMO_HR_EMPLOYEES B ON A.MANAGERID=B.USERID WHERE :"SYS_B_0"=:"SYS_B_1" AND A.USERID=:"SYS_B_2" AND UPPER (A.FIRSTNAME) LIKE :"SYS_B_3" ORDER BY A.LASTNAME,A.FIRSTNAME
SELECT A.USERID,A.FIRSTNAME,A.LASTNAME,A.EMAIL,A.PHONEMOBILE,A.PHONEFIX,A.PHONEFAX,A.EMPTYPE,A.POSITION,A.ISMANAGER,A.MANAGERID,A.DEPARTMENT,A.CITY,A.STARTDATE,A.ENDDATE,A.ACTIVE,A.COSTCENTER,B.FIRSTNAME AS MGR_FIRSTNAME,B.LASTNAME AS MGR_LASTNAME,B.USERID AS MGR_USERID FROM DEMO_HR_EMPLOYEES A LEFT OUTER JOIN DEMO_HR_EMPLOYEES B ON A.MANAGERID=B.USERID WHERE :"SYS_B_0"=:"SYS_B_1" AND UPPER (A.DEPARTMENT) LIKE :"SYS_B_2" AND UPPER (A.CITY) LIKE :"SYS_B_3" AND UPPER (A.POSITION) LIKE :"SYS_B_4" ORDER BY A.LASTNAME,A.FIRSTNAME
SELECT A.USERID,A.FIRSTNAME,A.LASTNAME,A.EMAIL,A.PHONEMOBILE,A.PHONEFIX,A.PHONEFAX,A.EMPTYPE,A.POSITION,A.ISMANAGER,A.MANAGERID,A.DEPARTMENT,A.CITY,A.STARTDATE,A.ENDDATE,A.ACTIVE,A.COSTCENTER,B.FIRSTNAME AS MGR_FIRSTNAME,B.LASTNAME AS MGR_LASTNAME,B.USERID AS MGR_USERID FROM DEMO_HR_EMPLOYEES A LEFT OUTER JOIN DEMO_HR_EMPLOYEES B ON A.MANAGERID=B.USERID WHERE :"SYS_B_0"=:"SYS_B_1" AND UPPER (A.DEPARTMENT) LIKE :"SYS_B_2" ORDER BY A.LASTNAME,A.FIRSTNAME
UPDATE DEMO_HR_EMPLOYEES SET FIRSTNAME=:"SYS_B_00",LASTNAME=:"SYS_B_01",PHONEMOBILE=:"SYS_B_02",PHONEFIX=:"SYS_B_03",PHONEFAX=:"SYS_B_04",EMPTYPE=:"SYS_B_05",POSITION=:"SYS_B_06",STARTDATE=TO_DATE (:"SYS_B_07",:"SYS_B_08"),ENDDATE=TO_DATE (:"SYS_B_09",:"SYS_B_10"),CITY=:"SYS_B_11",ISMANAGER=:"SYS_B_12",ISHEADOFDEPARTMENT=:"SYS_B_13",MANAGERID=:"SYS_B_14",COSTCENTER=:"SYS_B_15",DEPARTMENT=:"SYS_B_16",ORGANIZATION=:"SYS_B_17",ACTIVE=:"SYS_B_18" WHERE USERID=:"SYS_B_19"
SELECT A.USERID,A.FIRSTNAME,A.LASTNAME,A.EMAIL,A.PHONEMOBILE,A.PHONEFIX,A.PHONEFAX,A.EMPTYPE,A.POSITION,A.ISMANAGER,A.MANAGERID,A.DEPARTMENT,A.CITY,A.STARTDATE,A.ENDDATE,A.ACTIVE,A.COSTCENTER,B.FIRSTNAME AS MGR_FIRSTNAME,B.LASTNAME AS MGR_LASTNAME,B.USERID AS MGR_USERID FROM DEMO_HR_EMPLOYEES A LEFT OUTER JOIN DEMO_HR_EMPLOYEES B ON A.MANAGERID=B.USERID WHERE :"SYS_B_0"=:"SYS_B_1" AND UPPER (A.FIRSTNAME) LIKE :"SYS_B_2" AND A.ACTIVE=:"SYS_B_3" ORDER BY A.LASTNAME,A.FIRSTNAME
SELECT A.USERID,A.FIRSTNAME,A.LASTNAME,A.EMAIL,A.PHONEMOBILE,A.PHONEFIX,A.PHONEFAX,A.EMPTYPE,A.POSITION,A.ISMANAGER,A.MANAGERID,A.DEPARTMENT,A.CITY,A.STARTDATE,A.ENDDATE,A.ACTIVE,A.COSTCENTER,B.FIRSTNAME AS MGR_FIRSTNAME,B.LASTNAME AS MGR_LASTNAME,B.USERID AS MGR_USERID FROM DEMO_HR_EMPLOYEES A LEFT OUTER JOIN DEMO_HR_EMPLOYEES B ON A.MANAGERID=B.USERID WHERE :"SYS_B_0"=:"SYS_B_1" ORDER BY A.LASTNAME,A.FIRSTNAME
SELECT ROLEID FROM DEMO_HR_ROLES WHERE UPPER (USERID)=:"SYS_B_0"
SELECT USERID,FIRSTNAME,LASTNAME FROM DEMO_HR_USERS WHERE (USERSTATUS IS NULL OR UPPER (USERSTATUS)=:"SYS_B_0") AND UPPER (USERID)=:"SYS_B_1" AND PASSWORD=:"SYS_B_2"
SELECT A.USERID,A.FIRSTNAME,A.LASTNAME FROM DEMO_HR_EMPLOYEES A WHERE A.ISMANAGER=:"SYS_B_0" AND A.ACTIVE=:"SYS_B_1" ORDER BY A.LASTNAME,A.FIRSTNAME
SELECT A.USERID,A.FIRSTNAME,A.LASTNAME,A.EMAIL,A.PHONEMOBILE,A.PHONEFIX,A.PHONEFAX,A.EMPTYPE,A.POSITION,A.ISMANAGER,A.MANAGERID,A.DEPARTMENT,A.CITY,A.STARTDATE,A.ENDDATE,A.ACTIVE,A.COSTCENTER,B.FIRSTNAME AS MGR_FIRSTNAME,B.LASTNAME AS MGR_LASTNAME,B.USERID AS MGR_USERID FROM DEMO_HR_EMPLOYEES A LEFT OUTER JOIN DEMO_HR_EMPLOYEES B ON A.MANAGERID=B.USERID WHERE :"SYS_B_0"=:"SYS_B_1" AND UPPER (A.DEPARTMENT) LIKE :"SYS_B_2" AND UPPER (A.CITY) LIKE :"SYS_B_3" ORDER BY A.LASTNAME,A.FIRSTNAME

Allow approved SQLs only



EMPLOYEESEARCH_PROD
10.0.0.8/ opc

select * from hr_employees where employee_id =‘210’

select * from hr_employees where employee_id =‘210’ OR 1=1

SQL Injection

SQL Firewall inside database kernel

Allowed SQL statements for the user

Application user: EMPLOYEESEARCH_PROD

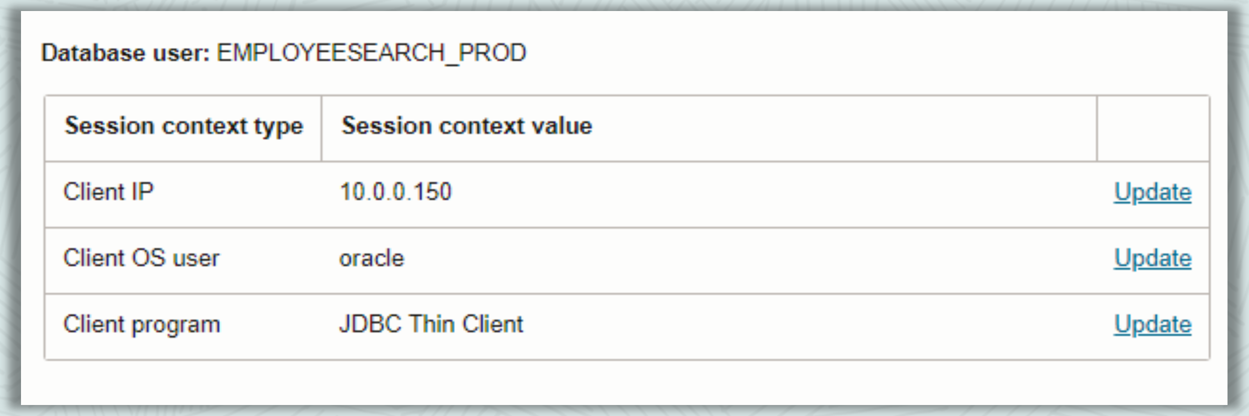
SQL Text	SELECT * FROM HR_EMPLOYEES WHERE EMPLOYEE_ID =:"SYS_B_0" ✓ ✗
SQL Signature	F83C7D7D228A5DDB98AAAFA57DE0838A8B CE748359E5DE459D3D7AB7DCEBA07B ✓ ✗
Accessed Objects	"EMPLOYEESEARCH_PROD"."HR_EMPLOYEES"
Current User	EMPLOYEESEARCH_PROD ✓
Top Level User initiated SQLs	Y ✓

Use Case – Allow only authorized database connections

Enforce trusted database connection paths

Benefit:

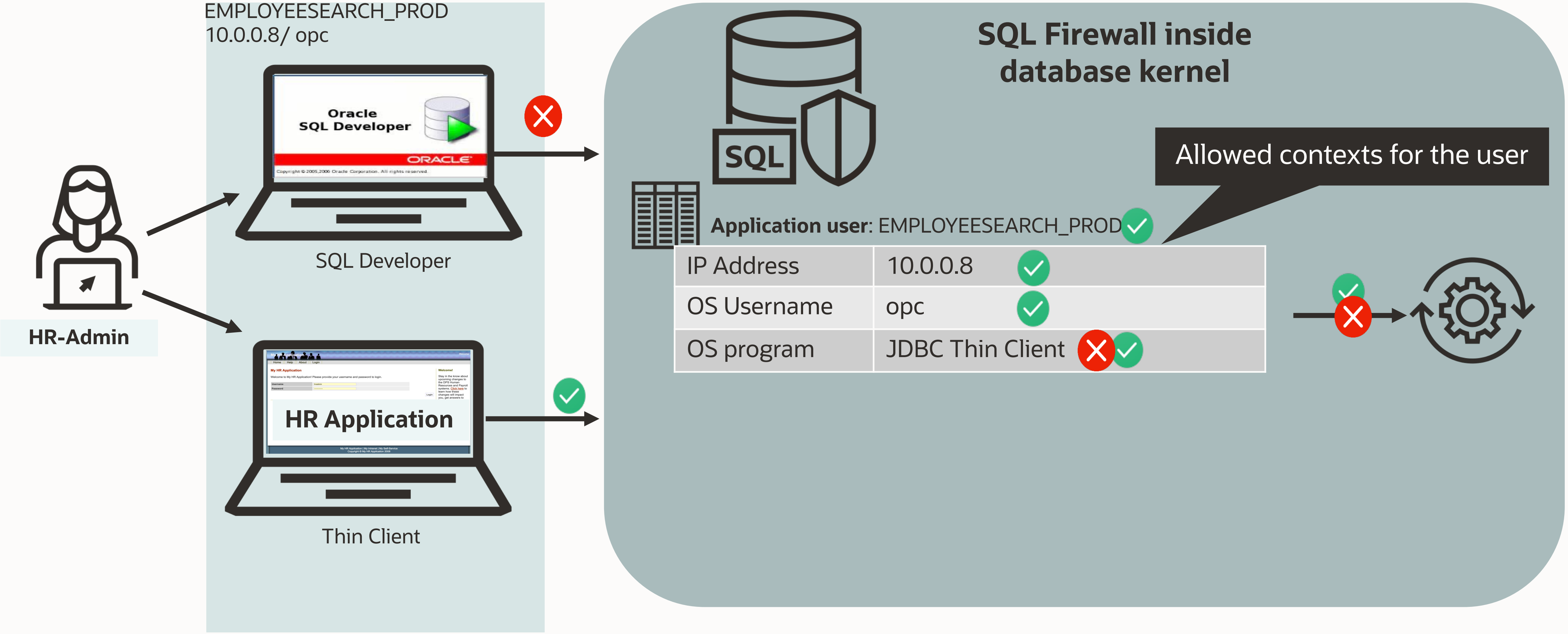
Mitigate risks from anomalous access, and credential theft/abuse



Database user: EMPLOYEESEARCH_PROD

Session context type	Session context value	
Client IP	10.0.0.150	Update
Client OS user	oracle	Update
Client program	JDBC Thin Client	Update

Enforces trusted database connection paths



Application user: EMPLOYEESEARCH_PROD ✓

IP Address	10.0.0.8 ✓
OS Username	opc ✓
OS program	JDBC Thin Client ✗ ✓

SQL Firewall

Easy configuration, management, and monitoring

New In 23ai

1

Collect

Turn on the SQL statement and user connection collection

2

Review & Modify

Review the SQL collection

Review and modify the allowed user connections (as required)

3

Enforce

Block or monitor any unauthorized SQL and/or user connections

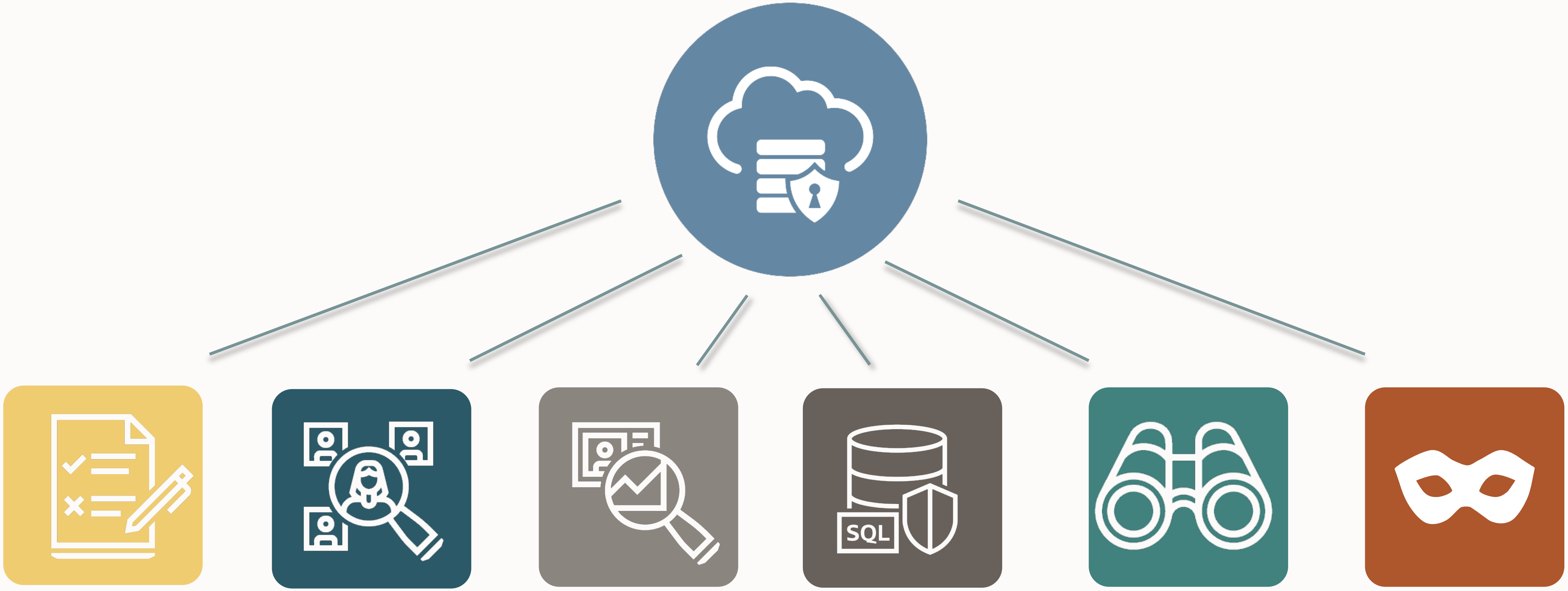
4

Monitor

Monitor any violations

Oracle Data Safe

Secure your Oracle Databases



Security Assessment

User Assessment

Activity Auditing

SQL Firewall*

Sensitive Data Discovery

Data Masking

**available for 23ai target databases only*

Oracle Database 23ai Security Enhancements

In-Database Firewall

An easy-to-use firewall solution, with minimal perf and operational overhead

Built-in to ensure it cannot be bypassed

Protection against attacks by monitoring and blocking "unauthorized SQL" and SQL injection attacks

Read-Only Users

Users may be created as, or altered to, `READ ONLY` status (default `READ WRITE`)

```
ALTER USER joe
READ ONLY;
```

Read-only users can not insert or update data, nor can they create database objects

Developer Role

It's complex to grant all the privileges developers need to create, debug, etc.

Now it's simple using the new DB_DEVELOPER_ROLE :

```
GRANT DB_DEVELOPER_ROLE
TO    scott;
```

Schema Privileges

Managing the privileges on all the tables, views, and procedures used by an app can be tricky

Now this is simple using GRANT on a schema

```
GRANT SELECT ANY TABLE
   ON SCHEMA sales
   TO mary;
```

Reduce risk with regulatory compliance

Supports a comprehensive set of international and industry-specific compliance standards

HIPA Health Insurance Portability and Accountability Act	**ISO/IEC 27017:2015** Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services
PCI DSS Payment Card Industry Data Security Standard is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment	**ISO/IEC 27018:2014** Code of Practice for Protection of Personally Identifiable Information (PII) In Public Clouds Acting as PII Processors
SOC 1 System and Organization Controls 1	**ISO 9001** Intended “to help organizations demonstrate its ability to consistently provide customers good quality products and services.”
SOC 2 System and Organization Controls 2	**GDPR** Applies to all entities processing data about EU residents, regardless of company location and /or locale of data storage.
SOC 3 System and Organization Controls 2	**CSA STAR** The Cloud Security Alliance (CSA) is an organization that promotes best practices for providing security assurance in cloud computing
ISO/IEC 27001:2013 International Organization for Standardization 27001	**MeitY IT Security Guidelines** Ministry of Electronics and Information Technology (MeitY) Information Technology (IT) Security Guidelines
European Union Digital Operational Resilience Act (DORA) It addresses gaps, overlaps, and inconsistencies in existing regulations related to information and communication technology (ICT).	

More information on regulatory compliance certification is here: https://bit.ly/adb-compliance

Key Areas Of European Union Digital Operational Resilience Act (DORA)

Autonomous Database supports key requirements out-of-the-box - nothing else to buy

Risk Management Framework

Comprehensive, documented risk management framework to quickly and efficiently address risk.

- ✓ Oracle Data Safe
- ✓ Database Vault

Highly Available Architecture

ICT systems, protocols and tools that are reliable, equipped with sufficient capacity, and resilient.

- ✓ **99.95%** Availability
- ✓ Oracle **R**eal **A**pplication **C**lusters
- ✓ Triple mirrored discs
- ✓ **Auto-scaling**
- ✓ Failover with **zero data loss**
- ✓ Automated issue detection
- ✓ Continuous monitoring

Prevention and Protection

Maintain high standards of availability, authenticity, integrity and confidentiality to protect data at rest, in use, and in transit.

- ✓ Encrypted, **immutable** backups
- ✓ **Database Vault**
- ✓ Automated discovery of sensitive data (*during data loading*)
- ✓ **Early patching** option
- ✓ **R**eal **A**pplication **T**esting
- ✓ Zero-regression **SLO**
- ✓ SQL **Firewall**

Backup/Restore procedures

Restoration of systems and data with minimum downtime, limited disruption and loss.

- ✓ **Automated** daily backups
- ✓ **60-day** rolling backup retention
- ✓ Long-term backups (up to **10yrs**)
- ✓ Point-in-time recovery

Response and Recovery

Implement business continuity policy to protect critical or important functions

- ✓ **Auto**nomous **D**ata **G**uard
  - ✓ **99.996%** availability
- ✓ **In-region** standby with automatic failover
- ✓ **Cross-region** standby
- ✓ **T**ransparent **A**pplication **C**ontinuity
- ✓ Full-stack disaster recovery

More information on how ADB supports DORA is here: https://blogs.oracle.com/datawarehousing/post/oracle-autonomous-database-and-dora

Industry-Leading Data Security

End-to-end data security; always enabled; no extra costs

HIPAA, PCI, FedRAMP, and country specific compliance

ZERO-TRUST ENTERPRISE SECURITY

Assumes no one and no device or application is universally trusted, whether inside or outside the network. **Continuous verification is required.**

Access is granted based on the context of the request, the level of trust, and the sensitivity of the asset.

BUILT-IN DATA RISK MANAGEMENT

Understand data **sensitivity**, evaluate data **risks**, mask sensitive data, implement and monitor security controls, assess user security, **monitor** user **activity**, scan all SQL traffic irrespective of where it comes from, without exceptions

MULTICLOUD-NATIVE SECURITY

Azure aws

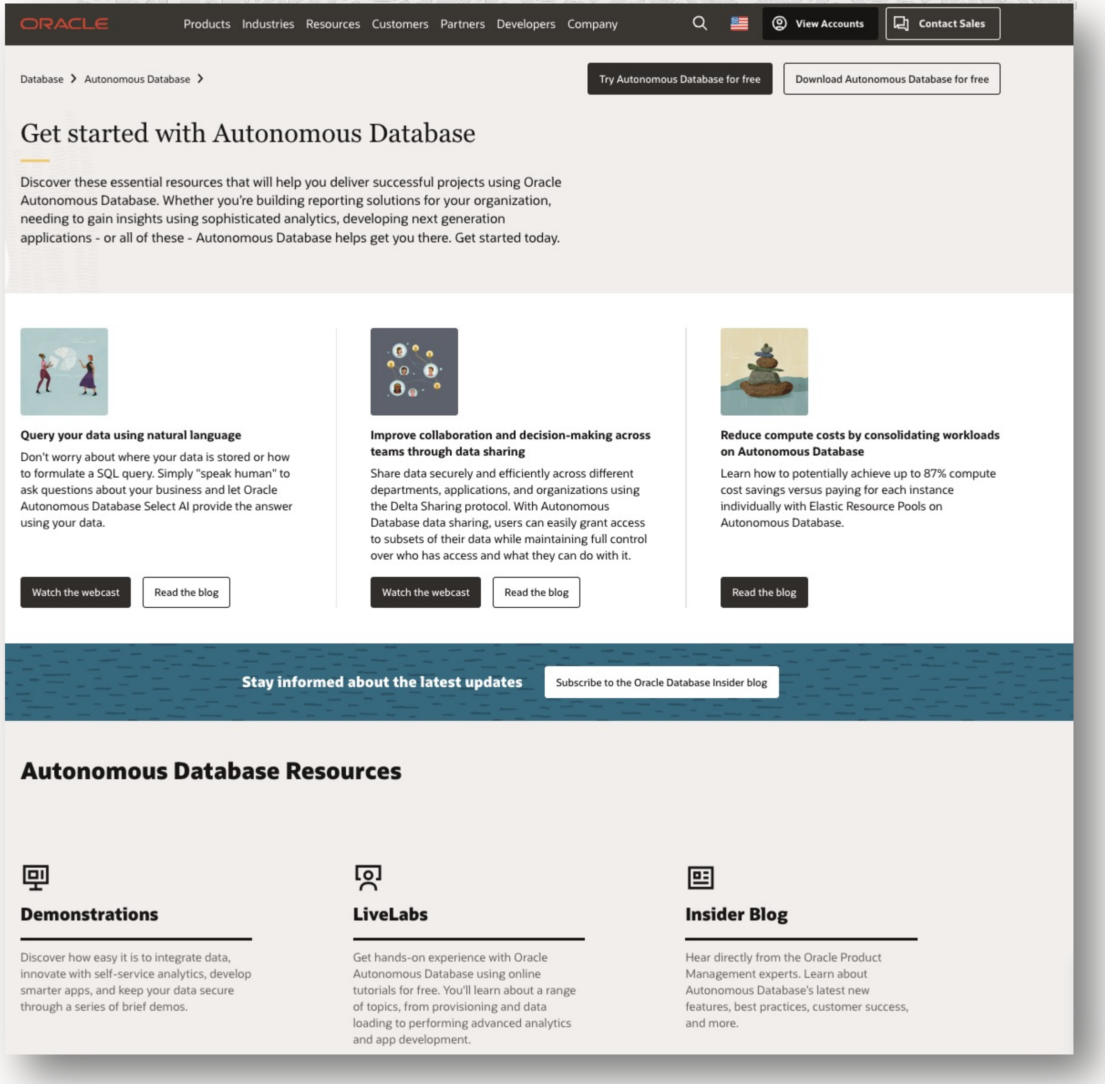
Deploy within private networking infrastructure for added protection and use preferred cloud vendor’s key management service

Security Patches Applied Automatically – Always Up-To-Date

Learn more

- Try Autonomous Database for free
- Watch demos
- Learn with self-service workshops
- Keep up with the latest news

https://www.oracle.com/autonomous-database/get-started/



ORACLE
Products Industries Resources Customers Partners Developers Company
View Accounts
Contact Sales
Database > Autonomous Database >
Try Autonomous Database for free
Download Autonomous Database for free

Get started with Autonomous Database

Discover these essential resources that will help you deliver successful projects using Oracle Autonomous Database. Whether you're building reporting solutions for your organization, needing to gain insights using sophisticated analytics, developing next generation applications - or all of these - Autonomous Database helps get you there. Get started today.

Query your data using natural language

Don't worry about where your data is stored or how to formulate a SQL query. Simply "speak human" to ask questions about your business and let Oracle Autonomous Database Select AI provide the answer using your data.

Improve collaboration and decision-making across teams through data sharing

Share data securely and efficiently across different departments, applications, and organizations using the Delta Sharing protocol. With Autonomous Database data sharing, users can easily grant access to subsets of their data while maintaining full control over who has access and what they can do with it.

Reduce compute costs by consolidating workloads on Autonomous Database

Learn how to potentially achieve up to 87% compute cost savings versus paying for each instance individually with Elastic Resource Pools on Autonomous Database.

Read the blog
Stay informed about the latest updates
Subscribe to the Oracle Database Insider blog

Autonomous Database Resources

Demonstrations

Discover how easy it is to integrate data, innovate with self-service analytics, develop smarter apps, and keep your data secure through a series of brief demos.

LiveLabs

Get hands-on experience with Oracle Autonomous Database using online tutorials for free. You'll learn about a range of topics, from provisioning and data loading to performing advanced analytics and app development.

Insider Blog

Hear directly from the Oracle Product Management experts. Learn about Autonomous Database's latest new features, best practices, customer success, and more.

Q&A Open

Important links to bookmark

Links to get you started and to keep up to date with Autonomous Database

GET STARTED

1 New Get Started page:
oracle.com/autonomous-database/get-started/

2 Join us:

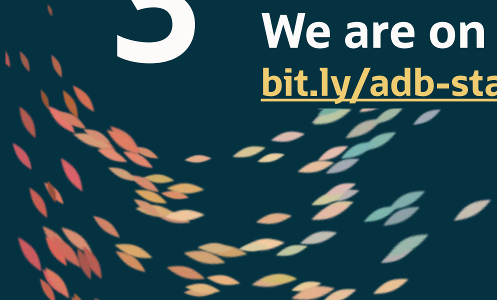
LinkedIn
bit.ly/adb-linkedin-grp

X
@AutonomousDW

Bluesky
autonomousdb.bsky.social

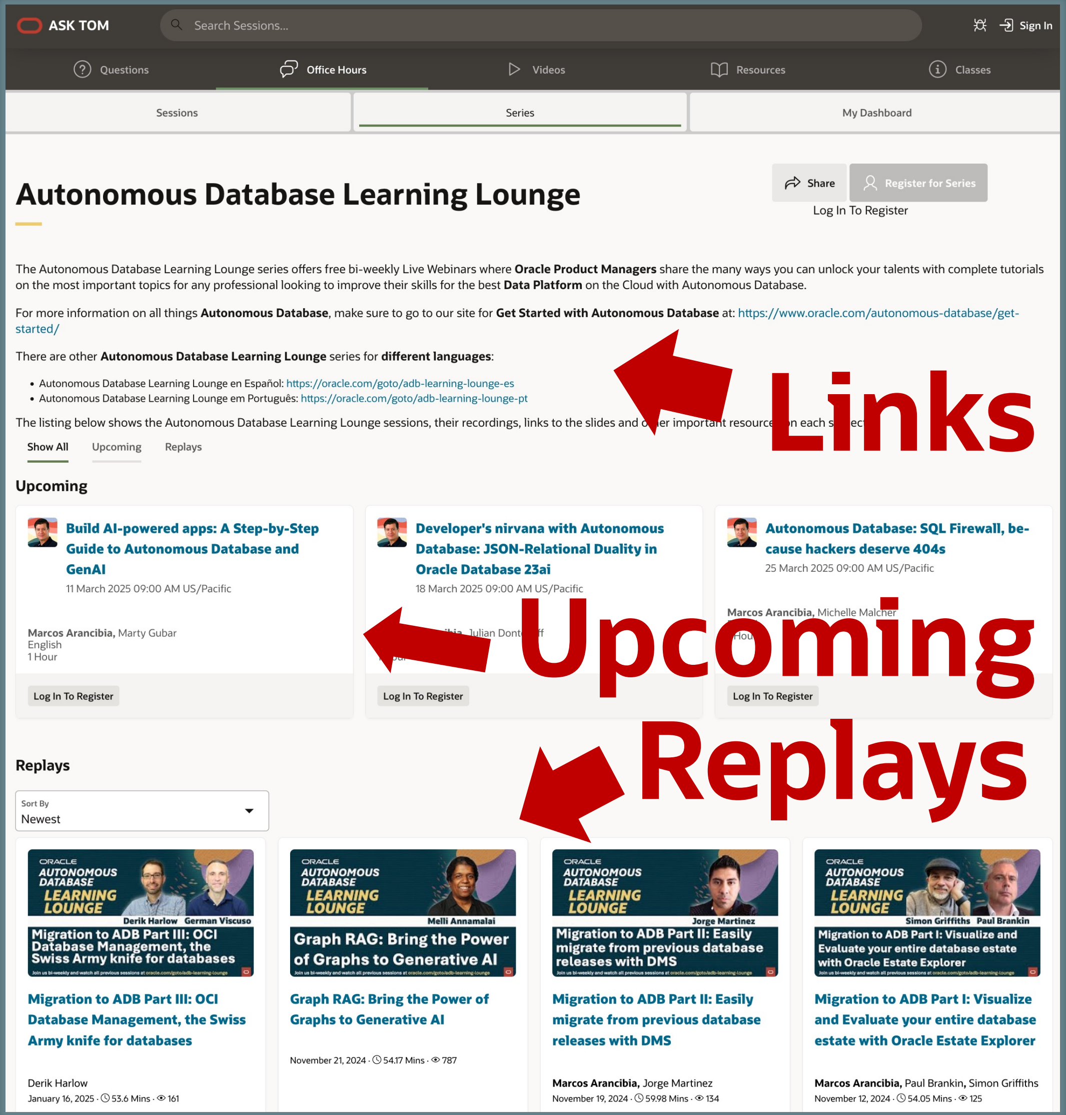
3 Got a question?
We are on stackoverflow
bit.ly/adb-stackoverflow

Join us on Developers Slack
(search #oracle-autonomous-database)
(odevrel_slack)



Final Thoughts

oracle.com/goto/adb-learning-lounge



Autonomous Database Learning Lounge

Log In To Register

The Autonomous Database Learning Lounge series offers free bi-weekly Live Webinars where **Oracle Product Managers** share the many ways you can unlock your talents with complete tutorials on the most important topics for any professional looking to improve their skills for the best **Data Platform** on the Cloud with Autonomous Database.

For more information on all things **Autonomous Database**, make sure to go to our site for **Get Started with Autonomous Database** at: https://www.oracle.com/autonomous-database/get-started/

There are other **Autonomous Database Learning Lounge** series for **different languages**:

- Autonomous Database Learning Lounge en Español: https://oracle.com/goto/adb-learning-lounge-es
- Autonomous Database Learning Lounge em Português: https://oracle.com/goto/adb-learning-lounge-pt

The listing below shows the Autonomous Database Learning Lounge sessions, their recordings, links to the slides and o er important resource n each s ec

Show All Upcoming Replays

Links

Upcoming

Build AI-powered apps: A Step-by-Step Guide to Autonomous Database and GenAI
11 March 2025 09:00 AM US/Pacific
Marcos Arancibia, Marty Gubar
English
1 Hour
Log In To Register

Developer's nirvana with Autonomous Database: JSON-Relational Duality in Oracle Database 23ai
18 March 2025 09:00 AM US/Pacific
ibia, Julian Dont ff
Log In To Register

Autonomous Database: SQL Firewall, because hackers deserve 404s
25 March 2025 09:00 AM US/Pacific
Marcos Arancibia, Michelle Malcher
Hou
Log In To Register

Upcoming

Replays

Replays

Sort By
Newest

Migration to ADB Part III: OCI Database Management, the Swiss Army knife for databases
Derik Harlow
January 16, 2025 · 53.6 Mins · 👁 161

Graph RAG: Bring the Power of Graphs to Generative AI
November 21, 2024 · 54.17 Mins · 👁 787

Migration to ADB Part II: Easily migrate from previous database releases with DMS
Marcos Arancibia, Jorge Martinez
November 19, 2024 · 59.98 Mins · 👁 134

Migration to ADB Part I: Visualize and Evaluate your entire database estate with Oracle Estate Explorer
Marcos Arancibia, Paul Brankin, Simon Griffiths
November 12, 2024 · 54.05 Mins · 👁 125

Thank you for joining !!!

AUTONOMOUS
DATABASE

LEARNING
LOUNGE