Oracle 23ai
SQL Firewall, here we go

Improving Database Security

Exposing SQL Firewall Capabilities

Stefan Oehrli

Stefan Oehrli – Modern Data Platforms

Modern
Data
Platforms

stefan.oehrli@accenture.com

SYM42

Oracle ACE Director

Terraform ASSOCIATE
HashiCorp CERTIFIED

Oracle ACE Director 2024

Tech Architecture Manager

- Since 1997 active in various IT areas
- More than 25 years of experience in Oracle databases
- Focus: Protecting data and operating databases securely
  - Security assessments and reviews
  - Database security concepts and their implementation
  - Oracle Backup & Recovery concepts and troubleshooting
  - Oracle Enterprise User and Advanced Security, DB Vault, …
  - Oracle Directory Services
- Co-author of the book The Oracle DBA (Hanser, 2016/07)

2. Auflage
DER ORACLE DBA
Handbuch für die Administration der Oracle Database 12c
EXTRA: E-Book inside
HANSER

oradba.ch

@stefanoehrli

Copyright © 2024 Accenture. All rights reserved.

Oracle ACE

450+ technical experts helping peers globally

The **Oracle ACE Program** recognizes and rewards community members for their technical and community contributions to the Oracle community

3 membership tiers

Oracle ACE Director

Oracle ACE Pro

Oracle ACE Associate

For more details on Oracle ACE Program:
ace.oracle.com

Oracle ACE

Nominate
yourself or someone you know:
ace.oracle.com/nominate

Connect: **aceprogram_ww@oracle.com** Facebook.com/OracleACEs @oracleace Oracle ACE Program Group

Copyright © 2024 Accenture. All rights reserved.

Modern Data Platforms VISON & MISSION

WHY? We are the game changer for our client's data platform projects

HOW? Maximum automation, maximum efficiency, maximum quality!

WHAT? We build innovative data platforms based on our blueprints and licensable assets and tools.

3 key benefits

1 Architecture expertise from hands-on projects

2 Delivery of tailor-made data platforms

3 Integrated Teams - Like a rowing team, perfect alignment and interaction.

Tools and Blueprints

Key enabler for the implementation of modern data platforms at a high speed and quality.

Continuous Optimization

Tools and Blueprints are continuously optimized to the customer and project’s needs.

Expertise & Light Towers

Expert group for modern data platforms from technical implementation to project management and organization

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall

A new approach to protect your data.

1 Introduction

2 SQL Firewall

3 CLI Management

4 GUI Management

5 Reporting, Audit and Alerts

6 Licensing

7 Challanges

8 Conclusion

Copyright © 2024 Accenture. All rights reserved.

1

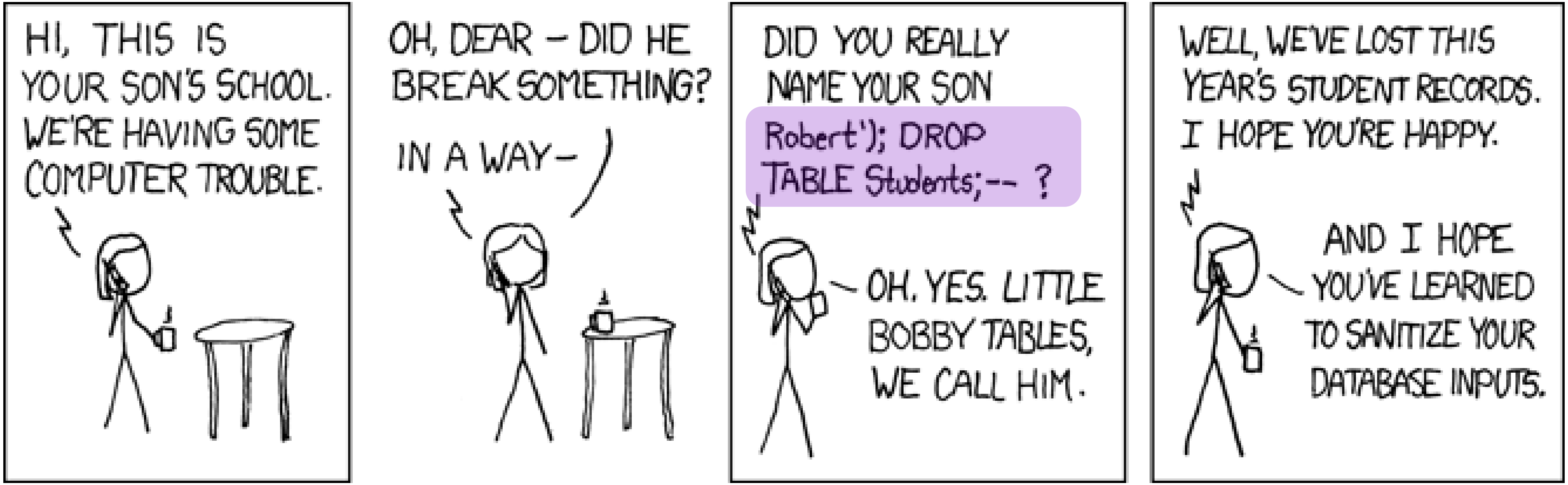
Introduction

What about the Database Security?

Copyright © 2024 Accenture. All rights reserved.

SQL Injection

Exploits of a Mom


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

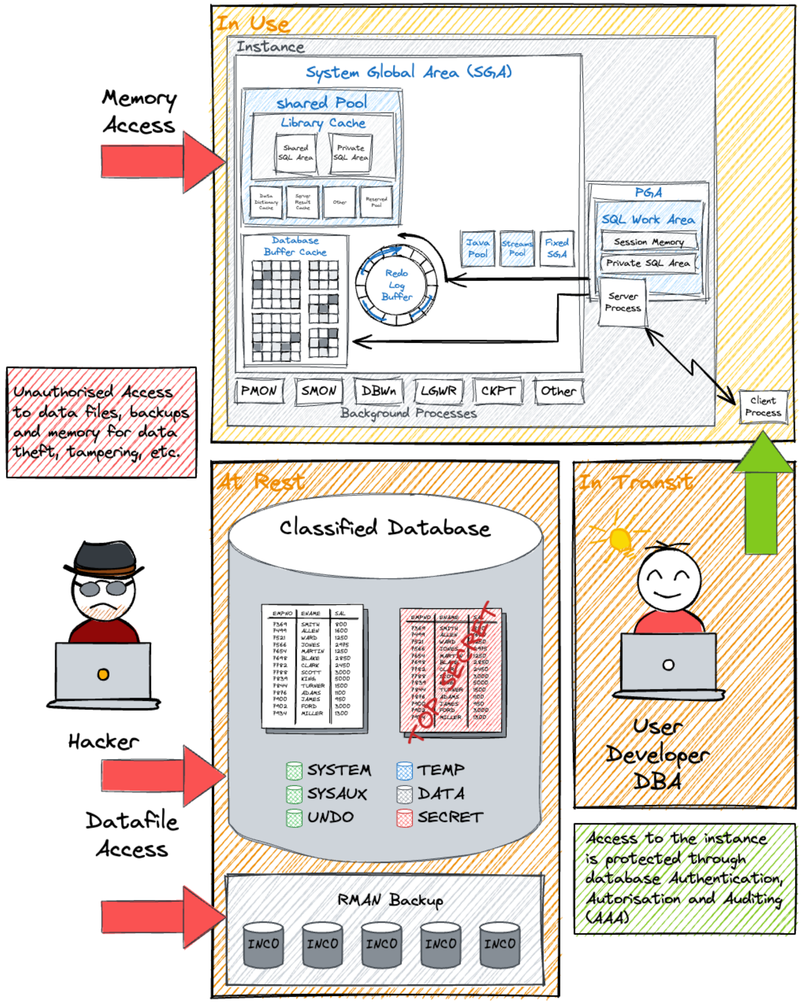
xkcd: https://xkcd.com/327

Copyright © 2024 Accenture. All rights reserved.

The Security Challenges of a Database

The dirty dozen…

- **Access Bypass**: Unpatched or misconfigured database vulnerabilities.
- **Privilege Abuse**: Exploiting application vulnerabilities for higher access.
- **Sensitive Data Search**: In unprotected systems and databases.
- **Credential Theft**: Via phishing, social engineering, or malware.
- **System Bridging**: Using less secure systems to target secure ones.
- **Password Exploitation**: Guessing or poor management.
- **SQL Injection**: Manipulating user input to exploit applications.
- **Rogue Accounts**: For reconnaissance and access escalation.
- **Non-Production Data Risks**: Targeting less secure dev/test environments.
- **Unencrypted Data Exposure**: Accessing or stealing files from disk or backups.

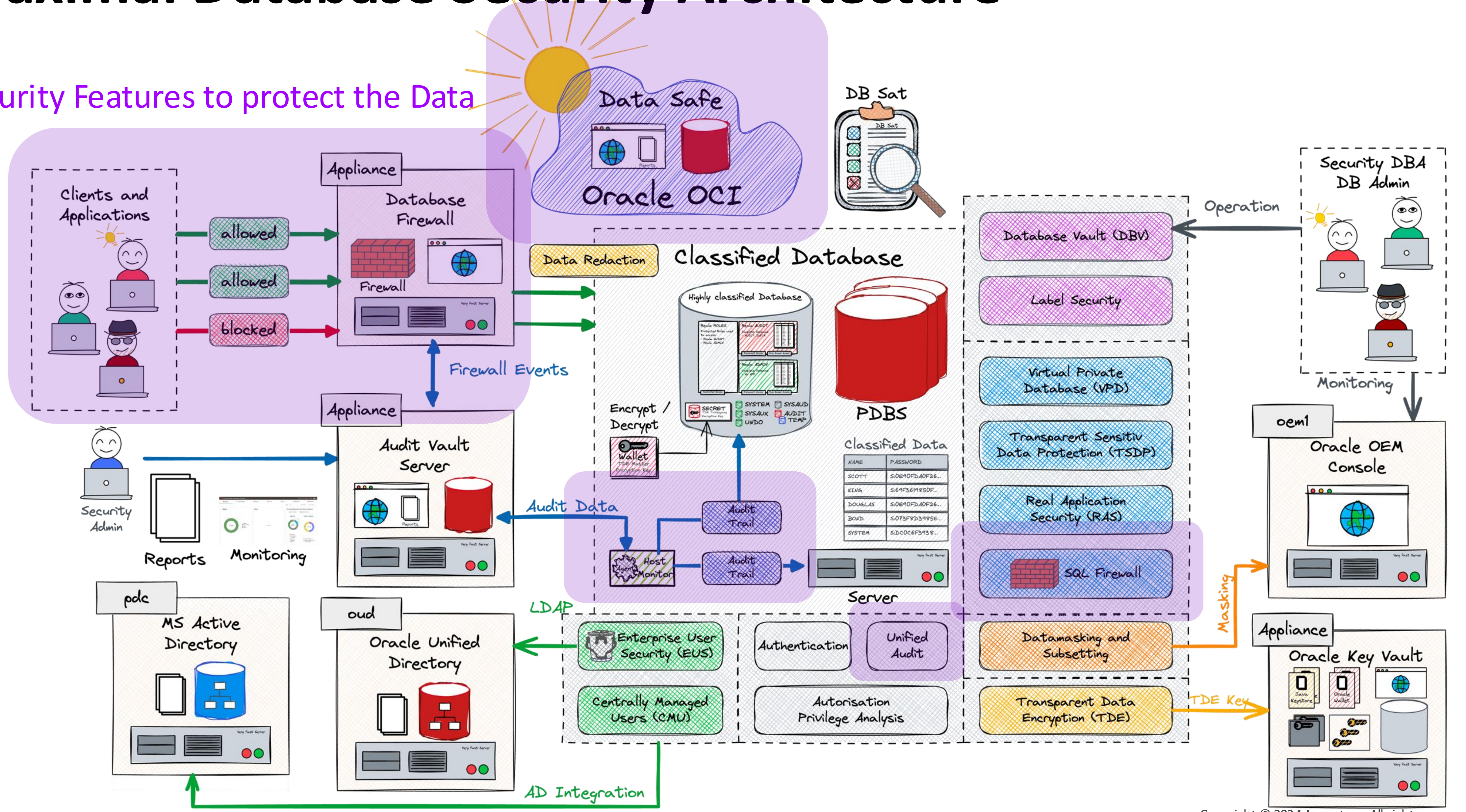


EMPNO	ENAME	SAL
7369	SMITH	800
7499	ALLEN	1600
7521	WARD	1250
7566	JONES	2975
7654	MARTIN	1250
7698	BLAKE	2850
7782	CLARK	2450
7788	SCOTT	3000
7839	KING	5000
7844	TURNER	1500
7876	ADAMS	1100
7900	JAMES	950
7902	FORD	3000
7934	MILLER	1300

Copyright © 2024 Accenture. All rights reserved.

Maximal Database Security Architecture

Security Features to protect the Data



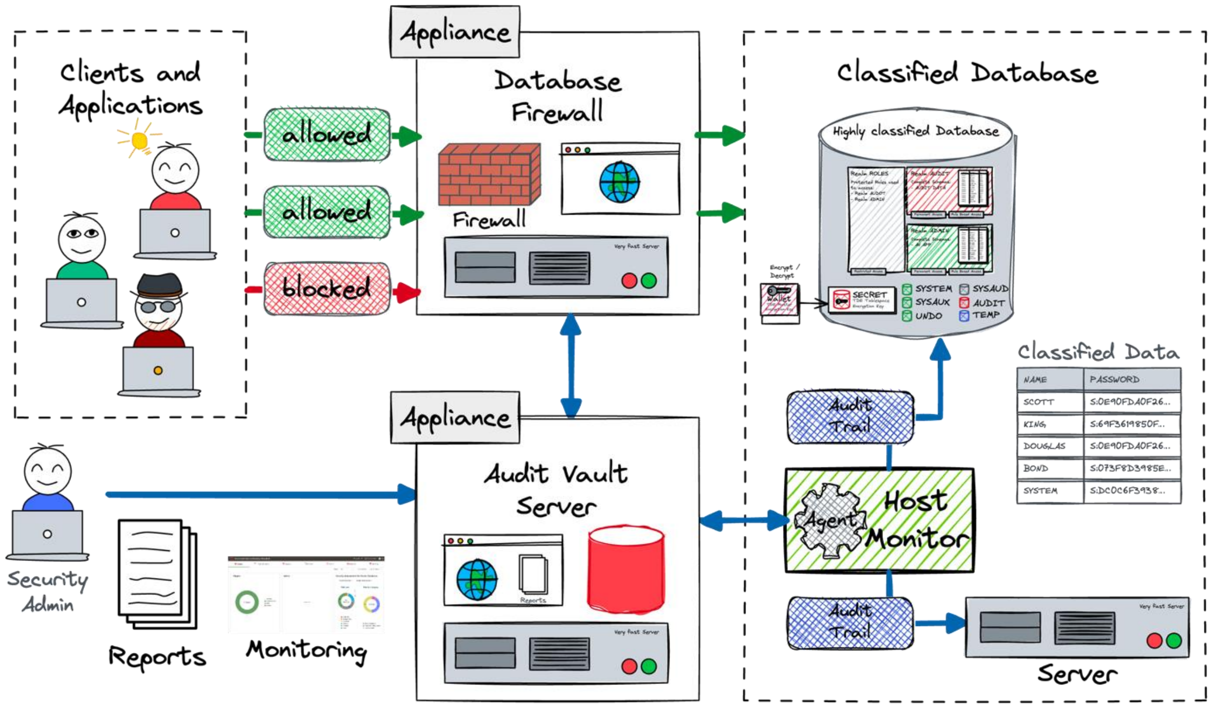
NAME	PASSWORD
SCOTT	S:0E90FDA0F26...
KING	S:69F3619850F...
DOUGLAS	S:0E90FDA0F26...
BOND	S:073F8D3985E...
SYSTEM	S:DC0C6F3938...

Copyright © 2024 Accenture. All rights reserved.

But we already have it, don't we?

Some kind of SQL firewall functionality

Oracle Audit Vault and Database Firewall



NAME	PASSWORD
SCOTT	S:0E90FDA0F26...
KING	S:69F3619850F..
DOUGLAS	S:0E90FDA0F26...
BOND	S:073F8D3985E...
SYSTEM	S:DC0C6F3938...

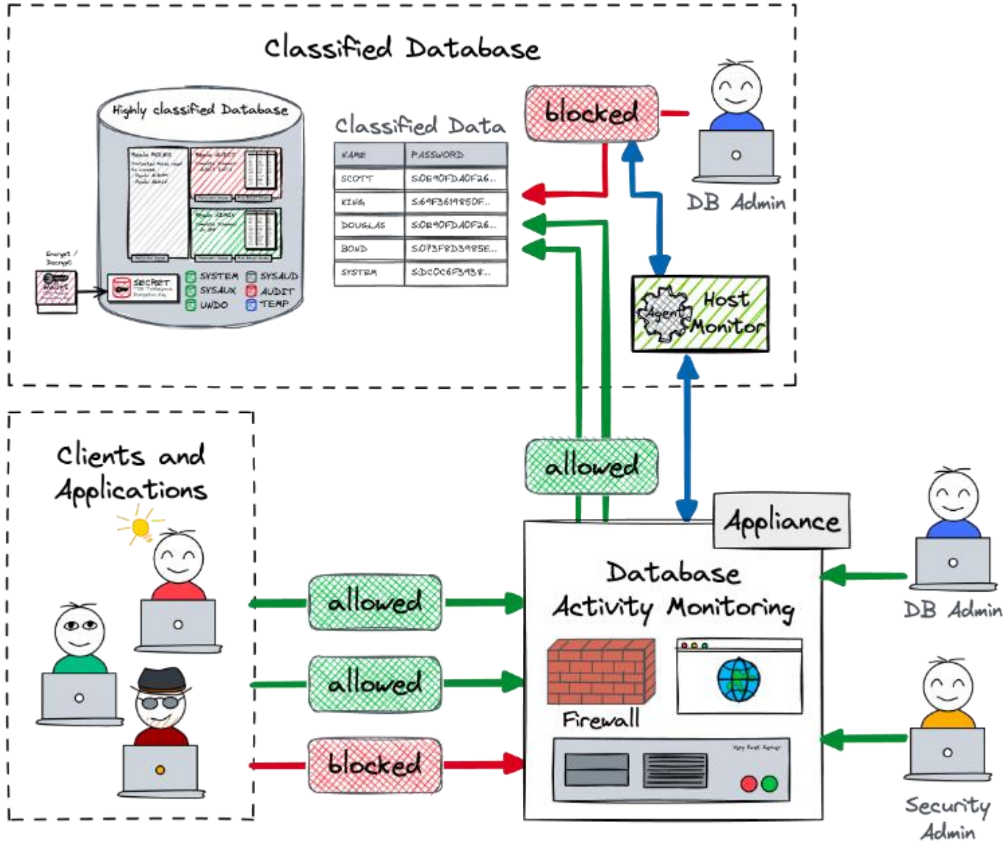
- Dedicated Product for central Audit Management and Reporting
- Two main Features
  - **Audit Vault Server** to control, manage, report
  - **Database Firewall** to monitors data access, enforces access policies
- Support a **wide range** of targets / databases
  - Oracle Database
  - Microsoft SQL Server
  - MySQL, PostgreSQL, MongoDB, IBM DB2
- Able to **log** and **block** database activities
- **Dedicate** Infrastructure
  - Requires corresponding system architecture

Copyright © 2024 Accenture. All rights reserved.

But we already have it, don't we?

Alternative solutions from third-party providers

Database Activity Monitoring



NAME	PASSWORD
SCOTT	S:0690FDA0F26..
KING	S:69F361985DF..
DOUGLAS	S:0B90FDA0F26..
BOND	S:073F8D3985E..
SYSTEM	S:DC0C6F3938..

- Various Solutions
  - *Imperva SecureSphere*
  - *IBM Guardium*
  - *Trellix Database Security, McAfee DAM, Sentrigo Hedgehog*
- Various Solution Approaches
  - Network Appliance
  - Agent based
- Able to **log** and **block** database activities
- Support a **wide range** of targets / databases

Copyright © 2024 Accenture. All rights reserved.

2

SQL Firewall

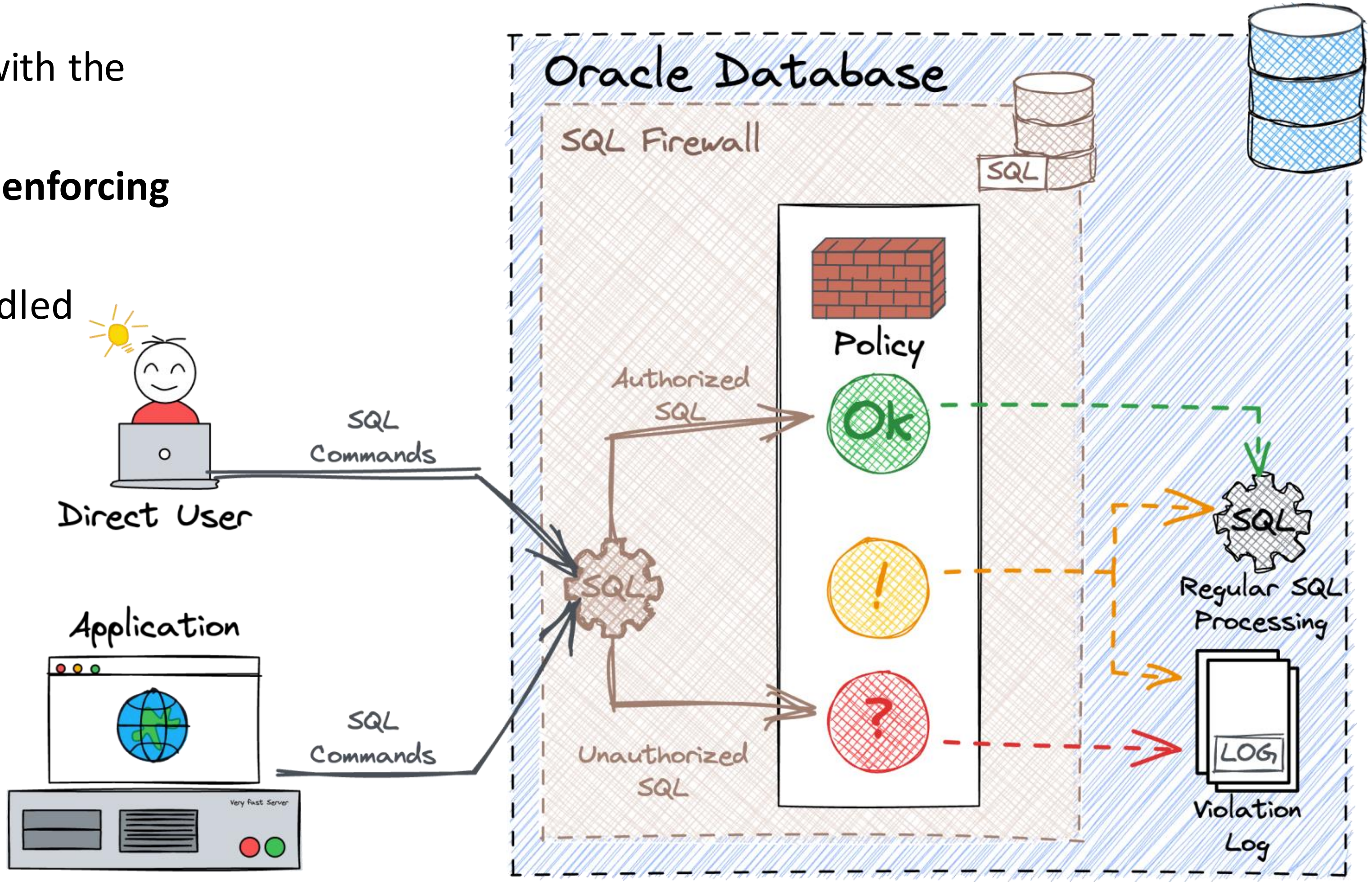
Enhancing Database Protection

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall Overview

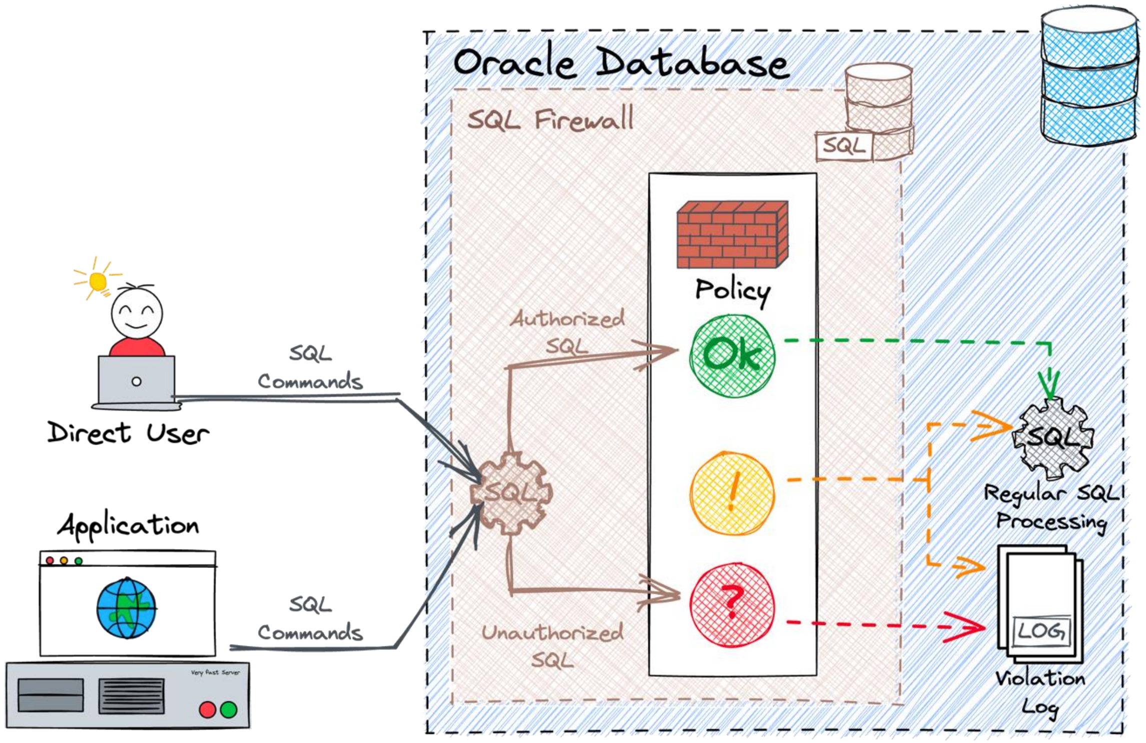
Anomaly and SQL Injection blocking and detection

- *"Learns"* how clients and applications work with the database
- Supports both **permissive** (logging only) and **enforcing** (logging and blocking) modes.
- Anomalies or SQL injection attempts are handled **before** any other **action** is taken
- The SQL firewall is **embedded** in the database and cannot be bypassed.



Copyright © 2024 Accenture. All rights reserved.

SQL Firewall Overview



What exactly is it about?

Real-Time Protection

- Blocks unauthorized SQL and preventing SQL injection and access anomalies

Customizable Allow-Lists

- Create specific SQL permissions for each user, with logging of unusual activities

Connection and **Statement** Control

- Manages **allowed** SQL **statements** and **connection** paths, e.g. IP addresses, context etc.

Integrated into Oracle Database

- Ensures inspection of all SQL activities, including encrypted and network SQL

Flexible Policy Application

- Tailored policies for different database accounts, enhancing gradual security improvement

Copyright © 2024 Accenture. All rights reserved.

Navigating SQL Firewall – Processes

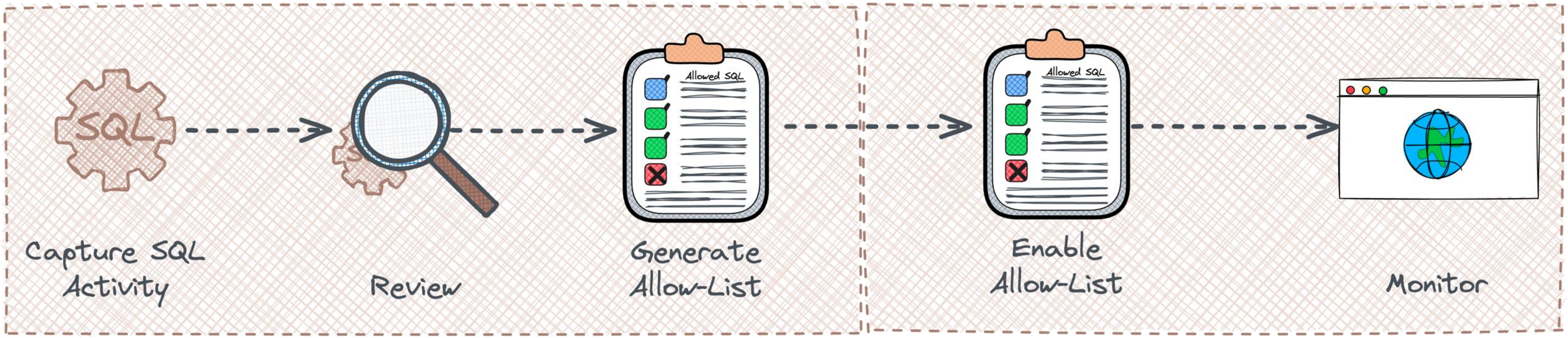
Understanding the Mechanics and Strategies for Optimal Deployment

Learning Stage

- **Capture** the user's SQL activities
- **Review** the capture
- **Generate** an allow-list

Protecting Stage

- **Enable** the allow-list
- **Monitor violations** SQL Firewall raises violation for any unexpected access patterns.



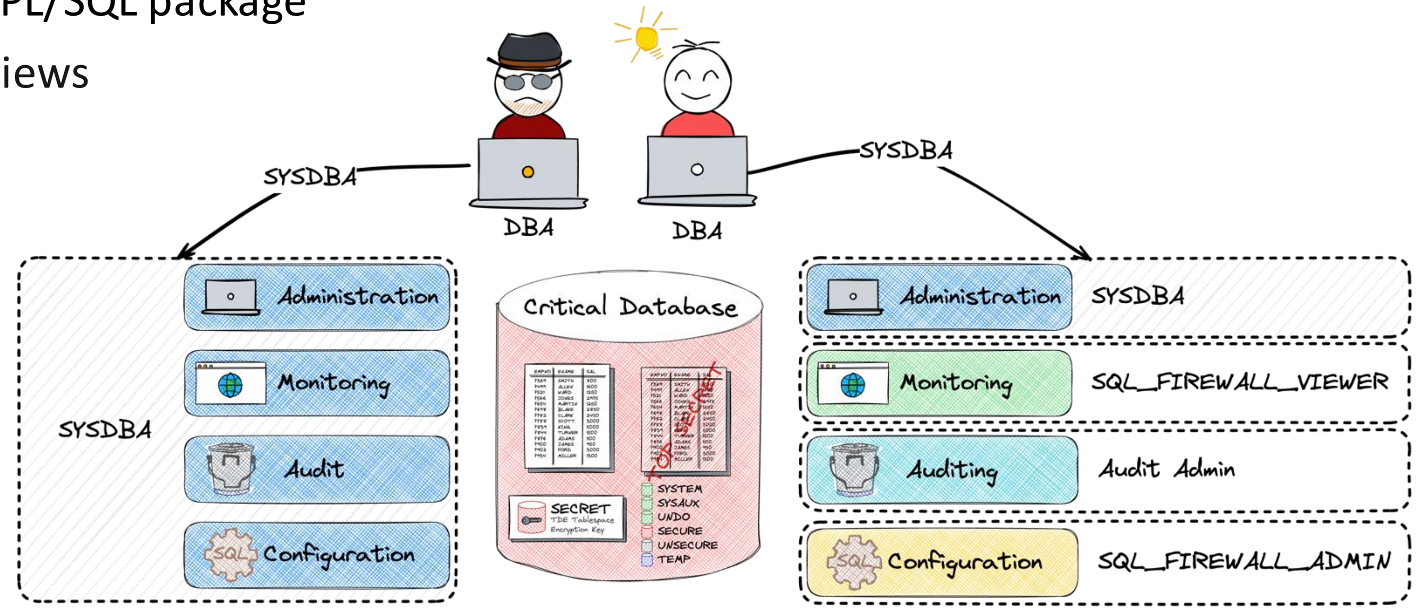
Copyright © 2024 Accenture. All rights reserved.

SQL Firewall Roles

Who should / can do what?

Dedicated roles for different purpose

- **SYSDBA** basic configuration and setup
- **SQL_FIREWALL_ADMIN**
  - ADMINISTER SQL FIREWALL system privilege
  - EXECUTE privilege on the DBMS_SQL_FIREWALL PL/SQL package
  - SELECT privilege for the SQL Firewall dictionary views
  - *DBA_SQL_FIREWALL_ **
- **SQL_FIREWALL_VIEWER**
  - SELECT privilege for the SQL Firewall dictionary views e.g. *DBA_SQL_FIREWALL_ **



Copyright © 2024 Accenture. All rights reserved.

Navigating SQL Firewall – Usage

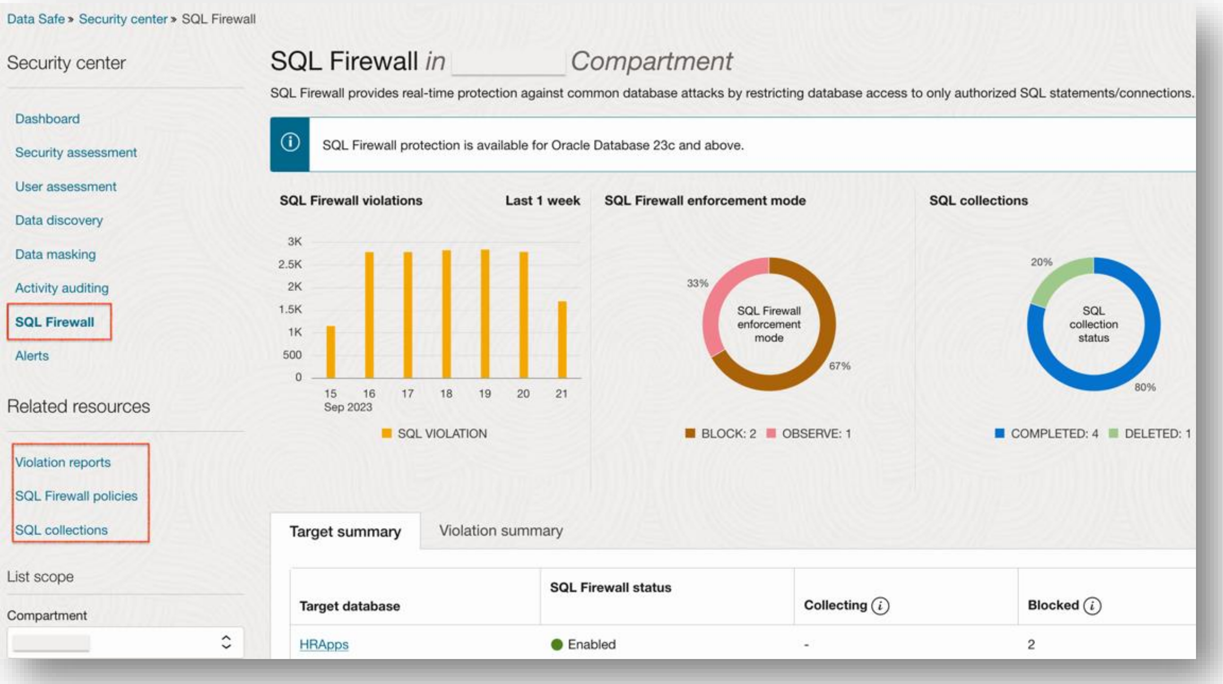
CLI or GUI you choose...

SQL Interface for the brave DBA

- System Privilege `ADMINISTER SQL FIREWALL`
- Predefined Roles
  - `SQL_FIREWALL_ADMIN`
  - `SQL_FIREWALL_VIEWER`
- Data Dictionary Views
- Violation Log `DBA_SQL_FIREWALL_VIOLATIONS`
- Capture Log `DBA_SQL_FIREWALL_CAPTURE_LOGS`
- A couple more `DBA_SQL_FIREWALL_%`
- Several base table in SYSAUX i.e. `FW_CAPTURE$, FW_ALLOW_LIST$, VIOLATION_LOG$, …`

Oracle Data Safe on Oracle Cloud

- Manage multiple SQL Firewalls centrally
- Comprehensive view of SQL Firewall violations



SQL Firewall *in* _______ *Compartment*

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

ⓘ SQL Firewall protection is available for Oracle Database 23c and above.

Target database	SQL Firewall status	Collecting ⓘ	Blocked ⓘ
HRApps	● Enabled	-	2

Copyright © 2024 Accenture. All rights reserved.

Beyond the Basics - SQL Firewall Insights

Key Considerations and Advanced Knowledge

Smooth integration with other Oracle products

- **Multitenant Environment** both the CDB root and the individual PDB levels are affected
- **Oracle Centrally Managed Users** capture global user’s activities is supported
- **Oracle Scheduler** jobs are excluded by default
- **Oracle Database Vault** not verified
- **Oracle Data Pump** Export and Import supports different use cases
  - Export and import SQL Firewall captures and allow-lists metadata e.g. `INCLUDE=SQL_FIREWALL`
  - Consider Procedures `DBMS_SQL_FIREWALL.EXPORT_ALLOW_LIST` or `DBMS_SQL_FIREWALL.IMPORT_ALLOW_LIST` to transfer allow-list

Copyright © 2024 Accenture. All rights reserved.

3

CLI Management

Use of *DBMS_SQL_FIREWALL* for firewall management

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Connect as user with `SQL_FIREWALL_ADMIN` role
- Enable SQL Firewall

```
EXEC DBMS_SQL_FIREWALL.ENABLE;
```

- Check the status of the SQL Firewall

```
SELECT * FROM dba_sql_firewall_status;

STATUS   STATUS_UPDATED_ON                  EXCLUDE_JOBS
-------- ---------------------------------- ------------
ENABLED  21.11.23 06:30:01.430118000 +01:00 Y
```

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Enable a capture for the user SCOTT

```
BEGIN
  DBMS_SQL_FIREWALL.CREATE_CAPTURE (
    username           => 'SCOTT',
    top_level_only     => TRUE,
    start_capture      => TRUE);
END;
/
```

- Verify what SCOTT is doing

```
SELECT sql_text FROM dba_sql_firewall_capture_logs
WHERE username = 'SCOTT';
```

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Disable capture for user SCOTT

```
EXEC DBMS_SQL_FIREWALL.STOP_CAPTURE ('SCOTT');
```

- Generate an allow-list for user SCOTT

```
EXEC DBMS_SQL_FIREWALL.GENERATE_ALLOW_LIST ('SCOTT');
```

- Query the allowed activity for user SCOTT
  - `DBA_SQL_FIREWALL_ALLOWED_IP_ADDR`
  - `DBA_SQL_FIREWALL_ALLOWED_OS_PROG`
  - `DBA_SQL_FIREWALL_ALLOWED_OS_USER`
  - `DBA_SQL_FIREWALL_ALLOWED_SQL`

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Customize the allow-list e.g. `DBMS_SQL_FIREWALL.ADD_ALLOWED_CONTEXT` and `DBMS_SQL_FIREWALL.DELETE_ALLOWED_CONTEXT`
- Enable the allow-list using `DBMS_SQL_FIREWALL.ENABLE_ALLOW_LIST`

```
BEGIN
  DBMS_SQL_FIREWALL.ENABLE_ALLOW_LIST (
    username       => 'SCOTT',
    enforce        => DBMS_SQL_FIREWALL.ENFORCE_SQL,
    block          => TRUE);
END;
/
```

- Start having fun with the protected Database…

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Limited availability of SCOTT

```
SQL> SELECT ename,sal FROM scott.emp  WHERE ename='SCOTT';
SELECT ename,sal FROM scott.emp  WHERE ename='SCOTT'
                            *
ERROR at line 1:
ORA-47605: SQL Firewall violation
```

- Chooses wisely what and when to capture application activity

Copyright © 2024 Accenture. All rights reserved.

4

GUI Management

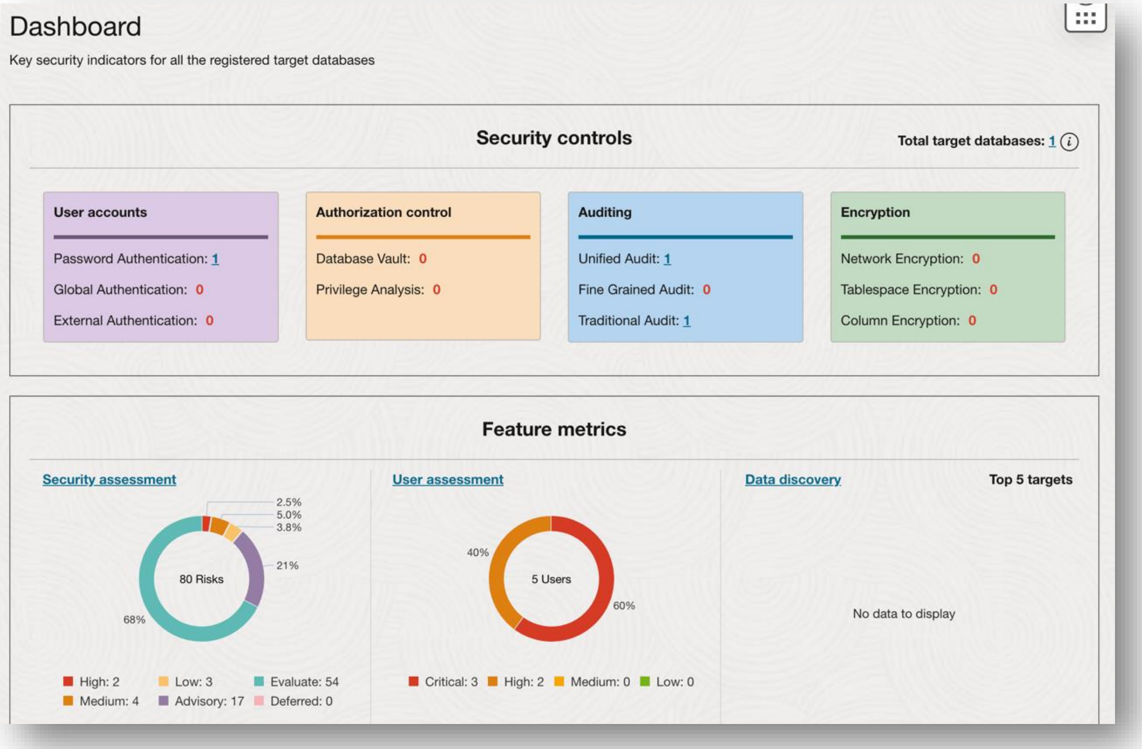
Effective Administration through Oracle Data Safe

Copyright © 2024 Accenture. All rights reserved.

GUI Management

Managing SQL Firewall via GUI

- **Oracle Data Safe** unifies data security controls for comprehensive database security
  - Cloud / OCI based tool
  - Control Cloud and On-Premises Targets
- **Centrall** Management and Reporting Platform
  - Risk Assessments
  - Audit Management
  - Sensitiv Data Discovery
  - SQL Firewall
  - Etc.



Dashboard

Key security indicators for all the registered target databases

Security controls

Total target databases: 1

User accounts

Password Authentication: 1

Global Authentication: 0

External Authentication: 0

Authorization control

Database Vault: 0

Privilege Analysis: 0

Auditing

Unified Audit: 1

Fine Grained Audit: 0

Traditional Audit: 1

Encryption

Network Encryption: 0

Tablespace Encryption: 0

Column Encryption: 0

Feature metrics

Security assessment

High: 2 Medium: 4 Low: 3 Advisory: 17 Evaluate: 54 Deferred: 0

User assessment

Critical: 3 High: 2 Medium: 0 Low: 0

Data discovery

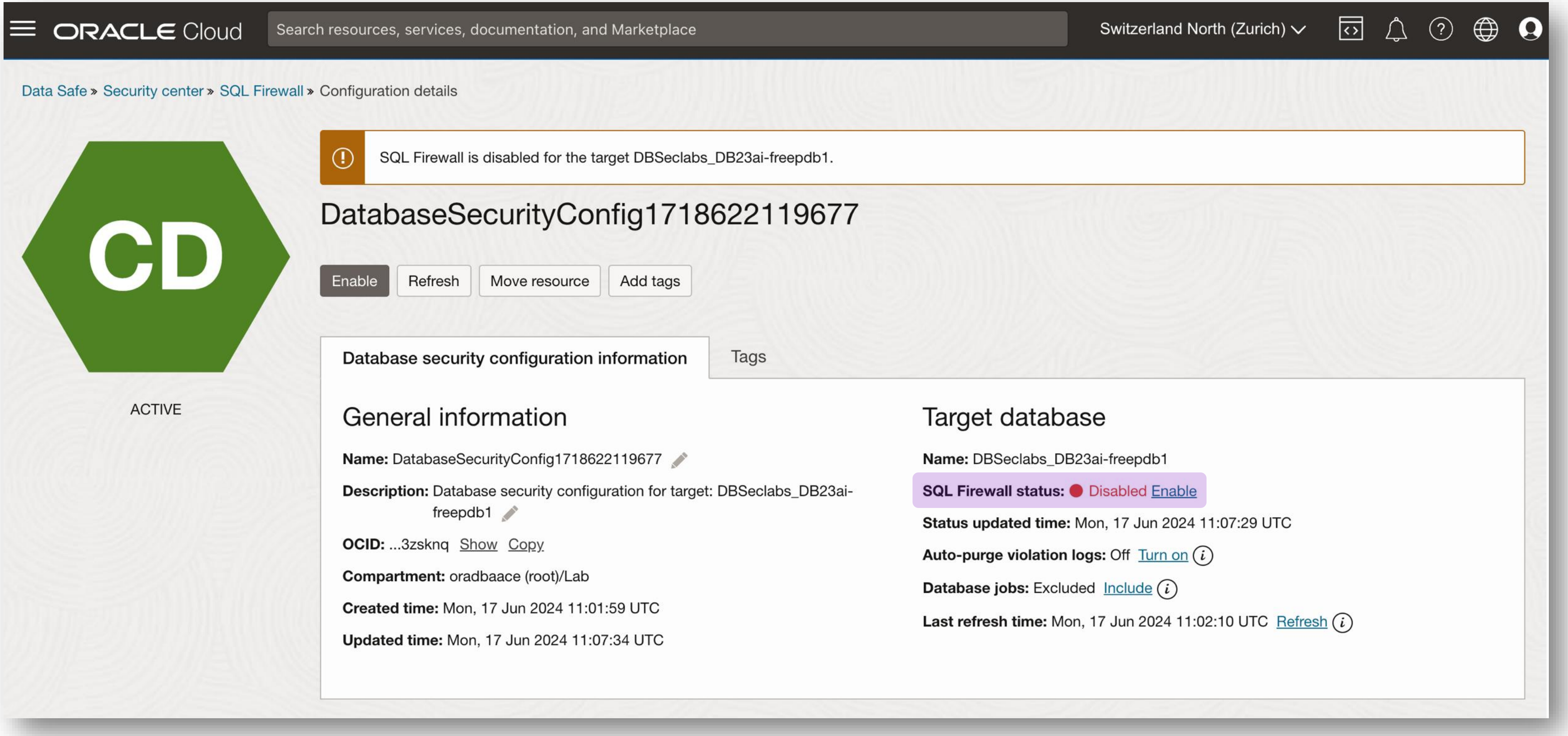
Top 5 targets

No data to display

Copyright © 2024 Accenture. All rights reserved.

Enable SQL Firewall

Initial Configuration



ORACLE Cloud
Search resources, services, documentation, and Marketplace
Switzerland North (Zurich)

Data Safe » Security center » SQL Firewall » Configuration details

SQL Firewall is disabled for the target DBSeclabs_DB23ai-freepdb1.

DatabaseSecurityConfig1718622119677

Enable
Refresh
Move resource
Add tags
Database security configuration information
Tags

General information

Name: DatabaseSecurityConfig1718622119677

Description: Database security configuration for target: DBSeclabs_DB23ai-freepdb1

OCID: ...3zsknq Show Copy

Compartment: oradbaace (root)/Lab

Created time: Mon, 17 Jun 2024 11:01:59 UTC

Updated time: Mon, 17 Jun 2024 11:07:34 UTC

Target database

Name: DBSeclabs_DB23ai-freepdb1

SQL Firewall status: ● Disabled Enable

Status updated time: Mon, 17 Jun 2024 11:07:29 UTC

Auto-purge violation logs: Off Turn on

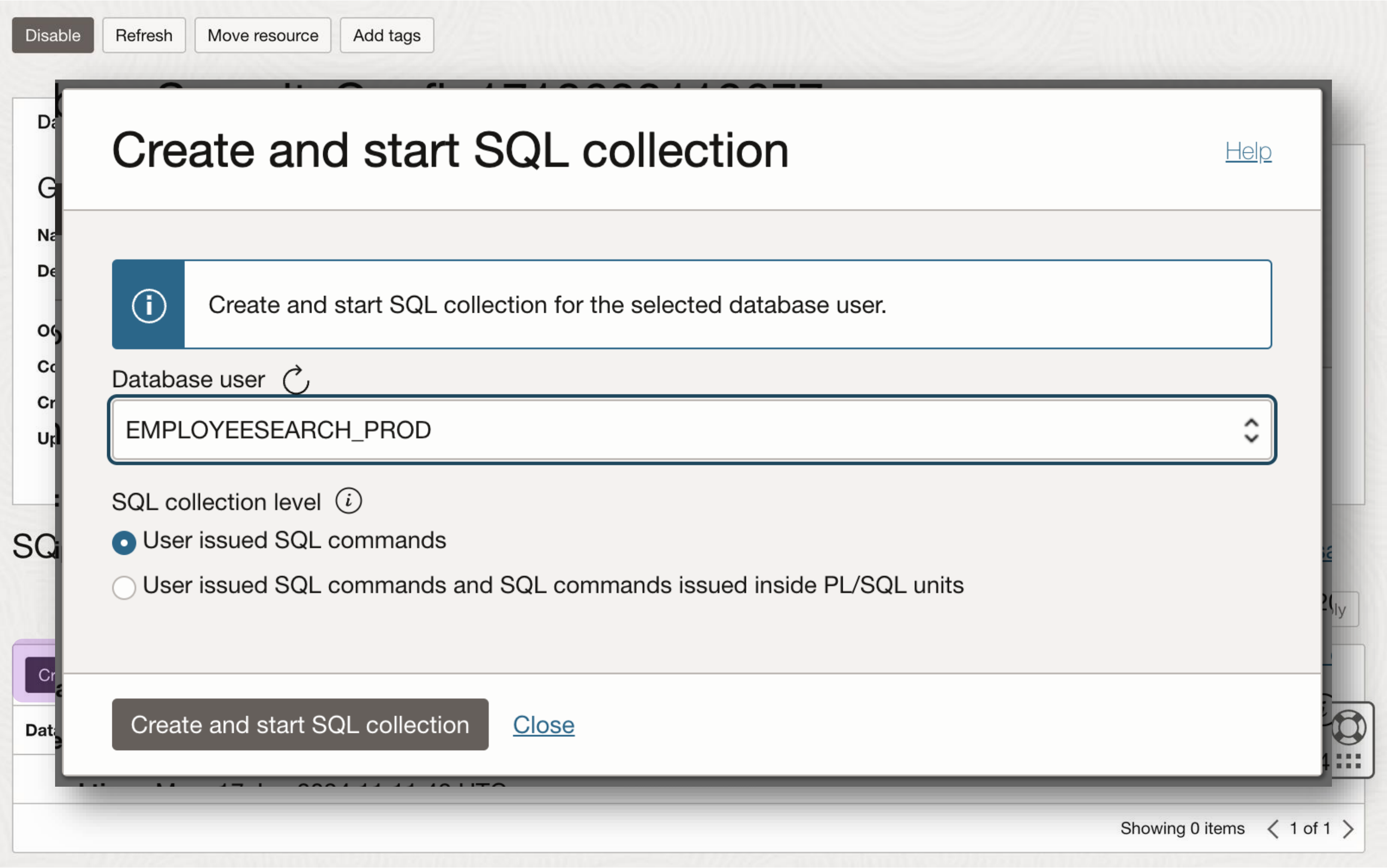
Database jobs: Excluded Include

Last refresh time: Mon, 17 Jun 2024 11:02:10 UTC Refresh

Copyright © 2024 Accenture. All rights reserved.

Initiate Collection

Start SQL Collection to “Learn”



Create and start SQL collection

Create and start SQL collection for the selected database user.

Database user: EMPLOYEESEARCH_PROD

SQL collection level

● User issued SQL commands

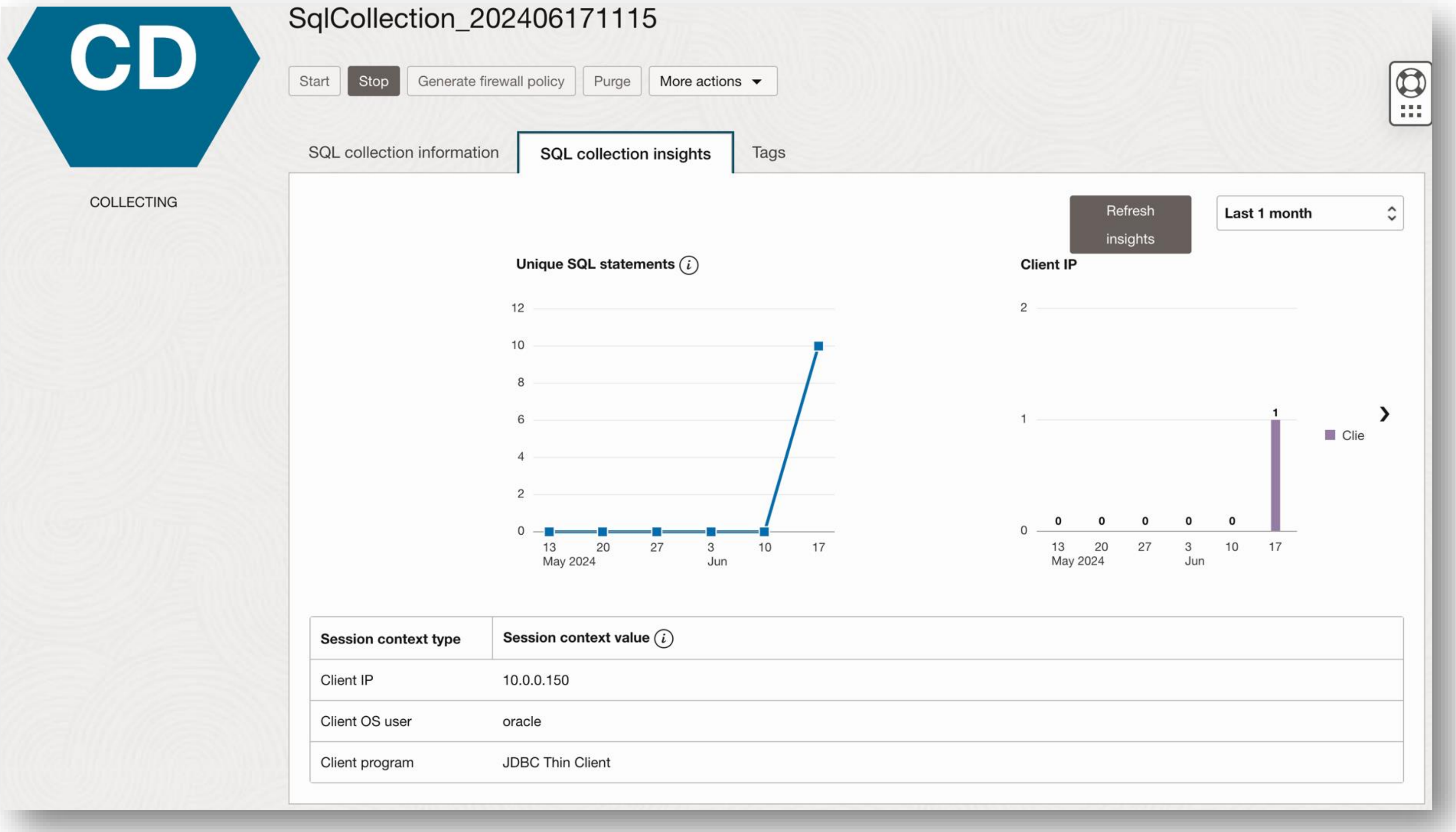
○ User issued SQL commands and SQL commands issued inside PL/SQL units

Create and start SQL collection

Copyright © 2024 Accenture. All rights reserved.

Collection Insights

Start SQL Collection to “Learn”

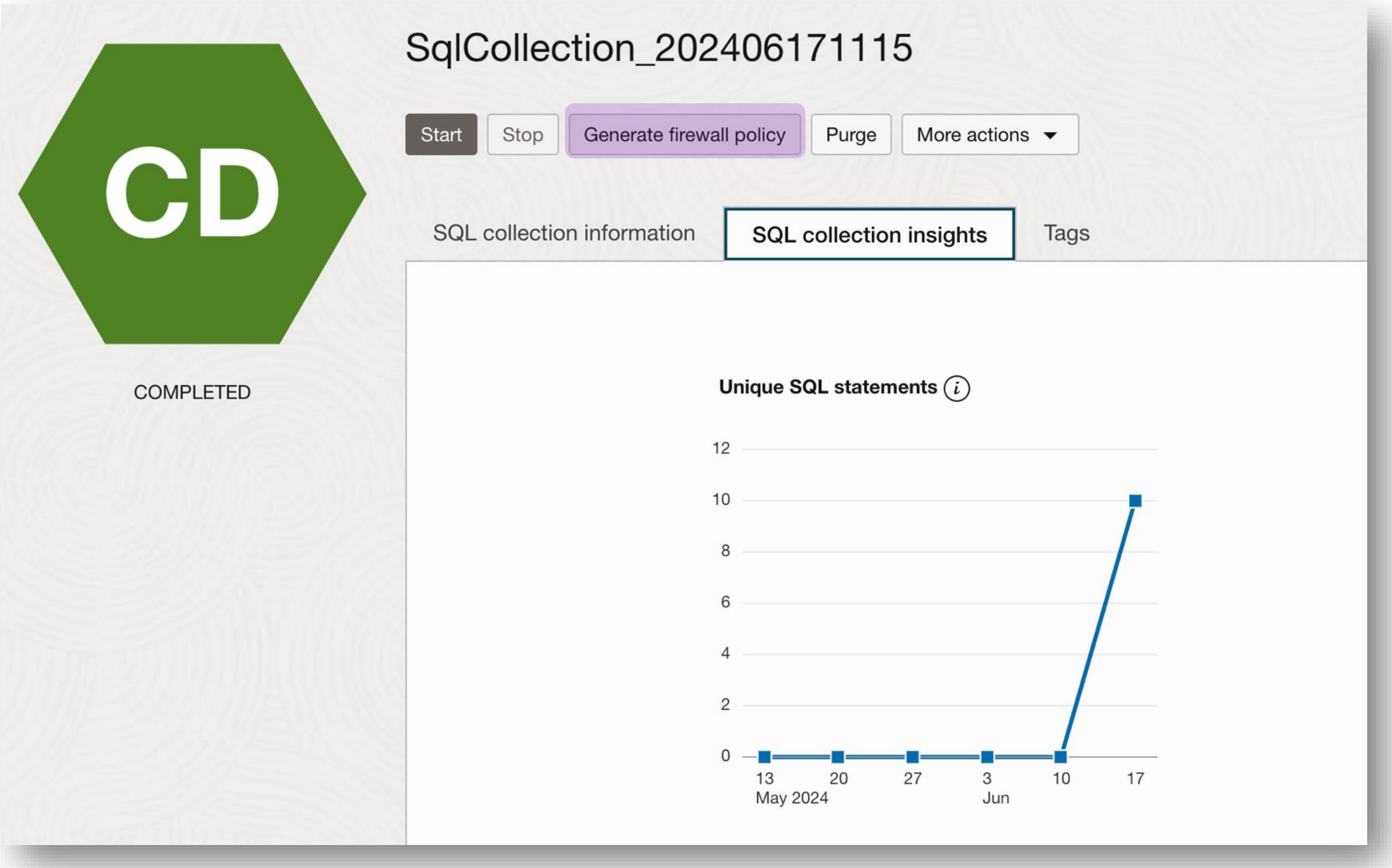


Session context type	Session context value
Client IP	10.0.0.150
Client OS user	oracle
Client program	JDBC Thin Client

Copyright © 2024 Accenture. All rights reserved.

Generate Firewall Policy

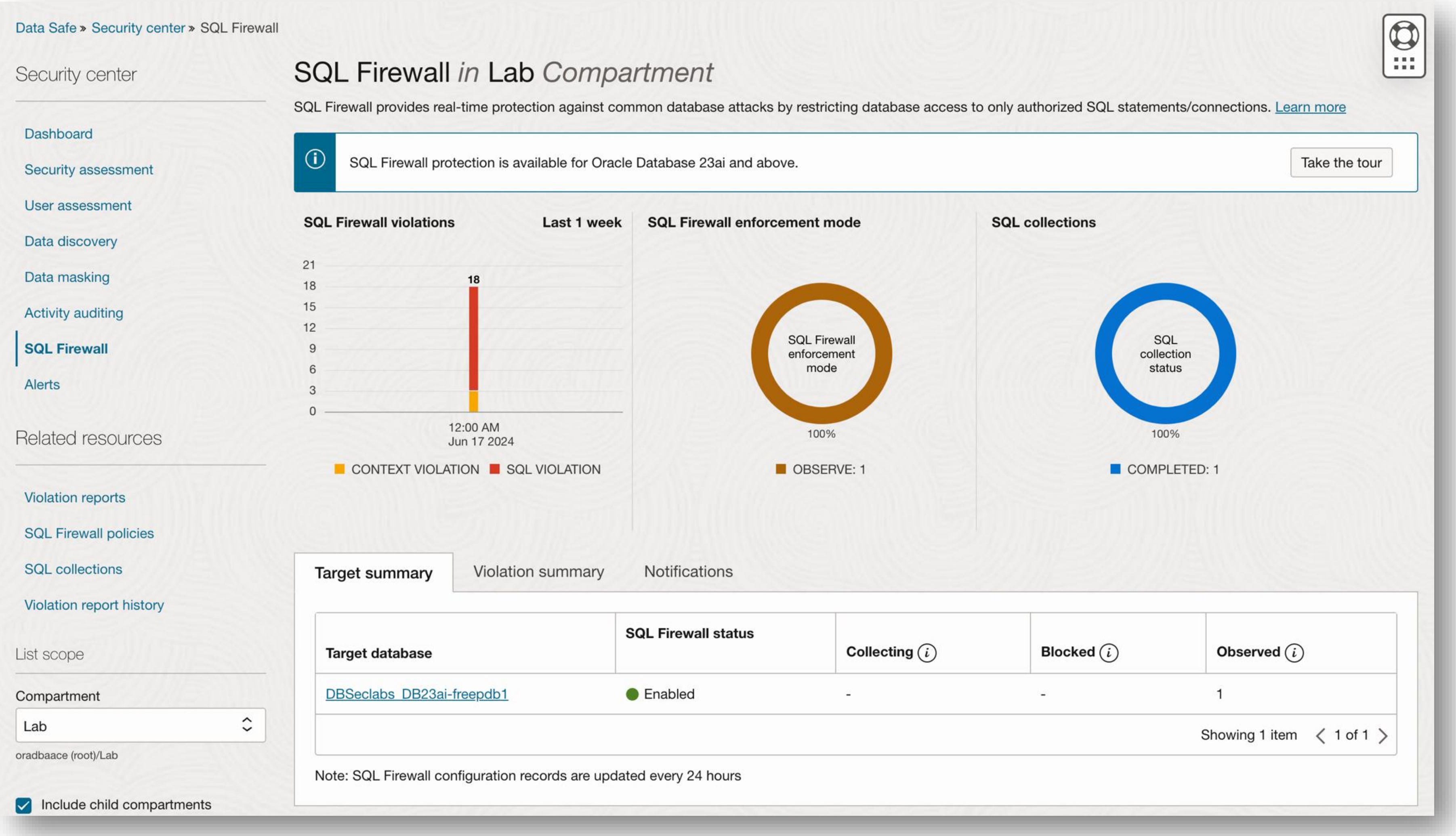
Review and define what to be protected



Copyright © 2024 Accenture. All rights reserved.

SQL Firewall – Overview

Status on the SQL Firewall



Data Safe » Security center » SQL Firewall

Security center

- Dashboard
- Security assessment
- User assessment
- Data discovery
- Data masking
- Activity auditing
- **SQL Firewall**
- Alerts

Related resources

- Violation reports
- SQL Firewall policies
- SQL collections
- Violation report history

List scope

Compartment

Lab

oradbaace (root)/Lab

☑ Include child compartments

SQL Firewall *in* Lab *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 protection is available for Oracle Database 23ai and above. Take the tour

Target summary | Violation summary | Notifications

Target database	SQL Firewall status	Collecting ⓘ	Blocked ⓘ	Observed ⓘ
DBSeclabs_DB23ai-freepdb1	● Enabled	-	-	1

Showing 1 item ‹ 1 of 1 ›

Note: SQL Firewall configuration records are updated every 24 hours

Copyright © 2024 Accenture. All rights reserved.

5

Reporting, Audit and Alerts

Strengthen Database Security through Proactive Monitoring and Auditing

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall – Data Dictionary

What's available within the Database?

- Views of the configuration

```
DBA_SQL_FIREWALL_ALLOW_LISTS
DBA_SQL_FIREWALL_ALLOWED_IP_ADDR
DBA_SQL_FIREWALL_ALLOWED_OS_PROG
DBA_SQL_FIREWALL_ALLOWED_OS_USER
DBA_SQL_FIREWALL_ALLOWED_SQL
DBA_SQL_FIREWALL_CAPTURE_LOGS
DBA_SQL_FIREWALL_CAPTURES
```

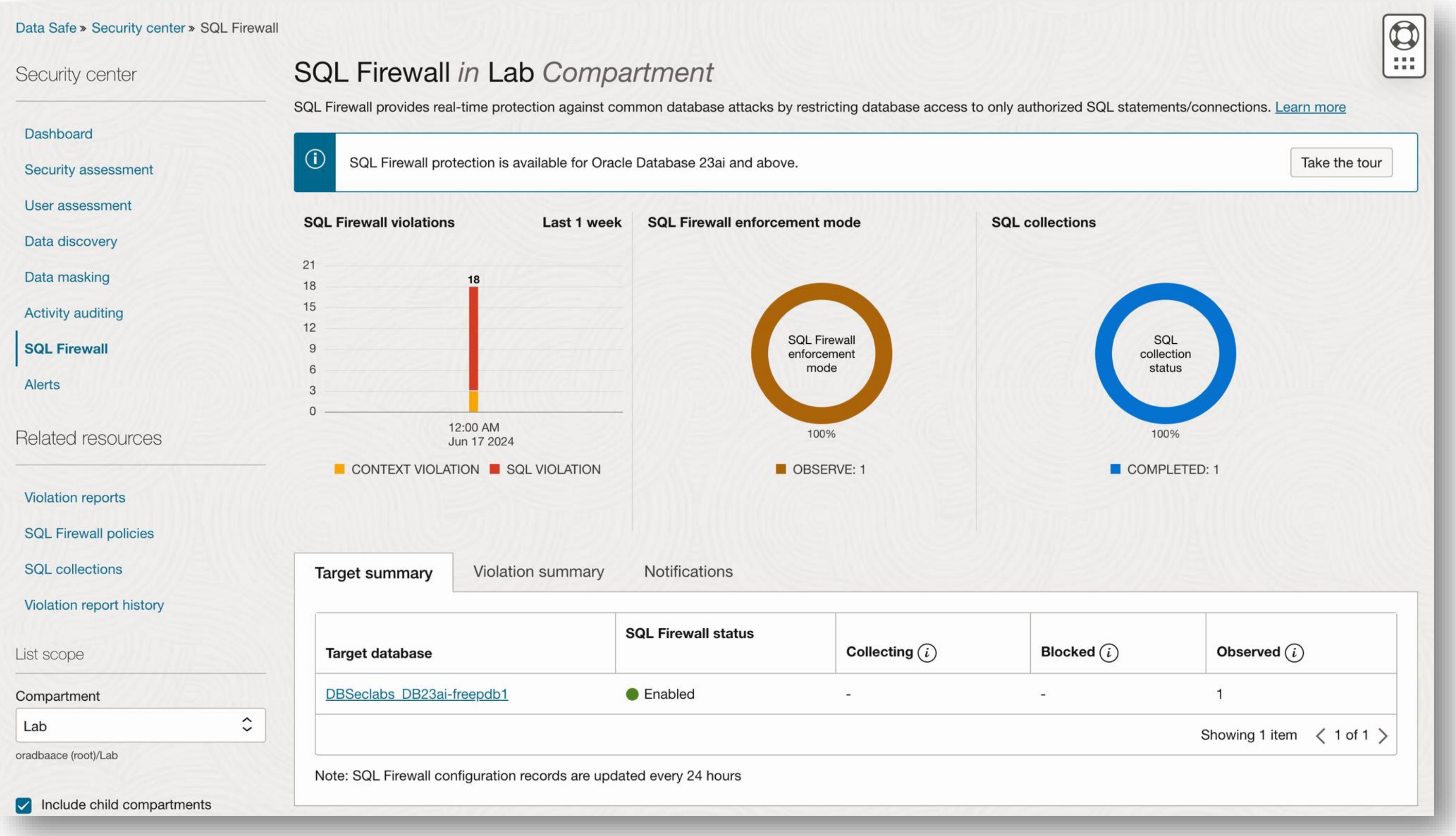
- Views on events and activity

```
DBA_SQL_FIREWALL_SESSION_LOGS
DBA_SQL_FIREWALL_SQL_LOGS
DBA_SQL_FIREWALL_STATUS
DBA_SQL_FIREWALL_VIOLATIONS
```

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall – SQL Firewall

Comprehensive reporting and alarm functions



Data Safe » Security center » SQL Firewall

Security center

- Dashboard
- Security assessment
- User assessment
- Data discovery
- Data masking
- Activity auditing
- **SQL Firewall**
- Alerts

Related resources

- Violation reports
- SQL Firewall policies
- SQL collections
- Violation report history

List scope

Compartment: Lab

oradbaace (root)/Lab

☑ Include child compartments

SQL Firewall *in* Lab *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 protection is available for Oracle Database 23ai and above. Take the tour

Target summary | Violation summary | Notifications

Target database	SQL Firewall status	Collecting (i)	Blocked (i)	Observed (i)
DBSeclabs_DB23ai-freepdb1	● Enabled	-	-	1

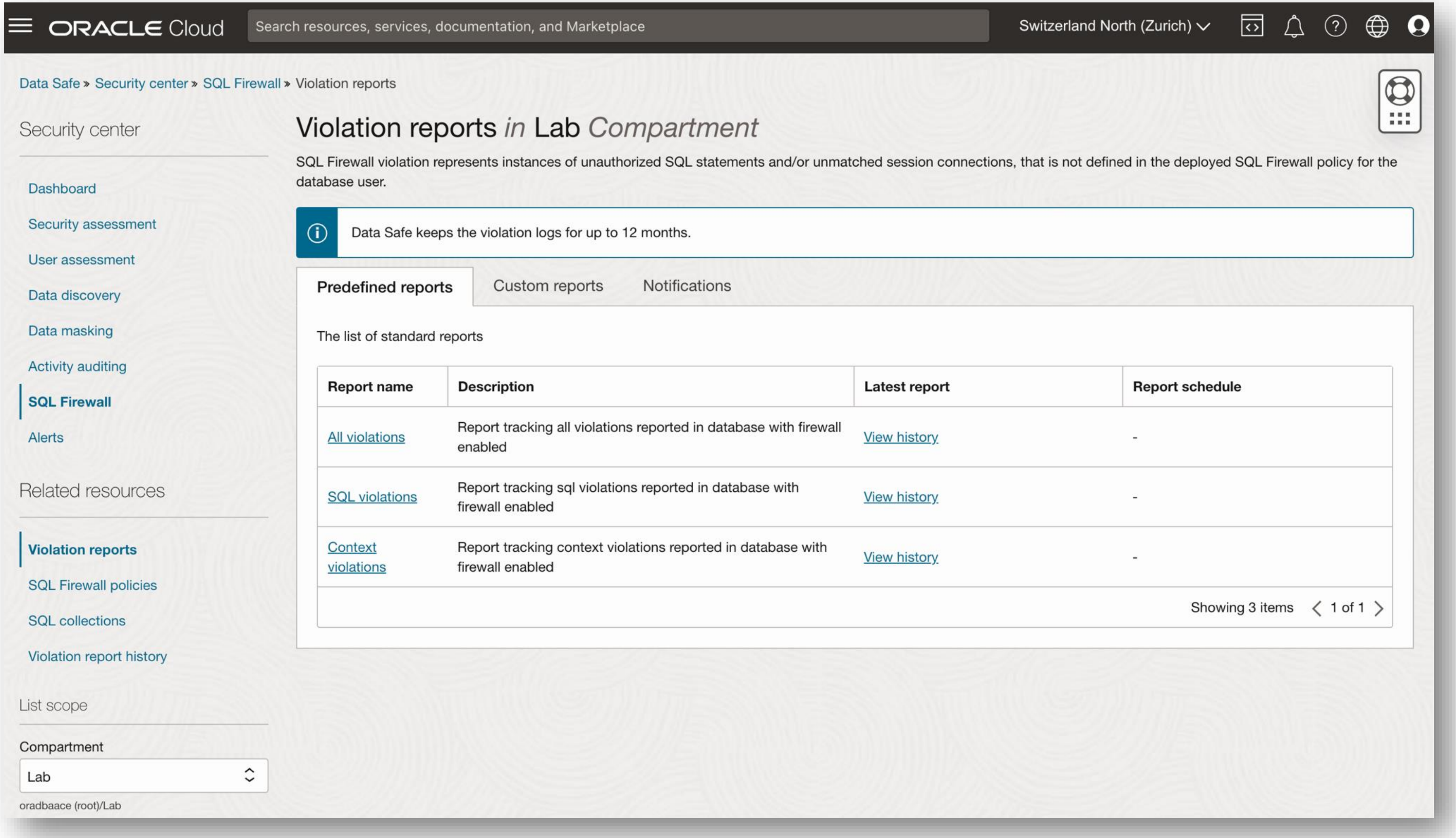
Showing 1 item < 1 of 1 >

Note: SQL Firewall configuration records are updated every 24 hours

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall – SQL Firewall

Comprehensive reporting and alarm functions



Violation reports *in* Lab *Compartment*

SQL Firewall violation represents instances of unauthorized SQL statements and/or unmatched session connections, that is not defined in the deployed SQL Firewall policy for the database user.

Data Safe keeps the violation logs for up to 12 months.

The list of standard reports

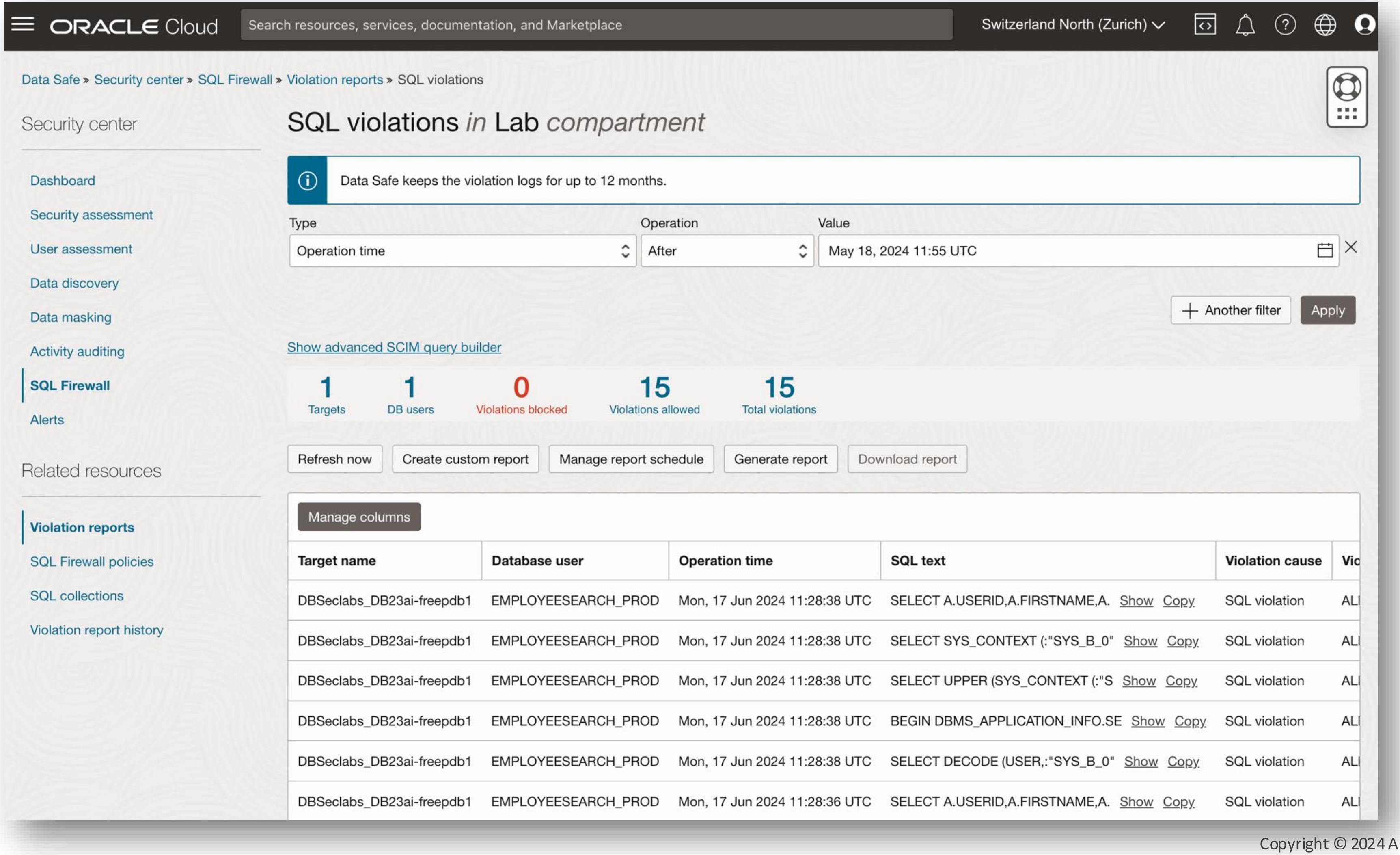
Report name	Description	Latest report	Report schedule
All violations	Report tracking all violations reported in database with firewall enabled	View history	-
SQL violations	Report tracking sql violations reported in database with firewall enabled	View history	-
Context violations	Report tracking context violations reported in database with firewall enabled	View history	-

Showing 3 items 1 of 1

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall – SQL Firewall

Comprehensive reporting and alarm functions



ORACLE Cloud
Search resources, services, documentation, and Marketplace
Switzerland North (Zurich)

Data Safe » Security center » SQL Firewall » Violation reports » SQL violations

SQL violations *in* Lab *compartment*

Data Safe keeps the violation logs for up to 12 months.

Type	Operation	Value
Operation time	After	May 18, 2024 11:55 UTC

1	1	0	15	15
Targets	DB users	Violations blocked	Violations allowed	Total violations

Target name	Database user	Operation time	SQL text	Violation cause	Vio
DBSeclabs_DB23ai-freepdb1	EMPLOYEESEARCH_PROD	Mon, 17 Jun 2024 11:28:38 UTC	SELECT A.USERID,A.FIRSTNAME,A. Show Copy	SQL violation	AL
DBSeclabs_DB23ai-freepdb1	EMPLOYEESEARCH_PROD	Mon, 17 Jun 2024 11:28:38 UTC	SELECT SYS_CONTEXT (:"SYS_B_0" Show Copy	SQL violation	AL
DBSeclabs_DB23ai-freepdb1	EMPLOYEESEARCH_PROD	Mon, 17 Jun 2024 11:28:38 UTC	SELECT UPPER (SYS_CONTEXT (:"S Show Copy	SQL violation	AL
DBSeclabs_DB23ai-freepdb1	EMPLOYEESEARCH_PROD	Mon, 17 Jun 2024 11:28:38 UTC	BEGIN DBMS_APPLICATION_INFO.SE Show Copy	SQL violation	AL
DBSeclabs_DB23ai-freepdb1	EMPLOYEESEARCH_PROD	Mon, 17 Jun 2024 11:28:38 UTC	SELECT DECODE (USER,:"SYS_B_0" Show Copy	SQL violation	AL
DBSeclabs_DB23ai-freepdb1	EMPLOYEESEARCH_PROD	Mon, 17 Jun 2024 11:28:36 UTC	SELECT A.USERID,A.FIRSTNAME,A. Show Copy	SQL violation	AL

Copyright © 2024 Accenture. All rights reserved.

6

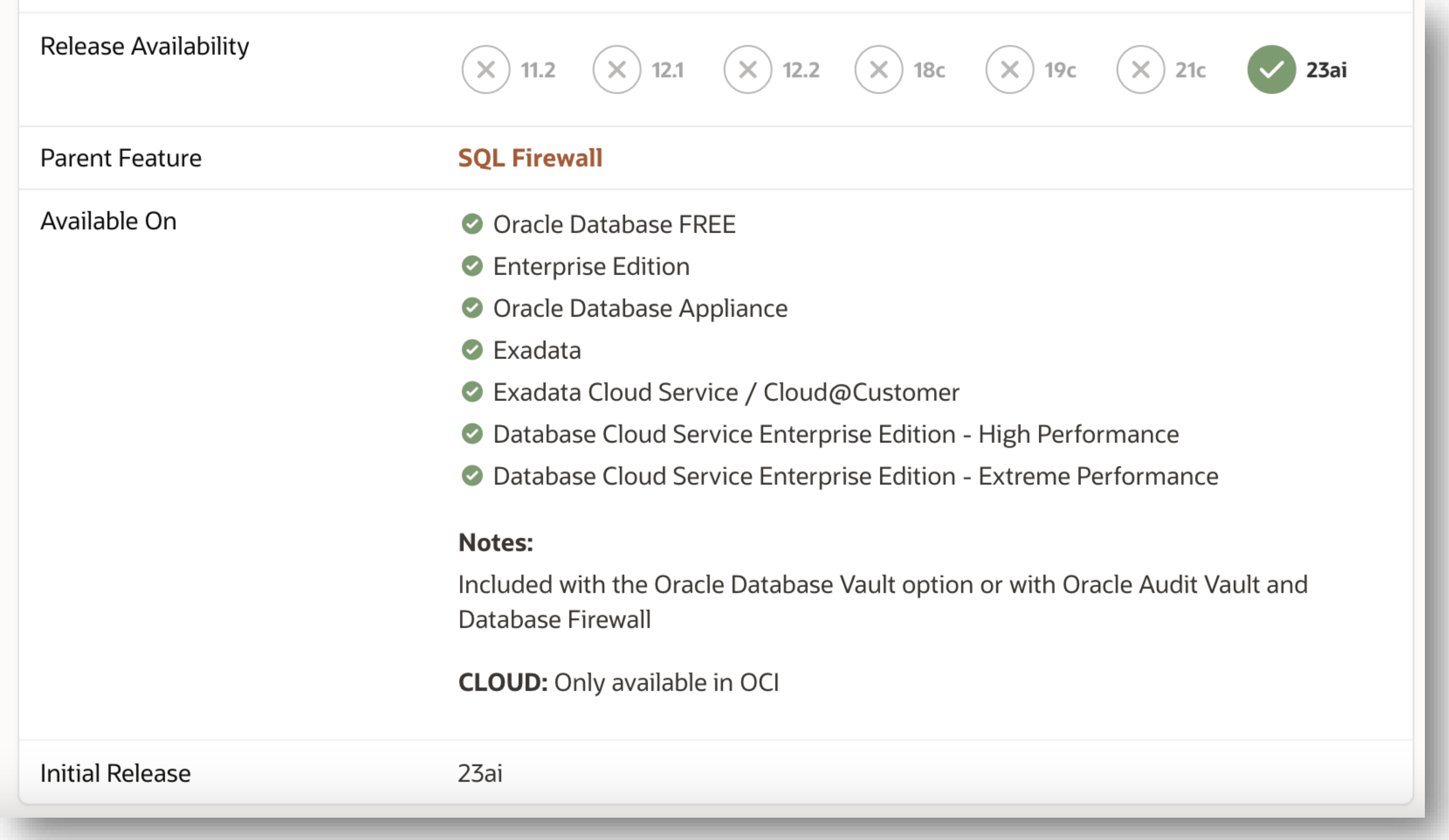
Licensing

Exploring Oracle SQL Firewall Licensing Options

Copyright © 2024 Accenture. All rights reserved.

Licensing

Exploring Oracle SQL Firewall Licensing Options



Release Availability	✗ 11.2 ✗ 12.1 ✗ 12.2 ✗ 18c ✗ 19c ✗ 21c ✓ 23ai
Parent Feature	**SQL Firewall**
Available On	✓ Oracle Database FREE ✓ Enterprise Edition ✓ Oracle Database Appliance ✓ Exadata ✓ Exadata Cloud Service / Cloud@Customer ✓ Database Cloud Service Enterprise Edition - High Performance ✓ Database Cloud Service Enterprise Edition - Extreme Performance **Notes:** Included with the Oracle Database Vault option or with Oracle Audit Vault and Database Firewall **CLOUD:** Only available in OCI
Initial Release	23ai

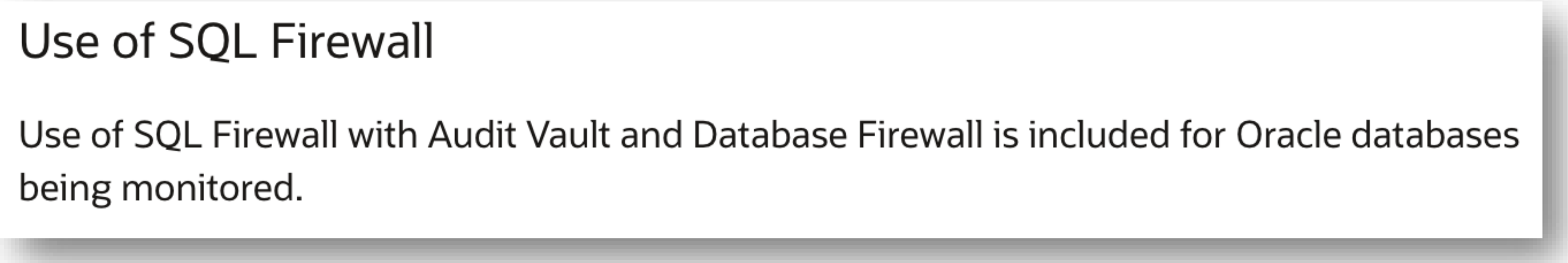
Source: https://apex.oracle.com/database-features

Copyright © 2024 Accenture. All rights reserved.

Licensing

Exploring Oracle SQL Firewall Licensing Options

- **Oracle Database FREE**
  - Use it to test, develop and engineer…
- **Oracle Database Enterprise Edition** either via
  - Oracle Database Vault Option
  - Oracle Audit Vault and Database Firewall see AVDF Licensing Information section 1.3 Restricted-Use Licensing



Use of SQL Firewall

Use of SQL Firewall with Audit Vault and Database Firewall is included for Oracle databases being monitored.

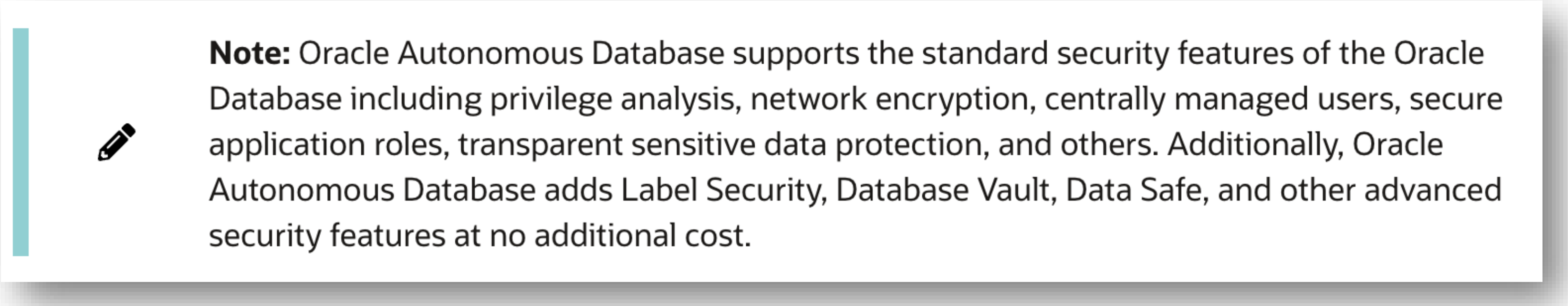
  - AVDF enables SQL Firewall on Oracle Database Standard Edition.

Copyright © 2024 Accenture. All rights reserved.

Licensing

Exploring Oracle SQL Firewall Licensing Options

- Consider using **Autonomous Database** e.g., shared, dedicated, Cloud@Customer,…
  - License includes as part of Database Vault
  - Combine it with Data Safe



Note: Oracle Autonomous Database supports the standard security features of the Oracle Database including privilege analysis, network encryption, centrally managed users, secure application roles, transparent sensitive data protection, and others. Additionally, Oracle Autonomous Database adds Label Security, Database Vault, Data Safe, and other advanced security features at no additional cost.

Copyright © 2024 Accenture. All rights reserved.

7

Challanges

Mastering Challenges: Main Challenges and Key Measures

Copyright © 2024 Accenture. All rights reserved.

Challanges

Things to consider when using the SQL firewall

Doing the Homework

- Know the application and workload
- When to collect information
- What are my Clients / Networks etc.

SQL Statements

- Are you SQL Statements “stable”
- Whitelist vs. Blacklist approach

Start as early as possible

- It is easier when the application is not yet finished

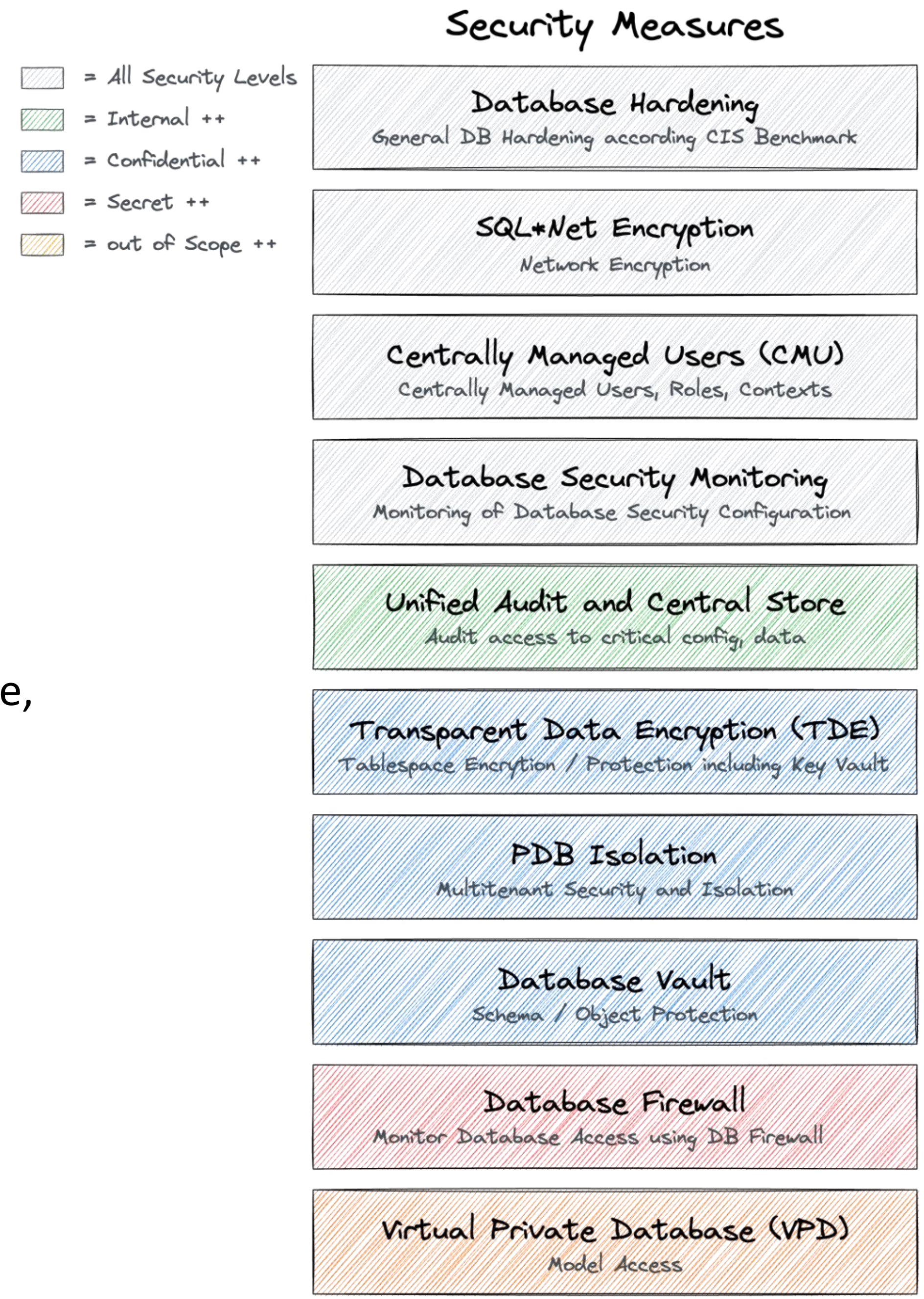
For the security we said we'd hire someone to...
Hold on, that's not the priority. Let's get the project started first, we'll see about that later...
Hey the project is nearly done, we should do a security audit to...
Too late man, we don't have the time or the budget for that
The site's been online for 10 days, and we haven't done any security testing, I'm nervous...
Don't worry, we'll take care of it later...
LATER...
DOWN! THE SITE IS DOWN! WE'VE BEEN HACKED!
How could you let this happen!?
CommitStrip.com

Copyright © 2024 Accenture. All rights reserved.

Additional Measures

SQL Firewall alone is not enough

- Defining and Implementing a Comprehensive Security Concept
- Implementation of **further** measures
  - User and role concept
  - Unified audit with corresponding assessment **and** housekeeping
  - Consider central Security Monitoring / Assessment e.g. AVDF, Data Safe, third party options



Security Measures

- ⬜ = All Security Levels
- 🟩 = Internal ++
- 🟦 = Confidential ++
- 🟥 = Secret ++
- 🟧 = out of Scope ++

Database Hardening
General DB Hardening according CIS Benchmark

SQL*Net Encryption
Network Encryption

Centrally Managed Users (CMU)
Centrally Managed Users, Roles, Contexts

Database Security Monitoring
Monitoring of Database Security Configuration

Unified Audit and Central Store
Audit access to critical config, data

Transparent Data Encryption (TDE)
Tablespace Encrytion / Protection including Key Vault

PDB Isolation
Multitenant Security and Isolation

Database Vault
Schema / Object Protection

Database Firewall
Monitor Database Access using DB Firewall

Virtual Private Database (VPD)
Model Access

Copyright © 2024 Accenture. All rights reserved.

Conclusion

Oracle SQL Firewall: Embedded security enforcement

SQL Firewall: A Major Milestone

- The SQL Firewall stands out as a pivotal feature in Oracle 23ai

Embedded permissive and enforcement modes

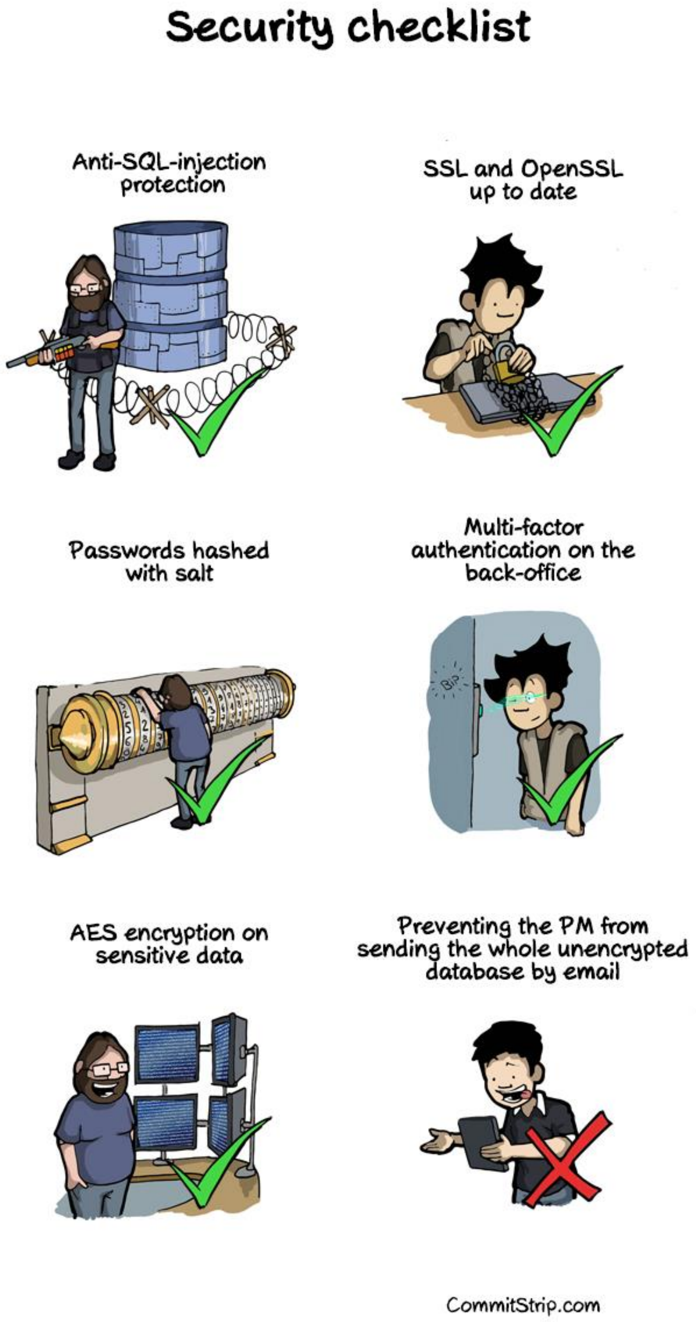
- Moves with the database e.g., cloning, backup & recovery etc.
- No additional infrastructure
- Differentiation from alternative solutions

A **good** foundation is a prerequisite

- Comprehensive Security Concept
- Additional Security Measures

The challenge: what needs to be protected and how

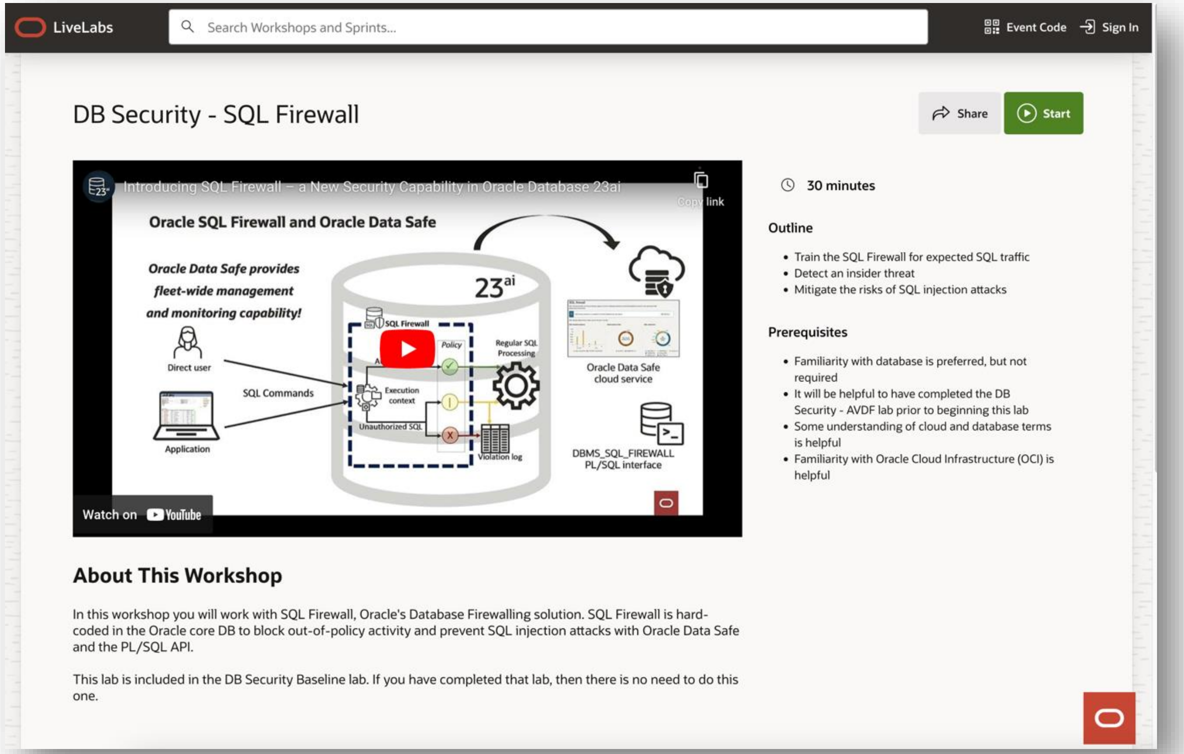
- Which Clients, IP’s, Statements?
- When to collect information?


Security checklist
Anti-SQL-injection protection
SSL and OpenSSL up to date
Passwords hashed with salt
Multi-factor authentication on the back-office
AES encryption on sensitive data
Preventing the PM from sending the whole unencrypted database by email
CommitStrip.com

Copyright © 2024 Accenture. All rights reserved.

Oracle LiveLabs – DB Security

Trial the SQL Firewall functionality in just a few minutes…


LiveLabs
Search Workshops and Sprints...
Event Code
Sign In
Share
Start
Introducing SQL Firewall – a New Security Capability in Oracle Database 23ai
Copy link
Oracle SQL Firewall and Oracle Data Safe
Oracle Data Safe provides fleet-wide management and monitoring capability!
23ai
SQL Firewall
Policy
Regular SQL Processing
Direct user
SQL Commands
Execution context
Unauthorized SQL
Violation log
Application
Oracle Data Safe cloud service
DBMS_SQL_FIREWALL PL/SQL interface
Watch on YouTube

DB Security - SQL Firewall

30 minutes

Outline

- Train the SQL Firewall for expected SQL traffic
- Detect an insider threat
- Mitigate the risks of SQL injection attacks

Prerequisites

- Familiarity with database is preferred, but not required
- It will be helpful to have completed the DB Security - AVDF lab prior to beginning this lab
- Some understanding of cloud and database terms is helpful
- Familiarity with Oracle Cloud Infrastructure (OCI) is helpful

About This Workshop

In this workshop you will work with SQL Firewall, Oracle's Database Firewalling solution. SQL Firewall is hard-coded in the Oracle core DB to block out-of-policy activity and prevent SQL injection attacks with Oracle Data Safe and the PL/SQL API.

This lab is included in the DB Security Baseline lab. If you have completed that lab, then there is no need to do this one.

DB Security - **SQL Firewall** ID 3875

- Train the SQL Firewall for expected SQL traffic
- Detect an insider threat
- Mitigate the risks of SQL injection attacks

- https://apexapps.oracle.com/pls/apex/r/dbpm/livelabs/view-workshop?wid=3875

Copyright © 2024 Accenture. All rights reserved.

SQL Firewall offers infrastructure-free database protection, needing solid security concepts for full potential.

Copyright © 2024 Accenture. All rights reserved.

Thank You