ORACLE

DatabaseWorld @ CloudWorld

Security Posture Management with Audit Vault and Database Firewall

LRN1646

Nazia Zaidi
Product Manager
Audit Vault and Database Firewall
September 2023

Stefan Oehrli
Technical Architecture Manager
Accenture

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regarding the integration of any EMEA Cerner and/or Enviza entities have been made where an integration has not already occurred.

Introduction to Audit Vault and Database Firewall (AVDF)

1

AVDF Overview

A single pane of glass solution for data security and monitoring

2

What is DSPM & Why?

Understand the DSPM use cases

3

AVDF - DSPM

Extending AVDF beyond Database Activity Monitoring Solution

4

Deployment Experience

Best Practices to follow in the real world

5

Wrap-up and Next steps

How to get the most out of AVDF

Overview - Audit Vault and Database Firewall

A Single Pane of Glass for Database Activity Monitoring and Beyond!

Audit Vault and Database Firewall

Prevent & Protect

Prevent unauthorized activities.
Protect against unknown threats.

Assess & Discover

Assess your security posture. Discover sensitive data and privileged users.

Report & Alert

Report on database activity and security posture. Alert for suspicious events.

Audit & Monitor

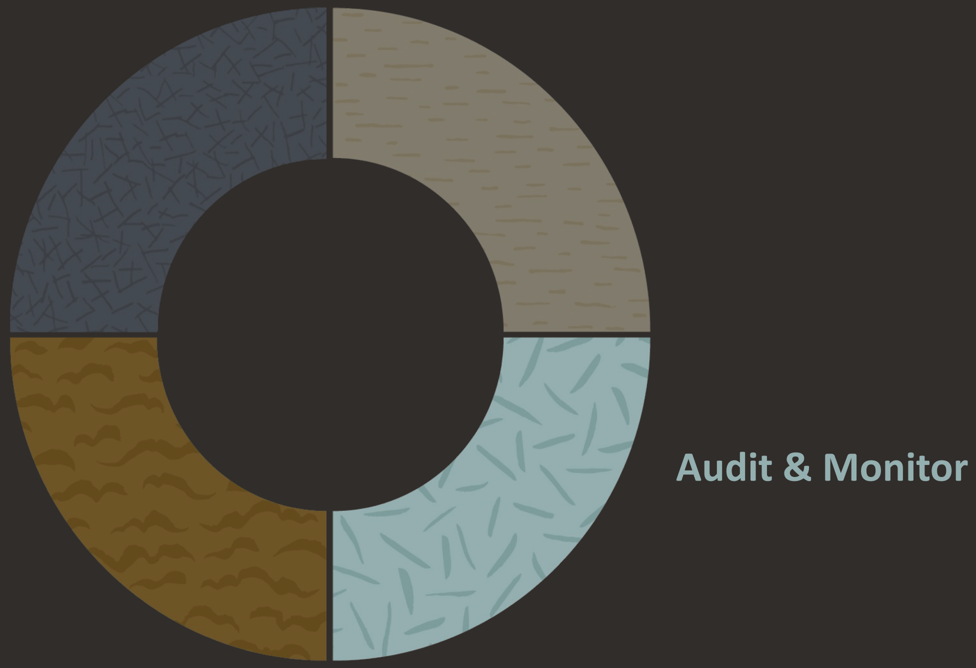
Monitor all database activity for anomalies. Audit security-relevant actions.

Assess and Discover

- Fleet-wide database security posture management
- Compliance mapping and recommendations
- Discover sensitive data and privileged users
- User entitlement monitoring with drift management

Audit and Monitor

- Activity monitoring – database, network-based SQL traffic, OS, directory, Rest, JSON, XML, CSV, and custom tables
- Detect data exfiltration
- Before/after values for Oracle & Microsoft SQL Server Databases
- Centrally managed Oracle unified audit policies. Pre-defined STIG, and CIS-compliant audit policies



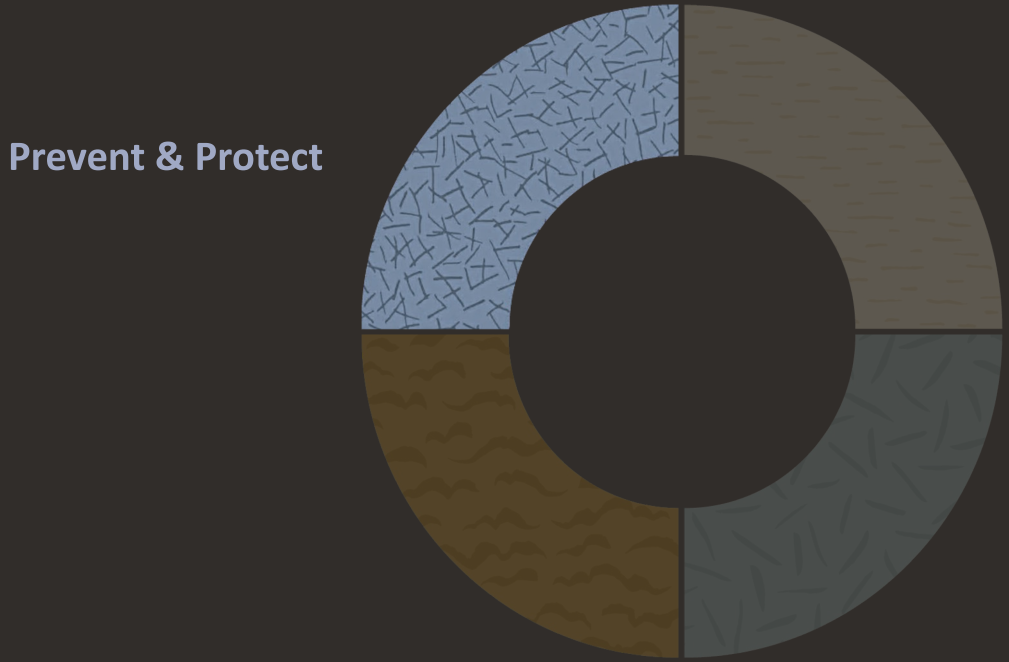
Report and Alert

- Out-of-the-box reports for security and compliance regulations
- Powerful interactive reporting with a filterable interface for rapid data analysis
- Audit insights into the top user activities across multiple databases
- Policy-based alert engine
- Built-in separation of duty

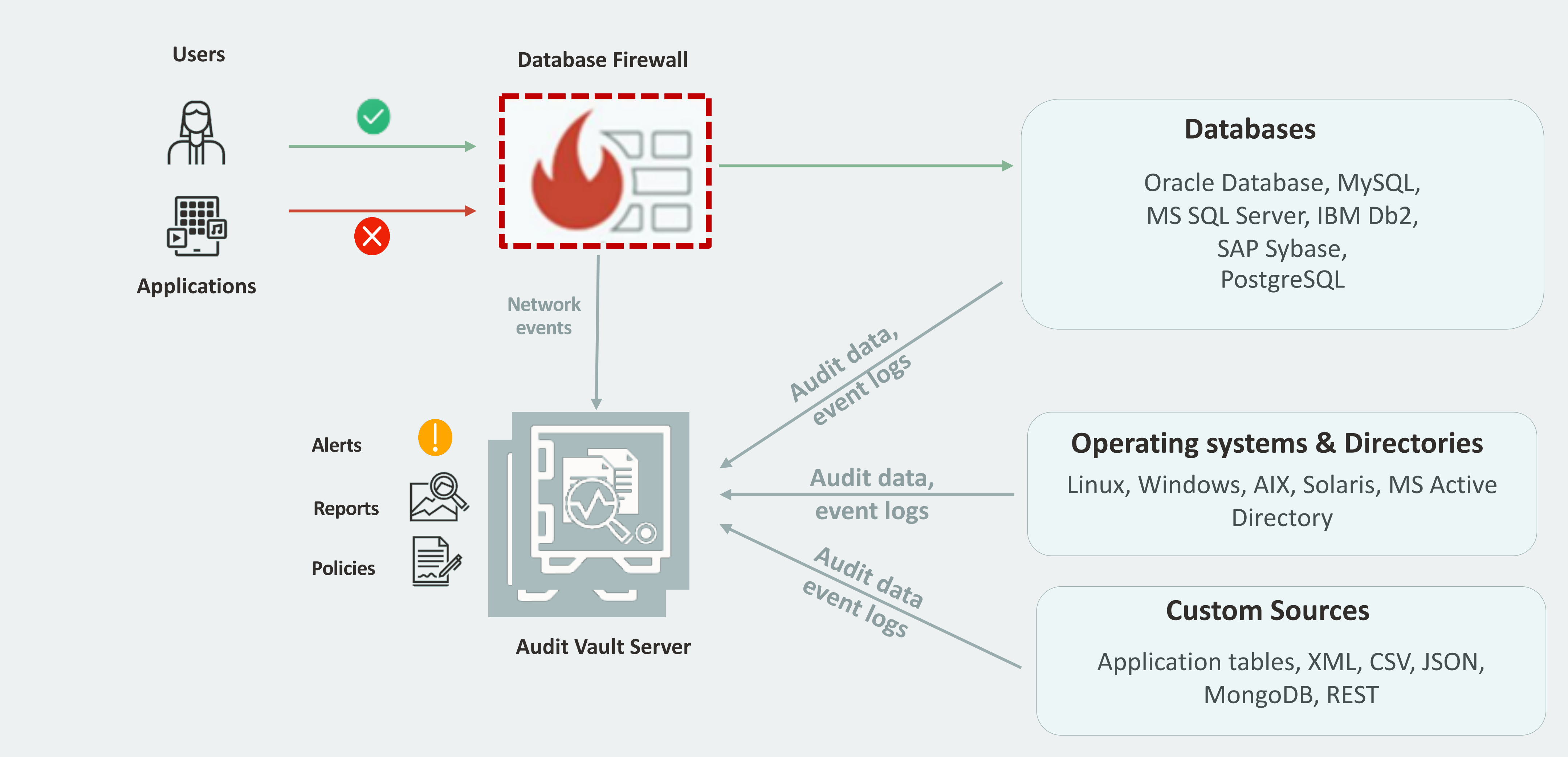
Report & Alert

Prevent and Protect

- Powerful policy engine that detects unauthorized access to sensitive tables
- Inspect SQL traffic to accurately detect and block unauthorized SQL including SQL injection attacks
- Profile an application's SQL and block deviations from normal access patterns



Database Activity Monitoring and Auditing with AVDF



Databases

Oracle Database, MySQL, MS SQL Server, IBM Db2, SAP Sybase, PostgreSQL

Operating systems & Directories

Linux, Windows, AIX, Solaris, MS Active Directory

Custom Sources

Application tables, XML, CSV, JSON, MongoDB, REST

Database Security Posture Management

Know your security posture

What is Database Security Posture Management

Security Assessment

Know your security configuration and identify drift from your accepted security baseline

Sensitive Data Discovery

Know what your sensitive objects are and where they are stored

Privileged User Discovery

Know who your privileged users are and what permissions they have

Audit Insights

Know how your sensitive data has been used by database users

Why Security Assessment?

Is my Oracle Database configured securely?

Am I following the best practices?

Am I compliant with my own security standards?

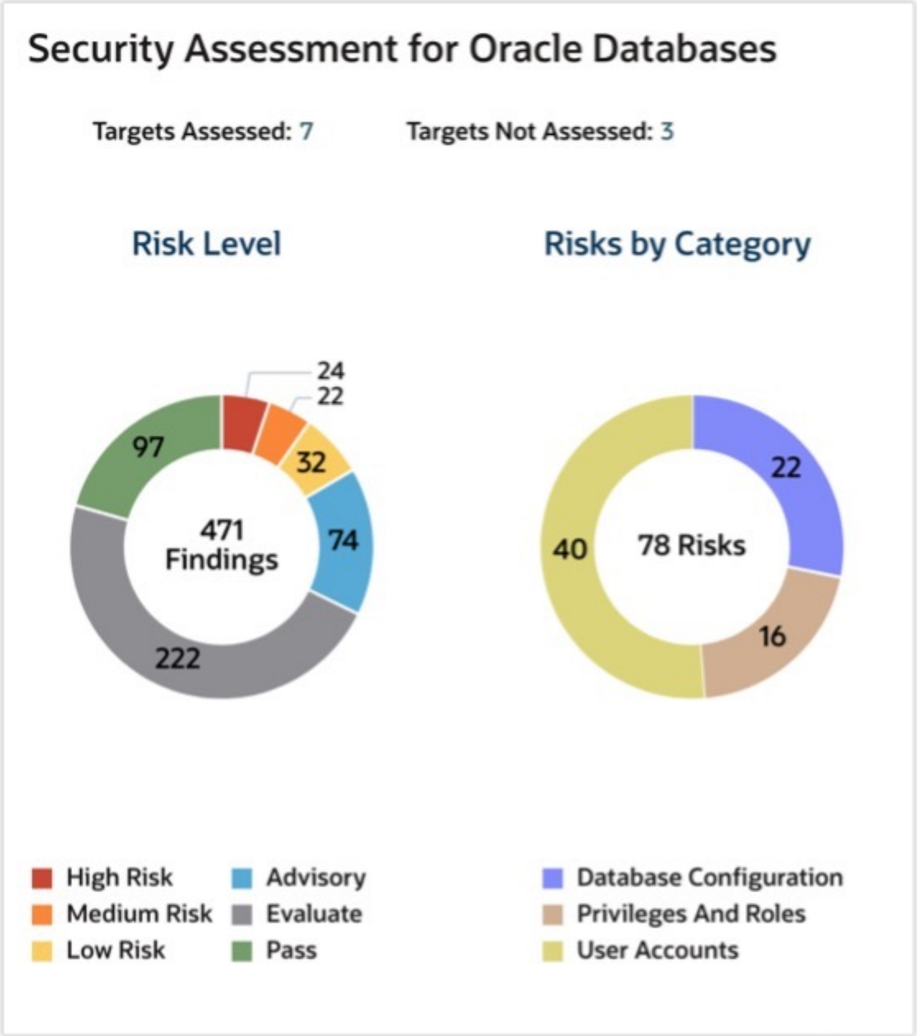
What else should I do to further strengthen my Oracle Database deployment?

AVDF Security Assessment

69 Findings

8 Categories

6 Risk levels

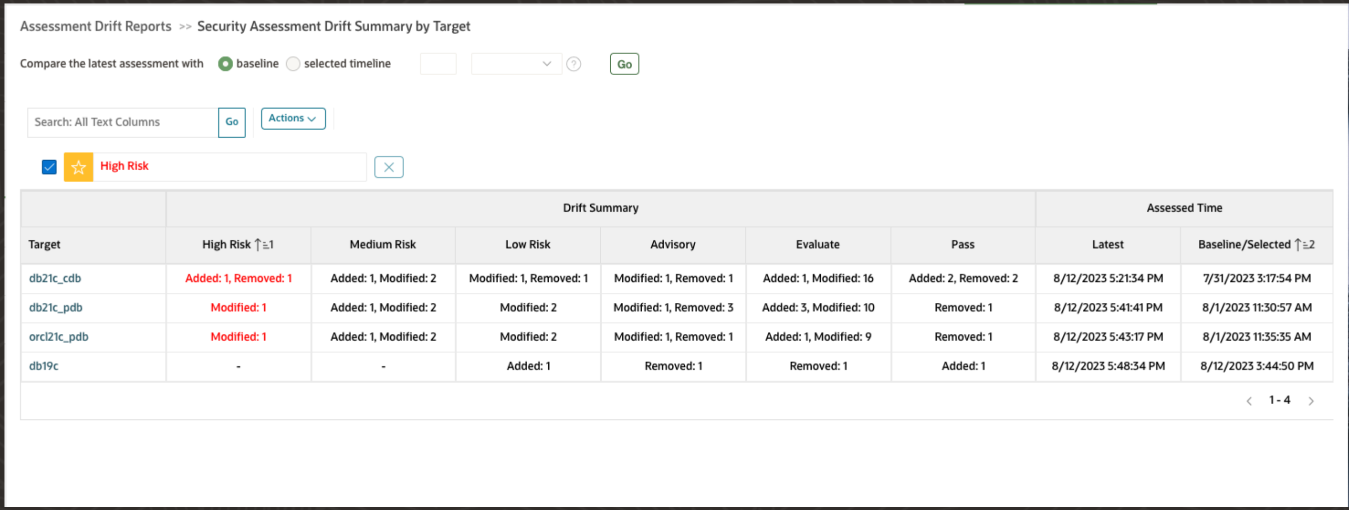

Security Assessment for Oracle Databases

Targets Assessed: 7 Targets Not Assessed: 3

Security Assessment for Enterprise

Know the security posture for your enterprise!

- **Fleet-wide database security assessment**
  Integration with the proven Oracle Database Security Assessment Tool (DBSAT)
- **Improved Productivity**
  Single view of all the assessed and unassessed targets
- **Interactive reporting**
  Drill-down charts and reports
  Helps you take quick action on potential risk
- ***Drift management**
  Define an assessment baseline
  Monitor for deviation from that baseline



Assessment Drift Reports >> Security Assessment Drift Summary by Target

Compare the latest assessment with ● baseline ○ selected timeline

☑ ☆ High Risk

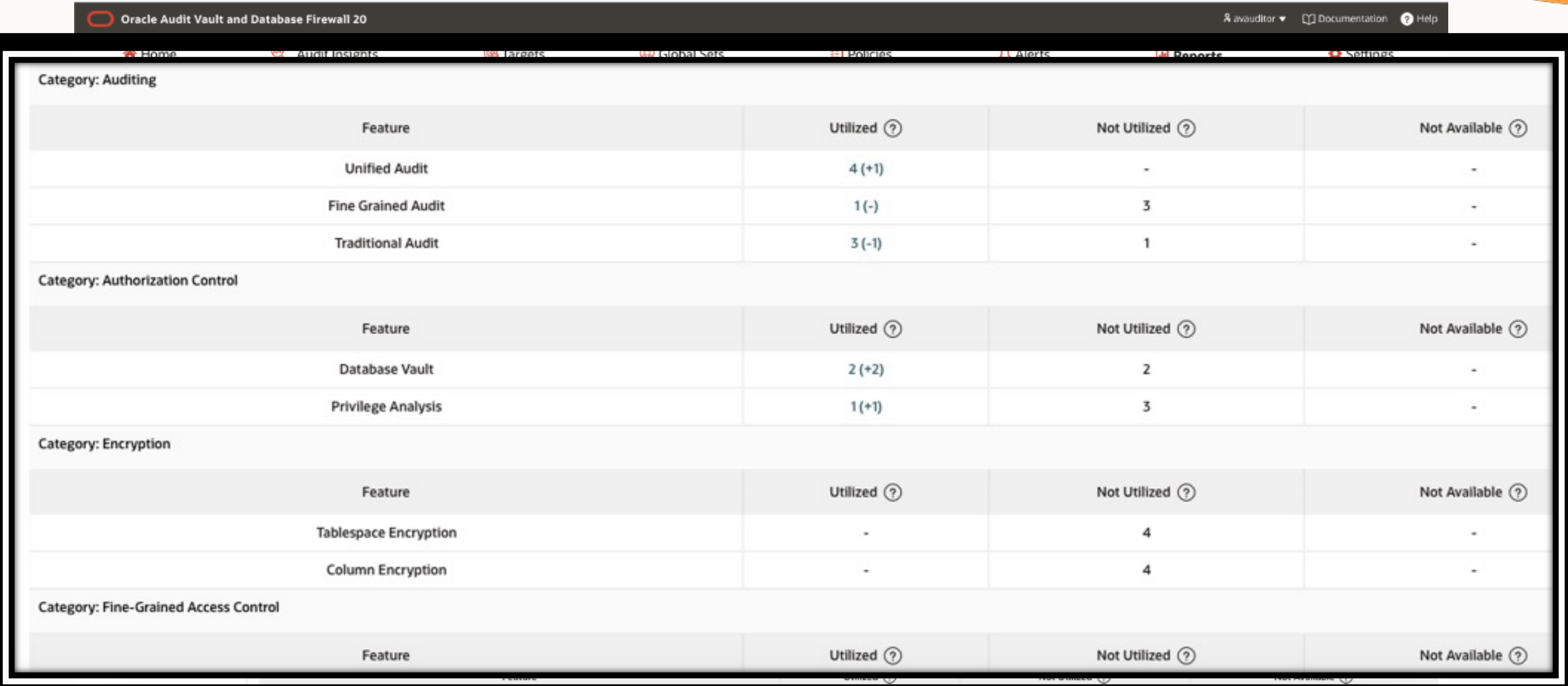
	Drift Summary						Assessed Time	
Target	High Risk ↑≡1	Medium Risk	Low Risk	Advisory	Evaluate	Pass	Latest	Baseline/Selected ↑≡2
db21c_cdb	Added: 1, Removed: 1	Added: 1, Modified: 2	Modified: 1, Removed: 1	Modified: 1, Removed: 1	Added: 1, Modified: 16	Added: 2, Removed: 2	8/12/2023 5:21:34 PM	7/31/2023 3:17:54 PM
db21c_pdb	Modified: 1	Added: 1, Modified: 2	Modified: 2	Modified: 1, Removed: 3	Added: 3, Modified: 10	Removed: 1	8/12/2023 5:41:41 PM	8/1/2023 11:30:57 AM
orcl21c_pdb	Modified: 1	Added: 1, Modified: 2	Modified: 2	Modified: 1, Removed: 1	Added: 1, Modified: 9	Removed: 1	8/12/2023 5:43:17 PM	8/1/2023 11:35:35 AM
db19c	-	-	Added: 1	Removed: 1	Removed: 1	Added: 1	8/12/2023 5:48:34 PM	8/12/2023 3:44:50 PM

< 1 - 4 >

*Very Near Future

Very Near Future

Fleet-wide drift on security controls



Category: Auditing

Feature	Utilized	Not Utilized	Not Available
Unified Audit	4 (+1)	-	-
Fine Grained Audit	1 (-)	3	-
Traditional Audit	3 (-1)	1	-

Category: Authorization Control

Feature	Utilized	Not Utilized	Not Available
Database Vault	2 (+2)	2	-
Privilege Analysis	1 (+1)	3	-

Category: Encryption

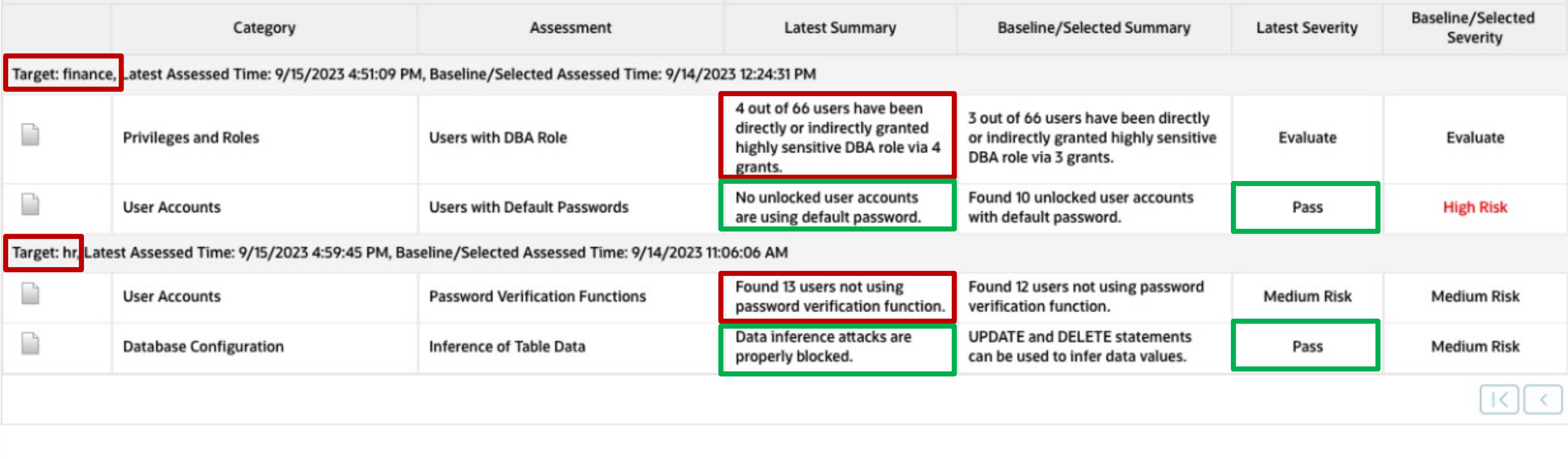
Feature	Utilized	Not Utilized	Not Available
Tablespace Encryption	-	4	-
Column Encryption	-	4	-

Category: Fine-Grained Access Control

Feature	Utilized	Not Utilized	Not Available

Very Near Future

Detailed Fleet-wide drift on security controls



	Category	Assessment	Latest Summary	Baseline/Selected Summary	Latest Severity	Baseline/Selected Severity
Target: finance, Latest Assessed Time: 9/15/2023 4:51:09 PM, Baseline/Selected Assessed Time: 9/14/2023 12:24:31 PM						
🗋	Privileges and Roles	Users with DBA Role	4 out of 66 users have been directly or indirectly granted highly sensitive DBA role via 4 grants.	3 out of 66 users have been directly or indirectly granted highly sensitive DBA role via 3 grants.	Evaluate	Evaluate
🗋	User Accounts	Users with Default Passwords	No unlocked user accounts are using default password.	Found 10 unlocked user accounts with default password.	Pass	High Risk
Target: hr, Latest Assessed Time: 9/15/2023 4:59:45 PM, Baseline/Selected Assessed Time: 9/14/2023 11:06:06 AM						
🗋	User Accounts	Password Verification Functions	Found 13 users not using password verification function.	Found 12 users not using password verification function.	Medium Risk	Medium Risk
🗋	Database Configuration	Inference of Table Data	Data inference attacks are properly blocked.	UPDATE and DELETE statements can be used to infer data values.	Pass	Medium Risk

Why Sensitive Data and Privileged User Discovery?

Compromised accounts are the most common cause of data breaches

Where is my sensitive data stored?

Who are my privileged users?

What permission do they have?

Understanding sensitive data and privileged users is critical to managing risk from compromised credentials

Discover – Data & User

Discover privileged users and sensitive objects. Create global sets to define Database Firewall (DBFW) policies

- **User entitlement analysis**

  Reporting and attestation

  Detect drift

- **Single-Click Discovery**

  Integration with DBSAT and Entitlement Reporting

- **Global Profiling**

  Create global sets of similar types like DB Objects and Privilege Users

- **Quick Deployment**

  Easy implementation

  Reduced time to market

Audit Insights

Know your TOP 5s!

- **Birds-Eye View**

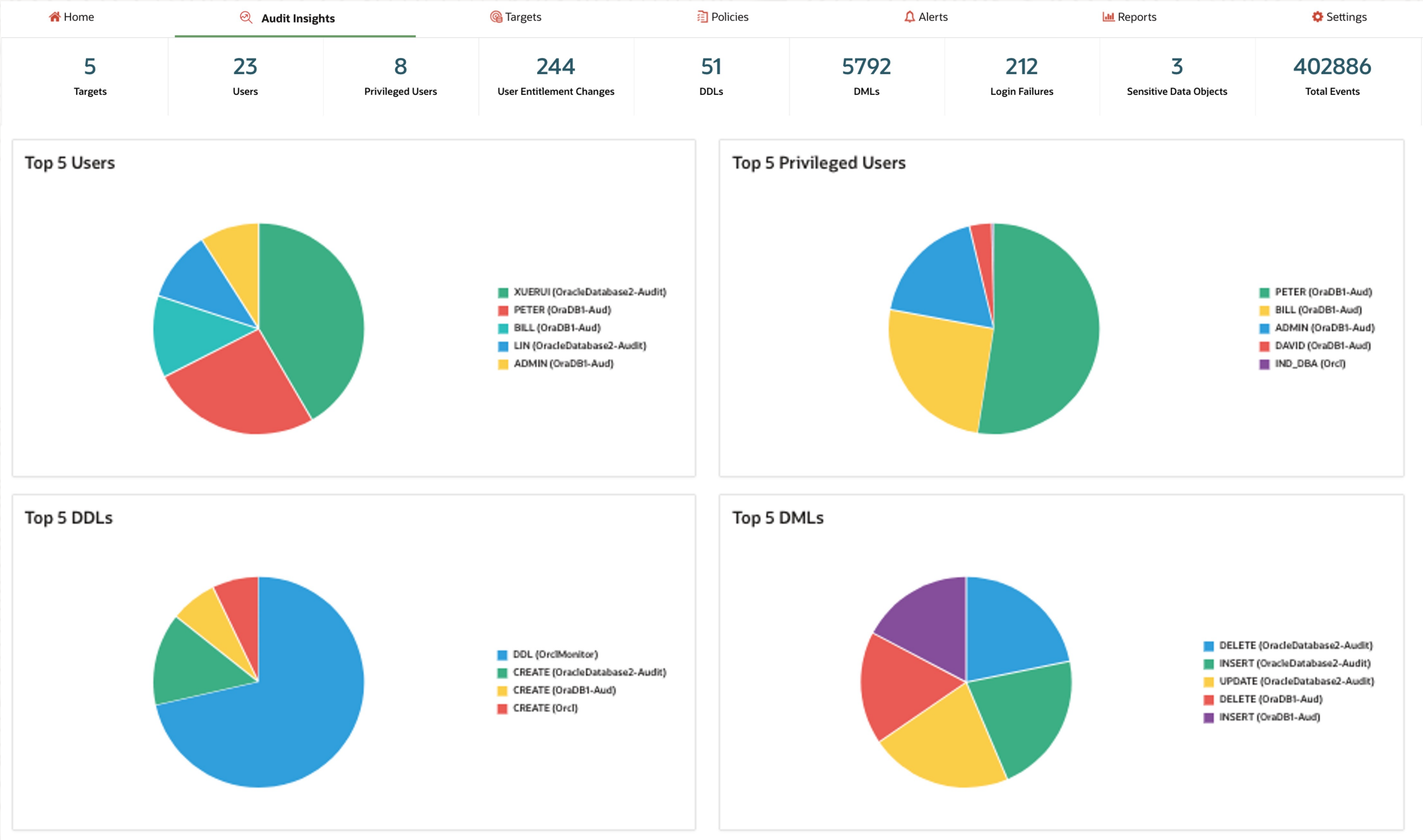
  Immediate insight into top user activities

- **Enterprise-Class reporting**

  Summarized view of all the events across multiple targets

- **Reduce Noise**

  Focus on top activities with different context



5	23	8	244	51	5792	212	3	402886
Targets	Users	Privileged Users	User Entitlement Changes	DDLs	DMLs	Login Failures	Sensitive Data Objects	Total Events

Deployment Experiences

Best Practices to follow in the real world

Stefan Oehrli

Tech Architecture Manager - Accenture

September 2023

Project Information

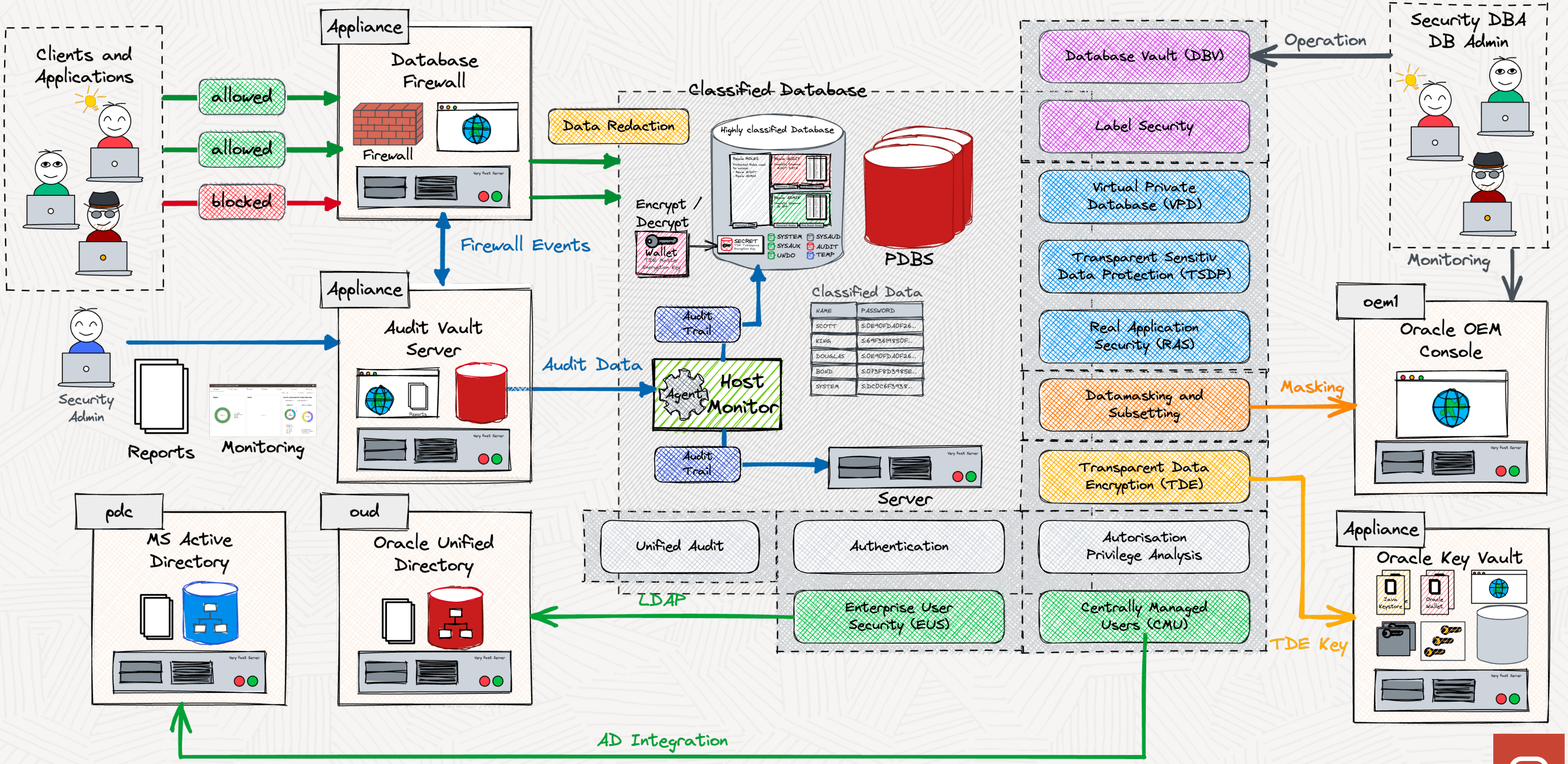
About the Customer Environment

- Larger retail / DIY store chain in Germany
- Moderate number of Oracle databases 12c- 19c
- Running on Oracle Engineered Systems
- Other database systems such as MS SQL Server

The client's major pain Points and Challenges

- No specific security measures in place
- Small database operations team
- Latent risk of a ransomware attack
- Regulatory requirements for security / traceability

Maximum Data Security Architecture



Classified Data

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

A few more Projects

Larger Swiss bank

- Oracle Audit Vault and Database Firewall as successor of Oracle Audit Vault
- Exclusively used for the administration and evaluation of Oracle database audit trails
- In operation for several years

Swiss Privat Bank

- Monitoring and protection of databases from high-privilege and administrative access
- Several different database technologies in use i.e., Oracle, MS SQL Server, PostgreSQL, etc.
- PoC for the options where Hardening, AVDF, and Oracle DB Vault were evaluated

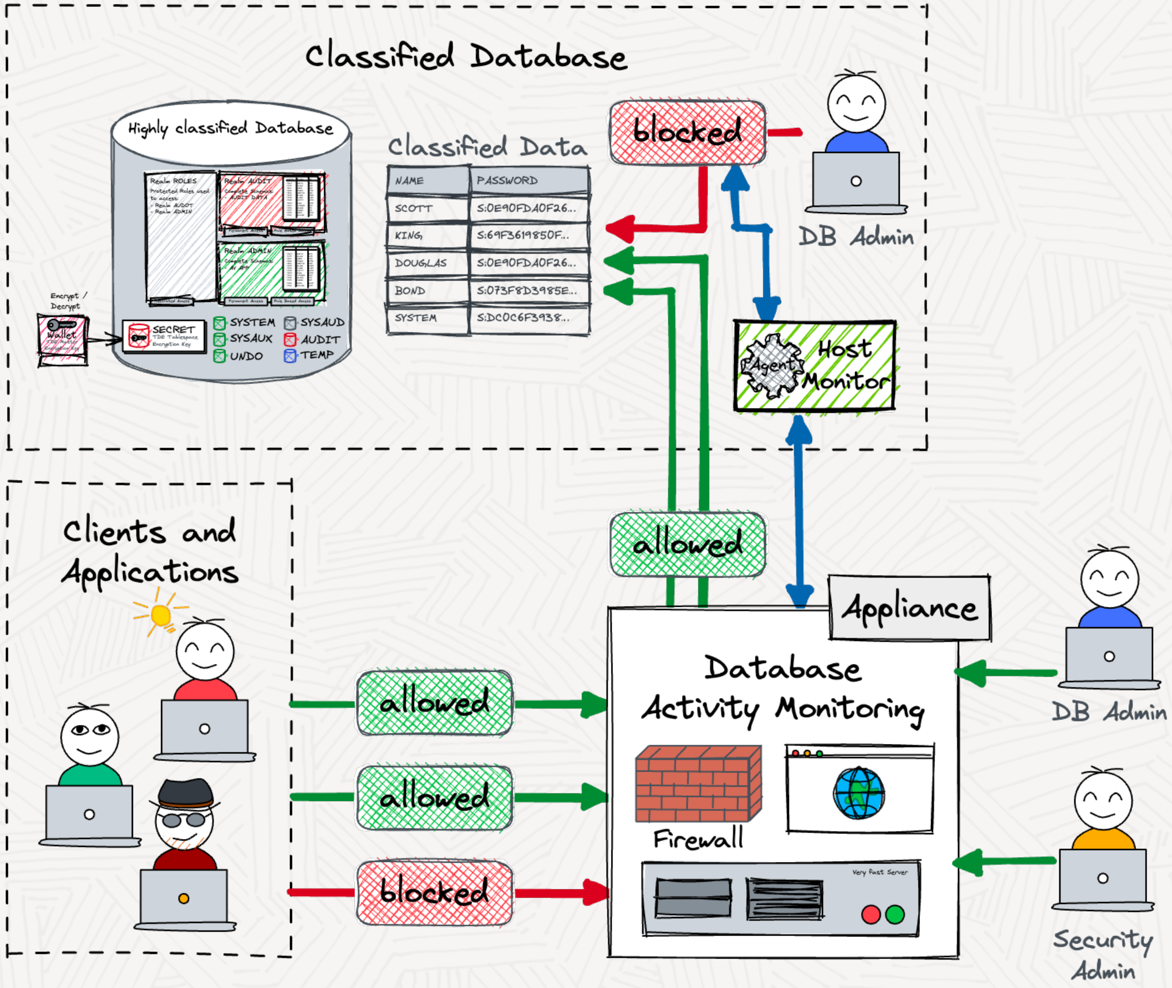
Roles and Responsibilities

Who does **what**?

- Setup the Appliance
- Configure the Agents
- Define and configure Audit Policies
- Review Audit Data
- Monitor the Oracle AVDF Environment

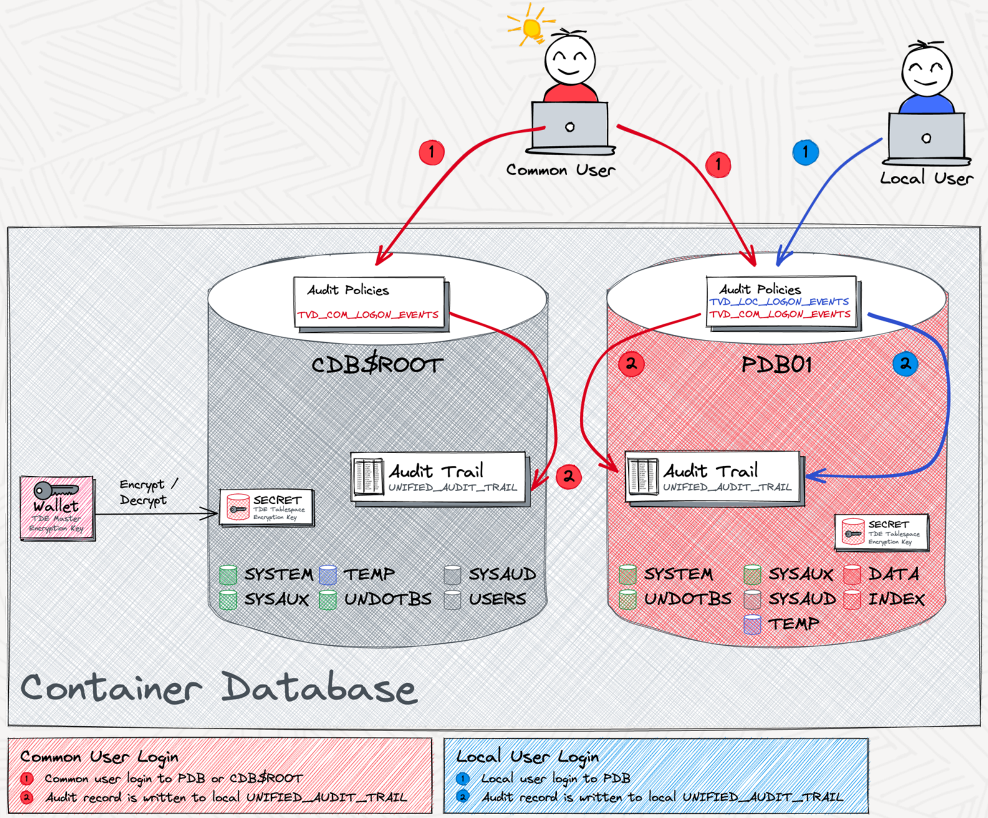
In a small team, there tends to be one admin for everything

- Shortcuts, workarounds, and tweaking
  →*Does not lead to a stable/secure environment*.



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

~~Storage~~ Space: the Final Frontier



Common User Login

1. Common user login to PDB or CDB$ROOT
2. Audit record is written to local UNIFIED_AUDIT_TRAIL

Local User Login

1. Local user login to PDB
2. Audit record is written to local UNIFIED_AUDIT_TRAIL

Problem

- Poor Role and User Management
- Comprehensive Audit Policies for Critical DB Activities
  → *Leads to up to 30 million Audit Records per DB / day*
- Instant Integration into AVDF
  → *Tablespace for Audit Trail as well as AVDF Event Log have been blown up*

Solution

- Settle and implement the Safety Concept in Advance
- Step-by-step implementation of the measures
- Be aware and prepared for side effects

Right Setup for High Availbility

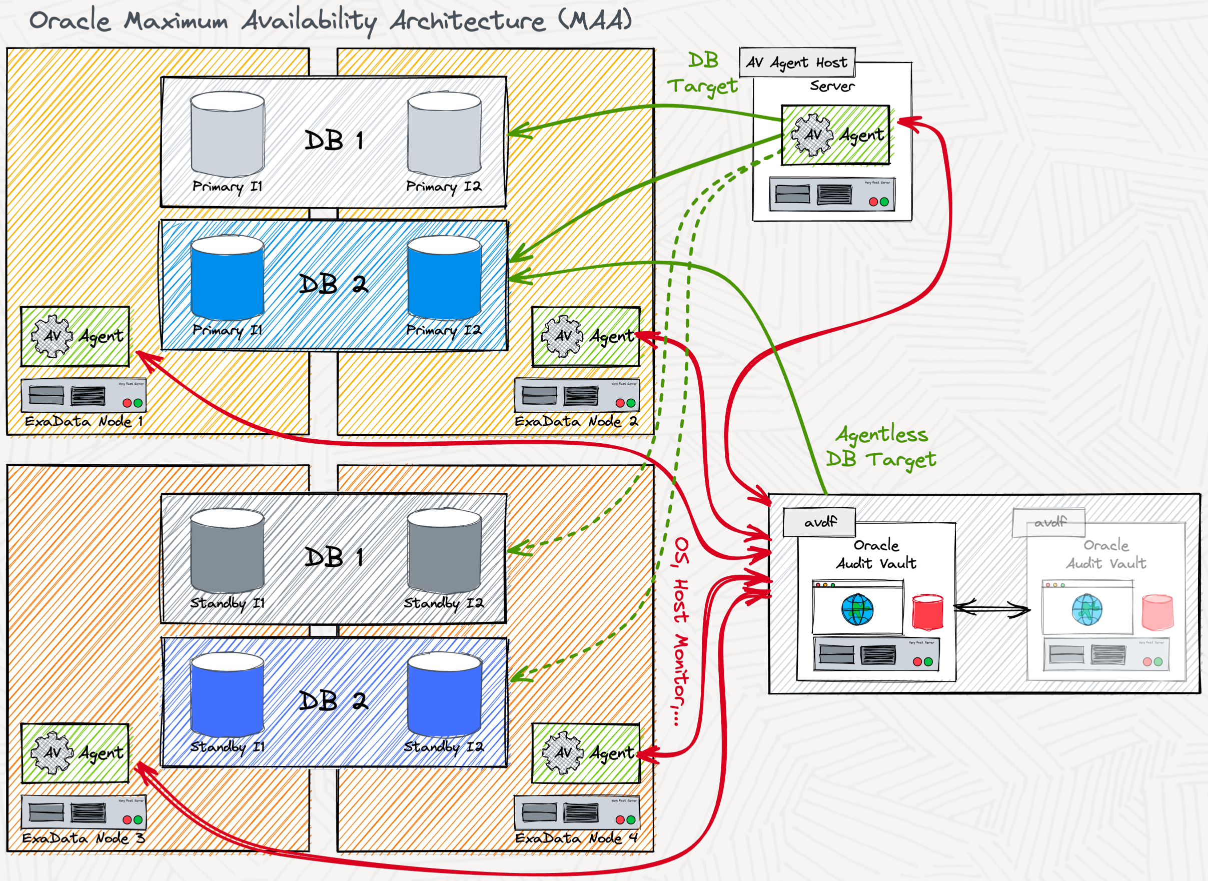
How should the Audit Trail be accessed in an MAA setup?

Which components must be highly available?

- Everything?
- Just AVDF?
- What about RAC and Standby Databases?

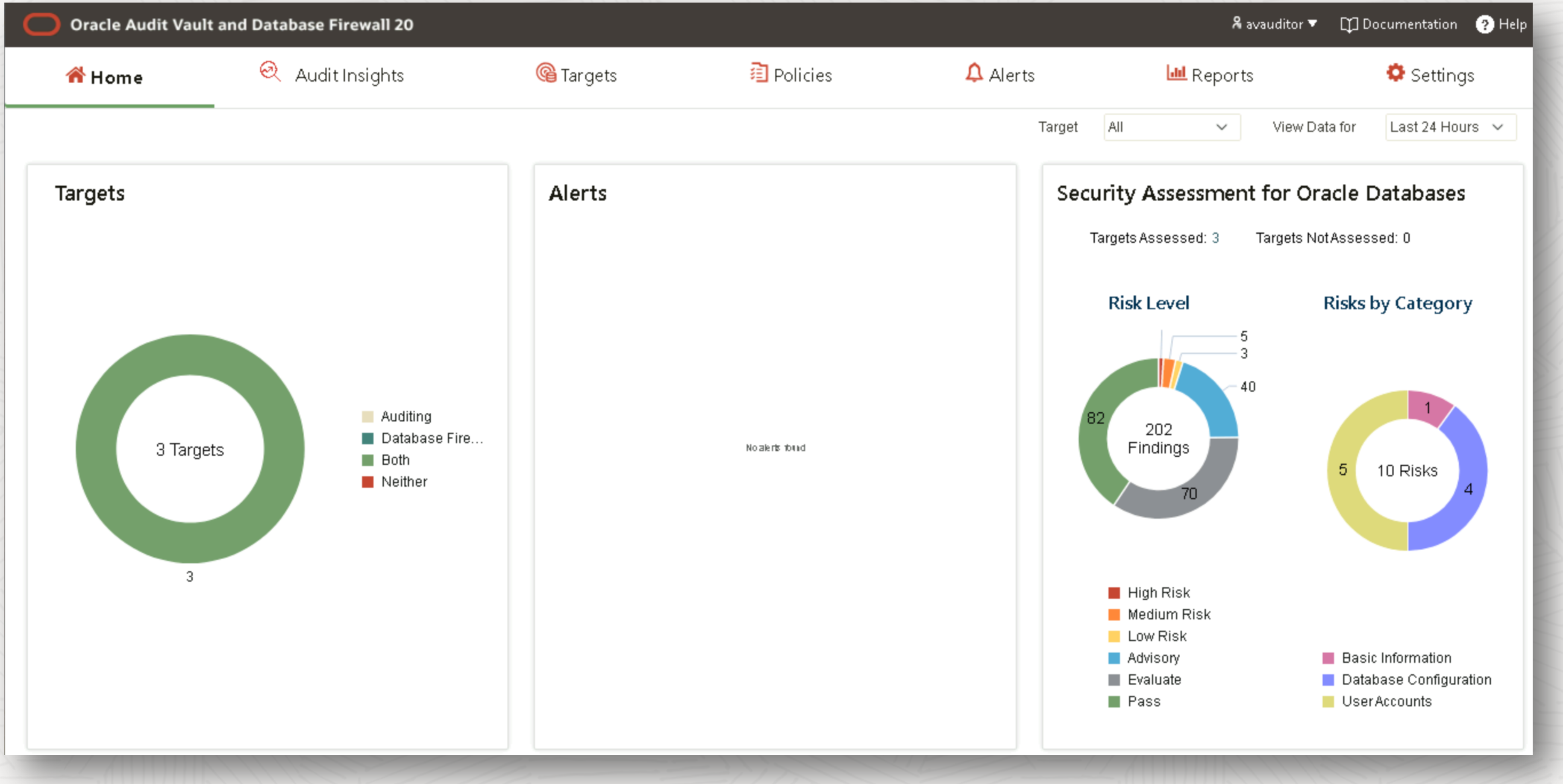
Should the Audit Event be available immediately in AVDF?

- Can an audit agent be offline for a certain amount of time?
- How much “buffer” is required to keep local audit events?



Benefits from the latest AVDF Release

Out of the box Security Assessment Information for Oracle Databases



Target: All

View Data for: Last 24 Hours

Targets

Alerts

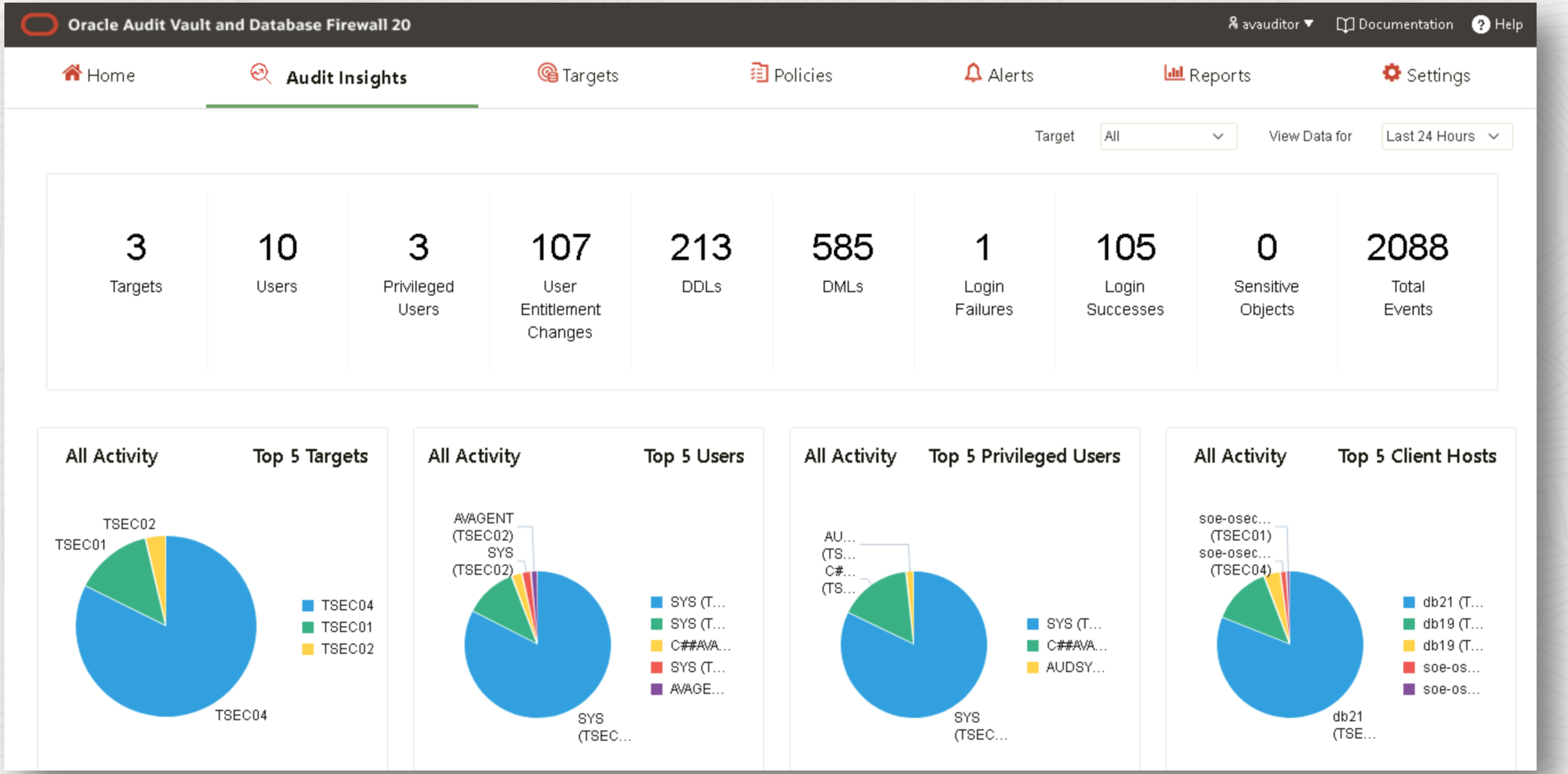
No alerts found

Security Assessment for Oracle Databases

Targets Assessed: 3 Targets Not Assessed: 0

Benefits from the latest AVDF Release

Audit insights for the most common Use Cases



Target: All

View Data for: Last 24 Hours

Targets	Users	Privileged Users	User Entitlement Changes	DDLs	DMLs	Login Failures	Login Successes	Sensitive Objects	Total Events
3	10	3	107	213	585	1	105	0	2088

Lessons Learned

Oracle Audit Vault and Database Firewall is a **Software Appliance**

- *Smooth installation and configuration*
- *Manual configuration at runtime is possible, but you should know what you are doing*
  The less the better...
- *It is crucial that all involved project parties know What AVDF Can and Cannot Do*

Distinction between what is done with DB Audit and what is done with the DB Firewall

- *Certain Information can be collected with audit as well as with firewall policies*

Not too much at **once**

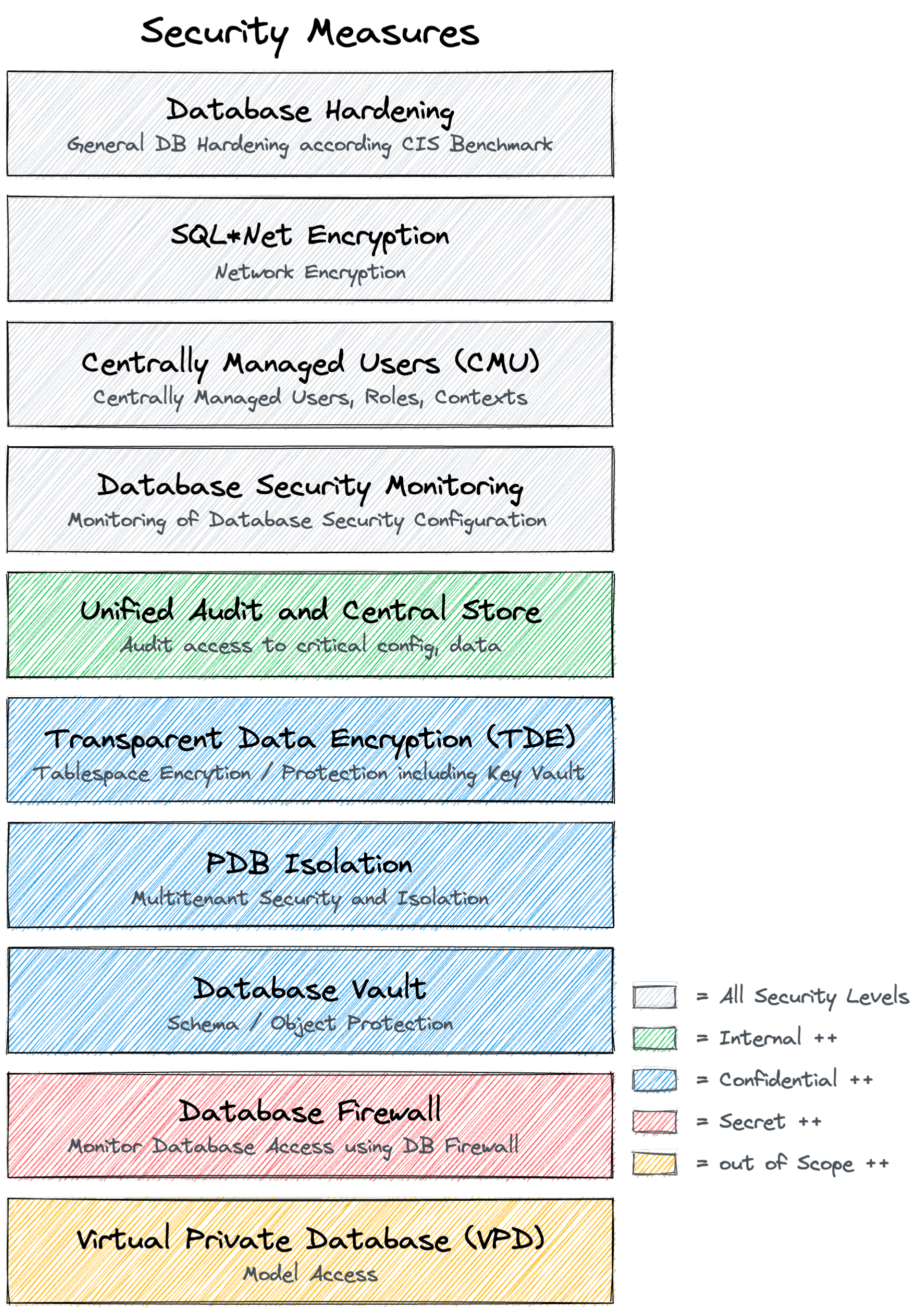
- *It is recommended to work with a solid base. E.g., Solidified implementation of a Security Concept*

Best Practice Considerations

Good and best practice in the implementation of AVDF and security projects

Security Concept before hand

- **Understand Security Measure Objectives**
  Grasp the purpose behind security measures for focused implementation.
- **Classify Database Environments**
  Categorize by sensitivity (internal, confidential, secret) for tailored security.
- **Adapt Security to Classification**
  Align measures with environment sensitivity for efficiency.
- **Layered Security Approach**
  Build multiple layers of defence for robust protection.
- **Structured Implementation**
  Follow a step-by-step process for clear and efficient execution.



Security Measures

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

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

Database Audit

- **Start with Unified Audit:** Choose unified audit over the old database audit for modern, streamline auditing.
- **Plan Holistically:** Create a comprehensive audit strategy aligned with security classifications to cover all aspects effectively.
- **Follow Oracle Best Practices:** Implement Oracle Database Unified Audit using established guidelines for optimal results. Consider using the best practice guidelines from Oracle.
- **Maintain Clarity:** Develop and adhere to a clear audit implementation strategy for efficiency.
- **Gradual Implementation:** Verify and introduce changes incrementally to enhance accuracy and minimize disruption.
- **Allocate Audit Coverage:** Distinguish between database, application audit, and firewall coverage to assign responsibilities effectively.

Blueprint of the Audit Use Cases

Privileged user activity

Administrative database users
i.e. SYSDBA, SYSBACKUP and similar user

Database admin users / roles
roles like DBA or user like SYSTEM

Database user with direct access
e.g. user with direct access from the database server

Individual high risk users / roles
to be specified individually

! We recommend that customer collect there audit records centrally. Either by collecting them directly from the audit trail or by using Kafa Log forwarding

Considerations / Challanges

- OEM access
- Dataguard access
- Direct schema access
- Developer must use proxy connect
- Verify if all actions or dedicated system privileges should be used

Security relevant events

Database logon events
i.e., all failed / successfull logon of any user

Instance configuration
all instance / database configuration changes

Security Configuration
all changes related to security configuration e.g. audit trail

Critical database activity
critical database security events based on CIS recommendation

Account management
all account and privilege related changes

Schema changes
database schema modifications

Datapump export / import
use of DataPump

Directory access in general
access to any database directory object

Considerations / Challanges

- Unused system privileges

Sensitive data access

Access to critical objects
in particular user / application objects

Access to sensitiv columns (FGA)
in particular user / application objects

Access protected objects (DBV)
in particular user / application objects

Access to critical SYS objects
highly critical SYS objects like DBMS_SYS_SQL

Considerations / Challanges

- Management of critical objects
- Application specific policies

Events not audited

General schema owner activity

General application activity

Low privileged user activity

Direct schema access by developer

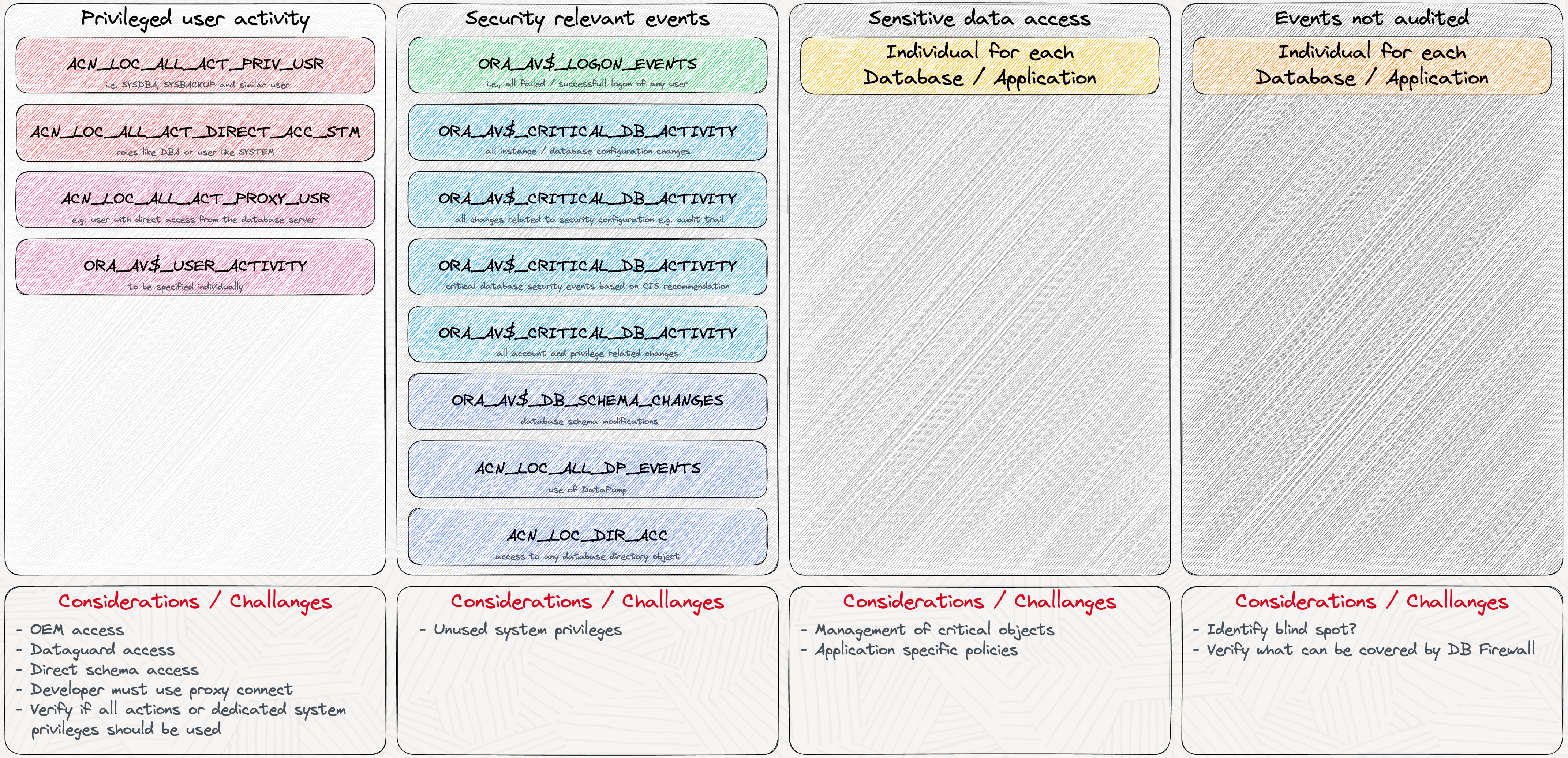
Scheduler events

Java events

Considerations / Challanges

- Identify blind spot?
- Verify what can be covered by DB Firewall

Defined Audit Policies



Privileged user activity

- ACN_LOC_ALL_ACT_PRIV_USR
  i.e. SYSDBA, SYSBACKUP and similar user
- ACN_LOC_ALL_ACT_DIRECT_ACC_STM
  roles like DBA or user like SYSTEM
- ACN_LOC_ALL_ACT_PROXY_USR
  e.g. user with direct access from the database server
- ORA_AV$_USER_ACTIVITY
  to be specified individually

Considerations / Challanges

- OEM access
- Dataguard access
- Direct schema access
- Developer must use proxy connect
- Verify if all actions or dedicated system privileges should be used

Security relevant events

- ORA_AV$_LOGON_EVENTS
  i.e., all failed / successfull logon of any user
- ORA_AV$_CRITICAL_DB_ACTIVITY
  all instance / database configuration changes
- ORA_AV$_CRITICAL_DB_ACTIVITY
  all changes related to security configuration e.g. audit trail
- ORA_AV$_CRITICAL_DB_ACTIVITY
  critical database security events based on CIS recommendation
- ORA_AV$_CRITICAL_DB_ACTIVITY
  all account and privilege related changes
- ORA_AV$_DB_SCHEMA_CHANGES
  database schema modifications
- ACN_LOC_ALL_DP_EVENTS
  use of DataPump
- ACN_LOC_DIR_ACC
  access to any database directory object

Considerations / Challanges

- Unused system privileges

Sensitive data access

Individual for each Database / Application

Considerations / Challanges

- Management of critical objects
- Application specific policies

Events not audited

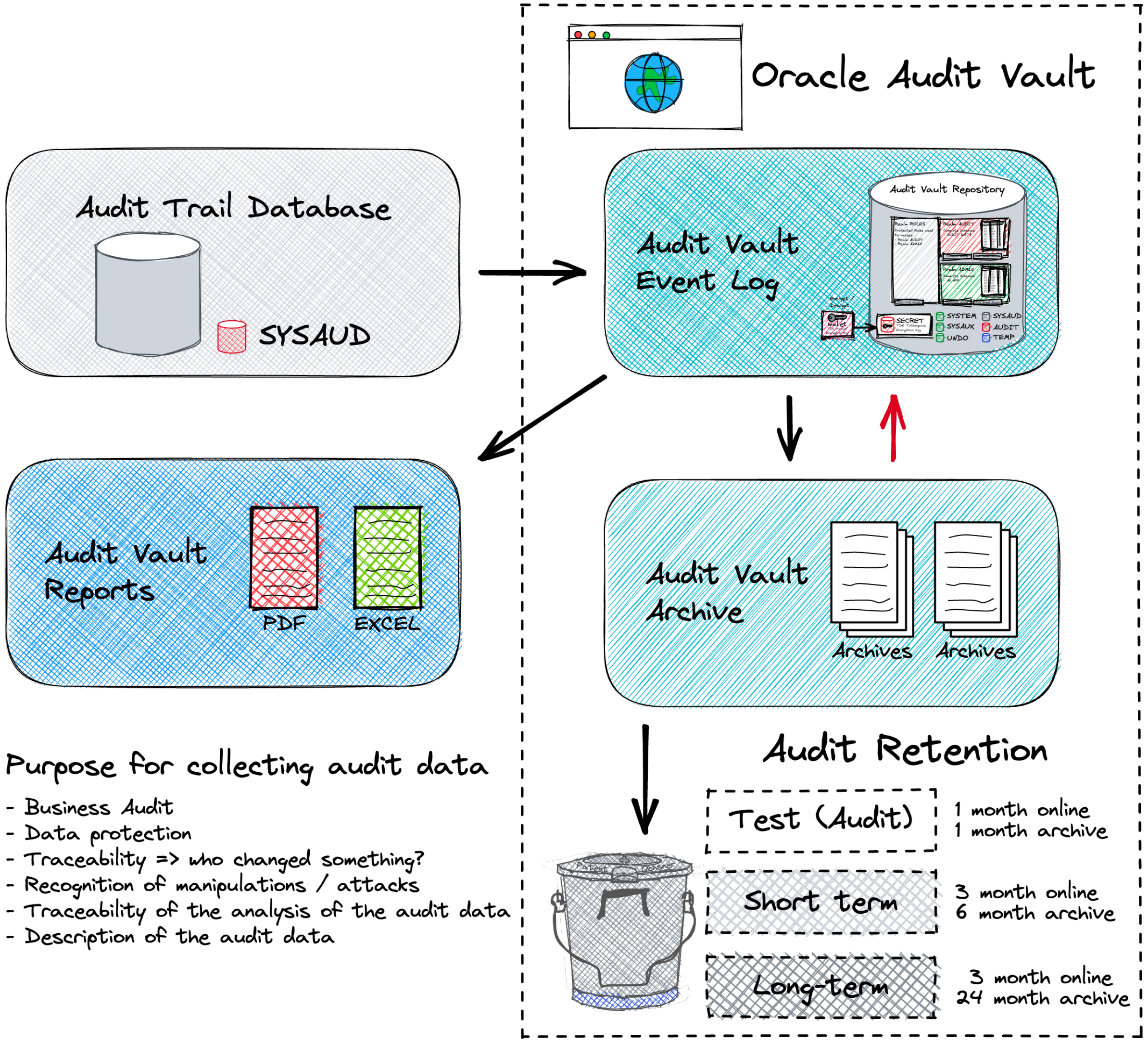
Individual for each Database / Application

Considerations / Challanges

- Identify blind spot?
- Verify what can be covered by DB Firewall

Data Retention

- **Audit Trail:** decentral source of audit data
  Storage requirements on source system, relatively cost intensive, risk of data tampering, no overall analysis
- **Audit Vault Event Log:** central online storage of audit data
  Detailed central audit information, overall analysis, Appliance size sets storage limits
- **Audit Vault Archives:** offline storage of audit data
  Offline archive freeing storage on the Audit Vault server, must be brought back online for analysis
- **Audit Vault Reports:** summarized audit information
  consolidated information, low memory requirements, long-term storage possible



Purpose for collecting audit data

- Business Audit
- Data protection
- Traceability => who changed something?
- Recognition of manipulations / attacks
- Traceability of the analysis of the audit data
- Description of the audit data

Audit Retention

Test (Audit)	1 month online 1 month archive
Short term	3 month online 6 month archive
Long-term	3 month online 24 month archive

Sizing

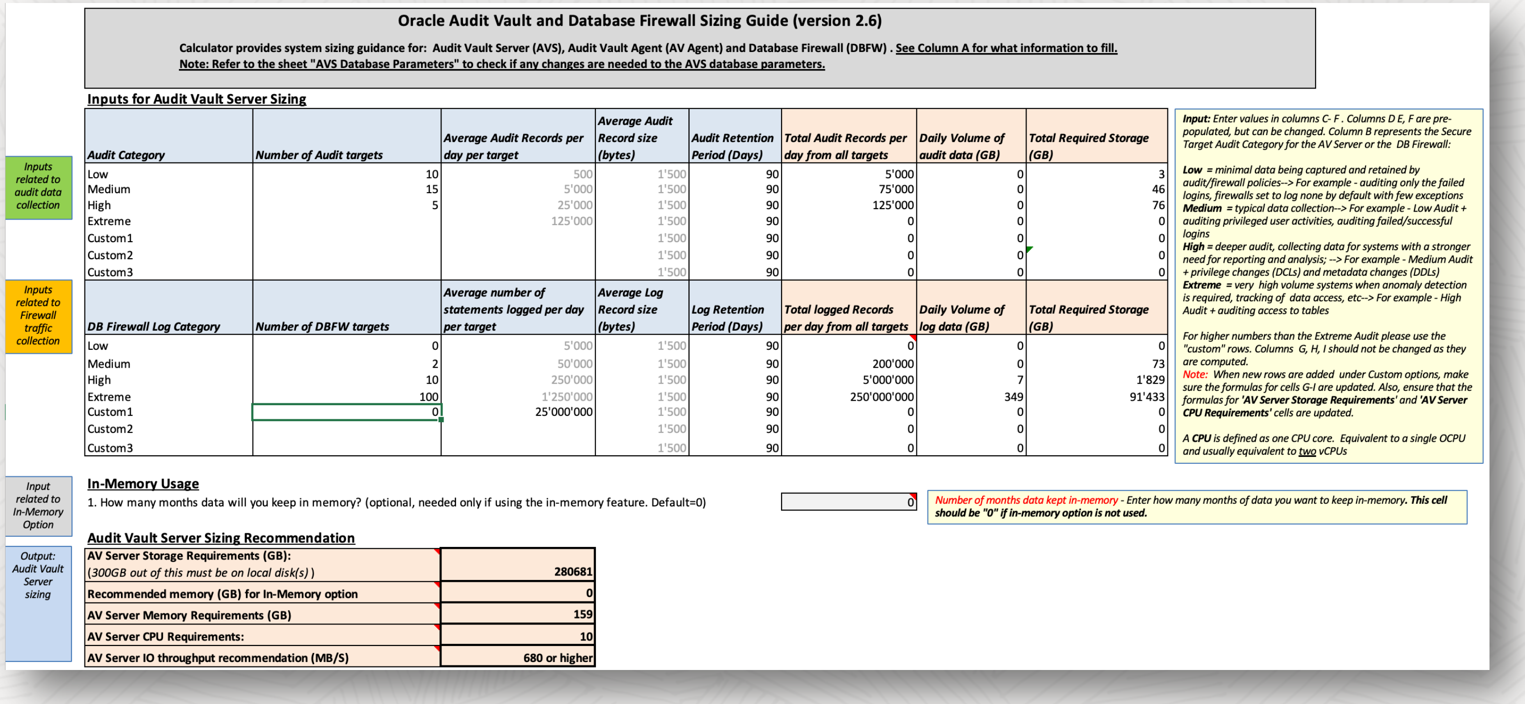
Driver for Audit Vault and Firewall Sizing

Audit Policies / Trails

- Type of audit trails
- Size of audit records
- Number of audit trails

Retention period of the data

- What and how long
- Business and compliance needs
- Oracle Calculation Guideline



Oracle Audit Vault and Database Firewall Sizing Guide (version 2.6)

Calculator provides system sizing guidance for: Audit Vault Server (AVS), Audit Vault Agent (AV Agent) and Database Firewall (DBFW) . See Column A for what information to fill.
Note: Refer to the sheet "AVS Database Parameters" to check if any changes are needed to the AVS database parameters.

Inputs for Audit Vault Server Sizing

Inputs related to audit data collection

Audit Category	*Number of Audit targets*	*Average Audit Records per day per target*	*Average Audit Record size (bytes)*	*Audit Retention Period (Days)*	*Total Audit Records per day from all targets*	*Daily Volume of audit data (GB)*	*Total Required Storage (GB)*
Low	10	500	1'500	90	5'000	0	3
Medium	15	5'000	1'500	90	75'000	0	46
High	5	25'000	1'500	90	125'000	0	76
Extreme		125'000	1'500	90	0	0	0
Custom1			1'500	90	0	0	0
Custom2			1'500	90	0	0	0
Custom3			1'500	90	0	0	0

Inputs related to Firewall traffic collection

DB Firewall Log Category	*Number of DBFW targets*	*Average number of statements logged per day per target*	*Average Log Record size (bytes)*	*Log Retention Period (Days)*	*Total logged Records per day from all targets*	*Daily Volume of log data (GB)*	*Total Required Storage (GB)*
Low	0	5'000	1'500	90	0	0	0
Medium	2	50'000	1'500	90	200'000	0	73
High	10	250'000	1'500	90	5'000'000	7	1'829
Extreme	100	1'250'000	1'500	90	250'000'000	349	91'433
Custom1	0	25'000'000	1'500	90	0	0	0
Custom2			1'500	90	0	0	0
Custom3			1'500	90	0	0	0

***Input:** Enter values in columns C- F . Columns D E, F are pre-populated, but can be changed. Column B represents the Secure Target Audit Category for the AV Server or the DB Firewall:*

***Low** = minimal data being captured and retained by audit/firewall policies--> For example - auditing only the failed logins, firewalls set to log none by default with few exceptions*
***Medium** = typical data collection--> For example - Low Audit + auditing privileged user activities, auditing failed/successful logins*
***High** = deeper audit, collecting data for systems with a stronger need for reporting and analysis; --> For example - Medium Audit + privilege changes (DCLs) and metadata changes (DDLs)*
***Extreme** = very high volume systems when anomaly detection is required, tracking of data access, etc--> For example - High Audit + auditing access to tables*

For higher numbers than the Extreme Audit please use the "custom" rows. Columns G, H, I should not be changed as they are computed.
*Note: When new rows are added under Custom options, make sure the formulas for cells G-I are updated. Also, ensure that the formulas for **'AV Server Storage Requirements'** and **'AV Server CPU Requirements'** cells are updated.*

*A **CPU** is defined as one CPU core. Equivalent to a single OCPU and usually equivalent to two vCPUs*

Input related to In-Memory Option

In-Memory Usage

1. How many months data will you keep in memory? (optional, needed only if using the in-memory feature. Default=0) 0

*Number of months data kept in-memory - Enter how many months of data you want to keep in-memory. **This cell should be "0" if in-memory option is not used.***

Output: Audit Vault Server sizing

Audit Vault Server Sizing Recommendation

AV Server Storage Requirements (GB): *(300GB out of this must be on local disk(s))*	**280681**
Recommended memory (GB) for In-Memory option	**0**
AV Server Memory Requirements (GB)	**159**
AV Server CPU Requirements:	**10**
AV Server IO throughput recommendation (MB/S)	**680 or higher**

Simple **excel spreatsheet** to calculate requirements for *Audit Vault Server*, *Audit Vault Agents*, *Database Firewall* storage, CPU and memory reuirements

Oracle Support Document 2092683.1

Summary of What to Consider

- **Prioritize finalizing your Audit configuration before hand**
  At least a rough and verified idea of it. Otherwise, you run the risk of fighting several fires at the same time.

- **Choose wisely where to store data and for how long**
  The retention period of audit data determines storage needs

- **Is it necessary to keep all components high available?**
  Prioritize high availability for key Oracle Audit components to maintain data integrity, security, and compliance. Factor in classification and security needs

- **Use AVDF functionality during deployment / engineering**
  e.g., discover sensitive data, privileged users, DB Sec assessment…

- **The main challenge is still the security concept of the databases**
  Inadequate Role and Privilege settings can lead to too much data.

Wrap up and Next Steps

How to get most out of AVDF

Next Steps

Visit Database Security Demo pod

DEM008

AVDF Blogs

Read AVDF blogs here

Try out yourself

If you want to try out these features, visit the **LiveLabs guided workshop**

AVDF Forum

Category: On-Premises Infrastructure: Database Software

Tag: database-security audit-vault-database-firewall

Customer adoption program

Worldwide program to ensure customers deploy AVDF with their implementation partners successfully

AVDF Café

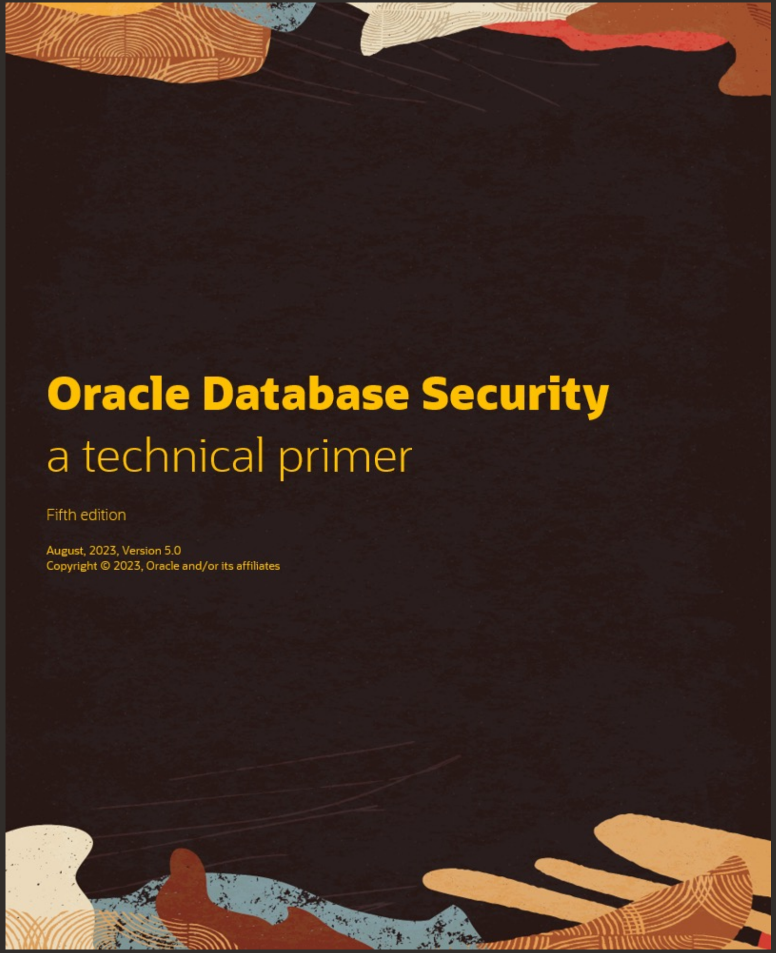
Quarterly series for customers, prospects, and partners to learn something new about AVDF in every session. Every session runs in 3 different time zones

Updated Database Security eBook

The fifth edition of our database security primer includes:

- Managing SQL Injection risk with Database 23c's SQL Firewall
- Latest updates for Data Safe
- Database security posture management with Audit Vault and Database Firewall
- Preparing your databases for ransomware attacks
- Removing security and regulatory risk from test and development databases

And much more!



Oracle Database Security

a technical primer

Fifth edition

August, 2023, Version 5.0
Copyright © 2023, Oracle and/or its affiliates

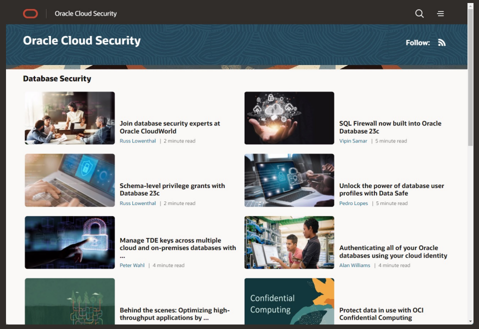
Helping you keep up

Monthly office hours

Ask Tom
Database Security

Second Wednesday of each month at
10:00 am US Central

Database security blog



Oracle Cloud Security

Oracle Cloud Security

Follow:

Database Security

Join database security experts at Oracle CloudWorld
Russ Lowenthal | 2 minute read

SQL Firewall now built into Oracle Database 23c
Vipin Samar | 5 minute read

Schema-level privilege grants with Database 23c
Russ Lowenthal | 2 minute read

Unlock the power of database user profiles with Data Safe
Pedro Lopes | 5 minute read

Manage TDE keys across multiple cloud and on-premises databases with ...
Peter Wahl | 4 minute read

Authenticating all of your Oracle databases using your cloud identity
Alan Williams | 4 minute read

Behind the scenes: Optimizing high-throughput applications by ...

Confidential Computing

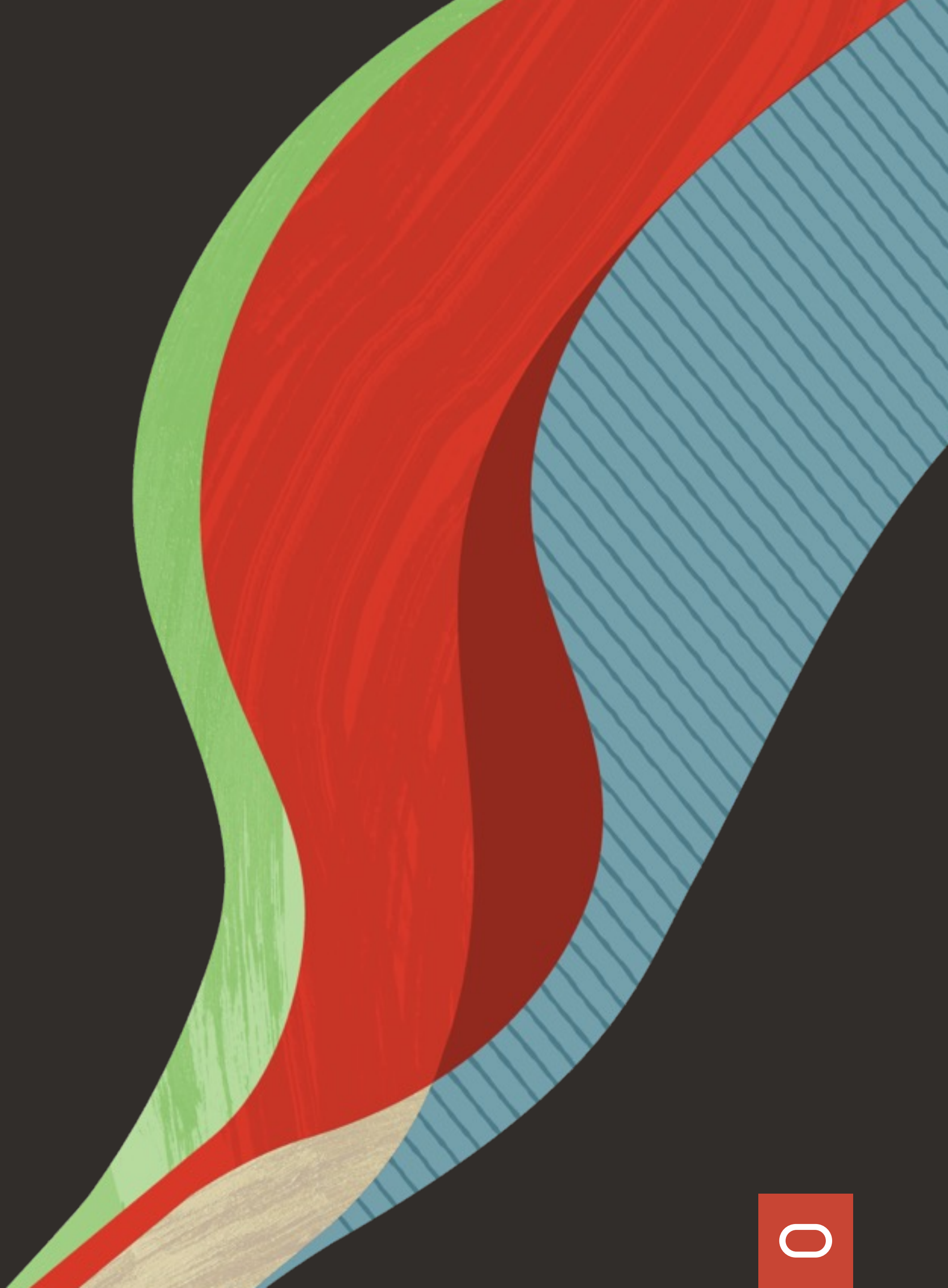
Protect data in use with OCI Confidential Computing

Documentation and support notes

Oracle LiveLabs – your database security playground

Session Survey

Session ID: LRN1646



Want to talk more about Database Security?

Protecting the Crown Jewels
The state of Database Security
– Vipin Samar, SVP Database Security

Wednesday, 8:30 am in Ballroom G (level 2)

Session ID: LRN1643

ORACLE
DatabaseWorld

Thank you

ORACLE