Administration and Operation of Hardened Databases

Best Practices and Operational Challenges in Securing Database Environments

Stefan Oehrli

Stefan Oehrli – Modern Data Platforms

Modern Data Platforms

stefan.oehrli@accenture.com

SYM42

Oracle ACE Director

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)

oradba.ch

@stefanoehrli

Oracle ACE

The Oracle ACE Program

400+ 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 levels: Director, Pro, and Associate
- Nominate yourself or a colleague at ace.oracle.com/nominate
- Learn more at ace.oracle.com

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

Accenture’s Oracle Expertise and Partnership
Proven leader, focused on customer success

Highlights presented at our booth:

- The Power of AI
- Journey to Multicloud
- OCI and FinOps
- Oracle Apex
- Oracle Applications

Agenda

Key Topics for Securing and Operating Hardened Databases

1. Intro to Hardened Database Ops
2. Core Security & Hardening
3. Encryption & Data Protection
4. Segregation of Duties
5. Monitoring & Auditing
6. Performance Tuning
7. Best Practices & Key Takeaways

1

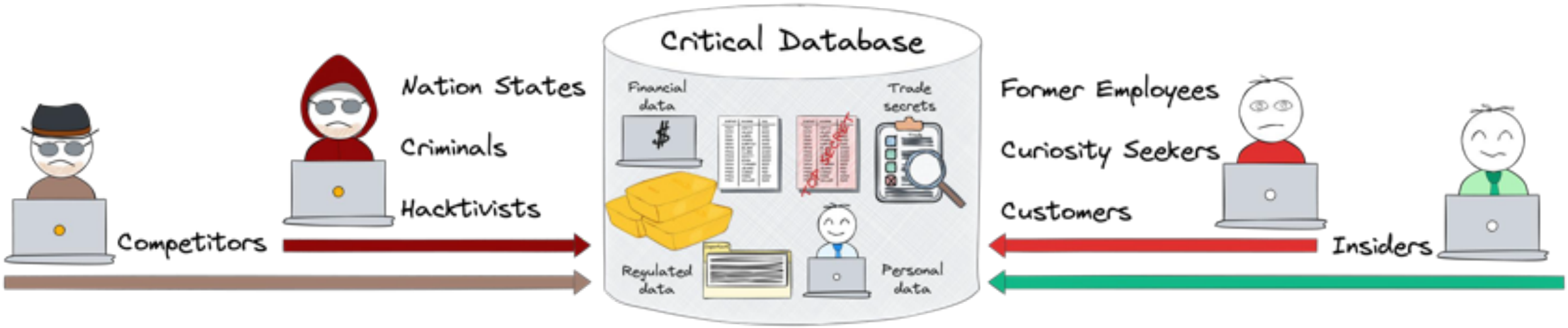
Intro to Hardened Database Ops

Balancing Security and Efficiency in Database Administration

Data: The Crown Jewel of Your Organization

Protecting Data to Prevent Liability

- **Data is a Key Asset**: While data holds immense value, it can quickly turn into a major liability if not adequately protected.
- **Rising Cybercrime:** Cybercrime is expected to cause $8 trillion in global damages in 2023, with databases being prime targets due to their concentration of valuable information.
- **Increasing Regulations:** New and expanding data protection laws demand stricter security and accountability.



External and Internal Database Threats

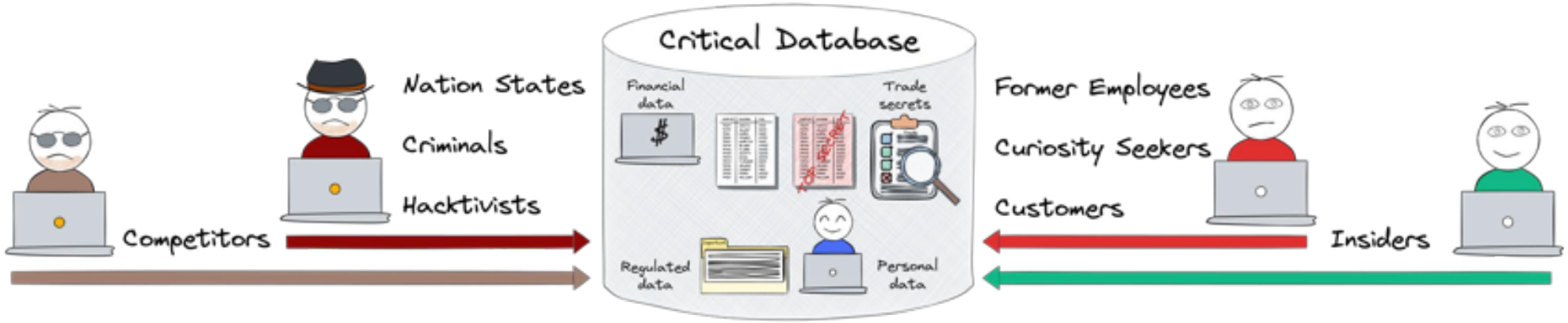
Understanding the Diverse Threat Landscape

External Threats

- **Cyber Attacks:** SQL injection, ransomware, and privilege escalation.
- **Data Exfiltration**: Theft of sensitive data (e.g., customer information, intellectual property).
- **Advanced Persistent Threats (APTs)**: Long-term, stealthy attacks often backed by state actors.

Internal Threats

- **Insider Threats**: Misuse of access by employees or contractors.
- **Privilege Abuse**: Over-privileged accounts accessing restricted data.
- **Human Error**: Weak passwords, misconfigurations, and delayed updates.

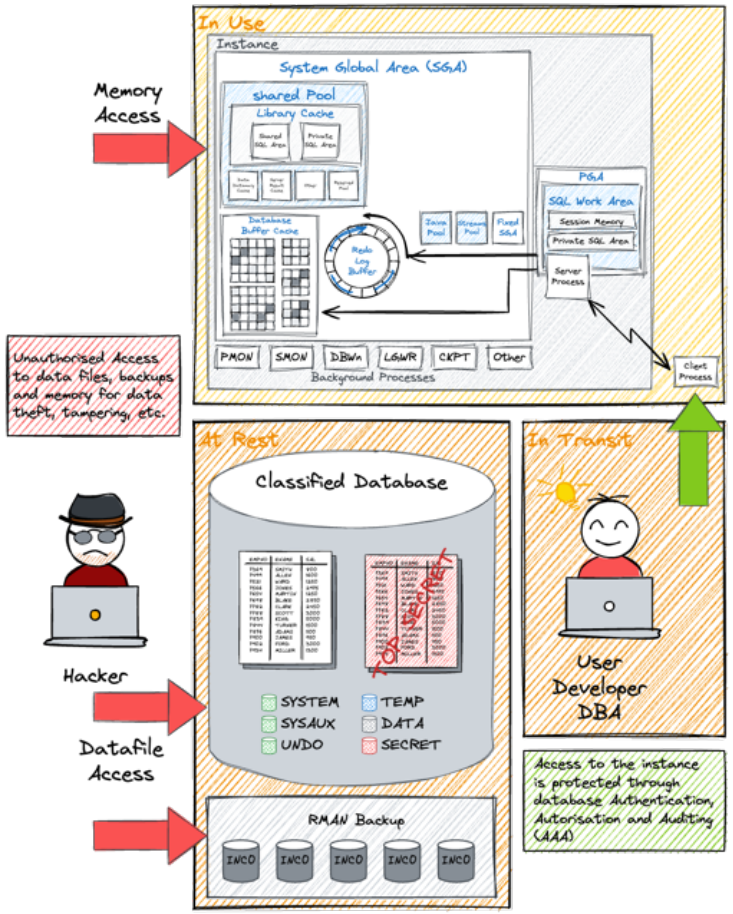


*Threats can come from both outside and within. A comprehensive approach addresses both external attacks **and** internal vulnerabilities.*

Top 12 Database Security Risks

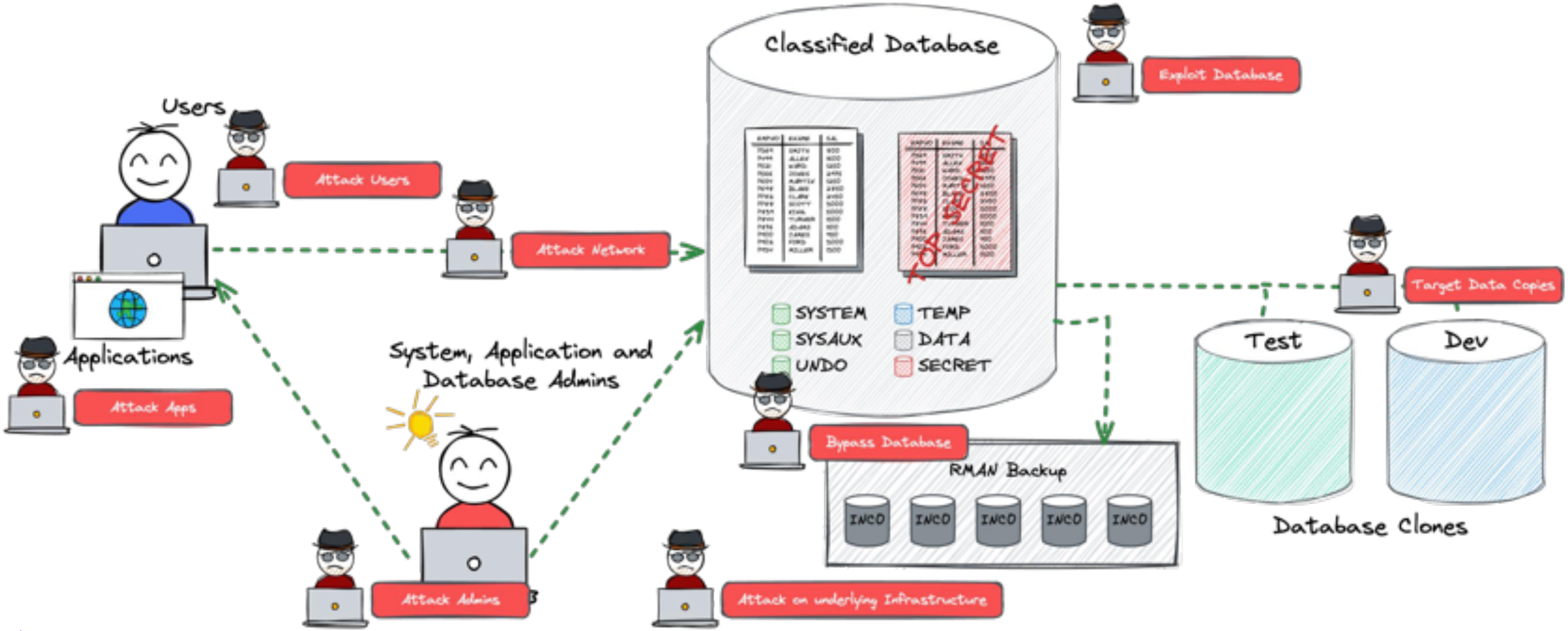
The dirty dozen…

- **Access Bypass:** Exploiting unpatched vulnerabilities.
- **Privilege Abuse:** Using excessive privileges to access restricted data.
- **Sensitive Data Search**: In unprotected systems and databases.
- **Credential Theft:** Obtained via phishing 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.



Common Database Attack Vectors

Understanding Key Points of Entry for Potential Threats



Key Elements of Oracle's Security Architecture

Layers, Security Tiers, and Focus on Essentials

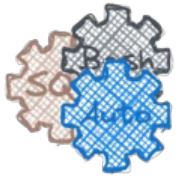
Layered Defense Approach

- Oracle's architecture employs a multi-layered strategy that combines different security layers to create comprehensive protection.

Prevention and Control Measures

- Security features are categorized into preventive measures (e.g., encryption, authentication) and control measures (e.g., auditing, user management).

Security vs. Operation



Scalable Architecture

- This security setup is adaptable, allowing organizations to implement basic layers first and add advanced features as needed.

Keeping the Balance

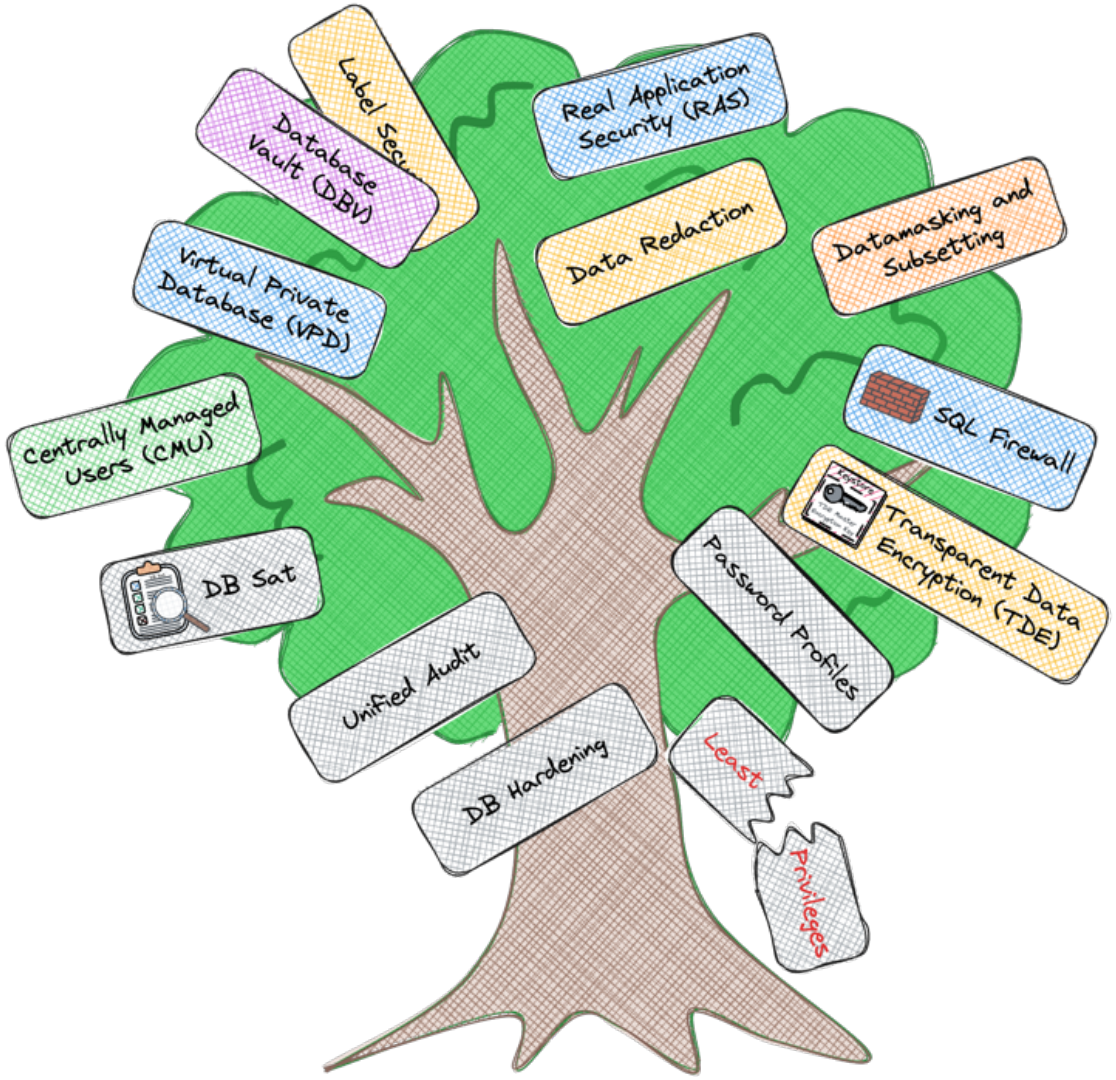
2

Core Security & Hardening

Foundational Steps for a Secure Oracle Database

Core Security and Hardening

Building a Strong Foundation for Database Security



Follow Security Standards

- Implement best practices such as *CIS Benchmarks* to ensure consistent and reliable database hardening.

Identify and Strengthen Weak Links

- Security is only as strong as its weakest link—address overlooked areas such as misconfigurations and unused features.

Focus on Essentials:

- Prioritize simple, impactful measures.
- Examples: Enable password policies, configure network encryption, and implement unified auditing.

Foundation for Advanced Measures

- Basic hardening lays the groundwork for implementing more sophisticated security solutions, such as TDE and Database Vault.

Balancing Security and Usability

Practical Trade-offs in Database Hardening

Security Goals:

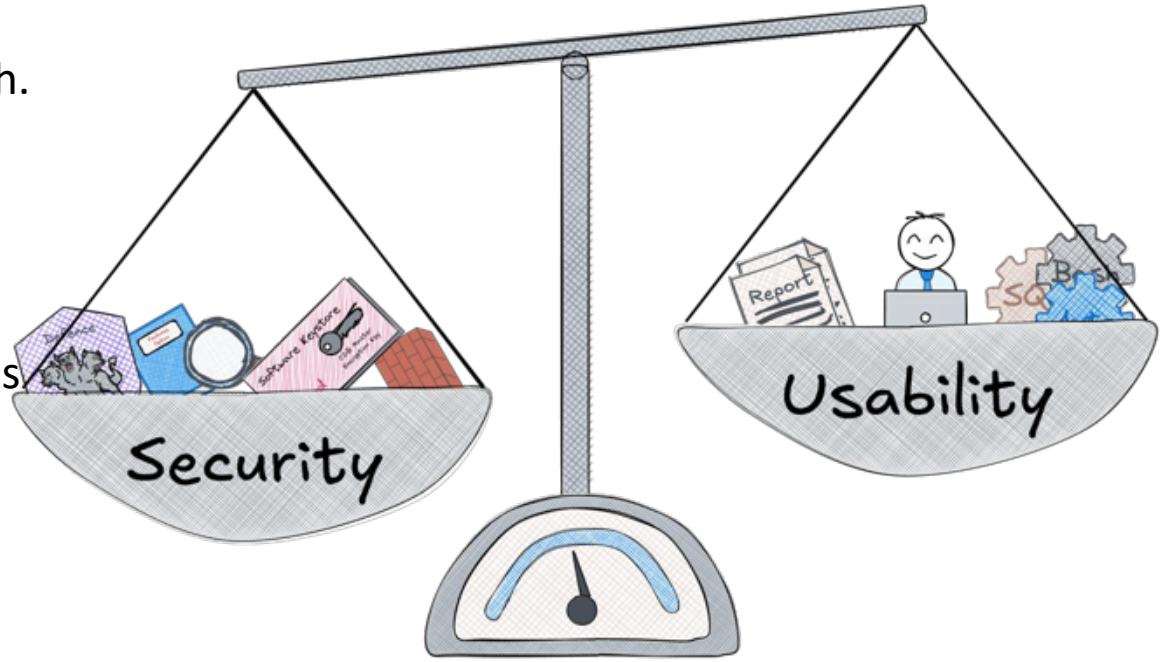
- Apply CIS recommendations (e.g., revoke grants to PUBLIC).
- Disable unused features to reduce attack surfaces.

Operational Conflicts:

- Revoking PUBLIC grants may disrupt operations like datapatch.
- Strict configurations can increase complexity.

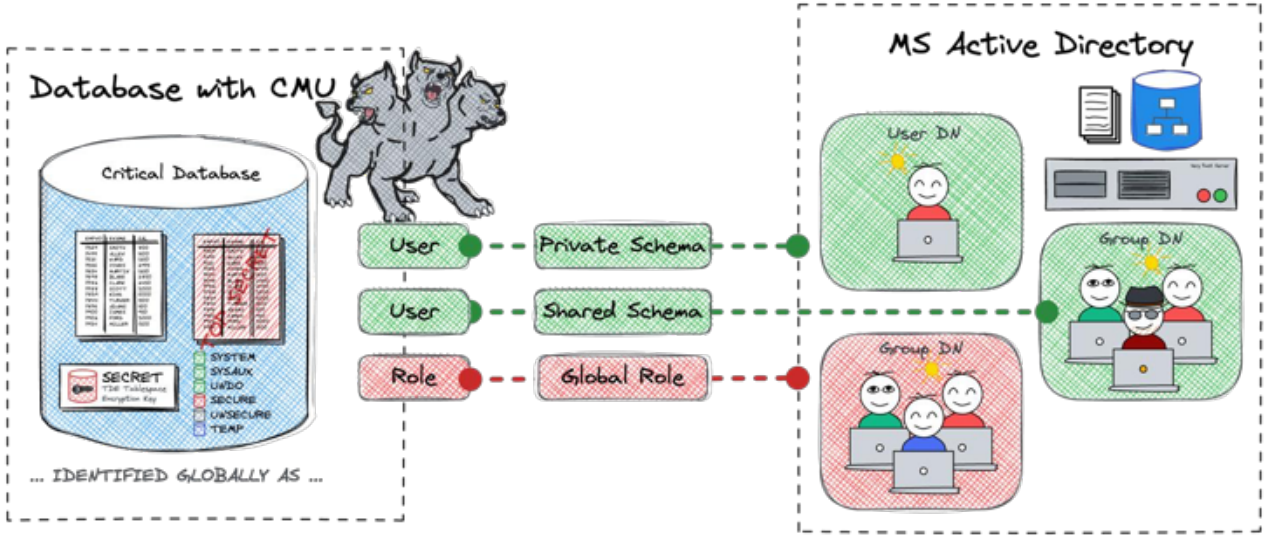
Finding Balance:

- Prioritize impactful measures (e.g., TDE, auditing).
- Adjust strict settings where necessary (e.g., re-grant privileges for patching).



Secure Authentication, CMU and others

Enhancing Security with Centralized Authentication and Strong Verifiers



Strong Password Verifiers

- Set `ALLOWED_LOGON_VERSION_SERVER` to 12a to enforce strong password hashes.

Advanced Authentication Options

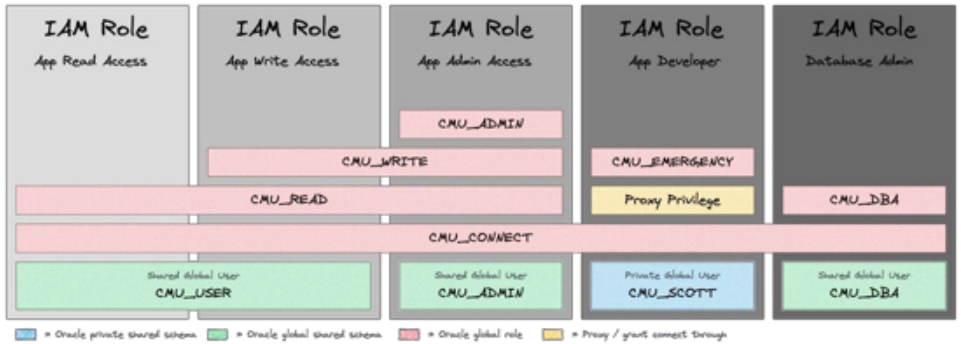
- Implement SSL or Kerberos authentication for secure, certificate-based login.

Centrally Managed Users (CMU)

- Use CMU for centralized authentication and authorization across databases.
- Supports both user and group Distinguished Names (DN) for streamlined management.

Users, Roles and Privileged Access

Structuring Roles with Least Privilege and Role Consolidation



Define User Groups and Consolidated Roles

- Group database roles into functional roles (e.g., combine **APP_READ** and **APP_WRITE** into **APP_CLERK**) for streamlined management.
- Create roles based on function (e.g., **APP_CLERK**, **APP_DEVELOPER**).

Apply Principle of Least Privilege

- Grant only necessary **READ** or **EXECUTE** privileges based on role requirements.
- Consider using rather **READ** than **SELECT** privileges.

Utilize Proxy Functionality

- Implement proxy access for secure delegation and indirect access where needed.

Collaborate with Application Owners

- Define roles with application owners to meet user and developer needs.

Refine Roles with Privilege Capture

- Analyse actual usage to fine-tune privileges.

Managing Privileged Access: SYSDBA and Beyond

Assigning Admin Roles for Enhanced Control

Limit SYSDBA Usage

- Avoid running all tasks as SYSDBA to track activities more effectively.

Apply Least Privilege

- Grant only necessary privileges to each role.

Use Specialized Admin Roles

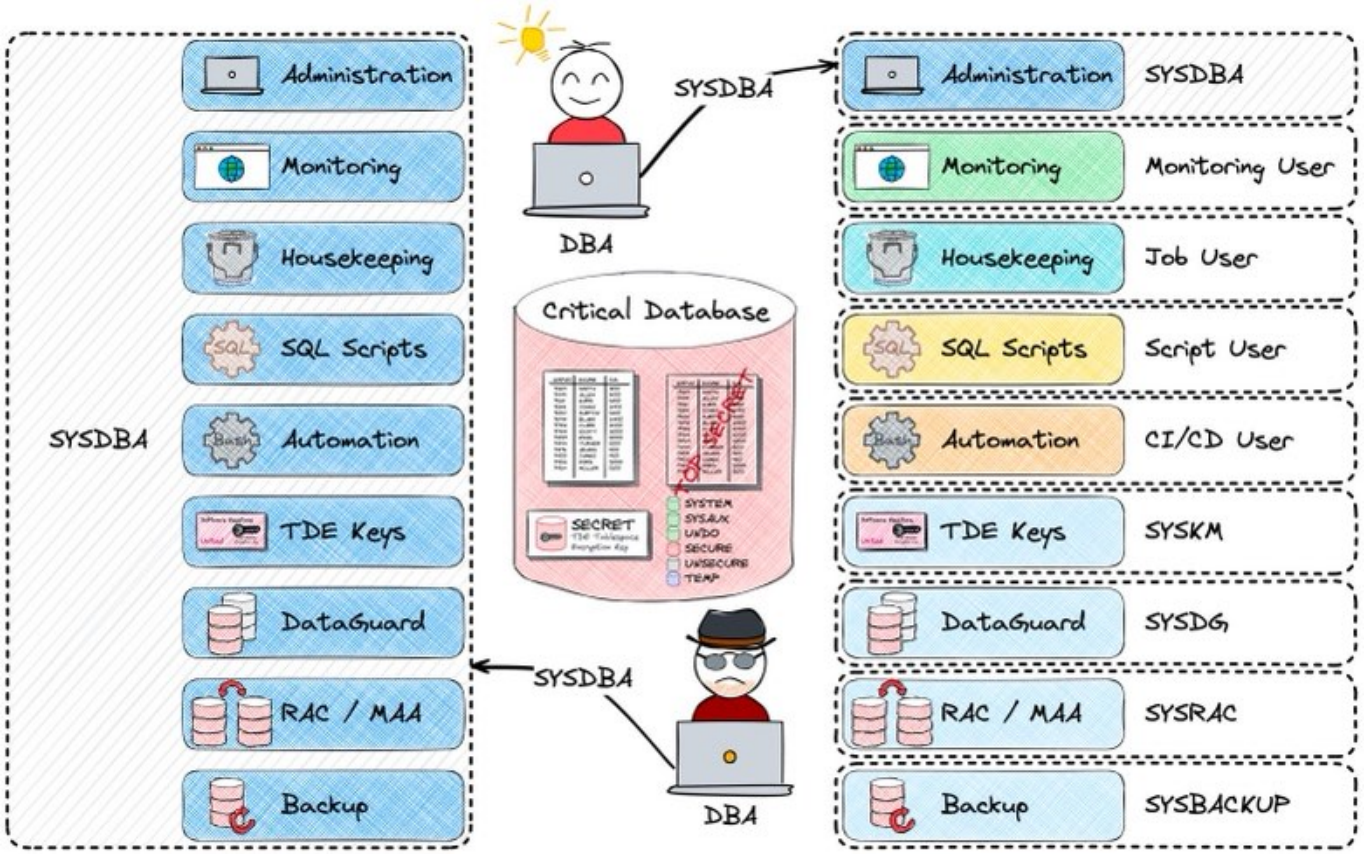
- Assign roles like **SYSDG**, **SYSBACKUP**, and **SYSRAC** for specific tasks.

Create Dedicated Operational Accounts

- Monitoring User for health checks.
- Job/Batch User for automated tasks.

Leverage Privilege Capture

- Analyse actual usage to align privileges with real needs.



The Importance of Regular Patching

Staying Ahead with Up-to-Date Systems

Stay Updated Regularly

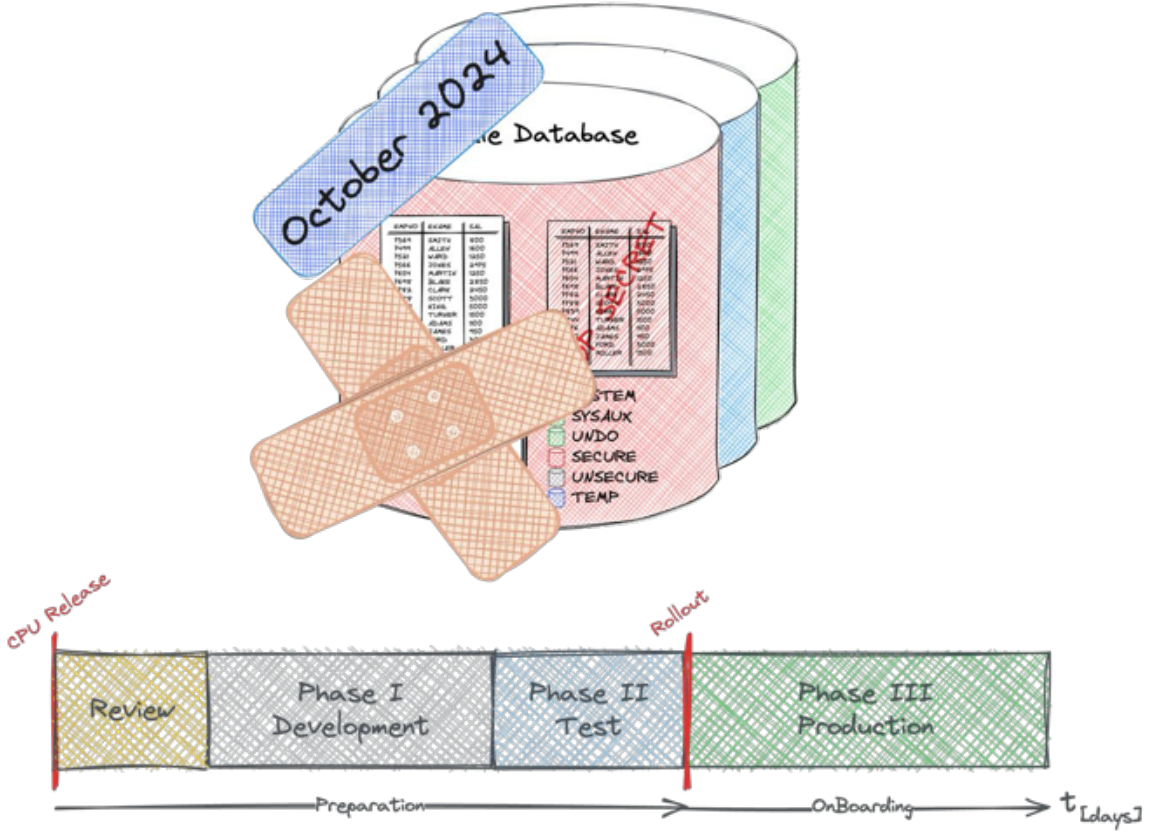
- Apply patches frequently to protect against known vulnerabilities.
- Long gaps between patches increase security risks and operational challenges.

Automate Where Possible

- Use automation tools to streamline patch application.
- Reduce human errors and minimize downtime.

Avoid Infrequent Updates

- One or two patch cycles per year are insufficient for secure systems.
- Frequent updates ensure compatibility and reduce the risk of cumulative issues.

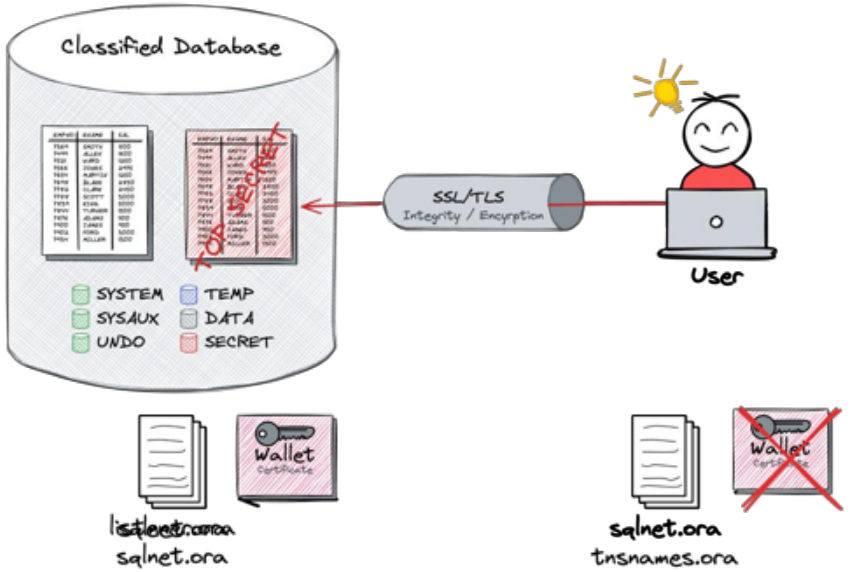


3

Encryption & Data Protection

Foundational Steps for a Secure Oracle Database

Network Encryption



Protecting Data in Transit

Native Oracle Net Encryption

- Configured through `sqlnet.ora` for straightforward, secure communication over standard Oracle Net (TCP) ports.
- Ideal for environments that need simpler setup without certificates.

SSL/TLS for Secure Connections

- Provides encrypted network traffic between applications and databases.
- Requires certificates and a dedicated port configuration.

Start Simple with Native Encryption

- Begin with Oracle Net encryption, then consider SSL/TLS for higher security needs.

Best Practices

- Configure network encryption as part of the overall security framework.

TDE (Transparent Data Encryption)

Prioritizing Tablespace Encryption for Comprehensive Data Security

TDE Column Encryption (Selective Use)

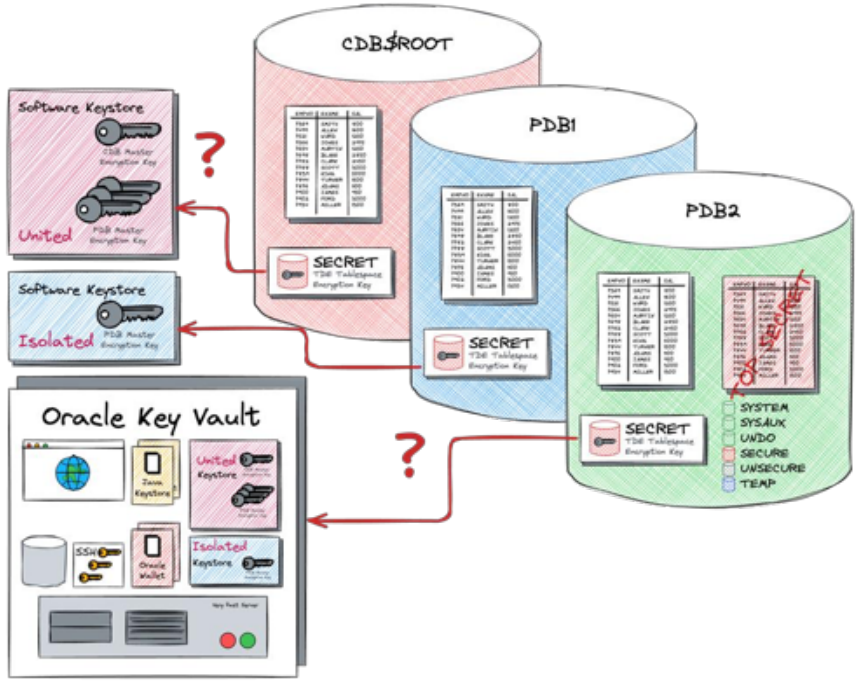
- Encrypts specific columns within tables.
- May impact the data model and has data type limitations.
- Master key stored in a wallet; keys stored in the data dictionary.
- Effects on storage 1-52Byte per value

TDE Tablespace Encryption

- Encrypts entire tablespaces or databases transparently.
- No changes required to the data model (foreign keys, indexes).
- Master key stored securely in a wallet.
- Supports online and offline encryption and rekeying operations.

Oracle Key Vault

- Centralized storage for encryption keys and credentials
- Strengthens Oracle database security and simplifies key management



Keystore Management

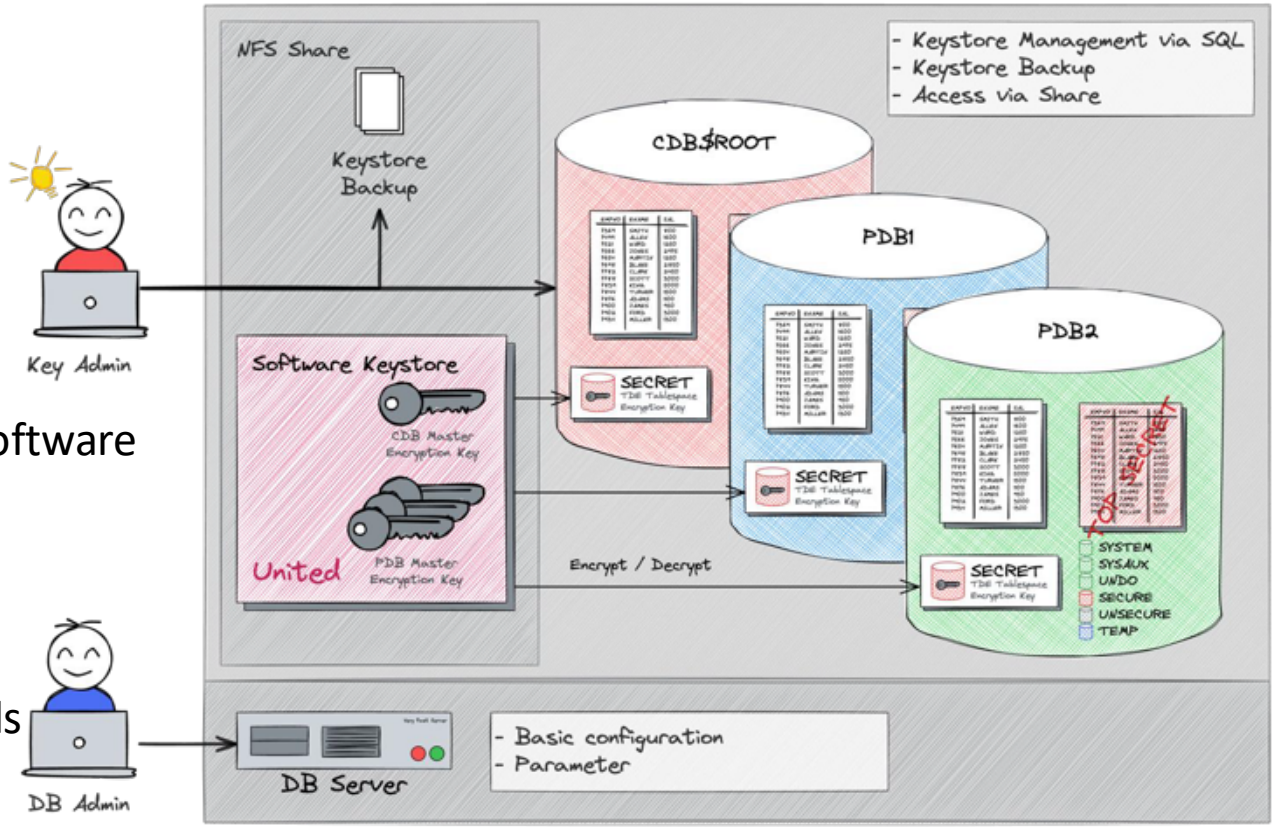
Rules and Responsibilities for Keystore Management

DB Admin

- Initial setup of the infrastructure i.e., *init.ora* parameter like, TDE_CONFIGURATION, ENCRYPT_NEW_TABLESPACES, WALLET_ROOT
- Provide a common user / privileges for maintaining the software Keystore using *ADMINISTER KEY MANAGEMENT*
- ”Use” the auto login local keystore

App Owner / Security Operation

- Create the software Keystore and maintain any credentials
- Create / maintain master encryption key
- Create backup of software keystore



Database Operations with TDE

Adapting Administration Tasks for Enhanced Security

Operation	Keystore Required	DBA Task	Keystore Admin	Notes
Startup Database	Yes	Yes (with auto-login)	No	Auto-login simplifies operations; password required if not configured.
Backup & Restore	Yes	Yes (with auto-login)	No	Keystore must be open to encrypt backup files.
Create/Alter Tablespaces	Yes	Yes (with auto-login))	No	Required for encrypted tablespaces; auto-login recommended.
Database Cloning	Yes	No	Yes	Requires keystore password and configuration on target system.
Rekey Master Key	Yes	No	Yes	Only the keystore admin can perform master key rekeying.
Data Pump Export/Import	Yes	Yes (with auto-login)	No	Keystore must be open for encrypted data export/import.
Table/Index Maintenance	Yes	Yes (with auto-login)	No	Applies to encrypted data; auto-login reduces manual intervention.
Database Upgrade	Yes	Yes (with auto-login)	No	Required for encrypted data integrity during upgrade processes.

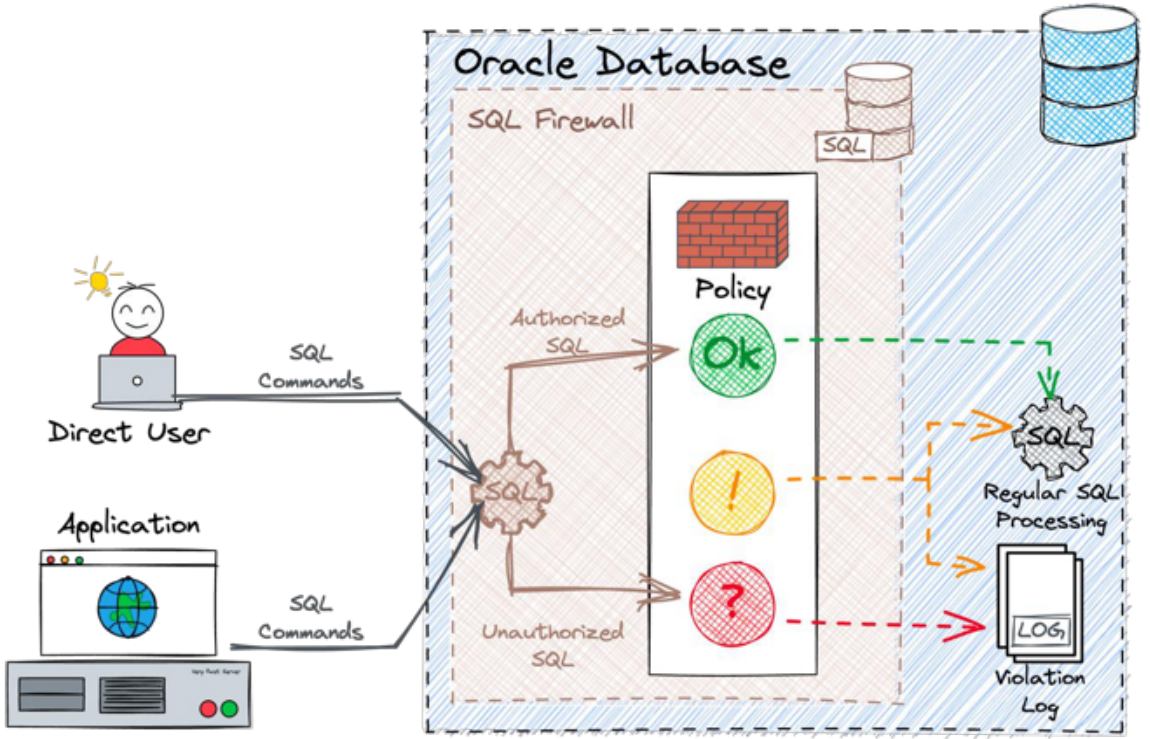
4

Segregation of Duties

Enforcing Segregation of Duties with Database Vault and SQL Firewall

SQL Firewall Overview

Real-Time SQL Protection and Access Control



Real-Time Protection

- Blocks unauthorized SQL to prevent SQL injection and access anomalies.

Customizable Allow-Lists

- Define specific SQL permissions for users; log unusual activities.

Connection and Statement Control

- Control allowed SQL statements and connection paths (IP addresses, context).

Integrated with Oracle Database

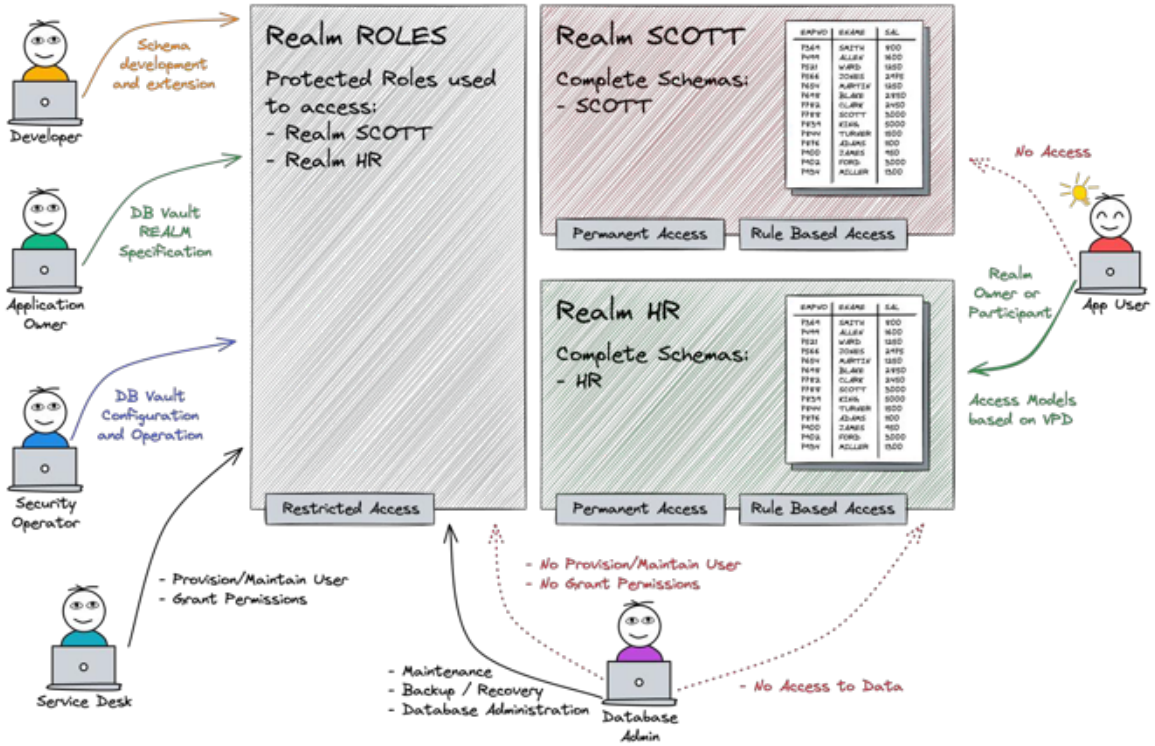
- Inspects all SQL activity, including encrypted and network traffic.

Flexible Policy Application

- Apply tailored policies for different database accounts to enhance security.

Oracle Database Vault

Enhanced Access Control and Separation of Duties



Privileged Account Control

- Restricts high-privilege access with defined realms.

Configuration Protection

- Secures critical settings, enforcing separation of duties.

Separation of Duty

- Role-based access for routine DB tasks.

Seamless Integration

- Minimal impact on daily operations; implemented via binary change.

Realm-Based Security

- Protects grouped data (schemas, roles) within realms; setup required post-activation.

Enhanced Access Policies

- Supports rules (e.g., four-eyes principle) for sensitive actions.

Database Vault Administration Use Cases

Practical Scenarios for Implementing and Managing Database Vault

Administration Task	Oracle Database Vault operational controls required?	Comments
Starting up and shutting down the database	No	
Managing database initialization parameters	Yes	Some parameters are protected by the ALTER SYSTEM command rule.
Managing users and roles	Yes	
Oracle Data Pump	Yes	Proper Oracle Database Vault authorization should be granted before doing this task.
EXPLAIN PLAN	Yes	PLAN_TABLE should be accessible to DBA.

Database Vault Administration Use Cases

Practical Scenarios for Implementing and Managing Database Vault

Administration Task	Oracle Database Vault operational controls required?	Comments
Performing database patching	Yes	
Performing software upgrade	No	Performed by the App Owner
Performing database upgrade	Yes	
Oracle RMAN	no	
Flashback	Yes	Proper Oracle Database Vault authorization must be granted before doing this task.

Estimate Operational overhead

Assessing the Impact of Database Vault on Daily Operations

Activity	Who	Efforts (FTE)						
		Initial			Anuall			Quarterly
		Estimate	Factor	Total	Estimate	Factor	Total	
Database Vault Concept	Application Owner	3	1	3			0	0
Database Vault Concept	Database Admin	4	1	4			0	0
Database Vault Introduction	Application Owner	1	1	1			0	0
Database Vault Training	Database Admin	2	1	2			0	0
Adapt the operating processes	Database Admin	15	1	15			0	0
Adapt the development processes	Application Owner	5	1	5			0	0
Database Vault Initial Setup	Database Admin	2	1	2			0	0
Database Vault Initial Realm Configuration	Application Owner	2	1	2			0	0
Database TDE	Database Admin	2	1	2	2	1	2	0.5
Database Patching	Database Admin	5	1	5	4	1	4	1
Database Upgrade	Database Admin			0	5	1	5	1.25
Database Upgrade	Application Owner			0	5	1	5	1.25
Application Update / Patching	Application Owner			0	2	1	2	0.5
Onboard MyAccess	Application Owner	2	1	2			0	0
Onboard MyAccess	Database Admin	2	1	2			0	0
MyAccess Workflows	Identity and Access Management			0				
User / Role Management	Database Admin	4	1	4	1	1	1	0.25
Performance Tuning	Database Admin			0	4	1	4	1
Enhanced Troubleshooting	Database Admin			0	4	1	4	1
Database Vault Audit Configuration	Database Admin	5	1	5			0	0
Monitoring	Operation	5	1	5			0	0
Security Monitoring	Not assigned	10	1	10	1	1	1	0.25

Estimate Operational overhead

Assessing the Impact of Database Vault on Daily Operations

Who	Initial	Anuall	
Application Owner	13	7	FTE
Database Admin	41	20	FTE
Identity and Access Management	0	0	FTE
Operation	5	0	FTE
Not assigned	10	1	FTE
Summary (one stage)	69	28	FTE

5

Monitoring & Assessment

Tools and Techniques for Continuous Security Evaluation

Proactive Security and Monitoring

Staying Ahead of Threats with Continuous Oversight

Why Proactive Security?

- Prevent vulnerabilities instead of reacting to breaches.
- Regular assessments mitigate risks and strengthen defenses.

Key Components

- **Automated Monitoring:** Tools like AWR and Performance Hub for real-time insights.
- **Regular Assessments:** Use DBSAT, Data Safe, and audit reports to identify weak points.
- **Config Review:** Ensure policies, user privileges, and security settings remain up to date.

Best Practices

- Establish a schedule for monitoring and security checks.
- Automate where possible to minimize manual intervention.
- Use dashboards and alerts to stay informed on security posture.

Unified Audit

Centralized and Flexible Auditing with Standard Audit Policies

Standard Audit Policies

- Predefined policies for common audit needs (not enabled by default).
- Regularly updated with new releases. Examples:
  - ORA_ACCOUNT_MGMT: Monitors account changes.
  - ORA_CIS_RECOMMENDATIONS: Aligns with CIS benchmarks.

```
SELECT policy_name FROM audit_unified_policies
WHERE oracle_supplied='YES' GROUP BY policy_name;
```

Best Practices and Guidance

- Refer to Oracle Database Unified Audit - Best Practice Guidelines.
- Detailed recommendations for plain databases, Data Safe, and AVDF.

Best Practice Use guidelines to develop tailored audit policies for specific needs.

Unified Audit Use Cases

Practical Applications for Security and Compliance

Unified Audit Use Cases

Practical Applications for Security and Compliance

Mandatory Audit Retention

Ensuring Compliance and Data Availability

Define Retention Policies

- Set clear retention periods for audit records to meet compliance requirements.

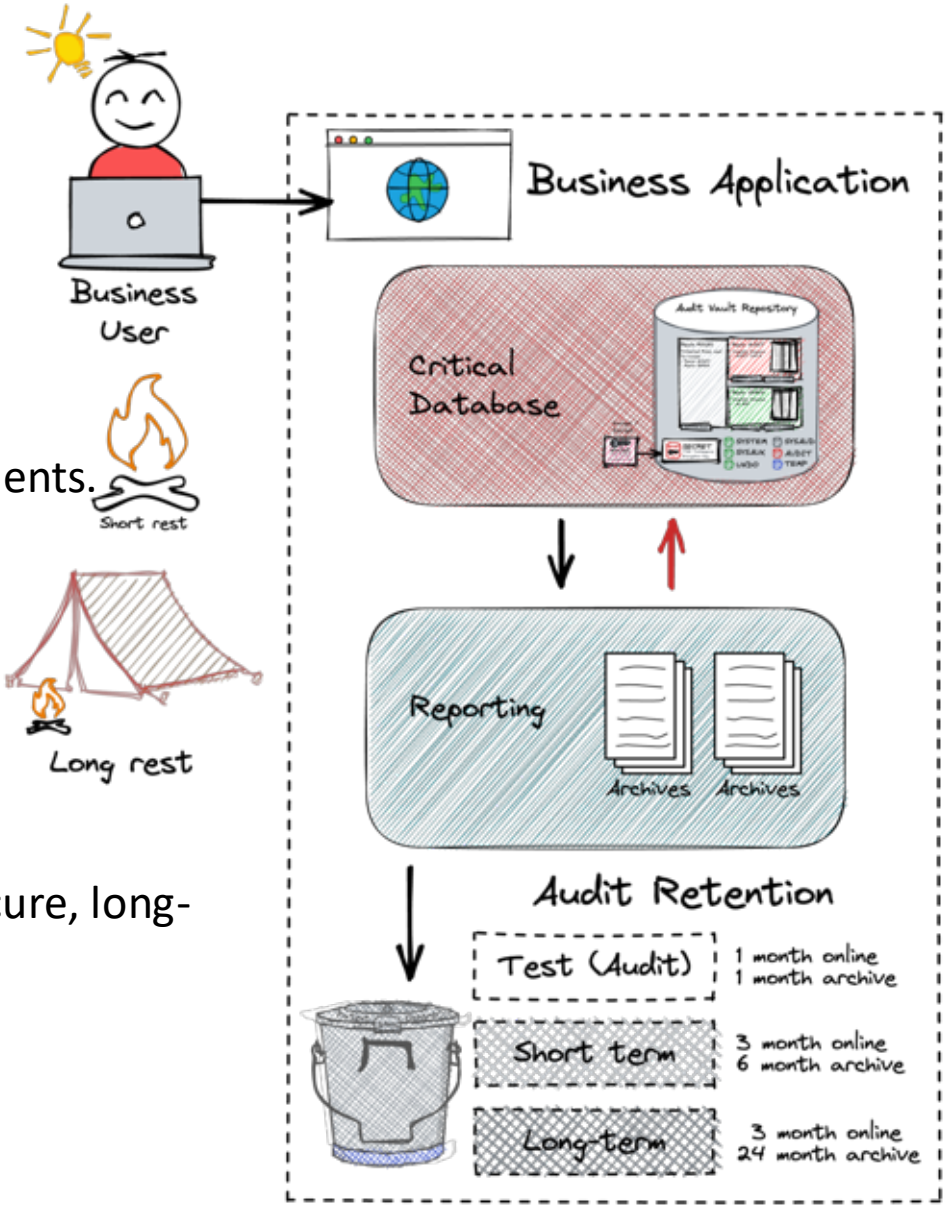
Centralize Audit Data Storage

- Store audit data in a secure, centralized repository for easy access and management.

Long-Term and Short-Term Storage

- **Short-Term Storage:** Retain audit logs locally for operational purposes.
- **Long-Term Storage:** Archive essential audit records for compliance in a secure, long-term location.

Consider **central storage** and **automatic housekeeping** of Audit Data



Database Security Assessment Tool (DBSat)

Latest Release Ready for Oracle 23c – Version 3.1.0 April 2024

STIG V2R8 compliance

- includes 30 new STIG findings and revised STIG group IDs

Enhanced Auditing and Security

- New auditing results, overall, up to 120 Security checks
- Support for Oracle Database 23c SQL Firewall

Sensitive Data Discovery

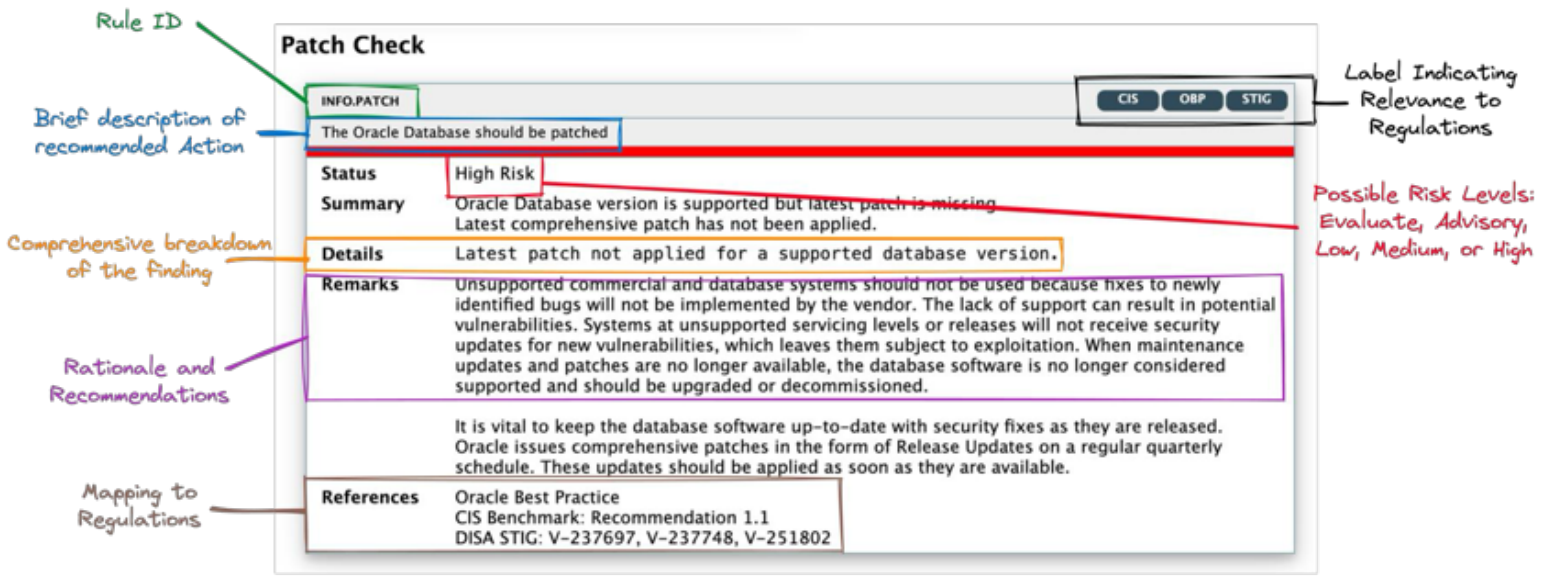
- Indian PAN and Aadhaar numbers

Improved Clarity and Quality

- one-line summary outlin
- Compliance labels

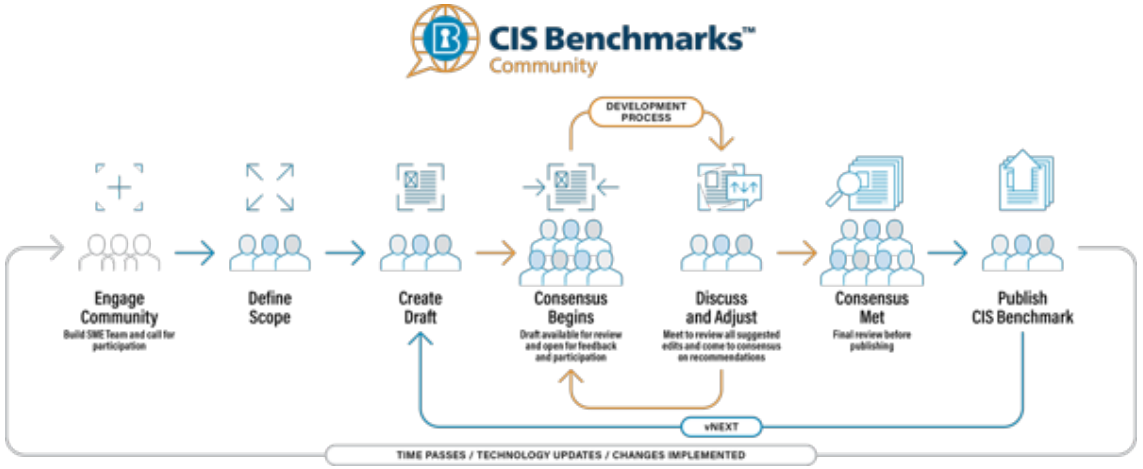
Operational Enhancements

- New parameter
- Linux 64-bit ARM Support



CIS Security Benchmarks

Industry-Standard Framework for Database Hardening



Center for Internet Security (CIS)

CIS provides widely recognized security benchmarks for database hardening.

- **Configuration Guidance**: CIS benchmarks offer detailed recommendations for secure configurations, helping reduce vulnerabilities.
- Compliance Support: Following CIS benchmarks helps organizations meet regulatory and compliance standards.

Additional Standards / Best Practices

- **Department of Defense (DoD) STIGs**: The DoD Security Technical Implementation Guides (STIGs) offer configuration guidelines for robust security. DoD STIGs
- **Oracle Database Security Primer**: Oracle's technical primer provides a comprehensive overview of database security best practices.
  Oracle Database Security Primer

Data Safe for Security Enhancements

Leverage Data Safe for Comprehensive Security Management

The use of Data Safe for ADB is straight forward

Security Assessments

- Identify vulnerabilities and misconfigurations.

Audit Configuration and Reporting

- Automate audit setup and reporting to ensure compliance

User Assessments

- Monitor and analyse user access patterns.

Sensitive Data Discovery

- Identify and protect sensitive data automatically.

6

Performance Tuning

Optimizing Performance in Secure Database Environments

Tuning Performance with Segregation of Duties

Ensuring Security While Optimizing Database Performance

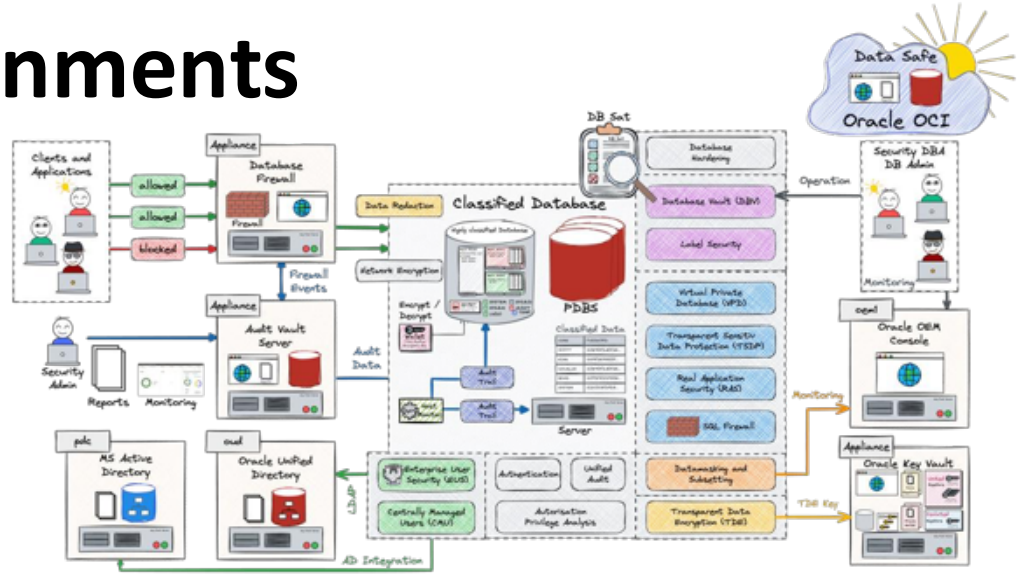
Challenges of Restricted Access

- Segregation of duties can limit DBA permissions, affecting performance diagnostics.
- Restricted access may prevent running queries or directly modifying certain configurations.

Practical Solutions

- Use tools like *SQL Monitoring*, *AWR (Automatic Workload Repository) Reports*, and *Database Performance Hub* for diagnostics.
- Implement **proxy users** to allow temporary, controlled access for performance tuning.
- Define clear processes for escalating and approving elevated permissions when necessary. e.g., break glass process

Performance Tuning in Secure Environments



Adapting Performance Tuning for Hardened Databases

Balancing Security and Performance

- Security features like TDE, Auditing, and Database Vault may introduce performance overhead.
- Assess impacts case-by-case based on workload type (I/O, CPU, or memory-bound).

Key Considerations:

- **TDE:** Potential I/O and CPU overhead during encryption/decryption.
- **Auditing:** Increased processing time depending on log volume and granularity.
- **Database Vault:** Additional checks may affect query execution speed.

Best Practices:

- Use tools like AWR, SQL Monitoring, and Performance Hub to identify bottlenecks.
- Optimize workloads and adjust configurations for critical operations.
- Avoid removing security measures solely for performance gains.

7

Best Practices & Key Takeaways

Essential Strategies for Effective Database Security

Best Practices Checklist

Key Steps for Secure and Efficient Database Operations

- ❑ **Start Securely**: Implement security measures from the beginning.
- ❑ **Know Your Data**: Identify and classify sensitive data and environments.
- ❑ **Understand Operations**: Map out routine tasks and operational workflows.
- ❑ **Minimize Attack Vectors**: Disable unnecessary features and close security gaps.
- ❑ **Enforce Least Privilege**: Apply segregation of duties and restrict privileges.
- ❑ **Automate Processes**: Reduce manual intervention wherever possible.
- ❑ **Use Adequate Privileges**: Perform manual tasks with appropriate, limited access.
- ❑ **Audit Critical Activities**: Log and review sensitive operations.
- ❑ **Monitor Security Settings**: Track and enforce secure configurations.
- ❑ **Regularly Assess:** Evaluate configurations, users, and privileges on a recurring basis.
- ❑ **Review Security Concepts**: Periodically revisit and update the security strategy.

Importance of Layered Defense

A Multi-Layered Approach to Database Security

Why Layered Defense?

- **Redundancy**: Multiple layers ensure that if one control fails, others can still provide protection.
- **Comprehensive Coverage**: Protects against different types of threats, from user access to data encryption.
- Scalability: Easily add new layers as threats evolve and requirements change.

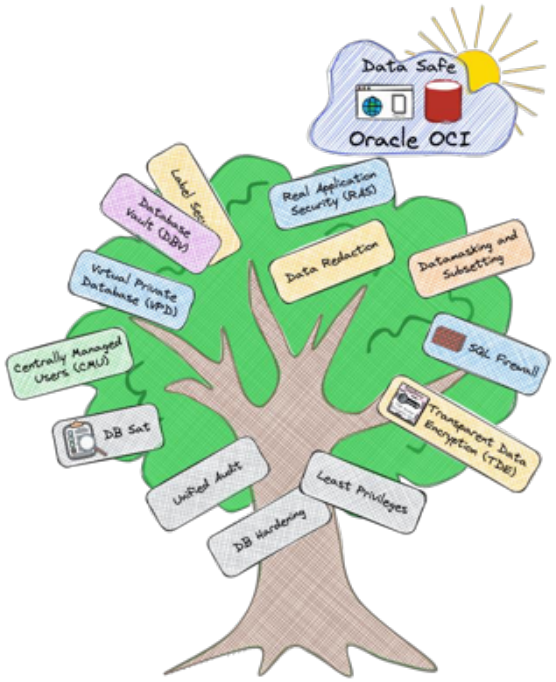
Examples of Security Layers:

- **Database Hardening & SQL Net Encryption**: Secure the basics and ensure encrypted communication.
- **Unified Audit & TDE**: Centralized logging and encryption for robust control.
- **Database Vault & VPD**: Restrict access and ensure data privacy, even for sensitive information.

Best Practices for Database Security

Best Practices for Effective Database Security

- **Apply Least Privilege**: Grant only necessary access.
- **Use Strong Authentication**: Implement SSL, Kerberos, or Centrally Managed Users (CMU). **Regular Auditing**: Set up Unified Audit to monitor critical actions.
- **Regularly Update**: Keep Oracle versions and patches up to date.
- **Customize Policies**: Tailor security policies to match organizational needs.
- **Leverage basic Features:** Use hardening, network encryption etc.
- **Enable Encryption**: Use TDE for comprehensive data protection.
- **Security Assessment**: Check the security measures regularly



Key Takeaways

Essential Principles for Database Security

Balance Security and Efficiency

- Security must protect without disrupting operations.
- Performance should not justify omitting critical controls.

Focus on Fundamentals

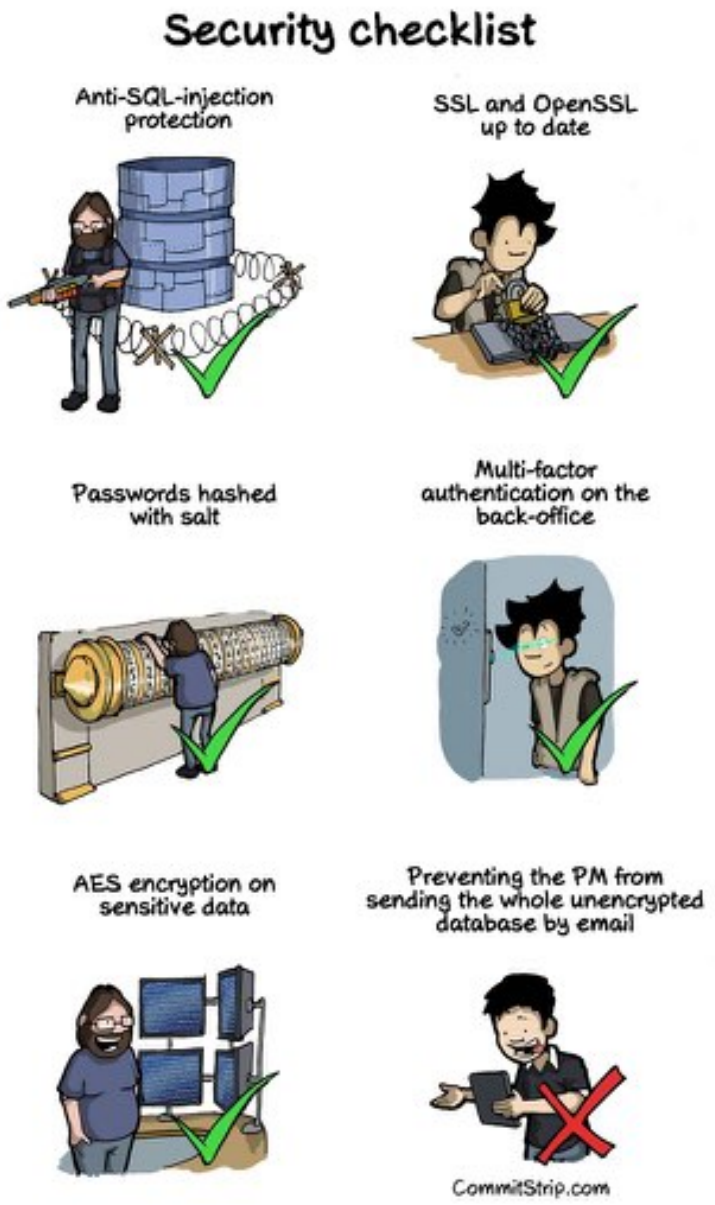
- Implement hardening, auditing, and encryption as a baseline.
- Automate repetitive tasks to minimize errors.

Enforce Roles and Access

- Use tools like Database Vault to segregate duties.
- Limit access to sensitive operations.

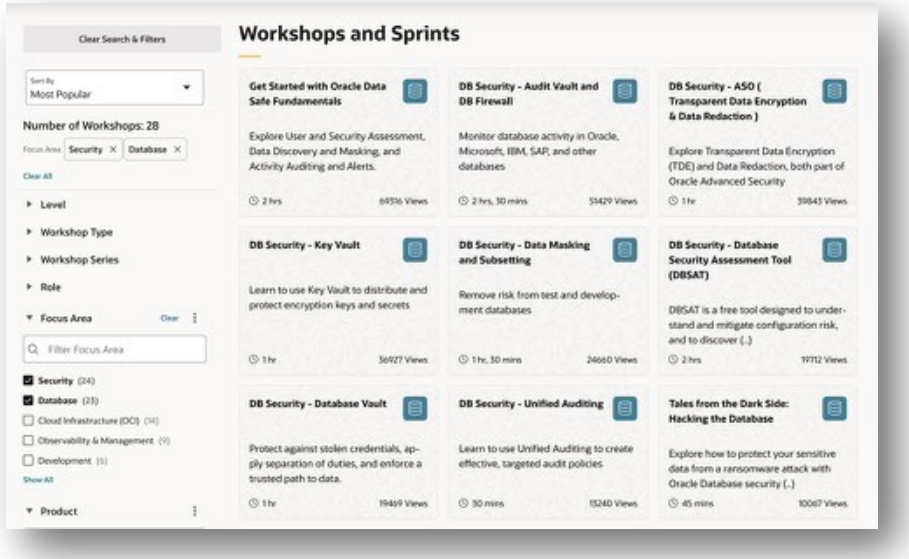
Monitor and Update

- Regularly audit activity and security configurations.
- Stay updated with patches and test measures in realistic setups.



Test Oracle Security Features in LiveLabs

Hands-On Experience with Oracle's Security Tools



Explore Security Features

- Access a variety of labs focused on Oracle Database Security, including Transparent Data Encryption (TDE), Database Vault, Unified Audit, and more.

Hands-On Learning

- Get practical, guided experience with Oracle security tools in a real environment.

Self-Paced Labs

- Work at your own pace, with step-by-step instructions to help you learn and implement security features.

Accessible and Free

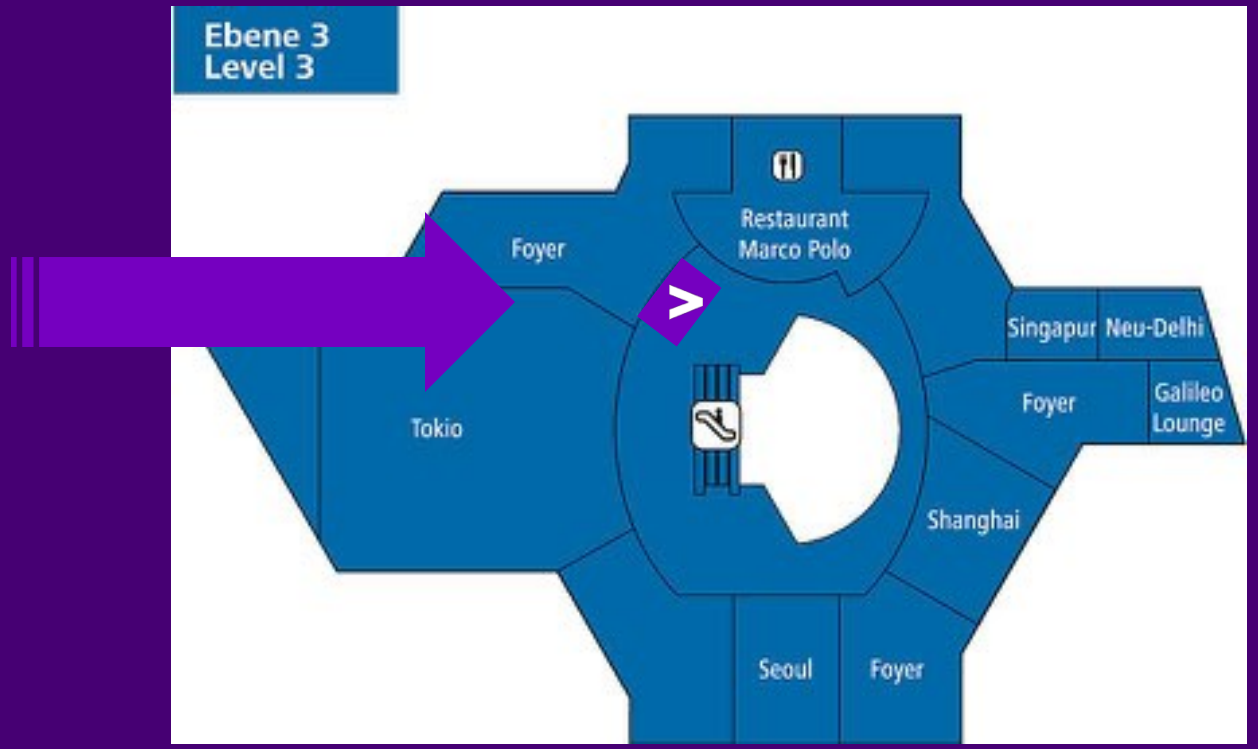
- Available to anyone; no need for a personal Oracle setup.

Get Started

- Visit Oracle LiveLabs Security to begin exploring.

Meet me at the Accenture Booth!

- Für weitere Gespräche treffen Sie mich gleich am Accenture Stand auf Ebene 3



ACES
PRIZES
DRINKS

Quiz and Win Test your knowledge in a fun quiz!

Meet the ACEs If you are an ACE, join us and meet your peers!

- Tuesday 14:45
- Wednesday 12:45
- Thursday 11:00

Accenture ACEs talk about the **ACE Program**

- Wednesday 14:45

Where: Accenture Booth on Level 3

Join us in the Happy Hour on
Wednesday evening:
Drinks are on us!

Secure your data with balanced measures, automation, and continuous monitoring for strong protection and efficiency.

Thank You