MySQL Reference Architectures for Security

Table of Contents

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. 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 in this document remain at the sole discretion of Oracle

Introduction

This whitepaper focuses on protecting your MySQL data. Your databases contain valuable and often sensitive information, including intellectual property, personal data, and financial records. Whether you're a data owner, security administrator, or simply interested in best practices, this document outlines key elements of a successful database security program, emphasizing goal-oriented strategies and efficient task management.

Security projects are typically driven by three key factors: regulatory compliance, the threat of malicious activity (particularly ransomware), and the demand for business agility. Nearly every organization faces multiple regulatory mandates. However, the fear of cybercrime, especially ransomware, now dominates boardroom discussions. This whitepaper lays the groundwork for database security by outlining common regulatory compliance goals and the essential steps to protect your data.

Database Security

Today's complex systems are vulnerable to small errors, which attackers readily exploit. Regularly checking your database security against established rules and best practices is crucial. Failing to implement basic security measures can expose sensitive personal data, damaging your reputation and finances. Consistent database strengthening and scanning are essential. Regulations like GDPR, PCI DSS, DORA, HIPAA, and DISA STIG mandate security checks. DISA STIG provides detailed requirements, while others offer broader guidelines. Security organizations like CIS also offer valuable advice. This chapter demonstrates how MySQL features and tools can help you identify, organize, and resolve security issues, ensuring your databases remain secure.

Key Security Considerations

- **Sensitive Data Identification:**
    - Effective data protection begins with understanding what sensitive data you have and where it resides.
    - Knowing the type, volume, and location of sensitive data allows you to implement appropriate security controls.

- **Authentication:**
    - Secure database access begins with verifying user identities (authentication). Your authentication strategy safeguards users and data from unauthorized access.

- Manage user accounts directly within the database or via external identity management systems.

- **Authorization:**
    - Controlling user actions (authorization) is crucial for database security.
    - A strong authorization strategy prevents errors, misuse, and attacks.
    - Manage user permissions locally or through centralized identity services.

- **Separation of Duties:**
    - Strong security controls for insider and privileged accounts are vital.
    - Since compromised privileged accounts are a primary attack vector for database breaches, and rogue users can cause substantial harm, implement separation of duties and least privilege to reduce potential losses.
    - Though consolidating administrative functions may seem convenient, dividing responsibilities and maintaining granular privilege control significantly improves security.

- **SQL Injection:**
    - Although developers have been educated on SQL injection prevention for years, it remains a common and dangerous attack vector.
    - Database's SQL Firewalls provide a crucial layer of defense against SQL injection attacks, supplementing application-level security.

- **Data Masking:**
    - Protecting sensitive data, complying with regulations, and securely providing data for various uses—development, testing, analytics, research, and collaboration—require methods like data masking, de-identification, and substitution.
    - Data masking effectively balances data usability and security, allowing organizations to work with data safely and efficiently.

- **Data Encryption and Key Management:**
    - Encryption is the most effective defense against database bypass attacks, where attackers steal data without logging in.
    - This includes capturing network traffic, accessing database files via the operating system, or stealing backups.
    - Protect data in transit and at-rest and address secure encryption key management.

- **Database Activity Auditing:**
    - For effective incident investigation, malicious behavior detection, and regulatory compliance, database activity monitoring is vital.

- This can be achieved through MySQL event auditing.

Cyber Attacks, Data Theft, and Data Destruction

Malicious Attack Tactics

With cybersecurity incidents escalating daily, organizations risk losing sensitive personal and intellectual property data. Stolen data fuels financial and political gain. Since databases are the core of data storage, their security is critical.

Healthcare Information
Bank routing number
Credit Card Number
Billing Address
Aadhar Number
Employee Number
First Name
SSN
Driver's License Number
Card Expiration Date
Student Identification Number
Religion
CURP
Visa Number
Weight
County
Taxpayer ID
State
Bonus
Gender
Marital Status
Race
Date of Birth
Personally Identifiable Information
NINO
Username
IP Address
Nationality
Weight
Location
Next of Kin
Patient Identification Number
City
Cookie
Physical Characteristics
Password
Hire Date
Phone Number
Employment Data
Age
Place of Birth
Social Insurance Number
Bank Account Number
Annual Pay
Height
Next of Kin
Browser history
Fingerprint
Passport Number
Termination Date

Types of personal data

Hackers employ various tactics, including (approximate high to low frequency):

- Gaining access via password guessing or poor credential management.
- Exploiting application weaknesses like SQL injection.
- Bypassing access controls with unpatched systems or misconfigurations.
- Stealing administrator or application user credentials.
- Encrypting data or stealing keys for ransomware attacks.
- Escalating privileges through vulnerable applications.
- Finding sensitive data in unprotected areas.
- Using unprotected systems as attack bridges.
- Targeting less-protected development and test data copies.
- Accessing unencrypted database files and backups.
- Creating rogue user accounts for reconnaissance and privilege escalation.

Risk Mitigation

The most common security risks are:

1. Insecure configuration and configuration drift
2. Unpatched and out-of-date systems
3. Lack of a consistently enforced security policy
4. Lack of visibility into sensitive data placement and quantity

5. Overprivileged database users and administrators
6. Weak authentication and shared accounts
7. SQL Injection vulnerabilities and insecure application design
8. Trusting vulnerable networks
9. Insufficient or inefficient monitoring and auditing
10. Sensitive data proliferation to non-production databases
11. Unprotected servers and database backups
12. Insecure encryption keys and secrets

To mitigate the risk of malicious attacks, implement a multi-layered approach that focuses on the following 4 areas:

1. Security Assessment
2. Access Controls
3. Monitoring activity
4. Data Theft Protections

Category	Goal	Task	Threat Addressed
Assess security posture	Ensure systems do not deviate from their approved security baseline	Monitor databases for configuration changes that introduce risk	Insecure configuration
Monitor user activities	Detect inappropriate activity by privileged users	Audit all DBA activity	Insufficient or inefficient monitoring and auditing
Protect data against theft	Scramble sensitive data in test and development environments	Scramble sensitive data in test and development environments	Unprotected servers and database backups
Control access to data	Strengthen user authentication to prevent compromise of accounts	Implement multifactor authentication for the database	Weak authentication and shared accounts

Examples of Security Risks and Tasks

Insecure Configuration – check and fix using:

- CIS Benchmark for MySQL Enterprise Edition
- DISA STIG for MySQL Enterprise Edition
- MySQL Secure Guidelines

Over-privileged users – implement:

- SSO (Single Sign On)
- MFA (Multifactor Authentication)
- Privilege Analysis

Insufficient Monitoring – deploy:

- Enterprise Audit
- Telemetry Traces, Metrics, and Logging
- Oracle Enterprise Manager for MySQL

Unprotected data – use:

- Advanced Encryption
- Key Ring and TDE
- Data Masking
- High Availability and Disaster Recovery – InnoDB Cluster, Replica Set, Cluster Set

The Critical Threat of Ransomware

Ransomware is widely recognized by cybersecurity authorities (ENISA, CISA, NCSC) as a leading threat to organizations and infrastructure. It's a primary income source for cybercriminals and a tool used by nation-states for disruption, distraction, and funding.

The simplest definition of ransomware is a type of malicious software (malware) that encrypts a victim's files and offers to provide a decryption key in return for some form of compensation (usually monetary)

Mitigating Ransomware Data Destruction

Ransomware's "simple" denial-of-service, encrypting data files, leads to complex recovery. Beyond database restoration, it requires network malware removal, OS reinstallation, and storage reconnection.

Data consistency across databases, often backed up at different times, is crucial.

Mitigation requires:

- **Immutable Backups:** Protect backups from ransomware destruction.
- **Synchronized Recovery:** Restore to a consistent point in time – ideally with zero data loss.
- **Recovery Infrastructure:** Treat recovery as a disaster recovery scenario. Utilize warm sites with MySQL Cluster, Replica-Set, and Cluster-Set, replicate data to cloud-based secure enclaves, or recovery clean rooms for rapid restoration.

A key ransomware evolution is the focus on data theft. Rather than destruction, attackers now extort victims with threats of data release, a shift in monetization from typical data breaches.

Mitigating Data Theft in Ransomware Attacks

Ransomware typically steals data by scraping files, not directly targeting databases. Therefore, Transparent Data Encryption (TDE) is generally effective. However, protect encryption keys in off-server Key Vaults like Oracle Key Vault, OCI Vault to prevent them from being compromised during the same attack.

Government & Industry Regulations

To navigate the numerous government and industry security regulations (note: this is not legal advice; consult your legal department), we advise proactively establishing a security control framework. Despite variations in reporting and assessment, the technical controls required by most regulations share key similarities, including:

- Data Encryption
- Data Access Controls
- Data Access Auditing

Data Encryption

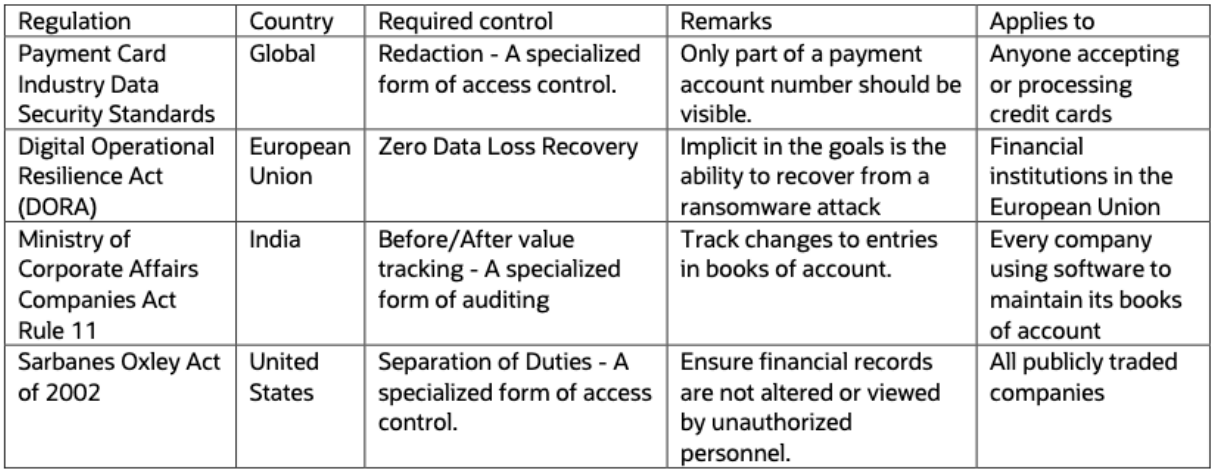
Encryption uses cryptographic algorithms to make data unreadable, ensuring access only with the correct decryption key. This is a vital technical control required by most regulations. Importantly, secure management of encryption keys is also necessary. While some consider encryption a type of access control, it's commonly treated as a separate security practice with its own unique advantages and challenges.

Data Access Controls

Access control defines who and when an account can access a database or its objects. As the broadest technical control, it includes authentication, session initiation, object visibility, and granular access to data at the row or column level.

Data Access Auditing

Auditing records system events, capturing action performed (insert, update, execute, etc.), date and time of the action, user accounts (database and OS), application used for connection, and source of the connection (IP address/hostname). Auditing allows for post-incident analysis, providing data for forensic investigation and compliance reporting. Unlike access control, auditing does not block unauthorized actions but supports breach investigations and troubleshooting.



Regulation	Country	Required control	Remarks	Applies to
Payment Card Industry Data Security Standards	Global	Redaction - A specialized form of access control.	Only part of a payment account number should be visible.	Anyone accepting or processing credit cards
Digital Operational Resilience Act (DORA)	European Union	Zero Data Loss Recovery	Implicit in the goals is the ability to recover from a ransomware attack	Financial institutions in the European Union
Ministry of Corporate Affairs Companies Act Rule 11	India	Before/After value tracking - A specialized form of auditing	Track changes to entries in books of account.	Every company using software to maintain its books of account
Sarbanes Oxley Act of 2002	United States	Separation of Duties - A specialized form of access control.	Ensure financial records are not altered or viewed by unauthorized personnel.	All publicly traded companies

Table 2-1 - Regulatory-influenced Controls

As you can see in this table the requirements generally fall into the above 3 main categories.

Database Security Assessment

Databases, with their complex configurations, are prime targets for security breaches. Secure systems are essential, as demonstrated by recent data losses. Human error and malicious exploits of misconfigurations jeopardize valuable data. Exposing sensitive information through inadequate security controls damages reputation and finances. Regulations like GDPR and PCI DSS necessitate regular security assessments. Regularly scan and remediate database vulnerabilities, considering best practices, regulations, and organizational standards. This chapter outlines how Oracle Database security solutions can quickly assess, categorize, and provide recommendations for database security.

Evaluate and Assess your Database Configuration

Cyber attackers invest considerable time in pre-attack reconnaissance. They employ automated tools to discover databases, identify open ports and vulnerabilities, and execute application, SQL injection, and brute-force password attacks. Following this probing phase, they pinpoint weaknesses and devise their attack strategy, essentially performing a security posture assessment to target sensitive data.

Some common questions attackers try to answer while probing your databases:

- What version of the database is running? – Identifying outdated versions with known vulnerabilities.
- Are default or weak credentials in use? – Exploiting accounts with weak or unchanged passwords.
- Which privileged users exist? – Escalating access by compromising high-privilege accounts.
- Is auditing enabled? – Determining whether actions will be logged and monitored.
- Is the data encrypted? – Assessing if they can steal raw data from storage or backups.
- Is there a copy of this database that is less likely to be audited? – Finding the least risky approach to data

To effectively secure your databases, adopt an attacker's mindset. Here are some key considerations for protecting your databases:

- Almost all databases hold sensitive data, but the level of importance of individual data attributes may differ. For example, a customer's date of birth may be more sensitive than their email address. It is essential to find out which databases contain what type of sensitive data so that controls can be implemented accordingly.

- Common points of attack against the database include unpatched systems, poor application design, weak user credentials, excessive privilege grants, lack of a trusted path to data, separation of duties, encryption, and inadequate auditing.

- Security configuration parameters are tightly related to how the database behaves and require understanding the parameters, what they do, the impact of changing them, and their dependencies.

- Not all database users are equal. Apart from the DBAs, several other actors/processes interact with your data through database user accounts—the application, application administrators, security administrators, and others, including service accounts, batch programs, etc. Identifying the different types of database users and the activities they need to execute on the database helps you properly manage privileges and roles and implement the principle of least privilege.

- Not all databases are created equal. Some databases may be more business-critical or contain more sensitive or highly regulated data. Your investment in security controls (which could be in tools, time, or operational resource commitment) is usually commensurate with the criticality or sensitivity of the database.

Risk and Security Assessment Tools for MySQL

CIS Benchmark for MySQL Enterprise Edition

The Center for Internet Security (CIS) provides consensus-based configuration benchmarks for various software and hardware systems. The CIS Benchmark for MySQL Enterprise Edition offers prescriptive guidance on securely configuring MySQL databases. These benchmarks are designed to help organizations reduce their security risk by adhering to industry-accepted best practices. CIS benchmarks are widely used across various industries to help organizations comply with regulations like PCI DSS, HIPAA, and others. They provide detailed configuration recommendations, are regularly updated to address emerging threats, and are designed to be applicable to a broad range of organizations.

MySQL Configuration Guidelines and Recommendations covering:

- OS
- Network
- File Permissions
- Updates and Patches
- Auditing and Logging
- Authentication
- High Availability (HA) and Disaster Recovery (DR)

Prescriptive Guidance for MySQL Enterprise Edition Including:

- Secure baseline for security auditing
- Risk explanation
- Impact assessment
- Steps to perform audit
- How to fix issues detected by auditing
- Cross-references to related resources

- Continuously benchmark updates
- Participation with CIS MySQL security community

Recognized as a Secure Configuration Standard by:

- DoD Cloud Computing Security Recommendation Guide (SRG)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Management Program (FedRAMP)
- National Institute of Standards and Technology (NIST)
- And more - for a complete list, see CIS Mapping and Compliance

About MySQL CIS Benchmark for MySQL Enterprise Edition
Download: CIS Benchmark for MySQL Enterprise Edition

DISA STIG for MySQL Enterprise Edition

The Defense Information Systems Agency (DISA) develops Security Technical Implementation Guides (STIGs) for the U.S. Department of Defense (DoD). The DISA STIG for MySQL Enterprise Edition provides highly specific security configuration requirements for DoD systems. These STIGs are very rigorous and are designed to meet the stringent security needs of military and government environments. They are very detailed and prescriptive, are primarily focused on DoD requirements, and tend to be more rigid than CIS Benchmarks. Despite not always being mandated for compliance, DISA STIGs are publicly accessible and frequently employed for security assessments.

DISA STIGs Include a Description of Requirements Explaining:

- What are the related security risks and vulnerabilities?
- Is a vulnerability applicable to a product?
- Whether the product has inherent protection or if you need to check the product settings.
- Which settings to inspect and how - pass (protected) or fail via a series of checks.
- Changes needed when a check fails.
- Other mitigating actions to put in place to minimize security risk.
- Use of additional products to provides added protection.

About MySQL DISA STIG for MySQL Enterprise Edition>>
Download: DISA STIG for MySQL Enterprise Edition>>

MySQL Security Guidelines

The MySQL Security Guidelines provides basic security guidelines for users of MySQL. It stresses the importance of securing the entire server host, not just the MySQL server, against various attacks. The guide includes recommendations such as controlling access to MySQL with GRANT and REVOKE statements, choosing strong passwords, using firewalls, auditing, and employing data encryption and encrypted protocols like SSL or SSH for data transmission.

Learn more about the MySQL Security Guidelines>>

Software Upgrade Management

Product upgrades are essential for maintaining robust security. Regular upgrades, at a minimum quarterly, are released by MySQL to address bugs and security vulnerabilities, including:

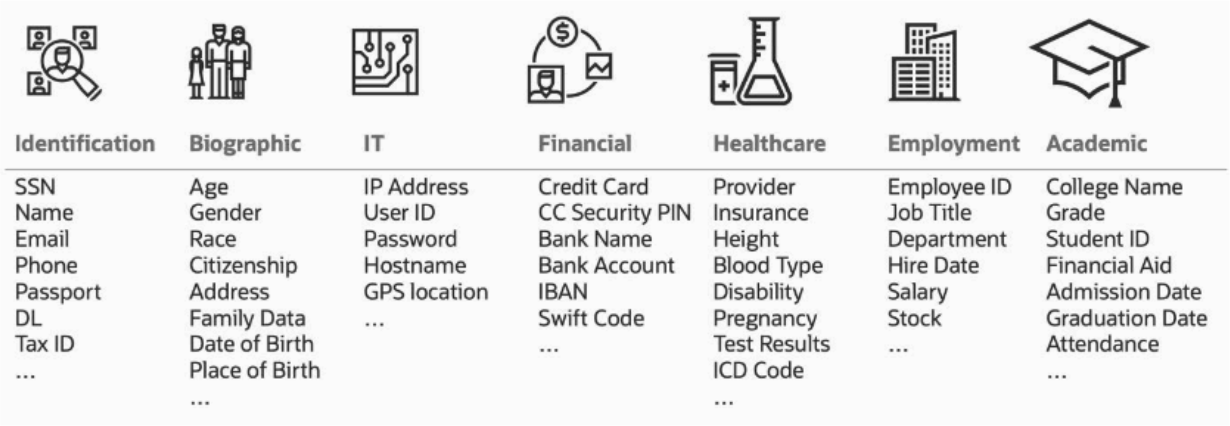
- Vulnerable SQL statements, buffer overflows, and SQL injections.
- Vulnerabilities in database clients, JDBC drivers, and third-party code.
- Weaknesses in cryptography, networking, and remote code execution.

Timely upgrades are critical for a strong security posture. Neglecting upgrades exposes organizations to known vulnerabilities.

Protecting Sensitive Data

Data is critical for organizational success, driving everything from customer relations to strategic decisions. However, its growing volume and sensitivity make it a prime target for theft, demanding robust protection. Database security effort should align with both regulatory requirements and the potential business risk of a data breach.

Sensitive data can be classified into categories such as identification, biographic, healthcare, financial, employment, and academic data. Here are a few examples of categories and types of sensitive data.



Identification	Biographic	IT	Financial	Healthcare	Employment	Academic
SSN	Age	IP Address	Credit Card	Provider	Employee ID	College Name
Name	Gender	User ID	CC Security PIN	Insurance	Job Title	Grade
Email	Race	Password	Bank Name	Height	Department	Student ID
Phone	Citizenship	Hostname	Bank Account	Blood Type	Hire Date	Financial Aid
Passport	Address	GPS location	IBAN	Disability	Salary	Admission Date
DL	Family Data	...	Swift Code	Pregnancy	Stock	Graduation Date
Tax ID	Date of Birth		...	Test Results	...	Attendance
...	Place of Birth			ICD Code		...
	...			...		

Examples of sensitive data categories and types

MySQL Enterprise Audit can be used to determine:

- **Activity on Sensitive Data:** Collects details about activity on sensitive data by all users
- **Activity on Sensitive Data by Privileged Users:** Collects activity on sensitive data by privileged users

Authentication

Sometimes it's best to start with what NOT to do.

- **Do NOT Store Passwords in plain text**:
  - While password-based authentication requires users to provide passwords, applications and automated processes cannot.
  - Historically, embedding credentials in code or scripts was common but insecure, increasing attack surfaces and requiring constant script updates for password changes.

- **Do NOT share accounts and passwords:**
  - Shared accounts create significant security risks.
  - When errors, sabotage, or data breaches occur, pinpointing responsibility becomes impossible.
  - Despite organizational policies against them, shared accounts remain prevalent, even among highly privileged users like developers and database administrators (DBAs).

DBAs often misuse the root administrator account, a practice that should be strictly prohibited for routine tasks. Instead, each DBA should have a personalized account with specific roles and privileges, tailored to their responsibilities. This could be a standard DBA role or a more granular set of permissions.

Similarly, application administrators and developers should avoid shared accounts. While they may require access to application schemas for maintenance, they should use individual credentials rather than the application service account.

Strong Passwords

Given the continued reliance of legacy applications on password authentication, it is imperative to establish and enforce stringent password policies. These policies should include, but not be limited to, requirements for password length, complexity, rotation, and history. MySQL provides the mechanisms necessary to implement such policies.

Centralized User Management

Managing database user identities is complex. Employee turnover and role changes create challenges, especially with numerous users or multi-database access. In practice, dormant accounts often persist, becoming prime targets for unauthorized access. MySQL supports centralized user management to address this. By managing users and credentials outside the database, typically via directories like LDAP, Microsoft Active Directory or cloud identity services such as Oracle Cloud Infrastructure IAM, Okta, or Microsoft Entra ID, organizations can enforce consistent policies and streamline the user lifecycle.

Centralized services simplify onboarding, offboarding, and role adjustments. Many, particularly cloud providers, offer multi-factor authentication. Even beyond passwords, centralized management integrates with authentication methods like Kerberos, OpenID Connection, PKI certificates and multi-factor authentication providing robust security.

Beyond internally managed MySQL User password authentication. MySQL Enterprise Edition offers a range of advanced authentication options:

- **MySQL OpenID Connect (OIDC) Authentication:**
  - Leverages the OIDC protocol, built on OAuth 2.0, for secure authentication.
  - Enhances security by eliminating the need to manage passwords directly, mitigating credential-based breaches.

- **MySQL External Authentication for LDAP:**

- Integrates with LDAP servers for user authentication.
- Provides granular control over user and group access through LDAP specifications.
- Supports various authentication methods, including username/password, SASL, and GSSAPI/Kerberos.

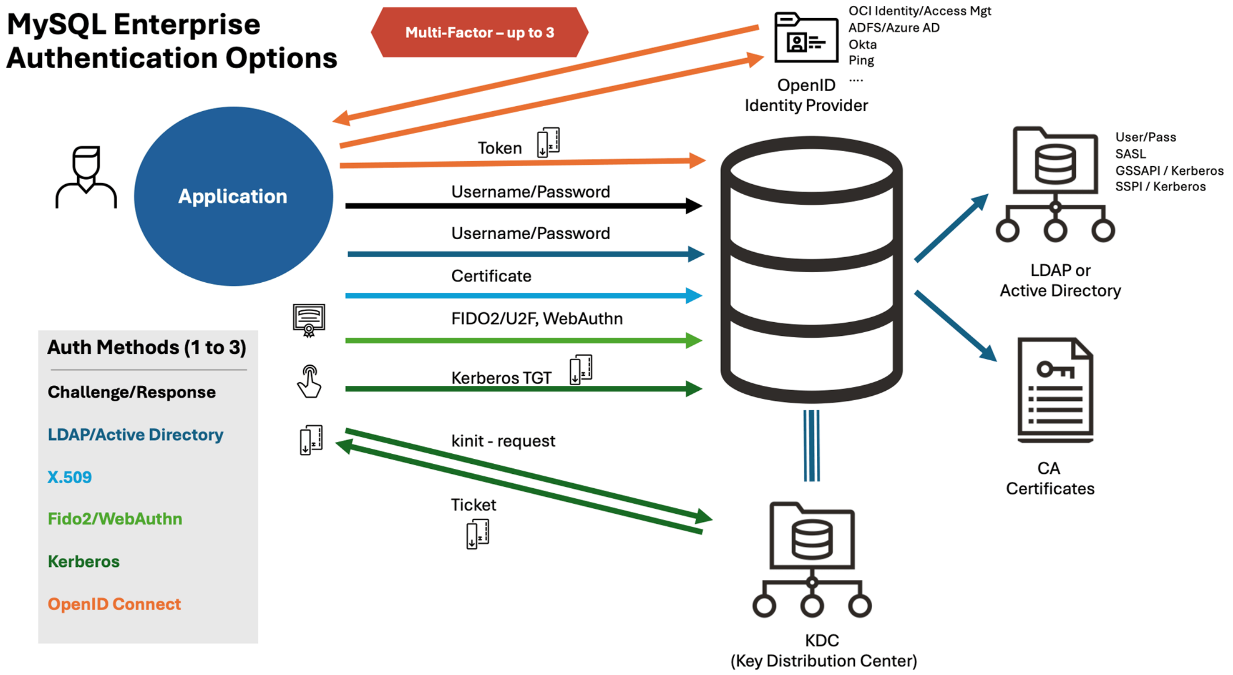
- **MySQL External Authentication for Windows:**
  - Utilizes native Windows services for client connection authentication.
  - Allows users logged into Windows to connect to MySQL without additional passwords, based on their environment's token information.

- **MySQL Native Kerberos Authentication:**
  - Enables integration with existing Kerberos infrastructure for single sign-on capabilities.
  - Supports both MIT (GSSAPI) and Microsoft (SSPI) Kerberos implementations (available in MySQL Enterprise Edition).

- **MySQL External Authentication for PAM:**
  - Integrates with Linux Pluggable Authentication Modules (PAMs) to support diverse authentication methods, such as Linux passwords and LDAP directories.

- **MySQL WebAuthn Authentication:**
  - Supports FIDO2 Web Authentication (WebAuthn) for secure authentication using devices like smart cards, security keys, and biometric readers.

- **MySQL Multifactor Authentication (MFA):**
  - Requires users to provide multiple verification factors, enhancing security against attacks targeting usernames and passwords.
  - Strengthens organizational security against cybercrime by allowing the combination of up to three authentication methods.



Advanced Authentication Options for Centralized User Management

Enforcing Security for Business Users

Business users cannot be solely relied upon to adhere to complex security guidelines. Database systems must enforce these policies to protect users. Key security measures include:

- **Prioritize strong authentication:** Move beyond passwords by implementing token-based authentication from cloud identity services, Kerberos, OpenID Connect, or PKI certificates.

- **Enforce robust password policies (if necessary):** If passwords are required, implement stringent profiles that dictate password strength, inactivity timeouts, and failed login limits.

- Centralize user management: Utilize identity services like Active Directory to minimize orphaned accounts resulting from employee turnover or role changes.

Securing Database Administrator (DBA) Accounts

DBA accounts, with their extensive database access, are prime targets for attackers. Implement these critical security measures to mitigate risks:

- **Enforce Individual Accounts and Strong Authentication:**
  - DBAs must use named accounts with robust authentication methods like cloud identity service tokens, PKI certificates, or Kerberos. Shared or default accounts (e.g., SYSTEM) are strictly prohibited.

- **Implement sudo for OS Access:**
  - When DBAs require operating system access, use sudo to maintain an audit trail of individual actions. Ensure each DBA has a personal OS account.

- **Restrict Direct Database Owner Access:**
  - DBAs connecting via the database server's OS must use their own named accounts, not the database owner's.

- **Implement Role-Based Access Control:**
  - For organizations with specialized DBA teams (backup/recovery, performance tuning, security), use tailored administrator roles with minimal necessary privileges, rather than granting the default admin (super) role.

Protecting application accounts

Application service accounts, possessing extensive application privileges and often maintenance rights, are highly vulnerable. Implement these security best practices:

- **Enforce Strong Authentication and Connection Restrictions:** Employ robust authentication methods like cloud identity service tokens or PKI certificates. Utilize controls such as MySQL Enterprise Firewall and user@host to restrict connection origins for these accounts.

- **Utilize Secrets Management:** Store credentials in a secrets manager like Oracle Key Vault, enabling applications to retrieve them via API calls. Avoid hardcoding credentials or storing them in clear-text files on application servers, which are more susceptible to compromise.

- **Implement Dual Password for Seamless Rotation:** Employ dual password functionality to minimize application outages during password rotation. This allows simultaneous use of old and new passwords until all application servers are updated.

- **Promote Individual Administrator Authentication:** Application administrators should use their own credentials rather than the application service account.

- **Implement Role-Based Privilege Management:** Assign specific roles and utilize SET ROLE for privilege de-escalation and escalation, adhering to the principle of least privilege.

Controlling Database Access

Access controls are fundamental for regulating data interactions, determining who can access what data and what actions they can perform. By limiting accounts to the precise capabilities required for their functions, access controls mitigate the significant risk posed by overprivileged users. This practice is essential for enforcing regulatory compliance and preventing data theft, destruction, or misuse.

Recognizing the critical nature of access control, MySQL Database provides a comprehensive suite of mechanisms to manage database access.

A database privilege grants the authorization to perform specific operations on data objects or execute specific statements. MySQL Database offers four primary privilege types: object, database (aka schema), and administrative. These privilege types provide progressively broader scopes of authorization.

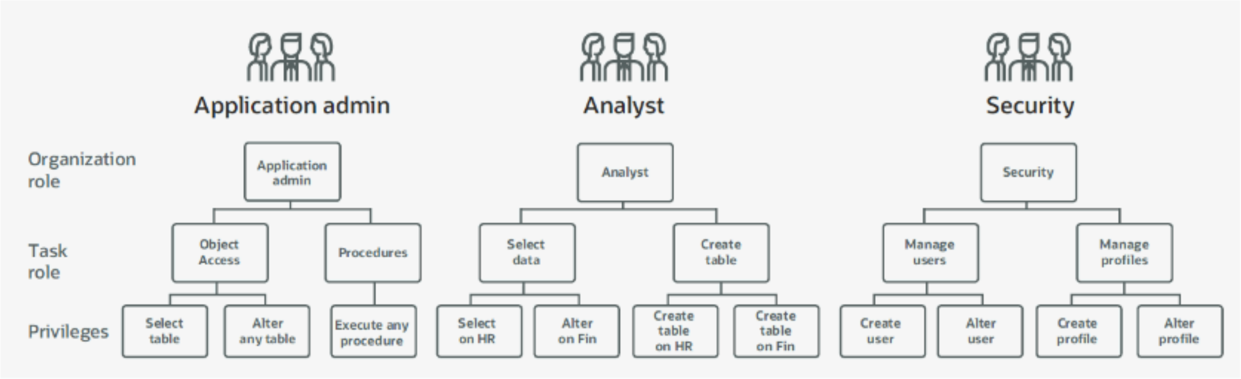
- Administrative privileges enable users to manage operation of the MySQL server. These privileges are global because they are not specific to a particular database.

- Database privileges apply to a database and to all objects within it. These privileges can be granted for specific databases, or globally so that they apply to all databases.

- Privileges for database objects such as tables, indexes, views, and stored routines can be granted for specific objects within a database, for all objects of a given type within a database (for example, all tables in a database), or globally for all objects of a given type in all databases.

Leveraging Roles for Efficient Privilege Management

Roles are named collections of privileges, designed to streamline privilege management. By grouping object, schema, and system privileges into task-based roles, administrators can efficiently grant or revoke identical privileges to multiple users. Roles can also be hierarchically structured, allowing for the aggregation of task roles into broader organizational roles. This hierarchical approach simplifies the assignment of complex privilege sets.



Sample role and privilege hierarchy

Simplifying User Management with Database Roles

Assigning multiple database roles to a single user streamlines user management. Instead of granting individual privileges, new employees can be assigned roles corresponding to their positions, simplifying onboarding. Similarly, when organizational changes occur, task roles can be efficiently reassigned, eliminating the need to manage individual privileges or redefine organizational roles. This approach significantly simplifies privilege management during organizational transitions.

Who can do what in your database?

One of the most critical components of a MySQL Database is its data dictionary (mysql), information schema, and performance schema. These contain tables and/or views that provide information about the database, including definitions (metadata) about all objects and users.

valuating MySQL database permissions is crucial for maintaining security. Here's a breakdown of how you can approach this, combining common practices and key considerations:

Understanding MySQL Privilege Levels

- **Global Privileges:**
  - These apply to the entire MySQL server.
  - Examples: CREATE USER, SHUTDOWN, GRANT OPTION.

- **Database Privileges:**
  - These apply to all objects within a specific database.
  - Examples: CREATE TABLE, SELECT, INSERT.
- **Table Privileges:**
  - These apply to a specific table within a database.
  - Examples: SELECT, UPDATE, DELETE.
- **Column Privileges:**
  - These apply to specific columns within a table.
  - Examples: SELECT, UPDATE.
- **Stored Routine Privileges:**
  - These apply to stored procedures and functions.
- **Proxy Privileges:**
  - These allow one user to act as another user.

Information_Schema Tables containing security metadata include:

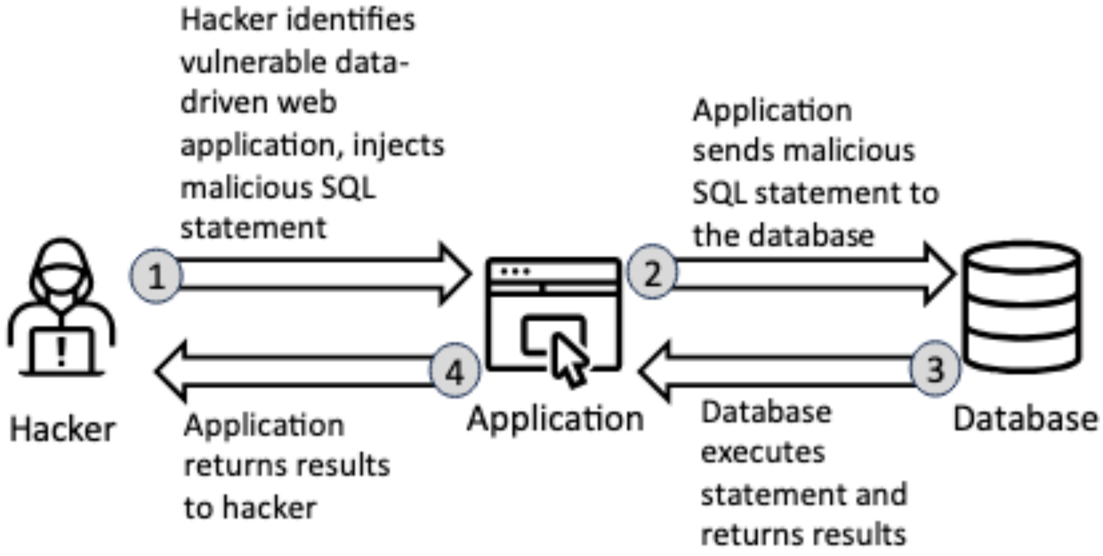
Information Schema Table	Description
APPLICABLE_ROLES	Roles that are applicable for the current user.
ROLE_COLUMN_GRANTS	Column privileges for roles that are available to or granted by the currently enabled roles.
ROLE_ROUTINE_GRANTS	Routine privileges for roles that are available to or granted by the currently enabled roles.
SCHEMA_PRIVILEGES	Schema (database) privileges.
TABLE_PRIVILEGES	Table privileges.
USER_PRIVILEGES	Global privileges.

In addition to the above, the SHOW GRANTS command displays the privileges and roles that are assigned to a MySQL user account or role, in the form of GRANT statements.

The Persistent Threat of SQL Injection

SQL injection remains a critical security concern, consistently ranking among OWASP's top web application vulnerabilities since 2004. This long-standing vulnerability persists because it exploits applications exposed to a wide range of attackers, including those on the internet. Despite extensive developer training and automated code scanning tools, SQL injection continues to plague data-driven web applications, highlighting the ongoing challenge of eliminating this fundamental security flaw. SQL injection poses a dual threat: direct database compromise (data corruption, destruction, exfiltration) and lateral network infiltration.

SQL injection is an application vulnerability that permits the insertion of malicious SQL code into database queries.


Hacker identifies vulnerable data-driven web application, injects malicious SQL statement
Application sends malicious SQL statement to the database
1
2
4
3
Hacker
Application returns results to hacker
Application
Database executes statement and returns results
Database

Hacker's Attack Workflow

Strategies for Mitigating SQL Injection Attacks

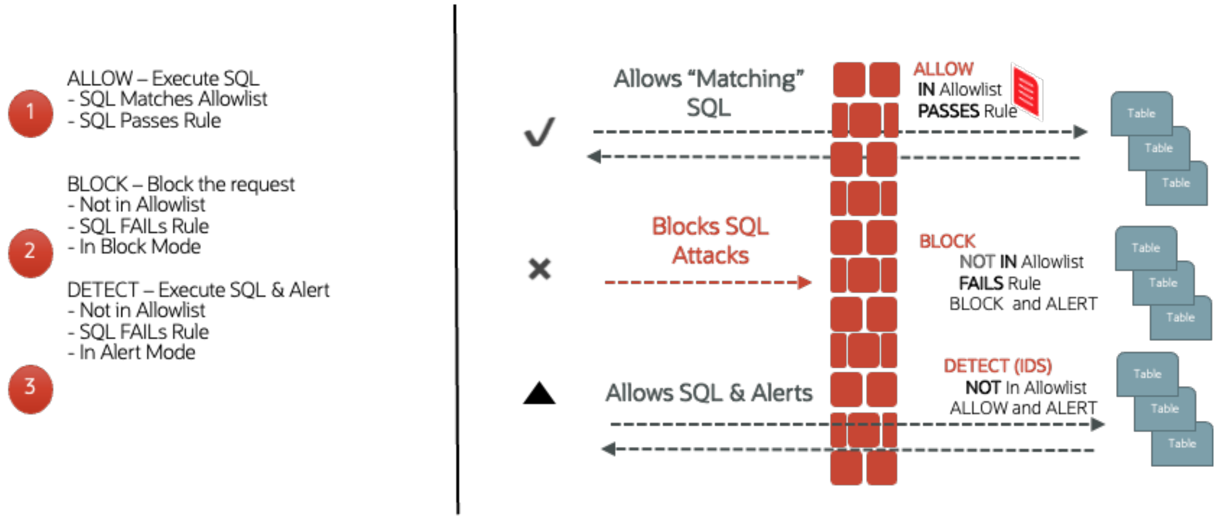
Effectively preventing SQL injection is challenging. While input validation is a fundamental security practice, developer errors and limitations in code reviews and automated scans can introduce vulnerabilities. Furthermore, legacy applications often lack accessible source code for remediation.

Web Application Firewalls (WAFs) offer a layer of protection by filtering suspicious HTTP traffic. However, their reliance on signature pattern matching limits their effectiveness against zero-day exploits and complex SQL injection techniques, as they lack deep payload analysis and SQL context awareness.

Database firewalls provide an additional defense by filtering database traffic before it reaches the database itself. A comprehensive security strategy incorporates both WAFs and database firewalls, creating a multi-layered approach to blocking SQL injection attempts at both the application and database levels.

MySQL Enterprise Firewall: Database-Resident SQL Protection

MySQL Enterprise Firewall mitigates SQL injection and other web application attacks targeting data-driven applications. Integrated directly within the MySQL Database, it eliminates the need for external installations or network configurations. Operating close to the data, the firewall cannot be bypassed. It inspects all incoming SQL statements, regardless of origin, encryption, or transmission method, ensuring only authorized SQL from trusted sources is executed. MySQL Enterprise Firewall employs an allow-list approach. The allow-list can be created by putting the firewall in RECORDING mode (or manually as well). Once the list has been created the firewall can either block SQL not included in the allow list in PROTECTING MODE or collect SQL not in the allow-list in DETECTING MODE.



MySQL Enterprise Firewall protects your data by blocking unauthorized database activity.

The Importance of Sensitive Data Masking

Organizations manage vast amounts of sensitive data, including PII, financial records, healthcare information, and proprietary data. Limiting exposure to users who don't require access is a significant challenge. However, leveraging application data outside its primary application is often crucial for various business functions. These include efficient application development and testing, insightful marketing and customer service analysis, and effective call center operations. While these use cases offer clear business benefits, they must be balanced with the imperative to protect sensitive information.

Data masking addresses this challenge by modifying sensitive data, rendering it useless to data thieves while preserving its utility for legitimate purposes. This mitigates the risk of data breaches and safeguards customer and employee privacy. By masking data such as credit card numbers, taxpayer identifiers, sales figures, and other personal or proprietary information, organizations can confidently utilize their data while maintaining security. For instance, testing a point-of-sale application might require realistic inventory and store information but not actual customer details. In such cases, fictitious yet realistic customer data can be substituted.

Static Data Masking Use Cases:

- **Reduce Breach Risk & Compliance:** Limit sensitive data storage, potentially excluding systems from GDPR/CCPA.
- **Secure Dev/Test:** Enable realistic data use without exposing sensitive information, meeting regulatory needs.
- **Save Time & Costs:** Use masked production clones, avoiding artificial test data creation.
- **Secure Data Sharing:** Protect sensitive data for third-party analytics or vendors, using reversible masking when needed.
- **Privacy in Training:** Allow realistic data practice without exposing private details.

MySQL Enterprise Masking and De-Identification addresses these challenges by providing a library of anonymization and masking formats, functions and dictionary transformations, and data deny listing. Sensitive information, such as credit card numbers, national identifiers, and other personally identifiable information (PII) can easily be masked with an out-of-the-box library of masking, randomization, dictionary, and deny listing capabilities.

Masking data in non-production environments can help to keep Development, Test and other environments

Data Encryption and Key Management

The Critical Role of Encryption

Even the strongest security measures are vulnerable if circumvented. Consider a physical analogy: instead of breaching a fortified front door, thieves often seek weaker entry points like back doors or unlocked windows. Similarly, while database authentication and authorization secure the "front door" by restricting access to authorized users, attackers may attempt to bypass these controls and directly target the data.

Encryption addresses this by rendering data unintelligible to unauthorized access, effectively transforming the challenge of securing vast amounts of data into the simpler task of protecting a smaller encryption key. Without the key, encrypted data is useless to attackers. Furthermore, encryption is frequently mandated by regulatory requirements and security standards for sensitive or personally identifiable information.

Prioritize Encryption to Protect Data Beyond Database Controls

Encryption safeguards data against attacks that bypass database access controls. Attackers can intercept unencrypted network traffic, directly access database files via privileged OS accounts, or steal unencrypted backups stored locally, remotely, or in the cloud. Since these attacks occur outside database sessions, encryption is essential to render data unreadable without a valid database connection.

Encrypting MySQL Database Connections (Data in Motion)

MySQL Database supports industry-standard Transport Layer Security (TLS) for encrypting network data. TLS provides confidentiality, integrity, and server authentication, with optional client authentication. It's essential for PKI certificate authentication.

TLS can be configured for server-authenticated or mutually authenticated (mTLS) modes, using certificates stored in system stores or MySQL wallets. Self-signed or CA-issued certificates are supported.

TLS can operate in FIPS mode for stricter encryption control. During connection, the server and client negotiate cipher suites, typically selecting the strongest mutual algorithm. Specific algorithms can be enforced.

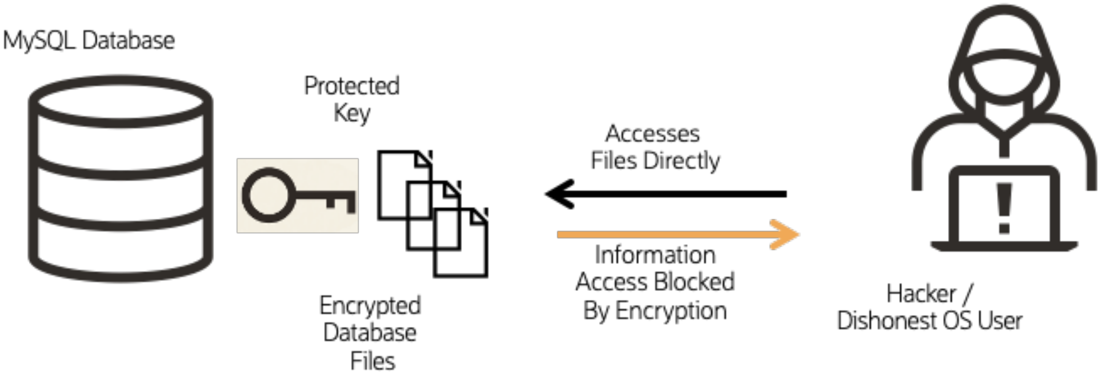
TLS 1.3 optimizes connection negotiation, reducing overhead and improving speed compared to TLS 1.2. Its optimized cipher suites provide stronger cryptography with slightly better performance.

Transparent Data Encryption

TDE enhances security by encrypting data at rest, mitigating bypass attacks. The encryption and decryption processes are seamless for authorized database sessions. Data is automatically encrypted before storage and decrypted upon retrieval, presenting plaintext to authorized users and applications.

Direct OS or storage access reveals only encrypted data, and backups are encrypted, safeguarding against data theft.

Authorized users continue normal database operations; TDE works in conjunction with existing access control policies, ensuring unauthorized access is denied.



How Hackers can copy files and how encryption thwarts attacks

TDE's Two-Tier Key Architecture

Encryption security hinges on key secrecy. TDE employs a two-tier key system: a master encryption key (MEK) for the database and unique data encryption keys (DEKs) for tablespaces or tables. This architecture, mandated by regulations like PCI-DSS, ensures key separation and facilitates secure key rotation and archiving, crucial for protecting encrypted data.

Encrypt Data-at-rest Using Transparent Data Encryption

Encryption is clearly an important and affective data protection technique. One of the challenges to organizations while implementing data encryption is ensuring that not only is the data in tables encrypted, but also in backups. Locating and encrypting data from all these sources can be a resource-intensive task.

MySQL Transparent Data Encryption (TDE) addresses this challenge by encrypting the data in InnoDB tablespaces, redo, and undo logs, as well as MySQL Enterprise Audit Logs directly in the source (database layer). TDE encrypts data automatically when written to storage including backups. Encrypted data is correspondingly decrypted automatically when read from storage. This automatic encryption-decryption capability at the database layer makes the solution transparent to database applications. Access controls that are enforced at the database and application layers remain in effect. SQL queries are never altered, and hence no application code or configuration changes are required. MySQL Enterprise Edition comes pre-installed with TDE and can be enabled easily.

Another concern when encrypting data is the performance impact on database and application operations. The encryption and decryption process are fast as TDE leverages

MySQL Database caching optimizations and utilizes CPU-based hardware acceleration available on various chipsets.

Centrally Manage Encryption Keys Using Key Vaults

Centralization helps controllers enforce same security controls everywhere and be able to take immediate and quick actions in case of a breach. Key Managers such as Oracle Key Vault (OKV) or other Key Vaults supporting KMIP protocol provide centralized control over data encrypted with Transparent Data Encryption (TDE). TDE provides two-tier encryption key management with data encryption keys and master encryption keys. The master encryption keys can be centrally controlled and managed using Key Vaults. Key Vaults provide the ability to suspend access to the master key and render the encrypted data unintelligible in the event of a data breach or suspicious activity. Smaller organizations with few servers may wish to also review use of the MySQL Encrypted Keyring file or other options for key protection.

Oracle's OKV is a software appliance that enables users to quickly deploy encryption and other security solutions by centrally managing not only MySQL encryption keys, but much more - Oracle wallets, Java key stores, application keys, credential files, etc. MySQL supports various key vaults – whether Oasis KMIP complaint or accessible via HTTPS protocols.

Oasis KMIP protocol implementations:

- Oracle Key Vault
- Gemalto KeySecure
- Thales Vormetric Key Management Server
- Fornetix Key Orchestration
- Townsend Alliance Key Manager
- Entrust KeyControl

MySQL Enterprise TDE also supports HTTPS based APIs for Key Management such as:

- Oracle Cloud Infrastructure Vault
- Hashicorp Vault
- AWS KMS

Importance of Database Activity Monitoring

Database activity monitoring is crucial for detecting malicious behavior, ensuring regulatory compliance, and supporting incident investigations. Audit trails provide essential records for accountability and security.

Key benefits include:

- Malicious activity detection and investigation.
- Deterring misconduct.
- Non-repudiation (proof of actions).
- Regulatory compliance auditing.
- Monitoring privileged user activity (DBAs, analysts).
- Troubleshooting connection issues.
- Data recovery assistance.

Prioritize Effective Activity Monitoring

While conceptually simple, effective database activity monitoring requires understanding its capabilities and options to avoid performance impacts and excessive management overhead. Organizational security mandates auditing privileged user activity, login events, and sensitive data access. The aim is to capture essential data while minimizing disruption to database operations.

Strategic Database Auditing

Auditing all database activity is impractical due to storage costs, performance impacts, and the risk of obscuring malicious events. Instead, implement selective audit policies focused on significant events.

Effective policies prioritize:

- Security-relevant events
- Privileged user activity
- Sensitive Data Access

This approach minimizes unnecessary audit records, enabling faster and more reliable threat detection, while ignoring routine activity from trusted sources.

Effective Audit Data Management & Utilization

Collecting audit data is insufficient; it must be actively used. Centralized repositories are crucial for managing audit data from numerous databases, enabling analysis, alerting, and reporting. Solutions like Oracle Data Safe and AVDF consolidate audit data, offering features like:

- Centralized, secure repository.
- Near real-time monitoring and alerting.
- Security and compliance reporting.
- Forensic analysis support.
- Historical data storage and retrieval.
- User privilege change tracking.
- Compliance demonstration for auditors.

Audit data management involves:

- Controlling storage consumption.
- Protecting data integrity.
- Meeting retention requirements.

Fortunately, MySQL Enterprise Edition audits provide storage size limits, data encryption for data integrity, and retention policies.

Centralization allows for data removal from source databases and implements lifecycle policies.

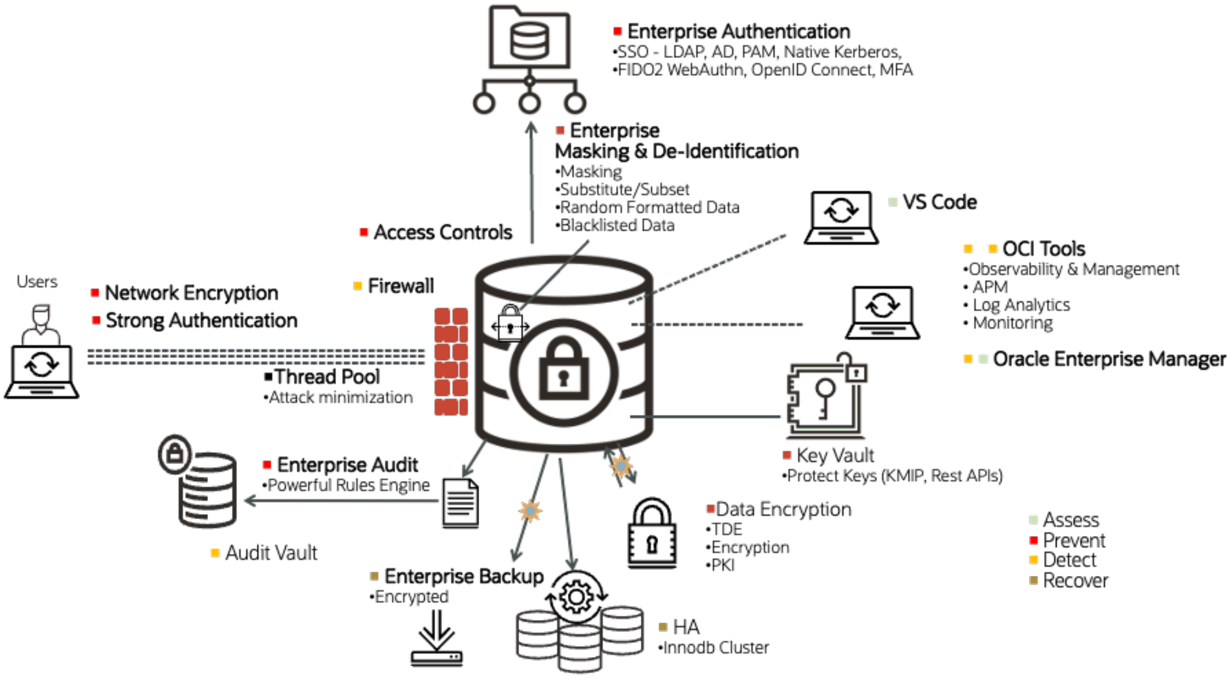
Effective utilization includes:

- Anomaly detection.
- Compliance audits.
- Troubleshooting.

Centralized repositories such as Oracle Audit Vault, OCI Log Analytics, and others - facilitate forensic analysis, alerting, and reporting, supporting regulatory compliance (GDPR, CCPA, PCI-DSS, HIPAA, etc.) by providing access records and retention management.

Putting it All Together - MySQL Reference Architectures for Security

By applying the defense-in-depth strategies outlined in this guide, you can establish MySQL Reference Architectures for Security, ensuring robust data protection and risk mitigation for your MySQL Databases.

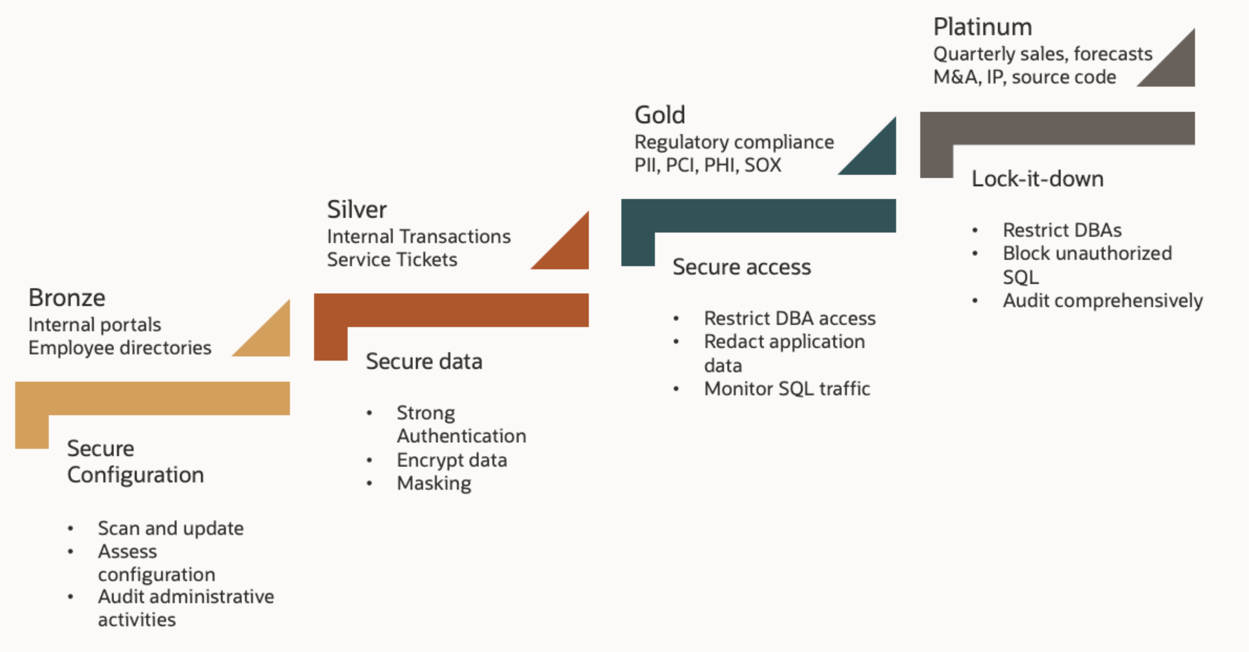


MySQL Enterprise Security Overview

Tailored Security Implementation

Implement security controls based on data sensitivity, business criticality, and threat environment. Categorize systems (Bronze, Silver, Gold, Platinum) by sensitivity. Bronze: internal portals. Silver: business transactions. Gold: regulated data (GDPR, CCPA, etc.). Platinum: highly sensitive data (sales forecasts, IP).

Apply layered controls per category. All levels require secure configuration and patching to prevent breaches. Monitor privileged user activity across all systems.



MySQL Reference Architectures for Security

Tiered Security Measures for Data Protection

Each level is additive from Bronze up to Platinum.

- **Bronze Databases:** Require robust security configurations and timely security patching. Failure to maintain these standards exposes the system to vulnerabilities, potentially allowing attackers to establish command-and-control or use it as a staging area for data exfiltration. Furthermore, comprehensive monitoring and auditing of privileged user activities are essential to detect unauthorized configuration changes or privilege escalations.

- **Silver Databases:** Implement network encryption, OS-level data protection, and secure non-production environments. Enforce strong authentication, encryption (in transit and at rest), and data masking.

- **Gold Databases:** Add privileged user access restrictions, SQL activity monitoring, and PII/PCI/PHI data protection.

- **Platinum Databases:** Apply all Gold controls, plus server access restrictions, real-time SQL monitoring, SQL injection prevention, and comprehensive audit policies for forensic analysis.

Implementation can be control-focused (global application) or system-focused (critical systems first), or a hybrid approach. Develop a strategy aligning with business objectives, resources, and time to optimize security investments.

Conclusion

To effectively safeguard our assets, a strategic approach is required. This strategy must integrate business goals, available resources, and realistic timelines. By doing so, we can implement appropriate security measures for all data, ensuring a strong return on our security investment.

Additional Resources

MySQL Enterprise Edition : Product Information
http://www.mysql.com/products/enterprise

MySQL Enterprise Edition: Documentation
https://dev.mysql.com/doc/index-enterprise.html

MySQL Customers and Case Studies
http://www.mysql.com/customers