



ORACLE

Security and Compliance with MySQL Enterprise Edition

Protect your data and business



Recent Data Breach Statistics

7.9 billion

records stolen in 2019, up by 33%

1.76 billion

records leaked in January 2020

48%

of breaches are malicious attacks

\$3.86 million

average cost of a data breach

7 out of 10

businesses not prepared to react

\$2 trillion

global cost of cybercrime in 2020

Data: Your Most Valuable Asset

In today's digital world, data is your organization's single most valuable asset.

Data is about your customers, employees, and partners. Data is about your IP, mergers and acquisitions, strategy, and sales figures.

The data might be generated by your organization or it might have been entrusted to you, such as PII (Personally Identifiable Information), PCI (Payment Card), or PHI (Personal Health Information) data.

Your data presents a great value for thieves, state sponsored criminals and malicious insiders who will do anything to get their hands onto it.



Top Investment Priorities for CIOs

1. Security
2. People/Talent
3. Digital Transformation
4. Analytics/BI/AI
5. Cloud
6. Improve Applications & Infrastructure
7. Low Code/No Code
8. Business/IT Continuity
9. Application Upgrades
10. Getting More Value from Investments

CIOs have one of the hardest C-level jobs. Technology has become the backbone to organization's efficiency, communication, security, and ultimately profitability.

Source: CIO from IDG, Top Priorities for CIOs in 2019

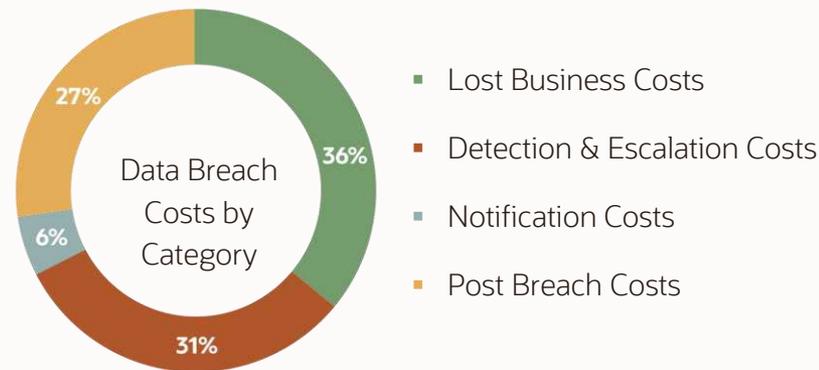


Costs of a Security Breach

Data breaches continue to cost more and result in more consumer records being lost or stolen.

In the first half of 2019 there were 3,800 publicly disclosed data breaches. More than 4.1 billion records were exposed. A data breach involving more than one million compromised records is referred to as a mega breach.

A mega breach of 10 million records reaches an average total cost of \$163 million, while a breach of 50 million records yields an average total cost of \$350 million.



The following factors contribute to these costs:

- Loss of company reputation.
- Business loss: revenue loss, business disruption, system downtime, new customer acquisition.
- Detection and escalation costs: forensics and auditing services that enable a company to detect and report the breach.
- Notification costs: activities that allow the company to notify individuals who had their data compromised in the breach, as well as communication with regulators.
- Post data breach costs: activities to help customers communicate with the company, legal costs and regulatory fines.

Source: Experian Data Breach Industry Forecast 2020



Enterprise Security

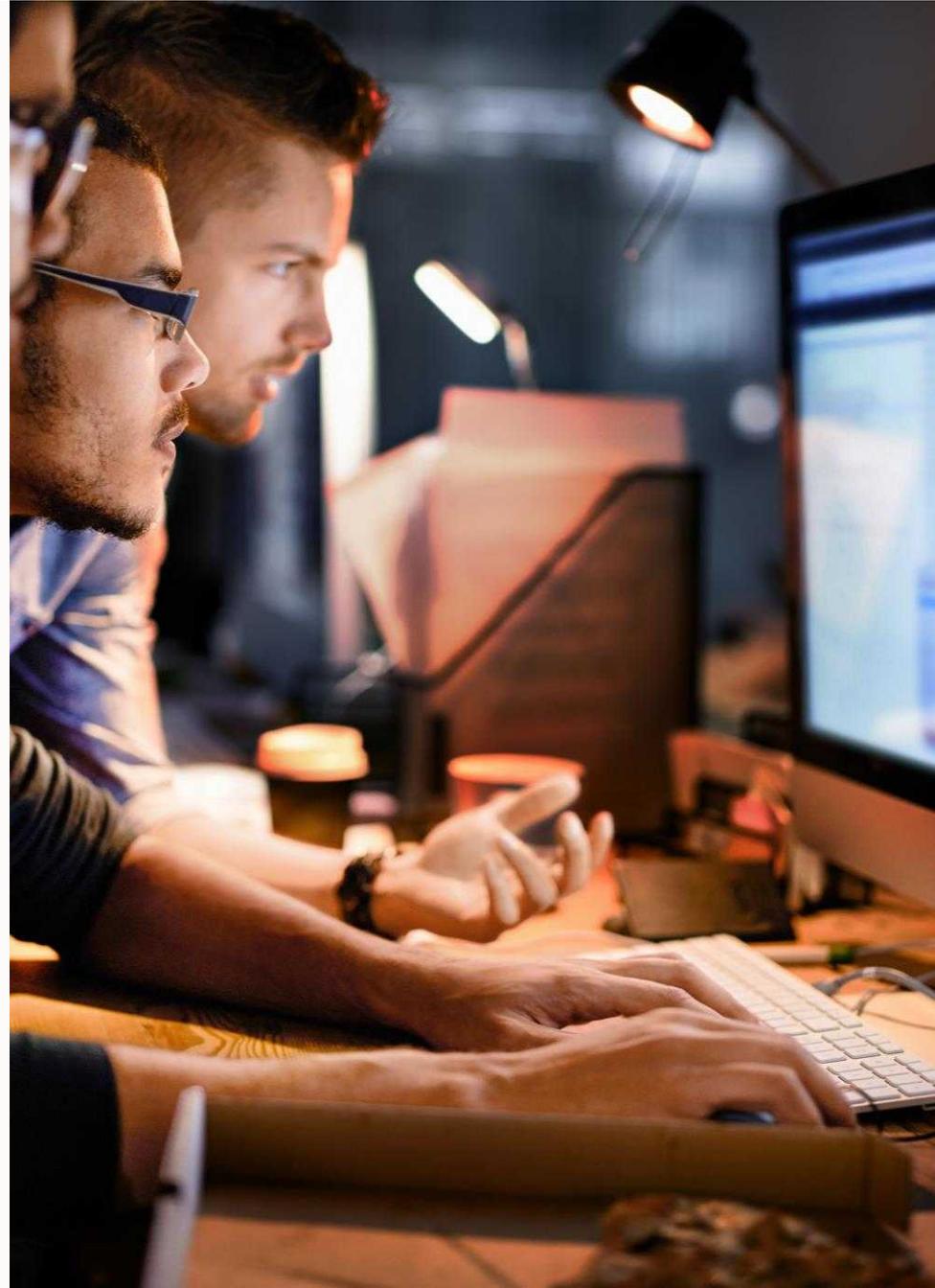
Information technology has disrupted entertainment, media, retail, finance, banking, insurance and, recently, the hospitality and the transportation industries.

Everyday billions of logins, forms and payments contribute to the existing pile of confidential data stored on enterprise servers. If that information is entrusted to your organization, do you know how to make it secure?

Enterprise security is the number and quality of tools and processes a company employs to protect its properties, such as applications and databases, from breach of integrity.

It includes guidelines that determine how employees interact with data and keep their workstations safe, as well as policies and procedures that IT should implement to keep everyone's data secure.

Effective enterprise security programs protect the organization's data from theft or unlawful distribution, empowering the enterprise to execute its mission despite malicious intent of bad actors and criminal activity.



Regulatory Compliance

To protect sensitive data and privacy of personal information, governments and industry organizations have developed multiple privacy regulations and data protection laws.

The main data protection and privacy laws include:

GDPR (General Data Protection Regulation): A wide ranging data protection and privacy regulation covering the European Union (EU). It also addresses the transfer of personal data outside the EU areas.

PCI DSS (Payment Card Industry Data Security Standard): A data security standard for organizations that handle credit card transactions. Merchants accepting credit cards must comply with PCI DSS.

HIPAA (Health Insurance Portability and Accountability Act): A federal law in the United States that sets a national standard for healthcare providers to protect personal and health information stored in medical records.



Regulatory Compliance (cont.)

Over 100 countries have adopted data protection laws that often include multiple regulations for different industries.

Multiple regulations exist within countries that organization must comply with. For example, in the USA, every state has created its own consumer protection law, such as the California Consumer Privacy Act (CCPA).

Government Agencies at the federal, state, and local levels have their own privacy and security standards to comply with. Some of them include:

STIG (Security Technical Implementation Guide):
Department of Defense organizations in the United States must comply with STIG configuration standards. The STIGs specify how IT assets should be configured in order to be secure. In the case of databases, this includes authorizing accounts and privilege management.

NIST (National Institute of Standards and Technology):
Provides the set of standards for protecting data of federal agencies. NIST guidelines also help agencies meet specific regulatory compliance requirements such as HIPAA.

FedRAMP (Federal Risk and Authorization Management Program): A government-wide program that provides a set of security standards for cloud products and services.

FIPS (Federal Information Processing Standards):
Defines a set of standards around encryption and cryptography for the use within non-military government agencies.

Complying with this patchwork of laws and regulations can be a very difficult task for any organization.



Five Steps to Regulatory Compliance

Even though many Data Protection Laws and Industry Regulations are separate laws, they all share common requirements.

Let's have a look at five steps that you can take to secure your sensitive data. That's how MySQL Enterprise Edition will help you protect your sensitive information and be compliant:

1. **Assess Security Risks:** Identify sensitive data such as Personally Identifiable Information and vulnerable configurations.
2. **Manage User Privileges and Restrict Access to Sensitive Data:** Grant access to data only on a need-to-know basis. Authenticate users with strong passwords.
3. **Protect Development and Test Data:** Organizations can reduce the risk of a data breach by masking sensitive or confidential application data, so it can be used in non-production systems.
4. **Encrypt Sensitive Data:** Implement a mechanism to encrypt your data so if data is stolen, it can't be read.

5. **Detect Database Activity:** Detect and stop malicious database activity in case of a breach to determine what information was stolen and by whom, which is legally required to be reported to regulators.



Security Features of MySQL Enterprise Edition

As companies expand their digital footprint with critical workloads, users, applications, data and infrastructure, it becomes critical to go beyond individual best practices to proofing your datacenter by adopting enterprise security for your MySQL environment.

MySQL Enterprise Edition includes the most comprehensive set of advanced features, management tools, and technical support to achieve the highest levels of MySQL scalability, security, reliability and uptime.

MySQL Enterprise Edition reduces risk, cost and complexity in developing, deploying and managing critical MySQL applications.

Only MySQL Enterprise Edition allows you to:

- Encrypt the physical files of the database using MySQL Enterprise Transparent Data Encryption.
- Protect sensitive data in transit using encryption, key generation and digital signatures with MySQL Enterprise Encryption.
- Anonymize personal data for development and testing using MySQL Masking and De-identification.
- Leverage existing, centralized security infrastructures with MySQL Enterprise Authentication.
- Block SQL injection attacks that can result in loss of valuable personal and financial data using MySQL Enterprise Firewall.
- Add policy-based auditing compliance of existing MySQL applications using MySQL Enterprise Audit.
- Identify security vulnerabilities including at-risk configurations, privileges and passwords using MySQL Enterprise Monitor.
- Reduce risk of data loss with MySQL Enterprise Backup for hot backup and recovery backup encryption.



MySQL Security Architecture



Assess

- MySQL Enterprise Monitor

Prevent

- MySQL Enterprise Authentication
- MySQL Enterprise Firewall
- MySQL Enterprise Encryption
- MySQL Enterprise Data Masking

Detect

- MySQL Enterprise Audit

Recover

- MySQL Enterprise HA
- MySQL Enterprise Backup

MySQL Roles

MySQL Roles improves the security of your data and simplifies database privilege management.

Database applications have multiple users with the same set of privileges. Granting and revoking privileges to individual users is time consuming and error prone.

MySQL Roles allow you to assign permissions to a role or group of users, instead of to individual users enabling your DBAs to be more productive and enforce account privilege policies.

All the major industry and government security regulations such as GDPR, PCI and HIPAA, require organizations to analyze user privileges in order to prevent unauthorized access to their sensitive data.

In fact, they require organizations to follow the principle of least privilege (POLP), the practice of limiting user access rights to the minimum, granting only the permissions they need to perform their work.

Using MySQL Roles, DBAs will easily implement this policy and reduce the risk of rogue accounts with excessive privileges.



MySQL Passwords

MySQL has a powerful password management system that enables organizations to protect their sensitive data in order to comply with industry and government security regulations.

Using MySQL, DBAs can implement strong password policies and best practices, such as:

- Password expiration to require passwords to be changed periodically.
- Password reuse restrictions to prevent old passwords from being chosen again.
- Password verification to require an entry of a current password in order to create a new one.
- Dual passwords to enable clients to connect using either a primary or secondary password.
- Password strength assessment to require strong passwords.
- Random password generation as an alternative to requiring explicit administrator-specified literal passwords.
- Password failure tracking to enable temporary account locking after multiple consecutive password login failures.



MySQL Authentication

MySQL Enterprise Edition provides ready-to-use external authentication modules to integrate existing security infrastructures, including Linux Pluggable Authentication Modules (PAM) and Windows Active Directory.

By authenticating MySQL users from centralized directories, organizations can use the same usernames, passwords and permissions for MySQL across their entire infrastructure.

This makes MySQL DBAs more productive by eliminating the need to manage credentials in individual systems. It also makes IT infrastructures more secure by leveraging existing security rules and processes.

MySQL users can be authenticated using PAM or native Windows OS services.

- ✓ MySQL External Authentication for PAM: Use Linux Pluggable Authentication Modules (PAMs) to authenticate users for various authentication methods, such as Linux passwords or an LDAP directory.
- ✓ MySQL External Authentication for Windows: Use native Windows services to authenticate client connections. Users who have logged into Windows can connect to the server from MySQL client programs based on the token information in their environment, without entering an additional password.
- ✓ MySQL External Authentication for LDAP: Authenticate users via Lightweight Directory Access Protocol servers. Users or groups of users can be defined through LDAP specifications. Both SASL authentication and username/password authentication are supported.

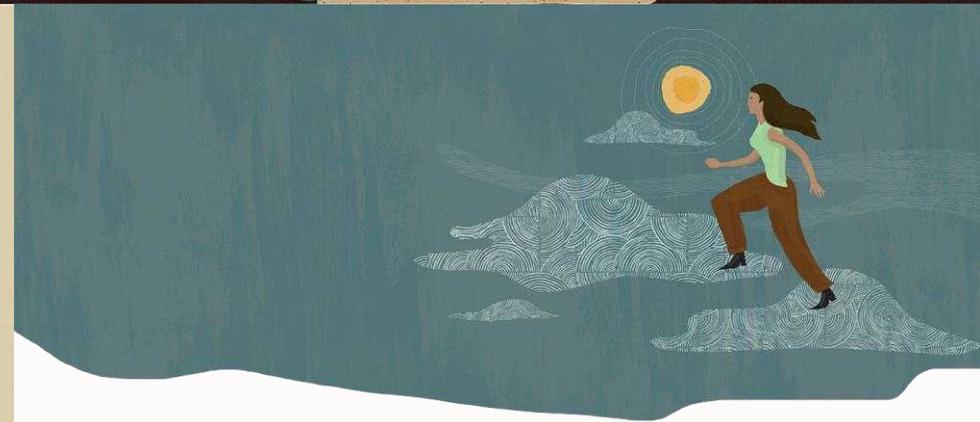


Transparent Data Encryption TDE

To protect sensitive data throughout its lifecycle, MySQL Enterprise Encryption provides industry standard functionality for asymmetric encryption (Public Key Cryptography).

MySQL Enterprise Transparent Data Encryption (TDE) protects your critical data by enabling data-at-rest encryption in the database. It protects the privacy of your information, prevents data breaches, and helps meet regulatory requirements, including:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- California Consumer Protection Act (CCPA)



MySQL Enterprise Transparent Data Encryption allows you to:

- Secure data using combination of public, private, and symmetric keys to encrypt and decrypt data.
- Encrypt data stored in MySQL using RSA, DSA or DH encryption algorithms.
- Digitally sign messages to confirm the authenticity of the sender and message integrity.
- Eliminate unnecessary exposure to data by enabling database administrators for encrypted data management.
- Interoperate with other cryptographic systems and appliances without adjusting existing applications.
- Avoid exposure of asymmetric keys within client applications or on disk.



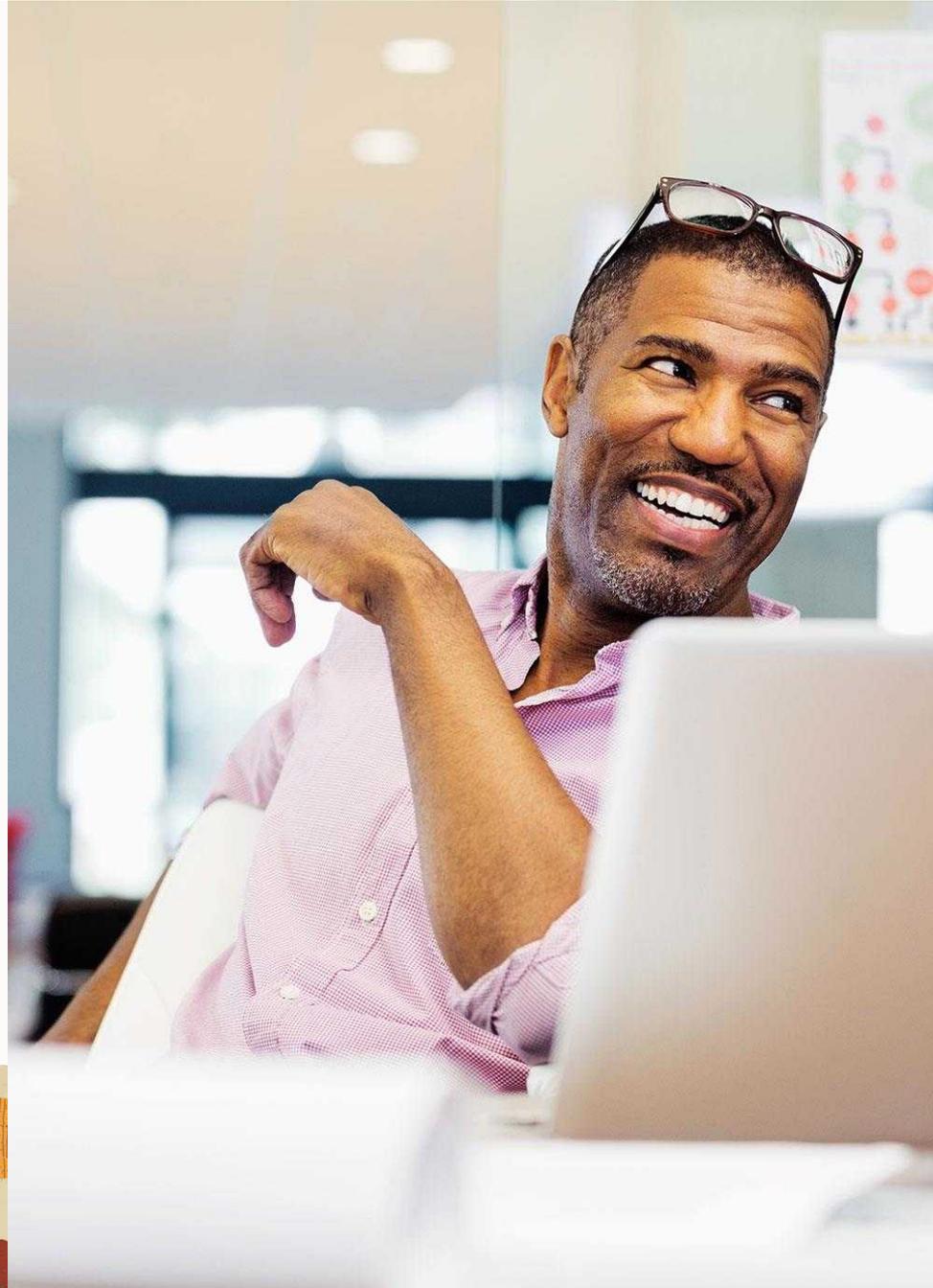
MySQL Enterprise Firewall

MySQL Enterprise Firewall is an application-level firewall that enables DBAs to permit or deny SQL statement execution by matching against whitelists of accepted statement patterns.

Acting as an intrusion detection system, MySQL Enterprise Firewall notifies administrators about SQL statements that do not match an approved whitelist.

This process strengthens MySQL Server to withstand attacks such as SQL injections or attempts to exploit applications by using them outside of legitimate query workload characteristics.

Each MySQL account registered with the firewall has its own statement whitelist, enabling protection to be tailored. The firewall records the accepted statement patterns and protects against unacceptable statements.



MySQL Enterprise Audit

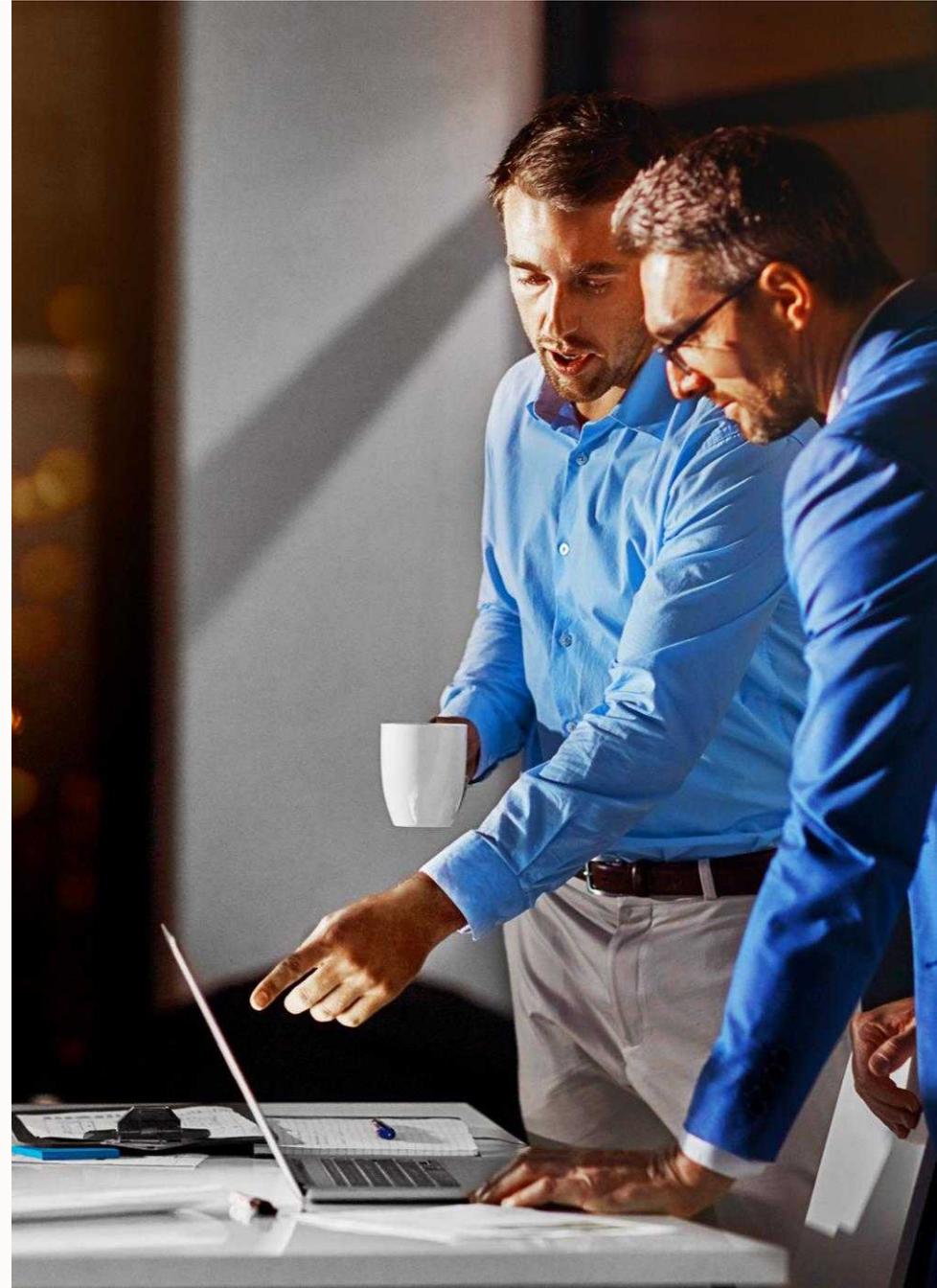
Designed to meet the Oracle audit specification, MySQL Enterprise Audit provides an out-of-the-box and easy-to-use auditing and compliance solution for applications that are governed by internal and external regulatory guidelines.

MySQL Enterprise Audit uses the open MySQL Audit API for policy-based monitoring of user connections and queries on specific MySQL servers.

MySQL Enterprise Audit enables you to quickly and seamlessly add policy-based auditing compliance to existing applications.

You can dynamically log user activity, implement activity-based policies, manage audit log files and integrate MySQL auditing with Oracle and third-party solutions.

When installed, the audit plugin enables MySQL Server to produce a log file containing an audit record of server activity. The log content shows when clients connect and disconnect and what actions they perform, such as accessing specific databases and tables.





Conclusion

Data is an organization's most valuable asset. Securing that data is a top priority for CIOs.

Personal Identifiable Information, sales data, intellectual property, and corporate strategy information is valuable to identity thieves, competitors, malicious insiders, and state sponsored criminals. As a result, data breaches continue to dominate news headlines and costs soar.

More than 100 countries have adopted data privacy and data protection laws such as GDPR. Industry regulations, including PCI and HIPAA, have their own data protection requirements. Companies that are out of compliance can face hefty fines.

MySQL delivers a powerful suite of products to help companies defend themselves against the risk of a data breach and comply with regulations. These can be grouped into four categories:

- **Assess:** MySQL Enterprise Monitor helps identify security vulnerabilities such as weak password policies.
- **Prevent:** Multiple tools to create a resilient database infrastructure and implement the appropriate safeguards such as encrypting data at rest and in motion.
- **Detect:** MySQL Enterprise Audit helps organizations to identify who accessed what information to aid in the timely discovery of cybersecurity events.
- **Recover:** MySQL Enterprise High Availability and MySQL Enterprise Backup helps companies to recover and reduce the impact of a cybersecurity event.

MySQL Enterprise Edition provides support for your organization's most value asset and helps maintain your customers' trust.





[Chat with the MySQL team](#)

[Talk to a MySQL sales representative](#)

[Book a MySQL Solution Architect to optimize your database](#)

[Buy MySQL subscriptions, licenses, support, and training from the Oracle store](#)

