MongoDB Queryable Encryption

Perform expressive queries directly on encrypted data while ensuring robust data protection and enhanced regulatory compliance.

End-to-End Data Protection

Data protection is essential for every organization. With the increasing complexity and volume of data being stored across diverse environments, safeguarding sensitive information—whether it resides in the cloud, on-premises, or elsewhere—has become more critical than ever. In order to implement robust data protection, organizations must ensure data encryption at all stages: in transit, at rest, and in use.

Data can be protected through encryption in-transit when traveling over networks, at-rest when stored, and in-use when it is being processed. In-use encryption is important for data privacy and regulatory compliance, but working with encrypted data in-use poses significant challenges because it usually needs to be decrypted before it can be processed. Historically, organizations have resorted to less secure workarounds or complex, custom encryption solutions to keep their data encrypted throughout its entire lifecycle, introducing operational complexity and costs.

MongoDB Queryable Encryption

With Queryable Encryption, a first-of-its-kind in-use encryption technology, MongoDB helps organizations protect their sensitive data when it is queried and in use. It allows applications to encrypt sensitive data on the client side, securely store it in the MongoDB database, and perform equality and range queries directly on the encrypted data.

MongoDB Queryable Encryption

Queryable Encryption was developed by the MongoDB Cryptography Research Group, drawing on their decades of pioneering expertise in cryptography and encrypted search, and has been peer-reviewed by leading cryptography experts worldwide. Unmatched in the industry, MongoDB is the only data platform that allows customers to run expressive queries directly on non-deterministically encrypted data. This represents a groundbreaking advantage for customers, allowing them to maintain robust protection for their sensitive data without sacrificing operational efficiency or developer productivity by still enabling expressive queries to be performed on it.

Stronger Data Protection

With Queryable Encryption, data stays encrypted at every stage—whether in-transit, at-rest, or in-use. This greatly reduces the risk of sensitive data exposure and breaches without sacrificing operational efficiency.

Enhanced Regulatory Compliance

Encryption is a crucial tool for organizations to comply with data protection regulations like GDPR and HIPAA. However, encrypting data only in-transit and at-rest isn't enough. To achieve full compliance, you must also encrypt data in use. Queryable Encryption offers a unique solution that makes this possible.

Streamlined Operations

Streamlined Operations: With Queryable Encryption, your organization can avoid the need for costly custom encryption solutions, specialized cryptography teams, or complex third-party tools, simplifying their operations.

Solidified Separation of Duties

Ensure stronger security and minimize risks by limiting who can access sensitive data. With Queryable Encryption, you can enforce separation of duties, preventing any single individual from having excessive control while maintaining strict access controls over who can query your encrypted data.

Resources

For more information on Queryable Encryption, refer to these resources:

- Visit the MongoDB Data Encryption web page
- Read the Queryable Encryption documentation
- Visit the MongoDB Cryptography Research Group webpage
- Read the Queryable Encryption Technical Paper