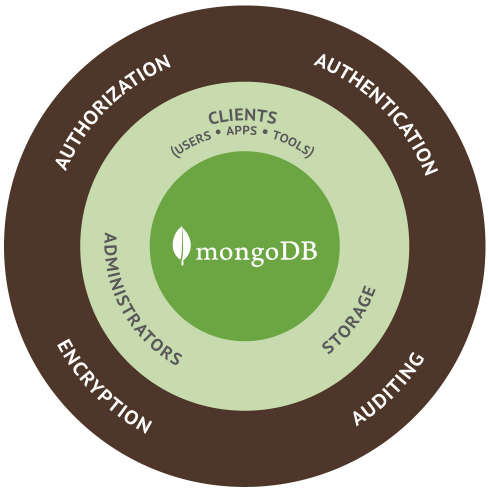
mongoDB

Leading Security for Compliance & Data Protection

Data security and privacy is a critical concern in today's connected world. Data analyzed from new sources such as social media, logs, mobile devices and sensor networks has become as sensitive as traditional transaction data generated by back-office systems.

For this reason, big data technologies must evolve to meet the regulatory compliance standards demanded by industry and government.



MongoDB Subscriptions feature extensive capabilities to defend, detect and control access to online big data with the most complete security controls of any NoSQL database.

- **User Rights Management**. Control access to sensitive data using industry standard mechanisms for authentication and authorization, including field-level redaction implemented by a redaction stage to the MongoDB Aggregation Pipeline.
- **Auditing**. Ensure regulatory and internal compliance.
- **Encryption**. Protect data in motion over the network and at rest in persistent storage.
- **Administrative controls**, including monitoring and backup.

Authentication

Authentication can be managed from within the database itself or via MongoDB Enterprise integration with external security mechanisms including LDAP, Windows Active Directory, Kerberos and x.509 certificates.

Authorization

MongoDB allows administrators to define permissions for an user or application, and what data it can see when querying the database. MongoDB has a number of built-in roles, along with the ability to configure granular user-defined roles. This makes it possible to realize a separation of duties between different entities accessing and managing the database.

Additionally, MongoDB offers field-level redaction as a critical building block for trusted systems. By redacting data at the document or field level, a single record can contain data with multiple security levels, avoiding the complexity of separating data across multiple databases.

Auditing

Security Administrators can use MongoDB's native audit log to track access and administrative actions taken against the database, with events written to the console, syslog or a file. The DBA can then merge these events into a single log, enabling a cluster-wide view of operations that affected multiple nodes.

Encryption

MongoDB data can be encrypted on the network and on disk.

Support for SSL allows clients to connect to MongoDB over an encrypted channel. MongoDB supports FIPS 140-2 encryption when run in FIPS Mode with a FIPS validated Cryptographic module.

Data at rest can be protected using either certified database encryption solutions from MongoDB partners such as IBM and Gazzang, or within the application itself.

Monitoring and Backup

Database monitoring and backup are critical in identifying and protecting against potential exploits, reducing the impact of any attempted breach. The MongoDB Management Service (MMS) is delivered as a free, cloud-based monitoring and backup service and is also available as an on-premise solution as part of the MongoDB subscription.

MMS users can visualize database performance and set custom alerts that notify when particular metrics are out of normal range. MMS is also the only continuous backup solution for MongoDB, providing point-in-time recovery for replica sets and cluster-wide snapshots of sharded systems.

Resources

For more information, please visit mongodb.com or contact us at sales@mongodb.com.

Resource	Website URL
MongoDB Enterprise Download	mongodb.com/download
Free Online Training	education.mongodb.com
Webinars and Events	mongodb.com/events
White Papers	mongodb.com/white-papers
Case Studies	mongodb.com/customers
Presentations	mongodb.com/presentations
Documentation	docs.mongodb.org