MongoDB Atlas: Security Controls

August 2018

Table of Contents

Overview

Security is a top priority at MongoDB and we understand how important your data is to you and those who depend on you. MongoDB has been entrusted with a significant variety and amount of sensitive application and user data. We do not take our responsibility lightly; we work diligently to continuously improve security processes and controls, as well as provide our customers the right features to secure data as necessary.

MongoDB handles data with the utmost care and integrity, designing our systems to reduce the chance of errors from human factors, employing industry standard information security best practices and continuously testing to find and fix vulnerabilities, amongst other things. Whether it's encrypting your data from end to end and at-rest, or providing you with important access control features, we want customers to have confidence in the systems and services handling sensitive workloads as they are transported, processed and stored.

We believe transparency in security processes and controls is essential. We frequently get asked to document our security controls and standards for MongoDB Atlas. For users of Cloud Services, it is imperative to know who can access data when, and what controls prevent unauthorized access. These are the same concerns that MongoDB Inc. has with any of our vendors. We're hopeful this document provides clarity on MongoDB's security controls by providing you a more detailed understanding of MongoDB Atlas Security Controls and Features as well as a deeper view into the cloud automation behind the scenes.

Introduction

What is MongoDB Atlas?

MongoDB Atlas is a database-as-a-service (DBaaS) created by the experts who design and engineer MongoDB. With MongoDB Atlas, MongoDB Inc. helps customers by managing the underlying systems, operations, and infrastructure components that make up Atlas, allowing customers to focus on their applications instead of database systems.

While this document is focused on Security Features for MongoDB Atlas, if you would like more information about MongoDB Atlas overall, please see our FAQ.

Security Overview

This document is separated into five sections. The following sections will provide details in various areas.

- **Data Storage and Access Controls** discusses where your data is stored (physically and logically), data encryption and how we prevent unauthorized access.
- **MongoDB Atlas: Customer's Security Controls** describes what options you as a customer can configure for your security needs.
- **MongoDB Atlas: Infrastructure and Application Security** describe security controls pertaining to the MongoDB Atlas Application, its development and its underlying infrastructure.
- **Cloud Services Compliance** describes the set of compliance offerings of MongoDB Atlas.
- **Information Security Program Overview** describes MongoDB Inc.'s Information Security program and policies.

Data Storage and Access Controls

Data Centers and Physical Storage

MongoDB Atlas is built atop of Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Amazon Web Services

Customer data is stored in MongoDB Atlas Systems; these systems are single-tenant dedicated AWS EC2 virtual servers that are created solely for an Atlas Customer. These virtual servers are isolated within their own VPC and do not share logical data storage or processing with other customers.

Amazon AWS data centers are compliant with a number of physical security and information security standards. Please visit AWS's Compliance page if more detail regarding physical security is required.

Please note: MongoDB Atlas customers deploying M0, M2, and M5 instances will use a multi-tenant system.

Microsoft Azure

Customer data is stored in MongoDB Atlas Systems; these systems are single-tenant dedicated Microsoft Azure Virtual Machines that are created solely for an Atlas Customer. These virtual servers are isolated within their own VNET and do not share logical data storage or processing with other customers.

Microsoft Azure data centers are compliant with a number of physical security and information security standards. Please visit Microsoft's Compliance website if more detail regarding physical security is required.

Please note: MongoDB Atlas customers deploying M2, and M5 instance sizes will use a multi-tenant system.

Google Cloud Platform

Customer data is stored in MongoDB Atlas Systems; these systems are single-tenant dedicated GCP virtual machine instances that are created solely for an Atlas Customer. These virtual servers are isolated within their own Virtual Private Cloud (VPC) and do not share logical data storage or processing with other customers.

Google Cloud Platform data centers are compliant with a number of physical security and information security standards. Please visit Google's Compliance website if more detail regarding physical security is required.

Please note: MongoDB Atlas customers deploying M0, M2, and M5 instance sizes will use a multi-tenant system.

Region Information

Customers are able to choose which geographical region they wish to store their data in. MongoDB Atlas supports a large number of AWS, Azure, and GCP regions globally; this includes US, EMEA and APAC locations. Please see the FAQ for a full list of region availability.

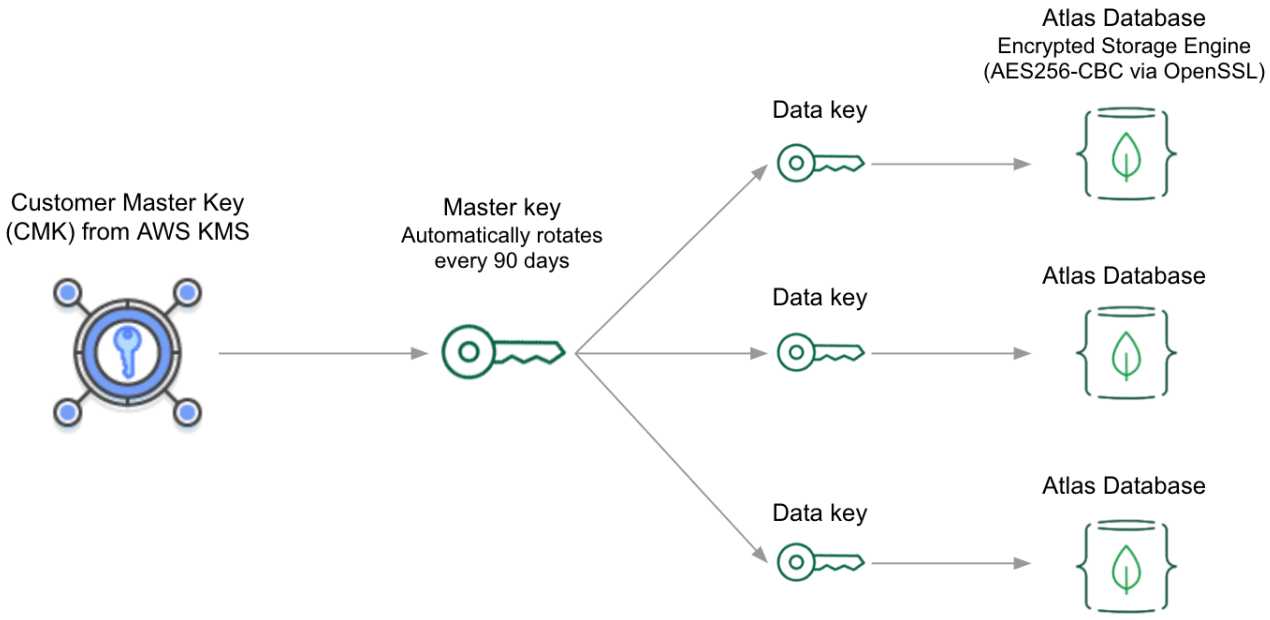

Figure 1: Envelope encryption using encryption key management in MongoDB Atlas

Encryption in Transit and At-Rest

TLS/SSL and authentication (SCRAM) is enabled by default and cannot be disabled. Traffic from clients to Atlas is authenticated and encrypted in-transit, and traffic between the customer's internally managed MongoDB nodes is also authenticated and encrypted in-transit using TLS/SSL. Administrators can control the TLS version required for their database clusters (e.g. requiring TLS 1.2), with TLS 1.1 being the default. The MongoDB Security Team continuously monitors the status of transport protocols and requirements are continually updated in order to ensure weak ciphers are deprecated.

Amazon Web Services

Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS.

For an additional level of encryption, MongoDB Atlas integrates with your AWS Key Management Service (KMS) in your AWS account, allowing you to centralize control of the keys used to encrypt your data and backups. When encryption key management is enabled, MongoDB Atlas will use MongoDB's encrypted storage engine (AES256-CBC via OpenSSL) for database-level encryption, and your AWS customer master key (CMK) to encrypt and decrypt your MongoDB master keys, which are used to encrypt your database keys. Atlas automatically rotates your MongoDB master keys every ninety days while you will control the ability to create, import, and rotate your CMK as well as define usage policies and audit usage with the same console / CLI used to manage keys for your other cloud services.

Microsoft Azure

Encryption for data at rest is automated using Azure's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by Azure.

Google Cloud Platform

Encryption for data at rest is automated using GCP's transparent disk encryption, which uses Advanced Encryption Standard (AES) algorithm with 256 bit key length, in Galois/Counter Mode (GCM). This is implemented in the BoringSSL library that Google maintains. In addition to the storage system level encryption, data is also encrypted at the storage device

level with AES-256 on solid state drives (SSD), using a separate device-level key (different key than storage level). All keys are fully managed by GCP.

Backup

Continuous backups

MongoDB Atlas provides continuous backups, an optional fully managed backup service using Amazon S3 in the region nearest to the associated database deployment.

The mappings are as follows:

- Databases deployed in the UK backup data to Amazon S3 in the UK
- Databases deployed in Australia backup data to Amazon S3 in Australia
- Databases deployed in Germany backup data to Amazon S3 in Germany
- Databases deployed in the United States backup data to Amazon S3 in the United States
- Databases deployed in Ireland backup data to Amazon S3 in Ireland
- Databases deployed in any other region backup data to Amazon S3 in Ireland

Backup data is protected using server-side encryption. Amazon S3 encrypts backup data at the object level as it writes it to disks in its data centers and decrypts it for you when you restore it. All keys are fully managed by AWS.

Cloud Provider Snapshots

Available for Atlas clusters deployed in Amazon Web Services and Microsoft Azure, cloud provider snapshots use the native snapshot capabilities of the underlying cloud provider. Backups are stored in the same cloud region as the corresponding cluster. For multi-region clusters, snapshots are stored in the cluster's preferred region. All managed snapshots and images are automatically encrypted. If the encryption key management integration with AWS KMS is enabled, your AWS Customer Master Key (CMK) and IAM credentials are required to perform restores of backup snapshots.

If you wish to use MongoDB Atlas Backups and have specific concerns regarding where your data must live, please contact us directly to ensure your compliance needs are met.

MongoDB, Inc. Employee Access

MongoDB engineers will never access customer data, or the systems that store and process customer data, under normal circumstances. In "break glass" reliability situations, customer data can be accessed by appropriate personnel to investigate and restore critical services. MongoDB fully manages underlying systems, which means MongoDB's Site-Reliability-Engineers (SREs) need access to underlying systems for operational health management.

MongoDB uses a combination of technical and logical controls to limit and audit the personnel who access systems with sensitive data. Technical role-based access controls (RBAC) are in place to ensure only the set of MongoDB employees with pre-approved operational roles are granted access to MongoDB Atlas underlying systems.

Access to underlying hosts is restricted solely to MongoDB operational personnel who have been granted express access by senior management to maintain system health. Access to underlying hosts also requires multi-factor authentication and a bastion host. Operational personnel permissions and entitlements are audited on a periodic basis.

MongoDB Atlas: Customer's Security Controls

Database Authentication, Authorization, and User Rights Management

For MongoDB Atlas, we will discuss two components:

- MongoDB Atlas Web UI
- MongoDB Atlas Database Cluster

The MongoDB Atlas Web UI is the web application where your administrators will manage the MongoDB Atlas Cluster, including initial user and permissions setup. The MongoDB Atlas Web UI supports authentication via

username/password and multi-factor authentication. The Web UI does not currently support federated identity, such as SAML.

For the MongoDB Atlas Cluster, authentication is automatically enabled by default via SCRAM to help ensure a secure system out of the box.

MongoDB Atlas allows administrators to define permissions for a user or application, and what data can be accessed when querying MongoDB. MongoDB Atlas provides the ability to provision users with roles specific to a group or database, making it possible to realize a separation of duties between different entities accessing and managing the data.

Administrators can also create temporary MongoDB users, meaning Atlas will delete the user at a specified date. Once Atlas deletes the user, any client or application attempting to authenticate with the user will lose access to the database.

IP Address Whitelisting

By default, your MongoDB Atlas Cluster will have no access from the internet. Each Atlas cluster is deployed within a VPC, and that VPC is configured to allow no inbound access by default.

Customers can configure IP whitelisting to limit what network(s) can connect to their database. Application servers are prevented from accessing the database unless their IP addresses (or a CIDR covering their IP addresses) have been added to the IP whitelist for the appropriate MongoDB Atlas project.

Atlas also supports creating temporary whitelist entries that automatically expire within a user-configurable period.

As a general best practice to reduce attack surface, MongoDB recommends customers only permit IP access to the smallest network segments possible (e.g., individual /32 address), and to avoid overly large CIDR blocks.

VPC Peering

Amazon Web Services only

Many of MongoDB Atlas customers have their applications living within their own AWS account and virtual private cloud. The AWS VPC Peering option allows peering your MongoDB Atlas network to your own VPC network, thereby allowing your encrypted traffic to never traverse the public internet and instead use your internal private network. Additionally, this eliminates the need to whitelist IP addresses. This feature requires that the two connecting VPCs are located in the same AWS region.

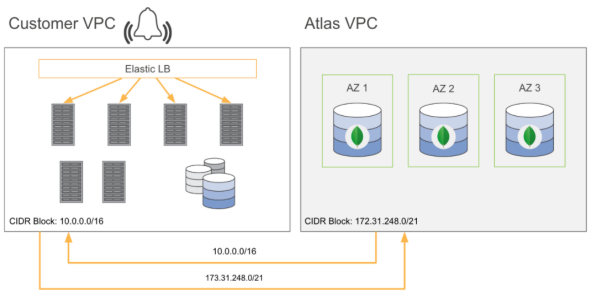

Figure 2: MongoDB Atlas VPC peered to an AWS VPC containing a customer's application servers

Multi-Factor Authentication

For the MongoDB Atlas Web UI, user credentials are stored using industry-standard and audited one-way hashing mechanisms. Additionally, customers can choose to optionally utilize multi-factor authentication, or require all of the users in their Atlas Organization to use multi-factor authentication. Customer sensitive data provided within the GUI, such as passwords, keys, and credentials which must be used as part of the service are stored encrypted.

LDAP Integration

User authentication and authorization against MongoDB Atlas clusters can be managed via a customer's Lightweight Directory Access Protocol (LDAP) server over TLS/SSL. A single LDAP configuration applies to all database clusters within an Atlas project. For customers running their LDAP server in an AWS Virtual Private Cloud (VPC), a peering connection is recommended between that environment and the VPC containing their Atlas databases.

Auditing

Granular database auditing in MongoDB Atlas allows administrators to answer detailed questions about systems activity by tracking all DDL, DML, and DCL commands against the database. Admins can select the actions that they want to audit, as well as the MongoDB users, Atlas roles, and LDAP groups whose actions they wanted audited, right from the Atlas UI. A single auditing configuration applies to all database clusters within an Atlas project. When needed, audit logs can be downloaded in the UI or retrieved using the MongoDB Atlas API.

In addition, the Atlas API allows administrators to audit all events triggered from the Atlas UI at the Project or Organization level.

MongoDB Atlas: Infrastructure and Application Security

Configuration Management

MongoDB Atlas' infrastructure is designed to be fully automated via modern configuration management systems. Reducing human elements increases a security posture by reducing the chance for human error and making audit and alerting standardized. MongoDB Atlas Virtual Machines on GCP use in-house built machine images with hardening applied, and all of our virtual servers are configuration managed using Chef, which includes hardening steps. All systems run with a known set of running processes/components, which in turn is utilized for update/patching.

Network Isolation

MongoDB Atlas customers' data and underlying systems are fully isolated from other customers.

Amazon Web Services

Each customer group is contained in its own Amazon Virtual Private Cloud (VPC) and dedicated firewall (security group). All database clusters associated with a group are deployed inside the associated VPC. MongoDB Atlas instances are provisioned for customers when they create a cluster; each mongod process is deployed to its own AWS EC2 instance.

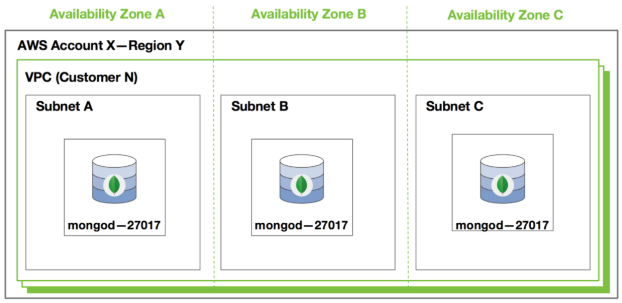

Figure 3: MongoDB Atlas's isolation and dedicated assets on AWS

As shown in the above graphic, the Virtual Private Cloud (VPC) and all assets within each subnet are unique and dedicated per customer and are not shared between customers.

Microsoft Azure

Each customer project is contained in its own Azure VNet and dedicated firewall. All database clusters associated with a project are deployed inside the associated VNet. MongoDB Atlas instances are provisioned for customers when they create a cluster; each mongod process is deployed to its own Azure VM instance.

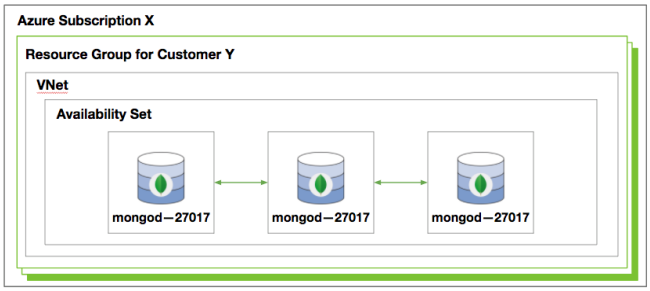

Figure 4: MongoDB Atlas's isolation and dedicated assets on Azure

The above graphic represents MongoDB Atlas's isolation and dedicated assets. VNets are unique to each customer.

Google Cloud Platform

Each customer project is contained in its own Virtual Private Cloud and dedicated firewall. All database clusters

associated with a project are deployed inside the associated VPC. MongoDB Atlas instances are provisioned for customers when they create a cluster; each mongod process is deployed to its own GCP VM instance.

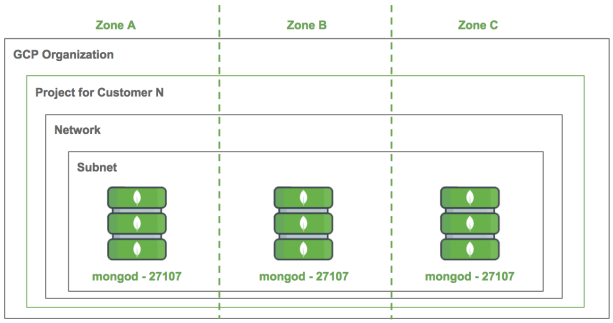

Figure 5: MongoDB Atlas's isolation and dedicated assets on GCP

The above graphic represents MongoDB Atlas's isolation and dedicated assets. VPCs are unique to each customer.

Separation of Production and Non-Production Environments

MongoDB Atlas has strict separation between production and non-production environments. Production and Customer data is never utilized for non-production purposes. Non production environments are utilized for development, testing and staging.

MongoDB Policies require the principle of least privilege and separation of duties. As a result, developers are provided access to developer environments only and production environments are limited to personnel who have an operational need and appropriate authorizations.

Firewalls and Bastion Hosts

MongoDB Atlas infrastructure is only accessible via bastion hosts. Bastion hosts are configured to require SSH keys (not passwords). Bastion hosts also require multi-factor authentication, and users must additionally be approved by senior management for backend access.

High Availability and Failover

With regard to service availability, every MongoDB Atlas cluster is deployed as a self-healing replica set which provides automatic failover in the event of a failure. Replica set members are automatically provisioned by MongoDB Atlas across multiple fault domains within a region, providing resilience to localized site failures. All replica set members are full data bearing nodes, ensuring majority writes in the event of single node failure and higher resilience during recovery.

- For more details about the MongoDB Atlas SLA, please see our SLA page.
- For real time updates for MongoDB Atlas operational status, please see our status page.

Amazon Web Services

MongoDB Atlas supports cross-region deployments on AWS, which can be enabled to provide service availability in the unlikely event that an entire AWS region goes down.

- For more information, please see AWS's regions and availability zones documentation.

Microsoft Azure

MongoDB Atlas supports cross-region deployments on Azure, which can be enabled to provide service availability in the unlikely event that an entire Azure region goes down.

- For more information, please see Azure's regions and availability documentation.

Google Cloud Platform

MongoDB Atlas supports cross-region deployments on GCP, which can be enabled to provide service availability in the unlikely event that an entire GCP region goes down.

- For more information, please see GCP's regions and availability documentation.

Logging and Alerting

MongoDB maintains a centralized log management system for collection, storage and analysis of log data for production environments. This information is used for health monitoring, troubleshooting, and security purposes.

Alerts are configured on systems in order to notify SREs of any operational concerns.

Input Validation

Input validation is done for data submitted to web applications, and verified with manual source code checks and peer reviews, as well as internal and external security team tests. Fuzz testing also is used for core product assessments.

Cloud Services Compliance

SOC

Service Organization Controls (SOC) framework establish a standard for controls that safeguard the confidentiality and privacy of information stored and processed in the cloud. MongoDB Atlas is audited at least annually against the SOC reporting framework by independent third-party auditors. The audit covers controls for data security; the report is available to customers who've signed an NDA with MongoDB, Inc.

EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield is a legal mechanism designed by the U.S. Department of Commerce and the European Commission that enables transfers of personal data from the EU to the United States. MongoDB complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States.

HIPAA

For customers who are subject to the requirements of the Health Insurance Portability and Accountability Act of 1996, MongoDB Atlas supports HIPAA compliance and enables covered entities and their business associates to use a secure MongoDB Atlas environment to process, maintain, and store protected health information. MongoDB, Inc. will enter into Business Associate Agreements covering MongoDB Atlas with customers as necessary under HIPAA.

Information Security Program Overview

Security Program

MongoDB Inc. has a dedicated Information Security Team. This team is responsible for the Information Security program at MongoDB. MongoDB internal security practices and policies are aligned to be compliant with ISO 27002 controls. Program priority is regularly reviewed, and is based upon threat modeling and internal continual capability and maturity assessments.

MongoDB employees are required to take and attest to periodic security training. Additionally the Security Team employs a number of education outreach efforts, such as internal security reading groups, Capture-the-Flag / Hacking Contests to teach developers security issues, hackathons, and more. Internal policies include data classification and handling and specific information regarding handling customer data.

MongoDB has a vulnerability enumeration and management program; this program identifies internet-accessible company assets, scans for known vulnerabilities, evaluates risk and tracks issue remediation. Vulnerability scans occur at least daily, with results reporting to a centralized security dashboard. A central company-wide ticketing system is used to track all security issues until remediation.

Human Resources performs multi-residence criminal background checks on all prospective employees. The HR employee off-boarding processes includes verification of account access termination.

Application Security

MongoDB Atlas undergoes regular reviews from both internal and external security teams. Internally, MongoDB Atlas undergoes periodic risk assessments, which includes technical vulnerability discovery as well as business risks and concerns. Additionally, the MongoDB Security Team is

routinely involved in source code review, architecture review, code commit / peer-review and in security decision making.

Application level security testing uses a standard application assessment methodology (e.g., OWASP). Additionally, external engagements with security consults includes social engineering and phishing testing. A summary of our most recent third-party penetration test is available for customers to review. Systems are patched as needed; security-related patches are applied commensurate to their severity.

Communications and Notifications

MongoDB has an established Incident Response and Critical Communications Policy and associated processes. In the event that a security alert/event, or other signal results in MongoDB declaring a security incident, MongoDB will follow its internal incident response protocols and inform affected customers as soon as practicable. If your organization has very specific breach notification or communications requirements, please contact us directly.

Patching and Change Management

Patching of operating system and applications are performed on a need-to-update basis. MongoDB, Inc. employees utilize automated tooling in conjunction with monitoring security bulletins for relevant software and implement patches if security issues are discovered. The MongoDB server software itself is continuously updated as new versions are released.

With respect to change management, development tasks are defined as issues for specific target releases. A release is deployed to production after it has transitioned through the requisite checkpoints, including testing, staged deployment, and management review. All internal release notes include a QA test plan.

Additional Resources

- MongoDB Security Alerts and Contact
- MongoDB Atlas Best Practices White Paper
- MongoDB Atlas FAQ
- MongoDB Atlas Implementation Details
- MongoDB Security Checklist
- MongoDB Privacy Policy
- MongoDB Atlas SLA

We Can Help

We are the MongoDB experts. Over 6,600 organizations rely on our commercial products. We offer software and services to make your life easier:

MongoDB Enterprise Advanced is the best way to run MongoDB in your data center. It's a finely-tuned package of advanced software, support, certifications, and other services designed for the way you do business.

MongoDB Atlas is a database as a service for MongoDB, letting you focus on apps instead of ops. With MongoDB Atlas, you only pay for what you use with a convenient hourly billing model. With the click of a button, you can scale up and down when you need to, with no downtime, full security, and high performance.

MongoDB Stitch is a serverless platform which accelerates application development with simple, secure access to data and services from the client – getting your apps to market faster while reducing operational costs and effort.

MongoDB Mobile (Beta) MongoDB Mobile lets you store data where you need it, from IoT, iOS, and Android mobile devices to your backend – using a single database and query language.

MongoDB Cloud Manager is a cloud-based tool that helps you manage MongoDB on your own infrastructure. With automated provisioning, fine-grained monitoring, and continuous backups, you get a full management suite that reduces operational overhead, while maintaining full control over your databases.

MongoDB Consulting packages get you to production faster, help you tune performance in production, help you scale, and free you up to focus on your next release.

MongoDB Training helps you become a MongoDB expert, from design to operating mission-critical systems at scale. Whether you're a developer, DBA, or architect, we can make you better at MongoDB.

Resources

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

Case Studies (mongodb.com/customers)
Presentations (mongodb.com/presentations)
Free Online Training (university.mongodb.com)
Webinars and Events (mongodb.com/events)
Documentation (docs.mongodb.com)
MongoDB Enterprise Download (mongodb.com/download)
MongoDB Atlas database as a service for MongoDB (mongodb.com/cloud)
MongoDB Stitch backend as a service (mongodb.com/cloud/stitch)

mongoDB

US 866-237-8815 ▪ INTL +1-650-440-4474 ▪ info@mongodb.com