

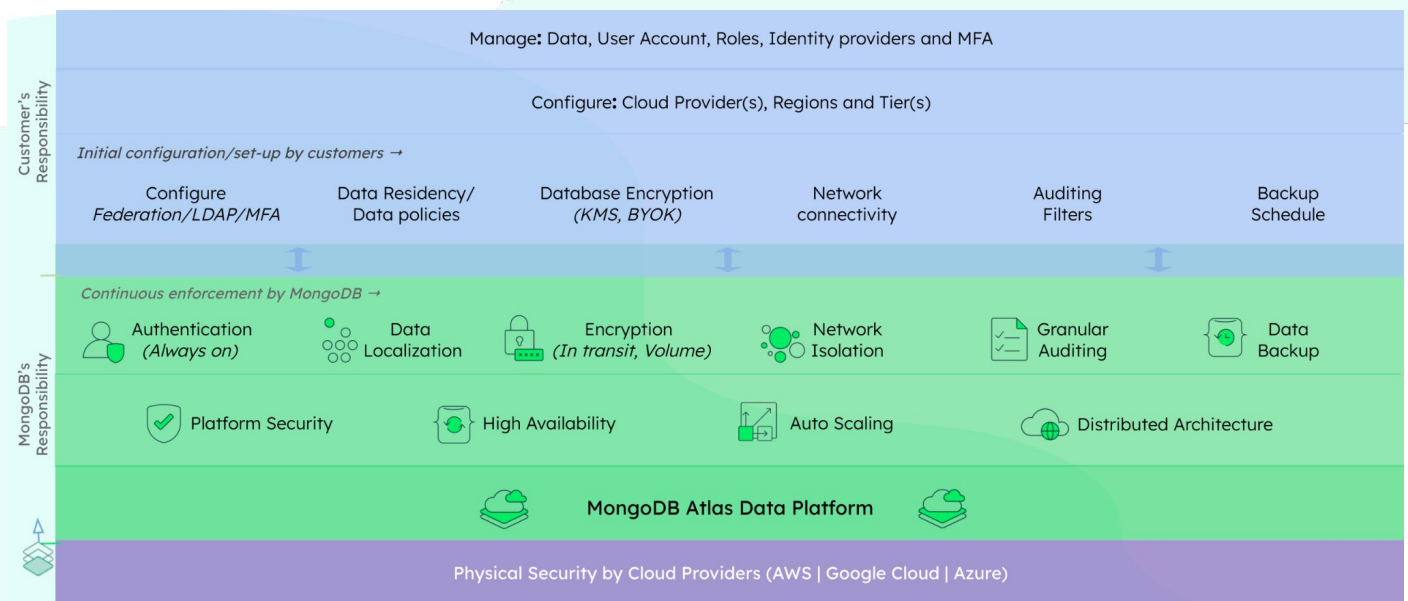


# MongoDB Atlas Data Platform Shared Responsibility Model

Cloud security is a shared responsibility between a customer and cloud provider. MongoDB strives to take the maximum burden of that responsibility, so customers can focus on application development and business requirements.

MongoDB Atlas has been designed with strong security defaults in mind so that the burden of securely using the service is minimized for the customer. These defaults include always-on authorization, authentication, encryption in transit, encryption at rest, and no access from the Internet by default. Additionally, MongoDB provides automated patching of the underlying infrastructure and MongoDB clusters with zero downtime.

Customers are responsible for creating users and roles to access Atlas, selecting cloud provider(s) and region(s) to create their clusters, and choosing the cluster type. They can optionally enable backup, configure advanced auditing, bring their own keys for storage engine encryption, and configure client-side field-level encryption.



## Cloud Advantages with MongoDB Atlas

MongoDB provides the industry's first application data platform that allows developers to accelerate and simplify how they build their applications, by providing key advantages –

- Leading document-based database built for rapid application development
- Strong security default settings, so customers can focus on the application and business needs
- Multi-cloud and self-managed data platform – extends across 3 major cloud providers, with the flexibility to deploy in 80+ regions
- Addresses a range of application use cases without adding complexity – full text search, live data analytics

# Shared Responsibility Model

## Customer

## MongoDB

← Framework

Develop

Protect







Detect

Recover

		Customer	MongoDB
	Cloud Infrastructure	<ul style="list-style-type: none"> <li>Select cloud provider, region &amp; tier</li> <li>Select MongoDB version and auto-scaling options</li> </ul>	<ul style="list-style-type: none"> <li>Provision and deploy cluster in dedicated VPC and firewalls</li> <li>Apply configuration changes without service disruption</li> </ul>
	Customer data, accounts and identities	<ul style="list-style-type: none"> <li>Provide and manage customer data</li> <li>Maintain user accounts and access continuity</li> </ul>	<ul style="list-style-type: none"> <li>Provide secure access to customer data</li> <li>Provide tools to upload/store data securely</li> </ul>
	Network isolation & connectivity	<ul style="list-style-type: none"> <li>Configure network connectivity; options include IP access list, VPC peering connections, private endpoints</li> </ul>	<ul style="list-style-type: none"> <li>Provision peering containers</li> <li>Provision private endpoint resources</li> <li>Only allow connections to the cluster from entries in a project's access list</li> </ul>
	Atlas Database/ Cluster access	<ul style="list-style-type: none"> <li>Configure user authentication</li> <li>Assign user and role privileges</li> <li>Manage certificate authority *</li> <li>Configure AWS IAM, LDAP integration *</li> <li>Configure Data API access keys</li> </ul>	<ul style="list-style-type: none"> <li>Maintain always-on authentication (SCRAM, x509 certificates)</li> <li>Provide always-on role-based access controls (RBAC) with predefined roles</li> <li>Provide audit log access</li> </ul>
	Atlas Console/ API access	<ul style="list-style-type: none"> <li>Manage access – users and roles</li> <li>Configure MFA and federated auth</li> <li>Configure API keys</li> </ul>	<ul style="list-style-type: none"> <li>Maintain always-on authentication</li> <li>Provide integrations interface to integrate with Identity providers, MFA tools</li> </ul>
	Data Encryption (in transit and at rest)	<ul style="list-style-type: none"> <li>Configure cloud provider Key Management System (KMS) *</li> <li>Set minimum TLS version</li> </ul>	<ul style="list-style-type: none"> <li>Encryption always on, in transit and at rest</li> <li>Ensure data is stored on encrypted storage volumes with cloud provider managed keys</li> <li>Encrypt data at rest using customer provided keys</li> </ul>
	Data Encryption (in use, BYOK)	<ul style="list-style-type: none"> <li>Configure client side field-level encryption *</li> <li>Configure cloud provider KMS *</li> </ul>	<ul style="list-style-type: none"> <li>Provide tools, drivers, and shared libraries for seamless field-level encryption</li> <li>Drivers to communicate with KMS</li> </ul>
	Granular auditing	<ul style="list-style-type: none"> <li>Enable granular database auditing</li> <li>Configure audit filter</li> </ul>	<ul style="list-style-type: none"> <li>Maintain database access history</li> <li>Security events in the activity feed</li> </ul>
	Data Locality	<ul style="list-style-type: none"> <li>Choose regions &amp; providers</li> <li>Understand and comply with data locality regulations</li> </ul>	<ul style="list-style-type: none"> <li>Support multiple regions and global clusters</li> <li>Ensure cloud snapshots for backup are located in chosen regions</li> </ul>
	Performance Troubleshooting	<ul style="list-style-type: none"> <li>Enable/disable performance advisor and query profiler</li> <li>Review and apply performance advisor recommendations</li> </ul>	<ul style="list-style-type: none"> <li>Automatically run query profiler and performance advisor</li> </ul>
	Security patches and maintenance	<ul style="list-style-type: none"> <li>Set maintenance window *</li> </ul>	<ul style="list-style-type: none"> <li>Apply minor version upgrades</li> <li>Apply security patches</li> </ul>
	Monitoring & Alerting	<ul style="list-style-type: none"> <li>Configure alert thresholds</li> <li>Enable real-time performance panel</li> </ul>	<ul style="list-style-type: none"> <li>Collect monitoring metrics</li> <li>Proactively monitor cluster health metrics</li> </ul>
	Backups	<ul style="list-style-type: none"> <li>Configure backup policy and retention</li> <li>Configure point in time restore</li> </ul>	<ul style="list-style-type: none"> <li>Operate backups according to policy</li> <li>Ensure backup retention according to policy</li> </ul>
	Online archive	<ul style="list-style-type: none"> <li>Enable automatic archival</li> <li>Configure archiving rules</li> <li>Configure query patterns</li> </ul>	<ul style="list-style-type: none"> <li>Provision archival storage and manage archival data format</li> <li>Ensure automatic scalability of Online Archive federated query engine</li> </ul>

# MongoDB's Responsibility in Securing the Application Data Platform

Developers should be able to focus on making sure applications serve customers well, instead of spending all their time in infrastructure security settings and controls. MongoDB strives to secure the data platform, so customers can focus on fulfilling their business requirements.

MongoDB's Responsibility in Securing Atlas		
Data Storage		<ul style="list-style-type: none"> <li>• Encryption at rest is always on                             <ul style="list-style-type: none"> <li>◦ Data always stored in encrypted storage volumes</li> </ul> </li> <li>• Integrate with AWS, Azure, and GCP key management system for database at-rest encryption</li> </ul>
Data Access and Control Plane Access		<ul style="list-style-type: none"> <li>• Authentication and Authorization is always on                             <ul style="list-style-type: none"> <li>◦ Provide SCRAM, x.509, LDAP, Federation, MFA tool integrations</li> <li>◦ Role-based access controls provided with predefined roles</li> </ul> </li> <li>• Encryption in transit is always on</li> <li>• Customer tenants are isolated</li> </ul>
Data Safety and Privacy		<ul style="list-style-type: none"> <li>• Independent verification of platform security, privacy, and compliance controls.                             <ul style="list-style-type: none"> <li>◦ ISO 27001, 27017, 27018, CSA STAR II, SOC 2, SOC2 + HITRUST mapping, PCI, HIPAA, VPAT</li> <li>◦ FedRAMP (Atlas for Government)</li> </ul> </li> </ul>
Platform Capabilities		<ul style="list-style-type: none"> <li>• Global cloud region availability (80+ regions) across AWS, Azure, &amp; Google Cloud, supporting data residency requirements</li> <li>• Always-on cloud user action and database authentication tracking</li> <li>• Availability and scalability of Data Lake federated query engine, Realm, Charts and Atlas Search components</li> </ul>
MongoDB Technical Services		<ul style="list-style-type: none"> <li>• MongoDB support has Service Level Agreements (SLAs) to ensure that support cases are prioritized based on severity and are handled in timely manner</li> <li>• Provide technical assistance on any issues when requested by customers, including -                             <ul style="list-style-type: none"> <li>◦ The MongoDB Atlas service control plane</li> <li>◦ MongoDB clusters managed by Atlas</li> <li>◦ Consultation on query performance or driver issues</li> </ul> </li> </ul>
MongoDB Professional Services		<ul style="list-style-type: none"> <li>• Provide consultation and act as advisors in areas including - :                             <ul style="list-style-type: none"> <li>◦ Schema design and query / index optimization</li> <li>◦ Infrastructure and architecture design</li> <li>◦ Integration with cloud provider and third party services</li> <li>◦ Data access layer code review</li> </ul> </li> </ul>



Customer responsible for initial configuration; ongoing responsibility is MongoDB's



Ongoing shared responsibility of customer and MongoDB

\* Optional configuration/setup by customers



Customer has ongoing responsibility; MongoDB provides tools and services



MongoDB's responsibility

## Resources

We are the MongoDB experts, with over 33K+ customers relying on our commercial products. We offer software and services to make your life easier. For more information, please visit [mongodb.com](https://mongodb.com) or contact us at [sales@mongodb.com](mailto:sales@mongodb.com).

- Documentation ([docs.mongodb.com](https://docs.mongodb.com))
- MongoDB Realm ([mongodb.com/realml](https://mongodb.com/realml))
- MongoDB Atlas ([mongodb.com/atlas](https://mongodb.com/atlas))
- Free online training ([university.mongodb.com](https://university.mongodb.com))
- MongoDB download ([mongodb.com/download](https://mongodb.com/download))
- Case studies ([mongodb.com/customers](https://mongodb.com/customers))
- Resources ([mongodb.com/resource-center](https://mongodb.com/resource-center))
- Trust center ([mongodb.com/cloud/trust](https://mongodb.com/cloud/trust))