



# Shared Responsibility in the Cloud

Who owns security in the cloud? In the shared responsibility model, everyone has a part to play.

Businesses are all in on the cloud. But they're not so sure about cloud security. Roles and responsibilities need to be defined. Only then can they be confident in their cloud workloads.

Before the cloud, businesses owned and managed their entire environment and were responsible for ensuring the security of all the assets under their control. Cloud security follows a different approach. Some responsibilities fall clearly on the business, some

on cloud providers, and some on the vendors of the cloud services being used. This is known as the shared responsibility model.

A shared responsibility model defines the roles you and your software vendors assume for security in the cloud. Different offerings use different models. There are currently three: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

## IaaS

Infrastructure is hosted within a cloud service provider's facility. Compute, storage, and networking are delivered to customers on demand while being fully managed by the service provider.

## PaaS

A cloud service provider hosts the hardware and software on its own infrastructure, allowing developers to focus on developing and running applications.

## SaaS

A ready-to-use, cloud-hosted application.

Roles and responsibilities for different cloud service models

	SaaS	PaaS	IaaS
Data			
Devices			
Accounts and Identities			
Applications			
Network Controls			
Operating System			
Physical Hosts			
Physical Network			
Physical Datacenter			



Customer  
Managed



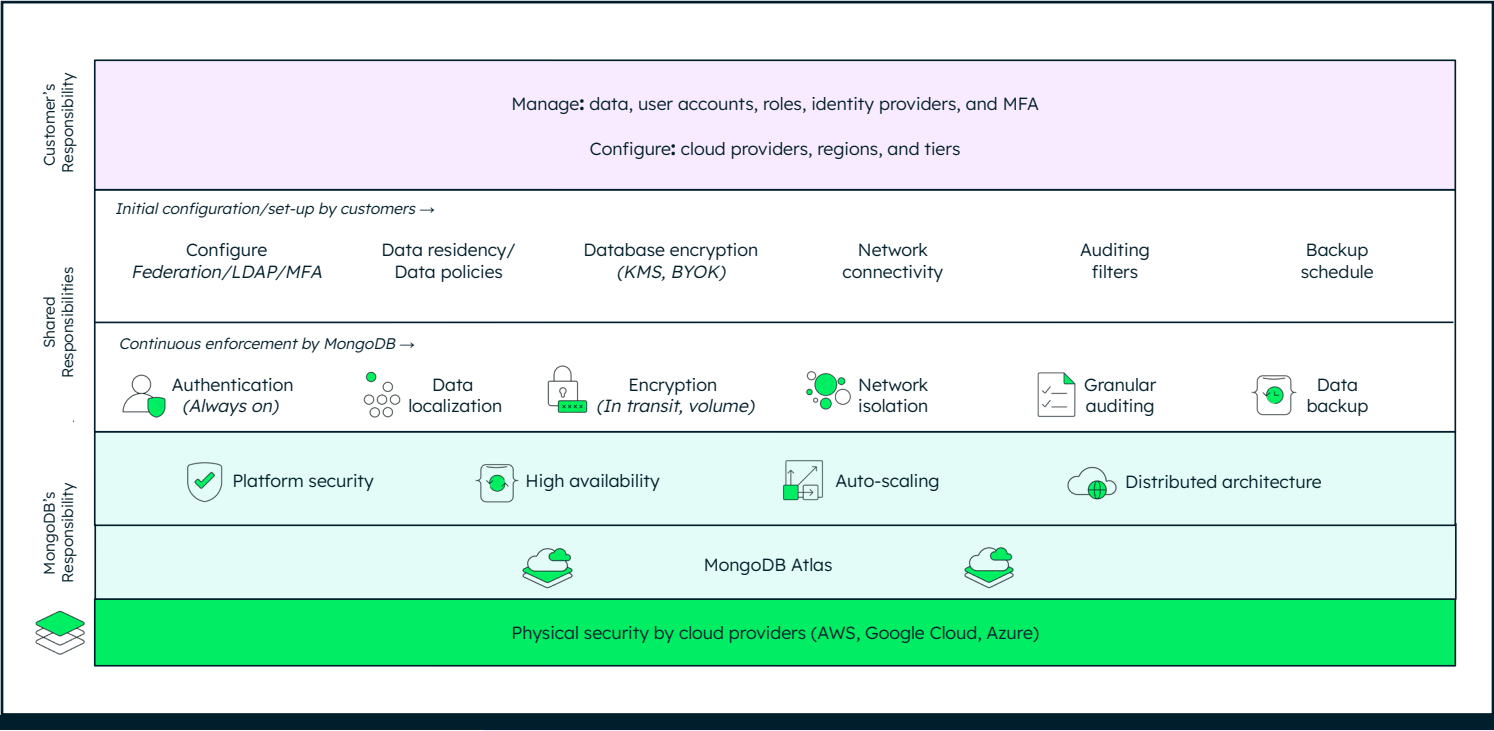
Vendor  
Managed



Shared

Shared responsibility recognizes that cloud vendors such as MongoDB must ensure the security and availability of their services and infrastructure, and that customers must take appropriate steps to protect the data they keep in the cloud. These are the prerequisites for cloud security and resilience.

## Security responsibilities in MongoDB Atlas



The MongoDB shared responsibility model applies to our SaaS database offering, MongoDB Atlas, and the services available in the platform.

The security defaults found in Atlas enable developers to be both agile and comfortable that risks are appropriately governed while using our services. Atlas gives developers the building blocks they need to move fast without having to worry about the minutiae of administrative security tasks. For a more detailed breakdown of shared responsibilities in MongoDB Atlas, download our [shared responsibility white paper](#).

To get started with MongoDB Atlas, sign up for a [free account](#) today. →

