Redis Cloud shared responsibility model

The security of all Redis Enterprise Cloud deployments is a shared responsibility. Redis, the public cloud providers (Amazon Web Services [AWS], Google Cloud Platform [GCP], and Microsoft Azure), and our customers all help ensure the security of these deployments.

Redis responsibility

Redis Enterprise Cloud’s offerings are managed by Redis and deployed on AWS, Azure, and Google Cloud infrastructure.

Redis is responsible for the software that runs Redis Enterprise Cloud. This includes the patching and maintenance of the operating systems that Redis is deployed on as well as the patching and maintenance of Redis Enterprise Cloud.

Cloud provider responsibility

The public cloud provider hosting your Redis Enterprise Cloud databases is responsible for the physical security of their data centers and the security of the network, storage, servers, and virtualization that form the core infrastructure of your deployment.

Amazon, Microsoft, and Google’s public clouds embrace a wide range of security best practices and compliance standards. Compliance information—including audits, attestations, and certifications about resources hosted—can be found in the following compliance pages:

- AWS Compliance
- GCP Compliance
- Azure Compliance

Customer responsibility

Customers are responsible for the security configurations in their Redis databases and the Redis Enterprise Cloud admin console. Customers must understand and implement the Redis Enterprise Cloud security features and best practices.

Customers are also responsible for the applications built on Redis and the data they store in Redis. Customers determine the cloud provider, region, and availability zone of their deployments.

Customers understand that Redis Enterprise Cloud Fixed plans (including Free) are deployed to multi-tenant infrastructure. Flexible and Annual plans are deployed to single-tenant infrastructure dedicated to one specific customer.

Updated: January 12, 2022