Amazon Shared Responsibility Model

Security and compliance are shared responsibilities between us and the customer. This shared model can help relieve a customer’s operational burden because we operate, manage, and control the components from the host operating system and virtualization layer down to the physical security of the facilities where the service operates. The customer is responsible for--and manages--the guest operating system (including updates and security patches) and other associated application software, in addition to the configuration of the AWS-provided security group firewall. Customers should carefully consider the services that they choose because their responsibilities will vary depending on the services that they use, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. This differentiation of responsibility is commonly referred to as Security *of* the Cloud versus Security *in* the Cloud.

AWS responsibility

*Security of the Cloud:* We are responsible for protecting the infrastructure that runs all of the services that are offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility

*Security in the Cloud:* Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.

AWS uses a pay-as-you-go pricing model. This allows you to easily adapt to changing business needs without over-committing budgets, and it improves your responsiveness to changes. General pricing information can be found at: <https://aws.amazon.com/pricing/>.

As mentioned in the segment on Regions, AWS pricing varies by Region. When you explore costs, make sure that you select the appropriate Region.

Pricing for each service can be found on the AWS website under the specific service listing. For example, Amazon EC2 pricing can be found at: <https://aws.amazon.com/ec2/pricing/>. The price for Amazon S3 can be found at: <https://aws.amazon.com/s3/pricing/>.

## AWS Pricing Calculator

AWS has announced a new pricing tool, the [AWS Pricing Calculator](https://calculator.aws/#/). This new tool, which is currently in beta, can be used to calculate Amazon EC2 and Amazon EBS pricing. For further information about this tool, see [this blog post](https://aws.amazon.com/blogs/aws/check-it-out-new-aws-pricing-calculator-for-ec2-and-ebs/). For other services, you can use the [AWS Simple Monthly Calculator.](https://calculator.s3.amazonaws.com/index.html)

## AWS Cost Explorer

[AWS Cost Explorer](https://aws.amazon.com/aws-cost-management/aws-cost-explorer/) lets you visualize, understand, and manage your AWS costs and usage over time. You can create custom reports (including charts and tabular data) that analyze cost and usage data, both at a high level (e.g., total costs and usage across all accounts) and for highly specific requests (e.g., m2.2xlarge costs within account Y that are tagged**project: secret Project**).

## AWS Trusted Advisor

[AWS Trusted Advisor](https://aws.amazon.com/premiumsupport/trustedadvisor/) is an online resource to help you reduce costs, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real-time guidance to help you provision your resources by following our best practices.