AWS Backup

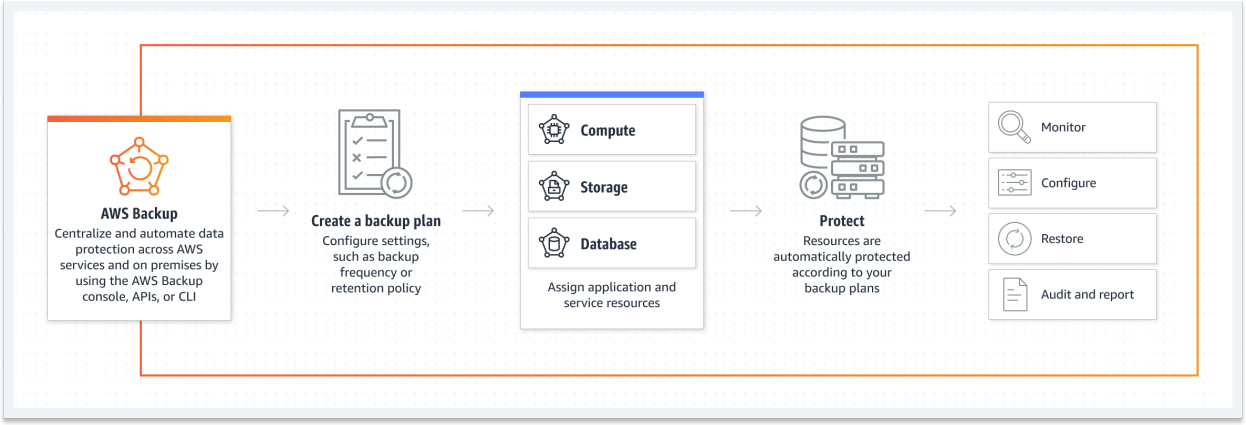
No business is completely immune from the loss of information. Breakdown of hardware, malware, hacking, unwanted intrusion and accidental deletion are just some of the ways in which data relating to business operations may be lost. Having backups of said data therefore may be a desirable thing for many businesses and is in fact, a necessity by law in many countries.

In the early days of cloud computing, companies had to manually script backup jobs, store data offsite, and frequently monitor backup operations, tasks that are prone to error. As cloud usage grew, these processes became an increasingly significant (and also often increasingly tedious) task. It was in this environment that AWS first launched **AWS Backup** in January 2019, offering an easy-to-use fully managed backup service that centralizes and automates the backup of data stored within a group of select AWS services which are listed below:

- **Amazon EC2** / **Amazon EBS**
- **Amazon S3**
- **Amazon RDS** (including all DB engines like **Aurora** and **DynamoDB**)
- **Amazon DocumentDB** / **Amazon Neptune**
- **Amazon EFS** / **Amazon FSx** (including Lustre and Windows File Server)
- **AWS Storage Gateway** (Volume Gateway)
- **Amazon Redshift**
- **Amazon Timestream**
- **AWS CloudFormation**
- **VMWare Cloud on AWS**

Note that AWS Backup is limited to the above set of services, and data stored in any other AWS offering must either be manually backed up or backed up using a third party tool.

AWS Backup also allows us to create data backup plans for the mentioned services, define backup policies for the data within them, automate backup scheduling, manage backup retention periods and store said backups across both multiple AWS regions and multiple AWS accounts. An infographic on how AWS Backup works is given below:



Source: AWS

The service definitely simplifies a myriad of data protection tasks and helps companies ensure the resilience of their data, meet regulatory compliances and perform recovery tasks without the need for custom scripting and/or manual intervention and has led to AWS Backup becoming the somewhat default option for backing up data related to AWS-specific resources. Implementations of the **Backup and Restore** method of disaster recovery mentioned in the Databases section for example, are often based on the AWS Backup service.