Database Encryption

Encryption at rest and in transit

Amazon RDS allows you to encrypt your databases using keys you manage through AWS Key Management Service (KMS). On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots.

Amazon RDS supports Transparent Data Encryption in SQL Server and Oracle. Transparent Data Encryption in Oracle is integrated with AWS CloudHSM, which allows you to securely generate, store, and manage your cryptographic keys in single-tenant Hardware Security Module (HSM) appliances within the AWS cloud.

Amazon RDS supports the use of SSL to secure data in transit.

Network isolation

AWS recommends that you run your database instances in Amazon VPC, which allows you isolate your database in your own virtual network and connect to your on-premises IT infrastructure using industry-standard encrypted IPsec VPNs. You can configure firewall settings and control network access to your database instances.

Resource-level permissions

Amazon RDS is integrated with AWS Identity and Access Management (IAM) and provides you the ability to control the actions that your AWS IAM users and groups can take on specific Amazon RDS resources, from database instances through snapshots, parameter groups, and option groups. You can also tag your Amazon RDS resources and control the actions that your IAM users and groups can take on groups of resources that have the same tag and associated value. For example, you can configure your IAM rules to ensure developers are able to modify "Development" database instances, but only Database Administrators can make changes to "Production" database

Information on Amazon RDS Security can be found at https://aws.amazon.com/rds/features/#security