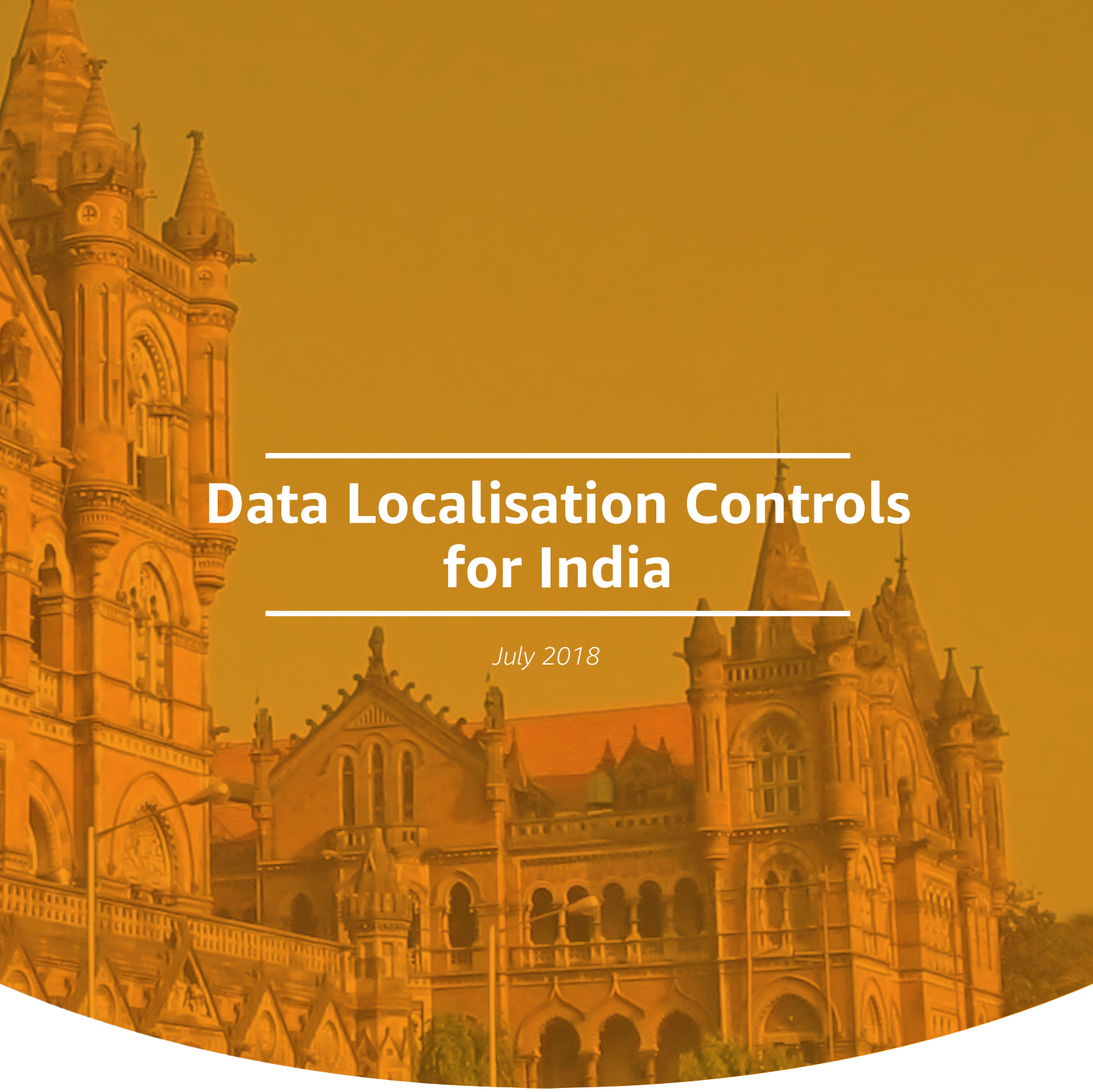

Data Localisation Controls for India

July 2018

aws

[Resource Guide]

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Introduction

India is going through an unprecedented transformation as government, regulators, financial institutions, technology companies, small-to-medium businesses, and enterprises collaborate realize the vision of Digital India. From time to time there may be a regulatory requirement to store and/or process data within India. This document details how AWS customers can use technical and non-technical controls to store and/or process their content within India.

AWS Regions: Where will content be stored?

The AWS Cloud infrastructure[1] is built around Regions and Availability Zones (AZs). AWS Regions provide multiple, physically separated and isolated Availability Zones, which are connected with low latency, high throughput, and highly redundant networking. These Availability Zones offer AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures. As mentioned, Availability Zones are connected to each other with fast, private fiber-optic networking, enabling customers to easily architect applications that automatically fail-over between Availability Zones without interruption.

AWS customers have access to a number of AWS Regions around the world, including an **Asia Pacific (Mumbai) Region** within India. The AWS Asia Pacific (Mumbai) Region is designed and built to meet rigorous compliance standards globally, providing high levels of security for all AWS customers and includes certification with ISO27001, ISO27017, ISO27018 and many more.

AWS customers choose the AWS Region in which their content will be processed and stored. AWS customers in India can choose to subscribe for AWS services exclusively in one AWS Region such as the Asia Pacific (Mumbai) Region and store their content within India, if this is their preferred location. AWS customers have the option to choose and change the AWS Region anytime while using AWS services.

How can customers select their Region(s)?

When using the AWS management console, or placing a request through an AWS Application Programming Interface (API), the customer identifies the particular AWS Region(s) where they wish to use AWS services.

Customers can also prescribe the AWS Region to be used for their compute resources by taking advantage of the Amazon Virtual Private Cloud (VPC) capability. Amazon VPC lets the customer provision a private, isolated section of the AWS Cloud where the customer can launch AWS resources in a virtual network that the customer defines. With Amazon VPC, customers can define a virtual network topology that closely resembles a traditional network that might operate in their own data center.

1 https://aws.amazon.com/about-aws/global-infrastructure/

Any compute and other resources launched by the customer into the VPC will be located in the AWS Region designated by the customer. For example, by creating a VPC in the Asia Pacific (Mumbai) Region all compute resources launched into that VPC would only reside in the Asia Pacific (Mumbai) Region.

AWS' Commitments

Customers always retain control of which AWS Region(s) are used to store and process content. AWS customers may specify the AWS Region(s) in which their content will be stored. AWS only stores and processes each customers' content in the AWS Region(s), and using the services, chosen by the customer, and otherwise will not move customer content without the customer's consent, except as legally required. AWS is vigilant about customers' security and does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or court order, or as is otherwise required by applicable law. Additionally, our practice is to notify customers where practicable before disclosing their content so that they can seek protection from disclosure, unless we are legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. For additional information, please visit the Amazon Information Requests Portal online.

Technical Controls - Preventative

AWS provides a wide selection of security tools and features that customers can use to design, implement, and operate their own secure AWS environment.

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM)[2] enables customers to manage access to AWS services and resources securely. Using IAM, customers can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

AWS IAM supports conditions that lets customers specify special circumstances under which the policy grants or denies permission. AWS allows customers to control access to specific AWS regions (Mumbai for example) by using the IAM "Requested Region" condition.

For example, to deny access to AWS services that are not in the Mumbai (ap-south-1) Region[3], customers can use the global condition key aws:RequestedRegion in an IAM policy attached to users and roles. This condition can be used in conjunction with other IAM access control permissions. When a request is made, the AWS service decides whether a given request should be allowed or denied. An explicit deny overrides any allows, hence it would restrict access to the Mumbai region only. For example, the following IAM policy restricts access to the AWS Region in Mumbai:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Deny",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "StringNotEquals": {
               "aws:RequestedRegion": "ap-south-1"
            }
         }
      }
   ]
}
```

For more information on the requested region IAM condition, see https://aws.amazon.com/blogs/security/easier-way-to-control-access-to-aws-regions-using-iam-policies/.

2 https://aws.amazon.com/iam/
3 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-available-regions

Technical Controls – Detective

Customers can use detective controls to identify a potential security threat or incident. They are an essential part of governance frameworks and can be used to support a quality process, a legal or compliance obligation, and threat identification and response efforts. AWS provides a wide selection of tools and features that customers can use to implement detective controls.

AWS CloudTrail

AWS CloudTrail[4] is a service that enables governance, compliance, and audit of customers AWS account. With CloudTrail, customers can log, continuously monitor, and retain account activity related to actions across their AWS account. CloudTrail provides event history of customer's account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. Customers can also configure CloudTrail to send events to Amazon CloudWatch Logs5 (CloudWatch Logs) for monitoring.

Amazon CloudWatch

CloudWatch Logs[5] can be used to detect if resources like EC2 and S3 are being created outside of the desired AWS Region. Customers can create CloudWatch metric filter and alarm to detect and notify if the EC2 instance or S3 bucket is created outside of a desired AWS Region. CloudWatch offers the capability to send notifications, using Amazon Simple Notification Service (SNS)[6], to assigned individuals via email.

Amazon GuardDuty

Amazon GuardDuty[7] is a managed threat detection service that continuously monitors for malicious or unauthorized behaviour to help customers protect their AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise.

GuardDuty can detect signs of account compromise, such as access of AWS resources from an unusual geo-location. GuardDuty gives customers accurate threat detection of account compromise, which can be particularly difficult to detect if they are not continuously monitoring for factors in near real-time. With one-click in the AWS Management Console or a single API call, customers can enable Amazon GuardDuty on a single account.

4 https://aws.amazon.com/cloudtrail/
5 https://aws.amazon.com/cloudwatch/details/
6 https://aws.amazon.com/sns/
7 https://aws.amazon.com/guardduty/

Conclusion

Customers in India can use the Asia Pacific (Mumbai) Region to meet their data localization requirements. AWS also provides both Preventive and Detective technical controls to help customers ensure only the Asia Pacific (Mumbai) Region is used and notify them of any exceptions. Lastly, AWS provides contractual assurances to its customers by committing that it will not move customer content from the AWS Region(s) selected by the customer without their consent, except as legally required.

Document Revisions

Date	Description
July 2018	First publication.