Barracuda Cloud Archiving Service

Data Protection and Security

TABLE OF CONTENTS

Overview 3

1. Deployment Model 3

1.1 Barracuda Cloud Archiving Service Deployment Model 3

2. Product Security 3

2.1 Barracuda Cloud Archiving Service Access Controls 3

2.2 Data Transmission and Storage 3

3. Data Center Location 3

3.1 Data Locations 3

Overview

This document describes product security measures and data storage policies that are specific to the Barracuda Cloud Archiving Service.

1. Deployment Model

1.1 Barracuda Cloud Archiving Service Deployment Model

The Barracuda Cloud Archiving Service utilizes Barracuda's cloud infrastructure and delivered to customers in a Software-as-a-Service (SaaS) model.

2. Product Security

2.1 Barracuda Cloud Archiving Service Access Controls

The Barracuda Cloud Archiving Service provides the following features to control access to the product:

- Customers can configure multiple user roles to determine the level of access to the functionality of the Barracuda Cloud Archiving Service. More information about this feature is available here: https://campus.barracuda.com/product/cloudarchiving/doc/46891920/how-to-manage-user-accounts-and-roles
- Customers use the Barracuda Cloud Control interface to access the Barracuda Cloud Archiving Service. Barracuda Cloud Control supports Multifactor Authentication. More information about this feature is available here: https://campus.barracuda.com/product/cloudcontrol/doc/69960137/multi-factor-authentication-in-barracuda-cloud-control

All data replicated to Barracuda Cloud is encrypted using AES 256-bit encryption. These emails are written into storage at Barracuda data centers in an encrypted state and remain encrypted until requested for retrieval.

2.2 Data Transmission and Storage

Customers can transmit data for archiving with the Barracuda Cloud Archiving Service in multiple ways:

- Email data can be transmitted to the Barracuda Cloud Archiving Service using SMTP and can be secured with TLS encryption. This configuration is controlled by the customer.
- Customers can configure the Barracuda Cloud Archiving Service to remotely retrieve data from Microsoft Exchange servers and Microsoft Office 365. These connections are secured using HTTPS.
- Customers can upload PST files to Barracuda Cloud Archiving Service. These connections are secured using HTTPS or Secure FTP.
- Customers can upload PST files to Barracuda Cloud Archiving Service using Barracuda PST Enterprise. These connections are secured using HTTPS or Secure FTP.

3. Data Center Location

3.1 Data Locations

Barracuda maintains a network of datacenters by geographic location around the globe and requires that each meet defined security requirements. The cloud infrastructure for Barracuda Cloud Archiving Service is deployed in the following geographical regions. Customer data is stored in the respective region where the customer is located. Any transfer of customer data outside the European Union will be done in compliance with the GDPR and applicable local privacy laws.

Barracuda's Standard Contractual Clauses are located within our DPA at the following address:
https://www.barracuda.com/company/legal/trust-center

- United States of America: infrastructure deploys in this region stores data for all customers in the United States, as well as any region not specifically configured to send data to an available local location.
- United Kingdom: stores data for all customers in the United Kingdom, Europe, Middle East and Africa.
- Canada: stores data for all customers in Canada.
- Germany: stores data for all customers in Germany, Austria, Belgium, Netherlands, and Luxembourg.
- Australia: stores data for all customers in Australia.