Barracuda Message Archiver

Data Protection and Security

TABLE OF CONTENTS

Overview

This document describes product security measures and data storage policies that are specific to the Barracuda Message Archiver.

1. Product Security

1.1 Barracuda Message Archiver Appliance Security

The Barracuda Message Archiver is typically deployed behind the customer's corporate firewall and is protected by the same security that the customer uses to protect primary data sources. There are several ways the Barracuda Message Archiver can be accessed locally, and each is dedicated to a specific function:

- The local web interface provides access for appliance configuration and all product functionality.
- A monitor and keyboard provide access to the terminal configuration for network setup and troubleshooting. Command-line access to the unit is disabled locally.

The Barracuda Message Archiver runs on a hardened Linux kernel. In the event that a security flaw is discovered, updates are pushed out to Message Archivers in a security definition administered by Barracuda.

2. Access Control and Data Center Location

2.1 Barracuda Message Archiver Access Controls

The Barracuda Message Archiver 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 Message Archiver appliance. More information about this feature is available here: https://campus.barracuda.com/product/messagearchiver/doc/2490376/how-to-manage-user-accounts-and-roles
- Customers that replicate Barracuda Message Archiver data to the Barracuda Cloud will use the Barracuda Cloud Control interface to access their cloud data. The 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
- IP login restrictions can be set for administrative users of the Barracuda Message Archiver appliance. Those restrictions prevent access to the web user interface from an IP address outside the range specified. Video-monitored access points

For Barracuda Message Archiver units that are configured to replicate data to the Barracuda Cloud, emails are AES 256-bit symmetrically encrypted before transmission to the Barracuda Cloud. These emails are written into storage at Barracuda data centers in an encrypted state and remain encrypted until requested for retrieval.

2.2 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 Message Archiver 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.