Barracuda Backup
Data Protection and Security
# TABLE OF CONTENTS

**Overview** ........................................................................................................................................... 3

1. **Product Security** .................................................................................................................................... 3
   1.1 Barracuda Backup Appliance (Hardware and Virtual) Security ................................................................. 3

2. **Access Control, Data Transmission and Data Storage Data Center Location** ........................................... 3
   2.1 Barracuda Backup Access Controls ........................................................................................................... 3
   2.2 Data Transmission and Storage ................................................................................................................... 4

3. **Data Center Location** ................................................................................................................................ 4
   3.1 Data Locations ............................................................................................................................................ 4
Overview
This document describes product security measures and data storage policies that are specific to the Barracuda Backup product.

1. Product Security

1.1 Barracuda Backup Appliance (Hardware and Virtual) Security
Barracuda Backup appliances are typically deployed as cloud-connected appliances, enabling customers to remotely manage their Barracuda Backup appliances from a web browser without requiring a physical connection to the appliance.

The Barracuda Backup appliance 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. Barracuda Backup appliances support encryption of data at rest via AES 256-bit encryption and is enabled by default on all Barracuda Backup models (190 – 1191).

Communication between the appliance and Barracuda Cloud utilizes a 256-bit encrypted VPN tunnel for administration and backup configuration, and a "lifeline" status check that runs over https port 443, which provides details of the appliance status in the event the tunnel is down.

There are several ways the Barracuda Backup appliance can be accessed locally:

- The local web interface provides access for basic system maintenance, and provides restore and reporting 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 Backup appliance runs on a hardened Linux kernel. In the event that a security flaw is discovered, updates are pushed out to cloud-connected Backup appliances in a security definition administered by Barracuda.

2. Access Control, Data Transmission and Data Storage

Data Center Location

2.1 Barracuda Backup Access Controls
Barracuda Backup provides the following features to give customers additional flexibility to limit access to their Barracuda Backup appliance and account when operating in cloud-connected mode:

- IP login restrictions can be set for each user who has access to the Barracuda Backup account. Those restrictions prevent access to the hosted web user interface from an IP address outside the range specified.
- Customers can enable an option in the web user interface which provides the ability to grant or deny Technical Support remote access to a backup appliance. This will prevent access to both the command line and to the user interface. This tool does not lock out the Barracuda Cloud engineering team.
2.2 Data Transmission and Storage
In order to perform deduplication, Barracuda Backup breaks files down into parts that are variable in size and fingerprints those parts for analysis and comparison. Before transmission to the Barracuda Cloud or a secondary Barracuda Backup appliance, those parts are AES 256-bit symmetrically encrypted and AES keys are securely transmitted. These parts are written into storage at the Barracuda Cloud or a secondary Barracuda Backup appliance in an encrypted state and remain encrypted until requested for restore. When replication is active, the process of replicating data begins immediately after data is written to disk on a Barracuda Backup appliance and runs continuously.

3. Data Center Location

3.1 Data Locations
Barracuda maintains a network of datacenters by geographic location around the globe and requires that each meets defined security requirements. The cloud infrastructure for Barracuda Backup 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

Americas:
- Microsoft Azure Region - East US 2 (Virginia)
- Microsoft Azure Region - Canada East (Quebec City)

EMEA:
- Microsoft Azure Region - UK South (London)
- Microsoft Azure Region - Germany West Central (Frankfurt)

APAC:
- Microsoft Azure Region - Australia East (New South Wales)
- Microsoft Azure Region - Japan East (Tokyo, Saitama)